CHAPTER 13: OVERVIEW OF DISASTER RECOVERY OPERATIONS ................................. 269
The Failover Test Operation ................................................................. 269
The Move Operation ........................................................................... 270
The Failover Operation ................................................................. 270

CHAPTER 12: ADVANCED SITE CONFIGURATION ............................................. 258
Site Settings ....................................................................................... 258
  Editing Information About a Site ...................................................... 260
  Defining Performance and Throttling ............................................. 261
  Defining Site Policies ...................................................................... 262
  Configuring Email Settings ............................................................. 263
  Defining Resource Report Sampling Period .................................. 264
  Reviewing Supported Host Versions ............................................. 265
Seeing What Is Licensed ................................................................. 265
Submitting a Support Ticket ............................................................ 266
About Zerto Virtual Replication .......................................................... 267

CHAPTER 11: MANAGING A ZERTO VIRTUAL MANAGER ............................... 252
Check Connectivity Between Zerto Virtual Replication Components .... 252
Reconfiguring the Zerto Virtual Manager Setup ................................. 253
Replacing the SSL Certificate ............................................................. 256
Pair to Another Site and Unpair Sites ................................................. 256

CHAPTER 10: MANAGING VRAS .......................................................... 241
Installing a VRA .................................................................................. 242
Upgrading VRAs ................................................................................ 245
Editing VRA Settings ......................................................................... 246
Editing the VRA Connection Method or Password ................................ 247
Changing a Recovery VRA ................................................................. 248
Uninstalling VRAs ............................................................................. 249
Handling a VRA in an Error State (Ghost VRA) ................................ 249
Managing Protection During VMware Host Maintenance .................... 250
Managing Protection When Moving a Host to a Different Cluster ......... 251
Support for VMware Virtual Update Manager (VUM) .......................... 251

Exporting and Importing VPG Definitions ........................................ 230
VPG Statuses and Synchronization Triggers ..................................... 232
  VPG Statuses ................................................................................ 232
  VPG Synchronization Triggers ....................................................... 238
Managing Protection When the Recovery Datastore Will Be Unavailable (Datastore Maintenance) ................................................... 239
Modifying a Protected RDM Volume ............................................... 221
Pausing and Resuming the Protection of a VPG ................................. 221
Forcing the Synchronization of a VPG ............................................. 222
Handling a VPG in an Error State .................................................... 222
Deleting a VPG .................................................................................. 223
  Deleting a VPG When the Status is Deleting .................................. 223
Running an Unscheduled Offsite Backup ......................................... 223
Ensuring Application Consistency – Checkpoints ............................... 224
  Adding a Checkpoint to a VPG to Identify a Key Point .................... 225
Running Scripts Before or After Recovering a VPG ............................ 225
  Creating a Script ............................................................................. 227
  Example Scripts ............................................................................. 228

Defining Resource Report Sampling Period .................................. 264
Reviewing Supported Host Versions ................................................. 265
Seeing What Is Licensed ................................................................. 265
Submitting a Support Ticket ............................................................ 266
About Zerto Virtual Replication .......................................................... 267

CHAPTER 12: ADVANCED SITE CONFIGURATION ............................................. 258
Site Settings ....................................................................................... 258
  Editing Information About a Site ...................................................... 260
  Defining Performance and Throttling ............................................. 261
  Defining Site Policies ...................................................................... 262
  Configuring Email Settings ............................................................. 263
  Defining Resource Report Sampling Period .................................. 264
  Reviewing Supported Host Versions ............................................. 265
Seeing What Is Licensed ................................................................. 265
Submitting a Support Ticket ............................................................ 266
About Zerto Virtual Replication .......................................................... 267

CHAPTER 13: OVERVIEW OF DISASTER RECOVERY OPERATIONS ................................. 269
The Failover Test Operation ............................................................ 269
The Move Operation ........................................................................... 270
The Failover Operation ................................................................. 270
CHAPTER 25: GLOSSARY ................................................................. 396
Zerto Virtual Replication provides a business continuity (BC) and disaster recovery (DR) solution in a virtual environment, providing near real-time replication, with write-order fidelity, with minimal impact on product workloads. Fully automated orchestration delivers failover and failback in one click. Non-disruptive disaster recovery testing gives you confidence that your DR solution will work predictably and consistently. Protection groups ensure that all virtual machines that comprise an application are protected in the exact same manner no matter where they are in the environment.

With support for different hypervisors, such as vSphere or Hyper-V, workloads can be protected, migrated, and recovered, either within the same hypervisor environment or across hypervisor environments.

This guide describes how to configure and manage Zerto Virtual Replication to implement business continuity and disaster recovery (DR) solutions in a VMware, Hyper-V, AWS, Azure or mixed environments.

**Intended Audience**

This guide is for the use of experienced VMware administrators.

**Overview of Content in This Guide**

This guide contains the following chapters:

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction to Zerto Virtual Replication</td>
<td>Describes the underlying concepts and architecture of Zerto Virtual Replication.</td>
</tr>
<tr>
<td>2</td>
<td>Accessing the Zerto User Interface</td>
<td>Describes how to access the Zerto User Interface.</td>
</tr>
<tr>
<td>3</td>
<td>Initial Site Configuration</td>
<td>Describes how to configure Zerto Virtual Replication.</td>
</tr>
<tr>
<td>4</td>
<td>Overview of Recovery Flows</td>
<td>Describes disaster recovery and offsite backup flows from the initial protection to the recovery of virtual machines. It also describes, at a high level, the file level recovery process.</td>
</tr>
<tr>
<td>5</td>
<td>Introduction to Protecting Virtual Machines</td>
<td>Describes how to set up protection for virtual machines.</td>
</tr>
<tr>
<td>6</td>
<td>Protecting Virtual Machines from a vCenter Server</td>
<td>Describes how to protect virtual machines from a vCenter Server to a vCenter, Hyper-V host, Azure or to AWS.</td>
</tr>
<tr>
<td>7</td>
<td>Protecting Virtual Machines to and From vCloud Director</td>
<td>Describes how to protect virtual machines from a vCloud Director to a vCloud Director, vCenter Server, Hyper-V host, Azure or to AWS.</td>
</tr>
<tr>
<td>8</td>
<td>Monitoring Zerto Virtual Replication</td>
<td>Describes the different ways of monitoring the protected virtual machines and the protection and recovery sites.</td>
</tr>
<tr>
<td>9</td>
<td>Managing VPGs</td>
<td>Describes the processes available to manage VPGs using Zerto Virtual Replication.</td>
</tr>
<tr>
<td>10</td>
<td>Managing VRAs</td>
<td>Describes the processes available to manage VRAs using Zerto Virtual Replication.</td>
</tr>
<tr>
<td>11</td>
<td>Managing a Zerto Virtual Manager</td>
<td>Describes various management activities performed by Zerto Virtual Replication.</td>
</tr>
<tr>
<td>12</td>
<td>Advanced Site Configuration</td>
<td>Describes advanced configuration for Zerto Virtual Replication.</td>
</tr>
<tr>
<td>13</td>
<td>Overview of Disaster Recovery Operations</td>
<td>Describes the available recovery procedures and when they are used.</td>
</tr>
</tbody>
</table>
Support and Feedback

Please send suggestions to improve the documentation to Zerto support.

<table>
<thead>
<tr>
<th>CHAPTER</th>
<th>TITLE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>14</td>
<td>Testing Recovery</td>
<td>Describes how to test recovery to ensure the results you want.</td>
</tr>
<tr>
<td>15</td>
<td>Migrating a VPG to a Recovery Site</td>
<td>Describes the process of migrating protected virtual machines from the protected site to the recovery site.</td>
</tr>
<tr>
<td>19</td>
<td>Recovering Files and Folders</td>
<td>Describes the process of restoring files and folders from the recovery site.</td>
</tr>
<tr>
<td>17</td>
<td>Managing Failover</td>
<td>Describes the process of recovery from the protected site to the recovery site.</td>
</tr>
<tr>
<td>18</td>
<td>Cloning a VPG to the Recovery Site</td>
<td>Describes the process of cloning protected virtual machines from the protected site to the recovery site.</td>
</tr>
<tr>
<td>20</td>
<td>Restoring an Offsite Backup</td>
<td>Describes the process of restoring an offsite backup from a repository.</td>
</tr>
<tr>
<td>21</td>
<td>Zerto Virtual Replication Reports</td>
<td>Describes the reporting and monitoring capabilities available with Zerto Virtual Replication.</td>
</tr>
<tr>
<td>22</td>
<td>Troubleshooting</td>
<td>Describes how to resolve problems, including generating logs.</td>
</tr>
<tr>
<td>23</td>
<td>Zerto Virtual Replication and VMware Features</td>
<td>Describes the interaction between Zerto Virtual Replication and commonly used VMware features such as vMotion, DRS, and HA.</td>
</tr>
<tr>
<td>24</td>
<td>The Zerto Virtual Manager User Interface</td>
<td>Describes the Zerto User Interface.</td>
</tr>
<tr>
<td>25</td>
<td>Glossary</td>
<td>A glossary of terms used throughout Zerto Virtual Replication.</td>
</tr>
</tbody>
</table>
CHAPTER 1: INTRODUCTION TO ZERTO VIRTUAL REPLICATION

Disaster recovery is the process of preparing for recovery or continuation of IT processing tasks that support critical business processes in the event of a threat to the IT infrastructure. Zerto Offsite Backup is the additional process of enabling recovery of IT processing tasks after an extended period. This chapter describes Zerto Virtual Replication general concepts to enable replication and recovery in a virtual environment.

The following topics are described in this chapter:
- “What is Zerto Virtual Replication?”
- “Zerto Virtual Replication Architecture”, on page 12
- “How Zerto Virtual Replication Recovery Works”, on page 13
- “Zerto Analytics - Overview”, on page 13
- “Benefits of Using Zerto Virtual Replication”, on page 16

What is Zerto Virtual Replication?

Zerto Virtual Replication provides a business continuity (BC) and disaster recovery (DR) solution in a virtual environment, providing near real-time replication, with write-order fidelity, with minimal impact on product workloads. Fully automated orchestration delivers failover, failback, and reverse protection in one click. Non-disruptive disaster recovery testing gives you confidence that your DR solution will work predictably and consistently. Consistency groups ensure all virtual machines that comprise an application are protected in the exact same manner no matter where they are in the environment.

With support for different hypervisors, such as vSphere or Hyper-V, workloads can be protected, migrated, and recovered, either within the same hypervisor environment or across hypervisor environments.

Zerto Virtual Replication is installed in both the protected and the recovery sites. The disaster recovery across these sites is managed by a browser-based user interface. Managing Zerto Virtual Replication is also possible programmatically, either via a set of RESTful APIs or PowerShell cmdlets.

Recovery that does rely on native replication functionality, such as recovery available with Microsoft Active Directory or SQL Server, can also be replicated using Zerto Virtual Replication, and whether the native replication functionality is used or not is determined by site considerations, such as increased complexity of having multiple points of control and possible additional costs incurred when using vendor native replication.

You configure replication by first pairing the site with virtual machines to be protected with a recovery site. You then define what virtual machines you want replicated in consistency groups, where the virtual machines in a group comprise the application and data you want to protect. You can group different virtual machines together or keep them separate. By creating different replication groups, you can customize the replication requirements for each group to better optimize the recovery plan.

Disaster recovery is based on the premise that you will want to recover with a minimum RPO. However, to enable full recovery in cases such as virus attacks, Zerto Virtual Replication provides the ability to recover to a point in time up to 30 days prior to the disaster. When recovery earlier than 30 days is required, Zerto Virtual Replication provides an extended recovery, using an offsite backup mechanism that enables you to recover to a recovery site based on a daily or weekly backup going as far back as a year. The majority of the processing for both disaster recovery and extended recovery is done at the recovery site, minimizing the impact on the production site.
Zerto Virtual Replication Architecture

Zerto Virtual Replication provides disaster recovery between hypervisors such as VMware ESX/ESXi hosts managed by vCenter Servers and Microsoft Hyper-V hosts managed by SCVMM. In addition, you can protect virtual machines in these environments to a public cloud, such as Amazon Web Services.

When Zerto Virtual Replication is installed to work with a hypervisor it comprises the following components:

**Zerto Virtual Manager (ZVM):** A Windows service that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the hypervisor management user interface, such as vCenter Server or Microsoft SCVMM, to get the inventory of VMs, disks, networks, hosts, etc. and then the Zerto User Interface manages this protection. The ZVM also monitors changes in the hypervisor environment and responds accordingly. For example, a VMware vMotion operation, or Microsoft Live Migration of a protected VM from one host to another is intercepted by the ZVM and the Zerto User Interface is updated accordingly.

- For the maximum number of virtual machines, either being protected or recovered to that site, see Sizing Considerations for Zerto Virtual Replication.

**Virtual Replication Appliance (VRA):** A virtual machine installed on each hypervisor hosting virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.

A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.

**Virtual Backup Appliance (VBA)** – A VBA is a Windows service, which manages back-ups within Zerto Virtual Replication. The VBA service runs on the same machine as the Zerto Virtual Manager service 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 in a browser.

The following diagram shows how the main Zerto Virtual Replication components are deployed across hypervisor-based enterprise sites to provide disaster recovery across these sites.1

When you plan to recover the enterprise site to a public cloud, Zerto Virtual Replication is installed in the cloud environment. Zerto Virtual Replication comprises the same components but the VRA runs as a service, so that the ZVM, VRA, and VBA all run as services on a single virtual machine instance in the public cloud.

---

1. For the architecture diagrams when one of the sites is a cloud service provider, see Zerto Cloud Manager Administration Guide.
How Zerto Virtual Replication Recovery Works

Installing Zerto Virtual Replication installs the Zerto Virtual Manager, which sits in the hypervisor layer on the enterprise site. You manage the Zerto Virtual Manager, one on each of the protected and recovery sites, using the Zerto User Interface.

Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts or programs.

In the protected site you define the virtual machines that you want to replicate, either individually or together, as a virtual protection group (VPG). The virtual machines that you include in the VPG can come from one or more hypervisor hosts. In this way, you can protect applications that run on multiple virtual machines and disks as a single unit – a VPG. An example of an application that runs on multiple virtual machines includes software that requires a web server and database, both of which run on virtual machines different than the virtual machine where the application software runs.

A virtual machine can be included in several VPGs so that you can recover it to several sites, depending on the needs of the organization. For example the same workload can be protected to a local or a remote location as well as to the cloud. Using several recovery sites also enables migrating disaster recovery datacenters from one location to another.

Note: CD and DVD drives cannot be protected.

Every write is copied by Zerto Virtual Replication and sent, asynchronously, to the recovery site, while the write continues to be processed on the protected site. For greater efficiency and performance, the write can be compressed before being sent to the recovery site with throttling techniques being used to prioritize network traffic.

On the recovery site the write is written to a journal managed by a Virtual Replication Appliance (VRA). Each protected virtual machine has its own journal. Every few seconds, a checkpoint is also written to each journal. These checkpoints ensure write order fidelity and crash-consistency to each checkpoint. During recovery you pick one of these crash-consistent checkpoints and recover to this point. Additionally, checkpoints can be manually added by the administrator, with a description of the checkpoint. For example, when an event is going to take place that might result in the need to perform a recovery, you can pinpoint when this event occurs as a checkpoint written to each journal.

The VRA manages the journals for every virtual machine that will be recovered to the hypervisor hosting that VRA. It also manages images of the protected volumes for these virtual machines. During a failover, you can specify that you want to recover the virtual machines in the VPG using the last checkpoint or you can specify an earlier checkpoint, in which case the recovery of the mirror images under the VRA are synchronized to this checkpoint. Thus, you can recover the environment to the point before any corruption and ignore later writes in the journal that were corrupted, regardless of the cause of the corruption, such as a crash in the protected site or a virus attack.

To improve the RTO during recovery, the user is able to start working even before the virtual machine volumes on the recovery site have been fully synchronized. Every request is analyzed and the response returned either from the virtual machine directly or from the journal if the information in the journal is more up-to-date. This continues until the recovery site virtual environment is fully synchronized, up until the last checkpoint or an earlier checkpoint, when the integrity of the protected site was assured.

When recovery to a point is required that is further in the past than the time saved in the journal, an offsite backup can be restored. Offsite backups are an extension of disaster recovery, with the virtual machine files, such as the configuration and virtual disk files, saved to a repository for up to one year. These files are then used to restore the virtual machines to the point of the stored offsite backup at the recovery site.

Zerto Analytics - Overview

Zerto Analytics allows you to track, monitor and check the health of your data center from any device.

All your alerts, tasks, events and information on Virtual Protection Groups (VPGs) can be viewed together.

This allows you to monitor your Disaster Recovery and Business Continuity status from any location that has internet connectivity. No VPN is required.
Using Zerto Analytics, you can see aggregated information from the Zerto Virtual Managers, and view the status of your environment.

Before you Get Started
There are only a few requirements to get started with Zerto Analytics:

- At least 1 ZVM running Zerto Virtual Replication version 5.0 or higher.
- Make sure to select the checkbox Enable Online Services and Zerto Mobile. This appears for each ZVM in Settings > About.
- You must have internet access.
- You must also have a myZerto account using your corporate email address.

Accessing the Zerto Analytics Portal
Once you have your myZerto login information, and you have upgraded to Zerto version 5.0 or higher, you can enter Zerto Analytics through https://analytics.zerto.com, or through www.zerto.com/myzerto and sign in using your myZerto credentials.

Using Zerto Analytics
When you access Zerto Analytics, the Summary tab opens by default. This tab displays a summary of the data center, including the average RPO, status of the sites, VPG status’s, as well as alerts and tasks.

Following is a best practice flow, to keep track of the overall health of your systems:
1. Monitor the Alerts
2. Troubleshoot the VPGs
3. Review Reports

Monitor the Alerts
To view the alerts and tasks related to your data center, click the Monitoring tab and review the alerts and their descriptions.

TIP!
Click the Alert ID to view full details on the type of the alert.

TIP!
To handle any issues in the ZVM site, in the Monitoring tab > Site column, click the icon Open ZVM in a new tab. This routes you to the specific ZVM site.

Troubleshoot the VPGs
From the Summary tab, review the Errors and Warnings in the VPG Status area, then review the Active Alerts list to detect faulty VPGs.

After identifying any issues which need to be addressed or resolved, you need to drill down.
To do this, click the VPGs tab and click the VPG name to drill down even further.
Review Reports

Use the Reports tab to see RPO, Journal and Network performance history on the VPGs.

In each section of the report, get additional information by clicking the icon ?.

TIP!

Toggle between the Report Types list and the VPG list.

**TIP!**

To get even further insight, after clicking the VPG name, click the button VPG History, and select RPO, or Journal. This opens the Reports page (see Review Reports).

**TIP!**

To handle the issue in the ZVM site, in the Summary tab > SITES area, click the icon Open ZVM in a new tab. This routes you to the specific ZVM site.
Benefits of Using Zerto Virtual Replication

Datacenter optimization and virtualization technologies have matured and are now commonly used in IT infrastructure. As more applications are deployed in a virtualized infrastructure, there is a growing need for recovery mechanisms that support mission critical application deployments while providing complete BC and DR.

Traditional replication and disaster recovery solutions were not conceived to deal with the demands created by the virtualization paradigm. For example, most replication solutions are not managed in the hypervisor layer, considering the virtual machines and disks, but at the physical disk level. Hence they are not truly virtualization aware.

The lack of virtualization awareness creates a huge operational and administrative burden. It also results in operational inflexibility. Zerto Virtual Replication has been designed to resolve these issues by being fully virtualization aware.

See the following topics:
- Fully Virtual – Sits in the Hypervisor or Cloud
- Hardware Agnostic
- Hypervisor Agnostic
- Focus is on the Application, Not the Physical Storage
- Compatibility Across Virtual Environments – Cross-Hypervisor Platform and Version Agnostic
- Fully Scalable
- Efficient Asynchronous Replication
- One-Click Failover and Control of the Recovery Process
- One-Click Migration
- File and Folder Recovery
- Offsite Backup
- Policy-based
- Minimal RPO
- WAN Optimization Between Protected and Recovery Sites
- WAN Resilience on Both the Protected and Recovery Sites
- DR Management Anywhere

Fully Virtual – Sits in the Hypervisor or Cloud

Zerto Virtual Replication software sits in the hypervisor level. Protection groups are configured with virtual machines and virtual disks, without the need to consider the physical disks.

Hardware Agnostic

Because Zerto Virtual Replication software manages recovery of virtual machines and virtual disks only, it does not matter what hardware is used in either the protected or recovery sites; it can be from the same vendor or different vendors. With Zerto Virtual Replication the logical storage is separated from the physical storage so that the vendor and actual type of storage hardware do not need to be considered.

Zerto Virtual Replication provides a workload mobility and protection layer providing seamless connectivity, portability, protection, orchestration, and application encapsulation of workloads across clouds without vendor lock-in. High scale, mission critical applications, and data are encapsulated, as well as features, specifications, and configurations, and can be seamlessly migrated across different servers, storage, hypervisors, and clouds without any disruption to business services.

With Zerto Virtual Replication, IT managers can choose the right infrastructure for the right use case for the right price. One application can leverage several different environments for disaster recovery, bursting, production, backup, testing, and development. With Zerto Virtual Replication there is no vendor lock-in to a cloud, technology, or vendor. Any choice, any cloud, any technology, any price, any service level is available in minutes for any workload.

Hypervisor Agnostic

Zerto Virtual Replication runs both in VMware vCenter Server and Microsoft SCVMM. It is compatible with VMware hypervisor management features, such as vMotion and Microsoft hypervisor management features, such as Live Migration.
Focus is on the Application, Not the Physical Storage

By considering the physical disk level and not the virtual disk level, traditional replication is not truly application aware. Even virtual replication recovers block writes at the SCSI level and not at the application level. Zerto Virtual Replication is truly application focused, replicating the writes from the application in a consistent manner.

Compatibility Across Virtual Environments – Cross-Hypervisor Platform and Version Agnostic

Zerto Virtual Replication enables replication across multiple hypervisor managers, such as VMware vCenter Server and Microsoft SCVMM, and to public clouds such as Amazon Web Services (AWS) or Microsoft Azure. You can protect virtual machines in one hypervisor platform and recover to a different hypervisor platform. This feature can also be used to migrate virtual machines to a different hypervisor platform.

Also, virtual machines running in one version a hypervisor can be recovered in a different version of the same type of hypervisor, as long as Zerto Virtual Replication supports the hypervisor versions, virtual machines can be protected across versions.

Fully Scalable

Zerto Virtual Replication enables defining software-only Virtual Replication Appliances (VRAs) on each hypervisor host to manage the replication of virtual machines on that host. Increasing the number of hypervisor hosts is handled by defining a new VRA on each new host. There is no need to install additional software to the hypervisor management tool, such as VMware vCenter Server or Microsoft SCVMM, to handle additional hosts or virtual machines and no need to consider additional hardware acquisitions.

Efficient Asynchronous Replication

Writes are captured by the Zerto Virtual Replication software in the hypervisor level, before they are written to the physical disk at the protected site. These writes are sent to the recovery site asynchronously, thus avoiding long distance replication latency for the production applications.

Also, because these writes are captured and sent to the recovery site, it is only the delta changes and not the whole file or disk that is sent to the recovery site, reducing the amount of network traffic, which reduces WAN requirements and significantly improves the ability to meet both RPO and RTO targets.

One-Click Failover and Control of the Recovery Process

When recovery is required, the administrator clicks on a button in the Zerto User Interface to initiate failover. This means that controlling the start of a recovery remains in the hands of the administrator, who can decide when to initiate the recovery and, by selecting a checkpoint, to what point-in-time to recover to.

One-Click Migration

Application migrations can be resource intensive projects that take weeks of planning, execution, and downtime. With Zerto Virtual Replication migrations are greatly simplified and can be completed without extended outages or maintenance windows and across different types of hardware and even different hypervisors, such as VMware ESXi or Microsoft Hyper-V. Migrations across different versions within a type of hypervisor, such as from a VMware vCenter environment to a vCloud environment or even cross hypervisor migration, such as migration from a vCenter environment to a Hyper-V environment is as easy as a migration from one site to another using the same hypervisor infrastructure.

File and Folder Recovery

You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto Virtual Replication and running Windows or Linux operating systems. You can recover the files and folders from a specific point-in-time.

You can choose to recover one or several files or folders from the recovery site.
Offsite Backup

Zerto Virtual Replication provides an offsite back up option that enables saving the protected virtual machines offsite for up to one year in a state where they can be easily deployed. Because the backups use the same mechanism used for disaster recovery, there is no performance impact on the production site, since the processing is performed on the recovery site. The offsite backups are fixed points saved daily, weekly or monthly.

**Note:** Zerto recommends **weekly** backups.

Policy-based

In the protected site you define the virtual machines that you want to recover, either individually or as groups, as a virtual protection group (VPG). The virtual machines that you include in the VPG can come from one or more hypervisor hosts. In this way, you can protect applications that run on multiple virtual machines and disks as a single unit, in a single VPG.

Minimal RPO

Zerto Virtual Replication utilizes continuous data protection, sending a record of every write in the virtual protection group to the recovery site. The transfer of this information is done over an optimized WAN asynchronously. If recovery is required, all the data that was transferred to the recovery site is available resulting in recovery within the requested RPO.

WAN Optimization Between Protected and Recovery Sites

Using compression to minimize bandwidth and other techniques such as throttling to prioritize network traffic to reduce the impact on day-to-day operations, you can make sure that the communication between the protected and recovery sites is fully optimized.

Zerto Virtual Replication also uses signature matching to reduce the amount of data sent across the WAN. During synchronization of the protected site and recovery site for every virtual machine in a VPG, Zerto Virtual Replication maintains a map of disk sectors so that if there is a need to resynchronize sites, the map signatures can be used to ensure that only data where changes occurred are passed over the WAN.

WAN Resilience on Both the Protected and Recovery Sites

Zerto Virtual Replication is highly resilient to WAN interruptions. In order to reduce storage overhead used for replication purposes, on WAN failure or when the load over the WAN is too great for the WAN to handle, Zerto Virtual Replication starts to maintain a smart bitmap in memory, in which it tracks and records the storage areas that changed. Since the bitmap is kept in memory, Zerto Virtual Replication does not require any LUN or volume per VPG at the protected side. The bitmap is small and scales dynamically, but does not contain any actual IO data, just references to the areas of the protected disk that have changed. The bitmap is stored locally on the VRA within the available resources. Once the WAN connection resumes or the load returns to normal traffic, Zerto Virtual Replication uses this bitmap to check whether there were updates to the protected disks and if there were updates to the disks, these updates are sent to the recovery site.

DR Management Anywhere

With Zerto Virtual Replication everything is managed from a standalone browser-base user interface, enabling disaster recovery management from anywhere using any device.
CHAPTER 2: ACCESSING THE ZERTO USER INTERFACE

You manage the protection and replication of virtual machines in vSphere, between the protected and recovery sites, using the Zerto User Interface. On first access to the user interface, you might have to add a security certificate to set up secure communication. Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts or programs.

You manage the protection and replication of virtual machines between the protected and recovery sites, using one of the following:
- The Zerto Virtual Manager Web Client.
- The vSphere Web Client.
- The vSphere Client console.

Note: 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.

Note: 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.

Note: The following topics are described in this chapter:
- “Using the Zerto User Interface From a Browser”, below
- “Using the Zerto User Interface Within vSphere”, on page 19
- “Adding a Security Certificate”, on page 21
- “Working With the Zerto User Interface”, on page 22

Using the Zerto User Interface From a Browser

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 site you want to manage.
2. Login using the user name and password for the vCenter Server connected to the Zerto Virtual Manager.

Using the Zerto User Interface Within vSphere

The Zerto User Interface is embedded in both the vSphere Web Client and Client console as a plug-in. When accessing the Zerto User Interface from within vSphere the interface is available via a tab in the vSphere user interface. When using the Zerto User Interface via vSphere you add a virtual machine, that is not already protected in a VPG, directly via the Zerto tab for the virtual machine in the vSphere Web Client and Client console.

Using the vSphere Web Client

You can use the VMware Web Client to manage Zerto Virtual Replication.

The vSphere Web Client is a service that when installed enables a browser-based interface for configuring and administering virtual machines enabling you to connect to a vCenter Server system to manage an ESXi host through a browser. The following procedure describes how to configure the vSphere Web Client to display Zerto Virtual Replication dialogs.

This procedure is valid for vSphere Web Client version 5.1 communicating with vCenter Server from version 5.0 and higher.
Accessing the Zerto User Interface

**Note:** The following procedure assumes that the vSphere Web Client version 5.1 has been installed. Although you can run the vSphere Web Client version 5.1 with vSphere Server 5.0 and 5.1, when installing the vSphere Web Client you need access to a vSphere Server version 5.1 which includes an option for single sign-on, required by the vSphere Web Client installation.

**Note:** Setting up Zerto Virtual Replication to be used via the vSphere Web Client disables the use of other VMware plug-ins, such as VDP and VSA, causing them to disappear from the web client. This is a known VMware problem, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042455. To resolve this issue, set up two web clients, on different servers. On one run Zerto Virtual Replication and on the other run the VMware plug-ins.

**To set up the vSphere Web Client to work with Zerto Virtual Replication:**

1. When the vSphere Web Client service is installed on a Microsoft Windows platform: Copy and run VsphereWebClientPluginEnabler.exe to the machine where you run the web client service. This file is located in the Zerto Virtual Replication folder under the folder where Zerto Virtual Replication was installed. You can copy VsphereWebClientPluginEnabler.exe to any folder on the relevant machine. Run VsphereWebClientPluginEnabler.exe as an administrator.

   When the vSphere Web Client is installed on a Linux platform, via the vCenter Server Linux Virtual Appliance (vCSA): In the directory /var/lib/vmware/vsphere-client, open the webclient.properties file in a text editor and add the following to the file:
   ```
   scriptPlugin.enabled = true
   ```

2. Restart the vSphere Web Client service.

   **Note:** After the service has started you might have to wait a few minutes before you can open the vSphere Web Client in your browser.

**To use the vSphere Web Client:**

1. Log in using the vCenter Server access credentials (username and password) for the vCenter Server connected to the Zerto Virtual Manager.

2. In the browser, navigate to a vSphere node supported by Zerto Virtual Replication, such as the root node or a virtual machine, and choose the Classic Solutions tab, which is now displayed after the Related Objects tab.
   
   **Note:** With Chrome and Firefox browsers, you must load the script plug-in page in an external tab at least once before it appears inside the vSphere Web Client. The Classic Solutions tab is displayed when there is a plug-in installed, in this case the Zerto Virtual Replication user interface plug-in.

3. If prompted, allow blocked content to be displayed.

4. If more than one plug-in is installed, click Zerto to display the Zerto Virtual Replication user interface.
Using the vSphere Client Console

To use the vSphere Client console:
1. Login using the user name and password for the vCenter Server connected to the Zerto Virtual Manager.
2. Access the Zerto tab, displayed for the root node.
   
   **Note:** The Zerto tab is also displayed for a datacenter node showing the same information as for the root node. For a virtual machine or vApp node the Zerto tab displays information specific to the virtual machine or vApp.

Adding a Security Certificate

Communication between the Zerto Virtual Manager and the user interface uses HTTPS. On the first login to the Zerto User Interface, you must install a security certificate in order to be able to continue working without each login requiring acceptance of the security.

**To install a security certificate for the Zerto User Interface:**
On first access to the Zerto User Interface, if you haven’t installed the security certificate, a security alert is issued.

Note the following:
- To run this procedure run Microsoft Internet Explorer as administrator. The procedure is similar for Google Chrome and for Mozilla Firefox.
- Access the Zerto User Interface using the IP and not the name of the machine where Zerto Virtual Replication is installed.
1. Click **View Certificate**.
   The Certificate dialog is displayed.
2. Click **Install Certificate**.
   The Certificate Import wizard dialog is displayed.
3. Follow the wizard: Place all the certificates in the **Trusted Root Certification Authorities store**: Select the **Place all certificates in the following store** option and browse to select the **Trusted Root Certification Authorities store**.
4. Continue to the end of the wizard. Click **Yes** when the Security Warning is displayed.
5. Click **OK** that the installation was successful.
6. Click **OK** when prompted and then **Yes** in the **Security Alert** dialog to continue.

**Working With the Zerto User Interface**

After logging on to the Zerto User Interface for the first time, the dashboard is displayed. The dashboard provides summary information about the status of the site, as shown in the following diagram:

![Dashboard Diagram]

Use the tabs to access the specific information you want:

**DASHBOARD**: General information about the site, including the status of the VPGs being protected or recovered to the site.
Accessing the Zerto User Interface

**VPGs:** All the VPGs from both the local and remote sites and provides summary details of each VPG.

**VMs:** All the protected virtual machines from both the local and remote sites and provides summary details of each virtual machine.

**SITES:** Details of the paired sites. This tab lists all the paired sites to the local site and provides summary details of each paired site.

**SETUP:** Details about VRAs, storage and repositories.

**OFFSITE BACKUP:** Details of the offsite backup jobs either by VPG or virtual machine. This tab lists all the defined offsite backups and their statuses.

**MONITORING:** Details about the alerts, events and tasks for the site.

**REPORTS:** General reports.

**Subtabs**

The SETUP, OFFSITE BACKUP and MONITORING tabs and details of a specific VPG and VRA can be viewed from different perspectives via subtabs. For example, under SETUP you can manage VRAs, storage and repositories via subtabs.

**Views**

Lists can be displayed with different views. For each view you can filter the information in columns via the filter icon next to each column title. Clicking the column title enables sorting the column in ascending to descending order.

You can customize the default views or add a new view by clicking the view configuration button.

Customize a default view by selecting Show/Hide Columns and then checking the columns you want displayed. Create a new view by selecting Create View.
There are a number of configuration tasks that you should do as part of the initial site configuration.

The following configuration topics are described in this chapter:

- "Setting Up Role-based Access Control", below
- "Enabling Replication to the Same Site", on page 24
- "Sizing Considerations", on page 26
- "Setting Up Offsite Backups", on page 28

### Setting Up Role-based Access Control

You can define permissions within Zerto Cloud Manager and via VMware vCenter Server.

- **Zerto Cloud Manager**: Within Zerto Cloud Manager you can apply permissions to specific Zerto Virtual Replication entities such as ZORGs, VPGs, and sites.
  - Permissions determine the roles that apply to a specific user or user group on a specific Zerto Virtual Replication entity.
  - Roles are a set of privileges, and privileges define an operation or a set of operations that can be performed, such as managing a VPG or VRA.
  - Roles can be assigned to users and groups of users.
  - You can manage roles and update the privileges associated with both new roles that you create and the roles supplied with Zerto Virtual Replication.
  - You can then manage the permissions per Zerto Virtual Replication entity.

For details, see the [Zerto Cloud Manager Administration Guide](#).

- **VMware vCenter Server**: VMware roles and permissions are the core of VMware infrastructure security.
  - Permissions are a combination of a user/group and a security role that is applied to some level of the VMware Infrastructure.
  - Zerto Virtual Replication supplies a number of default privileges that enable a VMware administrator to perform specific actions.
  - You can define additional roles and assign these roles the privileges they need.
  - All privileges are implemented at the root level, and thus apply to every object in the vCenter Server.

For details, see the "Zerto Virtual Replication Permissions in vCenter Server", on page 345.

**Note**: When upgrading vCenter Server be sure that the user entity that Zerto Virtual Replication is using is preserved in the user/permissions hierarchy.

### Enabling Replication to the Same Site

When a single vCenter is used, for example with remote branch offices, when replicating from one datacenter to another datacenter, both managed by the same vCenter Server, you have to enable replication to the same vCenter Server and pairing is not required. In this case, replication to the same vCenter must be set in the Site Settings dialog.

**To enable replication to the same vCenter Server:**
1. In the Zerto User Interface, click **SETTING** ( ) in the top right of the header and select **Site Settings**. The Site Settings dialog is displayed.

![Site Settings Dialog](image)

2. Click **Policies**.

![Policies Settings](image)

3. Select the **Enable Replication to Self** checkbox.

4. Click **APPLY** or **SAVE**.

   The Zerto Virtual Manager, when used to protect to itself, can manage the protection of up to 5000 virtual machines.
Sizing Considerations

There are a number of sizing issues to consider when setting up your disaster recovery.

To identify the issues, first review the “VMware VMDK Size Limitations”, below, and “Protected Virtual Machine Considerations”, below.

Then, review “WAN Sizing Requirements with Zerto Virtual Replication”, on page 26

VMware VMDK Size Limitations

VMware imposes the following limits that affect Zerto Virtual Replication:

- **ESXi 5.5 and higher hosts**: A protected VMDK cannot be more than **32TB**. The sum of all VMDKs of all virtual machines protected on a particular ESXi must be lower than **40TB**. Using an ESX tweak, this can be extended to **64TB**.

- **ESXi 5.0 and 5.1 hosts**: The sum of all VMDKs of all virtual machines protected on a particular ESXi must be lower than, by default, **20TB**. Using an ESX tweak, this can be extended to **64TB**.

- **ESX/ESXi 4.x hosts**: The sum of all VMDKs of all virtual machines protected on a particular ESXi must be lower than, by default, **4TB**. Using an ESX tweak, this can be extended to **32TB**.

These limits include all virtual machines running on that host as well as the VRA and any shadow VRAs.

Use the following procedure to adjust the VMDK size limitation.

**Note:** The net effect of adjusting the VMDK size limitation is that the ESX/ESXi kernel will require a small amount of additional memory, such as the 128MB used to get a maximum of 32TB for ESX/ESXi 4.x hosts specified in the procedure, for the larger heap, but it will allow virtual machines with more than 4TB (ESXi/ESX 4.x) or 8TB (ESXi 5.0/5.1) of virtual disk to be addressed.

**To adjust the VMDK size limitation:**

1. Log in to vCenter Server or the ESX/ESXi host using VMware Infrastructure (VI) Client. If connecting to vCenter Server, select the ESX/ESXi host from the inventory.
2. Click the **Configuration** tab.
3. Click **Advanced Settings**.
4. Select **VMFS3**.
5. Update the field in **VMFS3.MaxHeapSizeMB**.
   - In **ESX/ESXi 4.x**, the maximum heap size is **128MB**.
   - In **ESXi 5.x**, the maximum heap size is **256MB**.
6. Reboot the host for the changes to take effect.

Protected Virtual Machine Considerations

- The sum of all protected volumes on a single host should not exceed **96TB**. If you exceed this Zerto recommended limitation, performance issues might occur.
- Each protected volume can have a maximum of **32TB**.
- When using Thin Provisioning, Zerto takes into account the Provisioned number.

WAN Sizing Requirements with Zerto Virtual Replication

When preparing your deployment, you need to verify that the connectivity between the two sites has bandwidth capacity that can handle the data to be replicated between the sites.
You must use a minimum dedicated bandwidth of at least 5 Mb/sec.

Zerto Virtual Replication employs sophisticated compression algorithms to reduce the bandwidth required between the sites. While compression can be very effective in reducing the bandwidth requirements, its efficiency is dependent on data characteristics.

Note: Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.

Estimating the bandwidth requirements between the protected and recovery sites involves the following:

1. Collecting data characteristics for protected VMs, for either of the following environments:
   - vSphere
   - Hyper-V

2. Calculating the estimated bandwidth requirements. You can use one of the following methods:
   - Estimating sizing using the Zerto WAN Sizing Estimator
   - Estimating sizing without the Zerto WAN Sizing Estimator

Note: When the recovery site is Amazon Web Services (AWS), you estimate the required bandwidth for the protected machines, either in vSphere or Hyper-V.

For all sizing details, see Sizing Considerations for Zerto Virtual Replication.
Setting Up Offsite Backups

Disaster recovery using Zerto Virtual Replication enables recovering from a disaster to any point between the moment just before the disaster and a specified amount of time in the past up to 30 days. The recovery is done in real time at the recovery site with a minimal RTO.

If there is an additional requirement to extend the recovery ability to more than 30 days, Zerto Virtual Replication provides an offsite backup option that enables saving the protected virtual machines offsite for up to one year in a state where they can be easily deployed.

The virtual machine files are saved in a repository for the required period. Each virtual machine can have multiple offsite backups created according to a fixed schedule.

The offsite backups are managed by a Windows service, the Virtual Backup Appliance (VBA). The VBA is installed as part of the Zerto Virtual Replication installation. During an offsite backup, the VBA communicates with the VRAs on the recovery site to create the virtual machine files, such as the configuration and virtual disk files in a repository. The offsite backups are fixed points saved either weekly or monthly in the repository. Before you can create an offsite backup for virtual machines, you must first create one or more repositories for the offsite backup jobs.

The following offsite backup setup options are described in this section:

- “Creating an Offsite Backup Repository”, below.
- “Editing an Offsite Backup Repository”, on page 30.

Creating an Offsite Backup Repository

You define the repositories where offsite backups are defined on the recovery site and can be stored, either locally at the recovery site, or on a network share that uses the SMB, Server Message Block, protocol. The repository where you want this offsite backup stored is specified when an offsite backup is defined.

To create an offsite backup repository:

1. In the Zerto User Interface, click SETUP > REPOSITORIES.
2. Click NEW REPOSITORY.
   The New Repository dialog is displayed.
3. Specify the following settings:
   - Repository Name: Specify a unique name for the repository.
   - Repository Type: Specify the type of repository:
     - Local: Backups are stored on the local machine where the Zerto Virtual Manager is installed.
Setting Up Offsite Backups

- **Network Share (SMB):** The network share drive must be an SMB drive and if specified, the username and password to access the drive must be provided.
  When the repository location is a network drive, this drive can be mounted to third party storage, such as Amazon Web Services, AWS, or Microsoft Azure.
  Using TntDrive, from Amazon, enables you to save your offsite backups to a cloud repository mounted disk as if you are using a LAN or locally mounted drive. You can mount one or more Amazon S3 buckets as network drives or as removable local drives, and to use them exactly as you would use any other drive folder on your computer.
- **Username:** Username to access the Network Share drive.
  This field is not displayed when the type is **Local**.
  The username can be entered using either of the following formats:
  - `username`
  - `domain\username`
- **Password:** Password to access the Network Share drive. This field is not displayed when the type is **Local**.
- **Path:** The path where the repository will reside. The path must be accessible from the Zerto Virtual Manager, so if the repository is on a different domain to the Zerto Virtual Manager, the domain must be included in the path.
- **Set as default repository:** Select this to use the repository as the default when specifying extended recovery in a VPG.

4. Click **VALIDATE**. You must validate the path specified. If the folder does not exist, you are asked if you want to create it.
5. Click **SAVE**.
   The repository is created.

You can define more than one repository. When defining offsite backup, you specify which repository to use.

**Note:** When using Zerto Cloud Manager, you must also add the repository to either the vCenter resources or vCD resources in the Zerto Cloud Manager, as described in the Zerto Cloud Manager Administration Guide.
Setting Up Offsite Backups

Editing an Offsite Backup Repository

From the **Repositories** tab, edit repositories.

**To edit an offsite backup repository:**

1. In the Zerto User Interface, click **SETUP > REPOSITORIES**.
2. Select the repository to edit and click the edit pencil icon.
   The Edit Repository dialog is displayed.

   Edit any of the following settings:
   - **Repository Name**: Specify a unique name for the repository.
   - **Repository Type**: Specify the type of repository:
     - **Local**: Backups are stored on the local machine where the Zerto Virtual Manager is installed.
     - **Network Share (SMB)**: The network share drive must be an SMB drive and if specified, the username and password to access the drive must be provided.
       When the repository location is a network drive, this drive can be mounted to third party storage, such as Amazon Web Services, AWS, or Microsoft Azure.
       Using TntDrive, from Amazon, enables you to save your offsite backups to a cloud repository mounted disk as if you are using a LAN or locally mounted drive. You can mount one or more Amazon S3 buckets as network drives or as removable local drives, and to use them exactly as you would use any other drive folder on your computer.
   - **Username**: Username to access the Network Share drive.
     This field is not displayed when the type is **Local**.
     The name can be entered using either of the following formats:
     - **username**
     - **domain\username**
   - **Password**: Password to access the Network Share drive.
     This field is not displayed when the type is **Local**.
   - **Path**: The path from the recovery site where the repository will reside.
     The path must be accessible from the Zerto Virtual Manager, so if the repository is on a different domain to the Zerto Virtual Manager, the domain must be included in the path.
   - **Set as default repository**: Select to use the repository as the default when specifying extended recovery in a VPG.

3. Click **VALIDATE**. You must validate the path specified. If the folder does not exist, you are asked if you want to create it.
4. Click **SAVE**.
   The updated definition of the repository is saved.
Zerto Virtual Replication enables protecting virtual machines, for both disaster recovery or for extended, longer term recovery from an offsite backup, by protecting the relevant virtual machines in virtual protection groups. A virtual protection group (VPG) is a group comprised of virtual machines that are grouped together for recovery purposes. For example, the virtual machines that comprise an application like Microsoft Exchange, where one virtual machine is used for the software, one for the database, and a third for the Web Server require that all three virtual machines be replicated to maintain data integrity.

In addition to disaster recovery and recovery from an offsite backup, Zerto Virtual Replication enables recovery of individual files or folders from a certain point of time.

The following topics are described in this chapter:
- “Flow for a Disaster Recovery Operation”, below
- “Flow for a File or Folder Level Restore Operation”, on page 32
- “Flow for an Offsite Backup and Restore Operation”, on page 32

Once a VPG has been created, each virtual machine in the VPG can be replicated on the recovery site under the VRA on the host specified in the VPG definition as the host for the recovery of the virtual machine.

Every write to the protected virtual machine in a VPG is copied by the VRA on the same host as the protected machine and passed to the VRA on the host in the recovery site specified in the VPG definition as the host for the recovery of the virtual machine. These writes first are saved in a journal for a specified period and then moved to replica virtual disks managed by the VRA, which mirror the protected virtual machine disks.

**Flow for a Disaster Recovery Operation**

Disaster recovery using Zerto Virtual Replication enables recovering from a disaster to any point between the moment just before the disaster and a specified amount of time in the past up to 30 days. The recovery is done in real time at the recovery site with a minimal RTO.

A recovery operation is one of the following:
- A failover.
- A planned move of the protected virtual machines from the protected site to the recovery site.
- A clone of the protected virtual machine to the recovery site.

Virtual machines are protected in VPGs. Once a VPG is created, Zerto Virtual Replication creates a copy under the management of a Virtual Replication Appliance, VRA, on the recovery site, of the protected virtual machine files, such as the configuration and data files. A VRA is installed on every host where the machines are to be recovered.

When a recovery operation is performed, the VRA creates the virtual machines defined in the VPG and attaches the virtual disks to these machines. It then promotes the data from the journal to the virtual machine disks.

The following references the appropriate procedure to protect virtual machines:
- “Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server”, on page 40
- “Replication From a Protected vCenter Server to the Same Site”, on page 57
- “Replication From a Protected Site vCenter Server To a Recovery Site Hyper-V Host”, on page 60
- “Replication From a Protected Site vCenter Server to a Recovery Site AWS”, on page 76
- “Protecting Virtual Machines to and From vCloud Director”, on page 98

After initializing the VPG, all writes to the protected virtual machines are sent by the VRA on the relevant host for each virtual machine on the protected site to the VRA on the recovery site specified as the recovery host for the virtual machine. The information is saved in the journal for the virtual machine with a timestamp, ensuring write-fidelity. Every few seconds the Zerto Virtual Manager causes a checkpoint to be written to every journal on the recovery site for every virtual machine in the VPG, ensuring crash-consistency.
The data remains in the journal until the time specified for the journal when it is moved to the relevant mirror disks, also managed by the VRA for the virtual machine. In this way, you can recover the virtual machines using the mirror disks and then promoting the data from the journal to include the final few hours of data for each virtual machine. Refer to “The Role of the Journal During Protection”, on page 34 for more details about the journal.

The following references the procedures to recover virtual machines protected in a VPG:
- “Overview of Disaster Recovery Operations”, on page 269
- “Managing Failover”, on page 295
- “Migrating a VPG to a Recovery Site”, on page 284
- “Cloning a VPG to the Recovery Site”, on page 305

**Flow for a Test Failover Operation**

When testing that the recovery works as planned, the VRA creates the virtual machines defined in the VPG and uses scratch disks to simulate the virtual machine disks for the duration of the test. This enables the ongoing protection of the virtual machines and the possibility of a failover if required during the test.

The following references the procedure to recover virtual machines:
- “Overview of Disaster Recovery Operations”, on page 269
- “Testing Recovery”, on page 273

**Flow for a File or Folder Level Restore Operation**

You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto Virtual Replication and running Windows operating systems. You can recover the files and folders from a specific point-in-time.

To recover files and folders, see “Recovering Files and Folders”, on page 309.

**Flow for an Offsite Backup and Restore Operation**

If there is a requirement to extend the recovery ability to more than the 30 days that are available with disaster recovery, Zerto Virtual Replication provides an offsite backup option that enables saving the protected virtual machines offsite for up to one year in a state where they can easily be deployed. The recovery virtual machines are saved in a repository of offsite backups that can extend as far back as a year. These offsite backups are fixed points saved either daily or weekly. To save space the offsite backups can be compressed before they are stored in the repository.

When an offsite backup job starts, the Virtual Backup Appliance (VBA) on the recovery site communicates with the VRA on the recovery site to create the backup files of the virtual machines in the VPG, including the data in the journal and saves these files in the repository.

To set up repositories to protect virtual machines in a VPG with offsite backup, see “Setting Up Offsite Backups”, on page 28.

Setting up offsite backups is part of defining a VPG.

After initializing the VPG, Zerto Virtual Replication periodically checks that the time to run an offsite backup has not passed. At the scheduled backup time, the offsite backup is run and the offsite backup file stored in the specified repository.

Offsite backups are kept for the retention period specified in the VPG. Over time the number of stored offsite backups is reduced to save space.

To restore virtual machines to the recovery site, see “Restoring an Offsite Backup”, on page 317.
Virtual machines are protected in virtual protection groups (VPG). A VPG is a group of virtual machines that you group together for recovery purposes. For example, the virtual machines that comprise an application like Microsoft Exchange, where one virtual machine is used for the software, one for the database, and a third for the Web Server require that all three virtual machines be replicated to maintain data integrity.

Any virtual machine whose operating system is supported in both the protected site and recovery site can be protected in a VPG.

Once a virtual machine is protected, all changes made on the machine are replicated in the remote site. The replicated virtual machines in the remote site can be recovered to any point in time defined for the VPG or if a period further in the past is required, an offsite backup can be restored.

When a VPG is created, a replica of each virtual machine disk in the VPG is created under a VRA on the recovery site. These replica virtual disks must be populated with the data in the protected virtual machines, which is done by synchronizing the protected virtual machines with the recovery site replicas. This synchronization between the protected site and remote site takes time, depending on the size of the virtual machines.

After the initial synchronization completes, only the writes to disk from the virtual machines in the protected site are sent to the remote site. These writes are stored by the VRA in the remote site in journals for a specified period, after which they are promoted to the replica virtual disks managed by the VRA.

Any virtual machine that is supported by the hypervisor can be protected. When recovering to a different hypervisor, the protected virtual machines must also be supported by the recovery hypervisors.

The following topics are described in this chapter:

- “Configuring Virtual Protection Groups”, below
- “The Role of the Journal During Protection”, on page 34
- “What Happens After the VPG is Defined”, on page 36

Configuring Virtual Protection Groups

You protect one or more virtual machines in a VPG. The VPG must include at least one virtual machine. After creating a VPG, you can add or remove virtual machines as required. You can only protect a virtual machine in a VPG when the virtual machine has no more than 60 disks.

**Note:** 60 disks requires 4 SCSI controllers each with a maximum of 15 disks.

The 60 disks can be a combination of IDE and SCSI disks, where each virtual machine can have up to 2 IDE controllers each with a maximum of 4 IDE disks and up to 4 SCSI controllers each with a maximum of 15 disks, so that the total of IDE and SCSI disks does not exceed 60 disks.

Any machine that can be hosted in a vCenter Server can be protected as long as it can be hosted in the recovery site environment. Note that a Windows Server 2000 can be protected but re-IP is not supported.

When the recovery site is Amazon Web Services (AWS), you can only protect virtual machines in the protected site that are supported by AWS in the recovery site. The maximum number of supported disks is 22 for virtual machines running a Windows operating system and 12 for virtual machines running a Linux operating system.

The virtual machines can be defined under a single hypervisor host or under multiple hosts. The recovery can also be to a single host or multiple hosts. For example, if a virtual machine in the protected site is configured so that space is allocated on demand and this machine is protected in a VPG, then during recovery the machine is defined in the recovery site with the same space allocation configuration. You protect virtual machines by creating the VPG on the site hosting these virtual machines. After the VPG is created, you can add or remove virtual machines from the VPG by editing the VPG in the Zerto User Interface running on either the protected or recovery site.
**Note:** To create a VPG you must have a recovery site available with a host with a VRA installed. The recovery site can either be a remote site, paired with the protected site, or the protected site itself, where both protection and recovery are to the same Zerto Virtual Manager site.

You can protect a single virtual machine in several VPGs. A virtual machine can be in a maximum of three VPGs. VPGs that contain the same virtual machine cannot be recovered to the same site.

**Note:** 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.

The VPG definition consists of the following:

**General** – A name to identify the VPG and the priority to assign to the VPG.

**Virtual Machines** – The list of virtual machines being protected as well as the boot order and boot delay to apply to the virtual protection groups during recovery.

**Replication Settings** – VPG replication settings, such as the recovery site, host and storage and the VPG SLA. SLA information includes the default journal history settings and how often tests should be performed on the VPG. The defaults are applied to every virtual machine in the VPG but can be overridden per virtual machine, as required.

Cloud service providers can group the VPG SLA properties together in a service profile. When a service profile is used, the VPG SLA settings cannot be modified unless a **Custom** service profile is available.

**Storage Settings** – By default the storage used for the virtual machine definition is also used for the virtual machine data. This storage can be overridden per virtual machine, as required.

**Recovery Settings** – Recovery details include the networks to use for recovered virtual machines and scripts that should be run either at the start or end of a recovery operation.

**NIC Settings** – Specify the network details to use for the recovered virtual machines after a live or test failover or migration.

**Backup Settings** – Specify the backup properties that govern the VPG backup, including the repository where the backups are saved.

You can protect most types of virtual machines running in a vCenter. However, you cannot protect virtual machines with VirtualEthernetCardLegacyNetworkBackingInfo NICs nor with IDE devices. Also, protected virtual machine VMDK descriptor files should be default disk geometry settings. Both the disk geometry and BIOS geometry are written in the descriptor file under ddb.geometry.sectors and ddb.geometry.biosSectors respectively. If these values do not each equal 63 then there may be recovery issues unless you configure the VPG using preseeded volumes.

**The Role of the Journal During Protection**

After defining a VPG, the protected virtual machine disks are synced with the recovery site.

After initial synchronization, every write to a protected virtual machine is copied by Zerto Virtual Replication to the recovery site.

The write continues to be processed normally on the protected site and the copy is sent asynchronously to the recovery site and written to a journal managed by a Virtual Replication Appliance (VRA).

Each protected virtual machine has its own journal.

In addition to the writes, every few seconds all journals are updated with a checkpoint time-stamp.

Checkpoints are used to ensure write order fidelity and crash-consistency.

A recovery can be done to the last checkpoint or to a user-selected, crash-consistent, checkpoint.

This enables recovering the virtual machines, either to the last crash-consistent point-in-time or, for example, when the virtual machine is attacked by a virus, to a point-in-time before the virus attack.

Data and checkpoints are written to the journal until the specified journal history size is reached, which is the optimum situation.
At this point, as new writes and checkpoints are written to a journal, the older writes are written to the virtual machine recovery virtual disks.

When specifying a checkpoint to recover to, the checkpoint **must still be in the journal**. For example, if the value specified is 24 hours then recovery can be specified to any checkpoint up to 24 hours. After the time specified, the mirror virtual disk volumes maintained by the VRA are updated.

During recovery, the virtual machines at the recovery site are created and the recovery disks for each virtual machine, managed by the VRA, are attached to the recovered virtual machines.

Information in the journal is promoted to the virtual machines to bring them up to the date and time of the selected checkpoint.

To **improve the RTO** during recovery, the virtual machine can be used **even before the journal data has been fully promoted**. Every request is analyzed and the response is returned from the virtual machine directly or, if the information in the journal is more up-to-date, it comes from the journal.

This continues until the recovery site’s virtual environment is fully restored to the selected checkpoint.

Each protected virtual machine has its own dedicated journal, consisting of one or more volumes.

A dedicated journal enables journal data to be maintained, even when changing the host for the recovery.

The default storage used for a journal is the storage used for recovery of each virtual machine. Thus for example, if protected virtual machines in a VPG are configured with different recovery storage, the journal data is by default stored for each virtual machine on that virtual machine recovery storage.

The default storage used for a journal when protecting to a VMware vCloud Director is the storage with the most free space, that has either been defined as journal storage for the provider vDC, in the Configure Provider vDCs dialog, or any storage that is visible to the recovery host, even if the journal storage was not defined in the Configure Provider vDCs dialog.

**Journal Sizing**

The journal space is always allocated on demand. The provisioned journal size initially allocated for a journal is 16GB. The provisioned journal size is the current size of all the journal volumes.

If the journal grows to approximately 80% of the provisioned journal size or less than 6GB remains free, a new volume is added to increase the journal size. Each new journal volume added is bigger than the previous volume. The journal size can increase up until a specified hard limit. If the size of the journal is reduced in the VPG definition after new volumes have been added, these volumes are not reduced and continue to be used if required. In this case, the journal size can be bigger than the set size and the reduced journal size definition is not applied, except to ensure that no new volumes are created if the new journal size is reached or exceeded.
The provisioned journal size reported in the Resources report can fluctuate considerably when new volumes are added or removed.

When the amount of the journal used is approximately 50% of the provisioned journal size, the biggest unused journal volume from the added volumes is marked for removal. This volume is then removed after the time equivalent to three times the amount specified for the journal history, or twenty-four hours, whichever is more if it is still not used.

**Note:** With VMware vSphere, with VMFS datastores and when the VRA is on a host ESXi that is version 5.1 or higher, the journal can also reclaim unused space on a volume. Unused space is not reclaimed when using NFS datastores or any datastore with a ESXi host that is lower than version 5.1.

Reclaiming space on a volume does not change the provisioned journal size, which is the current size of all the journal volumes.

When a virtual machine journal comes close to a specified hard limit, Zerto Virtual Replication starts to move data to the target disks. Once this begins, the maintained history begins to decrease. If the journal history falls below 75% of the value specified for the journal history, a warning alert is issued in the GUI. If the history falls below one hour, an error is issued. However, if the amount of history defined is only one hour, an error is issued if it is less than 45 minutes.

The size of the datastore where the journal resides must have at least 30GB free, or have 15% free space, relative to the total datastore space, whichever number of GBs is smaller.

If the available storage of the journal datastore falls below 30GB or 15% of the total datastore size:

- The datastore itself is considered full.
- An error alert is issued and all writes to the journal volumes that datastore storage are blocked.
- Replication is halted, but history is not lost.
- The RPO begins to steadily increase until additional datastore space is made available.

Examples:

- For a large (2TB) datastore: 15% free space remaining = 307GB.
  - The ZVM would not consider the datastore full if 307GB of free space were remaining. 30GB free space remaining would trigger an alert, as it is the smaller figure.
- For a small (100GB) datastore: 15% free space free space remaining = 15GB.
  - The ZVM would not consider the datastore full if 30GB of free space were remaining. 15GB free space remaining would trigger an alert, as it is the smaller figure.

**Testing Considerations When Determining Journal Size**

When a VPG is tested, either during a failover test or before committing a Move or Failover operation, a scratch volume is created for each virtual machine being tested. The scratch volume created uses the same size limit defined for the virtual machine journal.

The size limit of the scratch volume determines the length of time that you can test for. Larger limits enable longer testing times if the constant rate of change is constant. If a small hard limit size is set for this amount of history, for example 2–3 hours, the scratch volume created for testing will also be small, thus limiting the time available for testing.

**What Happens After the VPG is Defined**

After defining a VPG, the VPG is created. For the creation to be successful, the storage used for the recovery must have either 30GB free space or 15% of the size free. This requirement ensures that during protection the VRA, which manages the virtual machine journal and data, cannot completely fill the storage, which would result in the VRA freezing and stopping to protect all virtual machines using that VRA.

The VRA in the remote 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.

During this synchronization, you cannot perform any replication task, such as adding a checkpoint.
For synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the protected data to replicate to the target recovery disks and an alert is issued.

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.

For details of the screen, see “Monitoring a Single VPG”, on page 191.

Recovery

After initializing the VPG, all writes to the protected virtual machines are sent by the VRA on the relevant host for each virtual machine on the protected site to the VRA on the recovery site specified as the recovery host for the virtual machine. The information is saved in the journal for the virtual machine with a timestamp, ensuring write-fidelity. Every few seconds the Zerto Virtual Manager writes a checkpoint to every journal on the recovery site for every virtual machine in the VPG, ensuring crash-consistency.

The data remains in the journal for the time defined by the journal history configuration, after which it is moved to the relevant mirror disks for each virtual machine. Both the journal and the mirror disks are managed by the VRA.

When recovering, either a failover or move, or testing failover or cloning protected virtual machines in the recovery site, you specify the checkpoint at which you want the recovered virtual machines to be recovered. The mirror disks and journal are used to recover the virtual machines to this point-in-time.
File and Folder Recovery

After initializing the VPG, instead of recovering a virtual machine, you can recover specific files and folders in the protected virtual machines from a checkpoint.

Offsite Backups

After initializing the VPG, Zerto Virtual Replication periodically checks that the schedule to run an offsite backup has not been passed, either a daily offsite backup or a weekly offsite backup. At the scheduled backup time, the offsite backup is run and the offsite backup file stored in the specified repository.

Offsite backups are kept on the recovery site for the retention period specified in the VPG. However, over time the number of stored offsite backups is reduced to save space.

The number of stored offsite backups for daily backups is as follows:

<table>
<thead>
<tr>
<th>RETENTION PERIOD</th>
<th>DAILY</th>
<th>WEEKLY</th>
<th>MONTHLY</th>
<th>NUMBER OF BACKUPS</th>
<th>MAXIMUM NUMBER OF DAYS TO OLDEST BACKUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 week</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>1 month</td>
<td>7</td>
<td>4</td>
<td>0</td>
<td>11</td>
<td>35</td>
</tr>
<tr>
<td>3 months</td>
<td>7</td>
<td>4</td>
<td>2</td>
<td>13</td>
<td>91</td>
</tr>
<tr>
<td>6 months</td>
<td>7</td>
<td>4</td>
<td>5</td>
<td>16</td>
<td>175</td>
</tr>
<tr>
<td>9 months</td>
<td>7</td>
<td>4</td>
<td>8</td>
<td>19</td>
<td>259</td>
</tr>
<tr>
<td>12 months</td>
<td>7</td>
<td>4</td>
<td>11</td>
<td>22</td>
<td>343</td>
</tr>
</tbody>
</table>

That is, an offsite backup is kept for each day for the current week and then the oldest offsite backup for the previous week is kept for the previous four weeks and then the oldest monthly backup is kept for the rest of the retention period.

The number of stored offsite backups for weekly backups is as follows:

<table>
<thead>
<tr>
<th>RETENTION PERIOD</th>
<th>WEEKLY</th>
<th>MONTHLY</th>
<th>NUMBER OF BACKUPS</th>
<th>MAXIMUM NUMBER OF DAYS TO OLDEST BACKUP</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 week</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>1 month</td>
<td>4</td>
<td>1</td>
<td>5</td>
<td>58</td>
</tr>
<tr>
<td>3 months</td>
<td>4</td>
<td>3</td>
<td>7</td>
<td>121</td>
</tr>
<tr>
<td>6 months</td>
<td>4</td>
<td>6</td>
<td>10</td>
<td>205</td>
</tr>
<tr>
<td>9 months</td>
<td>4</td>
<td>9</td>
<td>13</td>
<td>289</td>
</tr>
<tr>
<td>12 months</td>
<td>4</td>
<td>12</td>
<td>16</td>
<td>373</td>
</tr>
</tbody>
</table>

That is, an offsite backup is kept for each week for the current month and then the oldest backup for the month is kept and then the oldest monthly backup is kept for the rest of the retention period.
CHAPTER 6: PROTECTING VIRTUAL MACHINES FROM A VCENTER SERVER

When the protected site is vCenter Server, protection can be set up to cope with the following situations:

- A disaster, enabling recovery to a point in time in the 30 days prior to the disaster.
- The need to back up to files saved either daily or weekly for a period of up to one year. The same wizard is used to set up both disaster recovery and backup.

Use any of the following procedures depending on the site to which you need to recover:

<table>
<thead>
<tr>
<th>PROTECTED SITE</th>
<th>RECOVERY SITE</th>
<th>SEE PROCEDURE...</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Server</td>
<td>To a different vCenter Server site</td>
<td>&quot;Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server&quot;, below</td>
</tr>
<tr>
<td></td>
<td>To the same vCenter Server site (local replication)</td>
<td>&quot;Replication From a Protected vCenter Server to the Same Site&quot;, on page 57</td>
</tr>
<tr>
<td></td>
<td>To a different site using the Client Console or VMware Web Client</td>
<td>“Protecting a Single Virtual Machine (Via the VMware Web Client or Client Console)”, on page 58</td>
</tr>
<tr>
<td></td>
<td>To a Hyper-V site</td>
<td>“Replication From a Protected Site vCenter Server To a Recovery Site Hyper-V Host”, on page 60</td>
</tr>
<tr>
<td></td>
<td>To a Amazon Web Services (AWS) site</td>
<td>“Replication From a Protected Site vCenter Server to a Recovery Site AWS”, on page 76</td>
</tr>
<tr>
<td></td>
<td>To a Microsoft Azure site</td>
<td>“Replication From a Protected Site vCenter Server to a Recovery Site Microsoft Azure”, on page 89</td>
</tr>
</tbody>
</table>

Requirements for vSphere Environments

Before protecting your virtual machines, review Zerto Virtual Replication - Prerequisites & Requirements for vSphere Environments

Considerations

- If one or both of the sites have vCloud Director installed, see “Protecting Virtual Machines to and From vCloud Director”, on page 98.
- You cannot protect virtual machines with VirtualEthernetCardLegacyNetworkBackingInfo NICs or with IDE devices.
- Any virtual machine that is supported by the hypervisor can be protected. When recovering to a different hypervisor, the protected virtual machines must also be supported by the recovery hypervisor.
- Zerto does not support protecting virtual machines that are connected to CDs / DVDs.
Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server

You can protect virtual machines to a recovery site vCenter Server. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

To create a virtual protection group (VPG) to recover in vCenter:
1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it.
   Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
   During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click NEXT.
The VMs step is displayed.

4. 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.
   - When using the Search field, you can use the wildcards; * or ?

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.

5. You can view protected virtual machines in the Advanced (One-to-Many) section, by clicking Select VMs. The Select VMs dialog is displayed.

   ![Select VMs dialog](image)

   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.

6. 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 (5) virtual machines may boot on a host simultaneously. Following the boot, a 300 second (default) 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.

7. Click **ADD GROUP** to add a new group. Then, do the following:
   a) To change the name of a group, click the Pencil icon next to the group.
   b) 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, or, 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.
   e) Click **OK** to save the boot order.

8. Click **NEXT**.

The REPLICATION step is displayed.

**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 SLA and Advanced settings, as shown below.
9. Specify the **Recovery Site**. This is the site to which you want to recover the virtual machines. After specifying the recovery site, additional fields are displayed including the host and datastore to use for replication.

![Zerto Virtual Manager Interface](image)

**Note:** You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

10. **ZORG:** If the site is defined in **Zerto Cloud Manager**, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see **Zerto Cloud Manager Administration Guide**.

11. **Host:** The default cluster, resource pool or host in the recovery site that handles the replicated data. If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been specified as a resource in Zerto Cloud Manager. For details about Zerto Cloud Manager, refer to **Zerto Cloud Manager Administration Guide**.

**Note:** If Zerto Cloud Manager is used, vSphere Standard edition cannot be used.

When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for any virtual machines specified in the VPG.

All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are specified as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.

**Note:** If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery will be to any one of the hosts in the recovery site with a VRA installed on it.

12. **Datastore:** The default datastore to use for recovered virtual machine files and for their data volumes. Every datastore for the selected recovery host is included in the drop-down list. If a cluster or resource pool is selected for the host, only datastores that are accessible by every host in the cluster or resource pool are displayed.

13. In the **SLA** area, you define the Service Level Agreement for which this VPG is associated.

   - **When Zerto Cloud Manager** is used, select the **Service Profile** to use.
     The Service Profile determines the VPG SLA settings for the group. This applies predefined settings for the Journal History, Target RPO Alert and the Test Reminder. These settings apply to every virtual machine in the group.
   
   - **When a Custom** service profile is available, the VPG SLA settings are editable, and the **Advanced** button becomes available. When you change these settings, they apply to every virtual machine in the group.

14. Click **ADVANCED**. The Advanced Journal Settings dialog is displayed.
### Setting & Description

#### Journal History

The time that all write commands are saved in the journal.

The longer the information is saved in the journal, the more space is required for each journal in the VPG.

- **Select...**
  - **Number of hours** from 1 to 24
  - **Number of days** from 2 to 30

#### Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)

The storage/datastore used for the journal data for each virtual machine in the VPG.

**Note:** This field is not relevant when replicating to a vCD recovery site.

- **Select the storage/datastore accessible to the host.**
  - When you select a specific journal storage/datastore, the journals for each virtual machine in the VPG are stored in this storage/datastore, regardless of where the recovery storage/datastore is for each virtual machine. All protected virtual machines are recovered to the hosts that can access the specified journal storage/datastore.

#### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

The journal is always thin-provisioned.

**Note:** The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.

**For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

- **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.
  - If Unlimited is selected, Size and Percentage options are not displayed.

- **Size (GB):** The maximum journal size in GB.
  - The minimum journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.

- **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.
  - This value can be configured to more than 100% of the protected VM’s volume size.
16. **Target RPO Alert:** The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

17. **Test Reminder:** The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

18. **Enable WAN Traffic Compression:** Whether or not data is compressed before being transferred to the recovery site. Compressing the data is more efficient, but results in a small performance degradation.

   - Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
   - When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
   - Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
   - When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

19. To change the replication settings per virtual machine, click **VM SETTINGS**. The Advanced VM Replication Settings dialog is displayed.
In this dialog, you can edit the values of one or more of the virtual machines in the VPG.

20. To edit information in one field, click the field and update the information.

21. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

The Edit VM dialog is displayed.

Define as follows:

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Host (not relevant when replicating to vCD)</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
</tr>
<tr>
<td>(Hyper-V) The cluster or host that will host the recovered virtual machine.</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
</tr>
<tr>
<td>(vSphere) The cluster, resource pool, or host that will host the recovered virtual machine.</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
</tr>
<tr>
<td>If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager.</td>
<td>If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.</td>
</tr>
<tr>
<td>For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.</td>
<td>All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.</td>
</tr>
<tr>
<td>Recovery Storage (Hyper-V)</td>
<td>If a cluster is selected for the host, only storage that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located.</td>
</tr>
<tr>
<td>The location where the metadata files for the virtual machine are stored, such as the VHDX file.</td>
<td>If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed.</td>
</tr>
</tbody>
</table>
22. In the Advanced VM Replication Settings dialog, click **OK**.

## Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

- The journal is always **thin-provisioned**.
- The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume.  
  
  **For Example**: If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
</table>
| Journal Size Hard Limit | **Unlimited**: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.  
If Unlimited is selected, Size and Percentage options are **not** displayed.  
**Size (GB)**: The maximum journal size in GB.  
- The **minimum** journal size, set by Zerto Virtual Replication, is **8GB** for Hyper-V and vSphere environments, and **10GB** for Microsoft Azure environments.  
**Percentage**: The percentage of the virtual machine volume size to which the journal can grow.  
- This value can be configured to more than 100% of the protected VM's volume size. |

## Journal Size Warning Threshold

The size of the journal that triggers a warning that the journal is nearing its hard limit.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
</table>
| Journal Size Warning Threshold | **Unlimited**: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.  
If Unlimited is selected, Size and Percentage options are **not** displayed.  
**Size* (GB)**: The size in GB that will generate a warning.  
**Percentage***: The percentage of the virtual machine volume size that will generate a warning.  
*The values of **Size** and **Percentage** must be **less** than the configured **Journal Size Hard Limit** so that the warning will be generated when needed.  
In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full. |

## Journal Storage (Hyper-V), or Journal Datastore (vSphere) (not relevant when replicating to vCD)

The storage/datastore used for the journal data for each virtual machine in the VPG.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
</table>
| Journal Storage (Hyper-V), or Journal Datastore (vSphere) (not relevant when replicating to vCD) | **(vSphere)** To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore.  
**(Hyper-V)** To change the default, specify a host and then select the storage location accessible by this host to be used as the journal storage. When you select specific journal storage, the journals for each virtual machine in the VPG are stored in this storage, regardless of where the recovery storage is for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal storage. |
23. Click NEXT.

The STORAGE step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

**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.

You can define **Thin** provisioning and **Temp Data** in this window, or you can alternatively define them when you separately select and edit each VMs volume.

**IMPORTANT:**

Changing the VPG recovery volume from thin-provisioned to thick-provisioned or vice versa, results in **volume initial synchronization**.

See the following considerations regarding Thin provisioning:

- Unless the user explicitly requests Thin provisioning, provisioning type is the same type as provisioning in the source VM.
- If the source disk is Thin provisioned, the default for the recovery volume is also Thin provisioned.
- If the user uses preseed disks, Zerto maintains the provisioning types of the disks, so they can have other provisioning types.

<table>
<thead>
<tr>
<th>PRESEED</th>
<th>PROVISIONING IN THE RECOVERY VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not selected</td>
<td>User can select Thin provisioning</td>
</tr>
<tr>
<td>Selected</td>
<td>User cannot select Thin provisioning</td>
</tr>
<tr>
<td></td>
<td>Provisioning is the same as defined in source VMs</td>
</tr>
</tbody>
</table>

24. To define whether the recovery volumes are thin-provisioned or not, select the **Thin** checkbox.

25. If the virtual machine to be replicated includes a temp data disk as part of its configuration, select the **Temp Data** checkbox to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.
26. To edit storage information for one of the virtual machines' volume location, first select the virtual machine, then click **EDIT SELECTED**. The Edit Volumes window is displayed.

- In Hyper-V environments, the following window appears.

- In vSphere environments, the following window appears.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Volume Source</strong></td>
<td></td>
</tr>
<tr>
<td>(Hyper-V) Select a <strong>Volume Source</strong> for recovery from one of the drop-down options:</td>
<td></td>
</tr>
<tr>
<td>■ Storage</td>
<td>Volume Source &gt; Storage: A new volume is used for replicated data. From the <strong>Storage</strong> drop-down list, specify the storage to use to create disks for the replicated data. The storage specified for the replication must have at least the same amount of space as the protected volume and then an additional amount for the journal. The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.</td>
</tr>
<tr>
<td>■ Preseeded volume</td>
<td>Volume Source &gt; Preseeded volume: Whether to copy the protected data to a virtual disk in the recovery site. <strong>Zerto recommends</strong> using this option particularly for large disks so that the initial synchronization will be faster since a <strong>Delta Sync</strong> can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When <strong>not</strong> using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN. When using a preseeded virtual disk, you select the storage and exact location, folder, and name of the preseeded disk. <strong>Zerto Virtual Replication</strong> takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk. The storage where the preseeded disk is placed is also used as the recovery storage for the replicated data.</td>
</tr>
</tbody>
</table>
(vSphere) Select a Volume Source for recovery from one of the drop-down options:

- Datastore
- RDM
- Preseeded volume

**Volume Source > Datastore:** A new volume is used for replicated data.

- Specify the Datastore to use to create disks for the replicated data.
- If the source disk is thin provisioned, the default for the recovery volume is also thin provisioned.
- The datastore specified for replication must have at least the same amount of space as the protected volume and an additional amount for the journal.
- The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.
- Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

Then, define the following:

- **Datastore:** The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.

**Volume Source > RDM:** The VMware RDM (Raw Device Mapping) which will be used for the replication.

By default, RDM is recovered as thin-provisioned VMDK in the datastore specified in the VM Recovery Datastore/Storage field in the Edit VM dialog, and not to RDM.

Only a raw disk with the same size as the protected disk can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

The RDM is always stored in the recovery datastore, used for the virtual machine.

The following limitations apply to protecting RDM disks:

- RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
- RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.
- You cannot define an RDM disk to be protected to a cloud service provider via a Zerto Cloud Connector nor if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.
**Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server**

**Protecting Virtual Machines from a vCenter Server**

- **(vSphere) Volume Source** continued

**Volume Source > Preseeded volume**: Select this when you want to copy the protected data to a virtual disk in the recovery site.

Consider the following, then proceed to define the Datastore and the Path:

- **Zerto recommends** using this option particularly for **large disks** so that the initial synchronization is **faster** since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.
- If a preseeded disk is **not** selected, the initial synchronization phase must copy the **whole disk** over the WAN.
- If you use a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.
- If the preseeded disk is **greater than 1TB on NFS storage**, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter by using the command: `esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout`.
- If the protected disks are **non-default geometry**, configure the VPG using preseeded volumes.
- If the protected disk is an **RDM disk**, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. See [Zerto Cloud Manager Administration Guide](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919).

Then, define the following:

- **Datastore**: The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.
- **Path**: The full path to the preseeded disk.

**Temp Data disk**

If the virtual machine to be replicated includes a temp data disk as part of its configuration.

Specifying a mirror disk for replication that is marked as a temp data disk.

In this case, data is not replicated to the temp data disk after initial synchronization.
27. Click **OK**.

28. Click **NEXT**.

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

29. Select the default recovery settings. These are applied to every virtual machine in the VPG.

- **Failover/Move Network**: The network to use during a failover or move operation in which the recovered virtual machines will run.
- **Failover Test Network**: The network to use when testing the failover of virtual machines in the recovery site. Zerto recommends using a fenced-out network so as not to impact the production network at this site.
- **Recovery Folder**: The folder to which the virtual machines are recovered.

**Note**: If the recovery site is a Cloud Service Provider site, it is not possible to select a recovery folder.

30. To specify a recovery folder for each virtual machine in the VPG, click **VM SETTINGS**.
The Advanced VM Recovery Settings window is displayed.

![Advanced VM Recovery Settings window](image)

In this window, you can edit the values of one or more of the virtual machines in the VPG.

31. To edit information in **one field**, click the field and update the information.

32. To edit information for **several virtual machines** at the same time, select the virtual machines and click **EDIT SELECTED**. The Edit VM window is displayed.

- **Recovery Folder:** The folder to which the virtual machine is recovered.

33. Click **SAVE**.

34. In the Advanced VM Recovery Settings window, click **OK**.

35. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.

- **Pre-recovery Script:** The information about a script that should run at the beginning of the recovery process.
- **Post-recovery Script:** The information about a script that should run at the end of the recovery process.

For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command to run</strong></td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td><strong>Params</strong></td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
</tbody>
</table>

- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.
- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.
- The default time-out value is specified in **Site Settings > Performance and Throttling** tab.

36. Click **NEXT**.
The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

37. To edit information in **one field**, click the field and update the information.

38. To edit information for **several virtual machines** at the same time, select the virtual machines and click **EDIT SELECTED**.

39. Otherwise, go to step 42.

The Edit vNIC dialog is displayed.

40. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, **specify** the following:

- **Network**: The network to use for this virtual machine.
- **Create New MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites. Note that if you check this option, to create a new MAC address, and the current IP address is not specified, the protected virtual machine static IP address might not be used for the recovered virtual machine.
- **Change vNIC IP Configuration**: Whether or not to keep the default virtual NIC (vNIC) IP configuration. The vNIC IP is only changed after recovery for virtual machines with VMware Tools running.

See the [Zerto Virtual Replication Interoperability Matrix](#) for the list of operating systems for which Zerto supports Re-IPing.
To change the vNIC IP, in the Failover/Move or Test column, select **Yes**. If you select to use a static IP connection, set the **IP address**, **subnet mask**, and **default gateway**.

Optionally, change the preferred and **alternate DNS server IPs** and the DNS suffix.

If you leave the DNS server and suffix entries empty, or select to use DHCP, the IP configuration and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the Default gateway field for the NICs with no default gateway.

During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP than the original IP, after the virtual machine has started it is automatically rebooted so that it starts up with the correct IP. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.

**Copy to failover test:** Select this to copy the settings in the Failover/Move column to the Test column.

**Copy to failover/move:** Select this to copy the settings in the Test column to the Failover/Move column.

41. Click **OK**.

42. 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.

43. By default, backup is **OFF**. To keep this value, go to step 45.

44. Otherwise, toggle OFF to **ON** and enter the following information:

   - **Target Repository:** The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
   - **Retention Period:** The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
   - **Run Job Every:** The day and time to start the backup.
   - **Retries:** Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
   - **Post-Backup Script:** The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>
45. Click **NEXT**.
   The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

46. Click **DONE**. The VPG is created.

For details of what happens after saving the VPG, see “What Happens After the VPG is Defined”, on page 36.
Replication From a Protected vCenter Server to the Same Site

The same site can be used as both the protected and recovery sites. Even if the site is not paired with another site, VPGs can be created.

See also “When to Replicate to the Same Site”, on page 57.

When to Replicate to the Same Site

The following scenarios show when replicating to the same site can be beneficial. The list is not inclusive.

- Where the same vCenter Server manages different datacenters in different geographical locations. The main datacenter can be used as the recovery site. This scenario describes situations where there are remote offices or branch offices (ROBOs).
- In an organization that does not have a recovery site but wants to protect its virtual machines that use one datastore by creating recovery on a second datastore. This protects against a disaster happening to the primary datastore.
- Between hosts in different clusters.
- Protection against viruses, even in a single cluster: A different host within the cluster can serve as the recovery host for a host with an internal problem with a virtual machine, such as a virus.

To protect from a vCenter Server to the same site:

1. Select Site Settings. In the Site Settings dialog, select Policies.
2. In the Replication section, select Enable replication to self.
3. Then, click SAVE or APPLY.

To define a VPG to recover to the protection site:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG. The Create VPG wizard is displayed.
2. Continue by using the procedure for protecting virtual machines, as described in “Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server”, on page 40. In the REPLICATION tab, select the local site as the Recovery Site.
Protecting a Single Virtual Machine (Via the VMware Web Client or Client Console)

You can protect a virtual machine, which is not already included in a VPG, directly via the Zerto tab for the virtual machine in vSphere Web Client or Client console. You are presented with the following options:

- To add the virtual machine to an existing VPG. The virtual machine is added to the VPG, as described in “To protect a single virtual machine via the vSphere Client console or Web Client:”, below.
- To create a new VPG that you intend should only include one virtual machine, as described in “To protect a single virtual machine:”, on page 59.
- To create a VPG that includes the virtual machine, as described in “Protecting Virtual Machines from a vCenter Server”, on page 39. When using the Zerto User Interface, use this procedure.

To protect a single virtual machine via the vSphere Client console or Web Client:
1. In the vSphere Web Client or Client console, select the Zerto tab for the virtual machine to be added.
2. Click ADD TO EXISTING VPG.
   The Select VPG dialog is displayed.
3. Select the VPG from the list of VPGs.
4. Click OK.
   The Edit VPG wizard is displayed.
5. Configure the virtual machine configuration, as described in “Protecting Virtual Machines from a vCenter Server”, on page 39, starting with step 20.
   - The virtual machine is added to the VPG. This process may take a few minutes.
   - The protected and recovery sites are then synchronized so that the recovery site includes the replication of the added virtual machine in the VPG.
   - After synchronization, the delta changes to the virtual machine are sent to the recovery site.

To protect a single virtual machine:
1. In the vSphere Web Client or Client console, select the Zerto tab for the virtual machine to be protected.
2. Click **PROTECT AS A STANDALONE VM**.
   The Create VPG wizard is displayed. The **VPG Name** defaults to the name of the virtual machine and in the VMs tab, the virtual machine is selected. Note that you can select other virtual machines to add to the VPG.
3. Make any required changes to the VPG, as described in “Replication From a Protected Site vCenter Server to a Recovery Site vCenter Server”, on page 40.
Replication From a Protected Site vCenter Server To a Recovery Site Hyper-V Host

You can protect virtual machines to recovery Hyper-V hosts. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

When creating a VPG from a VMware vCenter Server environment to Hyper-V all recovery operations bring up the recovered machines on Microsoft Hyper-V hosts in SCVMM.

When protecting virtual machines from a VMware vCenter Server environment to Hyper-V, the operating systems of the protected machines must be supported by Hyper-V. Refer to Hyper-V documentation for the list of supported operating systems. Also, virtual machine names cannot include any of the following special characters: * ? : < > / \ " .

Conversion considerations for a protected virtual machine in vSphere when it is recovered in Hyper-V:

■ A machine using BIOS is recovered in Hyper-V as a Generation 1 virtual machine.
■ A machine using UEFI is recovered in Hyper-V as a Generation 2 virtual machine.
■ A machine with a 32bit operating system is recovered in Hyper-V as a Generation 1 virtual machine.
■ A machine with a 64bit operating system is recovered in Hyper-V as either a Generation 1 or Generation 2 virtual machine, dependent on the operating system support in Hyper-V.
■ The boot disk is ported to a disk on an IDE controller. The boot location is 0:0.
■ A virtual machine using up to 4 SCSI controllers is recovered as a virtual machine with 1 SCSI controller.
■ The virtual machine NICs are recovered with Hyper-V network adapters except for protected Windows 2003 virtual machines which are recovered with Hyper-V legacy network adapters.
■ When VMware Tools is installed on the protected virtual machine running Windows Server 2012, Integration Services is installed on the recovered virtual machine automatically.
■ RDM disks are replicated to Hyper-V vhd or vhdx disks, and not to Pass-through disks.

To create a virtual protection group (VPG) to recover in Hyper-V:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   ■ **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   ■ **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.
     ■ **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     ■ **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     ■ **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it.
Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync. During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click **NEXT**.
   The VMs step is displayed.

4. 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.
   - When using the **Search** field, you can use the wildcards; * or ?
   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.

5. You can view protected virtual machines in the **Advanced (One-to-Many)** section, by clicking **Select VMs**.
   The Select VMs dialog is displayed.

**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.

6. 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.

   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.

   ![Boot Order](image)

   7. Click **ADD GROUP** to add a new group. Then, do the following:
      a) To change the name of a group, click the Pencil icon next to the group.
      b) 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, or, 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.
      e) Click **OK** to save the boot order.

   8. Click **NEXT**.
The REPLICATION step is displayed.

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 SLA and Advanced settings, as shown below.

9. Specify the recovery site and default values to use for the replication to this site.
   - **Recovery Site**: The site to which you want to recover the virtual machines. After specifying the Microsoft SCVMM recovery site, the host and storage on the site to use for the replication can be specified.

10. Optionally, change the VPG SLA settings, which apply to every virtual machine in the group.
    - **Journal History**: The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG. Select the number of hours from 1 to 24 or the number of days from 2 to 30.

11. For additional journal-related fields, click **ADVANCED**.
    The Advanced Journal Settings dialog is displayed.
### Journal History

The time that all write commands are saved in the journal.

The longer the information is saved in the journal, the more space is required for each journal in the VPG.

- **Number of hours** from 1 to 24
- **Number of days** from 2 to 30

### Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)

The storage/datastore used for the journal data for each virtual machine in the VPG.

*Note:* This field is **not** relevant when replicating to a vCD recovery site.

### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

The journal is always **thin-provisioned**.

*Note:* The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume.

*For Example:* If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

- **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.
  
  If Unlimited is selected, Size and Percentage options are **not** displayed.
  
  - **Size (GB):** The maximum journal size in GB.
    - The **minimum** journal size, set by Zerto Virtual Replication, is **8GB** for Hyper-V and vSphere environments, and **10GB** for Microsoft Azure environments.
  
  - **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.
    - This value can be configured to more than 100% of the protected VM's volume size.
12. **Target RPO Alert**: The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

13. **Test Reminder**: The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

14. **Enable WAN Traffic Compression**: Whether or not data is compressed before being transferred to the recovery site. Compressing the data is more efficient, but results in a small performance degradation.
   - Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
   - When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
   - Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
   - When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

15. To change the replication settings per virtual machine, click **VM SETTINGS**. The Advanced VM Replication Settings dialog is displayed.

---

**Journal Size Warning Threshold**

The size of the journal that triggers a warning that the journal is nearing its hard limit.

- **Unlimited**: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.
- **Size** (GB): The size in GB that will generate a warning.
- **Percentage**: The percentage of the virtual machine volume size that will generate a warning.

*The values of Size and Percentage must be less than the configured Journal Size Hard Limit so that the warning will be generated when needed.*

In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.
In this window, you can edit the values of one or more of the virtual machines in the VPG.

16. To edit information in one field, click the field and update the information.

17. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

The Edit VM dialog is displayed.

18. Define as follows:

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recovery Host</strong> (not relevant when replicating to vCD)</td>
<td>(Hyper-V) The cluster or host that will host the recovered virtual machine.</td>
</tr>
<tr>
<td>(<strong>vSphere</strong>) The cluster, resource pool, or host that will host the recovered virtual machine.</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
</tr>
<tr>
<td>If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager.</td>
<td>If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.</td>
</tr>
<tr>
<td>For details about Zerto Cloud Manager, see <strong>Zerto Cloud Manager Administration Guide</strong>.</td>
<td>All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.</td>
</tr>
<tr>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
<td></td>
</tr>
<tr>
<td><strong>VM Recovery Datastore</strong> (<strong>vSphere</strong>) (not relevant when replicating to vCD)</td>
<td>The datastore where the VMware metadata files for the virtual machine are stored, such as the VMX file.</td>
</tr>
<tr>
<td>If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located.</td>
<td></td>
</tr>
<tr>
<td><strong>Recovery Storage</strong> (Hyper-V)</td>
<td>The location where the metadata files for the virtual machine are stored, such as the VHDX file.</td>
</tr>
<tr>
<td>If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed.</td>
<td></td>
</tr>
<tr>
<td>SETTING &amp; DESCRIPTION</td>
<td>SELECT...</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| **Journal Size Hard Limit**                   | **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.  
|                                               | **Size (GB):** The maximum journal size in GB.  
|                                               | ▪ The minimum journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.  
|                                               | **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.  
|                                               | ▪ This value can be configured to more than 100% of the protected VM's volume size.  
|                                               | **For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit. |
| **Journal Size Warning Threshold**            | **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.  
|                                               | **Size* (GB):** The size in GB that will generate a warning.  
|                                               | **Percentage*: The percentage of the virtual machine volume size that will generate a warning.  
|                                               | ▪ The values of Size and Percentage must be less than the configured Journal Size Hard Limit so that the warning will be generated when needed.  
|                                               | In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full. |
| **Journal Storage (Hyper-V), or Journal Datastore (vSphere)** (not relevant when replicating to vCD) | (Hyper-V) To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore.  
|                                               | (vSphere) To change the default, specify a host and then select the storage location accessible by this host to be used as the journal storage. When you select specific journal storage, the journals for each virtual machine in the VPG are stored in this storage, regardless of where the recovery storage is for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal storage. |

19. Click **OK**.
20. In the Advanced VM Replication Settings dialog, click **OK**.

21. Click **NEXT**.

The **STORAGE** step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

**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.

- **Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

22. To edit storage information for one of the virtual machines' volume location, first select the virtual machine, then click **EDIT SELECTED**. The Edit Volumes window is displayed.

- In Hyper-V environments, the following window appears.

- In vSphere environments, the following window appears.
<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Source</td>
<td></td>
</tr>
<tr>
<td>(Hyper-V) Select a <strong>Volume Source</strong> for recovery from one of the drop-down options:</td>
<td><strong>Volume Source &gt; Storage</strong>: A new volume is used for replicated data.</td>
</tr>
<tr>
<td>■ Storage</td>
<td>■ From the <strong>Storage</strong> drop-down list, specify the storage to use to create disks for the replicated data.</td>
</tr>
<tr>
<td>■ Preseeded volume</td>
<td>■ The storage specified for the replication must have at least the same amount of space as the protected volume and then an additional amount for the journal.</td>
</tr>
<tr>
<td></td>
<td>■ The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.</td>
</tr>
<tr>
<td></td>
<td><strong>Volume Source &gt; Preseeded volume</strong>: Whether to copy the protected data to a virtual disk in the recovery site.</td>
</tr>
<tr>
<td></td>
<td>■ Zerto <strong>recommends</strong> using this option particularly for large disks so that the initial synchronization will be faster since a <strong>Delta Sync</strong> can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>■ When <strong>not</strong> using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN.</td>
</tr>
<tr>
<td></td>
<td>■ When using a preseeded virtual disk, you select the storage and exact location, folder, and name of the preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>■ Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.</td>
</tr>
<tr>
<td></td>
<td>■ Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>■ The storage where the preseeded disk is placed is also used as the recovery storage for the replicated data.</td>
</tr>
</tbody>
</table>
(vSphere) Select a Volume Source for recovery from one of the drop-down options:

- Datastore
- RDM
- Preseeded volume

### Volume Source > Datastore: A new volume is used for replicated data.

- Specify the **Datastore** to use to create disks for the replicated data.
- If the **source disk is thin provisioned**, the default for the recovery volume is also thin provisioned.
- The datastore specified for replication must have at least the same amount of space as the **protected volume** and an additional amount for the **journal**.
- The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.
- Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

Then, define the following:

- **Datastore**: The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.

### Volume Source > RDM: The VMware RDM (Raw Device Mapping) which will be used for the replication.

By default, **RDM is recovered as thin-provisioned VMDK** in the datastore specified in the **VM Recovery Datastore/Storage** field in the Edit VM dialog, and not to RDM.

Only a raw disk with the **same size as the protected disk** can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

The RDM is always stored in the recovery datastore, used for the virtual machine.

The following **limitations** apply to protecting RDM disks:

- RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
- RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.
- You cannot define an RDM disk to be protected to a cloud service provider via a Zerto Cloud Connector nor if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.
(vSphere) **Volume Source** continued

**Volume Source > Preseeded volume**: Select this when you want to copy the protected data to a virtual disk in the recovery site.

Consider the following, then proceed to define the Datastore and the Path:

- **Zerto recommends** using this option particularly for **large disks** so that the initial synchronization is **faster** since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.
- If a preseeded disk is **not** selected, the initial synchronization phase must copy the **whole disk** over the WAN.
- If you use a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.
- If the preseeded disk is **greater than 1TB on NFS storage**, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter by using the command: `esxcfg-advcfg -s <Timeout>/NFS/SetAttrRPCTimeout`
- If the protected disks are **non-default geometry**, configure the VPG using preseeded volumes.
- If the protected disk is an **RDM disk**, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. See [Zerto Cloud Manager Administration Guide](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919).

Then, define the following:

- **Datastore**: The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.
- **Path**: The full path to the preseeded disk.

**Temp Data disk**

If the virtual machine to be replicated includes a temp data disk as part of its configuration. Specify a mirror disk for replication that is marked as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.
23. Click OK.
24. Click NEXT.
   The RECOVERY step is displayed. Recovery details include the networks to use for failover, move, and for testing failover, and whether scripts should run as part of the recovery operation.

25. Select the default recovery settings.
   - **Failover/Move Network**: The network to use during a failover or move operation in which the recovered virtual machines will run.
   - **Failover Test Network**: The network to use when testing the failover of virtual machines in the recovery site. Zerto recommends using a fenced-out network so as not to impact the production network at this site.

26. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.
   - **Pre-recovery Script**: The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script**: The information about a script that should run at the end of the recovery process.

   For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>- The default time-out value is specified in Site Settings &gt; Performance and Throttling tab.</td>
</tr>
</tbody>
</table>

27. Click NEXT.
The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

28. To edit information in one field, click the field and update the information.
29. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.
30. Otherwise, go to step 33.

The Edit vNIC dialog is displayed.

31. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, **specify** the following:
- **Network**: The network to use for this virtual machine.
- **Create New MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites. Note that if you check this option, to create a new MAC address, and the current IP address is not specified, the protected virtual machine static IP address might not be used for the recovered virtual machine.
- **Change vNIC IP Configuration**: Whether or not to keep the default virtual NIC (vNIC) IP configuration. Configuration is possible only when the guest operating system is defined in the hypervisor manager and Integration Services or VMware Tools are detected. The vNIC IP address is only changed after recovery for virtual machines with VMware Tools and Microsoft Integration Services running.
To change the vNIC IP configuration, select Yes in the Failover/Move or Test column. If you select to use a statically-assigned IP address, set the IP address, subnet mask, and default gateway. Optionally, change the preferred and alternate DNS server IP addresses and the DNS suffix. If you leave the DNS server and suffix entries empty, or select to use DHCP, the IP address and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the Default gateway field for the NICs with no default gateway.

**Note:** During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP address than the original IP address, after the virtual machine has started it is injected with the correct IP address. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP address clash between the test machines and the production machines.

- **Copy to failover test:** Select this to copy the settings in the Failover/Move column to the Test column.
- **Copy to failover/move:** Select this to copy the settings in the Test column to the Failover/Move column.

### IMPORTANT Re-IP Information:

To utilize re-IP during failback, make sure that:

- VMware Tools is **installed** on the virtual machine in vCenter server.
- The user who is logged on to VMWare Tools has **sufficient privileges** to execute re-IP changes.

See the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-IP.

To change the vNIC IP configuration, select Yes in the Failover/Move or Test column. If you select to use a statically-assigned IP address, set the IP address, subnet mask, and default gateway. Optionally, change the preferred and alternate DNS server IP addresses and the DNS suffix. If you leave the DNS server and suffix entries empty, or select to use DHCP, the IP address and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the Default gateway field for the NICs with no default gateway.

**Note:** During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP address than the original IP address, after the virtual machine has started it is injected with the correct IP address. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP address clash between the test machines and the production machines.

- **Copy to failover test:** Select this to copy the settings in the Failover/Move column to the Test column.
- **Copy to failover/move:** Select this to copy the settings in the Test column to the Failover/Move column.

32. Click **OK**.

33. 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.

34. By default, backup is **OFF**. To keep this value, go to step 26.

35. Otherwise, toggle **OFF** to **ON** and enter the following information:

- **Target Repository:** The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
- **Retention Period:** The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
- **Run Job Every:** The day and time to start the backup.
- **Retries:** Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
■ **Post-Backup Script**: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

36. Click **NEXT**.

The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

37. Click **DONE**. The VPG is created.

For details of what happens after saving the VPG, see “What Happens After the VPG is Defined”, on page 36.
Replication From a Protected Site vCenter Server to a Recovery Site AWS

You can protect a vCenter site to Amazon Web Services (AWS).

When creating a VPG from vCenter to AWS the data is stored in S3 and all replicated data from protected virtual machines to AWS is encrypted in S3. All recovery operations bring up the recovered machines in EC2 in AWS.

Before replicating from a protected vCenter site to a recovery AWS site, review the following guidelines for AWS environments, and considerations when protecting to AWS: Zerto Virtual Replication - Prerequisites & Requirements for Amazon Web Services (AWS)

See also:
- “Import Methods for AWS”, on page 76
- “ZertoTools for AWS”, on page 78

After reviewing the guidelines and considerations, proceed with “Protecting From a vCenter Server - To an AWS Recovery Site”, on page 79.

Import Methods for AWS

During recovery operations, Zerto uses a combination of the following APIs and methods to convert the Amazon S3 objects into recovery disks in EC2 as EBS disks:

- **AWS Import**:
  - Import-instance: for the boot volume
  - Import-volume: for data volumes

  For more information see the relevant AWS documentation:
  - API_ImportInstance
  - API_ImportVolume

  **Note:** The ImportImage API is not used by Zerto.

- **Zerto Import - zImport**, an import method that does not have the same limitations as the AWS APIs. It creates an AWS EC2 instance per protected VM volume, called zImport, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk have been attached to the recovered instance, the zImport instance is terminated.

  **Notes:**
  - zImport is based on an official AWS Linux AMI (Amazon Machine Image), into which a script is injected to perform the import. The script is located online and downloaded to the zImport, and thus the zImport requires internet access in order to access and download the script. The zImport instance is therefore created with a public IP.
  - The only network in the customer environment that is certain to have internet access is the network that the ZCA is connected to.
  - To ensure that the zImport instance cannot be accessed from the outside world, a security group is created. During a recovery operation the zImport instance is connected to this security group. All inbound traffic is blocked and only outbound traffic to access the script online is allowed. The security group is deleted at the end of the recovery operation.
  - The default zImport instance type is c4.8xlarge and the AWS EC2 default maximum instance quota is 20. If during the creation of zImport instances the maximum EC2 instance quota is reached, the creation of the next and subsequent zImport instances will be queued, increasing the RTO. If during recovery operations, the ZVM identifies a VPG with the potential to exceed the EC2 instance quota, the user will receive an alert with advice to contact AWS support to increase the service limits in order to improve RTO.
  - GPT formatted disks are supported for data volumes only, when using either of the zImport methods.
  - When using either of the zImport methods, each volume is created with EBS disk of type io1 with maximum 1000 EBS Provision IOPS allocated. EBS disk type can be changed post recovery without downtime, see the relevant AWS documentation. The minimum disk size for io1 is 4GB.
  - The default Max EBS Provision IOPS quota in a region across all io1 disks is 40000 EBS Provision IOPS, meaning that with 1000 EBS Provision IOPS per volume, the maximum possible number of volumes is 40. If the Max EBS Provision IOPS quota is reached, the failover process will switch to using slower gp2 disks. An event will notify the user of this, and recommend that the user contact AWS support to increase the Max EBS Provision IOPS quota.
Depending on the desired RTO during recovery operations, or when testing failover, the user can select an import method per VPG or per virtual machine from the following options:

- **“Zerto Import for Data Volumes”, on page 77**
- **“Zerto Import for All Volumes”, on page 77**
- **“AWS Import”, on page 78**

### Zerto Import for Data Volumes

This method is the default setting and has a faster RTO than AWS Import. This method uses a combination of the AWS import-instance API for the boot volume, and the zImport method for data volumes.

- **Each machine that you intend to protect** must have at least 250MB free space. This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.
- **Protected boot volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Temporary disks may be created based on the selected instance size.
- **Temporary disks** may be created based on the selected instance size.
- **The maximum protected data volume size** is 16TB, while the boot volume can be up to 1TB.
- 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)

### Zerto Import for All Volumes

This method uses the zImport method for all volumes and ensures the fastest RTO.

This method creates an AWS EC2 instance per protected VM volume, called zImporter, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk have been attached to the recovered instance, the zImport instance is terminated.

- **Temporary disks** may be created based on the selected instance size.
- **This import method cannot be used** for the recovery of protected virtual machines running Windows Server 2008R2. To support this operating system please contact Zerto support.
- **The maximum protected data volume size** is 16TB, while the boot volume can be up to 2047GiB.

**Note:** 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 2TB or larger, the VM you are using may be limited to a 2047 GiB boot volume size. Non-boot volumes do not have this limitation. See AWS Documentation for more information: [http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html](http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html)

When using this import method, if the protected virtual machine using this import method is running Windows 2012, Windows 2012R2 or Windows 2016, the following drivers must be installed on the protected virtual machine before starting recovery operations:

- Windows PV (Paravirtualization) Drivers
- Windows ENA (Elastic Network Adapter) Drivers

The following steps must be performed to ensure that the virtual machine will be able to run on the recovery site:

1. **Download and Install Windows PV Drivers:**
   - Follow the instructions at the site for downloading and installing all the Windows PV Drivers 8.2.0 drivers.

2. **Download and Install Windows ENA Drivers:**
   - If you are running Windows 2012 or Windows 2016 on any of the following AWS instance types:
     - C3
     - C4
     - D2
     - I2
     - R3
     - M4 (excluding M4.16xlarge)
   - Follow the instructions at the site for downloading and installing the Windows ENA Drivers.
Note: If these drivers are installed on a VM running Windows 2012R2, the other AWS import methods will fail. To overcome this, you must uninstall the drivers before using the other AWS import methods.

AWS Import

This method uses a combination of the AWS import-instance and import-volume APIs for the boot and data volumes respectively. This was the only method supported until version 5.5.

- **Each machine that you intend to protect** must have at least **250MB free space**. This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.

- **Protected boot volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored.

- **Protected volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored. Temporary disks may be created based on the selected instance size.

- The **maximum protected data volume and boot disk size** is **1TB**.

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)

ZertoTools for AWS

ZertoTools for AWS is required for protecting VMs running Windows operating system in VMware, while AWS is the recovery site platform. The tool enables the following:

- **re-IP** for Windows machines upon failback to on-premises VMware site. (Due to AWS expected behavior, VMware tools are removed for virtual machines that were imported from VMware.)

- Supporting zImport for All Volumes method for Windows machines upon failback to on-premise site. (For more information about the zImport method, see: “Import Methods for AWS”, on page 17)

ZertoTools can be downloaded from **myZerto > Support & Downloads**.

Access ZertoTools and run it on the **protected** Windows virtual machine in VMware before VPG creation.

Running ZertoTools will initiate the AWS PV driver download. If the AWS PV driver download fails, manually download it from the following link: [https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/7.4.6/AWSPVDriver.zip](https://s3.amazonaws.com/ec2-windows-drivers-downloads/AWSPV/7.4.6/AWSPVDriver.zip)

**NOTE:**

- When downloading the PV driver manually, the zip file name AWSPVDRIVER should not be changed.

ZertoTools will also backup the VMtools to ensure re-IP works upon Failback to the protected VMware site.

When running ZertoTools, note the following:

- Ensure that the windows execution message says the **process was successfully completed** when running the tool.

- A folder named **ZertoTools** is created on C:/ProgramData folder.
This folder must not be deleted.
- Upon failover to AWS, the AWS PV driver update may force reboot of the recovered instances in AWS.

Protecting From a vCenter Server - To an AWS Recovery Site

Use the following procedure to create a virtual protection group to protect to AWS.

To create a virtual protection group (VPG) to recover in AWS:

1. In the Zerto User Interface, select **ACTIONS > CREATE VPG**.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it. Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
     During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click **NEXT**.
   The VMs step is displayed.
4. Select the VMs that will be part of this VPG and click the arrow pointing right to include these VMs in the VPG.
   - When using the Search field, you can use the wildcards; * or ?.
   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.

5. You can view protected virtual machines in the Advanced (One-to-Many) section, by clicking Select VMs. The Select VMs dialog is displayed.

   **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.

6. To define the boot order of the virtual machines in the VPG, click **DEFINEBOOT 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 (5) virtual machines may boot on a host simultaneously. Following the boot, a 300 second (default) 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.

7. Click **ADD GROUP** to add a new group. Then, do the following:
   a) To change the name of a group, click the Pencil icon next to the group.
   b) 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, or, 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.
   e) Click **OK** to save the boot order.

   When configuring boot order settings, define the boot disk to be first in the boot sequence in order to avoid boot failure.

8. Click **NEXT**.

   The **REPLICATION** step is displayed.

   **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, as shown below.

9. Specify the recovery site.
   - **Recovery Site:** The site to which you want to recover the virtual machines. After specifying the recovery site, other fields are displayed.
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.

You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

10. Optionally, change the default SLA values:
   - **Journal History**: The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG. Select the number of hours from 1 to 24 or the number of days from 2 to 30.

11. **Target RPO Alert**: The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

12. **Test Reminder**: The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

13. Click **NEXT**. The STORAGE step is displayed.

   By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.
14. Specify whether the protected volume is a temp data disk.

**Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

15. Click **NEXT**.

The RECOVERY step is displayed. Recovery details include the networks, security group, instance family, and instance type 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.

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

**Import Method**

The Import Method drop-down list allows you to select an import method.
Zerto Import for data volumes: Uses the zImport method for **data volumes** only. This is the default setting and usually has a faster RTO than AWS Import.

Zerto Import for all volumes: This is usually the fastest import method and uses a zImport VM for **all volumes**. **IMPORTANT:** When using this import method, the following setup steps **must be performed** on the protected virtual machine **prior to the start of recovery operations** to ensure that the virtual machine will be able to run on the recovery site. This is applicable if the protected virtual machine using this import method is running Windows.

b) Follow the instructions at the site for downloading and installing all the Windows PV Drivers 8.2.0 drivers.

**Notes:**
- This import method cannot be used for the recovery of protected virtual machines running Windows Server 2008R2. To support this operating system please contact Zerto support.
- If these drivers are installed on a VM running Windows Server 2008R2, the import of the VM using either the Zerto Import for data volumes or AWS Import method will fail.

AWS Import: This was the only import method supported until version 5.5.

**VPC Network**: The virtual network dedicated to your AWS account. A security group and subnet must be assigned to this VPC.

**Subnet**: The subnet for the VPC network.

Depending on the import method selected, the list of subnets available for selection is shown.

**Zerto Import - zImport**: The subnet drop-down list shows the options available when either the Zerto Import for data volumes or the Zerto Import for all volumes is selected. Only the subnets that are supported by the zImport method are selectable. Other Subnets are grayed out and are not selectable.

**AWS Import**: The Subnet drop-down list shows options available when AWS Import method is selected. All subnets are listed. A tool tip alert is displayed when the user hovers over a subnet that is not supported.
Note: If a subnet is chosen in a network that is not in the same Availability Zone as the one in which the ZCA resides, options that utilize the zImport method will not be made available for selection.

**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 being protected in the VPG.

**Instance Type:** The instance type, within the instance family, to assign to recovered instances. Different types within an instance family vary, for example in vCPU, RAM, and local storage size. Choose the instance type appropriate for the application being protected in the VPG. The price per instance is related to the instance configuration.

17. For additional settings, click **ADVANCED VM SETTINGS**.

The Advanced VM Settings window is displayed, which shows the recovery network settings for **FAILOVER/MOVE** for virtual machines in the VPG. You can see the recovery network settings for failover tests by clicking **TEST**.

18. To edit information in one field, click the field and update the information.

19. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**. The Edit VM Settings dialog is displayed.
20. Update the values for Import Method, VPC network, subnet, security group, instance family, instance type, and private IP as necessary.

   **Note:** Only private IPs specified for Windows machines are assigned during a recovery operation. For Linux machines, the IP is assigned from the specified subnet range.

   Clearing the values in the **Private IP** field results in an IP being automatically assigned from the subnet range during a recovery operation.

   See the [Zerto Virtual Replication Interoperability Matrix](#) for the list of operating systems for which Zerto supports re-IP.

21. Click **OK** twice to return to the main page of the RECOVERY step.

22. Enter the name of the script to run in the **Command to run** text box. You can then enter details about the script.

   - **Pre-recovery Script:** The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script:** The information about a script that should run at the end of the recovery process.

For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>■ The default time-out value is specified in <strong>Site Settings &gt; Performance and Throttling</strong> tab.</td>
</tr>
</tbody>
</table>

23. 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 for up to one year.

24. By default, backup is **OFF**. To keep this value, go to step 26.

25. Otherwise, toggle OFF to **ON** and enter the following information:
   - **Target Repository**: The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
   - **Retention Period**: The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
   - **Run Job Every**: The day and time to start the backup.
   - **Retries**: Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
   - **Post-Backup Script**: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

**Note**: You cannot restore a backup in AWS.

26. Click **NEXT**.
The SUMMARY step is displayed. It shows the VPG configuration that you defined in the previous steps.

27. Click **DONE**. The VPG is created.

For details of what happens after creating the VPG, see "What Happens After the VPG is Defined", on page 36.
Replication From a Protected Site vCenter Server to a Recovery Site Microsoft Azure

You can protect virtual machines to Microsoft Azure. The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

When creating a VPG from vCenter server to Azure the data is stored in a storage account and all replicated data from protected virtual machines to Azure is encrypted in the storage account. All recovery operations bring up the recovered machines in resource groups in Azure.

- Azure ZCA can be installed only on Windows Server 2012 R2 and higher.
- Only virtual machines that are supported by Azure can be protected by Zerto Virtual Replication. All Windows operating systems are supported.

**Note:** Microsoft does not support operating systems that are past the **End of Support date**, without a **Custom Support Agreement (CSA)**. For more information about Microsoft operating systems support for Microsoft Azure, refer to [https://support.microsoft.com/en-us/kb/2721672](https://support.microsoft.com/en-us/kb/2721672).

- To replicate between Azure and your site, you must have a virtual machine in Azure with a Zerto Cloud Appliance installed on it. This ZCA must be paired with your site.

- For **Linux** distribution, refer to Azure documentation:

**Requirements for Replication From Azure**

- For Virtual Machines to be protected from Azure, the VM volumes must reside in the Standard storage account defined during ZCA installation.
  - A Standard storage account is created or selected upon ZCA installation.
    - Type: Standard storage
    - Recovery and journal volumes reside on this Zerto Storage Account
    - Azure VMs with all disks on this Zerto Storage Account can be protected by Zerto.
    - Blob Storage is not supported.
    - Managed Disks are not supported.
  - VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.

**Requirements for Replication To Azure**

- **Protected volumes** are recovered in Azure as **VHD disks** in a page blob. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB.
  - **Note:** For some instance sizes, the Azure virtual machine is created with a Local SSD disk which is a temporary disk. This disk is in addition to the disks associated with each protected virtual machine.

- The following limits apply when protecting to Azure
  - Virtual machines with **UEFI Firmware** cannot be protected.
  - You **cannot** protect machines that have a disk **larger than 4 TB**.
  - The **protected** virtual machines needs to have at **least one NIC**.
  - Reserve at least **2 CPUs** and **4GB RAM** for the machine using a subnet accessible by other Zerto Virtual Replication sites.
  - The **supported** number of **data disks and NICs per virtual machine** is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.

**Requirements for Replication within Azure**

- Azure ZCA on both Azure sites need to be version 6.0 and higher.
- The following limitations apply when protecting within Azure:
  - Self replication is not supported.
Additional Azure Considerations

For additional considerations, see Azure subscription and service limits, quotas and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits.

For example from the link, see the following default values:
- There can be multiple Zerto Cloud Appliances per Azure subscription and region.
- 20 cores per subscription
- 200 Storage accounts per subscription
- 20 VMs per region per subscription
- 20 VMs per series (Dv2, F, etc.) cores per subscription per Region

Additionally, see the following example for maximum values:
- A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not exceed this limit.

<table>
<thead>
<tr>
<th>VM TIER</th>
<th>BASIC TIER VM</th>
<th>STANDARD TIER VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk size</td>
<td>4 TB</td>
<td>4 TB</td>
</tr>
<tr>
<td>Max 8 KB IOPS per persistent disk</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Max number of disks performing max IOPS</td>
<td>66</td>
<td>50</td>
</tr>
</tbody>
</table>

See also “Azure Limitations Which Affect Installation and Recoverability”, on page 90.

Azure Limitations Which Affect Installation and Recoverability

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

Default Azure Limitations which Affect Installation

- **Storage Limitations:**
  - Number of storage accounts: **200 per subscription** (note: max is 250)

Default Azure Limitations which Affect Recovery

<table>
<thead>
<tr>
<th>Virtual Machines Limitations</th>
<th>VMs per subscription per region: 20 (max: 10K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM total cores per subscription per region: 20</td>
<td></td>
</tr>
<tr>
<td>Instance sizes: Limited per region. Many of them are 20 cores per region per subscription</td>
<td></td>
</tr>
<tr>
<td>Resource groups per subscription: 800</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>Network interfaces per region: 350</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICs per instance: Depends on instance size:</td>
<td></td>
</tr>
<tr>
<td>Private IP Addresses per VNET per subscription per region: 4096</td>
<td></td>
</tr>
<tr>
<td>Cloning of IP addresses during recovery operations: Due to an Azure limitation, failing over Linux VMs with static IP is <strong>not</strong> supported.</td>
<td></td>
</tr>
</tbody>
</table>

See also "Azure Limitations Which Affect Installation and Recoverability", on page 90.
Protecting From a vCenter Server - To a Microsoft Azure Recovery Site

Use the following procedure to replicate from a protected site vCenter Server to a recovery site Microsoft Azure.

To create a virtual protection group (VPG) to recover in Microsoft Azure:
1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have used it. Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click NEXT.

The VMs step is displayed.

4. Select the VMs that will be part of this VPG and click the arrow pointing right to include these VMs in the VPG.
   - When using the Search field, you can use the wildcards; * or ?.

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.

5. You can view protected virtual machines in the Advanced (One-to-Many) section, by clicking Select VMs.

The Select VMs dialog is displayed.

6. Click NEXT.

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.

6. Click NEXT.
The REPLICATION step is displayed.

![Create VPG](image)

**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, as shown below.

7. Specifying the recovery site.
   - **Recovery Site:** The site to which you want to recover the virtual machines. After specifying the recovery site, other fields are displayed.

![Create VPG](image)

**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.

You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

8. Optionally, change the default **SLA** values:
   - **Journal History:** The time that all write commands are saved in the journal.
     The longer the information is saved in the journal, the more space is required for each journal in the VPG.
     Select the number of **hours** from 1 to 24 or the number of **days** from 2 to 30.

9. Click **NEXT**.
    The STORAGE step is displayed.

    By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.
10. Specify whether the protected volume is a temp data disk.

**Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

11. Click NEXT.

The RECOVERY step is displayed. Recovery details include the networks, network security group, instance family, and instance size 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.

12. Select recovery settings for failover/move and failover testing.
   - **VNet:** The virtual network dedicated to your Azure subscription.
   - **Subnet:** The subnet or the VNet network.
   - **Network Security Group:** The Azure network security to be associated with the virtual machines in this VPG. You can associate one network security group with the virtual machines. The NIC will be associated with the network security group defined at the virtual machine level.
   - **Virtual Machine Series:** The virtual machine series from which to select the size. Azure virtual machine series are optimized for different types of applications. The default is set to **Dv2-series**. You can choose the virtual machine series appropriate for the application being protected in the VPG.
Virtual Machine Size: The virtual machine size, within the virtual machine series, to assign to recovered virtual machines. Different sizes within a virtual machine series vary, for example in a number of cores, RAM, and local storage size. The default is set to Standard_D1_v2. You can choose the virtual machine size appropriate for the application being protected in the VPG. The price per virtual machine is related to the virtual machine configuration.

13. For additional settings, click ADVANCED VM SETTINGS.

The Advanced VM Settings dialog is displayed, which shows the recovery network settings for failover and move for virtual machines in the VPG. You can see the recovery network settings for failover tests by clicking TEST.

14. To edit information in one field, click the field and update the information.

15. To edit information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED.

The Edit VM Settings dialog is displayed.

16. Update the values for VNet, subnet, network security group, instance family, instance size, and private IP as necessary.

Note: Only private IPs specified for Windows machines are assigned during a recovery operation. For Linux machines, the IP is assigned from the specified subnet range.

Clearing the values in the Private IP field results in an IP being automatically assigned from the subnet range during a recovery operation.

Refer to the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-IP.

17. Click OK twice to return to the main page of the RECOVERY step.

18. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.

Pre-recovery Script: The information about a script that should run at the beginning of the recovery process.

Post-recovery Script: The information about a script that should run at the end of the recovery process.
For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>■ The default time-out value is specified in Site Settings &gt; Performance and Throttling tab.</td>
</tr>
</tbody>
</table>

19. 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 for up to one year.

20. By default, backup is OFF. To keep this value, go to step 26.

21. Otherwise, toggle OFF to ON and enter the following information:
   - **Target Repository**: The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in "Setting Up Offsite Backups", on page 28.
   - **Retention Period**: The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see "Offsite Backups", on page 38.
   - **Run Job Every**: The day and time to start the backup.
   - **Retries**: Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
   - **Post-Backup Script**: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

**Note**: You cannot restore a backup in Azure.
22. Click **NEXT**.
   The SUMMARY step is displayed. It shows the VPG configuration that you defined in the previous steps.

23. Click **DONE**. The VPG is created.

For details of what happens after creating the VPG, see "What Happens After the VPG is Defined", on page 36.
CHAPTER 7: PROTECTING VIRTUAL MACHINES TO AND FROM VCLOUD DIRECTOR

When VMware vCloud Director (vCD) is installed at either the protected or recovery site, protection involving vCD can be set up to cope with the following situations:

- A disaster, enabling recovery to a point in time in the 30 days prior to the disaster.
- The need to back up to files saved either daily or weekly for a period of up to one year. The same wizard is used to set up both disaster recovery and backup.

Use any of the following procedures depending on the site to which you need to recover:

| FROM A PROTECTED SITE | TO A RECOVERY SITE | SEE PROCEDURE...
|-----------------------|--------------------|-------------------|
| VMware vCloud Director (vCD) | To a different recovery site vCD | "Replication From a Protected Site vCenter Server to a Recovery Site vCD", on page 100
| | To a recovery site vCD | "Replication From a Protected Site vCD to a Recovery Site vCD", on page 115
| | | Note: The protected machines are protected as a vCD vApp in the recovery site vCD. To review which settings are maintained, see vApp Settings Maintained when Replicating from a Protected Site vCD to a Recovery Site vCD.
| | To a vCenter Server | "Replication From a Protected Site vCD to a Recovery Site vCenter Server", on page 131
| | To a Hyper-V site | "Replication From a Protected Site vCD to Hyper-V", on page 148
| | To a Amazon Web Services (AWS) site | "Replication From a Protected Site vCD to AWS", on page 164
| | To a Microsoft Azure site | "Replication From a Protected Site vCD to Azure", on page 175

Consider the following:

- When the vCloud Director (vCD) site is set up within Zerto Cloud Manager, as described in Zerto Cloud Manager Administration Guide, the vCenter Server underlying the vCD for the site cannot be specified as either the protected site or recovery site. When Zerto Cloud Manager is not used, the vCenter Server underlying the vCD can be specified.
- Both the VM-level and vCD vApp-level metadata is also replicated to the recovery site. However, Zerto Virtual Replication does not replicate fenced mode settings. If fenced mode is configured in the vCD, it must be enabled for recovered virtual machines after a failover or move. This can lead to clashes with MAC addresses and IP addresses. If this occurs the MAC address or IP address must be configured after the failover or move. Both the VM-level and vCD vApp-level metadata is not replicated when the recovery site is not vCD.
- In the properties for the vCD vApp to be protected make sure that the Start Action in the Starting and Stopping VMs tab is set to Power On.
- When vCD is used, you can have the journals on separate datastores from the recovery volumes. For example, you might prefer to keep the recovery volumes on storage with better performance, security, and reliability and the journal on less expensive storage.
- As part of recovery after a failover or move operation, the data in the journal is promoted to the recovered virtual machines. During this promotion, the virtual machines can be used, and Zerto Virtual Replication makes sure that what the user sees is the latest data, whether from the virtual machine disks or from the journal. If the journal is on a slow storage device, this is reflected in the response time the user experiences.
■ You cannot protect virtual machines with `VirtualEthernetCardLegacyNetworkBackingInfo` NICs or with IDE devices.
To create a virtual protection group (VPG) to recover in vCD:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.

   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have used it. Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
   Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.

3. Click **NEXT**. The VMs step is displayed.
4. 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.
   - When using the Search field, you can use the wildcards; * or ?

   The hardware version of the virtual machine must be the same or less than the hardware version supported by the vDC in vCloud Director (vCD) otherwise recovery of the virtual machine in vCD is not permitted. Set the supported hardware level in the Provider vDC Properties for the vDC in the vCloud Director console.

   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.

5. You can view protected virtual machines in the Advanced (One-to-Many) section, by clicking Select VMs.
   The Select VMs window is displayed.

6. Select a protected virtual machine, then click OK.
   **Note:** You define the boot order for the recovered vCD vApp in the vCloud Director console.

7. Click NEXT.
8. Select the Recovery vCD Site, and select vCD from the drop-down list. The REPLICATION step is re-displayed, with additional fields relevant for vCD.

Define as follows:

9. ZORG: If the site is defined in Zerto Cloud Manager, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.

10. Specify the Recovery Org vDC to use in the recovery site. Note: You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

11. In the SLA area, you define the Service Level Agreement for which this VPG is associated.

   ■ When Zerto Cloud Manager is used, select the Service Profile to use. The Service Profile determines the VPG SLA settings for the group. This applies predefined settings for the Journal History, Target RPO Alert and the Test Reminder. These settings apply to every virtual machine in the group.

   ■ When a Custom service profile is available, the VPG SLA settings are editable, and the Advanced button becomes available. When you change these settings, they apply to every virtual machine in the group.

12. Click ADVANCED. The Advanced Journal Settings dialog is displayed.
### Journal History

The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG.

- **Number of hours** from 1 to 24
- **Number of days** from 2 to 30

### Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)

The storage/datastore used for the journal data for each virtual machine in the VPG.

**Note:** This field is **not** relevant when replicating to a vCD recovery site.

### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

The journal is always **thin-provisioned**.

**Note:** The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume.

**For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

- **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.

  If Unlimited is selected, Size and Percentage options are **not** displayed.

- **Size (GB):** The maximum journal size in GB.
  - The **minimum** journal size, set by Zerto Virtual Replication, is **8GB** for Hyper-V and vSphere environments, and **10GB** for Microsoft Azure environments.

- **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.
  - This value can be configured to more than 100% of the protected VM's volume size.
13. **Target RPO Alert**: The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

14. **Test Reminder**: The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

15. **Enable WAN Traffic Compression**: Whether or not data is compressed before being transferred to the recovery site. Compressing the data is more efficient, but results in a small performance degradation.
   - Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
   - When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
   - Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
   - When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

16. To change the replication settings per virtual machine, click **VM SETTINGS**.

---

**Journal Size Warning Threshold**

<table>
<thead>
<tr>
<th>Setting &amp; Description</th>
<th>Select...</th>
</tr>
</thead>
</table>
| The size of the journal that triggers a warning that the journal is nearing its hard limit. | ■ **Unlimited**: The size of the journal is unlimited and it can grow to the size of the recovery storage/datasource. If Unlimited is selected, Size and Percentage options are not displayed.  
■ **Size** (GB): The size in GB that will generate a warning.  
■ **Percentage**: The percentage of the virtual machine volume size that will generate a warning.  
*The values of Size and Percentage must be less than the configured Journal Size Hard Limit so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full. |
The Advanced VM Replication Settings window is displayed. In this window, you can edit the values of one or more of the virtual machines in the VPG.

17. To edit information for a **single** VM, click the field **Storage Policy**, or **Journal Storage Policy**, and update the information.
   - **Storage Policy**: The Storage Policy in which the **VM configuration files** will reside. For considerations, see step 19.
   - **Journal Storage Policy**: The Storage Policy in which the **VM Journal files** will reside. For considerations, see step 20.

18. To edit information for **several** virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

The Edit VM window is displayed.

19. When selecting **Storage Policy**, consider the following:
   - Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - Zerto will try to determine a default Storage Policy according to:
     - A Storage Policy with the same name as the protected Storage Policy.
     - The default Orgvdc Storage Policy.
   - If Zerto did not manage to determine a default Storage Policy, this field appears empty.
   - When you **click to edit**, a list of Storage Policies appear. These Storage Policies:
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
     - Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.
   - To review site-specific configurations, see **Configure Provider vDCs Dialog**.

20. When selecting **Journal Storage Policy**, consider the following:
   - Zerto will select a datastore from the selected Storage Policy in which to place the Journal files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - The default Journal Storage Policy is the same as the default VM Storage Policy.
   - If Zerto did not manage to determine a default Journal Storage Policy, this field appears empty.
   - When you **click to edit**, the option **Auto Select** appears, and a list of Storage Policies.
   - The list of Storage Policies associated with the Journal:
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
- Have at least one Datastore that was not excluded as a **Journal** in the Configure Provider vDCs Dialog.
- **Auto Select:** Selecting this means that the journal can be placed in any datastore visible to the host that Zerto selected for recovery, unless the datastore is excluded in the Configure Provider vDCs Dialog.

21. Define the remaining fields as follows:

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
</table>
| **Recovery Host** *(not relevant when replicating to vCD)* | **(Hyper-V)** The cluster or host that will host the recovered virtual machine.  
If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager.  
For details about Zerto Cloud Manager, see [Zerto Cloud Manager Administration Guide](#).  
When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG. |
| **(vSphere)** The cluster, resource pool, or host that will host the recovered virtual machine.  
If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.  
All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager. | When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.  
If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.  
All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager. |
| **VM Recovery Datastore** *(vSphere)* *(not relevant when replicating to vCD)* | The datastore where the VMware metadata files for the virtual machine are stored, such as the VMX file.  
If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located. |
| **Recovery Storage** *(Hyper-V)* | The location where the metadata files for the virtual machine are stored, such as the VHDX file.  
If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed. |
| **Journal Size Hard Limit** | **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.  
If Unlimited is selected, Size and Percentage options are not displayed.  
**Size (GB):** The maximum journal size in GB.  
- The **minimum** journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.  
**Percentage:** The percentage of the virtual machine volume size to which the journal can grow.  
- This value can be configured to more than 100% of the protected VM’s volume size.  
**The journal is always thin-provisioned.**  
The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.  
*For Example:* If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit. |
22. Click **Save**.
23. In the Advanced VM Replication Settings window, click **OK**.
24. Click **NEXT**.

The STORAGE step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data.

For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.
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.

You can define Thin provisioning and Temp Data in this window, or you can alternatively define them when you separately select and edit each VM's volume.

**IMPORTANT:**

Changing the VPG recovery volume from thin-provisioned to thick-provisioned or vice versa, results in **volume initial synchronization**.

See the following considerations regarding Thin provisioning:

- Unless the user explicitly requests Thin provisioning, provisioning type is the same type as provisioning in the source VM.
- If the source disk is Thin provisioned, the default for the recovery volume is also Thin provisioned.
- If the user uses preseed disks, Zerto maintains the provisioning types of the disks, so they can have other provisioning types.

<table>
<thead>
<tr>
<th>PRESEED</th>
<th>PROVISIONING IN THE RECOVERY VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not selected</td>
<td>User can select Thin provisioning</td>
</tr>
<tr>
<td>Selected</td>
<td>User cannot select Thin provisioning</td>
</tr>
<tr>
<td></td>
<td>Provisioning is the same as defined in source VMs</td>
</tr>
</tbody>
</table>

25. To define whether the recovery volumes are thin-provisioned or not, select the Thin checkbox.

26. If the virtual machine to be replicated includes a temp data disk as part of its configuration, select the Temp Data checkbox to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

27. To edit storage information for one of the virtual machines volumes, select the volume/s and click **EDIT SELECTED**.

When protecting to vCenter, the following Edit Volumes window is displayed. Continue with step 26.

When protecting to vCD environments, the following Edit Volumes window is displayed. Continue with step 28.
28. **Volume Source:** The source on the recovery site for the replicated data: **Datastore, RDM** or **Preseeded volume**.
   - **Volume Source > Datastore.**

   **Datastore:** A new volume is used for replicated data. Specify the datastore to use to create disks for the replicated data. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned. The datastore specified for replication must have at least the same amount of space as the protected volume and an additional amount for the journal. The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.

   You can use the vSphere Client console Performance tab for each virtual machine to help estimate the change rate. For more details, see the section **Collecting Data Characteristics for VMs.**

   Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

   - **Volume Source > RDM.**

   **Raw Disk:** The VMware RDM (Raw Device Mapping) to use for the replication.

   - By default, RDM is recovered as **thin-provisioned** VMDK in the datastore specified in the **VM Recovery Datastore** field in the Edit VM dialog, and **not to RDM.**

   - You cannot define an RDM disk if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.

   - Only a raw disk with the same size as the protected disk can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

   - The RDM is always stored in the recovery datastore used for the virtual machine.

   - The following **limitations** apply to protecting RDM disks:

     - RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.

     - RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.

   - **Volume Source > Preseeded volume.**
Whether to copy the protected data to a virtual disk in the recovery site. Zerto recommends using this option particularly for large disks so that the initial synchronization will be faster since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.

- **When not** using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN.
- **When using** a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk.
- Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.
- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.
- If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See the VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter using the command: `esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout`

**Note the following conditions:**

- If the protected disks are non-default geometry, configure the VPG using preseeded volumes.
- If the protected disk is an RDM disk, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, see [Zerto Cloud Manager Administration Guide](#).

**Datastore:** The datastore where the preseeded disk is located.

**Path:** The full path to the preseeded disk.

29. Continue with step 30.

30. Specify the **Volume Source** for recovery from one of the options.

- **vCD managed storage policy:** Zerto will select a datastore, from the list of available datastores, in the selected Storage Policy in which to place the Volume, unless the datastore is excluded in the Configure Provider vDCs Dialog.
  - If there are several valid datastores, the datastore with the most available space is selected.
  - Zerto recalculates the datastore available space for each volume sequentially, taking into consideration previously allocated volumes.

- **Preseeded volume:** A virtual disk (the VMDK flat file and descriptor) in the recovery site that has been prepared with a copy of the protected data. Zerto recommends using this option particularly for large disks so that the initial synchronization is much faster since a Delta Sync is used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When not using a preseeded disk the initial synchronization phase has to copy the whole disk over the WAN. Browse to the preseed folder configured for the customer and the disk name, of the preseeded disk. In order to use a preseeded VMDK, do the following:
  - Create a folder in vCD to use for the preseeded disks in the datastore you want to use for the customer.
  - Specify this datastore as a provider datastore for preseeded disks in the Configure Provider vDCs window, from the Advanced Settings window, as described in [Zerto Cloud Manager Administration Guide](#).
  - In the Zerto Cloud Manager specify the Preseed Folder Name for the ZORG, in the Manage ZORG tab. Zerto Virtual Replication searches for the preseeded folder in the available datastores in the Org vDCs specified in the vCD Cloud Resources for the ZORG in the Zerto Cloud Manager and takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Note that if the virtual machine has more than one preseeded disk, these disks must reside on the same datastore. If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS
storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds.

Refer to the VMware documentation, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919, which describes the configuration option to tune the RPC timeout parameter using the esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout command.

If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, refer to Zerto Cloud Manager Administration Guide.

Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified. Virtual machine RDMs in a vCenter Server are replicated as VMDKs in a vCD environment.

31. Specify the Storage Policy for recovery from one of the options. When selecting the Storage Policy, consider the following:
   - Storage Policy per volume is supported only in vCD supported versions, and when the selected Orgvdc is not configured for fast provisioning.
   - Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - The Storage Policies which appear in the drop-down list:
     - Include the Use VM Default option (default), which will apply the VM’s storage policy to this volume. This is also the Storage Policy default value.
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
     - Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.
   
   To review site-specific configurations, see Configure Provider vDCs Dialog.

32. If the virtual machine to be replicated includes a Temp Data disk as part of its configuration, select Temp Data disk to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

33. You can specify whether the recovery volume is thin-provisioned or not, unless the Org vDC only supports thin-provisioned volumes.

34. Click OK.

35. Click NEXT.

The RECOVERY step is displayed. Recovery details include the scripts that should be run either at the start or end of a recovery operation.

36. Select the default recovery settings.
   - **vCD Guest Customization**: When selected, VMware Guest OS Customization is enabled for the virtual machine in vCloud Director. Enabling guest customization means that the computer name and network settings configured for this virtual machine are applied to its Guest OS when the virtual machine is powered on. vCD Guest Customization must be selected to enable re-IPing the recovered virtual machines.

   **Copy NAT Rules**: When checked, NAT rules on source vCD vApp networks are copied to the recovery vCD vApp during recovery. One of the following options can be selected:
Use automatically allocated IP: Allow the recovery site to automatically assign an external IP.
Use source external IP: Copy the rule’s external IP as the external IP on the recovery site.
vApp Network Mapping: The networks to use for failover and move operations, for failover test operations, and for test failover operations after a failover or move when reverse protection is configured. The list of current Org Networks is displayed and you can specify what network to use in each of the situations. <Isolated> means that the network is an internal only vApp network.

37. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.
   - Pre-recovery Script: The information about a script that should run at the beginning of the recovery process.
   - Post-recovery Script: The information about a script that should run at the end of the recovery process.

For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>■ If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>■ The default time-out value is specified in Site Settings &gt; Performance and Throttling tab.</td>
</tr>
</tbody>
</table>

38. Click NEXT.

The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

39. To edit information in one field, click the field and update the information.

40. To edit information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED.

41. Otherwise, go to step step 44.
The Edit VNIC window is displayed.

42. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, specify the following:

- **Network**: The network to use for this virtual machine.
- **MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites.
- **vNIC IP Mode**: Which IP mode to use. Specify the IP address if you choose static IP pool.
  
  See the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-IP.

  During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP than the original IP, after the virtual machine has started it is automatically rebooted so that it starts up with the correct IP. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.

- **Copy to failover test**: Select this to copy the settings in the Failover/Move column to the Test column.
- **Copy to failover/move**: Select this to copy the settings in the Test column to the Failover/Move column.

43. Click OK.

44. 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.

45. By default, backup is OFF. To keep this value, go to step step 47.

46. Otherwise, toggle OFF to ON and enter the following information:
■ **Target Repository**: The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.

■ **Retention Period**: The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.

■ **Run Job Every**: The day and time to start the backup.

■ **Retries**: Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.

■ **Post-Backup Script**: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

47. Click **NEXT**. The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous steps.

48. Click **DONE**. The VPG is created.

For details of what happens after saving the VPG, see “What Happens After the VPG is Defined”, on page 36.

The virtual machines in the VPG are protected as a vCD vApp in the recovery site. When recovering the VPG, reverse protection is configured back the virtual machines.
Replication From a Protected Site vCD to a Recovery Site vCD

When both sites have vCloud Director installed, you can protect:

- Virtual machines in the underlying vCenter Server.
- vCD vApps. For details of protecting from vCD to a vCenter Server, refer to “Replication From a Protected Site vCD to a Recovery Site vCenter Server”, on page 131.

To create a VPG from and to vCloud Director:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - VPG Name: The VPG name must be unique. The name cannot be more than 80 characters.
   - 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.
     - High Priority: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - Medium Priority: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - Low Priority: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it. Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.

NOTES:

- When the vCD site is set up within Zerto Cloud Manager, as described in Zerto Cloud Manager Administration Guide, virtual machines in the underlying vCenter Server cannot be specified.
- When machines are protected as a vCD vApp in a recovery site vCD, certain vCD settings are retained. To review which settings are retained, see “vApp Settings Maintained when Replicating from a Protected Site vCD to a Recovery Site vCD”, on page 129.

NOTE:

The screen examples in the procedure below are based on VMware vCD version 5.6.3 and above, or 8.1 and above.
3. Click **NEXT**. The VMs step is displayed.

4. Select **vCloud Director** then select the vCD vApp to protect in this VPG. The protected vCD vApp is recovered as a vCD vApp.
   - Zerto Virtual Replication uses the **SCSI protocol**. Only virtual machines with disks that support this protocol can be specified.
   - When using the Search field, you can use the wildcards; * or ?.
   - The **boot order** for vCD vApps is defined in the **vCloud Director** console.
   - Only vCD vApps that are **unprotected** are displayed in the list. A VPG can include:
     - Only one vApp.
     - vApps that are **not yet** protected.
     - vApps that are **already** protected.

5. To view **protected** vApps, in the **Advanced (One-to-Many)** section, click **Select vApp**. The Select vApp window is displayed.

**Note:** With the One-to-Many feature, a VPG containing a single vApp can be recovered to a **maximum of three different sites** and **cannot be recovered to the same site more than once**.

vApps protected in the maximum number of VPGs are **not displayed** in the Select VMs window.
Protecting vApps in several VPGs is enabled only if both the protected and recovery sites, and the VRAs installed on these sites, are of version 5.0 and higher.

6. Click NEXT.

The REPLICATION step is displayed.

7. Select the recovery vCD site. The REPLICATION step is re-displayed, displaying additional fields relevant for vCD.

Define as follows:

8. **ZORG:** If the site is defined in Zerto Cloud Manager, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.

9. Specify the **Recovery Org vDC** to use in the recovery site.

   **Note:** You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

10. In the SLA area, you define the Service Level Agreement for which this VPG is associated.
   - When Zerto Cloud Manager is used, select the **Service Profile** to use.
     The Service Profile determines the VPG SLA settings for the group. This applies predefined settings for the Journal History, Target RPO Alert and the Test Reminder. These settings apply to every virtual machine in the group.
   - When a **Custom** service profile is available, the VPG SLA settings are editable, and the **Advanced** button becomes available. When you change these settings, they apply to every virtual machine in the group.

11. Click **ADVANCED**. The Advanced Journal Settings dialog is displayed.
Define as follows:

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Journal History</strong></td>
<td></td>
</tr>
</tbody>
</table>
| The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG. | Number of **hours** from 1 to 24  
Number of **days** from 2 to 30 |
| **Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)** |           |
| The storage/datastore used for the journal data for each virtual machine in the VPG. | Select the storage/datastore accessible to the host.  
When you select a specific journal storage/datastore, the journals for each virtual machine in the VPG are stored in this storage/datastore, regardless of where the recovery storage/datastore is for each virtual machine. All protected virtual machines are recovered to the hosts that can access the specified journal storage/datastore. |
| **Journal Size Hard Limit** |           |
| The maximum size that the journal can grow, either as a percentage or a fixed amount. The journal is always **thin-provisioned**. \n**Note:** The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume. \n**For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit. | **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.  
If Unlimited is selected, Size and Percentage options are **not** displayed.  
- **Size (GB):** The maximum journal size in GB.  
The **minimum** journal size, set by Zerto Virtual Replication, is **8GB** for Hyper-V and vSphere environments, and **10GB** for Microsoft Azure environments.  
- **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.  
This value can be configured to more than 100% of the protected VM's volume size. |

**Note:** This field is **not** relevant when replicating to a vCD recovery site.
119Replication From a Protected Site vCD to a Recovery Site vCD

Zerto Virtual Manager Administration Guide for VMware vSphere Environments -Version 6.0
Protecting Virtual Machines to and From vCloud Director

12. Target RPO Alert: The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

13. Test Reminder: The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

14. Enable WAN Traffic Compression: Whether or not data is compressed before being transferred to the recovery site. Compressing the data is more efficient, but results in a small performance degradation.
   - Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
   - When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
   - Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
   - When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

15. Journal Size Warning Threshold
   The size of the journal that triggers a warning that the journal is nearing its hard limit.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unlimited: The size of the journal is</td>
<td></td>
</tr>
<tr>
<td>unlimited and it can grow to the size</td>
<td></td>
</tr>
<tr>
<td>of the recovery storage/datastore.</td>
<td></td>
</tr>
<tr>
<td>If Unlimited is selected, Size and</td>
<td></td>
</tr>
<tr>
<td>Percentage options are not displayed.</td>
<td></td>
</tr>
<tr>
<td>Size* (GB): The size in GB that will</td>
<td></td>
</tr>
<tr>
<td>generate a warning.</td>
<td></td>
</tr>
<tr>
<td>Percentage*: The percentage of the</td>
<td></td>
</tr>
<tr>
<td>virtual machine volume size that will</td>
<td></td>
</tr>
<tr>
<td>generate a warning.</td>
<td></td>
</tr>
<tr>
<td>*The values of Size and Percentage must</td>
<td></td>
</tr>
<tr>
<td>be less than the configured Journal</td>
<td></td>
</tr>
<tr>
<td>Size Hard Limit so that the warning</td>
<td></td>
</tr>
<tr>
<td>will be generated when needed.</td>
<td></td>
</tr>
<tr>
<td>In addition to the warning threshold,</td>
<td></td>
</tr>
<tr>
<td>Zerto Virtual Replication will issue a</td>
<td></td>
</tr>
<tr>
<td>message when the free space available</td>
<td></td>
</tr>
<tr>
<td>for the journal is almost full.</td>
<td></td>
</tr>
</tbody>
</table>

16. To change the replication settings per virtual machine, click VM SETTINGS.
The Advanced VM Replication Settings window is displayed.
In this window, you can edit the values of one or more of the virtual machines in the VPG.

17. To edit information for a **single** VM, click the field **Storage Policy**, and/or **Journal Storage Policy**, and update the information.

   - **Storage Policy**: The Storage Policy in which the **VM configuration files** will reside. For considerations, see step 19.
   - **Journal Storage Policy**: The Storage Policy in which the **VM Journal files** will reside. For considerations, see step 20.

18. To edit information for **several** virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

The Edit VM window is displayed.

19. When selecting **Storage Policy**, consider the following:

   - Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - Zerto will try to determine a default Storage Policy according to:
     - A Storage Policy with the same name as the protected Storage Policy.
     - The default Orgvdv Storage Policy.
   
   If Zerto did not manage to determine a default Storage Policy, this field appears empty.

   - When you **click to edit**, a list of Storage Policies appear. These Storage Policies:
     - Were defined in VMware vCloud Director and are configured in the Orgvdv.
     - Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.
     - To review site-specific configurations, see **Configure Provider vDCs Dialog**.
20. When selecting **Journal Storage Policy**, consider the following:

- Zerto will select a datastore from the selected Storage Policy in which to place the Journal files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
- The default Journal Storage Policy is the same as the default VM Storage Policy.
- If Zerto did not manage to determine a default Journal Storage Policy, this field appears empty.
- When you **click to edit**, the option **Auto Select** appears, and a list of Storage Policies.
- The list of Storage Policies associated with the Journal:
  - Were defined in VMware vCloud Director and are configured in the Orgvdc.
  - Have at least one Datastore that was not excluded as a **Journal** in the Configure Provider vDCs Dialog.
- **Auto Select**: Selecting this means that the journal can be placed in any datastore visible to the host that Zerto selected for recovery, unless the datastore is excluded in the Configure Provider vDCs Dialog.

### SETTING & DESCRIPTION

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Recovery Host</strong> (not relevant when replicating to vCD)</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.</td>
</tr>
<tr>
<td><em>(Hyper-V)</em> The cluster or host that will host the recovered virtual machine.</td>
<td>If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.</td>
</tr>
<tr>
<td><em>(vSphere)</em> The cluster, resource pool, or host that will host the recovered virtual machine.</td>
<td>All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.</td>
</tr>
</tbody>
</table>

**If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager.**

For details about Zerto Cloud Manager, see **Zerto Cloud Manager Administration Guide**.

When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.

### VM Recovery Datastore *(vSphere)* (not relevant when replicating to vCD)

The datastore where the VMware metadata files for the virtual machine are stored, such as the VMX file.

If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located.

### Recovery Storage *(Hyper-V)*

The location where the metadata files for the virtual machine are stored, such as the VHDX file.

If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed.
### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

- The journal is always **thin-provisioned**.
- The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume.

**For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

<table>
<thead>
<tr>
<th>Setting &amp; Description</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong> The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.</td>
<td></td>
</tr>
<tr>
<td><strong>Size (GB):</strong> The maximum journal size in GB. - The minimum journal size, set by Zerto Virtual Replication, is <strong>8GB</strong> for Hyper-V and vSphere environments, and <strong>10GB</strong> for Microsoft Azure environments.</td>
<td></td>
</tr>
<tr>
<td><strong>Percentage:</strong> The percentage of the virtual machine volume size to which the journal can grow. - This value can be configured to more than 100% of the protected VM's volume size.</td>
<td></td>
</tr>
</tbody>
</table>

### Journal Size Warning Threshold

The size of the journal that triggers a warning that the journal is nearing its hard limit.

<table>
<thead>
<tr>
<th>Setting &amp; Description</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong> The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.</td>
<td></td>
</tr>
<tr>
<td><em><em>Size</em> (GB):</em>* The size in GB that will generate a warning.</td>
<td></td>
</tr>
<tr>
<td><em><em>Percentage</em>:</em>* The percentage of the virtual machine volume size that will generate a warning. - The values of Size and Percentage must be less than the configured Journal Size Hard Limit so that the warning will be generated when needed.</td>
<td></td>
</tr>
</tbody>
</table>

In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.

### Journal Storage (Hyper-V), or Journal Datastore (vSphere) (not relevant when replicating to vCD)

The storage/datastore used for the journal data for each virtual machine in the VPG.

<table>
<thead>
<tr>
<th>Setting &amp; Description</th>
<th>Select...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(vSphere) To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore.</td>
<td></td>
</tr>
<tr>
<td>(Hyper-V) To change the default, specify a host and then select the storage location accessible by this host to be used as the journal storage. When you select specific journal storage, the journals for each virtual machine in the VPG are stored in this storage, regardless of where the recovery storage is for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal storage.</td>
<td></td>
</tr>
</tbody>
</table>

21. In the Advanced VM Replication Settings window, click **OK**.
22. Click **NEXT**.

The STORAGE step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

**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.

You can define **Thin** provisioning and **Temp Data** in this window, or you can alternatively define them when you separately select and edit each VMs volume.

**IMPORTANT:**

Changing the VPG recovery volume from thin-provisioned to thick-provisioned or vice versa, results in **volume initial synchronization**.

See the following considerations regarding Thin provisioning:

- Unless the user **explicitly** requests Thin provisioning, provisioning type is the same type as provisioning in the **source VM**.
- If the **source** disk is Thin provisioned, the default for the **recovery** volume is also Thin provisioned.
- If the user uses preseed disks, Zerto maintains the provisioning types of the disks, so they can have other provisioning types.

<table>
<thead>
<tr>
<th><strong>PRESEED</strong></th>
<th><strong>PROVISIONING IN THE RECOVERY VM</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Not selected</td>
<td>User <strong>can</strong> select Thin provisioning</td>
</tr>
<tr>
<td>Selected</td>
<td>User <strong>cannot</strong> select Thin provisioning</td>
</tr>
<tr>
<td></td>
<td>Provisioning is the same as defined in source VMs</td>
</tr>
</tbody>
</table>

23. To define whether the recovery volumes are thin-provisioned or not, select the **Thin** checkbox.

24. If the virtual machine to be replicated includes a temp data disk as part of its configuration, select the **Temp Data** checkbox to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

25. To edit storage information for one of the virtual machines volumes, select the volume/s and click **EDIT SELECTED**.
When protecting to vCenter, the following Edit Volumes window is displayed. Continue with step 26.

When protecting to vCD environments, the following Edit Volumes window is displayed. Continue with step 28.

26. **Volume Source**: The source on the recovery site for the replicated data: **Datastore, RDM or Preseeded volume**.
   - Volume Source > **Datastore**.

**Datastore**: A new volume is used for replicated data. Specify the datastore to use to create disks for the replicated data. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned. The datastore specified for replication must have at least the same amount of space as the protected volume and an additional amount for the journal. The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.

You can use the vSphere Client console **Performance** tab for each virtual machine to help estimate the change rate. For more details, see the section **Collecting Data Characteristics for VMs**.

Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

   - Volume Source > **RDM**.

**Raw Disk**: The VMware RDM (Raw Device Mapping) to use for the replication.
   - By default, RDM is recovered as **thin-provisioned** VMDK in the datastore specified in the **VM Recovery Datastore** field in the Edit VM dialog, and **not to RDM**.
   - You cannot define an RDM disk if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.
   - Only a raw disk with the same size as the protected disk can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.
   - The RDM is always stored in the recovery datastore used for the virtual machine.
   - The following **limitations** apply to protecting RDM disks:
     - RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
     - RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.
Volume Source > Preseeded volume.

Whether to copy the protected data to a virtual disk in the recovery site. Zerto recommends using this option particularly for large disks so that the initial synchronization will be faster since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.

- When not using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN.
- When using a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk.
- Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.
- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.
- If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See the VMware documentation, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919, which describes the configuration option to tune the RPC timeout parameter using the command:

```bash
esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout
```

Note the following conditions:

- If the protected disks are non-default geometry, configure the VPG using preseeded volumes.
- If the protected disk is an RDM disk, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, see Zerto Cloud Manager Administration Guide.

Datastore: The datastore where the preseeded disk is located.
Path: The full path to the preseeded disk.

27. Continue with step 30.
28. Specify the Volume Source for recovery from one of the options.

vCD managed storage policy: Zerto will select a datastore, from the list of available datastores, in the selected Storage Policy in which to place the Volume, unless the datastore is excluded in the Configure Provider vDCs Dialog.

- If there are several valid datastores, the datastore with the most available space is selected.
- Zerto recalculates the datastore available space for each volume sequentially, taking into consideration previously allocated volumes.

Preseeded volume: A virtual disk (the VMDK flat file and descriptor) in the recovery site that has been prepared with a copy of the protected data. Zerto recommends using this option particularly for large disks so that the initial synchronization is much faster since a Delta Sync is used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When not using a preseeded disk the initial synchronization phase has to copy the whole disk over the WAN. Browse to the preseed folder configured for the customer and the disk name, of the preseeded disk. In order to use a preseeded VMDK, do the following:

- Create a folder in vCD to use for the preseeded disks in the datastore you want to use for the customer.
Specify this datastore as a provider datastore for preseeded disks in the Configure Provider vDCs window, from the Advanced Settings window, as described in Zerto Cloud Manager Administration Guide.

■ In the Zerto Cloud Manager specify the Preseed Folder Name for the ZORG, in the Manage ZORG tab.

Zerto Virtual Replication searches for the preseeded folder in the available datastores in the Org vDCs specified in the vCD Cloud Resources for the ZORG in the Zerto Cloud Manager and takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Note that if the virtual machine has more than one preseeded disk, these disks must reside on the same datastore. If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds.

Refer to the VMware documentation, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919, which describes the configuration option to tune the RPC timeout parameter using the esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout command.

If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, refer to Zerto Cloud Manager Administration Guide. Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified. Virtual machine RDMs in a vCenter Server are replicated as VMDKs in a vCD environment.

29. Specify the Storage Policy for recovery from one of the options. When selecting the Storage Policy, consider the following:

■ Storage Policy per volume is supported only in vCD supported versions, and when the selected Orgvdc is not configured for fast provisioning.

■ Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.

■ The Storage Policies which appear in the drop-down list:

- Include the Use VM Default option (default), which will apply the VM's storage policy to this volume. This is also the Storage Policy default value.

- Were defined in VMware vCloud Director and are configured in the Orgvdc.

- Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.

To review site-specific configurations, see Configure Provider vDCs Dialog.

30. If the virtual machine to be replicated includes a Temp Data disk as part of its configuration, select Temp Data disk to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

31. You can specify whether the recovery volume is thin-provisioned or not, unless the Org vDC only supports thin-provisioned volumes.

32. Click OK.

33. Click NEXT.

The RECOVERY step is displayed. Recovery details include the scripts that should be run either at the start or end of a recovery operation.
34. Select the default recovery settings.
   - **vCD Guest Customization**: When selected, VMware Guest OS Customization is enabled for the virtual machine in vCloud Director. Enabling guest customization means that the computer name and network settings configured for this virtual machine are applied to its Guest OS when the virtual machine is powered on. vCD Guest Customization must be selected to enable **re-IPing** the recovered virtual machines.
   - **Copy NAT Rules**: When checked, NAT rules on source vCD vApp networks are copied to the recovery vCD vApp during recovery. One of the following options can be selected:
     - **Use automatically allocated IP**: Allow the recovery site to automatically assign an external IP.
     - **Use source external IP**: Copy the rule’s external IP as the external IP on the recovery site.
   - **vApp Network Mapping**: The networks to use for failover and move operations, for failover test operations, and for test failover operations after a failover or move when reverse protection is configured. The list of current Org Networks is displayed and you can specify what network to use in each of the situations. **<Isolated>** means that the network is an internal only vApp network.

35. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.
   - **Pre-recovery Script**: The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script**: The information about a script that should run at the end of the recovery process.

   For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>- The default time-out value is specified in <strong>Site Settings &gt; Performance and Throttling</strong> tab.</td>
</tr>
</tbody>
</table>

36. Click **NEXT**.

   The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

37. To edit information in one field, click the field and update the information.
38. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**. Otherwise, go to step **step 44**.
39. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, specify the following:

- **Network**: The network to use for this virtual machine.
- **MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites.
- **vNIC IP Mode**: Which IP mode to use. Specify the IP address if you choose static IP pool. See the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-IP.
  
  During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP than the original IP, after the virtual machine has started it is automatically rebooted so that it starts up with the correct IP. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.
- **Copy to failover test**: Select this to copy the settings in the Failover/Move column to the Test column.
- **Copy to failover/move**: Select this to copy the settings in the Test column to the Failover/Move column.

40. Click **OK**.

41. 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.

42. By default, backup is **OFF**. To keep this value, go to step **step 47**.
43. Otherwise, toggle OFF to ON and enter the following information:
   - **Target Repository:** The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
   - **Retention Period:** The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
   - **Run Job Every:** The day and time to start the backup.
   - **Retries:** Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
   - **Post-Backup Script:** The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

44. Click NEXT.

   The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous steps.

45. Click DONE. The VPG is created.

### vApp Settings Maintained when Replicating from a Protected Site vCD to a Recovery Site vCD

The following tables display settings that are retained when replicating from a protected site vCloud Director to a recovery site vCloud Director:

- **Edge Gateway Services, on page 129**
- **vApp Properties, on page 129**
- **Network, on page 130**
- **VM Properties, on page 130**

#### Edge Gateway Services

<table>
<thead>
<tr>
<th>SETTING</th>
<th>SETTING RETAINED?</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP</td>
<td>No</td>
</tr>
<tr>
<td>Firewall</td>
<td>No</td>
</tr>
<tr>
<td>Static Routing</td>
<td>No</td>
</tr>
<tr>
<td>NAT</td>
<td>Configurable</td>
</tr>
</tbody>
</table>

#### vApp Properties

<table>
<thead>
<tr>
<th>SETTING</th>
<th>SETTING RETAINED?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Leases (Runtime / Storage)</td>
<td>No</td>
</tr>
<tr>
<td>vApp Description</td>
<td>No</td>
</tr>
<tr>
<td>VM Start / Stop</td>
<td>Yes</td>
</tr>
<tr>
<td>Sharing</td>
<td>No</td>
</tr>
<tr>
<td>Metadata</td>
<td>Yes</td>
</tr>
</tbody>
</table>
### Network

<table>
<thead>
<tr>
<th>SETTING</th>
<th>SETTING RETAINED?</th>
</tr>
</thead>
<tbody>
<tr>
<td>ORG Network</td>
<td>No</td>
</tr>
<tr>
<td></td>
<td>(protected ORG vDC networks need to be mapped to recovery ORG vDC networks)</td>
</tr>
<tr>
<td>Isolated vApp network</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(same gateway address used)</td>
</tr>
<tr>
<td>Routed vApp Network</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(same gateway address used, routed organization network mapped)</td>
</tr>
<tr>
<td>vApp Network Without NIC On It</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>(same gateway address used)</td>
</tr>
</tbody>
</table>

### VM Properties

<table>
<thead>
<tr>
<th>SETTING</th>
<th>SETTING RETAINED?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata and Description</td>
<td>No</td>
</tr>
</tbody>
</table>
Replication From a Protected Site vCD to a Recovery Site vCenter Server

If you want to recover to a vCenter Server, the vCD vApp is replicated in the recovery site as individual VMs.

To create a VPG to protect a vCD vApp to a vCenter Server:
1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it.

   Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
   During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click NEXT.
The VMs step is displayed.

4. Select the VMs or vCD vApp that will be part of this VPG and click the arrow pointing right to include these VMs in the VPG. The protected virtual machines are recovered as a vCD vApp.
   - Zerto Virtual Replication uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.
   - When using the Search field, you can use the wildcards; * or ?.
   - Only vCD vApps that are unprotected are displayed in the list. A VPG can include:
     - Only one vApp.
     - vApps that are not yet protected.
     - vApps that are already protected.

5. To view protected vApps, in the Advanced (One-to-Many) section, click Select vApp. The Select vApp window is displayed.

   Note: With the One-to-Many feature, a VPG containing a single vApp can be recovered to a maximum of three different sites and cannot be recovered to the same site more than once.
   vApps protected in the maximum number of VPGs are not displayed in the Select VMs window.
Protecting vApps in several VPGs is enabled only if both the protected and recovery sites, and the VRAs installed on these sites, are of version 5.0 and higher.

**Note:** Define any required boot order for vCD vApps in the vCloud Director console.

6. Click **NEXT**.

The REPLICATION step is displayed.

![Create VPG: asfd](image)

**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 SLA and Advanced settings, as shown below.

7. Specify the recovery site and default values to use for the replication to this site.

- **Recovery Site:** The site to which you want to recover the virtual machines. After specifying the recovery site, other fields are displayed including the host and datastore to use for replication.

8. **ZORG:** If the site is defined in Zerto Cloud Manager, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.

   You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

9. **Host:** The default cluster, resource pool or host in the recovery site that handles the replicated data. If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been specified as a resource in Zerto Cloud Manager.

   **Note:** If Zerto Cloud Manager is used, vSphere Standard edition cannot be used.

   For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.
When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for any virtual machines specified in the VPG.

All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are specified as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.

**Note:** If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery will be to any one of the hosts in the recovery site with a VRA installed on it.

10. **Datastore:** The default datastore to use for recovered virtual machine files and for their data volumes. Every datastore for the selected recovery host is included in the drop-down list. If a cluster or resource pool is selected for the host, only datastores that are accessible by every host in the cluster or resource pool are displayed.

11. In the **SLA** area, you define the Service Level Agreement for which this VPG is associated.
   - **When Zerto Cloud Manager** is used, select the **Service Profile** to use. The Service Profile determines the VPG SLA settings for the group. This applies predefined settings for the Journal History, Target RPO Alert and the Test Reminder. These settings apply to every virtual machine in the group.
   - **When a Custom** service profile is available, the VPG SLA settings are editable, and the **Advanced** button becomes available. When you change these settings, they apply to every virtual machine in the group.

12. Click **ADVANCED.** The Advanced Journal Settings dialog is displayed.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Journal History</strong></td>
<td></td>
</tr>
</tbody>
</table>
| The time that all write commands are saved in the journal. | Number of **hours** from **1** to **24**
| The longer the information is saved in the journal, the more space is required for each journal in the VPG. | Number of **days** from **2** to **30**

<table>
<thead>
<tr>
<th><strong>Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>The storage/datastore used for the journal data for each virtual machine in the VPG.</td>
<td>Select the storage/datastore accessible to the host. When you select a specific journal storage/datastore, the journals for each virtual machine in the VPG are stored in this storage/datastore, regardless of where the recovery storage/datastore is for each virtual machine. All protected virtual machines are recovered to the hosts that can access the specified journal storage/datastore.</td>
</tr>
<tr>
<td><strong>Note:</strong> This field is <strong>not</strong> relevant when replicating to a <strong>vCD</strong> recovery site.</td>
<td></td>
</tr>
</tbody>
</table>
### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount.

The journal is always **thin-provisioned**.

**Note:** The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.

**For Example:** If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong></td>
<td>The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.</td>
</tr>
<tr>
<td><strong>Size (GB):</strong></td>
<td>The <strong>minimum</strong> journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.</td>
</tr>
<tr>
<td><strong>Percentage:</strong></td>
<td>The percentage of the virtual machine volume size to which the journal can grow.</td>
</tr>
<tr>
<td><em><em>Percentage</em>:</em>*</td>
<td>This value can be configured to more than 100% of the protected VM's volume size.</td>
</tr>
</tbody>
</table>

### Journal Size Warning Threshold

The size of the journal that triggers a warning that the journal is nearing its hard limit.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong></td>
<td>The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.</td>
</tr>
<tr>
<td><em><em>Size</em> (GB):</em>*</td>
<td>The size in GB that will generate a warning.</td>
</tr>
<tr>
<td><em><em>Percentage</em>:</em>*</td>
<td>The percentage of the virtual machine volume size that will generate a warning.</td>
</tr>
</tbody>
</table>

*The values of **Size** and **Percentage** must be less than the configured **Journal Size Hard Limit** so that the warning will be generated when needed.

In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.

---

13. **Target RPO Alert:** The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

14. **Test Reminder:** The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

15. **Enable WAN Traffic Compression:** Whether or not data is compressed before being transferred to the recovery site.

Compressing the data is more efficient, but results in a small performance degradation.

- Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
- When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
- Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
- When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

16. To change the replication settings per virtual machine, click **VM SETTINGS**.
The Advanced VM Replication Settings window is displayed.

In this window, you can edit the values of one or more of the virtual machines in the VPG. All the virtual machines from a vCD vApp are displayed.

17. To edit information in one field, click the field and update the information.

18. To edit information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED.

The Edit VM window is displayed.

19. Configure as follows:

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Host (not relevant when replicating to vCD)</td>
<td>(Hyper-V) The cluster or host that will host the recovered virtual machine.</td>
</tr>
</tbody>
</table>

(Continued on the next page...)

Replication From a Protected Site vCD to a Recovery Site vCenter Server
The cluster, resource pool, or host that will host the recovered virtual machine.

If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager.

For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.

When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.

When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG.

If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it.

All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.

The datastore where the VMware metadata files for the virtual machine are stored, such as the VMX file.

If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located.

The location where the metadata files for the virtual machine are stored, such as the VHDX file.

If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed.

The maximum size that the journal can grow, either as a percentage or a fixed amount.

- The journal is always thin-provisioned.
- The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.

For Example: If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

- Unlimited: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.
- If Unlimited is selected, Size and Percentage options are not displayed.

Size (GB): The maximum journal size in GB.

- The minimum journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.

Percentage: The percentage of the virtual machine volume size to which the journal can grow.

- This value can be configured to more than 100% of the protected VM’s volume size.
20. Click **OK**.
21. In the Advanced VM Replication Settings window, click **OK**.
22. Click **NEXT**.

The STORAGE step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data.

For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

### Journal Size Warning Threshold

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Journal Size Warning Threshold</td>
<td>Unlimited: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are <strong>not</strong> displayed. Size* (GB): The size in GB that will generate a warning. Percentage*: The percentage of the virtual machine volume size that will generate a warning. *The values of Size and Percentage must be <strong>less</strong> than the configured Journal Size Hard Limit so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.</td>
</tr>
</tbody>
</table>

### Journal Storage (Hyper-V), or Journal Datastore (vSphere) (not relevant when replicating to vCD)

The storage/datastore used for the journal data for each virtual machine in the VPG.

**Hyper-V** To change the default, specify a host and then select the storage location accessible by this host to be used as the journal storage. When you select specific journal storage, the journals for each virtual machine in the VPG are stored in this storage, regardless of where the recovery storage is for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal storage.

**vSphere** To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore.
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.

You can define **Thin** provisioning and **Temp Data** in this window, or you can alternatively define them when you separately select and edit each VMs volume.

### IMPORTANT:

Changing the VPG recovery volume from thin-provisioned to thick-provisioned or vice versa, results in **volume initial synchronization**.

See the following considerations regarding Thin provisioning:
- Unless the user explicitly requests Thin provisioning, provisioning type is the same type as provisioning in the **source VM**.
- If the **source** disk is Thin provisioned, the default for the **recovery** volume is also Thin provisioned.
- If the user uses preseed disks, Zerto maintains the provisioning types of the disks, so they can have other provisioning types.

<table>
<thead>
<tr>
<th>PRESEED</th>
<th>PROVISIONING IN THE RECOVERY VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not selected</td>
<td>User can select Thin provisioning</td>
</tr>
<tr>
<td>Selected</td>
<td>User <strong>cannot</strong> select Thin provisioning</td>
</tr>
<tr>
<td></td>
<td>Provisioning is the <strong>same</strong> as defined in source VMs</td>
</tr>
</tbody>
</table>

23. To define whether the recovery volumes are thin-provisioned or not, select the **Thin** checkbox.

24. If the virtual machine to be replicated includes a temp data disk as part of its configuration, select the **Temp Data** checkbox to mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

25. To edit storage information for one of the virtual machines' volume location, first select the virtual machine, then click **EDIT SELECTED**. The Edit Volumes window is displayed.

- In Hyper-V environments, the following window appears.

- In vSphere environments, the following window appears.
**Prerequisites: Replication From a Protected Site vCD to a Recovery Site vCenter Server**

Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk. The storage where the preseeded disk is placed is also used as the recovery storage for the replicated data.

### Volume Source

- **Select a Volume Source for recovery from one of the drop-down options:**
  - **Storage**
  - **Preseeded volume**

#### Volume Source > Storage:
A new volume is used for replicated data. From the Storage drop-down list, specify the storage to use to create disks for the replicated data.

The storage specified for the replication must have at least the same amount of space as the protected volume and then an additional amount for the journal.

The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.

#### Volume Source > Preseeded volume:
Whether to copy the protected data to a virtual disk in the recovery site.

Zerto recommends using this option particularly for large disks so that the initial synchronization will be faster since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.

When not using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN.

When using a preseeded virtual disk, you select the storage and exact location, folder, and name of the preseeded disk.

Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
(vSphere) Select a **Volume Source** for recovery from one of the drop-down options:

- **Datastore**
- **RDM**
- **Preseeded volume**

**Volume Source > Datastore:** A new volume is used for replicated data.

- Specify the **Datastore** to use to create disks for the replicated data.
- If the **source disk is thin provisioned**, the default for the recovery volume is also thin provisioned.
- The datastore specified for replication must have at least the same amount of space as the **protected volume** and an additional amount for the **journal**.
- The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.
- Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

Then, define the following:

- **Datastore:** The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.

**Volume Source > RDM:** The VMware RDM (Raw Device Mapping) which will be used for the replication.

By default, **RDM is recovered as thin-provisioned VMDK** in the datastore specified in the **VM Recovery Datastore/Storage** field in the Edit VM dialog, and not to RDM.

Only a raw disk with the **same size as the protected disk** can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

The RDM is always stored in the recovery datastore, used for the virtual machine.

The following **limitations** apply to protecting RDM disks:

- RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
- RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.
- You cannot define an RDM disk to be protected to a cloud service provider via a Zerto Cloud Connector nor if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.
Consider the following, then proceed to define the Datastore and the Path:

- **Zerto recommends** using this option particularly for **large disks** so that the initial synchronization is **faster** since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.

- If a preseeded disk is **not** selected, the initial synchronization phase must copy the **whole disk** over the WAN.

- If you use a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.

- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.

- If the preseeded disk is **greater than 1TB on NFS storage**, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter by using the command: `esxcfg-advcfg -s <Timeout>/NFS/SetAttrRPCTimeout`

- If the protected disks are **non-default geometry**, configure the VPG using preseeded volumes.

- If the protected disk is an **RDM disk**, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.

- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. See [Zerto Cloud Manager Administration Guide](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919).

Then, define the following:

- **Datastore**: The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.

- **Path**: The full path to the preseeded disk.
You can use the vSphere Client console Performance tab for each virtual machine to help estimate the change rate. For more details, refer to “WAN Sizing Requirements with Zerto Virtual Replication”, on page 26.

26. Click OK.
27. Click NEXT.

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

28. Select the default recovery settings. These are applied to every virtual machine in the VPG.
   - **Failover/Move Network**: The network to use during a failover or move operation in which the recovered virtual machines will run.
   - **Failover Test Network**: The network to use when testing the failover of virtual machines in the recovery site. Zerto recommends using a fenced-out network so as not to impact the production network at this site.

29. **Recovery Folder**: The folder to which the virtual machines are recovered.
   - **Note**: If the recovery site is a cloud service provider site, it is not possible to select a recovery folder.

30. To specify a recovery folder for each virtual machine in the VPG, click VM SETTINGS.
The Advanced VM Recovery Settings window is displayed.

In this window, you can edit the values of one or more of the virtual machines in the VPG.

31. To edit information in **one field**, click the field and update the information.
32. To edit information for **several virtual machines** at the same time, select the virtual machines and click **EDIT SELECTED**. The Edit VM window is displayed.

- **Recovery Folder**: The folder to which the virtual machine is recovered.

33. Click **SAVE**.
34. In the Advanced VM Recovery Settings window, click **OK**.
35. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.
   - **Pre-recovery Script**: The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script**: The information about a script that should run at the end of the recovery process.

For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Params</td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
</tbody>
</table>

- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.
- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.
- The default time-out value is specified in **Site Settings > Performance and Throttling** tab.

36. Click **NEXT**.
The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

37. To edit information in one field, click the field and update the information.
38. To edit information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED.
39. Otherwise, go to step 42.

The Edit vNIC window is displayed.

40. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, specify the following:

- **Network:** The network to use for this virtual machine.
- **Create New MAC Address:** Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites. Note that if you check this option, to create a new MAC address, and the current IP address is not specified, the protected virtual machine static IP address might not be used for the recovered virtual machine.
- **Change vNIC IP Configuration:** Whether or not to keep the default virtual NIC (vNIC) IP configuration. The vNIC IP is only changed after recovery for virtual machines with VMware Tools running.

See the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports Re-IPing.
To change the vNIC IP, in the Failover/Move or Test column, select Yes. If you select to use a static IP connection, set the IP address, subnet mask, and default gateway.

Optionally, change the preferred and alternate DNS server IPs and the DNS suffix.

If you leave the DNS server and suffix entries empty, or select to use DHCP, the IP configuration and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the Default gateway field for the NICs with no default gateway.

During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP than the original IP, after the virtual machine has started it is automatically rebooted so that it starts up with the correct IP. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.

Copy to failover test: Select this to copy the settings in the Failover/Move column to the Test column.

Copy to failover/move: Select this to copy the settings in the Test column to the Failover/Move column.

41. Click OK.
42. 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.

43. By default, backup is OFF. To keep this value, go to step 45.
44. Otherwise, toggle OFF to ON and enter the following information:

- **Target Repository:** The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
- **Retention Period:** The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
- **Run Job Every:** The day and time to start the backup.
- **Retries:** Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
- **Post-Backup Script:** The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>
45. Click **NEXT**.

   The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

46. Click **DONE**. The VPG is created.

For details of what happens after saving the VPG, see “What Happens After the VPG is Defined”, on page 36.
Replication From a Protected Site vCD to Hyper-V

When creating a VPG from a vCD to Hyper-V, all recovery operations bring up the recovered machines on Microsoft Hyper-V hosts.

When protecting a vCD vApp to Hyper-V, the operating systems of the protected machines must be supported by Hyper-V. Refer to Hyper-V documentation for the list of supported operating systems. Also, virtual machine names cannot include any of the following special characters: * ? : <> | \ ".

The following conversions are done to a protected virtual machine when it is recovered in Hyper-V:

- A machine using BIOS is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine using EUFI is recovered in Hyper-V as a Generation 2 virtual machine.
- A vCD vApp machine with a 32bit operating system is recovered in Hyper-V as a Generation 1 virtual machine.
- A vCD vApp machine with a 64bit operating system is recovered in Hyper-V as either a Generation 1 or Generation 2 virtual machine, dependent on the operating system support in Hyper-V.
- The boot disk is ported to a disk on an IDE controller. The boot location is 0:0.
- A vCD vApp virtual machine using up to 4 SCSI controllers is recovered as a virtual machine with 1 SCSI controller.
- The vCD vApp virtual machine NICs are recovered with Hyper-V network adapters except for protected Windows 2003 virtual machines which are recovered with Hyper-V legacy network adapters.
- When VMware Tools is installed on the protected vCD vApp virtual machine running Windows Server 2012, Integration Services is installed on the recovered virtual machine automatically.

To create a VPG to protect a vCD vApp to Hyper-V:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name:** The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority:** When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority:** Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority:** Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it.
   Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.
   During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.
3. Click **NEXT**.

   The VMs step is displayed.

4. Select the vCD vApp to protect in this VPG. The protected vCD vApp is recovered as a vCD vApp.
   - Zerto Virtual Replication uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.
   - When using the Search field, you can use the wildcards; * or ?.
   - Only vCD vApps that are unprotected are displayed in the list. A VPG can include:
     - Only one vApp.
     - vApps that are not yet protected.
     - vApps that are already protected.

5. To view protected vApps, in the **Advanced (One-to-Many)** section, click **Select vApp**.

   The Select vApp window is displayed.

   **Note:** With the One-to-Many feature, a VPG containing a single vApp can be recovered to a **maximum of three different sites** and **cannot be recovered to the same site more than once**.

   vApps protected in the maximum number of VPGs are not displayed in the Select VMs window.
Protecting vApps in **several VPGs** is enabled **only if both** the protected and recovery sites, **and** the VRAs installed on these sites, are of **version 5.0 and higher**.

6. Select the vCD vApp to protect in this VPG.
   **Note:** Define the required boot order for vCD vApps in the vCloud Director console.

7. Click **NEXT**.
   The **REPLICATION** step is displayed.

![Create VPG](image)

**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 SLA and Advanced settings, as shown below.

8. Specify the recovery site and default values to use for the replication to this site.
   - **Recovery Site:** The site to which you want to recover the virtual machines. After specifying the Microsoft SCVMM recovery site, the host and storage on the site to use for the replication can be specified.

![Create VPG: VPG1](image)

**Note:** You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.
   - **Host:** The default cluster or host, in the recovery site that handles the replicated data.
   - **Storage:** The default storage volume to use for the recovered virtual machine files and for their data volumes. Every storage for the recovery host is included in the drop-down list. If a cluster is selected for the host, only storage accessible by every host in the cluster are displayed.
9. **ZORG:** If the site is defined in Zerto Cloud Manager, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see Zerto Cloud Manager Administration Guide.

10. Optionally, change the VPG SLA settings, which apply to every virtual machine in the group.
    - **Journal History:** The time that all write commands are saved in the journal.
      The longer the information is saved in the journal, the more space is required for each journal in the VPG.
      Select the number of **hours** from 1 to 24 or the number of **days** from 2 to 30.

11. For additional journal-related fields, click ADVANCED.
    The Advanced Journal Settings dialog is displayed.

    ![Advanced Journal Settings Dialog](image)

    - Configure as follows:

    | SETTING & DESCRIPTION          | SELECT...                                      |
    |--------------------------------|------------------------------------------------|
    | **Journal History**            | • Number of **hours** from 1 to 24             |
    |                                | • Number of **days** from 2 to 30             |
    | **Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)** | • Select the storage/datastore accessible to the host. |
    | **Note:** This field is *not* relevant when replicating to a vCD recovery site. |
    | **Journal Size Hard Limit**    | • **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. |
    |                                | If Unlimited is selected, Size and Percentage options are *not* displayed. |
    |                                | • **Size (GB):** The maximum journal size in GB. |
    |                                |     • The *minimum* journal size, set by Zerto Virtual Replication, is **8GB** for Hyper-V and vSphere environments, and **10GB** for Microsoft Azure environments. |
    |                                | • **Percentage:** The percentage of the virtual machine volume size to which the journal can grow. |
    |                                |     • This value can be configured to more than 100% of the protected VM’s volume size. |
12. **Target RPO Alert:** The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

13. **Test Reminder:** The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

14. **Enable WAN Traffic Compression:** Whether or not data is compressed before being transferred to the recovery site. Compressing the data is more efficient, but results in a small performance degradation.

   - Enable WAN traffic compression if network considerations are more critical than CPU usage considerations.
   - When WAN compression is enabled, the compressed data is written in compressed format to the recovery site journal. Even if WAN compression is selected, Zerto Virtual Replication decreases the level of compression if it takes too many resources. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed. Zerto recommends enabling WAN compression.
   - Zerto Virtual Replication can also work with third-party WAN optimization and acceleration technologies, such as those supplied by Riverbed Technologies and Silver Peak.
   - When third-party WAN optimization is implemented, Zerto recommends disabling VPG WAN compression.

16. To change the replication settings per virtual machine, click **VM SETTINGS**.
The Advanced VM Replication Settings window is displayed.

17. To edit information in one field, click the field and update the information.
18. To edit information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED. The Edit VM window is displayed.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Host (not relevant when replicating to vCD) (Hyper-V)</td>
<td>The cluster or host that will host the recovered virtual machine.</td>
</tr>
<tr>
<td>Setting &amp; Description</td>
<td>Select...</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------</td>
</tr>
<tr>
<td><strong>(vSphere)</strong> The cluster, resource pool, or host that will host the recovered virtual machine.</td>
<td>When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for all the virtual machines specified in the VPG. If a resource pool is specified and DRS is disabled for the site later on, all the resource pools are removed by VMware and recovery is to any one of the hosts in the recovery site with a VRA installed on it. All resource pool checks are made at the level of the VPG and do not take into account multiple VPGs using the same resource pool. If the resource pool CPU resources are defined as unlimited, the actual limit is inherited from the parent but if this inherited value is too small, failover, move, and failover test operations can fail, even without a warning alert being issued by Zerto Virtual Manager.</td>
</tr>
</tbody>
</table>

**VM Recovery Datastore** *(vSphere) (not relevant when replicating to vCD)*

The datastore where the VMware metadata files for the virtual machine are stored, such as the VMX file. If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located.

**Recovery Storage** *(Hyper-V)*

The location where the metadata files for the virtual machine are stored, such as the VHDX file. If a cluster is selected for the host, only storage that are accessible by every host in the cluster are displayed.

**Journal Size Hard Limit**

The maximum size that the journal can grow, either as a percentage or a fixed amount.

- The journal is always thin-provisioned.
- The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.

*For Example:* If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

<table>
<thead>
<tr>
<th>Unlimited: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are not displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Size (GB):</strong> The maximum journal size in GB.</td>
</tr>
<tr>
<td>The minimum journal size, set by Zerto Virtual Replication, is <strong>8GB</strong> for Hyper-V and vSphere environments, and <strong>10GB</strong> for Microsoft Azure environments.</td>
</tr>
<tr>
<td><strong>Percentage:</strong> The percentage of the virtual machine volume size to which the journal can grow.</td>
</tr>
<tr>
<td>This value can be configured to more than 100% of the protected VM’s volume size.</td>
</tr>
</tbody>
</table>
19. Click **OK**.

20. In the Advanced VM Replication Settings window, click **OK**.

21. Click **NEXT**.

The STORAGE step is displayed.

- By default the storage used for the virtual machine definition is also used for the virtual machine data.
- For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Journal Size Warning Threshold</strong></td>
<td><strong>Unlimited:</strong> The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore. If Unlimited is selected, Size and Percentage options are <strong>not</strong> displayed. <strong>Size</strong> <em>(GB):</em> The size in GB that will generate a warning. <strong>Percentage</strong>*: The percentage of the virtual machine volume size that will generate a warning. *The values of Size and Percentage must be <strong>less</strong> than the configured <strong>Journal Size Hard Limit</strong> so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.</td>
</tr>
</tbody>
</table>

| **Journal Storage (Hyper-V), or Journal Datastore (vSphere) (not relevant when replicating to vCD)** | **(vSphere)** To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore. **(Hyper-V)** To change the default, specify a host and then select the storage location accessible by this host to be used as the journal storage. When you select specific journal storage, the journals for each virtual machine in the VPG are stored in this storage, regardless of where the recovery storage is for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal storage. |

The size of the journal that triggers a warning that the journal is nearing its hard limit.
■ **Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

22. To edit storage information for one of the virtual machines’ volume location, first select the virtual machine, then click **EDIT SELECTED**. The Edit Volumes window is displayed.

■ In Hyper-V environments, the following window appears.

![Edit Volumes Hyper-V](image)

■ In vSphere environments, the following window appears.

![Edit Volumes vSphere](image)
### SETTING & DESCRIPTION

<table>
<thead>
<tr>
<th>Volume Source</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>(Hyper-V) Select a <strong>Volume Source</strong> for recovery from one of the drop-down options:</td>
<td></td>
</tr>
<tr>
<td>■ Storage</td>
<td>■ <strong>Volume Source &gt; Storage</strong>: A new volume is used for replicated data.</td>
</tr>
<tr>
<td>■ Preseeded volume</td>
<td>■ From the <strong>Storage</strong> drop-down list, specify the storage to use to create disks for the replicated data.</td>
</tr>
<tr>
<td></td>
<td>The storage specified for the replication must have at least the same amount of space as the protected volume and then an additional amount for the journal.</td>
</tr>
<tr>
<td></td>
<td>The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Volume Source &gt; Preseeded volume</strong>: Whether to copy the protected data to a virtual disk in the recovery site.</td>
</tr>
<tr>
<td></td>
<td>Zerto recommends using this option particularly for large disks so that the initial synchronization will be faster since a <strong>Delta Sync</strong> can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>When <strong>not</strong> using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN.</td>
</tr>
<tr>
<td></td>
<td>When using a preseeded virtual disk, you select the storage and exact location, folder, and name of the preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.</td>
</tr>
<tr>
<td></td>
<td>Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.</td>
</tr>
<tr>
<td></td>
<td>The storage where the preseeded disk is placed is also used as the recovery storage for the replicated data.</td>
</tr>
</tbody>
</table>
(vSphere) Select a **Volume Source** for recovery from one of the drop-down options:
- Datastore
- RDM
- Preseeded volume

**Volume Source > Datastore:** A new volume is used for replicated data.

- Specify the **Datastore** to use to create disks for the replicated data.
- If the **source disk is thin provisioned**, the default for the recovery volume is also thin provisioned.
- The datastore specified for replication must have at least the same amount of space as the **protected volume** and an additional amount for the **journal**.
- The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.
- Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

Then, define the following:
- **Datastore:** The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.

**Volume Source > RDM:** The VMware RDM (Raw Device Mapping) which will be used for the replication.

By default, **RDM is recovered as thin-provisioned VMDK** in the datastore specified in the **VM Recovery Datastore/Storage** field in the Edit VM dialog, and not to RDM.

Only a raw disk with the **same size as the protected disk** can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

The RDM is always stored in the recovery datastore, used for the virtual machine.

The following **limitations** apply to protecting RDM disks:
- RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
- RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.
- You cannot define an RDM disk to be protected to a cloud service provider via a Zerto Cloud Connector nor if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.
Replication From a Protected Site vCD to Hyper-V

Zerto Virtual Manager Administration Guide for VMware vSphere Environments - Version 6.0
Protecting Virtual Machines to and From vCloud Director

Volume Source > Preseeded volume: Select this when you want to copy the protected data to a virtual disk in the recovery site.

Consider the following, then proceed to define the Datastore and the Path:

- Zerto recommends using this option particularly for large disks so that the initial synchronization is faster since a Delta Sync can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk.
- If a preseeded disk is not selected, the initial synchronization phase must copy the whole disk over the WAN.
- If you use a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.
- If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter by using the command: `esxcfg-advcfg -s <Timeout>/NFS/SetAttrRPCTimeout`
- If the protected disks are non-default geometry, configure the VPG using preseeded volumes.
- If the protected disk is an RDM disk, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. See Zerto Cloud Manager Administration Guide.

Then, define the following:

- **Datastore**: The Datastore where the preseeded disk is located. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk.
- **Path**: The full path to the preseeded disk.

Temp Data disk

If the virtual machine to be replicated includes a temp data disk as part of its configuration.

Specify a mirror disk for replication that is marked as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.
23. Click **OK**.
24. Click **NEXT**.

The **RECOVERY** step is displayed. Recovery details include the networks to use for failover, move, and for testing failover, and whether scripts should run as part of the recovery operation.

25. Select the default recovery settings.
   - **Failover/Move Network**: The network to use during a failover or move operation in which the recovered virtual machines will run.
   - **Failover Test Network**: The network to use when testing the failover of virtual machines in the recovery site. Zerto recommends using a fenced-out network so as not to impact the production network at this site.

26. Enter the name of the script to run in the **Command to run** text box. You can then enter details about the script.
   - **Pre-recovery Script**: The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script**: The information about a script that should run at the end of the recovery process.

For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Command to run</strong></td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td><strong>Params</strong></td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>- The default time-out value is specified in <strong>Site Settings &gt; Performance and Throttling</strong> tab.</td>
</tr>
</tbody>
</table>

27. Click **NEXT**.
The NICs step is displayed. In this step, you can specify the NIC details to use for the recovered virtual machines after a failover, a test failover, or migration.

28. To edit information in one field, click the field and update the information.

29. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

30. Otherwise, go to step step 42.

The Edit VNIC window is displayed.

31. Specify the network details to use for the recovered virtual machines after a failover or move operation, in the Failover/Move column, and for the recovered virtual machines when testing replication, in the Test column.

In each column, **specify** the following:

- **Network**: The network to use for this virtual machine.
- **Create New MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites. Note that if you check this option, to create a new MAC address, and the current IP address is not specified, the protected virtual machine static IP address might not be used for the recovered virtual machine.
To change the vNIC IP configuration, select Yes in the Failover/Move or Test column. If you select to use a statically-assigned IP address, set the IP address, subnet mask, and default gateway. Optionally, change the preferred and alternate DNS server IP addresses and the DNS suffix. If you leave the DNS server and suffix entries empty, or select to use DHCP, the IP address and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the Default gateway field for the NICs with no default gateway.

**Note:** During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP address than the original IP address, after the virtual machine has started it is injected with the correct IP address. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP address clash between the test machines and the production machines.

- **Copy to failover test:** Select this to copy the settings in the Failover/Move column to the Test column.
- **Copy to failover/move:** Select this to copy the settings in the Test column to the Failover/Move column.

33. Click **OK**.

34. 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.

35. By default, backup is **OFF**. To keep this value, go to step **45**.

36. Otherwise, toggle **OFF** to **ON** and enter the following information:

- **Target Repository:** The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in "Setting Up Offsite Backups", on page 28.
- **Retention Period:** The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see "Offsite Backups", on page 38.
- **Run Job Every:** The day and time to start the backup.
- **Retries:** Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.

**IMPORTANT Re-IP Information:**

To utilize re-IP during failback, make sure that:

- VMware Tools is **installed** on the virtual machine in vCenter server.
- The user that is logged on to VMWare Tools has **sufficient privileges** to execute re-IP changes.

Refer to the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-IP.
Post-Backup Script: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings dialog.</td>
</tr>
</tbody>
</table>

37. Click NEXT.

The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

38. Click DONE. The VPG is created.

For details of what happens after saving the VPG, see “What Happens After the VPG is Defined”, on page 36.
Replication From a Protected Site vCD to AWS

You can protect a vCD vApp to Amazon Web Services (AWS).

When creating a VPG from vCloud Director to AWS the data is stored in S3 and all replicated data from protected virtual machines to AWS is encrypted in S3. All recovery operations bring up the recovered machines in EC2 in AWS.

Before replicating from a protected vCD site to a recovery AWS site, review the following guidelines for AWS environments, and considerations when protecting to AWS: Zerto Virtual Replication - Prerequisites & Requirements for Amazon Web Services (AWS)

See also: “Import Methods for AWS”, on page 164

After reviewing the guidelines and considerations, proceed with “Creating a VPG from vCloud Director to AWS”, on page 166.

Import Methods for AWS

During recovery operations, Zerto uses a combination of the following APIs and methods to convert the Amazon S3 objects into recovery disks in EC2 as EBS disks:

- **AWS Import:**
  - **Import-instance:** for the boot volume
  - **Import-volume:** for data volumes

For more information see the relevant AWS documentation:

- API_ImportInstance
- API_ImportVolume

**Note:** The ImportImage API is not used by Zerto.

- **Zerto Import - zimport**, an import method that does not have the same limitations as the AWS APIs. It creates an AWS EC2 instance per protected VM volume, called zimporter, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk have been attached to the recovered instance, the zImport instance is terminated.

**Notes:**
- zimporter is based on an official AWS Linux AMI (Amazon Machine Image), into which a script is injected to perform the import. The script is located online and downloaded to the zimporter, and thus the zimporter requires internet access in order to access and download the script. The zimporter instance is therefore created with a public IP.
- The only network in the customer environment that is certain to have internet access is the network that the ZCA is connected to.
- To ensure that the zimport instance cannot be accessed from the outside world, a security group is created. During a recovery operation the zimport instance is connected to this security group. All inbound traffic is blocked and only outbound traffic to access the script online is allowed. The security group is deleted at the end of the recovery operation.
- The default zimporter instance type is c4.8xlarge and the AWS EC2 default maximum instance quota is 20. If during the creation of zimport instances the maximum EC2 instance quota is reached, the creation of the next and subsequent zimport instances will be queued, increasing the RTO. If during recovery operations, the ZVM identifies a VPG with the potential to exceed the EC2 instance quota, the user will receive an alert with advice to contact AWS support to increase the service limits in order to improve RTO.
- GPT formatted disks are supported for data volumes only, when using either of the zimport methods.
- When using either of the zimport methods, each volume is created with EBS disk of type io1 with maximum 1000 EBS Provision IOPS allocated. EBS disk type can be changed post recovery without downtime, see the relevant AWS documentation. The minimum disk size for io1 is 4GB.
- The default Max EBS Provision IOPS quota in a region across all io1 disks is 40000 EBS Provision IOPS, meaning that with 1000 EBS Provision IOPS per volume, the maximum possible number of volumes is 40. If the Max EBS Provision IOPS quota is reached, the failover process will switch to using slower gp2 disks. An event will notify the user of this, and recommend that the user contact AWS support to increase the Max EBS Provision IOPS quota.
- Depending on the desired RTO during recovery operations, or when testing failover, the user can select an import method per VPG or per virtual machine from the following options:
  - “Zerto Import for Data Volumes”, on page 165
Zerto Import for Data Volumes

This method is the default setting and has a faster RTO than AWS Import. This method uses a combination of the AWS import-instance API for the boot volume, and the zImport method for data volumes.

- Each machine that you intend to protect must have at least 250MB free space. This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.
- Protected boot volumes are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Temporary disks may be created based on the selected instance size.
- Temporary disks may be created based on the selected instance size.
- The maximum protected data volume size is 16TB, while the boot volume can be up to 1TB.
- 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

Zerto Import for All Volumes

This method uses the zImport method for all volumes and ensures the fastest RTO.

This method creates an AWS EC2 instance per protected VM volume, called zImporter, to convert the S3 objects and write them to a zImport local disk. When all the data has been imported and its disk have been attached to the recovered instance, the zImport instance is terminated.

- Temporary disks may be created based on the selected instance size.
- This import method cannot be used for the recovery of protected virtual machines running Windows Server 2008R2. To support this operating system please contact Zerto support.
- The maximum protected data volume size is 16TB, while the boot volume can be up to 2047GiB.

Note: 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 2TB or larger, the VM you are using may be limited to a 2047 GiB boot volume size. Non-boot volumes do not have this limitation. See AWS Documentation for more information: http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumeTypes.html

When using this import method, if the protected virtual machine using this import method is running Windows 2012, Windows 2012R2 or Windows 2016, the following drivers must be installed on the protected virtual machine before starting recovery operations:

- Windows PV (Paravirtualization) Drivers
- Windows ENA (Elastic Network Adapter) Drivers

The following steps must be performed to ensure that the virtual machine will be able to run on the recovery site:

1. **Download and Install Windows PV Drivers:**
   b) Follow the instructions at the site for downloading and installing all the Windows PV Drivers 8.2.0 drivers.

2. **Download and Install Windows ENA Drivers:**
   If you are running Windows 2012 or Windows 2016 on any of the following AWS instance types:
   - C3
   - C4
   - D2
   - M4 (excluding M4.16xlarge)
   a) Go to http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/sriov-networking.html#enable-enhanced-networking
   b) Follow the instructions at the site for downloading and installing the Windows ENA Drivers.

Note: If these drivers are installed on a VM running Windows 2012R2, the other AWS import methods will fail. To overcome this, you must uninstall the drivers before using the other AWS import methods.
AWS Import

This method uses a combination of the AWS import-instance and import-volume APIs for the boot and data volumes respectively. This was the only method supported until version 5.5.

- **Each machine that you intend to protect** must have at least 250MB free space. This is because AWS adds files to the recovered machines during failover, move, test failover, and clone operations.
- **Protected boot volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored.
- **Protected volumes** are recovered in EC2 as EBS disks with magnetic disk type. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB. Additional volumes might be created in the recovered instance, dependent on the instance type used for the recovery. These volumes can be ignored. Temporary disks may be created based on the selected instance size.
- The **maximum protected data volume and boot disk size** is 1TB.

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)

Creating a VPG from vCloud Director to AWS

Use the following procedure to create a virtual protection group to protect to AWS.

**To create a VPG from vCloud Director to AWS:**
1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The GENERAL step of the Create VPG wizard is displayed.

2. Specify the name of the VPG and the priority of the VPG.
   - **VPG Name:** The VPG name must be unique. The name cannot be more than 80 characters.
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.

- **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
- **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
- **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have use it. Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync. During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

3. Click **NEXT**.

The VMs step is displayed.

You can select virtual machines to protect from the underlying vCenter Server or as a vCD vApp.

4. Select the vCD vApp to protect in this VPG.
   - When using the Search field, you can use the wildcards; * or ?.
   - Only vCD vApps that are **unprotected** are displayed in the list. A VPG can include:
     - Only one vApp.
     - vApps that are **not yet** protected.
     - vApps that are **already** protected.

5. To view **protected** vApps, in the **Advanced (One-to-Many)** section, click **Select vApp**.

The Select vApp window is displayed.
Note: With the One-to-Many feature, a VPG containing a single vApp can be recovered to a maximum of three different sites and cannot be recovered to the same site more than once.

vApps protected in the maximum number of VPGs are not displayed in the Select VMs window.

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

Note: Define the required boot order for vCD vApps in the vCloud Director console.

6. Click NEXT.

The REPLICATION step is displayed.

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, as shown below.

7. Specify the recovery site.
   - **Recovery Site**: The site to which you want to recover the virtual machines. After specifying the recovery site, other fields are displayed.
Note: You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

8. **ZORG:** If the site is defined in **Zerto Cloud Manager**, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see **Zerto Cloud Manager Administration Guide**.
   - **Service Profile:** The name of the service profile to use which determines the VPG SLA settings for the group, which apply to every virtual machine in the group. To change the VPG SLA settings, select the **Custom Service Profile**.

9. If the **VPG SLA** settings are editable, when the Zerto Cloud Manager is not used or when a **Custom** service profile is available, specify these settings for the group, which apply to every virtual machine in the group.
   - **Journal History:** The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG.
     Select the number of **hours** from **1 to 24** or the number of **days** from **2 to 30**.

10. **Target RPO Alert:** The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

11. **Test Reminder:** The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

12. Click **NEXT**.
    The **STORAGE** step is displayed.
    By default the storage used for the virtual machine definition is also used for the virtual machine data. For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.
13. Specify whether the protected volume is a temp data disk.

**Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

14. Click **NEXT**.

The RECOVERY step is displayed. Recovery details include the networks, security group, instance family, and instance type 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.

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

- **VPC Network:** The virtual network dedicated to your AWS account. A security group and subnet must be assigned to this VPC.
- **Subnet:** The subnet for the VPC network.

Depending on the import method selected, the list of subnets available for selection is shown.

- **Zerto Import - zImport:** The subnet drop-down list shows the options available when either the Zerto Import for data volumes or the Zerto Import for all volumes is selected. Only the subnets that are supported by the zImport method are selectable. Other Subnets are grayed out and are not selectable.
Note: The zImport virtual machine must have access to the internet in order to access the S3 Bucket and the AMI in EC2. The only network in the customer environment that is certain to have internet access is the network that the ZCA is connected to. If the import method is not AWS Import, then the user can select only subnets that are part of the same Availability Zone as the one in which the ZCA resides. Other Subnets are disabled.

**AWS Import:** The Subnet drop-down list shows options available when AWS Import method is selected. All subnets are listed. A tool tip alert is displayed when the user hovers over a subnet that is not supported.

Note: If a subnet is chosen in a network that is not in the same Availability Zone as the one in which the ZCA resides, options that utilize the zImport method will not be made available for selection.

**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 being protected in the VPG.

**Instance Type:** The instance type, within the instance family, to assign to recovered instances. Different types within an instance family vary, for example in vCPU, RAM, and local storage size. Choose the instance type appropriate for the application being protected in the VPG. The price per instance is related to the instance configuration.

16. For additional settings, click **ADVANCED VM SETTINGS**.
The Advanced VM Settings window is displayed, which shows the recovery network settings for **FAILOVER/MOVE** for virtual machines in the VPG. You can see the recovery network settings for failover tests by clicking **TEST**.

17. To edit information in one field, click the field and update the information.

18. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**. The Edit VM Settings window is displayed.

19. Update the values for VPC network, subnet, security group, instance family, instance type, and private IP as necessary.

   **Note:** Only private IPs specified for Windows machines are assigned during a recovery operation. For Linux machines, the IP is assigned from the specified subnet range.

   Clearing the values in the **Private IP** field results in an IP being automatically assigned from the subnet range during a recovery operation.

   See the [Zerto Virtual Replication Interoperability Matrix](#) for the list of operating systems for which Zerto supports re-IP.

20. Click **OK** twice to return to the main page of the RECOVERY step.

21. Enter the name of the script to run in the Command to run text box. You can then enter details about the script.

   - **Pre-recovery Script:** The information about a script that should run at the beginning of the recovery process.
   - **Post-recovery Script:** The information about a script that should run at the end of the recovery process.

   For both types of scripts, enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
</tbody>
</table>
22. 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 for up to one year.

23. By default, backup is **OFF**. To keep this value, go to step step 45.

24. Otherwise, toggle **OFF** to **ON** and enter the following information:

   - **Target Repository**: The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
   - **Retention Period**: The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
   - **Run Job Every**: The day and time to start the backup.
   - **Retries**: Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
   - **Post-Backup Script**: The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Params</strong></td>
<td>The parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td><strong>Timeout</strong></td>
<td>The time-out, in seconds, for the script to run.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs before executing a failover, move, or test failover, and the script fails or the timeout value is reached, an alert is generated and the failover, move, or test failover is not performed.</td>
</tr>
<tr>
<td></td>
<td>- If the script runs after executing a failover, move, or test failover, and the timeout value is reached, an alert is generated.</td>
</tr>
<tr>
<td></td>
<td>- The default time-out value is specified in <strong>Site Settings &gt; Performance and Throttling</strong> tab.</td>
</tr>
</tbody>
</table>

25. Click **NEXT**.

26. **Note**: You cannot restore a backup in AWS.

27. Click **NEXT**.
The SUMMARY step is displayed. It shows the VPG configuration that you defined in the previous steps.

26. Click **DONE**. The VPG is created.

For details of what happens after creating the VPG, see “What Happens After the VPG is Defined”, on page 36.
Replication From a Protected Site vCD to Azure

You can protect a vCD vApp to Microsoft Azure.

When creating a VPG from vCloud Director to Azure the data is stored in a storage account and all replicated data from protected virtual machines to Azure is encrypted in the storage account. All recovery operations bring up the recovered machines in resource groups in Azure.

- Azure ZCA can be installed only on Windows Server 2012 R2 and higher.
- Only virtual machines that are supported by Azure can be protected by Zerto Virtual Replication. All Windows operating systems are supported.

**Note:** Microsoft does not support operating systems that are past the End of Support date, without a Custom Support Agreement (CSA). For more information about Microsoft operating systems support for Microsoft Azure, refer to [https://support.microsoft.com/en-us/kb/2721672](https://support.microsoft.com/en-us/kb/2721672).

- To replicate between Azure and your site, you must have a virtual machine in Azure with a Zerto Cloud Appliance installed on it. This ZCA must be paired with your site.
- For Linux distribution, refer to Azure documentation:

**Requirements for Replication From Azure**

- For Virtual Machines to be protected from Azure, the VM volumes must reside in the Standard storage account defined during ZCA installation.
  - A Standard storage account is created or selected upon ZCA installation.
    - Type: Standard storage
    - Recovery and journal volumes reside on this Zerto Storage Account
    - Azure VMs with all disks on this Zerto Storage Account can be protected by Zerto.
    - Blob Storage is not supported.
    - Managed Disks are not supported.
    - VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.

**Requirements for Replication To Azure**

- **Protected volumes** are recovered in Azure as VHD disks in a page blob. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB.
  
  **Note:** For some instance sizes, the Azure virtual machine is created with a Local SSD disk which is a temporary disk. This disk is in addition to the disks associated with each protected virtual machine.

- The following **limitations** apply when protecting to Azure
  - Virtual machines with **UEFI Firmware** cannot be protected.
  - You **cannot** protect machines that have a disk **larger than 4 TB**.
  - The protected virtual machines needs to have **at least one NIC**.
  - Reserve at least **2 CPUs** and **4GB RAM** for the machine using a subnet accessible by other Zerto Virtual Replication sites.
  - The **supported** number of **data disks and NICS per virtual machine** is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.

**Requirements for Replication within Azure**

- Azure ZCA on both Azure sites need to be version 6.0 and higher.
- The following limitations apply when protecting within Azure:
  - Self replication is not supported.
Additional Azure Considerations

For additional considerations, see Azure subscription and service limits, quotas and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits.

For example from the link, see the following default values:

- There can be multiple Zerto Cloud Appliances per Azure subscription and region.
- 20 cores per subscription
- 200 Storage accounts per subscription
- 20 VMs per region per subscription
- 20 VMs per series (Dv2, F, etc.) cores per subscription per Region

Additionally, see the following example for maximum values:

- A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not exceed this limit.

<table>
<thead>
<tr>
<th>VM TIER</th>
<th>BASIC TIER VM</th>
<th>STANDARD TIER VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk size</td>
<td>4 TB</td>
<td>4 TB</td>
</tr>
<tr>
<td>Max 8 KB IOPS per persistent disk</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Max number of disks performing max IOPS</td>
<td>66</td>
<td>50</td>
</tr>
</tbody>
</table>

See also “Azure Limitations Which Affect Installation and Recoverability”, on page 176.

Azure Limitations Which Affect Installation and Recoverability

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

Default Azure limitations which Affect Installation

- Storage Limitations:
  - Number of storage accounts: 200 per subscription (note: max is 250)

Default Azure Limitations which Affect Recovery

<table>
<thead>
<tr>
<th>Virtual Machines Limitations</th>
<th>VMs per subscription per region: 20 (max: 10K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM total cores per subscription per region:</td>
<td>20</td>
</tr>
<tr>
<td>Instance sizes:</td>
<td>Limited per region. Many of them are 20 cores per region per subscription</td>
</tr>
<tr>
<td>Resource groups per subscription:</td>
<td>800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>Network interfaces per region: 350</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICs per instance:</td>
<td>Depends on instance size:</td>
</tr>
<tr>
<td>Windows:</td>
<td><a href="https://docs.microsoft.com/en-us/azure/virtual-machines/windows-sizes">https://docs.microsoft.com/en-us/azure/virtual-machines/windows-sizes</a></td>
</tr>
<tr>
<td>Linux:</td>
<td><a href="https://docs.microsoft.com/en-us/azure/virtual-machines/linux-sizes?toc=%2fazure%2fvirtual-machines%2flinux%2ftoc.js">https://docs.microsoft.com/en-us/azure/virtual-machines/linux-sizes?toc=%2fazure%2fvirtual-machines%2flinux%2ftoc.js</a></td>
</tr>
<tr>
<td>Private IP Addresses per VNET per subscription per region:</td>
<td>4096</td>
</tr>
<tr>
<td>Cloning of IP addresses during recovery operations:</td>
<td>Due to an Azure limitation, failing over Linux VMs with static IP is not supported.</td>
</tr>
</tbody>
</table>
To create a VPG from vCloud Director to Azure:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.

   The GENERAL step of the Create VPG wizard is displayed.

   To specify the name of the VPG and the priority of the VPG:
   - **VPG Name**: The VPG name must be unique. The name cannot be more than 80 characters.
   - **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.
     - **High Priority**: When there are updates to virtual machines protected in VPGs with different priorities, updates from the VPG with the highest priority are passed over the WAN first.
     - **Medium Priority**: Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it.
     - **Low Priority**: Low priority VPGs will use whatever bandwidth is left after the medium priority VPGs have used it.

2. Click **NEXT**.

   Updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a bitmap or delta sync.

   During synchronization, data from the VPG with the highest priority is passed over the WAN before data from medium and low priority VPGs.

   Storage account total size limitation: 500 TB
   *(# of entities (blobs, containers etc) within a storage account: unlimited)*

   Max size of a page blob (vhd): 4 TB

   Min size of a page blob (vhd): 20 MB

   Max number of data disks: Depends on instance size

The VMs step is displayed.

You can select virtual machines to protect from the underlying vCenter Server or as a vCD vApp.

4. Select the vCD vApp to protect in this VPG.
   - When using the Search field, you can use the wildcards; * or ?.
   - Only vCD vApps that are unprotected are displayed in the list. A VPG can include:
     - Only one vApp.
     - vApps that are not yet protected.
     - vApps that are already protected.

5. To view protected vApps, in the Advanced (One-to-Many) section, click Select vApp.
The Select vApp window is displayed.

Note: With the One-to-Many feature, a VPG containing a single vApp can be recovered to a maximum of three different sites and cannot be recovered to the same site more than once.

vApps protected in the maximum number of VPGs are not displayed in the Select VMs window.
Protecting vApps in several VPGs is enabled only if both the protected and recovery sites, and the VRAs installed on these sites, are of version 5.0 and higher.

Note: Define the required boot order for vCD vApps in the vCloud Director console.

6. Click NEXT.
The REPLICATION step is displayed.

**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, as shown below.

7. **Specify the Recovery Site.** This is the site to which you want to recover the virtual machines. After specifying the recovery site, other fields are displayed.

**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.

You cannot select a recovery site if any of the virtual machines you selected are already in VPGs that recover to that site.

8. **ZORG:** If the site is defined in **Zerto Cloud Manager**, select the name used by the cloud service provider (CSP) to identify you as a Zerto Organization (ZORG). For details about Zerto Cloud Manager, see **Zerto Cloud Manager Administration Guide**.

9. When the Zerto Cloud Manager is used, select the service profile.
   - **Service Profile** - The name of the service profile to use which determines the VPG SLA settings for the group, which apply to every virtual machine in the group. To change the VPG SLA settings, select the **Custom Service Profile**.

10. If the **VPG SLA** settings are editable, when the Zerto Cloud Manager is not used or when a **Custom** service profile is available, specify these settings for the group, which apply to every virtual machine in the group.
   - **Journal History:** The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG.
Select the number of **hours** from 1 to 24 or the number of **days** from 2 to 30.

11. **Target RPO Alert:** The maximum desired time between each automatic checkpoint write to the journal before an alert is issued.

12. **Test Reminder:** The amount of time in months recommended between each test, where you test the integrity of the VPG. A warning is issued if a test is not performed within this time frame.

Click **NEXT**.

The STORAGE step is displayed.

By default the storage used for the virtual machine definition is also used for the virtual machine data.

For each virtual machine in the VPG, Zerto Virtual Replication displays its storage-related information.

13. Specify whether the protected volume is a temp data disk.

**Temp Data:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, mark the recovery disk for this disk as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

14. Click **NEXT**.

The RECOVERY step is displayed. Recovery details include the networks, network security group, instance family, and instance size 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.
15. Select recovery settings for failover/move and failover testing.
   ■ **VNet**: The virtual network dedicated to your Azure subscription.
   ■ **Subnet**: The subnet or the VNet network.
   ■ **Network Security Group**: The Azure network security to be associated with the virtual machines in this VPG. You can associate one network security group with the virtual machines. The NIC will be associated with the network security group defined at the virtual machine level.
   ■ **Virtual Machine Series**: The virtual machine series from which to select the size. Azure virtual machine series are optimized for different types of applications. The default is set to **Dv2-series**. You can choose the virtual machine series appropriate for the application being protected in the VPG.
   ■ **Virtual Machine Size**: The virtual machine size, within the virtual machine series, to assign to recovered virtual machines. Different sizes within a virtual machine series vary, for example in a number of cores, RAM, and local storage size. The default is set to **Standard_D1_v2**. You can choose the virtual machine size appropriate for the application being protected in the VPG. The price per virtual machine is related to the virtual machine configuration.

16. For additional settings, click **ADVANCED VM SETTINGS**.

   The Advanced VM Settings window is displayed, which shows the recovery network settings for **FAILOVER/MOVE** for virtual machines in the VPG. You can see the recovery network settings for failover tests by clicking **TEST**.

17. To edit information in one field, click the field and update the information.
18. To edit information for several virtual machines at the same time, select the virtual machines and click **EDIT SELECTED**.

   The Edit VM Network window is displayed.

19. Update the values for VNet, subnet, security group, instance family, instance size, and private IP as necessary.

   **Note**: Only private IPs specified for Windows machines are assigned during a recovery operation. For Linux machines, the IP is assigned from the specified subnet range.

   Clearing the values in the **Private IP** field results in an IP being automatically assigned from the subnet range during a recovery operation.
Refer to the Zerto Virtual Replication Interoperability Matrix for the list of operating systems for which Zerto supports re-
IP.

20. Click OK twice to return to the main page of the RECOVERY step.

21. 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 for up to one year.

22. By default, backup is OFF. To keep this value, go to step 45.

23. Otherwise, toggle OFF to ON and enter the following information:

- **Target Repository** – The name of the repository where the offsite backups are written. Repositories are configured via the SETUP tab as described in “Setting Up Offsite Backups”, on page 28.
- **Retention Period** – The length of time to keep offsite backups, up to a maximum of one year. For details of how this affects the number of backups saved, see “Offsite Backups”, on page 38.
- **Run Job Every** – The day and time to start the backup.
- **Retries** – Whether to rerun the backup job automatically if the job fails. If you select this option, you must also define the number of retries that will be attempted and the time to wait after a job fails before running the backup job again.
- **Post-Backup Script** – The information about a script that should run at the end of the recovery process. Enter the following information:

<table>
<thead>
<tr>
<th>TEXT BOX</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command to run</td>
<td>The full path of the script. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.</td>
</tr>
<tr>
<td>Parameters</td>
<td>The values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>Timeout</td>
<td>The time-out, in seconds, for the script to run. If the timeout value is reached, an alert is generated. The default time-out value is specified in the Performance and Throttling tab of the Site Settings window.</td>
</tr>
</tbody>
</table>

**Note:** You cannot restore a backup in AWS.

24. Click NEXT.
The SUMMARY step is displayed. It shows the VPG configuration that you defined in the previous steps.

25. Click **DONE**. The VPG is created.

For details of what happens after creating the VPG, see “What Happens After the VPG is Defined”, on page 36.
You can monitor information about all the VPGs either protected at the local site or recovered to the local site in the VPGs tab. You can also drill-down to monitor information about a specific VPG displayed in the VPGs tab or about the virtual machines being protected by VPGs. You can also view summary details of the protected and recovery sites in either the protected or recovery site as well as monitor the status of each virtual protection group and any of the virtual machines being protected in either site.

The following general monitoring options are described in this chapter:

- “The DASHBOARD Tab”, below
- “Monitoring VPGs – The VPGs Tab”, on page 187
- “Monitoring a Single VPG”, on page 191
- “Monitoring Tasks”, on page 194
- “Monitoring Protected Virtual Machines – The VMs Tab”, on page 196

The following site monitoring option is described in this chapter:

- “Monitoring Peer Sites – The SITES Tab”, on page 198

The following VRA monitoring option is described in this chapter:

- “Monitoring Virtual Replication Appliances”, on page 199

The following storage monitoring option is described in this chapter:

- “Monitoring Datastores – The SETUP Tab – The DATASTORES Tab”, on page 205

The following offsite backup monitoring options are described in this chapter:

- “Monitoring Repositories – The SETUP Tab – The REPOSITORIES Tab”, on page 207
- “Monitoring Offsite Backups – The OFFSITE BACKUP Tab”, on page 208

The following performance counters are described in this chapter:

- “Zerto Performance Counters”, on page 210

For details about monitoring Zerto Virtual Manager alerts and events, refer to Zerto Virtual Replication Guide to Alarms, Alerts and Events."
The DASHBOARD Tab

The DASHBOARD provides an overview of the sites and VPGs being protected at the site or recovered to the site.

The following information is displayed:

**VPG HEALTH**

The VPGs being recovered with the health of each VPG, represented by a colored block, where the color represents the following:

- **Green**: The VPG is being replicated, including syncing the VPG between the sites.
- **Orange**: The VPG is being replicated but there are problems, such as an RPO value larger than the target RPO value specified for the VPG.
- **Red**: The VPG is not being replicated, for example because communication with the site is down.

Positioning the mouse over a block displays the VPG name as a tooltip. Clicking the block opens the details tab for the VPG.

**STATUS**

The status of the site, including the following:

- The number of VPGs and virtual machines being protected or recovered.
- The amount of storage being protected.
- The average RPO.
- The percentage compression of data passed between the site and peer sites.
Performance Graphs

The current site performance, which includes the following information:

**IOPS (I/O per Second):** The total amount of I/O write operations generated by the protected virtual machines on the viewed site.

**Throughput (MB per second):** The total amount of uncompressed data written by the virtual machines protected to the recovery sites.

During synchronization processes (such as bitmap sync, initial sync and delta sync) this value will also consist of the uncompressed data read from the protected disks.

**WAN Traffic (MB per second):** The total amount of compressed data transferred between the viewed site and all its recovery sites.

A listing of the currently active alerts and running tasks, and the events run during the last few hours.

User input, for example, stopping a failover test or committing or rolling back a Move or Failover operation, can be initiated from the relevant task displayed in the RUNNING TASKS section.

**ACTIVE ALERTS, RUNNING TASKS, and EVENTS**

A listing of the currently active alerts and running tasks, and the events run during the last few hours.

User input, for example, stopping a failover test or committing or rolling back a Move or Failover operation, can be initiated from the relevant task displayed in the RUNNING TASKS section.
Monitoring VPGs – The VPGs Tab

View details of all VPGs in the VPGs tab. This tab lists all the VPGs from both the local and remote sites and provides summary details of each VPG.

You can create a query using the view buttons ( ) to display VPG information in a list or as a grid. In both list and grid views you can filter the VPGs that will be displayed according to their status by checking the checkboxes alongside the VPG status icons ( ). The query can be customized by adding and removing filters.

The QUERY option allows you to save or run a personal query, or set the VPG tab back to its default view.

List View - GENERAL

The following information is displayed in the GENERAL view:

Alert status indicator: The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:

- **Green**: The VPG is being replicated, including syncing the VPG between the sites.
- **Orange**: The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- **Red**: The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the Alert status indicator to display details of the alert.
**VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab. The number of VMs protected in the VPG is displayed in parentheses.

**Direction:** The direction of the replication, from this site to the remote site or from the remote site to this site.

**Peer Site:** The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.

**Priority:** The priority of the VPG.

**Protection Status:** The current status of the VPG, such as Meeting SLA. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

**State:** The current substatus of the VPG, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

**Actual RPO:** The time since the last checkpoint was written to the journal. This should be less than the Target RPO Alert value specified for the VPG.

**Operation:** The operation, such as Move, that is currently being performed.

---

**List View - PERFORMANCE**

The following information is displayed in the PERFORMANCE view:

**IOPS (I/O per Second):** The total amount of I/O write operations generated by the protected virtual machines comprising the Virtual Protection Group (VPG)

**Throughput (MB per Second):** The total amount of uncompressed data written by the protected virtual machines comprising the Virtual Protection Group (VPG).

During synchronization processes (such as bitmap sync, initial sync and delta sync) this value will also consist of the uncompressed data read from the protected disks.

**Network** - The amount of WAN traffic.

**Provisioned Storage** (not shown by default) - The provisioned storage for all the virtual machines in the VPG. This value is the sum of the values that are used in the vSphere Client console per virtual machine in the Virtual Machines tab for the root vCenter Server node. Each value is the sum of both the hard disk and memory. Thus, a virtual machine with 1GB hard disk and 4GB memory will show 5GB provisioned storage.

**Used Storage** - The storage used by all of the virtual machines in the VPG. This value is the sum of the values that are used in the vSphere Client console per virtual machine in the Virtual Machines tab for the root vCenter Server node.

---

**List View - BACKUP**

The following information is displayed in the BACKUP view:

**Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:

- **Green:** The VPG is being replicated, including syncing the VPG between the sites.
- **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.
Move the cursor over the Alert status indicator to display details of the alert.

<table>
<thead>
<tr>
<th>VPG Name (#VMs):</th>
<th>The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retention Policy:</td>
<td>Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 30 days before the disaster, or protection is extended to include offsite backups of the virtual machines, going back for a maximum of one year.</td>
</tr>
<tr>
<td>Backup Status:</td>
<td>The status of the backup.</td>
</tr>
<tr>
<td>Backup Repository:</td>
<td>The name of the repository where the jobs are stored.</td>
</tr>
<tr>
<td>Restore Point Range:</td>
<td>The restore points for the backup jobs out of the total backup jobs run for the VPG.</td>
</tr>
<tr>
<td>Backup Scheduling:</td>
<td>The schedule for offsite backups.</td>
</tr>
</tbody>
</table>

**Additional Fields and Options**

In the GENERAL, PERFORMANCE, and BACKUP views you can:

- Show/Hide Columns, Create View and Reset Columns using the settings ( ) menu.
- Sort the list by a column by clicking in the column title.
- Filter information in the columns by clicking the filter button ( ) that is displayed when the mouse cursor is moved into the column title. Active filters are displayed with a yellow background.

In the grid view each VPG is displayed as a card.

The default view is of all the VPG cards, un-grouped and sorted by VPG name.

The cards displayed can be filtered by clicking the filter button ( ). The default filters are Direction and Protection Status. You can click the ADD button to open the filters drop-down, and select additional filters. Active filters are displayed with a yellow background.

Each card contains the following:

**Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:

- **Green:** The VPG is being replicated, including syncing the VPG between the sites.
- **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the Alert status indicator to display details of the alert.
**VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab. The number of VMs protected in the VPG is displayed in parentheses.

**Direction:** The direction of the replication, from this site to the remote site or from the remote site to this site.

**Peer Site:** The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.

**State:** The current substatus of the VPG, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

**Actual RPO:** The time since the last checkpoint was written to the journal. This should be less than the Target RPO Alert value specified for the VPG.

**Operation:** The operation, such as Move, that is currently being performed.

---

**Saving Details of Virtual Protection Groups to a File**

You can save details of every VPG displayed in the VPGs tab to a CSV file, which can be opened using programs such as Microsoft Excel.

In the VPGs tab, click **EXPORT** and specify where to save the VPG details.
Monitoring a Single VPG

You can monitor the status of a specific VPG by clicking the VPG name in the VPGs tab or clicking the VPG name in the VMs tab. The VPG details are displayed in a dynamic tab.

**General Tab**

The tab on the left side shows the status of the VPG. The following information is displayed in this tab:

**Performance Graphs**

The current VPG performance, which includes the following information:

- **RPO:** The current Recovery Point Objective (RPO) of the Virtual Protection Group (VPG).
- **IOPS (I/O per second):** The total amount of I/O write operations generated by the protected virtual machines comprising the Virtual Protection Group (VPG).
- **Throughput (MB per Second):** The total amount of uncompressed data written by the protected virtual machines comprising the Virtual Protection Group (VPG).

During synchronization processes (such as bitmap sync, initial sync and delta sync) this value will also consist of the uncompressed data read from the protected disks.

- **WAN Traffic (MB per second):** The total amount of compressed data transferred between the protected and recovery sites of the Virtual Protection Group (VPG).

**JOURNAL HISTORY**

The journal history shows:
- The SLA defined for the VPG.
- The amount of time currently covered by information in the journal.
- The earliest—oldest—checkpoint currently in the journal that can be used for a recovery operation.

**OFFSITE BACKUP**

If backup is enabled, the following backup details are displayed:
Retention Policy: Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 30 days before the disaster, or protection is extended to include offsite backups of the virtual machines, going back for a maximum of one year.

Backup Status: The status of the backup.

Backup Repository: The name of the repository where the jobs are stored.

Restore Point Range: The restore points for the backup jobs out of the total backup jobs run for the VPG.

Backup Scheduling: The schedule for offsite backups.

ACTIVE ALERTS, RUNNING TASKS, and EVENTS

A listing of the currently active alerts and running tasks, and the events run during the last few hours.

User input, for example, stopping a failover test or committing or rolling back a Move or Failover operation, can be initiated from the relevant task displayed in the RUNNING TASKS section.

PROTECTED VMs Tab

The PROTECTED VMs tab shows details about the protected virtual machines:

- **Name**: The name of the virtual machine.
- **Group**: The boot order group to which the virtual machine belongs.
- **Protection Host**: The protected virtual machine host.
- **Storage Protected**: The name of the protected storage.
- **Provisioned**: The protected virtual machine provisioned storage.
- **Used**: The amount of data used on the recovery site for this virtual machine.
- **Recovery Data Size**: The total size of the data on the recovery site.
- **Failover Network**: The failover network used when recovering this virtual machine.
- **Test Network**: The test network used when testing the recovery of this virtual machine.

The following details are displayed with a vSphere recovery site:

- **Recovery Host**: The host to use for recovery.
Monitoring a Single VPG

VM Recovery Datastore: The name of the recovery datastore.
Folder: The folder where the virtual machine is recovered to.

The following details are displayed with a Hyper-V recovery site:

Recovery Host: The host to use for recovery.
VM Recovery Storage: The name of the recovery storage.

The following details are displayed with an AWS recovery site:

Failover/Move VPC: The virtual network dedicated to your AWS account during a failover or move operation. A security group and subnet must be assigned to this VPC.
Failover/Move Subnet: The subnet mask for the VPC network during a failover or move operation.
Failover/Move Security Groups: The AWS security to be associated with the virtual machines in this VPG during a failover or move operation.
Test VPC: The virtual network dedicated to your AWS account during a failover test operation. A security group and subnet must be assigned to this VPC.
Test Subnet: The subnet mask for the VPC network during a failover test operation.
Test Security Groups: The AWS security to be associated with the virtual machines in this VPG during a failover test operation.
Folder: The folder where the virtual machine is recovered to.

SITES Tab

The SITES tab shows the topology of the VPG, including both the protected and recovery sites.
Monitoring Zerto Virtual Replication

**SETTINGS Tab**

The SETTINGS tab shows details about the VPG settings, divided into general, replication, recovery, and backup categories.

**Monitoring Tasks**

Tasks initiated by Zerto Virtual Replication are also displayed in the vSphere Web Client and Client console. Recent tasks can also be reviewed for a site by clicking the TASKS area in the status bar at the bottom of the user interface.

The following information is displayed for each task:

- **Status**: The task status.
- **Name**: The name of the task.
- **Description**: A description of the task.
- **Action**: The ability to perform an action directly. For example, stop a failover test, or commit or rollback a move or failover operation.
The full details of the tasks can be monitored in the TASKS subtab under the MONITORING tab.

The following information is displayed for each task:

**Task status indicator:** The color indicates the status of the task. The following statuses exist for each task:

- **Green:** The task was completed successfully.
- **Red:** The task failed.

**Task:** The task name.

**Status:** The task status.

**Related Entities:** The sites which were effected by the task.

**User:** The user who initiated the task.

**Started:** The date and time the task started.

**Completed:** The date and time the task completed.

**Notes:** Notes added at the completion of a failover test.
Monitoring Protected Virtual Machines – The VMs Tab

View details of the protected VMs in the VMs tab. This tab lists all the protected virtual machines from both the local and remote sites and provides summary details of each virtual machine.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

GENERAL View

The following information is displayed in the GENERAL view:

Alert status indicator: The color indicates the status of the VPG:
- Green: The VPG is being replicated, including syncing the VPG between the sites.
- Orange: The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- Red: The VPG is not being replicated, for example, because communication with the remote site is down.

VM Name: The name of the virtual machine. The name is a link.

VPG Name: The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab.

Direction: The direction of the replication, from this site to the remote site or from the remote site to this site.

Peer Site: The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.

Priority: The priority of the VPG.

Protection Status: The current status of the virtual machine, such as Meeting SLA. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

State: The current substatus of the VPG, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

Actual RPO: The time since the last checkpoint was written to the journal. This should be less than the Target RPO Alert value specified for the VPG.

Operation: The operation, such as Move, that is currently being performed.
PERFORMANCE View

The following information is displayed in the PERFORMANCE view:

**IO:** The IO per second between all the applications running on the virtual machine and the VRA that sends a copy to the remote site for replication.

**Throughput:** The MB per second for all the applications running on the virtual machines being protected. There can be a high IO rate with lots of small writes resulting in a small throughput as well as a small IO with a large throughput. Thus, both the IOPS and Throughput values together provide a more accurate indication of performance.

**Network:** The amount of WAN traffic.

**Provisioned Storage** – The provisioned storage for the virtual machine in the recovery site. This value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Client console per virtual machine in the *Virtual Machines* tab for the root vCenter Server node. Each value is the sum of both the hard disk and memory. Thus, a virtual machine with 1GB hard disk and 4GB memory will show 5GB provisioned storage.

**Used Storage** – The storage used by the virtual machine in the recovery site. This value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Client console per virtual machine in the *Virtual Machines* tab for the root vCenter Server node.

BACKUP View

The following information is displayed in the BACKUP view:

**Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:

- **Green:** The VPG is being replicated, including syncing the VPG between the sites.
- **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the Alert status indicator to display details of the alert.

**VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab.

**Retention Policy:** Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 30 days before the disaster, or protection is extended to include offsite backups of the virtual machines, going back for a maximum of one year.

**Backup Status:** The status of the backup.

**Backup Repository:** The name of the repository where the jobs are stored.

**Restore Point Range:** The restore points for the backup jobs out of the total backup jobs run for the VPG.

**Backup Scheduling:** The schedule for offsite backups.

Additional Fields

In the GENERAL, PERFORMANCE, and BACKUP views you can:

- Show/Hide Columns, Create View and Reset Columns using the settings ( ) menu.
- Sort the list by a column by clicking in the column title.
- Filter information in the columns by clicking the filter button ( ) that is displayed when the mouse cursor is moved into the column title. Active filters are displayed with a yellow background.
Monitoring Peer Sites – The SITES Tab

View details of the paired sites in the SITES tab. This tab lists all the sites paired to the local site and provides summary details of each paired site.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

GENERAL View

The following information is displayed in the GENERAL view:

Alert status indicator: The color indicates the alert status of the site:
- **Green**: The Zerto Virtual Manager for the site is running without problems.
- **Orange**: The Zerto Virtual Manager for the site has a problem that does not stop the protection of virtual machines, such as an RPO value larger than the Target RPO Alert value for a VPG.
- **Red**: The Zerto Virtual Manager for the site is not running correctly, for example, because communication with the site is down.

Site Name: The name specified for the paired site during installation or in the Site Settings dialog.

Location: The location specified for the paired site during installation or in the Site Settings dialog.

Site IP: The IP of the peer site.

Network: The amount of WAN traffic.

IOPS: The IO per second between all the applications running on the virtual machine in the VPG and the VRA that sends a copy to the remote site for replication.

Incoming Throughput: The MBs for all the applications running on the virtual machine being protected. There can be a high IO rate with lots of small writes resulting in a small throughput as well as a small IO with a large throughput. Thus, both the IO and Incoming Throughput values together provide a more accurate indication of performance.

Provisioned Storage (GB): The maximum storage that can be protected.

# VPGs: The total number of VPGs being protected by the site and replicated to the site.

# VMs: The total number of virtual machines being protected by the site and replicated to the site.
Monitoring Zerto Virtual Replication

Additional Fields

There are additional fields that you can display that are listed when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon ( ):

Used Storage (GB) – The amount of storage used by the virtual machines in the site.

ZORG Name – A name given to an organization by a cloud service provider. For details refer to Zerto Cloud Manager Administration Guide.

Version – The Zerto Virtual Replication version installed at this site.

Monitoring Virtual Replication Appliances

You can monitor information about all the VRAs for the local site in the VRAs subtab under the SETUP tab. You can also drill-down to monitor information about a specific VRA displayed in the VRAs tab:

- “Monitoring VRAs – The SETUP Tab – VRAs Tab”, below.
- “Monitoring a Single VRA”, on page 201.

Monitoring VRAs – The SETUP Tab – VRAs Tab

View details of the VRAs in the VRAs subtab, under the SETUP tab. All the hosts in the vCenter Server are listed, and details of VRAs for each host, when installed, are also shown.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

General View

In this view, the number of installed VRAs is displayed in the VRAs tab. The following information is displayed in this view:

Cluster – The cluster name, if relevant.

Host Address – The host IP address for the VRA. If the host is part of a cluster, the cluster name is displayed with the hosts under the cluster.

Host Version – The host version.

Alert Status – The status of alerts in the VRA virtual machine.

VRA Name – The name of the VRA virtual machine.

VRA Status – The VRA status. For example, Installed or Ghost VRA.

VRA Version – Either Latest if the version installed is the most current version or Outdated if it can be upgraded. A tooltip displays the actual version.
VRA Address – The IP address of the VRA virtual machine.

# VPGs – The number of VPGs with a virtual machine for which the VRA either manages the protection or the recovery of the data.

# VMs – The number of virtual machines managed by the VRA.

**SETTINGS View**

The following information is displayed in the SETTINGS view:

VRA Group – The group of VRAs to which this VRA belongs. When VRAs use different networks, they can be grouped by network.

VRA RAM – The amount of memory allocated to the VRA to buffer data before it is sent to the recovery site or at the recovery site before it is written to the journal.

Datastore – The datastore used by the VRA.

Datastore Cluster – The datastore cluster used by the VRA, if relevant.

**WORKLOAD PROTECTION View**

The following information is displayed in the WORKLOAD PROTECTION view:

# VPGs: The number of VPGs with a virtual machine for which the VRA is used either for protection or recovery.

# VMs: The number of virtual machines for which the VRA is used either for protection or recovery.

# of Protected VPGs: The number of VPGs with a virtual machine for which the VRA manages the protection of their data.

# of Protected VMs: The number of virtual machines for which the VRA manages the protection of their data.

# of Protected Volumes: The number of volumes for which the VRA manages the protection of their data.

# of Recovery VPGs: The number of VPGs with a virtual machine for which the VRA manages the recovery of the data.

# of Recovery VMs: The number of virtual machines for which the VRA manages the recovery of the data.

# of Recovery Volumes: The number of volumes for which the VRA manages the recovery of the data.

**Additional Fields**

There are additional fields that you can display that are listed when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon ( ▼ ):

Cluster: The cluster with the host used by the VRA.

VC Network: The network used by the VRA.

# Volumes: The number of volumes for which the VRA manages the protection or recovery of data.
Monitoring a Single VRA

You monitor the status of a single VRA by clicking the VRA name in the VRAs tab. The VRA details are displayed in a dynamic tab.

![Monitoring a Single VRA](image)

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

**Installed Tab**

The tab on the left side shows the status of the VRA. The following information is displayed when this tab is selected:

**Performance Graphs**

- CPU Usage – The percentage of CPU used by the VRA.
- Local Memory – The percentage of the VRA memory used by protected volumes managed by the VRA. If the memory consumption is high you can consider vMotioning some of the virtual machines to a different host.
- Remote Memory – The percentage of the VRA memory used by recovery volumes managed by the VRA. If the memory consumption is high you can consider changing the target host of some of the virtual machines to a different host.

**ACTIVE ALERTS, RUNNING TASKS, and EVENTS**

A listing of the currently active alerts and running tasks, and the events run during the last few hours.
VPGs Tab

Information about the VPGs with virtual machines that are on the host with the VRA is displayed in the VPGs tab.

**GENERAL View**

The following information is displayed in the **GENERAL** view:

- **Alert status indicator** - The color indicates the status of the VPG:
  - Green - The VPG is being replicated, including syncing the VPG between the sites.
  - Orange - The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
  - Red - The VPG is not being replicated, for example, because communication with the remote site is down.

- **Direction** - The direction of the replication, from this site to the remote site or from the remote site to this site.

- **Protected Site** - The name of the protected site.

- **Recovery Site** - The name of the recovery site.

- **Name** - The name of the VPG.

- **Protection Status** - The current status of the VPG, such as Meeting SLA. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

- **State** - The current substatus of the VPG, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

**PERFORMANCE View**

The following information is displayed in the **PERFORMANCE** view:

- **# VMs on VRA/#VMs in VPG** - The number of virtual machines on the VRA and the number of virtual machines in the VPG.

- **Provisioned** - The provisioned storage for all the virtual machines in the VPG. This value is the sum of the values that are used in the vSphere Client console per virtual machine in the **Virtual Machines** tab for the root vCenter Server node. Each value is the sum of both the hard disk and memory. Thus, a virtual machine with 1GB hard disk and 4GB memory will show 5GB provisioned storage.

- **Used** - The storage used by all virtual machines in the VPG. This value is the sum of the values that are used in the vSphere Client console per virtual machine in the **Virtual Machines** tab for the root vCenter Server node.
**Monitoring Virtual Replication Appliances**

**IOPS** - The IO per second between all the applications running on the virtual machines in the VPG and the VRA that sends a copy to the remote site for replication.

**Throughput** - The MB per second for all the applications running on the virtual machines being protected. There can be a high IO rate with lots of small writes resulting in a small throughput as well as a small IO with a large throughput. Thus, both the **IOPS** and **Throughput** values together provide a more accurate indication of performance.

**BACKUP View**

The following information is displayed in the BACKUP view:

**Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:

- **Green:** The VPG is being replicated, including syncing the VPG between the sites.
- **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
- **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the Alert status indicator to display details of the alert.

**VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab.

**Retention Policy:** Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 30 days before the disaster, or protection is extended to include offsite backups of the virtual machines, going back for a maximum of one year.

**Backup Status:** The status of the backup.

**Backup Repository:** The name of the repository where the jobs are stored.

**Restore Point Range:** The restore points for the backup jobs out of the total backup jobs run for the VPG.

**Backup Scheduling:** The schedule for offsite backups.

**Additional Fields**

There is an additional field that you can display. This field is listed when you select *Show/Hide Columns* from the dropdown list shown by clicking the configuration icon ( ).

**ZORG** – A name given to an organization by a cloud service provider. For details refer to *Zerto Cloud Manager Administration Guide.*
Monitoring Zerto Virtual Replication

**VMs Tab**

Information about the virtual machines that are on the host with the VRA is displayed in the VMs tab.

**GENERAL View**

The following information is displayed in the **GENERAL** view:

- **Alert status indicator** - The color indicates the status of the VPG:
  - **Green** - The VPG is being replicated, including syncing the VPG between the sites.
  - **Orange** - The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
  - **Red** - The VPG is not being replicated, for example, because communication with the remote site is down.

- **Direction** - The direction of the replication, from this site to the remote site or from the remote site to this site.

- **Protected Site** - The name of the protected site.

- **Recovery Site** - The name of the recovery site.

- **VM Name** - The name of the virtual machine.

- **VPG Name** - The name of the VPG with which this virtual machine is associated.

- **Protection Status** - The current status of the virtual machine, such as Meeting SLA. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

- **State** - The current substatus of the virtual machine, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.

**PERFORMANCE View**

The following information is displayed in the **PERFORMANCE** view:

- **Provisioned on Host** - The provisioned storage for the virtual machine on the host. This value is the sum of the values that are used in the vSphere Client console for the virtual machine in the **Virtual Machines** tab for the root vCenter Server node. Each value is the sum of both the hard disk and memory. Thus, a virtual machine with 1GB hard disk and 4GB memory will show 5GB provisioned storage.

- **Used on Host** - The storage used by the virtual machine in the VPG. This value is the sum of the values that are used in the vSphere Client console for the virtual machine in the **Virtual Machines** tab for the root vCenter Server node.
Monitoring Virtual Replication Appliances

**Monitoring Zerto Virtual Replication**

**IO** - The IO per second between all the applications running on the virtual machines in the VPG and the VRA that sends a copy to the remote site for replication.

**Throughput** - The MB per second for all the applications running on the virtual machine. There can be a high IO rate with lots of small writes resulting in a small throughput as well as a small IO with a large throughput. Thus, both the IOPS and Throughput values together provide a more accurate indication of performance.

**Additional Fields**

There is an additional field that you can display. This field is listed when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon ( • ):

**ZORG** - A name given to an organization by a cloud service provider. For details refer to Zerto Cloud Manager Administration Guide.

**SETTINGS Tab**

Information about the VRA is displayed in the SETTINGS tab. This includes its version, the host on which it is located, its definition, the networks it uses, and its replication and recovery settings.

**Monitoring Datastores – The SETUP Tab – The DATASTORES Tab**

View details of the datastores used by Zerto Virtual Replication in the DATASTORES subtab, under the SETUP tab. This tab lists all the datastores used by Zerto Virtual Replication with an option to show all the datastores per cluster or for the hosts, whether used by Zerto Virtual Replication or not.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.
GENERAL View

In this view, the number of available datastores is displayed in the DATASTORES subtab. The following information is displayed in the GENERAL view:

Datastore – The name of the datastore or cluster.

Alert status indicator – The color indicates the alert status of the datastore:
- Green – The datastore is functioning as required.
- Orange – The datastore is functioning, but there are problems, such as not enough free space.
- Red – There is a problem with the datastore.

Status – The status of the datastore.

Device – The datastore device identifier.

Cluster – The cluster that the datastore is associated with.

Total Usage (GB) – The amount of GB used in relation to the total amount available.

DR Usage (GB) – The amount of GB used by Zerto Virtual Replication in relation to the total amount available.

# VRAs – The number of VRAs using the datastore.

WORKLOAD PROTECTION View

The following information is displayed in the WORKLOAD PROTECTION view:

Datastore – The name of the datastore or cluster.

Alert status indicator – The color indicates the alert status of the datastore:
- Green – The datastore is functioning as required.
- Orange – The datastore is functioning, but there are problems, such as not enough free space.
- Red – There is a problem with the datastore.

Total Usage (GB) – The amount of space, in GB, used in relation to the total amount available.

Type – The type of datastore.

Recovery Size – The amount of space used for recovery.

Journal Size – The amount of space used by the journals.

# Protected VMs – The number of protected virtual machines using the datastore.
Zerto Virtual Manager Administration Guide for VMware vSphere Environments - Version 6.0

Monitoring Zerto Virtual Replication

# Incoming VMs - The number of virtual machines to be recovered using the datastore.

Additional Fields

There are no additional fields that you can display. However, you can display all the fields shown in these views when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon (●).

Monitoring Repositories – The SETUP Tab – The REPOSITORIES Tab

View details of the repositories that can be used for offsite backup jobs in the REPOSITORIES subtab, under the SETUP tab. This tab lists all the repositories created for the site.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

GENERAL View

In this view, the available repositories are displayed. The following information is displayed:

- **Star** - A colored star indicates that this is the default repository.
- **Repository Name**: The name of the repository. This field contains icons that you can click to edit or delete the repository.
- **Repository Type**: The type of repository. The options are Local or Network Share (SMB).
- **Connectivity**: Whether the repository is connected or not.
- **Path**: The path to the repository.
- **Capacity**: The overall capacity of the repository.
- **Free Space**: The amount of free space currently available on the repository.
- **Active Backups**: The number of backup jobs currently active that are stored in the repository.
- **Restore Points**: The restore points for the backup jobs out of the total backup jobs saved to the repository.
- **Compression**: A check in this field means that the backups stored in the repository are compressed.

Click **NEW REPOSITORY** to display the New Repository dialog that you can use to create a new repository.
Monitoring Offsite Backups – The OFFSITE BACKUP Tab

View details of the offsite backup jobs in the OFFSITE BACKUP tab either by VPG or virtual machine. This tab lists all the defined offsite backups and their statuses.

See also:

- “VPGs Tab”, on page 208
- “VMs Tab”, on page 209

VPGs Tab

View details of the offsite backup jobs by VPG.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

GENERAL View

The following information is displayed in the GENERAL view:

- **VPG Name**: The name of the VPG.
- **Backup Site**: The site where the VPG is backed up. The backup jobs are stored either locally at this site or on a network shared drive which is accessible from this site.
- **Status**: The status of the job: Running or Scheduled.
- **Repository Name**: The name of the repository where the job is stored.
- **VPG Size**: The size of the VPG in the last run stored on disk.
- **Result of Last Run**: The result of the last run: Full success, Partial success, or Failed.
- **Restore Points**: The restore points for the backup jobs out of the total backup jobs run for the VPG.

RUN DETAILS View

The following information is displayed in the RUN DETAILS view:

- **VPG Name** – The name of the VPG.
Monitoring Offsite Backups – The OFFSITE BACKUP Tab

Result of Last Run – The result of the last run: Full success, Partial success, or Failed.

Time of Last Run – The time of the last run. If a backup job has not yet run on this VPG, the field is empty.

Next Scheduled Run – The time of the next scheduled run.

Last Full Backup – The date and time of the last full backup.

Additional Fields

There are additional fields that you can display that are listed when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon ( ):

Protected Site: The name of the site.

Last Backup Size: The size of the last backup performed by Zerto Virtual Manager.

ZORG: A name given to an organization by a cloud service provider. For details refer to Zerto Cloud Manager Administration Guide.

# VMs: The total number of virtual machines protected by the VPG.

# of Volumes: The number of volumes protected by the VPG.

VMs Tab

View details of the offsite backup jobs by virtual machine.

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

GENERAL View

The following information is displayed in the GENERAL view:

VM Name: The name of the virtual machine.

VPG Name: The name of the VPG.

Protected Site: The name of the site where the VPG is protected.

Backup Site – The site where the virtual machine is backed up. The backup jobs are stored either locally at this site or on a network shared drive which is accessible from this site.
Status: The status of the job.

Repository Name: The name of the repository where the job is stored.

VM Size: The size of the VMs stored on disk.

Result of Last Run: The result of the last run: Full success, Partial success, or Failed.

Restore Points: The restore points for the backup jobs out of the total backup jobs run for the VPG.

RUN DETAILS View

The following information is displayed in the RUN DETAILS view:

VM Name: The name of the Virtual machine.

VPG Name: The name of the VPG.

Result of Last Run: The result of the last run: Full success, Partial success, or Failed.

Time of Last Run: The time of the last run.

Next Scheduled Run: The time of the next scheduled run.

Last Full Backup: The date and time of the last full backup.

MORE Options

Click MORE > Edit to edit the backup parameters of the VPG.

Click MORE > Abort Backup to abort a running job. Any virtual machine volumes already stored in the repository are not removed and the job status is partial if there are any stored volumes.

Click MORE > Run Backup to start a job for a selected VPG, outside of the schedule for that VPG.

Click EXPORT to export the backup list as a Microsoft Excel worksheet.

Additional Fields

There are additional fields that you can display that are listed when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon (่า):  

Last Backup Size: The size of the last backup performed by Zerto Virtual Manager.

ZORG: A name given to an organization by a cloud service provider. For details refer to Zerto Cloud Manager Administration Guide.

# of Volumes: The number of volumes associated with the VM.

Zerto Performance Counters

During installation of Zerto Virtual Replication, Zerto-related performance counters are added to the Windows Performance Monitor on the machine where the Zerto Virtual Manager runs.

Uninstalling Zerto Virtual Replication, uninstalls the Zerto-related performance counters. Upgrading Zerto Virtual Replication updates any changes to the Zerto-related performance counters.
The Zerto-related performance counters are collected on the protected site only. These counters are described as follows.

<table>
<thead>
<tr>
<th>Category</th>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Zerto Checkpoints</strong></td>
<td>Checkpoint failures in last 10 minutes</td>
<td>Number of checkpoints that failed to be inserted in last 10 minutes.</td>
</tr>
<tr>
<td></td>
<td>Checkpoint insertions in last 10 minutes</td>
<td>Number of checkpoints inserted in last 10 minutes. The maximum is 120; normal performance is 90–115; less than 40 indicates a problem.</td>
</tr>
<tr>
<td></td>
<td>Time to insert last checkpoint</td>
<td>Time in milliseconds needed to insert the last checkpoint; normal is less than 5 seconds.</td>
</tr>
<tr>
<td><strong>Zerto Connectivity</strong></td>
<td># of connected VRAs</td>
<td>Number of VRAs connected to the local Zerto Virtual Manager.</td>
</tr>
<tr>
<td></td>
<td># of peer Zerto Virtual Managers (ZVMs)</td>
<td>Number of Zerto Virtual Managers connected to the local Zerto Virtual Manager.</td>
</tr>
<tr>
<td><strong>Zerto GUI</strong></td>
<td>Concurrent GUI calls to the ZVM</td>
<td>Number of concurrent GUI calls to the local Zerto Virtual Manager.</td>
</tr>
<tr>
<td><strong>Zerto Reflections</strong></td>
<td>AWS reflection collection time</td>
<td>Time in milliseconds needed to collect AWS environment data.</td>
</tr>
<tr>
<td></td>
<td>Hypervisor reflection collection time</td>
<td>Time in milliseconds needed to collect vCenter Server or SCVMM environment data.</td>
</tr>
<tr>
<td></td>
<td>Reflection data pushed in last 10 minutes</td>
<td>Size in bytes of environment data pushed in last 10 minutes to Zerto Virtual Managers connected to this site.</td>
</tr>
<tr>
<td></td>
<td>Reflection data pushed to peer ZVMs</td>
<td>Size in bytes of last pushed environment data.</td>
</tr>
<tr>
<td></td>
<td>Reflection data received from peer ZVMs</td>
<td>Size in bytes of last received environment data.</td>
</tr>
<tr>
<td></td>
<td>Reflection data received in last 10 minutes</td>
<td>Size in bytes of environment data received in last 10 minutes from Zerto Virtual Managers connected to the local Zerto Virtual Manager.</td>
</tr>
<tr>
<td></td>
<td>Reflections pushed to peer ZVMs in last 10 minutes</td>
<td>Number of times environment data was pushed to peer Zerto Virtual Managers in the last 10 minutes.</td>
</tr>
<tr>
<td></td>
<td>Reflections received from peer ZVMs in last 10 minutes</td>
<td>Number of times environment data was received from peer Zerto Virtual Managers in the last 10 minutes.</td>
</tr>
<tr>
<td></td>
<td>Retained data</td>
<td>Size in bytes of total retained pushed or received data.</td>
</tr>
<tr>
<td></td>
<td>vCD reflection collection time</td>
<td>Time in milliseconds needed to collect vCD environment data.</td>
</tr>
<tr>
<td><strong>Zerto Remote Calls</strong></td>
<td>Active incoming remote calls</td>
<td>Current number of active incoming calls being processed.</td>
</tr>
<tr>
<td></td>
<td>Active outgoing remote calls</td>
<td>Current number of calls sent to WCF services for which the Zerto Virtual Manager is still waiting for a response.</td>
</tr>
<tr>
<td></td>
<td>Incoming remote calls in last minute</td>
<td>Number of incoming remote calls received in last minute.</td>
</tr>
<tr>
<td></td>
<td>Outgoing remote calls in last minute</td>
<td>Number of outgoing remote calls executed in last minute.</td>
</tr>
<tr>
<td><strong>Zerto RPO</strong></td>
<td>Average RPO</td>
<td>Average RPO in seconds for all VPGs, displayed in the Dashboard.</td>
</tr>
<tr>
<td></td>
<td>Current maximum RPO</td>
<td>Current maximum RPO in seconds for all VPGs in this site.</td>
</tr>
<tr>
<td></td>
<td>Current minimum RPO</td>
<td>Current minimum RPO in seconds for all VPGs in this site.</td>
</tr>
<tr>
<td>Category</td>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Zerto System State</td>
<td>Number of alerts</td>
<td>Current number of active alerts.</td>
</tr>
<tr>
<td></td>
<td>System state loop length</td>
<td>Execution time of one system state loop. This should be less than 40 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>Time to calculate statistics</td>
<td>Time in milliseconds needed to calculate statistics during a system state loop.</td>
</tr>
<tr>
<td></td>
<td>Time to retrieve active alerts</td>
<td>Time in milliseconds needed to collect local Zerto Virtual Manager active alerts during a system state loop.</td>
</tr>
<tr>
<td></td>
<td>Time to save VRA performance counters</td>
<td>Time in milliseconds needed to save VRA performance information to a file.</td>
</tr>
<tr>
<td>Zerto Visual Query</td>
<td>Time to execute a VQ build loop</td>
<td>Time in milliseconds needed to execute a single VQ build loop. This should be less than 25 milliseconds.</td>
</tr>
<tr>
<td></td>
<td>Time to retrieve hypervisor information</td>
<td>Time in milliseconds to execute a remote query on peer Zerto Virtual Managers to retrieve hypervisor information from remote sites.</td>
</tr>
<tr>
<td></td>
<td>(reflection)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Time to retrieve local VM list</td>
<td>Time in milliseconds needed to retrieve the list of virtual machines from the local hypervisor.</td>
</tr>
<tr>
<td></td>
<td>Time to retrieve local VPG data</td>
<td>Time in milliseconds needed to retrieve VPG data from the local Zerto Virtual Manager.</td>
</tr>
<tr>
<td></td>
<td>Time to retrieve VPG list</td>
<td>Time in milliseconds to execute a remote query on peer Zerto Virtual Managers to build a list of VPGs on remote sites.</td>
</tr>
<tr>
<td>Zerto VRA Counters</td>
<td># of VRAs not updated</td>
<td>Should be zero or close to zero.</td>
</tr>
<tr>
<td></td>
<td># of VRAs updated</td>
<td>Should be near or equal to the number of active VRAs.</td>
</tr>
<tr>
<td></td>
<td>Average time of 5 most time-consuming VRA updates</td>
<td>Should be close to the median VRA update time.</td>
</tr>
<tr>
<td></td>
<td>Median VRA update time</td>
<td>Median time in milliseconds of last 100 VRA updates.</td>
</tr>
</tbody>
</table>
CHAPTER 9: MANAGING VPGS

After defining virtual protection groups (VPGs) the virtual machines specified as part of each VPG are protected. There are a number of ongoing management tasks that you can perform on a VPG, such as specifying a checkpoint to enable recovery to that specific point or you can modify the configurations of existing VPGs.

The following VPG management options are described in this chapter:

- “Editing a VPG”, below
- “Adding Virtual Machines to a VPG”, on page 215
- “Removing Virtual Machines from a VPG”, on page 219
- “Removing Protected Virtual Machines from the Hypervisor Inventory”, on page 220
- “Modifying Protected Virtual Machine Volumes”, on page 220
- “Pausing and Resuming the Protection of a VPG”, on page 221
- “Forcing the Synchronization of a VPG”, on page 222
- “Handling a VPG in an Error State”, on page 222
- “Deleting a VPG”, on page 223
- “Running an Unscheduled Offsite Backup”, on page 223
- “Ensuring Application Consistency – Checkpoints”, on page 224
- “Running Scripts Before or After Recovering a VPG”, on page 225
- “Exporting and Importing VPG Definitions”, on page 230
- “VPG Statuses and Synchronization Triggers”, on page 232
- “Managing Protection When the Recovery Datastore Will Be Unavailable (Datastore Maintenance)” on page 239

Monitoring VPGs and the VMs that are protected is described in “Monitoring Zerto Virtual Replication”, on page 184.

Editing a VPG

You can edit a VPG definition, including adding virtual machines to the VPG, as described in “Adding Virtual Machines to a VPG”, on page 215, deleting virtual machines from the VPG, or changing the information about how virtual machines are recovered.

Note: You cannot edit the VPG while a backup job is running.

After modifying the VPG, the definition is updated.

While the VPG definition is being updated, you cannot perform any operations on the VPG, such as adding a checkpoint, editing the VPG properties, or failing the VPG.

After the definition is updated, the VPG is synchronized with the recovery site.

To modify a VPG:

1. In the VPGs tab in the Zerto User Interface, select the VPG to be edited and click MORE > Edit VPG. You can also select the VPG, display the VPG details, and click EDIT VPG.

   The Edit VPG wizard is displayed, enabling editing the VPG, including adding and removing virtual machines from the VPG.

   Note: If the VPG was previously viewed, and the tab for this VPG is still displayed, you can access the details by selecting the tab.

2. Make any required changes to the VPG definition, as described in “Protecting Virtual Machines from a vCenter Server”, on page 39 and in “Protecting Virtual Machines to and From vCloud Director”, on page 98.

   You can jump directly to a step to make a change in that step, for example, the REPLICATION step or the RECOVERY step, by clicking the step.

   Steps that have been completed are marked with a check.
Note: If the Journal Size Hard Limit or Journal Size Warning Threshold in the advanced journal settings for the VPG SLA settings, or the default values are changed, the changed values are applied only to new virtual machines added to the VPG, and not to existing virtual machines.

3. Click **DONE**.

The VPG is updated and then synchronized with the recovery site, if required, for example when the host was changed.

### NOTE:

Changing a recovery Org vDC when recovering to vCD, results in an initial synchronization, resulting in all the checkpoints being deleted.

See also:
- “Modifying the Journal Size Hard Limit”, on page 214
- “Modifying the Retention Period for Offsite Backups”, on page 214
- “Modifying VPG Recovery Volume”, on page 214

### Modifying the Journal Size Hard Limit

If the journal size hard limit is reduced, and if the current size is greater than the newly defined size, the journal remains at the current size. When the amount of the journal used falls below the hard limit value it will not grow greater than the new hard limit. Unused journal volumes from the added volumes are marked for removal and removed after the time equivalent to three times the amount specified for the journal history, or twenty-four hours, whichever is more.

**Note:** If the Journal Size Hard Limit or Journal Size Warning Threshold in the VPG SLA settings are changed, the changed values are not applied to existing virtual machines but only to new virtual machines added to the VPG.

### Modifying the Retention Period for Offsite Backups

If the retention period is shortened, the number of backup jobs older than the new retention period are deleted from the repository.

### Modifying VPG Recovery Volume

If you change the recovery volumes in the Storage step from thin-provisioned to thick-provisioned or vice versa the volume goes through initial synchronization.
Adding Virtual Machines to a VPG

You can add virtual machines that are not already included in a VPG, to an existing VPG. A virtual machine can be protected in a maximum of three existing VPGs, provided that the VPGs are recovered to different sites.

- 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.
- You cannot add a virtual machine in an existing VPG, while a backup job is running.
- Only virtual machines with a maximum of 60 disks can be protected.
- 60 disks requires 4 SCSI controllers each with a maximum of 15 disks.

See the following topics:

- “Adding Virtual Machines to a VPG - When the Recovery Site is AWS”, on page 215
- “Adding Virtual Machines to a VPG - When the Recovery Site is Azure”, on page 215

Adding Virtual Machines to a VPG - When the Recovery Site is 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>IMPORT METHOD</th>
<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></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>
<td>16 TB</td>
</tr>
<tr>
<td>Windows</td>
<td>1 TB</td>
<td>1 TB</td>
<td>1 TB</td>
<td>16 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.

See also: “Import Methods for AWS”, on page 76

Adding Virtual Machines to a VPG - When the Recovery Site is Azure

- Azure ZCA can be installed only on Windows Server 2012 R2 and higher.
- Only virtual machines that are supported by Azure can be protected by Zerto Virtual Replication. All Windows operating systems are supported.
  - Note: Microsoft does not support operating systems that are past the End of Support date, without a Custom Support Agreement (CSA). For more information about Microsoft operating systems support for Microsoft Azure, refer to [https://support.microsoft.com/en-us/kb/2721672](https://support.microsoft.com/en-us/kb/2721672).
To replicate between Azure and your site, you must have a virtual machine in Azure with a Zerto Cloud Appliance installed on it. This ZCA must be paired with your site.

For Linux distribution, refer to Azure documentation:

**Requirements for Replication From Azure**
- For Virtual Machines to be protected from Azure, the VM volumes must reside in the Standard storage account defined during ZCA installation.
  - A Standard storage account is created or selected upon ZCA installation.
  - Type: Standard storage
  - Recovery and journal volumes reside on this Zerto Storage Account
  - Azure VMs with all disks on this Zerto Storage Account can be protected by Zerto.
  - Blob Storage is not supported.
  - Managed Disks are not supported.
- VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.

**Requirements for Replication To Azure**
- **Protected volumes** are recovered in Azure as VHD disks in a page blob. Virtual machines with disks that are less than 1GB are recovered with disks of 1GB.
  - **Note:** For some instance sizes, the Azure virtual machine is created with a Local SSD disk which is a temporary disk. This disk is in addition to the disks associated with each protected virtual machine.
  - The following limitations apply when protecting to Azure
    - Virtual machines with UEFI Firmware cannot be protected.
    - You cannot protect machines that have a disk larger than 4 TB.
    - The protected virtual machines needs to have at least one NIC.
    - Reserve at least 2 CPUs and 4GB RAM for the machine using a subnet accessible by other Zerto Virtual Replication sites.
    - The supported number of data disks and NICs per virtual machine is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.

**Requirements for Replication within Azure**
- Azure ZCA on both Azure sites need to be version 6.0 and higher.
- The following limitations apply when protecting within Azure:
  - Self replication is not supported.

**Additional Azure Considerations**
For additional considerations, see Azure subscription and service limits, quotas and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits.

For example from the link, see the following default values:
- There can be multiple Zerto Cloud Appliances per Azure subscription and region.
- 20 cores per subscription
- 200 Storage accounts per subscription
- 20 VMs per region per subscription
- 20 VMs per series (Dv2, F, etc.) cores per subscription per Region

Additionally, see the following example for maximum values:
A Standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a Standard storage account should not exceed this limit.

<table>
<thead>
<tr>
<th>VM TIER</th>
<th>BASIC TIER VM</th>
<th>STANDARD TIER VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk size</td>
<td>4 TB</td>
<td>4 TB</td>
</tr>
<tr>
<td>Max 8 KB IOPS per persistent disk</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Max number of disks performing max IOPS</td>
<td>66</td>
<td>50</td>
</tr>
</tbody>
</table>

See also "Azure Limitations Which Affect Installation and Recoverability", on page 217.

Azure Limitations Which Affect Installation and Recoverability

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

Default Azure limitations which Affect Installation

- Storage Limitations:
  - Number of storage accounts: **200 per subscription** (note: max is 250)

Default Azure Limitations which Affect Recovery

<table>
<thead>
<tr>
<th>Virtual Machines Limitations</th>
<th>VMs per subscription per region: 20 (max: 10K)</th>
</tr>
</thead>
<tbody>
<tr>
<td>VM total cores per subscription per region:</td>
<td>20</td>
</tr>
<tr>
<td>Instance sizes:</td>
<td>Limited per region.</td>
</tr>
<tr>
<td>Many of them are 20 cores per region per subscription</td>
<td></td>
</tr>
<tr>
<td>Resource groups per subscription:</td>
<td>800</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Networking</th>
<th>Network interfaces per region: 350</th>
</tr>
</thead>
<tbody>
<tr>
<td>NICs per instance:</td>
<td>Depends on instance size:</td>
</tr>
<tr>
<td>Private IP Addresses per VNET per subscription per region:</td>
<td>4096</td>
</tr>
<tr>
<td>Cloning of IP addresses during recovery operations:</td>
<td>Due to an Azure limitation, failing over Linux VMs with static IP is not supported.</td>
</tr>
</tbody>
</table>
To add a virtual machine to an existing VPG:

1. In the VPGs tab in the Zerto User Interface, select the VPG and click MORE > Edit VPG. You can also select the VPG to display the VPG details and click EDIT VPG.
   
   The Edit VPG wizard is displayed, enabling you to edit the VPG, including adding and removing virtual machines from the VPG.

   In the VMs step, select the virtual machines to add and click the arrow pointing right to include these machines in the VPG.
   
   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 (Multi Target) section.

   Virtual machines protected in the maximum number of VPGs are not displayed in the Select VMs dialog.

   **Note:** 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.

   If you want to define the boot order of the VPGs, click DEFINE BOOT ORDER.

2. Configure the settings for the new virtual machines in the same way that you configured the other virtual machines in the VPG, when you created the VPG.

3. Click DONE.

   The virtual machines are added to the VPG. This process may take a few minutes. While the VPG definition is being updated, you cannot perform any operation on the VPG, such as adding a checkpoint, editing its properties, or recovering it.

   After the VPG definition has been updated, the protected and recovery sites are then synchronized. During the synchronization period, the Protection Status displayed in the VPGs tab of the Zerto User Interface is: Meeting SLA n/m VMs where n is the number of virtual machines that were originally in the VPG, and m is the total number of virtual machines in the VPG, including the virtual machines that are currently being synced. While the virtual machines that were added are being synced, the VPG can be failed over but the failover only includes the original virtual machines in the VPG.

   For example, in the following screen shot, two virtual machines were added to the VPG, Operations, that originally contained 2 other virtual machines.
When the sync process for a virtual machine is complete, Zerto Virtual Manager tags the first checkpoint that includes a new virtual machine with: VM ‘XXX’ is fully synced where XXX is the name of the virtual machine that was synced.

When you perform a recovery operation using one of these checkpoints, or any later checkpoint, all the virtual machines that have completed syncing will be recovered.

For example, in the following screen shot, two virtual machines were added to the VPG Operations. When the sync process for each machine completed, a checkpoint was added to show this. If you use the checkpoint written on Dec 20, 2015 at 15:39:48, the recovery will include the virtual machine Clients but not FX history.

If you select the checkpoint at 15:40:03 or a later checkpoint, a recovery operation will also include the virtual machine FX history.

If the virtual machine is added to a VPG replicating to a resource pool in VMware vSphere environments, Zerto Virtual Replication checks that the additional virtual machine doesn’t exceed the resource pool capacity, such that the sum of the virtual machine reservation is less than or equal to the resource pool CPU and storage settings.

**Removing Virtual Machines from a VPG**

If a user removes a virtual machine from a VPG, the checkpoints of the VPG are retained.

**Note:** Once a virtual machine is removed, it is no longer possible to recover it.

**Removing Virtual Machines from a vCD vApp**

If a user removes a virtual machine from a vCD vApp, the checkpoints of the VPG are retained. Once a virtual machine is removed, it is no longer possible to recover it.
Removing Protected Virtual Machines from the Hypervisor Inventory

From time to time, a virtual machine or a host is removed from the hypervisor inventory for various purposes, such as maintenance. If the removed virtual machines are protected in VPGs, the VPGs enter a pause state and the replication is paused. The checkpoints of the VPG are retained. The removed virtual machine is grayed out in the virtual machines tab in the dashboard as well as in the Edit VPGs, VMs tab.

When a VPG is in a state of pause, the recovery of all the virtual machines, including the removed, grayed out virtual machines, is possible.

For VPGs to enter a state of pause and to enable the replication to pause, the following conditions must apply:

- The ZVM on the protected and recovery sites are of version 5.5 and higher.
- The VRA installed on the recovery site is of version 5.5 and higher.

To resume replication, do one of the following:

- Return the virtual machine or the host back into the hypervisor inventory.
- In Edit VPG, remove from the VPG the virtual machine that was previously removed from VMware inventory.

Modifying Protected Virtual Machine Volumes

Adding or deleting volumes for a virtual machine protected in a VPG, is automatically reflected in the volumes used for the mirror virtual machine, managed by the VRA in the recovery site.

Adding or deleting a volume in any virtual machine protected in a VPG, causes the journal to be reset as all the checkpoints in the journal are removed.

If you add a volume to the virtual machine, the total number of disks cannot exceed 15 disks per SCSI controller and up to 4 SCSI controllers.

Resizing non-RDM volumes of a virtual machine protected in a VPG are automatically reflected in the volumes used for the mirror virtual machine, managed by the VRA in the recovery site.

**Note:** If the protected volume is associated with an RDM as a target for replication, the RDM will need to be resized manually, as described in “Modifying a Protected RDM Volume”, below.

Changing the defined size of a journal of a virtual machine in a VPG is automatically reflected in the VRA in the recovery site.

When protecting to AWS, if you add a volume to the virtual machine the total number of disks cannot exceed 12 for Linux machines and 22 for Windows machines, including the boot disk.

See the following topics:

- “Changing the Recovery Datastore for a Protected Virtual Machine”, on page 221
- “Modifying a Protected RDM Volume”, on page 221
Changing the Recovery Datastore for a Protected Virtual Machine

To change the recovery datastore for a virtual machine volume, the new datastore must have 45GB or 25% of the storage size for the change to be performed.

Modifying a Protected RDM Volume

If a RDM volume for a protected virtual machine is replicated to an RDM volume in the recovery site and the protected RDM volume is resized, it is not automatically resized in the recovery site.

Note: If the RDM volume is replicated to a VMDK in the recovery site, the recovery site VMDK is automatically resized when the protected site RDM is resized.

To enable protecting a VPG after resizing a protected virtual machine RDM volume:
1. Remove the protected virtual machine from the VPG.
   Note: If the VPG contains more than one virtual machine, remove the protected virtual machine from the VPG, and save the changes. If the VPG contains only one virtual machine, delete the VPG, and, if the virtual machine target disks are of VMDK format, make sure to choose to keep the target disks when the option is displayed.
2. Resize the RDM (both local and remote) as described in the VMware Expanding the size of a Raw Device Mapping (RDM) knowledge base article.
   Note: The vCenter will not detect that RDMs were resized unless this procedure is followed.
3. Protect the virtual machine again after resizing the RDM.

At this point, the VPG will go through a Delta Sync to compare protected and recovery volumes for changes, and once synchronized, it will enter the Meeting SLA state.

Pausing and Resuming the Protection of a VPG

During periods when the WAN bandwidth is utilized to its maximum, you can pause the protection of a VPG, to free up some of this bandwidth. After pausing the protection, the VPG can still be recovered to the last checkpoint written to the journal before the pause operation.

Note:
- Zerto recommends adding a checkpoint to the VPG immediately before pausing protection, if you might want to recover the VPG to the latest point in time before the pause.
- You cannot pause a VPG while a backup job is running.

To pause the protection of VPGs:
1. In the Zerto User Interface, click the VPGs or VMs tab and select one or more VPGs to pause protection.
2. Click MORE > PAUSE.
   A warning is displayed. If you click PROCEED in this warning, the VPG protection is paused.
   Note: If the VPG was previously viewed, and the tab for this VPG is still displayed, you can access the details by selecting the tab.
   The VPG protection is paused until you click Resume VPGs.

To resume the protection of VPGs:
1. In the Zerto User Interface, click the VPGs or VMs tab and select one or more VPGs to resume protection.
2. Click MORE > Resume.
   After resuming protection, a Bitmap Sync will most probably be performed to synchronize the protection and recovery sites.
Forcing the Synchronization of a VPG

If the protected virtual machines are updated such that they are no longer synchronized with their mirror machines in the recovery site, you can force the resynchronization of the machines. An example of when the machines can be out-of-sync is when there is a rollback of a virtual machine to a VMware snapshot. In this case, the recovery virtual machine will include changes that have been rolled back in the protected machine, so that they are no longer synchronized.

You can force the synchronization of the machines in a VPG to remedy this type of situation.

**Note:** You cannot force the synchronization of a VPG while a backup job is running.

**To forcibly synchronize a VPG:**
1. In the Zerto User Interface, select the VPGs or VMs tab and click the VPG to display the VPG details.
2. Click MORE > Force Sync.

   **Note:** If the VPG was previously viewed, and the tab for this VPG is still displayed, you can access the details by selecting the tab.

The VPG starts to synchronize with the recovery site. As the journal fills up during the synchronization, older checkpoints are deleted from the journal to make room for the new data and the data prior to these checkpoints are promoted to the virtual machine virtual disks. Thus, during the synchronization, you can recover the virtual machine to any checkpoint still in the journal, but as time progresses the list of checkpoints available can lessen. If the journal is not big enough to complete the synchronization without leaving at least ten minutes worth of checkpoints, the synchronization pauses for the time specified in the Replication Pause Time value for the VPG, to enable intervention to ensure recovery to a checkpoint remains available. The intervention can be, for example, increasing the size of the journal, or cloning the journal as described in “Deleting a VPG”, on page 223.

Handling a VPG in an Error State

When a volume connected to a virtual machine in a VPG is deleted, the VPG and all the virtual machines in that VPG enter an error state and an alert is issued.

**Note:** When a VPG is in an error state, recovery operations cannot be performed.

Edit the VPG definition to resolve the error in one of the following ways.

- Remove the virtual machine that was connected to the deleted volume from the VPG: In the VPGs tab in the Zerto User Interface, select the VPG to be edited and click MORE > Edit VPG. In the Edit VPG wizard, go to the VMs step. Select the virtual machine to be removed and click the arrow pointing left.
- Replace the volume that was deleted: In the VPGs tab in the Zerto User Interface, select the VPG to be edited and click MORE > Edit VPG. In the Edit VPG wizard, go to the STORAGE step and click the empty Recovery Volume Location field or select that row and click EDIT SELECTED. In the Edit Volumes dialog that is displayed, choose the volume source: Datastore, RDM, or Preseeded volume, specify other volume options and click OK.

**NOTE:**
- If you choose a new volume, a volume initial sync is performed. During this period, new checkpoints are not added to the journal and recovery operations cannot be performed on the VPG.
- If you choose a preseeded volume, a delta sync is performed. During this period, new checkpoints are not added to the journal but recovery operations are possible. During a delta sync, you can recover to the last checkpoint in the journal.

**IMPORTANT:**
It is not possible to perform a move during a delta sync.
Deleting a VPG

You can delete a VPG and either keep the target disks to use later for preseeding if you want to reprotect any of the virtual machines in the deleted VPG or delete these disks. Any offsite backups stored for the VPG are not deleted and the virtual machines that were backed up can be restored.

Note: You cannot delete a VPG while a backup job is running.

To delete a VPG:
1. In the Zerto User Interface, click the VPGs or VMs tab and select one or more VPGs to delete.
2. Click MORE > Delete.
   The Delete VPG dialog is displayed.
3. Check Keep the recovery disks at the peer site if you might reprotect the virtual machines. Checking this option means that the target replica disks for the virtual machines are saved so that they can be used as preseeded disks if the virtual machines are re-protected.
4. Click APPLY to delete the VPG.
   The VPG configuration is deleted. The VRA on the recovery site that handles the replication for the VPG is updated including keeping or removing the replicated data for the deleted VPG, dependent on the Keep the recovery disks at the peer site setting during the deletion.
   The locations of the saved target disks are specified in the description of the event for the virtual machines being removed, event EV0040, displayed in MONITORING > EVENTS.

See also “Deleting a VPG When the Status is Deleting”, on page 223.

Deleting a VPG When the Status is Deleting

If, for some reason, the VPG cannot be deleted, the VPG status changes to Deleting and the substatus is VPG waiting to be removed. Attempting to delete the VPG a second time causes the following to be displayed:

Retry: Retry deleting the VPG.
Force Delete: Forcibly delete the VPG.
Cancel: Cancel the delete operation.

Running an Unscheduled Offsite Backup

After initializing the VPG, Zerto Virtual Replication periodically checks that the schedule to run an offsite backup - either daily or weekly - has not passed. At the scheduled backup time, the offsite backup is run and the offsite backup file stored in the specified repository.

To run an unscheduled offsite backup:
1. In the Zerto User Interface, click the VPGs or VMs tabs and select one or more VPGs to be backed up.
   Note: You can also start from the OFFSITE BACKUP tab.
2. Click MORE > Run Backup.
Note: If the VPG was previously viewed, and the tab for this VPG is still displayed, you can access the details by selecting the tab.

3. Click OK.

The offsite backup starts. You can monitor the progress in the Offsite Backup tab and the tasks pane. During the backup job you cannot perform any other operation on the VPG without first aborting the job. You can start a live failover and you are then prompted to abort the job.

Scheduled backup runs for the VPG are skipped until the unscheduled run ends.

If the job runs out of the configured backup window, the virtual machines that are already stored in the repository are kept but remaining virtual machines in the VPG are not backed up. The job is reported as a partial backup.

Ensuring Application Consistency – Checkpoints

Checkpoints are recorded automatically every few seconds in the journal. These checkpoints ensure crash-consistency, and are written to the virtual machines journals by the Zerto Virtual Manager.

Each checkpoint has the same timestamp which is set by the Zerto Virtual Manager.

During recovery you pick a checkpoint in the journal and recover to this point. The crash-consistent checkpoints guarantee write order fidelity.

For Example:

If write A on a virtual machine in the VPG occurred before write B on a virtual machine in the VPG, then when a checkpoint is written, the journal will contain:

- Neither of the writes
- Both writes, and if they overlap the B data takes precedence
- Only A - indicating the checkpoint occurred between A and B

The coordination is done by the Zerto Virtual Manager.

You can also use a script to place the application in a quiesced mode, such as Oracle Hot Backup mode, and execute the Zerto Virtual Replication PowerShell cmdlet Set-Checkpoint, then release the quiesced mode. For more information about Zerto Virtual Replication PowerShell cmdlets, see Zerto Virtual Replication Cmdlets.

Note:

- To write application-consistent checkpoints, there is a performance impact on the virtual machine running the application as a result of the application-consistent mechanism used. This is because the guest operating system and any integrated applications will be quiesced.

  This impact on performance may be negligible and does not always happen since not all applications require these checkpoints in order to achieve successful application recovery. Also, Zerto Virtual Replication only requires the guest and application to quiesce for a brief moment, just long enough to add a checkpoint.

As previously mentioned, checkpoints are recorded every few seconds in the journal. After a while, the number of checkpoints available from which to choose a recovery point can be in excess of thousands per VPG.

When this threshold is reached, in order to enable efficient management and use of the checkpoints, the number of checkpoints is diluted with respect to time, as follows:

- Within the latest 2 hours: All of the checkpoints are available for recovery.
- Between 2 and ~4.5 hours: There are about two to three checkpoints every 15 minutes.
- From 4.5 hours and over: 1 checkpoint is kept every 15 minutes.

  Note: Checkpoints which are either added manually, or marked as part of a Failover test are not diluted.

This section describes the different options available to ensure application consistency:

- “Adding a Checkpoint to a VPG to Identify a Key Point”, below.
Adding a Checkpoint to a VPG to Identify a Key Point

In addition to the automatically generated checkpoints, you can add checkpoints manually to ensure application consistency and to identify events that might influence recovery, such as a planned switch-over to a secondary generator. You can recover the machines in a VPG to any checkpoint in the journal, to one added automatically or to one added manually. Thus, recovery is done to a point-in-time when the data integrity of the protected virtual machines is ensured.

Note:
- Adding a checkpoint manually does not guarantee transaction consistency.
- Changes to a VPG that result in re-synchronization of the VPG results in all checkpoints being removed. Adding checkpoints to the journal is resumed after synchronization completes. A forced synchronization of the VPG only removes checkpoints if the journal fills up during the synchronization.

To add a checkpoint to a VPG:

1. In the Zerto User Interface select ACTIONS > ADD CHECKPOINT.
   The Add Checkpoint dialog is displayed.

   ![Add Checkpoint dialog]

   A list of VPGs is displayed with the requested VPG selected. You can select more VPGs to add the same checkpoint to, for example, when something is happening at your site that affects multiple VPGs.

   Note: Crash-consistency is per VPG and not across VPGs, even if a checkpoint was added to multiple VPGs.

2. Enter a name for the checkpoint.
3. Click SAVE.

When testing a failover, as described in “Testing Recovery”, on page 273, or actually performing a failover, as described in “Managing Failover”, on page 295, you can choose the checkpoint as the point to recover to.

Running Scripts Before or After Recovering a VPG

Before and after executing a failover, move, or test failover, you can run executable scripts, such as Windows .bat files or PowerShell scripts. A pre-recovery script is always run at the beginning of the recovery operation. A post-recovery script is run after all the virtual machines are powered on at the recovery site.

The scripts must be saved to the machine where the remote Zerto Virtual Manager (ZVM) is installed.

Both pre-recovery and post-recovery scripts are run by the ZVM service on the ZVM machine. The account running the ZVM service is the account that will run the scripts when they are executed.
Zerto recommends duplicating scripts on the Zerto Virtual Managers for both the protected and recovery sites, so that if reverse protection is required, the scripts are available. The location of the script for reverse protection, on the machine where the Zerto Virtual Manager that manages the protected site is installed, must be to the same path as in the remote Zerto Virtual Manager machine. For example, if the scripts are saved to C:\ZertScripts on the remote Zerto Virtual Manager machine, they must be saved to C:\ZertScripts on the local Zerto Virtual Manager machine.

The scripts can include environment variables that can be included as part of the script itself, or passed to the script as parameters. When the script is passed an environment variable as a parameter, the variable is evaluated before executing the script. The following environment variables are available:

- `%ZertoVPGName%`: The name of the VPG. If the name includes a space, enclose the variable in double quotes ("."). For example, the VPG MyVPG uses the format `%ZertoVPGName%` but the VPG My VPG uses the format "%ZertoVPGName%".
- `%ZertoOperation%`: The operation being run: FailoverBeforeCommit, FailoverRollback, Test, MoveBeforeCommit, MoveRollback. Use the result returned for this variable to limit when the script runs, dependent on the operation. The scripts are run after all the virtual machines are powered on at the recovery site and the variable is set to FailoverBeforeCommit or MoveBeforeCommit. Use FailoverRollback or MoveRollback when rolling back the Failover or Move operation, to undo whatever changes a previous script has done (such as updating the DNS records).

- `%ZertoVCenterIP%` - The IP address of the hypervisor manager, VMware vCenter Server or Microsoft SCVMM, where the VPG is recovered.
- `%ZertoVCenterPort%` - The port used by the Zerto Virtual Manager to communicate with the hypervisor manager, VMware vCenter Server or Microsoft SCVMM.
- `%ZertoHypervisorManagerIP%`: The IP address of the hypervisor manager, VMware vCenter Server or Microsoft SCVMM, where the VPG is recovered.
- `%ZertoHypervisorManagerPort%`: The port used by the Zerto Virtual Manager to communicate with the hypervisor manager, VMware vCenter Server or Microsoft SCVMM.
- `%ZertoForce%`: A Boolean value, Yes/No, that dictates whether to abort the recovery operation if the script fails. For example, whether to rollback a Move operation when the script fails and returns a non-zero value.

For example, if a specific VPG should not be migrated, the pre-recovery script can determine whether to continue based on the values of the `%ZertoOperation%` and `%ZertoVPGName%`.

When specifying scripts in the definition of a VPG, enter values for the Pre-recovery Script and Post-recovery Script:
Command to run: The full path of the script to run. The script must be located on the same machine as the Zerto Virtual Manager for the recovery site.

Params: The values of any parameters to pass to the script. Separate parameters with a space.

Timeout (sec): The time-out in seconds for the script to run. If the script runs before executing a failover, move, or test failover and the script fails or a timeout value is reached, an alert is generated and the failover, move, or test failover is not performed. If the script runs after executing a failover, move, or test failover and the timeout value is reached, an alert is generated. The default timeout value is specified in the Site Configuration Advanced Settings dialog.

See also:
- “Creating a Script”, on page 227
- “Example Scripts”, on page 228

Creating a Script
There are many ways to create scripts to run before or after recovering a VPG. The following procedure uses a Windows PowerShell file (.ps1) or a batch (.bat) file.

To create a script:
1. Create a file on the machine where the Zerto Virtual Manager that manages the recovery is installed.
2. Enter the script that you want to run in the file.
3. Save the file as a Windows PowerShell file (.ps1) or batch (.bat) file.

When writing a PowerShell script, you can include the environment variables in the script. For example, the following code snippet shows the use of the %ZertoOperation% and %ZertoVPGName% environment variables:

```powershell
$Operation = $env:ZertoOperation
$VPG = $env:ZertoVPGName
$time = Get-Date
if ($Operation -eq "Test") {
    "$time VPG: $VPG was tested." >> "C:\ZertoScripts\VPG_DR.txt"
}
if ($Operation -eq "FailoverBeforeCommit") {
    "$time Failover before commit was performed. VPG: $VPG" >> "C:\ZertoScripts\VPG_DR.txt"
}
if ($Operation -eq "MoveBeforeCommit") {
    "$time Move before commit was performed. VPG: $VPG" >> "C:\ZertoScripts\VPG_DR.txt"
}
```

Pre-recovery scripts must be saved on the protected site Zerto Virtual Manager machine. Post-recovery scripts must be saved on the recovery site Zerto Virtual Manager machine.

Note: Zerto recommends having both pre- and post-recovery scripts, available on both the protected and recovery Zerto Virtual Manager machines, so that they will work from the protected site and after reverse protection from the recovery site.

4. Update Command to run and Params fields for all the VPG definitions that you want to run the script.

Passing parameters is implemented differently for the two script types. For information about passing command line parameters, refer to the relevant PowerShell or batch file documentation.
Using a BAT File

Windows Batch (.bat) is an executable file that does not require anything in order to run. Update Command to run and Params fields for all the VPG definitions that you want to run the script.

**Command to run** - `<script_including_path>`

C:\ZertoScripts\PostScript.bat

Use quotes (“”) around the path if it includes spaces. The bat file is an executable file and is therefore included in the Command to run field.

**Params** - `<Zerto_Params>`, for example:

```%ZertoOperation% %ZertoVPGName%```

Using a PowerShell Script

Windows PowerShell scripts require Windows PowerShell (.exe) to execute. To specify a PowerShell script, update Command to run and Params fields for all the VPG definitions that you want to run the script.

**Command to run** - `powershell.exe`

**Params** - `<script_including_path> <Zerto_Params>`, for example:

```C:\ZertoScripts\PostScript.ps1 %ZertoOperation% %ZertoVPGName%```

Use quotes (“”) around the path if it includes spaces.

**Note:** You might have to set the remote signed execution policy. For example, using the following:

```###PowerCLI requires remote signed execution policy - if this is not enabled,
###it may be enabled here by uncommenting the line below.
###Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force```

**Note:** Zerto recommends testing both PowerShell and batch scripts by running them from the command line, to ensure that they run correctly.

Example Scripts

**IMPORTANT:** The scripts are provided by example only and are not supported under any Zerto support program or service.

The following scripts are examples of how to provide scripts to use with Zerto Virtual Replication:

- “Example 1 – Recording Failover Tests”, below.
- “Example 2 – Moving Virtual Machines to a Resource Pool After a Failover”, on page 228.

Example 1 – Recording Failover Tests

The following script, c:\ZertoScripts\TestedVPGs.bat, writes the VPG name and date to the ListOfTestedVPGs.txt file every time a failover test is run:

```SET isodt=%date:~10,4%-%date:~7,2%-%date:~4,2% %time:~0,2%-%time:~3,2%-%time:~6,2%
IF %1==Test ECHO %2 %isodt% >> c:\ZertoScripts\Results\TestedVPGs.txt```

Where %1 is the first parameter in the list of parameters, %ZertoOperation%, and %2 is the second parameter in the list of parameters, %ZertoVPGName%.

**Note:** If the file TestedVPGs.txt does not exist it is created, as long as the folder, c:\ZertoScripts\Results, exists.

Example 2 – Moving Virtual Machines to a Resource Pool After a Failover

The following PowerShell script is an example of how to move virtual machines into resource pools as a post-recovery script. This script could be used when you want to move virtual machines into a resource pool following a failover and want to
designate the resource pool only at the time of the failover and not as part of the VPG definition. Note that this script is a basic example and requires some configuration, as noted in the comments of the script:

```powershell
##The following are a list of requirements for this script:
## - This script must be present in the same directory on both sites listed in
##   the Manage VPGs dialog
## - PowerShell v2.0 installed on both Zerto Virtual Managers
## - VMWare PowerCLI installed on both Zerto Virtual Managers
##
##This script was written by Zerto Support and is used at the customer's own risk
## and discretion.
##
##Note: The desired resource pool MUST exist on the hypervisor manager prior to
##running this script.
##
##To run this script from the VPG screen, an example command is 'powershell.exe'
##with the parameter 'C:\ZertoScripts\Move-VMs.ps1'
##
##START OF SCRIPT
##
##PowerCLI requires remote signed execution policy - if this is not enabled,
##it may be enabled here by uncommenting the line below.

##Set-ExecutionPolicy -ExecutionPolicy RemoteSigned -Force

##Below are the variables that must be configured.
```
## Variables:

### The location of this script
```
$strMoveScriptLoc = "C:\Zerto Scripts\"
```

### vCenter IP address
```
$strVCSPassIP = "10.10.10.10"
```

### vCenter user account to use; account must have ability to move desired machines
```
$strVCUser = "Administrator"
```

### vCenter user password
```
$strVCUserPass = "password"
```

### Name of resource pool in vCenter
```
$strResPool = "ResourcePool"
```

### Array of VMs to move; it includes ALL VMs in the VPG and is case sensitive.
```
$strVMtoMove = @("VM-1", "VM-2", "VM-3")
```

### The PowerCLI snap-in must first be registered
```
Add-PSSnapin VMware.VimAutomation.Core
```

### Move to directory where script is located
```
CD $strMoveScriptLoc
```

### Connect to target VC server based on variables above
```
Connect-VIServer -Server $strVCSPassIP -Protocol https -User $strVCUser -Password $strVCUserPass
```

### Execute the move for each VM specified
```
foreach ($objVM in $strVMtoMove){
    Move-VM -VM $objVM -Destination $strResPool }
```

### Disconnect from session with VC server
```
Disconnect-VIServer -Server $strVCSPassIP -Force
```

### End of script

---

**Exporting and Importing VPG Definitions**

You can save VPG definitions to an external file and import these definitions back to Zerto Virtual Replication, for example, exporting the settings before uninstalling a version of Zerto Virtual Replication and importing the settings after reinstalling Zerto Virtual Replication.

**Note:** Zerto Virtual Replication regularly exports settings to the `Zerto_Installation_Folder\Zerto Virtual Replication\ExportedSettings` folder. You can use one of these exported files instead of creating a new export file. The default location of `Zerto_Installation_Folder` is `C:\Program Files\Zerto`. 
To export VPG settings:
1. Open the Zerto Diagnostics application. For example, via Start > Programs > Zerto Virtual Replication > Zerto Diagnostics. The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the Export Protection Group Settings option and click Next.

3. Select the destination for the file to contain exported settings and specify the Zerto Virtual Manager IP address and port where the VPGs are protecting virtual machines.

4. Click Next. The list of exported VPGs is displayed.

5. Click Done.

Note: If you are uninstalling Zerto Virtual Replication, the VPGs are deleted. To prevent having to perform a full synchronization when the VPG definitions are imported, Zerto recommends deleting the VPGs in the Zerto User Interface, keeping their target disks.

To import VPG settings:
1. Click Start > Programs > Zerto Virtual Replication > Zerto Diagnostics. The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the Import Protection Group Settings option.

3. Click Next.
4. Select the file previously exported and enter the Zerto Virtual Manager IP address and port specified when exporting the VPGs.
5. Click Next. The list of exported VPGs is displayed.

6. Select the VPGs to import. Only VPGs with names that are not already defined can be imported. VPGs in the import files with the same name as an existing VPG are disabled.
7. Click Next. The list of imported VPGs is displayed. If the VPG could not be imported, the reason for the failure is specified.

   **Note:** If a host was removed from and then re-added to the environment it is advisable to wait approximately 5 minutes from when the host was re-added before performing the import of the VPGs.
8. Click Done.

### VPG Statuses and Synchronization Triggers

During normal operations the VPG status can change. For example, a change can be made to the VPG definition, or an operation such as move or failover is performed on the VPG, or an external event impacts the system such as the WAN going down. When the status changes, resulting in the VPG being synchronized, for example with a Delta Sync, the estimated time to complete the synchronization is displayed under the VPG status, and if relevant, the synchronization trigger, such as Network Congestion.

See also:
- “VPG Statuses”, on page 232
- “VPG Synchronization Triggers”, on page 238

### VPG Statuses

The following statuses are displayed:

<table>
<thead>
<tr>
<th>STATUS</th>
<th>SUBSTATUS</th>
<th>COMMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting</td>
<td>Deleting the VPG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VPG waiting to be removed</td>
<td></td>
</tr>
<tr>
<td>Failing Over</td>
<td>Committing Failover</td>
<td>The VPG is being failed over.</td>
</tr>
<tr>
<td></td>
<td>Failing over – Before commit</td>
<td>A VPG being failed over is in the initial stage, before committing the failover.</td>
</tr>
<tr>
<td></td>
<td>Promoting</td>
<td>The failover has completed and the data from the journal is being promoted to the failed over virtual machine disk.</td>
</tr>
<tr>
<td></td>
<td>Rolling back Failover</td>
<td>The failover is being rolled back to prior to the failover.</td>
</tr>
<tr>
<td>STATUS</td>
<td>SUBSTATUS</td>
<td>COMMENT</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>History Not Meeting SLA</td>
<td>See <em>Not Meeting SLA</em>, below.</td>
<td>The VPG is meeting the RPO SLA setting but not the journal history.</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Initial Sync</td>
<td>After adding a virtual machine to an existing VPG not meeting the journal history SLA.</td>
</tr>
<tr>
<td>Initializing</td>
<td>Creating VPG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Full Syncing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Initial Sync</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Syncing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Initial Sync</td>
<td></td>
</tr>
<tr>
<td>Meeting SLA or Based on Alerts</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bitmap Syncing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delta Syncing (When Force Sync is applied)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovery is Possible</td>
<td>After a rollback.</td>
</tr>
<tr>
<td></td>
<td>Rolling Back</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User Paused Protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Initial Sync</td>
<td>After adding a virtual machine to an existing VPG meeting SLA.</td>
</tr>
<tr>
<td></td>
<td>Zerto Virtual Manager paused protection</td>
<td></td>
</tr>
<tr>
<td>Moving</td>
<td>Committing Move</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moving – Before commit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Promoting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Rolling back Move</td>
<td></td>
</tr>
<tr>
<td>Not Meeting SLA</td>
<td>Site Delta Sync (when Force Sync is not applied)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Delta Syncing a volume</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Journal/recovery disks are missing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Journal storage error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Needs configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovery storage error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Recovery storage profile error</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Site disconnection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Site disconnection. No checkpoints</td>
<td></td>
</tr>
<tr>
<td></td>
<td>VM not protected</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Full Syncing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Initial Sync</td>
<td>After adding a virtual machine to an existing VPG not meeting the SLA.</td>
</tr>
<tr>
<td></td>
<td>VPG has no VMs</td>
<td></td>
</tr>
<tr>
<td>Recovered</td>
<td>—</td>
<td>The VPG has been recovered.</td>
</tr>
<tr>
<td>STATUS</td>
<td>SUBSTATUS</td>
<td>COMMENT</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>RPO Not Meeting SLA</td>
<td>See Not Meeting SLA, above.</td>
<td>The VPG is meeting the journal history SLA setting but not the RPO.</td>
</tr>
<tr>
<td></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Volume Initial Sync</td>
<td>After adding a virtual machine to an existing VPG not meeting the RPO SLA.</td>
</tr>
</tbody>
</table>
Managing VPGs

The following provides a full description of the sub-statuses:

<table>
<thead>
<tr>
<th>SUBSTATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bitmap Syncing</td>
<td>A change tracking mechanism of the protected machines during a disconnected state or when a VRA buffer is full. In these situations, Zerto Virtual Replication starts to maintain a smart bitmap in memory, in which it tracks and records the storage areas that changed. Since the bitmap is kept in memory, Zerto Virtual Replication does not require any LUN or volume per VPG at the protected side.</td>
</tr>
<tr>
<td>Note:</td>
<td>The VRA buffer is set via the <strong>Amount of VRA RAM</strong> value, specified when the VRA is installed.</td>
</tr>
<tr>
<td></td>
<td>The bitmap is small and scales dynamically, containing references to the areas of the protected disk that have changed but not the actual I/O. The bitmap is stored locally on the VRA within the available resources. For example, when a VRA goes down and is then rebooted.</td>
</tr>
<tr>
<td></td>
<td>When required, Zerto Virtual Replication starts to maintain a smart bitmap in memory, to track and record storage areas that change. When the issue that caused the bitmap sync is resolved, the bitmap is used to check updates to the protected disks and send any updates to the recovery site. A bitmap sync occurs when any of the following conditions occur:</td>
</tr>
<tr>
<td></td>
<td>- Synchronization after WAN failure or when the load over the WAN is too great for the WAN to handle, in which case the VPGs with the lower priorities will be the first to enter a bitmap sync.</td>
</tr>
<tr>
<td></td>
<td>- When there is storage congestion at the recovery site, for example when the VRA at the recovery site cannot handle all the writes received from the protected site in a timely fashion.</td>
</tr>
<tr>
<td></td>
<td>- When the VRA at the recovery site goes down and is then rebooted, for example during a Zerto Virtual Replication upgrade.</td>
</tr>
<tr>
<td></td>
<td>During the synchronization, new checkpoints are not added to the journal but recovery operations are still possible, assuming there are valid checkpoints in the journal. If a disaster occurs requiring a failover during a bitmap synchronization, the VPG status changes to <strong>Recovery Possible</strong> and you can recover to the last checkpoint written to the journal. For synchronization to work, the protected virtual machines must be powered on so that the VRA has an active IO stack, which is only available when the virtual machine is powered on.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If the synchronization takes longer than the configured history, all the checkpoints in the journal can be lost, preventing a failover from being performed. For the resolution of this situation, see “To configure disaster recovery policies:”, on page 262.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, depending on when the promotion to the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or initial sync, etc</td>
</tr>
<tr>
<td>Committing Failover</td>
<td>Failing over the VPG.</td>
</tr>
<tr>
<td>Committing Move</td>
<td>Completing the move, including removing the protected virtual machines.</td>
</tr>
<tr>
<td>Creating VPG</td>
<td>The VPG is being created based on the saved definition.</td>
</tr>
<tr>
<td>Deleting the VPG</td>
<td>Deleting the VPG.</td>
</tr>
</tbody>
</table>
### Delta Syncing

The Delta Sync uses a checksum comparison to minimize the use of network resources. A Delta Sync is used when the protected virtual machine disks and the recovery disks should already be synchronized, except for a possible few changes to the protected disks, for example:

- When a virtual machine was added to the VPG and the target recovery disk is defined as a preseeded disk.
- After a source VRA upgrade of a major release: Depending on the nature of the upgrade, a VRA upgrade on the protected side may trigger either a Delta Sync or a Bitmap Sync. See the version release notes to determine if a sync will be triggered with a source VRA upgrade.
- For reverse protection after a move or failover.
- A Force Sync operation was manually initiated on the VPG.
- A host protecting virtual machines was restarted and the protected virtual machines on the host had not been vMotioned to other hosts in the cluster or a protected virtual machine was vMotioned to another host without a VRA, and then vMotioned back to the original host.

For synchronization to work, the protected virtual machines must be powered on so that the VRA has an active IO stack, which is only available when the virtual machine is powered on.

During the synchronization, **new checkpoints are not added to the journal** but recovery operations are still possible, assuming there are valid checkpoints in the journal. If a disaster occurs requiring a failover during a delta synchronization, you can recover to the last checkpoint written to the journal.

**Note:** It is not possible to perform a move during a delta sync.

**Note:** Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, depending on when the promotion to the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or initial sync, etc.

### Delta syncing a volume

Synchronization when only delta changes for a volume needs synchronizing, for example, when a volume is added to a protected virtual machine in a VPG, and a preseeded disk is used.

For synchronization to work, the protected virtual machines must be powered on so that the VRA has an active IO stack, which is only available when the virtual machine is powered on.

During the synchronization, new checkpoints are not added to the journal but recovery operations are still possible, assuming there are valid checkpoints in the journal. If a disaster occurs requiring a failover during a delta volume synchronization, you can recover to the last checkpoint written to the journal.

**Note:** It is not possible to perform a move during a delta sync.

**Note:** Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, depending on when the promotion to the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or initial sync, etc.

### Error

Problem situation, for example, when a ZVM is disconnected from a VRA used to protect virtual machines. The VPG cannot be recovered until the problem is resolved.

### Failing over - Before commit

Preparing and checking the VPG virtual machines in the recovery site.
### MANAGING VPGs

#### Full Syncing

Full synchronization to ensure that the protected disks and recovery disks are the same after some change to the system. This type of sync is the same as an Initial Sync but occurs after protection started. In general, this type of sync should not happen.

For synchronization to work, the protected virtual machines must be powered on so that the VRA has an active IO stack, which is only available when the virtual machine is powered on.

**Note:** During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible.

**Note:** Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, depending on when the promotion to the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or initial sync, etc.

#### Initial Sync

Synchronization performed after creating the VPG to ensure that the protected disks and recovery disks are the same. Recovery operations cannot occur until after the initial synchronization has completed.

For synchronization to work, the protected virtual machines must be powered on so that the VRA has an active IO stack, which is only available when the virtual machine is powered on.

Adding a virtual machine to a VPG is similar to creating a new VPG, a volume initial sync is performed for the new virtual machine. For more information, see [Volume Initial Sync](#).

**Note:** Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, depending on when the promotion to the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or initial sync, etc.

#### Journal/recovery disks are missing

Zerto Virtual Manager cannot locate disks that were connected to a virtual machine. As a result, recovery operations cannot be performed on the VPG containing the virtual machine.

#### Journal storage error

There was an I/O error to the journal. For example, if the journal was full and the size was increased. Once the problem is resolved a synchronization is required.

#### Moving - Before commit

Preparing and checking the VPG virtual machines in the recovery site.

#### Needs Configuration

One or more configuration settings are missing, for example, when reverse protection is not specified.

#### Promoting Configuration

Updating recovered virtual machines in the VPG with data from the journal.

#### Recovery is possible

Communication with the Zerto Virtual Manager at the protected site is down so continuing protection is halted, but recovery on the remote site is available (compare with Site disconnection).

#### Recovery storage error

There was an I/O error to the recovery storage. For example, the datastore is almost full or the virtual machines are turned off and the recovery disks are inaccessible.

#### Recovery storage policy error

The storage policy in the recovery site specified to be used by the VPG cannot be found.

#### Rolling back

Rolling back to an initial status, for example, after canceling a cloning operation on the VPG.

#### Rolling back Failover

Rolling back a Failover operation before committing it.

#### Rolling back Move

Rolling back a Move operation before committing it.

#### Site disconnection

Communication with the Zerto Virtual Manager at the remote, recovery, site is down so continuing protection is halted (compare with Recovery is possible).

#### Site disconnection. No checkpoints

Communication with the Zerto Virtual Manager at the remote, recovery, site is down and there are no checkpoints to use to recover the VPG at the recovery site.

#### Syncing

Status while type of synchronization is being evaluated.
Managing VPGs

VPG Synchronization Triggers

The following synchronization triggers can be applied:

<table>
<thead>
<tr>
<th>TRIGGER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Sync</td>
<td>The user requested to synchronize the VPG, as described in “Forcing the Synchronization of a VPG”, on page 222.</td>
</tr>
<tr>
<td>Network Congestion</td>
<td>The network bandwidth is not wide enough to handle all the data, causing some of the data to be backed up.</td>
</tr>
<tr>
<td>Protected Storage Error</td>
<td>An I/O error occurred to a protected virtual machine, after the data was sent to the recovery side.</td>
</tr>
</tbody>
</table>
Managing Protection When the Recovery Datastore Will Be Unavailable (Datastore Maintenance)

When access to a recovery datastore is not available, for example, during maintenance of the datastore, you have to change the datastore in all affected VPGs to enable protection to continue.

**Note:** Changing the datastore directly in the *Edit VM* dialog or if the datastore used for the journal is not set to *Default* in the *Advanced Journal Settings* dialog, causes the VPG to undergo an initial synchronization.

During the following procedures the journal used for recovery is reset and until the VPG returns to a protecting state, recovery is not possible.

**To enable protection to continue when a virtual machine recovery storage will be unavailable:**

1. Remove all virtual machines from the VPG definitions that use the unavailable storage as the recovery storage. When saving the VPG a warning is displayed.
2. Click *No*.
   
   **Note:** A VPG must always have at least one virtual machine defined and therefore you cannot remove all the virtual machines from a VPG at once. If all the VPGs use a datastore that requires maintenance, remove all but one of the virtual machines and after completing this procedure, add the virtual machines back to the VPG and repeat the procedure with the last virtual machine.
3. Change the default recovery datastore in the VPG definition to a new default datastore, if it was set to the unavailable storage.
4. Move the saved volumes to the default datastore.
5. Add the virtual machine back to the VPG, and configure the virtual machine volumes to use the saved volumes as preseeded volumes.
6. Save the VPG definition with the new settings.

The VPG will undergo a Delta Sync before returning to a Meeting SLA status.

**To enable protection to continue when journal storage will be unavailable:**

1. Delete the VPG but check *Keep target disks at the peer site*. Checking this option means that the target replica disks for the virtual machines are kept so that you can preseed to these disks so the synchronization is faster.
2. Recreate the VPG, specifying the journal storage you want to use in the and the default recovery storage.
3. Add the virtual machine to the VPG, and configure the virtual machine volumes to use the saved volumes as preseeded volumes.
4. Save the VPG definition with the new settings.

---

<table>
<thead>
<tr>
<th>TRIGGER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protected VRA Congestion</td>
<td>The host where the VRA is installed is highly loaded: many updates are made to the protected machines at the same time, causing a time lapse before the updates are passed to the recovery site.</td>
</tr>
<tr>
<td>Recovery or Journal Storage Error</td>
<td>There was an I/O error either to the recovery storage or journal, for example if the journal was full and the size was increased. Once the problem is resolved a synchronization is required.</td>
</tr>
<tr>
<td>Recovery Storage Congestion</td>
<td>The recovery datastore is being written to a lot, causing a delay for some of the data passed from the protected site to be written to disk.</td>
</tr>
<tr>
<td>Recovery VRA Communication Problem</td>
<td>A network error, such as the network being down for a period, requires a synchronization of the VPG between the two sites, for example a Bitmap Sync.</td>
</tr>
<tr>
<td>VPG Configuration Changed</td>
<td>The configuration of the VPG changed resulting in a synchronization being required. For example, the size of the journal was changed.</td>
</tr>
</tbody>
</table>
The VPG will undergo a Delta Sync before returning to a Meeting SLA status.
CHAPTER 10: MANAGING VRAS

A VRA is a Zerto Virtual Replication virtual machine that manages the replication of virtual machines across sites. A VRA must be installed on every hypervisor that hosts virtual machines that require protecting in the protected site and on every hypervisor that will host the replicated virtual machines in the recovery site. The VRA compresses the data that is passed across the WAN from the protected site to the recovery site. The VRA automatically adjusts the compression level according to CPU usage, including totally disabling it if needed.

The VRA is a custom, very thin, Linux-based virtual machine with a small footprint, disk - memory and CPU - and increased security since there are a minimum number of services installed.

Zerto recommends installing a VRA on every host so that if protected virtual machines are moved from one host in the cluster to another host in the cluster there is always a VRA to protect the moved virtual machines.

A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.

Note: VRAs and shadow VRAs are configured and managed by the Zerto Virtual Manager. You cannot take snapshots of VRAs as snapshots cause operational problems for the VRAs.

The priority assigned to a VPG dictates the bandwidth used. The Zerto Virtual Manager distributes bandwidth among the VRAs based on the VPG priority, and the VPGs with higher priorities are handled before writes from VPGs with lower priorities.

There are a number of tasks that you might need to perform on VRAs, including installing a new VRA on a host added to the hypervisor management tool or uninstalling VRAs and moving the data maintained by a VRA to another VRA when a host requires maintenance.

During normal operation, a VRA might require more disks than a single virtual machine can support. If this situation arises, the VRA creates new shadow VRA virtual machines, used by the VRA to maintain additional disks (a diskbox). A shadow VRA does not have an operating system and therefore does not have an IP address, or use VMware tools. A shadow VRA is created proactively at the recovery site and prior to the recovery VRA reaching the SCSI target limit imposed by VMware: 15 SCSI targets per SCSI controller and 4 SCSI controllers per virtual machine. This amounts to a limitation of 60 SCSI targets per virtual machine. Similar to a VRA, a shadow VRA must be left to Zerto Virtual Replication to manage, and must not be modified or removed for any reason.

The following VRA management options are described in this chapter:

- “Installing a VRA”, below
- “Upgrading VRAs”, on page 245
- “Editing VRA Settings”, on page 246
- “Editing the VRA Connection Method or Password”, on page 247
- “Changing a Recovery VRA”, on page 248
- “Uninstalling VRAs”, on page 249
- “Handling a VRA in an Error State (Ghost VRA)”, on page 249
- “Managing Protection During VMware Host Maintenance”, on page 250
- “Managing Protection When Moving a Host to a Different Cluster”, on page 251
- “Support for VMware Virtual Update Manager (VUM)”, on page 251

Monitoring VRAs is described in “Monitoring Virtual Replication Appliances”, on page 199.
Installing a VRA

Zerto recommends installing a VRA on every host in every site so that if protected virtual machines are moved from one host in the cluster to another host in the cluster there is always a VRA to protect the moved virtual machines.

VRA Installation Requirements

To install a VRA you require the following:

- 12.5GB datastore space.
- At least 1GB of reserved memory.
- The ESX/ESXi host version must be 4.0U1 or higher and Ports 22 and 443 must be enabled on the host during the installation.

You must also know the following information to install a VRA:

- The datastore the VRA will use and the local network used by the host.
- The network settings to access the peer site; either the default gateway or the IP address, subnet mask and gateway.
- If a static IP is used, which is the Zerto recommendation1, instead of DHCP, the IP address, subnet mask and default gateway to be used by the VRA.

Note: For the duration of the installation of the VRA, the Zerto Virtual Manager enables SSH in the vCenter Server.

If the peer site VRAs are not on the default gateway, you must set up routing to enable the VRAs on this site to communicate with the peer site VRAs before defining the VRAs. Setting up routing after defining VRAs only applies to VRAs installed after the routing is set. Any existing VRA is not affected and access to these VRAs continues via the default gateway. If the default gateway stops being used, you must reinstall the VRAs that were installed before setting up paired site routing.

To set up routing:

1. In the SETUP > VRAs tab, select MORE > Paired Site Routing.
   The Configure Paired Site Routing dialog is displayed.

2. Click Enable Paired Site Routing.

3. Specify the following, and then click SAVE:
   - **Address**: The IP address of the next hop at the local site, the router or gateway address, that is used to access the peer site network.
   - **Subnet Mask**: The subnet mask for the peer site network.
   - **Gateway**: The gateway for the peer site network.

   These access details are used to access all VRAs installed on the peer site after the information is saved.

To install Zerto Virtual Replication Appliances (VRAs) on ESX/ESXi hosts:

1. In the Zerto User Interface, click SETUP > VRAs.
2. Select a host which requires a VRA and click NEW VRA.

---

1. In a non-production environment it is often convenient to use DHCP to allocate an IP to the VRA. In a production environment this is not recommended. For example, if the DHCP server changes the IP allocation on a reboot, the VRA does not handle the change.
The Configure and Install VRA dialog is displayed. The dialog displayed depends on the ESX/i version:

**ESXi versions from 5.5**

**ESXi versions before version 5.5**

**Note:** If you selected a cluster or multiple hosts, the VRA is installed on the first host in the displayed list.

Specify the following **Host Details**:

**Host** – The host on which the VRA is installed. The drop-down displays the hosts that do not have a VRA installed, with the selected host displayed by default.

From ESXi 5.5, by default, Zerto Virtual Manager uses a vSphere Installation Bundle, VIB, to connect to the host. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and logs it.

For ESX/i versions earlier than 5.5, when using a password, root access is required. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is issued, requesting the user enter the new password.

**Use credentials to connect to host** – When unchecked, the Zerto Virtual Manager uses VIB to connect to the host. This field is only relevant for ESXi 5.5 and later.

**Host Root Password** – When the VRA should connect to the host with a password, check Use credential to connect to host and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts.

**Datastore** – The datastore that the VRA will use for protected virtual machine data on the recovery site, including the journals. You can install more than one VRA on the same datastore.

- **Network** – The network used to access the VRA.
- **VRA RAM** – The amount of memory to allocate to the VRA. The amount determines the maximum buffer size for the VRA for buffering IOs written by the protected virtual machines, before the writes are sent over the network to the recovery VRA. The recovery VRA also buffers the incoming IOs until they are written to the journal. If a buffer becomes full, a Bitmap Sync is performed after space is freed up in the buffer.

<table>
<thead>
<tr>
<th>AMOUNT OF VRA RAM</th>
<th>VRA BUFFER POOL SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GB</td>
<td>450MB</td>
</tr>
<tr>
<td>2GB</td>
<td>1450MB</td>
</tr>
<tr>
<td>3GB</td>
<td>2300MB</td>
</tr>
</tbody>
</table>
244

Installing a VRA

**Managing VRAs**

The protecting VRA can use 90% of the buffer for IOs to send over the network and the recovery VRA can use 75% of the buffer.

For Example: A protecting VRA defined with 2GB of RAM can buffer approximately 1305MB before the buffer is full and a Bitmap Sync is required.

**Note:** The number of virtual machines that a VRA can support is not dependent on the amount of VRA RAM.

- **VRA Group** – Choose the VRA Group from the dropdown list. To create a new VRA group, type in the name of the new group and click **CREATE**. You can then choose the new group from the dropdown list.

You group VRAs together when VRAs use different networks so they can be grouped by network, for example when the protected and recovery sites are managed by the same vCenter Server and you want to replicate from the branch site to the main site. Within a group the priority assigned to a VPG dictates the bandwidth used and is applicable within a group and not between groups. Thus, a VPG with a high priority is allocated bandwidth before VPGs with lower priorities. VPGs that are on VRAs with different VRA groups, for example, VPG1 on VRA1 in group1 and VPG2 on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.

3. Specify the following VRA Network Details:

- **Configuration:** Either have the IP address allocated via a static IP address or a DHCP server. If you select the **Static** option, which is the recommended option, enter the following:
  - **Address:** The IP address for the VRA.
  - **Subnet Mask:** The subnet mask for the network. The default value is **255.255.255.0**.
  - **Default Gateway:** The default gateway for the network.

4. Click **INSTALL**.

The VRA installation starts and the status is displayed in the TASKS popup dialog in the status bar and under **MONITORING > TASKS**.

The VRA displayed name, and DNS name, is Z-VRA-hostname. If a virtual machine with this name exists, for example when a previous VRA was not deleted, the VRA name has a number appended to it.
Managing VRAs

Upgrading VRAs

This section is applicable if *Auto-Upgrade Virtual Replication Appliances* was not selected when upgrading Zerto Virtual Replication, or if a manual VRA upgrade is required.

- If a newer version of the installed VRAs exists, you can continue to use the current VRAs with the new version of Zerto Virtual Replication, or you can upgrade these VRAs from within the Zerto User Interface.
- VRAs installed with the previous version of Zerto Virtual Replication can work with VRAs installed with the current version of Zerto Virtual Replication in any combination (all from one version or a mix of VRA versions) as long as the VRAs are only one version lower than the version of Zerto Virtual Replication installed on the site.
- Zerto recommends that you always upgrade the VRAs on your site to the latest version.
- Not all new installations of Zerto Virtual Replication require upgrading VRAs. If your VRA is outdated relative to your current version of Zerto Virtual Replication and an upgrade is available, the VRA version will be reported in the column as outdated. In addition, an alert is issued on the site using the old VRA and on any site that is paired with it.

**Note:** You can move the mouse over the Outdated value to display the VRA version as a tooltip.

Considerations when upgrading VRAs:

- VRAs managing protected virtual machines: Either vMotion the protected virtual machines and datastores managed by the VRA to another host with a VRA, or upgrade the VRA without vMotioning the virtual machines and a Bitmap Sync will be performed following the upgrade.
- Upgrading a VRA that manages the recovery of virtual machines results in a bitmap sync being performed after the upgrade. Note that the time to upgrade a VRA is short so the bitmap sync should also be quick.

**To upgrade VRAs:**

1. For a VRA protecting virtual machines, if vMotioning the protected virtual machines:
   a) Remove affinity rules for protected virtual machines on the host with the VRA to be upgraded.
   b) vMotion these protected machines from the host to another host with a VRA.
2. In the Zerto User Interface, click SETUP > VRAs, select the VRAs to upgrade, and then click MORE > Upgrade. The Upgrade VRAs dialog is displayed, listing the selected VRAs and whether an upgrade is available.

3. Review the list for the VRAs that you want to upgrade. Deselect any VRAs that you decide not to upgrade.
4. Click Upgrade Selected VRAs.
5. The upgrade progress is displayed in the VRAs tab.
   - After the upgrade, a bitmap sync is performed at both the protected and recovered sites.

**Note:** The VRA name does not change, even if the naming convention in the latest version is different.
Note: You do not need to upgrade VMware Tools on a VRA.

Editing VRA Settings

If you need to change the connection method (VIB or password), host password, VRA group, or network settings for a VRA, for example when the gateway to the VRA is changed, you can do this by editing the VRA.

To edit the VRA:
1. In the Zerto User Interface, click SETUP > VRAs.
2. Select the VRA to edit, and click MORE > Edit.
   The Edit VRA dialog is displayed.

3. Edit the group if required.
   **VRA Group** – You can change the free text to change the group that a VRA belongs. If you create a group and then change the name when editing the VRA so that there is no VRA in the site that belongs to the originally specified group, the group is automatically deleted from the system.
   To create a new group, enter the new group name over the text New group and click CREATE.

4. Edit the VRA network settings as follows:
   **Configuration** – Either have the IP address allocated via a static IP address or a DHCP server. If the VRA was originally installed with a static IP, you cannot change this to DHCP. If the VRA was originally installed to use a DHCP server, you can change this to use a static IP. Zerto always recommends using a static IP.
   **Address** – The static IP address for the VRA to communicate with the Zerto Virtual Manager.
   **Subnet Mask** – The subnet mask for the network. The default value is 255.255.255.0.
   **Default Gateway** – The default mask for the network.

5. Click SAVE.
Editing the VRA Connection Method or Password

VRAs installed on ESXi 5.5 and later hosts can use either VIB or a password to access the host. VRAs installed on ESXi 5.1 and earlier hosts can only use a password to access the host. When installing a VRA on a ESXi 5.5 or later host, you define whether the VRA should use VIB or a password to connect to the host. After installation, you can change the method that VRAs use to access the host, and, if a password is the method used, you can change this password.

When using vSphere Installation Bundle, VIB, Zerto Virtual Manager checks that the VRA can connect to the host. If connecting fails, Zerto Virtual Manager re-initiates the connection automatically and notes this in the log.

When using a password, Zerto Virtual Manager checks that the password is valid once a day. If the password was changed, an alert is triggered, requesting the user enter the new password. You can change the password stored by the VRA by editing the VRA, either for a specific VRA, or when multiple hosts have their passwords changed, each with the same password, you can update the password information for the affected VRAs globally.

To edit the VRA connection method:

1. In the Zerto User Interface, click SETUP > VRAs.
2. Select the VRAs that need to be updated and click MORE > Change Host Password.
   
   The Change Host Password VRA dialog is displayed.

3. To change the connection method or host password, do one of the following:
   - If the VRA is using a password to connect to the host and should use vSphere Installation Bundle, VIB, deselect Use credentials to connect to host.
   - If the VRA is using VIB to connect to the host and should use a password, select Use credentials to connect to host and enter the password. To display the password in plain text, click in the box next to the field.
   - If the VRA is connecting to the host with a password and the password for the host has changed, enter the new password. To display the password in plain text, click in the box next to the field.

4. Click SAVE.

   1.
Changing a Recovery VRA

When a VPG is defined, the recovery host to use for each virtual machine in the VPG is specified. If required, you can change the recovery host for a protected virtual machine.

**Note:** The datastores used by the original VRA and the changed VRA must be accessible by both the original target host and by the changed target host.

**To change a recovery VRA:**

1. In the Zerto User Interface, click **SETUP > VRAs**.
2. Select the VRA to change and click **MORE > Change VM Recovery VRA**.

   The Change VM Recovery VRA dialog is displayed, listing all the virtual machines being recovered on that host.

3. Review the list and select the virtual machines to change the target host to another specified target host.
4. From the Select the replacement host drop-down list, select the target host for these virtual machines.
   - Validation is performed to make sure the selected target host can be used. For example, the datastores used by both the VRAs are accessible from both hosts.
   - Any implications of the change, such as whether synchronization might be required after the change is also displayed.
5. Click **SAVE**.
   - The VPG recovery host definitions are changed and the affected target data, including the journals, storage vMotioned to the VRA under the replacement host.
   - During this procedure you **cannot edit the affected VPGs** nor attempt a failover, move, failover test, or clone operation.
   - At the end of the procedure a **Delta Sync might be required** to resynchronize the protected machines with the recovery VRAs.
     - In order not to affect the recoverability of other VPGs replicating to the VRA, a **new virtual machine is created** to handle moving the disks.
     - This virtual machine is named **Z-VRAH-ESXihostname-xx**, where hostname is the name of the ESXi host where the original VRA is installed and xx is a unique index used for the virtual machine, with a format of yy-xxxx or xxxx.
6. Repeat this procedure for all the virtual machines.

**Note:** When a volume is moved using Storage vMotion, the datastore folder under which the volume is saved is the last datastore folder accessed by VMware.
Uninstalling VRAs

VRAs are uninstalled via the Zerto User Interface and not via the vCenter Server user interface. You cannot uninstall a VRA which is used to protect or recover virtual machines.

For a VRA protecting virtual machines - Before uninstalling the VRA, remove affinity rules for protected virtual machines on the host and vMotion these protected virtual machines to another host in the cluster with a VRA installed.

For a VRA recovering virtual machines - Before uninstalling the VRA, change the host for all virtual machines in VPGs recovering to this VRA to another host as described in “Changing a Recovery VRA”, on page 248. A bitmap sync occurs to synchronize the VPGs with the new host.

Note: If the VRA has crashed, or was accidentally deleted, it must be forcibly uninstalled, as described in “Handling a VRA in an Error State (Ghost VRA)”, on page 249.

For a VRA in a cluster, you can remove it and then install a new VRA. However, to ensure that virtual machines in the cluster are not moved to the host without a VRA from the time the VRA is removed to the time a new VRA is installed, it is recommended to perform the following procedure.

To uninstall a VRA with virtual machines being recovered to it:
1. When the VRA to be removed is in a cluster, set VMware DRS to manual for the duration of the procedure, so that virtual machines in the cluster are not moved to the host without a VRA from the time the VRA is removed to the time a new VRA is installed.
2. Remove affinity rules for protected virtual machines on the host and vMotion any protected virtual machines to another host with a VRA installed.
3. Change the host for all virtual machines in VPGs recovering to this VRA to another host as described in “Changing a Recovery VRA”, on page 248.
4. Wait for any synchronization to complete.
5. Either select the VRAs to uninstall in the VRAs tab or for a single VRA display the VRA details by clicking the VRA Name link in the VRAs tab, and click MORE > UNINSTALL.
6. Once the VRAs are completely removed, install a new VRA on the host.

Note: If a VRA cannot be removed, when the VRA was installed on an ESXi version 4.x or 5.x host and the password to the host was changed, contact Zerto support.

After the VRA is uninstalled, connectivity from that VRA to any Zerto Cloud Connector is lost. After a VRA is reinstalled on the host, the ports that were used for the connection to the Zerto Cloud Connector are not reused and new ports must be opened in the firewall for the cloud site. For details about Zerto Cloud Connectors, refer to Zerto Cloud Manager Administration Guide.

Handling a VRA in an Error State (Ghost VRA)

When an event occurs that causes a VRA to enter an error state, for example the host machine crashes or the VRA or a shadow VRA is accidentally deleted, if the VRA has shared storage disks that are accessible by other hosts in the site, you can copy these disks to another VRA in the site.

To recover VRA disks from an VRA:
1. Remove the VPGs, keeping the recovery disks when removing to use as preseeded disks.
2. Uninstall the VRA.
3. Reinstall the VRA, as described in “Installing a VRA”, on page 242.
4. Recreate the VPGs using the preseeded disks.
Managing Protection During VMware Host Maintenance

When a host machine requires VMware maintenance, at least for the duration of the maintenance, to ensure continuous protection:

**For a host machine on the protected site** - Remove affinity rules for protected virtual machines on the host that requires maintenance and vMotion these machines to any other host with a VRA installed. When the host tries to enter maintenance mode, the VRA will wait for the virtual machines to be removed from the host, or for a period of 10 minutes, whichever occurs first. The VRA will then shut down. When the host exits maintenance mode, the VRA must be manually powered on.

**Note:** If the protected virtual machines are powered off, and not vMotioned to another host, the VRA will wait 10 minutes before shutting down.

**For a host machine on the recovery site** – VRA data and recovery volumes maintained by the VRA on the host should be moved to another machine, by changing the destination host for all the virtual machines being recovered to that host, as described in “Changing a Recovery VRA”, on page 248. Once host attempts to enter maintenance mode, the VRA is automatically shut down. When the host exists maintenance mode, the VRA must be manually powered on.

The VRA shutdown will not complete if you cancel the host maintenance mode task.

**Note:** If the host is put into maintenance mode via the VMware’s vSphere Update Manager, the VRA is powered on automatically when the host exits maintenance mode.

**Note:** Changing the VPG default host does not change the hosts for virtual machines already included in the VPG. These virtual machine hosts must be changed directly by configuring the individual virtual machines in the VPG definition.

To enable VMware host maintenance for a VRA both protecting and recovering virtual machines:

1. Remove affinity rules for protected virtual machines on the host that requires maintenance and vMotion these machines to any other host with a VRA installed.
2. Change the host for all virtual machines in VPGs recovering to this VRA to another host as described in “Changing a Recovery VRA”, on page 248.
3. Wait for any synchronization to complete.
4. Enter VMware host into maintenance mode. If prompted, **do not migrate** powered-off virtual machines. The VRA is automatically shut down.
5. *(Optional)* Remove the host from the cluster; place it under the data center entity, rather than the cluster entity.
6. Perform required maintenance. For example, upgrading the host.
7. Exit VMware host maintenance mode.
8. Power on the VRA.

**Note:** If the host is put into maintenance mode via the VMware’s vSphere Update Manager, the VRA is powered on automatically when the host exits maintenance mode.

9. Wait for the Zerto Virtual Manager to connect to the local VRAs. You can monitor the alerts to determine when the connections have been established.
10. *(Optional)* Add the host back into the cluster.

**Note:** If you do **not remove** the host from the cluster, a delta sync may accrue once the VMs are vMotioned back to the host.
Managing Protection When Moving a Host to a Different Cluster

When a host machine has to be moved to another cluster:

**For a host machine on the protected site** – Remove affinity rules for protected virtual machines on the host that is going to be moved and vMotion these machines to any other host in the cluster with a VRA installed. Shut down the VRA before moving the host.

**For a host machine on the recovery site** – Shut down the VRA and place the host in VMware maintenance mode. After shutting down the VRA VPGs with virtual machines being recovered to the VRA will enter an error state. Move the host to the new cluster, exit maintenance mode and power on the VRA. The VPGs in an error state will enter a bitmap sync and then resume a Meeting SLA status.

**Note:** Any VPGs that were defined with a recovery resource pool in the original cluster must be edited to change the default and virtual machine specific target host settings for the new cluster, even when the new cluster has a resource pool that is displayed in the VPG definitions.

Support for VMware Virtual Update Manager (VUM)

Some Virtual Update Manager upgrades require the host to enter maintenance mode.

If the user selected an upgrade which requires maintenance mode, and also selected the option *Do not change VM power state*, the Remediation task might fail.

**Note:** Recovery and journal volumes that reside on the host are not automatically migrated to another host in the cluster.

To ensure the Remediation task is successful, use the following procedure.

**To ensure successful Virtual Update Manager upgrades:**

1. Open the Site Settings window.
2. Click the Policies tab.
3. In the VMware Virtual Update Manager area, select *Allow Zerto to always enter hosts to maintenance mode during remediation*.
   - When this is selected, if the Virtual Update Manager’s Remediation task is detected, Zerto will automatically enter the host into maintenance mode.
   - The host will exit maintenance mode when the Virtual Update Manager’s Remediation task is completed.
   - The VRA is powered on automatically when the host exits maintenance mode.

**Note:** Automatic detection and powering off the VRA when running host maintenance mode is supported in vCenter version 6.5. For more information see Zerto Virtual Replication Interoperability Matrix.
CHAPTER 11: MANAGING A ZERTO VIRTUAL MANAGER

The Zerto Virtual Manager runs as a Windows service and connects to Zerto Virtual Replication components, such as VRAs, as well as hypervisor management tools, such as VMware vCenter Server and Microsoft SCVMM.

For the maximum number of virtual machines, either being protected or recovered to the Zerto Virtual Manager, see Sizing Considerations for Zerto Virtual Replication.

The following topics are described in this section:

- “To check connectivity between Zerto Virtual Manager components:”, below
- “Reconfiguring the Zerto Virtual Manager Setup”, on page 253
- “Reconfiguring the Microsoft SQL Server Database Used by the Zerto Virtual Manager”, on page 255
- “Replacing the SSL Certificate”, on page 256
- “Pair to Another Site and Unpair Sites”, on page 256

Check Connectivity Between Zerto Virtual Replication Components

If you think that there are connectivity problems to or from a Zerto Virtual Manager, you can use the Zerto diagnostics utility to check the connectivity.

To check connectivity between Zerto Virtual Manager components:

1. Open the Zerto Diagnostics application. For example, via Start > Programs > Zerto Virtual Replication > Zerto Diagnostics. The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the Test Connectivity to Zerto Virtual Replication components option and click Next. The IP Connectivity dialog is displayed.

You can use this dialog to check the following:

- TCP communication between the Zerto Virtual Managers (ZVMs) on the protected and recovery sites. The default port, specified during installation, is 9081.
- Communication between VRAs on the protected and recovery sites, via the control port and the data port.
3. Select the connectivity you want to test and in the case of the Zerto Virtual Manager (ZVM), specify the TCP communication port specified during the installation, if the default port, 9081, was changed.

4. Specify the type of test to perform:
   - **Server**: Test for incoming communication.
   - **Client**: Test for outgoing communication. Specify the IP address of the receiving Zerto Virtual Manager.

5. Click Next to test the specified connectivity.
   - The Server option listens for communication from a paired VRA. Stop listening by clicking Stop.
   - The Client options tests the client; on completion a result dialog is displayed.

6. Click **Stop** (server test) or **OK** (client test) to return to the Zerto Virtual Replication Diagnostics dialog.

### Reconfiguring the Zerto Virtual Manager Setup

When installing Zerto Virtual Replication, you provide the IP address of the vCenter Server to connect the Zerto Virtual Manager with, and the IP address of the machine where the Zerto Virtual Manager runs to enable running the Zerto User Interface.

You can change these IP addresses if necessary, using the Zerto Virtual Replication Diagnostics utility.

**To reconfigure the Zerto Virtual Manager:**

1. Click **Start > Programs > Zerto Virtual Replication > Zerto Diagnostics.**
   - The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the **Reconfigure Zerto Virtual Manager** option and click **Next.**
The installation settings for the connection to the vCenter Server are displayed.

3. Change the IP and username and password if necessary.
   - **IP / Host Name:** The IP address or host name of the machine where the vCenter Server runs.
   - **User Name:** The user name for an administrator to the vCenter Server. The name can be entered using one of the following formats:
     - username
     - domain\username
   - **Password:** A valid password for the given user name.

4. Click Next.
   The dialog for Zerto Virtual Manager setup is displayed:

   - **IP/Host name used by Zerto User Interface:** The IP to access the Zerto Virtual Manager from the Zerto User Interface. If the machine has more than one NIC, select the appropriate IP from the list, otherwise the IP that is displayed is the only option.
   - **HTTPS Port (ZVM <-> Zerto User Interface):** The port used for inbound communication between the Zerto User Interface and the Zerto Virtual Manager.
   - **TCP Port (ZVM<->ZVMs on other sites):** The port used for communication between Zerto Virtual Managers.
     - Both the protected and recovery sites belong to the same enterprise: If you change the value, when pairing sites, use the TCP port value you specify here.
     - An enterprise using a cloud service provider to supply disaster recovery services: You must not change this value.
   - **TCP Port (ZVM->VBA):** The port used for communication between the Zerto Virtual Manager and the Virtual Backup Appliance.
   - **HTTP Certificate:** Check Replace SSL Certificate and browse for a certificate, if you change the certificate you have been using.

5. Click Next.
   The connectivity is checked.
255

Reconfiguring the Zerto Virtual Manager Setup

Note: If one of the tasks fails, click the link for information about why it failed. Usually it is a mistake when entering an IP address.

6. Click Next.
   The Zerto Virtual Manager is reconfigured.

7. Click Finish.

8. If you changed the IP address of the Zerto Virtual Manager, or the TCP port it uses to communicate with paired Zerto Virtual Managers on other sites, you have to unpair these sites, both from this site and from the remote sites and then pair the sites again.

Reconfiguring the Microsoft SQL Server Database Used by the Zerto Virtual Manager

1. Click Start > Programs > Zerto Virtual Replication > Zerto Diagnostics.
   The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the Change SQL Server Credentials option and click Next.
   The installation settings for the SQL Server are displayed. Change the IP and username and password if necessary.

   **Server Name:** The domain name and server instance to connect to, with the format \server_name\instance_name\ or \Server_IP\instance_name. Specify either of the following authentication options:

   **Windows Authentication:** Use Windows authentication. This option is only enabled if a specific service user account was specified in the previous Service User dialog, in which case the service account name and password are used.
Replacing the SSL Certificate

The communication between the Zerto Virtual Manager and the user interface uses HTTPS. When you first logged in to the Zerto User Interface you installed a security certificate to continue working without each login requiring acceptance of the security.

To replace the SSL certificate, follow the procedure “Reconfiguring the Zerto Virtual Manager Setup”, on page 253, and in the Zerto Virtual Manager Setup window, in the HTTP Certificate area, select Replace SSL Certificate, and browse for a replacement certificate.

Pair to Another Site and Unpair Sites

See the following sections:

- “Pair to Another Site”, below
- “Unpairing Sites”, on page 257
Pair to Another Site

You can pair to any site where Zerto Virtual Replication is installed.

To pair to a site:
1. In the Zerto User Interface, in the SITES tab click PAIR.
   The Add Site dialog is displayed.

   ![Add Site Dialog]

2. Specify the following:
   - **Remote Site ZVM IP Address**: IP address or 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 the installation. The default port during the installation was 9081.

3. Click PAIR.
   The sites are paired, meaning that the Zerto Virtual Manager for the local site is connected to the Zerto Virtual Manager at the remote site.

Unpairing Sites

You can unpair any two sites that are paired to each other.

**IMPORTANT**: if there is a VPG on either of the sites you are unpairing, the VPGs will be deleted.

To unpair two sites:
1. In the Zerto User Interface, in the SITES tab, select the site which you want to unpair.
2. Click UNPAIR.
   A message appears warning the user that the sites are about to unpair.
   If there are either protected or recovered VPGs on the paired sites, a message appears warning the user that the VPGs will be deleted.

3. For vSphere, Hyper-V and Azure platforms, you can select to keep disks to use for preseeding if the VMs are re-protected. If you select this option, the disks are not removed from the recovery site.
4. To unpair, click CONTINUE.
   The sites are no longer paired. If there are VPGs on either site, they are deleted.
   The VRA on the recovery site that handles the replication for the VPG is updated including keeping or removing the replicated data for the deleted VPG, depending if you selected to keep disks to use for preseeding.
   The locations of the saved target disks are specified in the **Events** tab in the ZVM application on the **Recovery** site.
There are a number of configuration tasks that you can perform, some of which should be done as part of the initial site configuration.

The following topics are described in this chapter:

- “Site Settings”, below
- “Seeing What Is Licensed”, on page 265
- “Submitting a Support Ticket”, on page 266
- “About Zerto Virtual Replication”, on page 267

Site Settings

The Site Settings dialog enables configuring various site settings. These include the default script timeout and protection policies such as the commit policy for a failover or move operation.

To specify site information:

1. In the Zerto User Interface (top right), click SETTING ( ) and select Site Settings.

   The Site Settings dialog is displayed.

   ■ In vSphere and Hyper environments, the following window is displayed.
In **AWS** environments, the following window is displayed.

**Site Details**

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Site Location</th>
<th>Bucket Name</th>
<th>Contact Name</th>
<th>Contact Email</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>zero-00de1573-115e-4c72-ae3a-42c902a7af6</td>
<td>Unconfigured contact info</td>
<td>Unconfigured contact email</td>
<td>Unconfigured contact phone</td>
</tr>
</tbody>
</table>

**User Credentials**

<table>
<thead>
<tr>
<th>Access Key ID</th>
<th>Secret Access Key</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In **Azure** environments, the following window is displayed.

**Site Details**

<table>
<thead>
<tr>
<th>Site Name</th>
<th>Site Location</th>
<th>Contact Name</th>
<th>Contact Email</th>
<th>Contact Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site-8 Cloud-1</td>
<td>Manhattan</td>
<td>Zerto Trial</td>
<td>Unconfigured contact email</td>
<td>Unconfigured contact phone</td>
</tr>
</tbody>
</table>

**Azure Settings**

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Client ID</th>
<th>Subscription</th>
<th>Resource Name</th>
<th>Storage Account Name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Make any required changes to the settings, click **SAVE** and then **APPLY**. The following settings can be defined:

- “**Editing Information About a Site**”, below
- “**Defining Performance and Throttling**”, on page 261
- “**Defining Site Policies**”, on page 262
- “**Configuring Email Settings**”, on page 263
- “**Defining Resource Report Sampling Period**”, on page 264
- “**Reviewing Supported Host Versions**”, on page 265

Licensing is described in “**Seeing What Is Licensed**”, on page 265. You also use the Site Settings to set up Zerto cloud connector static routes and VMware vCloud Director from the Cloud Settings item. For details, refer to Zerto Cloud Manager Administration Guide.
Editing Information About a Site

You provide information about the site during installation, to make it easier to identify the site in the user interface and to identify the contact person at the site. After installation you can update these settings.

To update information about the local site:

1. In the Zerto User Interface (top right), click **Site Settings** and select **Site Settings**. The Site Settings dialog is displayed.

<table>
<thead>
<tr>
<th>Site Details</th>
<th>Site Name</th>
<th>628</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Location</td>
<td></td>
<td>Unconfigured location</td>
</tr>
<tr>
<td>Bucket Name</td>
<td></td>
<td>zero-00da1f575-115e-4c72-ae38-b142c002a7af6</td>
</tr>
<tr>
<td>Contact Name</td>
<td></td>
<td>Unconfigured contact info</td>
</tr>
<tr>
<td>Contact Email</td>
<td></td>
<td>Unconfigured contact email</td>
</tr>
<tr>
<td>Contact Phone</td>
<td></td>
<td>Unconfigured contact phone</td>
</tr>
</tbody>
</table>

   | User Credentials                   | Access Key ID |   | Secret Access Key |   |

2. Define general information about the site.
   - **Site Name**: The name used to identify the site.
   - **Site Location**: Information such as the address of the site or a significant name with which to identify the site location.
   - **Bucket Name**: The name of the bucket that was created when Zerto Virtual Replication was installed. This cannot be changed.
   - **Contact Name**: The name of the person to contact if a need arises. Mandatory.
   - **Contact Email**: An email address to use if a need arises.
   - **Contact Phone**: A phone number to use if a need arises.

3. (On premise environments) To change the **User Credentials** to access the vCenter or Hyper-V SCVMM server from the Zerto Virtual Manager:
   - **User Name**: The administrator name used to access the vCenter or SCVMM server. The name can be entered using either of the following formats:
     - username
     - domain\username
   - **Password**: The password used to access the vCenter or SCVMM server for the given user name. To ensure security, after saving the settings, the password field is cleared.

4. (Azure environments only) **Azure Settings**:
   - **Application Name**: The name used to access Azure.
   - **Client ID**: A unique identifier that is associated with the access name.
   - **Subscription**: The subscription associated with the user.
   - **Resource Name**: The name of the resource the user created.
   - **Storage Account Name**: The name of the storage account created or selected for this site during installation.

5. Click **SAVE**.
Defining Performance and Throttling

Performance and throttling settings include bandwidth settings and the maximum time a script can run before timing out.

You can specify bandwidth throttling, which is the maximum bandwidth that Zerto Virtual Replication uses from this site to all peer recovery sites. The default value is for Zerto Virtual Replication to automatically assign the bandwidth used per VPG, based on using the maximum available and then prioritizing the usage according to priority set for the VPGs sending data over the WAN.

Note: The minimum supported bandwidth is 5 Mb/sec.

For details about estimating the bandwidth, see “WAN Sizing Requirements with Zerto Virtual Replication”, on page 26.

To configure bandwidth throttling:
1. Click **Performance and Throttling**.

2. **Bandwidth Throttling** by default is **Unlimited**. To change this, deselect Unlimited, and enter a bandwidth value.

   If you are going to protect virtual machines on this site as well as recover virtual machines to this site, for example via failback, you also have to set the bandwidth on the peer site out to this site.

3. **Time-based Throttling** is **Unlimited** by default. To change this, deselect Time-based Throttling, and enter a value for the bandwidth for a selected period of time:
   - **From**: The hour and the minute to start the throttling, using a 24-hour clock.
   - **To**: The hour and the minute to end the throttling, using a 24-hour clock.

   For Example: If you know that the bandwidth needs specific throttling during a certain period, during the daily peak transaction period you can override the throttling of the bandwidth for these specific times.

4. Click **APPLY** or **SAVE**.

**NOTE:**

**IO Throttling** values should be changed only in coordination with Zerto support.
Advanced Site Configuration

Defining Site Policies

You can set default recovery and replication policies.

Configuring Disaster Recovery Policies

**To configure disaster recovery policies:**

1. Click **Policies** tab.

2. In the **Disaster & Recovery** area, choose the **Failover/Move Commit Policy** to use during a failover or move operation, described in *Initiating a Failover* and *Moving Protected Virtual Machines to a Remote Site* respectively. The following options are available:
   - **None**: The failover or move operation must be manually committed or rolled back by the user.
   - **Commit**: After the time specified in the **Default Timeout** field the failover or move operation is committed, unless manually committed or rolled back by the user before the time-out value is reached. During the specified time you can check the recovered VPG virtual machines.
   - **Rollback**: After the time specified in the **Default Timeout** field the failover or move operation is rolled back, unless manually committed or rolled back by the user before the time-out value is reached. During the specified time you can check the recovered VPG virtual machines.

   The value set here applies as the default for all failover or move operations from this point on but can be changed when defining a failover or move operation.

3. Specify the **Default Timeout** after which a **Commit** or **Rollback** commit policy is performed. A value of zero indicates that the system will automatically perform the commit policy, without waiting for any user interaction.

4. In the **Pre/Post Recovery Operations Scripts** area, specify the timeout in seconds for a script to run before or after a failover, move, or test failover in the **Default Script Execution Timeout** field.

   For information about scripts, see “Running Scripts Before or After Recovering a VPG”, on page 225.

5. In the **Replication** area:
   - If the **same site** is to be used as both the protected and recovery site, select **Enable Replication to Self**. For more details, see “Enabling Replication to the Same Site”, on page 24.
   - Choose the **Replication Pause Time**, which is the time to pause when the journal might have problems, resulting in the loss of all checkpoints. For example, when the datastore for the journal is almost full.
     - Replication pause time is the amount of time that the **transfer of data** from the protected site to the **journal on the recovery site** is **paused**.
     - This time can then be used by the administrator to resolve the issue, for example by cloning the virtual machines in the VPG, described in “Cloning Protected Virtual Machines to the Remote Site”, on page 305.
Advanced Site Configuration

- The value defined here is applied to existing and new VPGs.
- The value defined here is applied to this site only.
- To pause the protection in both directions, for example to cover reverse protection back to the original site after a move operation, you must define **Replication Pause Time on both sites**.
- To preserve the BIOS UUID of the protected VM after recovery operations, in the recovery ZVM Site Settings window, select **For incoming replication, copy the BIOS UUID of the protected VM to the recovered VM**.

**Notes:**
- Preserving of the BIOS UUID is **not** supported in Clone and Self-Replication recovery operations.
- Preserving of the BIOS UUID is **not** supported in Public Cloud.
- Cross replication is **not** supported.

6. To enter the host to maintenance mode during remediation, in the **VMware Virtual Update Manager** area, select **Allow Zerto to always enter hosts to maintenance mode during remediation**. When this is selected, if the Virtual Update Manager’s Remediation task is detected, Zerto will automatically enter the host into maintenance mode. The host will exit maintenance mode when the Virtual Update Manager’s Remediation task is completed.

**Notes:**
- In some **upgrade** environments, Virtual Update Manager requires the host to enter maintenance mode. For further details, see “Support for VMware Virtual Update Manager (VUM)”, on page 251.

7. Click **APPLY** or **SAVE**.

Configuring Email Settings

You can configure Zerto Virtual Replication alerts to be sent to an email address, so as to be better informed when an alert occurs and backups are run.

**Email Settings**

**To configure email settings:**

1. Click **Email Settings**.

   - **Email Settings**
     - **SMTP Server Address**
     - **SMTP Server Port**
     - **Sender Account**
     - **To**

   ![Email Settings](image)

2. Specify the **SMTP server Address**. The Zerto Virtual Manager must be able to reach this address.
3. If the **SMTP Server Port** was changed from the default, **25**, specify the port number.

Site Settings
4. Specify a valid email address for the email sender name in the Sender Account field.
5. Specify a valid email address where you want to send the email in the To field.
   You can test that the email notification is set up correctly by clicking SEND TEST EMAIL. A test email is sent to the email address specified in the To field.
6. Click APPLY or SAVE.

Alerts and Reports

You can configure when to send alerts and backup reports.

To configure when to send emails about alerts and backups:
1. To send an email when an alert is issued, check Enable sending alerts.
2. To send an email with a backup report, check Enable backup reports.
3. Specify whether you want a backup report sent daily or weekly.
   Daily: Send a daily backup report
   Weekly: Send a weekly backup report. Select the day of the week from the dropdown list.
4. Specify day of the week and the time of day to send the backup report.
5. Click APPLY or SAVE.

Defining Resource Report Sampling Period

Specify when you want to take resource samples to identify resource usage, either daily at a specific hour and minute or hourly at a specific minute within each hour.

1. Click Reports.

   Resource Report
   Sampling Rate [1]
   Sampling Time [7]

2. Choose the Sampling Rate.
3. Choose the Sampling Time.
   If you set the daily time to be 12:00, you will get a sample taken at noon every day. Collecting a sample hourly provides a higher resolution picture of replication traffic than if collected daily.
4. Click APPLY or SAVE.
Information is saved for 90 days when the sampling period is hourly and for one year when the sampling period is daily. These samples are used to generate resource reports as described in “Zerto Virtual Replication Reports”, on page 323.

**Reviewing Supported Host Versions**

Zerto Virtual Replication works with most VMware hypervisor hosts. For a list of supported hosts, click **Compatibility**.

<table>
<thead>
<tr>
<th>Version</th>
<th>Supported Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX / ESXi 4.1</td>
<td>4.1, 4.1.1U1, 4.1.1U2, 4.1.1U3</td>
</tr>
<tr>
<td>ESXi 5.0</td>
<td>5.0, 5.0.1U1, 5.0.1U2, 5.0.1U3</td>
</tr>
<tr>
<td>ESXi 5.1</td>
<td>5.1, 5.1.1U1, 5.1.1U2, 5.1.1U3</td>
</tr>
<tr>
<td>ESXi 5.5</td>
<td>5.5, 5.5.1U1, 5.5.1U2, 5.5.1U3</td>
</tr>
<tr>
<td>ESXi 6.0</td>
<td>6.0, 6.0.1U1, 6.0.1U2, 6.0.1U3</td>
</tr>
<tr>
<td>ESXi 6.5</td>
<td>6.5, 6.5.1U1</td>
</tr>
</tbody>
</table>

**Seeing What Is Licensed**

The Zerto license includes information such as the number of virtual machines that can be protected and the license expiry date. You can see these details by clicking **SETTING ( )** in the top right of the header and selecting **License**.
The Zerto license includes the following details:

- **License**: The license key itself.
- **License Type**: What is licensed: whether the license restricts the number of virtual machines that can be protected or the number of sockets used.
- **Expiry Date**: The license expiry date.
- **Quantity**: The maximum amount licensed, either virtual machines or sockets, based on the license type. If blank, the quantity is unlimited.
- **Usage**: The sites using the license and the number of protected virtual machines in each site.

A warning is generated when either the license expires or more than the licensed number of virtual machines are being protected. Protection continues but the license should be updated. After getting a new license key you can update Zerto Virtual Replication with this key.

**To update a license key:**

1. In the Zerto User Interface, in the top right of the header click SETTING () and select License.
2. Enter a valid license key and click APPLY or SAVE.
   - The license is updated on the local site and the paired remote sites.

---

**Submitting a Support Ticket**

You can open a ticket to Zerto support directly from Zerto Virtual Replication.

**Note:** 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. If the clocks are not synchronized with UTC, submitting a support ticket can fail.

**To open a support ticket:**

Support tickets can be opened directly in the Zerto User Interface.

Creating a support ticket in the Zerto User Interface simplifies the submission process since much of the information that is required when entering a ticket using the Zerto Support Portal, such as the version and build numbers, is automatically added to the ticket when it is submitted via the Zerto User Interface.

In addition, when the ticket is submitted, a snapshot of the current environment is also attached to the ticket. The snapshot information includes the lists of alerts, events, tasks, VPGs, and virtual machines that are protected.

This information is used to help Zerto resolve the ticket quickly and, whenever possible, without the need to request more information from you.

**Note:** 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. If the clocks are not synchronized with UTC, submitting a support ticket can fail.
To open a support ticket:

1. In the Zerto User Interface, click **SETTING** ( ) in the top right of the header and select **Submit Support Ticket**. The Open Support Ticket dialog for the site is displayed.

2. Specify the ticket details:
   - **Subject**: The subject of the support ticket.
   - **Type**: The type of ticket being opened. Available options are:
     - Problem
     - Feature Request
     - Question
   - **Severity**: The severity of the issue.
   - **Description**: A description of the problem or question in addition to the information supplied in the subject.
   - **Allow remote log collection**: How many logs is Zerto allowed to collect. Available options are:
     - Only for this ticket
     - For the next 30 days
     - Never
   - **SSP Email Address**: A valid email address registered with Zerto, with permission to open tickets.

3. Click **SUBMIT**.

The ticket is processed and its progress is displayed. If the email address is not valid, the ticket is rejected. Once the ticket submission starts, it cannot be canceled.

### About Zerto Virtual Replication

In the About window, you can do the following:

- View the version of Zerto Virtual Replication being run.
- Enable or disable the **Zerto CALLHOME feature**. The Zerto CALLHOME feature enables support notification and analytics for the following purposes:
  - To improve Zerto Virtual Replication.
  - To send notifications to the user when a new Zerto Virtual Replication version is available, or when new hypervisor versions are supported by Zerto.
- Enable or disable Zerto Virtual Manager to send data to the SaaS platform for monitoring purposes, using the Zerto Mobile App. This action is done by licensed Zerto Virtual Manager users.

When clicking About, the following options appear:
To perform these actions, do the following:

1. In the Zerto User Interface, in the top right of the header, click SETTING ( ), and then click About.
   The version and build of Zerto Virtual Replication installed in the site are displayed.
2. To enable the Zerto CALLHOME feature, click **Enable Support notification and product improvement feedback**. This is selected by default.
   Note: This option is grayed out for Microsoft Azure and AWS.
   If the user deselects Enable Support notification and analytics, a warning appears notifying the user that deselecting this option will stop Zerto Virtual Replication from sending notifications when new Zerto Virtual Replication updates are available, or when new hosts are supported.
3. If you want Zerto Virtual Replication to send information to our Online Services and Zerto Mobile App, and enable remote upgrade, select **Enable SaaS features**. This is selected by default.
   This allows licensed Zerto Virtual Manager users to enable or disable data being sent from the Zerto Virtual Manager to the SaaS platform, thereby enabling site monitoring using the Zerto Mobile App.
   - If the user deselects Enable Online Services and Zerto Mobile, a warning appears notifying the user that deselecting this option will stop Zerto Virtual Replication from sending information to Online Services and to the Zerto Mobile Application, rendering these services inoperable for the entire installation.
Zerto Virtual Replication provides a number of operations to recover virtual machines at the remote site. This chapter describes these operations. The following topics are described in this chapter:

- “The Failover Test Operation”, on page 269
- “The Move Operation”, below
- “The Failover Operation”, on page 270
- “The Restore File Operation”, on page 271
- “The Clone Operation”, on page 271

In addition, when extended recovery is defined, an offsite backup can be restored as described in “Restoring Virtual Machines”, on page 317.

The Failover Test Operation

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 in a sandbox, using the test network specified in the VPG definition as opposed to a production network, to a specified point-in-time, using the virtual disks managed by the VRA. All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using scratch volumes makes cleaning up the test failover more efficient. For details, see “Testing Recovery”, on page 273.

During the test, any changes to the protected virtual machines at the protected site are sent to the recovery site and new checkpoints continue to be generated, since replication of the protected machines continues throughout the test. You can also add your own checkpoints during the test period.

The following diagram shows the positioning of the virtual machines before and during a Failover test operation.
The Move Operation

Use the Move operation to transfer protected virtual machines from the protected site to the recovery site in a planned migration.

When you perform a planned migration of the virtual machines to the recovery site, Zerto Virtual Replication assumes that both sites are healthy and that you planned to relocate the virtual machines in an orderly fashion. For details, see “Migrating a VPG to a Recovery Site”, on page 284.

The following diagram shows the positioning of the virtual machines before and after the completion of a Move operation.

Note: The Move operation without reverse protection does not remove the VPG definition but leaves it in a Needs Configuration state.

The Failover Operation

Following a disaster, use the Failover operation to recover protected virtual machines to the recovery site. A failover assumes that connectivity between the sites might be down, and thus the protected virtual machines and disks are not removed, as they are in a planned Move operation.

When you set up a failover you always specify a checkpoint to which you want to recover the virtual machines. When you select a checkpoint – either the last automatically generated checkpoint, an earlier checkpoint, or a tagged checkpoint – Zerto Virtual Replication makes sure that virtual machines at the remote site are recovered to this specified point-in-time. For details, see “Managing Failover”, on page 295.

Note: To identify the checkpoint to use, you can perform a number of test failovers, each to a different checkpoint.

Failback after the Original Site is Operational

After completing a failover, when the original site is back up and running you can move the recovered virtual machines back again using the Move operation. The VPG that is now protecting the virtual machines on the recovery site has to be configured and then a Delta Sync is performed with the disks in the original protected site. Once the VPG is in a protecting state the virtual machines can be moved back to the original site. For details, see “Moving Protected Virtual Machines to a Remote Site”, on page 286.
The following diagram shows the positioning of the virtual machines before and after the completion of a Failover operation.

Note: The Failover operation without reverse protection does not remove the VPG definition but leaves it in a Needs Configuration state.

The Restore File Operation

Use the Restore File operation to recover individual files and folders from the recovery site. You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto Virtual Replication and running Windows operating systems. You can recover the files and folders from a specific point-in-time. For details, see “Recovering Files and Folders”, on page 310.

The Clone Operation

Use the Clone operation to create a copy of the VPG virtual machines on the recovery site in the production network. The virtual machines on the protected site remain protected and live.

Note: When the recovery site is vCD, the clone is created in vCenter Server and the virtual machines have to be manually imported into vCD.

You might want to create a clone if you need to have a copy of the virtual machines saved to a specific point-in-time, for example, when the VPG enters a Replication Paused state, or when testing the VPG in a live DR test. For details, see “Cloning a VPG to the Recovery Site”, on page 305.

The cloned machines are named the after the protected virtual machine name along with the timestamp of the checkpoint used for the clone. The cloned virtual machines are not powered on.
The following diagram shows the positioning of the virtual machines before and after the completion of a Clone operation.
CHAPTER 14: TESTING RECOVERY

In order 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. This chapter describes how to test VPG recovery.

The following topics are described in this chapter:
- “The Test Failover Process”, below
- “Starting and Stopping Failover Tests”, on page 274
- “Viewing Test Results”, on page 278
- “Live Disaster Recovery Testing”, on page 278

Note: You cannot perform a failover test while a backup job is running.

The Test Failover Process

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 in a sandbox, using the test network specified in the VPG definition, as opposed to creating virtual machines in a production network, to a specified point-in-time, using the virtual disks managed by the VRA. All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal.

During the test, any changes to the protected virtual machines at the protected site are sent to the recovery site and new checkpoints continue to be generated, since replication of the protected machines continues throughout the test. You can also add your own checkpoints during the test period. You can initiate a failover during a test, as described in “Initiating a Failover During a Test”, on page 304.

The Failover Test operation has the following basic steps:

1. Starting the test.
   a) The test virtual machines are created at the remote site using the network specified for testing in the VPG settings and configured to the checkpoint specified for the recovery.
   b) The virtual machines 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.

2. Testing. The virtual machines in the VPG are created as test machines in a sandbox and powered on for testing using the test network specified in the VPG definition and using the virtual disks managed by the VRA. All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using scratch volumes makes cleaning up the test failover more efficient.

   Note: You must not delete, clone, migrate to another host or change the disk properties of any of the test virtual machines.

3. Stopping the test.
   a) The test virtual machines are powered off and removed from the inventory.
   b) The following tag is added to the checkpoint specified for the test: Tested at startDateAndTimeOfTest. The tagged 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. For example, in a cluster, if the HA configuration in a cluster includes admission control to prevent virtual machines being started if they violate availability
constraints, testing the failover of every VPG configured for recovery to this cluster, at the same time, will show whether the constraints are violated or not.

When configuring a VPG, specify the period between tests for that VPG in the Test Reminder field in the REPLI CATION step of the Create VPG wizard.

See also:
- “Starting and Stopping Failover Tests”, on page 274
- “Viewing Test Results”, on page 278
- “Live Disaster Recovery Testing”, on page 278

Starting and Stopping Failover Tests

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.

By default, test virtual machines are started with the same IPs as the protected machines in the protected site. This can create clashes so Zerto recommends ensuring that different IPs are assigned to the virtual machines when they start, by configuring virtual machine NIC properties in the VPG. For details, refer to “Protecting Virtual Machines from a vCenter Server”, on page 39. If you have defined the new virtual machines so that they are assigned different IPs, the re-IP cannot be performed until the new machine is started. Zerto Virtual Replication changes the machine IPs and then reboots these machines with their new IPs.

**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.

You can select the checkpoint to use for the recovery and see if a boot order and scripts are defined for the VPG.

4. By default, the last checkpoint added to the journal is displayed in the Checkpoint column
   - To use this checkpoint, proceed to the next step.
   - To change the checkpoint, click the link that appears as the checkpoint.

   A window appears, displaying a list of the VPGs’ checkpoints.

   **Latest:** Recovery is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery.

   When selecting the latest checkpoint, the checkpoint used is the latest at this point.

   If a checkpoint is added between this point and starting the failover, this later checkpoint is not used.

   **Latest Tagged Checkpoint:** The recovery operation is to the latest checkpoint added in one of the following situations:
   - By a user.
   - When a failover test was previously performed on the VPG that includes the virtual machine.
   - When the virtual machine was added to an existing VPG after the added virtual machine was synchronized.

   To use a checkpoint which is not the latest checkpoint, or the latest tagged checkpoint, choose Select from all available checkpoints. By default, this option displays all checkpoints in the system. You can choose to display only automatic, or tagged checkpoints, or any combination of these types.

5. Click OK.

6. Click NEXT.
The FAILOVER TEST step is displayed. The topology shows the number of VPGs and virtual machines being tested to failover to each recovery site. In the following example, 2 VPGs will be failed over to Site6-Ent2-R2, and they contain 5 virtual machines; and 1 VPG will be failed over to Site5-Ent2-P2-R2 and it contains 2 virtual machines.

7. 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 virtual machines are created in the recovery site.

**What Happens After Starting a Test?**

During the initiation phase, the virtual machines in the virtual protection group are created at the recovery site with the suffix `testing recovery`.

**Note:** The following conversions are done to a protected virtual machine when it is recovered in Hyper-V:
- A machine using BIOS is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine using EUFI is recovered in Hyper-V as a Generation 2 virtual machine.
- A machine with a 32bit operating system is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine with a 64bit operating system is recovered in Hyper-V as either a Generation 1 or Generation 2 virtual machine, dependent on the operating system support in hyper-V.
- The virtual machine NICs are recovered with Hyper-V network adapters except for protected Windows 2003 virtual machines which are recovered with Hyper-V legacy network adapters.
- When VMware Tools is installed on the protected virtual machine running Windows Server 2012, Integration Services is installed on the recovered virtual machine automatically.

All testing is written to scratch volumes. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using these test scratch volumes makes cleaning up the test failover more efficient.

While a test is running:
- The virtual machines in the VPGs continue to be protected throughout the test.
- You can add checkpoints to the VPGs, and if necessary fail over the VPGs, as described in "Initiating a Failover During a Test", on page 304.
- You cannot take a snapshot of a test machine, since the virtual machine volumes are still managed by the VRA and not by the virtual machine. Using a snapshot of a test machine will create a corrupted virtual machine.
- You cannot move VPGs being tested.
- You cannot delete, clone, migrate to another host or change the disk properties of any of the test virtual machines.
- 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.

- In the Zerto User Interface, click the VPGs tab, and then click the name of a VPG you are testing. A dynamic tab is created displaying the specific VPG details including the status of the 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.
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.

---

**Viewing Test Results**

After stopping a test, you can see the test results as part of Zerto Virtual Replication reports. Refer to “Recovery Reports”, on page 325.

---

**Live Disaster Recovery Testing**

This section describes how to use the basic Zerto Virtual Replication recovery operations to perform live disaster recovery tests, in different situations.

When performing a **live DR test** you need to consider the following:
- **Purpose** of the live DR test:
  - Do you only want to **verify that the VMs can recover properly**?
    - Or -
  - Do you want to conduct a **full DR test** that will include running user traffic against the recovered VMs?
- **Length of time** you want to test the recovery, a **few hours** or **several days**.
- Whether the **changes** to the recovered machine need to be **retained after the test** or can they be **discarded**?
- Whether you are willing to accept **temporary downtime** of the application.
- Whether you want to **simulate an actual disaster** at the protected site, for example by simulating a network outage or bringing down the protected site.
During any live test, Zerto recommends that you only maintain one working version of the same virtual machine. As such, the first step in any test, except for a Failover Test or Clone, is to make sure that the protected virtual machines are shut down before starting to test recovered machines.

During a Zerto Virtual Replication Move operation the first step Zerto Virtual Replication performs is to shut down the protected machines, to ensure data integrity. However, a Zerto Virtual Replication Failover operation assumes that the protected virtual machines are no longer accessible (the total site disaster scenario) and does not attempt to shut them down at the beginning of the operation.

In a live test using a Failover operation you have to manually shut down the virtual machines to be tested at the beginning of the test in order to prevent potential split-brain situations where two instances of the same applications are live at the same time.

If you want to perform a live DR test that includes a simulated disaster you can simulate the disaster, for example, by disconnecting the network between the two sites. In this type of test, once the disaster is simulated a Move operation cannot be used, since it requires both sites to be healthy, while a Failover operation can be used.

**Basic Verification – User Traffic Is Not Run against the Recovered VMs**

Basic testing that the virtual machines can recover is done using either a Failover Test operation or an uncommitted Move operation, using the Rollback setting.

**Using a Failover Test Operation**

You use a Failover Test operation if recovering the virtual machines in a sandbox, using the test network specified in the VPG definition for network isolation, is sufficient for a test. The Failover Test operation is described in "The Failover Test Operation", on page 269 and in "Starting and Stopping Failover Tests", on page 274.

See the following sections:
Using a Failover Test Operation: Recommended Procedure for a Live DR Test

1. Change the VPG Failover Test Network to the production network used at the recovery site.
2. Manually shut down the virtual machines in the VPG.
3. Insert a new checkpoint. This avoids potential data loss since the virtual machines are shut down and the new checkpoint is added after all I/Os have been written to disk.
4. Optionally simulate a disaster, for example by disconnecting the two sites.
5. Perform a test failover on the VPG, choosing the checkpoint you added in step 3.
6. Verify that the test machines are recovered as expected.
7. Run user traffic against the virtual machines.
8. Stop the failover test.
9. Reconnect the sites.

Using a Failover Test Operation: Failover Test Considerations

- You do not have to shut down the protected virtual machines, and changes from the test phase are not kept or applied to the protected applications.
- You can recover to a specific point-in-time.
- You can use an isolated network to enable testing in a sandbox environment and not a live DR environment. This is the recommended practice.
- During the testing period, every change is recorded in a scratch volume.
  - Therefore, since both the scratch volume and virtual machines tested are on the same site, performance can be impacted by the increased I/Os during the failover test.
  - In addition, the longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done.
  - The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed.
  - The scratch volumes reside on the storage defined for the journal.
- At the end of the test, if you powered off the virtual machines in the protected site, you can power them back on and continue to work without the need to save or replicate back any data changed during the test.
- You can also use a Failover Test operation if you want to simulate an actual disaster for around an hour or less and do not want to save any changes on the recovery site.

Using an Uncommitted Move Operation

Use a Move operation with the commit/rollback policy set to rollback after the test period, if you need to test the recovery of virtual machines in the recovery site production environment. The Move operation is described in “Moving Protected Virtual Machines to a Remote Site”, on page 286.

Note: Committing the Move operation requires failing the migrated virtual machines back to the production site after a Delta Sync has been performed on the committed machines in the recovery site.

Recommended Procedure for a Live DR Test

1. In the Move wizard, in the EXECUTION PARAMETERS tab, for commit policy, select None.
2. Either power off the relevant virtual machines or check the Force Shutdown checkbox, in the EXECUTION PARAMETERS tab, to make sure that the virtual machines are shut down, if they cannot be powered off using VMware Tools.
3. After testing the machines in the recovery site, roll back the Move operation, which will return the virtual machines to their pre-test state.
   - Changes from the pre-commit phase are not kept or applied to the protected applications.
   - The virtual machines are allocated disks and connected to the network for a full test of the environment.
   - The protected machines are turned off until the end of the test, ensuring that there are no conflicts between the protected site and recovery site.
During the testing period, every change is recorded in a scratch volume to enable rolling back. Therefore, since both the scratch volume and virtual machines being moved are on the same site, performance can be impacted by the increased IOs during the testing period. In addition, the longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. You can only recover to the last checkpoint written to the journal, at the start of the Move operation.

Run User Traffic Against the Recovered VMs
Testing actual user traffic against recovered virtual machines can be done using a Clone, Move, or Failover operation, as follows:

**Move operation:** When you can shut down the protected virtual machines but you do not want or need to simulate an actual disaster.

**Failover operation:** When you want to simulate an actual disaster.

**Clone operation** - When the protected application has to run throughout the test.

Using a Move Operation
Use a Move operation when you can shut down the protected virtual machines but you do not want to simulate an actual disaster. After the virtual machines have been recovered in the target site, they are used as the protected machines for as long as the test lasts. The Move operation is described in “The Move Operation”, on page 270 and in “Moving Protected Virtual Machines to a Remote Site”, on page 286.

See the following sections:
- “Using a Move Operation - Recommended Procedure for a Live DR Test”, on page 281
- “Using a Move Operation - Move Considerations”, on page 281

Using a Move Operation - Recommended Procedure for a Live DR Test
1. To enable using the Move functionality for a DR test, in the Move wizard, in the EXECUTION PARAMETERS tab, for commit policy, select None.
2. Move the VPG back to the original protected site. A Delta Sync is performed to copy the new transactions performed on the virtual machines in the recovery site back to the original protected site.

Using a Move Operation - Move Considerations
- You can test the moved machines before they are committed.
- You can test for as long as you want.
- The virtual machines are allocated disks and connected to the network for a full test of the environment.
- The originally protected disks are maintained for a faster failback when reverse replication is specified.
- The protected machines are turned off until the move is committed and then they are removed from the protected site. This ensures that there are no conflicts between the protected site and recovery site.
- You must test to the last checkpoint, taken after the protected virtual machines are shut down.
- An actual disaster is not simulated.
- During the testing period, if reverse replication is not specified, there is no protection for the recovered machines.
Using a Failover Operation

Use a Failover operation when you can shut down the protected virtual machines and you want to simulate an actual disaster. After the virtual machines have been recovered in the target site they are used as the protected machines for as long as the test lasts.

Using a Failover operation to test DR requires specific steps to ensure that the virtual machines are gracefully migrated to the target site, similar to a Move operation and that, like a Move operation, they can be verified prior to committing the failover. The Failover operation is described in “The Failover Operation”, on page 270.

See the following sections:
- “Using a Failover Operation - Recommended Procedure for a Live DR Test”, on page 282
- “Using a Failover Operation - Failover Considerations”, on page 282

Using a Failover Operation - Recommended Procedure for a Live DR Test

1. Manually shut down the virtual machines.
2. Insert a new checkpoint. This avoids potential data loss since the virtual machines are shut down and the new checkpoint is added after all I/Os have been written to disk.
3. Optionally simulate a disaster, for example by disconnecting the two sites.
4. Perform a live failover on the VPG, specifying the commit policy and choosing the checkpoint you added in step 2. Choose a commit policy that will give you the necessary time to check that the failed over virtual machines have been successfully recovered to the correct point-in-time and if they are not, you are able to roll back the failover.
5. Continue to use the recovered virtual machines.
6. The VPG is in a Needs configuration state, because there is no access to the protected site.

After testing the recovered virtual machine you can finalize the live DR test and fail the virtual machines back to the original protected site:

1. Reconnect the sites.
2. Enable protection for the virtual machines by editing the VPG and clicking DONE.
3. Zerto Virtual Replication uses the original disks to preseed the volumes and expedite the synchronization between the two sites, using a Delta Sync.
   - The time it will take for the Delta Sync to complete is based on total size of the disks and storage performance at both sites.
   - After the synchronization completes, the VPG enters the Meeting SLA state.
4. Perform a Move operation to fail back the virtual machines to the original protected site.
5. In the Move wizard, in the EXECUTION PARAMETERS tab, for commit policy, set the commit policy to enable basic testing before the move is committed.

The virtual machines are recovered at the original protected site, and the VPG enters a Delta Sync phase before it enters a Meeting SLA state.

Using a Failover Operation - Failover Considerations

- The originally protected disks are maintained for a faster failback.
- Using the Failover operation for testing is non-intuitive.
- Testing by using the Failover operation requires performing manual procedures, such as shutting down the protected virtual machines.
- During the testing period, there is no protection for the recovered machines.
Testing Recovery

Using a Clone Operation

Use the Clone operation when the protected application must continue to run throughout the test. Create a clone of the virtual machines in a VPG on the recovery site to a specific point-in-time. The clone is a copy of the protected virtual machines on the recovery site, while the virtual machines on the protected site remain protected and live. The Clone operation is described in “The Clone Operation”, on page 271 and in “Cloning a VPG to the Recovery Site”, on page 305.

The cloned virtual machines are independent of Zerto Virtual Replication. At the end of the test you can remove these machines or leave them.

- You use the Clone operation when the source application has to continue throughout the test.
- You can create a clone of the virtual machines in a VPG on the peer site to a specific point-in-time.
- The clone is a copy of the protected virtual machines on the recovery site, while the virtual machines on the protected site remain protected and live.
- The Clone operation is described above, and in the Zerto Virtual Manager Administration Guide for the VMware vSphere Environment.
- The cloned virtual machines are independent of Zerto Virtual Replication. At the end of the test you can remove these machines or leave them.

Using a Clone Operation - Clone Considerations

- You can clone to a specific point-in-time.
- There is no protection for the cloned machines.
- After use of the clone ends, no changes made to the cloned virtual machines are applied to the protected virtual machines.
- The original virtual machines on the source site are live and online throughout the test.
CHAPTER 15: MIGRATING A VPG TO A RECOVERY SITE

This chapter describes a planned migration of a VPG to a remote site. The following topics are described in this chapter:

- “The Move Process”, below
- “Moving Protected Virtual Machines to a Remote Site”, on page 286
- “Reverse Protection For a Moved VPG”, on page 291

**Note:** You cannot perform a move while a backup job is running.

### The Move Process

Use the Move operation to move groups of protected virtual machines from a protected site to a recovery site in a planned migration.

When you perform a planned migration of virtual machines to a recovery site, Zerto Virtual Replication assumes that both sites are healthy and that you plan to relocate the virtual machines in an orderly fashion without loss of data.

**Note:** To recover virtual machines on the recovery site during disaster recovery, see “Managing Failover”, on page 295.

The MOVE operation has the following basic steps:

- Shutting down the protected virtual machines gracefully. This ensures data integrity.
  
  If the machines cannot be gracefully shut down, for example, when VMware Tools or Microsoft Integration Services is not available, you must manually shut down the machines before starting the Move operation or forcibly power off the virtual machines as part of the Move operation. If the machines cannot be gracefully shut down automatically and are not shut down manually and the Move operation does not forcibly power them off, the Move operation stops and Zerto Virtual Replication rolls back the virtual machines to their original status.

- Inserting a clean checkpoint. This avoids potential data loss since the virtual machines are not on and the new checkpoint is created after all I/Os have been written to disk.

- Transferring all the latest changes that are still in the queue to the recovery site, including the new checkpoint.

- Creating the virtual machines in the recovery site and attaching each virtual machine to its relevant virtual disks, based on the last checkpoint.

  Also, as long as the virtual machines are created, the operation is considered successful, even if the virtual machines are not created with their complete definition, for example re-IP cannot be performed.

- Preventing automatically moving virtual machines to other hosts: Setting HA to prevent DRS. This prevents automatic vMotioning of the affected virtual machines during the Move operation.

- Powering on the virtual machines making them available to the user. If applicable, the boot order defined in the VPG settings is used to power on the machines.

  **Note:** If the virtual machines do not power on, the process continues and the virtual machines must be powered on manually. The virtual machines cannot be powered on automatically in a number of situations, such as when there are not enough resources in the resource pool, or the required MAC address is part of a reserved range, or there is a MAC address conflict or IP conflict, for example, if a clone was previously created with the MAC or IP address.

- Committing the Move operation. The default is to automatically commit the Move operation without testing. However, you can also run basic tests on the machines to ensure their validity to the clean checkpoint. Depending on the commit/rollback policy that you specified for the operation, the operation is committed, finalizing the move, or rolled back, aborting the operation.

- If Keep Source VMs is not selected, the protected virtual machines are removed from the inventory.

  **Note:** If Keep Source VMs is not selected, and the virtual machines or vCD vApp are already protected in other VPGs, continuing with the operation will cause the virtual machines or vCD vApp to be deleted from other VPGs that are protecting them and to the journals of these VPGs to be reset. In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be removed.
If reverse protection is not possible, the original protected site virtual machines or vCD vApp are not powered off and removed.

Protecting virtual machines or vCD vApps 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.

- Promoting the data from the journal to the machines. The machines can be used during the promotion and Zerto Virtual Replication ensures that the user sees the latest image, even if this image, in part, includes data from the journal.
  
  **Note:** Virtual machines cannot be moved to another host during promotion. If the host is rebooted during promotion, make sure that the VRA on the host is running and communicating with the Zerto Virtual Manager before starting up the recovered virtual machines.

- If reverse protection is specified, the virtual disks used by the virtual machines in the protected site are used for the reverse protection. A Delta Sync is performed to make sure that the two copies, the new recovery site disks and the original protected site disks, are consistent. A Delta Sync is required since the recovered machines can be updated while data is being promoted.

  If reverse protection is not specified, the VPG definition is saved but the state is **Needs configuration** and the virtual disks used by the virtual machines in the protected site are deleted. Thus, in the future if reverse protection is required, the original virtual disks are not available and an initial synchronization is required.

  **Note:** If reverse protection is specified, the **Keep Source VMs** option is grayed out because the virtual disks of the VMs are used for replication and cannot have VMs attached. If **Keep Source VMs** is selected before reverse protection is specified, the **Keep Source VMs** selection is canceled.

A move differs from a failover in that with a move you cannot select a checkpoint to restore the virtual machine to. Also, to ensure data integrity, the protected virtual machines are powered off completely and a final checkpoint created so that there is no data loss before the move is implemented.

You can initiate the Move operation from either the protected site or recovery site.
Moving Protected Virtual Machines to a Remote Site

You can move the virtual machines in a virtual protection group (VPG) to a remote site, where the virtual machines are replicated. As part of the process you can also set up reverse protection, where you create a VPG on the remote site for the virtual machines being moved, pointing back to the original site. This is commonly used, for example, when the protected site has planned downtime.

To initiate a move:

1. In the Zerto User Interface select ACTIONS > MOVE VPG.
   The Move wizard is displayed.

2. Select the VPGs to move.
   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.

You can change the following values to use for the recovery:

- Commit Policy
Moving Protected Virtual Machines to a Remote Site

- **Force Shutdown** policy
- **Reverse Protection** settings
- **Keep Source VMs** settings

You can also see if a **Boot Order** and **Scripts** are defined for the VPG.

4. To change the commit policy, click on the field or select the VPG and click **EDIT SELECTED**.

   ![Dropdown menu with options](image)

   a) To commit the recovery operation **automatically**, with **no** testing, select **Auto-Commit** and **0** minutes.
   b) Select **None** if you do **not** want an automatic commit or rollback. You must manually commit or roll back.
   c) To test **before** committing or rolling back, specify an **amount of time** to test the recovered machines, in minutes. This is the amount of time that the commit or rollback operation is **delayed**, before the automatic commit or rollback action is performed.

   During this time period, check that the new virtual machines are OK and then commit the operation or roll it back.

   The maximum amount of time you can **delay** the commit or rollback operation is **1440 minutes**, which is **24 hours**.

   Testing that involves I/O is done on **scratch volumes**.
   - The more I/Os generated, the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done.
   - The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed.
   - The scratch volumes reside on the storage defined for the journal.

5. To force a shutdown of the virtual machines, click the **Force Shutdown** checkbox. If the virtual machines cannot be gracefully shut down, for example if VMware Tools is not installed on one of the virtual machines in the VPG, the Move operation fails unless you specify that you want to force the shutdown. If a utility is installed on the protected virtual machines, the procedure waits five minutes for the virtual machines to be gracefully shut down before forcibly powering them off.

6. To specify reverse protection, where the virtual machines in the VPG are moved to the recovery site and then protected in the recovery site, back to the original site, double-click the Reverse Protection field and click the **REVERSE** link.

   The Edit Reverse VPG wizard is displayed.
   - You can edit the reverse protection configuration. The parameters are the same as described when you create a VPG, described in "Protecting Virtual Machines from a vCenter Server", on page 39, with the following differences:
     - You cannot add or remove virtual machines to the reverse protection VPG.
     - By default, reverse protection is to the original protected disks. You can specify a different datastore to be used for the reverse protection.
     - If VMware Tools are available, for each virtual machine in the VPG, the IP address of the originally protected virtual machine is used. Thus, during failback the original IP address of the virtual machine on the site where the machine was originally protected is reused. However, if the machine does not contain the utility, DHCP is used.
     - The host version must be 4.1 or higher for re-IP to be enabled.

7. To **prevent** the protected virtual machines or vCD vApp from being **deleted** in the protected site, click the **Keep source VMs** checkbox.

   **IMPORTANT:**
   - The **virtual machines** or **vCD vApp** will be **removed** from the other **VPGs** that are protecting them if the following conditions apply:
     - The virtual machines or vCD vApp are already protected in other VPGs
     - Reverse protection is specified
     - **Keep Source VMs** is not checked
   - If your VPG has a vCD vApp, or if there are no other virtual machines left to protect, the entire **VPG** will be **removed**.

   Protecting virtual machines or vCD vApps 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.

8. Click **NEXT**.
- A warning appears informing the user that the virtual machines or vCD vApp will be removed from the other VPGs that are protecting them.
- If your VPG has a vCD vApp, or if there are no other virtual machines left to protect, the entire VPG will be removed.
- When reverse protection is specified for a VPG residing on a vCD site that is replicating to either a vSphere or Hyper-V site, the boot order settings will not reserve the start delay vCD vApp settings for virtual machines with the same order number.

The MOVE step is displayed. The topology shows the number of VPGs and virtual machines being moved to each peer site. In the following example, 2 VPGs will be moved to Site6-Ent2-R2, and they contain 5 virtual machines; and 1 VPG will be moved to Site5-Ent2-P2-R2 and it contains 2 virtual machines.

9. Click **START MOVE** to start the migration.
   A warning message appears, presenting a summary of your Commit Policy.
10. Review the Commit Policy summary, and either click **Change Settings**, or click **START MOVE** to start the migration.
11. If a commit policy was set with a timeout greater than zero, as described in step 4, you can check the moved virtual machines on the recovery site before they are removed from the protected site.
Moving Protected Virtual Machines to a Remote Site

12. Check the virtual machines on the recovery site, then either:

   - Wait for the specified **Commit Policy** time to elapse, and the specified operation, either **Commit** or **Rollback**, is performed automatically.

   - Or, in the specific VPG tab, click the Commit or Rollback icon (✓

     ).

     - Click **Commit** to confirm the commit and, if necessary set, or reset, the reverse protection configuration. If the protected site is still up and you can set up reverse protection, you can reconfigure reverse protection by checking the Reverse Protection checkbox and then click the Reverse link. Configuring reverse protection here overwrites any of settings defined when initially configuring the failover.

     - Click **Rollback** to roll back the operation, removing the virtual machines that were created on the recovery site and rebooting the machines on the protected site. The Rollback dialog is displayed to confirm the rollback.

**Note:** If a virtual machine exists on the recovery site with the same name as a virtual machine being migrated, the machine is moved and named in the peer site with a number added as a suffix to the name, starting with the number 1.

The status icon changes to orange and an alert is issued, to warn you that the procedure is waiting for either a commit or rollback.

All testing done during this period, before committing or rolling back the Move operation, is written to thin-provisioned virtual disks, one per virtual machine in the VPG. These virtual disks are automatically defined when the machines are created on the recovery site for testing. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the storage defined for the journal. Using these scratch volumes makes committing or rolling back the Move operation more efficient.

**Note:** You cannot take a snapshot of a virtual machine before the Move operation is committed and the data from the journal promoted to the moved virtual machine disks, since the virtual machine volumes are still managed by the VRA and not directly by the virtual machine. Taking a snapshot of a machine that is in the process of being moved will corrupt that machine.
You can also commit or roll back the operation in the **TASKS** popup dialog in the status bar or under **MONITORING > TASKS**.

After the virtual machines are up and running and committed in the recovery site, the powered off virtual machines in the protected site are removed from the protected site. Finally, data is promoted from the journal to the moved virtual machines.

**Notes:**

- If virtual machines or vCD vApp are already protected in **several VPGs**, and reverse protection is configured, the **virtual machines or vCD vApp are deleted** from the protected site. This will result in the **removal of these virtual machines from other VPGs** that are protecting them and to the journals of these VPGs to be reset. In the event of vCD vApp or if no other virtual machines are left to protect, the **entire VPG will be removed**.

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.

- If **Keep Source VMs** is selected, the protected virtual machines are not removed from the protected site.

Protecting virtual machines or vCD vApps 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.

During promotion of data, you cannot move a host on the moved virtual machines. If the host is rebooted during promotion, make sure that the VRA on the host is running and communicating with the Zerto Virtual Manager before starting up the recovered virtual machines.

**Note:** If the virtual machines do not power on, the process continues and the virtual machines must be manually powered on. The virtual machines cannot be powered on automatically in a number of situations, such as when there are not enough resources in the resource pool or the required MAC address is part of a reserved range or there is a MAC address conflict or IP conflict, for example, if a clone was previously created with the MAC or IP address.

When a vCD vApp is moved to a vCenter Server recovery site, a vCenter Server vCD vApp is created in the recovery site. If reverse protection was specified, the VPG state is **Needs Configuration** and the VPG must be recreated by protecting the virtual machines in the vCD vApp as separate machines and not as part of the vCD vApp.
Conversion considerations for a **protected virtual machine in vSphere** when it is **recovered in Hyper-V**:

- A machine using BIOS is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine using EUFI is recovered in Hyper-V as a Generation 2 virtual machine.
- A machine with a 32bit operating system is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine with a 64bit operating system is recovered in Hyper-V as either a Generation 1 or Generation 2 virtual machine, dependent on the operating system support in Hyper-V.
- The boot disk is ported to a disk on an IDE controller. The boot location is 0:0.
- A virtual machine using up to 4 SCSI controllers is recovered as a virtual machine with 1 SCSI controller.
- The virtual machine NICs are recovered with Hyper-V network adapters except for protected Windows 2003 virtual machines which are recovered with Hyper-V legacy network adapters.
- When VMware Tools is installed on the protected virtual machine running Windows Server 2012, Integration Services is installed on the recovered virtual machine automatically.
- RDM disks are replicated to Hyper-V vhd or vhdx disks, and not to Pass-through disks.

### Reverse Protection For a Moved VPG

When moving the virtual machines in a VPG you specify whether you want reverse protection from the recovery site back to the original protected site.

#### Reverse Protection Specified

When you specify reverse protection, the virtual machines are moved to the recovery site and then protected using the values specified during the move. Data is promoted from the journal to the moved virtual machines and then synchronization with the original site is performed so that the VPG is fully protected. The synchronization performed uses the original protected disks and is either a **Delta Sync** or, if there is only one volume to synchronize, a **Volume Delta Sync**. A sync is required since the recovered machines can be updated while data is being promoted.

#### Reverse Protection Not Specified

If you do not specify reverse protection, the protected disks are removed along with the protected virtual machines at the end of the procedure. In this case, if you want to move the virtual machines back again to the original site, you will not be able to use the original disks and an initial synchronization will have to be performed. The VPG definition is kept with the status **Needs Configuration** and the reverse settings in the VPG definition are not set.
Clicking EDIT VPG displays the Edit VPG wizard with the settings filled in, using the original settings for the virtual machines in the VPG from the original protected site, except for the volumes, since the last step of the Move operation is to delete the virtual machines from the original protected site inventory, including the disks. To start replicating the virtual machines in the VPG, specify the disks to use for replication and optionally, make any other changes to the original settings and click DONE. An initial synchronization is performed.

**Notes:**
- If Keep Source VMs is not selected, and virtual machines or vCD vApp are already protected in several VPGs, the virtual machines or vCD vApp are deleted from the protected site. This will result in the removal of these virtual machines from other VPGs that are protecting them and to the journals of these VPGs to be reset. In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be removed. Protecting virtual machines or vCD vApps 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.
- You can edit the VPG definition from either of the sites, the site where the VPG virtual machines were initially protected or the site they were moved to.
- When reverse protection is specified for a VPG residing on a vCD site that is replicating to either a vSphere or Hyper-V site, the boot order settings will not reserve the start delay vCD vApp settings for virtual machines with the same order number.
CHAPTER 16: MIGRATING ZERTO VIRTUAL REPLICATION TO A NEW VIRTUAL MACHINE

This section describes how to migrate the Zerto Virtual Replication (ZVR) application to a new Virtual Machine.

When ZVR is installed, the installation includes the following:

- **Zerto Virtual Manager (ZVM):** A Windows service, Zerto Virtual Manager service, that manages the replication at the site level.
- **Virtual Replication Appliance (VRA):** A virtual machine installed on each Hyper-V hosting virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.
- **Virtual Backup Appliance (VBA):** A Windows service that manages back-ups within Zerto Virtual Replication. The VBA service runs on the same machine as the Zerto Virtual Manager service and manages 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 in a browser.

**Before you Begin**

From the **Source VM**, make a note of the following information which you will need later:

- Make a note of the exact Zerto Virtual Replication installation configuration settings.
- Navigate to **Control Panel > Network and Internet**, and make a note of the IP address
- If a DNS name was used instead of an IP address, make a note of the DNS name

**IMPORTANT:**

- The Optional steps that are included in the procedure below are **highly recommended**.
- Perform them before connecting the new ZVM to peer ZVM sites, in order to verify that the ZVM on the target VM is working correctly, and with the correct configurations.
- If the ZVM on the target VM is not working correctly with the correct configurations, **VPGs could be automatically deleted**.

**To migrate ZVR to a target VM:**

1. Prepare the **target VM** for the ZVR. To do this, review the machine requirements to install ZVR, and make sure that the target VM complies with these **minimum requirements**. For these details, see Zerto Virtual Replication Installation Guide for your environment, in the section **Installing Zerto Virtual Replication**.

2. On the **source VM**, verify which version of the Zerto Virtual Replication Installer file is currently installed, and then copy and paste that same version to the **target VM**.

3. On the **source VM**, stop all Zerto related services:
   - Zerto Virtual Manager Service
   - Zerto Virtual Backup Appliance Service
   - Zerto Remote Log Collection Service

4. On the **source VM**, navigate to the **Zerto installation** folder and copy the entire folder, including all its contents. By default, this folder is named **Zerto Virtual Replication**.
   - **TIP:** To save space, you can leave out, or delete old log files which are no longer relevant. Navigate to the path: \Zerto Virtual Replication\logs\.

5. On the **target VM**, create a **temp** folder, and into this folder paste the entire **Zerto installation** folder, including all its contents, which you copied in 4.

6. **(Optional)** If **Backup** was configured and used with local repository, do the following:
   a) On the **source VM**, copy the entire Backup folder, including contents and sub folders.
   b) On the **target VM**, navigate to the relevant path, and paste the Backup folder.
   c) Repeat for each Backup folder that you need to manually back up.
   d) Do not proceed to 7 until you have copied all the relevant Backup folders.
Migrating Zerto Virtual Replication to a New Virtual Machine

**Note:** Previous Backups can also be manually copied to the target VM, but this must be done before 7.

7. On the **source** VM, first change the IP address to a different IP address, then disconnect the source VM network connection.

8. On the **target** VM, run the ZVM Installer and complete the installation with the same settings and configurations as the ZVM that was installed on the source VM.
   - If the ZVM on the **source** VM was configured to use VCD, and in addition the amqp service was installed, then on the **target** VM, the same amqp services must be reinstalled. These are the following:
     - amqp_installer
     - Erlang
     - RabbitMQ

9. On the **target** VM, stop all Zerto related services:
   - Zerto Virtual Manager Service
   - Zerto Virtual Backup Appliance Service
   - Zerto Remote Log Collection Service

10. **(Optional)** On the **target** VM, open the Windows Firewall and configure a new rule to block all outgoing TCP traffic on ports 9080 and 9081.

11. On the **target** VM, navigate to the temp folder which you created in 5 and copy the entire Zerto installation folder, then navigate to the Zerto installation folder which was created when you ran the ZVM installer, and paste and overwrite all files.

12. On the **target** VM, navigate to Control Panel > Network and Internet, and set the **target VM’s IP address** the same IP address as original IP address of the source VM.
   - If a DNS name was used instead of the IP address, set the **target VM’s DNS name** the same DNS name as the source VM.

13. **(Optional)** If the Log Archiver functionality was configured and in use on the **source** VM, make sure to create a folder on the **target** VM to which the logs are archived.

14. On the **target** VM, start all Zerto related services:
   - Zerto Virtual Manager Service
   - Zerto Virtual Backup Appliance Service
   - Zerto Remote Log Collection Service

15. **(Optional)** On the **target** VM, perform the following **optional validations**:
   a) Open an Internet browser, enter the URL https://localhost:9669, and log into the ZVM.
   b) If you blocked all outgoing TCP traffic on ports 9080 and 9081 as described in 10, make sure all the VPGs are present. Their state should be Error or Site disconnection, as there should be no connection to the peer ZVM sites.
   c) Make sure that the VRA status is Installed.
   d) Open the Windows Firewall and re-enable traffic for ports 9080 and 9081.

16. From anywhere in the network, log into the ZVM GUI and verify that the status of the VPGs and VRAs is OK.
   - If a DNS name was used instead of an IP address, it might take a while for the correct routing to occur. The sites will remain with the status disconnected until the correct routing occurs.

17. If the status of all the VPGs and VRAs is OK, first power off and then delete the source VM as it is no longer in use.
This section describes how to perform a failover to the recovery site after an unforeseen disaster. The following topics are described in this section:

- The Failover Process
- Initiating a Failover
- Reverse Protection for a Failed Over VPG
- What Happens When the Protected Site is Down
- Initiating a Failover During a Test

Note: If you need to perform a failover while a backup job is running, the backup job is aborted to enable the failover to run.

The Failover Process

Use the Failover operation following a disaster to recover protected virtual machines to the recovery site.

Note: You can also move virtual machines from the protected site to the recovery site in a planned migration. For details, see “Migrating a VPG to a Recovery Site”, on page 284.

When you set up a failover you always specify a checkpoint to which you want to recover the virtual machines. When you select a checkpoint – either the last automatically generated checkpoint, an earlier checkpoint, or a tagged checkpoint – Zerto Virtual Replication makes sure that the virtual machines at the remote site are recovered to this specified point-in-time. By setting a commit policy that enables checking the recovered machines before committing the failover, you can check the integrity of the recovered machines. If the machines are OK, you can commit the failover. Otherwise, you can roll back the operation and then repeat the procedure using a different checkpoint.

The Failover operation has the following basic steps:

- If the protected site or Zerto Virtual Manager is down, the process continues with the next step.
  - If the protected site or Zerto Virtual Manager is still running, the failover requirements are determined:
    - If the default is requested, doing nothing to the protected virtual machines, the Failover operation continues with the next step.
    - If shutting down the protected virtual machines is requested and the protected virtual machines do not have VMware Tools available, the Failover operation fails.
    - If forcibly shutting down the protected virtual machines is requested, the protected virtual machines are shut down and the Failover operation continues with the next step.
  - Creating the virtual machines at the remote site in the production network and attaching each virtual machine to its relevant virtual disks, configured to the checkpoint specified for the recovery.
    - Also, as long as the virtual machines are created, the operation is considered successful, even if the virtual machines are not created with their complete definition, for example re-IP cannot be performed.
      Note: The original protected virtual machines are not touched since the assumption is that the original protected site is down.
  - Preventing automatically moving virtual machines to other hosts: Setting HA to prevent DRS. This prevents automatic vMotioning of the affected virtual machines during the Failover operation.
  - Powering on the virtual machines making them available to the user. If applicable, the boot order defined in the VPG settings is used to power on the machines.
    - Note: If the virtual machines do not power on, the process continues and the virtual machines must be manually powered on. The virtual machines cannot be powered on automatically in a number of situations, such as when there are not enough resources in the resource pool or the required MAC address is part of a reserved range or there is a MAC address conflict or IP conflict, for example, if a clone was previously created with the MAC or IP address.
  - The default is to automatically commit the Failover operation without testing. However, you can also run basic tests on the machines to ensure their validity to the specified checkpoint. Depending on the commit/rollback policy that you specified
for the operation, after testing either the operation is committed, finalizing the failover, or rolled back, aborting the operation.

- If the protected site is still available, for example, after a partial disaster, and Reverse Protection is possible and specified for the Failover operation, the protected virtual machines are powered off and removed from the inventory. The virtual disks used by the virtual machines in the protected site are used for reverse protection. A Delta Sync is performed to make sure that the two copies, the new target site disks and the original site disks, are consistent. A Delta Sync is required since the recovered machines can be updated while data is being promoted.

If reverse protection is selected, and the virtual machines or vCD vApp are already protected in other VPGs, continuing with the operation will cause the virtual machines or vCD vApp to be deleted from other VPGs that are protecting them and to the journals of these VPGs to be reset. In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be removed.

If reverse protection is selected, and the virtual machines or vCD vApp are already protected in other VPGs, continuing with the operation will cause the other VPGs protecting the same virtual machines or vCD vApp to pause the protection. In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be removed. To resume the VPGs protection, you must edit the VPGs on the other sites and remove the virtual machine that was failed over from the protected site.

Note: If reverse protection is not possible, the original protected site virtual machines or vCD vApp are not powered off and removed.

Protecting virtual machines or a vCD vApp 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.

- The data from the journal is promoted to the machines. The machines can be used during the promotion and Zerto Virtual Replication ensures that the user sees the latest image, even if this image, in part, includes data from the journal.
  Note: Virtual machines cannot be moved to another host during promotion. If the host is rebooted during promotion, make sure that the VRA on the host is running and communicating with the Zerto Virtual Manager before starting up the recovered virtual machines.

**Failback after the Original Site is Operational**

To fail back to the original protected site, the VPG that is now protecting the virtual machines on the recovery site has to be configured and then a Delta Sync is performed with the disks in the original protected site. Once the VPG is in a protecting state the virtual machines can be moved back to the original protected site, as described in “Migrating a VPG to a Recovery Site”, on page 284.

**Initiating a Failover**

You can initiate a failover, whereby the virtual machines in the virtual protection group (VPG) are replicated to a set checkpoint in the recovery site. As part of the process you can also set up reverse protection, whereby you create a VPG on the recovery machine for the virtual machines being replicated, pointing back to the protected site.

You can initiate a failover to the last checkpoint recorded in the journal, even if the protected site is no longer up. You can initiate a failover during a test, as described in “Initiating a Failover During a Test”, on page 304.

If you have time to initiate the failover from the protected site you can. However, if the protected site is down, you initiate the failover from the recovery site.

Note:
- If a virtual machine is protected in several VPGs, and Reverse Protection is selected, the virtual machine is removed from all of the VPGs containing the virtual machine. The journals of these VPGs are reset.
  If a vCD vApp is protected in several VPGs, and reverse protection is selected, all VPGs containing the vCD vApp are deleted.
  If Reverse Protection is selected, and the virtual machines or vCD vApp are already protected in other VPGs, continuing with the operation will cause the other VPGs protecting the same virtual machines or vCD vApp to pause the protection.
In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be removed. To resume the VPGs protection, you must edit the VPGs on the other sites and remove the virtual machine that was failed over from the protected site.

Protecting virtual machines or a vCD vApp 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.

- Any VPGs that are in the process of being synchronized, cannot be recovered, unless the synchronization is a bitmap synchronization.

To initiate a failover:

1. In the Zerto User Interface set the operation to LIVE and click FAILOVER.
   The Failover wizard appears.

2. Select the VPGs to failover. 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 window is displayed.

You can change the following values to use for the recovery:

- Commit Policy
- Checkpoint to use
Initiating a Failover

- **Force Shutdown**
- **Reverse Protection** settings

In this window you can also see if a **Boot Order** and **Scripts** are defined for the VPG.

4. By default, the last checkpoint added to the journal is displayed in the Checkpoint column
   - To use this checkpoint, proceed to the next step.
   - To change the checkpoint, click the link that appears as the checkpoint.

   A window appears, displaying a list of the VPGs’ checkpoints.

- **Latest**: Recovery is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery.

   When selecting the latest checkpoint, the checkpoint used is the latest at this point.

   If a checkpoint is added between this point and starting the failover, this later checkpoint is not used.

- **Latest Tagged Checkpoint**: The recovery operation is to the latest checkpoint added in one of the following situations:
  - By a user.
  - When a failover test was previously performed on the VPG that includes the virtual machine.
  - When the virtual machine was added to an existing VPG after the added virtual machine was synchronized.

5. To use a checkpoint which is not the latest checkpoint, or the latest tagged checkpoint, choose **Select from all available checkpoints**. By default, this option displays all checkpoints in the system. You can choose to display only automatic, or tagged checkpoints, or any combination of these types.

6. Click **OK**.

7. To change the **commit policy**, click the field or select the VPG and click **EDIT SELECTED**.

   a) To commit the recovery operation automatically, with no testing, select **Auto-Commit** and 0 minutes.
   b) Select **None** if you do not want an automatic commit or rollback. You must manually commit or roll back.
   c) To test before committing or rolling back, specify an amount of time to test the recovered machines, in minutes.

      This is the amount of time that the commit or rollback operation is delayed, before the automatic commit or rollback action is performed.

      During this time period, check that the new virtual machines are OK and then commit the operation or roll it back.

      The maximum amount of time you can delay the commit or rollback operation is 1440 minutes, which is 24 hours.

     Testing that involves I/O is done on scratch volumes.

      - The more I/Os generated, the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done.
      - The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed.
      - The scratch volumes reside on the storage defined for the journal.

8. To specify the **shutdown policy**, click the **VM Shutdown** field and select the shutdown policy:
   - **No** (default): The protected virtual machines are not touched before starting the failover. This assumes that you do not know the state of the protected machines, or you know that they are not serviceable.
   - **Yes**: If the protected virtual machines have VMware Tools available, the virtual machines are gracefully shut down, otherwise the Failover operation fails. This is similar to performing a Move operation to a specified checkpoint.
   - **Force Shutdown**: The protected virtual machines are forcibly shut down before starting the failover. This is similar to performing a Move operation to a specified checkpoint. If the protected virtual machines have VMware Tools available, the procedure waits five minutes for the virtual machines to be gracefully shut down before forcibly powering them off.

9. To specify **reverse protection**, whereby the virtual machines in the VPG are failed over to the recovery site and then protected in the recovery site, back to the original site, either:
Initiating a Failover

- Click **REVERSE PROTECT ALL**. This activates reverse protection on all the VPGs that you plan to failover. The system default values for this procedure will be assigned to all the VPGs.
  - Or -
- Click the **Reverse Protection** field and select **REVERSE**.

  ![Reverse Protection Field](image)

  a) To configure the VPG for reverse protection, click the **REVERSE** link. The **Edit Reverse VPG** wizard is displayed.

  ![Edit Reverse VPG Wizard](image)

  You can edit the reverse protection configuration. The parameters are the same as described when you create a VPG, described in “Protecting Virtual Machines from a vCenter Server”, on page 39, with the following differences:

  - You cannot add or remove virtual machines to the reverse protection VPG.
  - By default, reverse protection is to the **original protected disks**. You can specify a different storage to be used for the reverse protection.
  - If VMware Tools is available, for each virtual machine in the VPG, the IP address of the originally protected virtual machine is used. Thus, during failback the original IP address of the virtual machine on the site where the machine was originally protected is reused. However, if the machine does not contain the utility, DHCP is used.
  - The host version must be 4.1 or higher for re-IP to be enabled.

**IMPORTANT:**

- The **virtual machines or vCD vApp** will be **removed** from the **other VPGs** that are protecting them if the following conditions apply:
  - The virtual machines or vCD vApp are already protected in other VPGs
  - Reverse protection is specified
- If your VPG has a vCD vApp, or if there are no other virtual machines left to protect, the **entire VPG will be removed**.
- If **Reverse Protection** is selected, and **the virtual machines or vCD vApp** are already protected in other VPGs, continuing with the operation will cause the **other VPGs protecting the same virtual machines or vCD vApp to pause the protection**. In the event of a vCD vApp or if no other virtual machines are left to protect, the **entire VPG will be removed**. To resume the VPGs protection, you must edit the VPGs on the other sites and remove the virtual machine that was failed over from the protected site.

Protecting virtual machines or vCD vApps 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.

When committing the failover, you can reconfigure reverse protection, regardless of the reverse protection settings specified here.

When reverse protection is specified for a VPG residing on a vCD site that is replicating to either a vSphere or Hyper-V site, the boot order settings will not reserve the start delay vCD vApp settings for virtual machines with the same order number.

10. Click **NEXT**.
  - A warning appears informing the user that the **virtual machines or vCD vApp** will be **removed** from the **other VPGs** that are protecting them.
  - If your VPG has a vCD vApp, or if there are no other virtual machines left to protect, the **entire VPG will be removed**.

11. Click **OK**. If a virtual machine is deleted from other VPGs, the journals of these VPGs are reset.
The **FAILOVER** step is displayed. The topology shows the number of VPGs and virtual machines being failed over to each recovery site. In the following example, 2 VPGs will be failed over to Site6-Ent2-R2, and they contain 5 virtual machines; and 1 VPG will be failed over to Site5-Ent2-P2-R2 and it contains 2 virtual machines.

12. Click **START FAILOVER**.

A warning message appears, presenting a summary of your Commit Policy.

13. Review the Commit Policy summary, and either click **Change Settings**, or click **START FAILOVER** to start the failover.

If a commit policy was set with a timeout greater than zero, you can check the failed over virtual machines on the recovery site before committing the failover operation.
The failover starts by creating the virtual machines in the recovery site to the point-in-time specified: either the last data transferred from the protected site or to one of the checkpoints written in the journal.

**Note:** If a virtual machine exists on the recovery site with the same name as a virtual machine being failed over, the machine is created and named in the peer site with a number added as a suffix to the name, starting with the number 1.

If the original protected site is still up and reverse protection is configured to use the protected virtual machines virtual disks, these virtual machines are powered off.

The status icon changes to orange and an alert is issued, to warn you that the procedure is waiting for either a commit or rollback.

All testing done during this period, before committing or rolling back the failover operation, is written to thin-provisioned scratch virtual disks. These virtual disks are automatically defined when the machines are created on the recovery site for testing. The longer the test period the more scratch volumes are used, until the maximum size is reached, at which point no more testing can be done. The maximum size of all the scratch volumes is determined by the journal size hard limit and cannot be changed. The scratch volumes reside on the same datastore defined for the journal. Using these scratch volumes makes committing or rolling back the failover operation more efficient.

**Note:** You cannot take a snapshot of a virtual machine before the failover operation is committed and the data from the journal promoted to the moved virtual machine disks, since the virtual machine volumes are still managed by the VRA and not directly by the virtual machine. Using a snapshot of a recovered machine before the failover operation has completed will result in a corrupted virtual machine being created.

14. Check the virtual machines on the recovery site, then either:

- Wait for the specified **Commit Policy** time to elapse, and the specified operation, either **Commit** or **Rollback**, is performed automatically.
- Or, in the specific VPG tab, click the Commit or Rollback icon ( ⬇️ ⬆️ ).
  a) If you clicked the **Commit** icon, the Commit window is displayed to confirm the commit and, if necessary set, or reset, the reverse protection configuration.
  - If the protected site is still up and you can set up reverse protection, you can reconfigure reverse protection by selecting the **Reverse Protection** checkbox and then click the **Reverse** link.
  - Configuring reverse protection at this point **overwrites** any of settings defined when initially configuring the move.
  b) If you clicked the **Rollback** icon, this rolls back the operation, **removing the virtual machines** that were created on the **recovery site** and reboots the machines on the protected site.
    The **Rollback** window is displayed to confirm the rollback.
    a) You can also commit or roll back the operation via the **TASKS** popup window in the status bar, or by selecting **MONITORING > TASKS**.

If the original protected site is still up and reverse protection is configured to use the virtual disks of the protected virtual machines, these virtual machines are **removed** from this site, unless the original protected site does not have enough **storage available** to fail back the failed over virtual machines. Finally, data is promoted from the journal to the recovered virtual machines.

**IMPORTANT:**

- If **Reverse Protection** is selected and the virtual machines or vCD vApp are already protected in other VPGs, the virtual machines or vCD vApp are **deleted** from the protected site and the **journals of these VPGs are reset**. This will result in the removal of these virtual machines from other VPGs that are protecting them, or the removal of the entire VPG, in the event of vCD vApp or if no other virtual machines are left to protect.
- If **Reverse Protection** is selected, and the virtual machines or vCD vApp are already protected in other VPGs, continuing with the operation will cause the other VPGs protecting the same virtual machines or vCD vApp to pause the protection. In the event of vCD vApp or if no other virtual machines are left to protect, the entire VPG will be **removed**. To resume the VPGs protection, you must edit the VPGs on the other sites and remove the virtual machine that was failed over from the protected site.

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.

During promotion of data, you cannot move a host on the recovered virtual machines. If the host is rebooted during promotion, make sure that the VRA on the host is running and communicating with the Zerto Virtual Manager before starting up the recovered virtual machines.
Managing Failover

By default the virtual machines are started with the same IPs as the protected machines in the protected site. If you do not specify Reverse Protection, the original machines still exist in the protected site and this can create clashes. In this case, Zerto recommends ensuring that a different IP is assigned to the virtual machines when they start, when configuring each virtual machine NIC properties in the VPG, during the definition of the VPG. For details, refer to “Protecting Virtual Machines from a vCenter Server”, on page 39. If you have defined the new virtual machines so that they will be assigned different IPs, the re-IP cannot be performed until the new machine is started. Zerto Virtual Replication changes the machine IPs and then reboots these machines with their new IPs.

Note: If the virtual machines do not power on, the process continues and the virtual machines must be manually powered on. The virtual machines cannot be powered on automatically in a number of situations, such as when there is not enough resources in the resource pool or the required MAC address is part of a reserved range or there is a MAC address conflict or IP conflict, for example, if a clone was previously created with the MAC or IP address.

When a vCD vApp is failed over to a vCenter Server recovery site, a vCenter Server vCD vApp is created in the recovery site. If Reverse Protection was specified, the VPG state is Needs Configuration and the VPG must be recreated by protecting the virtual machines in the vCD vApp as separate machines and not as part of the vCD vApp.

Conversion considerations for a protected virtual machine in vSphere when it is recovered in Hyper-V:

- A machine using BIOS is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine using UEFI is recovered in Hyper-V as a Generation 2 virtual machine.
- A machine with a 32bit operating system is recovered in Hyper-V as a Generation 1 virtual machine.
- A machine with a 64bit operating system is recovered in Hyper-V as either a Generation 1 or Generation 2 virtual machine, dependent on the operating system support in Hyper-V.
- The boot disk is ported to a disk on an IDE controller. The boot location is 0:0.
- A virtual machine using up to 4 SCSI controllers is recovered as a virtual machine with 1 SCSI controller.
- The virtual machine NICs are recovered with Hyper-V network adapters except for protected Windows 2003 virtual machines which are recovered with Hyper-V legacy network adapters.
- When VMware Tools is installed on the protected virtual machine running Windows Server 2012, Integration Services is installed on the recovered virtual machine automatically.
- RDM disks are replicated to Hyper-V vhd or vhdx disks, and not to Pass-through disks.

Reverse Protection for a Failed Over VPG

When you specify Reverse Protection, the following occurs:

- The virtual machines are recovered on the recovery site and then protected using the values specified during the failover.
- The original virtual machines are removed from the original protected site.
- On the target site the data is promoted from the journal to the recovered virtual machines
- The recovery site, which is now the protected site, is synchronized with the original protected site so that the VPG is fully protected.

The synchronization used is either a Delta Sync or if there is only one volume to synchronize, a Volume Delta Sync is performed. A sync is required since the recovered machines can be updated while data is being promoted.

Notes:

- For the Failover operation to complete successfully, when Reverse Protection is specified, the original protected site must have enough storage available to fail back the failed over virtual machines.
- When Reverse Protection is specified for a VPG residing on a vCD site that is replicating to either a vSphere or Hyper-V site, the boot order settings will not reserve the start delay vCD vApp settings for virtual machines with the same order number.
If you do not specify Reverse Protection, the VPG definition is kept with the status Needs Configuration and the reverse settings in the VPG definition are not set.

Clicking EDIT VPG displays the Edit VPG wizard with the settings filled in, using the original settings for the virtual machines in the VPG from the original protected site, except for the volumes. To start replicating the virtual machines in the VPG, specify the disks to use for replication and optionally, make any other changes to the original settings and click DONE.

Reverse Protection with One-to-Many

Zerto Virtual Replication enables you to protect virtual machines in a maximum of three VPGs. These VPGs cannot be recovered to the same site.

If Reverse Protection is selected, and the virtual machines are already protected in other VPGs, the following occurs:

- The virtual machines are deleted from the protected site.
- The replication of other VPGs containing these machines is paused.
- The recovery of all the virtual machines, including the virtual machine removed from the protected site, is possible.

To resume replication do the following:

1. Open the Edit VPG wizard.
2. Select the virtual machine that was previously deleted from the protected site.
3. Remove the virtual machine from the VPG.

If the protected VPG contains a vCD vApp, and the vCD vApp is protected in other VPGs, Reverse Protection is selected, the following occurs:

- The vCD vApp is deleted from the protected site.
- The vCD vApp is deleted from the other VPGs, and therefore can no longer be recovered.

VPGs enter a state of pause and pause replication if the following conditions apply:

- The ZVM on the protected and recovery sites are of version 5.5 and higher.
- The VRA installed on the recovery site is of version 5.5 and higher.

Protecting virtual machines or a vCD vApp in several VPGs is enabled if:

- The protected site and the recovery site are of version 5.0 and higher.
- The VRAs installed on these sites are of version 5.0 and higher.
What Happens When the Protected Site is Down

If the protected site is down, you can initiate the failover from the recovery site, as described above in "To initiate a failover," on page 297.

The specific VPG tab for a VPG shows whether recovery is possible.

If the Zerto Virtual Manager service is down the actual machines that are being protected can still be up, but they are only recoverable to the last checkpoint written before the Zerto Virtual Manager went down. If the vCenter Server is down, some of the protected virtual machines might not be protected.

When there is no connection with the protected site, the status for recovered VPGs is red with an Error status and green while recovery is being performed. If the protected site restarts so that Reverse Protection is possible, the status changes to orange.

Initiating a Failover During a Test

Replication continues during a test. If you need to initiate a failover during a test, you initiate the failover. The test stops to enable the failover and then a normal failover is performed, as described in "Initiating a Failover", on page 296. Any changes made to test the failover are not replicated, as only changes to the protected machines in the VPG are replicated.

Note: You cannot initiate a failover while a test is being initialized or closed.
You can create a clone of each virtual machine in a VPG. The clone is a copy of the protected virtual machine, located on the recovery site, while the virtual machine on the protected site remains protected and live.

The following topics are described in this chapter:

- “The Clone Process”, below
- “Cloning Protected Virtual Machines to the Remote Site”, on page 305

Note: You cannot clone virtual machines in a VPG test while a backup job is running. When the recovery site is vCD, the clone is created in vCenter Server and the virtual machines have to be manually imported into vCD.

The Clone Process

Use the Clone operation to create a copy of the VPG virtual machines on the recovery site. The virtual machines on the protected site remain protected and live.

The Clone operation has the following basic steps:

- Creating the cloned disks at the recovery site with the data from the journal to the specified checkpoint.
- Creating the virtual machines at the recovery site in the move/failover network and attach each virtual machine to its relevant cloned disks, configured to the checkpoint specified for the clone.

Note: The virtual machines are created without CD-ROM or DVD drives, even if the protected virtual machines have CD-ROM or DVD drives.

The cloned machines are named with the names of the protected machines, with the timestamp of the checkpoint used to create the clone. The cloned virtual machines are not powered on and are not protected by Zerto Virtual Replication.

Cloning Protected Virtual Machines to the Remote Site

You might want to create a clone if you need to have a copy of the virtual machines saved to a specific point-in-time, for example, when a VPG enters a Replication Paused state, or when testing a VPG in a live DR test.

To clone a VPG:

1. In the Zerto User Interface, in the VPGs tab click the name of the VPG to be cloned.

   A new tab is added to the Zerto User Interface, with the name of the VPG that you clicked. The tab displays data about the VPG.

   Note: If the VPG was previously viewed, and the tab for this VPG is still displayed, you can access the details by selecting the tab.

2. Select the new tab and click MORE > Offsite Clone.
When selecting the point to recover to:

- The refresh button is initially grayed out and is enabled for clicking after 5 seconds. It is also grayed out for 5 seconds after being clicked, before being re-enabled.
- A click the refresh button to view the latest checkpoints reminder is displayed 10 seconds after the refresh button is clicked to remind the user that there is a new Latest Checkpoint.
- If the user has scrolled to, and selected, a checkpoint anywhere in the checkpoints list, clicking the refresh button will automatically return the user to the selected checkpoint in the list.

4. Select the checkpoint to use:

5. By default, the last checkpoint added to the journal is displayed in the Checkpoint column

   - To use this checkpoint, proceed to the next step.
   - To change the checkpoint, click the link that appears as the checkpoint.

A window appears, displaying a list of the VPGs’ checkpoints.
Latest: Recovery is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery. When selecting the latest checkpoint, the checkpoint used is the latest at this point.

If a checkpoint is added between this point and starting the failover, this later checkpoint is not used.

Latest Tagged Checkpoint: The recovery operation is to the latest checkpoint added in one of the following situations:
- By a user.
- When a failover test was previously performed on the VPG that includes the virtual machine.
- When the virtual machine was added to an existing VPG after the added virtual machine was synchronized.

6. To use a checkpoint which is not the latest checkpoint, or the latest tagged checkpoint, choose Select from all available checkpoints. By default, this option displays all checkpoints in the system. You can choose to display only automatic, or tagged checkpoints, or any combination of these types.

7. Click OK.

8. Select the recovery datastore to use for the cloned virtual machines.

Note: All the cloned virtual machines use a single datastore, that is accessible by all the recovery site VRAs used by the VPG. In a vCD environment the datastore is selected from the list of available datastores that is accessible by all the recovery site VRAs and that has the most free space.

9. Click CLONE.

The cloning starts and the status is displayed in the VPG details tab.

The cloned machines are assigned the names of the protected machines with the addition of the timestamp of the checkpoint used for the clone. The cloned virtual machines are not powered on.

When cloning to VMware vSphere environments:
- The cloned virtual machines are created in the ZertoRecoveryFolder folder, and not the recovery folder defined in the VPG.
- The cloned virtual machines use a single datastore.
- The VMDKs are renamed (1).vmdk, (2).vmdk, etc.
- When the recovery site is VMware vCloud Director, the clone is created in vCenter Server and the virtual machines have to be manually imported into vCD.
- If the protected virtual machine has RDMs attached, these disks are always cloned as thin-provisioned VMDKs to the datastore specified in the Recovery Datastore field in the Edit VM dialog in the REPLICATION step in the Edit VPG wizard.
When cloning to Microsoft Hyper-V environments:

- The cloned virtual machines use a single storage.
- The VHDs are renamed (1).vhdx, (2).vhdx, etc.
CHAPTER 19: RECOVERING FILES AND FOLDERS

You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto Virtual Replication and running Windows operating systems. You can recover the files and folders from a specific point-in-time. Thus, you can recover files and folders for a virtual machine for as far back as the journal history is configured.

This section describes how to recover files and folders. The following topics are described in this section:

- “The File and Folder Recovery Process”, below
- “Recovering Files and Folders”, on page 310

The File and Folder Recovery Process

Use the RESTORE FILE operation to recover specific files and folders from the recovery site.

When you set up file and folder recovery, you always specify a checkpoint to which you want to recover the files and folders. When you select a checkpoint – either the last automatically generated checkpoint, an earlier automatically generated checkpoint, or a tagged checkpoint – Zerto Virtual Replication makes sure that the files and folders replicated at the remote site are recovered to this specified point-in-time.

The file and folder operation has the following basic steps:

1. Select the virtual machine that is protected, on which the files or folders to recover are located.
2. Select the checkpoint, at which the files and folders will be recovered.
3. Select the disk, which contains the files and folders to recover.
   - **Note:** You can only recover files and folders from one disk at a time.
4. Mount the selected disk.
5. Select the files and folders on the disk to recover.
6. Download the selected files and folders.
   - The files are downloaded to the machine where you run the Zerto User Interface.
   - Make sure that this machine has enough space for the recovered files.
7. Unmount the selected disk.

You can only recover files and folders from one disk at a time. After the required disk is mounted, if you want to recover files or folders from another disk, you can begin the mount process for the second disk. Zerto Virtual Replication does not support mounting the same volume twice, for example if you want a file from two different checkpoints.

**Considerations:**

- You cannot recover files or folders from a virtual machine when a test failover, live failover, move, clone, or backup is being performed on a VPG that contains the virtual machine.
- You cannot recover files or folders from the Zerto plugin.
- For File and Folder Restore **known issues**, see the Release Notes > Known Issues > File Level Restore.
- For a list of unsupported files, see the Interoperability Matrix.
Recovering Files and Folders

The procedure to recover files and folders involves the following steps:

1. “Mounting the Disk that Contains the Required Files and Folders”, on page 310
   
   **Note:** While the disk is mounted:
   - If you start a live failover or move, Zerto Virtual Manager forcibly unmounts the disk so the live failover or move can be performed.
   - Scheduled backups do not start.
   - Manual backups fail.
   - You can perform a test failover or clone.

2. “Downloading the Files and Folders from the Disk”, on page 313
   
   **Note:** When downloading, you may see grayed out files. These grayed out files are not supported files, and therefore cannot be selected. For a list of unsupported files see Zerto Virtual Replication - Interoperability Matrix for All Versions.

Mounting the Disk that Contains the Required Files and Folders

Before you can recover files or folders, you must first select the checkpoint in time from which you will recover the files or folders. Then you must select and access the disk in which the files or folders are contained.

**To mount a disk that includes files and folders to restore:**

1. From either the protected or recovery site, select ACTIONS > RESTORE FILE.
   The File and Folder Restore wizard is displayed.

   The list of all protected virtual machines is displayed. You can only recover files or folders from one virtual machine at a time.

   2. Select the virtual machine on which the file or folder is located and click NEXT.
The CHECKPOINT step is displayed. By default, all checkpoints are displayed.

3. Select the checkpoint from which to recover the file or folder.
   - **Auto:** Checkpoints generated by the Zerto Virtual Manager are displayed.
   - **Tagged:** Checkpoints that were added by a user, or were added by the Zerto Virtual Manager when a failover test was performed on the VPG that included the virtual machine, or when the virtual machine was added to an existing VPG after the virtual machine was synchronized.

4. Click **NEXT**.
   The DISK step is displayed. All disks associated with the selected virtual machine are displayed.
5. Select a disk to mount and click **NEXT**.
   The MOUNT step is displayed. The settings you selected are displayed.

6. Click **START MOUNT** to mount the disk.
   Mounting the disk may take some time, depending on the selected checkpoint and the number of files and folders on the disk.
   - When the first part of the restore process is done, icons appear next to the completed task.
   - By clicking the folder icon ( ■) you can browse the folders and files on the disk.
   - By clicking the unmount icon ( ■) you can unmount the disk without restoring any files or folders.

7. Continue with “**Downloading the Files and Folders from the Disk**” on page 313.
Recovering Files and Folders

Downloading the Files and Folders from the Disk

In this procedure you select the files and folders. The files are downloaded to the machine where you run the Zerto User Interface. Make sure that this machine has enough space for the recovered files.

To download folders or files:

1. Click the folder icon ( ).

The File and Folder Restore dialog is displayed.
2. Click **NEXT**.

   The **FILE/FOLDER** step is displayed.

   - Select the files and folders you want to download.

   **Note:** Grayed out files are not supported therefore cannot be selected. For a list of unsupported files, see the **Interoperability Matrix**. When a selected folder contains unsupported files, only the supported files will successfully download. Meaning, only the supported files will appear in the download folder.
The selected files or folders are displayed in the right pane of the dialog. The number of items selected is displayed and the size of the selected files is also displayed.

3. Click **NEXT**.
   The DOWNLOAD step is displayed. It shows the files and folders you selected for downloading.
   By default, when you select multiple files or one or more folders, the data is compressed before it is downloaded. If you select only one file, for download, you can choose whether or not the file is compressed.

4. Click **START DOWNLOAD**.
   The files and folders are downloaded by default to the downloads folder on the computer where you run the Zerto User Interface.
   When a selected folder contains unsupported files, only the supported files will successfully download. Meaning, only the supported files will appear in the download folder.
   **Note:** Saving the files and folders to a network share is dependent on the browser used to display the Zerto User Interface and the settings for this browser.
   - When you select one file to download, and do not compress the file, the name of the downloaded file is the name of the file. For example, if you download a file called **Important-file.docx**, the name of the file on your computer will be **Important-file.docx**.
   - When you choose one file and choose to compress it, or you select multiple files, the files are zipped into a file called **ZertoDownloads.zip**.
5. Zerto recommends that you **unmount the disk** after the files or folders are downloaded. To unmount the disk, click the unmount icon (■).
Zerto Virtual Replication enables recovering the virtual machines in a VPG from an offsite backup, up to one year back, to the recovery site.

The following topics are described in this chapter:
- “The Restore Process”, below
- “Restoring Virtual Machines”, on page 317

The Restore Process

Use the Restore operation to recover the VPG virtual machines on the recovery site from a backup job. The virtual machines on the protected site remain protected and live.

The Restore operation has the following basic steps:
1. The VBA accesses a specified backup, either by identifying the specific VPG that was backed up or by scanning a specified repository for offsite backups.
2. The VBA passes the offsite backup to the VRA.
   - **Note:** If backed up volumes were deleted after the backup was created, as long as there are still volumes to restore, the backup can continue, restoring the remaining volumes.
3. The VRA creates the virtual machines under the designated host and storage on the recovery site. The host and storage can be the same as the recovery host and storage specified in the VPG or any other host and associated storage in the site.
4. If requested, the restored virtual machines are powered on.

Restoring Virtual Machines

You can restore an offsite backup to the recovery site, either by specifying the VPG that has offsite backups or the repository where the backup was saved.

When the recovery site where the offsite backups are stored is managed by a cloud service provider using vCloud Director, only the cloud service provider can initiate the restore.
To restore a backup:

1. In the Zerto User Interface select ACTIONS > RESTORE BACKUP.
   The Restore from Zerto Backup wizard is displayed.

2. Select the VPG to restore from the backup list or the repository where the offsite backup was saved. If the VPG backups were saved to more than one repository, selecting the VPG collects all the offsite backups for the VPG from all the available repositories.
   
   **Note:** When restoring via the VPG backup option, the VPG must still be available. If the VPG was deleted, the restore must be performed from a repository.

3. Click NEXT.
   The RESTORE POINT step is displayed, showing all the available offsite backups.

   where:

   **Point in Time** – The date and time the offsite backup was performed.
Restoring Virtual Machines

4. Select the offsite backup to restore.

Selecting an offsite backup displays the list of virtual machines in the backup, including the following information:

**VM Name** – The name of the virtual machine in the package.

**Backup Status** – Whether the offsite backup of the virtual machine is complete or only partial, in which case only some of the volumes of the virtual machine were backed up.

**# Volumes Backed Up** – The number of backed up volumes out of the total number of volumes for the virtual machine.

**Note:** The number of offsite backups available depends on the frequency — daily or weekly — specified and the length of the retention period for the VPG. The exact number of offsite backups over time is described in “Offsite Backups”, on page 38.

5. If the restore site has the option to restore to vCD, select where to attach the restored VMs, either to VC or vCD.

6. Click NEXT.

The **VM SETTINGS** step is displayed.

7. You can specify the following default values, which are then applied to all the virtual machines to be restored:

**Restore on Host** – The IP address of the host where you want the virtual machine restored. After selecting a host the **Restore on Datastore** field is displayed.

**Restore on Datastore** – The datastore to use for the restored virtual machine files.

Alternatively, you can use the recovery host and storage specified for each virtual machine in the VPG definition by clicking **APPLY VPG CONFIGURATION**.

**Note:** The VPG must still be available to use **APPLY VPG CONFIGURATION**.
If you want to change the information in one field, click the field and update the information. If you want to change the host or datastore information for several virtual machines at the same time, select the virtual machines and click EDIT SELECTED.

The Configure VM Settings dialog is displayed.

![Configure VM Settings Dialog]

**Note:** If one or more of the backed up volumes was deleted after the backup was created, as long as there are still volumes to restore the backup can continue, restoring the remaining volumes.

You can specify the following values, which are then applied to all the selected virtual machines:

- **Restore on Host** - The IP address of the host where you want the virtual machines restored.
- **Restore on Datastore** - The datastore to use for the restored virtual machine files.
- **Power On** - Check this if you want the restored virtual machines to be powered on.

Alternatively, you can use the recovery host and storage specified for each virtual machine in the VPG definition by clicking APPLY VPG CONFIGURATION.

8. For each virtual machine, specify the volume information by clicking Volumes under Actions.

The Volumes dialog is displayed:

![Volumes Dialog]

9. If you want to edit information in a field, click the field and update the information. If you want to edit information for several datastores at the same time, select the datastores and click EDIT SELECTED.

The Edit Selected Volumes dialog is displayed.

![Edit Selected Volumes Dialog]

**Note:** If more than one datastore is selected, the path is not displayed.

10. Specify the datastore settings.

- **Datastore / Raw Disk** – The storage or RDM disk where the virtual machine files will be restored.
- **Thin** – Whether the virtual machine disks will be thin-provisioned or not.

11. Click SAVE.

12. Click DONE.
13. For each virtual machine, specify the NIC information by clicking NICs under Actions. The NICs dialog is displayed:

![NICs dialog](image)

14. If you want to edit information in one field, click the field and update the information. If you want to edit information for several virtual NICs at the same time, select the NICs and click **EDIT SELECTED**. The **Edit NIC** dialog is displayed.

![Edit NIC dialog](image)

15. Specify the NIC settings.

   **NIC Name** - The name of the selected NIC.

   **Network** - The network to use for the restored virtual machine.

   **Create new MAC address** - The Media Access Control address (MAC address) to use. The default is to use the same MAC address for the restored virtual machine that was used in the protected site. Check the box to create a new MAC address on the restore site.

   **Change vNIC IP Configuration** - Whether or not to keep the default virtual NIC (vNIC) IP configuration. You can only change the vNIC IP after the restore has completed with VMware Tools installed. If you select a static IP connection, you must set the IP address, subnet mask, and default gateway. Optionally, change the preferred and alternate DNS server IPs and the DNS suffix. If you select DHCP, the IP configuration and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

   **IP Address** - The IP for the restored virtual machine. This can be the same IP as the original protected virtual machine.

   **Subnet Mask** - The subnet mask for the network. The default value is **255.255.255.0**.

   **Default Gateway** - The default mask for the network.

   **Preferred DNS Server** - The IP address of the primary DNS server to handle Internet protocol mapping.

   **Alternate DNS Server** - The IP address of the alternate DNS server.
**DNS Suffix** – The DNS name excluding the host.

16. Click OK.
17. Click DONE.
18. Click NEXT.

The SUMMARY step is displayed. Check the details of the restore.

19. If this is the offsite backup you want to restore, click RESTORE.

The virtual machines are created from the repository at the recovery site.
Zerto Virtual Replication includes reporting for the following:

- “Outbound Protection Over Time Report”, below
- “Protection Over Time by Site Report”, on page 324
- “Recovery Reports”, on page 325
- “Resources Report”, on page 327
- “Monthly Usage Report” on page 331
- “VPG Performance Report”, on page 331
- “Backup Report”, on page 332

**Outbound Protection Over Time Report**

Information about how much data is actually being protected against the amount configured for any of the sites can be displayed in the *Outbound Protection Over Time* report under the REPORTS tab.

The data displayed can be up to 30 minutes old, since the Zerto Virtual Manager collects the relevant data every 30 minutes.

You can filter the information by the following:

**From** and **To**: The dates for which you want information.

**Recovery Site**: Select the site for which you want information or select all sites. If all sites are selected, **All** is displayed. The dropdown list displays all sites paired with the local site.

Click **APPLY** to apply the selected filtering and produce the report.

Click **RESET** to reset the display to the default values.
Zerto Virtual Manager Administration Guide for VMware vSphere Environments - Version 6.0
Zerto Virtual Replication Reports

Protection Over Time by Site Report

Information about the virtual machines and the amount of data on the recovery site can be displayed in the Protection Over Time by Site report under the REPORTS tab. When the report is displayed for the first time, information is shown per 30 minute intervals.

The data displayed can be up to 30 minutes old, since the Zerto Virtual Manager collects the relevant data every 30 minutes.

You can filter the information by the following:

**From** and **To**: Select the dates for which you want information.

**Protected Site**: Select the sites for which you want information. The list displays all sites paired with the local site.

**Resolution**: Select the resolution for the report: daily, weekly, monthly, or All.

Click **APPLY** to apply the selected filtering and produce the report.

Click **RESET** to reset the display to the default values.

**Note**: By default, the Protection Over Time By Site report is only available for the last 90 days.

Differences might occur between the value displayed in the **Used Journal** column in this report and the value displayed in the **Recovery Journal Used Storage** column retrieved from vCenter or Hyper-V in the Resources report.

The **Used Journal** value displayed here is calculated by the VRA, based on internal journal allocations for each recovery volume. vCenter and Hyper-V Resources reports are expected to display a larger size than in this report, and may reach up to 500MB per virtual machine higher than reported in this report.
Recovery Reports

Information about recovery operations — failover tests, moves, and failovers — can be displayed in Recovery Reports under the REPORTS tab.

The information includes the name of the user who initiated the report, which recovery operation, the point in time, protected and the recovery sites involved, when the recovery operation was started, when it ended, the time it took to bring up the machines in the recovery site, the RTO, whether the operation succeeded or not, the VPG recovery settings, the virtual machine recovery settings, and detailed recovery steps, and any notes added during a failover test.

Recovery Reports are always kept, and never deleted.

You can filter the tests by the following:
- **Dates**: The dates for which you want information. Only operations performed between these dates are displayed.
- **VPG**: Select the VPGs for which you want information. The number of VPGs you selected is displayed. If you select All, the total number of VPGs is shown.
- **Type**: Select the recovery operations for which you want information: Failover, Move, Failover Test. If more than one operation is selected, the number of recovery operations you selected is displayed.
- **Status**: Select the statuses for which you want information: Success, Failed. If more than one status is selected, the number of statuses you selected is displayed.

Click **APPLY** to apply the selected filtering.

Click **RESET** to reset the display to the default values.

Click **EXPORT** and choose PDF or ZIP to generate a report.

The report displays information by VPG, and then by virtual machine within the VPG.

The VPG information includes who initiated the operation, the type of operation, the start time and the end time of the operation, the recovery host, storage, network, any boot order information, etc.

The information for each machine includes the steps taken during the operation, such as creating a machine and scratch volumes for testing, when each process began and ended, and whether the operation succeeded or not.

**Note**: When FOT is still in progress, the **end time** in the Recovery Report appears as **NA**.
The Recovery operation start time and Recovery operation end time values are shown in UTC according to the Zerto Virtual Manager clock in the recovery site. The Point in time value takes the checkpoint UTC time, which was created in the protected site, and converts it to the recovery site time zone.

**Branding the Recovery Report**

A branded logo can be placed in the report in the top left corner by adding the logo as a .png file to the `<ZertoInstallFldr>\Zerto\Zerto Virtual Replication\gui\` folder with the name `provider_logo.png`.

The folder `ZertoInstallFldr` is the root folder where Zerto Virtual Replication in the recovery site is installed. For example, `C:\Program Files\Zerto`. 
Resources Report

Information about the resources used by the virtual machines being recovered to a particular site is displayed in the Resources report under the REPORTS tab. The information is collected at fixed times that are defined in the Reports tab of the Site Settings dialog in the recovery site. Information for the report is saved for 90 days when the sampling period is hourly and for one year when the sampling period is daily.

The report collects the resource information for the virtual machines being recovered to the site where the report is run. If no virtual machines are recovered to the site where the report is run, the report is empty.

You can filter the information by the following:

From and To: The dates for which you want information.
Click EXPORT to generate the report, which is produced as an Excel file.

The information presented in this report is divided into three tabs:

Details Tab: Shows information for each protected virtual machine.
Performance Tab: Shows bandwidth and throughput information for each virtual machine in a table and in a graph.
Target Host Tab: Shows information per host in the recovery site.

Using a REST API to Generate a Report

Zerto Virtual Replication exposes a REST API to produce resource data. The report is generated by passing a URL. For details about the ResourcesReport API (and all other Zerto Virtual Replication REST APIs), see the Zerto Virtual Replication RESTful API Reference Guide.

Details Tab

The Details tab includes the names and IDs of the virtual machines being protected and, for each virtual machine, the timestamp for the information, where it is protected, the CPU used, the memory used by the host and the guest, the storage used, and other information.

Interpreting the Details Tab

The Details tab provides a breakdown of every protected virtual machine, identified by its internal identifier and name in the hypervisor manager. The report also includes the name of the VPG that is protecting the virtual machine and information such as the protected and recovery sites, the protected and recovery vCD Org, cluster, etc.

The Timestamp column displays the time when the last sample, as defined in the Reports tab of the Site Settings dialog, was taken.

The VPG Type column is one of:
- VC2VC - vCenter to vCenter replication
- VC2VCD - vCenter to vCloud Director replication
- VCD2VCD - vCloud Director to vCloud Director replication
- VCD2VC - vCloud Director to vCenter replication

The ZORG column defines organizations set up in the Zerto Cloud Manager that use a cloud service provider for recovery.
bandwidth (Bps) and throughput (Bps) columns display the average between two consecutive samples. With daily samples, these figures represent the average daily bandwidth and throughput. For hourly samples, the timestamp represents an average between the sample at the timestamp and the previous sample. A value of -1 means that the system failed to calculate the value, which can happen for several reasons, for example:

- Sites were disconnected when the sample was collected. Although the protected site measures the throughput and bandwidth, the recovery site logs the results.
- The bandwidth or throughput values at the time of the sample was lower than the bandwidth or throughput value in the previous sample. This can happen, for example, if the protected site VRA is rebooted since the sample values are not stored persistently by the VRA.
- If valueInLastSample does not exist, since currentValue is the first sample for the virtual machine, the data is not calculated.

Bandwidth is calculated as: \( \frac{\text{currentValue} - \text{valueInLastSample}}{\text{elapsedTime}} \)

For example:

<table>
<thead>
<tr>
<th>TIME</th>
<th>ACTION/DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:29:59.999</td>
<td>A virtual machine is placed in a VPG</td>
</tr>
<tr>
<td>2:30</td>
<td>A sample is generated. The total transmitted bytes is zero since the virtual machine was just placed in the VPG</td>
</tr>
<tr>
<td>2:30-2:59.999</td>
<td>The VM is writing data at 1MB/minute</td>
</tr>
<tr>
<td>3:00</td>
<td>The virtual machine lowers its write rate to 0.5MB/minute</td>
</tr>
<tr>
<td>3:30</td>
<td>A new sample is calculated. Current value of total data transmitted is 45MB:</td>
</tr>
<tr>
<td></td>
<td>(1\text{MB/minute}) \times (30 \text{ minutes}) + (0.5\text{MB/minute}) \times (30 \text{ minutes}) )</td>
</tr>
<tr>
<td></td>
<td>Last value of total data transmitted is 0, from the 2:30 sample.</td>
</tr>
<tr>
<td></td>
<td>Bandwidth = ( \frac{45\text{MB}-0}{60 \text{ minutes}} ) = 0.75\text{MB/minute} = 13107\text{Bps}</td>
</tr>
</tbody>
</table>

Report output fields

The following describes the fields in the Details tab.

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Guest Memory (MB)</td>
<td>The active memory of the virtual machine.</td>
</tr>
<tr>
<td>Bandwidth (Bps)</td>
<td>The average bandwidth used between two consecutive samples, in bytes per second.</td>
</tr>
<tr>
<td>Consumed Host Memory (MB)</td>
<td>The amount of host memory consumed by the virtual machine.</td>
</tr>
<tr>
<td>CPU Limit (MHz)</td>
<td>The maximum MHz available for the CPUs in the virtual machine.</td>
</tr>
<tr>
<td>CPU Reserved (MHz)</td>
<td>The MHz reserved for use by the CPUs in the virtual machine.</td>
</tr>
<tr>
<td>CPU Used (MHz)</td>
<td>The MHz used by the CPUs in the virtual machine.</td>
</tr>
<tr>
<td>CrmId</td>
<td>The CRM identifier specified in Zerto Cloud Manager for an organization that uses a cloud service provider for recovery.</td>
</tr>
<tr>
<td>Memory (MB)</td>
<td>The virtual machine defined memory.</td>
</tr>
<tr>
<td>Memory Limit (MB)</td>
<td>The upper limit for this virtual machine’s memory allocation.</td>
</tr>
<tr>
<td>Memory Reserved (MB)</td>
<td>The guaranteed memory allocation for this virtual machine.</td>
</tr>
<tr>
<td>Number Of vCPUs</td>
<td>The number of CPUs for the virtual machine.</td>
</tr>
<tr>
<td>Number Of Volumes</td>
<td>The number of volumes attached to the virtual machine.</td>
</tr>
<tr>
<td>Recovery Journal Provisioned Storage (GB)</td>
<td>The amount of provisioned journal storage for the virtual machine. The provisioned journal size reported can fluctuate considerably when new volumes are added or removed.</td>
</tr>
<tr>
<td>PARAMETER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Recovery Journal Used Storage (GB)</td>
<td>The amount of journal storage used by the virtual machine. Differences might occur between the value displayed in the <em>Used Journal</em> column in the <em>Protection Over Time by Site</em> report and the value displayed here, which is retrieved from vCenter or Hyper-V. The <em>Used Journal</em> value displayed in the <em>Protection Over Time by Site</em> report is calculated by the VRA, based on internal journal allocations for each recovery volume. vCenter and Hyper-V <em>Resources</em> reports are expected to display a larger size than in the <em>Protection Over Time by Site</em> report, and may reach up to 500MB higher per virtual machine than reported in the <em>Protection Over Time by Site</em> report.</td>
</tr>
<tr>
<td>Recovery Volumes Provisioned Storage (GB)</td>
<td>The amount of provisioned storage for the virtual machine in the target site. This value is the sum of volumes' provisioned size.</td>
</tr>
<tr>
<td>Recovery Volumes Used Storage (GB)</td>
<td>The amount of storage used by the virtual machine in the target site.</td>
</tr>
<tr>
<td>Service Profile</td>
<td>The service profile used by the VPG.</td>
</tr>
<tr>
<td>Source Cluster</td>
<td>The source cluster name hosting the virtual machine.</td>
</tr>
<tr>
<td>Source Host</td>
<td>The source host name hosting the virtual machine.</td>
</tr>
<tr>
<td>Source Organization VDC</td>
<td>The name of the source vDC organization.</td>
</tr>
<tr>
<td>Source Resource Pool</td>
<td>The source resource pool name hosting the virtual machine.</td>
</tr>
<tr>
<td>Source Site</td>
<td>The source protected site name, defined in the Zerto User Interface.</td>
</tr>
<tr>
<td>Source vCD Organization</td>
<td>The name of the source vCD organization.</td>
</tr>
<tr>
<td>Source Volumes Provisioned Storage (GB)</td>
<td>The amount of provisioned storage for the virtual machine in the source site. This value is the sum of volumes' provisioned size.</td>
</tr>
<tr>
<td>Source Volumes Used Storage (GB)</td>
<td>The amount of storage used by the virtual machine in the source site. This value is the sum of the volumes' used size.</td>
</tr>
<tr>
<td>Source VRA Name</td>
<td>The name of the source VRA used to send data to the recovery site.</td>
</tr>
<tr>
<td>Target Cluster</td>
<td>The target cluster name hosting the virtual machine.</td>
</tr>
<tr>
<td>Target Datastores</td>
<td>The target storage used by the virtual machine if it is recovered.</td>
</tr>
<tr>
<td>Target Host</td>
<td>The target host name hosting the virtual machine when it is recovered.</td>
</tr>
<tr>
<td>Target Organization vDC</td>
<td>The name of the target vDC organization.</td>
</tr>
<tr>
<td>Target Resource Pool</td>
<td>The target resource pool name where the virtual machine will be recovered.</td>
</tr>
<tr>
<td>Target Site</td>
<td>The target site name, defined in the Zerto User Interface.</td>
</tr>
<tr>
<td>Target Storage Policy</td>
<td>The target vCD storage policy used.</td>
</tr>
<tr>
<td>Target vCD Organization</td>
<td>The name of the target vCD organization.</td>
</tr>
<tr>
<td>Target VRA Name</td>
<td>The name of the VRA managing the recovery.</td>
</tr>
<tr>
<td>Throughput (Bps)</td>
<td>The average throughput of the VM used between two consecutive samples, in bytes per second.</td>
</tr>
</tbody>
</table>
| Timestamp                                      | The date and time the resource information was collected. The value can be converted to an understandable date using code similar to the following:  
  ```javascript
  var date = new Date(jsonDate);
  ```  
  or code similar to the Perl code example, `jsonDateToString($)` described in *Zerto Virtual Replication RESTful API Reference Guide*. |
| VM Hardware Version                            | The VMware hardware version.                                                                                                                  |
| VM Id                                          | The internal virtual machine identifier.                                                                                                       |
| VM Name                                        | The name of the virtual machine.                                                                                                              |
The Performance tab shows bandwidth and throughput information for each virtual machine per sampling period in a table and in a graph. The Performance tab enables the user to view the total bandwidth and throughput per sampling period. The graph allows the user to view performance trends over time per VM. For full explanation of the bandwidth and throughput information, refer to the “Details Tab”, on page 327. You can filter information by date and VM name.

The following describes the fields in the Performance tab:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPG Name</td>
<td>The name of the VPG.</td>
</tr>
<tr>
<td>VPG Type</td>
<td>The VPG type:</td>
</tr>
<tr>
<td></td>
<td>VCVpg – VMware vCenter Server</td>
</tr>
<tr>
<td></td>
<td>VCvApp – Deprecated</td>
</tr>
<tr>
<td></td>
<td>VCDvApp – VMware vCloud Director vApp</td>
</tr>
<tr>
<td></td>
<td>PublicCloud – Amazon WebServices or Microsoft Azure</td>
</tr>
<tr>
<td></td>
<td>HyperV – Microsoft SCVMM</td>
</tr>
<tr>
<td>ZORG</td>
<td>The name assigned to an organization using a cloud service provider for recovery. The name is created in the Zerto Cloud Manager. For details, see the Zerto Cloud Manager Administration Guide.</td>
</tr>
</tbody>
</table>

**Target Host Tab**

The Target Host tab shows information per host in the recovery site. This enables the user to perform capacity planning on the recovery host. You can filter information by time and by host.

The following describes the fields in the Target Host tab:

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Guest Memory (MB)</td>
<td>The active memory of the virtual machine.</td>
</tr>
<tr>
<td>CPU Used (MHz)</td>
<td>The MHz used by the CPUs in the virtual machine.</td>
</tr>
<tr>
<td>Host</td>
<td>The Target Host’s IP address or DNS name.</td>
</tr>
<tr>
<td>Total Bandwidth</td>
<td>The total bandwidth of all VMs replicating to the host during the measured period.</td>
</tr>
<tr>
<td>Total Throughput</td>
<td>The total throughput of all VMs replication to the host during the measured period.</td>
</tr>
<tr>
<td>vCPUs</td>
<td>The number of CPUs for the virtual machine.</td>
</tr>
<tr>
<td>VMs</td>
<td>The number of VMs protected.</td>
</tr>
<tr>
<td>Volumes</td>
<td>The number of volumes attached to the virtual machine.</td>
</tr>
</tbody>
</table>
Monthly Usage Report

Information about usage can be displayed in the Monthly Usage report under the REPORTS tab. The Monthly Usage Report can only be viewed with a cloud license.

The information is organized by organization and within each organization by site, then virtual protection group (VPG) and then by the virtual machines in each VPG.

This report is mostly used by cloud service providers.

You can filter the information by the following:

Year: The year of interest.
Month: Select the month to review.

For each month, the usage report displays the number of virtual machines protected during the month and the average number per day in the month. For example, if fifteen virtual machines are protected in a few VPGs starting on the 28th of the month in a thirty day month, the total days will be 30 (two days multiplied by fifteen machines) and the VM Count will be 1 (Total days divided by the number of days in the month).

Click EXPORT to a CSV or ZIP file to generate the report.

The ZIP file option saves the report as a zipped CSV file in a zipped file called UsageReport.zip.

VPG Performance Report

Performance graphs for all VPGs or for an individual VPG can be seen in the VPG Performance report under the REPORTS tab. These graphs show more detailed resolution than the corresponding graphs in the DASHBOARD tab.

You can specify the VPGs whose performance should be displayed. When you request information about multiple VPGs, each VPG is shown in a different color, with a key at the top of the report that maps each color to the VPG it represents.

Position the cursor on a graph line to see exact information about that point.

Click APPLY to apply the selected filtering and produce the report.

Click RESET to reset the display to the default values.
Backup Report

Information about offsite backups can be sent as a report every day or weekly on a specified day. To set up the report, select Site Settings > Email Settings.

Enter an email address to receive Zerto Virtual Replication backup reports.

**SMTP Server Address:** The SMTP server address of the hypervisor manager. The Zerto Virtual Manager must be able to reach this address.

**SMTP Server Port:** The SMTP server port, if it was changed from the default, 25.

**Sender Account:** A valid email address for the email sender name.

**To:** A valid email address where that will receive the email containing the backup reports.

**SEND TEST EMAIL button:** Tests that the email notification is set up correctly. A test email is sent to the email address specified in the To field.

**To configure backup reports:**

1. Select *Enable backup reports*.
2. Specify whether you want a backup report sent daily or weekly.
   - **Daily:** Sends a daily backup report.
   - **Weekly:** Sends a weekly backup report. Select the day of the week from the dropdown list.
3. Specify the time of day to send the backup report.

The backup report is sent as HTML with the following information:

- A summary listing every VPG for which an offsite backup job has run. The summary information includes the following:
  - An entry for each backup job that was run.
  - The result of the job: successful, partial successful, or failed.
    - A partially successful job means that some, but not all, of the virtual machines were successfully backed up.
  - The time the job started.
  - The time the job completed.
  - The duration of the job.
  - The size of the backup that was stored in the repository.
  - The type of the job: automatic, meaning a scheduled run, or manually initiated.
  - Summary details of the run.
- Specific details about the job, including:
  - The name of the ZORG of the VPG.
  - The protected site.
The backup site where offsite backup can be restored.
- The number of virtual machines backed up from the totally number in the VPG.
- The number of virtual machines only partially backed up.
- The start and end times of the run and the run duration.
- The backup size.
- Whether the backup was scheduled or initiated manually.
- The repository name.
- The next time a backup of the VPG is scheduled.
- The previous run time.
CHAPTER 22: TROUBLESHOOTING

You can handle problems related to the WAN connecting the protecting or recovery sites, or other problems using a variety of diagnostic and troubleshooting tools.

The following topics are described in this chapter:

- “Ensuring the Zerto Virtual Manager is Running”, below
- “Troubleshooting Needs Configuration Problems”, on page 335
- “Troubleshooting GUI Problems”, on page 335
- “Troubleshooting VRA Problems”, on page 336
- “Handling Lack of Storage Space for Recovered Virtual Machines”, on page 336
- “Zerto Virtual Replication Diagnostics Utility”, on page 336
- “Collecting Zerto Virtual Replication Logs”, on page 337
- “Re-IP Configured As Static Fails During FOL with Reverse Protection”, on page 344

For details about Zerto Virtual Manager alarms, alerts, and events, refer to Zerto Virtual Replication Guide to Alarms, Alerts and Events.

Ensuring the Zerto Virtual Manager is Running

If you have problems accessing the Zerto User Interface, check under Windows Services, on the machine where Zerto Virtual Replication is installed, that the Zerto Virtual Manager Windows service is started.
Troubleshooting Needs Configuration Problems

When the VPG status changes to **Needs Configuration**, the settings in the VPG need to be checked and, when necessary, updated.

The following scenarios result in the VPG status changing to **Needs Configuration**:

- A protected disk resize operation fails, for example when there is not enough disk space.
- When a volume is added to a protected virtual machine and the added volume has no matching storage or not enough room on the recovery storage.
- When a volume is added to a protected virtual machine and the VPG settings are not updated because of a site disconnection or a vCenter Server error. In some situations, after the sites reconnect, the state corrects itself automatically.
- When performing a Failover or Move operation, if you do not specify reverse protection.
- An Org vDC network is removed from the recovery site that has a VPG replicating to it.

Troubleshooting GUI Problems

**Host is Not Displayed in List of Hosts in the Create VPG Wizard**

If the installation of a VRA completes successfully, but the allocation of the IP takes too long, when attempting to specify the host to recover a VPG, the host where the VRA is installed does not appear in the list, you have to uninstall and then re-install the VRA.
Troubleshooting VRA Problems

VPG Syncing Takes a Long Time - Network Problems
Check the network. If the firewall configuration is modified, the VRA TCP connections have to be reset. After a VRA disconnect and reconnect the system can wait for up to fifteen minutes before syncing the sites after the reconnection.

Host is Not Displayed in List of Hosts in the Create VPG Wizard
If the installation of a VRA completes successfully, but the allocation of the IP takes too long, when attempting to specify the host to recover a VPG, the host where the VRA is installed does not appear in the list, you have to uninstall and then re-install the VRA.

VRA Crashes During Promotion
If a VRA is promoting data to a recovery virtual machine and the VRA fails, the VRA starts up automatically but you might have to restart the virtual machine manually and then the promotion will continue.

Cannot Install a VRA After Uninstalling a VRA on the Host
Uninstalling a VRA sometimes leaves a zagentid folder and you cannot install a new VRA, because of an old, unused, zagentid folder. Delete the zagentid folder manually.

Note: This only happens if a file was manually added to the zagentid folder.

Handling Lack of Storage Space for Recovered Virtual Machines
If a recovery virtual machine does not have enough space on the recovery site, the promotion of data to the recovered virtual machine hangs. If this occurs you should add more space to the machine and then start the machine. The promotion will then continue. You can check the available space for each datastore in SETUP > DATASTORES.

Zerto Virtual Replication Diagnostics Utility
Zerto Virtual Replication includes a diagnostics utility to help resolve actual and potential problems. Using the diagnostics tool, you can do the following:

- Collect logs to help Zerto support resolve problems. The Zerto Virtual Manager must be running on each site for which you want logs. See “To collect logs for Zerto support to use when troubleshooting:“, below.
- Collect local Zerto Virtual Manager logs. Use this option if the Zerto Virtual Manager is not running. See “To collect local Zerto Virtual Manager logs when the Zerto Virtual Manager is not running:“, on page 342.
- Check the connectivity between Zerto Virtual Replication components. See “Check Connectivity Between Zerto Virtual Replication Components“, on page 252.
- Reconfigure the Zerto Virtual Manager, including the IP addresses of the vCenter Server and of the machine running the Zerto Virtual Manager, and the SSL certificate used when accessing the Zerto User Interface. See “Reconfiguring the Zerto Virtual Manager Setup“, on page 253.
- Export VPG settings to an external file and import these settings. This option is used when upgrading Zerto Virtual Replication, described in the Zerto Virtual Replication Installation Guide.
- Reconfigure access to the Microsoft SQL Server that is used by the Zerto Virtual Manager. This database was specified during the installation of Zerto Virtual Replication. See “Reconfiguring the Microsoft SQL Server Database Used by the Zerto Virtual Manager“, on page 255.

Note: A separate installation kit is available for download from the Zerto Support Portal downloads page that installs the Zerto Virtual Replication Diagnostics utility as a standalone utility on any Windows machine that has Microsoft .NET Framework 4 installed. The installation executable is included as part of the standalone utility installation kit and it requires an additional 1.8GB of free disk space.
Collecting Zerto Virtual Replication Logs

Virtual replication logs can be collected to help Zerto support resolve problems related to Zerto Virtual Replication. Virtual replication logs can be collected in the following ways:

"Using Remote Log Collection", below
"Using the Zerto Diagnostics application", on page 338

Using Remote Log Collection

Remote Log Collection allows customers to authorize Zerto support engineers to collect logs from their environment. By using remote log collection customers can avoid having to use the Diagnostic Tool on their ZVM server in order to collect logs for analysis, a potentially complex and time-consuming procedure.

To enable Remote Log Collection:

1. In the Zerto User Interface, click SETTING ( ) in the top right of the header and select Remote Support. The Remote Support dialog is displayed.

2. Click the drop down menu to display the remote log collection options.

3. Select the remote log collection option you wish to allow:
   - Never – Remote log collection is not allowed (default). If remote log collection is currently is allowed, it will be terminated if you select this option.
   - For the next 30 days - Remote log collection is allowed. This permission will automatically terminate in 30 days unless terminated by selecting the Never option.
   - Only for a specific case - You will be prompted to enter the Case number opened via the Salesforce Self-service Portal. Remote log collection will be allowed for as long as the case is active or until remote log collection is terminated by selecting the Never option.

4. Click Save.
Collecting Zerto Virtual Replication Logs

Using the Zerto Diagnostics application

You can collect logs using the diagnostics tool to help Zerto support resolve problems when the Zerto Virtual Manager is running or when the Zerto Virtual Manager is not running.

- When the Zerto Virtual Manager is running, see “To collect logs for Zerto support to use when troubleshooting:”, below. This option enables you to specify the logs that you want to collect, generated by Zerto Virtual Replication, for example VRA logs, as well as logs generated by VMware, for example, vCenter Server logs or host logs. The Zerto Virtual Replication generated logs can be filtered by any alerts issued and by the VPGs that require analysis to identify problems.
- When the Zerto Virtual Manager is not running, see “To collect local Zerto Virtual Manager logs when the Zerto Virtual Manager is not running:”, on page 342.

To collect logs for Zerto support to use when troubleshooting:

1. Open the Zerto Diagnostics application. For example, via Start > Programs > Zerto Virtual Replication > Zerto Diagnostics.

   The Zerto Virtual Replication Diagnostics menu dialog is displayed.

2. Select the Collect the Zerto Virtual Replication logs for use by Zerto support option.

3. Click Next.

   The Initialize dialog is displayed.

4. Specify the following and click Next.

   - **IP / Host Name**: The IP of the Zerto Virtual Manager where the log collection runs from. Logs are collected from this site and from the paired site.
   - **Port**: The port used for inbound communication with the Zerto Virtual Manager.
   - **Your Company Name**: A name to identify the log collection for the customer. This information is used by Zerto support. An account name must be entered. After this information is added, it is displayed in subsequent uses of the diagnostics utility.
   - **Email**: An email address for use by Zerto support when analyzing the logs. An email address must be entered. After this information is added, it is displayed in subsequent uses of the diagnostics utility.
   - **Timeframe**: The amount of time you want to collect logs for. The more time, the bigger the collection package.
   - **Case Number**: The case number assigned by Zerto support, if one already exists. Optional.
   - **Description**: An optional free text description of the reason for collecting the logs.

   After clicking Next the utility connects to the Zerto Virtual Replication and if any alerts have been issued, they are displayed in the Select Alerts dialog.

   If there are no alerts, this dialog is skipped.
5. Select any alerts that need analyzing from the list and click **Next**. The Select VPGs dialog is displayed.

6. Select the VPGs that you want analyzed and click **Next**. The **Customize** dialogs are displayed. These dialogs can generally be left with their default values. The following **Customize** dialogs are displayed:
   - The **Select Sites** dialog
   - The **Select VRA Hosts** dialog
   - The **Select vSphere Logs** dialog
   - The **Select vCloud Director Logs** dialog
   The **Select Sites** dialog is displayed, with the list local site and all the sites paired to it listed.

Those sites that are either protecting or used for recovery for any of the selected VPGs from the previous dialog are automatically selected.

**Note:** Zerto Virtual Manager logs from both sites are collected when both sites are trusted sites otherwise only logs from the local site are collected.

7. Verify that the sites that need analyzing are selected and click **Next**.
The Select VRA Hosts dialog is displayed.

Those hosts with VRAs that are used to protect or recover any of the selected VPGs are automatically selected. You can change the collection criteria using the plus and minus buttons. The expected size of the collection package is updated dependent on the selected VRAs.

8. Verify that the host with VRAs that need analyzing are selected and click Next.

The Select vCenter Server Logs dialog is displayed.

Specify the vSphere data to collect.

**Collect vCenter Server Diagnostics** – Collects vCenter Server diagnostics.

**Collect Host Logs** – Collects logs generated for hosts. If you check the Collect host logs checkbox, you can select the host logs to be included in the collection by using the plus and minus buttons.

The vSphere data that can be collected enlarges the size of the log collection package significantly and is not collected by default.

9. Click Next.

The Select vCloud Director Logs dialog is displayed.

10. Click Next.
The Save Log Destinations dialog is displayed.

11. Specify destination for the files that you want collected.
   - **Destination:** The name and location where the log collection will be saved.
   - **Automatically upload files to Zerto FTP Server:** When this option is checked, the log collection is automatically uploaded to a specified FTP site.
     
     If you choose to upload the log collection to a site that you specify, make sure that the site is up.

12. Specify the FTP site to send the collection and the protocol to use, either FTP or HTTP.

13. Click **Next**.

   The Review dialog is displayed.

14. Click **Start**.

   The data is collected and stored in the destination file which, by default, is timestamped. If specified, the collection is also sent to an FTP site.

   **Note:** The log collection is performed on the server. Canceling the collection in the GUI does not stop the collection from continuing on the server and a new log collection cannot be run until the running collection finishes.
When the log collection has completed the result is displayed. For example:

```
15. Click Done to return to the Zerto Virtual Replication Diagnostics menu dialog.
16. Send the log to Zerto support, unless the Automatically upload files to Zerto FTP Server option was specified, in which case it is automatically sent to Zerto.

To collect local Zerto Virtual Manager logs when the Zerto Virtual Manager is not running:
1. Open the Zerto Diagnostics application. For example, via Start > Programs > Zerto Virtual Replication > Zerto Diagnostics. The Zerto Virtual Replication Diagnostics menu dialog is displayed.
2. Select the Local Zerto Virtual Manager diagnostics option and click Next.
   You are prompted to use the first option to collect more comprehensive diagnostics. If you continue, the Initialize dialog is displayed.
3. Specify the details that you want collected.
   IP / Host Name – The IP of the Zerto Virtual Manager where the log collection runs from. Logs are collected from this site and from the paired site.
   Port – The port used for inbound communication with the Zerto Virtual Manager.
   Your Company Name – A name to identify the log collection for the customer account. This information is used by Zerto support. An account name must be entered.
   Email – An email address for use by Zerto support when analyzing the logs. An email address must be entered.
   Timeframe – The amount of time you want to collect logs for. The more time, the bigger the collection package.
   Case Number – An optional field for the case number assigned to the issue by Zerto.
   Description – An optional free text description of the reason for collecting the logs.
4. Click Next.
   The Save Log Destinations dialog is displayed.
5. Specify the details that you want collected.
   Destination – The name and location where the log collection will be saved.
   Automatically upload files to Zerto FTP Server – When this option is checked, the log collection is automatically uploaded to a specified FTP site.
If you choose to upload the log collection to a site that you specify, make sure that the site is up before clicking Finish. The data is collected and stored in the destination file which, by default, is timestamped. If specified, the collection is also sent to an FTP site.

6. Click Next.
   The collection progress is displayed. When the log collection has completed the result is displayed.

7. Click Done to return to the Zerto Virtual Replication Diagnostics menu dialog.

8. Send the log to Zerto support, unless the Automatically upload files to Zerto FTP Server option was specified, in which case it is automatically sent to Zerto.

Understanding the Logs

If problems arise with Zerto Virtual Manager, you can view the Zerto Virtual Manager logs to see what is happening.

The current log is called logfile.csv and resides in the <Zerto_Install_Dir>\Zerto Virtual Replication\logs folder, where Zerto_Install_Dir is the folder specified during the installation.

When the log reaches 10MB its name is changed to log.nnnn.csv, where nnnn is a number incremented by one each time logfile.csv reaches 10MB. Up to 150 log files are kept.

The log file has the following format:
FFFF, yyyy-mm-dd hh:mm:ss, ####, LVL, Component, API, Message

where:

FFFF: A HEX code. For internal use.
yyyy-mm-dd hh:mm:ss: Timestamp for the message.
####: Number for internal use.
LVL: Severity level of the message. The more messages written to the log the bigger the impact on performance. The number of messages written to the log decreases from Debug to Error. The level can be one of the following:
   - Debug: All messages are written to the log. This level should only be specified during testing.
   - Info: Information messages.
   - Warn: Warning messages such as a reconnect ion occurred.
   - Error: Error messages that need handling to find the problem.
Component: The specific part in the Zerto Virtual Manager that issued the message.
API: The specific API that issued the message.
Message: The message written in the log.
The following is a sample from a log:

Re-IP Configured As Static Fails During FOL with Reverse Protection

Problem:
After performing a failover, the IP settings for the recovery site (re-IP) appear as DHCP in the network settings, instead of as static, as they were configured in the protected VM. The customer must manually change the IP settings back to static from DHCP.

Solution:
Verify that the user that is logged on to VMWare Tools, has sufficient privileges to execute re-IP changes.
This chapter describes the interaction between Zerto Virtual Replication and commonly used VMware features such as vMotion, DRS and HA.

The following topics are described in this chapter:

- “Zerto Virtual Replication Permissions in vCenter Server”, below
- “Stopping a vCenter Server”, on page 345
- “Thin-Provisioning”, on page 346
- “VMware Clusters”, on page 346
- “Storage Profiles and Storage Clusters”, on page 347
- “Fault Tolerance”, on page 347
- “Host Affinity Rules and CPU Pinning”, on page 347
- “vMotion”, on page 347
- “Storage vMotion”, on page 347
- “VMware Host Maintenance Mode”, on page 348
- “Resiliency to vSphere Environment Changes”, on page 348

Zerto Virtual Replication Permissions in vCenter Server

VMware roles and permissions are the core of VMware infrastructure security. Permissions are a combination of a user/group and a security role that is applied to some level of the VMware Infrastructure. Zerto Virtual Replication supplies a number of default privileges that enable a VMware administrator to perform specific actions.

You can define additional roles and assign these roles the privileges they need. All privileges are implemented at the root level, and thus apply to every object in the vCenter Server. The following privileges are required by Zerto Virtual Replication:

- **Live Failover / Move** - Enables performing a failover or move.
- **Manage cloud connector** - Enables installing and uninstalling Zerto Cloud Connectors. For details, refer to *Zerto Cloud Manager Administration Guide*.
- **Manage Sites** - Enables editing the site configuration, including site details, pairing and unpairing sites, updating the license and editing advanced site settings.
- **Manage VPG** - Enables creating, editing, and deleting a VPG and adding checkpoints to a VPG.
- **Manage VRA** - Enables installing and uninstalling VRAs.
- **Test Failover** - Enables performing a test failover.
- **Viewer** - For internal use only.

These privileges are assigned as to the *Administrator* role when Zerto Virtual Replication is installed.

**Note:** When upgrading vCenter Server be sure that the user entity that Zerto Virtual Replication is using is preserved in the user/permissions hierarchy.

Stopping a vCenter Server

If the recovery vCenter Server service is stopped, recovery operations are not possible until the service is restarted.
Thin-Provisioning

VMware vStorage thin-provisioning is a component of vStorage that enables over-allocation of storage capacity for increased storage utilization, enhanced application uptime and simplified storage capacity management.

When migrating or recovering the virtual machines in a VPG, the virtual machines are migrated or recovered with the same configuration as the protected machines. Thus, if a virtual machine in a VPG is configured with thin provisioning, then during migration or recovery the machine is also defined in the recovery site as thin provisioned.

VMware Clusters

A cluster is a group of tightly coupled hosts that work closely together so that in many respects they can be viewed as though they are a single computer. Clusters are used for high availability and load balancing. With a cluster, you define two or more physical machines that will provide resources for the hosts that are assigned to that cluster. By using clusters, you can achieve high availability and load balancing of virtual machines. Load balancing is referred to as DRS (Distributed Resource Scheduler) by VMware.

Thus, you use clusters for the following:

- If one of the physical hosts goes down, the other physical host starts up the VMs that the original host was running (high availability).
- If one physical host is over utilized by a VM, that VM is moved to the other physical host (DRS).

Both of these features use vMotion to move these virtual guests from one system to another.

You cannot apply high availability nor DRS to a Virtual Replication Appliance (VRA).

Also, see “DRS”, below.

VMware High Availability (VMHA)

VMware high availability decreases downtime and improves reliability with business continuity by enabling another ESX/ESXi host to start up virtual machines that were running on another ESX/ESXi host that went down.

High availability is automatically disabled by Zerto Virtual Replication while updating recovered virtual machines in the recovery site from the VRA journal. After the promotion of the data from the journal to the virtual machine completes, high availability is automatically re-enabled.

The HA configuration can include admission control to prevent virtual machines being started if they violate availability constraints. If this is the case, then a failover, test failover or migration of the virtual machines in a VPG to the cluster with this configuration will fail, if the availability constraints are violated when the virtual machines are recovered. It is recommended to test the failover, as described in “Testing Recovery”, on page 273, to ensure recovery will succeed, even when HA is configured with admission control.

DRS

VMware DRS enables balancing computing workloads with available resources in a cluster.

DRS is automatically disabled by Zerto Virtual Replication while updating recovered virtual machines in the recovery site from the journal for these recovered virtual machines. After the promotion of the data from the journal to the recovered virtual machine completes, DRS is automatically re-enabled.

If DRS is disabled for the site, VMware removes all resource pools in the site. If the recovery was defined to a resource pool, recovery will be to any one of the hosts in the recovery site with a VRA installed on it.

Note: If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.
Storage Profiles and Storage Clusters

Profile-Driven Storage provides visibility into your storage pool, letting you optimize and automate storage provisioning.

Zerto Virtual Replication supports the use of storage profiles and storage clusters defined within a profile. If Zerto Virtual Replication cannot find a storage profile that can be used as target storage, the value is set to Zerto_Any. In this case, any of the datastores configured in the Configure Provider vDCs dialog can be selected as recovery datastores, provided they are exposed to the relevant recovery hosts. Upon recovery, Zerto Virtual Replication chooses a storage profile available to the Org vDC, for the recovered vApp, that contains all of the datastores on which recovery volumes of the VPG reside. If there is no such storage profile, the recovery operation cannot start. The storage profile can be set to Zerto_Any for a number of reasons, such as adding a virtual machine to the VPG which does not have a storage profile that can be used as the target.

Fault Tolerance

VMware fault tolerance provides uninterrupted availability by eliminating the need to restart a virtual machine by copying a functional virtual machine to a second ESX/ESXi host while making sure that both virtual machines are synchronized, so that if the ESX/ESXi that is hosting the primary virtual machine goes down, the secondary virtual machine takes over.

Zerto Virtual Replication does not support fault tolerance for machines in a VPG, nor for a Virtual Replication Appliance (VRA).

Host Affinity Rules and CPU Pinning

VMware host affinity rules enable specifying which ESX/ESXi hosts a virtual machine can or cannot run under. CPU pinning ties a specific workload to a specific processor within an ESX/ESXi host. Thus, when DRS is enabled, the rules for which ESX/ESXi hosts a virtual machine can be enforced regardless of the load.

Zerto Virtual Replication works whether host affinity and CPU pinning is used or not.

Note: Host affinity rules are applied to Virtual Replication Appliances (VRAs) to tie it to the host.

vMotion

If you use vMotion to migrate a virtual machine, which is part of a VPG, from one ESX/ESXi host to another ESX/ESXi host, make sure of the following before moving the virtual machine:

- The ESX/ESXi host where you are moving the virtual machine to has a Virtual Replication Appliance (VRA) installed on it, as described in the Zerto Virtual Replication Installation Guide.
- The virtual machine is not a test virtual machine running on the recovery site during the performance of a failover test, as described in “Testing Recovery”, on page 273.

You cannot move a Virtual Replication Appliance (VRA) from one ESX/ESXi host to another. Also a virtual machine that is being updated from the VRA journal, after recovery has been initiated, cannot be moved until the promotion of data to the virtual machine completes.

Storage vMotion

VMware Storage vMotion enables you to perform live migration of virtual machine disk files across heterogeneous storage arrays with complete transaction integrity and no interruption in service for critical applications enabling you to perform proactive storage migrations, simplify array refreshes/retirements, improve virtual machine storage performance, and free up valuable storage capacity in your data center.

Zerto Virtual Replication supports Storage vMotion for protected and recovered virtual machine volumes and for journal volumes in the recovery site, but not for a machine volume in a VPG being promoted.
VMware Host Maintenance Mode

You place a host in maintenance mode when you need to service it, for example, to install more memory. A host enters or leaves maintenance mode only as the result of a user request.

Virtual machines that are running on a host entering maintenance mode need to be migrated to another host (either manually or automatically by DRS) or shut down.

Zerto Virtual Replication enables moving recovery disks managed by a VRA on a host that needs maintaining to be moved to another host for the duration of the maintenance, as described in "Managing Protection During VMware Host Maintenance", on page 250.

Note: Automatic detection and powering off the VRA when running host maintenance mode is supported in vCenter version 6.5. For more information see Zerto Virtual Replication Interoperability Matrix.

Resiliency to vSphere Environment Changes

VMware vSphere identifies and manages all its objects: VMs, ESXi hosts, networks, data stores, resource pools, etc. using the MoRef ID (Managed Object Reference Identifier). MoRef IDs are allocated to virtual machines and other objects incrementally by vCenter.

When Zerto maps an environment within vCenter for its configuration and operations, for example when creating a VPG, it acquires and maps the MoRef IDs of the available virtual machines, and refers to these MoRef IDs in its own environment management and replication operations.

If an ESXi host is removed from inventory and is then re-added, everything that was on it gets a new MoRef ID. As a result, a virtual machine, protected by Zerto that was running on that host will be allocated a new MoRef ID. The new MoRef ID would not be known to the Zerto Virtual Manager, and the virtual machine would no longer be protected. The same result applies to the VRA, which becomes a ghost VRA, unknown to the Zerto Virtual Manager.

In order to avoid these issues Zerto Virtual Replication maintains the old MoRef ID map containing the original MoRef IDs as well as unique identifiers of the hosts and VMs. Zerto Virtual Manager constantly monitors the vCenter environment and maintains a mapping of MoRef IDs - new to original.

The re-mapping of MoRef IDs can take several minutes. When system administration tasks require the importing of VPG definitions of a host that was removed and then re-added, it is advisable to wait approximately 5 minutes from when the host was re-added before performing the import of the VPGs.
Configuration and management of disaster recovery for a site are performed in the Zerto User Interface.

The following dialogs and tabs are described in this section:

- “About Dialog”, on page 350
- “Add Checkpoint Dialog”, below
- “Add Site Dialog”, on page 352
- “Add Static Route Dialog”, on page 352
- “Advanced Journal Settings Dialog”, on page 353
- “Advanced Journal Settings Dialog (vCD)”, on page 353
- “Advanced VM Recovery Settings Dialog”, on page 355
- “Advanced VM Replication Settings Dialog”, on page 356
- “Advanced VM Replication Settings Dialog (vCD)”, on page 356
- “Advanced VM Settings for Cloud Dialog”, on page 357
- “ALERTS”, on page 357
- “Boot Order Dialog”, on page 358
- “Browse for File Dialog”, on page 359
- “Change Host Password VRA Dialog”, on page 359
- “Change VM Recovery VRA Dialog”, on page 360
- “Checkpoints Dialog”, on page 361
- “Configure and Install VRA Dialog”, on page 362
- “Configure Paired Site Routing Dialog”, on page 363
- “Configure Provider vDCs Dialog”, on page 364
- “Configure VM Settings Dialog”, on page 365
- “Configure Volume Dialog (vCD)”, on page 365
- “Edit NIC Dialog”, on page 366
- “Edit Repository Dialog”, on page 367
- “Edit Selected Volumes Dialog”, on page 368
- “Edit VM Dialog”, on page 368
- “Edit VM Dialog (vCD)”, on page 369
- “Edit VM Settings Dialog (AWS)”, on page 371
- “Edit VM Settings Dialog (Azure)”, on page 372
- “Edit vNIC Dialog”, on page 372
- “Edit vNIC Dialog (vCD)”, on page 373
- “Edit Volumes Dialog”, on page 374
- “Edit Volumes Dialog (vCD)”, on page 376
- “Edit VRA Dialog”, on page 377
- “License Dialog”, on page 378
- “Manage Static Routes Dialog”, on page 379
- “New Repository Dialog”, on page 379
- “NICs Dialog”, on page 381
- “Offsite Clone Window”, on page 381
- “Open Support Ticket Dialog”, on page 381
- “Remote Support Dialog”, on page 383
- “Restore from Zerto Backup”, on page 384
- “Restore Volumes Dialog”, on page 386
- “Site Settings Dialog”, on page 387
- “Stop Failover Test Dialog”, on page 393
- “TASKS”, on page 394
- “Volumes Dialog”, on page 394
About Dialog

In the About window, you can do the following:

- View the version of Zerto Virtual Replication being run.
- Enable or disable the **Zerto CALLHOME feature**. The Zerto CALLHOME feature enables support notification and analytics for the following purposes:
  - To improve Zerto Virtual Replication.
  - To send notifications to the user when a new Zerto Virtual Replication version is available, or when new hypervisor versions are supported by Zerto.
- Enable or disable Zerto Virtual Manager to send data to the SaaS platform for monitoring purposes, using the Zerto Mobile App. This action is done by licensed Zerto Virtual Manager users.

When clicking About, the following options appear:

- Enable Support notification and product improvement feedback.
- Enable Zerto SaaS features. Includes Zerto Analytics, Zerto Mobile App and Remote upgrade.

To perform these actions, do the following:

1. In the Zerto User Interface, in the top right of the header, click **SETTING ( )**, and then click About. The version and build of Zerto Virtual Replication installed in the site are displayed.
2. To enable the Zerto CALLHOME feature, click **Enable Support notification and product improvement feedback**. This is selected by default.
   
   **Note:** This option is grayed out for Microsoft Azure and AWS.
   
   If the user deselects Enable Support notification and analytics, a warning appears notifying the user that deselecting this option will stop Zerto Virtual Replication from sending notifications when new Zerto Virtual Replication updates are available, or when new hosts are supported.
3. If you want Zerto Virtual Replication to send information to our Online Services and Zerto Mobile App, and enable remote upgrade, select **Enable SaaS features**. This is selected by default.
   
   This allows licensed Zerto Virtual Manager users to enable or disable data being sent from the Zerto Virtual Manager to the SaaS platform, thereby enabling site monitoring using the Zerto Mobile App.
   
   - If the user deselects Enable Online Services and Zerto Mobile, a warning appears notifying the user that deselecting this option will stop Zerto Virtual Replication from sending information to Online Services and to the Zerto Mobile Application, rendering these services inoperable for the entire installation.
Add Checkpoint Dialog

Checkpoints are recorded automatically every few seconds in the journal. These checkpoints ensure crash-consistency and are written to the virtual machine journals by the Zerto Virtual Manager. Each checkpoint has a timestamp set by the Zerto Virtual Manager. In addition to the automatically generated checkpoints, you can manually add checkpoints to identify events that might influence the recovery, such as a planned switch over to a secondary generator.

The list of VPGs is displayed. You can select more VPGs to add the same checkpoint.

- **Enter a name for the checkpoint**: The name to assign to the checkpoint.
- **Dir**: The direction of the protection.
- **VPG Name**: The name of the VPG.
- **Protected Site Name**: The name of the site where virtual machines are protected.
- **Recovery Site Name**: The name of the site where protected virtual machines are recovered.

You can filter columns in the list via the filter icon next to each column title. You can also sort the list by each column. Clicking the cog on the right side of the table enables you to change the columns that are displayed and to create a permanent view of the columns you want displayed.
Add Site Dialog

Pair sites

- **Host name**: 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.

Add Static Route Dialog

Add a static route for a specified group, defined in “Manage Static Routes Dialog”, on page 379, when the Zerto Cloud Connector and cloud site Zerto Virtual Manager are on different networks.

- **Address**: The network address for the static route that you want to route to.
- **Subnet Mask**: The subnet mask for the network.
- **Gateway**: The gateway address for the network on the local network of the Zerto Cloud Connector cloud network interface.

**Note**: If you change the Zerto Virtual Manager and VRAs cloud network, changing the static route settings for a group to the new network only changes the access for new Zerto Cloud Connectors with the specified group. Existing Zerto Cloud Connectors must be redeployed to use the changed static route.

Also see: “Manage Static Routes Dialog”, on page 379.
**Advanced Journal Settings Dialog**

Manage the journal used for recovery.

**Journal History:** The time that all write commands are saved in the journal.

The longer the information is saved, the more space is required for each journal in the VPG to store the saved information.

You can select the number of hours from 1 to 23 or the number of days from 1 to 30.

**Default Journal Datastore:** The datastore used for the journal data for each virtual machine in the VPG.

Select a datastore accessible to the host.

When you select a specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine.

In this case, all protected virtual machines must be recovered to the hosts that can access the specified journal datastore.

**Journal Size Hard Limit:** The maximum size that the journal can grow, either as a percentage or a fixed amount.

The journal is always thin-provisioned.

- **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery datastore.
  
  **Note:** If Unlimited is selected, the **Size** and **Percentage** options are not displayed.

- **Size (GB):** The maximum journal size in GB.
  
  - The **minimum** journal size, set by Zerto Virtual Replication, is **8GB**.
  
  - **Percentage:** The percentage of the virtual machine volume size to which the journal can grow.
    
    - This value can be configured to more than 100% of the protected VM’s volume size.

**Journal Size Warning Threshold:** The size of the journal that triggers a warning that the journal is nearing its hard limit.

- **Unlimited:** The size of the journal is unlimited and it can grow to the size of the recovery datastore.
  
  **Note:** If Unlimited is selected, the **Size** and **Percentage** options are not displayed.

- **Size (GB):** The size in GB that will generate a warning.

- **Percentage:** The percentage of the virtual machine volume size that will generate a warning.

Both the values of Size and Percentage must be less than the configured **Hard Limit** so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.

**Advanced Journal Settings Dialog (vCD)**
Used **only** in environments with **vCD**.

Manage the journal used for recovery in a vCD environment.

<table>
<thead>
<tr>
<th>SETTING &amp; DESCRIPTION</th>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Journal History</strong></td>
<td></td>
</tr>
</tbody>
</table>
| The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG. | ▪ Number of **hours** from 1 to 24  
▪ Number of **days** from 2 to 30 |
| **Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)** | |
| The storage/datastore used for the journal data for each virtual machine in the VPG. | ▪ Select the storage/datastore accessible to the host.  
When you select a specific journal storage/datastore, the journals for each virtual machine in the VPG are stored in this storage/datastore, regardless of where the recovery storage/datastore is for each virtual machine. All protected virtual machines are recovered to the hosts that can access the specified journal storage/datastore. |
| **Journal Size Hard Limit** | |
| The maximum size that the journal can grow, either as a percentage or a fixed amount. The journal is always **thin-provisioned**. **Note:** The Journal Size Hard Limit applies independently both to the Journal History and also to the Scratch Journal Volume.  
*For Example:* If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit. | ▪ **Unlimited**: The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.  
If Unlimited is selected, Size and Percentage options are not displayed.  
▪ **Size (GB)**: The maximum journal size in GB.  
  ▪ The minimum journal size, set by Zerto Virtual Replication, is 8GB for Hyper-V and vSphere environments, and 10GB for Microsoft Azure environments.  
▪ **Percentage**: The percentage of the virtual machine volume size to which the journal can grow.  
  ▪ This value can be configured to more than 100% of the protected VM’s volume size. |
Advanced VM Recovery Settings Dialog

Displays the recovery settings for the virtual machines in the VPG. You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit information for several virtual machines at the same time by selecting the virtual machines and clicking **EDIT SELECTED**.
Advanced VM Replication Settings Dialog

Displays the replication settings for the virtual machines in the VPG. You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit information for several virtual machines at the same time by selecting the virtual machines and clicking EDIT SELECTED. For more details, see “Edit VM Dialog” on page 368.

Advanced VM Replication Settings Dialog (vCD)

Used only in environments with vCD.

Displays the settings of the virtual machines in the VPG.

- To edit information in one field by clicking the field and updating the information.
- To edit information for several virtual machines at the same time by selecting the virtual machines and clicking EDIT SELECTED.

For more details, see “Edit VM Dialog (vCD)” on page 369.
Advanced VM Settings for Cloud Dialog

Displays the recovery settings for the virtual machines in the VPG. You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit information for several virtual machines at the same time by selecting the virtual machines and clicking *EDIT SELECTED*.

**ALERTS**

Monitor the recent alerts by clicking the ALERTS area in the status bar at the bottom of the Zerto User Interface. The following information is displayed for the most recent alerts:

- The alert status.
- The site where the alert is issued.
- A description of the alert.

Click *All Alerts* to access MONITORING > ALERTS.
Boot Order Dialog

To specify the boot order of virtual machines in a VPG. When machines are started up on recovery, for example, after a move operation, the virtual machines in the VPG 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.

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.

There is no boot order for virtual machines within a group, only between groups.

**ADD GROUP button:** Adds a group. After adding a group you can edit the group name by clicking the Edit icon at the right of the group name and remove the group via the delete icon at the right of the group. You cannot remove the Default group nor a group that contains a virtual machine.

**Boot Delay:** Specifies 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 Start-up 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 up.
**Browse for File Dialog**

To select the folder with the preseeded disk to use. Drill-down to select the disk.

**Note:** Disks that are not viable for preseeding are grayed out.

**Change Host Password VRA Dialog**

To change the connectivity, VIB or password, used by the VRA to connect to the host. If using a password to connect to the host, to change the password used by the VRA.

- If the VRA is using a password to connect to the host and using VIB is required, check **Use credentials to connect to host**.
- If the VRA is using VIB to connect to the host and using a password is required, uncheck **Use credentials to connect to host** and enter the password. To display the password in plain text, click in the checkbox next to the field.
- If the VRA is connecting to the host with a password and the password for the host has changed, enter the new password. To display the password in plain text, click in the checkbox next to the field.
To change the recovery host required by the VRA to access the host.

**Alert icon status indicator** - The color indicates the status of the alert:
- **Green icon** - The virtual machine can be moved to the replacement host.
- **Red icon** - The virtual machine cannot be moved to the replacement host.

**Direction** - The direction of the replication, from this site to the remote site or from the remote site to this site.

**VM Name** - The name of the virtual machine.

**VPG Name** - The name of the VPG.

**ZORG** - The Zerto name given to the organization, the ZORG, by a cloud service provider. For details, refer to Zerto Cloud Manager Administration Guide.

**VM Size GB** - The virtual machine size in gigabytes.

**# of Volumes** - The number of volumes used by the virtual machine.

**VM Hardware Version** - The hardware version of the virtual machine.

**Select the replacement host** - The name of the host to move the recovery virtual machines information.
Checkpoints Dialog

When selecting the point to recover to, remember the following:

- The refresh button is initially grayed out and is enabled for clicking after 5 seconds. It is also grayed out for 5 seconds after being clicked, before being re-enabled.
- A reminder, **Click the refresh button to view the latest checkpoints** is displayed 10 seconds after the refresh button is clicked to remind the user that there is a new Latest Checkpoint.
- If the user has scrolled to, and selected, a checkpoint anywhere in the checkpoints list, clicking the refresh button will automatically return the user to the selected checkpoint in the list.

Use the following filters:

- **Latest**: Recovery is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery. When selecting the latest checkpoint, the checkpoint used is the latest at this point. If a checkpoint is added between this point and starting the failover, the later checkpoint is not used.
- **Latest Tagged Checkpoint**: The recovery operation is to the latest checkpoint added in one of the following situations:
  - By a user.
  - When a failover test was previously performed on the VPG which includes the virtual machine.
  - When the virtual machine was added to an existing VPG after the added virtual machine was synchronized.
- **Select from all available checkpoints**: If you do not want to use the latest checkpoint, latest tagged checkpoint, choose **Select from all available checkpoints**. By default, this option displays all checkpoints in the system. You can choose to display only automatic, or tagged checkpoints, or any combination of these types.
Configure and Install VRA Dialog

Host - The host on which the VRA is installed. The drop-down displays the hosts that do not have a VRA installed, with the selected host displayed by default.

From ESXi 5.5, by default, Zerto Virtual Manager uses a vSphere Installation Bundle, VIB, to connect to the host. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and logs it.

For ESXi versions earlier than 5.5, when using a password, root access is required. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is issued, requesting the user enter the new password.

Use credentials to connect to host - When unchecked, the Zerto Virtual Manager uses VIB to connect to the host. This field is only relevant for ESXi 5.5 and later.

Host Root Password - When the VRA should connect to the host with a password, check Use credential to connect to host and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts.

Datastore - The datastore that the VRA will use for protected virtual machine data on the recovery site, including the journals. You can install more than one VRA on the same datastore.

Network - The network used to access the VRA.

VRA RAM - The amount of memory to allocate to the VRA. The amount determines the maximum buffer size for the VRA for buffering I/Os written by the protected virtual machines, before the writes are sent over the network to the recovery VRA. The recovery VRA also buffers the incoming I/Os until they are written to the journal. If a buffer becomes full, a Bitmap Sync is performed after space is freed up in the buffer.

<table>
<thead>
<tr>
<th>AMOUNT OF VRA RAM</th>
<th>VRA BUFFER POOL SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1GB</td>
<td>450MB</td>
</tr>
<tr>
<td>2GB</td>
<td>1450MB</td>
</tr>
<tr>
<td>3GB</td>
<td>2300MB</td>
</tr>
</tbody>
</table>

Configure and Install VRA Dialog
The protecting VRA can use 90% of the buffer for IOs to send over the network and the recovery VRA can use 75% of the buffer. That is, for example, a protecting VRA defined with 2GB of RAM can buffer approximately 1305MB before the buffer is full and a Bitmap Sync is required.

**VRA Group** - Specify the VRA Group as free text to identify the group or select from a previously specified group. You group VRAs together when VRAs use different networks so they can be grouped by network, for example when the protected and recovery sites are the same site and you want to replicate to different datastores in the site. The group name is free text you use to identify the group.

The priority assigned to a VPG dictates the bandwidth used. The Zerto Virtual Manager distributes bandwidth among the VRAs based on this priority and the VPGs with higher priorities are handled before writes from VPGs with lower priorities.

To create a new group, enter the new group name over the text *New group* and click *CREATE*.

**Configuration** – Either have the IP address allocated via a static IP address or a DHCP server. The Static option is the recommended option.

**Address** – The IP address for the VRA.

**Subnet Mask** – The subnet mask for the network. The default value is `255.255.255.0`.

**Default Gateway** – The default mask for the network.

---

**Configure Paired Site Routing Dialog**

<table>
<thead>
<tr>
<th>AMOUNT OF VRA RAM</th>
<th>VRA BUFFER POOL SIZE</th>
</tr>
</thead>
<tbody>
<tr>
<td>4GB</td>
<td>3,300MB</td>
</tr>
<tr>
<td>5GB</td>
<td>4,300MB</td>
</tr>
<tr>
<td>6GB</td>
<td>5,300MB</td>
</tr>
<tr>
<td>7GB</td>
<td>6,300MB</td>
</tr>
<tr>
<td>8GB</td>
<td>7,300MB</td>
</tr>
<tr>
<td>9GB</td>
<td>8,300MB</td>
</tr>
<tr>
<td>10GB</td>
<td>9,300MB</td>
</tr>
<tr>
<td>11GB</td>
<td>10,300MB</td>
</tr>
<tr>
<td>12GB</td>
<td>11,300MB</td>
</tr>
<tr>
<td>13GB</td>
<td>12,300MB</td>
</tr>
<tr>
<td>14GB</td>
<td>13,300MB</td>
</tr>
<tr>
<td>15GB</td>
<td>14,300MB</td>
</tr>
<tr>
<td>16GB</td>
<td>15,300MB</td>
</tr>
</tbody>
</table>

The IP address, subnet mask, and gateway to access the peer site VRAs when access to the peer site VRAs is not via the default gateway.
Configure Provider vDCs Dialog

Accessed from Site Settings > Cloud Settings tab > Datastore Configuration area.

Used by Zerto Cloud Service Providers to define provider vDCs, and to define which datastores can be used by Zerto, to which purpose.

Datastores which are not listed in this window may be used by Zerto, unless they are explicitly excluded.

To configure access to provider vDCs, and their datastore’s configuration:

1. In the Provider vDCs area (top), click Add. A list of provider vDCs appear.
   - The provider vDCs were created by the Cloud Service Providers according to predefined service levels, storage availability, performance requirements or cost.
     - Add the provider vDCs which will be available for use in Zerto Virtual Replication.

2. In the Provider Datastore area select one of the following:
   - **Unlisted datastores are not used by Zerto Virtual Replication**: Clearly define that datastores which are not listed in this window cannot be used.
   - **Unlisted datastores can be used for all purposes**: Allow unlisted datastores of all provider vDCs, even those provider vDCs that were not added to the list of Provider vDCs can be used for any purpose.

3. In the Provider Datastore area, click Add, to add datastores.
Select the **Recovery Volume** checkbox, if the datastore can be used as a recovery datastore.

Select the **Journal** checkbox if the datastore can be used for the journal.

Select the **Preseed** checkbox if the datastore can be used for preseeded disks. Only datastores marked as preseeded can be used, preventing different organizations being exposed to datastores of other customers using the preseed option.

In order to exclude a datastore, add it to the list, then deselect all checkboxes.

### Configure VM Settings Dialog

Specifies the values to use when restoring the selected virtual machines.

- **Restore on Host:** The IP address of the host where you want the virtual machine restored.
- **Restore on Datastore:** The datastore to use for the restored virtual machine files.
- **Power On:** Select this if you want the restored virtual machine to be powered on.

### Configure Volume Dialog (vCD)

Used only in environments with vCD.

To configure the datastore for recovery. If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed.

- **Temp Data disk:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, you can specify a mirror disk for replication that is marked as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

- **Volume Source > vCD Managed Storage policy:** Zerto will select a datastore, from the list of available datastores, in the selected Storage Policy in which to place the Volume, unless the datastore is excluded in the Configure Provider vDCs Dialog.
  - If there are several valid datastores, the datastore with the most available space is selected.

- Zerto recalculates the datastore available space for each volume sequentially, taking into consideration previously allocated volumes.
**Volume Source > Preseeded volume:** A virtual disk (the VMDK flat file and descriptor) in the recovery site that has been prepared with a copy of the protected data. Zerto recommends using this option particularly for large disks so that the initial synchronization is much faster since a Delta Sync is used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When not using a preseeded disk the initial synchronization phase has to copy the whole disk over the WAN. Browse to the preseed folder configured for the customer and the disk name, of the preseeded disk. In order to use a preseeded VMDK, do the following:

- Create a folder in vCD to use for the preseeded disks in the datastore you want to use for the customer.
- To use preseeded disks, a provider datastore must have been specified for preseeded disks in the “Configure Provider vDCs Dialog”, on page 364 dialog.
- When using a preseeded VMDK, you specify the exact location, the preseed folder configured for the customer and the disk name, of the preseeded disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.
- If the VPG is defined for a **Zerto Organization (ZORG)**, the location of the preseeded disk must be defined in the **Zerto Cloud Manager**. For details, see **Zerto Cloud Manager Administration Guide**.
- If the virtual machine has **more than one preseeded disk**, these disks must reside on the **same datastore**.
- If the preseeded disk is **greater than 1TB on NFS storage**, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See VMware documentation which describes the configuration option to tune the RPC timeout parameter using the command: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externallId=1027919

```
esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout
```

**Note:** Zerto Virtual Replication supports the **SCSI protocol**. Only disks that support this protocol can be specified.

---

**Edit NIC Dialog**

Specify the NIC settings when restoring an offsite backup to the recovery site.

- **NIC Name** – The name of the selected NIC.
- **Network** – The network to use for the restored virtual machine.
- **Create new MAC address** – The Media Access Control address (MAC address) to use. The default is to use the same MAC address for the restored virtual machine that was used in the protected site. Check the box to create a new MAC address on the restore site.
- **Change vNIC IP Configuration** – Whether or not to keep the default virtual NIC (vNIC) IP configuration. The vNIC IP is changed after the restore has completed when VMware Tools are installed. If **Static** is selected, the IP address, subnet mask, and default gateway must be set. If **DHCP** is selected, the IP configuration and DNS server configurations are assigned automatically, to match the protected virtual machine.
The Zerto Virtual Manager User Interface

- **IP Address** – The IP for the restored virtual machine. This can be the same IP as the original protected virtual machine.
- **Subnet Mask** – The subnet mask for the network. The default value is 255.255.255.0.
- **Default Gateway** – The default mask for the network.
- **Preferred DNS Server** – The IP address of the primary DNS server to handle Internet protocol mapping.
- **Alternate DNS Server** – The IP address of the alternate DNS server.
- **DNS Suffix** – The DNS name excluding the host.

**Edit Repository Dialog**

Edits a repository used for backups.

**Repository Name** – The name of the repository.

**Repository Type** – The type of repository. The options are Local or Network Share (SMB). If Local is specified, backups are stored on the local machine where the Zerto Virtual Manager is installed. If Network Share (SMB) is specified, the network share drive must be an SMB drive and if specified the username and password to access the drive must be provided.

**Username** – The username to access the Network Share drive. The name can be entered using either of the following formats:

- username
- domain\username

This field is not displayed when the type is Local.

**Password** – The password to access the Network Share drive. This field is not displayed when the type is Local.

**Path** – The path where the repository resides. The path must be accessible from the Zerto Virtual Manager, so if the repository is on a different domain than the Zerto Virtual Manager, the domain must be included in the path.

**Free Space** – The amount of free space currently available for the repository.

**Used Space** – The amount of space currently used in the repository.

**Capacity** – The overall capacity of the repository.

**VALIDATE** – Click to validate the path. The path must be valid in order to save the information.

**Enable compression** – Check this option to compress backups stored in the repository. Compression is done using zip compression, set to level six. If you want better compression, which requires more CPU, or less compression to reduce the CPU overhead, contact Zerto support.

**Set as default repository** – Check this option to make the repository the default repository.
Edit Selected Volumes Dialog

If more than one datastore is selected, the path is not displayed.

- **Datastore / Raw Disk** – The storage or RDM disk where the virtual machine files will be restored.
- **Thin** – Whether the virtual machine disks will be thin-provisioned or not.

Edit VM Dialog

Edit the replication settings for a particular virtual machine in a VPG.

- **Recovery Host** – The cluster, resource pool, or host that will host the recovered virtual machine. If the site is defined in Zerto Cloud Manager, only a resource pool can be specified and the resource pool must also have been defined in Zerto Cloud Manager. For details about Zerto Cloud Manager, see [Zerto Cloud Manager Administration Guide](#).

When a resource pool is specified, Zerto Virtual Replication checks that the resource pool capacity is enough for the specified virtual machine.

- **VM Recovery Datastore** – The datastore where the VMware metadata files for the virtual machine are stored, such as the vmx file. If a cluster or resource pool is selected for the host, only datastores that are accessible by every ESX/ESXi host in the cluster or resource pool are displayed. This is also the datastore where RDM backing files for recovery volumes are located. When specifying the recovery datastore for a virtual machine with a storage cluster, specify a datastore in the cluster.

- **Journal Size Hard Limit** – The maximum size that the journal can grow, either as a percentage or a fixed amount. The minimum journal size, set by Zerto Virtual Replication, is 8GB. The journal is always thin-provisioned.
  - **Unlimited** – The size of the journal is unlimited and it can grow to the size of the recovery datastore. If **Unlimited** is chosen, the fields **Size** and **Percentage** are not relevant.
  - **Size (GB)** – The maximum journal size in GB.
  - **Percentage** – The percentage of the virtual machine volume size the journal can grow to.

- **Journal Size Warning Threshold** – The size of the journal that triggers a warning that the journal is nearing its hard limit.
  - **Unlimited** – The size of the journal is unlimited and it can grow to the size of the recovery datastore. If **Unlimited** is chosen, the fields **Size** and **Percentage** are not relevant.
  - **Size (GB)** – The size in GB that will generate a warning.
  - **Percentage** – The percentage of the virtual machine volume size that will generate a warning.
Both the value of Size and Percentage must be less than the configured hard limit so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.

**Journal Datastore** - The datastore used for the journal data for each virtual machine in the VPG. To change the default, specify a host and then select one of the datastores accessible by this host to be used as the journal datastore. When you select specific journal datastore, the journals for each virtual machine in the VPG are stored in this datastore, regardless of where the recovery datastores are for each virtual machine. In this case, all the protected virtual machines must be recovered to hosts that can access the specified journal datastore.

**Edit VM Dialog (vCD)**

![Edit VM Dialog](image)

Used **only** in environments with **vCD**.

- **Storage Policy**: The Storage Policy in which the **VM configuration files** will reside. For considerations, see step 1.
- **Journal Storage Policy**: The Storage Policy in which the **VM Journal files** will reside. For considerations, see step 2.

1. When selecting **Storage Policy**, consider the following:
   - Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - Zerto will try to determine a default Storage Policy according to:
     - A Storage Policy with the same name as the protected Storage Policy.
     - The default Orgvdc Storage Policy.
   If Zerto did not manage to determine a default Storage Policy, this field appears empty.

   - When you **click to edit**, a list of Storage Policies appear. These Storage Policies:
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
     - Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.
     - To review site-specific configurations, see Configure Provider vDCs Dialog.

2. When selecting **Journal Storage Policy**, consider the following:
   - Zerto will select a datastore from the selected Storage Policy in which to place the Journal files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - The default Journal Storage Policy is the same as the default VM Storage Policy.
   - If Zerto did not manage to determine a default Journal Storage Policy, this field appears empty.
   - When you **click to edit**, the option **Auto Select** appears, and a list of Storage Policies.
   - The list of Storage Policies associated with the Journal:
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
     - Have at least one Datastore that was not excluded as a **Journal** in the Configure Provider vDCs Dialog.
     - **Auto Select**: Selecting this means that the journal can be placed in any datastore visible to the host that Zerto selected for recovery, unless the datastore is excluded in the Configure Provider vDCs Dialog.
### Setting & Description

#### Journal History

The time that all write commands are saved in the journal. The longer the information is saved in the journal, the more space is required for each journal in the VPG.

<table>
<thead>
<tr>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of <strong>hours</strong> from 1 to 24</td>
</tr>
<tr>
<td>Number of <strong>days</strong> from 2 to 30</td>
</tr>
</tbody>
</table>

#### Default Journal Storage (Hyper-V), or Default Journal Datastore (vSphere)

The storage/datastore used for the journal data for each virtual machine in the VPG.

**Note:** This field is **not** relevant when replicating to a **vCD** recovery site.

<table>
<thead>
<tr>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select the storage/datastore accessible to the host.</td>
</tr>
<tr>
<td>When you select a specific journal storage/datastore, the journals for each virtual machine in the VPG are stored in this storage/datastore, regardless of where the recovery storage/datastore is for each virtual machine. All protected virtual machines are recovered to the hosts that can access the specified journal storage/datastore.</td>
</tr>
</tbody>
</table>

#### Journal Size Hard Limit

The maximum size that the journal can grow, either as a percentage or a fixed amount. The journal is always **thin-provisioned**.

**Note:** The Journal Size Hard Limit applies independently **both** to the Journal History and also to the Scratch Journal Volume.

*For Example:* If the Journal Size Hard Limit is configured to a maximum size of 160 GB limit, then during Failover Test, both the Journal History and the Scratch Journal Volume together can take up to 320 GB. Each one with a maximum size of 160 GB limit.

<table>
<thead>
<tr>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong> The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.</td>
</tr>
<tr>
<td>If Unlimited is selected, Size and Percentage options are <strong>not</strong> displayed.</td>
</tr>
<tr>
<td><strong>Size (GB):</strong> The maximum journal size in GB.</td>
</tr>
<tr>
<td><strong>The minimum</strong> journal size, set by Zerto Virtual Replication, is <strong>8GB</strong> for Hyper-V and vSphere environments, and <strong>10GB</strong> for Microsoft Azure environments.</td>
</tr>
<tr>
<td><strong>Percentage:</strong> The percentage of the virtual machine volume size to which the journal can grow.</td>
</tr>
<tr>
<td>This value can be configured to more than 100% of the protected VM's volume size.</td>
</tr>
</tbody>
</table>

#### Journal Size Warning Threshold

The size of the journal that triggers a warning that the journal is nearing its hard limit.

<table>
<thead>
<tr>
<th>SELECT...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Unlimited:</strong> The size of the journal is unlimited and it can grow to the size of the recovery storage/datastore.</td>
</tr>
<tr>
<td>If Unlimited is selected, Size and Percentage options are <strong>not</strong> displayed.</td>
</tr>
<tr>
<td><strong>Size</strong> (GB): The size in GB that will generate a warning.</td>
</tr>
<tr>
<td><strong>Percentage</strong>: The percentage of the virtual machine volume size that will generate a warning.</td>
</tr>
</tbody>
</table>

*The values of **Size** and **Percentage** must be less than the configured Journal Size Hard Limit so that the warning will be generated when needed. In addition to the warning threshold, Zerto Virtual Replication will issue a message when the free space available for the journal is almost full.*
Edit VM Settings Dialog (AWS)

Edit the network settings for one or more virtual machines in a VPG that will be recovered to AWS. There are recovery settings for failovers and moves, and for failover tests.

**Import Method**
- **AWS Import**: The method that has been used in all past implementations.
- **Zerto Import for all volumes**: This is the fastest import method and uses a zImport VM for all volumes. A zImport virtual machine is created, per volume. For each recovered volume, the zImport virtual machine is terminated when all the data has been imported and its disk has been attached to the recovered virtual machine.
- **Zerto Import for data volumes**: Uses the zImport method for data volumes only. This is the default setting and has a faster RTO than AWS Import.

**VPC Network**: A virtual network dedicated to your AWS account.

**Subnet**: A range of IP addresses in your VPC.

**Security Group**: The AWS security to be associated with the virtual machines in this VPG. You can associate one or more security groups with the virtual machines.

**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 virtual machine protected 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.

**Private IP**: The private IP of an instance from the selected subnet. If you do not set the private IP, during recovery, AWS sets the private IP from the defined subnet range.
Edit VM Settings Dialog (Azure)

Edit the network settings for one or more virtual machines in a V_PG that will be recovered to Azure. There are recovery settings for failovers and moves, and for failover tests.

**VNet:** A The virtual network dedicated to your Azure subscription.

**Subnet:** A range of IP addresses in your VPC.

**Network Security Group:** The Azure network security to be associated with the virtual machines in this V_PG. You can associate one or more network security groups with the virtual machines.

**Instance Family:** The instance family from which to select the type. Azure instance families are optimized for different types of applications. Choose the instance family appropriate for the application in the virtual machine protected in the V_PG.

**Instance Type:** The instance size, within the instance family, to assign to recovered instances. Different sizes 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.

**Private IP:** The private IP of an instance from the selected subnet. If you do not set the private IP, during recovery, Azure sets the private IP from the defined subnet range.

Edit vNIC Dialog
To configure the NIC used for the replicated VM disks. You can configure a maximum of four NICs.

**Note:** You can only change the vNIC IP for virtual machines with VMware Tools running.

Specify the network details to use for the recovered virtual machines after a live recovery or migration, in the **Failover/Move** column, and for the recovered virtual machines when testing replication, in the **Test** column.

**Network** – The recovery site network to use. For testing, this network can be a fenced-out network to avoid impacting the production network.

**Create New MAC Address** – Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites.

**Change vNIC IP Configuration** – Whether or not to keep the default virtual NIC (vNIC) IP configuration. You can only change the vNIC IP after recovery has completed with VMware Tools installed.

To change the vNIC IP, select **Yes** in the **Failover/Move** or **Test** column. If you select a static IP connection, set the IP address, subnet mask, and default gateway. Optionally, change the preferred and alternate DNS server IPs and the DNS suffix. If you select DHCP, the IP configuration and DNS server configurations are assigned automatically, to match the protected virtual machine. You can change the DNS suffix.

If the virtual machine has multiple NICs but is configured to only have a single default gateway, fill in a 0 for each octet in the **Default gateway** field for the NICs with no default gateway.

**Note:** During a failover, move, or test failover, if the recovered virtual machine is assigned a different IP than the original IP, after the virtual machine has started it is automatically rebooted so that it starts up with the correct IP. If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.

**Copy to failover test** – When clicked, copies the settings in the **Failover/Move** column to the **Test** column.

**Copy to failover/move** – When clicked, copies the settings in the **Test** column to the **Failover/Move** column.

### Edit vNIC Dialog (vCD)

Used only in environments with vCD.

To configure the network details to use for the recovered virtual machines after a FAILOVER or MOVE or TEST operation:
**Network**: The network to use for this virtual machine.

**MAC Address**: Whether the Media Access Control address (MAC address) used on the protected site should be replicated on the recovery site. The default is to use the same MAC address on both sites.

**vNIC IP Mode**: Which IP mode to use. If you define static IP pool, also specify the IP address.

### NOTE:

During a FAILOVER, MOVE, or TEST failover:

- If the recovered virtual machine is assigned a different IP than the original IP, then after the virtual machine has started, it is automatically rebooted so that it starts up with the correct IP.

- If the same network is used for both production and test failovers, Zerto recommends changing the IP address for the virtual machines started for the test, so that there is no IP clash between the test machines and the production machines.

**Copy to failover test**: Copies the settings in the Failover/Move column to the Test column.

**Copy to failover/move**: Copies the settings in the Test column to the Failover/Move column.

### Edit Volumes Dialog

To edit recovery datastore information for a protected virtual machine.

**Volume Source**: The source on the recovery site for the replicated data: **Datastore, RDM** or **Preseeded volume**.

#### Volume Source > Datastore

**Datastore**: A new volume is used for replicated data. Specify the datastore to use to create disks for the replicated data. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned.

The datastore specified for replication must have at least the same amount of space as the protected volume and an additional amount for the journal. The amount of additional space needed for the journal can be fixed by specifying a maximum size for the journal, or can be calculated as the average change rate for the virtual machines in the VPG, multiplied by the length of time specified for the journal history.

You can use the vSphere Client console Performance tab for each virtual machine to help estimate the change rate. For more details, refer to “WAN Sizing Requirements with Zerto Virtual Replication”, on page 26.

Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

#### Volume Source > RDM

**Raw Disk**: The VMware RDM (Raw Device Mapping) to use for the replication.
By default, RDM is recovered as **thin-provisioned** VMDK in the datastore specified in the **VM Recovery Datastore** field in the Edit VM dialog, and **not to RDM**.

You cannot define an RDM disk if the virtual machine uses a BusLogic SCSI controller, nor when protecting or recovering virtual machines in an environment running vCenter Server 5.x with ESX/ESXi version 4.1 hosts.

Only a raw disk with the same size as the protected disk can be selected from the list of available raw disks. Other raw disks with different sizes are not available for selection.

The RDM is always stored in the recovery datastore used for the virtual machine.

The following **limitations** apply to protecting RDM disks:

- RDM disks with an even number of blocks can replicate to RDM disks of the same size with an even number of blocks and to VMDKs.
- RDM disks with an odd number of blocks can only replicate to RDM disks of the same size with an odd number of blocks and not to VMDKs.

### Volume Source > Preseeded volume

Whether to copy the protected data to a virtual disk in the recovery site. Zerto recommends using this option particularly for large disks so that the initial synchronization will be faster since a **Delta Sync** can be used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When not using a preseeded disk, the initial synchronization phase must copy the whole disk over the WAN. When using a preseeded virtual disk, you select the datastore and exact location, folder, and name of the preseeded disk, which cannot be an IDE disk. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Only disks with the same size as the protected disk can be selected when browsing for a preseeded disk. The datastore where the preseeded disk is placed is also used as the recovery datastore for the replicated data.

If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. See the VMware documentation, [http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919), which describes the configuration option to tune the RPC timeout parameter using the `esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout` command.

Note the following conditions:

- If the protected disks are non-default geometry, configure the VPG using preseeded volumes.
- If the protected disk is an RDM disk, it can be used to preseed to a recovery VMDK disk. Zerto Virtual Replication makes sure that the VMDK disk size is a correct match for the RDM disk.
- If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, see [Zerto Cloud Manager Administration Guide](http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919).

**Datapstore:** The datastore where the preseeded disk is located.

**Path:** The full path to the preseeded disk.

**Temp Data disk:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, specify a mirror disk for replication that is marked as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

**Thin provisioning:** If the recovery volumes are thin-provisioned or not.
Edit Volumes Dialog (vCD)

Used only in environments with vCD.

To edit storage information for one of the virtual machines volumes, in the STORAGE tab select the volume/s and click EDIT SELECTED.

1. **Volume Source:** The source on the recovery site for the replicated data.
   - **vCD managed storage policy:** Zerto will select a datastore, from the list of available datastores, in the selected Storage Policy in which to place the Volume, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - If there are several valid datastores, the datastore with the most available space is selected.
   - Zerto recalculates the datastore available space for each volume sequentially, taking into consideration previously allocated volumes.
   - **Preseeded volume:** A virtual disk (the VMDK flat file and descriptor) in the recovery site that has been prepared with a copy of the protected data. Zerto recommends using this option particularly for large disks so that the initial synchronization is much faster since a Delta Sync is used to synchronize any changes written to the recovery site after the creation of the preseeded disk. When not using a preseeded disk the initial synchronization phase has to copy the whole disk over the WAN. Browse to the preseed folder configured for the customer and the disk name, of the preseeded disk. In order to use a preseeded VMDK, do the following:
     - Create a folder in vCD to use for the preseeded disks in the datastore you want to use for the customer.
     - Specify this datastore as a provider datastore for preseeded disks in the Configure Provider vDCs dialog, from the Advanced Settings dialog, as described in Zerto Cloud Manager Administration Guide.
     - In the Zerto Cloud Manager specify the Preseed Folder Name for the ZORG, in the Manage ZORG tab.
   Zerto Virtual Replication searches for the preseeded folder in the available datastores in the Org vDCs specified in the vCD Cloud Resources for the ZORG in the Zerto Cloud Manager and takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA. Note that if the virtual machine has more than one preseeded disk, these disks must reside on the same datastore. If the preseeded disk is greater than 1TB on NFS storage, the VPG creation might fail. This is a known VMware problem when the NFS client does not wait for sufficient time for the NFS storage array to initialize the virtual disk after the RPC parameter of the NFS client times out. The timeout default value is 10 seconds. Refer to the VMware documentation, http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1027919, which describes the configuration option to tune the RPC timeout parameter using the esxcfg-advcfg -s <Timeout> /NFS/SetAttrRPCTimeout command.
   - If the VPG is being defined for a Zerto Organization, ZORG, the location of the preseeded disk must be defined in the Zerto Cloud Manager. For details, refer to Zerto Cloud Manager Administration Guide.
   Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified. Virtual machine RDMs in a vCenter Server are replicated as VMDKs in a vCD environment.

2. **Specify the Storage Policy** for recovery from one of the options. When selecting the Storage Policy, consider the following:
   - Storage Policy per volume is supported only in vCD supported versions, and when the selected Orgvdc is not configured for fast provisioning.
   - Zerto will select a datastore from the selected Storage Policy in which to place these files, unless the datastore is excluded in the Configure Provider vDCs Dialog.
   - The Storage Policies which appear in the drop-down list:
     - Include the **Use VM Default** option (default), which will apply the VM's storage policy to this volume. This is also the Storage Policy default value.
     - Were defined in VMware vCloud Director and are configured in the Orgvdc.
     - Have at least one Datastore that was not excluded as a Recovery Volume in the Configure Provider vDCs Dialog.
     - To review site-specific configurations, see Configure Provider vDCs Dialog.
3. **Temp Data Disk:** If the virtual machine to be replicated includes a temp data disk as part of its configuration, specify a mirror disk for replication that is marked as a temp data disk. In this case, data is not replicated to the temp data disk after initial synchronization.

Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.

4. You can specify whether the recovery volume is **thin-provisioned** or not, unless the Org vDC only supports thin-provisioned volumes.

**Edit VRA Dialog**

To change the network settings for a VRA, for example when the gateway to the VRA is changed.

**Host** - The IP of the host on which the VRA is installed.

For ESXi 5.5 and later hosts, by default, Zerto Virtual Manager uses a vSphere Installation Bundle, VIB, to connect to the host. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and notes this in the log.

When using a password, root access is required if the Zerto host component is down and needs an automatic restart. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is triggered, requesting the user enter the new password.

- **Use credentials to connect to host** - When unchecked, the Zerto Virtual Manager uses VIB to connect to the host. This field is only relevant for ESXi 5.5 and later.
- **Host Root Password** - When the VRA should connect to the host with a password, check **Use credential to connect to host** and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts.
- **VRA Group** - The free text to identify the group to which a VRA belongs. If you create a group and then change the name when editing the VRA so that there is no VRA in the site that belongs to the originally specified group, the group is automatically deleted from the system.

To create a new group, enter the new group name over the text **New group** and click **CREATE**.

- **Configuration** - Either have the IP address allocated via a static IP address or a DHCP server. If the VRA was originally installed with a static IP, you cannot change this to DHCP. If the VRA was originally installed to use a DHCP server, you can change this to use a static IP.
- **Address** - The static IP address for the VRA to communicate with the Zerto Virtual Manager.
- **Subnet Mask** - The subnet mask for the network. The default value is **255.255.255.0**.
License Dialog

The Zerto license includes information such as the number of virtual machines that can be protected and the license expiry date.

The cloud and enterprise license include the following details:

- **License** – The license key itself.
- **License Type** – What is licensed: whether the license restricts the number of virtual machines that can be protected or the number of sockets used.
- **Expiry Date** – The license expiry date.
- **Quantity** – The maximum number of virtual machines or sockets licensed, based on the license type. If blank, the quantity is unlimited.

An enterprise license also includes the following:

- **Usage** – The sites using the license and number of protected virtual machines in each site. The number of virtual machines is independent of whether they are in vApps or not.
**Manage Static Routes Dialog**

When providing DR as a Service, the cloud service provider needs to ensure complete separation between the organization network and the cloud service provider network. The cloud service provider needs to be able to route traffic between an organization network and the cloud replication network, in a secure manner without going through complex network and routing setups.

The cloud service provider can define a Zerto Cloud Connector per organization site, that has two Ethernet interfaces, one to the organization’s network and one to the cloud service provider’s network. If the cloud service provider wants to add additional security, considering both cloud connector interfaces as part of the organization network, the cloud service provider can define a static route that will hop to a different cloud network, specifically for use by the Zerto Virtual Manager and VRAs in the cloud site.

**ADD** – Click this field to add an entity and to define the static route it will use. Once you click ADD, the dialog changes:

![Manage Static Routes Dialog](image)

**NEW GROUP** – Defines a group that will use a static route to the subnet used by the Zerto Virtual Manager. Enter the name of the organization that will use this static route.

**Add Static Route** – Opens the Add Static Route Dialog.

---

**New Repository Dialog**

You define the repositories where offsite backups are defined on the recovery site and can be stored, either locally at the recovery site, or on a network share that uses the SMB, Server Message Block, protocol. The repository where you want this offsite backup stored is specified when an offsite backup is defined.
To create an offsite backup repository:
1. In the Zerto User Interface, click SETUP > REPOSITORIES.
2. Click NEW REPOSITORY.
   The New Repository dialog is displayed.

3. Specify the following settings:
   - **Repository Name:** Specify a unique name for the repository.
   - **Repository Type:** Specify the type of repository:
     - **Local:** Backups are stored on the local machine where the Zerto Virtual Manager is installed.
     - **Network Share (SMB):** The network share drive must be an SMB drive and if specified, the username and password to access the drive must be provided.
       When the repository location is a network drive, this drive can be mounted to third party storage, such as Amazon Web Services, AWS, or Microsoft Azure.
       Using TntDrive, from Amazon, enables you to save your offsite backups to a cloud repository mounted disk as if you are using a LAN or locally mounted drive. You can mount one or more Amazon S3 buckets as network drives or as removable local drives, and to use them exactly as you would use any other drive folder on your computer.
   - **Username:** Username to access the Network Share drive.
     This field is not displayed when the type is **Local**.
     The username can be entered using either of the following formats:
     - username
     - domain\username
   - **Password:** Password to access the Network Share drive. This field is not displayed when the type is **Local**.
   - **Path:** The path where the repository will reside. The path must be accessible from the Zerto Virtual Manager, so if the repository is on a different domain to the Zerto Virtual Manager, the domain must be included in the path.
     - **Set as default repository:** Select this to use the repository as the default when specifying extended recovery in a VPG.

4. Click **VALIDATE**. You must validate the path specified. If the folder does not exist, you are asked if you want to create it.
5. Click **SAVE**.
   The repository is created.
NICs Dialog

When restoring an offsite backup to the recovery site, this dialog shows the NIC settings for the virtual machines in the VPG. You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit the NIC settings for several virtual machines at the same time by selecting the NICs and clicking EDIT SELECTED.

For more details, see “Restore Volumes Dialog”, on page 386.

Offsite Clone Window

To create a clone of each virtual machine in a VPG on the recovery site in the production network. The clone is a copy of the protected virtual machines on the recovery site, while the virtual machines on the protected site remain protected and live.

SELECT A CHECKPOINT button – Opens the Checkpoints Dialog dialog to select the checkpoint to use to make the clone.

Recovery Datastore – Select the datastore to use for the recovery virtual machines.

Open Support Ticket Dialog

Support tickets can be opened directly in the Zerto User Interface.

Creating a support ticket in the Zerto User Interface simplifies the submission process since much of the information that is required when entering a ticket using the Zerto Support Portal, such as the version and build numbers, is automatically added to the ticket when it is submitted via the Zerto User Interface.
In addition, when the ticket is submitted, a snapshot of the current environment is also attached to the ticket. The snapshot information includes the lists of alerts, events, tasks, VPGs, and virtual machines that are protected.

This information is used to help Zerto resolve the ticket quickly and, whenever possible, without the need to request more information from you.

**Note:** 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. If the clocks are not synchronized with UTC, submitting a support ticket can fail.

**To open a support ticket:**

1. In the Zerto User Interface, click **SETTING ( )** in the top right of the header and select **Submit Support Ticket**. The Open Support Ticket dialog for the site is displayed.

2. Specify the ticket details:
   - **Subject:** The subject of the support ticket.
   - **Type:** The type of ticket being opened. Available options are:
     - Problem
     - Feature Request
     - Question
   - **Severity:** The severity of the issue.
   - **Description:** A description of the problem or question in addition to the information supplied in the subject.
   - **Allow remote log collection:** How many logs is Zerto allowed to collect. Available options are:
     - Only for this ticket
     - For the next 30 days
     - Never
   - **SSP Email Address:** A valid email address registered with Zerto, with permission to open tickets.

3. Click **SUBMIT**.

   The ticket is processed and its progress is displayed. If the email address is not valid, the ticket is rejected. Once the ticket submission starts, it cannot be canceled.
Remote Support Dialog

Remote Log Collection allows customers to authorize Zerto support engineers to collect logs from their environment. By using remote log collection customers can avoid having to use the Diagnostic Tool on their ZVM server in order to collect logs for analysis, a potentially complex and time-consuming procedure.

- **Never**: Remote log collection is not allowed (default). If remote log collection is currently is allowed, it will be terminated if you select this option.
- **For the next 30 days**: Remote log collection is allowed. This permission will automatically terminate in 30 days unless terminated by selecting the **Never** option.
- **Only for a specific case**: You will be prompted to enter the Case number opened via the Salesforce Self-service Portal. Remote log collection will be allowed for as long as the case is active or until remote log collection is terminated by selecting the **Never** option.
Restore from Zerto Backup

To restore the virtual machines in a VPG from the backup list or the repository where the offsite backup was saved.

If the VPG backups were saved to more than one repository, selecting the VPG collects all the offsite backups for the VPG from all the available repositories.

When restoring via the VPG option, the VPG must still be available. If the VPG was deleted, the restore must be performed from a repository.

After clicking NEXT, the RESTORE POINT step displays all available offsite backups.

Point in Time: The date and time the offsite backup was performed.

Restore Site: The recovery site for the VPG.
Backup Status: Whether the offsite backup of the virtual machines was fully completed or only partially completed, in which case only some of the virtual machine were fully backed up.

VMs: The number of backed up virtual machines out of the total number of virtual machines.

Volumes: The number of backed up volumes out of the total number of volumes for the virtual machines.

Repository: The name of the repository where the offsite backup is stored.

Compression: A value in this field denotes that the backups stored in the repository are compressed.

ZORG: The Zerto organization for which the offsite backup was created. For details, refer to Zerto Cloud Manager Administration Guide.

Selecting an offsite backup displays the list of virtual machines in the backup, including the following information:

VM Name: The name of the virtual machine in the package.

Backup Status: Whether the offsite backup of the virtual machine was fully completed or only partially completed, in which case only some of the volumes for the virtual machine were backed up.

# Volumes Backed Up: The number of backed up volumes out of the total number of volumes for the virtual machine.

Note: The list of offsite backups is dependent on the whether a daily or weekly backup was specified in the VPG and the retention period. The exact number of offsite backups over time is described in “Offsite Backups”, on page 38.

After clicking NEXT, the VM SETTINGS step displays all virtual machines that can be restored from the selected offsite backup.

For each machine, you specify the host and datastore to use to restore the virtual machine. The following values are applied to all the virtual machines to be restored:

Restore on Host – The IP address of the host where you want the virtual machine restored.

Restore on Datastore – The datastore to use for the restored virtual machine files.

Alternatively, you can use the recovery host and storage specified for each virtual machine in the VPG definition by clicking APPLY VPG CONFIGURATION. The VPG must still be available to use APPLY VPG CONFIGURATION.

You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit host and datastore information of several virtual machines at the same time by selecting the virtual machines and clicking EDIT SELECTED.
The volumes to be restored for the selected virtual machine. You can choose to edit information in one field by clicking the field and updating the information. You can choose to edit information for several datastores or volumes at the same time by selecting the datastores and clicking *EDIT SELECTED*. 
Site Settings Dialog

Contains site-wide settings:

- “Site Information Dialog”, below
- “Performance and Throttling Dialog”, on page 388
- “Policies Dialog”, on page 389
- “Email Settings Dialog”, on page 390
- “Reports Dialog”, on page 391
- “Compatibility Dialog”, on page 392
- “Cloud Settings Dialog”, on page 392

Site Information Dialog

Site Details

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Site10</td>
</tr>
<tr>
<td>Site Location</td>
<td>Unconfigured location</td>
</tr>
<tr>
<td>Contact Name</td>
<td>Unconfigured contact info</td>
</tr>
<tr>
<td>Contact Email</td>
<td>Unconfigured contact email</td>
</tr>
<tr>
<td>Contact Phone</td>
<td>Unconfigured contact phone</td>
</tr>
</tbody>
</table>

User Credentials

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username</td>
<td>administrator</td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
</tbody>
</table>

During installation, information about the site is entered to identify the site in the user interface and to identify the contact person at the site. After installation you can update this information.

- **Site Name**: The name used to identify the site.
- **Site Location**: Information such as the address of the site or a significant name to identify it.
- **Contact Name**: The name of the person to contact if a need arises.
- **Contact Email**: An email address to use if a need arises.
- **Contact Phone**: A phone number to use if a need arises.
- **User Name**: The administrator name used to access the hypervisor management tool. The name can be entered using either of the following formats:
  - username
  - domain\username
- **Password**: The password used to access the hypervisor management tool for the given user name. If the password changes, specify the new password. To ensure security, after saving the settings, the password field is cleared.
Performance and Throttling Dialog

Bandwidth

Bandwidth Throttling

- Limited
- 1 MB/sec

Time-based Throttling

- Limited
- From
- To

Limited: Select to define the limit. The default is bandwidth throttling is Unlimited.

Set the Mb/sec: The valid range is from 0 to 100 Mb/sec. With 0 Mb/Sec, Zerto Virtual Replication automatically assigns the bandwidth used per VPG, based on using the maximum available and then prioritizing the usage according to the priority set for the VPGs sending data over the WAN.

Text box: Mb/sec. when the value required is 100 Mb/sec. or more.

Time-based Throttling: To throttle the bandwidth during specific times. For example, during the daily peak transaction period you can change the bandwidth throttling, to override the general setting.

Limited: Select to define the limit. The default is time-based throttling is Unlimited.

From: The hour and the minute to start the throttling, using a 24-hour clock.

To: The hour and the minute to end the throttling, using a 24-hour clock.

IMPORTANT:

Performance and Throttling > advanced settings must only be changed in coordination with Zerto support.

Enable Bandwidth Regulation: To enable regulating the bandwidth to troubleshoot problems.

Enable IO throttling: If a host is handling too many IOs, then the IOs begin to get high latencies. To offset this the VRA sends fewer concurrent IOs. The latency is measured by taking the average latency for all IOs over a set period of time. For example, when the period is 5000 milliseconds and the bad IO latency is 40, the average latency is calculated every 5 seconds, and if the average latency exceeds 40, the VRA sends fewer concurrent IOs.

Bad IO Latency VM: The threshold above which the latency is considered high, and therefore bad.

Requested Duration (ms): The period of time used to measure the average latency.
Policies Dialog

Failover/Move Commit Policy: The commit policy to use during a failover or move operation. The value set here is the default for all failover or move operations from this point on but can be changed when defining a failover or move operation. The following options are available:

- **None**: The failover or move operation must be manually committed or rolled back by the user.
- **Commit**: After the time specified in the Default Timeout field, the failover or move operation is committed. During the specified time you can check the recovered VPG virtual machines, and you can manually commit or roll back.
- **Rollback**: After the time specified in the Default Timeout field the failover or move operation is rolled back, unless you manually commit it or roll it back before the time out value is reached. During the specified time you can check the recovered VPG virtual machines.

**Default Timeout**: The time-out in minutes after which a Commit or Rollback is performed. A value of zero indicates that the system automatically performs the commit policy, without waiting for any user interaction.

**Default Script Execution Timeout**: The length of time in seconds after which a script times out.

**Enable Replication to Self**: Enable the same site to be used as both the protected and recovery site.

**Replication Pause Time**: The time to pause when synchronizing a VPG if continuing the synchronization will cause all the checkpoints in the journal to be removed.

**US8057** For incoming replication, copy the BIOS UUID of the protected VM to the recovered VM: Select this to preserve the BIOS UUID of the protected VM after recovery operations, in the recovery ZVM Site Settings window.

**Note**: Preserving of the BIOS UUID is not supported in Clone and Self-Replication recovery operations. Preserving of the BIOS UUID is not supported in Public Cloud. Cross replication is not supported.

**Allow Zerto to always enter hosts to maintenance mode during remediation**: When this is selected, if the Virtual Update Manager’s Remediation task is detected, Zerto will automatically enter the host into maintenance mode.

**Note**: Automatic detection and powering off the VRA when running host maintenance mode is supported in vCenter version 6.5. For more information see Zerto Virtual Replication Interoperability Matrix.

In some upgrade environments, Virtual Update Manager requires the host to enter maintenance mode. For further details, see “Support for VMware Virtual Update Manager (VUM)”, on page 251.

Notes:

- Recovery and journal volumes that reside on the host are not automatically migrated to another host in the cluster.
Email Settings Dialog

Define an email address to receive Zerto Virtual Replication alerts and backup reports.

- **SMTP Server Address**: The SMTP server address. The Zerto Virtual Manager must be able to reach this address.
- **SMTP Server Port**: The SMTP server port, if it was changed from the default, 25.
- **Sender Account**: A valid email address for the email sender name.
- **To**: A valid email address where you want to send the email.
- **SEND TEST EMAIL** button: Tests that the email notification is set up correctly. A test email is sent to the email address specified in the To field.
- **Enable sending alerts**: Check to be notified by email about any Zerto Virtual Replication alerts issued. An email is sent when the alert is issued, and after it has been successfully handled and the alert is no longer valid.
- **Enable backup reports**: Defines when backup reports will be emailed.
### Reports Dialog

**Resource Report**

**Sampling Rate [1]**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Daily</td>
<td></td>
</tr>
</tbody>
</table>

**Sampling Time [2]**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>00</td>
</tr>
</tbody>
</table>
Configures the Resource Report.

- **Sampling Rate:** When to take resource samples to identify resource usage, either daily at a specific hour and minute or hourly at a specific minute within each hour. Note that collecting a sample hourly provides a higher resolution picture of replication traffic than if samples are only collected once a day.
- **Sampling Time:** The time that the sample is taken.

### Compatibility Dialog

Supported Host Versions

<table>
<thead>
<tr>
<th>ESX Version</th>
<th>Supported Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX / ESXi 4.0</td>
<td>4.0U1, 4.0U2, 4.0U3, 4.0U4</td>
</tr>
<tr>
<td>ESX / ESXi 4.1</td>
<td>4.1, 4.1U1, 4.1U2, 4.1U3</td>
</tr>
<tr>
<td>ESXi 5.0</td>
<td>5.0, 5.0U1, 5.0U2, 5.0U3</td>
</tr>
<tr>
<td>ESXi 5.1</td>
<td>5.1, 5.1U1, 5.1U2, 5.1U3</td>
</tr>
<tr>
<td>ESXi 5.5</td>
<td>5.5, 5.5U1, 5.5U2, 5.5U3</td>
</tr>
<tr>
<td>ESXi 6.0</td>
<td>6.0, 6.0U1, 6.0U2</td>
</tr>
<tr>
<td>ESXi 6.5</td>
<td>6.5</td>
</tr>
<tr>
<td>ESXi 6.3.0600</td>
<td>6.3.0600</td>
</tr>
</tbody>
</table>

Lists supported host versions.*

**Note:** *This screen shot is for illustration purposes only, and may differ from your specific installation.

- **ESX Version** – The ESX or ESXi version.
- **Supported Update** – The supported updates for the ESX or ESXi version.

### Cloud Settings Dialog
Stop Failover Test Dialog

Stops the testing of the selected VPG.

- **Result**: Whether the test passed or failed.
- **Notes**: A description of the test. For example, defines where external files that describe the tests are saved. Notes are limited to 255 characters.

Clicking the **Stop** button stops the testing. After stopping a test, the virtual machines in the recovery site are powered off and then removed, and the checkpoint that was used for the test has the following tag added to identify the test:

```
Tested at startDateAndTimeOfTest.
```

---

**vCD Settings**

- **Use vCD**: Select to enter the VMware vCloud Director access details:
  - **IP Address**: The IP address or host name of the machine where vCD runs. When connecting to vCD with multiple cells, enter the virtual IP for the network load balancing used by the cells.
  - **Username**: The user name for an administrator to vCD.
  - **Password**: A valid password for the given user name.
  - **AMQP Username**: The user name for the AMQP server.
  - **AMQP Password**: A valid password for the given AMQP user name.

- **Manage Static Routes**: Click **Configure** to define static route details. Go to **Manage Static Routes Dialog**.

- **Provider vDC Settings**: Click **Configure** to define provider vDC settings and their datastore configuration. Go to **Configure Provider vDCs Dialog**.

---

---

---

---
Monitor the recent tasks by clicking the TASKS area in the status bar at the bottom of the Zerto User Interface. The following information is displayed for the most recent tasks:

- The task status.
- The name of the task.
- A description of the task.

Also, actions, such as stopping a failover test, can be performed from this dialog.

Click **See All Tasks** to access MONITORING > TASKS.

---

### Volumes Dialog

![Volumes Dialog](image-url)

The Volumes Dialog allows users to view and manage virtual disks and their properties.
When restoring an offsite backup to the recovery site, this window shows the datastores for a selected virtual machine in the VPG.

- You can edit information in one field by clicking the field and updating the information.
- You can edit several datastore settings at the same time by selecting the datastores and clicking **EDIT SELECTED**.

For more details, see “Edit VM Dialog”, on page 368.
### CHAPTER 25: GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Access Key (AWS)</strong></td>
<td>An alphanumeric text string that uniquely identifies the AWS account owner. No two accounts can have the same AWS Access Key.</td>
</tr>
<tr>
<td><strong>Amazon Web Services (AWS)</strong></td>
<td>A collection of remote computing services, also called web services, that make up a cloud computing platform by Amazon.com. The most central and well-known of these services are Amazon EC2 and Amazon S3. The service is advertised as providing a large computing capacity (potentially many servers) much faster and cheaper than building a physical server farm.</td>
</tr>
<tr>
<td><strong>Asynch Replication</strong></td>
<td>See Replication, Asynchronous.</td>
</tr>
<tr>
<td><strong>Backup</strong></td>
<td>See Extended Recovery.</td>
</tr>
<tr>
<td><strong>Bare Metal</strong></td>
<td>A computer system or network in which a virtual machine is installed directly on hardware rather than within the host operating system (OS).</td>
</tr>
</tbody>
</table>
| **Bitmap Sync¹** | A change tracking mechanism of the protected machines during a disconnected state when Zerto Virtual Replication starts to maintain a smart bitmap in memory to track and record changed storage areas. Since the bitmap is kept in memory, Zerto Virtual Replication does not require any LUN or volume per VPG at the source side. The bitmap is small and scales dynamically, containing references to the areas of the source disk that have changed but not the actual I/O. The bitmap is stored locally on the VRA within the available resources. For example, when a VRA goes down and is then rebooted. When required, Zerto Virtual Replication starts to maintain a smart bitmap in memory, to track and record storage areas that change. When the issue that caused the bitmap sync is resolved, the bitmap is used to check updates to the source disks and send any updates to the recovery site. A bitmap sync occurs during the following conditions:  
- Synchronization after WAN failure or when the load over the WAN is too great for the WAN to handle, in which case the VPGs with the lower priorities will be the first to enter a Bitmap Sync.  
- When there is storage congestion at the recovery site, for example when the VRA at the recovery site cannot handle all the writes received from the protected site in a timely fashion.  
- When the VRA at the recovery site goes down and is then rebooted.  
During the synchronization, new checkpoints are not added to the journal but recovery operations are still possible. If a disaster occurs requiring a failover during a bitmap synchronization, you can recover to the last checkpoint written to the journal. |
<p>| <strong>Bucket (AWS)</strong> | Amazon buckets are like a container for your files. You can name your buckets the way you like but it should be unique across the Amazon system. |
| <strong>Business Continuity &amp; Disaster Recovery (BC/DR)</strong> | An organization’s ability to recover from a disaster and/or unexpected event and resume or continue operations. A disaster recovery, DR, plan is a subset of a Business Continuity plan. Organizations should have a business continuity, BC, plan in place that outlines the logistics and business operations. The key metrics to be measured in a disaster recovery environment are the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). |
| <strong>Business Continuity Management (BCM)</strong> | Holistic management process that identifies potential threats to an organization and the impacts to business operations that those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. (ISO 22313, formerly BS 25999-1). |</p>
<table>
<thead>
<tr>
<th>Glossary Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan</td>
<td>Contains the instructions, procedures and guidelines that are developed and maintained in readiness for use during and after any potentially disruptive event in order to enable the organization to continue to deliver its critical activities at an acceptable, predefined level.</td>
</tr>
<tr>
<td>Business Impact Analysis (BIA)</td>
<td>The process of analyzing business functions and processes and the effects that a business disruption might have upon them.</td>
</tr>
<tr>
<td>Checkpoint</td>
<td>Zerto Virtual Replication ensures crash consistency by writing checkpoints to the journal every few seconds. These checkpoints ensure write order fidelity and crash-consistency to each checkpoint. During recovery you pick one of these crash-consistent checkpoints and recover to this point. Additionally, checkpoints can be manually added by the administrator, with a description of the checkpoint. For example, when an event is going to take place that might result in the need to perform a recovery, you can pinpoint when this event occurs as a checkpoint in each journal.</td>
</tr>
<tr>
<td>Cloud Service Provider (CSP)</td>
<td>A service provider that offers customers storage or software services available via a private (private cloud) or public network (cloud). Usually, it means the storage and software is available for access via the Internet. Typically Infrastructure as a Service (IaaS), Software as a Service (SaaS), or Platform as a Service (PaaS) – are offered to their customers. Zerto enables them to offer Disaster Recovery As A Service (DRaaS) and In-Cloud DR (ICDR), too.</td>
</tr>
<tr>
<td>Crisis Management Plan</td>
<td>Provides the overall coordination of the organization’s response to a crisis (which is a critical event that needs to be handled appropriately to prevent a damaging impact to the organization’s profitability, reputation or ability to operate).</td>
</tr>
<tr>
<td>Data Deduplication</td>
<td>A specialized data compression technique for eliminating duplicate copies of repeating data.</td>
</tr>
<tr>
<td>Delta Sync¹</td>
<td>The Delta Sync uses a checksum comparison to minimize the use of network resources. A Delta Sync is used when the protected virtual machine disks and the recovery disks should already be synchronized, except for a possible few changes to the protected disks, for example, when the target recovery disk is defined as a preseeded (not available in the cloud) disk or after a VRA upgrade, or for reverse protection after a move or failover. During the synchronization, new checkpoints are not added to the journal but recovery operations are still possible. If a disaster occurs requiring a failover during a delta synchronization, you can recover to the last checkpoint written to the journal. It is not possible to perform a move during a delta sync. <strong>Note:</strong> For the synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the source data to replicate to the target recovery disks.</td>
</tr>
<tr>
<td>Disaster</td>
<td>The occurrence of one or more events which, either separately or cumulatively, activate disaster recovery.</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>The ability to restart operations after an interruption to the business according to a plan that ensures an orderly and timely restoration.</td>
</tr>
<tr>
<td>Disaster Recovery Plan</td>
<td>The disaster recovery, DR, plan is a component of the Business Continuity plan that details the process and procedures to recover the organization’s resources to continue business operations. The Technology DR plan focuses on the IT disaster recovery. Also see Business Continuity Plan.</td>
</tr>
<tr>
<td>Disaster Recovery As A Service (DRaaS)</td>
<td>A disaster recovery solution that incorporates a service provider to replace or augment the organization’s data protection implementation. In a DRaaS scenario, the customer may manage and have complete control over the production data. The Cloud Service Provider (CSP) may provide a partial or completely managed service. In either case, the CSP must ensure the availability of the data and adapt as the customers infrastructure changes. An advantage of this model is the CSP has dedicated resources skilled in DR operations.</td>
</tr>
<tr>
<td>DRS (vSphere)</td>
<td>Enables balancing computing workloads with available resources in a VMware vCenter cluster.</td>
</tr>
<tr>
<td>Emergency Management</td>
<td>Covers the immediate response to a situation or set of circumstances that present a clear and present threat to the safety of personnel or other assets of the organization.</td>
</tr>
<tr>
<td><strong>Estimated Recovery Time (ERT)</strong></td>
<td>This is the estimated timings based on full resource provision available during a live invocation. This time typically sits between the Net Recovery Time and the Recovery Time Achieved (RTA) time.</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ESX/ESXi (vSphere)</strong></td>
<td>Bare-metal hypervisor from VMware, meaning it installs directly on top of the physical server and partitions it into multiple virtual machines that can run simultaneously, sharing the physical resources of the underlying server. ESXi is the most recent version.</td>
</tr>
<tr>
<td><strong>Extended Recovery</strong></td>
<td>Extended DR includes the ability to configure both disaster recovery and offsite backups for the protected virtual machines in the VPG, according to a user-defined data retention policy.</td>
</tr>
<tr>
<td><strong>High Availability (VMHA)</strong></td>
<td>VMware high availability decreases downtime and improves reliability with business continuity by enabling another ESX/ESXi host to start up virtual machines that were running on another ESX/ESXi host that went down. High availability is automatically disabled by Zerto Virtual Replication while updating recovered virtual machines in the recovery site from the VRA journal. After the promotion of the data from the journal to the virtual machine completes, high availability is automatically re-enabled. The HA configuration can include admission control to prevent virtual machines being started if they violate availability constraints. If this is the case, then a failover, test failover or migration of the virtual machines in a VPG to the cluster with this configuration will fail, if the availability constraints are violated when the virtual machines are recovered.</td>
</tr>
<tr>
<td><strong>Hyper-V</strong></td>
<td>A hybrid hypervisor, which is installed in the operating system. However, during installation it redesigns the operating system architecture and becomes just like a next layer on the physical hardware.</td>
</tr>
<tr>
<td><strong>Hypervisor</strong></td>
<td>The host for multiple VMs in a virtualized environment. vSphere, ESX/ESXi, is the VMware brand hypervisor. The hypervisor is the virtualization architecture layer that allows multiple operating systems, termed guests, to run concurrently on a host computer.</td>
</tr>
<tr>
<td><strong>Hypervisor Manager</strong></td>
<td>The tool used to manage the host. For example VMware vCenter Server and Microsoft SCVMM.</td>
</tr>
<tr>
<td><strong>I/O (Input/Output)</strong></td>
<td>Describes any operation, program, or device that transfers data to or from a computer. Typical I/O devices are printers, hard disks, keyboards, and mouses. In fact, some devices are basically input-only devices (keyboards and mouses); others are primarily output-only devices (printers); and others provide both input and output of data (hard disks, diskettes, writable CD-ROMs). In computer architecture, the combination of the CPU and main memory (memory that the CPU can read and write to directly, with individual instructions) is considered the brain of a computer, and from that point of view any transfer of information from or to that combination, for example to or from a disk drive, is considered I/O.</td>
</tr>
<tr>
<td><strong>In-Cloud DR (ICDR)</strong></td>
<td>A disaster recovery solution that incorporates a service provider to replace or augment the organization’s data protection implementation. When customers leverage an ICDR service, the CSP hosts the production and DR sites. The virtual machines (VMs) are typically replicated from one CSP datacenter to another CSP datacenter as a managed service or as managed co-located datacenters. The customers have the ability to interact with their applications as if they were locally hosted.</td>
</tr>
<tr>
<td><strong>Initial Sync¹</strong></td>
<td>Synchronization performed after creating the VPG to ensure that the protected disks and recovery disks are the same. Recovery operations cannot occur until after the initial synchronization has completed. Adding a virtual machine to a VPG is equivalent to creating a new VPG and an initial synchronization is performed. In this case, any checkpoints in the journal become unusable and only new checkpoints added after the initial synchronization completes can be used in a recovery. The data in the journal however remains and is promoted to the recovered virtual machine as part of a recovery procedure. <strong>Note:</strong> For the synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the source data to replicate to the target recovery disks.</td>
</tr>
<tr>
<td><strong>iSCSI</strong></td>
<td>An Internet Protocol (IP)-based storage networking standard for linking data storage facilities. By carrying SCSI commands over IP networks, iSCSI is used to facilitate data transfers over intranets and to manage storage over long distances.</td>
</tr>
</tbody>
</table>
### Journal

Every write to a protected virtual machine is intercepted by Zerto Virtual Replication and a copy of the write is sent, asynchronously, to the recovery site, while the write continues to be processed on the protected site. On the recovery site the write is written to a journal managed by the Virtual Replication Appliance. Each protected virtual machine has its own journal.

Each journal can expand to a size specified in the VPG definition and automatically shrinks when the expanded size is not needed.

### LUN

Disk drives are the foundation of data storage, but operating systems cannot use physical disk storage directly. The platters, heads, tracks and sectors of a physical disk drive must be translated into a logical space, which an OS sees as a linear address space comprised of fixed-size blocks. This translation creates a logical entity that allows operating systems to read/write files. Storage networks must also partition their physical disks into logical entities so that host servers can access storage area network (SAN) storage. Each logical portion is called a logical unit number (LUN). A LUN is a logical entity that converts raw physical disk space into logical storage space, which a host server’s OS can access and use. Any computer user recognizes the logical drive letter that has been carved out of their disk drive. For example, a computer may boot from the C: drive and access file data from a different D: drive. LUNs do the same basic job.

### Level of Business Continuity

The reduced level of service that has been agreed if there is an interruption to business operations.

### Managed Service Provider (MSP)

See Cloud Service Provider (CSP).

### Maximum Tolerable Data Loss

The maximum tolerable data loss an organization can endure without compromising its business objectives.

### Maximum Tolerable Outage (MTO)

The maximum time after which an outage will compromise the ability of the organization to achieve its business objectives.

### Maximum Tolerable Period of Disruption

The duration after which an organization’s viability will be irrevocably threatened if product and service delivery cannot be resumed.

### NAS

A network-attached storage (NAS) device is a server that is dedicated to nothing more than file sharing. NAS does not provide any of the activities that a server in a server-centric system typically provides, such as e-mail, authentication or file management. NAS allows more hard disk storage space to be added to a network that already utilizes servers without shutting them down for maintenance and upgrades. With a NAS device, storage is not an integral part of the server. Instead, in this storage-centric design, the server still handles all of the processing of data but a NAS device delivers the data to the user. A NAS device does not need to be located within the server but can exist anywhere in a LAN and can be made up of multiple networked NAS devices.

### Net Recovery Time

The net time achieved in recovering one or more VPGs after a disaster.

### Offsite Backup

See Extended Recovery.

### Operational Level Agreement (OLA)

The agreement between the service management and the Service Provision Partners. It defines the responsibilities for support and delivery of the services provided.

### Pair

Zerto Virtual Replication can be installed at one or more sites and each of these sites can connect to any of the other sites enabling enterprises to protect virtual machines across multiple vCenters or within the same vCenter. Two sites connected to each other are considered paired. Also see Replication to Self.

### Preseed

A virtual disk (a vmdk flat file and descriptor or a .vhdx file) in the recovery site that has been prepared with a copy of the protected data. Using this option is recommended particularly for large disks so that the initial synchronization is much faster. When not using a preseeded disk the initial synchronization phase has to copy the whole disk over the WAN. Zerto Virtual Replication takes ownership of the preseeded disk, moving it from its source folder to the folder used by the VRA.

### Quiesce

Pausing or altering the state of running processes on a computer, particularly those that might modify information stored on disk during a backup, in order to guarantee a consistent and usable backup. Critical applications, such as databases have quiescent mechanisms that Zerto Virtual Replication can use to get application consistent checkpoints.
<p>| <strong>RBAC</strong> | Role-based Access control, available in the Zerto Cloud Manager via the <strong>Permissions</strong> tab. |
| <strong>RDM (vSphere)</strong> | RDM is a mapping file in a separate VMFS volume that acts as a proxy for a raw physical storage device. The RDM allows a virtual machine to directly access and use the storage device. The RDM contains metadata for managing and redirecting disk access to the physical device. The file gives you some of the advantages of direct access to a physical device while keeping some advantages of a virtual disk in VMFS. As a result, it merges VMFS manageability with raw device access. Zerto Virtual Replication supports both physical and virtual mode RDMs. |
| <strong>Recovery Point Objective (RPO)</strong> | The maximum amount of data that may be lost when the activity or service is restored after an interruption. Expressed as a length of time before the interruption. |
| <strong>Recovery Time Achieved (RTA)</strong> | The actual times achieved during a DR test. |
| <strong>Recovery Time Objective (RTO)</strong> | Related to downtime. The metric refers to the amount of time it takes to recover from a data loss event and how long it takes to return to service. The metric is an indication of the amount of time the system’s data is unavailable or inaccessible, thus preventing normal service. |
| <strong>Replication, Asynchronous</strong> | Technique for replicating data between databases or file systems where the system being replicated does not wait for the data to have been recorded on the duplicate system before proceeding. Asynchronous Replication has the advantage of speed, at the increased risk of data loss during due to communication or duplicate system failure. |
| <strong>Replication to Self</strong> | When a single vCenter is used, for example with remote branch offices, when replicating from one datacenter to another datacenter, both managed by the same vCenter Server, you have to enable replication to the same vCenter Server and pairing is not required. |
| <strong>Resource</strong> | The elements (such as staff, site, data, IT systems) that are required to deliver an activity or service. |
| <strong>Resource Recovery Plan</strong> | Contains the instructions, procedures and guidelines to recover one or more resources and return conditions to a level of operation that is acceptable to the organization. Recovery Plans include detailed recovery procedures for IT equipment and infrastructure. |
| <strong>Rolling Back</strong> | Rolling back to an initial status, for example, after canceling a cloning operation on the VPG. |
| <strong>RPO</strong> | See <strong>Recovery Point Objective (RPO)</strong>. |
| <strong>RTO</strong> | See <strong>Recovery Time Objective (RTO)</strong>. |
| <strong>SAN</strong> | A storage area network (SAN) is any high-performance network whose primary purpose is to enable storage devices to communicate with computer systems and with each other. A storage device is a machine that contains nothing but a disk or disks for storing data. A SAN’s architecture works in a way that makes all storage devices available to all servers on a LAN or WAN. As more storage devices are added to a SAN, they too will be accessible from any server in the larger network. In this case, the server merely acts as a pathway between the end user and the stored data. Because stored data does not reside directly on any of a network’s servers, server power is utilized for business applications, and network capacity is released to the end user. |
| <strong>SCSI</strong> | Acronym for Small Computer System Interface. SCSI is a parallel interface standard used by many servers for attaching peripheral devices to computers. SCSI interfaces provide for faster data transmission rates (up to 80 megabytes per second) than standard serial and parallel ports. In addition, you can attach many devices to a single SCSI port, so that SCSI is really an I/O bus rather than simply an interface. |
| <strong>SCVMM</strong> | A Microsoft management solution for the virtualized datacenter, enabling you to configure and manage your virtualization host, networking, and storage resources in order to create and deploy virtual machines and services to private clouds that you have created. |
| <strong>Secret Access Key (AWS)</strong> | A password. The Secret Access Key with the Access Key forms a secure information set that confirms the user’s identity. |
| <strong>Security Group</strong> | A virtual firewall that controls the traffic for one or more instances. |</p>
<table>
<thead>
<tr>
<th>Glossary Topic</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Continuity Plan</td>
<td>The continuity plan that acts as an umbrella document for a service, referencing other plans as required and providing service-specific emergency management and recovery plans.</td>
</tr>
<tr>
<td>Service Level Agreement (SLA)</td>
<td>The agreement between the customer and service provider which defines the service that is to be delivered to the customer.</td>
</tr>
<tr>
<td>Service Profile</td>
<td>A predefined set of default properties to use when VPGs are defined or edited. Zerto provides a default service profile and the option for the organization to specify their own requirements. The cloud service provider can define service profiles to manage specific service level agreements (SLAs) with its customers.</td>
</tr>
<tr>
<td>Service Test Plan</td>
<td>Detailed plan defining the activities required to test the recovery of an individual IT service to meet business requirements documented in the RTO and RPO.</td>
</tr>
<tr>
<td>Shadow VRA</td>
<td>During normal operation, a VRA might require more disks than a single virtual machine can support. If this situation arises, the VRA creates new shadow VRA virtual machines, used by the VRA to maintain additional disks. These virtual machines must not be removed. A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.</td>
</tr>
<tr>
<td>Snapshots</td>
<td>A snapshot is a block device which presents an exact copy of a logical volume, frozen at some point in time. Typically this would be used when some batch processing, a backup for instance, needs to be performed on the logical volume, but you don’t want to halt a live system that is changing the data. Zerto does NOT use a snapshot mechanism, but is constantly replicating data writes.</td>
</tr>
<tr>
<td>Storage Account (Azure)</td>
<td>Storage accounts re like a container for your files. You can name your storage account the way you like but it should be unique across the Azure system.</td>
</tr>
<tr>
<td>Subnet</td>
<td>A logical, visible subdivision of an IP network.[1] The practice of dividing a network into two or more networks is called subnetting.</td>
</tr>
</tbody>
</table>
| Subscription (Azure)              | The description uses information derived from the following site: https://blogs.msdn.microsoft.com/arunrakwal/2012/04/09/create-windows-azure-subscription/ An Azure subscription grants access to Azure services and Platform Management Portal. A subscription has two aspects:  
  ■ The Windows Azure account, through which resource usage is reported and services are billed.  
  ■ The subscription itself, which governs access to and use of the Azure services that are subscribed to.                                                                 |
| System Center Virtual Machine Manager | See SCVMM.                                                                                                                                   |
| Virtual Machine (VM)              | A virtual machine (VM) is an environment, usually a program or operating system, which does not physically exist but is created within another environment. In this context, a VM is called a guest while the environment it runs within is called a host.                           |
| Virtual Network (VNet) (Azure)     | A virtual network dedicated to an Azure subscription.                                                                                           |
| Virtual Private Cloud (VPC) (AWS) | An on demand configurable pool of shared computing resources allocated within a public cloud environment, providing a certain level of isolation between the different organizations (denoted as users hereafter) using the resources. The isolation between one VPC user and all other users of the same cloud (other VPC users as well as other public cloud users) is achieved normally through allocation of a Private IP Subnet and a virtual communication construct (such as a VLAN or a set of encrypted communication channels) per user. |
| Virtual Protection Group          | See VPG.                                                                                                                                                                                                    |
| Virtual Replication Appliance     | See VRA.                                                                                                                                                                                                     |
| VMDK, Virtual Machine Disk        | Virtual Machines created with VMware products typically use virtual disks. The virtual disks, stored as files on the host computer or remote storage device, appear to the guest operating systems as standard disk drives. |

[1] The practice of dividing a network into two or more networks is called subnetting.
<table>
<thead>
<tr>
<th>Glossary Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume Delta Sync</td>
<td>Synchronization when only delta changes for a volume needs synchronizing, for example, when a virtual machine is added to a VPG using a preseeded disk. During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible during a <strong>Volume Delta Sync</strong>. For the synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the source data to replicate to the target recovery disks.</td>
</tr>
<tr>
<td>Volume Full Sync</td>
<td>Synchronization when a full synchronization is required on a single volume. During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible during a <strong>Volume Full Sync</strong>. <strong>Note:</strong> For the synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the source data to replicate to the target recovery disks.</td>
</tr>
<tr>
<td>Volume Initial Sync</td>
<td>Synchronization when a full synchronization is required on a single volume, for example, when changing the target datastore or adding a virtual machine to the VPG without using a preseeded (not available in the cloud) disk. During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible during a <strong>Volume Initial Sync</strong>. For the synchronization to work, the protected virtual machines must be powered on. The VRA requires an active IO stack to access the virtual machine data to be synchronized across the sites. If the virtual machine is not powered on, there is no IO stack to use to access the source data to replicate to the target recovery disks.</td>
</tr>
<tr>
<td>VPG</td>
<td>Virtual machines are protected in virtual protection groups. A virtual protection groups (VPG) is a group of virtual machines that you want to group together for replication purposes. For example, the virtual machines that comprise an application like Microsoft Exchange, where one virtual machine is used for the software, one for the database and a third for the Web Server, require that all three virtual machines are replicated to maintain data integrity.</td>
</tr>
<tr>
<td>VRA</td>
<td>A virtual machine installed on each hypervisor hosting virtual machines to be protected or recovered, that manages the replication of protected virtual machine writes across sites. A VRA must be installed on every hypervisor that hosts virtual machines that require protecting in the protected site and on every hypervisor that will host the replicated virtual machines in the recovery site.</td>
</tr>
<tr>
<td>vSphere</td>
<td>VMware’s server virtualization platform for building a cloud infrastructure.</td>
</tr>
<tr>
<td>Zerto Cloud Connector (ZCC)</td>
<td>A virtual machine installed on the cloud side, one for each customer organization replication network. The Zerto Cloud Connector requires both cloud-facing and customer-facing static IP addresses. The ZCC routes traffic between the customer network and the cloud replication network, in a secure manner ensuring complete separation between the customer network and the cloud service provider network. The ZCC has two Ethernet interfaces, one to the customer’s network and one to the cloud service provider’s network. Within the cloud connector a bidirectional connection is created between the customer and cloud service provider networks. Thus, all network traffic passes through the ZCC, where the incoming traffic on the customer network is automatically configured to IP addresses of the cloud service provider network.</td>
</tr>
<tr>
<td>Zerto Cloud Manager (ZCM)</td>
<td>A Windows service, which enables managing all the cloud sites offering disaster recovery using a single interface. The ZCM manages the DR either as a service (DRaaS) or completely within the cloud environment, protecting on one cloud site and recovering to a second site (ICDR).</td>
</tr>
<tr>
<td>Zerto User Interface</td>
<td>Recovery using Zerto Virtual Replication is managed via a user interface: in a browser via the Zerto Virtual Manager Web Client, or in either the vSphere Web Client or vSphere Client console in the Zerto tab.</td>
</tr>
<tr>
<td><strong>Zerto Self-service Portal (ZSSP)</strong></td>
<td>An out-of-the-box DR portal solution with a fully functioning browser-based service portal to enable cloud service providers to quickly introduce disaster recovery as part of their portal offering.</td>
</tr>
<tr>
<td><strong>Zerto Virtual Backup Appliance (VBA)</strong></td>
<td>A Zerto Virtual Replication service that manages the offsite backup.</td>
</tr>
<tr>
<td><strong>Zerto Virtual Manager (ZVM)</strong></td>
<td>A Windows service, which manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the vCenter Server to get the inventory of VMs, disks, networks, hosts, etc. The ZVM also monitors changes in the VMware environment and responds accordingly. For example, a vMotion operation of a protected VM from one host to another is intercepted by the ZVM so the Zerto User Interface is updated accordingly.</td>
</tr>
<tr>
<td><strong>ZORG, Zerto Organization</strong></td>
<td>Cloud customers are defined to Zerto Cloud Manager as Zerto organizations, ZORGs. A ZORG is defined with the cloud resources it can use, the permissions that it has to perform operations, such as testing a failover or defining a VPG.</td>
</tr>
</tbody>
</table>

1. Synchronization after a recovery starts after the promotion of data from the journal to the virtual machine disks ends. Thus, synchronization of virtual machines can start at different times, dependent on when the promotion for the virtual machine ends. All synchronizations are done in parallel, whether a delta sync or full sync, etc.
F
failover test ........................................... 276
failover tests report ................................ 325
file recovery ........................................... 309
Firefox .................................................. 19
folder recovery ....................................... 309
force delete of VPG ................................. 223
full synchronization
for volumes .................................. 238

G
glossary .................................................. 396–403
generation ............................................. 34
geometry, non-default ......................... 51, 71, 110, 125, 142, 159, 375
ghost VRA ............................................. 249
HA, see high availability ........................... 346
high availability ..................................... 256
HTTPS .................................................... 265

I
IDE devices ............................................. 34
IDE disks ............................................... 33
initial synchronization ......................... 34, 222, 366
definition ............................................. 237
Internet Explorer, supported versions ...... 19

J
journal .................................................... 63, 82, 93, 151, 169, 179, 353
adding a checkpoint ............................... 225
defining save time ................................ 353
history in VPG tab .................................. 191
location ............................................... 35
sizing ...................................................... 35

K
Keep Source VMs .................................... 284, 290

L
license ..................................................... 265
logs ......................................................... 343
collecting ............................................. 338–343
description ......................................... 343

M
MAC address ........................................ 113
Microsoft SQL Server Database, reconfiguring ............ 255
migration, see move ................................
modify volumes .................................... 220
RDM ....................................................... 221
VRA ....................................................... 201
move .................................................... 289
commit policy ....................................... 262, 389
description .......................................... 284
failing back .......................................... 287
initiating ............................................... 286
reverse replication ................................ 287
using a scratch volume ......................... 289

N
NAT rules ................................................ 111, 127
needs configuration ................................ 237
troubleshooting ..................................... 335
network .................................................. 52, 72
for failing over or moving ....................... 143, 160
for testing ........................................... 52, 72, 143, 160
NIC ......................................................... 381
defining network details ....................... 381
NTP clock synchronization .................... 266, 382

O
offsite backup ......................................... 13, 32, 38, 317
changing repository ............................... 367
creating a repository .............................. 28
editing a repository ............................... 30
flow ...................................................... 32
number saved ...................................... 38
restoring .............................................. 32, 317
retention period .................................... 32, 38, 214
running unscheduled ......................... 223
setting up ............................................. 28
status in Dashboard .................................................188, 197, 203
status in single VPG tab ..............................................191
status in VPGs tab .......................................................188, 189
offsite backup repository
  creating .................................................................28, 380
  editing ........................................................................30
Offsite Backups report ..................................................332
offsite clone, see cloning
Outbound Protection Over Time report .........................323

P
pairing ........................................................................256, 363
pass-through disks .......................................................60, 291, 302
pause protection ..........................................................221
performance graphs
  for a single VPG ............................................................191
  for a single VRA ...........................................................201
  for a site .......................................................................186
permissions in vCenter Server ......................................345
PowerShell cmdlet
  Set-Checkpoint .............................................................224
preseed .................................................................34, 51, 71, 110, 125, 142, 159, 375, 376
recovery volume ..........................................................110, 125
promotion of data ..........................................................290, 301, 336, 347
  hangs .........................................................................336
  when VRA fails .............................................................336
protected site, pairing ...................................................256
Protection Over Time by Site report ..............................324
provisioned storage .....................................................188, 197, 202, 204

R
raw disk (RDM) ..............50, 60, 70, 109, 124, 141, 158, 291, 302, 374
  modifying .....................................................................221
recovery
  during a test ...............................................................304
  report ........................................................................325
to Hyper-V ..................................................................60
to same site .................................................................57
to VMware vCenter Server .........................................40
to VMware vCloud Director .......................................100
types .........................................................................31
derevoy flows ................................................................31
recovery host, changing .............................................360
Recovery report ..........................................................325
  branding ....................................................................326
recovery site, pairing ....................................................256
recovery volume
  preseeding ................................................................110, 125
  swap ..........................................................................110, 125
registration .................................................................265
re-IP .................................................................55, 74, 113, 128, 146, 162
  in AWS ......................................................................86, 95, 172, 181
  vNIC configuration ......................................................54, 145
Replication Pause Time ................................................222
reconfiguration ..............................................................57
enabling ........................................................................57
reports
  Offsite Backups ............................................................332
  Outbound Protection Over Time ..................................323
  Protection Over Time by Site ......................................324
  Recovery .................................................................325
  Resources .................................................................327
  Usage .........................................................................331
  VPG Performance .......................................................331
reposistory for offsite backup .......................................28, 30
resize volumes .............................................................220
RDM .................................................................28, 30, 362
Resources report ..........................................................327
  configuring ................................................................392
  generating with REST API ..........................................327
  output ..........................................................................328
restore .......................................................................317
definition .....................................................................317
offsite backup .............................................................32
retention period
  offsite backup .............................................................32, 38
reverse replication
  move .........................................................................287
rollback
  setting for failover or move .........................................262

S
same site replication .....................................................57
scratch volume ............................................................276, 289, 301
scripts
  creating ......................................................................227
  execution timeout
    advanced settings ....................................................262
  running ......................................................................225
  ZertoForce environment variable .................................226
  ZertoOperation environment variable ..........................226
  ZertoVCENTERIP environment variable ........................226
  ZertoVCENTERPORT environment variable ..................226
  ZertoVPGName environment variable ..........................226
SCSI disks ....................................................................33
security certificate
  adding ......................................................................21
  replacing ...................................................................256
security group ..............................................................215
self replication ..............................................................57
service profile .............................................................34
Set-Checkpoint cmdlet ..................................................224
settings
  importing VPG ..........................................................231
shadow VRA ........................................ 241, 401
signature matching, WAN optimization ............... 18
site details
  monitoring .............................................. 185
site information ........................................ 260
site settings ............................................ 387
  commit policy ...................................... 389
  defining .............................................. 258
  email .................................................. 263
  enabling replication to self ....................... 57
sites tab .................................................. 198
sizing
  volumes .............................................. 50, 70, 109, 124, 141, 158, 374
  WAN .................................................. 26
status
  VPG ................................................... 232
storage
  for replicated data .................................. 49, 69, 140, 157
  provisioned ........................................ 188, 197, 202, 204
sizing
  for vCD ............................................. 110, 125
Storage vMotion .................................... 248, 347
stored offsite backups ................................ 38
subnet .................................................. 215
summary tab ......................................... 185
swap disk
  recovery volume ................................... 110, 125
synchronization
  delta .................................................. 49, 69, 140, 157, 222
  forcing ............................................. 222
  full .................................................. 238
  initial .............................................. 36, 110, 125, 222, 366
synchronization triggers
  VPG ................................................... 232, 238
T
  tasks .................................................. 194
    monitoring ....................................... 394
test failover ......................................... 273
  initiating ......................................... 304
    process ......................................... 273
    scratch volume ................................ 276
    stopping ........................................ 277
test scratch volume ................................ 276
thin provisioning ..................................... 346
throttling ............................................ 18
  setting ............................................ 261
  site settings ..................................... 388
time-based bandwidth throttling ....................... 261
  site settings ..................................... 388
topology
  for failover ...................................... 300
    for move ........................................ 288
  for testing failover .............................. 276
  in Dashboard ..................................... 186
  in Sites tab ...................................... 193
triggers
  synchronization .................................. 232
  VPG synchronization .............................. 238
troubleshooting
  disk space ........................................ 336
  VRA crashes during promotion .................. 336
  Zerto Virtual Manager service .................. 334
U
  usage
    report ............................................ 331
Usage report ........................................... 331
V
  v
    vApp network mapping .......................... 112, 127
  VBA ................................................ 28
    offsite backup .................................. 32
  vCD guest customizing ........................... 111, 127
  VIB ............................................... 243, 247, 359, 362, 377
    Virtual Backup Appliance, see VBA
  virtual machine
    modify RDM ....................................... 221
    modify volumes .................................. 220
    modifying replication settings .............. 368
    monitoring ...................................... 196
  virtual protection group, see VPG
  Virtual Replication Appliance, see VRA
  VirtualEthernetCardLegacyNetworkBackingInfo NIC ........................................ 34
  VM in Several VPGs 13, 34, 41, 61, 80, 92, 101, 116, 132, 149, ........................................ 167, 178, 215, 218, 284
  VMDK size limitations ............................. 26
    adjusting ......................................... 26
  vMotion .......................................... 347
  VMware high availability (VMHA) ................ 346
  VMware host maintenance ......................... 250
  VMware vCenter Server
    cloning to it ..................................... 307
  vNIC
    configuring ...................................... 113, 128
    configuring re-IP ................................ 73
    vNIC configuration
      re-IP .......................................... 54, 145
  volume
    estimating size .................................. 50, 70, 109, 124, 141, 158, 374
    full synchronization ................................ 238
    preseed ......................................... 110, 125
  VPC (AWS) ........................................... 215
  VPG
    add a virtual machine ............................ 215, 218
    add a virtual machine via a vSphere console ........................................ 58
    creating to AWS ................................ 76
    creating to Hyper-V ................................ 60
    creating to same site ............................ 57
creating to vCenter Server ...................................................... 40, 56
definition ............................................................................. 31, 33
deleting ..................................................................................... 223
editing .................................................................................... 371, 372
handling error ......................................................................... 222
importing settings .................................................................... 231
modify ..................................................................................... 213
monitoring ............................................................................... 187, 191
pausing protection .................................................................... 221
saving details to file .................................................................. 190
synchronization triggers .......................................................... 232, 238
synchronize ............................................................................. 222
synchronizing ........................................................................... 222
testing ....................................................................................... 273
VPG Performance report ........................................................... 331
VPG status ............................................................................... 232
VPG waiting to be removed ...................................................... 223
VPG waiting to be removed
  force delete ............................................................................ 223
VPGs tab
  monitoring .............................................................................. 187
VRA .......................................................................................... 13, 401
changing recovery host ............................................................. 360
crash during promotion ............................................................ 336edit connection method .............................................................. 247
edit host password .................................................................... 247
editing settings ......................................................................... 246
ghost ......................................................................................... 249
monitoring ............................................................................... 201
shadow VRA ............................................................................ 241
uninstalling ............................................................................... 249
upgrading ................................................................................... 245–250
vSphere Client console ............................................................. 19, 58
vSphere Web Client .................................................................... 19, 58
  working with Zerto Virtual Replication ................................... 20
vStorage
  thin provisioning ..................................................................... 346
W
WAN
  compressing traffic ................................................................. 45, 65, 104, 119, 135, 152
  signature matching .................................................................. 18
WAN bandwidth, freeing up ...................................................... 221
WAN optimization ..................................................................... 18
WAN sizing ............................................................................... 26
Windows service
  Zerto Virtual Manager ........................................................... 334
Z
Zerto User Interface
  configuration ............................................................................ 22
  customizing ............................................................................. 23
Zerto Virtual Manager ............................................................... 12
Windows service ....................................................................... 334
Zerto Virtual Manager Web Client ................................................ 19
Zerto Virtual Replication
  architecture ............................................................................... 12
  benefits .................................................................................... 16
  definition .................................................................................. 11
  how it works ............................................................................. 13
  logs ......................................................................................... 343
  monitoring ............................................................................... 184
ZertoForce script ....................................................................... 226
ZertoOperation script ................................................................. 226
ZertoVCenterIP script ................................................................. 226
ZertoVCenterPort script ............................................................... 226
ZertoVPGName script ................................................................. 226
ZORG
  preseeding ............................................................................... 111, 126
ZVM, see Zerto Virtual Manager
  how it works ............................................................................. 11

408
Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. Replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With unmatched scale, Zerto’s software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. Zerto is trusted by over 6,000 enterprise customers globally, and is powering resiliency offerings for Microsoft Azure, IBM Cloud, AWS, Sungard and more than 350 cloud services providers.

Learn more at Zerto.com

Copyright © 2018, Zerto Ltd. All rights reserved.