Zerto Virtual Manager Administration Guide
VMware vSphere Environment
TABLE OF CONTENTS

CHAPTER 1: INTRODUCTION TO ZERTO VIRTUAL REPLICAION. .......................................................... 10
What is Zerto Virtual Replication? ................................................................. 10
Zerto Virtual Replication Architecture ......................................................... 11
How Zerto Virtual Replication Recovery Works ........................................... 12
Benefits of Using Zerto Virtual Replication .................................................. 12

CHAPTER 2: ACCESSING THE ZERTO USER INTERFACE ........................................................... 15
Using the Zerto User Interface From a Browser .............................................. 15
Using the Zerto User Interface Within vSphere ............................................. 15
Using the vSphere Web Client ................................................................. 16
Using the vSphere Client Console ............................................................. 17
Adding a Security Certificate .................................................................... 17
Working With the Zerto User Interface ....................................................... 19
Subtabs .................................................................................. 19
Views ..................................................................................... 20

CHAPTER 3: INITIAL SITE CONFIGURATION ................................................................. 21
Enabling Replication to the Same Site ......................................................... 21
Sizing Considerations ................................................................. 22
VMDK Size Limitations ................................................................... 22
WAN Sizing .............................................................................. 23
Setting Up Offsite Backups ..................................................................... 27
Creating an Offsite Backup Repository .................................................. 28
Editing an Offsite Backup Repository ...................................................... 29

CHAPTER 4: OVERVIEW OF RECOVERY FLOWS ........................................................ 31
Flow for a Disaster Recovery Operation .................................................. 31
Flow for a Test Failover Operation ........................................................ 32
Flow for an Offsite Backup and Restore Operation ................................. 32

CHAPTER 5: INTRODUCTION TO PROTECTING VIRTUAL MACHINES ......................... 33
Configuring Virtual Protection Groups ..................................................... 33
The Role of the Journal During Protection .............................................. 34
What happens After the VPG is Defined .................................................. 36
Disaster Recovery ................................................................... 37
Offsite Backups .............................................................................. 37

CHAPTER 6: PROTECTING VIRTUAL MACHINES FROM A VCENTER SERVER ................... 39
Protecting Virtual Machines to a Recovery Site vCenter Server .................. 39
Protecting Virtual Machines to the Same Site ............................................. 50
When to Replicate to the Same Site ......................................................... 50
Protecting a Single Virtual Machine (Via the VMware Web Client or Client Console) ......................................................... 51
Protecting a vApp (Via the VMware Web Client or Client Console) ................ 53
Protecting Virtual Machines to Recovery Hyper-V Hosts ......................... 53
Protecting Virtual Machines on a vCenter Server to AWS ......................... 63
CHAPTER 10: MANAGING VRAS ................................................................. 162
Installing a VRA ................................................................................. 162
Upgrading VRAs ................................................................................. 165
Editing VRA Settings ........................................................................ 167
Resetting the Host Passwords Required By More Than One VRA ...... 167
Changing a Recovery VRA For Virtual Machines ......................... 168
Uninstalling VRAs ............................................................................. 169
Handling a Ghost VRA ...................................................................... 169
Managing Protection When Moving a Host to a Different Cluster ... 170

CHAPTER 11: MANAGING A ZERTO VIRTUAL MANAGER ............... 172
Check Connectivity Between Zerto Virtual Replication Components 172
Reconfiguring the Zerto Virtual Manager Setup ............................. 173
Reconfiguring the Microsoft SQL Server Database Used by the Zerto Virtual Manager ............................................................. 175
Replacing the SSL Certificate ............................................................ 176
Pair to Another Site ........................................................................... 177

CHAPTER 12: ADVANCED SITE CONFIGURATION ............................ 178
Site Settings ....................................................................................... 178
Editing Information About a Site ..................................................... 179
Defining Performance and Throttling ............................................... 179
Defining Site Policies ........................................................................ 181
Configuring Email Settings ............................................................... 182
Defining Resource Report Sampling Period ................................. 183
Reviewing Supported Host Versions ............................................. 184
Seeing What is Licensed ................................................................. 184
Submitting a Support Ticket ......................................................... 185
About Zerto Virtual Replication .................................................... 186

CHAPTER 13: OVERVIEW OF DISASTER RECOVERY OPERATIONS 187
The Failover Test Operation ............................................................... 187
The Move Operation ......................................................................... 187
The Failover Operation .................................................................... 188
The Clone Operation ......................................................................... 189

CHAPTER 14: TESTING RECOVERY ................................................ 190
The Test Failover Process ................................................................. 190
Starting and Stopping Failover Tests .............................................. 191
After Starting a Test, What Happens? ........................................... 193
Viewing Test Results ....................................................................... 195
Live Disaster Recovery Testing ....................................................... 195
Basic Verification - User Traffic Is Not Run against the Recovered VMs. .................................................................................. 197
Run User Traffic Against the Recovered VMs ............................... 198

CHAPTER 15: MIGRATING A VPG TO A RECOVERY SITE ................ 201
The Move Process ............................................................................ 201
Moving Protected Virtual Machines to a Remote Site .................... 202
Reverse Protection For a Moved VPG ............................................ 206
CHAPTER 16: MANAGING FAILOVER ................................................................. 208
The Failover Process ................................................................................. 208
Initiating a Failover ................................................................................. 209
Reverse Protection for a Failed Over VPG ................................................. 214
What Happens When the Protected Site is Down ....................................... 215
Initiating a Failover During a Test ............................................................ 215

CHAPTER 17: CLONING A VPG TO THE RECOVERY SITE .................. 216
The Clone Process .................................................................................. 216
Cloning Protected Virtual Machines to the Remote Site ............................. 216

CHAPTER 18: RESTORING AN OFFSITE BACKUP ............................... 219
The Restore Process ............................................................................... 219
Restoring Virtual Machines ..................................................................... 219

CHAPTER 19: ZERTO VIRTUAL REPLICATION REPORTS .................. 225
Outbound Protection Over Time ............................................................... 225
Protection Over Time by Site ................................................................. 225
Recovery Reports ................................................................................... 226
Resources Report ................................................................................... 227
Usage ....................................................................................................... 230
VPG Performance .................................................................................... 230
Backup Report ........................................................................................ 231

CHAPTER 20: TROUBLESHOOTING ...................................................... 233
Ensuring the Zerto Virtual Manager is Running ......................................... 233
Troubleshooting Needs Configuration Problems ....................................... 234
Troubleshooting GUI Problems .............................................................. 234
Troubleshooting VRA Problems .............................................................. 234
Handling Lack of Storage Space for Recovered Virtual Machines ............... 235
Zerto Virtual Replication Diagnostics Utility ............................................ 235
Collecting Zerto Virtual Replication Logs ................................................ 236
Collecting Log Information for the ZertoVssAgent ..................................... 241
Understanding the Logs .......................................................................... 241

CHAPTER 21: ZERTO VIRTUAL REPLICATION AND VMWARE FEATURES ........................................................................ 243
Zerto Virtual Replication Permissions in vCenter Server .............................. 243
Stopping a vCenter Server ...................................................................... 243
Protecting Virtual Machines in a vApp ...................................................... 244
Thin-Provisioning ................................................................................... 244
VMware Clusters .................................................................................... 244
VMware High Availability (VMHA) .......................................................... 245
DRS ......................................................................................................... 245
Storage Profiles and Storage Clusters ....................................................... 245
Fault Tolerance ....................................................................................... 245
Host Affinity Rules and CPU Pinning ........................................................ 246
vMotion ................................................................................................ 246
Storage vMotion ..................................................................................... 246
VMware Host Maintenance Mode ............................................................. 246
CHAPTER 22: THE ZERTO VIRTUAL MANAGER USER INTERFACE ................................. 247

Add Checkpoint Dialog .......................................................... 248
Add Site Dialog ................................................................. 248
Add Static Route Dialog .......................................................... 249
Advanced Journal Settings Dialog .............................................. 249
Advanced Journal Settings Dialog (vCD) ..................................... 250
Advanced VM Recovery Settings Dialog .................................... 250
Advanced VM Replication Settings Dialog ................................ 251
Advanced VM Replication Settings Dialog (vCD) ....................... 252
Advanced VM Settings for AWS Dialog .................................... 252
ALERTS ................................................................................. 253
Boot Order Dialog ................................................................. 253
Browse for VMDK File Dialog .................................................. 254
Change Host Password VRA Dialog .......................................... 254
Change VM Recovery VRA Dialog ............................................ 254
Checkpoints Dialog ............................................................... 255
Configure and Install VRA Dialog .............................................. 256
Configure Paired Site Routing Dialog ......................................... 257
Configure Provider vDCs Dialog ............................................... 258
Configure VM Settings Dialog .................................................. 259
Configure Volume Dialog (vCD) ................................................ 259
Edit NIC Dialog .................................................................... 260
Edit Repository Dialog ........................................................... 261
Edit Selected Volumes Dialog .................................................. 262
Edit VM Dialog .................................................................... 262
Edit VM Dialog (vCD) ............................................................ 263
Edit VM Network Dialog (AWS) ................................................ 264
Edit vNIC Dialog .................................................................. 264
Edit vNIC Dialog (vCD) .......................................................... 265
Edit Volumes Dialog ............................................................... 266
Edit Volumes Dialog (vCD) ...................................................... 267
Edit VRA Dialog .................................................................. 268
Manage Static Routes Dialog ..................................................... 269
New Repository Dialog ........................................................... 270
NICs Dialog ......................................................................... 271
Offsite Clone Dialog ............................................................... 271
Open Support Ticket Dialog ..................................................... 272
Restore from Zerto Backup ....................................................... 272
Restore Volumes Dialog .......................................................... 275
Site Settings Dialog ............................................................... 275
Site Information Dialog ........................................................... 276
Performance and Throttling Dialog ............................................ 277
Policies Dialog ..................................................................... 278
Reports Dialog ..................................................................... 279
Compatibility Dialog ............................................................. 280
Cloud Settings Dialog ............................................................ 280
License Dialog ..................................................................... 281
About Dialog ..................................................................... 282
Stop Failover Test Dialog ......................................................... 282
TASKS ..................................................................................... 283
Volumes Dialog ..................................................................... 283

CHAPTER 23: GLOSSARY ............................................................. 284
ABOUT THIS GUIDE

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, or mixed environment.

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.</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 to a vCenter Server, including protecting a vApp.</td>
</tr>
<tr>
<td>7</td>
<td>Protecting Virtual Machines to and From vCloud Director</td>
<td>Describes how to protect virtual machines to vCloud Director.</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>
<tr>
<td>14</td>
<td>Testing Recovery</td>
<td>Describes how to test recovery to ensure the results you want.</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>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>16</td>
<td>Managing Failover</td>
<td>Describes the process of recovery from the protected site to the recovery site.</td>
</tr>
<tr>
<td>17</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>18</td>
<td>Restoring an Offsite Backup</td>
<td>Describes the process of restoring an offsite backup from a repository.</td>
</tr>
<tr>
<td>19</td>
<td>Zerto Virtual Replication Reports</td>
<td>Describes the reporting and monitoring capabilities available with Zerto Virtual Replication.</td>
</tr>
<tr>
<td>20</td>
<td>Troubleshooting</td>
<td>Describes how to resolve problems, including generating logs.</td>
</tr>
<tr>
<td>21</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>22</td>
<td>The Zerto Virtual Manager User Interface</td>
<td>Describes the Zerto User Interface.</td>
</tr>
<tr>
<td>23</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?”, below
- “Zerto Virtual Replication Architecture”, on page 11
- “How Zerto Virtual Replication Recovery Works”, on page 12
- “Benefits of Using Zerto Virtual Replication”, on page 12

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, and 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 14 days prior to the disaster. When recovery earlier than 14 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 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.

A Zerto Virtual Manager can manage up to 5000 virtual machines, either being protected by, or recovered to, the Zerto Virtual Manager.

**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.

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.

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.
Fully Virtual – Sits in the Hypervisor

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.

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.

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.

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

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).

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.

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, the performance impact on the production site is minimal, since the processing is performed on the recovery site. The offsite backups are fixed points saved either weekly or monthly.

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 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 scrips 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.

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 15
- “Adding a Security Certificate”, on page 17
- “Working With the Zerto User Interface” on page 19

Using the Zerto User Interface From a Browser

To use the Zerto Virtual Manager Web Client:

1. In a browser, enter the following URL:
   https://zvm_IP:9669
   where zvm_IP is the IP address of the Zerto Virtual Manager for the 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 have the following additional features:

- You can protect a vApp as a single entity in a VPG for any vApp defined under an ESX/ESXi host. All the virtual machines defined in the vApp VPG are protected and you can migrate or recover the whole vApp as a single entity to the recovery site.
  
  Note: The recovery site cannot be Microsoft SCVMM nor Amazon Web Services (AWS).

- You can protect a virtual machine, that is not already included in a VPG, directly via the Zerto tab for the virtual machine in vSphere 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.

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 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 (user name 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:

- This procedure is based on Microsoft Internet Explorer. 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:

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.

**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**.
CHAPTER 3: INITIAL SITE CONFIGURATION

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:

- "Enabling Replication to the Same Site", below
- "Sizing Considerations", on page 22
- "Setting Up Offsite Backups", on page 27

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.

2. Click Policies.
3. Check the Enable Replication to Self checkbox.
4. Click 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, including the following:

- “VMDK Size Limitations”, below
- “WAN Sizing”, on page 23

### VMDK Size Limitations

VMware imposes the following limits that impact on Zerto Virtual Replication.

**ESXi 5.5 and higher hosts** – Zerto does not apply any restrictions. Refer to any VMware documentation for any sizing restrictions imposed by VMware.

**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.

#### 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.
Note: The net effect of this change 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 above 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.

WAN Sizing

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. Collect data characteristics for protected VMs.
2. Calculate the estimated bandwidth requirements.

Note: When the recovery site is Amazon Web Services (AWS), you estimate the required bandwidth for the protected machines as described below.

Collecting Data Characteristics for VMs

Before you can collect the required data, you must first enable data collection in vCenter Server.

Enabling vCenter Server Data Collection

To enable vCenter Server data collection:
1. Connect to the vCenter Server.
2. In the Administration menu item, select vCenter Server Settings. The vCenter Server Settings dialog is displayed.
4. Make sure that the Statistics Level value for all interval durations up to and including the one day duration is at least 2. If any of the durations have a value less than 2, do the following, starting with the smallest interval:
   a) Select the interval and click Edit.
   b) Change Statistics Level to Level 2.
   c) Click OK.

5. Repeat step 4 for all the values up to and including the 1 day interval duration.
6. Click OK and wait for at least a day before using the aggregate usage data.

Collecting Data Characteristics for VMs

You can collect data characteristics for the virtual machines in a VPG in one of the following ways:

- Via vSphere Client console performance statistics.
- By running a script to collect the data characteristics.
- By using operating system performance monitors, such as the Microsoft Performance Monitor utility for Windows operating systems or the iostat command for Linux operating systems.

Collect data for a minimum of one day. Collecting this information impacts on performance and therefore the collection period should be long enough to gather a true representation of usage but not too long.
The first procedure described below, to collect data characteristics for the VMs via the vSphere Client console performance statistics, uses a timeframe of one day. The second procedure, to collect data characteristics for the VMs by running a script to collect the data characteristics, uses a timeframe of seven days.

**Note:** When running vCenter Server versions before version 5.x, if any of the virtual machines use NFS storage, metrics for the NFS storage are not generated by the vCenter Server.

**To collect data characteristics for the VMs via the vSphere Client console performance statistics:**
1. In the vSphere Client console select the VM and open the **Performance** tab.
2. Click **Advanced**.
3. Click the **Charts Options** link.
   The Customize Performance Chart dialog is displayed.

   ![Customize Performance Chart](image_url)

4. In **Chart Options**, drill-down in **Disk** and select **Past day**.
5. In **Counters**, click **None** to clear all the selections and then select **Disk Write Rate** or **Write Rate**.
6. Click **OK**.

Initial Site Configuration
A chart similar to the following is generated:

Use the chart for the average write rate of the VM.
To collect data characteristics for the VMs via a script:
Note: The following script and the samples supplied with the download, require vSphere PowerCLI and permissions to access
the vCenter Server using the script.
■

Run a script similar to the following:
$report = @()
Get-VM | %{
$stats = Get-Stat -Entity $ -Stat disk.write.average -Start (Get-Date).adddays(-7) ErrorAction SilentlyContinue
if($stats){
$statsGrouped = $stats | Group-Object -Property MetricId
$row = "" | Select Name, WriteAvgKBps, WriteAvgMBps
$row.Name = $_.Name
$row.WriteAvgKBps = ($statsGrouped |
where {$_.Name -eq "disk.write.average"} |
%{$_.Group | Measure-Object -Property Value -Average}).Average
$row.WriteAvgMBps = $row.WriteAvgKBps/1024
$row.WriteAvgKBps = "{0:N2}" -f $row.WriteAvgKbps
$row.WriteAvgMBps = "{0:N2}" -f $row.WriteAvgMBps
$report += $row
}
}
$report | Export-Csv "C:\ZertoOutput.csv"

Note: If you want a value other than seven days, change the value of the adddays() function. For example to collect data
for three days, use adddays(-3).
Use the resulting file, C:\ZertoOutput.csv, for the average write rate of the VM.
Note: Versions of this script are included in the download with this document.

Initial Site Configuration

26


Calculating the Estimated Bandwidth Requirement

Use the average write rate for the virtual machines in a VPG in the Zerto WAN Sizing Estimator to estimate the minimum bandwidth required.

For each VM you also must decide whether compression will be enabled for the VM, based on the data characteristics.

To estimate sizing using the Zerto WAN Sizing Estimator:
1. Open the Zerto WAN Sizing Estimator.
2. Enter the following information:
   - The VM name.
   - The Write KB/s data, based on the statistics gathered in the previous task. Use a period for the decimal mark.
   - Define whether compression is enabled for this VM: Select Yes or No.
   - The application data characteristics: Select Compressed or Compressible.

   Note: The Zerto WAN Sizing Estimator colors the cell red if you decide to employ compression on compressible data and orange if you decide to avoid compression for compressible data.

The Zerto WAN Sizing Estimator calculates the total bandwidth estimation for your deployment, using a minimum value of 5 Mb/sec. The estimation is displayed on the top of each page of the Zerto WAN Sizing Estimator.

You can estimate the WAN sizing required without using the Zerto WAN Sizing Estimator using the following procedure.

To estimate sizing without using the Zerto WAN Sizing Estimator:
1. For each virtual machine in the VPG multiply the KB/sec, based on the statistics gathered, by 8 and divide the result by 1024 to provide an answer in Mb/sec. Divide this result by 2 if compression is enabled for the VM and the data is compressible.
2. Sum the results of step 1.

\[ \text{WAN Mb/sec} = \text{SUM}(\text{KB/sec} \times (8/1024/(1 \text{ or } 2 \text{ if compressible data that will be compressed}))) \]

The result is an estimate of the required Mb/sec for the WAN.

Note: If the result is less than 5 Mb/sec, you must use a minimum dedicated bandwidth of at least 5 Mb/sec.

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 14 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 14 days, 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.

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 set up options are described in this section:
- “Creating an Offsite Backup Repository”, below.
- “Editing an Offsite Backup Repository”, on page 29.
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. 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. If the repository location is a network drive, this drive can be mounted to third party storage, such as Amazon Web Services (AWS). 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 (Simple Storage Service) 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.
   - **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.
   - **Username** – 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** – Password to access the Network Share drive. This field is not displayed when the type is Local.
   - **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 if you want the repository to be used 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.

**Editing an Offsite Backup Repository**

You edit the repositories from the **Repositories** tab.

**To edit an offsite backup repository:**

1. In the Zerto User Interface, click **SETUP > REPOSITORIES**.
2. Click **EDIT** for the repository to edit.
   
   The **Edit Repository** dialog is displayed.

   Edit any of the following settings:

   - **Repository Name** – Specify a unique name for the repository.
   - **Repository Type** – Either specify that the repository resides on a local or shared network disk, using the SMB protocol, accessible from the recovery site. If the repository location is a network drive, this drive can be mounted to third party storage, such as Amazon Web Services, AWS.
   - **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.
   - **Username** – 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** - Password to access the Network Share drive. This field is not displayed when the type is Local.

**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 if you want the repository to be used 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.
CHAPTER 4: OVERVIEW OF RECOVERY FLOWS

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.

The following topics are described in this chapter:

- “Flow for a Disaster Recovery Operation”, below
- “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 14 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:

- “Protecting Virtual Machines to a Recovery Site vCenter Server”, on page 39
- “Protecting Virtual Machines to the Same Site”, on page 50
- “Protecting a vApp (Via the VMware Web Client or Client Console)”, on page 53
- “Protecting Virtual Machines to Recovery Hyper-V Hosts”, on page 53
- “Protecting Virtual Machines on a vCenter Server to AWS”, on page 63
- “Protecting Virtual Machines to and From vCloud Director”, on page 71

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 187
- “Managing Failover”, on page 208
- “Migrating a VPG to a Recovery Site”, on page 201
- “Cloning a VPG to the Recovery Site”, on page 216

**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 187
- “Testing Recovery”, on page 190

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

If there is a requirement to extend the recovery ability to more than the 14 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 (offsite backup) to enable protecting virtual machines in a VPG with extended recovery, see “Setting Up Offsite Backups”, on page 27.

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 - 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.

Offsite backups are kept for the retention period specified in the VPG. However, 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 219.
CHAPTER 5: INTRODUCTION TO PROTECTING VIRTUAL MACHINES

Virtual machines are protected in virtual protection groups. A virtual protection group (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 Virtual Replication Appliance (VRA) in the remote site in a journals for a specified period, after which they are promoted to the replica virtual disks managed by the VRA.

The number of VPGs that can be defined on a site is limited only by the number of virtual machines that can be protected. Each site can manage a maximum of 5000 virtual machines.

**Note:** If the total number of protected virtual machines on the paired sites is 5000, then any additional machines are not protected.

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. 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 and the maximum number of supported disks is 12 for virtual machines running a Windows operating system and 1 for virtual machines running a Linux operating system.

Any machine that can be hosted in vCenter Server can be protected. Note that a Windows Server 2000 can be protected but the ZertoVssAgent and re-IPing 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 and the maximum number of supported disks is 12 for virtual machines running a Windows operating system and 1 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. The virtual machines are recovered with the same configuration as the protected machines. 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.

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 visible to the recovery host if the journal storage was not defined in the Configure Provider vDCs dialog.

The journals for the protected virtual machines are defined as part of the VPG definition and by default are defined to reside on the same storage as the virtual machine. This can be overridden at the virtual machine and VPG levels as follows.

<table>
<thead>
<tr>
<th>ALLOWS STORAGE TIERING</th>
<th>NOTES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Journal</td>
<td>No</td>
</tr>
<tr>
<td>Journal datastore separate from VM datastore for each VM</td>
<td>No</td>
</tr>
<tr>
<td>Journal datastore for each VPG</td>
<td>Yes</td>
</tr>
<tr>
<td>Journal datastore for multiple VPGs</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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 datstores 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 datstores 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 and checkpoints 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.

If the storage where the journal resides drops below 30GB or 15% of the total storage size, the storage itself is considered full and an error alert is issued and all writes to journal volumes on that storage are blocked. Replication is halted, but history is not lost. As such, the RPO begins to steadily increase until space is made available on the storage. Thus, with a large datastore where 30GB is less than 15%, the alert will be triggered when the amount of free space is less than 30GB. With a small datastore where 30GB is more than 15%, the alert will be triggered when the amount of free space is less than 15% of the total size.

If the storage where the journal resides drops below 45GB or 25% of the total storage size, a warning alert is issued.

**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 119.

Disaster 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. In this way, you can recover the virtual machines using the mirror disks and the data in the journal. Refer to “The Role of the Journal During Protection”, on page 34 for more details about the journal.

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>2</td>
<td>13</td>
<td>91</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, the following protection is available:

- “Protecting Virtual Machines to a Recovery Site vCenter Server”, below
- “Protecting Virtual Machines to the Same Site”, on page 50
- “Protecting a Single Virtual Machine (Via the VMware Web Client or Client Console)”, on page 51
- “Protecting a vApp (Via the VMware Web Client or Client Console)”, on page 53
- “Protecting Virtual Machines to Recovery Hyper-V Hosts”, on page 53
- “Protecting Virtual Machines on a vCenter Server to AWS”, on page 63

Protection can be set up to cope with the following situations:

- A disaster, enabling recovery to a point in time in the 14 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 dialog is used to set up both disaster recovery and backup.

If one or both of the sites have vCloud Director installed, see “Protecting Virtual Machines to and From vCloud Director”, on page 71.

**Note:** You cannot protect virtual machines with VirtualEthernetCardLegacyNetworkBackingInfo NICs or with IDE devices.

### Protecting Virtual Machines 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):**

1. In the Zerto User Interface, select **ACTIONS > CREATE VPG**. The **NEW VPG** 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN.
Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.

![Create VPG](image.png)

4. Select the VMs that will be part of this VPG and click the arrow pointing right 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.

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

   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.png)

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

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.

6. 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 including the host and datastore to use for replication.

ZORG – If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.

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\(^1\). 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 that 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.

**Datastore** – The datastore volume to use for all recovered virtual machine files as well as 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.

7. 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

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

![Advanced Journal Settings](image)

**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 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.
- **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.
- **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.

**Target RPO Alert** – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

---

1. If Zerto Cloud Manager is used, vSphere Standard edition cannot be used.
Protecting Virtual Machines from a vCenter Server

Test Reminder – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

9. Optionally, change the Advanced value.

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. 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 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.

10. If you want 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.

11. Select the virtual machines whose values you want to change and click EDIT SELECTED.

The Edit VM dialog is displayed.

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 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.

**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.

**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.
- **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.
- **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.

12. Click **SAVE**.
13. In the **Advanced VM Replication Settings** dialog, click **OK**.
14. 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.

![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.

- **Thin** – If the recovery volumes are thin-provisioned or not.
- **Swap** – If the virtual machine to be replicated includes a swap disk as part of its configuration, mark the recovery disk for this disk as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

15. If you want to edit storage information for one of the virtual machines, select the machine and click **EDIT SELECTED**.
The *Edit Volumes* dialog is displayed.

16. Specify the volume source for recovery from one of the following options.

**Datastore** - A new volume is used for replicated data.

**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.

**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](#).

17. Specify the other volume options.

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

**Datastore** – The datastore to use to create disks for the replicated data. Specify whether the target is thin provisioned. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned.

The datastore 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.

**Note:** You can use the vSphere Client console *Performance* tab for each virtual machine to help estimate the change rate. For more details, refer to “Collecting Data Characteristics for VMs”, on page 24.

**Thin provisioning** – If the recovery volumes are thin-provisioned or not.
18. Click OK.
19. 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.

20. 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.

21. To specify a recovery folder for each virtual machine in the VPG, click **VM SETTINGS**.

   The **Advanced VM Recovery Settings** dialog is displayed.

In this dialog, you can edit the values of one or more of the virtual machines in the VPG.
22. Select the virtual machines whose values you want to change and click **EDIT SELECTED**.
The Edit VM dialog is displayed.

Recovery Folder – The folder to which the virtual machine is recovered.

23. Click SAVE.

24. In the Advanced VM Recovery Settings dialog, click SAVE.

25. Check the Scripts box if scripts should run as part of the recovery process.

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>FIELD</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. 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 Performance and Throttling tab in the Site Settings dialog.</td>
</tr>
</tbody>
</table>

26. 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.

27. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click EDIT SELECTED. Otherwise, go to step 30.
The *Edit vNIC* dialog is displayed.

28. 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.

**Change vNIC IP Configuration**: Whether or not to keep the default virtual NIC (vNIC) IP configuration. You can only change the vNIC IP for virtual machines with VMware Tools running for the following operating systems: Windows 2003 and higher, Red Hat Enterprise Linux versions 5-7.x, SUSE Linux Enterprise versions 10-11, Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, CentOS versions 5-6.x, and Oracle Linux versions 5.9-6.6.

To change the vNIC IP, select *Yes* in the *Failover/Move* or *Test* column. 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 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.

**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** – 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.

29. Click *OK*.
30. 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.

31. By default, backup is off. If you do not want to change this value, go to step 32. 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 27.

   **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 37.

   **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>FIELD</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>

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

33. 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.

Protecting Virtual Machines 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.

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 enable replication to the same site:
1. Select Site Settings. In the Site Settings dialog, select Policies.

2. Check the Enable replication to self option in the Replication section. Click SAVE or APPLY.

To define a VPG to recover to the protection site:
- In the Zerto User Interface, select ACTIONS > CREATE VPG.
  The Create VPG wizard is displayed.

The procedure is the same as when protecting virtual machines, described in “Protecting Virtual Machines to a Recovery Site vCenter Server”, on page 39, selecting the local site as the Recovery Site in the REPLICATION step.

Protecting a Single Virtual Machine (Via the VMware Web Client or Client Console)
You can protect a virtual machine, that 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 add a virtual machine to an existing VPG 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 52.
- To create a VPG that includes the virtual machine, as described in “To create a virtual protection group (VPG):”, on page 39. When using the Zerto User Interface, use this procedure.

**To add a virtual machine to an existing VPG 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 “To create a virtual protection group (VPG):”, on page 39, starting with step 11.

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 step the virtual machine is selected. You select other virtual machines for the VPG.
3. Make any required changes to the VPG, as described in “Protecting Virtual Machines to a Recovery Site vCenter Server”, on page 39.
Protecting a vApp (Via the VMware Web Client or Client Console)

You can protect a vApp as a single entity in a VPG for any vApp defined under an ESX/ESXi host. All the virtual machines defined in the vApp VPG are protected and you can migrate or recover the whole vApp as a single entity to the recovery site. The recovery site cannot be Microsoft SCVMM nor Amazon Web Services (AWS).

In addition to being able to protect the vApp, you can protect individual virtual machines in the vApp, in the same way as you protect any other virtual machine. However, if you protect a virtual machine in the vApp, you cannot then protect the vApp as a single entity.

The individual machines in a vApp can be protected using the Zerto User Interface. A vApp can only be protected as a vApp via the vSphere Web Client or Client console.

**Note:** Nested vApps are not protected. Also, if you drag a protected vApp under another vApp to nest it, the protection is removed. You cannot protect vApps which include virtual machines with VirtualEthernetCardLegacyNetworkBackingInfo NICs or with IDE devices.

**To protect a vApp:**

1. In the vSphere Web Client or Client console, select the **Zerto** tab for the vApp to be protected.
   - If the vApp contains virtual machines that are protected, the tab displays a message that the vApp contains protected VMs and you have to remove the protection from these VMs before continuing to protect the vApp.
   - Each virtual machine in the vApp can have a maximum of 15 disks per SCSI controller and up to 4 SCSI controllers.
2. Click **CREATE VPG**.
   - The Create VPG wizard is displayed. The **VPG Name** defaults to the name of the vApp and in the **VMs** step the virtual machines in the vApp are selected. You cannot make any changes in this step.
3. Make any required changes to the VPG, as described in “Protecting Virtual Machines to a Recovery Site vCenter Server”, on page 39, starting with step .

Protecting Virtual Machines to Recovery Hyper-V Hosts

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: * ? : < > / \ ".

The following conversions are done to 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.
To create a virtual protection group to recover in Hyper-V:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The NEW VPG 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.
Zerto Virtual Replication uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.

5. If you want to define the boot order of the virtual machines in the VPG, click **DEFINE BOOT ORDER**, otherwise, go to step 6.

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.

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)

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

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 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 Microsoft SCVMM recovery site, the host and storage on the site to use for the replication can be specified.

![Recovery Site Selection](image)

**Host** – The default cluster or host, in the recovery site that handles the replicated data.

**Storage** – The storage volume to use for all the recovered virtual machine files as well as 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

For additional journal-related fields, click ADVANCED.

The Advanced Journal Settings dialog is displayed.

![Advanced Journal Settings](image)

**Default Journal Storage** – The storage used for the journal data for each virtual machine in the VPG. Select storage accessible to the host. When you select a 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 protected virtual machines must be recovered to the hosts that can access the specified journal storage.

**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.

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

Target RPO Alert – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

Test Reminder – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

9. Optionally, change the Advanced value.

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. 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 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.

10. If you want 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.

11. Select the virtual machines whose values you want to change and click EDIT SELECTED.

The Edit VM dialog is displayed.

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 all the virtual machines specified in the VPG.

**Recovery Storage** – 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 minimum journal size, set by Zerto Virtual Replication, is 8GB.
- **Unlimited** – The size of the journal is unlimited and it can grow to the size of the recovery storage.
- **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 storage.
- **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 Storage** – The storage used for the journal data for each virtual machine in the VPG. 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.

12. Click **SAVE**.
13. In the **Advanced VM Replication Settings** dialog, click **SAVE**.
14. 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.

![Screenshot of the Storage step in Zerto Virtual Replication](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.

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

15. If you want to edit storage information for one of the virtual machines, select the machine and click **EDIT SELECTED**.
The *Edit Volumes* dialog is displayed.

16. Specify the volume source for recovery from one of the options.

   **Storage** – A new volume is used for replicated data.

   **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. 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.

17. Specify the other volume options.

   **Swap disk** – If the virtual machine to be replicated includes a swap disk as part of its configuration, specify a mirror disk for replication that is marked as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

   **Storage** – 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.

18. Click **SAVE**.

19. Click **NEXT**.

   The *RECOVERY* step is displayed. Recovery details include the NIC to use for recovered virtual machines and scripts that should be run either at the start or end of a recovery operation.

20. 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.
21. Check the **Scripts** box if scripts should run as part of the recovery process.

**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>FIELD</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. 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 <em>Performance and Throttling</em> tab in the <em>Site Settings</em> dialog.</td>
</tr>
</tbody>
</table>

22. 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.

![NICs step](image)

23. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click **EDIT SELECTED**. Otherwise, go to step 30.
The *Edit VNIC* dialog is displayed.

24. 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.

**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 by installing Microsoft Integration Services and for the following operating systems: Windows 2003 and higher, Red Hat Enterprise Linux versions 5-6.x, SUSE Linux Enterprise versions 11 SP2 and SP3 and Open SUSE 12.3, Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, Debian versions 7.0-7.4, and CentOS versions 5-6.x.

**Note**: VMware Tools must also be installed, so that a failback after a recovery to Hyper-V will also be able to utilize repiping. VMware Tools must be installed on the virtual machine in the vCenter environment.

To change the vNIC IP, select Yes in the *Failover/Move* or *Test* column. 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 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.

**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** – 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.

25. Click OK.
26. 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.

27. By default, backup is off. If you do not want to change this value, go to step 20. 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 27.

**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 37.

**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>FIELD</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>

28. Click NEXT.

The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.
29. 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.

**Protecting Virtual Machines on a vCenter Server to AWS**

You can protect virtual machines to Amazon Web Services (AWS). The procedure is the same whether you intend to protect one virtual machine or multiple virtual machines.

When recovering to AWS, all recovery operations create the recovered machines in EC2 in AWS.

Only virtual machines that are supported by AWS can be protected by Zerto Virtual Replication. Refer to AWS documentation for the supported operating systems.

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

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.

**Note:** By default, every m3.xlarge instance is created with two SSD disks. These disks are in addition to the disks associated with each protected virtual machine.

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:

- You cannot protect machines that have a disk larger than 1TB.
- AWS supports virtual machines running a Windows operating system with up to 26 volumes, including the boot disk.
- AWS supports virtual machines running a Linux operating system with up to 40 volumes, including the boot disk.
- Protected virtual machines running a Linux operating system with more than 1 volume cannot be failed back from AWS after a failover or move operation.
To create a virtual protection group (VPG):

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The NEW VPG 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.

5. If you want to define the boot order of the VPGs, click DEFINE BOOT ORDER. If you do not want to define the boot order, go to step 6.
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.

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.

1. Click ADD to add a new group.
2. To change the name of a group, click the Pencil icon next to the group. To delete a group, click the delete icon on the right side. You cannot delete the Default group nor a group that contains a virtual machine.
3. Drag virtual machines to move them from one group to another.
4. Drag groups to change the order the groups are started.
5. 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.
6. Click OK to save the boot order.

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.

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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.
- **Target RPO Alert** – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.
- **Test Reminder** – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

9. Click NEXT.

10. Specify whether the protected volume is a swap disk.
- **Swap** – If the virtual machine to be replicated includes a swap disk as part of its configuration, mark the recovery disk for this disk as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.
11. 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.

12. 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 mask for the VPC network.

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

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

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 for one or more of the virtual machines, select the machines and click **EDIT SELECTED**. The **Edit VM Network** dialog is displayed.

![Edit VM Network dialog]

15. Update the values for VPC network, subnet, security group, instance family, instance type, and private IP as necessary. 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.

16. Click **SAVE** twice to return to the main page of the RECOVERY step.

17. Check the **Scripts** box if scripts should run as part of the recovery process.

   **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>FIELD</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. 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 <strong>Performance and Throttling</strong> tab in the <strong>Site Settings</strong> dialog.</td>
</tr>
</tbody>
</table>

18. 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.

19. By default, backup is off. If you do not want to change this value, go to step 20. 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 27.

**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 37.

**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>FIELD</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 values of parameters to pass to the script. Separate parameters with a space.</td>
</tr>
<tr>
<td>0</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>

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

21. 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 is installed at either the protected or recovery site, protection involving vCD can be as follows:

- “Replication From a Protected Site vCenter Server to a Recovery Site vCloud Director”, below
- “Replication From Protected Site vCloud Director to a Recovery Site vCloud Director”, on page 80
- “Replication From Protected Site vCloud Director to a Recovery Site vCenter Server”, on page 88
- “Replication From a Protected Site vCloud Director to Hyper-V”, on page 99
- “Replication From a Protected Site vCloud Director to AWS”, on page 108

The protection can be for set up to cope with a disaster, enabling recovery to any point in time in the 14 days prior to the disaster or extended recovery to backup files saved either daily or weekly for a period of up to one year. The same dialog is used to set up both disaster recover and extended recovery.

When the 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.

Note: 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 vCloud Director 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.¹

Note: You cannot protect virtual machines with VirtualEthernetCardLegacyNetworkBackingInfo NICs or with IDE devices.

Replication From a Protected Site vCenter Server to a Recovery Site vCloud Director

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

- Virtual machines and vApps in the underlying vCenter Server.
  - When the vCD site is set up within Zerto Cloud Manager, as described in Zerto Cloud Manager Administration Guide, virtual machines and vApps in the underlying vCenter Server cannot be specified.
- vCD vApps. For details of protecting from vCD, refer to “Replication From Protected Site vCloud Director to a Recovery Site vCloud Director”, on page 80, “Replication From Protected Site vCloud Director to a Recovery Site vCenter Server”, on page 88.

The protected machines are protected as a vCD vApp in the recovery site vCD.

¹. 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.
To create a virtual protection group (VPG) to recover in vCloud Director:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG.
   The NEW VPG 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.
   **Note:** If vCloud Director is also on the protected site, choose vCenter. For details of protecting from vCD, refer to “Replication From Protected Site vCloud Director to a Recovery Site vCloud Director”, on page 80.
   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.
Zerto Virtual Replication uses the SCSI protocol. Only virtual machines with disks that support this protocol can be specified.

The hardware version of the virtual machine must be the same or less than the hardware version supported by the vDC in vCloud Director 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.

**Note:** You define the boot order for the recovered vCloud Director vApp in the vCloud Director console.

5. Click **NEXT**.

The **REPLICATION** step is displayed.

6. Choose the recovery site and whether recovery will be to VC or vCD.

The **REPLICATION** step is re-displayed, with additional fields that are relevant for VC or vCD. If you chose vCD, this screen is displayed.

   ![Replication Screen](image)

   If **VC** is selected, the procedure is the same as described in "Protecting Virtual Machines to a Recovery Site vCenter Server", on page 39.

   If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.

   If **vCD** is selected, specify the **Recovery Org vDC** to use in the recovery site.

7. 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

For additional journal-related fields, click ADVANCED.

The Advanced Journal Settings dialog is displayed.

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.
- 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.
- 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.

Target RPO Alert - The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

Test Reminder - The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

9. Optionally, change the Advanced value.

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. 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 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.

10. If you want 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.

11. Select the virtual machines whose values you want to change and click EDIT SELECTED.

The Edit VM dialog is displayed.

Storage Profile – Storage profiles enable mapping virtual machines to storage levels according to predefined service levels, storage availability, performance requirements or cost. You can define and label storage tiers and then specify the tier to use as a storage profile, for each virtual machine in the VPG. The default storage profile is the default for the Recovery Org vDC. 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.

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.
- 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.
- 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.

12. Click SAVE.
13. In the Advanced VM Replication Settings dialog, click SAVE.

14. 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.

**Thin** - If the recovery volumes are thin-provisioned or not.

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

15. If you want to edit storage information for one of the virtual machines, select the machine and click **EDIT SELECTED**.

The Edit Volumes dialog is displayed.

16. Specify the volume source for recovery from one of the options.

**vCD managed storage profile** - The datastore is allocated based on the available free space. You can specify whether the recovery volume is thin-provisioned or not. If the Org vDC only supports thin-provisioned volumes, you cannot change the setting.

**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.

17. Specify the other volume options.

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

   **Thin provisioning** – If the recovery volumes are thin-provisioned or not.

18. Click **SAVE**.
19. 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.

20. Select the default recovery settings.

   **vCD Guest Customization** – When checked, 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.

   **Copy NAT Rules** – When checked, NAT rules for a NAT Router Org network are applied during recovery. The automatic setting is applied as automatic and the manual setting is applied as manual using the IPs on the source.

   **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.

21. Check the **Scripts** box if scripts should run as part of the recovery process.

   **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>FIELD</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. 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 <em>Performance and Throttling</em> tab in the <em>Site Settings</em> dialog.</td>
</tr>
</tbody>
</table>

22. 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.

23. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click *EDIT SELECTED*. Otherwise, go to step 26.

The *Edit VNIC* dialog is displayed.

24. 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.

**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** – 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.

25. Click OK.

26. 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.

27. By default, backup is off. If you do not want to change this value, go to step 28. 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 27.

**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 37.

**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>FIELD</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>

28. Click NEXT.

The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous steps.
29. 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 replication is configured to either virtual machines or vApps, depending on what was originally protected.

**Replication From Protected Site vCloud Director to a Recovery Site vCloud Director**

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

- Virtual machines and vApps in the underlying vCenter Server.
  
  When the vCD site is set up within Zerto Cloud Manager, as described in Zerto Cloud Manager Administration Guide, virtual machines and vApps in the underlying vCenter Server cannot be specified.

- vCD vApps. For details of protecting from vCD to a vCenter Server, refer to “Replication From Protected Site vCloud Director to a Recovery Site vCenter Server”, on page 88.

The protected machines are protected as a vCD vApp in the recovery site vCD. Both the VM-level and vCD vApp-level metadata is also replicated to the recovery site.

**To create a VPG from and to vCloud Director:**

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

   The NEW VPG 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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. 
   **Note:** Define the required boot order for vCloud Director vApps in the vCloud Director console.
5. Click NEXT.
   The REPLICATION step is displayed.

   **Note:** If there are multiple sites paired with the protected site, the VC/vCD field is not displayed until the site with vCD is selected.
6. Choose the recovery site and whether recovery will be to VC or vCD.
The REPLICATION step is re-displayed, with additional fields that are relevant for VC or vCD. If you chose vCD, this screen is displayed.

If VC is selected, the procedure is the same as described in “Protecting Virtual Machines to a Recovery Site vCenter Server”, on page 39.

If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.

If vCD is selected, specify the Recovery Org vDC to use in the recovery site.

7. 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

   For additional journal-related fields, click ADVANCED.

   The Advanced Journal Settings dialog is displayed.

   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.

      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.

      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.

**Target RPO Alert** – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

**Test Reminder** – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

9. Optionally, change the Advanced value.

**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. 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 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.

10. If you want 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.

11. Select the virtual machines whose values you want to change and click **EDIT SELECTED**.

The **Edit VM** dialog is displayed.

**Storage Profile** – Storage profiles enable mapping virtual machines to storage levels according to predefined service levels, storage availability, performance requirements or cost. You can define and label storage tiers and then specify the tier to use as a storage profile, for each virtual machine in the VPG. The default storage profile is the default for the Recovery Org vDC. 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.

**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.
- **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.
- **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.

12. Click **SAVE**.
13. In the **Advanced VM Replication Settings** dialog, click **SAVE**.
14. 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.

![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.

**Thin** – If the recovery volumes are thin-provisioned or not.

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

15. If you want to edit storage information for one of the virtual machines, select the machine and click **EDIT SELECTED**.

The **Edit Volumes** dialog is displayed.

![Edit Volumes](image)
16. Specify the volume source for recovery from one of the options.

- **vCD managed storage profile** - The datastore is allocated based on the available free space. You can specify whether the recovery volume is thin-provisioned or not. If the Org vDC only supports thin-provisioned volumes, you cannot change the setting.

- **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.

17. Specify the other volume options.

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

- **Thin provisioning** - If the recovery volumes are thin-provisioned or not.

18. Click **SAVE**.

19. 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.
20. Select the default recovery settings.

**vCD Guest Customization** – When checked, 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.

**Copy NAT Rules** – When checked, NAT rules for a NAT Router Org network are applied during recovery. The automatic setting is applied as automatic and the manual setting is applied as manual using the IPs on the source.

**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.

21. Check the **Scripts** box if scripts should run as part of the recovery process.

**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>FIELD</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. 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 Performance and Throttling tab in the Site Settings dialog.</td>
</tr>
</tbody>
</table>

22. 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.

23. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click **EDIT SELECTED**. Otherwise, go to step 26.
The Edit VNIC dialog is displayed.

24. 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.

**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** – 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.

25. Click OK.
26. 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.

27. By default, backup is off. If you do not want to change this value, go to step 28. 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 27.
**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 37.

**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>FIELD</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>

28. Click **NEXT**.

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

29. Click **DONE**.

The VPG is created.

When recovering the VPG, via a move or failover operation, reverse replication is configured to a vCD vApp.

**Replication From Protected Site vCloud Director to a Recovery Site vCenter Server**

If you want the replication to be to a vCenter Server, the vCD vApp is replicated in the recovery site as a vApp.

**Note:** Because recovery is a vApp, DRS must be enabled in the recovery site. When protecting virtual machines in vCenter Server and recovering to vCloud Director, after a recovery with reverse protection, from the vCD to the vCenter, the virtual machines are not replicated back to the original site as a vApp.

**To create a VPG to protect a vCD vApp to a vCenter Server:**

1. In the Zerto User Interface, select **ACTIONS > CREATE VPG**.
   The **NEW VPG** step of the Create VPG wizard is displayed.
   
   ![Create VPG](image)

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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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 either from the underlying vCenter Server or as a vCD vApp.

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.

**Note:** Define any required boot order for vCloud Director vApps in the vCloud Director console.

5. 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.

6. 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.

**ZORG** - If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.

**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.

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 that 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.

**Datastore** - The datastore volume to use for all recovered virtual machine files as well as 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.

7. 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

For additional journal-related fields, click **ADVANCED**.

1. If Zerto Cloud Manager is used, vSphere Standard edition cannot be used.
The Advanced Journal Settings dialog is displayed.

9. **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 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.
- **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.
- **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.

**Target RPO Alert** - The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

**Test Reminder** - The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

10. Optionally, change the Advanced value.

**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. 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 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.

11. If you want to change the replication settings per virtual machine, click **VM SETTINGS**.
The Advanced VM Replication Settings dialog is displayed.

![Advanced VM Replication Settings](image)

In this dialog, 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.

12. Select the virtual machines whose values you want to change and click **EDIT SELECTED**. The Edit VM dialog is displayed.

![Edit VM](image)

**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 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.

**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.

**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.
    - **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. 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.

13. Click SAVE.
14. In the Advanced VM Replication Settings dialog, click SAVE.
15. 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.

Thin – If the recovery volumes are thin-provisioned or not.
Swap – If the virtual machine to be replicated includes a swap disk as part of its configuration, mark the recovery disk for this disk as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

16. If you want to edit storage information for one of the virtual machines, select the machine and click EDIT SELECTED.

The Edit Volumes dialog is displayed.

17. Specify the volume source for recovery from one of the following options.

   **Datastore** – A new volume is used for replicated data.
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.

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 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.

18. Specify the other volume options.

Swap disk – If the virtual machine to be replicated includes a swap disk as part of its configuration, mark the recovery disk for this disk as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

Datastore – The datastore to use to create disks for the replicated data. Specify whether the target is thin provisioned. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned.

The datastore 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.

You can use the vSphere Client console Performance tab for each virtual machine to help estimate the change rate. For more details, refer to “Collecting Data Characteristics for VMs”, on page 24.

Thin provisioning – If the recovery volumes are thin-provisioned or not.

19. Click OK.
20. 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.

21. 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.
   - **Recovery Folder** – The folder to which the virtual machines are recovered.

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

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

23. Select the virtual machines whose values you want to change and click **EDIT SELECTED**.
The Edit VM dialog is displayed.

![Edit VM dialog](image)

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

24. Click SAVE.

25. In the Advanced VM Recovery Settings dialog, click SAVE.

26. Check the **Scripts** box if scripts should run as part of the recovery process.

**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>FIELD</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. 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 Performance and Throttling tab in the Site Settings dialog.</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.

![NICs step](image)

28. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click **EDIT SELECTED**. Otherwise, go to step 31.
The Edit VNIC dialog is displayed.

29. 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.

**Change vNIC IP Configuration:** Whether or not to keep the default virtual NIC (vNIC) IP configuration. You can only change the vNIC IP for virtual machines with VMware Tools running for the following operating systems: Windows 2003 and higher, Red Hat Enterprise Linux versions 5-7.x, SUSE Linux Enterprise versions 10-11, Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, CentOS versions 5-6.x, and Oracle Linux versions 5.9-6.6.

To change the vNIC IP, select *Yes* in the Failover/Move or Test column. 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 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.

**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** - 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.

30. Click OK.

31. 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.

32. By default, backup is off. If you do not want to change this value, go to step 33. 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 27.
- **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 37.
- **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>FIELD</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>

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

34. 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.

**Note:** When recovering the VPG, via a move or failover operation, reverse replication is configured to a vCD vApp.

---

### Replication From a Protected Site vCloud Director 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 NEW VPG 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. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.

   ![Create VPG](image)

   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.
   **Note:** Define the required boot order for vCloud Director vApps in the vCloud Director console.
5. Click NEXT.
   The REPLICAION 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.

6. 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](image)

   **ZORG** – If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.
   
   **Host** – The default cluster or host, in the recovery site that handles the replicated data.
   
   **Storage** – The storage volume to use for all the recovered virtual machine files as well as 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.

7. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.
   
   For additional journal-related fields, click ADVANCED.
The Advanced Journal Settings dialog is displayed.

**Default Journal Storage** – The storage used for the journal data for each virtual machine in the VPG. Select storage accessible to the host. When you select a 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 protected virtual machines must be recovered to the hosts that can access the specified journal storage.

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

**Target RPO Alert** – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

**Test Reminder** – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

8. Optionally, change the Advanced value.

**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. 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 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.

9. If you want 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.  

10. Select the virtual machines whose values you want to change and click EDIT SELECTED. The Edit VM dialog is displayed.

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 all the virtual machines specified in the VPG.

Recovery Storage – 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 minimum journal size, set by Zerto Virtual Replication, is 8GB.

- Unlimited – The size of the journal is unlimited and it can grow to the size of the recovery storage.
- 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 storage.
- 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 Storage – The storage used for the journal data for each virtual machine in the VPG. 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.

Click SAVE.

11. In the Advanced VM Replication Settings dialog, click SAVE.

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.

![Create VPG Step](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.

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

13. If you want to edit storage information for one of the virtual machines, select the machine and click **EDIT SELECTED**.

The **Edit Volumes** dialog is displayed.

14. Specify the volume source for recovery from one of the options.

- **Storage** – A new volume is used for replicated data.
- **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. 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.

15. Specify the other volume options.

- **Swap disk** – If the virtual machine to be replicated includes a swap disk as part of its configuration, specify a mirror disk for replication that is marked as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.
Storage – 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.

16. Click SAVE.
17. Click NEXT.

The RECOVERY step is displayed. Recovery details include the NIC to use for recovered virtual machines and scripts that should be run either at the start or end of a recovery operation.

18. 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.

19. Check the Scripts box if scripts should run as part of the recovery process.

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>FIELD</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. 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 <em>Performance and Throttling</em> tab in the <em>Site Settings</em> dialog.</td>
</tr>
</tbody>
</table>

20. 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.

21. If you want to edit NIC-related information for one or more of the virtual machines, select the machines and click **EDIT SELECTED**. Otherwise, go to step 31. The Edit VNIC dialog is displayed.

22. 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.

   **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 by installing Microsoft Integration Services and for the following operating systems: Windows 2003 and higher, Red Hat Enterprise Linux versions 5-6.x, SUSE Linux Enterprise versions 11 SP2 and SP3 and Open SUSE 12.3, Ubuntu 12.04, 12.10, 13.04, 13.10, 14.04, Debian versions 7.0-7.4, and CentOS versions 5-6.x.

   **Note**: VMware Tools must also be installed, so that a failback after a recovery to Hyper-V will also be able to utilize rerouting. VMware Tools must be installed on the virtual machine in the vCenter environment.
To change the vNIC IP, select Yes in the Failover/Move or Test column. 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 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.

**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** – 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.

23. Click OK.
24. 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.

25. By default, backup is off. If you do not want to change this value, go to step 33. 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 27.

**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 37.

**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>FIELD</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>
26. Click NEXT.
   The SUMMARY step is displayed. It shows the VPG configuration that you defined in previous tabs.

27. 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 vCloud Director to AWS**

You can protect a vCD vApp to Amazon Web Services (AWS).

When recovering to AWS, all recovery operations create the recovered machines in EC2 in AWS.

Only virtual machines that are supported by AWS can be protected by Zerto Virtual Replication. Refer to AWS documentation for the supported operating systems.

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

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.

**Note:** By default, every m3.xlarge instance is created with two SSD disks. These disks are in addition to the disks associated with each protected virtual machine.

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:

- You cannot protect machines that have a disk larger than 1TB.
- AWS supports virtual machines running a Windows operating system with up to 26 volumes, including the boot disk.
- AWS supports virtual machines running a Linux operating system with up to 40 volumes, including the boot disk.
  - Protected virtual machines running a Linux operating system with more than 1 volume cannot be failed back from AWS after a failover or move operation.
To create a VPG from vCloud Director to AWS:

1. In the Zerto User Interface, select ACTIONS > CREATE VPG. The NEW VPG 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.
   - **Priority** – Determine the priority for transferring data from the protected site to the recovery site when there is limited bandwidth and more than one VPG is defined on the protected site. When there are updates to virtual machines protected in VPGs with different priorities, first the updates from the VPG with the highest priority are passed over the WAN. Medium priority VPGs will only be able to use whatever bandwidth is left after the high priority VPGs have used it. This is also true between medium and low priorities. Note that updates to the protected virtual machines are always sent across the WAN before synchronization data, such as during a Bitmap Sync or Delta Sync. During a synchronization, only after updates to the virtual machines are sent over the WAN, based on the VPG priority, is synchronization data from the VPG sent, and the 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.

   ![Create VPG](image)

   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.
   - **Note:** Define the required boot order for vCloud Director vApps in the vCloud Director console.
5. 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.

6. 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.

![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.

If the site is defined in Zerto Cloud Manager, you specify the name the cloud service provider uses to identify you as a Zerto Organization, ZORG. For details about Zerto Cloud Manager, refer to Zerto Cloud Manager Administration Guide.

7. 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.

8. 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. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

Target RPO Alert – The maximum desired time between each automatic checkpoint write to the journal before an alert is issued. To increase the value, move the slider right; to decrease the value, move the slider left.

Test Reminder – The time recommended between testing the integrity of the VPG. A warning is issued if a test is not done within this time frame.

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 swap disk.

Swap – If the virtual machine to be replicated includes a swap disk as part of its configuration, mark the recovery disk for this disk as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

11. 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.
12. 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 mask for the VPC network.
- **Security Group** - The AWS security to be associated with the virtual machines in this VPG.
- **Instance Family** - The instance family from which to select the type. AWS instance families are optimized for different types of applications. Choose the instance family appropriate for the application 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.

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 for one or more of the virtual machines, select the machines and click **EDIT SELECTED**.

The **Edit VM Network** dialog is displayed.

15. Update the values for VPC network, subnet, security group, instance family, instance type, and private IP as necessary.

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.

16. Click **SAVE** twice to return to the main page of the **RECOVERY** step.

17. Check the **Scripts** box if scripts should run as part of the recovery process.

- **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>FIELD</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. 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 Performance and Throttling tab in the Site Settings dialog.</td>
</tr>
</tbody>
</table>

18. 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.

19. By default, backup is off. If you do not want to change this value, go to step 33. 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 27.
- **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 37.
- **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>FIELD</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 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>

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

21. 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 8: MONITORING ZERTO VIRTUAL REPLICATION

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 VPG monitoring options are described in this chapter:
- “Monitoring Sites – The DASHBOARD Tab”, below
- “Monitoring VPGs – The VPGs Tab”, on page 117
- “Monitoring a Single VPG”, on page 119
- “Monitoring Tasks”, on page 122
- “Monitoring Protected Virtual Machines – The VMs Tab”, on page 124

The following site monitoring option is described in this chapter:
- “Monitoring Peer Sites – The SITES Tab”, on page 125

The following VRA monitoring option is described in this chapter:
- “Monitoring Virtual Replication Appliances”, on page 126

The following storage monitoring option is described in this chapter:
- “Monitoring Datastores – The DATASTORES Tab”, on page 133

The following offsite backup monitoring options are described in this chapter:
- “Monitoring Repositories – The REPOSITORIES Tab”, on page 134
- “Monitoring Offsite Backups – The OFFSITE BACKUP Tab”, on page 135

For details about monitoring Zerto Virtual Manager alerts and events, refer to Zerto Virtual Replication Guide to Alarms, Alerts and Events.
Monitoring Sites – The DASHBOARD Tab

The DASHBOARD provides an overview of the sites and VPGs being protected at the site or recovered to the site.

![Dashboard Image]

The following information is displayed:

**VPG HEALTH**

The VPGs being recovered to AWS with the number of active alerts and 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 AWS 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** – The IO per second between all the applications running on the virtual machines being protected and the VRA that sends a copy to the remote site for replication.
**Throughput (MB/sec)** - The MBs 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.

**WAN Traffic (MB/sec)** - The outgoing traffic between the sites.

**VPG STATUS**

![VPG Status Chart]

The status of the VPGs displayed as a pie chart. The legend describes what the pie chart colors represent.

**SITE TOPOLOGY**

A graphical display of the sites including the number of VPGs.

**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 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.

- **VPG Name (#VMs)** - The name of the VPG. The name is a link: Click on 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.

**PERFORMANCE View**

The following information is displayed in the **PERFORMANCE** view:

- **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 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** (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.

**BACKUP View**

The following information is displayed in the **BACKUP** view:

- **Retention Policy** - Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 14 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 are additional fields that you can display. These fields are listed when you select *Show/Hide Columns* from the dropdown list shown by clicking the configuration icon (○):

- **Protected Site** – The name of the protected site.
- **Recovery Site** – The name of the recovery site.
- **ZORG** – A name given to an organization by a cloud service provider. For details refer to *Zerto Cloud Manager Administration Guide*.
- **Last Test** – The date and time of the last Test Failover operation.

**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 (sec) - 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.

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 (MB/sec) - 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.

WAN TRAFFIC (MB/sec) - The outgoing traffic between the sites.

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 backup details.

Retention Policy - Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 14 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.
The PROTECTED VMs tab shows details about the protected virtual machines. This includes:

- The name of the virtual machine.
- The boot order group to which the virtual machine belongs.
- The protected virtual machine host.
- The host to use for recovery.
- The datastore used on the protected site.
- The recovery datastore.
- The protected virtual machine provisioned storage.
- The protected virtual machine used storage.
- The amount of data used on the recovery site for this virtual machine.
- The storage profile of the recovery site.
- The failover and test networks that will be used for this virtual machine.
- 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.

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 tab under the MONITORING tab.

The following information is displayed for each task:

**Task** - The task.

**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 on 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:

**Retention Policy** – Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 14 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 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 protected site.

**Recovery Site** – The name of the recovery site.

**ZORG** – A name given to an organization by a cloud service provider. For details refer to Zerto Cloud Manager Administration Guide.

**Last Test** – The time and date of the last backup performed by Zerto Virtual Manager.

**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.

**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** tab under the **SETUP** tab. You can also drill-down to monitor information about a specific VRA displayed in the **VRAs** tab:

- “Monitoring VRAs – The **VRAs** Tab”, below.
- “Monitoring a Single VRA”, on page 128.
Monitoring VRAs – The VRAs Tab

View details of the VRAs in the VRAs tab, under the SETUP tab. All the hosts in the local hypervisor manager 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 their data.

# of Recovery VMs - The number of virtual machines for which the VRA manages the recovery of their data.

# of Recovery Volumes - The number of volumes for which the VRA manages the recovery of their 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.
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.
**Monitoring Zerto Virtual Replication**

**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.

**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:

**Retention Policy** – Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 14 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*.
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.
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 DATASTORES Tab

View details of the datastores used by Zerto Virtual Replication in the DATASTORES tab, 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.

**# 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 REPOSITORIES Tab**

View details of the repositories that can be used for offsite backup jobs in the **REPOSITORIES** tab, under the **SETUP** tab.

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.

**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.

Additional Fields

There are no additional fields that you can display. However, you can display all the fields shown when you select Show/Hide Columns from the dropdown list shown by clicking the configuration icon ( ).

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.

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.

Result of Last Run – The result of the last run: Full success, Partial success, or Failed. If a backup job has not yet run on this VPG, the field is empty.

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.

Result of Last Run – The result of the last run: Full success, Partial success, or Failed. If a backup job has not yet run on this VPG, the field is empty.

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 (≠):

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.
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 a Virtual Machine to an Existing VPG”, on page 139
- “Modifying Protected Virtual Machine Volumes”, on page 140
- “Moving a Virtual Machine To or From a Protected vApp”, on page 141
- “Pausing the Protection of a VPG”, on page 141
- “Forcing the Synchronization of a VPG”, on page 142
- “Deleting a VPG”, on page 142
- “Running an Unscheduled Offsite Backup”, on page 143
- “Ensuring Application Consistency – Checkpoints”, on page 144
- “Running Scripts Before or After Recovering a VPG”, on page 151
- “Exporting and Importing VPG Definitions”, on page 154
- “VPG Statuses and Synchronization Triggers”, on page 156
- “Managing Protection When the Recovery Datastore Will Be Unavailable (Datastore Maintenance)”, on page 161

Monitoring VPGs and the VMs that are protected is described in “Monitoring Zerto Virtual Replication”, on page 115.

Editing a VPG

You can edit a VPG definition, including adding virtual machines to the VPG, as described in “Adding a Virtual Machine to an Existing VPG”, on page 139, deleting virtual machines from the VPG, or changing the information about how virtual machines are recovered, such as adding or removing volumes from the virtual machine.

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, and during this time you cannot perform any task that requires the protected and recovery sites to be synchronized together, such as adding a checkpoint or failing the VPG. You can however make changes to the VPG definition, such as changing the history that is maintained as long as the data requirements for the VPG or any of the virtual machines in the VPG are not changed. If you change the storage requirements for any of the virtual machines in the VPG, the VPG definition is re-updated and the synchronization process is restarted.

Note: Synchronization after adding a virtual machine volume to, or removing a virtual machine volume from, a virtual machine in the VPG results in all checkpoints being removed and the checkpoint mechanism restarts after synchronization completes.

To modify a VPG:

1. In the Zerto User Interface, in the VPGs tab 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 “To create a virtual protection group (VPG):”, on page 39. 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 tick.
   
   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 not applied to existing virtual machines but only to new virtual machines added to the VPG.
3. Click DONE.

When a virtual machine is removed from a VPG, a warning is displayed. Another message is displayed when trying to save the VPG, whether to save the recovery volumes or not, which can be used for preseeding, if the virtual machine is added back to the VPG.

The VPG is updated and then synchronized with the recovery site, if required, for example when the host was changed.

**Note:** Synchronization after deleting a virtual machine from a VPG results in all checkpoints being removed and the checkpoint mechanism restarts after synchronization completes.

### 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 was shortened, the number of backup jobs older than the new retention period are deleted from the repository.

### Adding a Virtual Machine to an Existing VPG

You can add a virtual machine that is not already included in a VPG, to an existing VPG.

**Note:** You cannot edit the VPG to add a virtual machine 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.

**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.

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

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.

**Note:** By default, every m3.xlarge instance is created with two SSD disks. These disks are in addition to the disks associated with each protected virtual machine.

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:

- You cannot protect machines that have a disk larger than 1TB.
- AWS supports virtual machines running a Windows operating system with up to 26 volumes, including the boot disk.
- AWS supports virtual machines running a Linux operating system with up to 40 volumes, including the boot disk.
Protected virtual machines running a Linux operating system with more than 1 volume cannot be failed back from AWS after a failover or move operation.

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. During synchronization, you cannot perform any task that requires the protected and recovery sites to be synchronized, such as adding a checkpoint or failing the VPG. You can, however, make changes to the VPG definition, as described in “Editing a VPG”, on page 138.

**Note:** Adding a virtual machine to a VPG results in all checkpoints being removed and new ones are not added until the added virtual machine is synchronized.

**To add a virtual machine to an existing VPG via the VPG definition:**

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.
2. In the VMs step, select the virtual machine that will be part of this VPG and click the arrow pointing right to include this machine in the VPG. If you want to define the boot order of the VPGs, click DEFINE BOOT ORDER.
3. Configure the virtual machine configuration.
4. Click DONE.

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.

If the virtual machine is added to a VPG replicating to 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.

You configure the virtual machine in the VPG in the same way that you configured the other virtual machines in the VPG, when you created the VPG, including the storage and NICS.

### Modifying Protected Virtual Machine Volumes

Adding or deleting volumes for 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.

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.

Changing the defined size of a journal of a virtual machine in a VPG is automatically reflected in 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 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.

Moving a Virtual Machine To or From a Protected vApp

In vSphere Client console you can reconfigure vApps by dragging virtual machines to or from the vApp. In this case the Zerto Virtual Replication protection is updated automatically to recognize the changes to the vApp.

Removing a virtual machine from the vApp results in that virtual machine no longer being protected. However, protection of the remaining virtual machines continues uninterrupted. Conversely, moving a virtual machine to the vApp causes that machine to be automatically added to the VPG, with, wherever possible, the vApp default values set. The vApp VPG is updated and synchronization begins for the added VM between the protected and recovery sites.

Whenever a virtual machine is moved to or from a vApp, all the checkpoints are removed, since the VPG configuration is essentially new.

**Note:** If the default values cannot be set, for example the default recovery datastore does not have enough room, then the VPG is saved with a status of **Needs Configuration**. To initiate protecting the added virtual machine, you have to edit the VPG to define the datastore to use for the virtual machine and the test and failover networks.

If the added virtual machine was protected, it is unprotected before being protected as part of the vApp. If the added virtual machine was originally protected in a VPG containing other virtual machines, the VPG is resynchronized after the virtual machine which is added to the vApp is removed. If the added virtual machine was protected as the only virtual machine in the VPG, the VPG is deleted.

Pausing 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 times 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”, below.

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.

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. This option leaves the target disks, regardless of whether they are wanted or not.
- 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 machine journals by the Zerto Virtual Manager and each checkpoint has the same timestamp 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 integrate Microsoft Volume Shadow Copy Service (VSS) with Zerto Virtual Replication to ensure transaction consistency in a Microsoft Windows server environment.

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, refer to [Zerto Virtual Replication Cmdlets](#).

**Note:** To write application-consistent checkpoints, there is a performance impact on the virtual machine itself as a result of the application-consistent mechanism used, such as VSS, since 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.

This section describes the different options available to ensure application consistency:

- “Adding a Checkpoint to Identify a Key Point”, below.
- “Ensuring Transaction Consistency in Microsoft Windows Server Environments”, on page 146.

Adding a Checkpoint 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 190, or actually performing a failover, as described in “Managing Failover”, on page 208, you can choose the checkpoint as the point to recover to.

![Forex Trading (Site 4): Checkpoints]

The checkpoints listed include checkpoints added via the ZertoVssAgent, as described in “Ensuring Transaction Consistency in Microsoft Windows Server Environments”, below.
Ensuring Transaction Consistency in Microsoft Windows Server Environments

The Microsoft Volume Shadow Copy Service (VSS) enables taking manual or automatic offsite backup copies or snapshots of data, even if it has a lock, on a specific volume at a specific point-in-time over regular intervals. This ensures not just that the data is crash consistent but also transaction consistent if recovery is needed.

Zerto Virtual Replication enables adding checkpoints to the journal that are synchronized with VSS snapshots.

To use Zerto Virtual Replication with VSS to ensure application consistency you must install the ZertoVssAgent on every virtual machine that uses VSS and that you want to protect with Zerto Virtual Replication. The ZertoVssAgent is available from Zerto Ltd. in both 32-bit and 64-bit versions.

You can install the ZertoVssAgent on the following supported Windows operating systems:

<table>
<thead>
<tr>
<th>32-BIT OPERATING SYSTEMS</th>
<th>64-BIT OPERATING SYSTEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2003 SP2</td>
<td>Windows Server 2003 SP2</td>
</tr>
<tr>
<td>Windows Server 2008, all versions (SPs and R2)</td>
<td>Windows Server 2012, all versions (SPs and R2)</td>
</tr>
</tbody>
</table>

To install the ZertoVssAgent:

1. Download and then run the appropriate version of the ZertoVssAgent from the Zerto Support Portal downloads page, either ZertoVss32Agent.msi or ZertoVss64Agent.msi on the virtual machines that uses VSS and that you want to protect with Zerto Virtual Replication.

ZertoVss32Agent.msi is for 32-bit Windows operating systems and ZertoVss64Agent.msi is for 64-bit Windows operating systems.

**Note:** Only a single virtual machine in a VPG can have application consistent checkpoints and the VSS checkpoint is only applied to the virtual machine where the ZertoVssAgent is installed. Thus, even if more than one virtual machine runs VSS, you only install the ZertoVssAgent on one of the virtual machines in the VPG. Also, the virtual machine where the ZertoVssAgent is installed must have network connectivity to the local Zerto Virtual Manager in order to be able to add VSS checkpoints successfully.

2. Follow the wizard through the installation.

   The Zerto Virtual Manager Connections Settings dialog is displayed.

3. Specify the IP address and HTTP port number for the Zerto Virtual Managers managing the protection of the virtual machines, both for the local site and optionally, for the paired, remote site. If the same hypervisor manager is used both for protecting and recovering virtual machines, specify the IP address and HTTP port number for the single Zerto Virtual Manager installed.

   **Note:** The default HTTP port number when Zerto Virtual Replication is installed is 9080.

   If you enter a wrong IP address or port you can correct the address or port after the installation completes by editing the ZertoVssAgentGUI.exe.conf file in the ZertoVssAgent folder under the folder where the ZertoVssAgent is installed, for example, C:\Program Files (x86)\Zerto.

4. Click OK.

   The ZertoVssAgent is installed and the Add VSS Checkpoint is placed on the desktop. The agent runs as a Windows service, ZertoVssprovider.

You can add a checkpoint to the Zerto Virtual Replication via the Add VSS Checkpoint dialog, via the command line or as a scheduled task. The ZertoVssAgent ensures that the virtual machine is in an application consistent state and then sends the
checkpoint to the Zerto Virtual Manager, which then adds the checkpoint to the journals for the VPG containing that virtual
machine.

The checkpoint is logged for the entire VPG, however any other virtual machine in the VPG will have a crash-consistent
checkpoint.

To add a checkpoint while ensuring application consistency via the Add VSS Checkpoint dialog:

1. On a virtual machine where the ZertoVssAgent has been installed, click Start > Programs > Zerto Virtual Replication > Add
   VSS Checkpoint or double-click the Add VSS Checkpoint icon on the desktop.
   The Add VSS Checkpoint dialog is displayed.

2. Enter a name for the checkpoint.
3. Click OK.

Note: A message that the process was completed is displayed on the machine where the ZertoVssAgent has been installed. The
handling of the checkpoint by the Zerto Virtual Manager is done asynchronously and you can check via the recent tasks list in
the Zerto User Interface that the checkpoint is added in the VPG.

To add a checkpoint while ensuring application consistency via the command line:

1. Open the command line dialog as an administrator.
2. Navigate to the directory where the ZertoVssAgent is installed. The default location is
   C:\Program Files\Zerto\ZertoVssAgent\
3. In the command line, run the following:
   
   \"ZertoVssAgent.exe <localURL> <localPort> <remoteURL> <remotePort> <checkpoint>\"

   where:
   localURL – The URL for the Zerto Virtual Manager that manages the protected site.
   localPort – The HTTP port for the Zerto Virtual Manager that manages the protected site.
   remoteURL – The URL for the Zerto Virtual Manager that manages the recovery site.
   remotePort – The HTTP port for the Zerto Virtual Manager that manages the recovery site.
   checkpoint – The name of the checkpoint.

Note: A message that the process was completed is displayed on the machine where the ZertoVssAgent has been installed. The
handling of the checkpoint by the Zerto Virtual Manager is done asynchronously and you can check via the recent tasks list in
the Zerto User Interface that the checkpoint is added in the VPG.

To schedule checkpoints:

1. Open the Task Scheduler.
2. Under the Actions menu item, select Create Task.
The Create Task dialog is displayed.

3. Enter the following:
   **Name** – A name for the task.
   **Run whether the user is logged on or not** – Make sure that this is checked.
   **Run with highest privileges** – Make sure that this is checked.
   The Windows Scheduled Task will be created and run by the currently logged in user. It is recommended after the task is created to change this to NT AUTHORITY\Network Service permissions and follow the steps to allow the correct permissions as described in “To set COM permissions for VSS when “Access Denied” errors are received:”, on page 149.

4. Select the **Triggers** tab and configure a new trigger.
   The New Trigger dialog is displayed.

5. Select the **Actions** tab and create a new action to start the ZertoVssAgent with the IP address and port of the Zerto Virtual Manager and the checkpoint to use. For example:
   C:\Program Files\Zerto\ZertoVssAgent\ZertoVssAgent.exe and
   106.18.206.10 9080 106.18.206.10 9080 "VSSTaskCP"
   That is, with the format: `<protecting_ZVM_IP> 9080 <recovery_ZVM_IP> 9080 "<CP_name>"`
6. Click OK.

7. Select the Settings tab and make changes as required. Make sure Stop the task if it runs longer than is not selected.

8. Click OK.

There are certain permissions required for the Windows scheduled task to execute successfully. For example, you may see the following in the event logs:

```
Volume Shadow Copy Service error: Unexpected error querying for the IVssWriterCallback interface. hr = 0x80070005
```

This is often caused by incorrect security settings in either the writer or requestor process.

If this is the case, the service which runs the Windows Scheduled Task must have NT AUTHORITY\Network Service permissions or be using the SYSTEM account to run the task. VSS operations are performed as NT AUTHORITY\Network Service which is not granted COM access by default on the service assigned to Windows Scheduled Tasks.

The following procedure is only required if the windows scheduled task is using the Network Services account.

The correct permissions can be assigned by using the Component Services application, accessed by running dcomcnfg.exe, in the windows guest.

**To set COM permissions for VSS when “Access Denied” errors are received:**

1. Run dcomcnfg.exe.
   
   The Component Services dialog is displayed.

2. Expand the Component Services node to My Computer and right-click to access the Properties menu.
   
   The My Computer Properties dialog is displayed.


4. Add the NETWORK SERVICE local access.
5. Click OK and verify that the user is now in the Access Permission list.

6. Click OK to commit these changes.

Access Denied messages should no longer be written in the event viewer for VSS. Additionally, you can grant Network Service full control over HKLM\SYSTEM\CurrentControlSet\Services\VSS\Diag. You can also check this key HKLM\SYSTEM\CurrentControlSet\Services\VSS\VssAccessControl which should at least contain the DWORD NT Authority\NetworkService set to value 1.

You may also add a new DWORD like DOMAIN\MyZertoServiceUserAccount and set its value to 1.

During recovery you can recover to the VSS checkpoint, ensuring both application consistency and that the data is crash-consistent for this virtual machine. For details, refer to “To test failover:” on page 191 and “To initiate a failover:”, on page 209.

Test to See if Guest Can be Quiesced Successfully

If you are not receiving the checkpoints or if you wish to test if the Windows guest can be quiesced successfully, a snapshot may be taken of the VM via the vSphere Client. If VMware tools are installed, VMware can quiesce the Windows guest operating system. If this snapshot takes a long time to generate, then the ZertoVssAgent checkpoints may fail. For example, if this operation takes longer than the frequency of the Windows scheduled task, then either the task must be set to a higher interval or the Windows guest must be troubleshooted to lower the quiesce time.

Note: To check if the Windows guest can be quiesced successfully, you must first uninstall the ZertoVssAgent and then take the VMware snapshot.
Changing the Zerto Virtual Manager Used by the ZertoVssAgent

When you install the ZertoVssAgent, you specify the Zerto Virtual Manager to use to manage the addition of checkpoints for the virtual machines that uses VSS and that you want to protect in VPGs. You can change the IP and port of the VPG that you specified during the installation either by rerunning the installation and selecting the Repair ZertoVssAgent option or by editing IP and port values in the ZertoVssAgentGUI.exe.conf file in the folder where the ZertoVssAgent is installed.

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 is installed.

**Note:** Zerto recommends duplicating scripts on the Zerto Virtual Managers for both the protected and recovery sites, so that if reverse replication is required, the scripts are available. The location of the script for reverse replication, 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. The default is 443.
- **%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.

**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 a 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%` environment variable:

   ```powershell
   $Operation = "%ZertoOperation%"
   If ($Operation -eq "FailoverBeforeCommit" -or "MoveBeforeCommit")
   { desired code here }
   else { alternative code here }
   ```

4. Update **Command to run** and **Params** fields for all the VPG definitions that you want to run the script.

   **Note**: Zerto recommends testing both PowerShell and batch scripts by running them from the command line, to ensure that they run correctly. Note that 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.

**Example Scripts**

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 153.
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\ListOfTestedVPGs.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 `ListOfTestedVPGs.txt` does not exist it is created, as long as the folder, `c:\ZertoScripts\Results`, exists.

Update Command to run and Params fields for all the VPG definitions that you want to run the script.

- **Command to run** – `c:\ZertoScripts\TestedVPGs.bat`
- **Params** – `%ZertoOperation% %ZertoVPGName%`

Whenever a failover test is run on the relevant VPGs, the `ListOfTestedVPGs.txt` file is updated with the name of the VPG and the date and time the test was run.

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.
```

Managing VPGs
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.

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.

![Export Protection Group Settings dialog box](image)

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.

![Import Protection Group Settings dialog box](image)

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.

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.

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>History Not Meeting SLA</td>
<td>See Not Meeting SLA, below.</td>
<td>The VPG is meeting the RPO SLA setting.</td>
</tr>
<tr>
<td>Initializing</td>
<td>Creating VPG</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>STATUS</td>
<td>SUBSTATUS</td>
<td>COMMENT</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------------------------</td>
</tr>
<tr>
<td>Meeting SLA</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>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>Delta Sync (When Force Sync is not applied)</td>
<td>This status means that the VPG is not meeting the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>journal history nor RPO SLA settings.</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>Needs configuration</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>VPG has no VMs</td>
<td></td>
</tr>
<tr>
<td>Recovered</td>
<td>—</td>
<td>The VPG has been recovered.</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.</td>
</tr>
</tbody>
</table>
The following provides a full description of the sub-statuses are displayed:

<table>
<thead>
<tr>
<th>SUBSTATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backing Up</td>
<td>An offsite backup is running.</td>
</tr>
</tbody>
</table>
| Bitmap Syncing¹       | 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.  
   **Note:** The VRA buffer is set via the Amount of VRA RAM value, specified when the VRA is installed  
   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.  
   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 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 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, the VPG status changes to Recovery Possible 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.  
   **Note:** 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 181. |
<p>| Committing Failover   | Failing over the VPG.                                                                                                                                                                                      |
| Committing Move       | Completing the move, including removing the protected virtual machines.                                                                                                                                     |
| Creating VPG          | The VPG is being created based on the saved definition.                                                                                                                                                     |
| Deleting the VPG      | Deleting the VPG.                                                                                                                                                                                          |</p>
<table>
<thead>
<tr>
<th>SUBSTATUS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
</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 VRA upgrade.  
  - For reverse protection after a move or failover.  
  - After the hypervisor manager was down and then restarted.  
  - 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. Also, recovery operations are not possible during a Delta Sync.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| 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. Also, recovery operations are not possible when delta syncing a volume.                                                                                                                                                                                                                                                                                                                                                     |
| 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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| 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 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.                                                                                                                                                                                                                   |
| 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 or a virtual machine is added to a vApp.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Promoting                   | 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.                                                                                                                                                                                                                                                                                                                                                                                                   |
### 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 142.</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>
<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>
</tbody>
</table>
Managing VPGs

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, adding the virtual machines back to the VPG, 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.

The VPG will undergo a Delta Sync before returning to a Meeting SLA status.

<table>
<thead>
<tr>
<th>TRIGGER</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<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>
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 this 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 165
- “Editing VRA Settings”, on page 167
- “Resetting the Host Passwords Required By More Than One VRA”, on page 167
- “Changing a Recovery VRA For Virtual Machines”, on page 168
- “Uninstalling VRAs”, on page 169
- “Handling a Ghost VRA”, on page 169
- “Managing Protection During VMware Host Maintenance”, on page 170
- “Managing Protection When Moving a Host to a Different Cluster”, on page 170

Monitoring VRAs is described in “Monitoring Virtual Replication Appliances”, on page 126.

Installing a VRA

It is recommended to install 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 recommendation\(^1\), 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.

### To set up routing:

1. In the SETUP > VRAs tab, select MORE > Paired Site Routing.
   
   The **Configure Paired Site Routing** dialog is displayed.

   ![Configure Paired Site Routing](image)

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 the VRAs on the peer site.

   The settings in the **Configure Paired Site Routing** dialog apply to all VRAs installed after the information is saved. 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 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.

3. Specify the following Host Details:

**Host** – The host under which the VRA is installed. The drop-down displays the hosts managed by the hypervisor management center which do not have a VRA installed, with the selected host displayed by default.

**Host Root Password** – The password used to access the host for the root user. This field is required for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts. When the checkbox at the side is checked, the password is displayed as asterisks. The password is used by the Zerto Virtual Manager when deploying and upgrading the VRA on this host. Also, root access is required in case the Zerto host component is down and needs an automatic restart. The 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.

**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>
<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>
</tbody>
</table>

**Note:** If you selected a cluster or multiple hosts, only the first host in the displayed list is installed.
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. 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.

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. If you want 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 is on VRA1 in group1 and VPG2 in on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.

4. 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.

5. Click INSTALL.

   The VRA installation starts and the status is displayed in either the TASKS popup dialog in the status bar or 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.

Upgrading VRAs

When upgrading Zerto Virtual Replication, the VRAs that were installed in the previous version are not upgraded automatically. Zerto Virtual Replication enables VRAs installed with the previous version of Zerto Virtual Replication to work with VRAs installed with the current version of Zerto Virtual Replication in any combination of VRAs (all from one version or a mix of VRA versions) as long as the VRAs are only one update higher or lower than the version of Zerto Virtual Replication installed on this site. Zerto recommends upgrading the VRAs to be consistent with the latest version and this can be done by selecting SETUP > VRAs.

After upgrading Zerto Virtual Replication, the VRAs might also require an upgrade. You can see if an upgrade is available in the VRAs tab.

Note: An alert is also issued that there are VRAs that can be upgraded.

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 Delta 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, remove affinity rules for protected virtual machines on the host with the VRA to be upgraded and 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 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.

4. Click UPGRADE SELECTED VRAs.

The upgrade progress is displayed in the VRAs tab.

A Delta Sync, for VRAs protecting virtual machines, or a Bitmap Sync, for VRAs managing recovery, is performed following the upgrade.

**Note:** The VRA name does not change, even if the naming convention in the latest version is different.

You do not need to upgrade VMware Tools on a VRA.
**Editing VRA Settings**

If you need to change the 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, select the VRAs to upgrade, and click MORE > Edit.
   
   The *Edit VRA* dialog is displayed.

2. Edit the host root password if the password for the host has changed. To display the password in plain text, click in the checkbox next to the field.

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. It is recommended to always 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.

   **Default Gateway** – The default mask for the network.

5. Click SAVE.

**Resetting the Host Passwords Required By More Than One VRA**

VRAs installed on ESXi 4.x and 5.x hosts require a password to access the host. This password is supplied as part of the installation of each VRA. The password is required for situations such as rebooting or upgrading the host. If the password for a host is changed 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.

The Zerto Virtual Manager checks the password is valid once a day. If the password was changed, an alert is triggered, requesting the user enter the new password.
To reset the host password required by one or more VRAs:

1. In the Zerto User Interface, click SETUP > VRAs, select the VRAs that need to be updated, and click MORE > Change Host Password.
   
   The Change Host Password VRA dialog is displayed.

2. Edit the host root password:
   - **New Password** - Enter the new password.
   
3. Click SAVE.

**Changing a Recovery VRA For Virtual Machines**

**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 host VRA:**

1. In the Zerto User Interface, select the VRA to change in the VRAs tab under the SETUP tab.
2. Click MORE > Change VM Recovery VRA.
   
   The Change VM Recovery VRA dialog is displayed, listing all the virtual machines that require a change to the recovery host.

3. Review the list and select the virtual machines to change the target host to another specified target host.
4. Select the target host for these virtual machines in the Select the replacement host drop-down list. You can move some virtual machines to one replacement target host and by repeating the operation, move other virtual machines to a different target host.

   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 target 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 2-VRAH-ESXi:hostname-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 from step 3 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 For Virtual Machines”, on page 168. 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 Ghost VRA”, on page 169.

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 For Virtual Machines”, on page 168.
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 Ghost VRA

When an event occurs, 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. The VRA is represented in the VRAs tab as a ghost VRA.

**To recover VRA disks from a ghost 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 162.
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. Shut down the VRA before starting the host maintenance. After the host maintenance power on the VRA.

**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 For Virtual Machines”, on page 168. Shut down the VRA before starting the host maintenance. After the host maintenance power on the VRA.

**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 For Virtual Machines”, on page 168.
3. Wait for any synchronization to complete.
4. Shutdown the VRA on the host manually in order to enable the host to enter VMware Maintenance.
5. Enter VMware Maintenance for the host.
   **Note:** Do not migrate powered-off virtual machines, if prompted to.
6. Remove the host from the cluster: Place it under the datacenter entity rather than the cluster entity.
7. Perform required maintenance, for example, upgrading the host.
8. Exit VMware maintenance mode.
9. Power on the VRA.
10. 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.
11. Add the host back in to the cluster.

**Managing Protection When Moving a Host to a Different Cluster**

When a host machine has to 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.
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.

A Zerto Virtual Manager can manage up to 5000 virtual machines, either being protected by, or recovered to, the Zerto Virtual Manager.

The following topics are described in this chapter:

- “Check Connectivity Between Zerto Virtual Replication Components”, below
- “Reconfiguring the Zerto Virtual Manager Setup”, on page 173
- “Reconfiguring the Microsoft SQL Server Database Used by the Zerto Virtual Manager”, on page 175
- “Replacing the SSL Certificate”, on page 176
- “Pair to Another Site”, on page 177

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 local site and paired site, 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 option 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 either 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.
   **HTTP Port (ZVM)** – The port used for inbound communication between the Zerto Virtual Manager and Zerto RESTful APIs, PowerShell Cmdlets and a VSS Agent.
   **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.
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.

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

When installing Zerto Virtual Replication, you can specify a Microsoft SQL Server database to use by the Zerto Virtual Manager. If the access to this database changes, you can change the access in the Zerto Virtual Manager.

To reconfigure the access to the Zerto Virtual Manager database:

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 \instance. 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.

SQL Server Authentication – Use SQL Server authentication.
  User Name – The user name for SQL Server database.
  Password – A valid password for the given user name.

3. Click Next to the end of the wizard and then click Finish.
The Zerto Virtual Manager service is restarted using the new credentials.

Replacing the SSL Certificate

The 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.

If you want to replace the SSL certificate, perform the procedure described in “To reconfigure the Zerto Virtual Manager:”, on page 173 and select a new SSL certificate when the dialog for Zerto Virtual Manager setup is displayed:

HTTP Certificate – Check Replace SSL Certificate and browse for a replacement certificate.
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.

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 hypervisor site is connected to the Zerto Virtual Manager at the remote hypervisor site.
CHAPTER 12: ADVANCED SITE CONFIGURATION

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 184
- “Submitting a Support Ticket”, on page 185
- “About Zerto Virtual Replication”, on page 186

Site Settings

The Site Settings dialog enables configuring various site settings. These include the maximum bandwidth that Zerto Virtual Replication uses between the protected and recovery sites, default script timeout, and protection policies such as the commit policy for a failover or move operation.

To specify site settings:

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.

2. Make any required changes to the settings, click Apply, and then Save. The following settings can be defined:
   - “Editing Information About a Site”, below
   - “Defining Performance and Throttling”, on page 179
   - “Defining Site Policies”, on page 181
   - “Configuring Email Settings”, on page 182
   - “Defining Resource Report Sampling Period”, on page 183
   - “Reviewing Supported Host Versions”, on page 184

Licensing is described in “Seeing What is Licensed”, on page 184. 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.

In the Zerto User Interface, site information is displayed at the top of the display.

To update information about the local site:

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.

2. Define general information about the site.
   - **Site Name** – The name used to identify the site. Mandatory.
   - **Site Location** – Information such as the address of the site or a significant name to identify it. Mandatory.
   - **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. If the credentials to access the vCenter Server from the Zerto Virtual Manager change, specify the new credentials:
   - **User Name** – The administrator name used to access the vCenter Server. The name can be entered using either of the following formats:
     - username
     - domain\username
   - **Password** – The password used to access the vCenter Server for the given user name. To ensure security, after saving the settings, the password field is cleared.

4. 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 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”, on page 23.
**Time-based Bandwidth Throttling** – If you know that the bandwidth needs specific throttling during a certain period, for example, during the daily peak transaction period you can override the general throttling of the bandwidth for these specific times.

**To configure bandwidth:**

1. Click *Performance and Throttling*.

![Bandwidth Configuration](image)

2. Specify the bandwidth throttling you want. You can use the slider to set the Mb/sec. 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.
   
   A value of 0 Mb/sec means that the bandwidth used is determined automatically by Zerto Virtual Replication.

3. To specify time-based throttling, check the *Time-based Throttling* checkbox.

4. Specify the maximum bandwidth for the period.
   
   If the *Unlimited* checkbox is checked, the bandwidth is always unlimited.
   
   A value of 0 Mb/sec means that the bandwidth used is determined automatically by Zerto Virtual Replication.
   
   You can use the slider to set the Mb/sec.
   
   a) In the *From* fields, select the start time for throttling.
   
   b) In the *To* fields, select the end time for throttling.

5. Click *APPLY* or *SAVE*.

IO Throttling values should be changed **only** in coordination with Zerto support.
Defining Site Policies

You can set default recovery and replication policies.

Configuring Disaster Recovery Policies

To configure disaster recovery policies:

1. Click Policies.

2. Choose the Failover/Move Commit Policy to use during a failover or move operation, described in "Initiating a Failover", on page 209 and "Moving Protected Virtual Machines to a Remote Site", on page 202 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 virtual machines in the VPG.

   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. 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 151.

5. 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 21.

6. Choose the Replication Pause Time, which is the time to pause when synchronizing a VPG if continuing the synchronization will cause all the checkpoints in the journal to be removed.

   During synchronization, the latest changes in the protection site are added to the journal and older data in the journal is moved to the mirror virtual disk managed by the VRA for the virtual machine. As the synchronization continues and more old data is moved out of the journal, the checkpoints associated with the data are also removed from the journal and new checkpoints are not added to the journal. If the synchronization continues for too long, all the checkpoints can be removed from the journal meaning all recovery operations, test failover, move, and failover, can no longer be performed.
The replication pause time is the amount of time that synchronization pauses, when the number of checkpoints in the journal becomes too small. Thus, 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 216, before continuing with the synchronization. The value set here is applied to existing and new VPGs.

**Note:** The setting is applied to the site only. If you want the ability to pause the protection in both directions, for example to cover reverse protection back to the original site after a move operation, set the replication Pause Time on both sites.

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.

![Image of Email Settings interface]

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.
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.

**To configure report settings:**

1. Click Reports.

![Resource Report Sampling Settings]

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 225.
Reviewing Supported Host Versions

Zerto Virtual Replication works with most VMware hypervisor hosts. For a list of supported hosts, click Compatibility.

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 in the Site Settings > License dialog.

The cloud and enterprise license include the following details:

License - The license key itself.

License ID - An identifier for the license.

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 number of licenses is unlimited.
**Maximum Sites** – The maximum number of sites allowed.

An enterprise license also includes the following:

**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.

**Note:** The number of virtual machines is independent of whether they are in vApps or not.

**To update a license key:**

1. In the Zerto User Interface, in the top right of the header click **SETTING ( )** and select **Site Settings**.
   The **Site Settings** dialog is displayed.
2. Click **License**.
3. 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:**

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.
   - **Description** – A description of the ticket in addition to the information supplied in the subject.
   - **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

You can see details about the version of Zerto Virtual Replication being run and specify whether the version can be automatically updated when new VMware vSphere versions are released, without the need to upgrade to a later version of Zerto Virtual Replication. This functionality is the Zerto CALLHOME feature.

To see version information and prepare to send analytics to Zerto:

1. In the Zerto User Interface, in the top right of the header click SETTING ( Settings) and select Site Settings. The Site Settings dialog is displayed.
2. Click About. The version and build of Zerto Virtual Replication that are installed in the site are displayed.
3. If you want to send analytics to Zerto automatically, check Send analytics to Zerto. This initiates the CALLHOME feature. This information is used solely to improve Zerto Virtual Replication.
4. Click SAVE or APPLY.
CHAPTER 13: OVERVIEW OF DISASTER RECOVERY OPERATIONS

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 187
- “The Move Operation”, below
- “The Failover Operation”, on page 188
- “The Clone Operation”, on page 189

In addition, when extended recovery is defined, an offsite backup can be restored as described in “Restoring Virtual Machines”, on page 219.

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 190.

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 201.
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 auto-generated checkpoint, an earlier checkpoint, or a user-defined 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 208.

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 202.
The following diagram shows the positioning of the virtual machines before and after the completion of a Failover operation.

**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.

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 216.

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 191
- “Viewing Test Results”, on page 195
- “Live Disaster Recovery Testing”, on page 195

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 215.

The Failover Test operation has the following basic steps:

- Starting the test.
  - 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.
  - The test virtual machines are created without CD-ROM drives, even if the protected virtual machines have CD-ROM drives.
  - 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.

- 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.

- Stopping the test.
  - The test virtual machines are powered off and removed from the inventory.
  - The following tag is added to the checkpoint specified for the test: Tested at startDateAndTimeOfTest

The updated checkpoint can be used to identify the point-in-time to restore the virtual machines in the VPG during a failover.

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

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 REPLICATION step of the Create VPG wizard.

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 “To create a virtual protection group (VPG):”, 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.

4. By default, the last checkpoint added to the journal is displayed. If you want to use this checkpoint, go to step 7. If you want to change the checkpoint, click on the checkpoint that is displayed. The \{VPG-Name\}: Checkpoints dialog is displayed.

5. Select the checkpoint to use. Click the refresh button to refresh the list. You can choose from one of the following checkpoints:
   - Latest – The recovery or clone is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery or clone. 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 or clone, the later checkpoint is **not** used.
   - Latest User Defined Checkpoint – The recovery operation is to the latest checkpoint created manually. Checkpoints added to the virtual machine journals in the VPG by the Zerto Virtual Manager ensure that the data is crash-consistent to this point. If a checkpoint is added between this point and starting the operation, this later checkpoint is **not** used.
   - Latest VSS – When VSS is used, recovery or clone is to the latest VSS snapshot, ensuring that the data is both crash-consistent and application consistent to this point. The frequency of VSS snapshots determines how much data can be recovered. For details about VSS checkpoints, see “ Ensuring Transaction Consistency in Microsoft Windows Server Environments”, on page 146.
If you do not want to use the latest checkpoint, latest user defined checkpoint, or latest VSS checkpoint, choose **Select from all available checkpoints**. By default, this option displays all checkpoints in the system. You can choose to display only automatic, VSS, or user defined checkpoints, or any combination of these types.

6. Click **OK**.

7. 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.

8. 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.

**After Starting a Test, What Happens?**

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 185.
- 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 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 on 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 test* icon, in either the Dashboard or the dynamic tab, to stop the test in the specific VPG tab.

![Dashboard Screenshot](image-url)

You can also stop the test via the TASKS popup dialog in the status bar or under MONITORING > TASKS. The *Stop Test* dialog is displayed.

![Stop Test Dialog](image-url)

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 virtual machines in the recovery site are powered off and removed, and 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 226.

### 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:

- The 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?
- The 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.

The following flowchart shows the testing decision flow:

During any live test, Zerto recommends that you only maintain one working version of the same virtual machine. Thus, 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 187 and in “Starting and Stopping Failover Tests”, on page 191.

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.

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. Thus, since both the scratch volume and virtual machines being tested are on the same site, performance can be impacted by the increased I/Os during the failover test. Also, 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 202.

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.

**Move Considerations**

- 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. Thus, 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. Also, 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 187 and in “Moving Protected Virtual Machines to a Remote Site”, on page 202.

**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.

**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 they are committed and then 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 188 and in “Initiating a Failover”, on page 209.

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.

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.

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 189 and in “Cloning a VPG to the Recovery Site”, on page 216.

The cloned virtual machines are independent of Zerto Virtual Replication. At the end of the test you can remove these machines or leave them.

Clone Considerations

- You can clone to a specific point-in-time.
- There is no protection for the cloned machines.
Testing Recovery

- 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 202
- “Reverse Protection For a Moved VPG”, on page 206

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 208.

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.
  
  Note: The virtual machines are created without CD-ROM drives, even if the protected virtual machines had CD-ROM drives.

- 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.

- Removing the protected virtual machines from the inventory.

- 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 replication 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 replication 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.

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 to a remote site, where the virtual machines are replicated. As part of the process you can also set up reverse replication, where you create a virtual protection group 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.

4. To change the commit policy, click it.
   a) To commit or roll back the recovery operation automatically, without any checking, select Auto-Commit or Auto-Rollback and 0 minutes.
   b) If you do not want an automatic commit or rollback, select None. You have to manually commit or roll back.
   c) To allow checking before committing or rolling back, specify the amount of time to check the recovered machines, in minutes, before the automatic commit or rollback action is performed, if you do not commit or rollback manually before this time. During this time you can 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.
   The amount of time for checking is incremented in blocks of ten minutes. If you want to specify a time with a different increment, either specify the time or select the VPG and click EDIT SELECTED. You can change the for amount of time for checking by increments of one minute.
   Checking that involves I/O is done on scratch volumes. The longer this period the more scratch volumes are used, until the maximum size is reached, at which point no more checking 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.

   Note: When deciding to commit the operation, you can decide to configure reverse protection, regardless of the reverse protection setting when the operation started.

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 VPG wizard is displayed.
   You can edit the reverse protection configuration, as described in “To create a virtual protection group (VPG):”, on page 39, with the following differences:
   ■ You cannot add or remove virtual machines to the reverse protection VPG.
   ■ By default, reverse replication is to the original protected disks. You can specify a different datastore to be used for the reverse replication. For details, refer to the procedure “To create a virtual protection group (VPG):”, on page 39.
   ■ 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. For details, see “To create a virtual protection group (VPG):”, on page 39.
   The vSphere version must be 4.1 or higher for re-IP to be enabled.
7. Click NEXT.

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.

8. Click START MOVE to start the migration.

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.

**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.

9. After checking the virtual machines on the recovery site, choose one of the following:
   - Wait for the specified Commit Policy time to elapse, and the specified operation, either Commit or Rollback, is performed automatically.
   - Click the Commit or Rollback icon (✓ ✓) in the specific VPG tab.
   - 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.

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.

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.

The following conversions are done to 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.

Note:
- When recovering the VPG to a vCloud Director site, reverse protection is configured to a vApp.
- When recovering RDM disk, the target for reverse protection is the original RDM.

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.

**Note:** 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.
CHAPTER 16: MANAGING FAILOVER

This chapter describes how to perform a failover to the recovery site after an unforeseen disaster. The following topics are described in this chapter:

- “The Failover Process”, below
- “Initiating a Failover”, on page 209
- “Reverse Protection for a Failed Over VPG”, on page 214
- “Initiating a Failover During a Test”, on page 215

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 201.

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 auto-generated checkpoint, an earlier checkpoint, or a user-defined 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. The virtual machines are created without CD-ROM drives, even if the protected virtual machines had CD-ROM drives.
    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.

**Note:** If reverse protection is not possible, the original protected site virtual machines are not powered off and removed.

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 201.

**Initiating a Failover**

You can initiate a failover, whereby the virtual machines in the virtual protection group are replicated to a set checkpoint in the recovery site. As part of the process you can also set up reverse replication, whereby you create a virtual protection group 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 215.

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:** 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 is displayed.

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 step is displayed.

4. By default, the last checkpoint added to the journal is displayed. If you want to use this checkpoint, go to step 7. If you want to change the checkpoint, click on the checkpoint that is displayed.

The {VPG-Name}: Checkpoints dialog is displayed.

5. Select the checkpoint to use. Click the refresh button to refresh the list. You can choose from one of the following checkpoints:

   Latest – The recovery or clone is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery or clone. 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 or clone, the later checkpoint is not used.

   Latest User Defined Checkpoint – The recovery operation is to the latest checkpoint created manually. Checkpoints added to the virtual machine journals in the VPG by the Zerto Virtual Manager ensure that the data is crash-consistent to this point. If a checkpoint is added between this point and starting the operation, this later checkpoint is not used.
**Latest VSS** – When VSS is used, recovery or clone is to the latest VSS snapshot, ensuring that the data is both crash-consistent and application consistent to this point. The frequency of VSS snapshots determines how much data can be recovered. For details about VSS checkpoints, see “Ensuring Transaction Consistency in Microsoft Windows Server Environments”, on page 146.

If you do not want to use the latest checkpoint, latest user defined checkpoint, or latest VSS checkpoint, choose Select from all available checkpoints. By default, this option displays all checkpoints in the system. You can choose to display only automatic, VSS, or user defined checkpoints, or any combination of these types.

6. Click OK.

7. To change the commit policy, double-click it.
   a) To commit or roll back the recovery operation automatically, without any checking, select Auto-Commit or Auto-Rollback and 0 minutes.
   b) If you do not want an automatic commit or rollback, select None. You have to manually commit or roll back.
   c) To allow checking before committing or rolling back, specify the amount of time to check the recovered machines, in minutes, before the automatic commit or rollback action is performed, if you do not commit or rollback manually before this time. During this time you can 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.
   The amount of time for checking is incremented in blocks of ten minutes. If you want to specify a time with a different increment, either specify the time or select the VPG and click EDIT SELECTED. You can change the for amount of time for checking by increments of one minute.
   Checking that involves I/O is done on scratch volumes. The longer this period the more scratch volumes are used, until the maximum size is reached, at which point no more checking 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.

   **Note:** When deciding to commit the operation, you can decide to configure reverse protection, regardless of the reverse protection setting when the operation started.

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** – 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, do one of the following:
   - 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. If you want to configure the VPG for reverse protection, click the REVERSE link.

   The Edit Reverse VPG wizard is displayed.

   You can edit the reverse protection configuration, as described in “To create a virtual protection group (VPG):”, on page 39, with the following differences:
   - You cannot add or remove virtual machines to the reverse protection VPG.
   - By default, reverse replication is to the original protected disks. You can specify a different storage to be used for the reverse replication. For details, refer to the procedure “To create a virtual protection group (VPG):”, on page 39.
   - If VMware Tools is available, for each virtual machine in the VPG, the IP address of the originally protected 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. For details, see “To create a virtual protection group (VPG):”, on page 39.

   The vSphere version must be 4.1 or higher for re-IP to be enabled.

   **Note:** When committing the failover, you can reconfigure reverse protection, regardless of the reverse protection settings specified here.
10. If you want the machines in the recovery site to be booted in the order you defined when you created the VPG, click the **Boot Order** field and check the field.

11. If you want the procedure to run the scripts you defined when you created the VPG, click the **Scripts** field and check the field.

12. Click **NEXT**.

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.

13. 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 replication 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. After checking the virtual machines on the recovery site, choose one of the following:

- Wait for the specified Commit Policy time to elapse, and the specified operation, either Commit or Rollback, is performed automatically.
- Click the Commit or Rollback icon (✓ ✓) in the specific VPG tab.

Click Commit. The Commit dialog 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 checking the Reverse Protection checkbox and then click the Reverse link. Configuring reverse protection here overwrites any of settings defined when initially configuring the move.

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.

You can also commit or roll back the operation via the TASKS popup dialog in the status bar, or by selecting MONITORING > TASKS.

If the original protected site is still up and reverse replication 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.

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.

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 “To create a virtual protection group (VPG):”, 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.

The following conversions are done to 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 Failed Over VPG

When you specify reverse protection, 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 and then on the target site the data is promoted from the journal to the recovered virtual machines and then synchronization with the original site is performed 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.

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.
Note:
- When recovering the VPG to a vCloud Director site, reverse protection is configured to a vApp.
- When recovering RDM disk, the target for reverse protection is the original RDM.

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*.

**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 209.

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 replication 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 209. 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.
CHAPTER 17: CLONING A VPG TO THE RECOVERY SITE

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 216

Note: You cannot clone virtual machines in a VPG test while a backup job is running.

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 drives, even if the protected virtual machines have CD-ROM 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 on 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.
   
   The {VPG-Name}: Offsite Clone dialog is displayed.

3. If you intend to use the last checkpoint, which is displayed in the dialog, go to step 6.
To select the checkpoint to use to create the clone, click SELECT A CHECKPOINT. The {VPG-Name}: Checkpoints dialog is displayed.

4. Select the checkpoint to use. Click the refresh button to refresh the list. You can choose from one of the following checkpoints:
   - **Latest** – The recovery or clone is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery or clone. 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 or clone, the later checkpoint is not used.
   - **Latest User Defined Checkpoint** – The recovery operation is to the latest checkpoint created manually. Checkpoints added to the virtual machine journals in the VPG by the Zerto Virtual Manager ensure that the data is crash-consistent to this point. If a checkpoint is added between this point and starting the operation, this later checkpoint is not used.
   - **Latest VSS** – When VSS is used, recovery or clone is to the latest VSS snapshot, ensuring that the data is both crash-consistent and application consistent to this point. The frequency of VSS snapshots determines how much data can be recovered. For details about VSS checkpoints, see “Ensuring Transaction Consistency in Microsoft Windows Server Environments”, on page 146.

   If you do not want to use the latest checkpoint, latest user defined checkpoint, or latest VSS checkpoint, choose Select from all available checkpoints. By default, this option displays all checkpoints in the system. You can choose to display only automatic, VSS, or user defined checkpoints, or any combination of these types.

5. Click OK.

6. 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.

7. 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.
- The cloned machines are created in vCenter Server, even if the recovery site is vCD. If the recovery site is vCD, manually import the clones to 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 18: RESTORING AN OFFSITE BACKUP

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 219

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.

**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. This field only has a value if the Zerto Cloud Manager is connected to the site. For details, refer to Zerto Cloud Manager Administration Guide.

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 37.

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.

The list of virtual machines that can be restored 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.

You can override the default host and datastore by selecting the machines and clicking EDIT SELECTED to specify the host and storage to use to restore the virtual machines.
The **Configure VM Settings** dialog is displayed.

![Configure VM Settings Dialog](image)

**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](image)

9. Select datastores and click **EDIT SELECTED**.
   The **Edit Selected Volumes** dialog is displayed.

![Edit Selected Volumes Dialog](image)

**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.
223

Restoring an Offsite Backup

The NICs dialog is displayed:

14. Select the NIC and click **EDIT SELECTED**.
   The *Edit NIC* dialog is displayed.

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.
CHAPTER 19: ZERTO VIRTUAL REPLICATION REPORTS

Zerto Virtual Replication includes reporting for the following:

- “Outbound Protection Over Time”, below
- “Protection Over Time by Site”, on page 225
- “Recovery Reports”, on page 226
- “Resources Report”, on page 227
- “Usage”, on page 230
- “VPG Performance”, on page 230
- “Backup Report”, on page 231

Outbound Protection Over Time

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.

Protection Over Time by Site

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.

### 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 protected and recovery sites involved, when the recovery operation was started, the time it took to bring up the machines in the recovery site, the RTO, and whether the operation succeeded or not, and any notes added during a failover test.

You can filter the tests by the following:

**From** and **To** – 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 and 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.

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 (x86).

Resources Report

Information about the resources used by the virtual machines being protected 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 generated report 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, etc.

Interpreting the Resource Report

The report 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.

The 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: 1MB/minute*(30 minutes) + 0.5MB/minute*(30 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 = (45MB-0)/(60 minutes) = 0.75MB/minute = 13107Bps</td>
</tr>
</tbody>
</table>

Resource Report Output

The following describes every field in the report.

<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>PARAMETER</td>
<td>DESCRIPTION</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</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>Recovery Journal Used Storage (GB)</td>
<td>The amount of journal storage used by the virtual machine.</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 Profile</td>
<td>The target vCD storage profile 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 used between two consecutive samples, in bytes per second.</td>
</tr>
<tr>
<td>Timestamp</td>
<td>The date and time the resource information was collected. The value can be converted to an understandable date using code similar to the following: var date = new Date(jsonDate); or code similar to the Perl code example, jsonDateString($), described in Zerto Virtual Replication RESTful API Reference Guide.</td>
</tr>
<tr>
<td>VM Hardware Version</td>
<td>The VMware hardware version.</td>
</tr>
<tr>
<td>VM Id</td>
<td>The internal virtual machine identifier.</td>
</tr>
<tr>
<td>VM Name</td>
<td>The name of the virtual machine.</td>
</tr>
<tr>
<td>VPG Name</td>
<td>The name of the VPG.</td>
</tr>
</tbody>
</table>
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.

Usage

Information about usage can be displayed in the Usage report under the REPORTS tab. The information is organized by organization and within each organization by site and then 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. You can also see, under the month, the virtual machine count for each day in the month.

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, PDF, or ZIP file to generate the report.

The ZIP file option saves the report as zipped CSV and PDF files in a zipped file called **UsageReport.zip**.

VPG Performance

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 20: 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 234
- “Troubleshooting GUI Problems”, on page 234
- “Troubleshooting VRA Problems”, on page 234
- “Handling Lack of Storage Space for Recovered Virtual Machines”, on page 235
- “Zerto Virtual Replication Diagnostics Utility”, on page 235
- “Collecting Zerto Virtual Replication Logs”, on page 236

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 a virtual machine is added to a protected vApp and the added virtual machine has no matching datastore or not enough room on the recovery datastore or the VPG settings are not updated because of a site disconnection or vCenter Server error.
- 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 240.
- Check the connectivity between Zerto Virtual Replication components. See “Check Connectivity Between Zerto Virtual Replication Components”, on page 172.
- 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 173.
- 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 175.

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.1

---

1. 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

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 240.

You can also collect logs for the ZertoVssAgent. For details, see “Collecting Log Information for the ZertoVssAgent”, on page 241.

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.

   ![Zerto Diagnostics Collection](image)

   Check that you have specified everything you want to collect and if you want to make changes, click **Back** to change the selection.

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.

Collecting Log Information for the ZertoVssAgent

When ZertoVssAgent is installed, adding checkpoints to the journal can be synchronized with Microsoft Volume Shadow Copy Service (VSS) snapshots, as described in “Ensuring Transaction Consistency in Microsoft Windows Server Environments”, on page 146.

Logs generated by the ZertoVssAgent are saved separately and not collected using the Zerto Virtual Replication diagnostics tool, described in “Collecting Zerto Virtual Replication Logs”, on page 236. These logs are small and can be zipped and sent to Zerto support separately.

The logs are saved to a Zerto folder under the program data folder. For example, depending on the Windows operating system, the logs are in via C:\Documents and Settings\All Users\Application Data\Zerto or C:\ProgramData\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 100 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:

```
07f4c878,2010-12-01 19:54:41.4237,Debug,5,
TestConnectivity,TestConnectivity returning true,
07f4c878,2010-12-01 19:54:41.7362,Info,11,
PromotionMonitoringThreadFunc,Promoting protection groups: ,
07f4c878,2010-12-01 19:54:42.7987,Info,9,
Zerto.Infra.ZvmReaderWriterLock,LogLock,Synchronizer: Enter Writer,
07f4c878,2010-12-01 19:54:42.7987,Info,9,
Zerto.Zvm.ZvmServices.ReconnectingConnectorProxy,
GetConnector,"Connecting IP=106.16.223.86, PORT=4005, attempt (1/3)”,
07f4c878,2010-12-01 19:54:42.7987,Debug,9,
Zerto.Zvm.VraConnector.VraNetworkConnector,
Connect,try to connect 106.16.223.86:4005 ..., 
07f4c878,2010-12-01 19:54:43.0643,Debug,17,
Zerto.Zvm.ZvmServices.CrossSiteService,Ping,Ping,
07f4c878,2010-12-01 19:54:43.0643,Debug,17,
Zerto.Zvm.ZvmServices.PingService,Ping,Ping called,
07f4c878,2010-12-01 19:54:43.8612,Error,9,
Zerto.Zvm.VraConnector.VraNetworkConnector,
ClearAndThrow,connection is closed: No connection could be made because the target machine actively refused it 106.16.223.86:4005,
07f4c878,2010-12-01 19:54:43.8612,Warn,9,
Zerto.Zvm.ZvmServices.ReconnectingConnectorProxy,GetConnector,failed,
```
CHAPTER 21: ZERTO VIRTUAL REPLICAION AND VMWARE FEATURES

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 243
- “Protecting Virtual Machines in a vApp”, on page 244
- “Thin-Provisioning”, on page 244
- “VMware Clusters”, on page 244
- “Storage Profiles and Storage Clusters”, on page 245
- “Fault Tolerance”, on page 245
- “Host Affinity Rules and CPU Pinning”, on page 246
- “vMotion”, on page 246
- “Storage vMotion”, on page 246
- “VMware Host Maintenance Mode”, on page 246

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.

Stopping a vCenter Server

If the vCenter Server service is stopped, a Zerto Virtual Replication Delta Sync is performed on all protected virtual machines when the vCenter Server is restarted.
Protecting Virtual Machines in a vApp

A VMware vApp is a resource container for multiple virtual machines that work together as part of a multi-tier application. An example of a multi-tier application is a typical Web-based application where you might have three tiers: Web, application and database; which are often run on three separate servers. For example, you may have Microsoft IIS running on one server (tier 1), IBM WebSphere running on another server (tier 2) and IBM DB2 database running on a third server (tier 3). The three applications on each server all work together and are mostly dependent on each other for the application to function properly. If one part of the tier became unavailable, the application will typically quit working as it relies on all the tiers for the application to work.

vApps provide a method for setting power-on options, IP address allocation and resource allocation, and provide application-level customization for all the virtual machines in the vApp. When you configure a vApp in vSphere you specify properties for it, including CPU and memory resources, IP allocation, application information, and start order.

Because the VMware treats the vApp as a single logical entity comprising one or more virtual machines, Zerto Virtual Replication also enables protecting a vApp as a single entity in a VPG for any vApp defined under an ESXi host.

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).

When protecting virtual machines in a cluster, if you are protecting a vApp, you must install a VRA on every ESX/ESXi host in the cluster on both the protected and recovery sites and ensure that DRS is enabled for these clusters. For other virtual machines, it is recommended to install a VRA on every ESX/ESXi host in the cluster, or to disable DRS on the machine with the virtual machines to be protected.

Note: When protecting virtual machines in vCloud Director and recovering to a vCenter Server, the virtual machines are recovered as a vApp and thus DRS must be enabled in the recovery site. When protecting virtual machines in vCenter Server and recovering to vCloud Director, after a recovery with reverse protection, from the vCD to the vCenter, the virtual machines are not replicated back to the original site as a vApp.

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 190, 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 190.

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.

**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.

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 170.
CHAPTER 22: THE ZERTO VIRTUAL MANAGER USER INTERFACE

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 chapter:

- “Add Checkpoint Dialog”, below
- “Add Site Dialog”, on page 248
- “Add Static Route Dialog”, on page 249
- “Advanced Journal Settings Dialog”, on page 249
- “Advanced Journal Settings Dialog (vCD)”, on page 250
- “Advanced VM Recovery Settings Dialog”, on page 251
- “Advanced VM Replication Settings Dialog”, on page 251
- “Advanced VM Replication Settings Dialog (vCD)”, on page 252
- “Advanced VM Settings for AWS Dialog”, on page 252
- “ALERTS”, on page 253
- “Boot Order Dialog”, on page 253
- “Browse for VMDK File Dialog”, on page 254
- “Change Host Password VRA Dialog”, on page 254
- “Change VM Recovery VRA Dialog”, on page 254
- “Checkpoints Dialog”, on page 255
- “Compatibility Dialog”, on page 280
- “Configure and Install VRA Dialog”, on page 256
- “Configure Paired Site Routing Dialog”, on page 257
- “Configure Provider vDCs Dialog”, on page 258
- “Configure VM Settings Dialog”, on page 259
- “Configure Volume Dialog (vCD)”, on page 259
- “Edit NIC Dialog”, on page 260
- “Edit Repository Dialog”, on page 261
- “Edit Selected Volumes Dialog”, on page 262
- “Edit VM Dialog”, on page 262
- “Edit VM Dialog (vCD)”, on page 263
- “Edit vNIC Dialog”, on page 264
- “Edit vNIC Dialog (vCD)”, on page 265
- “Edit Volumes Dialog”, on page 266
- “Edit Volumes Dialog (vCD)”, on page 267
- “Edit VRA Dialog”, on page 268
- “Manage Static Routes Dialog”, on page 269
- “New Repository Dialog”, on page 270
- “NICs Dialog”, on page 271
- “Offsite Clone Dialog”, on page 271
- “Open Support Ticket Dialog”, on page 272
- “Restore from Zerto Backup”, on page 272
- “Restore Volumes Dialog”, on page 275
- “Site Settings Dialog”, on page 275
- “Stop Failover Test Dialog”, on page 282
- “TASKS”, on page 283
- “Volumes Dialog”, on page 283
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.

Remote Site ZVM IP Address - IP address or fully qualified DNS host name of the remote site Zerto Virtual Manager to pair to.

Port – The TCP port communication between the sites. Enter the port that was specified during installation. The default port during the installation is 9081.
Add Static Route Dialog

Add a static route for a specified group, defined in “Manage Static Routes Dialog”, on page 269, 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 269.

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 24 or the number of days from 2 to 14.

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 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.

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.

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.

**Advanced Journal Settings Dialog (vCD)**

[Image]

Used in vCD environments only.

Manage the journal used for recovery in a vCD environment.

**Journal History** – The time that all write commands are saved in the journal. The longer history is saved, the more space is required for each journal in the VPG. You can select the number of hours from 1 to 24 or the number of days from 2 to 14.

**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.
- **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.
- **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.
Advanced VM Recovery Settings Dialog

Displays the recovery settings for the virtual machines in the VPG. You can choose to edit the settings for one or more virtual machines by selecting the virtual machines and clicking *EDIT SELECTED* or by clicking the pencil icon for inline editing.

Advanced VM Replication Settings Dialog

Displays the replication settings for the virtual machines in the VPG. You can choose to edit the settings for one or more virtual machines by selecting the virtual machines and clicking *EDIT SELECTED* or by clicking the pencil icon for inline editing. For more details, see “Edit VM Dialog” on page 262.
Advanced VM Replication Settings Dialog (vCD)

Used in vCD environments only.

Displays the settings of the virtual machines in the VPG. You can choose to edit the settings for one or more virtual machines by selecting the virtual machines and clicking EDIT SELECTED or by clicking the pencil icon for inline editing. For more details, see “Edit VM Dialog” on page 262.

Advanced VM Settings for AWS Dialog

Displays the recovery settings for the virtual machines in the VPG. You can choose to edit the settings for a particular virtual machine by selecting the virtual machine 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 See 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 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 VMDK 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 recovery host for virtual machines to move all the VRA information and recovery volumes maintained by the VRA to another host, maintaining full protection while the original host is out of service.

**New Password** - The new password required by the VRA to access the host.

Change VM Recovery VRA Dialog

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

The point to recover to.

**Latest** - The recovery or clone is to the latest checkpoint. This ensures that the data is crash-consistent for the recovery or clone. 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 or clone, the later checkpoint is **not** used.

**Latest User Defined Checkpoint** - The recovery operation is to the latest checkpoint provided manually. Checkpoints added to the virtual machine journals in the VPG by the Zerto Virtual Manager ensure that the data is crash-consistent to this point. If a checkpoint is added between this point and starting the operation, this later checkpoint is not used.

**Latest VSS** - When VSS is used, recovery or clone is to the latest VSS snapshot, ensuring that the data is both crash-consistent and application consistent to this point. The frequency of VSS snapshots determines how much data can be recovered.

If you do not want to use the latest checkpoint, latest user defined checkpoint, or latest VSS checkpoint, choose Select from all available checkpoints. By default, this option displays all checkpoints in the system. You can choose to display only automatic, VSS, or user defined checkpoints, or any combination of these types.
Configure and Install VRA Dialog

- **Host** - The host under which the VRA is installed. The drop-down displays the hosts managed by the hypervisor management center which do not have a VRA installed, with the selected host displayed by default.

- **Host Root Password** - The password used to access the host for the root user. This field is required for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts. When the checkbox at the side is checked the password is displayed as asterisks. The password is used by the Zerto Virtual Manager when deploying and upgrading the VRA on this host. Also, root access is required in case the Zerto host component is down and needs an automatic restart. The Zerto Virtual Manager checks the password is valid once a day. If the password was changed, an alert is triggered, requesting the user enter the new password.

- **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>
<tr>
<td>3GB</td>
<td>2300MB</td>
</tr>
<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>
</tbody>
</table>
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

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.

**Enable Paired Site Routing** – When checked, enables paired site routing.

**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 the VRAs on the peer site.

The settings in the *Configure Paired Site Routing* dialog apply to all VRAs installed after the information is saved. 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.

<table>
<thead>
<tr>
<th>AMOUNT OF VRA RAM</th>
<th>VRA BUFFER POOL SIZE</th>
</tr>
</thead>
<tbody>
<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>
Configure Provider vDCs Dialog

Set up access to provider vDCs and their datastore configuration.

**Provider vDCs:** *Add* button – Add the provider vDCs that you want to enable to use Zerto Virtual Replication. Only these provider vDCs are visible to the user in Zerto Virtual Replication.

**Provider vDCs:** *Remove* button – Remove a selected provider vDC.

**Provider Datastore**

- **Unlisted datastores are not used by Zerto Virtual Replication** – Unlisted datastores cannot be used.
- **Unlisted datastores are used only for recovery volumes** – Unlisted datastores of all provider vDCs, even those provider vDCs that have not been added to the list of Provider vDCs can be used as recovery datastores.

**Provider datastore:** *Add* button – Add datastores.

**Provider datastore:** *Remove* button – Remove a selected datastore.

**Datastore** – The name of the added datastore.

**Recovery Volume** – Check if the datastore can be used as a recovery datastore.

**Journal** – Check if the datastore can be used for the journal. If no datastores are configured as journals, all datastores in the provider vDC can serve as journals. If at least one datastore, on any provider vDC, is configured as a journal but the recovery provider vDC does not see any journal datastore, all datastores eligible to be recovery datastores on that provider vDC, can also serve as journal datastores. If at least one datastore is configured as a journal and the recovery provider vDC sees at least one journal datastore, only datastores configured as journal, that are visible to that provider vDC can serve as journal datastores.

**Preseed** – Check 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.
**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** – Check this if you want the restored virtual machine to be powered on.

**Configure Volume Dialog (vCD)**

Used in vCD environments only.

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.

- **Swap Disk** – If the virtual machine to be replicated includes a swap disk as part of its configuration, you can specify a mirror disk for replication that is marked as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

- **Use vCD Managed Storage Profile** – The datastore is allocated based on the available free space. You can specify whether the recovery volume is thin provisioned or not. If the Org vDC only supports thin-provisioned volumes, you cannot change the setting. 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.

- **Preseed** – A virtual disk (the vmdk flat file and header file) in the recovery site that has been prepared with a copy of the protected data, 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 using a preseeded VMDK, you specify the exact location, the preseed folder configured for the customer and the disk name, of the preseeded disk. A provider datastore must have been specified for preseeded disks in the “Configure Provider vDCs Dialog”, on page 258 dialog. Zerto Virtual Replication 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](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](#).

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

**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.

**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.

**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*.

**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.

**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.
- **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.
- **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)

Used in vCD environments only.

Storage Profile – Storage profiles enable mapping virtual machines to storage levels according to predefined service levels, storage availability, performance requirements, or cost. You can define and label storage tiers and then specify the tier to use as a storage profile, for each virtual machine in the VPG. The default storage profile is the default for the Recovery Org vDC. 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.

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 storage.
  - 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 storage.
  - 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.
Edit VM Network 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.

**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 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 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 for the following operating systems: Windows 2003 and higher, Red Hat Enterprise Linux versions 5-6, SUSE Linux Enterprise versions 10-11 and CentOS versions 5-6.x.

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 failsovers, 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 in vCD environments only.

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. Specify the IP address if you choose **static IP pool**.
**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** – 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.

**Datasource** – A new volume is used for replicated data.

**Preseed** – 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 `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**.

**Raw disk (RDM)** – The VMware RDM (Raw Device Mapping) to use for the replication: By default, RDM is recovered to vmdk 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.

**Swap Disk** – If the virtual machine to be replicated includes a swap disk as part of its configuration, specify a mirror disk for replication that is marked as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.
Datastore - The datastore to use to create disks for the replicated data. Specify whether the target is thin provisioned. If the source disk is thin provisioned, the default for the recovery volume is that it is also thin provisioned.

The datastore 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.

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

Thin provisioning - If the recovery volumes are thin-provisioned or not.

**Edit Volumes Dialog (vCD)**

![Edit Volumes Dialog](image)

To edit recovery datastore information in a vCD environment.

**Volume Source** - The source on the recovery site for the replicated data.

- **vCD managed storage profile** - The datastore is allocated based on the available free space. You can specify whether the recovery volume is thin-provisioned or not. If the Org vDC only supports thin-provisioned volumes, you cannot change the setting.

- **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](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. blocks and not to VMDKs.

**Swap Disk** - If the virtual machine to be replicated includes a swap disk as part of its configuration, specify a mirror disk for replication that is marked as a swap disk. In this case, data is not replicated to the swap disk after initial synchronization.

Zerto Virtual Replication supports the SCSI protocol. Only disks that support this protocol can be specified.
Thin provisioning – If the recovery volumes are thin-provisioned or not.

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.

Host Root Password – The password required by the VRA to access the host. To display the password in plain text, click in the checkbox next to the field.

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.

Default Gateway – The default mask for the network.
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:

**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**

To create a new repository 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.

**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.

**Username** – 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** – Password to access the Network Share drive. This field is not displayed when the type is *Local*.

**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.
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 the NIC settings for a particular virtual machine by selecting the virtual machine and clicking **EDIT SELECTED**.

For more details, see “Restore Volumes Dialog”, on page 275.

Offsite Clone Dialog

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

To open a support ticket directly from the user interface.

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.

**Subject** - The subject of the support ticket.

**Type** - The type of ticket being opened.

**Description** - A description of the ticket in addition to the information supplied in the subject.

**SSP Email Address** - A valid email address registered with Zerto, with permission to open tickets.

After a support ticket is submitted, its progress is displayed. If the email address is not valid, the ticket is rejected. Once ticket submission starts, it cannot be canceled.

**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 of 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 37.

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.

For one or more virtual machines, you can override the default host and datastore by selecting the machines and clicking EDIT SELECTED to specify the host and datastore to use to restore the virtual machines.
Restore Volumes Dialog

The volumes for the selected virtual machine to be restored. You can choose to edit the settings for a particular volume by selecting the volume and clicking "EDIT SELECTED."

Site Settings Dialog

Contains site-wide settings:

- “Site Information Dialog”, below
- “Performance and Throttling Dialog”, on page 277
- “Policies Dialog”, on page 278
- “Email Settings Dialog”, on page 278
- “Reports Dialog”, on page 279
- “Compatibility Dialog”, on page 280
- “Cloud Settings Dialog”, on page 280
- “License Dialog”, on page 281
- “About Dialog”, on page 282
Site Information Dialog

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 Throttling - The maximum bandwidth that Zerto Virtual Replication uses from this site to 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 the priority set for the VPGs sending data over the WAN. The minimum supported bandwidth is 5 Mb/sec.

- **Unlimited** – The bandwidth is unlimited.
- **Slider** – 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 Bandwidth Throttling – To throttle the bandwidth during specific times. For example, during the daily peak transaction period you can change the specific throttling of the bandwidth, to override the general throttling.

- **Unlimited** – The bandwidth is always unlimited.
- **Slider** – 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.
- **From** – The start time for the throttling, using a 24-hour clock, the hour and the minute.
- **To** – The end time for the throttling, using a 24-hour clock, the hour and the minute.

The IO Throttling values should be changed only in coordination with Zerto support:

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.

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**

![Reports Dialog](image)

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

Lists supported host versions.

**ESX Version** – The ESX or ESXi version.

**Supported Update** – The supported updates for the ESX or ESXi version.

<table>
<thead>
<tr>
<th>ESX Version</th>
<th>Supported Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX / ESXi 4.0</td>
<td>4.0.1, 4.0.2, 4.0.3, 4.0.4</td>
</tr>
<tr>
<td>ESX / ESXi 4.1</td>
<td>4.1.1, 4.1.2, 4.1.3</td>
</tr>
<tr>
<td>ESX 5.0</td>
<td>5.5.0, 5.5.2, 5.5.3</td>
</tr>
<tr>
<td>ESX 5.1</td>
<td>5.1.1, 5.1.2, 5.1.3</td>
</tr>
<tr>
<td>ESX 5.5</td>
<td>5.5.5, 5.5.5, 5.5.6</td>
</tr>
<tr>
<td>ESX 6.0</td>
<td>6.0</td>
</tr>
</tbody>
</table>

### Cloud Settings Dialog

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 display the dialog in which you can define static route details.

Provider vDC Settings – Click Configure to display the dialog in which you can define provider vDC settings and their datastore configuration.

License Dialog

![License Dialog Image]

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 ID** – An identifier for the license.
- **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.
- **Maximum Sites** – The maximum number of sites allowed.

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.
About Dialog

The About dialog includes the Zerto Virtual Replication version number and whether to allow analytics to be sent to the Zerto Call Home server to help improve Zerto Virtual Replication.

**Send analytics to Zerto** – When selected, analytics are sent to Zerto that are used to improve Zerto Virtual Replication and to automatically update Zerto Virtual Replication when a new version of a hypervisor is released that is supported by Zerto.

Stop Failover Test Dialog

Enables stopping 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.
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.

**TASKS**

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**

When restoring an offsite backup to the recovery site, this dialog shows the datastores for a selected virtual machine in the VPG. You can choose to edit the datastore settings by selecting one or more volumes and clicking EDIT SELECTED. For more details, see “Edit VM Dialog”, on page 262.
## CHAPTER 23: GLOSSARY

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</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 Sync**                               | 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.  
  **Note:** 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. |
<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><strong>Business Continuity Plan</strong></th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business Impact Analysis (BIA)</strong></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><strong>Checkpoint</strong></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><strong>Cloud Service Provider (CSP)</strong></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 (DRAaaS) and In-Cloud DR (ICDR), too.</td>
</tr>
<tr>
<td><strong>Crisis Management Plan</strong></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><strong>Data Deduplication</strong></td>
<td>A specialized data compression technique for eliminating duplicate copies of repeating data.</td>
</tr>
<tr>
<td><strong>Delta Sync(^1)</strong></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 disk or after a VRA upgrade, or for reverse protection after a move or failover. (Preseeding is not possible in AWS.) During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible during a Delta Sync. \textbf{Note:} 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>Disaster</strong></td>
<td>The occurrence of one or more events which, either separately or cumulatively, activate disaster recovery.</td>
</tr>
<tr>
<td><strong>Disaster Recovery</strong></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><strong>Disaster Recovery Plan</strong></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><strong>Disaster Recovery As A Service (DRAaaS)</strong></td>
<td>A disaster recovery solution that incorporates a service provider to replace or augment the organization’s data protection implementation. In a DRAaaS 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><strong>DRS (vSphere)</strong></td>
<td>Enables balancing computing workloads with available resources in a VMware vCenter cluster.</td>
</tr>
<tr>
<td><strong>Emergency Management</strong></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><strong>Glossary</strong></td>
<td></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 data center to another CSP data center 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 Sync</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>
<tr>
<td><strong>Journal</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>LUN</strong></td>
<td>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 OSes 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.</td>
</tr>
<tr>
<td><strong>Level of Business Continuity</strong></td>
<td>The reduced level of service that has been agreed if there is an interruption to business operations.</td>
</tr>
<tr>
<td><strong>Managed Service Provider (MSP)</strong></td>
<td>See Cloud Service Provider (CSP).</td>
</tr>
<tr>
<td><strong>Maximum Tolerable Data Loss</strong></td>
<td>The maximum tolerable data loss an organization can endure without compromising its business objectives.</td>
</tr>
<tr>
<td><strong>Maximum Tolerable Outage (MTO)</strong></td>
<td>The maximum time after which an outage will compromise the ability of the organization to achieve its business objectives.</td>
</tr>
<tr>
<td><strong>Maximum Tolerable Period of Disruption</strong></td>
<td>The duration after which an organization’s viability will be irrevocably threatened if product and service delivery cannot be resumed.</td>
</tr>
<tr>
<td><strong>NAS</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Net Recovery Time</strong></td>
<td>The net time achieved in recovering one or more VPGs after a disaster.</td>
</tr>
<tr>
<td><strong>Offsite Backup</strong></td>
<td>See Extended Recovery.</td>
</tr>
<tr>
<td><strong>Operational Level Agreement (OLA)</strong></td>
<td>The agreement between the service management and the Service Provision Partners. It defines the responsibilities for support and delivery of the services provided.</td>
</tr>
<tr>
<td><strong>Pair</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Preseed</strong></td>
<td>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. Note that preseeding is not available in AWS.</td>
</tr>
<tr>
<td>Glossary Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Quiesce</td>
<td>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.</td>
</tr>
<tr>
<td>RDM (vSphere)</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery Point Objective (RPO)</td>
<td>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.</td>
</tr>
<tr>
<td>Recovery Time Achieved (RTA)</td>
<td>The actual times achieved during a DR test.</td>
</tr>
<tr>
<td>Recovery Time Objective (RTO)</td>
<td>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.</td>
</tr>
<tr>
<td>Replication, Asynchronous</td>
<td>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.</td>
</tr>
<tr>
<td>Replication to Self</td>
<td>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.</td>
</tr>
<tr>
<td>Resource</td>
<td>The elements (such as staff, site, data, IT systems) that are required to deliver an activity or service.</td>
</tr>
<tr>
<td>Resource Recovery Plan</td>
<td>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.</td>
</tr>
<tr>
<td>Rolling Back</td>
<td>Rolling back to an initial status, for example, after canceling a cloning operation on the VPG.</td>
</tr>
<tr>
<td>RPO</td>
<td>See Recovery Point Objective (RPO).</td>
</tr>
<tr>
<td>RTO</td>
<td>See Recovery Time Objective (RTO).</td>
</tr>
<tr>
<td>SAN</td>
<td>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.</td>
</tr>
<tr>
<td>SCSI</td>
<td>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.</td>
</tr>
<tr>
<td>SCVMM</td>
<td>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.</td>
</tr>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Secret Access Key (AWS)</td>
<td>A password. The Secret Access Key with the Access Key forms a secure information set that confirms the user’s identity.</td>
</tr>
<tr>
<td>Security Group</td>
<td>A virtual firewall that controls the traffic for one or more instances.</td>
</tr>
<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>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>
<tr>
<td>System Center Virtual Machine Manager</td>
<td>See SCVMM.</td>
</tr>
<tr>
<td>Virtual Machine (VM)</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Private Cloud (VPC)</td>
<td>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.</td>
</tr>
<tr>
<td>Virtual Protection Group</td>
<td>See VPG.</td>
</tr>
<tr>
<td>Virtual Replication Appliance</td>
<td>See VRA.</td>
</tr>
<tr>
<td>VMDK, Virtual Machine Disk</td>
<td>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.</td>
</tr>
</tbody>
</table>
### Volume Delta Sync
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 **Volume Delta Sync**.

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.

Preseeding is not available in AWS.

### Volume Full Sync
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 **Volume Full Sync**.

**Note:** 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.

### Volume Initial Sync
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 disk. (Preseeding is not available in AWS.)

During the synchronization, new checkpoints are not added to the journal. Also, recovery operations are not possible during a **Volume Initial Sync**.

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.

### VPG
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.

### VRA
A virtual machine that manages the replication of protected virtual machine writes across sites. A VRA must be installed on every ESX/ESXi which hosts virtual machines that require protecting in the protected site and on every ESX/ESXi that will host the replicated virtual machines in the recovery site.

### vSphere
VMware’s server virtualization platform for building a cloud infrastructure.

### Zerto Cloud Connector (ZCC)
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.

### Zerto Cloud Manager (ZCM)
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).

### Zerto User Interface
Recovery using Zerto Virtual Replication is managed via a user interface, Zerto DR Management UI, vSphere Client console or vSphere Web Client.
| **Zerto Self-service Portal (ZSSP)** | 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. |
| **Zerto Virtual Backup Appliance (VBA)** | A Zerto Virtual Replication service that manages the offsite backup. |
| **Zerto Virtual Manager (ZVM)** | 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. |
| **ZORG, Zerto Organization** | 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. |

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.
INDEX

A
advanced settings .................................................. 179, 180
  commit policy ......................................................... 181
  script execution timeout ........................................ 181
alerts .......................................................... 253
email settings ...................................................... 182
analytics, send to Zerto ........................................... 186, 282
application-consistent checkpoints ......................... 144
architecture, Zerto Virtual Replication ..................... 11
AWS
  choosing instance family ........................................ 67, 112
  choosing instance type ........................................... 67, 112
  choosing security group ........................................ 67, 112
  choosing subnet .................................................. 67, 112
  choosing VPC ...................................................... 67, 112
  editing VPG settings ............................................ 264
  limitations ......................................................... 63, 108, 139
  re-IP process ..................................................... 68, 112
  supported operating systems .................................. 63, 108, 139

B
backups, see offsite backup
bandwidth ........................................................ 39, 54, 64, 72, 80, 89, 100, 109, 179, 180, 277
  advanced settings ................................................ 179, 180
  calculating requirements ...................................... 27
  calculating size .................................................. 27
  in resources report ............................................. 228
  site settings ...................................................... 277
bandwidth, freeing up ........................................... 141
bitmap sync ...................................................... 14, 142, 158, 284
boot order .......................................................... 212
boot order, defining ............................................. 40, 55, 65, 253
branding, Recovery report .................................... 227

C
CALLHOME ......................................................... 186
certificate, adding ................................................. 17
change rate
  estimating ....................................................... 45, 59, 94, 105, 267
checkpoint ....................................................... 12, 144, 248, 255
  add ................................................................. 144, 145
  add via Add VSS Checkpoint dialog ......................... 147
  add via command line ......................................... 147
  application-consistent ......................................... 144
  choosing ......................................................... 192, 210, 217
NTP clock synchronization ................................... 185, 272
renaming after testing failover ................................ 195
scheduling ....................................................... 147
clone .............................................................. 219
definition ......................................................... 216
to VMware vSphere ............................................. 218
COM permissions
  setting for VSS .................................................. 149
commit policy
  advanced settings .............................................. 181
  failover and move .............................................. 181, 278
  site setting ...................................................... 278
compression for offsite backup, enable ...................... 270
configuration
  VPG .............................................................. 39, 108
connecting sites
  see pairing
  crash consistency, VSS ........................................ 146
create VPG ....................................................... 108

D
Dashboard .......................................................... 19
alerts .............................................................. 117, 120
tasks .............................................................. 117, 120
data compression ................................................ 43, 57, 74, 83, 91, 102
datatstore maintenance ......................................... 161
datatstore, choosing for recovery .......................... 42, 90
dbb.geometry.biosSectors .................................... 34
dbb.geometry.sectors .......................................... 34
default disk geometry ........................................... 34
default gateway, defining ..................................... 61, 107
delta sync .......................................................... 59, 76, 85, 104
diagnostics utility ................................................ 235
disaster recovery
  during a test ................................................... 215
  initiating ......................................................... 209
types .............................................................. 31
disk size
  estimating ....................................................... 45, 59, 94, 105, 267
disk space ......................................................... 235
promotion hangs ................................................ 235
disk, IDE .......................................................... 33
disk, SCSI .......................................................... 33

E
EBS disks .......................................................... 63, 108, 139
EC2 ................................................................. 63, 108, 139
edit VRA host passwords ...................................... 167
edit VRA settings ............................................... 167
email settings .................................................... 279
  backups ......................................................... 182
  for alerts ....................................................... 182
storage vMotion ..................................................50
scheduling checkpoints ...................................147
scratch volume ..................................................193, 205, 213
scripts ...............................................................212
adding to recovery process 47, 60, 68, 77, 86, 96, 105, 112
creating ............................................................152
defining for offsite backup 49, 62, 79, 88, 98, 107
execution timeout
    advanced settings ............................................181
running ............................................................151
ZertoForce environment variable .......................151
ZertoOperation environment variable ................151
ZertoVCenterIP environment variable ................151
ZertoVCenterPort environment variable ...............151
ZertoVPGName environment variable ..................151
SCSI disks .........................................................33
security certificate, adding ................................17
security group ..................................................63, 108, 139
    choosing .......................................................67, 112
self replication ..................................................50
enabling ..........................................................51
service profile ..................................................34
selecting ..........................................................42, 74, 82, 90
Set-Checkpoint ..................................................144
settings
    importing VPG ...............................................155
shadow VRA .....................................................162, 289
site details
    monitoring ....................................................116
site information ...............................................179
site settings .....................................................276
    commit policy ...............................................278
    enable replication to self ................................51
version ...........................................................186
sites tab ..........................................................125
sizing
    volumes .......................................................45, 59, 94, 105, 267
    WAN ...........................................................23
status
    VPG ............................................................156
stop
testing ..........................................................195
storage
    for replicated data ...........................................59, 104
    provisioned .................................................118, 125, 130, 131
    sizing ..........................................................59, 105
storage profile ..................................................229
    for vCD .........................................................76, 85
Storage vMotion ...............................................169, 246
stored offsite backups .......................................37
subnet ...........................................................63, 108, 139
assigning ........................................................67, 112
synchronization
    bitmap ..........................................................14, 142
    delta .............................................................59, 104
    initial ...........................................................36, 76, 85
synchronization triggers
    VPG ............................................................156, 160
tasks .............................................................123
testing
    monitoring .......................................................283
test
    failover ...........................................................190
    initiating failover .........................................215
    stopping .........................................................195
    VPG ............................................................190
test failover .....................................................190
    process ........................................................190
test scratch volume ..........................................193
thin provisioning ..............................................77, 85, 244
throttling
    advanced settings ............................................179, 180
    site settings ....................................................277
ticket, see support ticket
time-based bandwidth throttling
    advanced settings ............................................180
    site settings ....................................................277
topology
    for testing failover .........................................193
transaction consistency
    VSS .............................................................146
triggers
    synchronization ..............................................156
    VPG synchronization .......................................160
troubleshooting
    disk space .....................................................235
    VRA crashes during promotion ..........................235
    Zerto Virtual Manager service ..........................233
U
usage
    report ..........................................................230
Usage report ...................................................230
V
vApp .............................................................244
protecting .......................................................15, 53
VBA ..............................................................27
offsite backup ..................................................32
Virtual Backup Appliance, see VBA
virtual machine
    modify RDM ......................................................... 141
    modify replication settings ................................ 262
    modify volumes ................................................... 140
    monitoring ......................................................... 124
virtual protection group, see VPG
Virtual Replication Appliance, see VRA
VirtualEthernetCardLegacyNetworkBackingInfo NIC 34, 39, 53
VM DK size limitations ................................................ 22
vMotion ................................................................. 246
VMware host maintenance ............................................ 170
VMware vCenter Server
    cloning to it ...................................................... 218
vNIC configuration
    re-IP .................................................................. 48, 61, 97, 106
volume
    estimating size .................................................. 45, 59, 94, 105, 267
    preseed ............................................................... 45, 76, 85
Volume Shadow Copy Service
    logs ................................................................. 241
Volume Shadow Copy Service, see VSS
VPC ................................................................. 63, 108, 139
VPC network
    assigning ............................................................. 67, 112
VPG
    add a virtual machine ........................................ 139, 140
    add a virtual machine via vSphere Client Console .... 52
    add a virtual machine via Web Client Console ....... 52
    creating to recover to AWS .................................. 63–70
    creating to recover to Hyper-V .............................. 53–63
    creating to same site .............................................. 51
    creating to vCenter Server ................................... 39–50
    definition ............................................................ 31, 33, 34
    deleting ............................................................... 142, 143
    importing settings ................................................ 155
    modify ............................................................... 138
    modifying for AWS .............................................. 264
    monitoring .......................................................... 117, 119
    pause protection .................................................. 141
    priority ......................................................... 39, 54, 64, 72, 80, 89, 100, 109
    saving details to file ............................................. 119
    settings ............................................................ 122
    synchronization triggers ...................................... 156, 160
    synchronize ...................................................... 142
    testing .............................................................. 190
VPG Performance report .................................................. 230
VPG status ............................................................... 156
VPG waiting to be removed .......................................... 143, 156
VPG waiting to be removed force delete ......................... 143, 156
VPGs tab
    monitoring .......................................................... 117
VRA ................................................................. 12, 289
changing recovery host .............................................. 254
    crash during promotion ...................................... 235
    edit host password ............................................. 167
    editing settings .................................................. 167
    ghost ................................................................. 169
    monitoring ........................................................ 128
    shadow VRA ....................................................... 162
    uninstalling ....................................................... 169
    upgrading ......................................................... 165–166
vSphere Client console .................................................. 15, 52
vSphere Web Client ..................................................... 16, 52
working with Zerto Virtual Replication ............................. 16
VSS ................................................................. 144, 146
    crash consistency ................................................. 146
    logs ................................................................. 241
    setting COM permissions .................................... 149
    transaction consistency ....................................... 146
vStorage
    thin provisioning ............................................... 244
W
WAN
    bitmap sync ....................................................... 14
    compressing traffic ............................................ 43, 57, 74, 83, 91, 102
    WAN bandwidth, freeing up ................................ 141
    WAN sizing ....................................................... 23
    Windows service
        Zerto Virtual Manager ................................... 233
        ZertoVssprovider ........................................... 146
Z
Zerto User Interface ..................................................... 12
    customizing ..................................................... 20
    Zerto Virtual Manager ....................................... 11
    Windows service ................................................. 233
    Zerto Virtual Manager Web Client ......................... 15
    Zerto Virtual Replication
        architecture .................................................. 11
        benefits ....................................................... 12
        definition .................................................... 10
        how it works ................................................. 12
        logs ........................................................... 241
        monitoring ................................................... 115
        version ......................................................... 186
        ZertoForce script ............................................ 151
        ZertoOperation script ..................................... 151
        ZertoVCenterIP script ..................................... 151
        ZertoVCenterPort script .................................. 151
        ZertoVPGName script ..................................... 151
Zerto is committed to keeping enterprise and cloud IT running 24/7 by providing scalable business continuity software solutions. Through the Zerto Cloud Continuity Platform, organizations seamlessly move and protect virtualized workloads between public, private and hybrid clouds. The company’s flagship product, Zerto Virtual Replication, is the standard for protection of applications in cloud and virtualized datacenters.

<table>
<thead>
<tr>
<th>ZertoVssAgent</th>
<th>install ................................................................. 146</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZertoVssAgent.exe</td>
<td>.............................................................................. 147</td>
</tr>
<tr>
<td>ZertoVssAgentGUI.exe.conf</td>
<td>.................................................. 146, 151</td>
</tr>
<tr>
<td>ZertoVssprovider</td>
<td>Windows service ................................................................ 146</td>
</tr>
<tr>
<td>ZORG</td>
<td>preseeding .................................................................... 77, 85</td>
</tr>
<tr>
<td>ZVM, see Zerto Virtual Manager</td>
<td></td>
</tr>
</tbody>
</table>

www.zerto.com

For further assistance using Zerto Virtual Replication, contact Zerto support at support@zerto.com.