

Zerto

Zerto Cloud Manager Administration Guide

Cloud Environments

Version 7.0

Copyright © 2019, Zerto Ltd. All rights reserved.

Information in this document is confidential and subject to change without notice and does not represent a commitment on the part of Zerto Ltd. Zerto Ltd. does not assume responsibility for any printing errors that may appear in this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the prior written permission of Zerto Ltd.

All other marks and names mentioned herein may be trademarks of their respective companies.

The scripts are provided by example only and are not supported under any Zerto support program or service.

All examples and scripts are provided "as-is" without warranty of any kind. The author and Zerto further disclaim all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose.

In no event shall Zerto, its authors, or anyone else involved in the creation, production, or delivery of the scripts be liable for any damages whatsoever (including, without limitation, damages for loss of business profits, business interruption, loss of business information, or other pecuniary loss) arising out of the use of or inability to use the sample scripts or documentation, even if the author or Zerto has been advised of the possibility of such damages. The entire risk arising out of the use or performance of the sample scripts and documentation remains with you.

ZVR-ADC-7.0 Rev01 U2 July2019

CHAPTER 1: INTRODUCTION TO THE ZERTO SOLUTION	5
What is the Zerto Solution?	5
The Zerto Solution Components	6
Zerto’s Billing	9
How a Cloud Service Provider Manages Disaster Recovery	10
Providing a Self-service Portal for Cloud Service Provider Customers	10
Benefits to Cloud Service Providers	11
Zerto DRaaS Architecture	12
Design Considerations for DRaaS	13
vCD Used by the Cloud Service Provider	14
Zerto ICDR Architecture	15
CHAPTER 2: CONFIGURING A ZERTO CLOUD MANAGER	16
Logging On to Zerto Cloud Manager	16
Defining and Configuring the Zerto Cloud Sites	18
Registering Zerto Sites	20
Adding a Security Certificate for the Zerto User Interface	22
Installing Virtual Replication Appliances on Hosts in Cloud Sites	23
(Optional) Configure vCloud Director	26
Setting Up Zerto Organizations, ZORGs	30
Defining DRaaS Components	36
Providing a Self-service Portal for Cloud Service Provider Customers	41
Creating Service Profiles	42
Defining Role-based Access Control	44
Enabling Role-based Permissions	45
Managing Roles	46
Managing Privileges, Roles, and Authorizable Entities	50
CHAPTER 3: SETTING UP DRAAS	57
CHAPTER 4: SETTING UP THE ZERTO SELF-SERVICE PORTAL	59
Setting Up Access to the Zerto Self-service Portal	60
Access the Zerto Self-service Portal as a Standalone Portal	60
Access the Zerto Self-service Portal by integrating it in a Cloud Service Provider Portal	61
Security	62
Branding the Zerto Self-service Portal	66
CHAPTER 5: ONGOING MANAGEMENT	67
Setting VMware Permissions	67
Managing All Sites	67
Zerto Cloud Manager VPGs	68
Zerto Cloud Manager Alerts	69
Managing a Specific Site	70
Managing a ZORG	70
ZORG VPGs	71
ZORG Alerts	72
Editing Zerto Cloud Manager Definitions	73
Resolving Zerto Cloud Connector Issues	74
Handling a Ghost Zerto Cloud Connector	74

vMotioning a Zerto Cloud Connector	75
Handling an Orphaned Zerto Cloud Connector	76
CHAPTER 6: THE ZERTO CLOUD MANAGER USER INTERFACE	77
Add Cloud Site Dialog	78
Add New Role Dialog	78
Add Permission Dialog	79
Add Service Profile Dialog	79
Add Static Route Dialog	80
Add ZORG Dialog	81
Alerts Tab	81
Cloud Settings Dialog	82
Configure & Install VRA Dialog	83
Configure Paired Site Routing Dialog	84
Configure Provider vDCs Dialog	85
Configure vCD Dialog	86
Customer Sites Tab	87
Edit Permission Dialog	90
Edit Resource Dialog	90
Edit Role Dialog	91
Edit VRA Dialog	91
Install Cloud Connector Dialog	92
Manage Static Routes Dialog	93
Manage ZORG Tab	94
Organizations Tab	95
Outbound Protection Over Time Report	96
Permissions Tab	97
Protection Over Time by ZORG Report	98
Recovery Reports	99
Redeploy Cloud Connector Dialog	100
Resource Report	100
Roles Dialog	104
Select User/Group Dialog	105
Service Profiles Tab	105
Sites Tab	107
Usage Report	108
vCD Cloud Resources Tab	108
vCenter Cloud Resources Tab	109
VMs Tab in the Zerto Virtual Manager	109
VPG Performance Report	110
VPGs Tab in the Zerto Virtual Manager	111
VPGs Tab in the Zerto Cloud Manager	113
VRAs Tab in the Zerto Virtual Manager	114

Disaster recovery is the process of preparing for recovery or the continuation of IT processing tasks that support critical business processes in the event of a threat to the IT infrastructure. This section describes Zerto general concepts that enable replication and recovery in a virtual environment for cloud service providers.

The following topics are described in this section:

- [What is the Zerto Solution?](#)
- [The Zerto Solution Components](#)
- [Zerto's Billing](#)
- [How a Cloud Service Provider Manages Disaster Recovery](#)
- [Providing a Self-service Portal for Cloud Service Provider Customers](#)
- [Benefits to Cloud Service Providers](#)
- [Zerto DRaaS Architecture](#)
- [Zerto ICDR Architecture'](#)

What is the Zerto Solution?

IT Resilience Platform™

Zerto's IT Resilience Platform™ converges disaster recovery, backup, and workload mobility whether on-premises or to, from and between hybrid and multi-cloud platforms. The platform is built on a foundation of continuous data protection (CDP) with built-in orchestration and automation providing IT leaders with simplicity, enterprise scale and agile data protection to save time, resources and costs. Analytics, with intelligent dashboards and live reports, provides complete visibility across multi-site and multi-cloud environments, giving organizations confidence that business service levels and compliance needs are met.

Disaster Recovery

Zerto is built from the ground up to be the simplest, most powerful disaster recovery solution for virtualized infrastructures. By including all the replication, recovery orchestration and automation in one simple software platform, users can recover one, all or a subset of virtualized applications, from anywhere to anywhere, maximizing the benefits of virtualization and cloud.

Through native integration into all supported platforms, Zerto not only allows replication and recovery between any storage, but it also protects across and between multiple hypervisors and public cloud platforms. This market-leading technology delivers a best of breed Business Continuity/Disaster Recovery (BC/DR) solution irrespective of underlying hypervisor, public cloud or storage.

Zerto supports replication between VMware vSphere, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services (AWS), and IBM Cloud. Zerto is the underpinning technology of hundreds of Cloud Service Providers (CSPs) globally who are leading the way in delivering Disaster Recovery as a Service (DRaaS) capabilities.

Backup

Elastic Journal

The Zerto Elastic Journal is a new concept in data protection bringing together both short-term retention and long-term retention capabilities. Using unified data protection workflows, powered by intelligent index and search, it enables quick recovery of data—regardless of whether it's from a few seconds ago or a few years ago. Data gets copied from the short-term retention storage into the long-term retention repositories. As the short-term retention is already stored on the target side, moving data to long-term retention has no impact on production, so copies can be taken as often as needed, eliminating the concept of "backup windows".

Workload Mobility

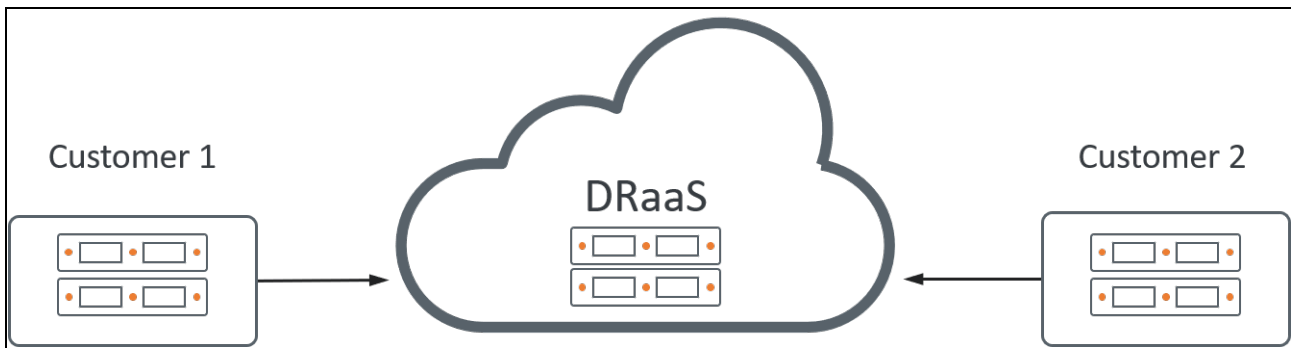
Workload mobility is the ability to move workloads to, from and between multiple platforms, on-premises or cloud, with minimal business impact and no traditional infrastructure constraints. With the recent rise of cloud computing, there is now a plethora of cloud platforms to choose from, with large players such as Microsoft Azure, AWS and IBM Cloud as well as plenty

of Cloud Service Providers (CSPs). Each of these platforms have their own attributes which make them suited to certain workloads, whether through compliance, pricing or otherwise. Despite this, the cloud is not always the right option for all workloads, and because of this, the traditional on-premises deployments with VMware vSphere or Microsoft Hyper-V are still prevalent. Ultimately, having all of these options has led to increasing adoption of a multi-cloud and/or hybrid cloud strategy. Organizations are challenged to ensure that workloads, whether in the cloud or on-premises, are not locked into any one platform or vendor, and can be moved around based on where they fit best today, rather than yesterday. This is where workload mobility comes in, removing the traditional lock-in to these platforms and allowing workloads to be moved across platforms seamlessly, on-premises or in the cloud, including the ability to validate mobility prior to the live event without production impact.

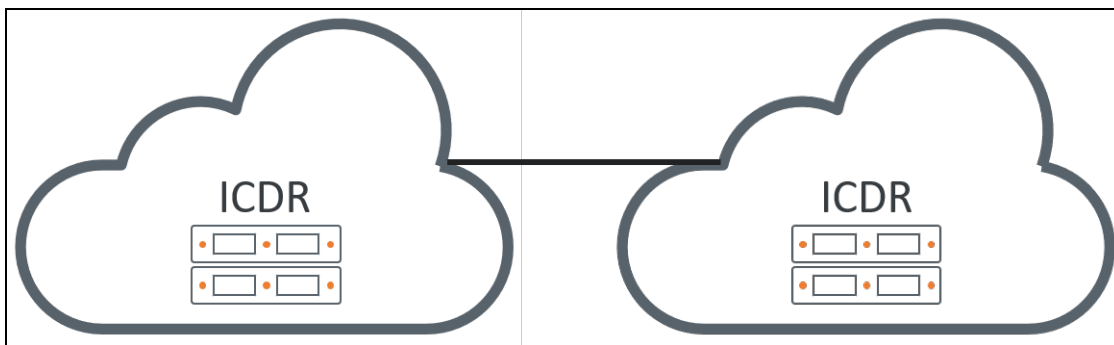
Zerto supports any-to-any mobility between VMware vSphere, Microsoft Hyper-V, AWS, IBM Cloud, Microsoft Azure and any of our hundreds of Zerto-powered Cloud Service Providers (CSPs). For a full list of supported platforms and their versions please see our [Interoperability Matrix](#).

As well as supporting disaster recovery for enterprises that want to protect their mission-critical applications to a recovery site, as described in the *Zerto Virtual Manager Administration Guides*, using Zerto enables cloud service providers to offer the following services:

- **Disaster Recovery as a Service (DRaaS):** In a DRaaS scenario, the customer may manage and have complete control over the production data or the Cloud Service Provider (CSP) may provide a partial or complete managed service. In either case, the CSP must ensure the availability of the data and adapt as customer infrastructures change.



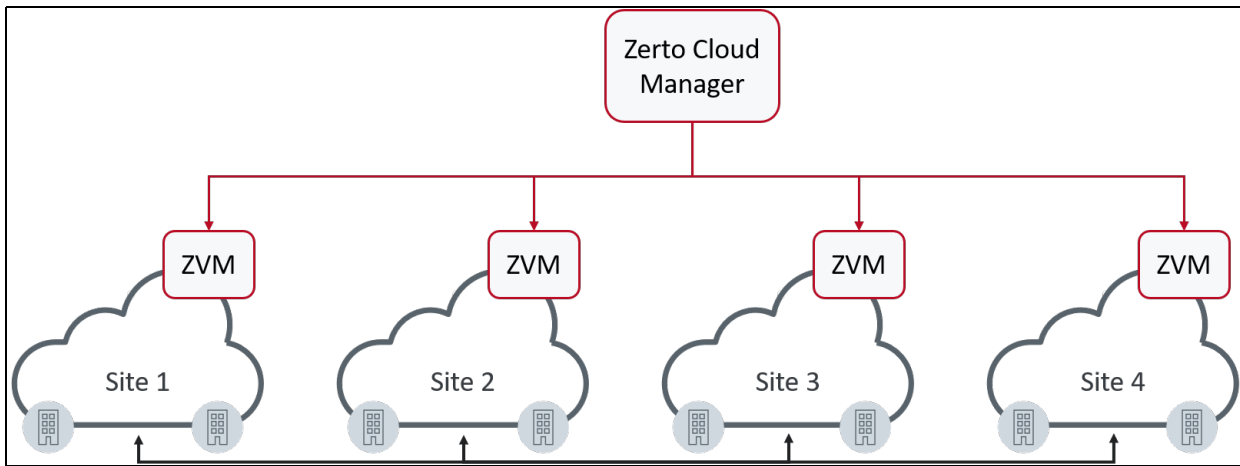
- **In-Cloud DR (ICDR):** When customers leverage an ICDR service, the CSP hosts the production and DR sites. The virtual machines (VMs) are typically replicated from one CSP datacenter to another CSP datacenter as a managed service or as managed co-located datacenters. The customers have the ability to interact with their applications as if they were locally hosted.



The Zerto Solution Components

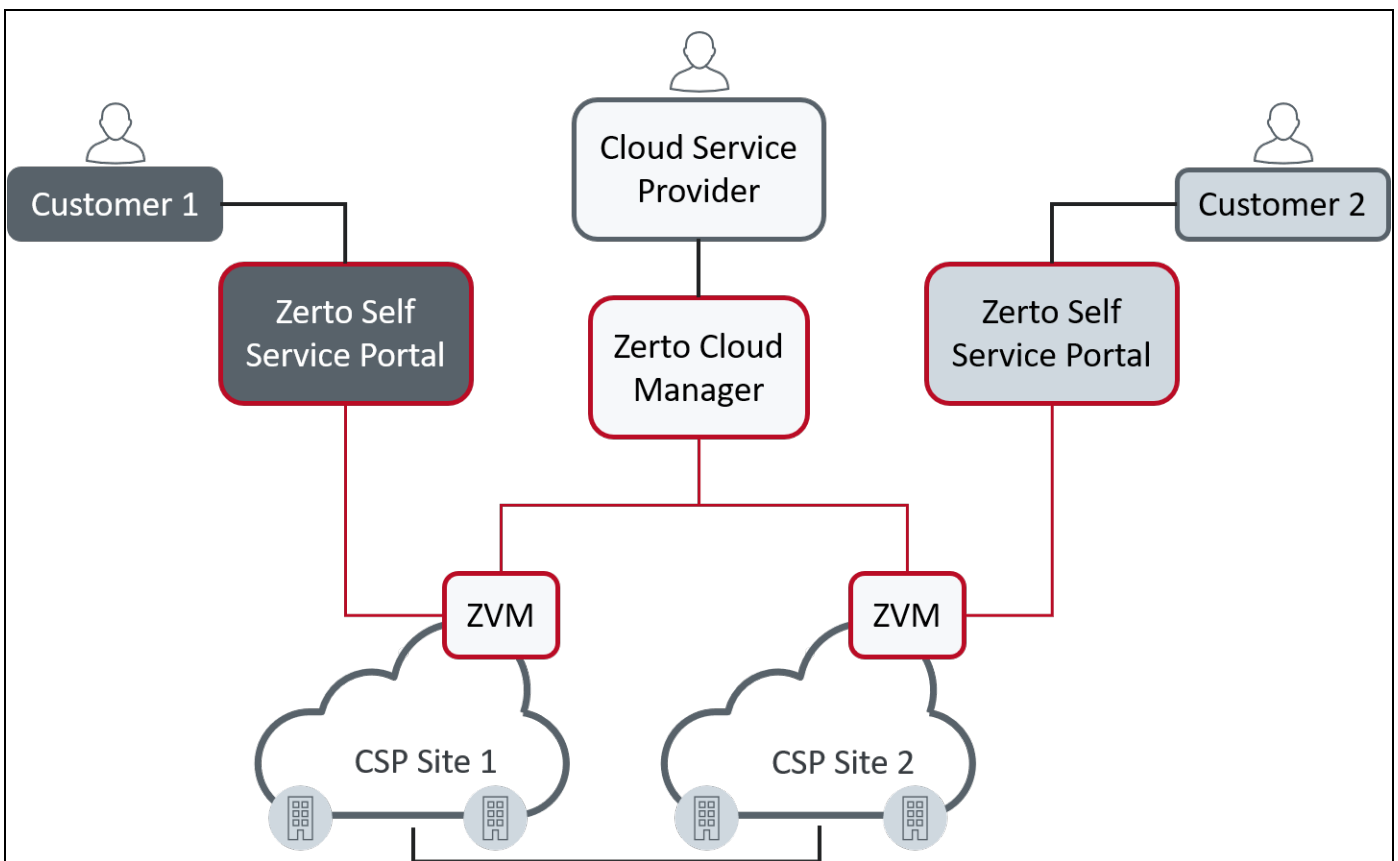
The Zerto solution comprises the following components:

- **Zerto Cloud Manager (ZCM):** A Windows service that enables managing all VMware sites offering disaster recovery either as a service (DRaaS) or completely within the cloud environment, protecting one site and recovering to a second site (ICDR).

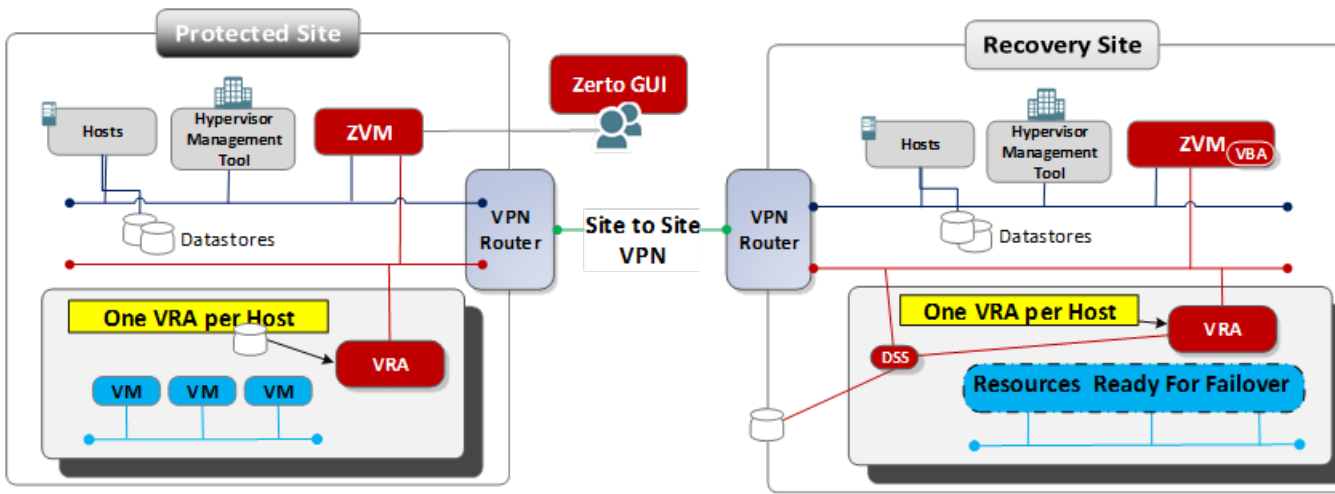


As can be seen in the above diagram, each site has a Zerto Virtual Manager installed, and one Zerto Cloud Manager manages all the sites.

- **Zerto Virtual Manager (ZVM):** A Windows service that manages the replication between the protection and recovery sites. A ZVM that is directly managed by a ZCM must be a VMware vCenter Server or vCloud Director site. DRaaS sites managed by the ZVM can be either VMware vCenter Server or Microsoft SCVMM sites.
- **Virtual Replication Appliance (VRA):** A virtual machine installed on each host that hosts virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.
- **Virtual Backup Appliance (VBA):** A Windows service that manages File Level Recovery operations within Zerto.
- **Zerto User Interface:** Recovery using Zerto is managed in a browser.
- **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.



The following diagram shows the basic architecture for sites with Zerto deployed. These sites are then managed by the Zerto Cloud Manager.



Zerto's Billing

A CSP's billing model is based on their ability to connect their Zerto Virtual Managers to Zerto's billing server.

In order to participate in Zerto's Automated Billing model, the CSP must have a steady connection to Zerto's billing server.

If the CSP is unable to connect to Zerto's billing server, they are manually billed based on usage data.

Zerto's Automated Billing

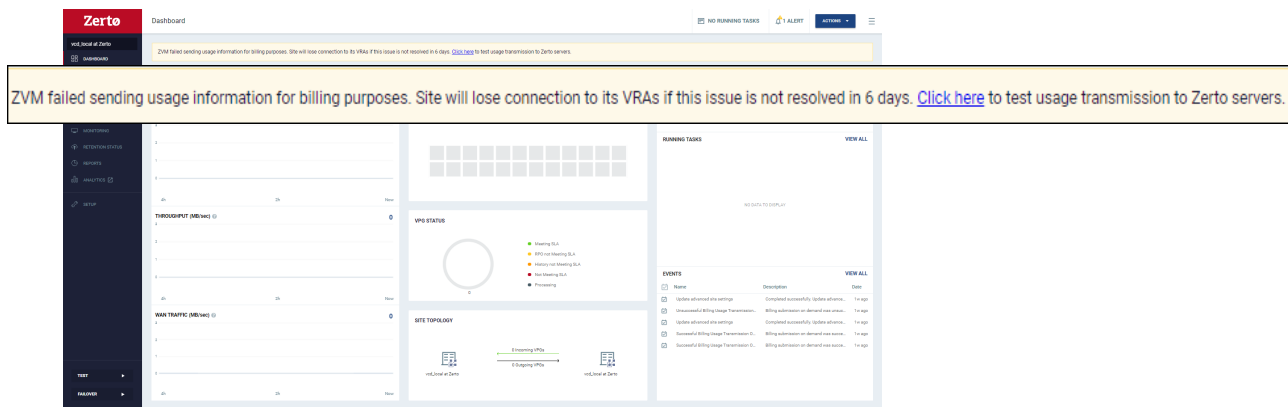
When the CSP is part of Zerto's Automated Billing program, unlike previous Zerto versions, they can no longer rely on ZCM to report usage data.

Instead of which, all their Zerto Virtual Managers must maintain a steady connection to Zerto's billing server. This can be done either:

- By connecting directly to Zerto's Billing server, which is **autologs.zerto.com** over port **443**.
- Or, by directing the connection via proxy server. For further guidelines on this, see [KB](#).

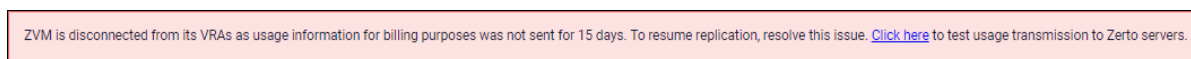
If, for any reason this usage information is not sent, an urgent and persistent alert appears in Zerto Virtual Manager in the form of a banner. The alert also appear in Monitoring > Alerts. The alert informs the CSP that Zerto Virtual Manager did not send site usage information for billing purposes to Zerto servers; that if the issue is not resolved within the specified days, Zerto Virtual Manager will stop communicating with its VRAs.

When the alert appears in the banner, the CSP is strongly advised to click the link to test connection to Zerto servers.



The CSP will have 15 days from the first appearance of the alert to resolve the issue, before the next alert appears. The next alert is the disconnection alert.

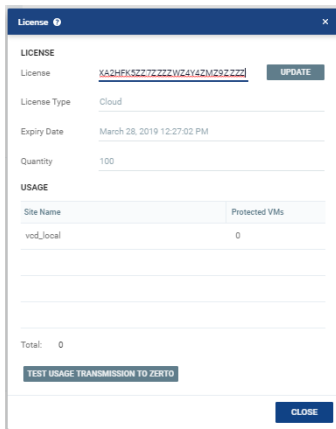
When the disconnection alert appears, ZVM has already stopped communicating with its VRAs. The disconnection alert informs the CSP that ZVM did not send site usage information for billing purposes to Zerto servers, and that ZVM will not communicate with its VRAs until this issue is resolved.



Manually Test Connection and Send Usage Data to Zerto Servers

To manually test connection to Zerto servers, and also send usage data for billing purposes:

1. In the top right of the ZVM window, click the options icon .
2. Select **License**, then click **TEST USAGE TRANSMISSION TO ZERTO**.



How a Cloud Service Provider Manages Disaster Recovery

Whether the cloud service provider (CSP) offers Disaster Recovery as a Service (DRaaS) or In-Cloud DR (ICDR), the CSP uses Zerto Cloud Manager to manage all cloud sites offering disaster recovery.

The Zerto Cloud Manager works with the Zerto Virtual Managers installed as part of the Zerto installation. Before using the Zerto Cloud Manager, make sure that all cloud sites that will be used to either protect virtual machines or recover virtual machines have Zerto installed.

For both DRaaS and ICDR, initial configuration of Zerto Cloud Manager involves the following tasks at the cloud sites:

1. Log on to Zerto Cloud Manager and define the cloud sites providing disaster recovery capabilities.
2. For each Zerto installation defined as a cloud site, register the use of Zerto.
3. Install Zerto Virtual Replication Appliances.
4. Set up vCloud Director, if it is being used.
5. Set up customers as ZORGs, Zerto organizations, including what each ZORG has permission to do. The cloud service provider can restrict the operations available to the organization. For example, the CSP can permit an organization to test the protection of its virtual machines.
6. When the cloud service provider offers DRaaS, it also installs a Zerto Cloud Connector (ZCC) per customer to route traffic between the customer organization network and the cloud replication network, in a secure manner without requiring the cloud vendor to go through complex network and routing setups, ensuring complete separation between the organization networks and the cloud service provider network.
7. Set up service profiles, which are templates for protection.
8. When the cloud service provider offers DRaaS, it instructs DRaaS customer organizations to set up their sites. The customer set-up involves installing Zerto, Virtual Replication Appliances, and pairing to the cloud service provider.
9. Provide a Self-service Portal for customers to manage their disaster recovery.

Providing a Self-service Portal for Cloud Service Provider Customers

Cloud Service Provider (CSP) customers that need to perform disaster recovery operations such as failing over, without the need to request this from their CSP, can use the Zerto Self-service Portal. The Zerto Self-service Portal is an out-of-the-box disaster recovery portal solution with a fully functioning browser-based service portal that enables cloud service providers to quickly introduce disaster recovery using Zerto. For example, when the CSP offers DRaaS, CSP customers can use the Zerto Self-service Portal to access the CSP recovery site to perform failover directly, without needing to request this from the CSP.

In Zerto Cloud Manager, the CSP can define the operations available to each customer in the Zerto Self-service Portal. For details, see [“Setting Up Access to the Zerto Self-service Portal”](#), on page 56.

Benefits to Cloud Service Providers

The cloud service provider must be able to support multiple organizations whether the organization site is a VMware vCenter or vCloud Director site, or a Microsoft Hyper-V site. The Zerto Cloud Manager enables consistent management regardless of the type of site, so disaster recovery planning and management is simplified using infrastructure that supports these environments.

Zerto makes disaster recovery a valuable addition to the services a cloud service provider can offer, either DRaaS or ICDR. Zerto Cloud Manager enables the cloud service provider to manage the service for all its customers. The following are just some of the main benefits.

Hardware Agnostic

Because Zerto software manages recovery of virtual machines and virtual disks in the hypervisor layer, 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. As long as Zerto supports the storage device, for example, SCSI with vSphere virtual machines, any storage device can be used. With Zerto the logical storage is separated from the physical storage so that the vendor and type of actual storage hardware do not need to be considered.

Fully Scalable

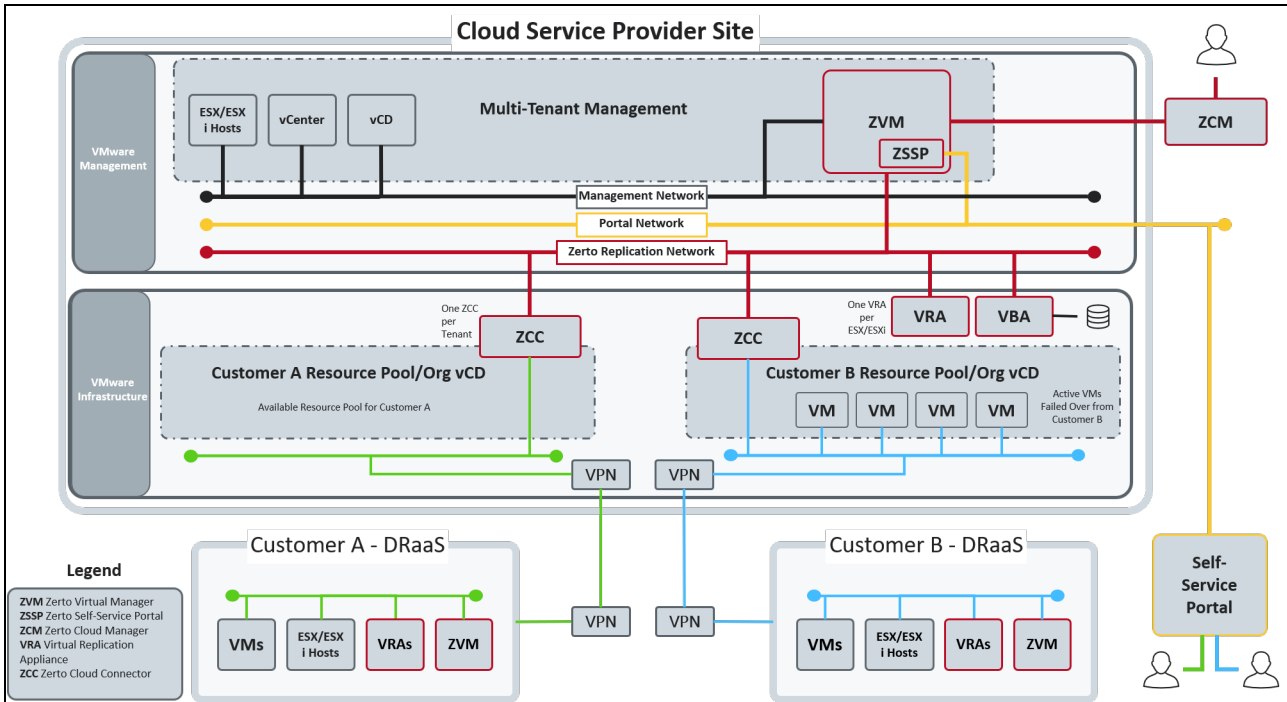
Zerto sits in the hypervisor level and enables defining software-only Virtual Replication Appliances (VRAs) on each host to manage the replication of virtual machines on that host. Increasing the number of hosts is handled by defining a new VRA on each new host. There is no need to install additional software to handle additional hosts or virtual machines and no need to consider additional hardware acquisitions.

Multi-tenant Support

Cloud service providers have to build a multi-tenant environment for their many customer environments. Each of these customer environments must be completely separate and secure. Zerto is designed to be multi-tenant.

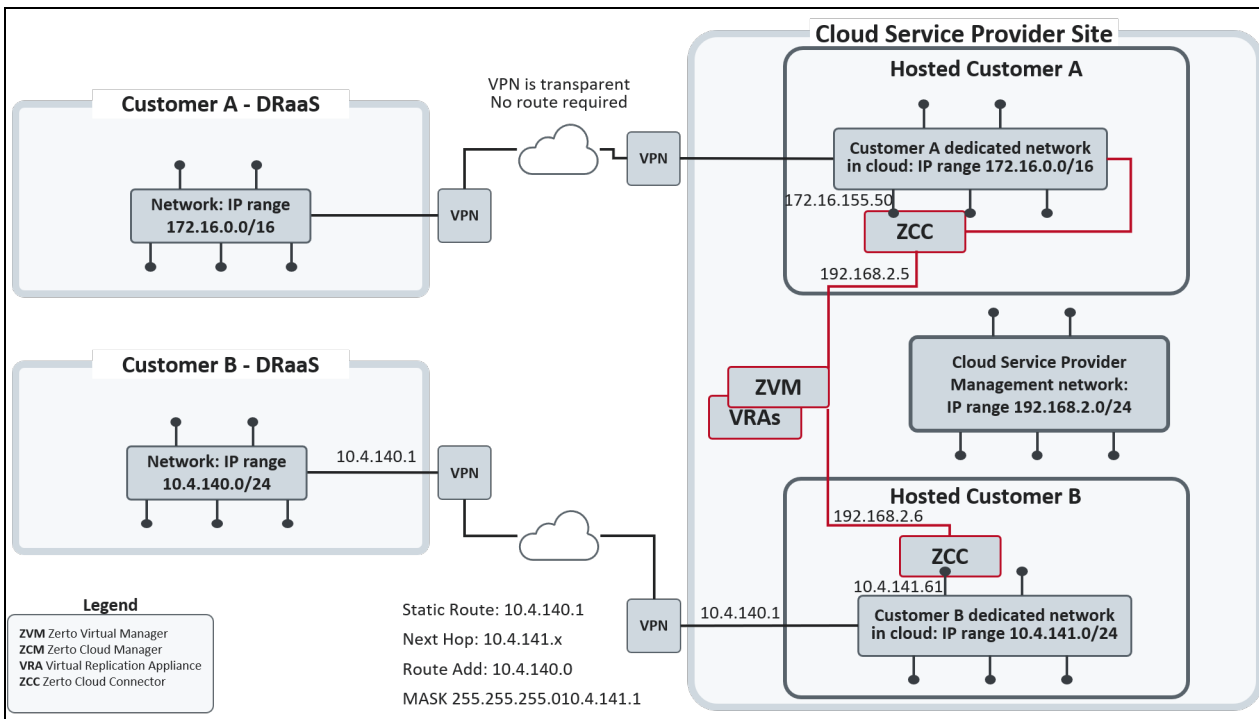
Zerto DRaaS Architecture

The following diagram shows the basic DRaaS architecture. DRaaS organizations can manage their disaster recovery via the Zerto User Interface. The diagram shows two users, both using VMware environments. These organizations can use either VMware vSphere or Microsoft SCVMM to connect to the Cloud Service Provider.



Design Considerations for DRaaS

The organization connects to the cloud service provider via VPN, to a network that has a connection to the internet or to a wider network that enables a connection between the cloud site and the customer site. All the traffic to and from the customer is routed through a Zerto Cloud Connector (ZCC).



A Zerto Cloud Connector is a virtual machine installed on the cloud side, one for each customer replication network. The Zerto Cloud Connector 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 cloud connector 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 Zerto Cloud Connector, where the incoming traffic from the customer network is automatically configured to IP addresses in the cloud service provider network.

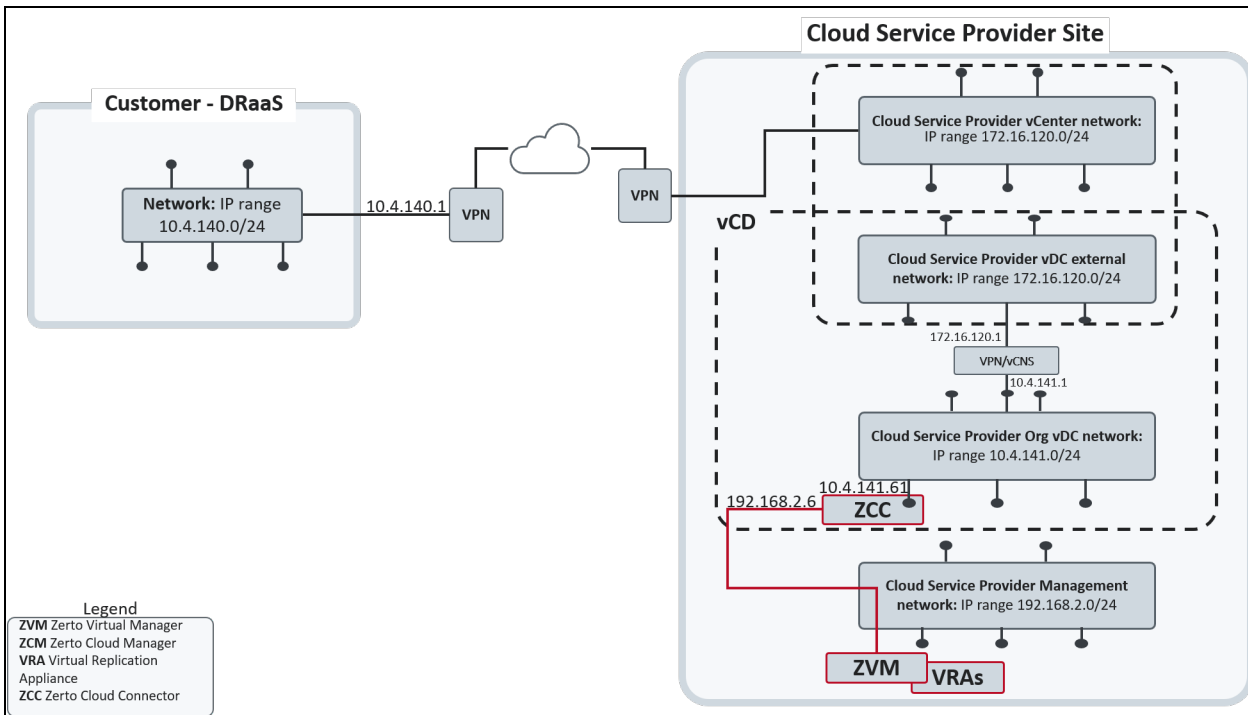
Using Zerto Cloud Connectors ensure the following:

- None of the customers have direct access to the cloud service provider network and cannot see any part of the cloud service provider network that the cloud service provider does not allow them to see.
- Each customer has no access to the network of another organization.

If the cloud service provider wants to add more security, it 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.

vCD Used by the Cloud Service Provider

The following diagram shows an example of an organization protecting virtual machines to the cloud service provider vCD:



Note: vCloud Networking and Security (vCNS) can be used instead of VPN. In this case the VPN component between the External Network and Org vCD Network is replaced by vCNS. Even though vCNS supports NAT, Zerto does not support NAT.

You can set up the cloud site infrastructure such that the cloud and organization networks are on different subnets or on the same subnet.

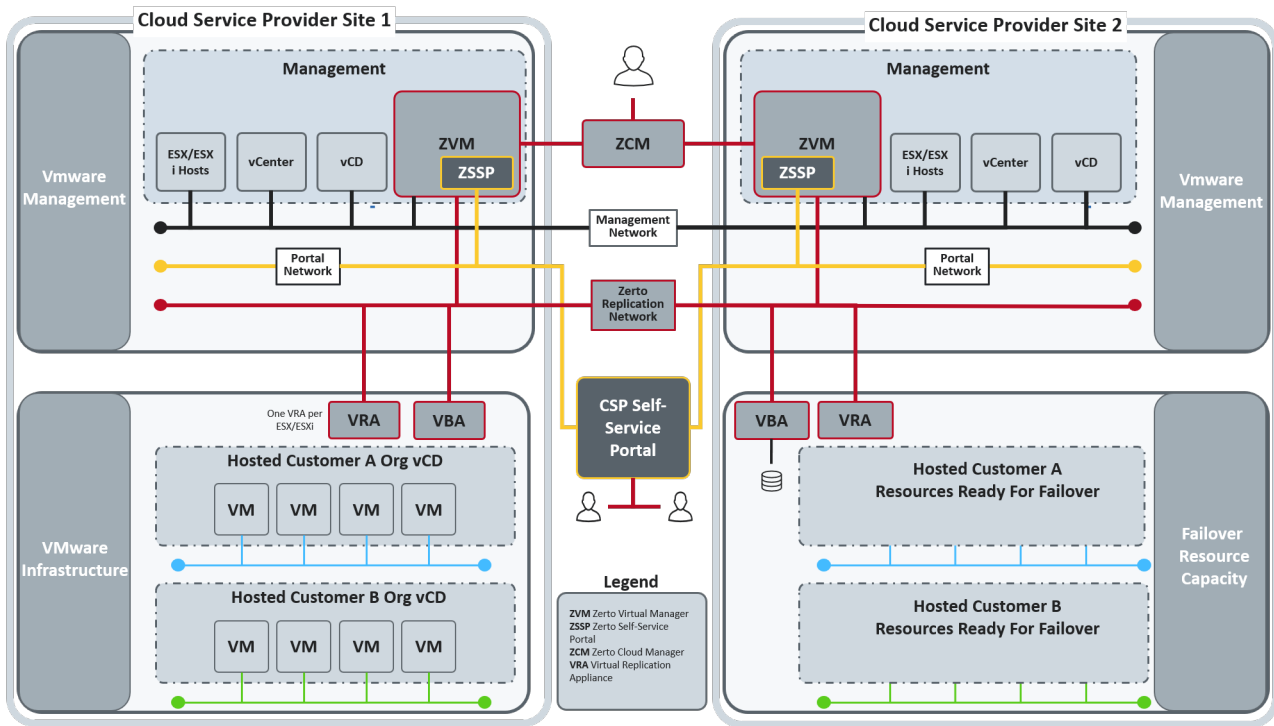
- **Cloud and Organization Networks on Different Subnets:** If the cloud service provider dedicated network IP addresses and the organization dedicated Org vDC Network IP addresses are on different IP subnets, make two IP addresses available for the Zero Cloud Connector component (IPs 10.4.141.32 and 192.168.2.42 in the above diagram), one IP address available for each network.
- **Cloud and Organization Networks on the Same Subnet:** If the cloud service provider dedicated network IP addresses and the organization dedicated Org vDC Network IP addresses are on the same IP subnet, there is no need for the Zerto Cloud Connector.

When creating the organization dedicated Org vDC Network, make sure it is connected to the External Network either directly or via a routed connection. The organization dedicated network must enable a connection between the Org vDC Network and the External Network, so that VPN can be used to connect to the outside world. Connect the VPN to the organization dedicated Org vDC network in order to create a connection between the organization site and its own internal Organization vDC in the cloud vCD.

Make sure that the VC Network and the External Network inside vCD on the cloud site have a connection to the internet or to a wider network that will enable a connection between the cloud site and the organization sites.

Zerto ICDR Architecture

The following diagram shows the basic ICDR architecture. ICDR organizations can manage their disaster recovery via the Zerto Self-service Portal.



The connection between the two cloud sites does not require a Zerto Cloud Connector since the traffic between the two cloud service provider Org vDC Networks belong to the same cloud service provider so separation of networks is not required.

The Zerto Cloud Manager is used by Cloud Service Providers and large enterprises to manage multiple Zerto sites from a single management tool.

You set up the Zerto Virtual Manager and VRAs via the Zerto Cloud Manager, via the following steps:

1. Log on to Zerto Cloud Manager and define the VMware cloud sites providing disaster recovery capabilities.
2. For each Zerto installation defined as a cloud site, register the use of Zerto.
3. Install Zerto Virtual Replication Appliances.
4. Set up vCloud Director, if it is being used and was not set up during the Zerto installation and also configure Provider vDC settings.
5. Set up customers as ZORGs, Zerto organizations, including what each ZORG has permission to do. The cloud service provider can restrict the operations available to the organization, such as whether the organization can test the recovery of protected virtual machines.
6. When the cloud service provider offers DRaaS, it also installs a Zerto Cloud Connector (ZCC) per customer to route traffic between the customer organization network and the cloud replication vCenter Server network, in a secure manner without requiring the cloud service provider to go through complex network and routing setups, ensuring complete separation between the organization networks and the cloud service provider network.
7. Set up service profiles, which are templates for protection.
8. When the cloud service provider offers DRaaS, it instructs DRaaS customer organizations to set up their sites. The customer set-up involves installing Zerto, Virtual Replication Appliances, and pairing to the cloud service provider.
9. Provide a Self-service Portal for customers to manage their disaster recovery.
10. Manage roles and permissions for Zerto users.

These steps are described in this section in the following topics:

- [Logging On to Zerto Cloud Manager](#)
- [Defining and Configuring the Zerto Cloud Sites](#)
- [Setting Up Zerto Organizations, ZORGs](#)
- [Defining DRaaS Components](#)
- [Creating Service Profiles](#)
- [Defining Role-based Access Control](#)

Setting up the Zerto Self-service Portal as a standalone portal is described in [Configuring a Zerto Cloud Manager](#). The Zerto Self-service Portal can also be incorporated by the CSP IT into an existing portal and this is also described in [Configuring a Zerto Cloud Manager](#).

Logging On to Zerto Cloud Manager

The Zerto Cloud Manager is run in a browser from any machine connected to the network where the Zerto Cloud Manager was installed.

Note: With Active Directory, in order to log on to Zerto Cloud Manager, you must assign read rights for both cn=users and CN=Computers default Active Directory containers for the application account.

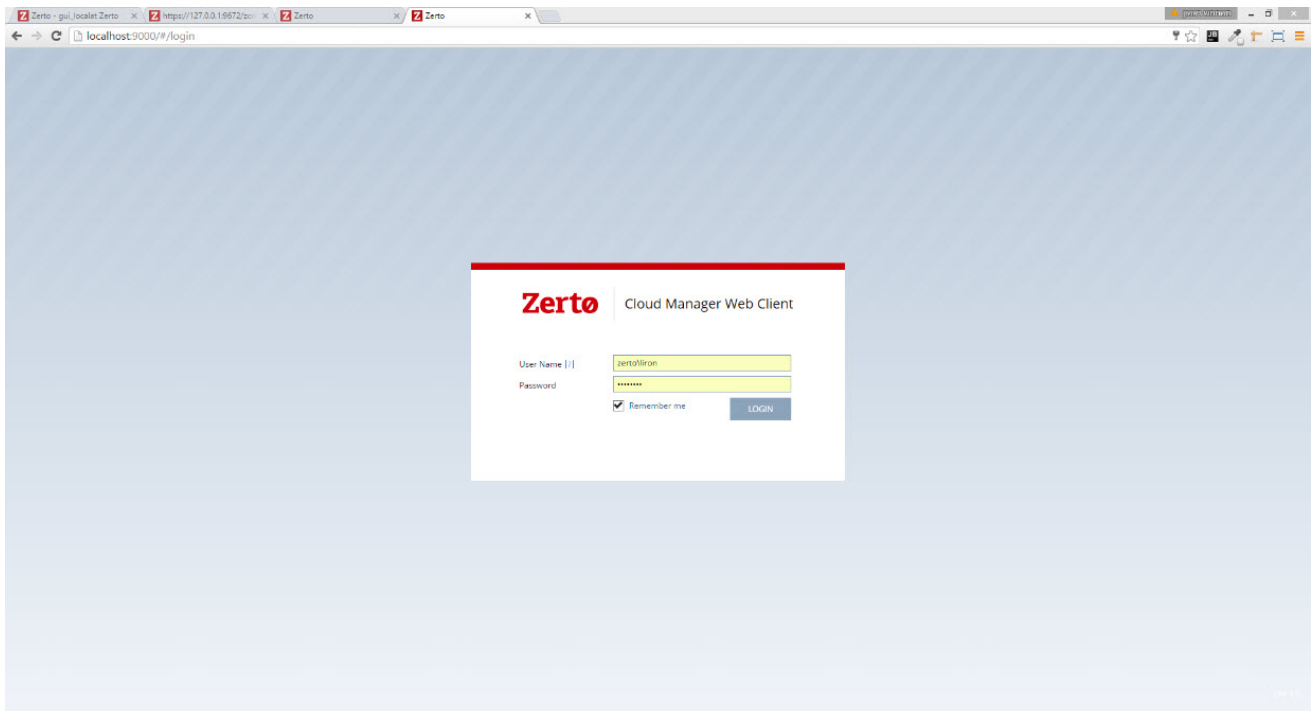
Running the Zerto Cloud Manager

To run the Zerto Cloud Manager:

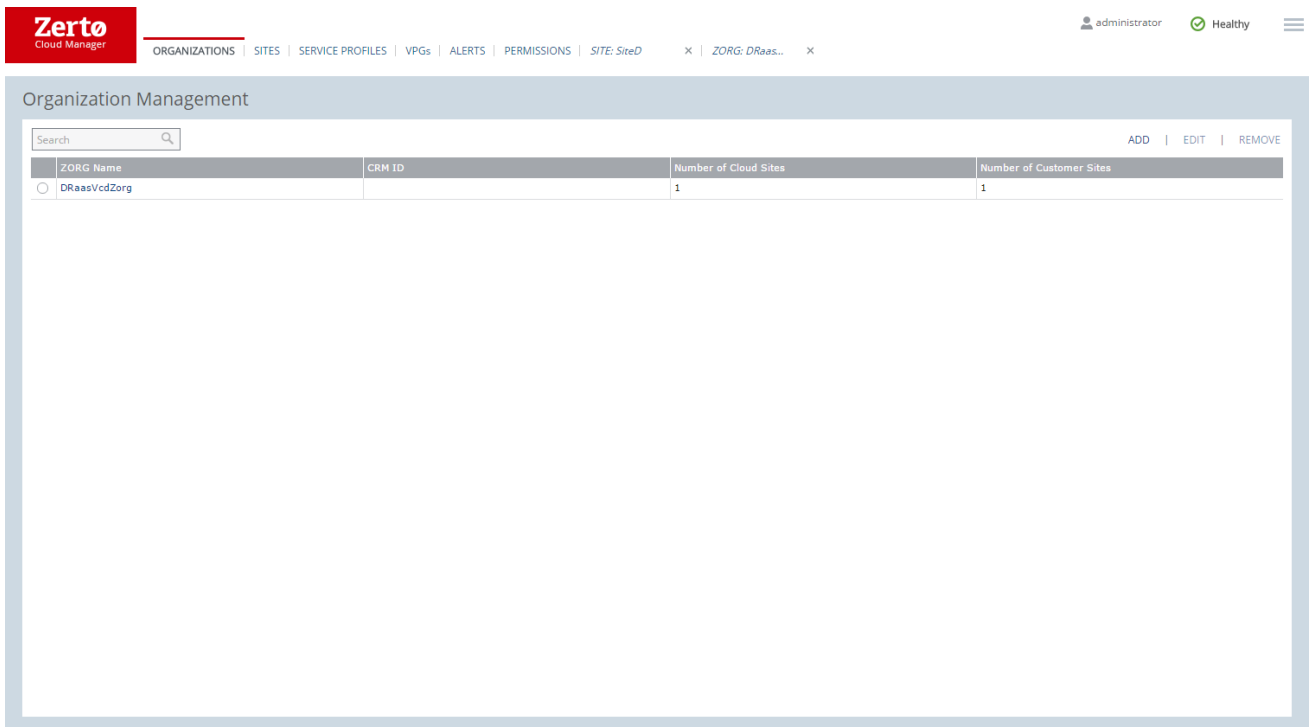
1. In a browser, enter the following URL:

https://zcm_IP:9989

where **zcm_IP** is the IP address of the machine where the Zerto Cloud Manager is installed.



2. Log in using the user name and password for the machine where the Zerto Cloud Manager is installed.
 - **Username:** The user name for the user for the machine where the Zerto Cloud Manager is installed. If the user is part of a domain, you must also specify the domain, with the following format:
domain\username
Only members of the Administrators group under a specified domain can login.
 - **Password:** A valid password for the given user name.



After logging in to the Zerto Cloud Manager you configure the cloud sites that you want to use for disaster recovery. See [Defining and Configuring the Zerto Cloud Sites](#)

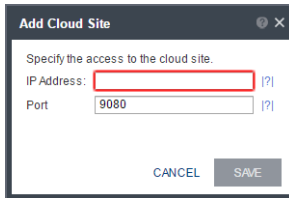
Defining and Configuring the Zerto Cloud Sites

The Zerto Cloud Manager is a single point of management for all the cloud sites providing either DRaaS or ICDR. Defining a site in the Zerto Cloud Manager involves defining a connection to a Zerto Virtual Manager.

To add a site:

1. Select the **Sites** tab.
2. Click **ADD**.

The Add Cloud Site dialog is displayed.



3. Specify the IP address of a VMware vSphere site where a Zerto Virtual Manager is running and the ZVM port specified during the installation to connect to the Zerto Virtual Manager. The default port is 9080.

NOTE:

When the ZCM is v5.5 and above, and the ZVM is 5.0, communication is via HTTP port **9080**.

When the ZCM and ZVM are both v5.5 and above, communication is via HTTPS port **9669**.

NOTE:

Zerto Cloud Manager supports CSP VMware vCenter Server and vCloud Director sites only.

4. Click **SAVE**.
The Zerto Cloud Manager connects to the site, as long as the Zerto Virtual Manager service is started.
5. Repeat this procedure for all the cloud sites.

The screenshot displays the 'Sites Management' section of the Zerto Cloud Manager interface. At the top, there is a navigation bar with the Zerto logo and several menu items: ORGANIZATIONS, SITES (highlighted), SERVICE PROFILES, VPGs, ALERTS, PERMISSIONS, and ZORG: B-Net... Below the navigation bar, there is a search bar and three action buttons: ADD, EDIT, and REMOVE. The main content area contains a table with the following data:

Connection Status	Site Name	Version	Host Name	Port	Type	# of ZORGs	ZVM Interface
<input type="radio"/> Connected	Site-30	5.0	172.20.99.30	9080	VCenter	1	Open ↗
<input checked="" type="radio"/> Connected	Site-50	5.0	172.20.99.50	9080	vCD	1	Open ↗

After defining sites in Zerto Cloud Manager, you must configure these sites. You can configure the sites using the Zerto User Interface, as described in the *Zerto Virtual Manager Administration Guide* for your environment, or configure the sites directly in Zerto Cloud Manager.

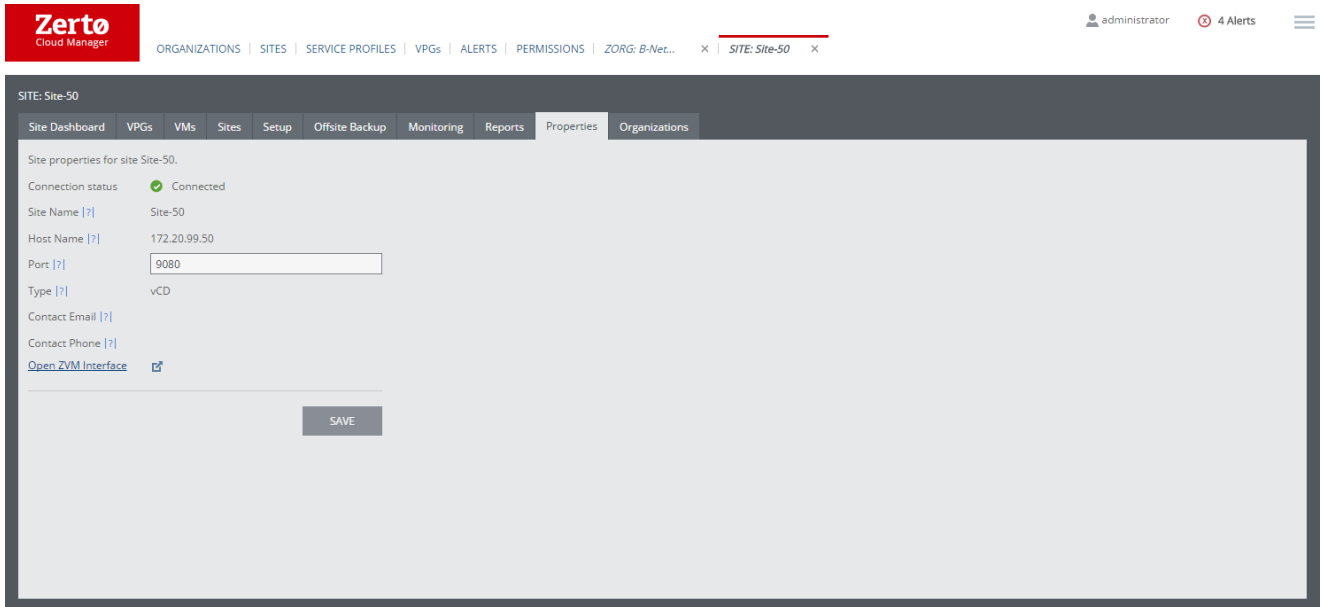
Configuring a site involves the following:

- [Registering Zerto Sites](#)
- [Adding a Security Certificate for the Zerto User Interface](#)
- [Installing Virtual Replication Appliances on Hosts in Cloud Sites](#)
- (Optional) [Configure vCloud Director](#)

Registering Zerto Sites

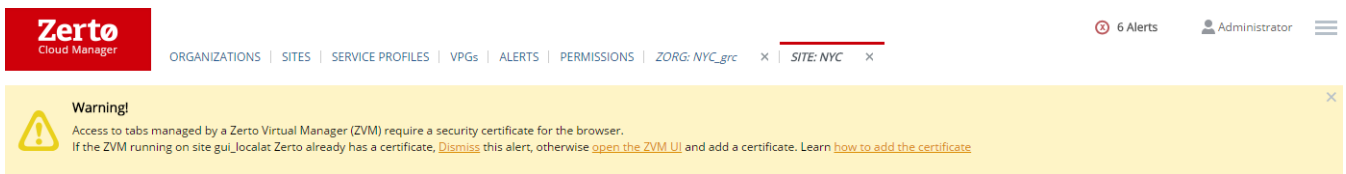
To register Zerto sites:

1. In the **Sites** tab, click a site name in the list, or check the check box of a site name in the list and click **Edit** to display site information.



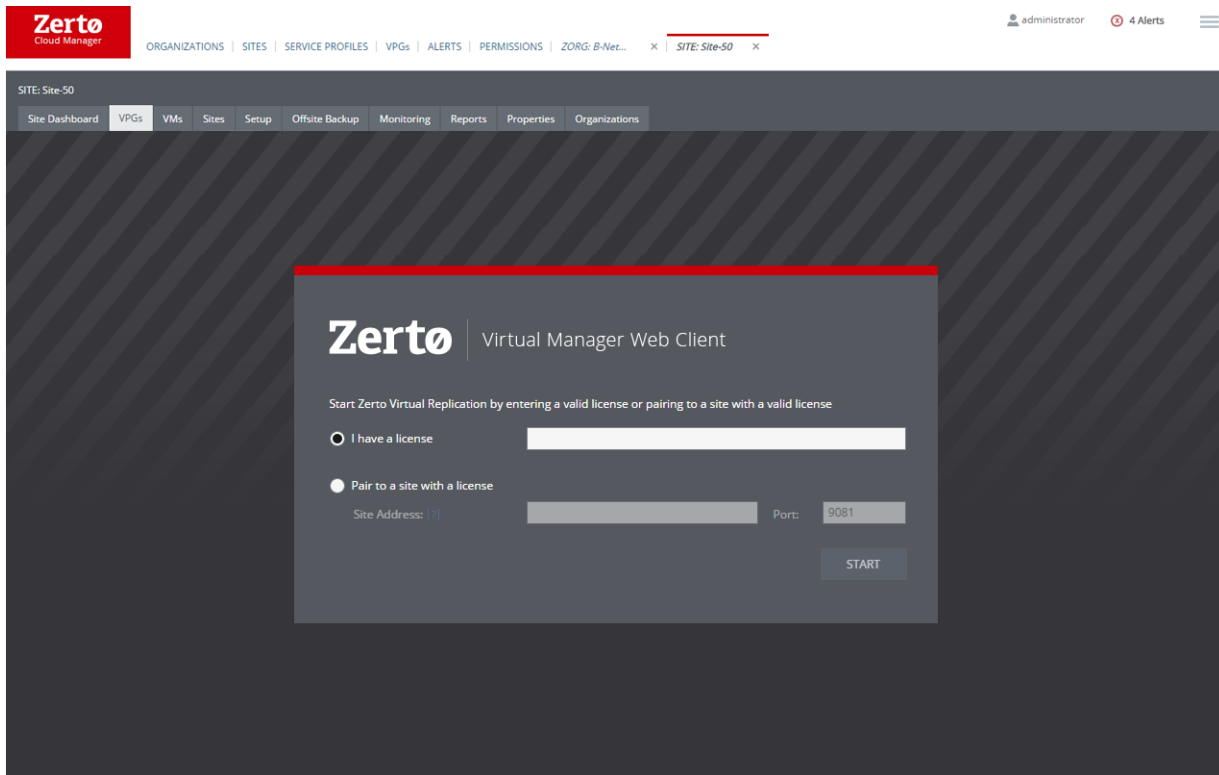
The **Properties** and **Organization** tabs manage the site in Zerto Cloud Manager. The Zerto Virtual Manager tabs – **Site Dashboard**, **VPGs**, **VMs**, **Sites**, **Setup**, **Retention Status**, **Monitoring**, and **Reports**, manage disaster recovery for the selected site in the Zerto Virtual Manager.

Note: If the Zerto Virtual Manager tabs are being displayed for the first time for this site, they are not displayed, and you see a warning that a certificate must be added to set up secure communication.



- Click the **Open the ZVM UI** link from the warning and if required, add the certificate for the Zerto Virtual Manager. After adding a certificate you can click the **Dismiss** link so this message is not displayed again.
 - For information about adding a certificate, see [Adding a Security Certificate for the Zerto User Interface](#).
2. In the Zerto Cloud Manager click one of the Zerto Virtual Manager tabs.

The first time you access the Zerto User Interface, the dialog in which you will enter the license key supplied by Zerto is displayed.



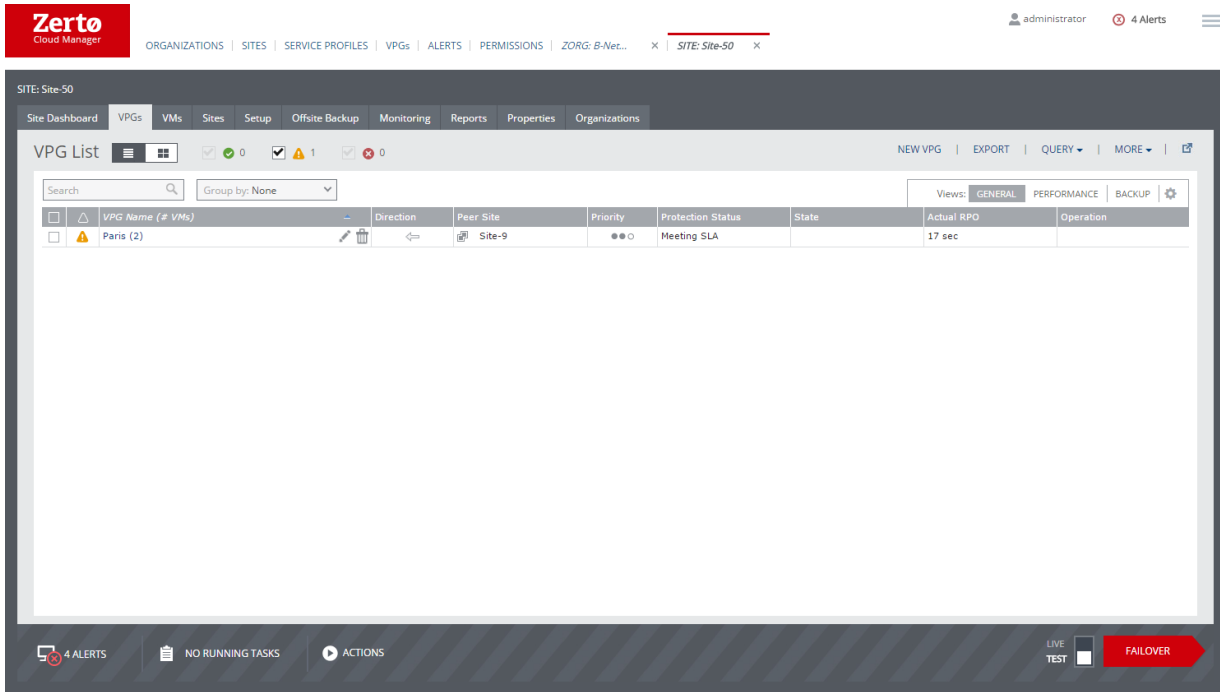
Note: A CSP with more than one cloud site must enter a license at each cloud site instead of pairing to a licensed cloud site. The license can be the same license used in another cloud site.

IMPORTANT:

The CSP must pair their customer's ZVMs with the IP address of their ZCC in order to view the sites within **Zerto Cloud Control** and **Zerto Analytics**.

3. Enter the license key and click **START**.

The **Zerto Virtual Manager** tab, for example, **VPGs**, is now displayed.



4. Return to the **Zerto Cloud Manager Sites** tab and click the next site name in the list to display the site tab.
5. Click one of the Zerto Virtual Manager tabs.
6. In the Zerto License dialog:
For an enterprise using the Zerto Cloud Manager (where DRaaS is not being offered): Pair to the first site you registered.
For a cloud service provider using the Zerto Cloud Manager (where DRaaS is being offered): A cloud service provider with more than one cloud site must enter a license for each cloud site and not pair to a licensed cloud site. The license can be the same license.
7. Repeat steps 4 to 6 for all the remaining sites.

Adding a Security Certificate for the Zerto User Interface

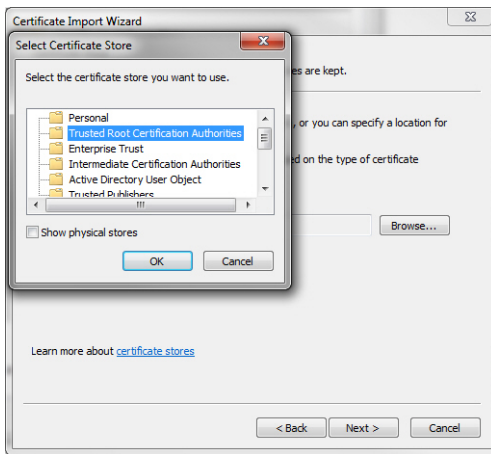
Communication between the Zerto Virtual Manager and the user interface uses HTTPS. On the first login to the Zerto User Interface, you must install a security certificate in order to be able to continue working without each login requiring acceptance of the security.

To install a security certificate for the Zerto User Interface:

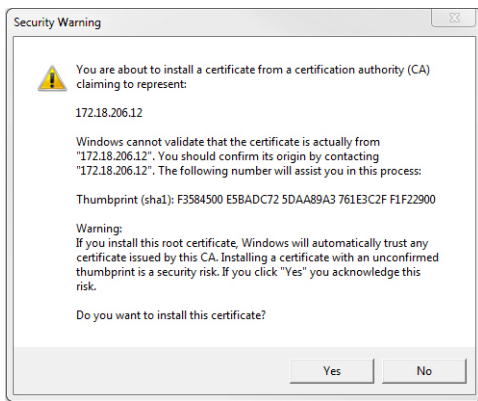
On first access to the Zerto User Interface, if you haven't installed the security certificate, a security alert is issued.

Note the following:

- To run this procedure run Microsoft Internet Explorer as administrator. The procedure is similar for Google Chrome and for Mozilla Firefox.
 - Access the Zerto User Interface using the IP and not the name of the machine where Zerto 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.

Note: If you click the **Dismiss** link by mistake, select the **Properties** tab for the site and click the **Open ZVM Interface** link to trigger the above procedure.

Installing Virtual Replication Appliances on Hosts in Cloud Sites

- Zerto recommends installing a VRA on every host in every cloud site.
- If virtual machines protected in the cloud are moved from one host in a cluster to another host in the cluster there is always a VRA to protect the moved virtual machines.
- If you are protecting a vApp, you must install a VRA on every host in the cluster on both the protected and recovery sites and ensure that DRS is enabled for these clusters.

VRA Installation Requirements

Setting up Routing

Installing a Zerto Virtual Replication Appliance (VRA) on a Host

VRA Installation Requirements

To install a VRA you require the following:

- 12.5GB datastore space.
- At least 1GB of reserved memory.
- The ESX/ESXi version must be in accordance with supported ESX/ESXi versions in the [Interoperability Matrix](#), 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:

- If the ESXi version is 5.5 or higher and the VRA should connect to the host with user credentials, or if the ESXi version is lower than 5.5 (4.x or 5.x), the password to access the host root account.

Note: For ESXi versions 5.5 or higher, by default the VRA connects to the host with a vSphere Installation Bundle, VIB. Therefore, it is not necessary to enter the password used to access the host root account.

- The storage 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.

Note: When the gateway is not required, you can specify 0.0.0.0 as the gateway, for example when performing self replication.

- If a static IP is used, which is the Zerto recommendation, instead of DHCP, the IP address, subnet mask, and default gateway to be used by the VRA.

Note: 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.

Note: For the duration of the installation of the VRA, the Zerto Virtual Manager enables SSH in the vCenter Server.

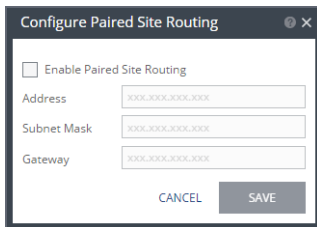
If the peer site VRAs are not on the default gateway, you must set up routing to enable the VRAs on this site to communicate with the peer site VRAs.

Setting up Routing

To set up routing:

1. In the Zerto Cloud Manager **Sites** tab, click a site name.
2. In the Zerto Virtual Manager GUI that opens, click the **Setup** tab.
3. Select **MORE > Paired Site Routing**.

The Configure Paired Site Routing dialog is displayed.



4. Click **Enable Paired Site Routing**.
5. 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 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.

Installing a Zerto Virtual Replication Appliance (VRA) on a Host

To install a Zerto Virtual Replication Appliance (VRA) on a host:

1. In the Zerto Cloud Manager **Sites** tab, click a site name.
2. In the Zerto Virtual Manager GUI that opens, in the **Setup** tab, select a host that needs a VRA and click **NEW VRA**. The Configure and Install VRA dialog is displayed. The dialog displayed depends on the ESX/i version:

ESXi versions from 5.5

ESXi versions before version 5.5

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

3. Specify the following **Host Details**:

- **Host:** The host on which the VRA is installed. The drop-down displays the hosts that do not have a VRA installed, with the selected host displayed by default.

(vSphere only) From ESXi 5.5, by default, Zerto Virtual Manager creates a **.VIB** (vSphere Installation Bundle) which is used to set up a secure communication channel to the host. The .VIB is installed on the host when the VRA is installed. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and logs it.

(vSphere only) For ESX/i versions earlier than 5.5, when using a password, Zerto Virtual Manager connects to the host using the root password. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is issued, requesting the user enter the new password.

- **Use credentials to connect to host:** When unchecked, the Zerto Virtual Manager uses VIB to set up a secure communication channel to the host. This field is only relevant for ESXi 5.5 and later.
- **Host Root Password:** When the VRA should connect to the host with a password, check **Use credential to connect to host** and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 5.x hosts.
- **Datastore:** The datastore that contains the OS disks of the VRA VM. 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. For details, refer to [Zerto Scale and Benchmarking Guidelines](#).

- **VRA Bandwidth Group:** Choose the VRA Bandwidth Group from the dropdown list. To create a new VRA group, type in the name of the new group and click **CREATE**. You can then choose the new group from the dropdown list. You group VRAs together when VRAs use different networks so they can be grouped by network, for example when the protected and recovery sites are managed by the same vCenter Server and you want to replicate from the branch site to the main site. Within a group the priority assigned to a VPG dictates the bandwidth used and is applicable within a group and not between groups. Thus, a VPG with a high priority is allocated bandwidth before VPGs with lower priorities. VPGs that are on VRAs with different VRA groups, for example, VPG1 on VRA1 in group1 and VPG2 on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.
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 the TASKS popup dialog in the status bar and under **MONITORING > TASKS**.

The VRA displayed name, and DNS name, is **Z-VRA-hostname**. If a virtual machine with this name exists, for example when a previous VRA was not deleted, the VRA name has a number appended to it.
 - 6.
 7. Add a VRA to every host that hosts virtual machines for which you want replication.

Zerto recommends installing a VRA on every listed host.

An alert is issued after the first VRA is installed in a cluster that tells you to install a VRA on the other hosts in the cluster. The alert is automatically removed when all the hosts in the cluster have VRAs installed.

 - Return to the Zerto Cloud Manager **Sites** tab and click the next site name in the list to display the site tab with nested tabs and install the VRAs for this site. Repeat this procedure for every site in the Zerto Cloud Manager.
 - A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.

Note: VRAs are configured and managed by the Zerto Virtual Manager. You cannot take snapshots of VRAs as snapshots cause operational problems for the VRAs.

(Optional) Configure vCloud Director

If you did not set up access to vCD for the Zerto Virtual Manager when installing Zerto, you can set it up from within the Zerto Cloud Manager.

Before setting up Zerto to work with vCD, you must have an AMQP server installed and configured for Zerto. Zerto provides an AMQP installation and configuration program.

[Installing and Configuring an AMQP Server for Zerto](#)

[Setting up Access to vCD](#)

[Configuring Provider vDCs](#)

Installing and Configuring an AMQP Server for Zerto

To install and configure an AMQP Server for Zerto:

1. Run the **ZertoAMQPInstallWizard** executable.
2. When prompted enter the IP or host name of the vCD and the administrator user and password to access this vCD. Note that the value here can be a Public REST API URL if this is configured in vCD.

The Zerto Virtual Manager connects to the vCD and checks whether an AMQP server is installed.

3. If an AMQP server is not installed, Zerto recommends using RabbitMQ, which in turn requires Erlang/OTP as a prerequisite. Links to the sites to install both Erlang/OTP and RabbitMQ are provided as part of the Zerto AMQP installation. Use these links to install Erlang/OTP and then RabbitMQ before continuing with the Zerto AMQP configuration.

After installing a version of RabbitMQ later than version 3.3, you must set up a user that Zerto can use:

- a) On the machine where you installed RabbitMQ, open a command line window, cmd.exe.
 - b) Browse to something like:
C:\Program Files (x86)\RabbitMQ Server\rabbitmq_server-3.4.4\sbin
 - c) Create a new user, that Zerto will use.
rabbitmqctl.bat add_user <username> <password>
 - d) Set permissions for the new user.
rabbitmqctl.bat set_permissions -p <vhostpath> <username> .* .* *
Zerto recommends using the default vhostpath, /.
e) Assign a user tag for the new user.
rabbitmqctl.bat set_user_tags <username> <tag>
4. If an AMQP server was already installed, change the connection details displayed to those defined in vCD.
 5. Specify the following AMQP connection settings:
 - **AMQP Host:** The local IP address that this machine uses to communicate with vCD.
 - **AMQP Port:** The default network port for communication.
 - **Exchange:** The name of the exchange to be configured on the AMQP for use by vCD and Zerto.
 - **vHost:** Defines this local machine as the AMQP server.
 - **User Name:** The AMQP user account Zerto will use. RabbitMQ prior to version 3.3 installs with a default administrator user: guest. With RabbitMQ versions from version 3.3, specify a user with administrator privileges.
 - **Password:** The password for the user. RabbitMQ prior to version 3.3 installs with a default password of guest.

If you installed the AMQP server as part of the Zerto AMQP installation and configuration, the default settings are displayed.

At the end of the Zerto AMQP installation and configuration, vCD is updated with these settings (for example, in vCD 5.5.1, in AMQP Broker Settings under Administration > Extensibility > Settings).

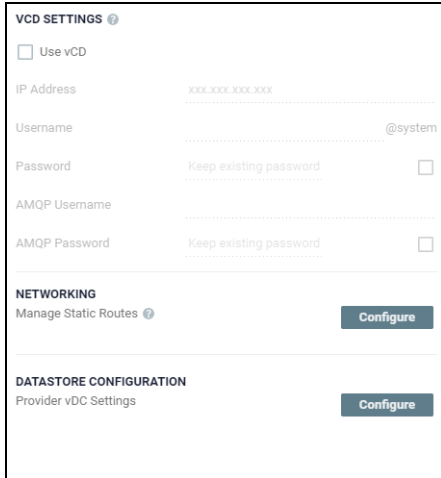
Once an AMQP server is installed and configured, you can set up access to vCD from Zerto.

Setting up Access to vCD

To set up access to vCD:

1. In the Zerto Cloud Manager **Sites** tab, select a site in the display that is using vCD.
2. In the ZVM Interface tab, click **Open**.
A new browser tab is displayed with the Zerto Virtual Manager Web Client.
3. Log on to the Zerto Virtual Manager Web Client.
4. Click the Site Settings (☰) button and select **Site Settings**.
The Site Settings dialog is displayed.
5. Click the tab **Cloud Settings**.

The Cloud Settings window is displayed.



6. Select **Use vCD**.

The fields in the vCD section are enabled.

7. 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 a vCD administrator.
- **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.

8. Click **SAVE**.

9. If a proxy server is defined on the machine where the Zerto Virtual Manager is installed, add the Zerto Virtual Manager IP address to the Internet Explorer exception list.

Configuring Provider vDCs

A Provider vDC is a collection of compute, memory, and storage resources from a vCenter. A Provider vDC provides resources to organization vDCs.

Datastores which are not listed in this window may be used by Zerto, unless they are explicitly excluded.

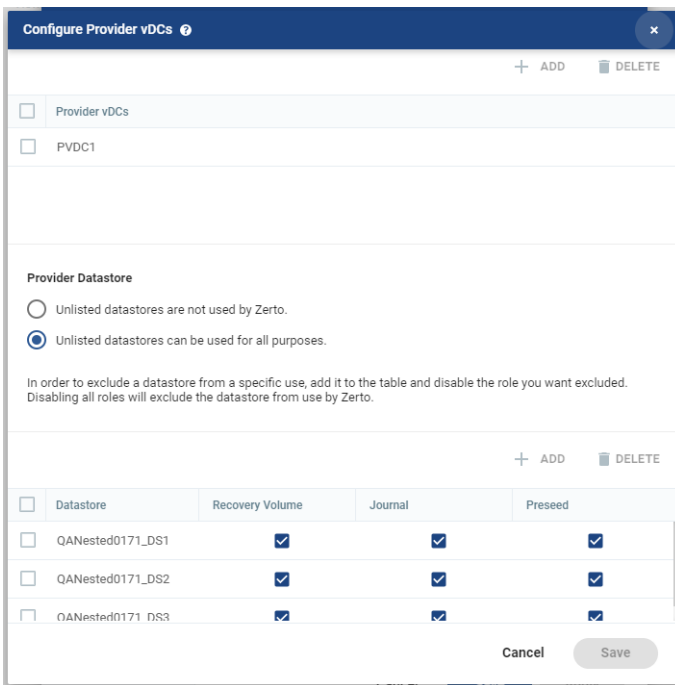
Note:

Before setting up Zerto to work with vCD, you must have an AMQP server installed.

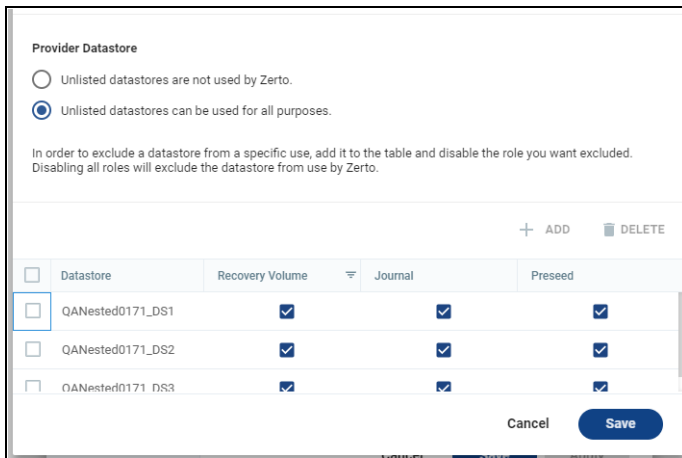
- Zerto provides an AMQP installation kit if you do not have one installed for vCD, available as a download from the Zerto Support Portal, from the downloads page.
- Run ZertoAMQPInstallWizard.exe from the kit and when prompted enter the IP or host name of the vCD and the administrator user and password to access this vCD.
- The Zerto Virtual Manager connects to the vCD and checks whether an AMQP server is installed.
 - If an AMQP server is not installed, Zerto recommends using RabbitMQ, which in turn requires Erlang/OTP.
 - Links to the sites to install both Erlang/OTP and RabbitMQ are provided as part of the Zerto AMQP installation. Use these links to install Erlang/OTP and then RabbitMQ, then you can continue with the Zerto AMQP installation.
- If an AMQP server was already installed, change the connection details displayed to those defined in vCD.
- If you installed the AMQP server as part of the Zerto AMQP installation, the default settings for these installations are displayed, with a user and password of **guest**.
- At the end of the Zerto AMQP installation, vCD is updated with these settings, in AMQP Broker Settings under Administration > Blocking Tasks > Settings.

To configure provider vDCs:

1. In the Zerto Cloud Manager **Sites** tab, click the site name of a site using vCD.
2. In the **Properties** tab, click **Open ZVM Interface**.
A new browser tab is displayed with the Zerto Virtual Manager Web Client.
3. Log on to the **Zerto Virtual Manager Web Client**.
4. Click the **Site Settings** (☰) button.
The Site Settings dialog is displayed.
5. Click **Cloud Settings**.
The Cloud Settings page is displayed.
6. Under **Datastore Configuration**, click **Configure** to access Provider vDC settings.
The Configure Provider vDCs dialog is displayed.



7. In the **Provider vDCs** area (top), click **Add**. A list of provider vDCs appear.
The provider vDCs were created by the Cloud Service Providers according to predefined service levels, storage availability, performance requirements or cost.
 - Add the provider vDCs which will be available for use in Zerto.
8. In the **Provider Datastore** area select one of the following:
 - **Unlisted datastores are not used by Zerto:** Clearly define that datastores which are not listed in this window cannot be used.
 - **Unlisted datastores can be used for all purposes:** Allow unlisted datastores of all provider vDCs, even those provider vDCs that were not added to the list of Provider vDCs can be used for any purpose.
9. In the **Provider Datastore** area, click **Add**, to add datastores.



- Select the **Recovery Volume** checkbox, if the datastore can be used as a recovery datastore.
 - Select the **Journal** checkbox if the datastore can be used for the journal.
 - Select the **Preseed** checkbox if the datastore can be used for preseeded disks. Only datastores marked as preseeded can be used, preventing different organizations being exposed to datastores of other customers using the preseed option.
 - In order to exclude a datastore, add it to the list, then deselect all checkboxes.
10. In the Configure Provider vDCs dialog, click **SAVE** and then click **SAVE** in the Site Settings dialog.

Setting Up Zerto Organizations, ZORGs

As a provider of disaster recovery services, the cloud service provider must set up individual customers to manage protection and recovery for these customers. The customers are defined to Zerto Cloud Manager as Zerto organizations, ZORGs.

You set up each ZORG, as described in [Defining a ZORG](#), and then configure it, regardless of whether the ZORG will use DRaaS or ICDR.

- [Manage ZORG - Defining Settings for a ZORG](#)
- [Defining ZORG Permissions](#)
- [Defining Resources that the Cloud Service Provider Enables the ZORG to Use](#)

When offering DRaaS to a ZORG you need to set up the ZORG for DRaaS:

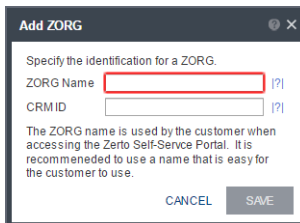
- [Defining DRaaS Components](#)

Defining a ZORG

To define a ZORG:

1. In the Zerto Cloud Manager row of tabs, click **Organizations**.
2. Click **Add**.

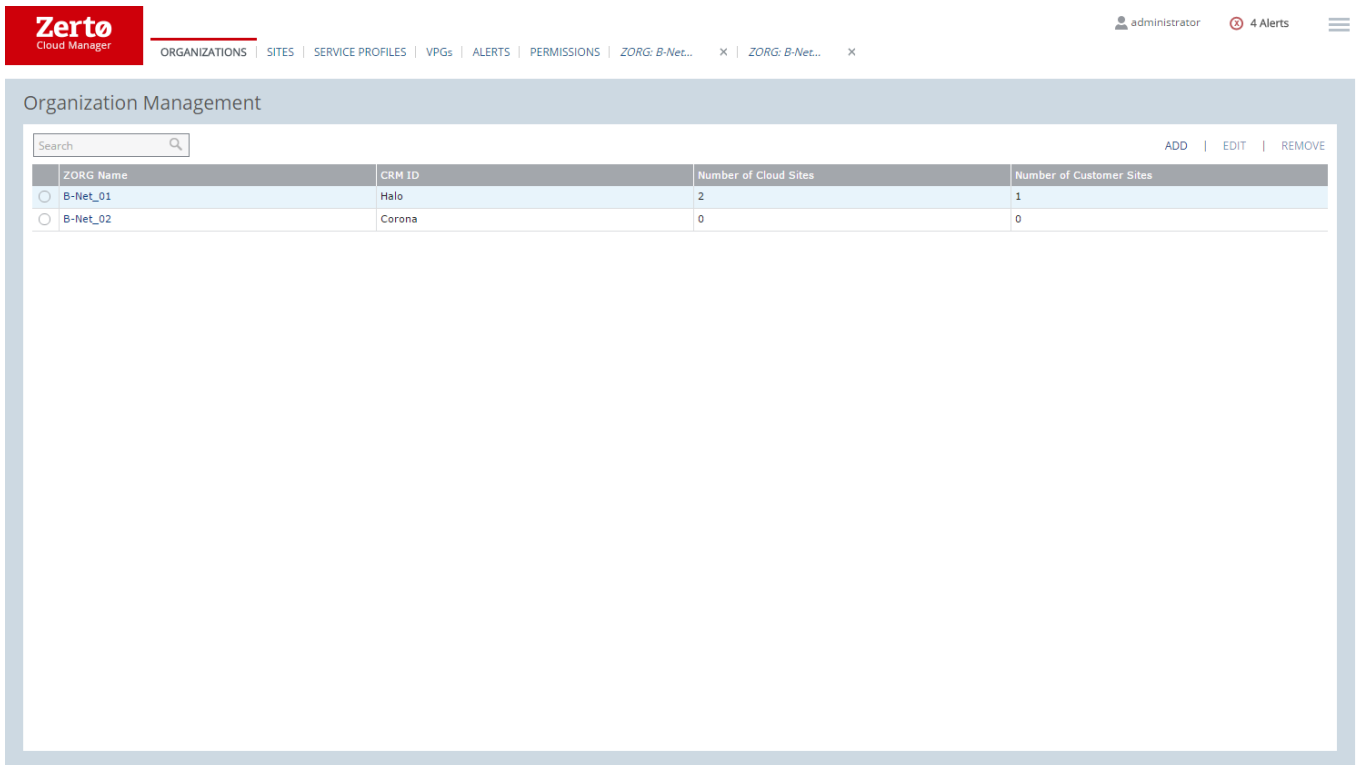
The Add ZORG dialog is displayed.



3. Specify the **ZORG Name** and optionally a **CRM ID** to identify the organization in a CRM.
 The ZORG name is used by the customer when accessing the Zerto Self-service Portal. Zerto recommends using a name that is easy for the customer to use.

Note: The ZORG name cannot contain special characters.

4. Click **SAVE**.
5. Repeat steps 2-4, for all the Zerto organizations, ZORGs.



The following information is displayed in the **Organizations** tab:

- **ZORG Name:** The name of the organization.
- **CRM ID:** An optional identifier to use to identify the organization in a CRM.
- **Number of Cloud Sites:** The number of cloud sites that the organization uses.
- **Number of Customer Sites:** The number of sites the organization has that use the cloud sites for disaster recovery.

Clicking an organization name in the list, or selecting a row and then clicking **Edit**, displays another row of tabs:

- **Manage ZORG**
- **vCenter Cloud Resources**
- **vCD Cloud Resources**
- **Customer Sites**
- **VPGs**
- **Alerts**

After defining the ZORG, you specify properties for the ZORG:

- [Manage ZORG - Defining Settings for a ZORG](#)
- [Defining ZORG Properties](#)
- [Defining ZORG Permissions](#)
- [Defining ZORG Service Profiles](#)
- [Defining ZORG ZSSP Login Credentials](#)
- [Defining Resources that the Cloud Service Provider Enables the ZORG to Use](#)

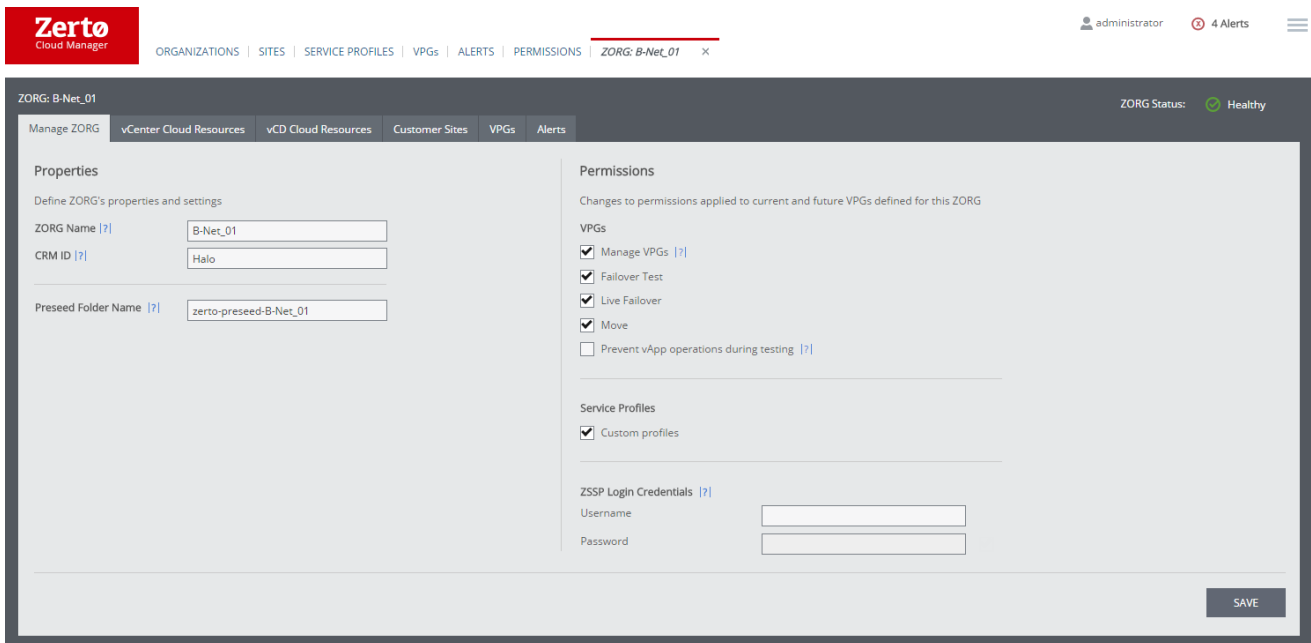
Manage ZORG - Defining Settings for a ZORG

You can edit the ZORG properties, for example, add a CRM ID if it was not specified when the ZORG was defined, or edit the ZORG name or CRM ID of the ZORG. You can also set the folder to use for preseeded volumes to make the initial synchronization of protected virtual machines in a VPG quicker.

Defining ZORG Properties

To define ZORG Properties:

1. Click a ZORG name link in the Zerto Cloud Manager **Organizations** tab or select a row in the display and then click **Edit**. The ZORG details are displayed.



2. In the **Properties** section, optionally, change the ZORG name or change or add a CRM ID for the ZORG.
3. Specify the folder to use to store preseeded volumes in **Preseed Folder Name**. A preseed volume is a virtual disk (the VMDK flat file and descriptor) 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 protected site after the creation of the preseeded disk. When using a preseeded VMDK, you select the datastore and exact location, folder, and name of the preseeded disk. Zerto 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.

Note: The preseeded disks must be saved in a folder with the exact name specified in this field.

When the recovery site is a vDC site:

- a) Create a folder in vCD to use for the preseeded disks in the datastore you want to use for the customer.
- b) Specify this datastore as a provider datastore for preseeded disks in the **Configure provider vDCs** dialog, from the **Advanced Settings** dialog, as described in [Configuring Provider vDCs](#).

- c) Specify the **Preseed Folder Name** for the ZORG.
4. Click **Save**.

Defining ZORG Permissions

The Permissions section at the ZORG level displays the permissions assigned to the ZORG. The ZORG is only able to perform actions for which it has permissions. The action applies to all VPGs defined for the ZORG. If a permission is not assigned to the ZORG, the option to perform the action by the ZORG is disabled.

These permissions are the minimum default permissions supplied by Zerto. You can manage an extended set of permissions for specific entities such as ZORGs, VPGs, and sites, as described in [Defining Role-based Access Control](#).

To define ZORG Permissions:

1. In the **Permissions** section, define the permissions to apply to all VPGs defined for the ZORG.
 - **Manage VPGs:** When selected, the organization can create and edit virtual protection groups (VPGs) to protect groups of virtual machines together.
 - **Failover Test:** When selected, the organization can test the failover of VPGs to verify that the disaster recovery that you have planned is the one being implemented.
 - **Live Failover:** When selected, the organization can recover the virtual machines in a VPG after an unforeseen disaster.
 - **Move:** When selected, the organization can migrate the virtual machines in VPGs to a remote site in a planned operation. ZORGs using DRaaS can also create offsite clones of the virtual machines in VPGs.
 - **Prevent vApp operations during testing:** When vCD resources are specified in the vCD Cloud Resources tab, vApp operations are blocked when a VPG is being tested.
2. Click **Save**.

Defining ZORG Service Profiles

In the **Service Profiles** section:

Custom Profile: When selected, the organization can specify general settings for a VPG instead of using one of the provided sets of default properties when a VPG is created or edited. This permission is only relevant if the **Manage VPGs** permission is checked. Long Term Retention is enabled when custom profile is selected.

Defining ZORG ZSSP Login Credentials

To define ZORG ZSSP Login Credentials:

When a ZORG has access to the disaster recovery user interface directly via the Zerto Self-service Portal, ZSSP, and not via a cloud service provider portal with the ZSSP embedded within, in the **ZSSP Login Credentials** section:

1. Specify the username and password that is required to log on to the ZSSP.

The password is hidden and is displayed as asterisks.
2. Click **Save**.

Defining Resources that the Cloud Service Provider Enables the ZORG to Use

ZORGs use specified cloud sites.

Each site has specific resources and you can select the resources you want to be made available to the specific ZORG as well as rename the information to something meaningful for the ZORG, hiding the internal naming conventions of the cloud site.

Note: SCVMM resources are not available to ZORGs.

You can also limit the number of virtual machines and amount of storage that the ZORG is able to protect.

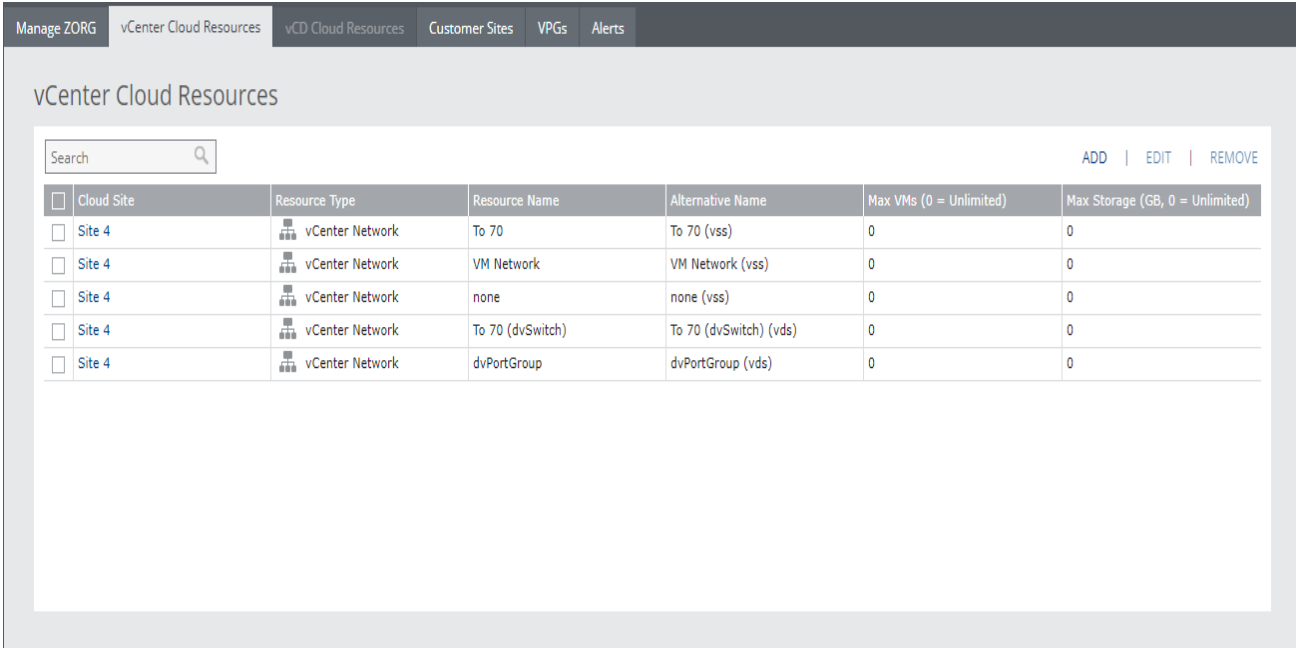
[To make vCenter Server resources available to the ZORG](#)

[To edit vCenter Server resources](#)

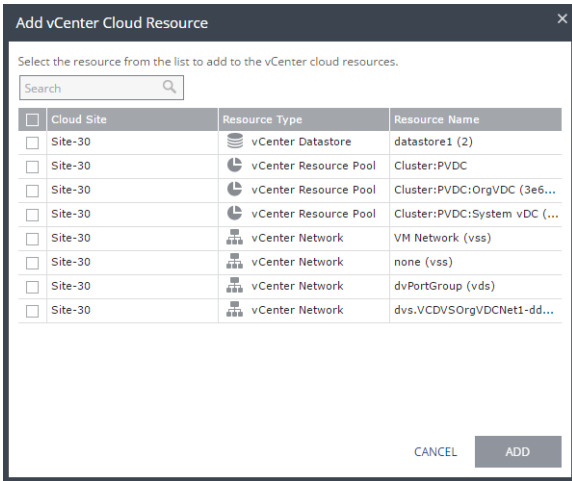
[To add and edit vCD resources](#)

To make vCenter Server resources available to the ZORG

1. In the Zerto Cloud Manager **Organizations** tab, click a **ZORG Name** link or select a row in the display and then click **Edit**.
2. Select the **vCenter Cloud Resources** tab.

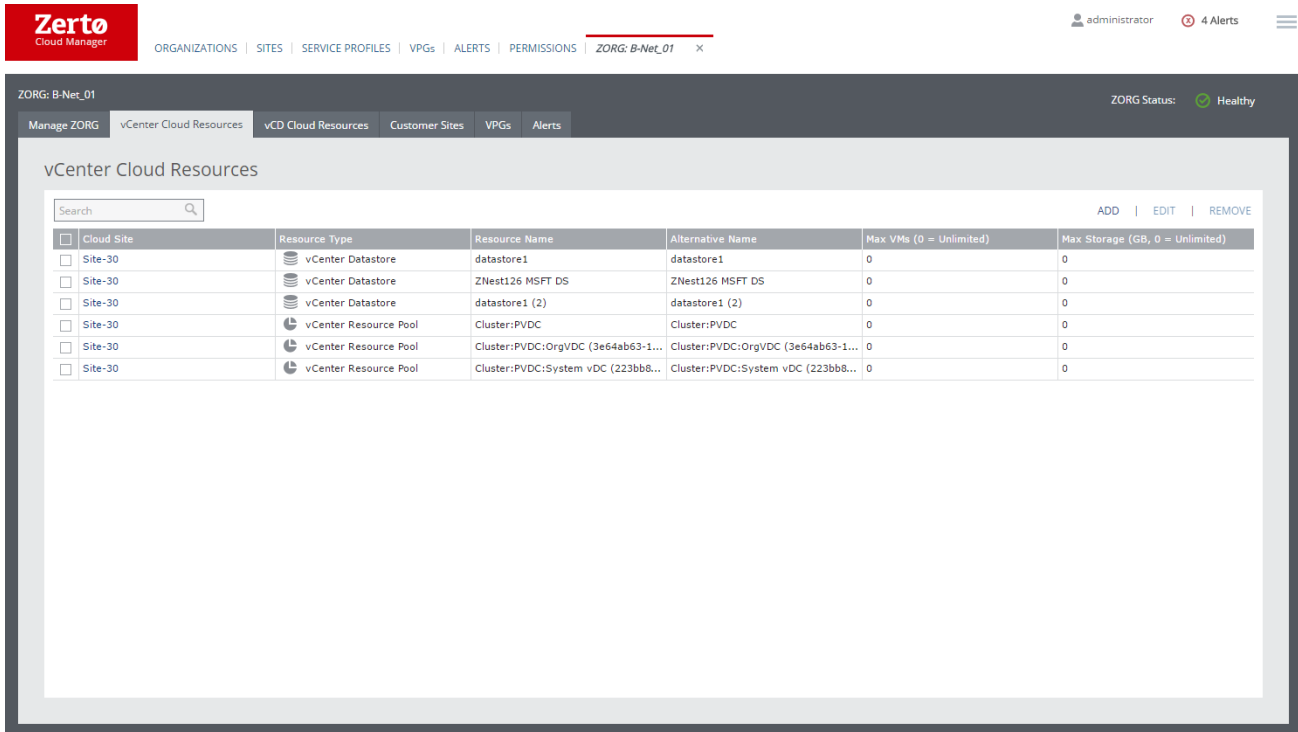


3. Click **ADD**.
 The Add vCenter Cloud Resource dialog is displayed.



4. Select all the resources you want to make available to the ZORG.
 When defining a VPG to be recovered in a cloud site, the recovery host must be a resource pool.
Note: Each resource pool can only be used by one ZORG.
5. Click **ADD**.

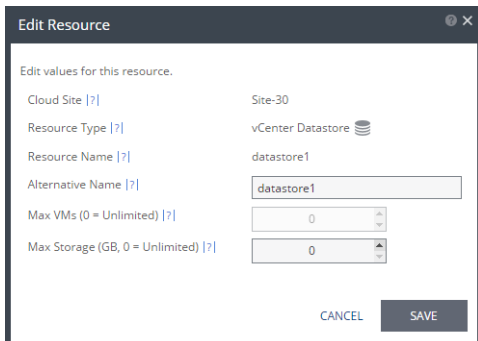
The selected resources are displayed.



Note: You cannot define an RDM disk as a vCenter Server resource.

To edit vCenter Server resources

1. In the vCenter Cloud Resources tab, select a row and click **EDIT**.
 The Edit Resource dialog is displayed.



The fields you can edit in this dialog change, depending on the type of resource you select. Update the relevant information:

- **Alternative Name:** The alternative name for the resource which is displayed to the ZORG when using the Zerto Self-service Portal or when pairing is via a Zerto Cloud Connector. If there is no value in this field, the ZORG sees the value in the Resource Name field.
- **Max VMs (0 = Unlimited):** The maximum number of virtual machines that can be protected when using this resource pool.
- **Max Storage (GB, 0 = Unlimited):** The maximum amount of storage that can be protected when using this datastore.

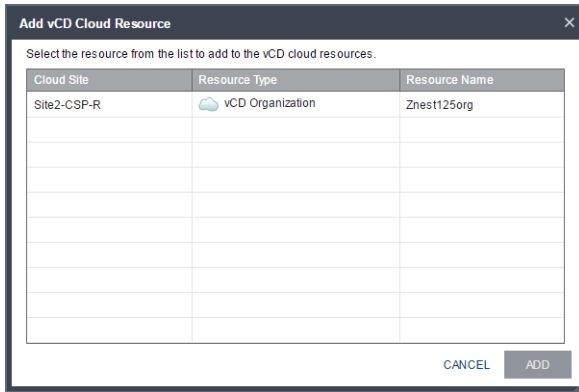
2. Click **SAVE**.

To add and edit vCD resources

1. In the Zerto Cloud Manager Organizations tab, click a **ZORG Name** link or select a row in the display and then click **Edit**.
2. Select the **vCD Cloud Resources** tab.

3. Click **ADD**.

The Add vCD Cloud Resource dialog is displayed.



4. Select the resource you want to make available to the ZORG.

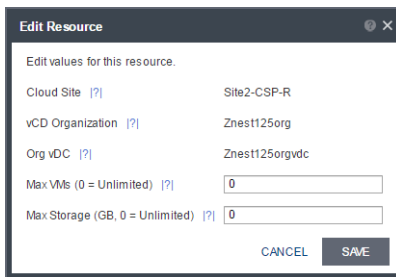
Note: Each vCD Org can only be used by one ZORG.

5. Click **ADD**.

The selected resources are displayed.

6. Select the row in the table and click **EDIT**.

The Edit Resource dialog is displayed.



The fields you can edit in this dialog change, depending on the type of resource you select. Update the relevant information:

- **Alternative Name:** The alternative name for the resource which is displayed to the ZORG when using the Zerto Self-service Portal or when pairing is via a Zerto Cloud Connector. If there is no value in this field, the ZORG sees the value in the Resource Name field.
 - **Max VMs (0 = Unlimited):** The maximum number of virtual machines that can be protected.
 - **Max Storage (GB, 0 = Unlimited):** The maximum amount of storage that can be protected.
7. Click **Save**.

Defining DRaaS Components

In a DRaaS configuration, the organization networks for disaster recovery are extended to the cloud. Zerto Cloud Connectors (ZCC) are installed to ensure that these networks have no touch points with the cloud infrastructure network, providing complete network separation between each organization network and the cloud service provider infrastructure network. All the traffic to and from the organization is routed through the cloud connector, so that the following is implemented:

- None of the organizations have direct access to the cloud service provider network and cannot see any part of the cloud service provider network that the cloud service provider does not allow them to see.
- Each organization has no access to the network of another organization.

A ZCC is a virtual machine installed on the cloud side, one for each customer organization replication network. The ZCC requires both cloud-facing and customer-facing static IP addresses. Also, for the cloud connector, the IP ranges used for the

organization network and cloud service provider infrastructure network cannot be the same. The cloud connector requires the following:

- 4GB disk space
- At least 1GB of reserved memory.
- 1 vCPU.

Zerto recommends using a 10Gbps NIC for each Zerto Cloud Connector, enabling it to handle 10Gbps of traffic.

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.

If the cloud service provider wants to institute additional security when using a ZCC, it 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.

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 ZCCs with the specified group. Existing ZCCs must be redeployed to use the changed static route.

ZCCs are defined per organization with one ZCC defined for each organization site. Each ZCC requires two ports for each VRA (one port for VRA port 4007 and one port for port 4008) accessed via the ZCC. There is directionality to these ports.

For example, Customer A network has three VRAs and customer B network has two VRAs and the cloud service provider network has four VRAs, then the following ports must be open in the firewall: The cloud service provider's VRAs need to use six ports to reach customer A's VRAs, while customer A's VRAs need eight ports to reach the cloud's VRAs. The cloud service provider's VRAs need to use four ports to reach customer B's VRAs, while customer B's VRAs need eight ports to reach the cloud's VRAs.

Customer A (CA) to Cloud Service Provider (CSP) VRAs via ZCC1:

```
ZCC1_CA:9082, ZCC1_CA:9083 > VRA_CSP_1:4007, VRA_CSP_1:4008
ZCC1_CA:9084, ZCC1_CA:9085 > VRA_CSP_2:4007, VRA_CSP_2:4008
ZCC1_CA:9086, ZCC1_CA:9087 > VRA_CSP_3:4007, VRA_CSP_3:4008
ZCC1_CA:9088, ZCC1_CA:9089 > VRA_CSP_4:4007, VRA_CSP_4:4008
```

Customer B (CB) to Cloud Service Provider (CSP) VRAs via ZCC2:

```
ZCC2_CB:9082, ZCC2_CB:9083 > VRA_CSP_1:4007, VRA_CSP_1:4008
ZCC2_CB:9084, ZCC2_CB:9085 > VRA_CSP_2:4007, VRA_CSP_2:4008
ZCC2_CB:9086, ZCC2_CB:9087 > VRA_CSP_3:4007, VRA_CSP_3:4008
ZCC2_CB:9088, ZCC2_CB:9089 > VRA_CSP_4:4007, VRA_CSP_4:4008
```

Cloud Service Provider (CSP) VRAs to customer VRAs:

```
ZCC1_CSP:9082, ZCC_CA:9083 > VRA_CA_1:4007, VRA_CA_1:4008
ZCC1_CSP:9084, ZCC_CA:9085 > VRA_CA_2:4007, VRA_CA_2:4008
ZCC1_CSP:9086, ZCC_CA:9087 > VRA_CA_3:4007, VRA_CA_3:4008
ZCC2_CSP:9082, ZCC_CB:9083 > VRA_CB_1:4007, VRA_CB_1:4008
ZCC2_CSP:9084, ZCC_CB:9085 > VRA_CB_2:4007, VRA_CB_2:4008
```

Note: If a VRA is uninstalled, connectivity from that VRA to any ZCC is lost. After a VRA is reinstalled on the host, the ports that were used for the connection to the ZCC are not reused and new ports must be opened in the firewall for the cloud site.

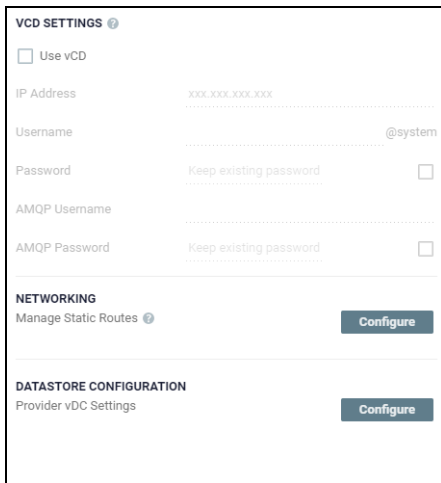
[Setting up Static Routes](#)

[Adding a Cloud Connector For a Site](#)

Setting up Static Routes

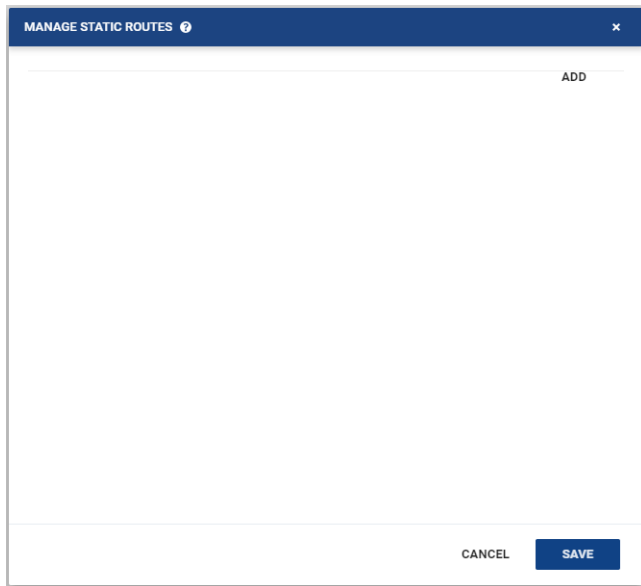
To set up static routes:

1. In the Zerto Cloud Manager **Sites** tab, click the site name of a site that provides DRaaS.
2. Click the **Site Settings** (☰) button.
The Site Settings dialog is displayed.
3. Click **Cloud Settings**.
The Cloud Settings page is displayed.



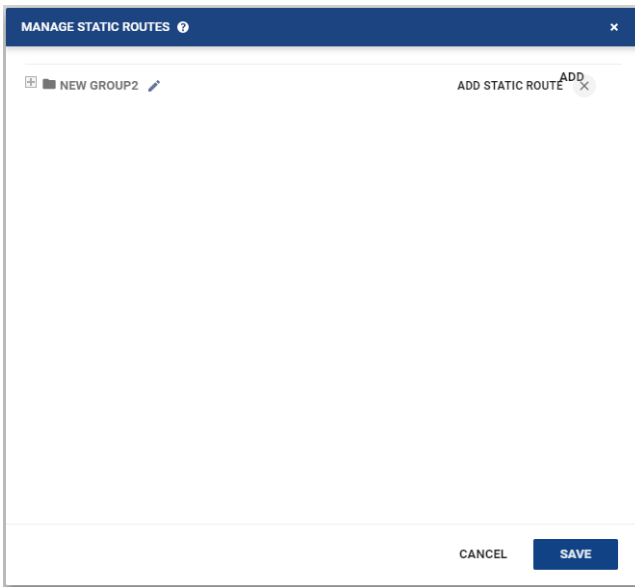
The screenshot shows the 'VCD SETTINGS' dialog box. It has a title bar with a question mark icon. Below the title bar, there is a checkbox labeled 'Use vCD'. Underneath, there are several input fields: 'IP Address' with a placeholder 'xxx.xxx.xxx.xxx', 'Username' with a placeholder '.....@system', 'Password' with a placeholder 'Keep existing password' and a checkbox, and 'AMQP Password' with a placeholder 'Keep existing password' and a checkbox. Below these fields, there are two sections: 'NETWORKING' with a sub-section 'Manage Static Routes' and a 'Configure' button, and 'DATASTORE CONFIGURATION' with a sub-section 'Provider vDC Settings' and a 'Configure' button.

4. In the Networking section, click **Configure**.
The Manage Static Routes dialog is displayed.

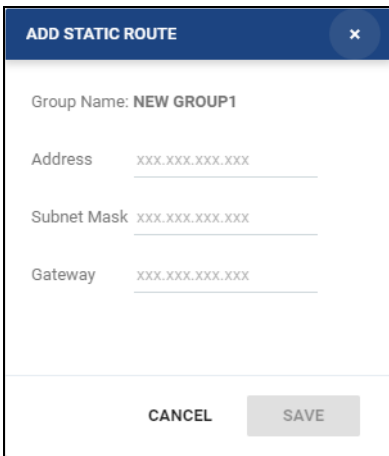


The screenshot shows the 'MANAGE STATIC ROUTES' dialog box. It has a title bar with a question mark icon and a close button (X). The main area is mostly empty, with the word 'ADD' in the top right corner. At the bottom, there are two buttons: 'CANCEL' and 'SAVE'.

- Click **ADD** to define a group. This group will contain a static route to the subnet used by the Zerto Virtual Manager and can be applied to more than one cloud connector.

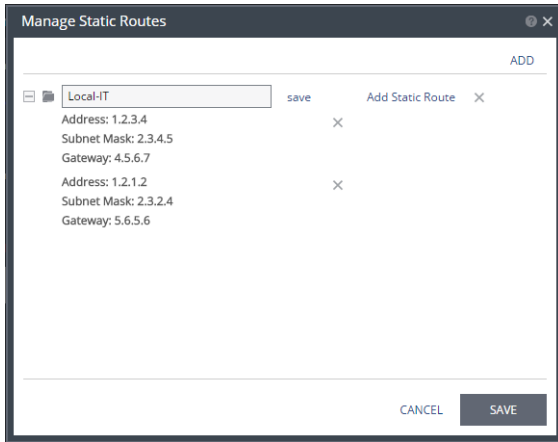


- To edit the name of the group, click the edit icon next to the newly added group name. Enter the name of the group and click **SAVE**.
- To define a static route for that group, click **Add Static Route**.



- Specify the static route:
 - **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.
- Click **SAVE**.
You can add more groups by repeating steps 5-9.

You can define more than one static route for a group. The static routes are displayed under each group.



10. Click **SAVE**.
 - You can use the group in the definition of a connector.
 - If you change the Zerto Virtual Manager and VRA cloud network, changing the static route settings for a group to the new network only changes the access for new ZCCs with the specified group. Existing ZCCs must be redeployed to use the changed static route.

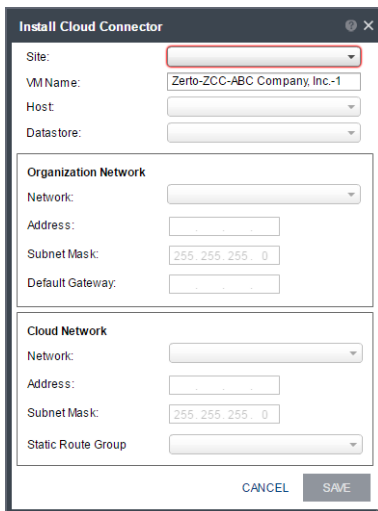
Adding a Cloud Connector For a Site

A cloud connector requires 4GB disk space, at least 1GB of reserved memory, and 1 vCPU.

To add a cloud connector for a site:

1. Click a ZORG in the Zerto Cloud Manager **Organizations** tab or select the row in the display and then click **EDIT**.
2. Select the **Customer Sites** tab.
3. Click **ADD**.

The Install Cloud Connector dialog is displayed.

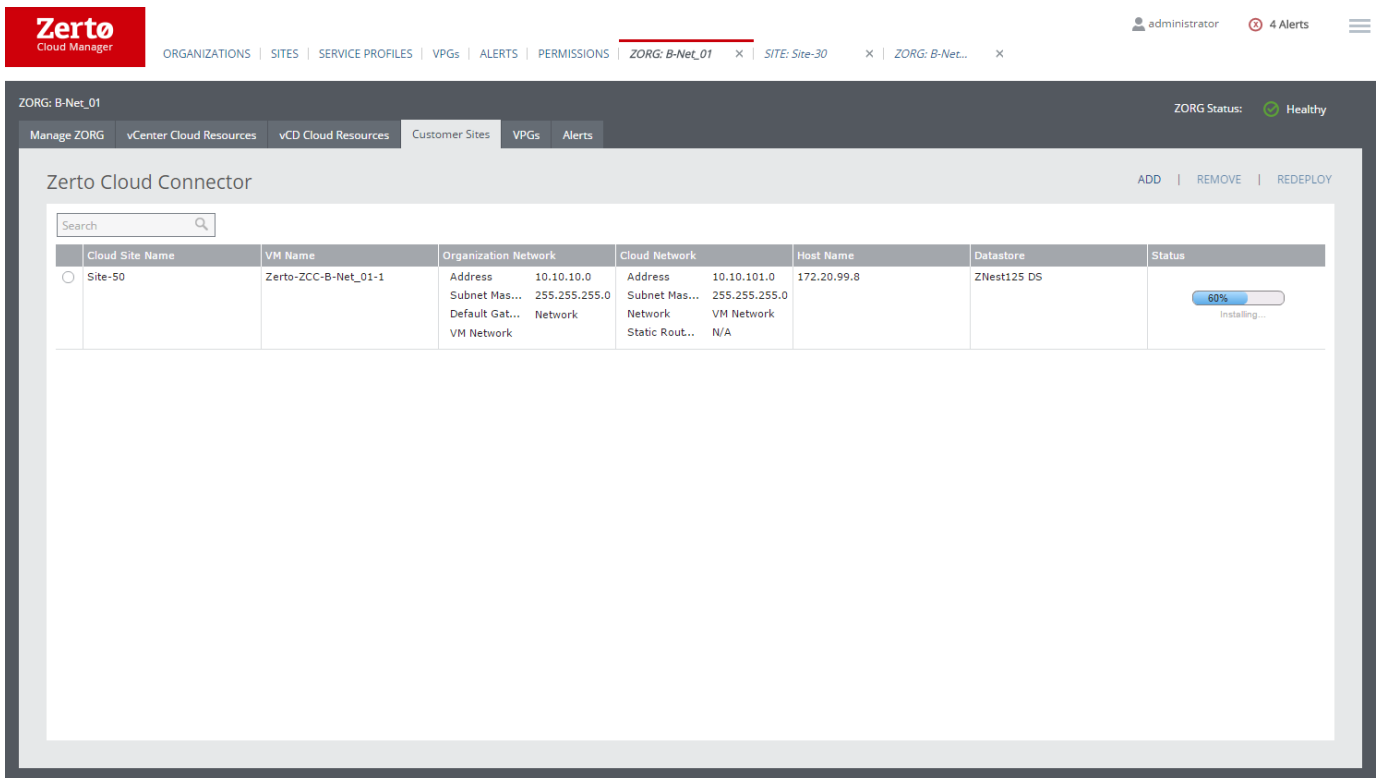


Specify the following:

- **Site:** The site used by the cloud service provider for the organization.
- **VM Name:** The name to assign to the cloud connector virtual machine.
- **Host:** The recovery host for the cloud connector virtual machine. The dropdown displays the hosts which do not have a cloud connector installed.
- **Datastore:** The datastore for the cloud connector virtual machine.
- **Organization Network:** The customer network details:

- **Network:** The name of the customer’s network.
 - **Address:** The IP address used to access the organization network. The customer pairs to this IP address.
 - **Subnet Mask:** The subnet mask for the customer network. The default value is **255.255.255.0**.
 - **Default Gateway:** The default gateway for the customer network.
 - **Cloud Network:** The cloud service provider local network details:
 - **Network:** The name of the cloud-side network.
 - **Address:** The IP address to access the cloud service provider network that communicates with the cloud connector.
 - **Subnet Mask:** The subnet mask for the cloud service provider network. The default value is **255.255.255.0**.
 - **Static Route Group:** The name of the group for which static routes are defined to the Zerto Virtual Manager network and VRA network. If a static route group is not specified, it is assumed that the Zerto Virtual Manager and VRAs are on the same network.
4. Click **SAVE**.

The cloud connector installation starts and the status is displayed in the table.



Providing a Self-service Portal for Cloud Service Provider Customers

When the CSP offer DRaaS, the Zerto Self-service Portal provides access to the cloud service provider recovery site so that customers of the CSP can perform failover instead of requesting that the cloud service provider perform the failover.

In Zerto Cloud Manager, the CSP can define the operations available to each customer via the Zerto Self-service Portal. For details, see [“Setting Up Access to the Zerto Self-service Portal”, on page 56](#).

Creating Service Profiles

A service profile provides 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.

Cloud service providers can create different service profiles for different situations and can assign one of the service profiles to be the default, to be displayed when a VPG is created.

The Zerto Cloud Manager Service Profiles tab displays the defined service profiles. Zerto Cloud Manager includes a predefined service profile, the System Service Profile.

The screenshot shows the Zerto Cloud Manager interface for the Service Profiles tab. At the top, there is a navigation bar with the Zerto logo and a breadcrumb trail: ORGANIZATIONS | SITES | SERVICE PROFILES | VPGs | ALERTS | PERMISSIONS | ZORG: B-Net... | SITE: Site-30 | ZORG: B-Net... . The user is logged in as 'administrator' and has 4 Alerts. The main content area is titled 'Service Profiles' and contains a search bar and a table. The table has the following columns: Profile Name, Recovery Policy, Target RPO, Journal History, Journal Size Hard Limit, Journal Size Warning Threshold, Test Frequency Reminder, Description, Retention Period, and Backup Schedule. A single row is visible for the 'System Service Profile'.

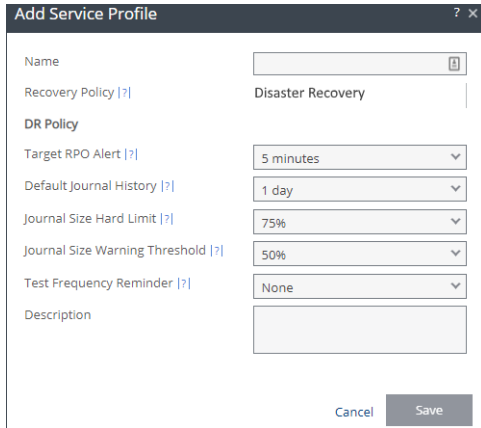
Profile Name	Recovery Policy	Target RPO	Journal History	Journal Size Hard Limit	Journal Size Warning Threshold	Test Frequency Reminder	Description	Retention Period	Backup Schedule
System Service Pr...	Disaster Re...	5 minutes	1 day	75%	50%	None	System Service Profile	N/A	N/A

Note: Specify in the Permissions tab for a ZORG whether or not the ZORG can set its own values for SLA properties when defining a VPG or whether it has to use a predefined service profile. For details, see ["Permissions Tab", on page 93](#).

To create a service profile:

1. Select the Zerto Cloud Manager **Service Profiles** tab.
2. Click **ADD**.

The Add Service Profile dialog is displayed.



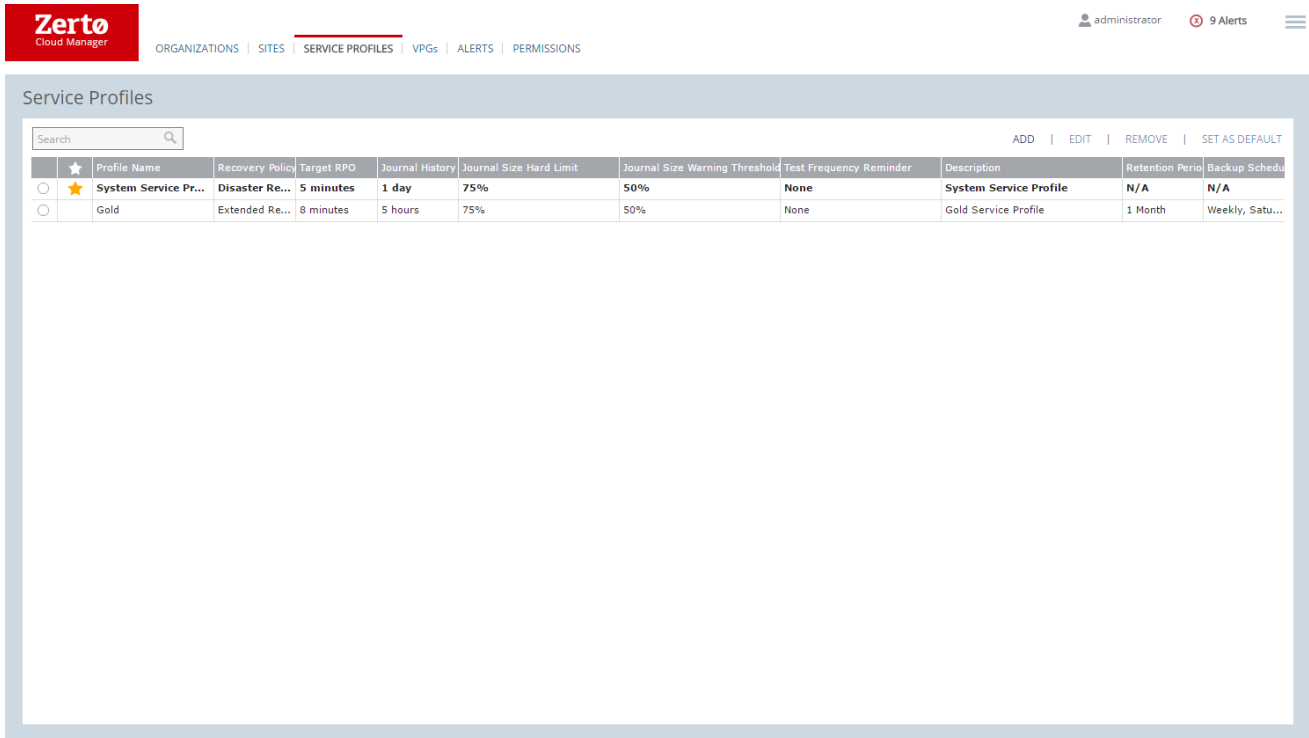
3. Specify the name of the service profile.
The default recovery policy is **Disaster Recovery**.
4. Select values for the service profile parameters.

- **DR Policy**

- **Target RPO Alert:** The maximum desired time between each automatic checkpoint being written to the journal before an alert is issued. In reality checkpoints are written more frequently.
- **Default Journal History:** The length of time all write commands are saved in the journal. Each protected virtual machine has a dedicated journal volume on the recovery site associated with the replicated virtual machine. This enables journal data to be maintained, even when changing the recovery host for the recovery. When specifying a checkpoint to recover to, the checkpoint must still be in the journal. For example, if the value specified here is 24 hours then recovery can be specified to any checkpoint in the last 24 hours. After the time specified, the mirror virtual disk volumes maintained by the VRA are updated.
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, with the same size as the journal for that virtual machine. The size of the scratch volume determines the length of time that you can test for. The larger the volume, the longer the testing can continue, assuming the same rate of change being tested. If the journal history required is small, for example two or three hours, the scratch volume that is created for testing will be small as well, limiting the time available for testing. Thus, when considering the journal history you should also consider the length of time you will want to test the VPG.
The longer the information is saved in the journal, the more space is required for each journal in the VPG.
- **Journal Size Hard Limit:** The maximum size that the journal can grow, as a percentage of the virtual machine volume size. The minimum is journal size is 8GB.
- **Journal Size Warning Threshold:** The size of the journal that triggers a warning that the journal is nearing its hard limit, as a percentage of the virtual machine volume size.
- **Test Frequency 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.

5. Click **SAVE**.

The new service profile is displayed.



6. After adding a service profile you can edit it by selecting the service profile and clicking **EDIT**.
7. You specify a service profile as the **default service profile** to be displayed when creating a VPG by selecting the service profile and clicking **SET AS DEFAULT**. The default service profile is identified by the yellow star next to its name.

Defining Role-based Access Control

By default, Zerto manages permissions that exist in the vCenter Server. When it is installed, Zerto adds privileges to vSphere and assigns these privileges to the Administrator role, which enables the administrator to perform specific actions in Zerto. These privileges include:

- **Manage VPG:** Creating, editing, and deleting a VPG, and adding checkpoints to a VPG.
- **Failover Test:** Performing a test failover.
- **Live Failover:** Performing failovers.
- **Move:** Performing VPG moves.
- **Manage cloud connector:** Installing and uninstalling Zerto Cloud Connectors (ZCCs). For details, see [Defining DRaaS Components](#).
- **Manage Sites:** Editing the site configuration, including site details, pairing and unpairing sites, updating the license, and editing advanced site settings.
- **Manage VRA:** Installing, updating and uninstalling Virtual Replication Appliances.
- **View:** Viewing information about an entity.

You can also set basic permissions for a ZORG, as described in [Defining ZORG Permissions](#).

If you want to extend these default permissions, you can activate Zerto role-based access control in the Zerto Cloud Manager. Zerto enables you to apply permissions to specific authorizable entities, such as ZORGs, VPGs, and sites, that you want to control access to. Privileges define an operation or a set of operations that can be performed, such as managing a VPG or VRA. A role is a set of privileges. Roles can be assigned to individual users or groups of users. Users and groups of users are defined in the local Active Directory. A permission is composed of an authorizable entity, a user or group, and a role.

Note: Once activated, the Zerto role-based access control replaces the basic permissions. If the Zerto role-based access control is deactivated, the default Zerto permissions are re-activated.

You can update the privileges associated with both new roles that you create and the roles supplied with Zerto. You can manage the permissions assigned to each Zerto authorizable entity. These permissions are defined in the Zerto Cloud Manager and affect the Zerto Virtual Manager sites defined in the Zerto Cloud Manager.

The following apply to Zerto role-based access control:

- The Zerto Cloud Manager and all the Zerto Virtual Manager sites defined in the Zerto Cloud Manager are defined in the same Active Directory domain. After you activate role-based access control, you must log in to the Zerto Virtual Manager sites defined in the Zerto Cloud Manager with the Active Directory domain user. If you deactivate role-based access control, when you log in to the Zerto Virtual Manager sites defined in the Zerto Cloud Manager, you must use the vCenter Server user again.
- All privileges are implemented at the Zerto Cloud Manager level. The levels are organized in a tree structure. For details of the levels, refer to [Managing Privileges, Roles, and Authorizable Entities](#).
- Users managing the Zerto Cloud Manager are a type of super user and Zerto-defined permissions do not limit the functions they can perform.
- A permission assigned to a child entity overrides the permission assigned to its parent entities.
- When users are assigned several permissions, or are members of several groups, they can perform all the functions associated with all those permissions and all those groups.
- Permissions apply both when using the Zerto User Interface and with Zerto APIs.

Enabling and managing **role-based access** is described in the following topics:

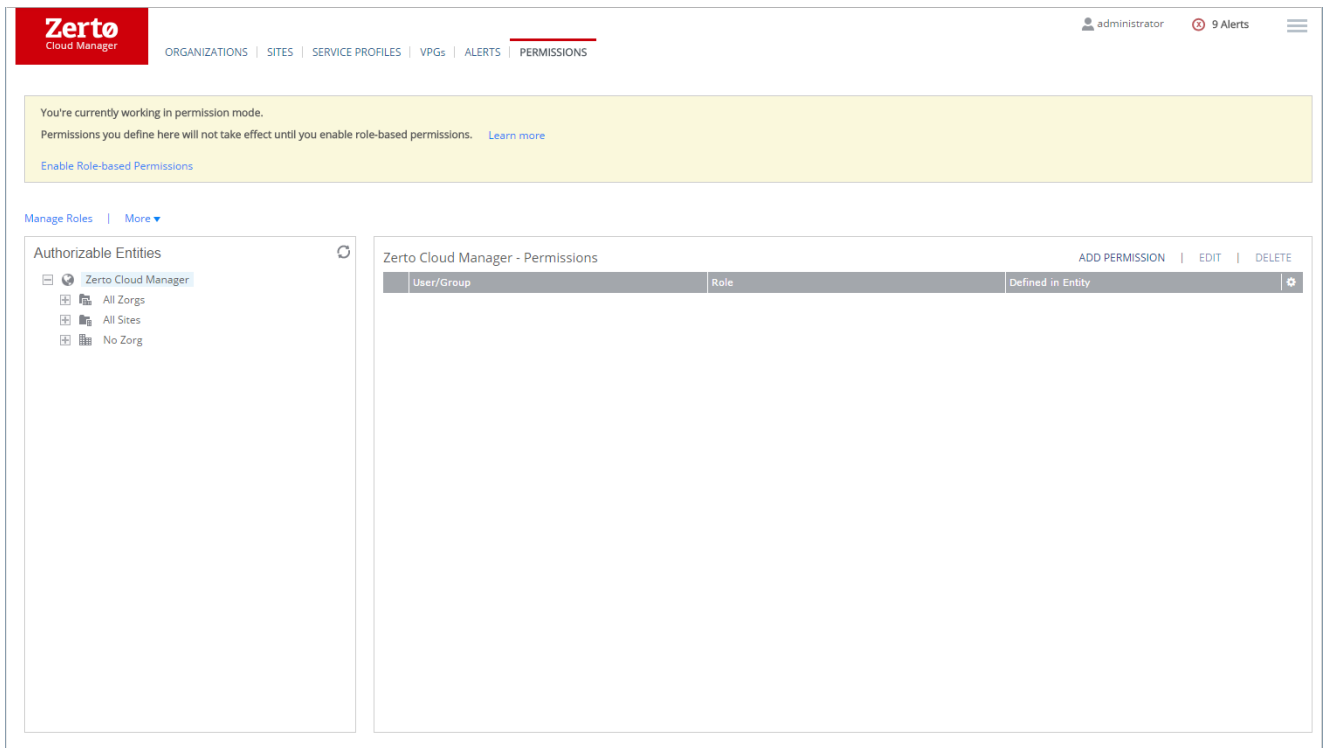
- [Enabling Role-based Permissions](#)
- [Managing Roles](#)
- [Managing Privileges, Roles, and Authorizable Entities](#)

Enabling Role-based Permissions

In addition to using Zerto basic permissions, you can enable Zerto role-based permissions.

To enable Zerto role-based permissions:

1. Make sure that the Zerto Cloud Manager and all the Zerto Virtual Manager sites defined in the Zerto Cloud Manager are defined in the same Active Directory domain.
2. In the Zerto Cloud Manager, select the **Permissions** tab.



3. Click **Enable Role-based Permissions**.
Zerto role-based permissions are enabled.
4. Once enabled, you must define roles and permissions as defined below, or access to Zerto, including to the user interface, is blocked.

See also

- [Managing Roles](#)
- [Managing Privileges, Roles, and Authorizable Entities](#)

Managing Roles

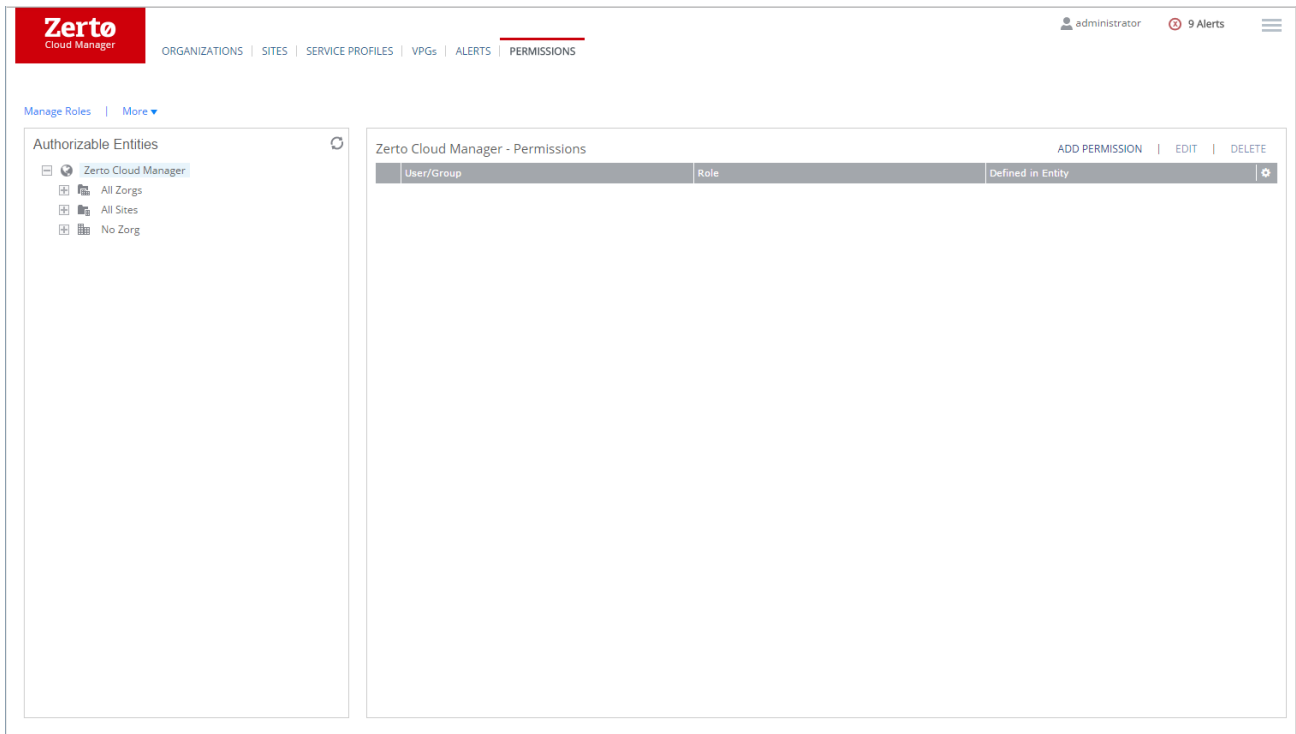
By default, Zerto contains several roles. You can create new roles, edit the privileges associated with a role, or delete roles. The following roles are provided by Zerto:

- **Admin:** Can perform all functions. These include performing a test failover, live failover, or move, managing cloud connectors, VPGs, VRAs, the protected and recovery sites, and viewing information.
- **Builder:** Can manage VPGs and view information.
- **User:** Can perform a test failover, live failover, or move, and view information.
- **Viewer:** Can view information provided by Zerto.

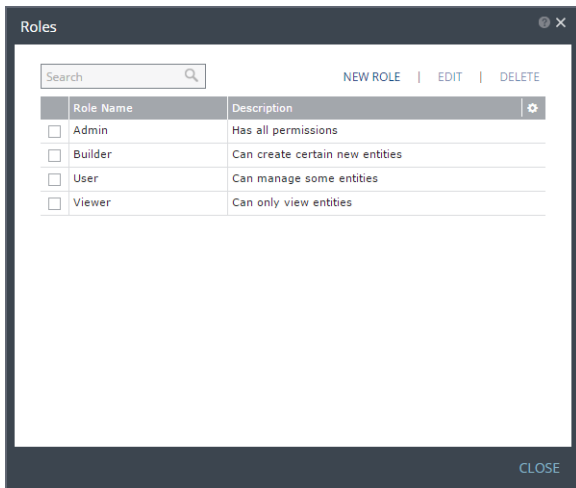
Note: Zerto extracts user information from the local Active Directory (AD) domain.

To create a new role:

1. Select the **Permissions** tab.

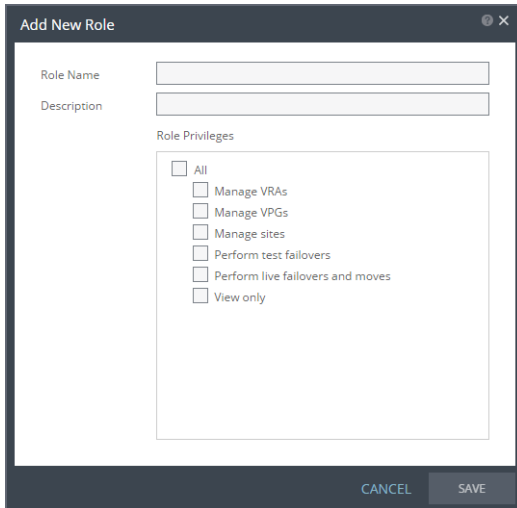


2. Click **Manage Roles**.
The Roles dialog is displayed.



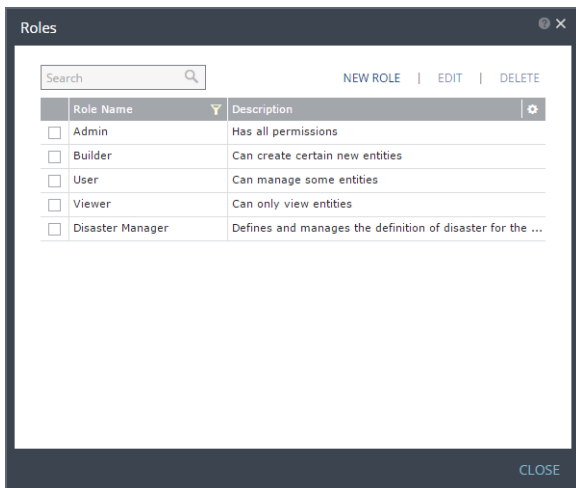
3. Click **NEW ROLE**.

The Add New Role dialog is displayed.



4. Enter the name of the new role and its description.
5. Select the privileges that will be assigned to the role.
6. Click **SAVE**.

The new role and its description is saved and displayed in the Roles dialog.



Every role includes the **View only** privilege. If it is not set, it is automatically added to the role when the role is saved.

7. Click **CLOSE**.

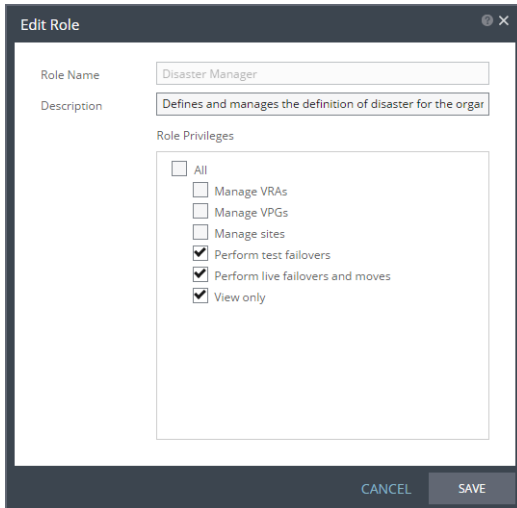
See also:

- [Enabling Role-based Permissions](#)
- [Managing Privileges, Roles, and Authorizable Entities](#)

To edit a role:

1. Select the **Permissions** tab.
2. Click **Manage Roles**.
The Roles dialog is displayed.
3. Select the role to edit and click **EDIT**.

The Edit Role dialog is displayed.



4. Update the role description or privileges.
Every role includes the View only privilege. If it is unset, it is automatically added to the role when the role is saved.
5. Click **SAVE**.
The updated role is saved and displayed in the Roles dialog.
6. Click **CLOSE**.

See also:

- [Enabling Role-based Permissions](#)
- [Managing Roles](#)
- [Managing Privileges, Roles, and Authorizable Entities](#)

To delete a role:

1. Select the **Permissions** tab.
2. Click **Manage Roles**.
The Roles dialog is displayed.
3. Select the role to delete and click **DELETE**.
4. In the warning, click **YES**.
The role is deleted and the Roles dialog is displayed again without the role.
5. Click **CLOSE**.

See also:

- [Enabling Role-based Permissions](#)
- [Managing Roles](#)
- [Managing Privileges, Roles, and Authorizable Entities](#)

Managing Privileges, Roles, and Authorizable Entities

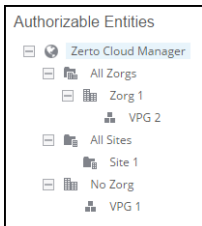
After Zerto role-based permissions has been enabled, the **Permissions** tab displays entities within the Zerto Cloud Manager, the users and groups within an entity, and the roles they have been assigned. Zerto recommends that you assign certain privileges to certain entities. The following table shows which privileges can affect specific entities.

THESE PRIVILEGES...	CAN AFFECT THESE ENTITIES
Manage sites and Manage VRAs	Zerto Cloud Manager One, some, or all sites
Manage VPGs, Perform test failovers, Perform live failovers and moves	Zerto Cloud Manager One, some, or all ZORGs and the No ZORG entity
View only	All VPGs

The entities are:

- **Zerto Cloud Manager:** The root of all entities. Permissions assigned to the Zerto Cloud Manager are, by default, assigned to all entities.
- **All sites:** Permissions assigned to the entity All Sites are, by default, assigned to all sites.
- **A specific site:** A particular site with permissions assigned to it.
- **All ZORGs:** Permissions assigned to the entity All ZORGs are, by default, assigned to all ZORGs.
- **A specific ZORG:** A particular ZORG with permissions assigned to it. By default, all of the permissions assigned to this ZORG are assigned to the VPGs that are associated to this ZORG.
- **No ZORG:** This category represents VPGs that are not associated with a ZORG. Permissions assigned to the entity No ZORG are, by default, assigned to all VPGs that are not associated with a ZORG.
- **A specific VPG:** A particular VPG with permissions assigned to it.

The entities are displayed as follows:



Certain functions are site level functions and other functions are VPG level functions, as follows:

Site Level Functions
Manage sites
Pair sites
Unpair sites
Manage a VRA
Create a VRA
Edit a VRA
Delete a VRA
Upgrade a VRA
Change the recovery VRA of a VM
Change host password

VPG Level Functions
Manage a VPG
Create a VPG
Edit a VPG
Delete a VPG
Export a VPG
View VPGs
Test failover a VPG
Stop a failover test
Move a VPG
Failover a VPG
Back up a VPG
Stop a backup
Add a checkpoint

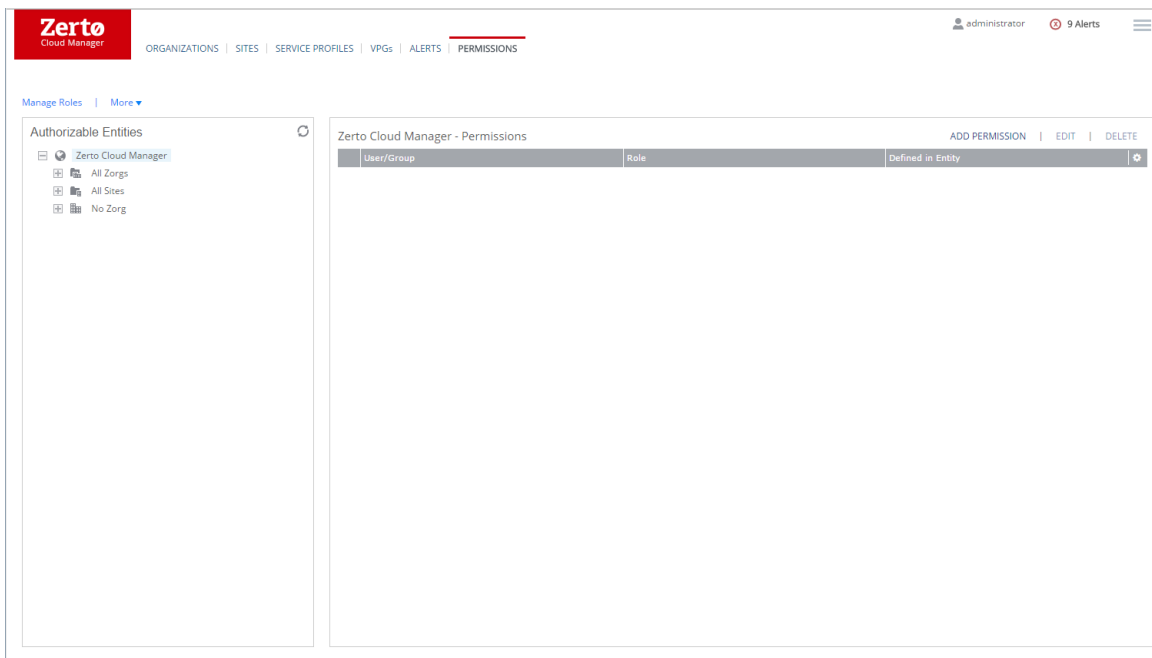
[To define user or group permissions](#)

[To edit user or group roles and permissions](#)

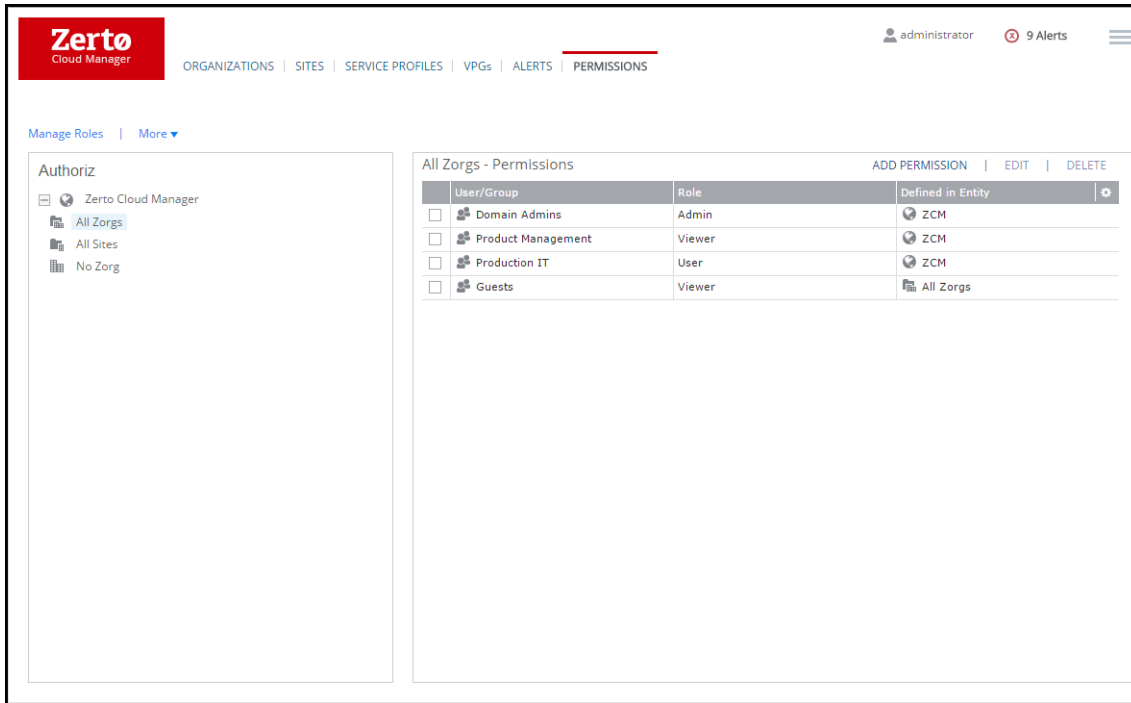
[To delete a permission from a user or group](#)

To define user or group permissions

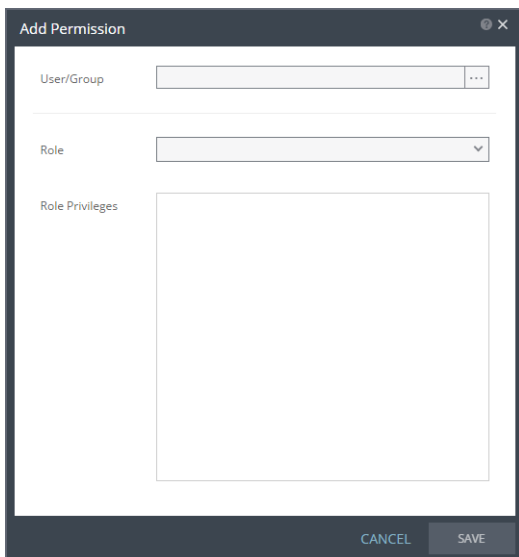
1. Select the **Permissions** tab.



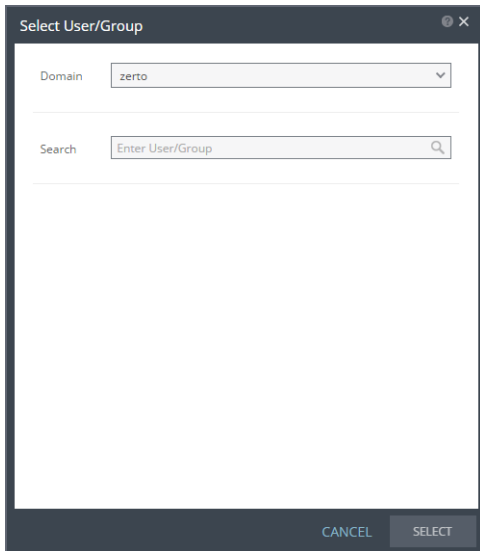
2. Click a Zerto entity to display its users and groups, and the roles assigned to them.



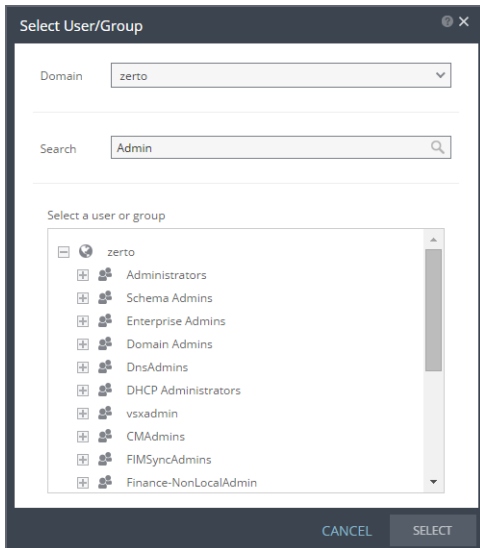
3. To add permissions to a user or group, click **ADD PERMISSION**.
The Add Permission dialog is displayed.



4. Browse to the available users and groups in the local Active Directory.
The Select User/Group dialog is displayed.

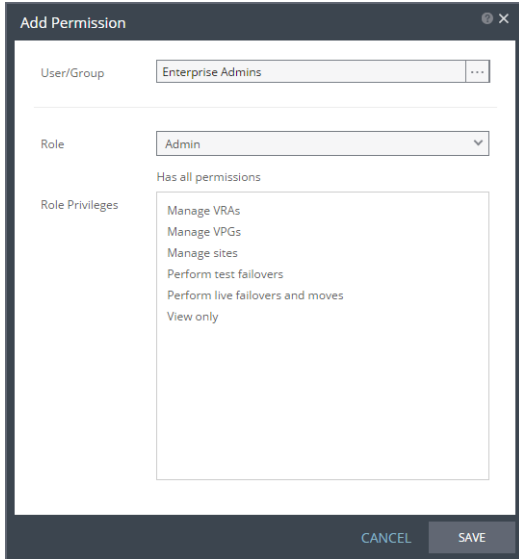


5. Select the domain and enter at least two characters in the **Search** field.
6. Click **Enter** to display the list of users and groups in the domain that meet your search criteria.



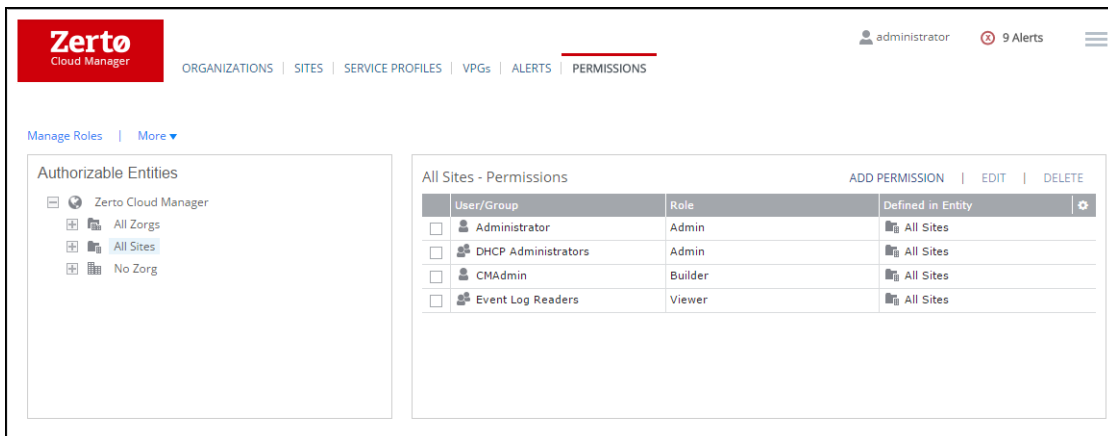
7. Select the user or group to which you want to add permissions and click **SELECT**.
The Add Permission dialog is displayed.
8. Select the role to be assigned to the user or group.

The privileges associated with the role are displayed.



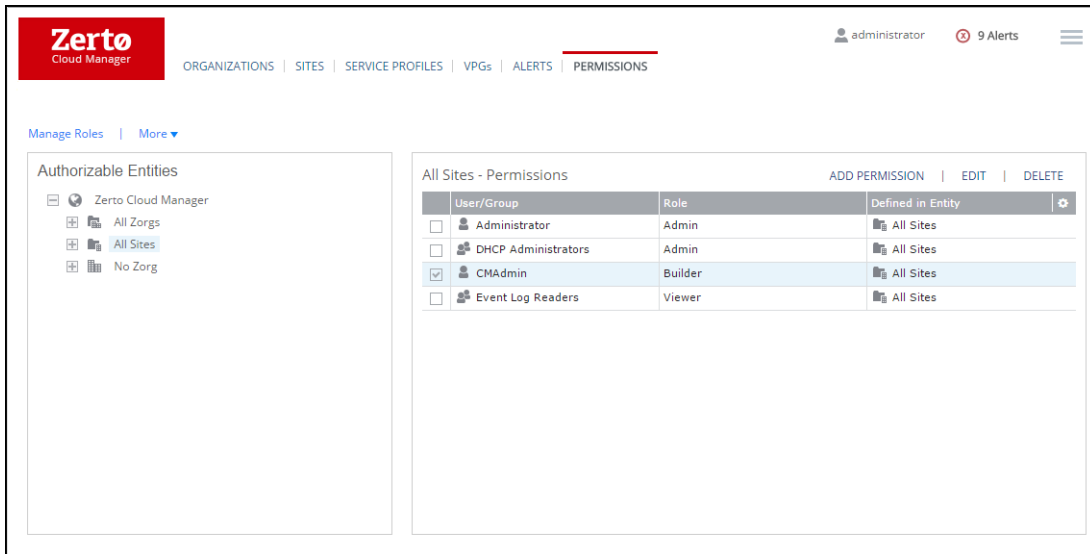
9. Click **SAVE**.

The updated list of users and groups and their roles is displayed.

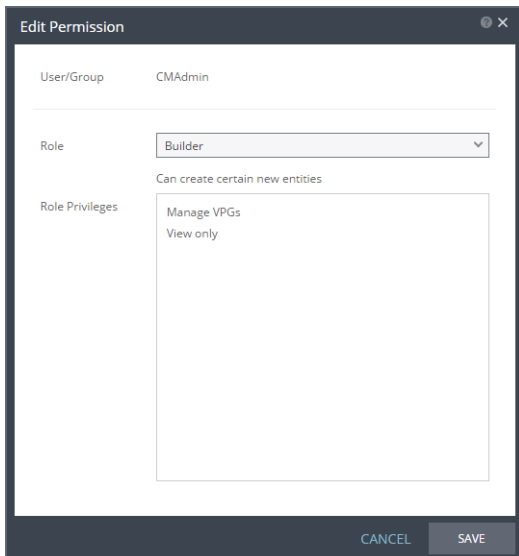


To edit user or group roles and permissions

1. Select the **Permissions** tab and then select the entity that contains the user or group you want to edit.
Note: You can only edit a permission in the entity to which it was defined, and not on its child entities
2. Select the user or group within the entity whose permissions you want to edit.



3. Click **EDIT**.
The Edit Permission dialog is displayed.



4. Select the role to assign to the user or group and click **SAVE**.
The updated role of the user or group is displayed.

To delete a permission from a user or group

1. Select the **Permissions** tab and then select the authorizable entity that contains the user or group with a permission you want to delete.
2. Select the user or group within the entity with a permission you want to delete.

The screenshot shows the Zerto Cloud Manager interface. At the top, there is a navigation bar with the Zerto logo and the text 'Cloud Manager'. To the right of the logo, there are navigation links: ORGANIZATIONS, SITES, SERVICE PROFILES, VPGs, ALERTS, and PERMISSIONS. The current user is 'administrator' and there are '9 Alerts'. Below the navigation bar, there is a 'Manage Roles' section with a 'More' dropdown. The main content area is divided into two panels. The left panel is titled 'Authorizable Entities' and contains a tree view with the following items: Zerto Cloud Manager, All Zorgs, All Sites (selected), and No Zorg. The right panel is titled 'All Sites - Permissions' and contains a table with the following columns: User/Group, Role, and Defined in Entity. The table has the following rows:

	User/Group	Role	Defined in Entity	
<input type="checkbox"/>	Administrator	Admin	All Sites	
<input type="checkbox"/>	DHCP Administrators	Admin	All Sites	
<input checked="" type="checkbox"/>	CMAAdmin	Builder	All Sites	
<input type="checkbox"/>	Event Log Readers	Viewer	All Sites	

3. Click **DELETE**.
A warning is displayed that asks you to confirm the delete.
4. Click **YES**.
The permission assigned to the user or group is removed.

Customers requiring DRaaS use the following procedure to set up their sites to enable connecting to the cloud service provider offering DRaaS:

1. Install Zerto on each customer site where there are virtual machines that need protecting.
2. Install VRAs.

For details about installing **Zerto** and **VRAs**, refer to the *Zerto Virtual Replication Installation Guide*.

The cloud service provider does the following:

1. Defines the customer in Zerto Cloud Manager as a Zerto organization, ZORG, as described in [Setting Up DRaaS](#).
2. Defines a Zerto Cloud Connector for the ZORG to secure the cloud service provider networks from the customer network and to secure each customer network from other customer networks, as described in [Setting Up DRaaS](#).

The customer pairs to the cloud service provider, using the IP address used in the definition of the Zerto Cloud Connector.

IMPORTANT:

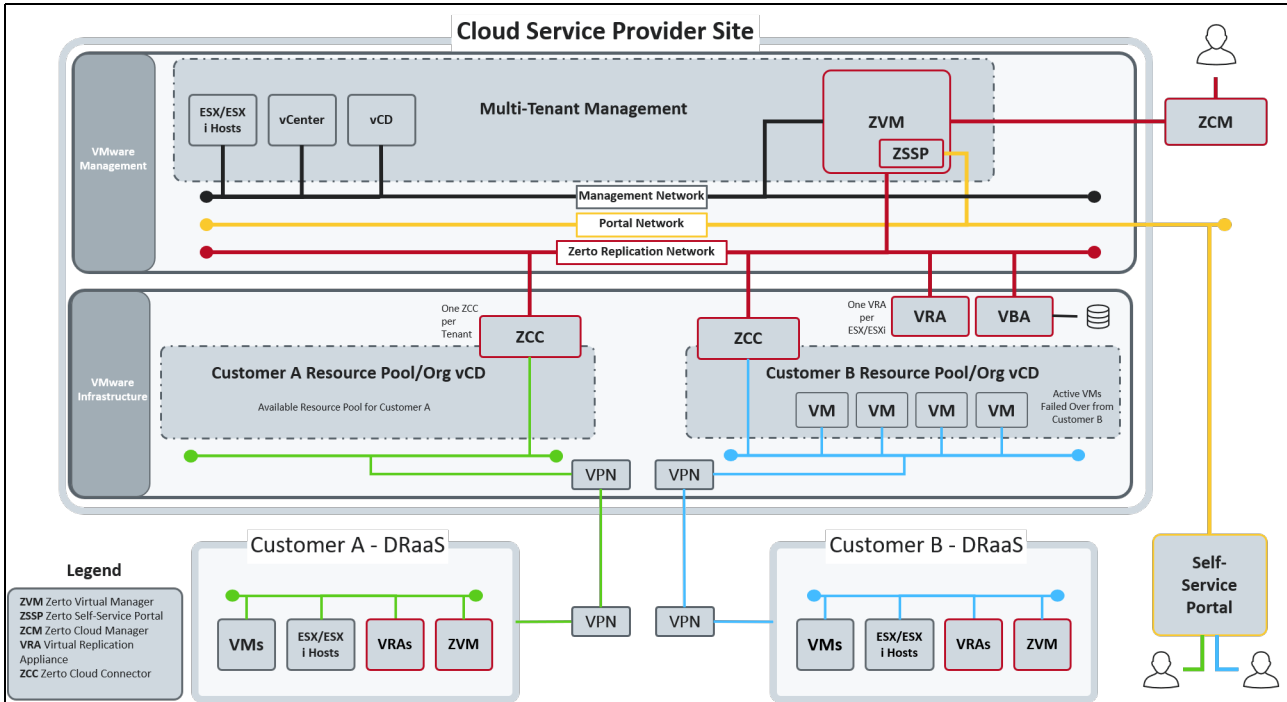
The CSP must pair their customer's ZVMs with the IP address of their ZCC in order to view the sites within **Zerto Cloud Control** and **Zerto Analytics**.

The customer can manage disaster recovery in one of the following ways:

- Via the Zerto User Interface, described in *Zerto Virtual Manager Administration Guide*.
- Via the Zerto Self-service Portal, described in [Setting Up DRaaS](#).

Note: In case of a disaster, when a failover is required, the customer must use the Zerto Self-service Portal to access the cloud service provider recovery site in order to perform the failover, or request that the cloud service provider perform the failover. In either case, the customer needs access to the recovery site to continue operations with the recovered virtual machines.

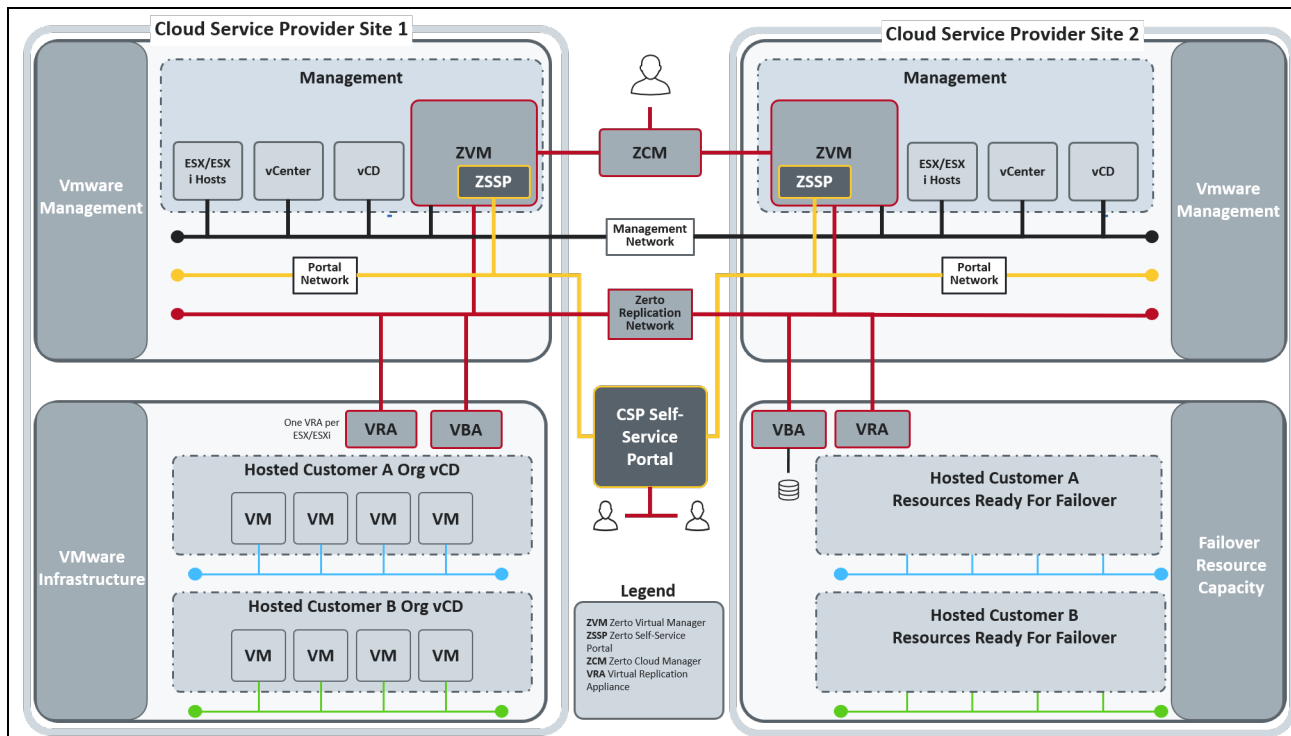
The following diagram shows the basic architecture when the cloud service provider provides disaster recovery as a service for the customer (DRaaS). In this case the customer uses a VMware vSphere environment but it could also use a Microsoft SCVMM environment.



Cloud service providers (CSPs) that manage IT infrastructure for customers require a way for the customer to interface with their IT environment. In addition, some CSP services required by the customer also require direct customer interaction. This requires that both the CSP and the customer have infrastructure level access. One way of providing this access is via a CSP portal open to the customer.

When the CSP provides Zerto as one of its services, it can include the Zerto Self-service Portal (ZSSP) in its portal offerings. The ZSSP portal enables customers to manage their recovery based on their SLA with the CSP. If the CSP does not provide a portal for other services, the ZSSP can be used as a standalone portal to enable customers to manage their disaster recovery.

The Zerto Self-service Portal is an out-of-the-box disaster recovery portal solution with a fully functioning browser-based service portal to enable cloud service providers to quickly introduce disaster recovery using Zerto. The following diagram illustrate the basic architecture when the cloud service provider hosts both the protected and recovered virtual machines on behalf of the customer, using *In Cloud Disaster Recovery (ICDR)*.



When the CSP offer DRaaS, the Zerto Self-service Portal enables the customer to access the cloud service provider recovery site in order to perform the failover instead of requesting that the cloud service provider perform the failover. Whether the customer instigates the failover or requests that the CSP performs the recovery, the customer needs access to the recovery site to continue operations with the recovered virtual machines.

See the following sections:

- [Setting Up Access to the Zerto Self-service Portal](#)
- [Security](#)
- [Branding the Zerto Self-service Portal](#)

Setting Up Access to the Zerto Self-service Portal

The cloud service provider must perform a number of steps, including the preliminary set-up of the customer in the Zerto Cloud Manager in order to give the customer access to the Zerto Self-service Portal (ZSSP). Each time a customer logs in to the ZSSP, a unique session is allocated with access only to data that is relevant to the customer.

The ZSSP is served by a specific Zerto Virtual Manager. If the customer needs access to a second cloud site, access to the ZSSP must be changed to use the Zerto Virtual Manager of the second site.

Access to the ZSSP can be as a standalone portal or integrated within a portal used by the cloud service provider.

[Access the Zerto Self-service Portal as a Standalone Portal](#)

[Access the Zerto Self-service Portal by integrating it in a Cloud Service Provider Portal](#)

Access the Zerto Self-service Portal as a Standalone Portal

When the Zerto Self-service Portal is accessed directly, the ZORG name, username, and password, specified by the cloud service provider for the ZORG, are required to log on to the Zerto Self-service Portal.

To set up access to the ZSSP as a standalone portal:

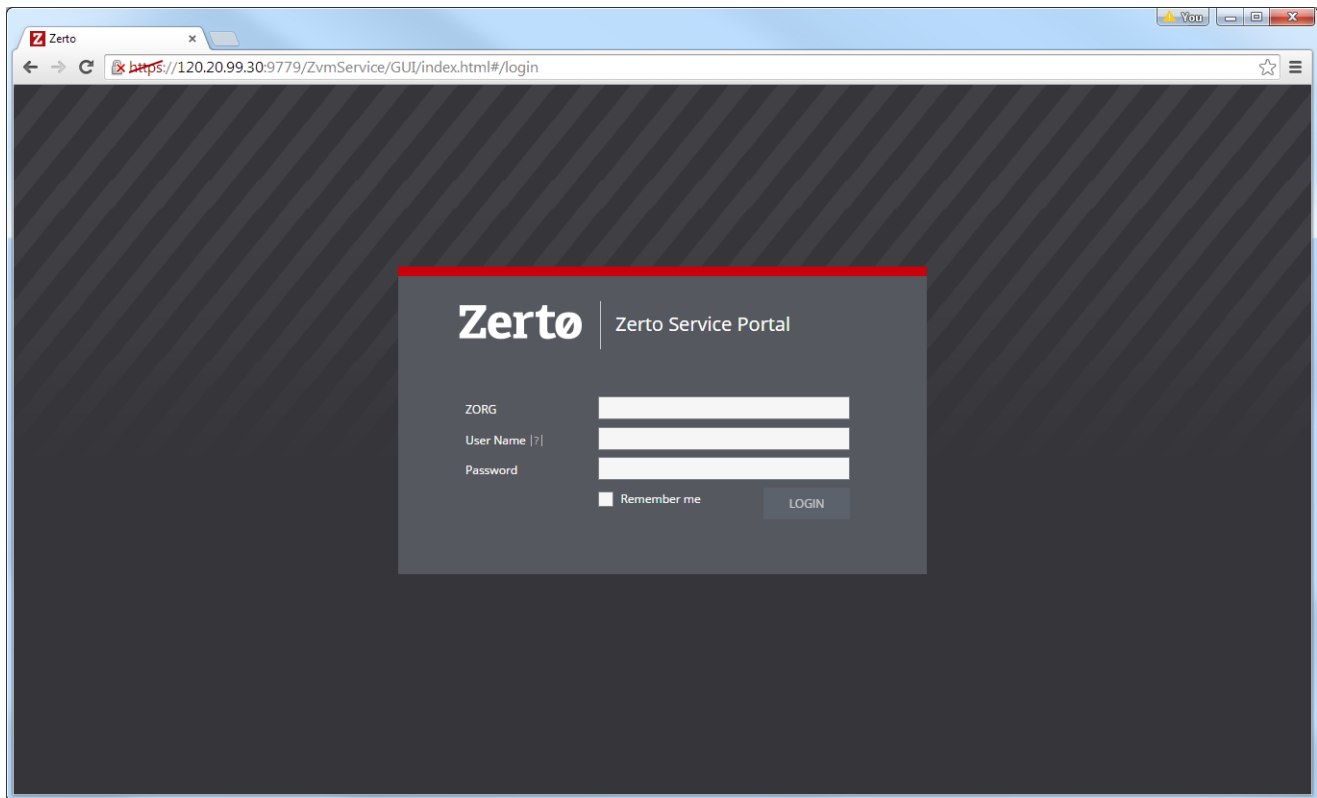
1. Using the Zerto Cloud Manager, set up the customers as Zerto Organizations, referred to as ZORGs.
Each ZORG is defined with its own SLA requirements within Zerto Cloud Manager, as described in [“Setting Up Zerto Organizations, ZORGs”](#), on page 28.
2. Specify a username and password for the ZORG in the Zerto Cloud Manager, as described in [“Defining ZORG Permissions”](#), on page 31.

Running the Zerto Self-service Portal Directly

The ZORG name, username, and password, specified by the cloud service provider for the ZORG, are required to log on to the Zerto Self-service Portal before the ZSSP **VPGs** tab is displayed. The customer logs on to the ZSSP with the following URL:

https://ZVM_IP:9779

where ZVM_IP is the IP of the Zerto Virtual Manager cloud site.



Access the Zerto Self-service Portal by integrating it in a Cloud Service Provider Portal

When the Zerto Self-service Portal is integrated within a cloud service provider portal, a session URL is used to access the CSP portal. The session URL is the URL text returned, as described in step 3 in the following procedure.

To set up access to the ZSSP when integrated in a Cloud Service Provider portal:

When the ZSSP is integrated in the cloud service provider portal, either as separate pages or as an iFrame inside an existing page of the cloud service provider portal, it is assumed that the security governing access to the cloud service provider portal will cover the additional access to the ZSSP pages when the ZSSP is incorporated in the cloud service provider portal.

1. Using the Zerto Cloud Manager, set up the customers as Zerto Organizations, **ZORGs**. Each ZORG is defined with its own SLA requirements within Zerto Cloud Manager, as described in [“Setting Up Zerto Organizations, ZORGs”](#), on page 28.
2. Determine the public address the customer will browse to in order to work with the ZSSP. The address needs to be resolved and directed to the Zerto Virtual Manager used to protect the virtual machines or the proxy server and from there to the Zerto Virtual Manager. For example, if the relevant Zerto Virtual Manager or Proxy IP is 10.0.0.138, you can determine that the public address can be `https://www.example.com`. However, this site needs to be resolved in the DNS on the customer browsers to 10.0.0.138.

Note: When recovery is implemented or for the customer to test and verify that recovery works as expected, the address used by the customer to access the ZSSP must be changed to enable accessing the recovery site. Also, access to the test virtual machines on the recovery site must be provided.

For more details about using a proxy server for additional security, see [Security](#).

3. Provide a mechanism so the customer can use the following URL to create the session URL text:

```
https://zvm_ip:port/v1/zsspSessions.
```

For more information about ZSSP APIs, see Zerto Virtual Replication RESTful APIs, in the section ZSSP Sessions API.

4. Provide a mechanism to take the unique session URL text generated in step 3 and redirect the customer to browse to this URL. For example, implement basic code on the backend, cloud service provider portal application server, or by simple javascript on the page itself.

To implement the redirection you must incorporate the URL text returned within the XML string into the URL the customer uses to access the CSP portal.

Running the Zerto Self-service Portal When Integrated in a Cloud Service Provider Portal

When the Zerto Self-service Portal is integrated in a cloud service provider (CSP) portal, a URL is used to return a session unique URL text which is then used to access the ZSSP. The session URL is similar to the following:

```
"https://address:port/ZvmService/GUI/Index.html#/  
?type=Portal&locale=en_US&sessionId=zsspSessionId"
```

Where:

address	The public address the customer will browse to in order to access the CSP's portal. For example: https://www.example.com
port	The port to access the CSP portal. The default port is 9669.
zsspSessionIdentifier	The identifier of the ZSSP session.

For more information about ZSSP APIs, see Zerto Virtual Replication RESTful APIs, in the section ZSSP Sessions API.

Security

The Zerto Self-service Portal is accessed by a URL that is session dependent and the connection is terminated at the end of the session, when the user logs out. The URL cannot be reused. The session also expires after 10 minutes of inactivity.

Note: The default timeout can be changed by contacting Zerto Support.

When the Zerto Self-service Portal is integrated within a cloud service provider portal the access URL is session dependent and unique to each ZORG and requires an SSL connection before it can be created. These combined requirements effectively provide multiple layers of security to ensure customer isolation.

When the Zerto Self-service Portal is accessed directly, the ZORG name, username, and password, specified by the cloud service provider for the ZORG, are required to log on to the Zerto Self-service Portal.

See the following:

[Zerto Self-service Portal integrated with the cloud service provider portal and using a reverse proxy](#)

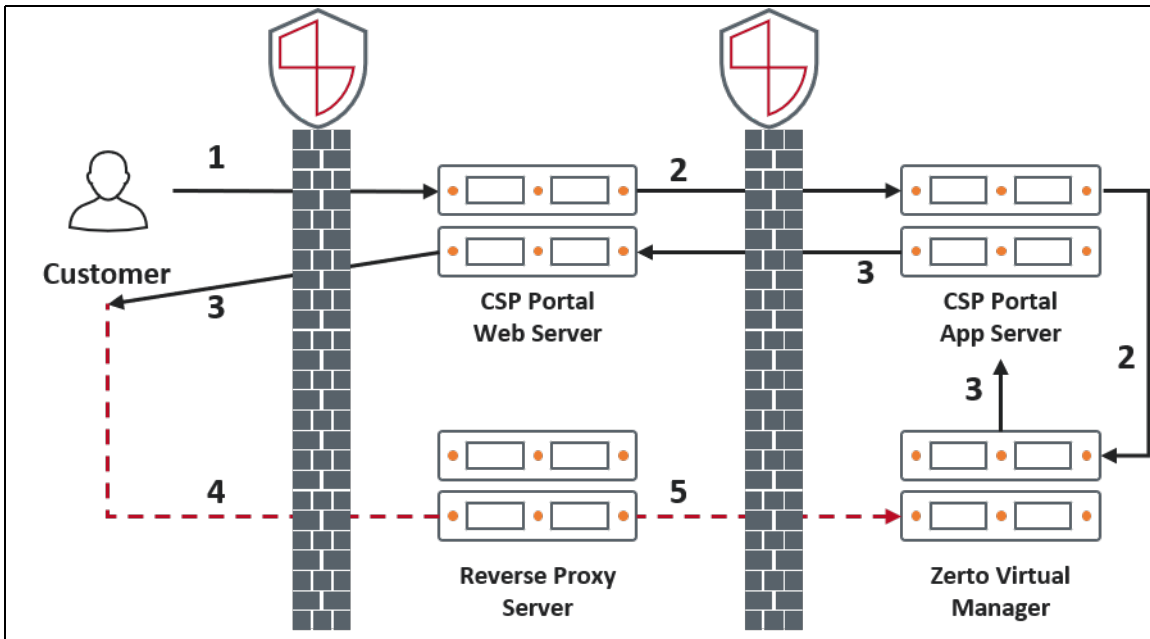
[Zerto Self-service Portal integrated with the cloud service provider portal without a reverse proxy](#)

[Zerto Self-service Portal accessed directly, with a reverse proxy](#)

[Zerto Self-service Portal accessed directly, without a reverse proxy](#)

The following diagrams show the user accessing the Zerto Self-service Portal:

Zerto Self-service Portal integrated with the cloud service provider portal and using a reverse proxy



Where:

1. In the cloud service provider portal, access the BC/DR functionality via a button/iFrame.
2. Internally, using HTTPS, retrieve the ZSSP session, as described in step 3, in [To set up access to the ZSSP when integrated in a Cloud Service Provider portal.](#)
3. Return the session link text as a custom URL.
4. Browse to the custom URL to access the unique session.
5. Access the unique session using HTTPS and port 9779.

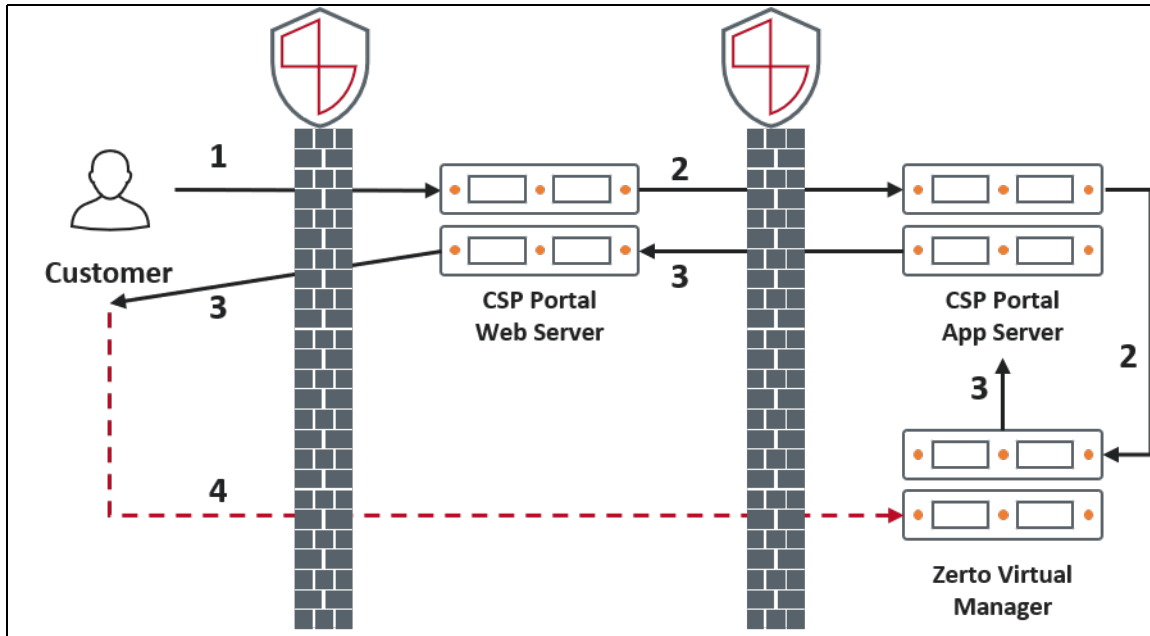
See also:

[Zerto Self-service Portal integrated with the cloud service provider portal without a reverse proxy](#)

[Zerto Self-service Portal accessed directly, with a reverse proxy](#)

[Zerto Self-service Portal accessed directly, without a reverse proxy](#)

Zerto Self-service Portal integrated with the cloud service provider portal without a reverse proxy



Where:

1. In the cloud service provider portal, access the BC/DR functionality via a button/iFrame.
2. Internally, using either HTTP or HTTPS, retrieve the ZSSP session:
For more information about ZSSP APIs, see Zerto Virtual Replication RESTful APIs, in the section ZSSP Sessions API.
3. Return the session link text as a custom URL.
4. Browse to the custom URL to access the unique session using HTTPS and port 9779.

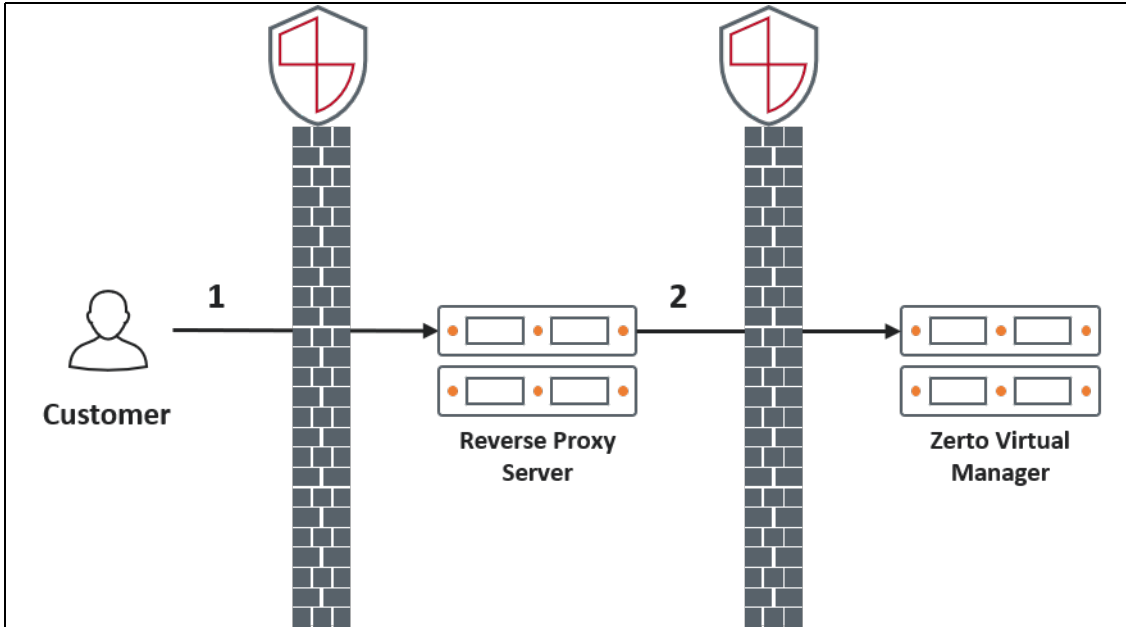
See also:

[Zerto Self-service Portal integrated with the cloud service provider portal and using a reverse proxy](#)

[Zerto Self-service Portal accessed directly, with a reverse proxy](#)

[Zerto Self-service Portal accessed directly, without a reverse proxy](#)

Zerto Self-service Portal accessed directly, with a reverse proxy



Where:

1. Pass the link to the reverse proxy server:
`https://ZVM_IP:9779`, where **ZVM_IP** is translated to the IP of the Zerto Virtual Manager cloud site.
2. Zerto Virtual Manager returns the Zerto Self-service Portal login page.

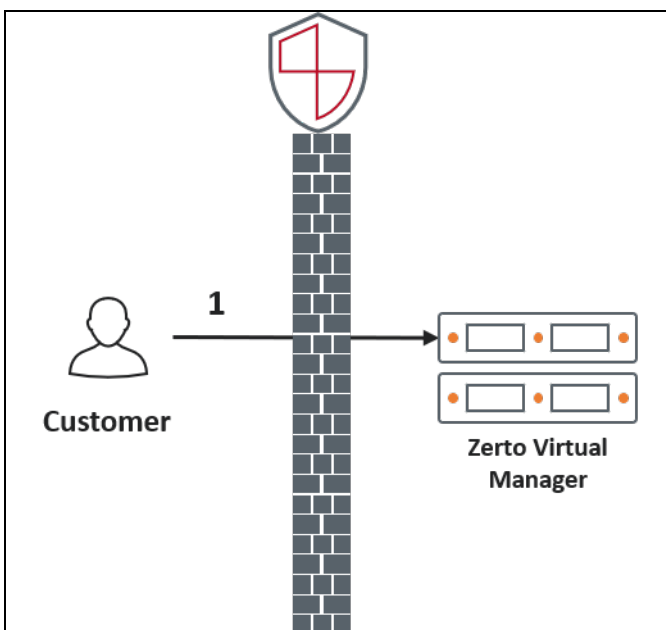
See also:

[Zerto Self-service Portal integrated with the cloud service provider portal and using a reverse proxy](#)

[Zerto Self-service Portal integrated with the cloud service provider portal without a reverse proxy](#)

[Zerto Self-service Portal accessed directly, without a reverse proxy](#)

[Zerto Self-service Portal accessed directly, without a reverse proxy](#)



Where:

- Access the ZSSP via the following URL: https://ZVM_IP:9779, where **ZVM_IP** is the IP of the Zerto Virtual Manager cloud site.

When a reverse proxy is used, a proxy server retrieves resources on behalf of the customer from one or more servers. The customer requests are forwarded by the proxy server to the Zerto Virtual Manager. Using a reverse proxy enables customers to keep the Zerto Virtual Manager secured with internal access only, and exposes only the reverse proxy server, on a preferred port.

Additional security can be implemented as follows:

- By making sure that port 9779 is the only port exposed to the proxy server.
- By setting up NAT redirection of the customer traffic, to protect the Zerto Virtual Manager and network from being exposed to the customer directly.

See also:

[Zerto Self-service Portal integrated with the cloud service provider portal and using a reverse proxy](#)

[Zerto Self-service Portal integrated with the cloud service provider portal without a reverse proxy](#)

[Zerto Self-service Portal accessed directly, with a reverse proxy](#)

Branding the Zerto Self-service Portal

The Zerto Self-service Portal can be branded by replacing the Zerto logo, both in the login page and the user interface after logging in.

To change the Zerto Self-service Portal login page logo:

- Overwrite the `<ZertoInstallFldr>\Zerto\Zerto Virtual Replication\gui\cloudLogoLogin.png` file with the logo of your choice.
Regardless of the size of the new logo, it is scaled to fit a maximum size of 136*45 pixels.
The `ZertoInstallFldr` is the root folder where Zerto is installed. For example, `C:\Program Files\Zerto`.

To change the Zerto Self-service Portal user interface page logo:

- Overwrite the `<ZertoInstallFldr>\Zerto\Zerto Virtual Replication\gui\cloudLogo.png` file with the logo of your choice.
Regardless of the size of the new logo, it is scaled to fit a maximum size of 110*80 pixels.
The `ZertoInstallFldr` is the root folder where Zerto is installed. For example, `C:\Program Files\Zerto`.

Separate documentation for customers that describes how to use the Zerto Self-service Portal is available for branding. It is distributed as Microsoft Word or RTF files.

There are a number of management tasks that you can perform in the Zerto Cloud Manager.

The following topics are described in this section:

- [Setting VMware Permissions](#)
- [Managing All Sites](#)
- [Managing a Specific Site](#)
- [“Managing a ZORG”, on page 70](#)
- [Editing Zerto Cloud Manager Definitions](#)
- [Resolving Zerto Cloud Connector Issues](#)

Initial and on-going configuration of Zerto Cloud Manager is described in [“Configuring a Zerto Cloud Manager”, on page 15](#). During day-to-day operations you can add new organizations and manage existing organizations, for example, adding vCenter resources, or changing the permissions for an organization, as well as add new cloud sites and service profiles to the Zerto Cloud Manager.

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

Zerto Cloud Manager includes access to the Zerto User Interface to manage the Zerto Virtual Manager as described in the Zerto Virtual Manager Administration Guides. Management tasks for ' include the following:

- Protecting virtual machines in VPGs, both to a vCenter Server and to vCloud Director.
- Managing an existing VPG, for example, by adding or removing a virtual machine, editing the VPG definition, pausing protection, adding checkpoints, and running recovery scripts for a VPG.
- Managing VRAs and Zerto Virtual Managers including handling host maintenance.
- Testing the recovery of virtual machines.
- Moving and failing over a VPG.

Setting VMware Permissions

Zerto supplies a number of permissions that enable a VMware administrator to perform specific actions. One of these permissions is Manage cloud connector, which enables installing and uninstalling Zerto Cloud Connectors. The permission is assigned to the Administrator role when Zerto Virtual Manager is installed. You can define additional roles and assign some or all permissions to these roles, as necessary. All permissions are implemented at the root level, and thus apply to every object in the vCenter Server.

These permissions are the minimum default permissions supplied by Zerto. For details, refer to [“Defining ZORG Permissions”, on page 31](#). You can manage an extended set of permissions for specific entities such as ZORGs, VPGs, and sites, as described in [“Defining Role-based Access Control”, on page 42](#).

Managing All Sites

You can monitor the VPGs and alerts for all cloud sites and ZORGs defined in the Zerto Cloud Manager.

See also:

- [Zerto Cloud Manager VPGs](#)
- [Zerto Cloud Manager Alerts](#)

Zerto Cloud Manager VPGs

All VPGs protected or recovered to a cloud site can be monitored from the Zerto Cloud Manager **VPGs** tab.

△	Direction	Peer Site	ZORG	Name	Protection Status	State	Priority	# VMs	Last Test
✓	⇐	siteA	ABC Company, Inc.	Clients	Meeting SLA		●●○	4	
✓	⇐	siteC	ABC Company, Inc.	Forex Trading	Meeting SLA		●●○	1	
✓	⇐	NYC	ABC Company, Inc.	Operations	Meeting SLA		●●○	1	
✓	⇐	siteA		Reconciliation - Back Office	Meeting SLA		●●○	1	

By clicking the VPG name link you can also drill down to details of the VPG and perform operations on the VPG such as adding a checkpoint. You can also initiate a Test Failover, Failover, or Move operation.

The screenshot shows the Zerto Cloud Manager interface for a VPG named 'Forex - back office'. The top navigation bar includes 'ORGANIZATIONS | SITES | SERVICE PROFILES | VPGs | ALERTS | PERMISSIONS | Paris'. The main dashboard features several panels: a 'MEETING SLA' panel with a green checkmark and a value of 9; 'PROTECTED VMs' showing 2 VMs and 1.8 GB protected; 'SITES' showing Site6-Ent2-R2 and Site4-Ent2-P1; 'SETTINGS' with Priority MEDIUM and Profile CUSTOM; 'SLA' and 'IOPS' line graphs; 'THROUGHPUT (MB/sec)' and 'WAN TRAFFIC (MB/sec)' line graphs; 'JOURNAL HISTORY' showing SLA = 4 hr and a 04:03 hr timer; 'OFFSITE BACKUP' status as DISABLED; and 'ACTINO ACTIVE ALERTS' and 'EVENTS' lists. At the bottom, there are status indicators for 'SITE IS OK', 'NO RUNNING TASKS', and 'ACTIONS', along with 'LIVE TEST' and 'FAILOVER' buttons.

You can view the current and recent activities of the VPG by looking at the list of running tasks and recent events in the panel on the right side.

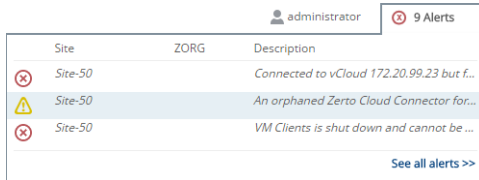
Zerto Cloud Manager Alerts

The alerts for all the sites defined to the Zerto Cloud Manager are displayed in the **Alerts** tab.

The screenshot shows the 'Alerts' tab in Zerto Cloud Manager. It features a search bar, a 'Display Acknowledged Alerts' checkbox, and a table of alerts. The table has columns for Alert ID, Entity, Description, Site Name, VPGs, ZORG, and Timestamp. The alerts listed include connection issues, RPO exceedances, VM client shutdowns, service profile changes, and orphaned connectors.

Alert ID	Entity	Description	Site Name	VPGs	ZORG	Timestamp
ZVM0003	ZVM	The Zerto Virtual Manager is not connected to site Site-9 (172.20.99.9:9081),	Site-50	Paris		31/08/2016 10:46...
ZVM0001	ZVM	The connection between site Site-9 and the hypervisor manager Pending vCenter connection at 0.0.0.0 is down.	Site-50	Paris		31/08/2016 10:09...
VPG0010	VPG	VPG Paris exceeds configured RPO of 5 minutes by more than 25%.	Site-50	Paris		31/08/2016 09:32...
VRA0020	ZVM	VM Clients is shut down and cannot be synced.	Site-50	Paris		31/08/2016 09:19...
VRA0020	ZVM	VM Operations (Site 5) is shut down and cannot be synced.	Site-50	Paris		31/08/2016 09:19...
VPG0026	VPG	The service profile you use in VPG Paris has been changed by your cloud provider.	Site-50	Paris		31/08/2016 09:04...
ZVM0002	VRA	Zerto Virtual Manager is not connected to VRA with IP fe80::250:56ff:fea9:2cdb on host 172.20.99.7.	Site-50			31/08/2016 09:04...
ZCC0003	Cloud Connector	An orphaned Zerto Cloud Connector for Site-50_B-Net_01 was installed.	Site-50			31/08/2016 09:04...
VCD0015	ZVM	Connected to vCloud 172.20.99.23 but failed to connect to AMQP-server for notifications. Last connection error: \None of the specified endpoints were	Site-50			31/08/2016 09:04...

Note: You can click the alerts status indicator in the Zerto Cloud Manager main screen to view the three most recent alerts.



Click **See all alerts >>** to open the Zerto Cloud Manager **Alerts** tab.

Note: To see alerts for an individual site, click on the site link in the Zerto Cloud Manager **Sites** tab, then in the Zerto Virtual Manager tabs, click **Monitoring > ALERTS**.

Warnings are indicated by the orange icon and alerts by the red icon. The information displayed includes the VPG name, the name of the entity that triggered the alert, the date and time the alert was issued, and a description of the alert.

The alert status indicator at the top shows the color for the most severe alert that is currently valid. After the alert has been resolved, the alert is removed from the Alerts tab and the alert status indicator changes, if appropriate, to show the new alert status.

You can filter all the columns with a filter icon. Click the filter icon to enter the value to filter by. The filter icon becomes visible when a filter is applied. Click **Clear** in the filter field to clear the filter.

You can dismiss alerts by selecting the relevant alerts and clicking **Acknowledge**. You can choose to display alerts you have acknowledged by checking **Display Acknowledged Alerts**. The number of alerts displayed in the **ALERTS** subtab is the number of unacknowledged alerts.

If the description of the alert is truncated, click the alert description.

A tooltip with the complete description is displayed.

Alerts that are not part of the current version are displayed with **Unknown** in the Alerts ID field.

For a listing of all Zerto alerts, see *Zerto Virtual Replication Guide to Alarms, Alerts and Events*.

Managing a Specific Site

In the **Sites** tab, click a site name to enable monitoring the specific site. You can manage the properties of the site and the organizations associated with the site. The tabs **VPGs**, **VMs**, **Sites**, **Setup**, **Monitoring**, and **Reports** are all described in the Zerto Virtual Manager Administration Guides.

See also:

- [Managing a ZORG.](#)
- [Editing Zerto Cloud Manager Definitions](#)

Managing a ZORG

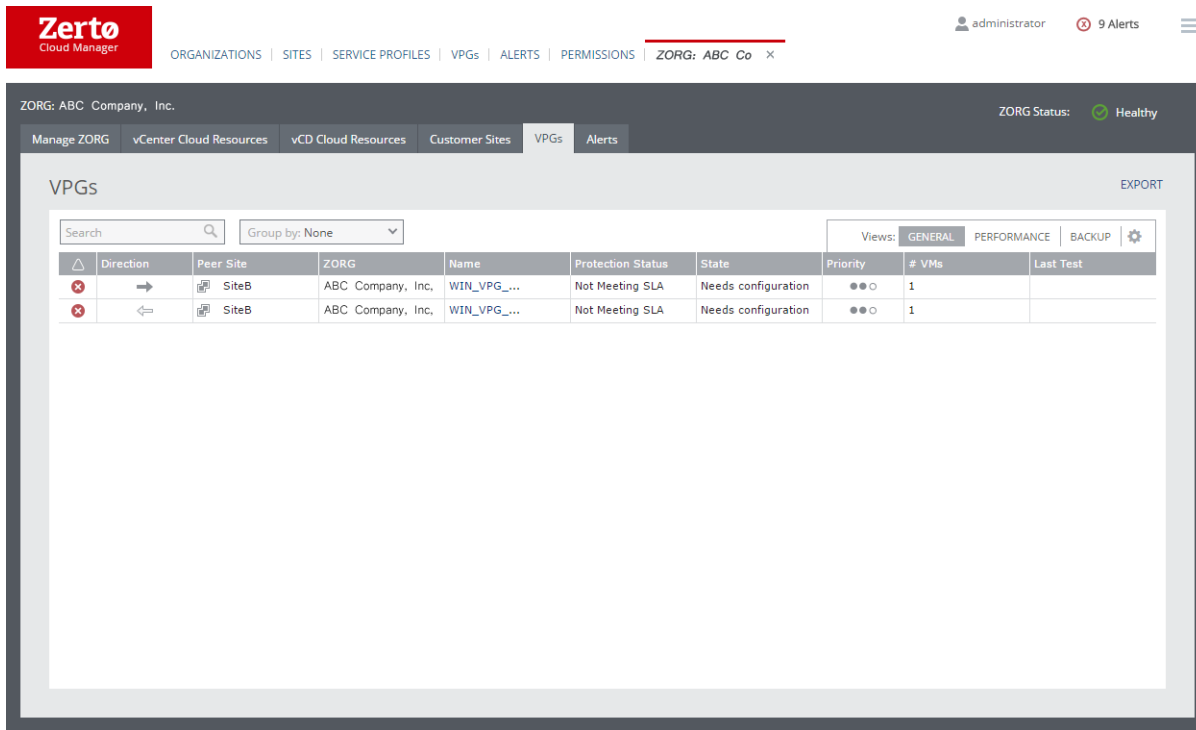
You can monitor the VPGs and alerts for a ZORG defined in Zerto Cloud Manager.

See also:

- [ZORG VPGs](#)
- [ZORG Alerts](#)

ZORG VPGs

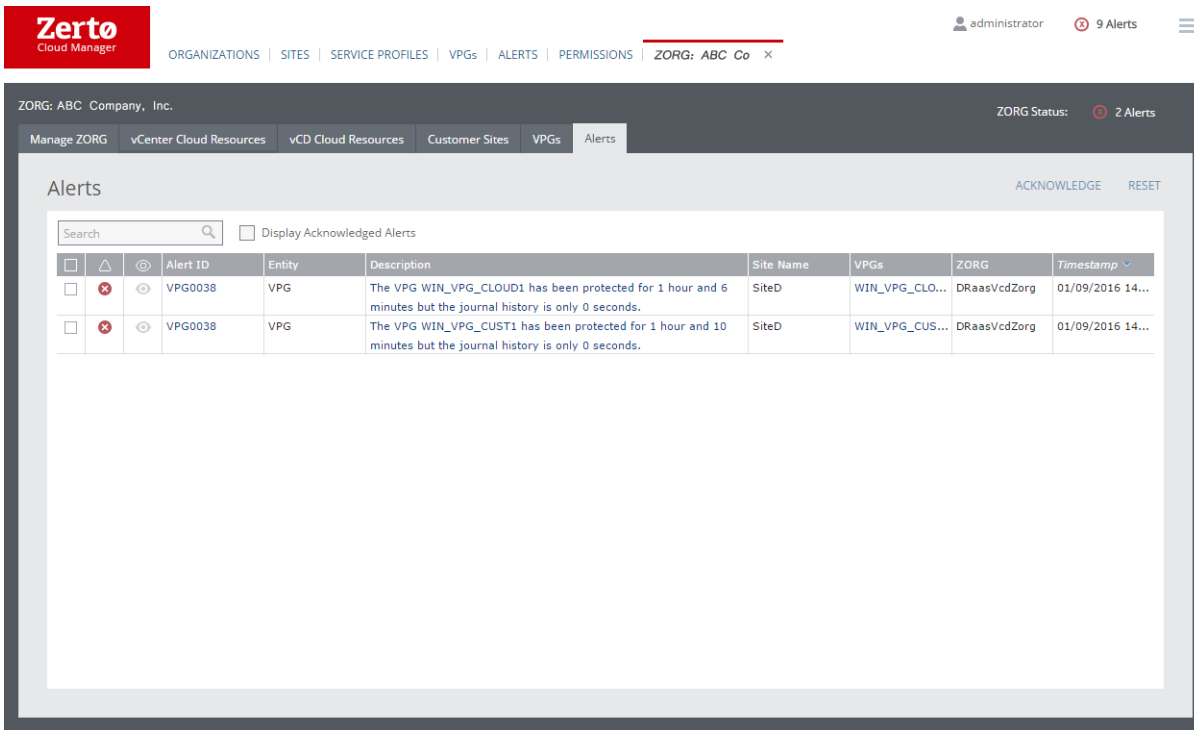
All VPGs protected or recovered for a specific ZORG can be monitored from the ZORG VPGs tab.



By clicking the VPG name link you can also drill-down to details of the VPG and perform operations on the VPG such as adding a checkpoint or testing the recovery of the VPG. You can also initiate a Move and Failover operation.

ZORG Alerts

The alerts for a specific ZORG are displayed in the ZORG **Alerts** tab.



Warnings are indicated by an orange icon and alerts by a red icon. The information displayed includes the VPG name, the name of the entity that triggered the alert, the date and time the alert was issued, and a description of the alert.

The alert status indicator in the title bar at the top shows the color of the most severe alert that is currently valid. After the alert has been resolved, the alert is removed from the **Alerts** tab and the alert status indicator changes, if appropriate, to show the new alert status.

You can filter Alerts by the columns with a filter icon. Click the filter icon to enter a value to filter by. The filter icon becomes visible when a filter is applied. Click Clear in the filter field to clear the filter.

You can dismiss alerts by selecting the relevant alerts and clicking **Acknowledge**. Even after acknowledging and dismissing alerts, you can choose to display them. Select or clear **Display Acknowledged Alerts** to display or not display alerts that have been dismissed (acknowledged). Note that the number of alerts displayed in the title bar alerts indicator is the number of unacknowledged alerts.

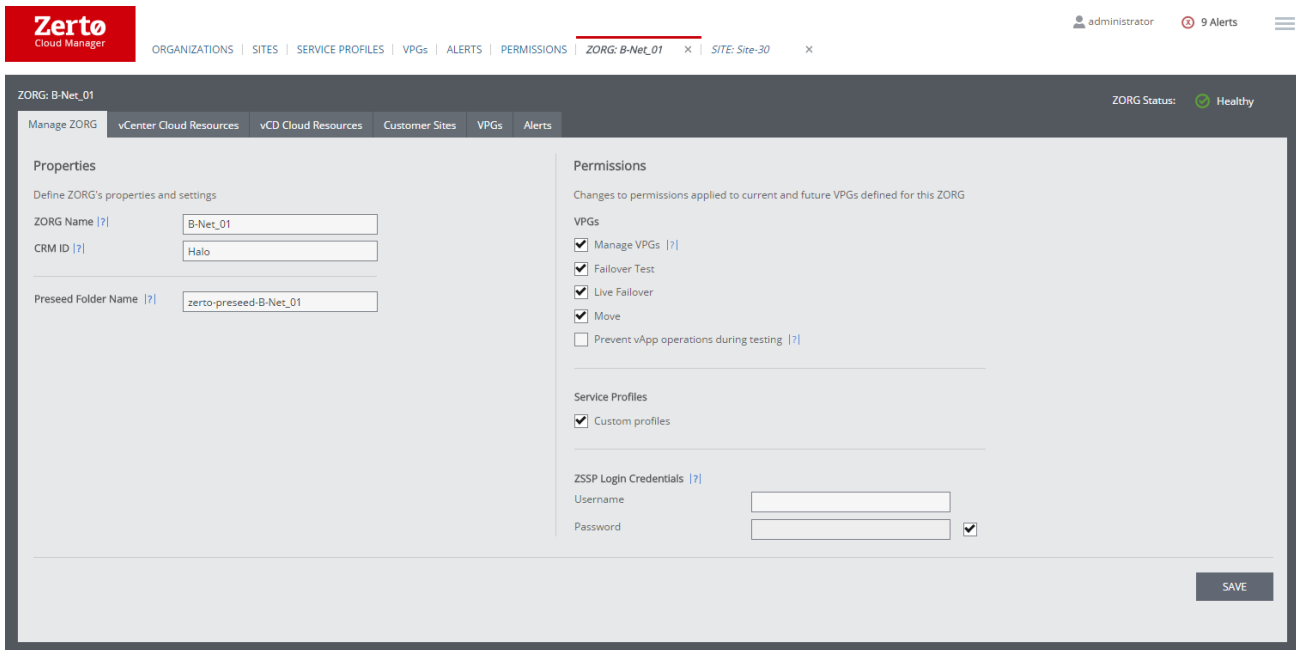
If the description of the alert is truncated, hover over the alert description to display a tooltip with the complete description.

Alerts from previous versions are displayed with an Unknown link.

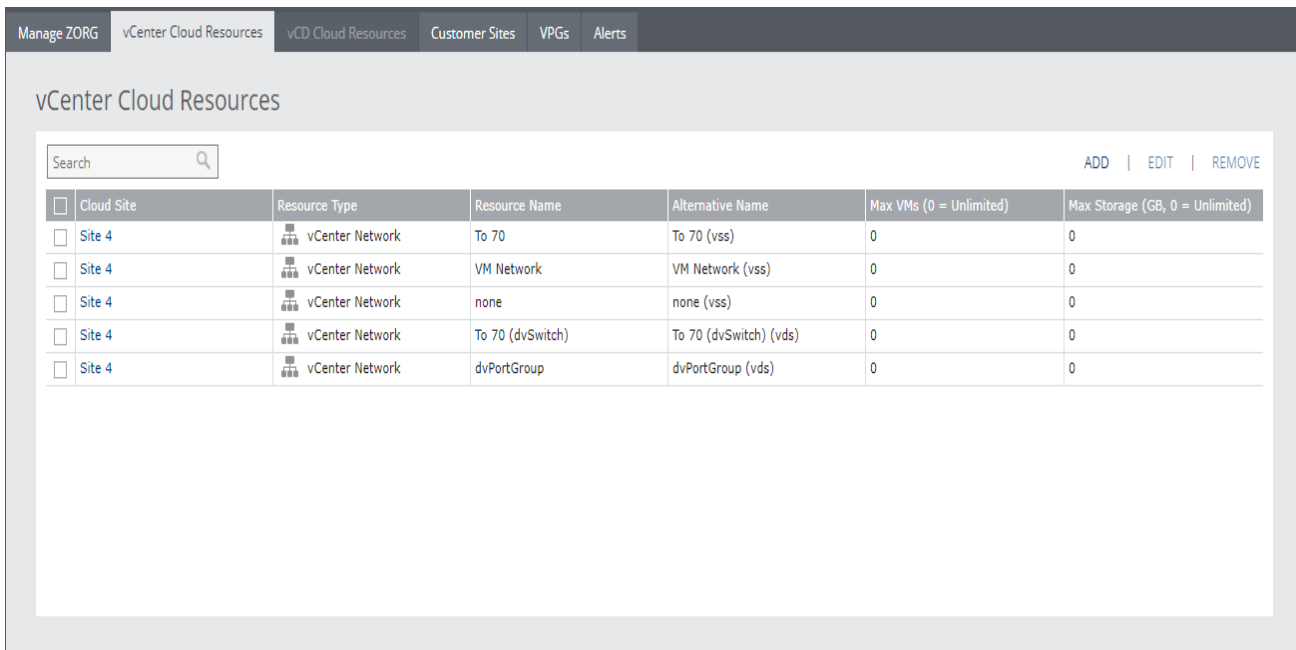
Editing Zerto Cloud Manager Definitions

You can edit any of the definitions in the Zerto Cloud Manager:

- Directly, for example Zerto organization, ZORG, permissions, in the Manage ZORG tab.



- By selecting the entity to edit and clicking **EDIT**, for example, to edit the alternative name for one of the vCenter Cloud Resources.



Resolving Zerto Cloud Connector Issues

Zerto cloud connectors are installed during configuration in Zerto Cloud Manager, as described in “[Defining DRaaS Components](#)”, on page 35. During normal operation there should be no need to manage the cloud connector. However if something happens to the cloud connector or the ESX/ESXi hosting it, you might need to remove or repair it.

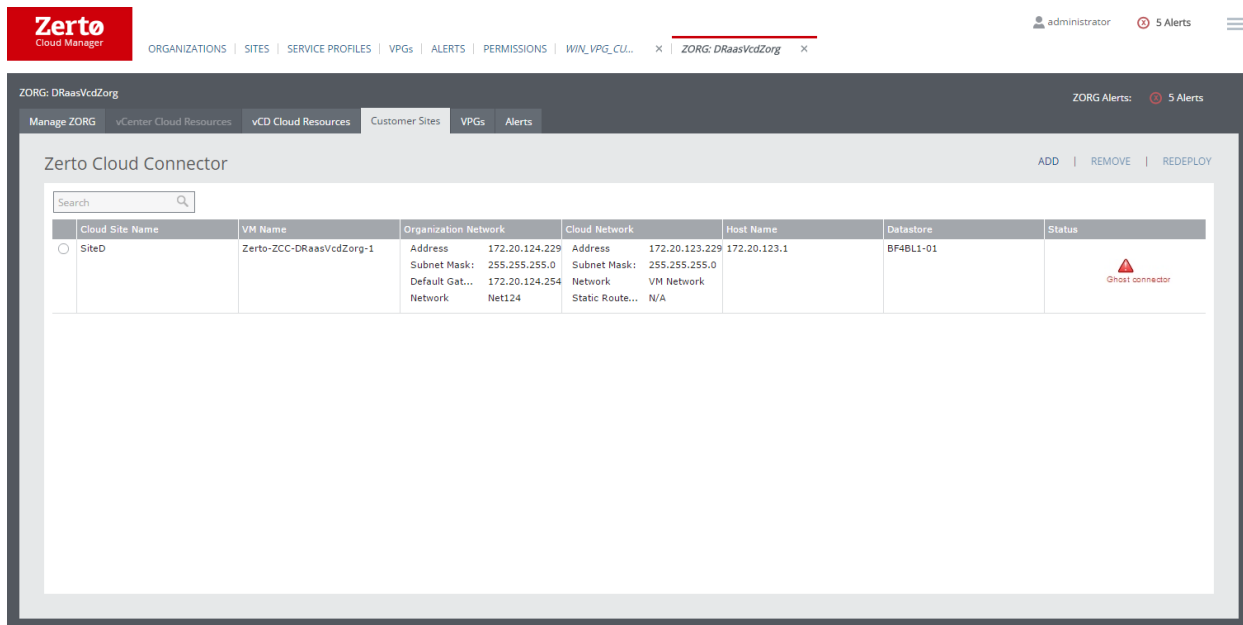
Note: Cloud connectors are configured and managed by the Zerto Cloud Manager. You cannot take snapshots of cloud connectors as snapshots cause operational problems for the cloud connectors.

The following management options are described in this section:

- [Handling a Ghost Zerto Cloud Connector](#)
- [vMotioning a Zerto Cloud Connector](#)
- [Handling an Orphaned Zerto Cloud Connector](#)

Handling a Ghost Zerto Cloud Connector

When an event occurs, for example the host machine crashes or the cloud connector is accidentally deleted, the cloud connector is displayed as a Ghost Cloud Connector.



To repair the cloud connector:

1. Repair the cloud connector by selecting it and clicking **Redeploy** to reinstall the cloud connector with the original addresses.

The **Redeploy Cloud Connector** dialog is displayed.

Some of the original values specified for the cloud connector must be used to redeploy the cloud connector, for example, the site where it will be redeployed.

2. Specify the following values that are enabled:
 - **Host and VM Name:** Specify the recovery host for the cloud connector virtual machine. The dropdown displays the hosts which do not have a cloud connector installed. You can change the host for the cloud connector. After specifying the host, the **VM Name** value is automatically updated to the original name with a number suffix added to make the name unique. After the name is displayed you can change it.
 - **Datastore:** The datastore for the cloud connector virtual machine.
 - **Organization Network:** The network details used by the customer. All the values from the original definition are fixed except for the network, which you can change:
 - **Network:** The name of the network from the list of available networks.
 - **Cloud Network:** The local network details for the cloud service provider. All the values from the original definition are fixed except for the network and static group, which you can change:
 - **Network:** The name of the cloud-side network from the list of available networks.
 - **Static Route Group:** The name of the group for which static routes are defined to the Zerto Virtual Manager network and VRA network. If a static route group is not specified, it is assumed that the Zerto Virtual Manager and VRAs are on the cloud network.

The cloud connector is recreated using the new settings.

See also:

- [vMotioning a Zerto Cloud Connector](#)
- [Handling an Orphaned Zerto Cloud Connector](#)

vMotioning a Zerto Cloud Connector

If a Zerto Cloud Connector has to be vMotioned to another host, for example when performing VMware maintenance on the host, if the new host has a different CPU or CPU architecture, Zerto recommends shutting down the Zerto Cloud Connector before vMotioning it.

The host must have the same access to the networks that are used by the Zerto Cloud Connector, including all appropriate VLAN tagging on the vSwitch or VDS and required trunking at the physical layer.

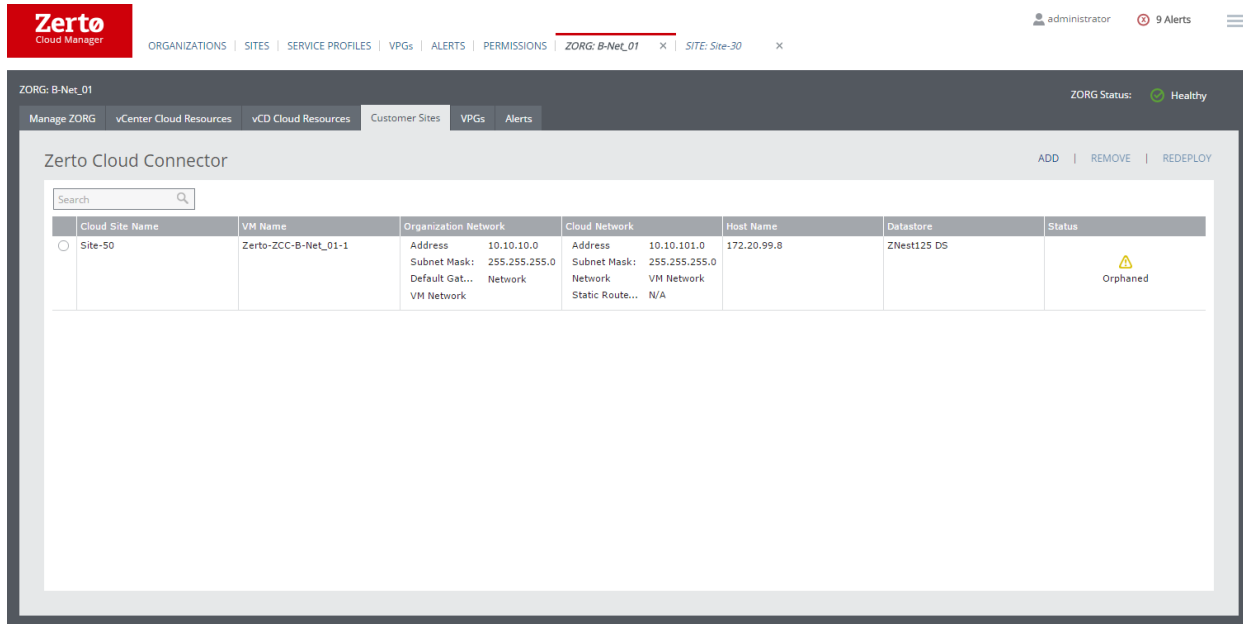
Note: When a Zerto Cloud Connector is powered off, the site paired to this Zerto Cloud Connector will be disconnected. Zerto recommends vMotioning the Zerto Cloud Connector to a similar host to avoid this disconnection.

See also:

- [Handling a Ghost Zerto Cloud Connector](#)
- [Handling an Orphaned Zerto Cloud Connector](#)

Handling an Orphaned Zerto Cloud Connector

If a cloud connector is orphaned, for example, when one of the specified networks is invalid or inaccessible, the cloud connector is displayed as an Orphaned Cloud Connector.



You must remove the cloud connector and then add a new one with valid settings to make the necessary connection between the organization network and the cloud network.

Note: An orphaned cloud connector means that a connection cannot be made to the cloud connector, often because the configuration is invalid or the ports to access the connector are blocked in the Zerto Virtual Manager.

See also:

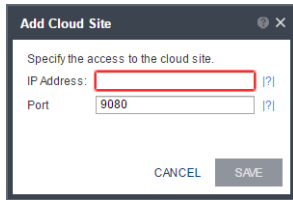
- [Handling a Ghost Zerto Cloud Connector](#)
- [vMotioning a Zerto Cloud Connector](#)

Configuration and management of the disaster recovery across multiple Zerto Virtual Managers is performed in the Zerto Cloud Manager. Zerto Cloud Manager interfaces with the Zerto User Interface and as such most of the tabs and dialogs in the Zerto User Interface can be accessed via the Zerto Cloud Manager. This section describes the Zerto Cloud Manager interface and the major dialogs and tabs in the Zerto User Interface. For full details of all the dialogs and tabs in the Zerto User Interface, and specifically for the dialogs involved with managing a Virtual Protection Group (VPG), including testing and failing over a VPG, refer to the *Zerto Virtual Manager Administration Guide* for your environment.

The following dialogs are described in this section:

- [Add Cloud Site Dialog](#)
- [Add New Role Dialog](#)
- [Add Permission Dialog](#)
- [Add Service Profile Dialog](#)
- [Add Static Route Dialog](#)
- [Add ZORG Dialog](#)
- [Alerts Tab](#)
- [Cloud Settings Dialog](#)
- [Configure & Install VRA Dialog](#)
- [Configure Paired Site Routing Dialog](#)
- [Configure Provider vDCs Dialog](#)
- [Configure vCD Dialog](#)
- [Customer Sites Tab](#)
- [Edit Permission Dialog](#)
- [Edit Resource Dialog](#)
- [Edit Role Dialog](#)
- [Edit VRA Dialog](#)
- [Install Cloud Connector Dialog](#)
- [Manage Static Routes Dialog](#)
- [Manage ZORG Tab](#)
- [Organizations Tab](#)
- [Outbound Protection Over Time Report](#)
- [Permissions Tab](#)
- [Protection Over Time by ZORG Report](#)
- [Recovery Reports](#)
- [Redeploy Cloud Connector Dialog](#)
- [Resource Report](#)
- [Roles Dialog](#)
- [Select User/Group Dialog](#)
- [Service Profiles Tab](#)
- [Sites Tab](#)
- [Usage Report](#)
- [vCD Cloud Resources Tab](#)
- [vCenter Cloud Resources Tab](#)
- [VMs Tab in the Zerto Virtual Manager](#)
- [VPG Performance Report](#)
- [VPGs Tab in the Zerto Virtual Manager](#)
- [VPGs Tab in the Zerto Cloud Manager](#)
- [VRAs Tab in the Zerto Virtual Manager](#)

Add Cloud Site Dialog

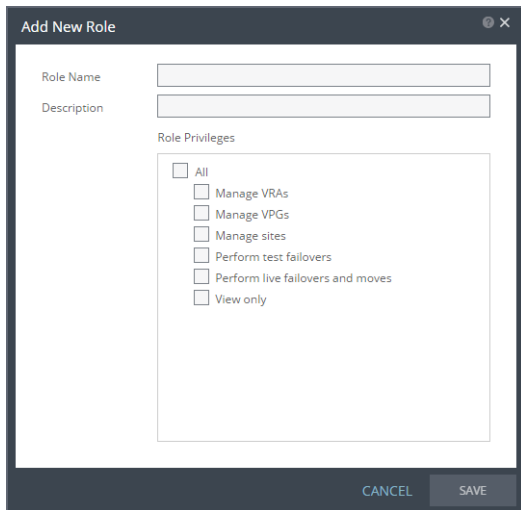


The screenshot shows a dialog box titled "Add Cloud Site". The text inside says "Specify the access to the cloud site." Below this are two input fields: "IP Address:" followed by a text box with a red border and a help icon, and "Port:" followed by a text box containing "9080" and a help icon. At the bottom are "CANCEL" and "SAVE" buttons.

The Zerto Cloud Manager is a single point of management for all the cloud sites providing either DRaaS or ICDR. You set up the sites to manage in the Zerto Cloud Manager by adding connections to the Zerto Virtual Managers running on the sites.

- **IP Address:** The IP address of a cloud site where a Zerto Virtual Manager is running.
- **Port:** The port specified during the installation to connect to the Zerto Virtual Manager.

Add New Role Dialog

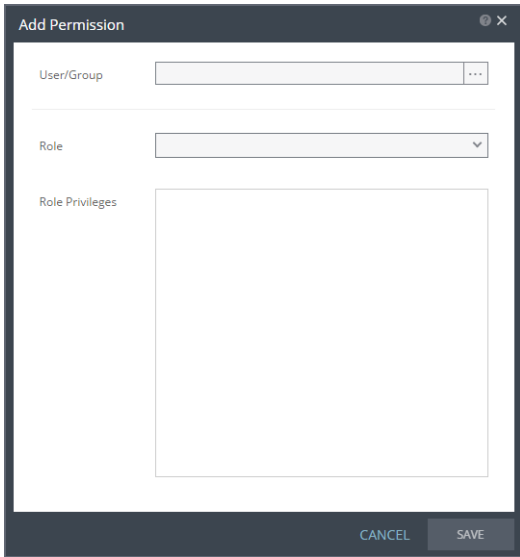


The screenshot shows a dialog box titled "Add New Role". It has two text input fields: "Role Name" and "Description". Below these is a section titled "Role Privileges" containing a list of checkboxes: "All", "Manage VRAs", "Manage VPGs", "Manage sites", "Perform test failovers", "Perform live failovers and moves", and "View only". At the bottom are "CANCEL" and "SAVE" buttons.

Enables adding new roles and assigning the roles the appropriate Zerto-related privileges.

- **Role Name:** The name of the new role.
- **Description:** The description of the new role.
- **Role Privileges:** The privileges that can be assigned to the role. Every role includes the **View only** privilege. If it is not set, it is automatically added to the role when the role is saved.

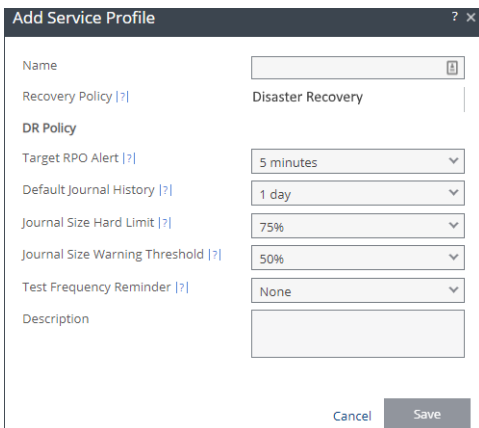
Add Permission Dialog



Enables adding permissions to a user or group.

- **User/Group:** The name of the user or group to be assigned permissions.
- **Role:** The role to be assigned to the user or group.
- **Role Privileges:** The privileges associated with the selected role.

Add Service Profile Dialog



A service profile provides a predefined set of properties to use when VPGs are defined or edited. Zerto provides a default service profile and the option to specify customized requirements. You can define service profiles to manage specific service level agreements (SLAs) with customers.

- **Name:** A name assigned to the service profile.
- **Recovery Policy:** The default is **Disaster Recovery**. **DR Policy**
 - **Target RPO:** The maximum desired time between each automatic checkpoint being written to the journal before an alert is issued. In reality checkpoints are written more frequently.
 - **Default Journal History:** The time for which all write commands are saved in the journal. Each protected virtual machine has a dedicated journal volume on the recovery site associated with the replicated virtual machine. This enables journal data to be maintained, even when changing the recovery host for the recovery. When specifying a checkpoint to recover to, the checkpoint must still be in the journal. For example, if the value specified here 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.

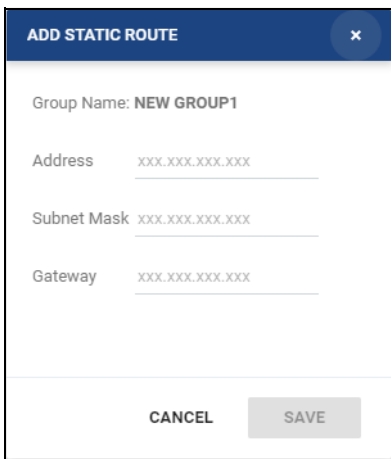
When a VPG is tested, either during a failover test or before committing a Move or Failover operation, a scratch volume is created for each virtual machine being tested, with the same size as the journal for that virtual machine. The size of the scratch volume determines the length of time that you can test for. The larger the volume, the longer the testing can continue, assuming the same rate of change being tested. If the journal history required is small, for example two or three hours, the scratch volume that is created for testing will be small as well, limiting the time available for testing. Thus, when considering the journal history you should also consider the length of time you will want to test the VPG.

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

- **Journal Size Hard Limit:** The maximum size that the journal can grow, as a percentage of the virtual machine volume size. The minimum journal size is 8GB.
- **Journal Size Warning Threshold:** The size of the journal that triggers a warning that the journal is nearing its hard limit, as a percentage of the virtual machine volume size.
- **Test Frequency 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.
- **Description:** A description of the service profile.

Add Static Route Dialog

Add a static route for a specified group, when the Zerto Cloud Connector and cloud site Zerto Virtual Manager are on different networks.

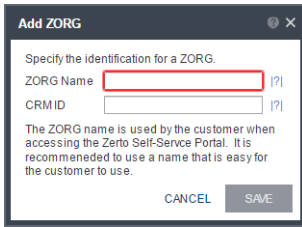


- **Address:** The network address for the static route that you want to route to.
- **Subnet Mask:** The subnet mask for the network.
- **Gateway:** The gateway address for the network on the local network of the Zerto Cloud Connector cloud network interface.

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](#).

Add ZORG Dialog



You set up each organization that uses either DRaaS or ICDR and attach the organization to the relevant site.

- **ZORG Name:** The name to identify the organization.
- **CRM ID:** An optional identifier to identify the organization in a CRM.

Alerts Tab

Alert ID	Entity	Description	Site Name	VPGs	ZORG	Timestamp
ZVM0003	ZVM	The Zerto Virtual Manager is not connected to site Site-9 (172.20.99.9:9081).	Site-50	Paris		31/08/2016 10:46...
ZVM0001	ZVM	The connection between site Site-9 and the hypervisor manager Pending vCenter connection at 0.0.0.0 is down.	Site-50	Paris		31/08/2016 10:09...
VPG0010	VPG	VPG Paris exceeds configured RPO of 5 minutes by more than 25%.	Site-50	Paris		31/08/2016 09:32...
VRA0020	ZVM	VM Clients is shut down and cannot be synced.	Site-50	Paris		31/08/2016 09:19...
VRA0020	ZVM	VM Operations (Site 5) is shut down and cannot be synced.	Site-50	Paris		31/08/2016 09:19...
VPG0026	VPG	The service profile you use in VPG Paris has been changed by your cloud provider.	Site-50	Paris		31/08/2016 09:04...
ZVM0002	VRA	Zerto Virtual Manager is not connected to VRA with IP fe80::250:56ff:fea9:2cdb on host 172.20.99.7.	Site-50			31/08/2016 09:04...
ZCC0003	Cloud Connector	An orphaned Zerto Cloud Connector for Site-50_B-Net_01 was installed.	Site-50			31/08/2016 09:04...
VCD0015	ZVM	Connected to vCloud 172.20.99.23 but failed to connect to AMQP-server for notifications. Last connection error: \None of the specified endpoints were	Site-50			31/08/2016 09:04...

Each Zerto alert is associated with an event. These events can trigger vCenter Server alarms. Thus, when a Zerto alert is fired, a corresponding event is also fired. This event can trigger a vCenter Server alarm.

- **Acknowledge button:** Dismiss selected alerts.
- **Reset button:** Undismiss selected alerts that were previously dismissed.

The following information is displayed for each alert:

- **Alert status indicator:** The color indicates the alert status:
 - **Orange:** A warning alert.
 - **Red:** An error alert.
- **Dismissed:** Whether the alert has been dismissed or not.
- **Alert ID:** The alert identifier, which can be clicked to provide more details.
- **Entity:** The type of alert.
- **Site Name:** The site where the alert occurred.
- **VPGs:** The name of any VPGs affected by the alert.
- **ZORGs:** The Zerto organizations affected by the alert.
- **Timestamp:** The date and time of the alert.

- **Description:** A description of the alert.

Cloud Settings Dialog

VCD SETTINGS

Use vCD

IP Address

Username

Password

AMQP Username

AMQP Password

NETWORKING

Manage Static Routes

DATASTORE CONFIGURATION

Provider vDC Settings

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.

Configure & Install VRA Dialog

The Configure and Install VRA dialog is displayed. The dialog displayed depends on the ESX/i version:

ESXi versions from 5.5

ESXi versions before version 5.5

1. Specify the following **Host Details**:

- **Host:** The host on which the VRA is installed. The drop-down displays the hosts that do not have a VRA installed, with the selected host displayed by default.

(vSphere only) From ESXi 5.5, by default, Zerto Virtual Manager creates a **.VIB** (vSphere Installation Bundle) which is used to set up a secure communication channel to the host. The .VIB is installed on the host when the VRA is installed. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and logs it.

(vSphere only) For ESX/i versions earlier than 5.5, when using a password, Zerto Virtual Manager connects to the host using the root password. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is issued, requesting the user enter the new password.

- **Use credentials to connect to host:** When unchecked, the Zerto Virtual Manager uses VIB to set up a secure communication channel to the host. This field is only relevant for ESXi 5.5 and later.
- **Host Root Password:** When the VRA should connect to the host with a password, check **Use credential to connect to host** and enter the root user password used to access the host. When the box on the right side is checked, the password is displayed in plain text. This field is only relevant for ESXi 5.x hosts.
- **Datastore:** The datastore that contains the OS disks of the VRA VM. 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. For details, refer to [Zerto Scale and Benchmarking Guidelines](#).
- **VRA Bandwidth Group:** Choose the VRA Bandwidth Group from the dropdown list. To create a new VRA group, type in the name of the new group and click **CREATE**. You can then choose the new group from the dropdown list. You group VRAs together when VRAs use different networks so they can be grouped by network, for example when the protected and recovery sites are managed by the same vCenter Server and you want to replicate from the branch site to the main site. Within a group the priority assigned to a VPG dictates the bandwidth used and is applicable

within a group and not between groups. Thus, a VPG with a high priority is allocated bandwidth before VPGs with lower priorities. VPGs that are on VRAs with different VRA groups, for example, VPG1 on VRA1 in group1 and VPG2 on VRA2 in group2, do not affect each other, as the priority is relevant only within each group.

2. 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.

3. Click **INSTALL**.

The VRA installation starts and the status is displayed in the TASKS popup dialog in the status bar and under **MONITORING > TASKS**.

The VRA displayed name, and DNS name, is **Z-VRA-hostname**. If a virtual machine with this name exists, for example when a previous VRA was not deleted, the VRA name has a number appended to it.

4. Add a VRA to every host that hosts virtual machines for which you want replication.

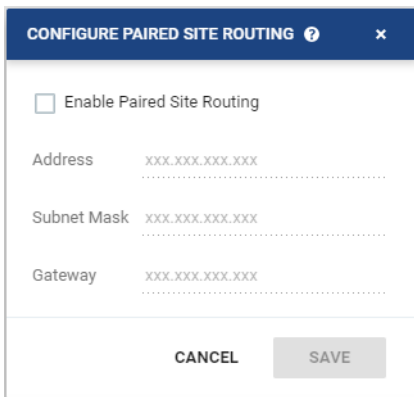
Zerto recommends installing a VRA on every listed host.

An alert is issued after the first VRA is installed in a cluster that tells you to install a VRA on the other hosts in the cluster. The alert is automatically removed when all the hosts in the cluster have VRAs installed.

- Return to the Zerto Cloud Manager **Sites** tab and click the next site name in the list to display the site tab with nested tabs and install the VRAs for this site. Repeat this procedure for every site in the Zerto Cloud Manager.
- A VRA can manage a maximum of 1500 volumes, whether these are volumes being protected or recovered.

Note: VRAs are configured and managed by the Zerto Virtual Manager. You cannot take snapshots of VRAs as snapshots cause operational problems for the VRAs.

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.

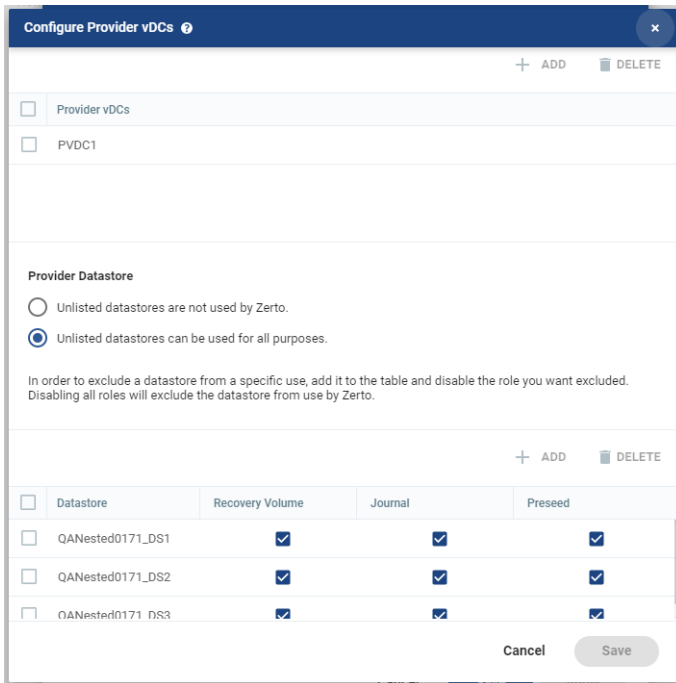
- **Enable Paired Site Routing:** When checked, enables paired site routing.
- **Address:** The IP address of the **next hop** at the local site, the router, or gateway address that is used to access the peer site network.
- **Subnet Mask:** The subnet mask for the peer site network.
- **Gateway:** The 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.

Configure Provider vDCs Dialog

Accessed from **Site Settings > Cloud Settings** tab > **Datastore Configuration** area.



Used by Zerto Cloud Service Providers to define provider vDCs, and to define which datastores can be used by Zerto, to which purpose.

Datastores which are not listed in this window may be used by Zerto, unless they are explicitly excluded.

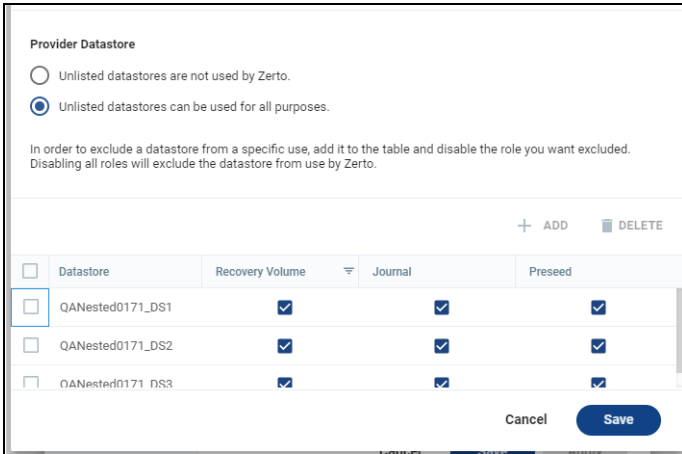
Note:

Before setting up Zerto to work with vCD, you must have an AMQP server installed.

- Zerto provides an AMQP installation kit if you do not have one installed for vCD, available as a download from the Zerto Support Portal, from the downloads page.
- Run ZertoAMQPInstallWizard.exe from the kit and when prompted enter the IP or host name of the vCD and the administrator user and password to access this vCD.
- The Zerto Virtual Manager connects to the vCD and checks whether an AMQP server is installed.
 - If an AMQP server is not installed, Zerto recommends using RabbitMQ, which in turn requires Erlang/OTP.
 - Links to the sites to install both Erlang/OTP and RabbitMQ are provided as part of the Zerto AMQP installation. Use these links to install Erlang/OTP and then RabbitMQ, then you can continue with the Zerto AMQP installation.
- If an AMQP server was already installed, change the connection details displayed to those defined in vCD.
- If you installed the AMQP server as part of the Zerto AMQP installation, the default settings for these installations are displayed, with a user and password of **guest**.
- At the end of the Zerto AMQP installation, vCD is updated with these settings, in AMQP Broker Settings under Administration > Blocking Tasks > Settings.

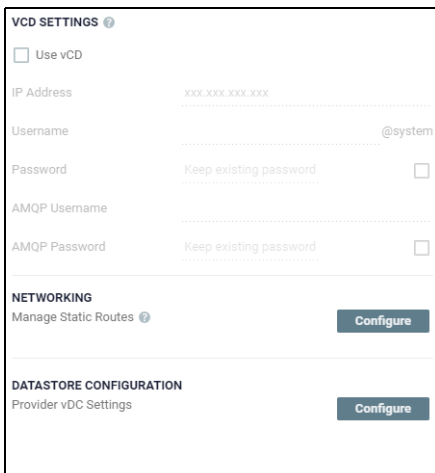
To configure access to provider vDCs, and their datastore's configuration:

- In the **Provider vDCs** area (top), click **Add**. A list of provider vDCs appear.
The provider vDCs were created by the Cloud Service Providers according to predefined service levels, storage availability, performance requirements or cost.
 - Add the provider vDCs which will be available for use in Zerto.
- In the **Provider Datastore** area select one of the following:
 - Unlisted datastores are not used by Zerto:** Clearly define that datastores which are not listed in this window cannot be used.
 - Unlisted datastores can be used for all purposes:** Allow unlisted datastores of all provider vDCs, even those provider vDCs that were not added to the list of Provider vDCs can be used for any purpose.
- In the **Provider Datastore** area, click **Add**, to add datastores.



- Select the **Recovery Volume** checkbox, if the datastore can be used as a recovery datastore.
 - Select the **Journal** checkbox if the datastore can be used for the journal.
 - Select the **Preseed** checkbox if the datastore can be used for preseeded disks. Only datastores marked as preseeded can be used, preventing different organizations being exposed to datastores of other customers using the preseed option.
 - In order to exclude a datastore, add it to the list, then deselect all checkboxes.
-

Configure vCD Dialog



Set up access to vCD for the Zerto Virtual Manager.

Note:

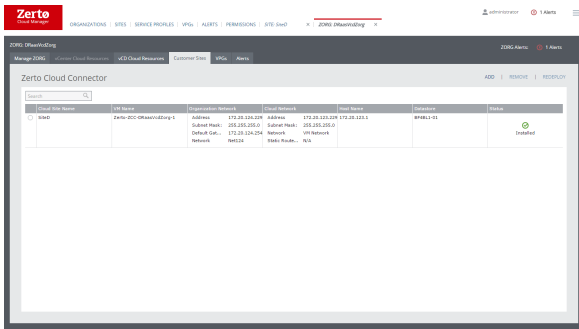
Before setting up Zerto to work with vCD, you must have an AMQP server installed.

- Zerto provides an AMQP installation kit if you do not have one installed for vCD, available as a download from the Zerto Support Portal, from the downloads page.
 - Run ZertoAMQPInstallWizard.exe from the kit and when prompted enter the IP or host name of the vCD and the administrator user and password to access this vCD.
 - The Zerto Virtual Manager connects to the vCD and checks whether an AMQP server is installed.
 - If an AMQP server is not installed, Zerto recommends using RabbitMQ, which in turn requires Erlang/OTP.
 - Links to the sites to install both Erlang/OTP and RabbitMQ are provided as part of the Zerto AMQP installation. Use these links to install Erlang/OTP and then RabbitMQ, then you can continue with the Zerto AMQP installation.
 - If an AMQP server was already installed, change the connection details displayed to those defined in vCD.
 - If you installed the AMQP server as part of the Zerto AMQP installation, the default settings for these installations are displayed, with a user and password of **guest**.
 - At the end of the Zerto AMQP installation, vCD is updated with these settings, in AMQP Broker Settings under Administration > Blocking Tasks > Settings.
- **Use vCD:** When checked, the fields to configure vCD settings are enabled.
 - **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 a vCD administrator.
 - **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.
 - **Provider vDC Settings:** Click **Configure** to define provider vDC settings and their datastore configuration. See “Configure Provider vDCs Dialog”, on page 85.

Customer Sites Tab

The screenshot shows the Zerto Cloud Manager interface. At the top, there is a navigation bar with the Zerto logo and various menu items like ORGANIZATIONS, SITES, SERVICE PROFILES, VPGs, ALERTS, PERMISSIONS, and SITE. Below this, there is a breadcrumb trail: Manage ZORG > vCenter Cloud Resources > vCD Cloud Resources > Customer Sites > VPGs > Alerts. The main content area is titled 'Zerto Cloud Connector' and contains a table with the following data:

Cloud Site Name	VM Name	Organization Network	Cloud Network	Host Name	Datastore	Status
SiteD	Zerto-ZCC-DRaaSvcdZorg-1	Address: 172.20.124.229 Subnet Mask: 255.255.255.0 Default Gat...: 172.20.124.254 Network: Net124	Address: 172.20.123.229 Subnet Mask: 255.255.255.0 Network: VM Network Static Route...: N/A	172.20.123.1	BF4BL1-01	Installed



Displays the ZORG Zerto Cloud Connector details.

In a DRaaS configuration, the organization networks for disaster recovery are extended to the cloud. The Zerto Cloud Connectors are installed to ensure that these networks have no touch points with the cloud infrastructure network, providing complete network separation between each organization network and the cloud service provider infrastructure network. All the traffic to and from the organization is routed through the cloud connector, so that the following is implemented:

- None of the organizations have direct access to the cloud service provider network and cannot see any part of the cloud service provider network that the cloud service provider does not allow them to see.
- Each organization has no access to the network of another organization.

A Zerto Cloud Connector is 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. Also, for the cloud connector, the IP ranges used for the organization network and cloud service provider infrastructure network cannot be the same. The cloud connector requires the following:

- 4GB disk space
- At least 1GB of reserved memory.
- 1 vCPU.

The Zerto Cloud Connector 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 Zerto Cloud Connector 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 Zerto Cloud Connector, where the incoming traffic on the customer network is automatically configured to IP addresses of the cloud service provider network.

If the cloud service provider wants to institute additional security, considering both Zerto Cloud Connector interfaces as part of the organization network, he 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. If you change the Zerto Virtual Manager and VRAs cloud network, changing the static route settings for a group to the new network, changes the access for all Zerto Cloud Connectors with the specified group.

Static routes are defined in the [Add Static Route Dialog](#).

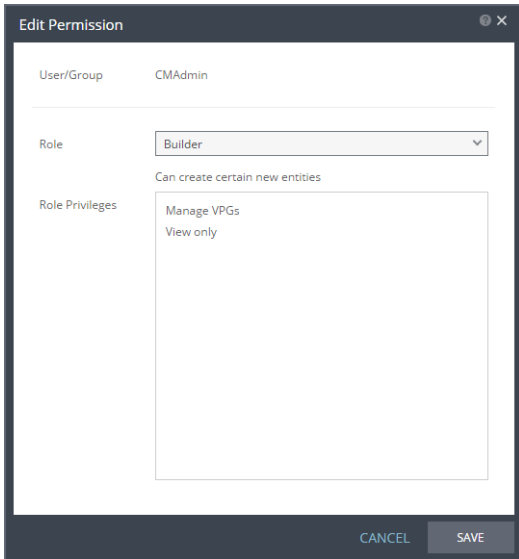
Zerto Cloud Connectors are defined per organization with one Zerto Cloud Connector defined for each organization site. Each Zerto Cloud Connector requires two ports for each VRA (one port for VRA port 4007 and one port for port 4008) accessed via the Zerto Cloud Connector. There is directionality to these ports.

- **Cloud Site:** The cloud site for which the Zerto Cloud Connector is required.
- **Connector VM Name:** The name of the cloud connector in the vCenter Server. The name has the format:
Z-Connector-nnnnnn
- **Organization Network:** The details about the connection to the ZORG network.
- **Cloud Network:** The details about the connection to the cloud network, including the static route group, if one is specified.
- **Host Name:** The name of the host where the cloud connector virtual machine is installed.
- **Datastore:** The name of the datastore used by the cloud connector virtual machine.
- **Status:** The status of the cloud connector.

Filtering Information

You can filter the list by clicking the filter icon in a column and entering a value to filter by. The filter icon becomes visible when a filter is applied. Click **Clear** in the filter field to clear the filter.

Edit Permission Dialog

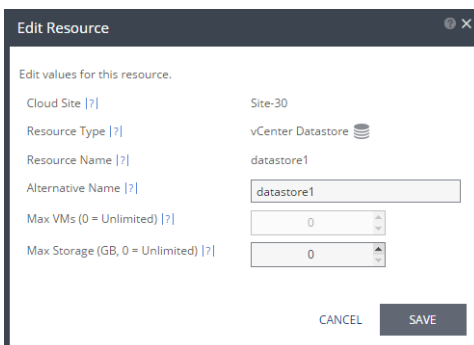


Enables editing the permissions of a user or group.

- **User/Group:** The user or group whose permissions are to be edited.
- **Role:** The role to be assigned to the user or group.
- **Role Privileges:** The privileges associated with the selected role.

Edit Resource Dialog

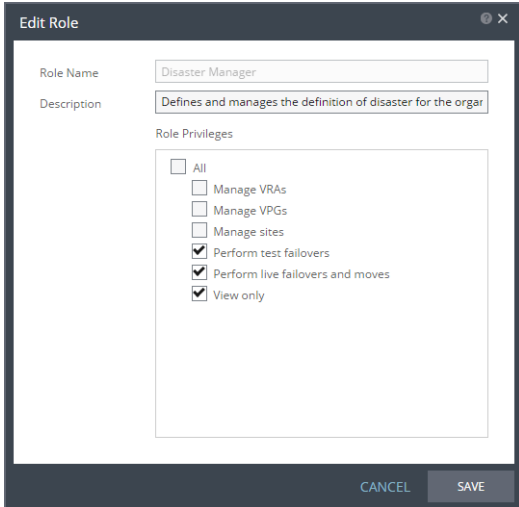
This dialog is specific for the type of resource selected to be edited. For example, editing a datastore enables changing the name of the datastore that is displayed to the customer and specifying the maximum amount of storage that can be recovered with this datastore. Editing a network enables changing the network name that is displayed to the customer. Editing a resource pool enables changing the resource pool name that is displayed to the customer and specifying the maximum number of virtual machines that can be protected to the resource pool.



- **Cloud Site:** The name of the cloud site that owns the resource.
- For a vCenter cloud resource:
 - **Resource Type:** The type of resource: Datastore, Network, or Resource Pool.
 - **Resource Name:** The cloud name for the resource.
 - **Alternative Name:** The name the organization sees for the resource.
- For a vCD cloud resource:
 - **vCD Organization:** The vCD organization name.
 - **Org vDC:** The organization vDC.
- **Max VMs:** The maximum number of virtual machines that can be protected for the ZORG.

- **Max Storage:** The maximum amount of storage that can be protected for the ZORG.

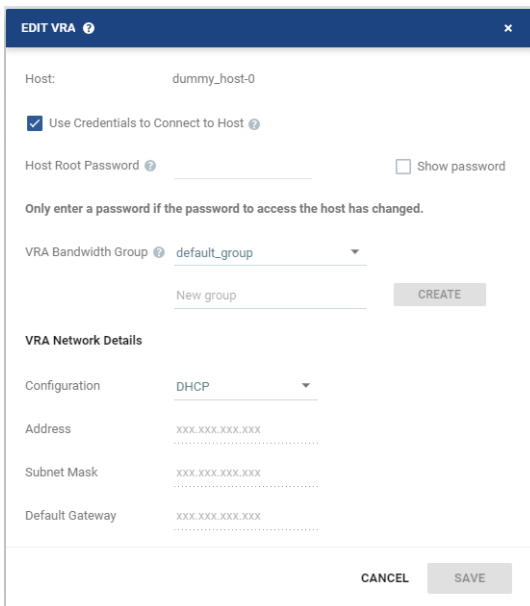
Edit Role Dialog



Enables editing the description of a role and to change the privileges assigned to this role.

- **Description:** The description of the role.
- **Role Privileges:** The privileges that can be assigned to the role. Every role includes the **View only** privilege. If it is unset, it is automatically added to the role when the role is saved.

Edit VRA Dialog



To change the network settings for a VRA, for example when the gateway to the VRA is changed.

- **Host:** The IP of the host on which the VRA is installed.
For ESXi 5.5 and later hosts, by default, Zerto Virtual Manager uses a vSphere Installation Bundle, VIB, to connect to the host. When using VIB:

- The user does not enter a password.
- Once a day, Zerto Virtual Manager checks that the VRA and host can connect. If the connection fails, Zerto Virtual Manager re-initiates the connection automatically and notes this in the log.

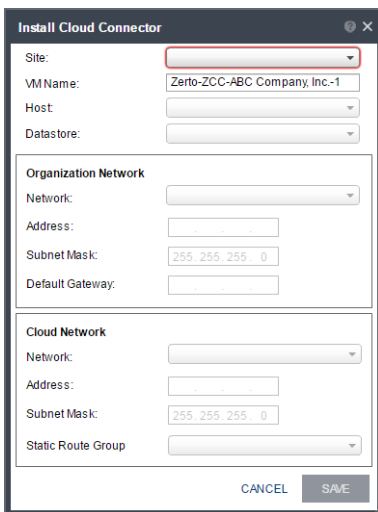
When using a password, root access is required if the Zerto host component is down and needs an automatic restart. Once a day, Zerto Virtual Manager checks that the password is valid. If the password was changed, an alert is triggered, requesting the user enter the new password.

- **Use credentials to connect to host:** When unchecked, the Zerto Virtual Manager uses VIB to connect to the host. This field is only relevant for ESXi 5.5 and later.
- **Host Root Password:** When the VRA should connect to the host with a password, select **Use credential to connect to host**, then enter the root user password used to access the host. When the box on the right side is selected, the password is displayed in plain text. This field is only relevant for ESXi 4.x and 5.x hosts. This field is disabled for ESX 4.x hosts.
- **VRA Group:** The free text to identify the group to which a VRA belongs. If you create a group and then change the name when editing the VRA so that there is no VRA in the site that belongs to the originally specified group, the group is automatically deleted from the system.

To create a new group, enter the new group name over the text **New group** and click **CREATE**.

- **Configuration:** Either have the IP address allocated via a static IP address or a DHCP server. If the VRA was originally installed with a static IP, you cannot change this to DHCP. If the VRA was originally installed to use a DHCP server, you can change this to use a static IP.
- **Address:** The static IP address for the VRA to communicate with the Zerto Virtual Manager.
- **Subnet Mask:** The subnet mask for the network. The default value is **255.255.255.0**.
- **Default Gateway:** The default gateway for the network.

Install Cloud Connector Dialog

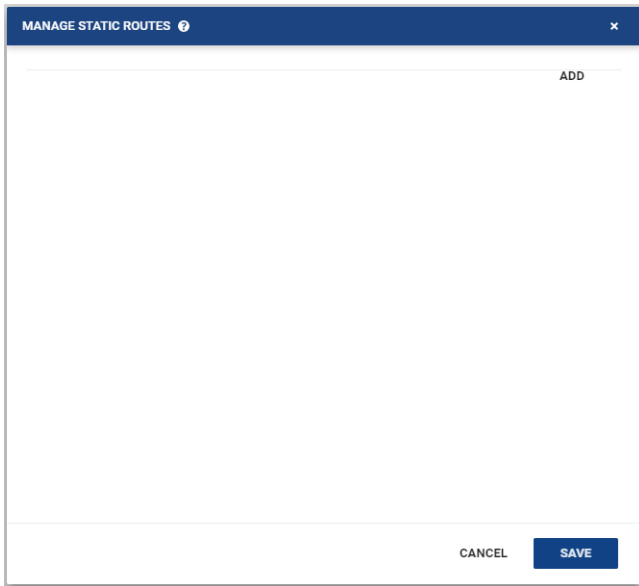


A Zerto Cloud Connector is a virtual machine installed on the cloud side, one for each customer organization replication network. The Zerto Cloud Connector routes traffic between the customer network and the cloud replication network, in a secure manner without requiring the cloud service provider to go through complex network and routing setups, ensuring complete separation between the customer network and the cloud service provider network. The Zerto Cloud Connector 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 Zerto Cloud Connector, where the incoming traffic on the customer network is automatically configured to IP addresses of the cloud service provider network.

- **Site:** The site used by the cloud service provider for the organization.
- **VM Name:** The name to assign to the cloud connector.

- **Host:** The recovery host for the cloud connector virtual machine. The dropdown displays the hosts which do not have a cloud connector installed.
- **Datastore:** The Datastore for the cloud connector virtual machine.
- **Organization Network:** The network details used by the customer:
 - **Network:** The name of the network from the list of available networks.
 - **Address:** The IP address to access the organization network. The customer pairs to this IP address.
 - **Subnet Mask:** The subnet mask for the network. The default value is **255.255.255.0**.
 - **Default Gateway:** The default gateway for the network.
- **Cloud Network:** The local network details for the cloud service provider:
 - **Network:** The name of the cloud-side network from the list of available networks.
 - **Address:** The IP address to access the network used by the cloud service provider to communicate with the cloud connector.
 - **Subnet Mask:** The subnet mask for the network. The default value is **255.255.255.0**.
 - **Static Route Group:** The name of the group for which static routes are defined to the Zerto Virtual Manager network and VRA network. If a static route group is not specified, it is assumed that the Zerto Virtual Manager and VRAs are on the cloud network.

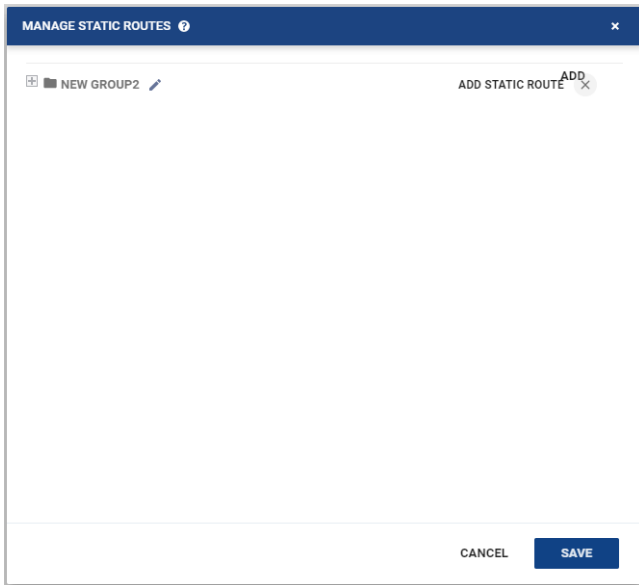
Manage Static Routes Dialog



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.

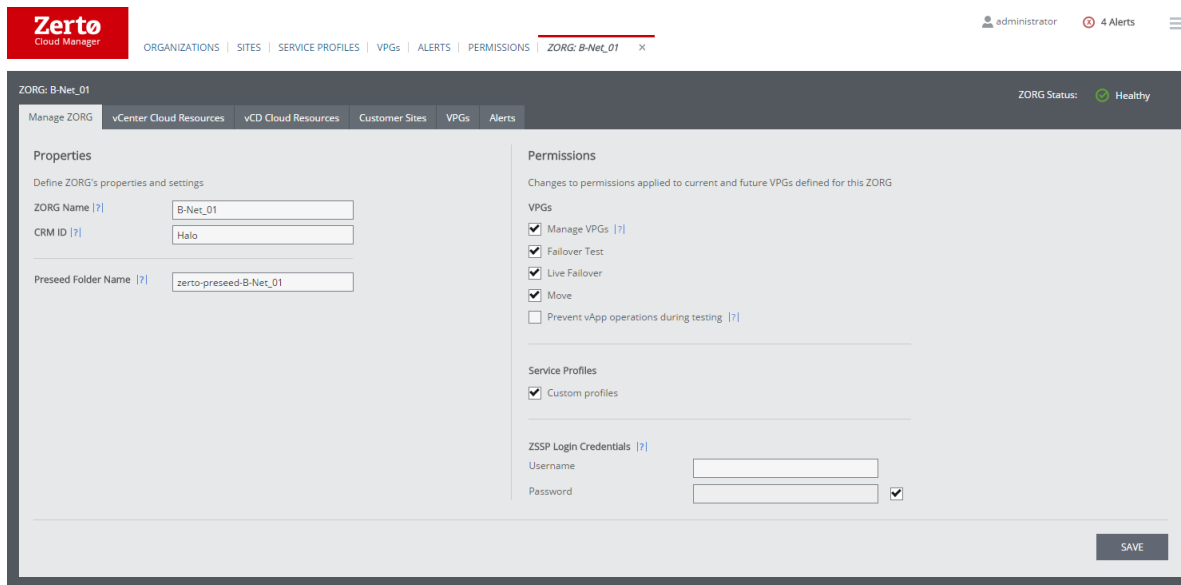
The cloud service provider can define a Zerto Cloud Connector per organization site, that has two Ethernet interfaces, one to the organization's network and one to the cloud service provider's network. If the cloud service provider wants to add additional security, considering both cloud connector interfaces 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](#).

Manage ZORG Tab



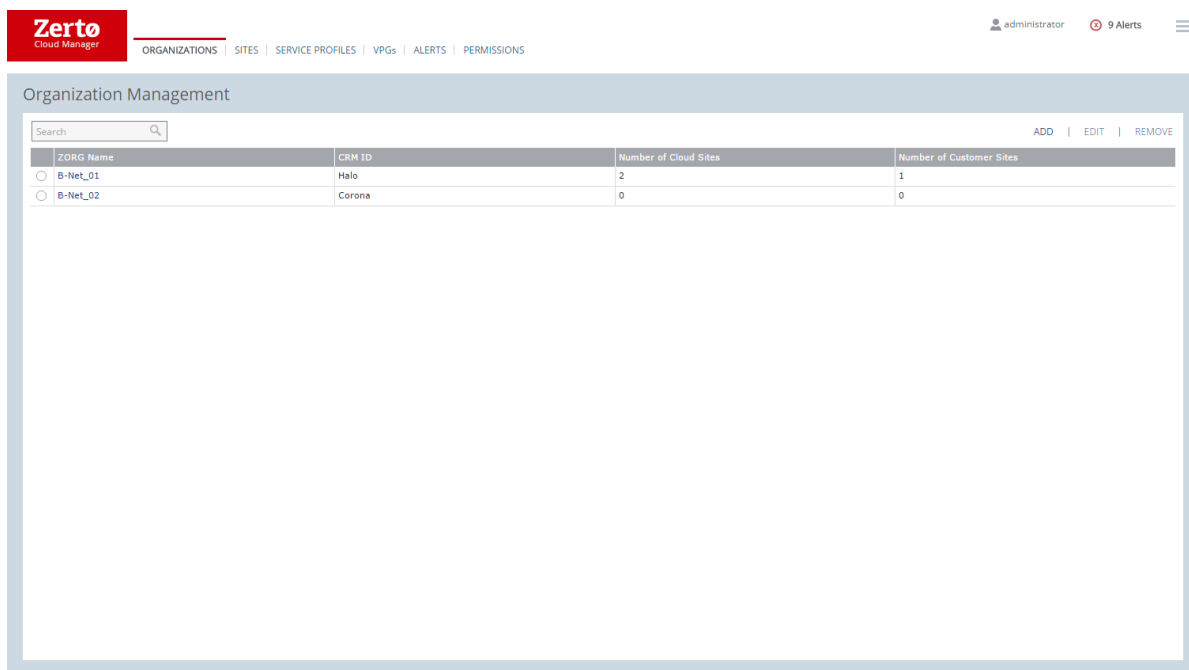
Displays the organization details in editable format.

- **ZORG Name:** The name of the organization.
- **CRM ID:** The optional identifier that identifies the organization in a CRM.
- **Preseed Folder Name:** The name of the folder containing the preseeded volumes. A preseed volume is 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 select the datastore and exact location, folder, and name of the preseeded disk. Zerto 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.

- **Manage VPGs:** When selected, the organization can create and edit virtual protection groups (VPGs) to protect groups of virtual machines together.
- **Failover Test:** When selected, the organization can test the failover of VPGs to verify that the disaster recovery that you have planned is the one being implemented.
- **Live Failover:** When selected, the organization can recover the virtual machines in a VPG after an unforeseen disaster.
- **Move:** When selected, the organization can migrate the virtual machines in VPGs to a remote site in a planned operation. ZORGS using DRaaS can also create offsite clones of the virtual machines in VPGs.
- **Prevent vApp operations during testing:** When vCD resources are specified in the vCD Cloud Resources tab, vApp operations are blocked when a VPG is being tested.
- **Custom Profile:** When selected, the organization can specify general settings for a VPG instead of using one of the provided sets of default properties when a VPG is created or edited. This permission is only relevant if the Manage VPGs permission is
- **ZORG ZSSP Login Credentials:** username and password required to log on to the ZSSP.

Organizations Tab



The screenshot displays the 'Organization Management' section of the Zerto Cloud Manager interface. At the top, there is a navigation bar with the Zerto logo and tabs for ORGANIZATIONS, SITES, SERVICE PROFILES, VPGs, ALERTS, and PERMISSIONS. The user is logged in as 'administrator' and there are '9 Alerts'. Below the navigation bar is a search bar and a table with the following data:

ZORG Name	CRM ID	Number of Cloud Sites	Number of Customer Sites
<input type="radio"/> B-Net_01	Halo	2	1
<input type="radio"/> B-Net_02	Corona	0	0

Displays the Zerto organizations, ZORGS, managed by the Zerto Cloud Manager.

- **ZORG Name:** The name of the organization.
- **CRM ID:** An optional identifier that identifies the organization in a CRM.
- **Number of Cloud Sites:** The number of cloud sites that the organization uses.
- **Number of Customer Sites:** The number of sites the organization has that use cloud sites for disaster recovery.

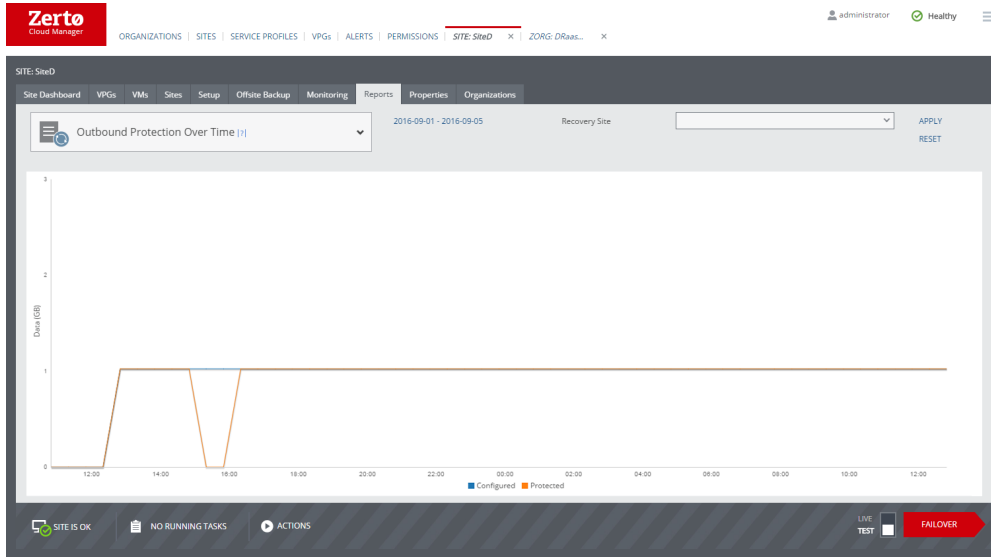
Clicking an organization name in the list, or selecting a row and then clicking **Edit**, displays another row of tabs:

Manage ZORG, Permissions, vCenter Cloud Resources, vCD Cloud Resources, Customer Sites, VPGs and Alerts.

Outbound Protection Over Time Report

Information about how much data is actually being protected against the amount configured for any of the sites can be displayed in the **Outbound Protection Over Time** report under the **REPORTS** tab.

The data displayed can be up to 30 minutes old, since the Zerto Virtual Manager collects the relevant data every 30 minutes.



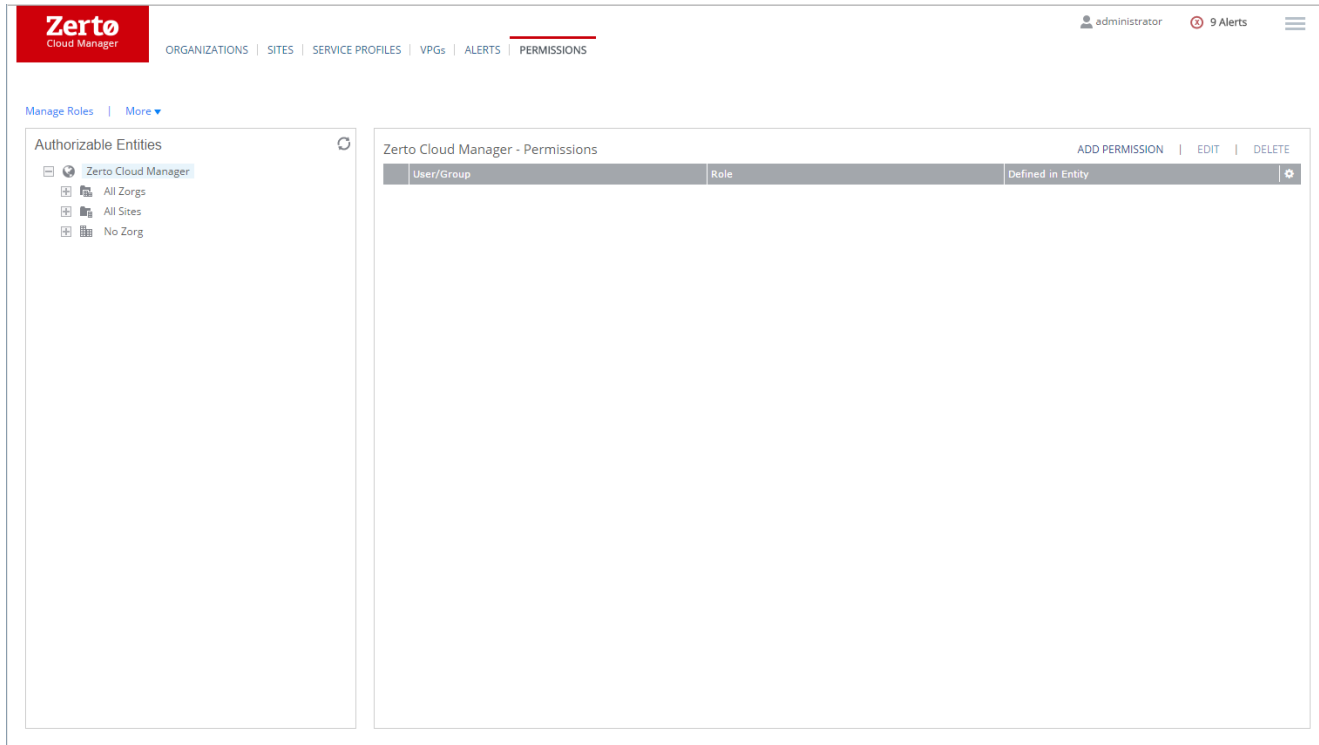
You can filter the information by the following:

- **From and To:** The dates for which you want information.
- **Recovery Site:** Select the site for which you want information or select all sites. If all sites are selected, **All** is displayed. The dropdown list displays all sites paired with the local site.

Click **APPLY** to apply the selected filtering and produce the report.

Click **RESET** to reset the display to the default values.

Permissions Tab

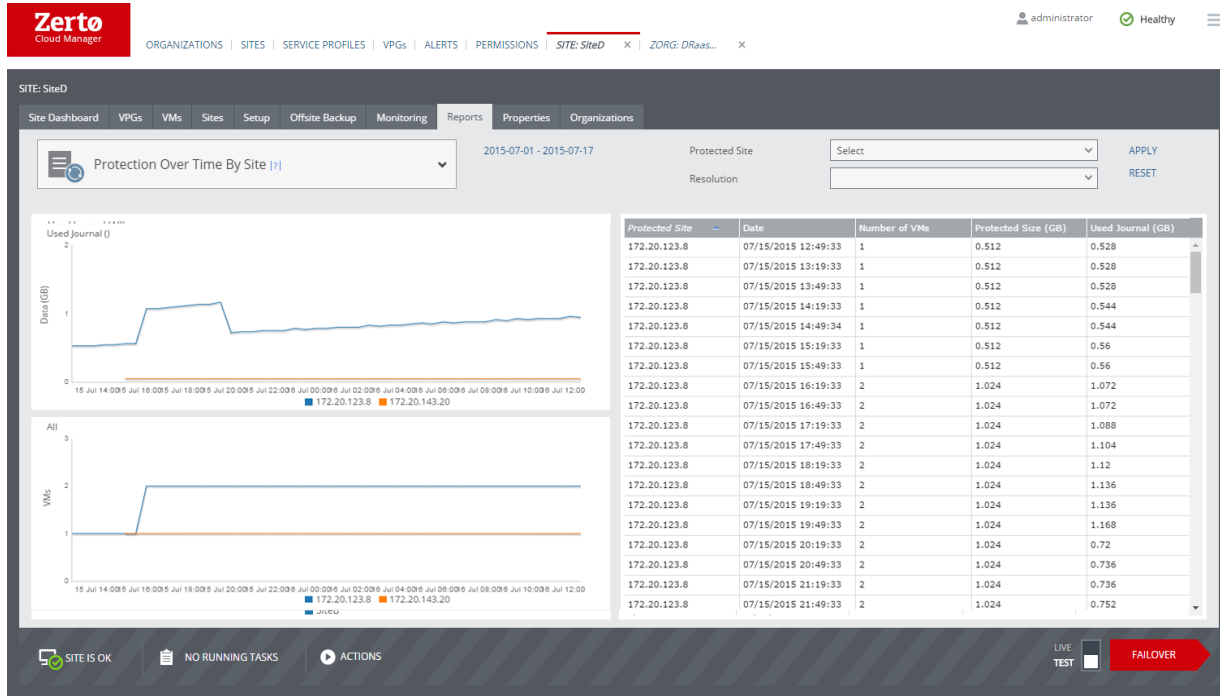


Enables adding, editing, or deleting permissions for Zerto entities and to manage roles for these entities.

Protection Over Time by ZORG Report

Information about the virtual machines and the amount of data on the recovery site can be displayed in the **Protection Over Time by Site** report under the **REPORTS** tab. When the report is displayed for the first time, information is shown per 30 minute intervals.

The data displayed can be up to 30 minutes old, since the Zerto Virtual Manager collects the relevant data every 30 minutes.



You can filter the information by the following:

- **From and To:** Select the dates for which you want information.
- **Protected Site:** Select the sites for which you want information. The list displays all sites paired with the local site.
- **Resolution:** Select the resolution for the report: daily, weekly, monthly, or All.

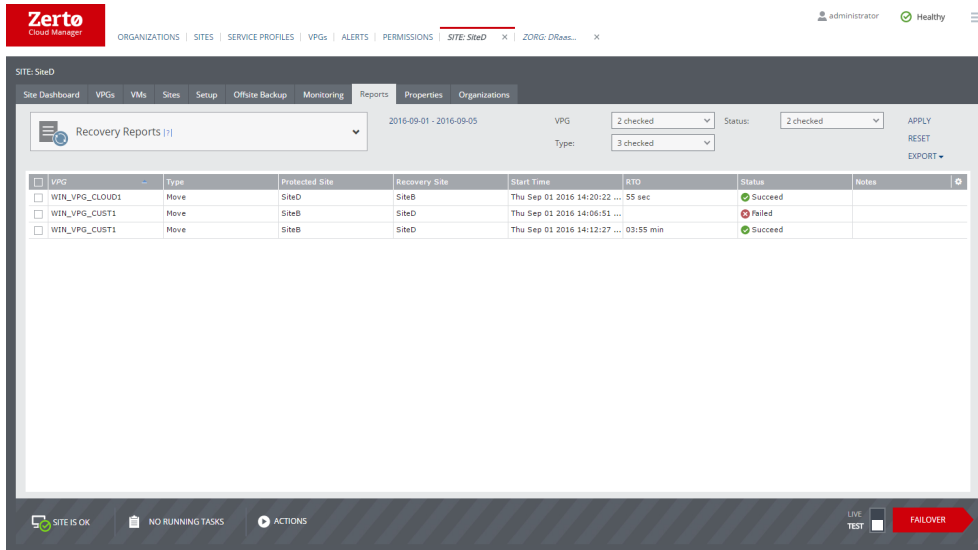
Click **APPLY** to apply the selected filtering and produce the report.

Click **RESET** to reset the display to the default values.

Note: By default, the **Protection Over Time By Site** report is only available for the last 90 days.

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.

Note: When FOT is in still in progress, the **end time** in the Recovery Report appears as **NA**.

The **Recovery operation start time** and **Recovery operation end time values** are shown in UTC according to the Zerto Virtual Manager clock in the recovery site. The **Point in time** value takes the checkpoint UTC time, which was created in protected site, and converts it to the recovery site time zone.

Branding the Recovery Report

A branded logo can be placed in the report in the top left corner by adding the logo as a .png file to the <ZertoInstallFldr>\Zerto\Zerto Virtual Replication\gui\ folder with the name provider_logo.png.

The folder ZertoInstallFldr is the root folder where Zerto in the recovery site is installed. For example, C:\Program Files\Zerto.

Redeploy Cloud Connector Dialog

The screenshot shows the 'Redeploy Cloud Connector' dialog box. It is divided into several sections:

- Site:** A dropdown menu showing 'Site5-Ent2-P2-R1'.
- VM Name:** A text input field containing 'Zerto-ZCC-ABC Company, Inc.-1'.
- Host:** A dropdown menu showing '[Cluster]172.20.99.3'.
- Datastore:** A dropdown menu showing 'ZNest123 MSFT Datastore (...)'. There is a small ellipsis icon to the right of the text.
- Organization Network:** A section with a dropdown menu set to 'VM Network' and three text input fields: 'Address: 172.20.89.11', 'Subnet Mask: 255.255.255.0', and 'Default Gateway: 172.20.255.12'.
- Cloud Network:** A section with a dropdown menu set to 'VM Network', two text input fields: 'Address: 172.20.99.13' and 'Subnet Mask: 255.255.255.0', and a dropdown menu for 'Static Route Group'.

At the bottom of the dialog are two buttons: 'CANCEL' and 'SAVE'.

Redeploy a ghost cloud connector. Some of the original values specified for the cloud connector must be used to redeploy the cloud connector, for example, the site where it will be redeployed. Specify the following values that are enabled:

- **Host and VM Name:** Specify the recovery host for the cloud connector virtual machine. The dropdown displays the hosts which do not have a cloud connector installed. You can change the host for the cloud connector. After specifying the host, the **VM Name** value is automatically updated to the original name with a number suffix added to make the name unique. After the name is displayed you can change it.
- **Datastore:** The datastore for the cloud connector virtual machine.
- **Organization Network:** The network details used by the customer. All the values from the original definition are fixed except for the network, which you can change:
 - **Network:** The name of the network from the list of available networks.
- **Cloud Network:** The local network details for the cloud service provider. All the values from the original definition are fixed except for the network and static group, which you can change:
 - **Network:** The name of the cloud-side network from the list of available networks.
 - **Static Route Group:** The name of the group for which static routes are defined to the Zerto Virtual Manager network and VRA network. If a static route group is not specified, it is assumed that the Zerto Virtual Manager and VRAs are on the cloud network.

Resource Report

Information about the resources used by the virtual machines being recovered to a particular site is displayed in the Resources report under the **REPORTS** tab. The information is collected at fixed times that are defined in the **Reports** tab of the **Site Settings** dialog in the recovery site. Information for the report is saved for 90 days when the sampling period is hourly and for one year when the sampling period is daily.

The report collects the resource information for the virtual machines being recovered to the site where the report is run.

If no virtual machines are recovered to the site where the report is run, the report is empty.

You can filter the information by the following:

From and **To:** The dates for which you want information.

Click **EXPORT** to generate the report, which is produced as an Excel file.

The information presented in this report is divided into three tabs:

Details Tab: Shows information for each protected virtual machine.

Performance Tab: Shows bandwidth and throughput information for each virtual machine in a table and in a graph.

Target Host Tab: Shows information per host in the recovery site.

Using a REST API to Generate a Report

Zerto 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 REST APIs), see the *Zerto Virtual Replication RESTful API Reference Guide*.

Details Tab

The **Details** tab includes the names and IDs of the virtual machines being protected and, for each virtual machine, the timestamp for the information, where it is protected, the CPU used, the memory used by the host and the guest, the storage used, and other information.

Interpreting the Details Tab

The **Details** tab provides a breakdown of every protected virtual machine, identified by its internal identifier and name in the hypervisor manager. The report also includes the name of the VPG that is protecting the virtual machine and information such as the protected and recovery sites, the protected and recovery vCD Org, cluster, etc.

The Timestamp column displays the time when the last sample, as defined in the Reports tab of the Site Settings dialog, was taken.

The VPG Type column is one of:

- VC2VC: vCenter to vCenter replication
- VC2VCD: vCenter to vCloud Director replication
- VCD2VCD: vCloud Director to vCloud Director replication
- VCD2VC: vCloud Director to vCenter replication

The ZORG column defines organizations set up in the Zerto Cloud Manager that use a cloud service provider for recovery.

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: $(currentValue - valueInLastSample) / elapsedTime$

For example:

TIME	ACTION/DESCRIPTION
2:29:59.999	A virtual machine is placed in a VPG
2:30	A sample is generated. The total transmitted bytes is zero since the virtual machine was just placed in the VPG
2:30-2:59.999	The VM is writing data at 1MB/minute
3:00	The virtual machine lowers its write rate to 0.5MB/minute
3:30	A new sample is calculated. Current value of total data transmitted is 45MB: $1MB/minute * (30 \text{ minutes}) + (0.5MB/minute) * (30 \text{ minutes})$ Last value of total data transmitted is 0, from the 2:30 sample. $Bandwidth = (45MB - 0) / (60 \text{ minutes}) = 0.75MB/minute = 13107Bps$

Report output fields

The following describes the fields in the **Details** tab.

PARAMETER	DESCRIPTION
Active Guest Memory (MB)	The active memory of the virtual machine.
Bandwidth (Bps)	The average bandwidth used between two consecutive samples, in bytes per second.
Consumed Host Memory (MB)	The amount of host memory consumed by the virtual machine.
CPU Limit (MHz)	The maximum MHz available for the CPUs in the virtual machine.
CPU Reserved (MHz)	The MHz reserved for use by the CPUs in the virtual machine.
CPU Used (MHz)	The MHz used by the CPUs in the virtual machine.
Crmlid	The CRM identifier specified in Zerto Cloud Manager for an organization that uses a cloud service provider for recovery.
Memory (MB)	The virtual machine defined memory.
Memory Limit (MB)	The upper limit for this virtual machine's memory allocation.
Memory Reserved (MB)	The guaranteed memory allocation for this virtual machine.
Number Of vCPUs	The number of CPUs for the virtual machine.
Number Of Volumes	The number of volumes attached to the virtual machine.
Recovery Journal Provisioned Storage (GB)	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.
Recovery Journal Used Storage (GB)	<p>The amount of journal storage used by the virtual machine.</p> <p>Differences might occur between the value displayed in the Used Journal column in the <i>Protection Over Time by Site</i> report and the value displayed here, which is retrieved from vCenter or Hyper-V.</p> <p>The Used Journal value displayed in the <i>Protection Over Time by Site</i> report is calculated by the VRA, based on internal journal allocations for each recovery volume.</p> <p>vCenter and Hyper-V Resources reports are expected to display a larger size than in the <i>Protection Over Time by Site</i> report, and may reach up to 500MB higher per virtual machine than reported in the <i>Protection Over Time by Site</i> report.</p>
Recovery Volumes Provisioned Storage (GB)	The amount of provisioned storage for the virtual machine in the target site. This value is the sum of volumes' provisioned size.
Recovery Volumes Used Storage (GB)	The amount of storage used by the virtual machine in the target site.
Service Profile	The service profile used by the VPG.
Source Cluster	The source cluster name hosting the virtual machine.
Source Host	The source host name hosting the virtual machine.
Source Organization VDC	The name of the source vDC organization.
Source Resource Pool	The source resource pool name hosting the virtual machine.
Source Site	The source protected site name, defined in the Zerto User Interface.
Source vCD Organization	The name of the source vCD organization.
Source Volumes Provisioned Storage (GB)	The amount of provisioned storage for the virtual machine in the source site. This value is the sum of volumes' provisioned size.
Source Volumes Used Storage (GB)	The amount of storage used by the virtual machine in the source site. This value is the sum of the volumes' used size.
Source VRA Name	The name of the source VRA used to send data to the recovery site.

PARAMETER	DESCRIPTION
Target Cluster	The target cluster name hosting the virtual machine.
Target Datastores	The target storage used by the virtual machine if it is recovered.
Target Host	The target host name hosting the virtual machine when it is recovered.
Target Organization vDC	The name of the target vDC organization.
Target Resource Pool	The target resource pool name where the virtual machine will be recovered.
Target Site	The target site name, defined in the Zerto User Interface.
Target Storage Policy	The target vCD storage policy used.
Target vCD Organization	The name of the target vCD organization.
Target VRA Name	The name of the VRA managing the recovery.
Throughput (Bps)	The average throughput of the VM used between two consecutive samples, in bytes per second.
Timestamp	The date and time the resource information was collected. The value can be converted to an understandable date using code similar to the following: <pre>var date = new Date(jsonDate);</pre> or code similar to the Perl code example, <code>jsonDateToString(\$)</code> , described in <i>Zerto Virtual Replication RESTful API Reference Guide</i> .
VM Hardware Version	The VMware hardware version.
VM Id	The internal virtual machine identifier.
VM Name	The name of the virtual machine.
VPG Name	The name of the VPG.
VPG Type	The VPG type: VCVpg: VMware vCenter Server VCvApp: Deprecated VCDvApp: VMware vCloud Director vApp PublicCloud: Amazon WebServices or Microsoft Azure HyperV: Microsoft SCVMM
ZORG	The name assigned to an organization using a cloud service provider for recovery. The name is created in the Zerto Cloud Manager. For details, see the <i>Zerto Cloud Manager Administration Guide</i> .

Performance Tab

The Performance tab shows bandwidth and throughput information for each virtual machine per sampling period in a table and in a graph. The Performance tab enables the user to view the total bandwidth and throughput per sampling period.

The graph allows the user to view performance trends over time per VM.

For full explanation of the bandwidth and throughput information, refer to the [“Details Tab”, on page 101](#).

You can filter information by date and VM name.

The following describes the fields in the **Performance** tab:

PARAMETERS	DESCRIPTION
Time Stamp	For explanation see the Details tab.
Bandwidth (Bps)	The average bandwidth of the VM used between two consecutive samples, in bytes per second.
Throughput (Bps)	The average throughput of the VM used between two consecutive samples, in bytes per second.

PARAMETERS	DESCRIPTION
Total Bandwidth	The total bandwidth of all VMs during the measured period.
Total Throughput	The total throughput of all VMs during the measured period.

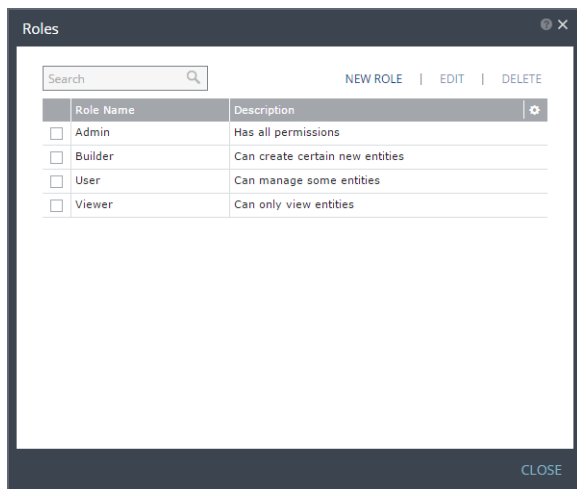
Target Host Tab

The Target Host tab shows information per host in the recovery site. This enables the user to perform capacity planning on the recovery host. You can filter information by time and by host.

The following describes the fields in the **Target Host** tab.

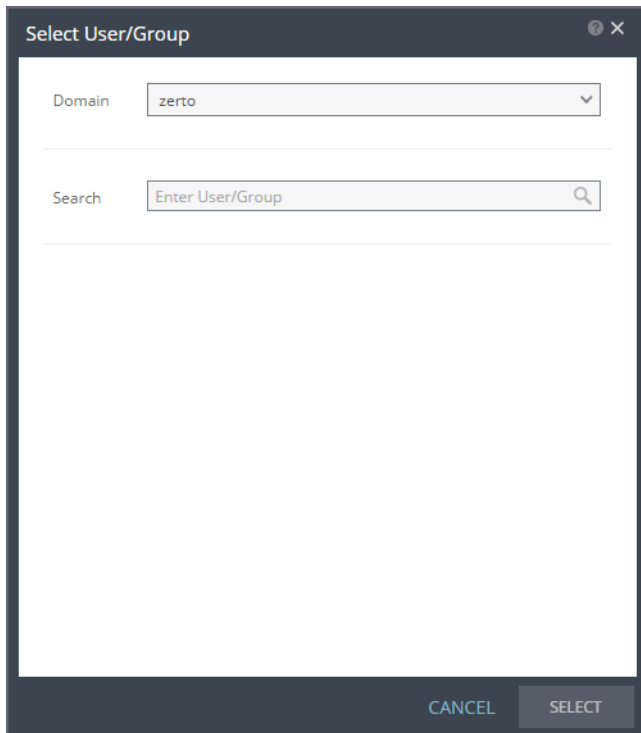
PARAMETERS	DESCRIPTION
Active Guest Memory (MB)	The active memory of the virtual machine.
CPU Used (MHz)	The MHz used by the CPUs in the virtual machine.
Host	The Target Host's IP address or DNS name.
Total Bandwidth	The total bandwidth of all VMs replicating to the host during the measured period.
Total Throughput	The total throughput of all VMs replication to the host during the measured period.
vCPUs	The number of CPUs for the virtual machine.
VMs	The number of VMs protected.
Volumes	The number of volumes attached to the virtual machine.

Roles Dialog



Enables adding new roles and editing or deleting existing roles.

Select User/Group Dialog

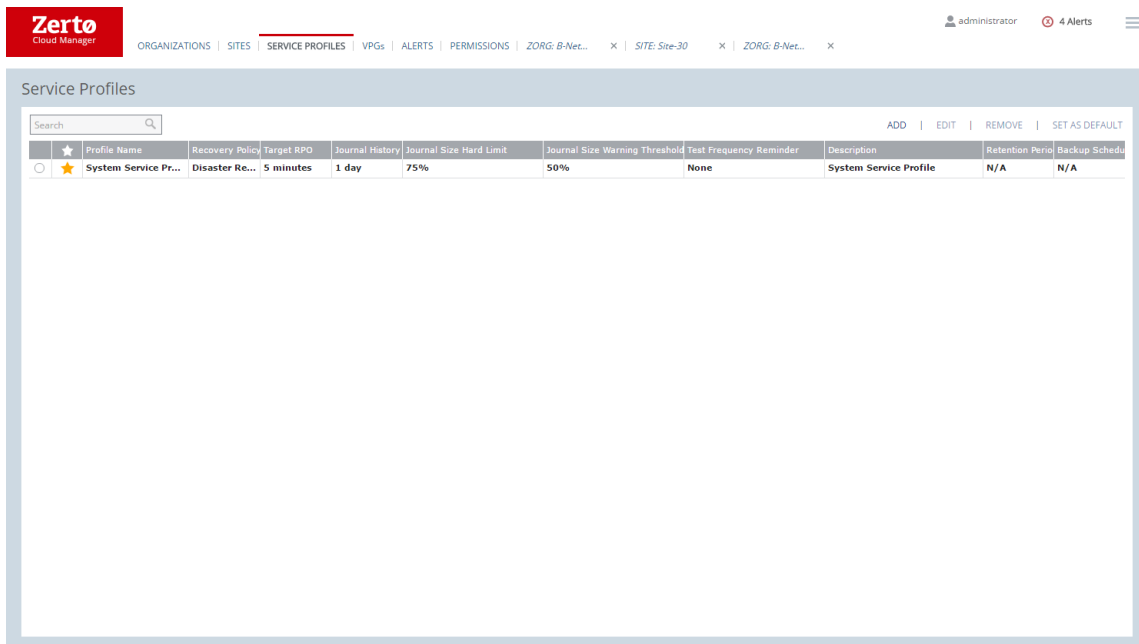


The dialog box is titled "Select User/Group". It contains a "Domain" dropdown menu with "zerto" selected. Below it is a "Search" input field with the placeholder text "Enter User/Group". At the bottom, there are two buttons: "CANCEL" and "SELECT".

Enables the selection of users and groups for the Active Directory domain and at least two characters of the user or group name that exists in the Active Directory.

After entering the search criteria, click **Enter** to display the results of the search to enable selecting a user or group.

Service Profiles Tab



The screenshot shows the Zerto Cloud Manager interface. The top navigation bar includes the Zerto logo and menu items: ORGANIZATIONS | SITES | SERVICE PROFILES | VPGs | ALERTS | PERMISSIONS | ZORG: B-Net... | SITE: Site-30 | ZORG: B-Net... The user is logged in as administrator with 4 Alerts. The main content area is titled "Service Profiles" and contains a search bar and a table of service profiles.

	Profile Name	Recovery Policy	Target RPO	Journal History	Journal Size Hard Limit	Journal Size Warning Threshold	Test Frequency Reminder	Description	Retention Period	Backup Schedule
<input type="radio"/>	★ System Service Pr...	Disaster Re...	5 minutes	1 day	75%	50%	None	System Service Profile	N/A	N/A

Defines a set of default properties to use when VPGs are defined or edited.

The first column contains a star in the row of the default service profile.

- **Profile Name:** A name used to identify the service profile.
- **Recovery Policy:** Disaster Recovery enables replication and recovery.
- **Target RPO:** The maximum desired time between each automatic checkpoint being written to the journal before an alert is issued. In reality checkpoints are written more frequently.
- **Journal History:** The time for which all write commands are saved in the journal. Each protected virtual machine has a dedicated journal volume on the recovery site associated with the replicated virtual machine. This enables journal data to be maintained, even when changing the recovery host for the recovery. When specifying a checkpoint to recover to, the checkpoint must still be in the journal. For example, if the value specified here 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.

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, with the same size as the journal for that virtual machine. The size of the scratch volume determines the length of time that you can test for. The larger the volume, the longer the testing can continue, assuming the same rate of change being tested. If the journal history required is small, for example two or three hours, the scratch volume that is created for testing will be small as well, limiting the time available for testing. Thus, when considering the journal history you should also consider the length of time you will want to test the VPG.

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

- **Journal Size Hard Limit:** The maximum size that the journal can grow, as a percentage of the virtual machine volume size rounded up to the first equal-or-higher value in the following list, all in GBs: 10, 15, 20, 25, 30, 35, 40, 45, 50, 75, 100, 150, 200, 250, 300, 400, 500, 750, 1000. Thus, a value of 12%, when the virtual machine has 100GB being protected, means 12GB for the journal, which is then rounded up to 15GB. The minimum journal size is 10GB. Each journal is defined as thin-provisioned and cannot be thick-provisioned, even when a SAN disk, which is natively thin-provisioned, is used.
- **Journal Size Warning Threshold:** The size of the journal that triggers a warning that the journal has neared its hard limit, as a percentage of the virtual machine volume size.
- **Test Frequency 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.
- **Description:** A description of the service profile.

Sites Tab

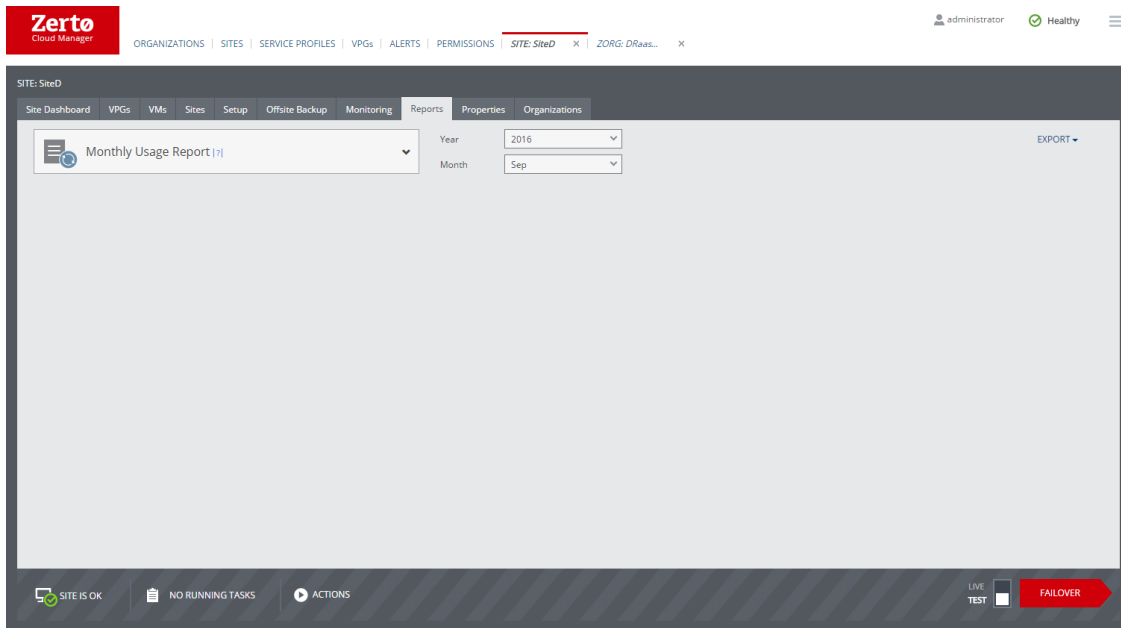
The screenshot displays the 'Sites Management' section of the Zerto Cloud Manager interface. At the top, there is a navigation bar with the Zerto logo and a menu containing 'ORGANIZATIONS', 'SITES', 'SERVICE PROFILES', 'VPGs', 'ALERTS', 'PERMISSIONS', and 'ZORG: B-Net...'. The 'SITES' tab is currently active. Below the navigation bar, there is a search input field and three action buttons: 'ADD', 'EDIT', and 'REMOVE'. The main content area features a table with the following data:

Connection Status	Site Name	Version	Host Name	Port	Type	# of ZORGs	ZVM Interface
<input checked="" type="checkbox"/> Connected	Site-30	5.0	172.20.99.30	9080	VCenter	1	Open
<input checked="" type="checkbox"/> Connected	Site-50	5.0	172.20.99.50	9080	vCD	1	Open

Enables adding sites and editing or deleting existing sites.

- **Connection Status:** Whether the site is connected or not. If the site is disconnected, check the status of the Zerto Virtual Manager service.
Note: If the site identifier was changed, the Connection Status shows the following: "Site identifier was changed. Please remove the site and then reconnect to it."
- **Site Name:** The name of the site, specified when installing the Zerto Virtual Manager, or after installation by editing the site configuration in the Zerto User Interface.
- **Host Name:** The IP address of the machine where the Zerto Virtual Manager service runs.
- **Port:** The port specified during installation to be used to access the Zerto Virtual Manager.
- **Type:** Whether the Zerto Virtual Manager communicates with vCloud Director or only a vCenter Server.
- **# of ZORGs:** The number of Zerto organizations, ZORGs, that will recover to this site.
- **ZM Interface:** Whether it is possible to open the Zerto User Interface.

Usage Report



Information about usage can be displayed in the **Monthly Usage** report under the **REPORTS** tab. The Monthly Usage Report can only be viewed with a cloud license.

The information is organized by organization and within each organization by site, then virtual protection group (VPG) and then by the virtual machines in each VPG.

This report is mostly used by cloud service providers.

You can filter the information by the following:

- **Year:** The year of interest.
- **Month:** Select the month to review.

For each month, the usage report displays the number of virtual machines protected during the month and the average number per day in the month. For example, if fifteen virtual machines are protected in a few VPGs starting on the 28th of the month in a thirty day month, the total days will be 30 (two days multiplied by fifteen machines) and the VM Count will be 1 (Total days divided by the number of days in the month).

Click **EXPORT** to a CSV or ZIP file to generate the report.

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

vCD Cloud Resources Tab

Displays the vCD resources available to the organization in editable format.

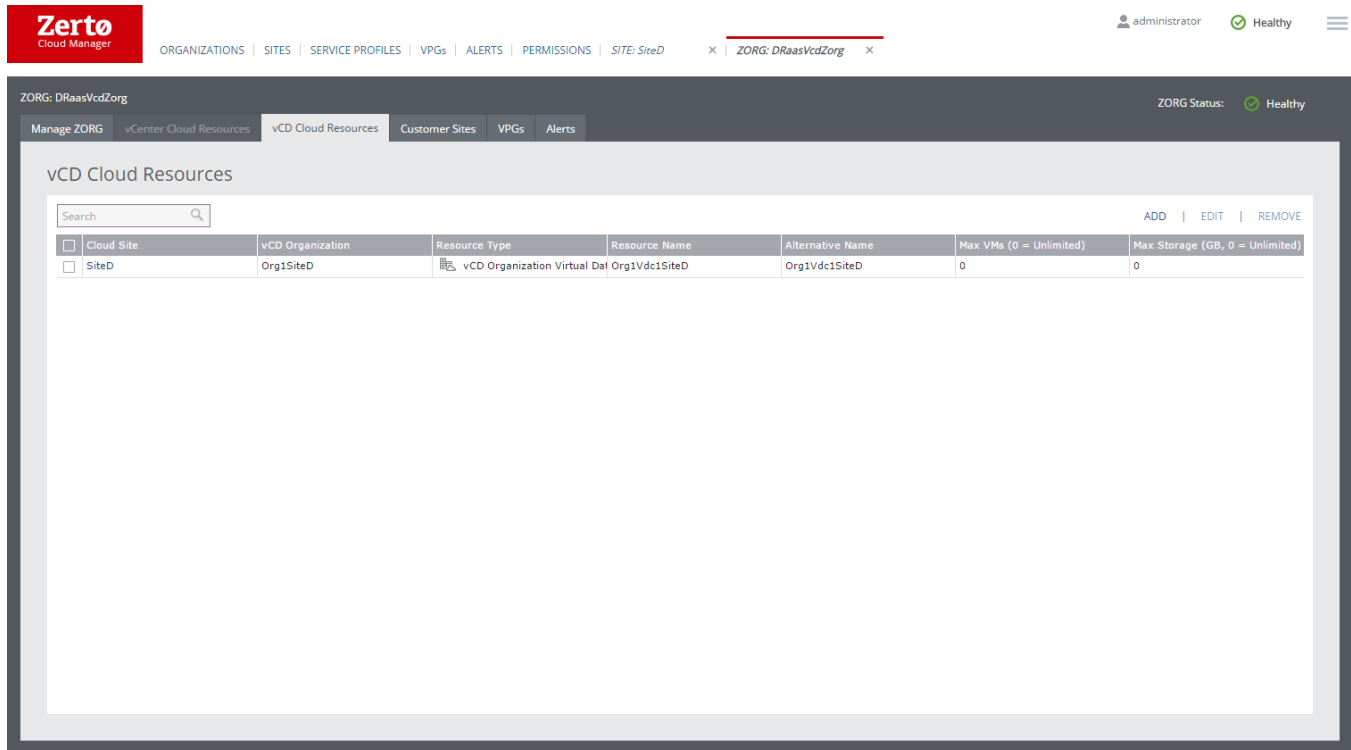
Note: If a site has vCD configured for the Zerto Virtual Manager, the underlying vCenter resources for that site cannot be used.

ZORG uses specified cloud sites. If the cloud site uses vCD you can select the cloud site to be used for recovery and for each vCD cloud site you can limit the number of virtual machines and storage that the organization is able to protect.

- **Cloud Site:** A link to open the details of the cloud site.
- **vCD Organization:** The vCD organization name.
- **Org vDC:** The organization vDC.
- **Max VMs:** The maximum number of virtual machines the organization can recover.

- **Max Storage:** The maximum amount of storage the organization can recover.

vCenter Cloud Resources Tab



Displays the vCenter resources available to the ZORG in editable format. Organizations use specified cloud sites. Each site has specific resources and you can select the resources you want to be made available to the specific organization as well as rename the information to something useful to the organization, hiding the internal naming conventions of the cloud site. You can also limit the number of virtual machines and storage that the organization is able to protect.

- **Cloud Site:** A link to open the details of the cloud site.
- **Resource Type:** The type of resource: Datastore, Network, or Resource Pool. You must have a resource pool in the list of resources, since all recovery of VPGs, when the recovery site is defined in Zerto Cloud Manager, is to a resource pool.
Note: If DRS is disabled for the site, later on all resource pools are removed by VMware and the recovery of affected VPGs to this site is halted until new resource pools are defined and assigned to Zerto organizations in Zerto Cloud Manager and then to all the VPGs.
- **Resource Name:** The cloud name for the resource.
- **Alternative Name:** The name the organization sees for the resource.
- **Max VMs:** The maximum number of virtual machines the organization can recover to the specified resource pool.
- **Max Storage:** The maximum amount of storage the organization can recover to the specified Datastore.

VMs Tab in the Zerto Virtual Manager

GENERAL View

The following information is displayed in the GENERAL view:

- **Alert status indicator:** The color indicates the status of the VPG:
 - **Green:** The VPG is being replicated, including syncing the VPG between the sites.

- **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the **Target RPO Alert** value specified for the VPG.
- **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.
- **VM Name:** The name of the virtual machine. The name is a link.
- **VPG Name:** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab.
- **Direction:** The direction of the replication, from this site to the remote site or from the remote site to this site.
- **Peer Site:** The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.
- **Priority:** The priority of the VPG.
- **Protection Status:** The current status of the virtual machine, such as **Meeting SLA**. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **State:** The current substatus of the VPG, such as **Delta syncing**. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **Actual RPO:** The time since the last checkpoint was written to the journal. This should be less than the Target RPO Alert value specified for the VPG.
- **Operation:** The operation, such as Move, that is currently being performed.

PERFORMANCE View

The following information is displayed in the PERFORMANCE view:

- **IO:** The IO per second between all the applications running on the virtual machine and the VRA that sends a copy to the remote site for replication.
- **Throughput:** The MB per second for all the applications running on the virtual machines being protected. There can be a high IO rate with lots of small writes resulting in a small throughput as well as a small IO with a large throughput. Thus, both the IOPS and Throughput values together provide a more accurate indication of performance.
- **Network:** The amount of WAN traffic.
- **Provisioned Storage:** The provisioned storage for the virtual machine in the recovery site.
Note: For virtual machines in a VMware environment, this value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Web client or 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.
Note: For virtual machines in a VMware environment, this value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Web client or Client console per virtual machine in the **Virtual Machines** tab for the root vCenter Server node.

VPG Performance Report

Performance graphs for all VPGs or for an individual VPG can be seen in the **VPG Performance** report under the **REPORTS** tab. These graphs show more detailed resolution than the corresponding graphs in the **DASHBOARD** tab.

You can specify the VPGs whose performance should be displayed. When you request information about multiple VPGs, each VPG is shown in a different color, with a key at the top of the report that maps each color to the VPG it represents.

Position the cursor on a graph line to see exact information about that point.

Click **APPLY** to apply the selected filtering and produce the report.

Click **RESET** to reset the display to the default values.

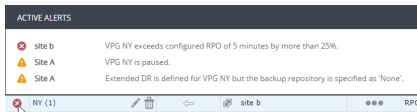
VPGs Tab in the Zerto Virtual Manager

List View - GENERAL

The following information is displayed in the GENERAL view:

- **Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:
 - **Green:** The VPG is being replicated, including syncing the VPG between the sites.
 - **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
 - **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the **Alert status indicator** to display details of the alert.



- **VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab. The number of VMs protected in the VPG is displayed in parentheses.
- **Direction:** The direction of the replication, from this site to the remote site or from the remote site to this site.
- **Peer Site:** The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.
- **Priority:** The priority of the VPG.
- **Protection Status:** The current status of the VPG, such as **Meeting SLA**. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **State:** The current substatus of the VPG, such as Delta syncing. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **Actual RPO:** The time since the last checkpoint was written to the journal. This should be less than the Target RPO Alert value specified for the VPG.
- **Operation:** The operation, such as Move, that is currently being performed.

List View - PERFORMANCE

The following information is displayed in the PERFORMANCE view:

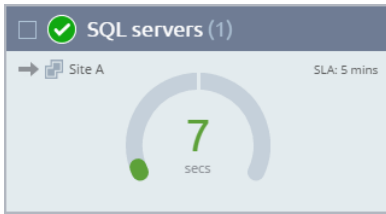
- **IO:** The IO per second between all the applications running on the virtual machines in the VPG and the VRA that sends a copy to the remote site for replication.
- **Throughput:** The MB per second for all the applications running on the virtual machines being protected. There can be a high IO rate 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.

List View - RETENTION STATUS

- **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.

Grid View

In the grid view each VPG is displayed as a card.



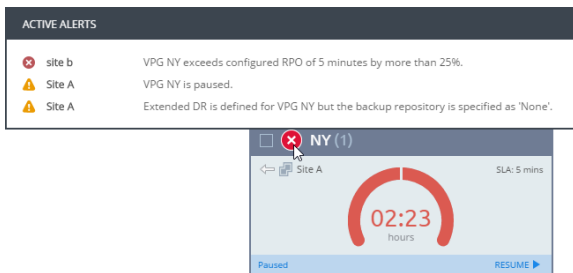
The default view is of all the VPG cards, un-grouped and sorted by VPG name.

The cards displayed can be filtered by clicking the filter button (☰). The default filters are Direction and Protection Status. You can click the **ADD** button to open the filters drop-down, and select additional filters. Active filters are displayed with a yellow background.

Each card contains the following:

- **Alert status indicator:** The color indicates the status of the VPG. Hovering over the alert displays a popup of all active alerts with descriptions:
 - **Green:** The VPG is being replicated, including syncing the VPG between the sites.
 - **Orange:** The VPG is being replicated but there are problems, such as an RPO value larger than the Target RPO Alert value specified for the VPG.
 - **Red:** The VPG is not being replicated, for example, because communication with the remote site is down.

Move the cursor over the **Alert status indicator** to display details of the alert.



- **VPG Name (#VMs):** The name of the VPG. The name is a link: Click the VPG name to drill-down to more specific details about the VPG that are displayed in a dynamic tab. The number of VMs protected in the VPG is displayed in parentheses.
- **Direction:** The direction of the replication, from this site to the remote site or from the remote site to this site.
- **Peer Site:** The name of the site with which this site is paired: the site where the VPG is protected or will be recovered to.
- **State:** The current substatus of the VPG, such as **Delta syncing**. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **Actual RPO:** The time since the last checkpoint was written to the journal. This should be less than the **Target RPO Alert** value specified for the VPG.
- **Operation:** The operation, such as Move, that is currently being performed.

Saving Details of Virtual Protection Groups to 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.

VPGs Tab in the Zerto Cloud Manager

The screenshot shows the Zerto Cloud Manager interface with the VPGs tab selected. The table displays the following data:

Direction	Peer Site	ZORG	Name	Protection Status	State	Priority	# VMs	Last Test
↔	siteA	ABC Company, Inc.	Clients	Meeting SLA		●●●○	4	
↔	siteC	ABC Company, Inc.	Forex Trading	Meeting SLA		●●●○	1	
↔	NYC	ABC Company, Inc.	Operations	Meeting SLA		●●●○	1	
↔	siteA		Reconciliation - Back Office	Meeting SLA		●●●○	1	

Lists details of VPGs from all sites defined in the Zerto Cloud Manager.

When you right-click anywhere in this display, a menu is displayed in which you can choose **Edit Columns**. After you select it, the **Edit Columns dialog** is displayed, in which you can specify what columns to display in the list. You can also drag-and-drop column headers to rearrange the order of the columns. A thick vertical bar shows where a column can be dragged and dropped. You can also reset the display to the default display by clicking **Reset Columns**.

You can filter the display by clicking the filter icon in a column heading. Depending on the contents of the column, you can either choose filter values from the dropdown list that is displayed, or you can enter a value in the text box that is displayed. For example, you can filter the values in the Protection Status column by choosing Initializing, Meeting SLA, or Not Meeting SLA, or a combination of these values. You can filter the values in the name column by entering a value in the text box. The filter icon becomes visible when a filter is applied. Click **Clear** in the filter field to clear the filter.

- **Alert status indicator:** The color indicates the alert status of the VPG:
 - **Green:** The VPG is being replicated, including syncing the VPG between 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.
- **Peer Site:** The name of the site with which this site is paired: the site where the VPG is currently located or will be recovered to. After the name, there is an icon that represents the type of site.
- **ZORG:** The name given to an organization in Zerto Cloud Manager.
- **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 is displayed in a dynamic tab.
- **Protection Status:** The current status of the VPG, such as Initializing or Meeting SLA. Where appropriate, the percentage of the operation completed, such as syncing, is displayed.
- **Priority:** The priority specified for the VPG.
- **# VMs:** The number of VMs in the VPG.
- **Provisioned Storage:** The provisioned storage for all virtual machines in the VPG.

Note: For virtual machines in a VMware environment, this value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Web client or 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 vCenter Server and displayed in the vSphere Client console per virtual machine in the **Virtual Machines** tab for the root vCenter Server node.
Note: For virtual machines in a VMware environment, this value is the sum of the values that are used in the vCenter Server and displayed in the vSphere Web client or Client console per 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 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.
 - **Network:** The amount of WAN traffic.
 - **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.
 - **Last Test:** The date and time of the last failover test performed on this VPG.
 - **Retention Policy:** Whether the VPG is protected against a disaster only with the ability to recover to a point in time up to 30 days before the disaster, or protection is extended to include retention sets of the virtual machines, going back for a maximum of one year.
 - **Retention Policy Status:** The status of the retention set.
 - **Repository Name:** The name of the repository where the jobs are stored.
 - **Restore Point Range:** The restore points for the retention job out of the total retention jobs run for the VPG.
 - **Retention Policy Scheduling:** The schedule for the retention process.

VRAs Tab in the Zerto Virtual Manager

You can filter information in columns via the filter icon next to each column title. You can also sort the list by each column.

General View

In this view, the number of installed VRAs is displayed in the **VRAs** tab. The following information is displayed in this view:

- **Cluster:** The cluster name, if relevant.
- **Host Address:** The host IP address for the VRA. If the host is part of a cluster, the cluster name is displayed with the hosts under the cluster.
- **Host Version:** The host version.
- **Alert Status:** The status of alerts in the VRA virtual machine.
- **VRA Name:** The name of the VRA virtual machine.
- **VRA Status:** The VRA status. For example, Installed or Ghost VRA.
- **VRA Version:** Either Latest if the version installed is the most current version or Outdated if it can be upgraded. A tooltip displays the actual version.
- **VRA Address:** The IP address of the VRA virtual machine.
- **# VPGs:** The number of VPGs with a virtual machine for which the VRA either manages the protection or the recovery of the data.
- **# VMs:** The number of virtual machines managed by the VRA.

SETTINGS View

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

- **VRA Group:** The group of VRAs to which this VRA belongs. When VRAs use different networks, they can be grouped by network.
- **VRA RAM:** The amount of memory allocated to the VRA to buffer data before it is sent to the recovery site or at the recovery site before it is written to the journal.
- **Datastore:** The datastore used by the VRA.
- **Datastore Cluster:** The datastore cluster used by the VRA, if relevant.

WORKLOAD PROTECTION View

The following information is displayed in the **WORKLOAD PROTECTION** view:

- **# VPGs:** The number of VPGs with a virtual machine for which the VRA is used either for protection or recovery.
- **# VMs:** The number of virtual machines for which the VRA is used either for protection or recovery.
- **# of Protected VPGs:** The number of VPGs with a virtual machine for which the VRA manages the protection of their data.
- **# of Protected VMs:** The number of virtual machines for which the VRA manages the protection of their data.
- **# of Protected Volumes:** The number of volumes for which the VRA manages the protection of their data.
- **# of Recovery VPGs:** The number of VPGs with a virtual machine for which the VRA manages the recovery of the data.
- **# of Recovery VMs:** The number of virtual machines for which the VRA manages the recovery of the data.
- **# of Recovery Volumes:** The number of volumes for which the VRA manages the recovery of the data.

Additional Fields

There are additional fields that you can display that are listed when you select **Show/Hide Columns** from the dropdown list shown by clicking the configuration icon (⚙):

- **Cluster:** The cluster with the host used by the VRA.
- **VC Network:** The network used by the VRA.
- **# Volumes:** The number of volumes for which the VRA manages the protection or recovery of data.

A			
alerts	69	ickdr	59
for ZORGs	72	in cloud disaster recovery	59
AMQP		J	
Erlang OTP	26, 28, 85, 87	journal	43, 79, 106
installation	28, 85, 87	L	
RabbitMQ	26, 28, 85, 87	license	21
B		logon to Zerto Cloud Manager	16
bandwidth		M	
in resources report	101	Manage cloud connector	
branding the Recovery report	99	VMware administrator permission	67
C		manage VPG permissions	33, 95
cloud connector		move	
ghost	74	permission to perform	33, 95
orphaned	76	O	
cloud service provider	59	orphaned cloud connector	76
configuring sites	18	Outbound Protection Over Time report	96
configuring ZORGs	30	P	
CRM ID	31, 94, 95	pairing	84
D		pairing sites	22
DRaaS	6	permission	
architecture	12	setting VMware	67
initial configuration	10	to manage VPGs	33, 95
setting up	57–58	to perform a failover	33, 95
E		to perform a failover test	33, 95
export to CSV		to perform a move	33, 95
VPG details	112	to perform vApp operations	33, 95
F		to update Manage cloud connector	67
failover		to update profile settings	33, 95
permission to perform	33, 95	permissions, assigned to ZORG	97
failover test		preseeded volumes	
permission to perform	33, 95	folder location	32
G		Protection Over Time by Site report	98
ghost cloud connector	74	provisioned storage	110, 111
I		R	
ICDR	6	RabbitMQ	
architecture	15	Erlang OTP	26, 28, 85, 87
initial configuration	10	installation	28, 85, 87
J		Recovery report	99
journal	43, 79, 106	branding	99
L		registering sites	20
license	21	reports	
logon to Zerto Cloud Manager	16	Outbound Protection Over Time	96
M		Protection Over Time by Site	98
Manage cloud connector			
VMware administrator permission	67		
manage VPG permissions	33, 95		
move			
permission to perform	33, 95		
O			
orphaned cloud connector	76		
Outbound Protection Over Time report	96		
P			
pairing	84		
pairing sites	22		
permission			
setting VMware	67		
to manage VPGs	33, 95		
to perform a failover	33, 95		
to perform a failover test	33, 95		
to perform a move	33, 95		
to perform vApp operations	33, 95		
to update Manage cloud connector	67		
to update profile settings	33, 95		
permissions, assigned to ZORG	97		
preseeded volumes			
folder location	32		
Protection Over Time by Site report	98		
provisioned storage	110, 111		
R			
RabbitMQ			
Erlang OTP	26, 28, 85, 87		
installation	28, 85, 87		
Recovery report	99		
branding	99		
registering sites	20		
reports			
Outbound Protection Over Time	96		
Protection Over Time by Site	98		

Recovery	99
Resources	100
Usage	108
VPG Performance	110
Resources report	100
generating with REST API	101
output	102

S

security certificate	
adding	22
security certificate, adding	22
service profile	
configuring	42
customizing	33, 95
site	
configuring	18
registering	20
standalone portal, ZSSP	60
storage	
provisioned	110, 111
storage profile	103

U

Usage report	108
--------------------	-----

V

v	
vApp operations	33, 95
vCD	
setting up access	27
VIB	25, 83, 91
Virtual Backup Appliance, see VBA	
Virtual Replication Appliance, see VRA	
VMware permissions, setting	67
VPG	
saving details to file	112
VPG Performance report	110
VRA	
definition	
installing	23, 25
requirements	23
setting up routing	24

Z

ZCC	
definition	13
ghost cloud connector	74
orphaned	76
vMotioning to another host	75
Zerto Cloud Connector, see ZCC	
Zerto Cloud Manager	
CRM ID	31
definition	6
Zerto Self-service Portal, see ZSSP	
Zerto Virtual Manager	
definition	7
Zerto Virtual Replication	
benefits	11
components	6
definition	5
ZORG	
alerts	72
configuring	30
managing	70
ZSSP	10
architecture	59
branding	66
definition	59
security	62
setting up	59–60
standalone portal	60
ZVM, see Zerto Virtual Manager	

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform™, Zerto is changing the way disaster recovery, backup and cloud are managed. At enterprise scale, Zerto's software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. Zerto is trusted by over 6,000 customers globally and is powering resiliency offerings for Microsoft Azure, IBM Cloud, AWS, SunGard AS and more than 350 cloud services providers.

Learn more at Zerto.com

For assistance using Zerto Virtual Replication software, contact: @Zerto_Support.