SECURITY AND HARDENING WITH ZERTO VIRTUAL REPLICATION

ZVR-SEC-6.0 Rev 01 Jan2018

Zerto delivers industry-leading virtual replication capabilities for the enterprise ensuring that business operations are not interrupted. A key concern for enterprise-class data is security – at the protected, or production site as well as at the replication site. Zerto has implemented several security features to ensure your data will not be compromised throughout your disaster recovery plans.

Zerto leverages the security features from proven, industry leaders – VMware and Microsoft – providing you with the highest confidence that your data remains secure. Zerto leverages several features throughout the information chain to harden the Virtual Replication Appliance, meeting the standards for enterprise-class, mission critical applications.

Zerto Components

Zerto Virtual Replication is installed in the sites with virtual machines to be protected as well as in the sites where these virtual machines will be recovered. The installation includes the following components:

- **Zerto Virtual Manager (ZVM)** – Plugs directly into VMware vSphere vCenter Server and is a Windows service, which manages the replication between the vCenter Servers on the protection and recovery sites.
- **Virtual Backup Appliance (VBA)** – A Windows service that manages offsite backups within Zerto Virtual Replication. The VBA service runs on the same machine as the Zerto Virtual Manager service.
- **Virtual Replication Appliance (VRA)** – A virtual machine installed on each ESX/ESXi hosting virtual machines to be protected or recovered, to handle the replication of data from protected virtual machines to the recovery site.
- **Zerto Cloud Manager (ZCM)** – A Windows service that enables managing all Zerto Virtual Replication sites from a single browser-based user interface.
- **Zerto Cloud Connector (ZCC)** – Routes traffic between a customer network and a 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 customer network and the cloud provider network.
- **Zerto Self-service Portal (ZSSP)** – An out-of-the-box DR portal solution with a fully functioning browser-based service portal to enable cloud providers to quickly introduce DR as part of their portal offering.

For more information on Zerto product features, visit the Zerto website.

See the following sections:

Communication with vSphere

Zerto Virtual Replication runs within a VMware environment and leverages the security capabilities provided by the vSphere virtualization platform. All communication between the Zerto components (Zerto Virtual Managers, a Zerto Cloud Manager and Zerto Self-service Portals), and between these components and vCenter Servers, vCloud Director, and ESX/ESXi hosts is secure, either via HTTPS or SSH.

Access to Zerto Virtual Replication

Managing replication with Zerto Virtual Replication requires access to the Zerto User Interface. The Zerto User Interface is accessible via one of the following ways:

- A Zerto Virtual Manager standalone browser-based user interface via HTTPS and using the credentials to the vCenter Server accessed by the Zerto Virtual Manager. The Zerto Virtual Manager runs as a Windows service and access to it requires access to the Windows machine running this service. This access relies on the authentication, authorization, and security mechanisms provided by Microsoft.
- The vSphere Web Client or Client console, using the authorization and security mechanisms provided by VMware, including access to Microsoft Active Directory or any other LDAP server.
- The VBA runs as a Windows service on the same machine as the Zerto Virtual Manager. Access to the VBA requires access to the Windows machine running this service. This access relies on the authentication, authorization, and security mechanisms provided by Microsoft.
- The Zerto Cloud Manager browser-based user interface via HTTPS and using the credentials to the machine where the Zerto Cloud Manager service runs. The Zerto Cloud Manager runs as a Windows service and access to it requires access to the Windows machine running this service. This access relies on the authentication, authorization, and security mechanisms provided by Microsoft.

Virtual Replication Appliance and Cloud Connector Hardening

Virtual Replication Appliances and Zerto Cloud Connectors are custom, very thin, Linux-based virtual machines with a small footprint and disk – memory and CPU – that have been hardened to limit the number of running services to the bare minimum. By default they run only the Zerto Virtual Replication protocols and SSH. All other protocols and services, such as the Cron services and ICMP redirects, are either not installed or are turned off. Also the /etc/securetty file has had all devices that are not required removed and the /etc/sysctl.conf file has been configured not to accept packets that have had their route through the network specified by the sender.

Zerto Virtual Replication uses different types of network services and was designed to work in conjunction with existing network security elements.

- **Firewall**

  Zerto Virtual Replication components can be deployed behind standard firewalls. Zerto Virtual Replication relies on the Virtual Replication Appliance's IPtables firewall to block ports that are not required by Zerto Virtual Replication.

  Note: Zerto Virtual Replication does not support NAT (Network Address Translation) firewalls.

- **SSH**

  The Zerto Virtual Replication components do not require SSH for remote access and access can be closed via the firewall software, only allowing SSH access from authorized clients. Zerto support can supply a hardened Virtual Replication Appliance that can limit SSH access to the console only.

  The Zerto Virtual Manager communicates, as a client, with ESX/ESXi hosts securely either via HTTPS, running Zerto Virtual Replication with VMware vSphere 4.x or SSH when running Zerto Virtual Replication with VMware vSphere 5.x.

Cmdlet and RESTful API Security

Zerto Virtual Replication cmdlets in Windows PowerShell and Zerto Virtual Replication RESTful APIs enable managing Zerto Virtual Replication programmatically, without using the Zerto User Interface.

Cmdlet Security

To run the Zerto Virtual Replication cmdlets, specify a username and password that is valid for the Zerto Virtual Manager, against which the command is run. Zerto provides a default username and password pair, `administrator/password`, where the password is saved as the SHA-1 hash of the password.

RESTful API Security

The Zerto Virtual Replication RESTful APIs are exposed over HTTPS and require basic authentication and a unique HTTP authorization header for every call during a session. The basic authentication used must be a valid username and password in the vCenter Server accessed by the Zerto Virtual Manager where the APIs will run. If a session is dormant for thirty minutes, the session is automatically terminated.

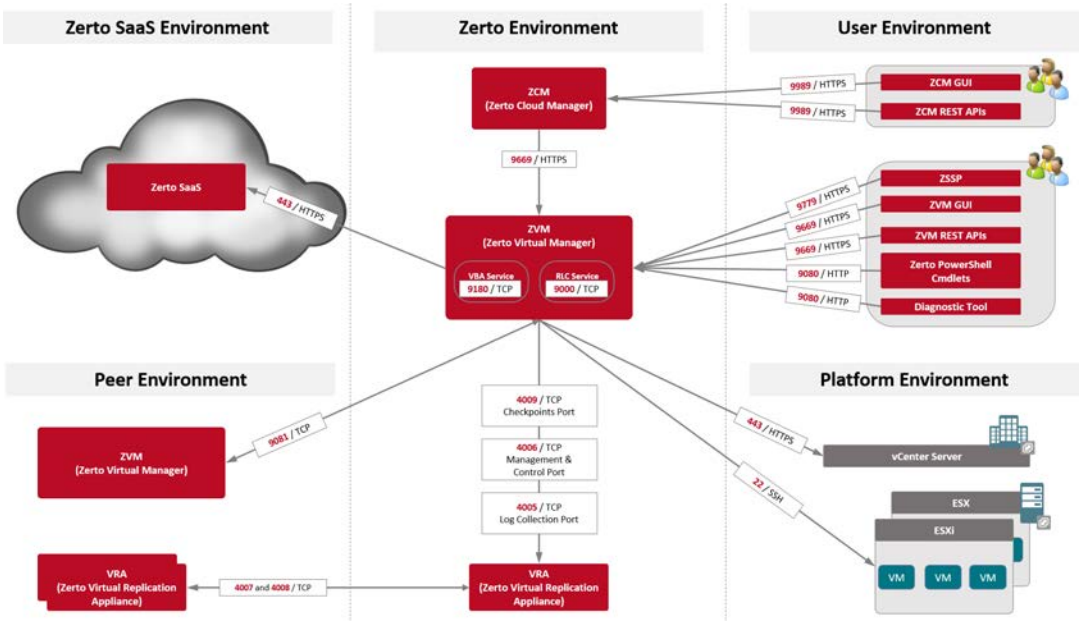
Port Usage

The following ports must be open in the protected and recovery site firewalls:

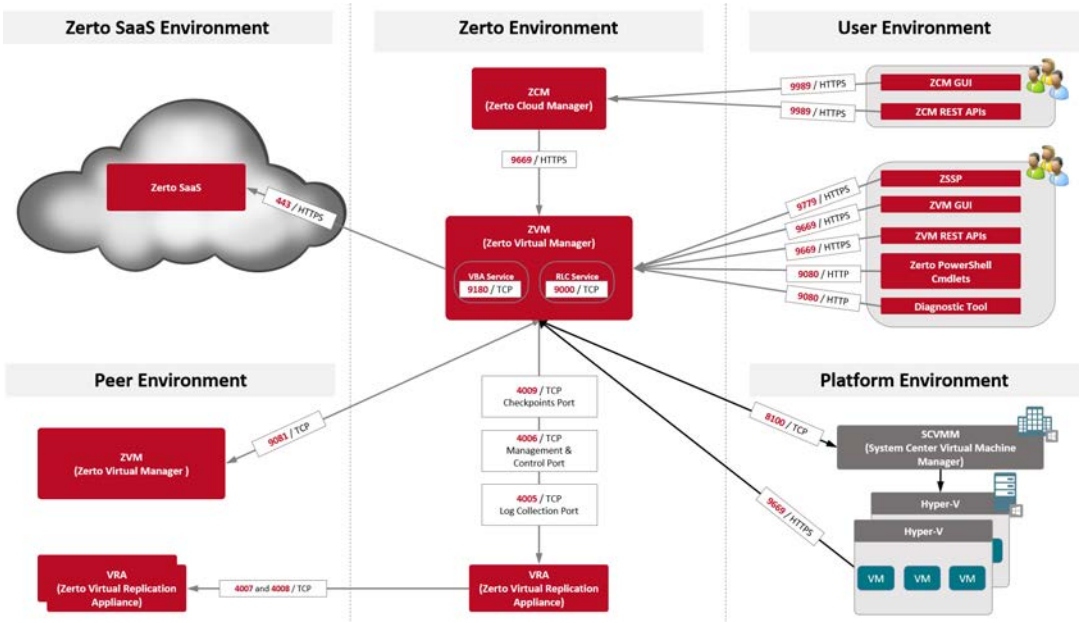
PORT	DESCRIPTION
22	During Virtual Replication Appliance installation on ESXi 4.x and 5.x hosts for communication between the Zerto Virtual Manager and the ESXi hosts IPs and for ongoing communication between the Zerto Virtual Manager and a Zerto Cloud Connector.
443	During Virtual Replication Appliance installation on ESX/ESXi hosts for communication between the Zerto Virtual Manager and the ESX/ESXi hosts IPs and for ongoing communication between the Zerto Virtual Manager and vCenter Server and vCloud Director.
8100	TCP communication between the Zerto Virtual Manager and Microsoft SCVMM.
4005	Log collection between the Zerto Virtual Manager and Virtual Replication Appliances on the same site.
4006	TCP communication between the Zerto Virtual Manager and Virtual Replication Appliances on the same site.
4007	TCP control communication between protecting and recovering Virtual Replication Appliances and between a Zerto Cloud Connector and Virtual Replication Appliances.
4008	TCP communication between Virtual Replication Appliances to pass data from protected virtual machines to a Virtual Replication Appliance on a recovery site and between a Zerto Cloud Connector and Virtual Replication Appliances.
4009	TCP communication between the Zerto Virtual Manager and site Virtual Replication Appliances to handle checkpoints.
5672	TCP communication between the Zerto Virtual Manager and vCloud Director for access to AMQP messaging.
9080	HTTP communication between the Zerto Virtual Manager and Zerto internal APIs, a Zerto Cloud Manager (ZCM), cmdlets, which should only be available to a customer using DRaaS and not ICDR.
9081	TCP communication between Zerto Virtual Managers and between a customer Zerto Virtual Manager and a Zerto Cloud Connector. **This port must not be changed when providing DRaaS.**

9082 and up	Two ports for each Virtual Replication Appliance (one for port 4007 and one for port 4008) accessed via the Zerto Cloud Connector installed by the cloud service provider. There is directionality to these ports. It is recommended to use a port range starting with port 9082. For example, Customer A network has 3 VRAs and customer B network has 2 VRAs and the cloud service provider management network has 4 VRAs, then the following ports must be open in the firewall for each cloud: The cloud service provider's VRAs need to use 6 ports to reach customer A's VRAs, while customer A's VRAs need 8 ports to reach the cloud's VRAs. The cloud service provider's VRAs need to use 4 ports to reach customer B's VRAs, while customer B's VRAs need 8 ports to reach the cloud's VRAs.
9180	Communication between the VBA and Virtual Replication Appliance.
9669	HTTPS communication between: ■ Machines running Zerto User Interface and Zerto Virtual Manager. ■ Zerto Virtual Manager and Zerto REST APIs. ■ Hyper-V hosts and the Zerto Virtual Manager.
9779	HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a Zerto Virtual Manager.
9989	HTTPS communication between the browser and the Zerto Cloud Manager.

The following architecture diagram shows the port usage within an enterprise using vSphere, with # references to the above table:



For Hyper-V environments, only the Zerto Virtual Manager Web Client is available.

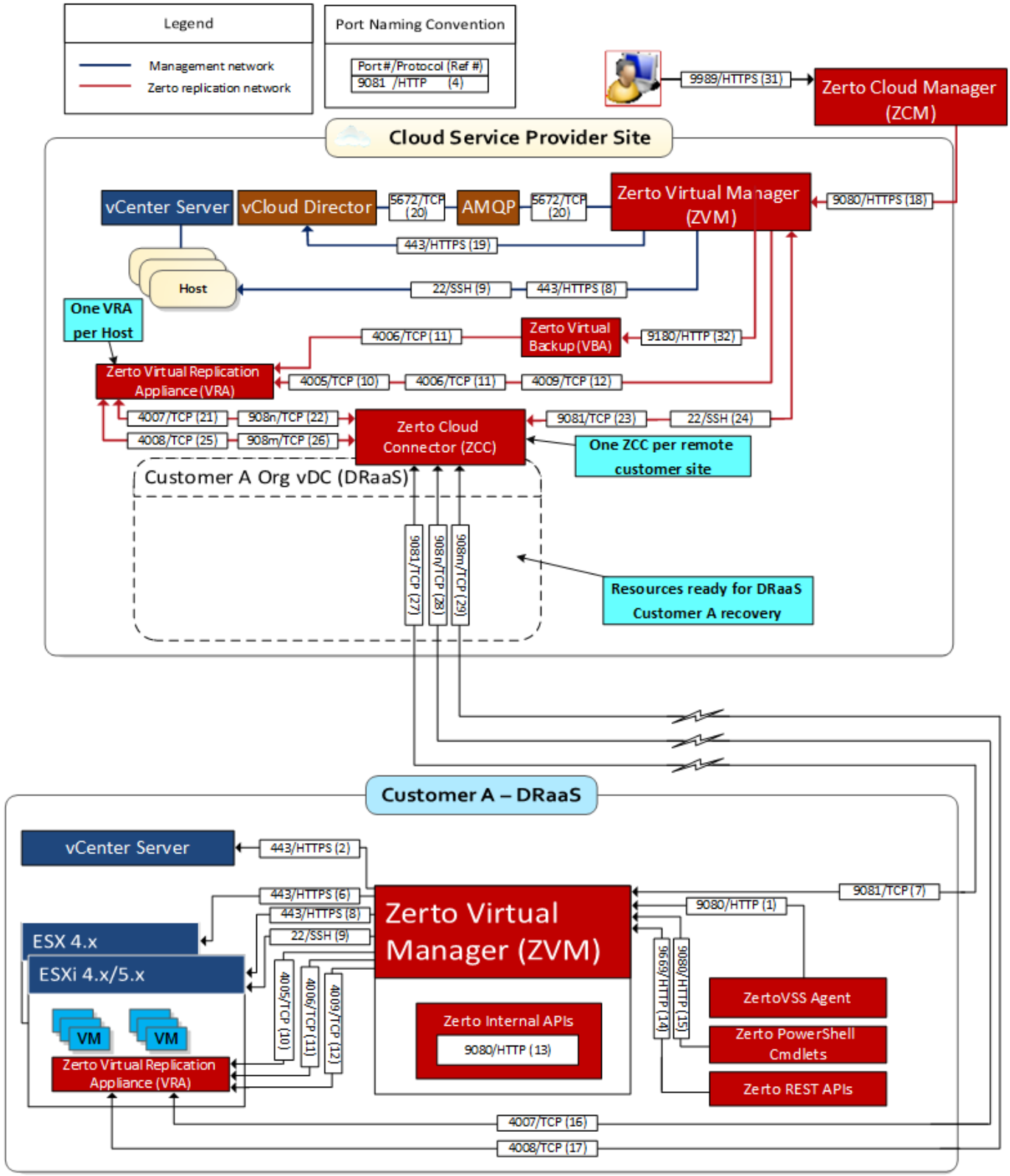


Zerto Virtual Replication can be installed at multiple sites, each site managed by its own vCenter Server and each of these sites can be paired to any of the other sites enabling enterprises to protect multiple datacenters as well as remote branch offices.

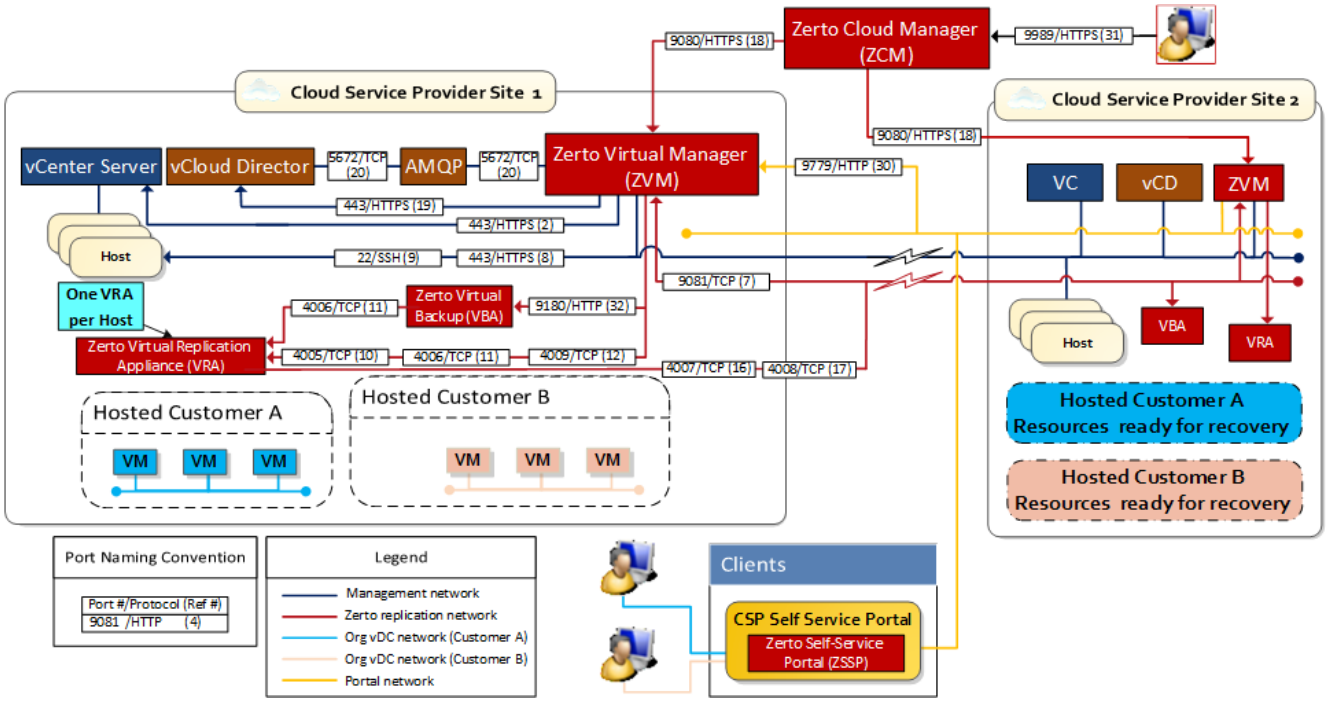
Zerto Virtual Replication also supports both the protected and recovery sites being managed by a single vCenter Server, for example, from one datacenter to another datacenter, both managed by the same vCenter Server. In this case, port 9081 shown in the above diagram is not used.

When Zerto Virtual Replication is installed on multiple sites, a Zerto Cloud Manager can be used to manage all the sites from one pane of glass for management, orchestration, reporting, and monitoring of recovery operations.

The following architecture diagram shows the port usage when a cloud service provider is involved, providing DRaaS to a customer using vSphere, with # references to the above table:



The following architecture diagram shows the port usage when a cloud service provider is involved, providing in-cloud disaster recovery, with # references to the above table:



Network Encryption

Zerto Virtual Replication leverages encryption throughout the environment to ensure that information cannot be compromised:

- Access to the Zerto Virtual Replication management UI is encrypted (HTTPS).
- Communication between the Zerto Virtual Manager and the vCenter Server is encrypted (HTTPS).
- Communication between the Zerto Virtual Manager and vCloud Connector is encrypted (HTTPS).
- Communication between the Zerto Virtual Manager and the ESX/ESXi hosts is encrypted (HTTPS).
- Communication between the Zerto Virtual Manager and the Microsoft SCVMM is encrypted (HTTPS).
- Communication across networks can be encrypted using network encryption software such as VPN and IPsec. Zerto Virtual Replication does not natively encrypt data across the WAN.

Roles and Permissions Within Zerto Virtual Replication

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

Permissions via Zerto Cloud Manager

Within Zerto Cloud Manager you can apply permissions to specific Zerto Virtual Replication entities such as ZORGs, VPGs, and sites. Permissions determine the roles that apply to a specific user or user group on a specific Zerto Virtual Replication entity. Roles are a set of privileges and privileges define an operation or a set of operations that can be performed, such as managing a VPG or VRA. Roles can be assigned to users and groups of users.

You can manage roles and update the privileges associated with both new roles that you create and the roles supplied with Zerto Virtual Replication. You can then manage the permissions per Zerto Virtual Replication entity.

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

Zerto Virtual Replication and VMware Permissions

VMware roles and permissions are the core of VMware infrastructure security. Permissions are a combination of a user/group and a security role that is applied to some level of the VMware Infrastructure.

Zerto Virtual Replication Privileges Added to vSphere

When it is installed, Zerto Virtual Replication adds privileges to vSphere and assigns these privileges to the Administrator role, which enables the administrator to perform specific actions in Zerto Virtual Replication. These privileges include:

- **Live Failover / Move:** Enables performing a failover or move.
- **Manage cloud connector:** Enables installing and uninstalling Zerto Cloud Connectors. For details, refer to *Zerto Cloud Manager Administration Guide*.
- **Manage Sites**: Enables editing the site configuration, including site details, pairing and unpairing sites, updating the license and editing advanced site settings.
- **Manage VPG:** Enables creating, editing, and deleting a VPG, and adding checkpoints to a VPG.
- **Manage VRA:** Enables installing and uninstalling Virtual Replication Appliances.
- **Test Failover:** Enables performing a test failover.
- **Viewer:** For internal use only.

You can define additional roles and assign these roles the privileges they need. All privileges are implemented at the root level, and thus apply to every object in the vCenter Server.

VMware Privileges Required by Zerto Virtual Replication

When Zerto Virtual Replication accesses the **vCenter Server**, it requires the **vSphere privileges** assigned to Administrator roles, which includes the following privileges.

Note: The **Zerto** role must also be available. This role is **added** to the **Administrator user** during the Zerto Virtual Replication installation.

CATEGORY	PRIVILEGE	NOTES	DESCRIPTION
ALARM			
	Create alarm	Only during install and uninstall	When Zerto is installed in vSphere environments, all Zerto alerts are propagated as Alarms in vCenter. As such, upon installation, the alarms matching the alerts are created. Zerto controls enabling and disabling the alarms. See the correlation between alerts and alarms here: http://s3.amazonaws.com/zertodownload_docs/Latest/Guide%20to%20vSphere%20Alarms,%20Alerts%20and%20Events.pdf
	Remove alarm	Only during install and uninstall	When Zerto is uninstalled, the alarm definitions added above are removed.
AUTHORIZATION (from vCenter 5.5 and 6.0) Permissions			
	Modify permission	Only during install and uninstall	When Zerto is installed in vSphere environments, it creates seven different privileges that can be assigned to vCenter users that login to Zerto (or when viewing Zerto UI from within vSphere Client).
DATASTORE			
	Allocate space	For source/target replication of datastores	Needed to allocate datastore space when Zerto creates or reconfigures VMs.
	Browse datastore	For source/target replication of datastores	Needed for in-GUI datastore browser and VPG import.
	Configure datastore	For source/target replication of datastores	Needed to create/remove directories within the Datastore.
	Remove file	For source/target replication of datastores	Used for cleanup of volumes in a number of situations (for example, cleanup of VRAs, journals, folders, etc.).
	Low level file operations	For source/target replication of datastores	Needed to move files managed by Zerto (for example, mirrors, journals, etc.) between folders. Specifically used in recovery operations (for example, Failover), but may be used during other procedures.
	Update virtual machine files	For source/target replication of datastores	
DATASTORE CLUSTER			
	Configure a datastore cluster	For installation of VRAs	Used when installing VRAs to enable/disable storage DRS within datastore clusters

CATEGORY	PRIVILEGE	NOTES	DESCRIPTION
EXTENSION			
	Register extension	Only during install and uninstall	Needed to create the vSphere Client plugin, 'ManagedBy' extension, and other features related to Zerto's integration with vCenter.
	Unregister extension	Only during install and uninstall	Needed to remove the vSphere Client plugin, 'ManagedBy' extension, and other features when removing ZVR.
FOLDER			
	Create folder		Used during recovery operations to create VM folders.
GLOBAL			
	Cancel task		Used to remove tasks created by ZVR to track operations.
	Diagnostics		Used when pulling diagnostic logs from vCenter/ESXi.
	Disable methods		Used to disable methods on protected objects like VRAs and 'Testing Recovery' VMs.
	Enable methods		Used to re-enable methods disabled by Zerto.
	Log event		Used for pushing Zerto events to vSphere for tracking.
Host > Configuration			
	Advanced settings		Not used by Zerto.
	Virtual machine autostart configuration		Used when creating new VRAs/diskboxes.
	Change settings		Used during VRA deployment.
	Security profile and firewall		Used during VRA deployment.
	Query Patch		Used during VRA deployment.
HOST > INVENTORY			
	Modify cluster		Used for settings affinity rules for VRAs, and disabling DRS/HA for recovery VMs before commit.
NETWORK			
	Assign network		Used for assigning VMs to various networks.
RESOURCE			
	Assign vApp to resource pool		Used for moving recovery vApps into the correct resource pools.
	Assign virtual machine to resource pool		Used for moving recovery VMs into the correct resource pool.
	Migrate a powered off virtual machine		Used for migrating VRAs back to the correct host if they've been moved off. Also for migrating recovery VMs back to the correct host when they are migrated by vCD when adding VMs into vCD vApp.

CATEGORY	PRIVILEGE	NOTES	DESCRIPTION
	Migrate a powered on virtual machine		Used for migrating VRAs back to the correct host if they've been moved off. Also for migrating recovery VMs back to the correct host when they are migrated by vCD when adding VMs into vCD vApp.
SESSIONS			
	Validate session		Used for validating the current session between ZVM and vCenter.
TASKS			
	Create task		Used for creating tracking tasks within vCenter.
	Update task		Used for updating tracking tasks created by Zerto.
vApp			
	vApp application configuration		Used for configuring recovery vApps created by ZVR.
	Assign resource pool		Used for moving recovery vApps into the correct resource pool.
	Add virtual machine		Used for moving recovery VMs into the correct vApp.
	Create		Used for creating recovery vApps.
	Delete		Used for deleting recovery vApps (for example, when stopping FOT).
	Import		Used during VRA OVF deployment.
	Power off		Used for powering off recovery vApps (for example, when stopping FOT).
	Power on		Used for powering on recovery vApps.
VIRTUAL MACHINE > CONFIGURATION			
	Add existing disk	TempDatafile placement is required to restore an offsite backup.	Used to attach disks to VRAs/recovery VMs.
	Add new disk	TempDatafile placement is required to restore an offsite backup.	Used to create new journal/mirror disks on VRAs.
	Add or remove device	TempDatafile placement is required to restore an offsite backup.	Used for adding various devices (NIC, SCSI adapter, etc.) to recovery VMs.
	Advanced	TempDatafile placement is required to restore an offsite backup.	Used to set ExtraConfig on Zerto appliances (ZCC/VRA/Diskbox).
	Change CPU count	TempDatafile placement is required to restore an offsite backup.	Used to set number of CPUs on VRA deployment.
	Extend virtual disk	TempDatafile placement is required to restore an offsite backup.	Used to resize mirror disks when disk resize occurs on protected site.

CATEGORY	PRIVILEGE	NOTES	DESCRIPTION
	Modify device settings	TempDatafile placement is required to restore an offsite backup.	Used to change settings of existing devices, such as NICs or SCSI adapters, on VRAs.
	Configure managedBy	TempDatafile placement is required to restore an offsite backup.	Used for setting the 'ManagedBy' property on VMs, such as the Zerto appliances and 'Testing Recovery' VMs.
	Memory	TempDatafile placement is required to restore an offsite backup.	Used to configure memory for VRA VMs.
	Raw device	TempDatafile placement is required to restore an offsite backup.	Used to assign RDM LUNs to VRAs and recovery VMs.
	Remove disk	TempDatafile placement is required to restore an offsite backup.	Used to detach disks from VMs during recovery operations/rollbacks.
	Change resource	TempDatafile placement is required to restore an offsite backup.	Used for configuring the resource allocation of a VM within a Resource Pool - specifically when creating a recovery vApp.
	Settings	TempDatafile placement is required to restore an offsite backup.	Used to change VM settings not covered by other permissions.
	Swapfile placement	TempDatafile placement is required to restore an offsite backup.	Used to set swapfile placement on recovery VMs where the protected VM has a custom setting.
	Upgrade virtual machine compatibility	TempDatafile placement is required to restore an offsite backup.	Used to upgrade VRA VM hardware version when upgrading VRA version.
VIRTUAL MACHINE > INTERACTION			
	Power off		Used for powering off VMs, such as when stopping/rolling back a Failover, or when shutting down protected VMs during a Failover/Move.
	Power on		Used for powering on VMs during recovery operations.
VIRTUAL MACHINE > INVENTORY			
	Create from existing		Used to deploy Zerto appliances.
	Create new		Used to create recovery VMs.
	Register		Used to move VMs into VM folders during recovery operations.
	Remove		Used to remove existing VMs (uninstall Zerto appliance, remove recovery VMs when stopping FOT, rolling back FOL, or on protected site when committing FOL or Move with reverse protection).
	Unregister		Used to remove VMs from inventory. Only used as part of Undo events, after failed task.

Logging Settings

Zerto Virtual Replication produces various logs to help resolve problems. Event logs and alerts are viewable from the vSphere Client console. For details, refer to the relevant sections in the *Zerto Virtual Manager Administration Guide*.

Logs recording Zerto Virtual Manager activity and Virtual Replication Appliance activity can be generated by Zerto support, using the Zerto Diagnostics utility, installed as part of the Virtual Replication Appliance installation. For details, refer to the relevant sections in the *Zerto Virtual Manager Administration Guide*.

Summary

This table summarizes the steps taken to ensure that servers are extremely resistant to security breaches.

ACTION	IMPLEMENTATION
User Authentication	Leveraging features within VMware vSphere and Microsoft, Zerto Virtual Replication limits users who can access the Virtual Replication Appliance through authentication.
Communications to VMware vSphere	Using standard APIs, Zerto Virtual Replication is able to securely communicate with the VMware components.
Network Services	The Virtual Replication Appliance limits the number of running services. By default, it runs only the Zerto Virtual Replication protocols and SSH.
Port Configuration	Zerto Virtual Replication has been configured to use the minimum number of ports to ensure the security of the environment. See the ports usage table, above.
Network Encryption	Communications between VMware vSphere components and across the network is encrypted.
Roles, Permissions, and Privileges	Zerto Virtual Replication activities are assigned to an administrator within your organization to ensure that the right person is able to execute Zerto Virtual Replication.
Log Settings	Zerto Virtual Replication produces various logs. Event logs and alerts are viewable from the vSphere Client console

ABOUT ZERTO

Zerto is committed to keeping enterprise and cloud IT running 24/7 by providing scalable business continuity software solutions. Through the Zerto Cloud Continuity Platform, organizations seamlessly move and protect virtualized workloads between public, private and hybrid clouds. The company's flagship product, Zerto Virtual Replication, is the standard for protection of applications in cloud and virtualized datacenters.

www.zerto.com

For further assistance using Zerto Virtual Replication, contact **@Zerto Support**.

Copyright © 2018, Zerto Ltd. All rights reserved.