SECURITY AND HARDENING WITH ZERTO VIRTUAL REPLICATION

ZVR-SEC-4.0U6-01-14-01-16

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.

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

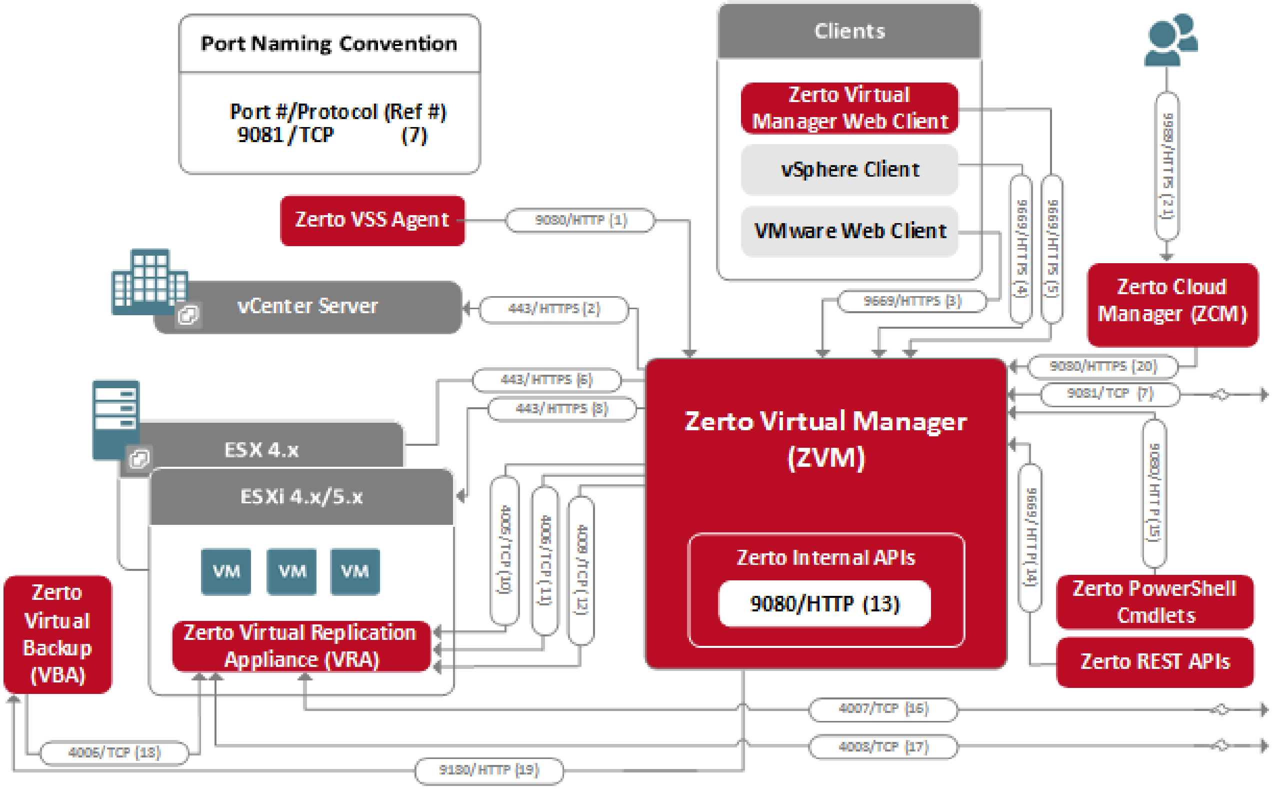
The Zerto Virtual Replication RESTful APIs are exposed over HTTPS and require basic authentication and a unique HTTP authorization header for every call during a session. The basic authentication used must be a valid username and password in the vCenter Server accessed by the Zerto Virtual Manager where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

Port Usage

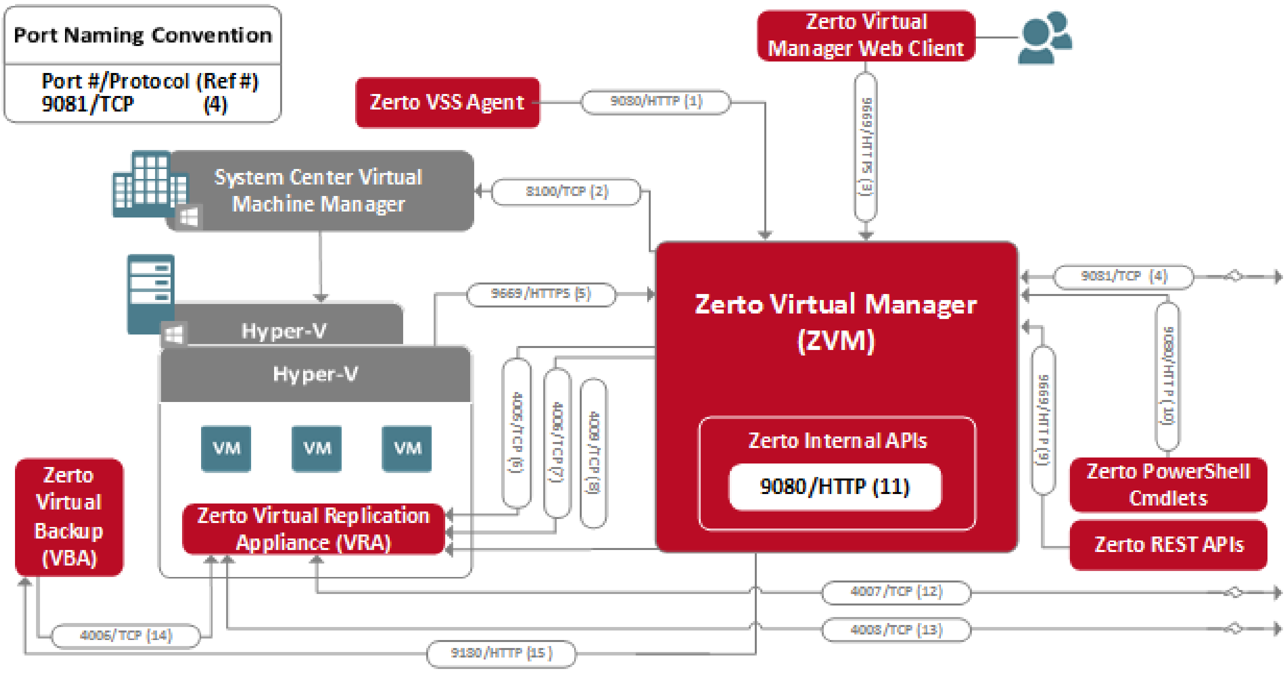
The following ports must be open in the protected and recovery site firewalls, with # references to the following architecture diagrams:

PORT	#	DESCRIPTION
22	9,24	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	2,6, 8,19	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	2	TCP communication between the Zerto Virtual Manager and Microsoft SCVMM.
4005	10	Log collection between the Zerto Virtual Manager and Virtual Replication Appliances on the same site.
4006	11	TCP communication between the Zerto Virtual Manager and Virtual Replication Appliances on the same site.
4007	16, 21	TCP control communication between protecting and recovering Virtual Replication Appliances and between a Zerto Cloud Connector and Virtual Replication Appliances.
4008	17, 25	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	12	TCP communication between the Zerto Virtual Manager and site Virtual Replication Appliances to handle checkpoints.
5672	20	TCP communication between the Zerto Virtual Manager and vCloud Director for access to AMQP messaging.
9080	1,13,15,18	HTTP communication between the Zerto Virtual Manager and Zerto internal APIs, a Zerto Cloud Manager (ZCM), cmdlets, and a VSS Agent, which should only be available to a customer using DRaaS and not ICDR.
9081	7,23, 27	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	22, 26, 28, 29	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	32	Communication between the VBA and Virtual Replication Appliance.
9669	3,4, 5,14	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	30	HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a Zerto Virtual Manager.
9989	31	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 Standalone UI is available and the Zerto Virtual Manager does not communicate directly with the Hyper-V hosts but only through the SCVMM.

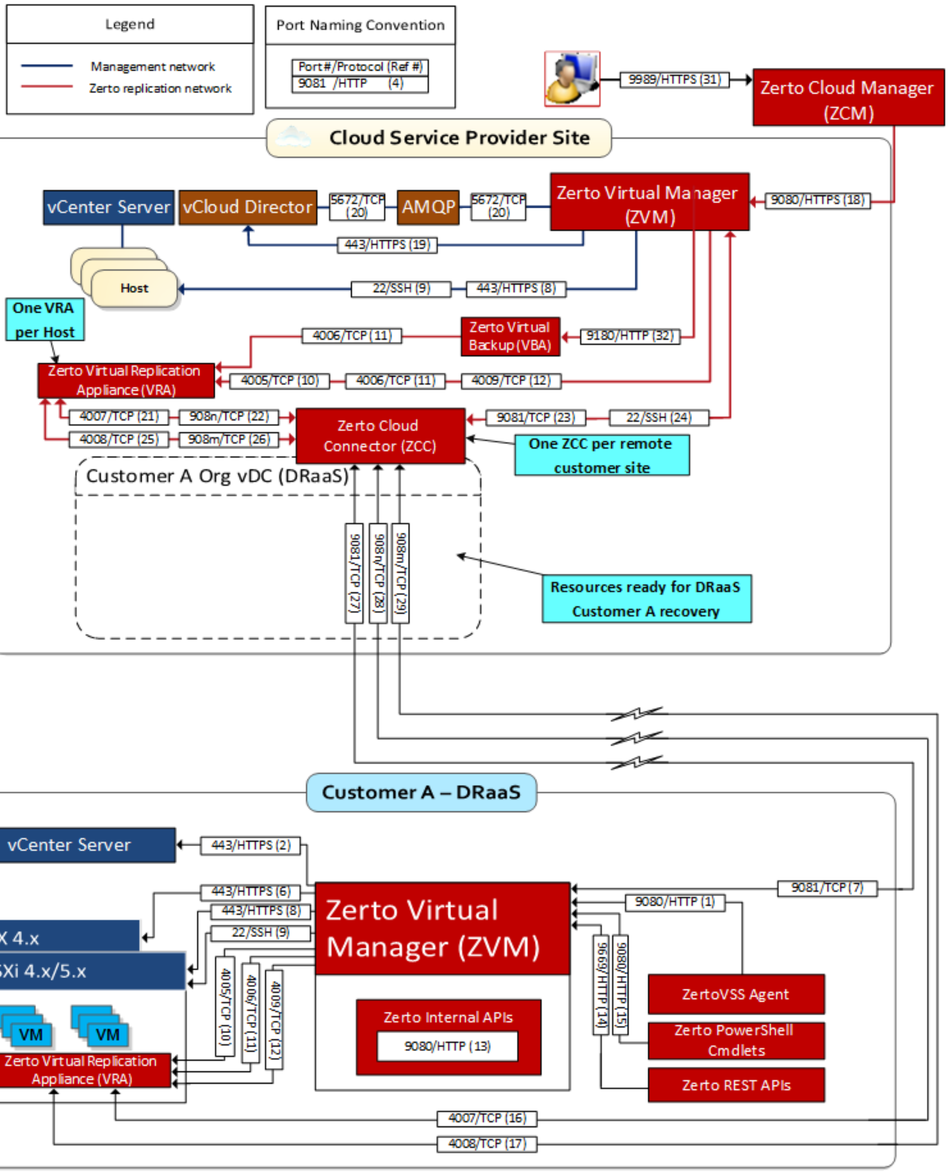


Zerto Virtual Replication can be installed at multiple sites, each site managed by its own vCenter Server and each of these sites can be paired to any of the other sites enabling enterprises to protect multiple datacenters as well as remote branch offices.

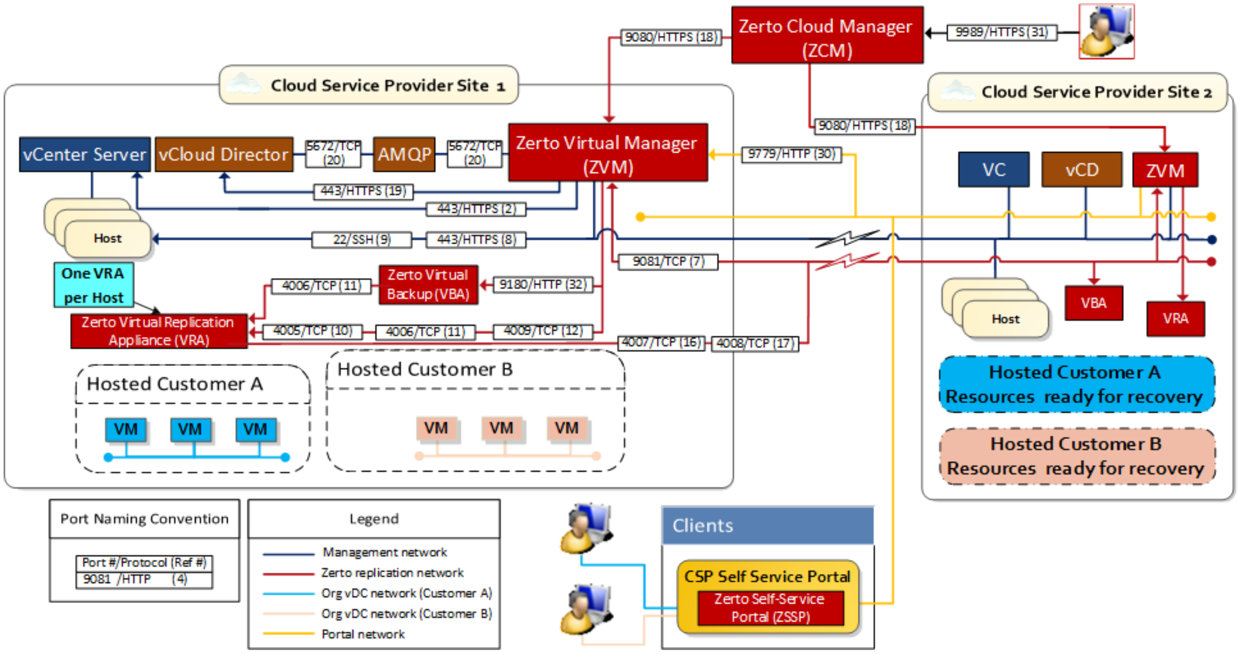
Zerto Virtual Replication also supports both the protected and recovery sites being managed by a single vCenter Server, for example, from one datacenter to another datacenter, both managed by the same vCenter Server. In this case, port 9081 shown in the above diagram is not used.

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.

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.

CATEGORY	PRIVILEGE	NOTES
Alarms	Create alarm	Only during install and uninstall
	Remove alarm	
Authorization	Modify permission	Only during install and uninstall
	Modify role	
	Reassign role permissions	
Datastore	Allocate space	For source/target replication of datastores
	Browse datastore	
	Remove file	
	Low level file operations	
	Move datastore	
	Update virtual machine files	
Datastore cluster	Configure a datastore cluster	For installation of VRAs
Extension	Register extension	Only during install and uninstall
	Unregister extension	
	Update extension	
Folder	Create folder	
	Delete folder	
	Move folder	
Global	Cancel task	
	Diagnostics	
	Global tag	
	Log event	
	Manage custom attributes	
	Script action	
	Set custom attribute	
Host > Configuration	Advanced settings	
	Virtual machine autostart configuration	
	Change settings	
	Security profile and firewall	
Host > Inventory	Modify cluster	
Network	Assign network	

CATEGORY	PRIVILEGE	NOTES
Resource	Assign vApp to resource pool	
	Assign virtual machine to resource pool	
Sessions	Validate session	
Tasks	Create task	
	Update task	
vApp	vApp application configuration	
	Assign resource pool	
	Add virtual machine	
	Create	
	Delete	
	Import	
	vApp instance configuration	
	vApp managedBy configuration	
	Power off	
	Power on	
	Rename	
	vApp resource configuration	
	Unregister	
Virtual Machine > Configuration	Add existing disk	Swapfile placement is required to restore an offsite backup.
	Add new disk	
	Add or remove device	
	Advanced	
	Set annotation	
	Change CPU count	
	Extend virtual disk	
	Modify device settings	
	Configure managedBy	
	Memory	
	Raw device	
	Remove disk	
	Rename	
	Change resource	
	Settings	
	Swapfile placement	
	Upgrade virtual machine compatibility	
Virtual machine > Interaction	Power off	
	Power on	

CATEGORY	PRIVILEGE	NOTES
Virtual machine > Inventory	Create from existing	
	Create new	
	Move	
	Register	
	Remove	
	Unregister	

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

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 at **support@zerto.com**.