Zerto

Security and Hardening with Zerto

Rev01
April 2021
ZVR-SEC8.5 U3

ZVR-SEC8.5 U3

Security and Hardening With Zerto

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, such as communication over a secure channel, and encryption to secure the communication between the ZVM and its peer ZVMs, and between the ZVM and its local VRAs.

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.

See the following sections:

Hardening Recommendations

Zerto recommends the following hardening steps to ensure the security and resilience of your Zerto solution:

1. Access to the Zerto management server (the ZVM service host, or Zerto Cloud Appliance) should be limited to a minimal set of accounts.
2. Unnecessary network services on the Zerto management server, such as SMB, should be disabled and blocked by a firewall.
3. The Zerto management server should be patched regularly.
4. The Zerto management server should not be used for other purposes. For example, unrelated web browsing.

5. Network traffic to Zerto components should be restricted to the ports and endpoints described in this document.
6. Network traffic between Zerto components should be as segregated from the rest of the network as possible. For example, a separate VLAN.

Zerto Components

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, retention and cloud are managed. This is done by providing enterprise-class disaster recovery and business continuity software for virtualized infrastructure and cloud environments.

In **on-premise** environments, Zerto Virtual Replication (ZVR) is installed with virtual machines to be protected and recovered.

In **public cloud** environments, Zerto Cloud Appliance (ZCA) is installed in the public cloud site that is to be used for recovery.

The installation includes the following:

- **Zerto Virtual Manager (ZVM)**: A Windows service that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the hypervisor management user interface, such as vCenter Server or Microsoft SCVMM, to get the inventory of VMs, disks, networks, hosts, etc. and then the Zerto User Interface manages this protection. The ZVM also monitors changes in the hypervisor environment and responds accordingly. For example, a VMware vMotion operation, or Microsoft Live Migration of a protected VM from one host to another is intercepted by the ZVM and the Zerto User Interface is updated accordingly.
    - For the maximum number of virtual machines, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.
- **Virtual Replication Appliance* (VRA)**: A virtual machine installed on each hypervisor hosting virtual machines to be protected or recovered, to manage the replication of data from protected virtual machines to the recovery site.
    - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

> **Note:** *In vSphere installations, OVF to enable installing Virtual Replication Appliances.

- **Virtual Backup Appliance (VBA)**: A Windows service that manages File Level Recovery operations within the Zerto solution.
- **Zerto User Interface**: Recovery using the Zerto solution is managed in a browser or, in VMware vSphere Web Client or Client console.Zerto

When Zerto is installed to work with an **on-premise** hypervisor it also comprises the following component:

- **Data Streaming Service (DSS)**: Installed on the VRA machine, and runs in the same process as the VRA. It is responsible for all the retention data path operations.

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

Port Usage

The architecture diagrams in the following sections show the port usage within an enterprise, with port number references in the relevant tables.

Firewall Considerations in VMware vSphere Environments on page 6

Firewall Considerations in Microsoft Hyper-V Environments on page 9

Firewall Considerations in Microsoft Azure Environments on page 11

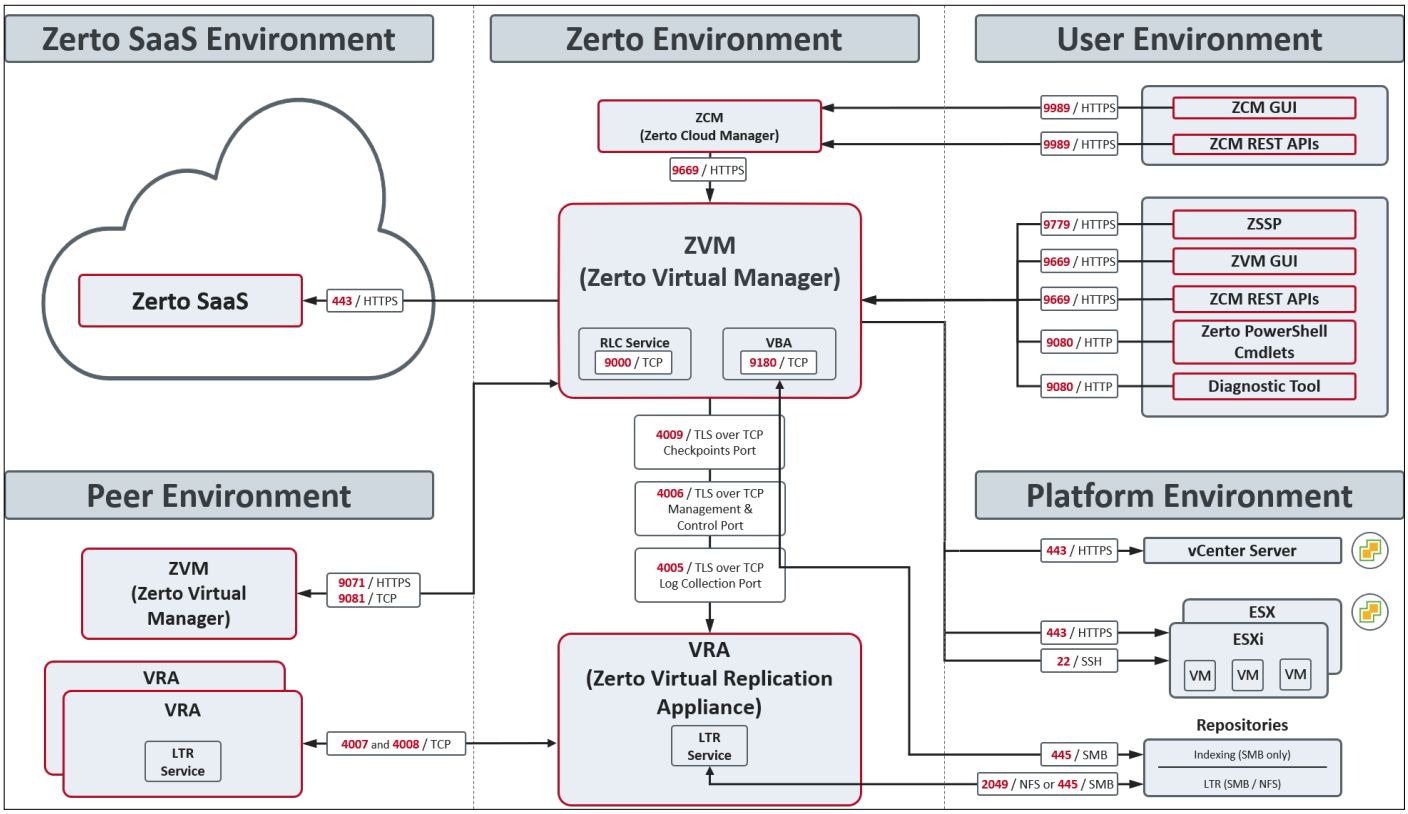
Firewall Considerations in AWS Environments on page 13

Firewall Considerations in VMware vSphere Environments on page 6

MSP Environments on page 14

Firewall Considerations in VMware vSphere Environments

The following architecture diagram shows the **ports** that must be opened in the firewalls **on all sites**.



Zerto can be installed at multiple sites and each of these sites can be paired to any of the other sites.

Zerto supports both the protected and recovery sites being managed by a single vCenter Server or System Center Virtual Machine Manager. For example, in the following scenario:

- From a branch office, to the main office, both managed by the same System Center Virtual Machine Manager.
- From one host to a second host, both managed by the same System Center Virtual Machine Manager.
- To the same host but using different storage for recovery.

It is recommended to install Zerto in the main office site where protected machines will be recovered.

The following table provides basic information about the ports shown in the above diagram by Zerto.

Consider firewall rules if the services are **not** installed on the same network.

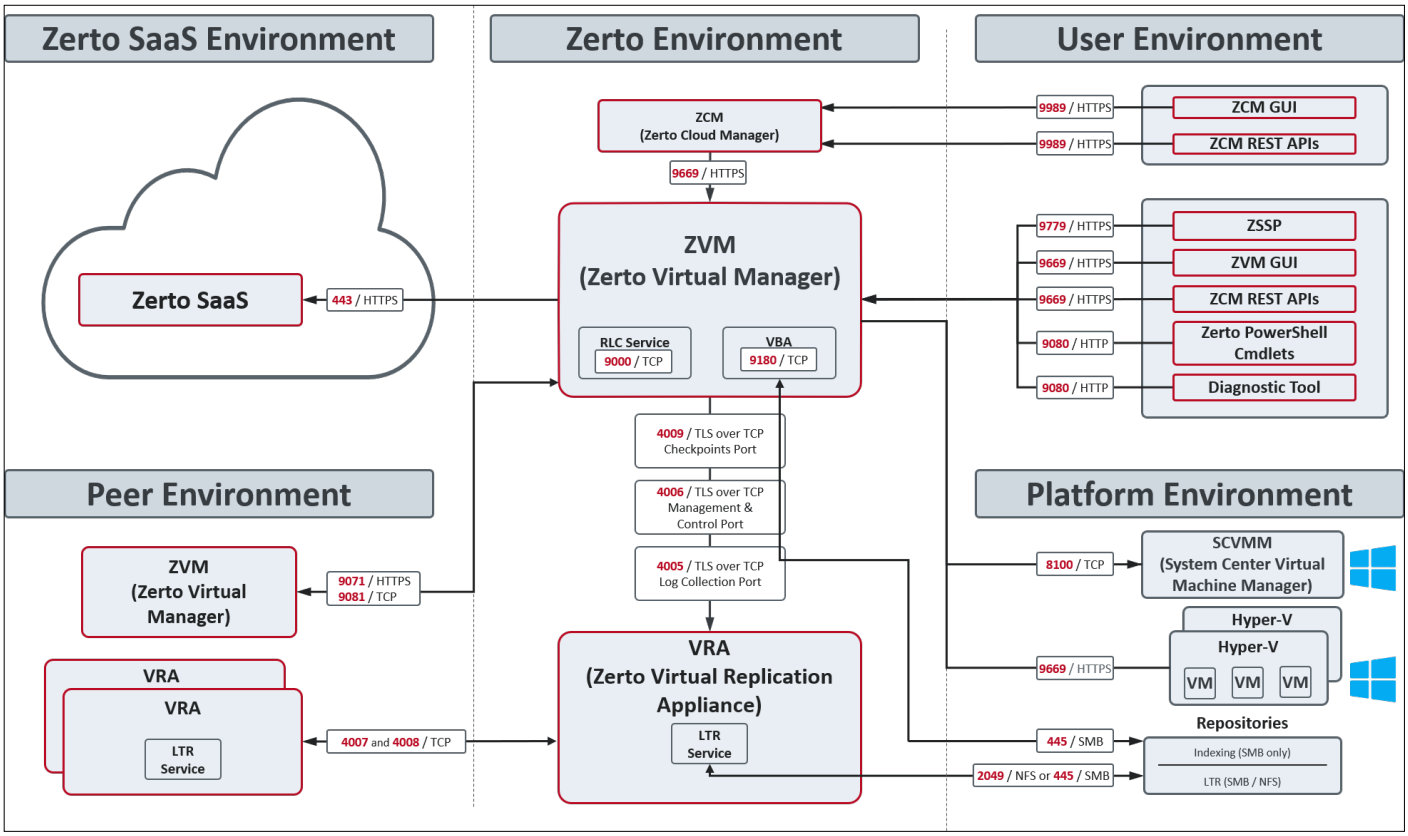
> **Note:** UDP ports in the 444xx range for DHCP are not required and can therefore be blocked.

Port	Purpose
22	Required between an ESXi host and the ZVM during installation of a VRA.
443	Required between the ZVM and the vCenter Server.
443	Required between an ESXi host and the ZVM during installation of a VRA.
445	Required between LTR service and a network shared repository on top of SMB protocol.
2049	Required between LTR service and a network shared repository on top of NFS protocol.
4005	Log collection between the ZVM and site VRAs , using TLS over TCP communication.
4006	TLS over TCP communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
4009	TLS over TCP communication between the ZVM and local site VRAs to handle checkpoints.
5672	TCP communication between the ZVM and vCloud Director for access to AMQP messaging.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
9071*	HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above. *The default port provided during the ZVR installation which can be changed during the installation.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool. *The default port provided during the ZVR installation which can be changed during the installation.
9081*	Communication between paired ZVMs**, maintained for backward compatibility purposes. *The default port provided during the ZVR installation which can be changed during the installation. **When the same vCenter Server is used for both the protected and recovery sites, ZVR is installed on one site only and this port can be ignored.

Port	Purpose
9180*	Communication between the ZVM and the VBA. *The default port provided during the ZVR installation which can be changed during the installation.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM. *The default port provided during the ZVR installation which can be changed during the installation.
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

Firewall Considerations in Microsoft Hyper-V Environments

The following architecture diagram shows the **ports** that must be opened in the firewalls on all sites.



Zerto can be installed at multiple sites and each of these sites can be paired to any of the other sites.

Zerto supports both the protected and recovery sites being managed by a single vCenter Server or System Center Virtual Machine Manager. For example, in the following scenario:

- From a branch office, to the main office, both managed by the same System Center Virtual Machine Manager.
- From one host to a second host, both managed by the same System Center Virtual Machine Manager.
- To the same host but using different storage for recovery.

It is recommended to install Zerto in the main office site where protected machines will be recovered.

The following table provides basic information about the ports shown in the above diagram by Zerto.

Consider firewall rules if the services are **not** installed on the same network.

The following table provides basic information about the ports shown in the above diagram by Zerto.

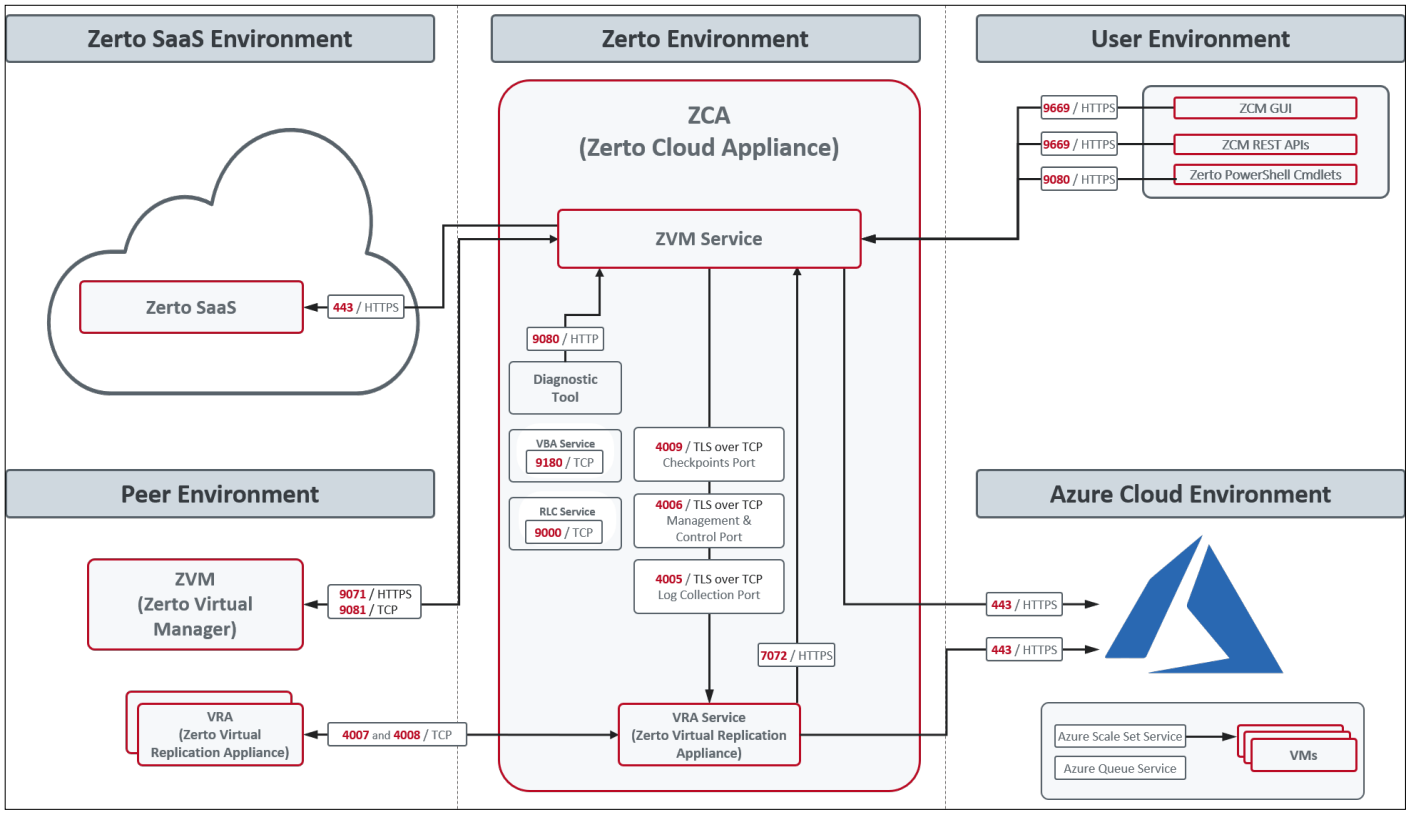
> **Note:** UDP ports in the 444xx range for DHCP are not required, and can therefore be blocked.

Port	Purpose
445	Required between LTR service and a network shared repository on top of SMB protocol.
2049	Required between LTR service and a network shared repository on top of NFS protocol.
4005	Log collection between the ZVM and site VRAs, using TLS over TCP communication.
4006	TLS over TCP communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
4009	TLS over TCP communication between the ZVM and local site VRAs to handle checkpoints.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
8100	Communication between the ZVM and the SCVMM (System Center Virtual Machine Manager).
9071*	HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs**, maintained for backward compatibility purposes. **Note:** • When a single SCVMM is used for both protection and recovery, only one ZVM is installed and port 9081 is not used. • Recovery to a different SCVMM uses port 9081 between the ZVMs in each site.
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM. Communication between every Hyper-V host and the Zerto Virtual Manager.
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

*The default port provided during the ZVR installation which can be changed during the installation.

Firewall Considerations in Microsoft Azure Environments

The following architecture diagram shows the **ports** that must be opened in the firewalls on all sites.



The following table provides basic information about the ports shown in the above diagram by Zerto.

Zerto Cloud Appliance (ZCA) requires the following **ports** to be open in the **Azure site firewall,** set in the **Azure network security group**:

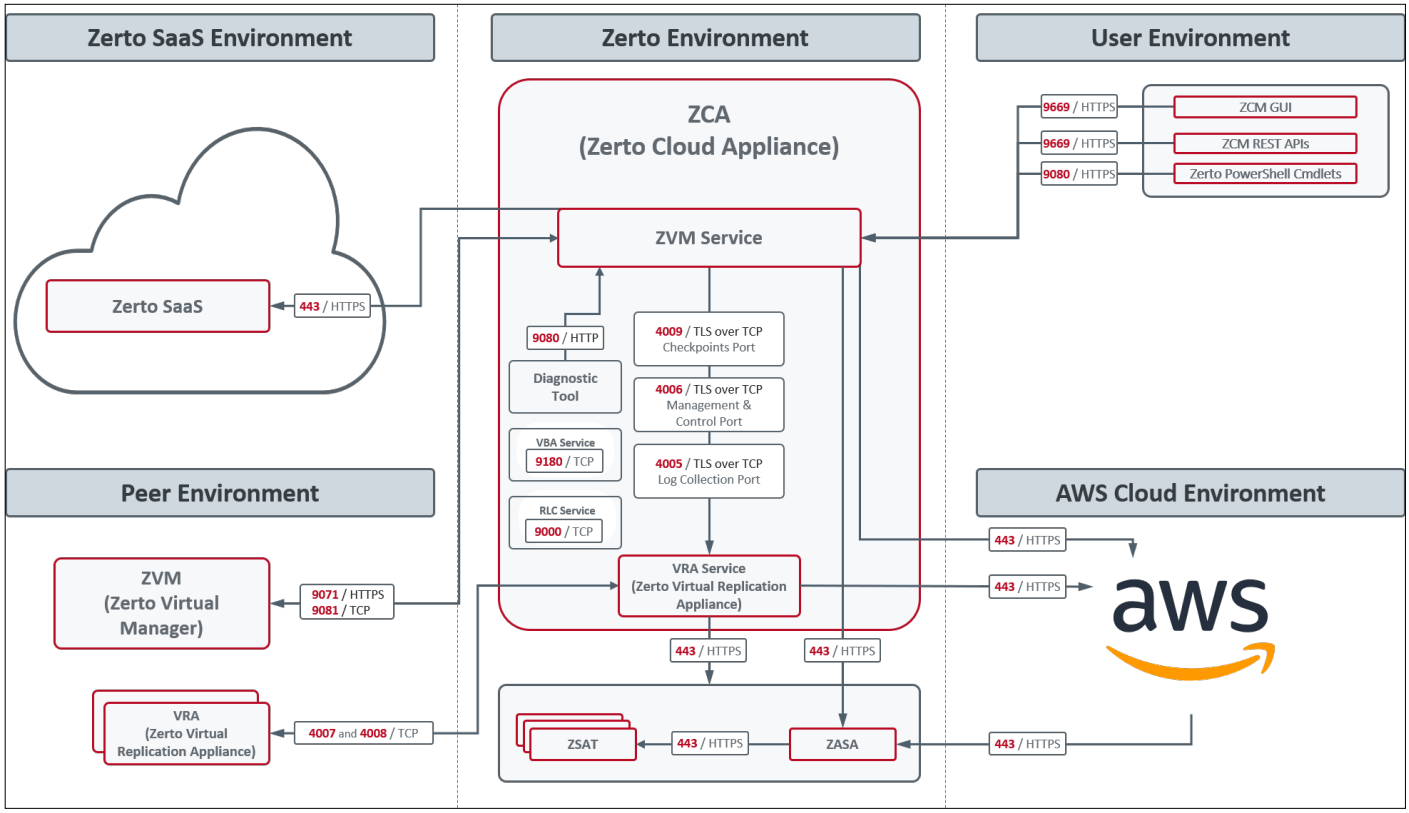
Port	Description
443	• Required between the ZVM and the Azure Cloud environment. • Required between the Azure REST Service and the ZVM during installation of a VRA. • Required for communication between the ZVM and Azure Scale Set and Queues services.
4005	Log collection between the ZVM and site VRAs, using TLS over TCP communication.
4006	TLS over TCP communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.

Port	Description
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.
4009	TLS over TCP communication between the ZVM and local site VRAs to handle checkpoints.
7072	Communication between the VRA and ZVM. Required for metadata promotion.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
9071*	HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs, maintained for backward compatibility purposes**.
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

*The **default** port provided during the ZVR installation which can be changed during the installation.

Firewall Considerations in AWS Environments

The following diagram shows Zerto components deployed on one site and the ports and communication protocols used between the components.



Zerto Cloud Appliance requires the following ports to be open in the AWS site firewall, set in the Amazon security group:

Port	Description
443	Required between the ZVM and the AWS Cloud environment.
443	Required between ZVM Service and ZASA.
4005	Log collection between the ZVM and site VRAs , using TLS over TCP communication.
4006	TLS over TCP communication between the ZVM and local site VRAs and the site VBA.
4007	Control communication between protecting and peer VRAs.
4008	Communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site.

Port	Description
4009	TLS over TCP communication between the ZVM and local site VRAs to handle checkpoints.
7073	Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is **not** transmitted to Zerto Analytics.
9071*	HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above.
9080*	Communication between the ZVM, Zerto Powershell Cmdlets, and Zerto Diagnostic tool.
9081*	Communication between paired ZVMs**, maintained for backward compatibility purposes.
9180*	Communication between the ZVM and the VBA.
9669*	Communication between ZVM and ZVM GUI and ZVM REST APIs, and the ZCM.
9779	Communication between ZVM and ZSSP (Zerto Self Service Portal).
9989	Communication between ZCM, and ZCM GUI and ZCM REST APIs.

*The **default** port provided during the ZVR installation which can be changed during the installation.
When the same vCenter Server is used for both the **protected and **recovery** sites, ZVR is installed on one site only and this port can be ignored.

Environments with Zerto Cloud Manager

When Zerto 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.

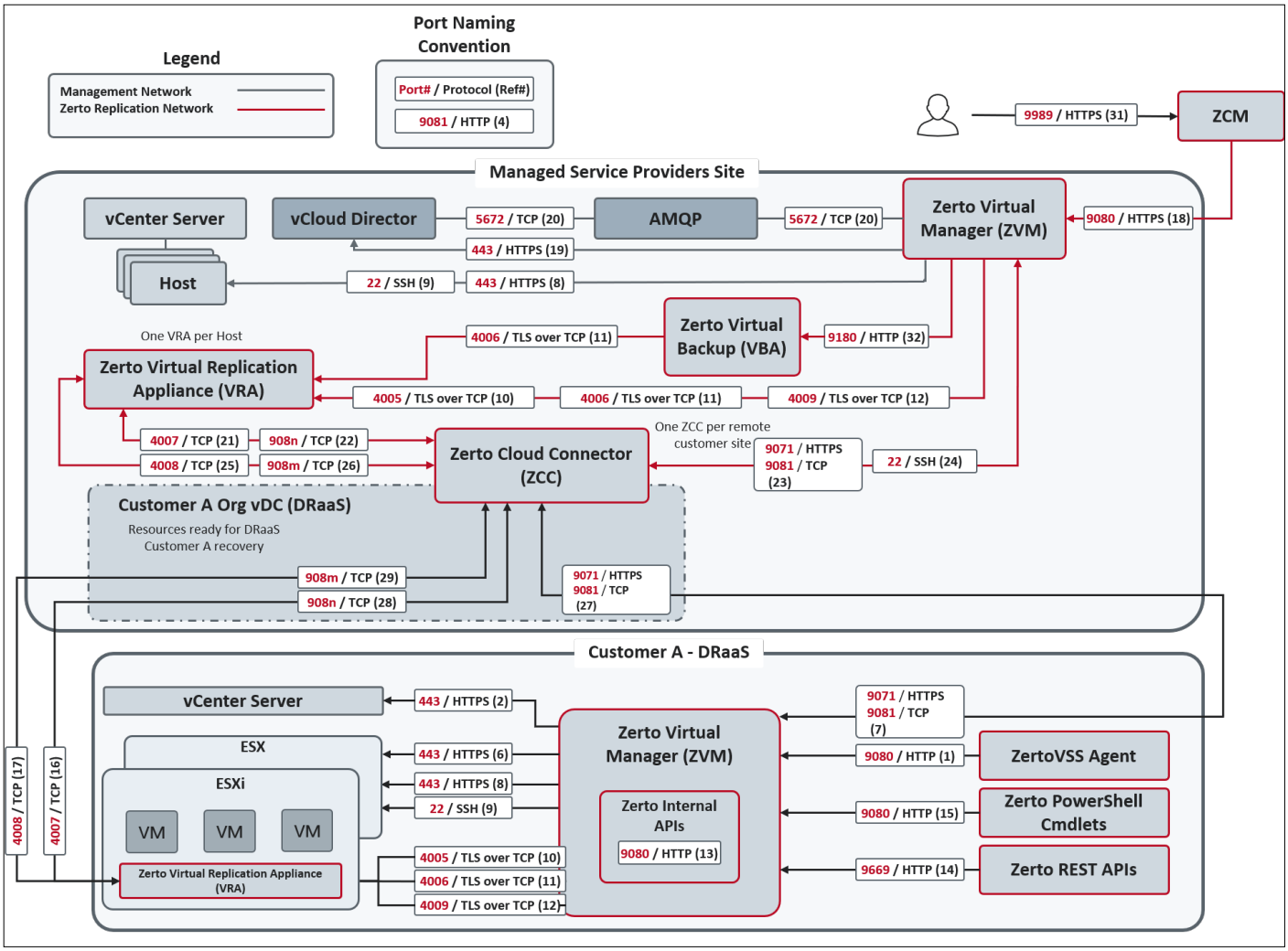
MSP Environments

The following **ports** must be opened in the firewalls in **both** the organization **and** Managed Service Provider sites.

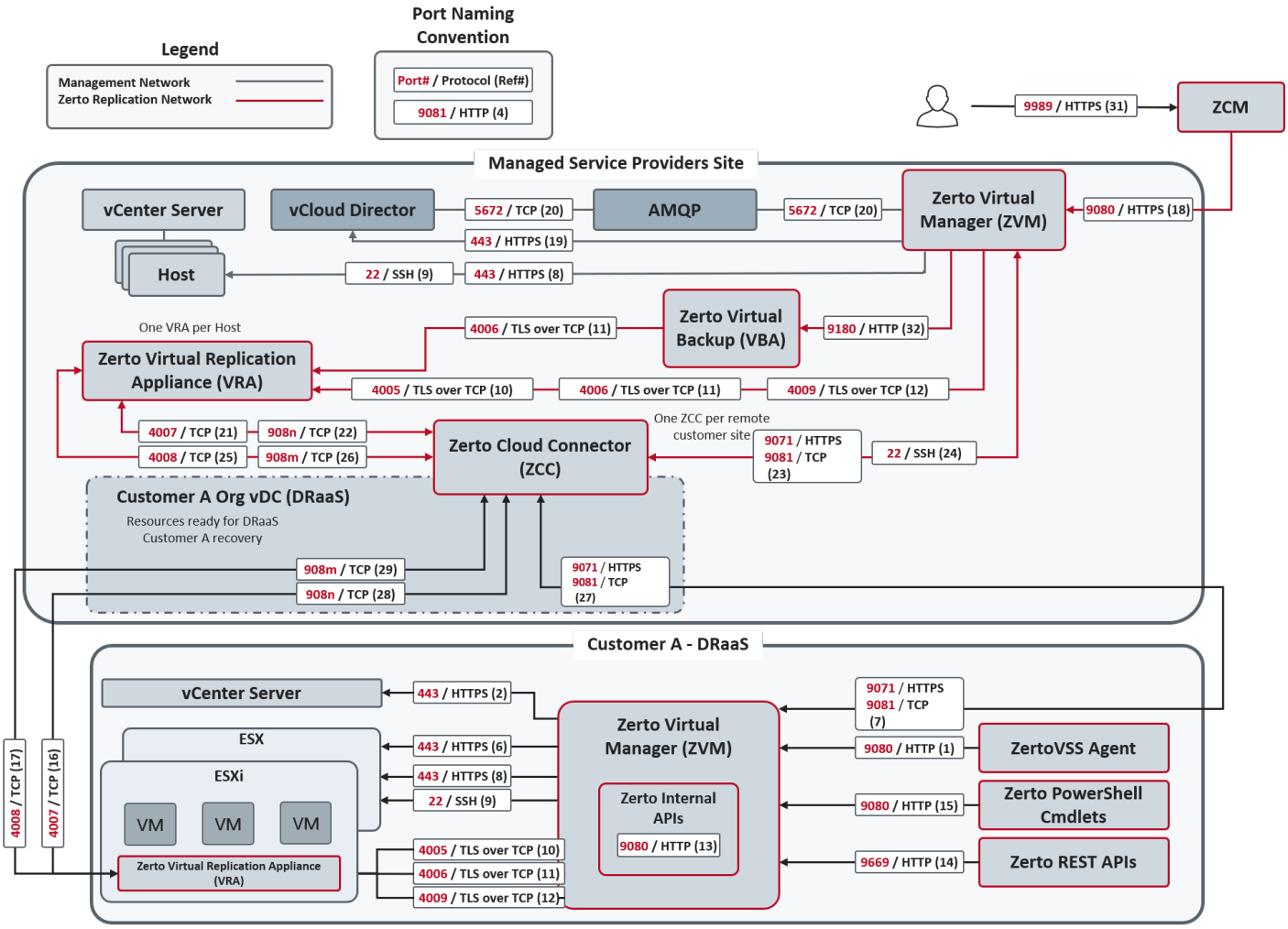
Port	#	Description
22	9, 24	During Virtual Replication Appliance (VRA) installation on ESXi 5.1 and higher for communication between the Zerto Virtual Manager (ZVM) and the ESXi hosts IPs and for ongoing communication between the ZVM in the cloud site – but not the customer site – and a Zerto Cloud Connector.

Port	#	Description
443	2, 6, 8, 19	During VRA installation on ESX/ESXi hosts for communication between the ZVM and the ESX/ESXi hosts IPs and for ongoing communication between the ZVM and vCenter Server and vCloud Director.
4005	10	Log collection between the Zerto Virtual Manager and Virtual Replication Appliances on the same site , using TLS over TCP communication.
4006	11	TLS over 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 VRAs and between a Zerto Cloud Connector and VRAs.
4008	17, 25	TCP communication between VRAs to pass data from protected virtual machines to a VRA on a recovery site and between a Zerto Cloud Connector and VRAs.
4009	12	TLS over TCP communication between the Zerto Virtual Manager and site Virtual Replication Appliances to handle checkpoints.
5672	20	TCP communication between the ZVM and vCloud Director for access to AMQP messaging.
7073		Internal port, used only on the ZVM VM. Used for communication with the service in charge of collecting data for the Zerto Resource Planner. **Note:** Unless you select the checkbox 'Enable Support notification and product improvement feedback', data is not transmitted to Zerto Analytics.
8100	-	Communication between the Zerto Virtual Manager and the System Center Virtual Machine Manager in a customer site running Zerto Virtual Replication with Hyper-V.
9071*		HTTPS communication between paired ZVMs, when both Zerto versions are 8.0 and above.
9080	1, 13, 15, 18	• HTTP communication between the ZVM and Zerto internal APIs, a Zerto Cloud Manager (ZCM), cmdlets, which should only be available to a customer using DRaaS and not ICDR. • HTTP communication between ZVM and Zerto Cloud Manager (ZCM). When the customer's ZCM is **v5.5 and above**, and their ZVM is **v5.0**, communication is via this port.

Port	#	Description
9081	7, 23, 27	TCP communication between Zerto Virtual Managers and between a customer Zerto Virtual Manager and a Zerto Cloud Connector, maintained for backward compatibility purposes. **This port must not be changed when providing DRaaS.**
9082 and up	22, 26, 28, 29	Two ports for each VRA (one for port 4007 and one for port 4008) accessed via the Zerto Cloud Connector installed by the Managed Service Provider. There is directionality to these ports. 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 Managed Service Provider management network has 4 VRAs, then the following ports must be open in the firewall for each cloud: The Managed 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 Managed 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 VRA.
9669	3, 4, 5, 14	HTTPS communication between: • Machines running Zerto User Interface and Zerto Virtual Manager • Zerto Virtual Manager and Zerto REST APIs • ZVM and Zerto Cloud Manager (ZCM). When the customer's ZCM and ZVM are both **v5.5 and above**, communication is via this port.
9779	30	HTTPS communication between the Zerto Self-Service Portal for in-cloud (ICDR) customers and a ZVM.
9989	31	HTTPS communication between the browser and the Zerto Cloud Manager.



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



Access Control

Managing replication with Zerto 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 authorization and security mechanisms provided by VMware, including access to Microsoft Active Directory or any other LDAP server. In Hyper-V environments, the credentials are authenticated on the local machine. 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

Virtual Replication Appliances 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 protocols and SSH. All other protocols and services, such as the Cron services and ICMP redirects, are either not installed or are turned off.

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

- **Firewall**

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

  > **Note:** Zerto does not support NAT (Network Address Translation) firewalls.

- **SSH**

  The Zerto 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 via SSH when running Zerto with VMware vSphere 5.x or later.

Managing VRA Authentication

Access to the VRA is possible via SSH. It is also possible to access the VRA via the hypervisor console, after setting a root password.

To set the root password, follow the instructions in KB1594 to connect to the VRA, and use the passwd command.

It is also possible to add trusted SSH keys using standard OpenSSH commands.

> **Important:** Following any changes to the user accounts and SSH settings, wait 10 minutes before restarting or shutting down the VRA, to ensure that these settings are maintained across upgrades.

VRA to VRA Encryption

Users can enable TLS-based VRA encryption to protect sensitive replication data in-flight.

By enabling VRA encryption, the VRA to VRA communication channel will be made secure and encrypted (TLS over TCP), and will be carried out over two new ports: **9007** and **9008**.

> **Note:** VRA to VRA Encryption is not intended to replace a VPN or any private connection.

Considerations:

- To avoid site disconnections, make sure ports 9007 and 9008 are open for communication between your peer VRAs.
- For encryption between cross site peer VRAs, enable VRA encryption on both sites.
- VRA encryption requires that your Hosts' CPU supports AES_NI.
- After enabling encryption, you may experience some degradation in replication performance due to CPU consumption.

  This is only likely to be noticed:

  - During a large Initial Sync between the sites.
  - In environments where the Network and Storage support large throughputs, where the CPU might become a bottleneck.
- Enabling encryption might also affect your VRAs compression ratio.
  - To reduce the encryption impact on performance, Zerto recommends you add a second vCPU to each VRA.

> **! Important:**
>
> - Increasing the number of vCPUs to two is recommended if the VRA is used for Long-term Retention, or for high loads.
> - Increasing the number of vCPUs to more than two should only be per Zerto Support recommendation.

Cloud Connector

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 protocols and SSH. All other protocols and services, such as the Cron services and ICMP redirects, are either not installed or are turned off.

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

- **Firewall**

  Zerto components can be deployed behind standard firewalls.

  > **Note:** Zerto does not support NAT (Network Address Translation) firewalls.

- **SSH**

  The Zerto components do not require SSH for remote access and access can be closed via the firewall software, only allowing SSH access from authorized clients.

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

Permissions via 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.

For details, see the Zerto Cloud Manager Administration Guide.

Network Encryption

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

- Access to the Zerto 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 does not natively encrypt data across the WAN.
  Zerto recommends segregating management and replication traffic from the rest of the network, in order to mitigate any unknown vulnerabilities.

Zerto helps customers accelerate IT transformation through a single, scalable platform for cloud data management and protection. Built for enterprise scale, Zerto's simple, software-only platform uses continuous data protection to converge disaster recovery, backup, and data mobility and eliminate the risks and complexity of modernization and cloud adoption

Learn more at Zerto.com.

For assistance using Zerto's Solution, contact: @Zerto Support.