Zerto

Zerto Virtual Replication - Prerequisites & Requirements for Cloud Service Providers

Rev01
April 2019
ZVR-RQC-7.0

ZVR-RQC-7.0

Zerto Virtual Replication - Prerequisites & Requirements for Cloud Service Providers

Zerto Virtual Replication is installed in sites with virtual machines to be protected and on sites where these protected machines will be recovered if a disaster occurs.

This document describes **Zerto Virtual Replication - Prerequisites and Requirements for Cloud Service Providers**.

A Zerto Virtual Replication solution comprises:

- A **Zerto Virtual Manager** (ZVM)

  This is installed at each site, and is a Windows service, which manages everything required for the replication between the protection and recovery sites.

- A **Virtual Backup Appliance** (VBA)

  A Windows service that manages File Level Recovery operations within Zerto Virtual Replication. These repositories can be local or on a shared network.

- **Virtual Replication Appliances** (VRAs)

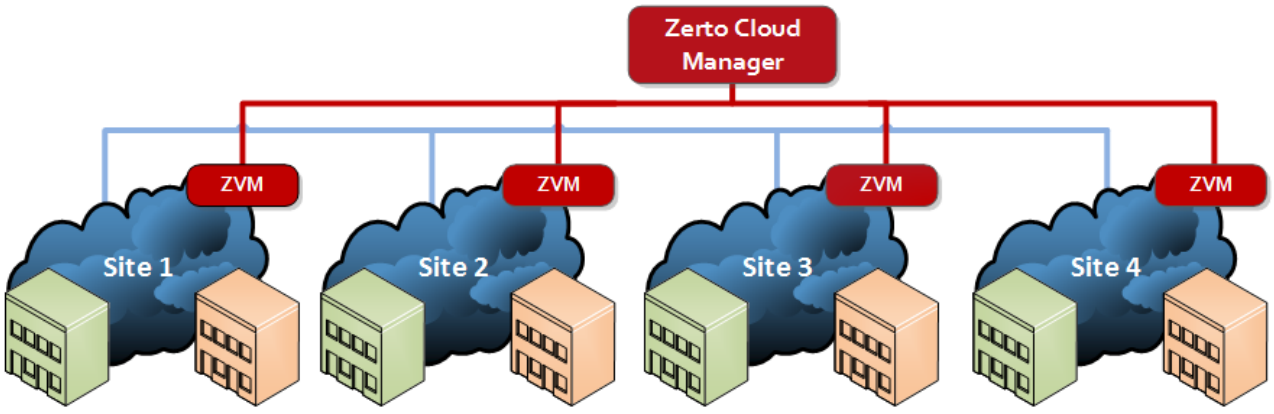
  These are virtual machines installed on each ESX/ESXi hosting virtual machines to be protected or recovered and responsible for the actual replication of data.

- A **Zerto Cloud Manager** (ZCM)

  This is a Windows service, which enables managing all the cloud sites offering disaster recovery either as a service (DRaaS) or completely within the cloud environment, protecting on one cloud site and recovering to a second site (ICDR).

- **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.



- As can be seen in the above diagram, each site has a Zerto Virtual Manager (ZVM) installed.
- One cloud site has the Zerto Cloud Manager (ZCM) installed to manage all the sites.

- The virtual replication appliances are installed on each host ESX/ESXi in each site running a ZVM.
- When the cloud service provider utilizes 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.

When using Zerto Cloud Manager, recovery is to a resource pool.

The **design considerations** described in this document cover the following:

- Using Zerto Virtual Replication when the cloud service provider hosts both the protection and recovery sites for a customer – In-Cloud Disaster Recovery, ICDR. See Design Considerations for ICDR 4.
- Using Zerto Virtual Replication from a customer to a cloud service provider – Disaster Recovery as a Service, DRaaS. See Design Considerations for DRaaS 4.

See the following topics:

- Zerto Virtual Replication Requirements 7
- Recommended Best Practices 13
- DRaaS Architecture Diagram Showing Ports 13
- ICDR Architecture Diagram Showing Ports 14

Design Considerations for ICDR

The cloud sites belong to the same provider, and so, the connection between the two sites does not require a Zerto Cloud Connector. This is because the traffic between the two cloud service provider networks belong to the same cloud service provider. Therefore, separation of networks is not required.

The cloud provider uses the Zerto Cloud Manager to manage the customers, defined as ZORGs (Zerto Organizations), and provides access to these ZORGs via the Zerto Self-Service Portal, either embedded within a cloud service provider portal, or as a standalone portal.

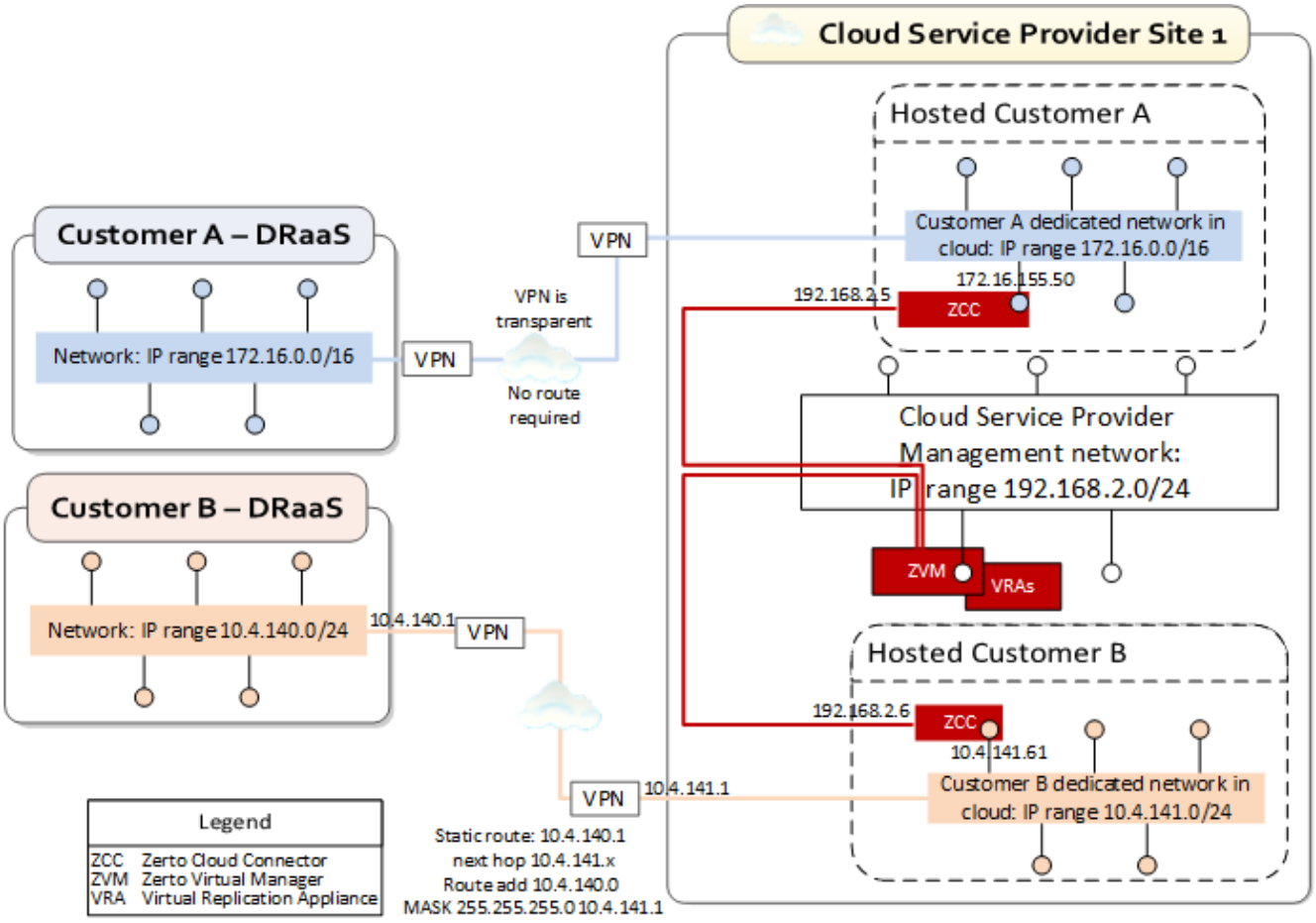
See also:

- Design Considerations for DRaaS 4

Design Considerations for DRaaS

The organization, defined in the Zerto Cloud Manager as a ZORG, Zerto 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.



A cloud connector is a virtual machine installed on the cloud side, one for each customer replication 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 management networks. Thus, all network traffic passes through the cloud connector, where the incoming traffic on the customer network is automatically configured to IP addresses of the cloud service provider management network.

The **Zerto Cloud Connectors** ensure the following:

- None of the customers have direct access to the cloud service provider management network and cannot see any part of the cloud service provider management 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 institute **additional security**, considering both cloud connector interfaces as part of the customer network, they 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.

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.

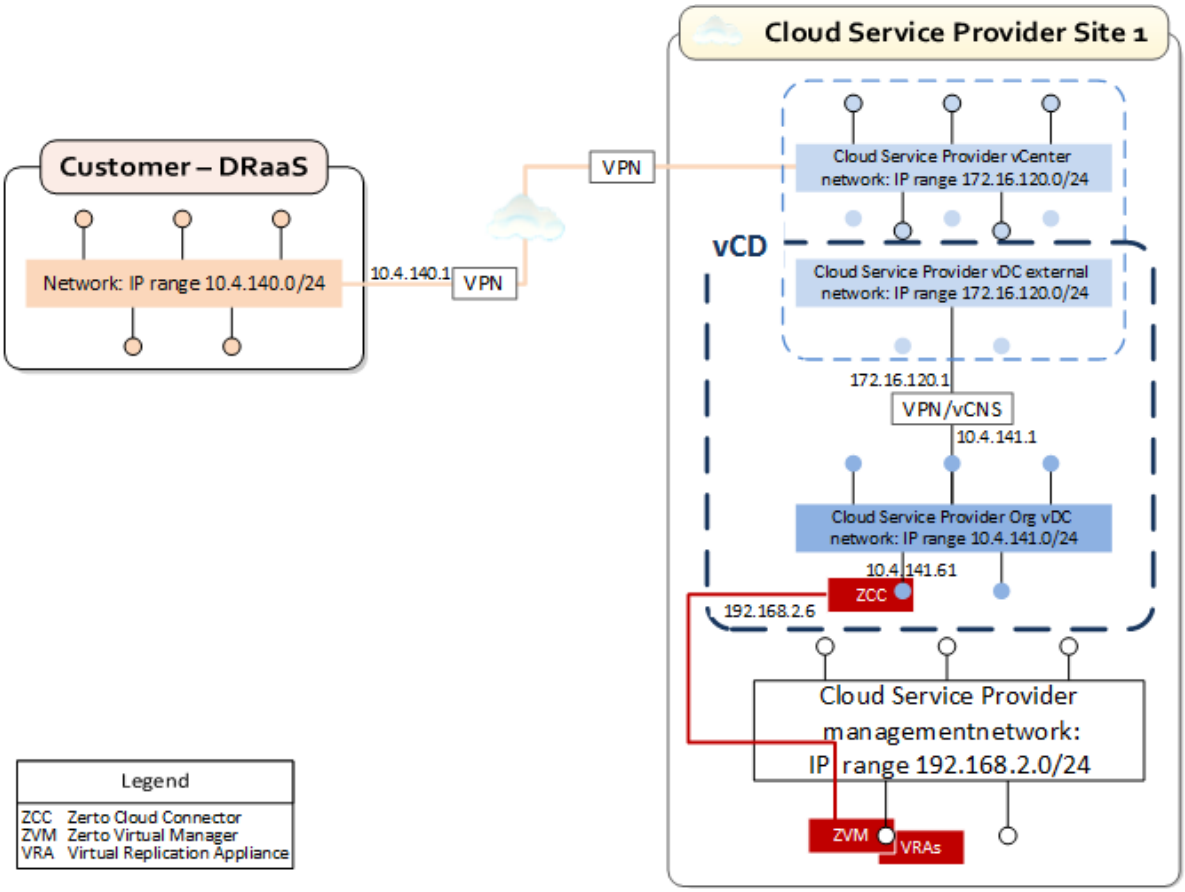
The cloud connector requires **2GB** of disk space.

See also:

- Design Considerations for ICDR 4

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 Virtual Replication does not support the usage of 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.

See DRaaS Architecture Diagram Showing Ports 13 and ICDR Architecture Diagram Showing Ports 14.

Zerto Virtual Replication Requirements

Zerto Virtual Replication for **vSphere** is installed on the **cloud service provider** sites and, when DRaaS is provided, on **organization** sites. Refer to the following sections:

- For Cloud Service Provider Sites 7
- For Each ZORG Site (DRaaS) 11
- Minimum Bandwidth 11
- Network Considerations 11
- Open Firewall Ports 12

For Cloud Service Provider Sites

- Zerto Virtual Manager Requirements 7
- Virtual Replication Appliances Requirements 9
- Zerto Cloud Manager Requirements 10
- Zerto User Interface Requirements 10
- Zerto Cloud Connectors (DRaaS) Requirements 11

Zerto Virtual Manager Requirements

- VMware vCenter Server version that is supported in the Interoperability Matrix with at least one ESX/ESXi host.
- The **Zerto Virtual Manager** must have access to the **vCenter Server** via a user with **administrator level privileges** to the vCenter Server.
- On the machines were **Zerto Virtual Replication** is installed:
  - 64-bit Operating System
  - The Operating system version number must be 6.1 or higher

  - The Windows operating system must be Server Edition
  - Supported Operating Systems:
    - Windows Server 2008 R2 SP1 with KB3033929 and KB2864202
    - Windows Server 2012 base
    - Windows Server 2012 R2
- Microsoft **.NET Framework 4.7.2. or higher**
  - The 4.7.2 installation executable is **included** as part of the Zerto Virtual Replication installation kit and needs an additional **4.5 GB of free disk space**
  - If you install .NET Framework 4.7.2 as part of the Zerto Virtual Replication installation, you will be prompted to restart.
- Make sure that you have the latest .NET and Windows updates, unless Zerto support warns against a specific update.
- Reserve at least **2 CPUs** and **4GB RAM** for the machine.
- The following **CPU** and **RAM** are recommended by Zerto for the machine running Zerto Virtual Replication, dependent on the size of the site:

  Zerto recommends running with at least 16GB memory.

Number of Virtual Machines or Peer Sites		Number of CPUs	RAM Size
Virtual Machines	Peer Sites		
Up to **150** virtual machines	And up to **2** peer sites	**4** CPUs	**8**GB
Between **150-750** virtual machines	And up to **5** peer sites	**4** CPUs	**8**GB
Between **750-5000** virtual machines	And up to **80** peer sites	**4** CPUs	**16**GB
Between **5000-10000** virtual machines	Or **80+** peer sites	**4** CPUs	**24**GB

- The **clocks** on the machines where Zerto Virtual Replication is installed must be **synchronized with UTC** and with each other (the timezones can be different). Zerto recommends synchronizing the clocks using NTP.
  - At least 4GB of free disk space.
- Optionally, **VMware vCloud Director** version, as defined in the Interoperability Matrix, running on either the protected site, the recovery site or on both sites.
  - Advanced Message Queuing Protocol (AMQP) Server: Zerto recommends RabbitMQ with Erlang/OTP and provides an installation that includes links to RabbitMQ and Erlang/OTP.

- IP address of the vCloud Director.
- vCloud Director system administrator username and password. You can create a dedicated user for Zerto Virtual Replication but it must have system administration privileges.

Make sure that the cloud service provider vDC has enough resources in order to replicate all the protected virtual machines into the Org vDC. Zerto Virtual Replication does not support replicating vApp networks and fence mode must not be enabled when performing a failover, test failover or move.

> **Note:** To ensure that vCD is correctly installed, you must be able to define and power on a vApp with at least one virtual machine for each organization vDC. After verifying the vCD installation, the vApp can be removed. After the installation, there is no need to create a vApp network in vCloud Director on the cloud site. Zerto Virtual Replication creates the vApp network when performing a failover or migration into the provider vDC.

- You must **exclude**he following foldersfrom **antivirus scanning**:

Zerto Virtual Replication
%ProgramData%\Zerto\Data\zvm_db.mdf
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Zvm.Service.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto.Vba.VbaService.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Zerto Online Services Connector\Zerto.Online.Services.Connector.exe
C:\Program Files\Zerto\Zerto Virtual Replication\Embedded DB Manager Service\Zerto.LocalDbInstanceManagerService.exe

Failure to do so may lead to the Zerto Virtual Replication folder being incorrectly identified as a threat and in some circumstances corrupt the Zerto Virtual Replication folder.

Virtual Replication Appliances 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.

Zerto Cloud Manager Requirements

Zerto Cloud Manager is installed on a machine running a Windows operating system with the following requirements:

- Windows Server 2008, 2008R2, 2012, 2012R2 or 2016 with at least 1 CPU and 2GB RAM reserved.
- At least 4GB of free disk space.
- Microsoft .NET Framework 4.5.2 or higher.

Zerto User Interface Requirements

- Adobe Flash Player 11.9 ActiveX or higher for the Zerto Cloud Manager user interface. If a valid version of the Flash Player is not installed, you are prompted to install it when first accessing the user interface.

  > **Note:** Adobe Flash Player is only necessary for Zerto Cloud Manager. It is not necessary for

> Zerto Virtual Manager.

- The minimum recommended screen resolution is 1024*768.

Zerto Cloud Connectors (DRaaS) Requirements

- Zerto Cloud Connectors can only be installed on ESX/ESXi hosts version 4.1 and higher with 2GB datastore space.
- You must know the following information to install a Zerto Cloud Connector:
  - The organization network to access the Zerto Cloud Connector.
  - The cloud network settings to access the Zerto Cloud Connector.

For Each ZORG Site (DRaaS)

- VMware vCenter Server version 4.0U1 and higher with at least one ESX/ESXi host and credentials for the vCenter Server with administration level privileges.
- On the dedicated machines where Zerto Virtual Replication is installed:

  Win 2008 R2 SP1 with KB3033929 and KB2864202, Win 2012 base, or Win 2012 R2.
  Reserve at least 2 CPUs and 4GB RAM for the machine.

  Microsoft .NET Framework 4.5.2 (included with the Zerto Virtual Replication installation kit).
- If you have a firewall in the environment, make sure to open the ports, described below.

> **Note:** If the organization and cloud service provider versions of VMware are different, any VMware limitations relating to mixing versions will apply.

Minimum Bandwidth

- The connectivity between sites must have the bandwidth capacity to handle the data to be replicated between the sites. The *minimum dedicated bandwidth* must be at least *5 Mb/sec*.

Network Considerations

Zerto Virtual Replication supports the following network configurations:

- Flat LAN networks.
- VLAN networks, including Private VLANs and stretched VLANs.
- WAN emulation.
- VPN IPsec. Zerto Virtual Replication supports both layer 2 and layer 3 third party VPNs.

The Zerto Virtual Replication architecture does not support NAT (Network Address Translation) firewalls.

Open Firewall Ports

The following **ports** must be opened in the firewalls in **both** the organization **and** cloud service provider sites. The # reference numbers refer to the architecture diagrams on the following pages:

Port	#	Description
22	9, 24	During Virtual Replication Appliance (VRA) installation on ESXi 4.x and 5.x hosts 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.
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 ZVM and VRAs on the same site.
4006	11	TCP communication between the ZVM and VRAs and the VBA 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	TCP communication between the ZVM and site VRAs to handle checkpoints.
5672	20	TCP communication between the ZVM and vCloud Director for access to AMQP messaging.
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.
9081	7, 23, 27	TCP communication between ZVMs and between a customer ZVM and a Zerto Cloud Connector. **This port must not be changed when providing DRaaS.**

Port	#	Description
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 cloud 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 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 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.

Recommended Best Practices

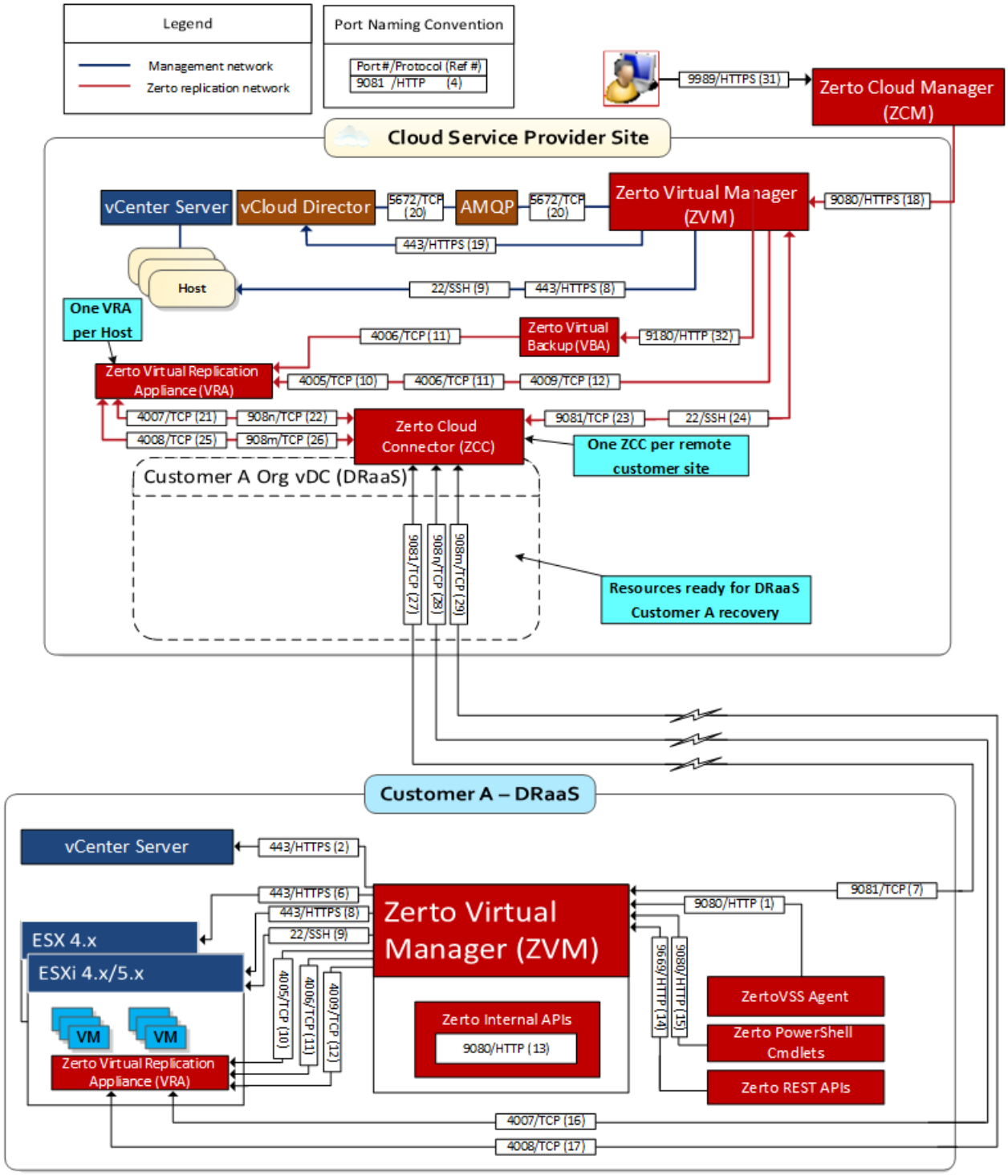
Zerto recommends the following best practices:

- Install Zerto Virtual Replication on a **dedicated virtual machine** with a **dedicated administrator account** and with VMware **High Availability (HA)** enabled. No other applications should be installed on this machine. If other applications are installed, the Zerto Virtual Manager service must receive enough resources and HA must remain enabled.
- Install a VRA on **every host in a cluster** so that if protected virtual machines are moved from one host to another, there is always a VRA to protect the moved virtual machines. When 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 the clusters.
- Install VRAs using **static IP addresses** and not DHCP.

DRaaS Architecture Diagram Showing Ports

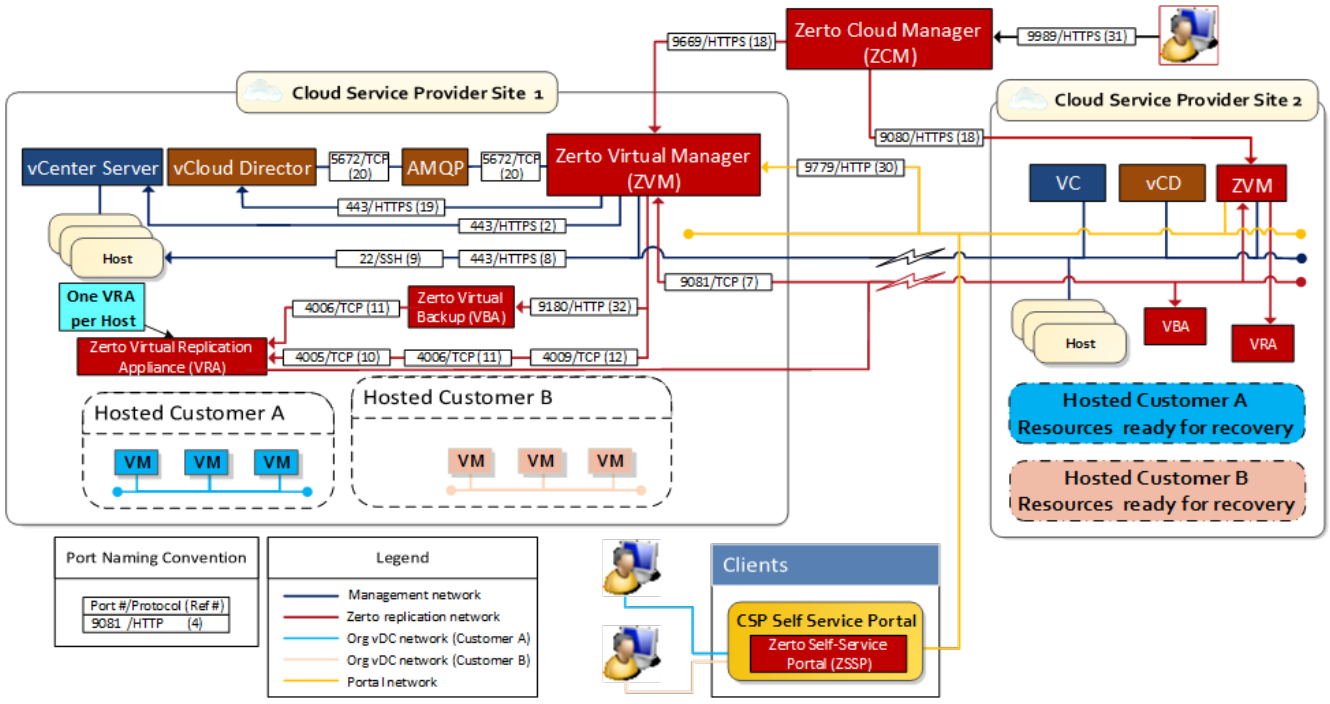
The following diagram shows a basic architecture, including vCloud Director, with required ports, when recovering to a cloud service provider, using DRaaS, with # references to the table, in Open Firewall Ports

12.



ICDR Architecture Diagram Showing Ports

The following diagram shows a basic architecture, including vCloud Director, with required ports, when recovering to a cloud service provider, using ICDR, with # references to the table, in Open Firewall Ports 12.


Zerto Cloud Manager (ZCM)
9669/HTTPS (18)
9989/HTTPS (31)
Cloud Service Provider Site 1
Cloud Service Provider Site 2
vCenter Server
vCloud Director
5672/TCP (20)
AMQP
5672/TCP (20)
Zerto Virtual Manager (ZVM)
9779/HTTP (30)
9080/HTTPS (18)
VC
vCD
ZVM
443/HTTPS (19)
443/HTTPS (2)
Host
22/SSH (9)
443/HTTPS (8)
9081/TCP (7)
One VRA per Host
4006/TCP (11)
Zerto Virtual Backup (VBA)
9180/HTTP (32)
Zerto Virtual Replication Appliance (VRA)
4005/TCP (10)
4006/TCP (11)
4009/TCP (12)
VBA
VRA
Hosted Customer A
VM
VM
VM
Hosted Customer B
VM
VM
VM
Hosted Customer A Resources ready for recovery
Hosted Customer B Resources ready for recovery
Port Naming Convention
Port #/Protocol (Ref #)
9081 /HTTP (4)
Legend
Management network
Zerto replication network
Org vDC network (Customer A)
Org vDC network (Customer B)
Portal network
Clients
CSP Self Service Portal
Zerto Self-Service Portal (ZSSP)

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. With 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's Solution, contact: @Zerto Support.