Zertø

Zerto Installation Guide for Microsoft Azure Environments

Rev01

June 2020

ZVR-INMZ-8.0 U2

The scripts are provided by example only and are not supported under any Zerto support program or service. All examples and scripts are provided "as-is" without warranty of any kind. The author and Zerto further disclaim all implied warranties including, without limitation, any implied warranties of merchantability or of fitness for a particular purpose.

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

ZVR-INMZ-8.0 U2

Table of Contents

Installing the Zerto Solution

Zerto provides a business continuity (BC) and disaster recovery (DR) solution in a virtual environment, enabling the replication of mission-critical applications and data as quickly as possible, with minimal data loss. When devising a recovery plan, these two objectives, minimum time to recover and maximum data to recover, are assigned target values: the recovery time objective (RTO) and the recovery point objective (RPO). Zerto enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto enables protecting virtual machines for extended, longer term recovery using a Long-term Retention process mechanism.

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^{TM}, 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)**: The ZVM is a Windows service, running on a dedicated Windows VM, 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. It 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 seen 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 VRA is a virtual machine installed on each hypervisor host where VMs are to be protected from or to. The VRA manages the replication of data from protected virtual machines to the recovery site. The target VRAs are responsible for maintaining any protected VMs disks. VMware limits the number of SCSI Controllers (4 per VM) and targets per Controller (15 per controller), leaving a maximum of 60 SCSI targets per VM. When managing a larger quantity of virtual disks, Zerto utilizes Virtual Replication Appliance Helpers (VRA-H), which act as a disk box with no IP and nearly no resources. VRA-Hs are spun up and down by Zerto automatically when nearing the 60-disk limit of the VRA or last VRA-H.
  - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

- **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.

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

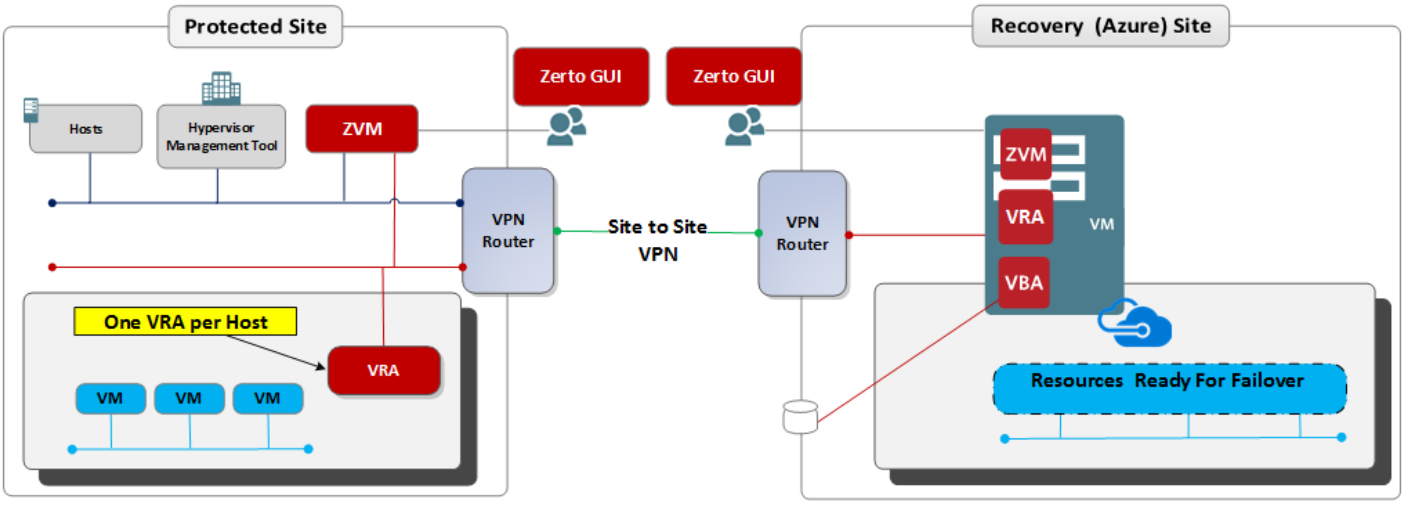
- **Data Streaming Service (DSS):** Installed on the VRA machine, and runs in the same process as the VRA. It is responsible for all the retention data path operations.

The following topics are described in this section:

Zerto Architecture in Azure Environments

The following diagram shows how the main components of Zerto are deployed across protected sites and Azure to provide disaster recovery.

> **Note:** For cloud-based architecture diagrams for cloud service providers, see Zerto Cloud Manager Installation Guide.



Zerto can be installed at multiple sites, all of which can be paired to Azure. For information about the ports used by Zerto, see Firewall Considerations in Microsoft Azure Environments on page 7.

Requirements - Zerto in Microsoft Azure Environments

For complete and detailed requirements, see Enterprise Guidelines for Microsoft Azure Environments.

- If either the production or recovery sites are protecting over 1000 VMs, then Zerto recommends the ZVM is configured with at least 16GB memory and at least 16 CPUs prior to installing Zerto 8.0 to ensure the new features in Zerto 8.0 release have enough resources to operate properly.

Before installing Zerto software, we recommend you follow the guidelines in the document Security and Hardening with Zerto.

Database Requirements in Microsoft Azure Environments

During the Zerto Virtual Manager installation, the user is able to select whether to install and use an **embedded** SQL Server (**localdb**) as the database.

Alternatively, and also during the installation, the user is able to choose whether to instead select and use an **external** SQL Server instance. To use an externally managed database, during the installation select the **Custom Installation** option.

The larger the environment protected by Zerto Virtual Manager, the larger the database size required to support it.

Supported **Microsoft SQL Server** versions: **2008**, **and higher**.

Before installing Zerto Virtual Manager, click to thoroughly review the following guides:

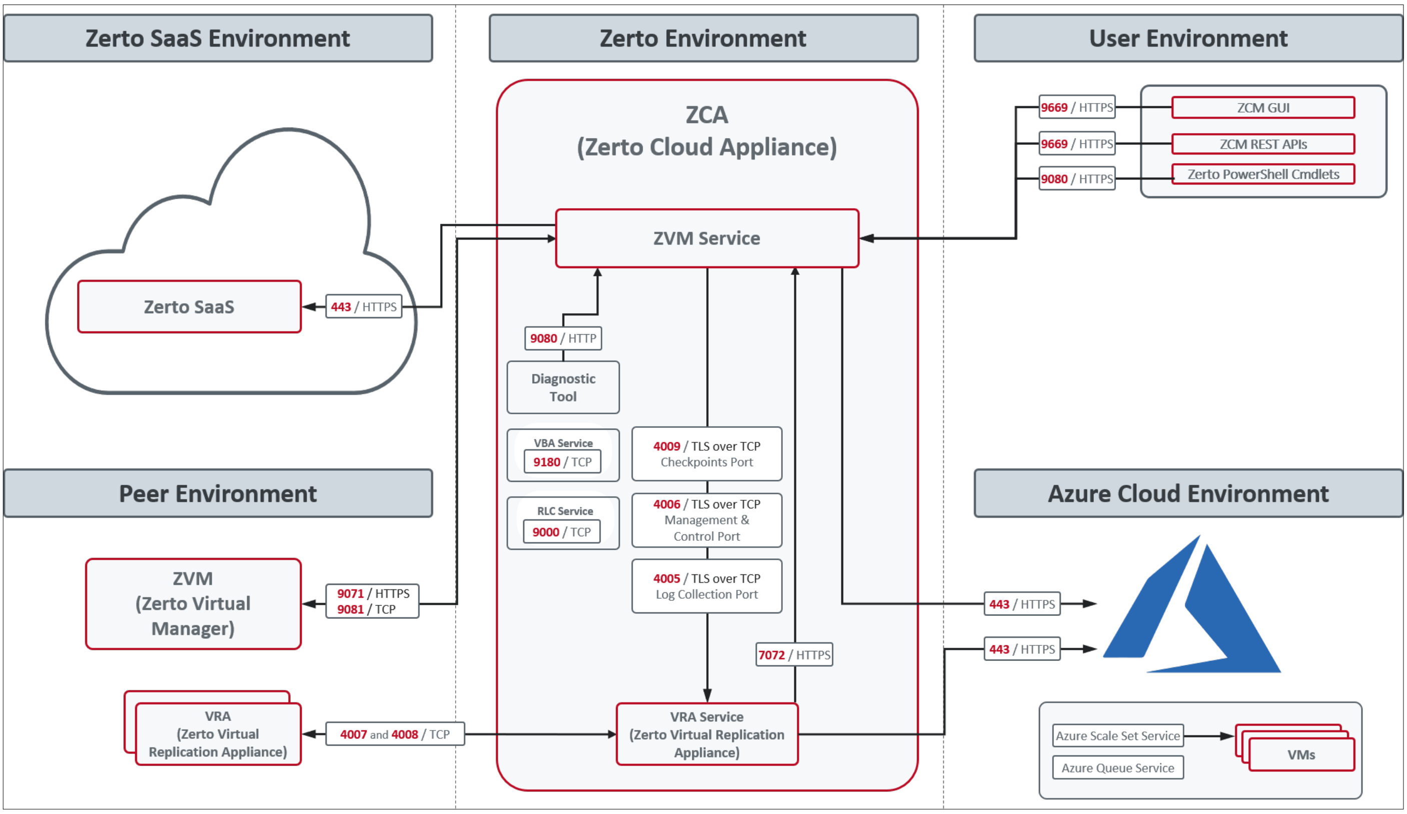
- Migrating the Zerto Database to Microsoft SQL Server.
- Zerto Scale and Benchmarking Guidelines.

You must have the following **permissions** set:

- **Public** and **dbcreator** server roles.
- Permission to connect to the database engine.
- Login enabled.
- In **User Mapping** choose the **master** database under which to create the Zerto database and set both **db_owner** and **public** for database role membership.

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.
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.

Access to Azure Cloud Environment

The followings list contains the endpoints required to set up replication to and from Azure:

- For **Azure global** and **Azure China** regions, set as follows:

Service category	Azure global URI	Azure URI (in China)
Azure service management	https://management.core.windows.net	https://management.core.chinacloudapi.cn
Azure Resource Manager	https://management.azure.com	https://management.chinacloudapi.cn

For further details see: https://docs.microsoft.com/en-us/azure/china/resources-developer-guide

- For **Azure Government** regions, set as follows:

Name	Azure Government endpoint
Azure API	https://management.usgovcloudapi.net/
Classic Deployment Model Url	https://management.core.usgovcloudapi.net/

For further details see: https://docs.microsoft.com/en-us/azure/azure-government/documentation-government-developer-guide#endpoint-mapping

- For **Azure Germany** regions, set as follows:

Name	Azure Germany endpoint
ServiceManagementUrl	https://management.core.cloudapi.de/
ResourceManagerUrl	https://management.microsoftazure.de/

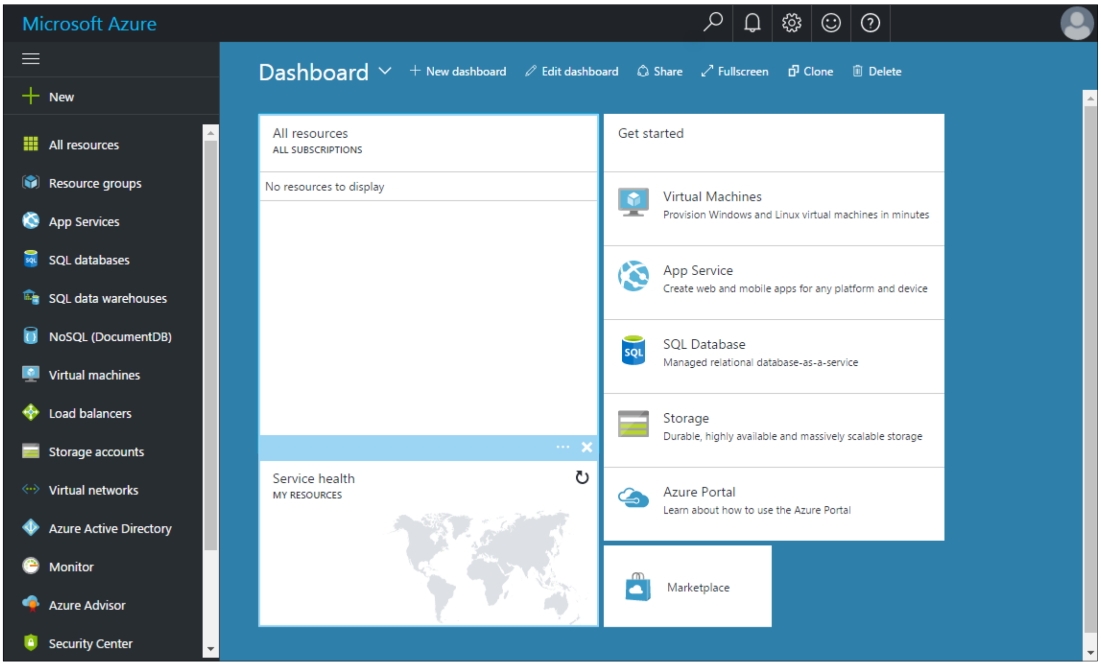
For further details see: https://docs.microsoft.com/en-us/azure/germany/germany-developer-guide#endpoint-mapping

Deploy Zerto Cloud Appliance from Azure Marketplace Portal

In order to install Zerto, you must first deploy Zerto Cloud Appliance VM. You will find Zerto Cloud Appliance in the Azure marketplace portal.

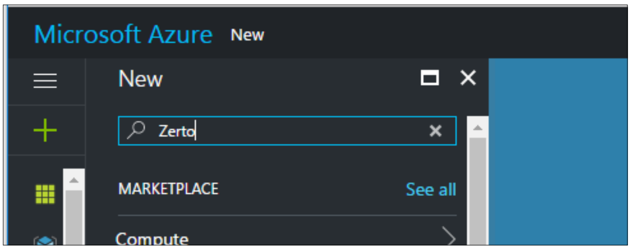
To deploy Zerto from the Microsoft Azure Marketplace:

1. Enter the URL: https://portal.azure.com. The Microsoft Azure portal opens.



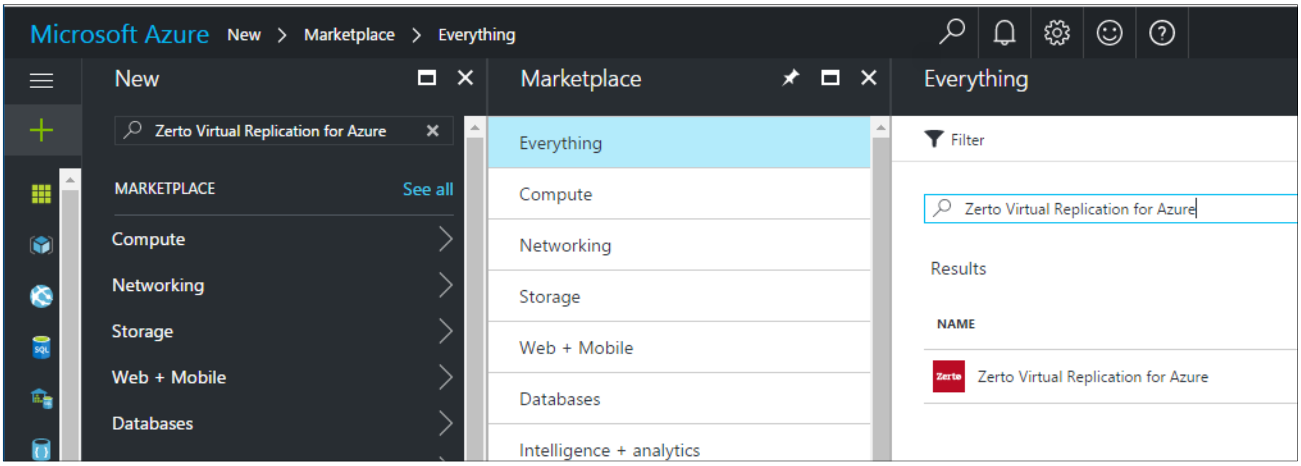
2. In the left pane at the top, click **New**, and in the search field that appears, enter the text **Zerto**.

   The predefined name, Zerto for Azure, appears in a drop-down.

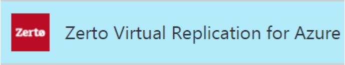


3. Select the predefined name, **Zerto for Azure**.

   The Zerto for Azure application appears in the right pane.



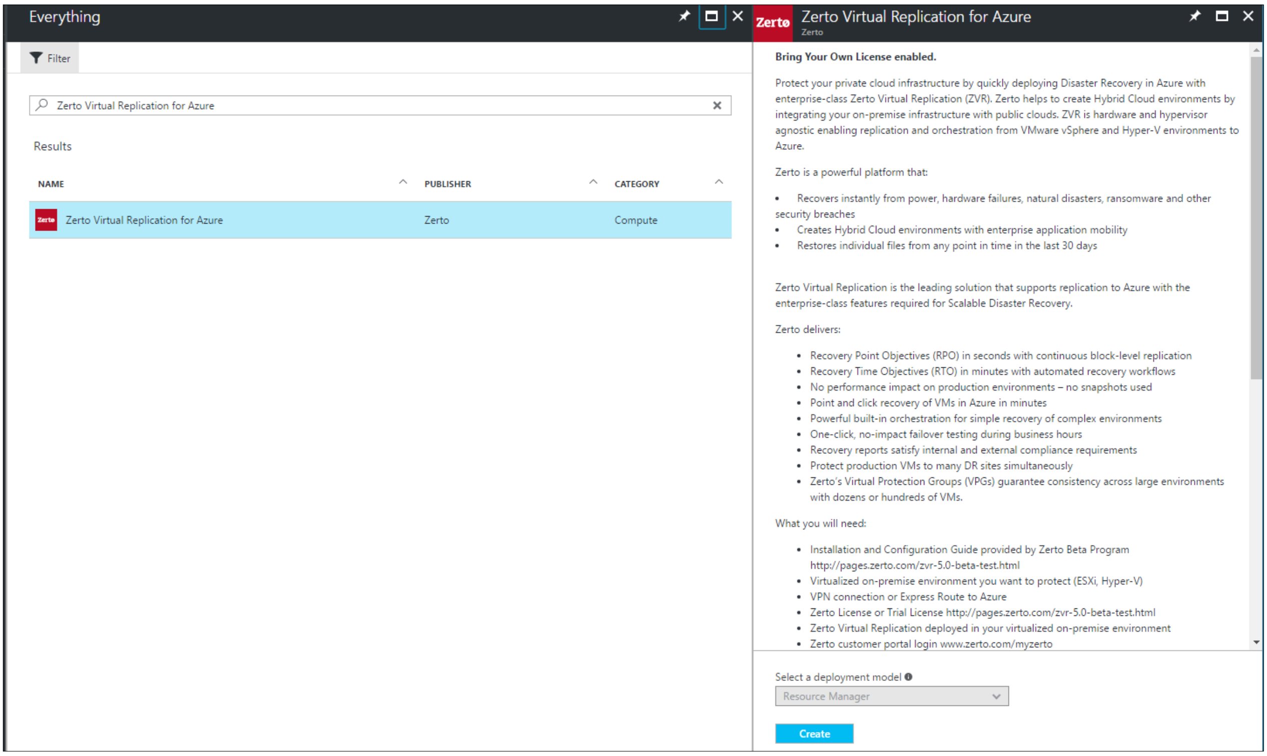
4. Click the Zerto for Azure application icon.



.

The Zerto for Azure application page appears.

Scroll down to read the section What you will need, and verify


Everything
Filter
Zerto Virtual Replication for Azure
Results
NAME
PUBLISHER
CATEGORY
Zerto Virtual Replication for Azure
Zerto
Compute
Zerto Virtual Replication for Azure
Zerto

Bring Your Own License enabled.

Protect your private cloud infrastructure by quickly deploying Disaster Recovery in Azure with enterprise-class Zerto Virtual Replication (ZVR). Zerto helps to create Hybrid Cloud environments by integrating your on-premise infrastructure with public clouds. ZVR is hardware and hypervisor agnostic enabling replication and orchestration from VMware vSphere and Hyper-V environments to Azure.

Zerto is a powerful platform that:

- Recovers instantly from power, hardware failures, natural disasters, ransomware and other security breaches
- Creates Hybrid Cloud environments with enterprise application mobility
- Restores individual files from any point in time in the last 30 days

Zerto Virtual Replication is the leading solution that supports replication to Azure with the enterprise-class features required for Scalable Disaster Recovery.

Zerto delivers:

- Recovery Point Objectives (RPO) in seconds with continuous block-level replication
- Recovery Time Objectives (RTO) in minutes with automated recovery workflows
- No performance impact on production environments – no snapshots used
- Point and click recovery of VMs in Azure in minutes
- Powerful built-in orchestration for simple recovery of complex environments
- One-click, no-impact failover testing during business hours
- Recovery reports satisfy internal and external compliance requirements
- Protect production VMs to many DR sites simultaneously
- Zerto's Virtual Protection Groups (VPGs) guarantee consistency across large environments with dozens or hundreds of VMs.

What you will need:

- Installation and Configuration Guide provided by Zerto Beta Program http://pages.zerto.com/zvr-5.0-beta-test.html
- Virtualized on-premise environment you want to protect (ESXi, Hyper-V)
- VPN connection or Express Route to Azure
- Zerto License or Trial License http://pages.zerto.com/zvr-5.0-beta-test.html
- Zerto Virtual Replication deployed in your virtualized on-premise environment
- Zerto customer portal login www.zerto.com/myzerto

Select a deployment model: Resource Manager

Create

5. Click **Create**, then define and deploy the VM. This VM is your **Zerto Cloud Appliance**.

6. Log into the Zerto Cloud Appliance VM, and install Zerto. To do this, continue with Installing Zerto in Microsoft Azure Environments on page 17.

Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure

Azure Managed Identities enables security best practices by allowing you to grant unique security credentials to users, groups and resources. Managed Identities is secure by default; users have no access to Azure resources until permissions are explicitly granted.

For installation of the ZCA to succeed in Azure, user assigned Managed Identities on the VM running the ZCA must be enabled and the permission level must be set to the following:

- Owner or Contributor
- Storage Blob Data Contributor
- Storage Queue Data Contributor

> **Important:**
>
> Zerto requires Owner or Contributor role as this level of permissions is required to manage Resource Groups.

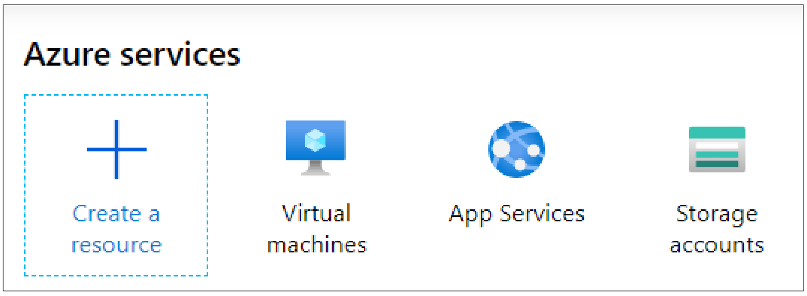
To enable user assigned Managed Identities on the ZCA VM:

1. Create the user assigned managed identity.
2. Assign the user assigned managed identity to the ZCA VM.
3. Add a role to user assigned managed identity of the ZCA VM.

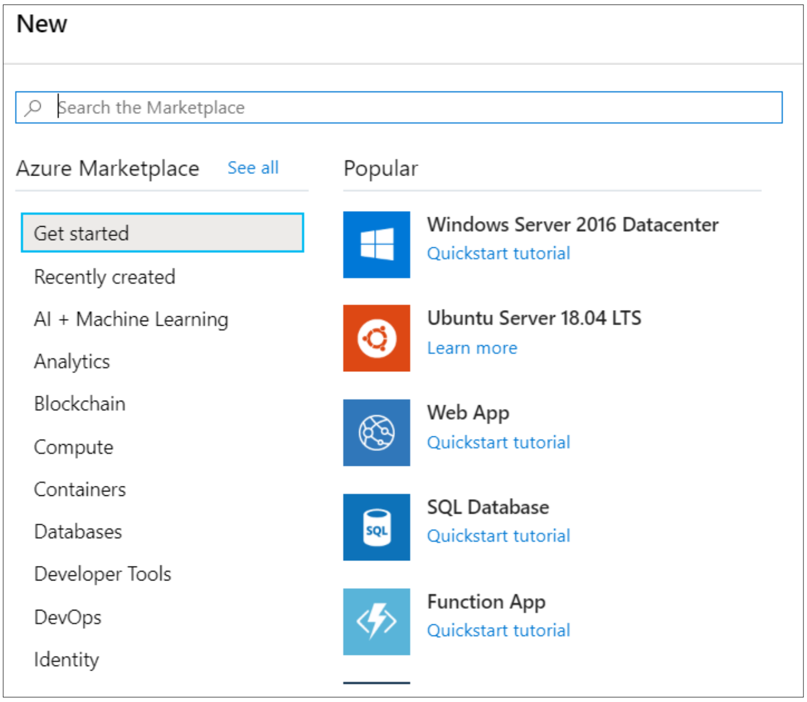
> **Important:**
>
> When adding or deleting role assignments, it can take up to 30 minutes for changes to take effect. The following error message will appear: “The ZCA was not assigned a role.”
>
> For further details, see https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting#rbac-changes-are-not-being-detected.

To create a user assigned Managed Identity:

1. In the Azure Portal, under Azure services navigate to **Create a resource**.

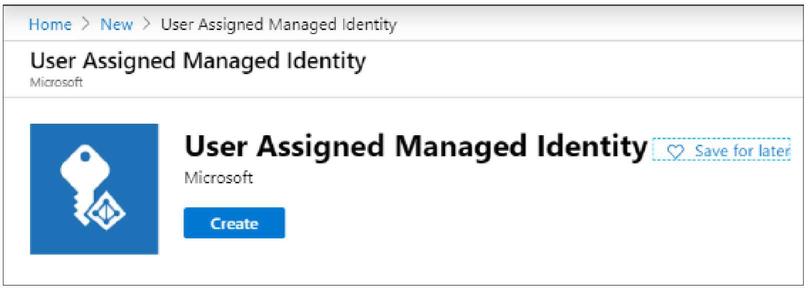


The Azure Marketplace page is displayed.



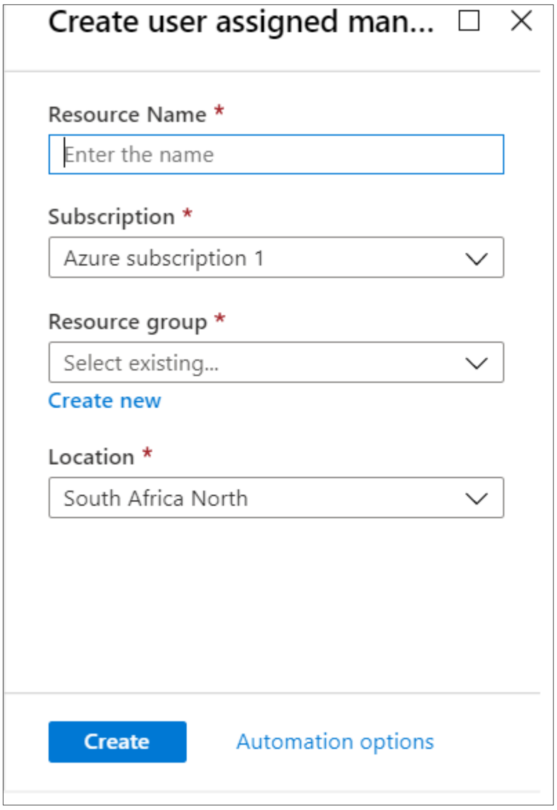
2. In the Search, type User Assigned Managed Identity.

The User Assigned Managed Identity page appears.


Home > New > User Assigned Managed Identity
User Assigned Managed Identity
Microsoft
User Assigned Managed Identity
Save for later
Microsoft
Create

3. Click **Create**.

The Create user assigned managed identity page is displayed.



Specify the following:

Resource Name	Enter the name of the resource.
Subscription:	Select the subscription to which the ZCA is associated.
Resource Group:	Select **any** resource group.
Location:	Select **Any** location.

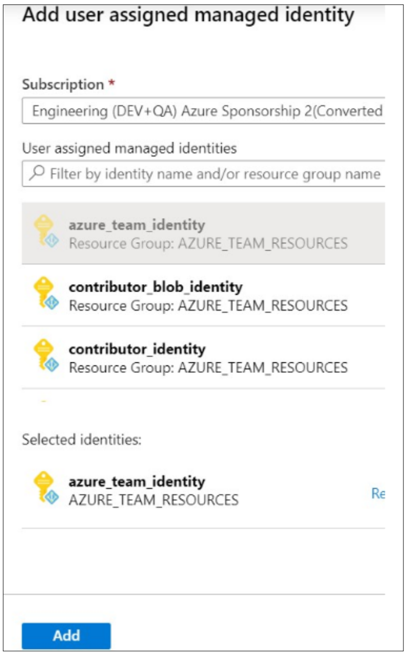
4. Click **Create**.

A user assigned managed identity is now created. Proceed to assigning the user managed identity to the ZCA VM.

To assign the user assigned managed identity to the ZCA VM:

1. In the Azure portal, navigate to the desired **VM** and click **Identity**.
2. Click **User assigned** and then **Add.** Make sure **System assigned** status is **Off**.

   The Add user assigned managed identity window appears.



Add user assigned managed identity

Subscription *

Engineering (DEV+QA) Azure Sponsorship 2(Converted

User assigned managed identities

Filter by identity name and/or resource group name

azure_team_identity
Resource Group: AZURE_TEAM_RESOURCES

contributor_blob_identity
Resource Group: AZURE_TEAM_RESOURCES

contributor_identity
Resource Group: AZURE_TEAM_RESOURCES

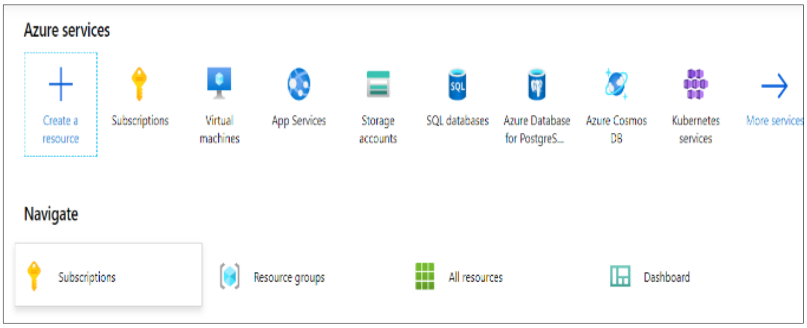
Selected identities:

azure_team_identity
AZURE_TEAM_RESOURCES

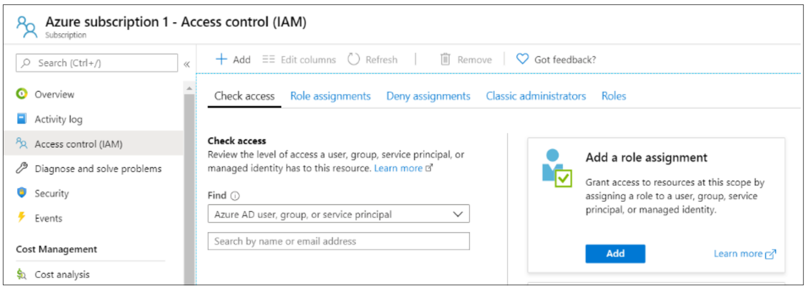
3. Select the user-assigned identity you want to add to the VM.
4. Click **Add** and proceed to setting a role assignment on the ZCA VM. **Only one user assigned managed identity can be set on the ZCA VM.**

To set the role on the user assigned managed identities:

1. Navigate to **All Services** and click **Subscriptions**.



2. Select the **Subscription** to which the ZCA is associated.
3. Navigate to **Access control (IAM)** and then click **Add** in the Add a role assignment area.



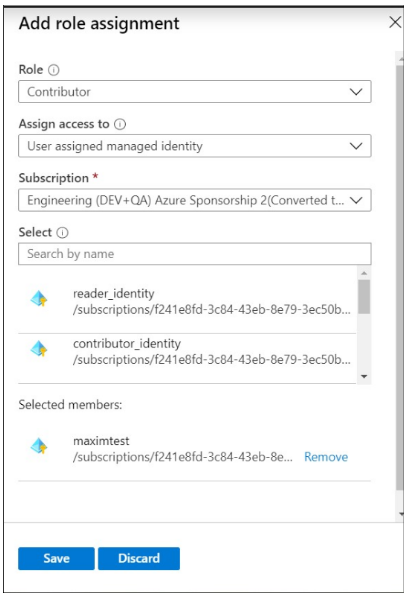
Azure subscription 1 - Access control (IAM)
Subscription

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find
Azure AD user, group, or service principal
Search by name or email address

Add a role assignment
Grant access to resources at this scope by assigning a role to a user, group, service principal, or managed identity.

The Add role assignment window appears.



Add role assignment

Role: Contributor

Assign access to: User assigned managed identity

Subscription *: Engineering (DEV+QA) Azure Sponsorship 2(Converted t...

Select: Search by name

reader_identity
/subscriptions/f241e8fd-3c84-43eb-8e79-3ec50b...

contributor_identity
/subscriptions/f241e8fd-3c84-43eb-8e79-3ec50b...

Selected members:

maximtest
/subscriptions/f241e8fd-3c84-43eb-8e... Remove

4. In the **Add role assignment** window, configure the following:

Role:	• **Owner** or **Contributor** • **Storage Blob Data Contributor** • **Storage Queue Data Contributor**
Assign access to:	**User Assigned Managed Identity**
Subscription:	The subscription to which the ZCA is associated
Select:	Select the user assigned managed identity.

5. Click **Save**.

6. Now proceed to install or upgrade the ZVM for Azure environments.

Installing Zerto in Microsoft Azure Environments

The process of installing the Zerto Virtual Manager in Azure also installs the Virtual Replication Appliance and the Zerto Backup Appliance.

You can install Zerto using the defaults provided by Zerto or perform a custom install, in which you determine the ports that will be used by Zerto.

- Performing an Express Installation on page 17
- Performing a Custom Installation on page 21

Performing an Express Installation

You can install Zerto using the defaults provided by Zerto. Site and connectivity information can be updated in the Zerto User Interface after installation, if required.

Before you Begin:

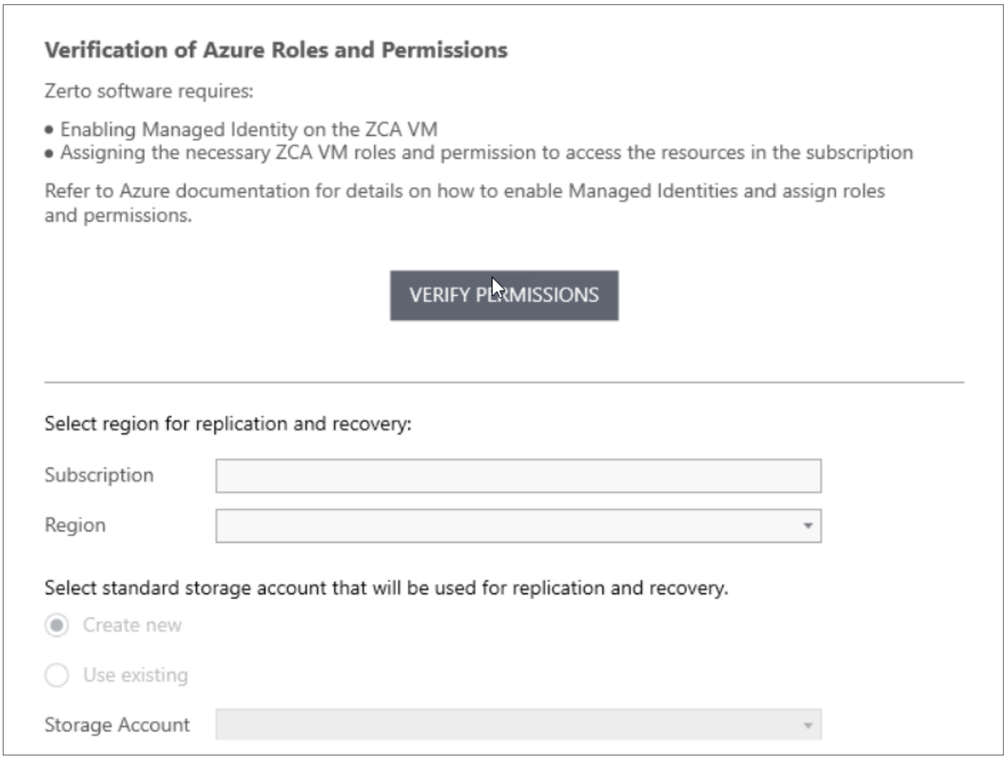
- Make sure you deployed Zerto Cloud Appliance.
- Make sure you reviewed Database Requirements in Microsoft Azure Environments on page 6.
- Internet access is not required in regions where the new Zerto AMI (Ubuntu 18.04 LTS with Python and Docker) exists in the Azure Marketplace. If the AMI does not exist then the following URLs are required:
    - azure.archive.ubuntu.com
    - security.ubuntu.com
- Make sure user assigned Managed Identities on the VM running the ZCA is enabled and the permission level is set to the following:
    - Owner or Contributor
    - Storage Blob Data Contributor
    - Storage Queue Data Contributor

  See Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure on page 12.

To perform an express install of Zerto:

1. Run the Zerto Installer for Microsoft Azure.
2. Follow the wizard through the installation until the window for the Installation Type and select the **Express Installation** option.
3. Click **NEXT**.

   The Verification of Azure Roles and Permissions window is displayed.



Verification of Azure Roles and Permissions

Zerto software requires:

- Enabling Managed Identity on the ZCA VM
- Assigning the necessary ZCA VM roles and permission to access the resources in the subscription

Refer to Azure documentation for details on how to enable Managed Identities and assign roles and permissions.

Select region for replication and recovery:

Subscription

Region

Select standard storage account that will be used for replication and recovery.

● Create new

○ Use existing

Storage Account

Important:

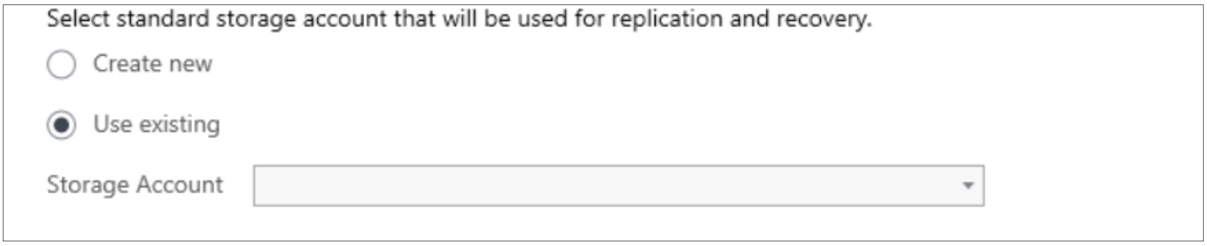
When adding or deleting role assignments, it can take up to 30 minutes for changes to take effect. The following error message will appear: “The ZCA was not assigned a role.”

For further details, see https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting#rbac-changes-are-not-being-detected.

4. Click **VERIFY PERMISSIONS**.
   - On success, proceed to step 5 on page 18.The Subscription field will be automatically populated. on page 18
   - On failure, verify that the VM running the ZCA has user assigned Managed Identities enabled. See Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure on page 12.
5. The **Subscription** field will be automatically populated.
6. Select the desired **Region**. If you do not select a region, the default is the VM’s Region
7. Define a **new** storage account that will be used for replication and recovery **or** select one from a list of **existing storage accounts** in the drop down menu.

Important:

Since all requests to the storage account are done through a secure connection the user can enable **Azure secure transfer** on the storage account.



Select standard storage account that will be used for replication and recovery.

○ Create new

● Use existing

Storage Account

By default, the Create new storage account option is selected.

Important:

Each ZCA requires a separate storage account. Multiple ZCAs using the same account is not supported.

a. By using the default option **Create new** in the **Storage Account** field, the installation creates a **new** resource group and a **Standard** storage account.

b. Click **Use existing** to select an existing storage account. When you select this option, the drop down menu becomes active.

    - Only **Standard storage accounts** which exist in the **selected region and subscription** are displayed in the storage account drop down menu.
    - General-purpose v1 (GPv1) accounts are supported.
    - Blob Storage accounts are not displayed for selection since the Blob Storage account type is not supported.
    - When you select an **existing** storage account, the account is automatically **tagged** with a **Zerto unique tag**.

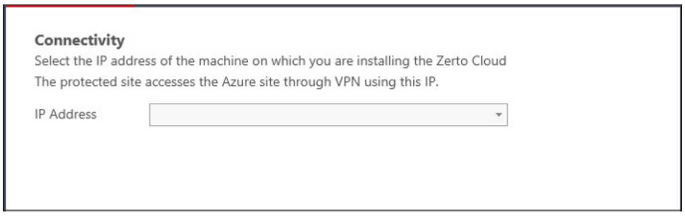
Note:

When a storage account is either **created or selected**, the following occurs:

- The **journal and recovery disks** are created in the storage account.
- The selected storage account appears in **Site Settings**, in the Site Information tab.

8. Click **NEXT**.

   The Connectivity window is displayed.



Connectivity

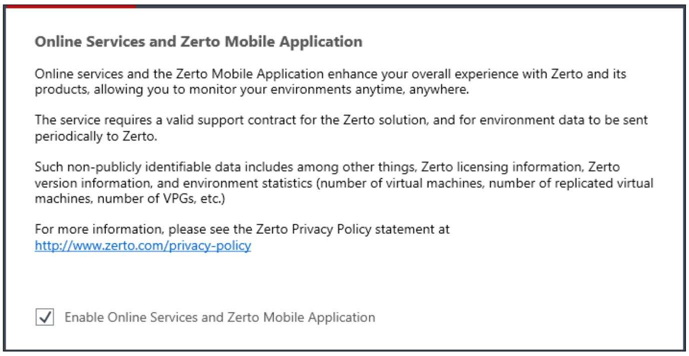
Select the IP address of the machine on which you are installing the Zerto Cloud

The protected site accesses the Azure site through VPN using this IP.

IP Address

9. Select the IP address of the machine on which you are installing the Zerto Cloud Appliance. The protected site accesses the Azure site through VPN using this IP.
10. Specify a name to identify this site.
11. Click **NEXT**.

    The Online Services and Zerto Mobile Application window is displayed.



Online Services and Zerto Mobile Application

Online services and the Zerto Mobile Application enhance your overall experience with Zerto and its products, allowing you to monitor your environments anytime, anywhere.

The service requires a valid support contract for the Zerto solution, and for environment data to be sent periodically to Zerto.

Such non-publicly identifiable data includes among other things, Zerto licensing information, Zerto version information, and environment statistics (number of virtual machines, number of replicated virtual machines, number of VPGs, etc.)

For more information, please see the Zerto Privacy Policy statement at http://www.zerto.com/privacy-policy

☑ Enable Online Services and Zerto Mobile Application

12. Click **NEXT**.
13. If you reached the subscription’s **maximum limit of storage accounts**, a message appears informing the user that creating a new storage account has **failed**.
14. After the checks complete successfully, click **RUN** and continue to the end of the installation.
15. If you are managing your disaster recovery from this machine, you can select to open the Zerto Virtual Manager (ZVM) Interface at the end of the installation, logging in with the user name and password for the Azure instance on which you installed the Zerto Virtual Manager. In this user interface you set up Zerto, as described in Initial Configuration on page 36.

You must **exclude** the following folders from **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.

Performing a Custom Installation

You can install Zerto providing specific details including the ports that will be used by Zerto and full contact details.

Before you Begin:

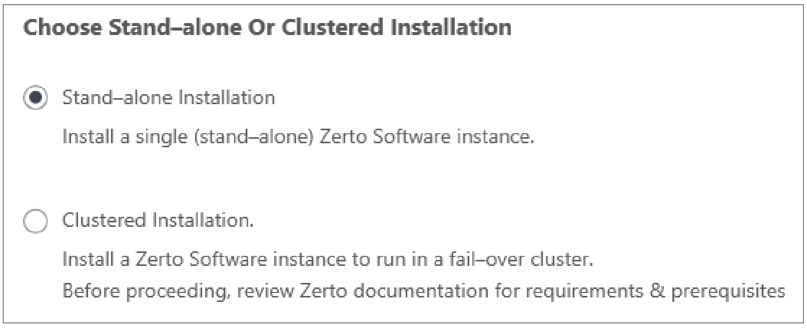
- Make sure you deployed Zerto Cloud Appliance.
- Make sure you reviewed Database Requirements in Microsoft Azure Environments on page 6.
- Internet access is not required in regions where the new Zerto AMI (Ubuntu 18.04 LTS with Python and Docker) exists in the Azure Marketplace. If the AMI does not exist then the following URLs are required:
  - azure.archive.ubuntu.com
  - security.ubuntu.com
- Make sure user assigned Managed Identities on the VM running the ZCA is enabled and the permission level is set to the following:
  - Owner or Contributor
  - Storage Blob Data Contributor
  - Storage Queue Data Contributor

  See Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure on page 12.

To perform a custom install of Zerto:

1. Run the Zerto Installer for Microsoft Azure.
2. Follow the wizard through the installation until the window for the **Installation Type** and select the **Custom Installation** option.
3. Click **Next**.

   The Choose Stand-alone Or Clustered Installation window appears.



Choose Stand–alone Or Clustered Installation

● Stand–alone Installation

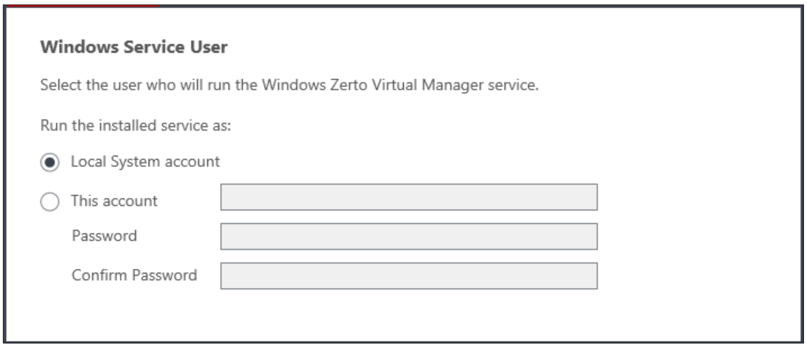
Install a single (stand–alone) Zerto Software instance.

○ Clustered Installation.

Install a Zerto Software instance to run in a fail–over cluster.
Before proceeding, review Zerto documentation for requirements & prerequisites

4. Select **Stand-alone Installation**, then click **Next**.

   The Windows Service User window is displayed.



Windows Service User

Select the user who will run the Windows Zerto Virtual Manager service.

Run the installed service as:

● Local System account

○ This account

Password

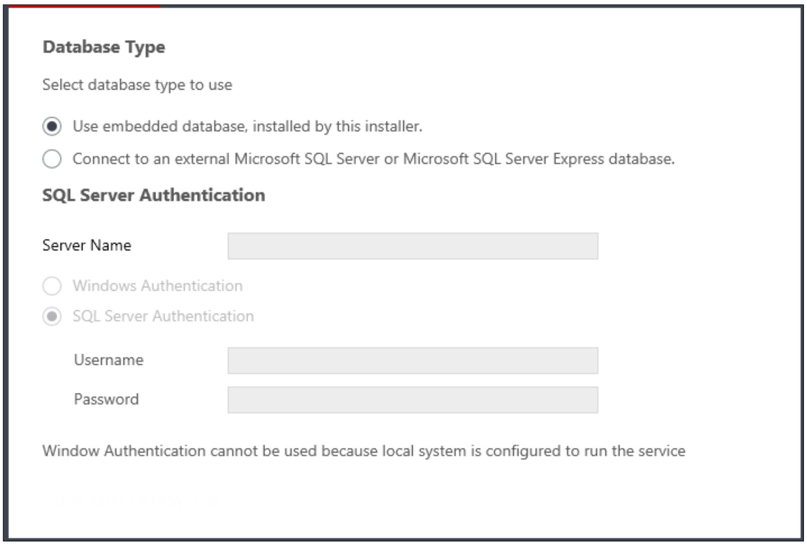
Confirm Password

5. Select either **Local System account** or **This account**:
   - **Local System account:** Use the Local System account to run the Zerto Virtual Manager service, which is installed as part of Zerto. The Local System account has unrestricted access to local resources.
   - **This account:** Use a specific account as the user account to run the Zerto Virtual Manager service, which is installed as part of Zerto. The account must have unrestricted access to local resources.
     - **Password:** The password to use to run the service under the specified account.
     - **Confirm Password:** Confirmation of the password.

Note: The account under which the Zerto Virtual Manager service runs must be able to authenticate against the Azure Active Directory Server if login authentication to the Zerto Virtual Manager is to be handled by Azure Active Directory.

6. Click **NEXT**.

   The Database Type window is displayed.



Database Type

Select database type to use

● Use embedded database, installed by this installer.

○ Connect to an external Microsoft SQL Server or Microsoft SQL Server Express database.

SQL Server Authentication

Server Name

○ Windows Authentication

● SQL Server Authentication

Username

Password

Window Authentication cannot be used because local system is configured to run the service

Information required by Zerto is stored in a database embedded in the Zerto Virtual Manager. This information includes details of the site where the Zerto Virtual Manager is installed, details of the Virtual Replication Appliance and the volumes it uses, and points-in-time recorded for recovery purposes. By default an embedded SQL-based database is used, but you can use an externally managed database, either Microsoft SQL Server or SQL Server Express.

> **Note:** Protection and recovery can only be performed when the database is running. Therefore, if you use an external database and it is down for any reason, protection and the possibility of recovery ceases.

7. To use the embedded database, leave the default, or select the option to connect to an external Microsoft SQL Server database.

   Zerto recommends using SQL Server when a site has more than 40 hosts that have virtual machines that need protecting, and the site has more than 400 virtual machines that need protecting.

   If you select the external database option, the SQL Server Authentication section is enabled.

   a. Enter the following details to enable access to the SQL Server database:

      - **Server Name**: The domain name and server instance to connect to, with the format <server_name>\<instance_name> or <Server_IP>\<instance_name>

   b. Specify one of the following authentication options:

      - **Windows Authentication**: Use Windows authentication. This option is only enabled if a specific service user account was specified in the previous Windows Service User dialog, in which case the service account name and password are used.

      - **SQL Server Authentication**: Use SQL Server authentication.

        Username: The user name for the SQL Server database.

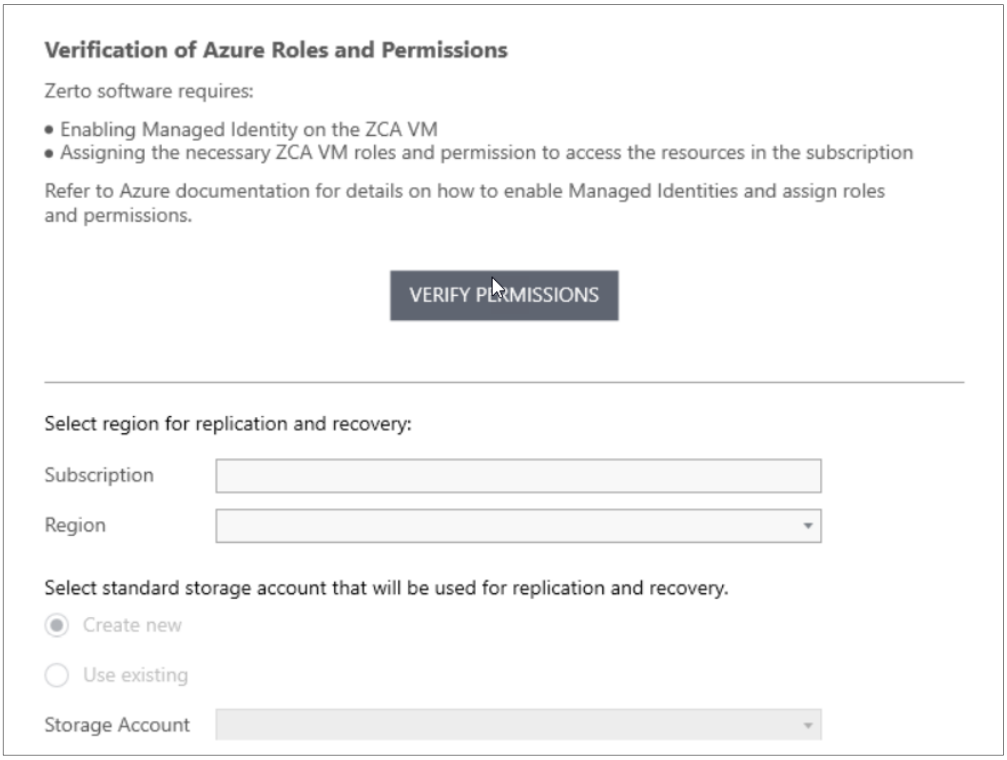
Password: A valid password for the given user name.

c. When you select SQL Server authentication and enter a user name and password, click **TEST AUTHENTICATION**, which is displayed.

The installer checks whether it can connect to the specified database with the specified username and password. You can only continue when the authentication is successful.

8. Click **NEXT**.

The Verification of Azure Roles and Permissions window is displayed.



Verification of Azure Roles and Permissions

Zerto software requires:

- Enabling Managed Identity on the ZCA VM
- Assigning the necessary ZCA VM roles and permission to access the resources in the subscription

Refer to Azure documentation for details on how to enable Managed Identities and assign roles and permissions.

Select region for replication and recovery:

Select standard storage account that will be used for replication and recovery.

● Create new

○ Use existing

! **Important:**

When adding or deleting role assignments, it can take up to 30 minutes for changes to take effect. The following error message will appear: “The ZCA was not assigned a role.”

For further details, see https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting#rbac-changes-are-not-being-detected.

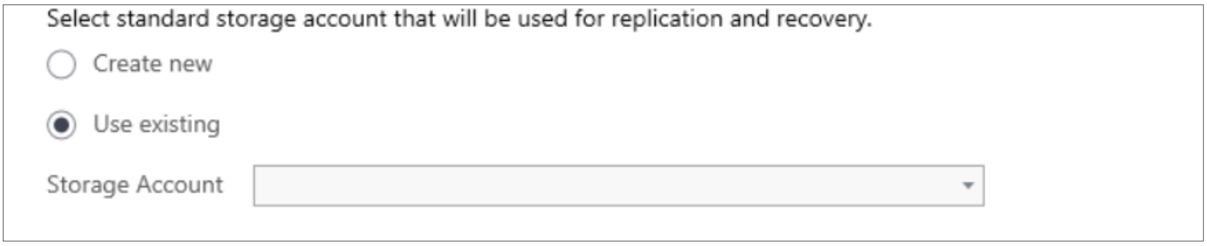
9. Click **VERIFY PERMISSIONS**.

- On success, proceed to step 10 on page 25.The Subscription field will be automatically populated. on page 25

- On failure, verify that the VM running the ZCA has user assigned Managed Identities enabled. See Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure on page 12.

10. The **Subscription** field will be automatically populated.
11. Select the desired **Region**. If you do not select a region, the default is the VM’s Region
12. Define a **new** storage account that will be used for replication and recovery **or** select one from a list of **existing storage accounts** in the drop down menu.

> **Important:**
>
> Since all requests to the storage account are done through a secure connection the user can enable **Azure secure transfer** on the storage account.



Select standard storage account that will be used for replication and recovery.

○ Create new

● Use existing

Storage Account

By default, the Create new storage account option is selected.

> **Important:**
>
> Each ZCA requires a separate storage account. Multiple ZCAs using the same account is not supported.

a. By using the default option **Create new** in the **Storage Account** field, the installation creates a **new** resource group and a **Standard** storage account.

b. Click **Use existing** to select an existing storage account. When you select this option, the drop down menu becomes active.

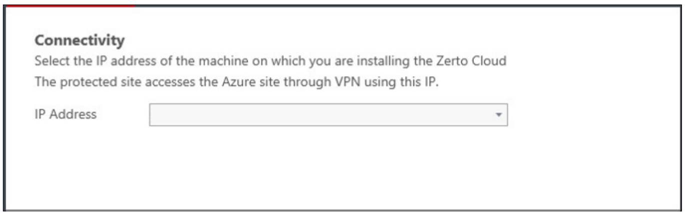
   - Only **Standard storage accounts** which exist in the **selected region and subscription** are displayed in the storage account drop down menu.
   - General-purpose v1 (GPv1) accounts are supported.
   - Blob Storage accounts are not displayed for selection since the Blob Storage account type is not supported.

- When you select an **existing** storage account, the account is automatically **tagged** with a **Zerto unique tag**.

> **Note:**
>
> When a storage account is either **created or selected**, the following occurs:
>
> - The **journal and recovery disks** are created in the storage account.
> - The selected storage account appears in **Site Settings**, in the Site Information tab.

13. Click **NEXT**.

    The Connectivity page is displayed.



Connectivity

Select the IP address of the machine on which you are installing the Zerto Cloud

The protected site accesses the Azure site through VPN using this IP.

IP Address

14. Select the IP address of the machine on which you are installing the Zerto Cloud Appliance. The protected site accesses the Azure site through VPN using this IP.
15. Click **NEXT**.

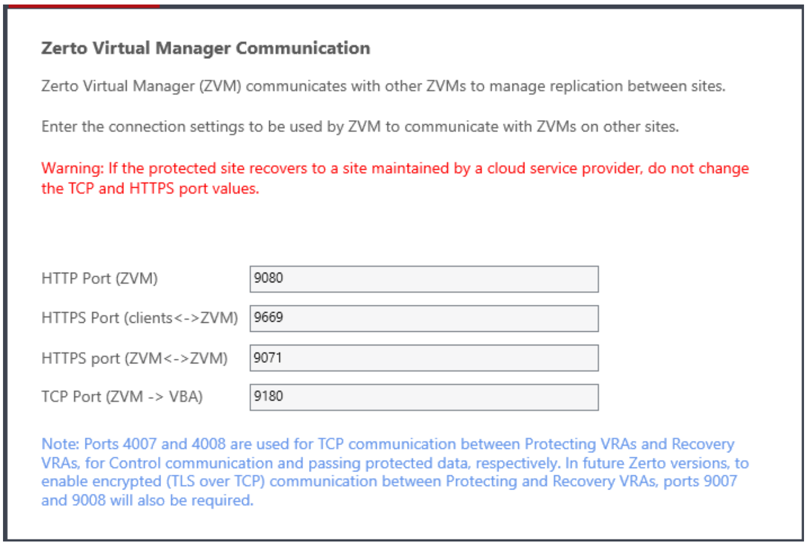
    The Zerto Virtual Manager Site Details window is displayed. Enter the site details:

16. Enter the site details:

Site Name:	(Optional) A name to identify the site. This name is displayed in the Zerto User Interface
Site Location:	(Mandatory) Information such as the address, or name of the site to identify it.
Contact Name:	(Mandatory) The name of the person to contact if a need arises.
Contact Email:	(Optional) The email address to contact if a need arises.
Contact Phone:	(Optional) The phone number to contact if a need arises.

17. Click **NEXT**.

    The Zerto Virtual Manager Communication window is displayed.



Zerto Virtual Manager Communication

Zerto Virtual Manager (ZVM) communicates with other ZVMs to manage replication between sites.

Enter the connection settings to be used by ZVM to communicate with ZVMs on other sites.

Warning: If the protected site recovers to a site maintained by a cloud service provider, do not change the TCP and HTTPS port values.

HTTP Port (ZVM): 9080

HTTPS Port (clients<->ZVM): 9669

HTTPS port (ZVM<->ZVM): 9071

TCP Port (ZVM -> VBA): 9180

Note: Ports 4007 and 4008 are used for TCP communication between Protecting VRAs and Recovery VRAs, for Control communication and passing protected data, respectively. In future Zerto versions, to enable encrypted (TLS over TCP) communication between Protecting and Recovery VRAs, ports 9007 and 9008 will also be required.

PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	Comments
HTTP Port (ZVM)	9080	Inbound	Zerto Virtual Manager *- and -* Zerto internal APIs, and Cmdlets	
HTTPS Port (clients<->ZVM)	9669	Inbound	Zerto User Interface *- and -* Zerto Virtual Manager	

PORT DESCRIPTION PARAMETER	DEFAULT PORT NUMBER	COMMUNICATION DIRECTION	BETWEEN...	Comments
TCP Port (ZVM<->ZVM) or **HTTPS Port (ZVM<->ZVM)**	9081 or 9071	Inbound and outbound	Zerto Virtual Manager *- and -* Zerto Virtual Manager	If you change the value, when pairing sites, use the TCP/HTTPS port value you specify here. Pairing the sites is described in Pairing an Azure Site on page 36.
TCP Port (ZVM->VBA)	9180	Inbound and outbound	Zerto Virtual Manager *- and -* Virtual Backup Appliance (VBA)	

18. Click **NEXT**.

    The Validation window is displayed. The installation checks that the installation can proceed successfully.

    > **Note:** If you reached the subscription’s **maximum limit of storage accounts**, a message appears informing you that creating a new storage account has **failed**.

19. After you see that Zerto can be installed successfully, click **RUN** and continue to the end of the installation.

20. If you intend managing your disaster recovery from this machine, you can select to open the Zerto Virtual Manager (ZVM) Interface at the end of the installation, logging in with the user name and password for the Azure instance on which you installed the Zerto Virtual Manager. In this user interface you set up Zerto, as described in Initial Configuration on page 36.

You must **exclude** the following folders from **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.

Performing a Silent Installation

You can perform a silent installation of Zerto, by running the installation executable in a script with the **-s** option.

Before you Begin:

- For silent installation of the ZCA to succeed in Azure, user assigned Managed Identities on the VM running the ZCA must be enabled and the permission level must be set to the following:
  - Owner or Contributor,
  - Storage Blob Data Contributor
  - Storage Queue Data Contributor

  See Enabling User Assigned Managed Identities and Setting Mandatory Permissions in Azure on page 12.

> **Important:**
>
> When adding or deleting role assignments, it can take up to 30 minutes for changes to take effect. The following error message will appear: “The ZCA was not assigned a role.”
>
> For further details, see https://docs.microsoft.com/en-us/azure/role-based-access-control/troubleshooting#rbac-changes-are-not-being-detected.

```
<installation>.exe [-s][PROPERTY=VALUE]
```

Where:

- **s** Runs the silent installation.
- **PROPERY=VALUE** Sets **PROPERTY** to **VALUE**. The **PROPERTY** can be anything in the table below.

Property	Description	Mandatory
ResourceGroupName	The name of the resource group containing the storage account	Yes
StorageAccountName	The name of the storage account.	Yes
RegionId	The region of the storage account. For a full list of available Azure regions, see: https://azure.microsoft.com/en-in/global-infrastructure/locations/	Yes
SiteContactEmail	The email address to contact if a need arises.	No
SiteContactInfo	The name of the person to contact if a need arises.	No
SiteContactPhone	The phone number to contact if a need arises.	No
SiteLocation	Information to identify the site location.	No
SiteName	A name to identify the site. This name is displayed in the Zerto User Interface.	No
SiteTcpPort	The port used for communication between Zerto Virtual Managers. Default is 9081.	No
SiteHttpPort	The port used for inbound communication between the Zerto Virtual Manager and Zerto internal APIs, and Cmdlets. Default is 9080.	No
SiteHttpsPort	The port used for inbound communication between the Zerto User Interface and the Zerto Virtual Manager. Default is 9669.	No
SiteTcpPortVba	The port used for communication between the Zerto Virtual Manager and the Virtual Backup Appliance. Default is 9180.	No

For example:

```
"Zerto ZCA Azure Installer.exe" -s -l install.log SiteName=max
ResourceGroupName=maxim_installer RegionId="West Europe"
StorageAccountName=maximinstaller
```

Executing a Silent Installation

A silent installation is executed via the ZCA machine’s Command Prompt window.

The following is an example command line to run a silent installation:

```
"Zerto ZCA Azure Installer.exe" -s -l install.log SiteName=max
ResourceGroupName=maxim_installer RegionId="West Europe"
StorageAccountName=maximinstaller
```

Installing Zerto Cmdlets

Windows PowerShell is a command-line shell running under Windows for system administrators. The Windows PowerShell includes both an interactive command line prompt and a scripting environment. Each can be used independently or they can be used together.

Windows PowerShell is built on top of the .NET Framework common language runtime (CLR), enabling it to accept and return .NET Framework objects.

To run the Zerto cmdlets you must first run the installation package supplied by Zerto.

> **Note:** You must have both Microsoft .NET Framework 4.7.2 and Windows PowerShell installed.

To install the Zerto cmdlets:

1. Make sure that Windows PowerShell is closed.
2. Run the installation file.

After installing the Zerto cmdlets, either add the cmdlets each time you open the Windows PowerShell or create a Windows PowerShell profile.

The following procedure describes how to add the Zerto cmdlets to every Windows PowerShell session.

To add the Zerto cmdlets to the current session:

1. Open Windows PowerShell with the following arguments:

```
-NoExit -Command Add-PSSnapIn Zerto.PS.Commands
```

The Add-PSSnapin cmdlet adds registered Windows PowerShell snap-ins to the current session.

2. To add the Zerto cmdlets to every session, in the **Properties** dialog for a PowerShell shortcut specify a Target value similar to the following:

```
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe -NoExit
-Command Add-PSSnapIn Zerto.PS.Commands
```

> **Note:** You can create a Windows PowerShell profile, as described in the Windows

> PowerShell Help, to add the snap-in to all future Windows PowerShell sessions.

For more details, see *Zerto Virtual Replication PowerShell Cmdlets Guide*.

Uninstalling Zerto

You uninstall Zerto via the *Uninstall a program* in the Windows Control Panel.

When you uninstall Zerto the following are also removed:

- The Zerto Cloud Appliance.
- All the virtual protection groups defined to protect virtual machines, including all the target disks managed by the Zerto Cloud Appliance for the virtual machines that were being protected.

If, for any reason, a Zerto Cloud Appliance cannot be removed, contact Zerto support.

Accessing the Zerto User Interface

You manage the protection and replication of virtual machines between the protected site and Azure using the Zerto User Interface. On first access to the Zerto User Interface, you might have to add a security certificate to set up secure communication. Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts or programs.

> **Note:**
>
> - For supported browsers, see Zerto Interoperability Matrix.
> - The **lowest** supported screen resolution is **1366x768**.

> **Note:** You must **exclude** the following folders from **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.

To use the Zerto Virtual Manager Web Client:

1. In a browser, enter the following URL:

   https://zvm_IP:9669

   where **zvm_IP** is the IP address of the Zerto Virtual Manager for the site you want to manage.

2. Log on using the user name and password of the virtual machine on which you installed the Zerto Cloud Appliance.

Adding a Security Certificate for the Zerto User Interface

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

To install a security certificate for the Zerto User Interface:

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

Note the following:

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

1. Click **View Certificate**.

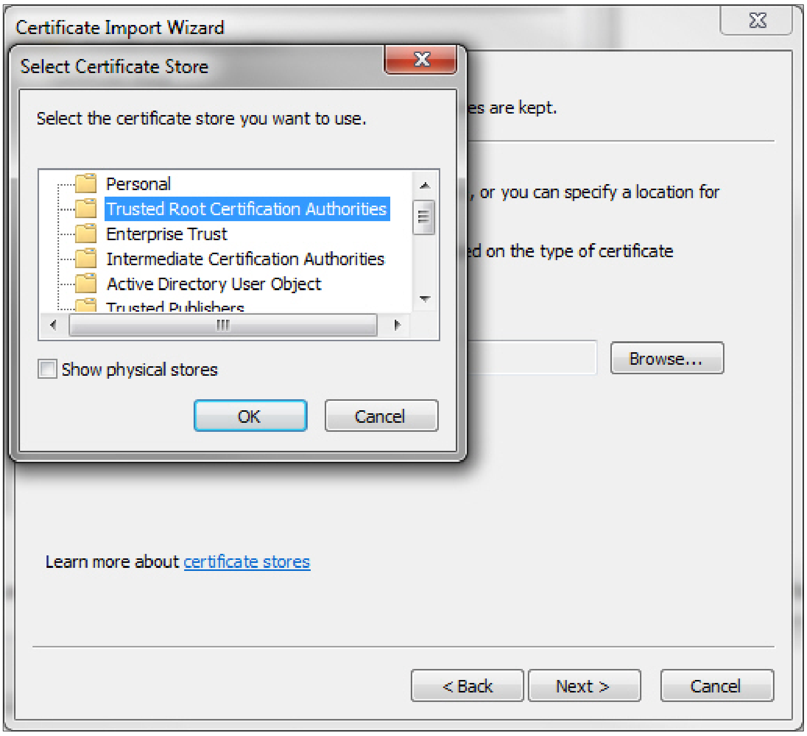
   The Certificate dialog is displayed.

2. Click **Install Certificate.**

   The Certificate Import wizard dialog is displayed.

3. Follow the wizard, and specifically:

- Place all the certificates in the **Trusted Root Certification Authorities store.**
- Select the **Place all certificates in the following store** option and browse to select the **Trusted Root Certification Authorities store**.

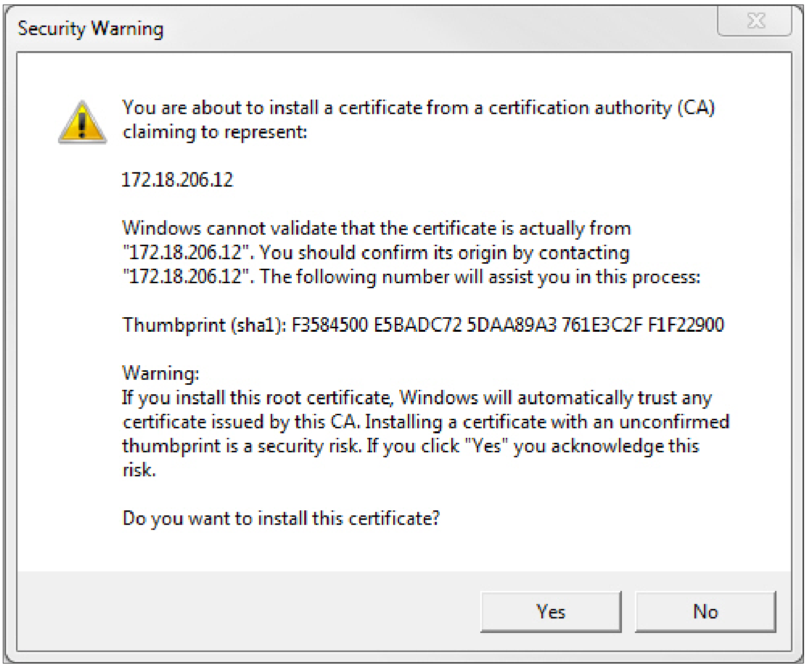


Select the certificate store you want to use.

Learn more about certificate stores

Certificate Import Wizard
Select Certificate Store
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
Show physical stores
OK
Cancel
es are kept.
, or you can specify a location for
d on the type of certificate
Browse...
< Back
Next >
Cancel

4. Continue to the end of the wizard. Click **Yes** when the Security Warning is displayed.



You are about to install a certificate from a certification authority (CA) claiming to represent:

172.18.206.12

Windows cannot validate that the certificate is actually from "172.18.206.12". You should confirm its origin by contacting "172.18.206.12". The following number will assist you in this process:

Thumbprint (sha1): F3584500 E5BADC72 5DAA89A3 761E3C2F F1F22900

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

5. Click **OK** that the installation was successful.

6. Click **OK** when prompted and then **Yes** in the **Security Alert** dialog to continue.

Initial Configuration

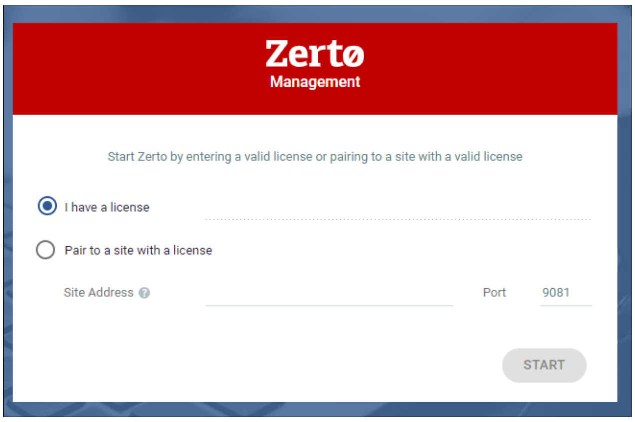
After installing Zerto, you configure the site. Zerto is configured and managed from within the Zerto User Interface. This section describes the initial configuration required after installing Zerto.

The following topics are described in this section:

- Registering the Zerto License on page 36
- Pairing an Azure Site on page 36

Registering the Zerto License

When you first access the Zerto User Interface, you must register your use of Zerto by entering the Zerto Cloud Appliance (ZCA) license, or Zerto Virtual Replication Enterprise Cloud Edition (ZVRCE) license supplied by Zerto.



Start Zerto by entering a valid license or pairing to a site with a valid license

● I have a license

○ Pair to a site with a license

Site Address

Port 9081

After entering a valid license, the DASHBOARD tab is displayed with a summary of the site.

In order to protect virtual machines to Azure, you must first pair the protected site containing the virtual machines that you want to protect with the Azure site on which you installed the Zerto Cloud Appliance. This is described in Pairing an Azure Site on page 36.

Pairing an Azure Site

See the following sections:

- Pair to Another Site on page 36
- Unpairing Sites on page 38

Pair to Another Site

You can pair to any site where Zerto is installed.

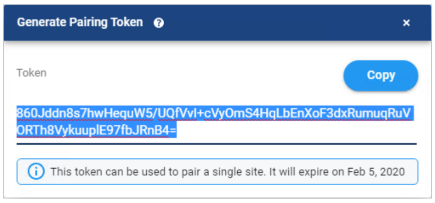
Zerto can be installed at multiple sites and each of these sites can be paired to any other site on which Zerto has been installed. Virtual machines that are protected on one site can be recovered to any paired site.

To pair to a site:

1. From the **remote** site to which you will pair, in Zerto Virtual Manager > Sites tab, click the button **Generate Pairing Token**.

2.

   The Generate Pairing Token window opens.

   Token

   860Jddn8s7hwHequW5/UQfVvl+cVyOmS4HqLbEnXoF3dxRumuqRuVORTh8VykuuplE97fbJRnB4=

   This token can be used to pair a single site. It will expire on Feb 5, 2020

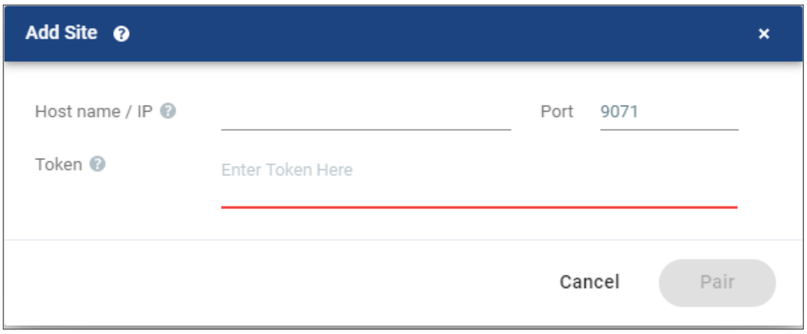
3. Click **Copy**, to copy the token.

   The token **expires** when the earliest of one of the following conditions is met:

   - 48 hours after clicking Copy
   - At the next ZVM process termination
   - After the token is used to authenticate the pairing request

4. From the site which will initiate the pairing, in the Zerto Virtual Manager > Sites tab, click **PAIR**.

   The Add Site window is displayed.

   Host name / IP

   Port 9071

   Token Enter Token Here

5. Specify the following:

   - **Host name/IP:** IP address or fully qualified DNS host name of the **remote** site Zerto Virtual Manager to pair to.

- **Port:** The HTTPS port communication between the sites. Enter the port that was specified during the installation. The default port during the installation was 9071.
- **Token:** Paste the token which you copied above.

6. Click **PAIR**.

   The sites are paired, meaning that the Zerto Virtual Manager for the local site is connected to the Zerto Virtual Manager at the remote site.

   After the pairing completes, the content of the SITES tab updates to include summary information about the paired site.

Unpairing Sites

You can unpair any two sites that are paired to each other.

> ! **Important:** If there is a VPG on either of the sites you are unpairing, the VPGs will be **deleted**.

To unpair two sites:

1. In the Zerto User Interface, in the SITES tab, select the site which you want to unpair.
2. Click **UNPAIR**.

   A message appears warning the user that the sites are about to unpair.

   If there are either protected or recovered VPGs on the paired sites, a message appears warning the user that the VPGs will be deleted.
3. For vSphere, Hyper-V and Azure platforms, you can select to keep disks to use for preseeding if the VMs are re-protected. If you select this option, the disks are not removed from the recovery site.
4. To unpair, click **CONTINUE**.

   The sites are no longer paired. If there are VPGs on either site, they are deleted.

   The VRA on the recovery site that handles the replication for the VPG is updated including keeping or removing the replicated data for the deleted VPG, depending if you selected to keep disks to use for preseeding.

   The locations of the saved target disks are specified in the **Events** tab in the ZVM application on the **Recovery** site.

Upgrading Zerto

Zerto releases regular updates. VMware and Microsoft also release new versions of their products which can impact Zerto. This document describes different options for different upgrade scenarios.

The following topics are described in this section:

- Guidelines to Upgrading Zerto on page 39
- Upgrading Multiple Sites Running Different Versions on page 43
- Upgrading To More Than One Version Higher on page 43
- Upgrading Zerto PowerShell Cmdlets on page 47.
- Upgrading Zerto Cloud Manager on page 47
- Upgrading Zerto Cloud Connectors on page 48

Guidelines to Upgrading Zerto

Before upgrading, review the following documents for **compatibility**:

- Product Version Lifecycle Matrix for Zerto
- Zerto Interoperability Matrix
- Zerto Scale and Benchmarking Guidelines

Then, review the following considerations:

- Zerto recommends upgrading to the **latest version** of Zerto that supports the environment you are using. See the Zerto Interoperability Matrix for the list of environments supported by this version of Zerto.
- The order you upgrade the sites, protected or recovery, is not relevant as long as **paired** sites remain only **one version apart**, that is, only one version higher or lower.
- When upgrading from versions prior to Zerto 6.0U2, changing the Journal Size Hard Limit requires restarting the VRAs.
- During an upgrade from v6.0x to v6.5, all back up and repositories configurations are deleted.

> **Note:** Upgrade releases are considered to be upgrades of the same version. Releases 6.0, 6.0U1, etc., are the same version.

- The following table shows what version you can upgrade to, based on the **current version** running at the site:

Current Version:	Can Upgrade to:
6.0, 6.0Ux	6.5Ux
6.5, 6.5Ux	7.0Ux
7.0, 7.0Ux	7.5Ux

- You do **not** need to move workloads during an upgrade.
- When upgrading a protected vSphere or Hyper-V environment, after the upgrade, a bitmap sync is performed for VPGs on the protected VRA.
- In a Hyper-V environment, SCVMM 2016 is supported on Zerto installations from version 6.0x.
- Zerto Cloud Appliance is supported for Azure and AWS (ZCA) on:
  - Windows 2016
  - Windows 2012R2
- A Zerto Virtual Manager can be used with a **different version** on another site, as long as the other version is only **one version** higher or lower.
- You can upgrade from version N to the next version (N+1) of Zerto including to any update within the current version. You cannot do an N+2 upgrade directly.

The following table shows what versions can be used on a **peer** site, based on the version on the **current** site.

Version (N-1)	Current Version (N)	Version (N+1)
5.0, 5.0Ux	5.5, 5.5Ux	6.0, 6.0Ux
5.5, 5.5Ux	6.0, 6.0Ux	6.5, 6.5Ux
6.0, 6.0Ux	6.5, 6.5Ux	7.0

See the following sections:

- Before Upgrading Zerto on page 41
- Upgrading the Current Installation on page 42
- Upgrading Environments Which are Connected to Zerto Cloud Manager on page 42

Before Upgrading Zerto

Before upgrading to a new version, either by installing the new version over the existing version or by uninstalling the existing version and then installing the new version, Zerto recommends doing the following:

- For any peer sites running **Zerto v7.5**, the ZVM to ZVM communication is backwards compatible and will continue to be carried out over port **9081**.
- For any peer sites running Zerto **v8.0Ux**, following the upgrade the ZVM to ZVM communication connection will be made secure and encrypted, and will be carried out over a new HTTPS port, **9071** by default.

  Therefore, **prior to upgrading to Zerto v8.0Ux**, if your site has any peer sites running v8.0Ux, make sure this new port, **9071**, is open for communication between the sites. In addition, make sure the current port used between the sites, **9081** by default, will **remain open** as well for the duration of the upgrade.
- Clear the Microsoft Internet Explorer cache of temporary Internet files. Not clearing the cache of temporary files can result in problems when accessing the Zerto Virtual Manager. In vSphere environments, this would be via the vSphere Client console.
- Make sure that all VPGs are in the state **Protecting**, and not in a sync state, such as Delta Sync, or in an error state, such as Needs Configuration.
- Make sure that the external ZVM SQL server database recovery model is configured to **Simple**.
- Complete any recovery operation before starting the upgrade.
- Create a **backup** of the machine where the Zerto Virtual Manager runs, which you will use if the upgrade fails. Zerto recommends taking a snapshot of the machine after stopping the Zerto Virtual Manager service.
- *(AWS environments only)* Make sure the permission level of the VM running the ZCA is set using **IAM Roles**.

  See Zerto Installation Guide for Amazon Web Services (AWS) Environments, in the section **Setting EC2 Instance Permissions in AWS**.
- *(Azure environments only)* Make sure user assigned Managed Identities on the VM running the ZCA is enabled and the permission level is set to the following:
  - **Owner** or **Contributor**,
  - **Storage Blob Data Contributor**
  - **Storage Queue Data Contributor**

  See Zerto Installation Guide for Microsoft Azure Environments, in the section **Enabling Managed Identities and Setting Mandatory Permissions in Azure**.

> **Note:** The snapshot should only be used to rollback to the pre-upgrade state immediately

> after the upgrade has completed. The snapshot should not be used after the protection of virtual machines has restarted.

The installation procedure checks for an existing installation that is either one version lower than the new version or is the same version. If an installation is found you can upgrade the installation.

Upgrading the Current Installation

The **existing**Virtual Replication Appliances and protected virtual machines, together with all other information, such as checkpoints, journals, sites, and pairing details, are **retained and are available in the upgraded installation**.

The upgrade is performed **without disrupting the protection**, but **no new checkpoints** are written to the journal during the actual upgrade.

This may temporarily cause alerts to be issued, even if only a single site was affected, stating that the journal history and RPO do not meet their specified target settings.

> **Notes:**
>
> - **VRAs** from the **existing** installation are **notautomatically upgraded** when upgrading Zerto.
> - Zerto recommends that you always upgrade the VRAs on your site to the latest version.
> - If a newer version of the installed VRAs exists, you can **continue to use the current VRAs** with the new version of Zerto, **or upgrade** these VRAs from within the Zerto User Interface.

To upgrade the version:

1. Run the Zerto installation executable for your environment.

   The Zerto Replication Installation Wizard is displayed.

2. Select **Upgrade** and click **Next**.

   The upgrade proceeds automatically.

3. Proceed to **completion**.

> **Note:** If the vSphere Client console was open during the upgrade, close it and reopen it.

Upgrading Environments Which are Connected to Zerto Cloud Manager

For environments using the Zerto Cloud Manager:

- Upgrade the Zerto Cloud Manager**before** upgrading the **Zerto Virtual Managers**.

- Zerto Cloud Manager (ZCM) supports Zerto Virtual Manager (ZVM) of N and N-1 versions.

For Example: ZCM of version 7.0 supports ZVM of versions 6.5, 6.0 and their updates.

- Upgrade the Zerto Cloud Manager to be **consistent** with the **latest version** of Zerto run by the **MSP**.
- Upgrade the version of Zerto run by the MSP after the Zerto Cloud Manager, so that they are **never** more than one version separated from each other.

For details about upgrading Zerto Cloud Manager, see *Zerto Cloud Manager Installation Guide*.

> **Note:** Zerto no longer supports vCenter Server vApps. Any VPG protecting a vAPP should be recreated using the virtual machines in the vApp.

Upgrading Multiple Sites Running Different Versions

A Zerto Virtual Manager can be installed on a site running a different version, as long as each version is **only one version higher or lower** than the other.

When you have **multiple sites**, make sure that the version of Zerto Virtual Manager is never more than one version higher or lower than any of the versions running on the **paired sites**.

To upgrade Zerto installed on multiple sites:

1. Upgrade a site whose version is lower than the required version. Start the upgrades with the site whose version is **lowest**.

   Make sure, at all times, that **no site is more or less than one version** higher or lower than any of the **paired sites**.

2. If the VRAs on the site need upgrading, upgrade these VRAs to ensure that they are no less than one version higher or lower than any of the VRAs on any of the paired sites.
3. Repeat the above step for **all sites**.

For Example:

- You have sites running versions 6.0U3, which are paired to a site running 6.5U3.
- You are planning to upgrade to 7.0.
- Upgrade first the 6.0U3 site to a 6.5U3 version, and then both of the sites to 7.0.

Upgrading To More Than One Version Higher

Before upgrading to a new version, make sure that all VPGs are in **Protecting** state and not in a sync state, such as **Delta Sync**, or an error state, such as **Needs Configuration**.

If you need to upgrade **more than one version higher**, do **one** of the following:

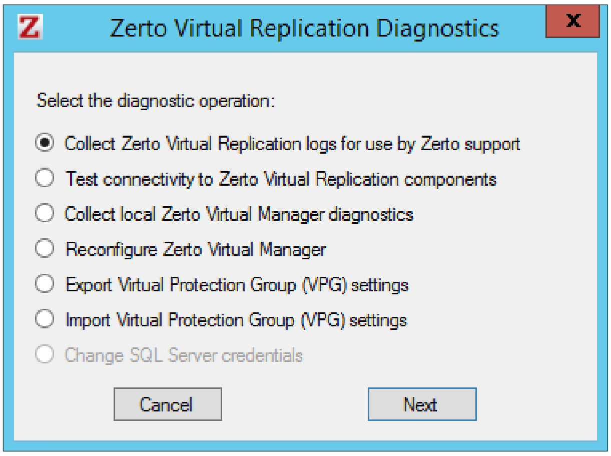
- Upgrade versions stepwise, one version at a time, as described above in **Upgrading Multiple Sites Running Different Versions**, until you reach the required version.
- Use the **Zerto Diagnostics** utility's export option to **export** the existing VPG definitions, then uninstall the old version of Zerto. Install the new version, then use the Zerto Diagnostics utility's **import** option to re-create the VPGs. Use the following procedure.

Upgrading Zerto Using the Zerto Diagnostics Utility

To upgrade Zerto using the Zerto Diagnostics utility:

1. Click **Start** > **Programs** > **Zerto** > **Zerto Diagnostics**.

   The Zerto Diagnostics menu dialog is displayed.



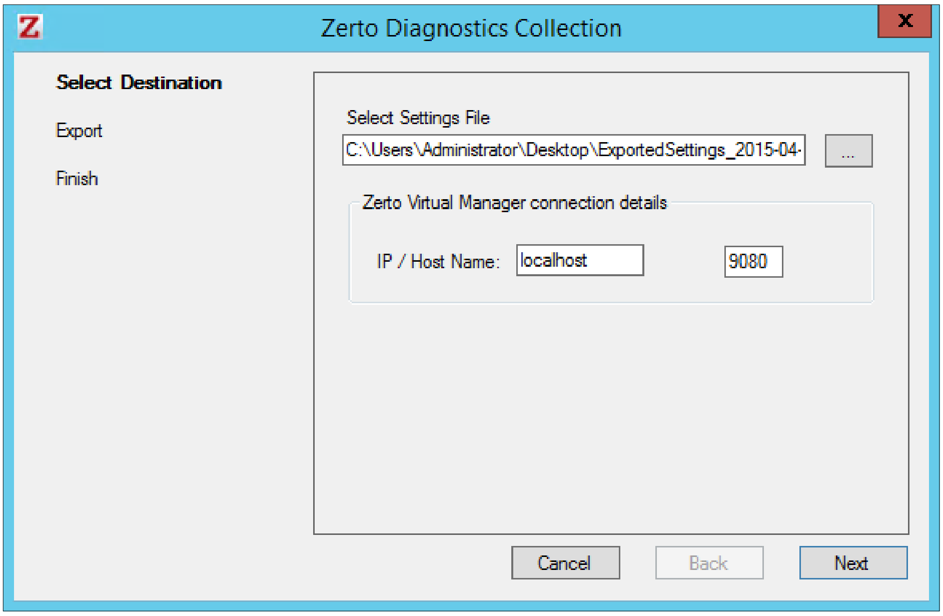
Zerto Virtual Replication Diagnostics

Select the diagnostic operation:

● Collect Zerto Virtual Replication logs for use by Zerto support
○ Test connectivity to Zerto Virtual Replication components
○ Collect local Zerto Virtual Manager diagnostics
○ Reconfigure Zerto Virtual Manager
○ Export Virtual Protection Group (VPG) settings
○ Import Virtual Protection Group (VPG) settings
○ Change SQL Server credentials

2. Select the **Export Virtual Protection Group (VPG)** settings option and click **Next**.

> **Note:** Zerto regularly exports settings to the folder **<Zerto_Installation_Folder>\Zerto Virtual Replication\ExportedSettings**. You can use the last exported file. The default location of ZVR_Installation_Folder is **C:\Program Files\Zerto**.



Zerto Diagnostics Collection

Select Settings File: C:\Users\Administrator\Desktop\ExportedSettings_2015-04-

Zerto Virtual Manager connection details

IP / Host Name: localhost 9080

3. Select the destination for the file that will contain the exported settings and enter the Zerto Virtual Manager IP address and port for the protected site.
4. Click **Next**.

   The list of exported VPGs is displayed.
5. Click **Done**.
6. In the Zerto User Interface delete the VPGs, and keep their target disks.

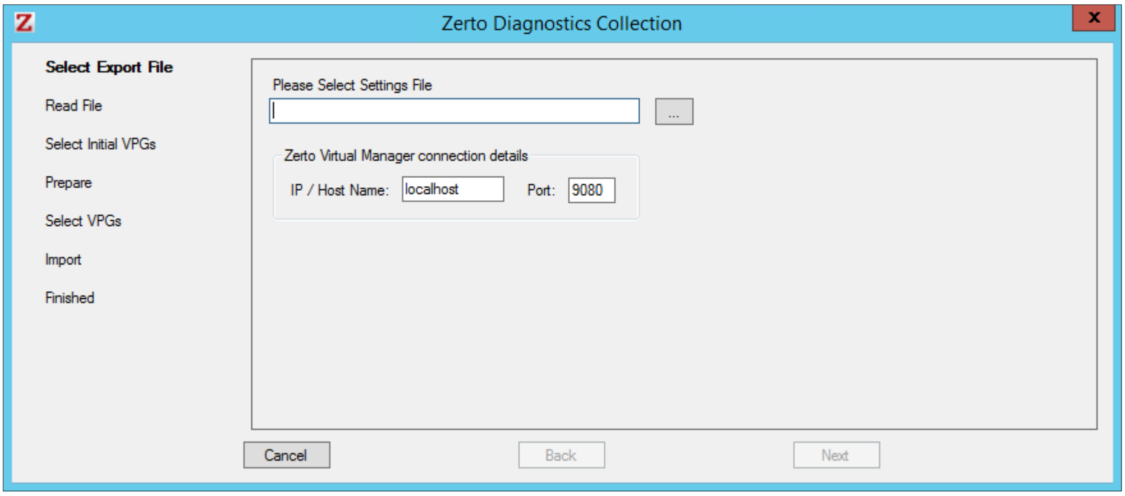
   > **Note:** If you did not export the settings, Zerto regularly exports settings to the folder **<Zerto_Installation_Folder>\ZVR\ExportedSettings**. You can use the last exported file as input to recreate the VPGs to this point in time. The default location of Zerto_Installation_Folder is **C:\Program Files\Zerto**.
7. Uninstall the existing Zerto version.
8. Install the new Zerto version, as described in the *Zerto Installation Guide*.
9. Install the VRAs on the hosts in the site and pair the sites, as described in *Zerto Installation Guide*.

   > **Note:** If the protected site and recovery site are the same for any of the VPGs that were exported, set **Enable replication** to **Self** in the **Advanced Settings** dialog, as described in Zerto Virtual Manager Administration Guide for the VMware vSphere Environment.
10. Click **Start** > **Programs** > **Zerto** > **Zerto Diagnostics**.

    The Zerto Diagnostics menu dialog is displayed.

11. Select **Import Virtual Protection Group (VPG) settings**.

12. Click **Next**.



Please Select Settings File

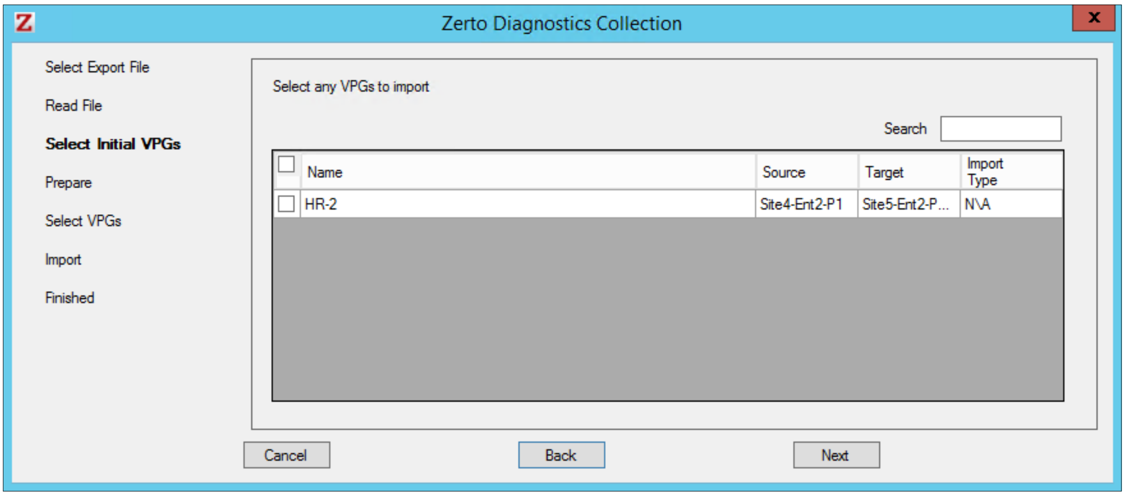
Zerto Virtual Manager connection details

IP / Host Name: localhost Port: 9080

13. Select the file previously exported and enter the Zerto Virtual Manager IP address and port for the protected site.

14. Click **Next**.

    The list of exported VPGs is displayed.



Select any VPGs to import

□	Name	Source	Target	Import Type
□	HR-2	Site4-Ent2-P1	Site5-Ent2-P...	N\A

15. Select the VPGs to import. You cannot import VPGs that have the same name as a VPG that is already defined in current installation. If a VPG in the import file has the same name as an existing VPG, it is disabled and is grayed-out.

16. Click **Next**.

    The list of imported VPGs is displayed. If the VPG cannot not be imported, the reason is specified.

17. Click **Done**.

Upgrading Zerto PowerShell Cmdlets

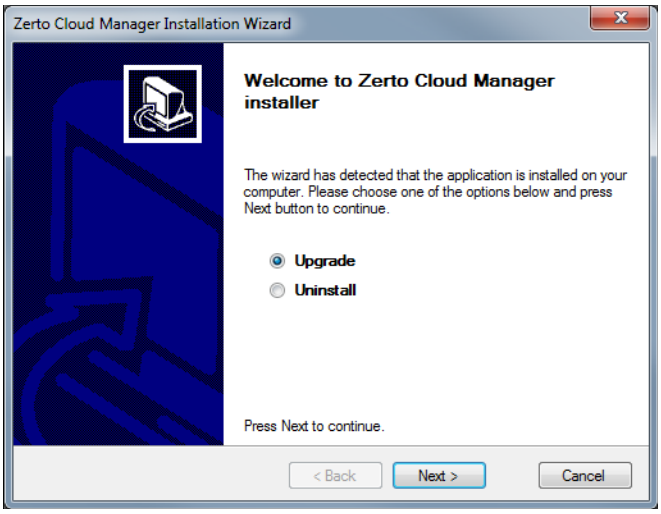
When upgrading Zerto PowerShell cmdlets, make sure that **Windows PowerShell** is **closed** before installing the new version.

Upgrading Zerto Cloud Manager

The Zerto Cloud Manager version must be the same as the Zerto Virtual Manager version.

An upgrade of the Zerto Cloud Manager moves all configuration definitions from the old version to the new version.

The installation checks for an existing installation. If an existing installation is identified, that is one version lower than the new version, you can upgrade or uninstall the existing version.



Welcome to Zerto Cloud Manager installer

The wizard has detected that the application is installed on your computer. Please choose one of the options below and press Next button to continue.

● Upgrade
○ Uninstall

Press Next to continue.

IMPORTANT!

You must upgrade Zerto and Zerto Cloud Managerin **parallel**, making sure that you upgrade the version of Zerto Cloud Manager**before** you upgrade the version of Zerto which is run by the **MSP**.

This is done so that they are never more than one version apart.

To upgrade the version:

1. Run **Zerto Cloud Manager Installer.exe**.

   The Zerto Cloud Manager Installation Wizard is displayed.

2. Select **Upgrade** and click **Next**.

   The upgrade proceeds automatically.

Upgrading Zerto Cloud Connectors

Zerto Cloud Connectors do not require upgrading when a new Zerto version is released.

Zerto enhances the Zerto IT Resilience Platform by converging disaster recovery and backup to deliver continuous availability within a simple, scalable platform. Zerto delivers enhanced analytics, platform improvements and cloud performance upgrades required in the future of IT resilience.

Learn more at Zerto.com.

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