Zerto

Release Notes for Zerto 8.5

Rev01
Nov 2020
ZVR-RN-8.5

ZVR-RN-8.5

Table of Contents

Zerto Release Notes

Zerto is the industry's first solution to converge disaster recovery, backup and cloud mobility into a single, simple, scalable platform. Designed to accelerate IT transformation, the Zerto Platform automates the disaster recovery and backup processes to remove systemic risk to the business, delivers the data protection needs across clouds while maximizing resources and reducing the cost and complexity of multiple solutions.

Based on a foundation of continuous data protection, the platform uses best of breed replication and unique journaling capabilities to deliver the fastest Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO) for both short-term and long-term retention of data. Built-in platform orchestration and automation enables faster management of workloads at scale with minimal touch. Analytics with intelligent dashboards and reports provide complete visibility across multi-site, multi-cloud environments to ensure performance standards are met.

The following topics are described in these Release Notes:

Important:

Cloud Control – Update Manager will not be available to Managed Service Providers (MSPs) to automatically upgrade remote customer Disaster Recovery as a Service (DRaaS) that are connected to the MSPs site(s).

Cloud Control – Upgrade Manager allows MSPs to execute an upgrade of a remote customer's DRaaS site that is connected to the MSPs site(s) on behalf of that customer. When the upgrade is initiated, the customer's local Zerto Virtual Manager (ZVM) is instructed to securely download the recommended version of Zerto and execute the upgrade. **This secure download cannot be performed when the recommended version for the customer's site is any of the following versions of Zerto: 7.0U3p1, 7.5U4p1, 8.0U3, 8.0U3p1, 8.0U4, 8.5**.

When MSPs access Cloud Control – Upgrade Manage and the recommended version is any of the above, the entry for that site will be greyed out and the following message is displayed in a tooltip next to the recommended version: "Unfortunately remote upgrade is not available for this recommended version - In order to keep using Upgrade Manager in the future, you must manually install the current recommended version on the customer site."

Due to this issue, the MSP must manually work with their customers to upgrade the currently installed version at the customer's site(s) to the recommended version of Zerto.

In case one of the above versions is installed on customer site, the Upgrade Manager will support any future upgrade.

Zerto recommends providers work with their customers to perform the following:

- Record the recommended version provided by Zerto via Cloud Control – Upgrade Manager.
- Contact and work with the customer to manually upgrade their site(s) to the recommended version.

End-of-Version Support Notice

To review the Zerto end-of-version support policies, see the document Product Version Lifecycle Matrix.

Prerequisites, Requirements and Installation Instructions

- Before installing Zerto, click to open and review **prerequisites** and **requirements** of the relevant platform:

VMware vSphere environments	Microsoft Hyper-V environments
Microsoft Azure environments	Amazon Web Services (AWS) environments
Cloud Service Providers (CSPs)	

- For **installation** instructions, click to open and review the installation guide:

VMware vSphere and Microsoft Hyper-V environments	Microsoft Azure environments
Amazon Web Services (AWS) environments	Zerto Cloud Manager Installation Guide

Upgrading Zerto and/or Zerto Cloud Manager

To review the upgrading guidelines and instructions, see Upgrading the Zerto Virtual Replication Environment.

Important: Starting with Zerto 8.5, new installations require a ZCM for RBAC to authorize users for roles and permissions.
If you use vCenter RBAC and install a new site, contact Zerto support to enable vCenter RBAC on those sites.
Customers who are using vCenter for Role-based Access (RBAC) and upgrade their environment are not affected by this change.

Important: Prior to ZCA installation/upgrade on AWS, the permission level of the VM running the ZCA must be set using IAM Roles. For further details, see Zerto - Prerequisites & Requirements for Amazon Web Services (AWS), in the section **Minimum Required AWS Permissions**.

Important: Prior to installing Zerto 8.5 ZCA installation/upgrade on Azure, you need to set up a Managed Identity.
For further details, see Zerto Installation Guide Microsoft Azure Environment > Installing the Zerto Solution, in the section **Enabling Managed Identities and Setting Mandatory Permissions in Azure**.

Important:

Before upgrading, it is important to follow the sizing guidelines. **Failure to follow the sizing guidelines can result in performance degradation and possible software errors.**

Additionally, if either the production or recovery sites are protecting **over 1000 VMs**, Zerto recommends the ZVM be configured with at least 32GB memory and at least 12 CPUs prior to installing Zerto 8.5. These ZVM requirements will ensure the new features in Zerto 8.5 release will have enough memory and CPU resources to operate properly.

For more information, click to review:

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

What's New & Resolved - Zerto 8.5

What's New in Zerto 8.5

Zerto 8.5 includes the following new features and functionalities:

Data Protection - Local Continuous Backup and Long-term Retention

Local Continuous Backup

Instant Restore of Files and Folders to Production

Instantly restore files and folders directly back into the source VM in production. This enhanced restore experience allows for the restoration of files and folders from the journal directly back into the source VM. These files and folders will inherit their original permissions once restored. This capability removes the need to download and manually restore these files and folders into the production VM.

Journal File Level Restore - Roles and Permissions

Introducing a new File Level Restore Operator role. This new role exists within Zerto's current Role-based Access (RBAC) functionality.

Long-Term Retention

Azure Blob Storage and Amazon AWS S3 Repository Support

Utilizing native cloud object storage for Long-term Retention offers cost savings and simplicity. Zerto 8.5 offers native Long-term Retention to public cloud repositories with both Microsoft Azure Blob Storage Hot and Cool tiers and Amazon S3 Standard, S3 Standard-IA, Standard One Zone-IA storage without the use of any gateway appliances. These new native cloud targets, along with built-in data compression from the source, enables public cloud storage as a scalable, cost-effective Long-term Retention target. Long-term Retention to Microsoft Azure and AWS has the following capabilities and benefits:

- Compression to reduce costs.
- Restore a VM back on premise.
- Native write without a gateway appliance.
- In-flight encryption via HTTPS.
- Scalable architecture to allow parallel operations to cloud storage.
- Supported in all available Azure and AWS regions.

Storage Compression for Long-term Retention

Delivering three levels of compression (low, medium, and high) to reduce cost and increase network and storage efficiency for Long-term Retention for both on-premise and cloud Long-term Retention Repositories. Data is stored as compressed and is decompressed upon Restore.

Ad-hoc Retention Sets Deletion from Long-term Repository

Now you can manually delete undesired Retention Sets and/or Retention Sets chains, out-of-policy, from the Long-term Repository. This includes an audit log trail.

Public Cloud

Support for VMware on Public Cloud on page 11

Support for Google Cloud VMware Engine on page 11

Support for the Oracle VMware Solution on page 11

Support for the Azure VMware Solution on page 11

Enhanced Security and Permissions on page 11

Enhanced Configuration and Settings for Azure on page 12

Updated the Linux AMI Version used as Workers (zImporters, ZASA, ZSAT) to Amazon Linux 2 on page 12

Support for VMware on Public Cloud

VMware on public cloud offers hardware for compute, storage and networking running VMware's Cloud Provider Stack, which consists of vSphere, vSAN, and NSX-T.

The provider offers cloud-style provisioning of the servers and VMware Cloud Provider Stack as a monthly service to their end customers. The servers and VMware Cloud Provider Stack are delivered as a dedicated, private cloud to each end customer. The provider manages the servers and the VMware Cloud Provider Stack across multiple regional data centers for all their customers. The provider's environment is built for scaling to 1000s of customers with each customer having a dedicated private cloud consisting of a vCenter with multiple ESXi hosts.

Zerto's lifecycle management features enable customers to protect workloads on-prem or in the Cloud with familiar VMware features and ecosystem. Using VMware on Public Cloud provides cost savings for recovery sites due to the provider managing the VMware infrastructure of the recovery site. VMware on Public Cloud also enables world-wide deployment of recovery sites and easy access to additional Public Cloud services such as analytics, storage resources and cloud-based applications.

Support for Google Cloud VMware Engine

VMware Engine is built on Google Cloud's highly performant, scalable infrastructure with fully redundant and dedicated 100Gbps networking, providing 99.99% availability to meet the needs of the most demanding enterprise workloads. Customers can benefit from full access to Google Cloud services. Learn more here.

Support for the Oracle VMware Solution

Oracle Cloud VMware Solution provides a customer managed, native VMware-based cloud environment, installed within a customer's tenancy. It offers complete control using familiar VMware tools. Move or extend VMware-based workloads to the cloud without rearchitecting applications or retooling operations. Learn more here.

Support for the Azure VMware Solution

Seamlessly move VMware-based workloads from on-prem datacenters to Azure and integrate VMware environments with Azure. Manage existing environments with the same VMware tools used on-prem while modernizing applications with Azure native services. Azure VMware Solution is a Microsoft service, verified by VMware, that runs on Azure infrastructure. Learn more here.

Enhanced Security and Permissions

Zerto consistently improves our security capabilities with each new release. Along with adding encryption in-flight between the on-premise VRA and the ZCA (Azure or AWS), we reduced the permission level and permissions needed to install and operate the Zerto Cloud Appliance in Azure.

Enhanced Configuration and Settings for Azure

The secure and streamlined nature of Linux, along with the vast number of Linux distributions and versions, makes Linux more of a challenge to re-platform when compared to Windows machines. Zerto adds Linux virtual machine tools for Azure to ease the configuration of the Linux machines moving to Azure from on-premises. With these tools and in some cases, interactive configuration steps, you can confidently move Azure-supported Linux distributions to Azure with Zerto.

Updated the Linux AMI Version used as Workers (zImporters, ZASA, ZSAT) to Amazon Linux 2

Zerto is now using the latest Amazon Linux 2 for all its workers including zImporter, ZASA, ZSAT. Using Amazon Linux 2 led to significant performance improvements (up to 30% in some cases).

Platform

Auto Evacuate for Recovery Hosts

Auto Evacuate for recovery hosts provides continuation of replication workloads whenever an ESXi host or hosts are put into maintenance mode from vCenter. Zerto detects when an ESXi recovery host has

entered maintenance mode and automatically transfers recovery volumes to other VRAs within the recovery host cluster.

VRA Auto Populate for Recovery Hosts

With VRA Auto Populate, Zerto automatically re-populates VRAs with recovery disks after one or more vCenter hosts exit maintenance mode.

Auto VRA Install

The Auto VRA Install feature enables customers to align their clustered hosts with VRAs automatically by installing a VRA upon host addition to a cluster.

Auto VRA Uninstall

Auto VRA Install supports the procedure of ESXi retirement by automatically removing a VRA if its host was removed from inventory.

VRA to VRA Encryption

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

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

Considerations:

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

  This is only likely to be noticed:

  - During a large Initial Sync between the sites.
  - In environments where the Network and Storage support large throughputs, where the CPU might become a bottleneck.
- Enabling encryption might also affect your VRAs compression ratio.

> ☑ **Tip:** To reduce the encryption impact on performance, Zerto recommends you add a second vCPU to each VRA.

Support for SQL High Availability

Zerto 8.5 supports communication with an external ZVM database configured with SQL High Availability. Database administrators can now use the SQL "full" recovery model to keep track of transactional logging to see points in time where the external ZVM database can be restored.

VRA Cluster Workload Automation

VRA Cluster Workload Automation allows administrators to configure host cluster level settings in Zerto. Once configured, Zerto will automatically install VRAs on any new hosts added to the cluster. Cluster level settings include the following settings to be used by the VRAs on installation: number of vCPUs, amount of vRAM, IP to be used from the provided IP pool, datastore for installation.

VRA Cluster Management

Starting with Zerto 8.5, customers are able to install, upgrade and uninstall VRAs on an entire cluster instead of separate ESXis.

VRA CPU Configuration

Zerto Administrators can set the number of vCPUs for VRAs during the VRA installation and upgrade, the setting is also available for the predefined VRA settings for a cluster.

Expand GUI Windows

ZVM and ZCA GUI windows have been expanded to provide enhanced information visibility without the need to manually resize Zerto windows.

VPG Description

Users can now include a brief description about what applications are being protected within a VPG without having to rely solely on VPG naming conventions.

Enhanced Journal Granularity

Zerto Administrators can set the specific number of hours for their VPG's journal history setting up to 72 hours. This provides a more granular setting for the journal to help users conserve storage and have a more finite view for checkpoint selection.

vSphere Tag Preservation

The vSphere tag preservation feature enables the customer to preserve protected VM vSphere tags upon recovery.

Zerto PowerShell Cmdlets Module

The Zerto PowerShell cmdlets module is an additional component of the PowerShell toolset provided to our users to assist with automation. This module greatly expands the capabilities available to administrators and is built off the Zerto REST API on the Zerto Virtual Manager. The module is provided in addition to the existing PowerShell snap-in and is installed from Microsoft's PowerShell Gallery. It allows users to perform actions via PowerShell or PowerShell scripts they write, such as the following:

- Establish a session with a ZVM for the available cmdlets in this module.
- Perform VPG operations such as creating a new VPG, editing an existing VPG, running a Live Failover operation, running a Move operation, and running a Clone operation.
- Install, edit, or uninstall a VRA.
- Query report data from the resources and recovery reports.
- Query Alert and Events data from the alerts and events available in the ZVM.

VSS

The Zerto VSS Agent can now also be installed in silent mode (unattended) using the command line.

ZVM CPU Improvements

For environments of over 1000 VMs, Zerto lowered the recommended minimum CPU resources required for ZVM configuration to 12 CPUs.

Managed Service Providers (MSP)

Tenant UI Integration

The Tenant UI Integration feature enables MSPs to seamlessly provide Zerto's self-service portal through vCD tenant UI.

Resolved Issues in Zerto 8.5

vCenter - resolved issues on page 16

Hyper-V - resolved issues on page 17

Azure - resolved issues on page 17

General - resolved issues on page 17

vCenter - resolved issues

Case Number	Issues Resolved in 8.5
162013, 163879	Resolved an issue where /v1/volumes API call returned "400 Bad Request" if a commit operation was in progress.
166287	Resolved an issue in which the VM BIOS UUID was not copied from the Protected VM to the test Recovery VM even when the user enabled the "For incoming replication, copy the BIOS UUID of the protected VM to the recovered VM" site setting.
138319, 151389	Resolved an issue which caused ESXI hosts to crash when Fault Tolerance was enabled.
149905,151207	Resolved an issue which caused environment metadata collection to fail when entity names contained non-Latin characters.
140468, 155550, 156557	Resolved a tooltip display issue in which sometimes the tooltip in the VPG Sites tab falsely indicated that VMs were removed from the inventory.
162561, 162242, 165981	Removed an unnecessary validation on the protected host, which caused the evacuate host operation to fail in some scenarios.
157836	Resolved an issue which caused the Change VM Recovery VRA operation to fail due to timeout on some VMs.
162385, 162433, 162145, 162194, 162625, 162593	(vCenter to Azure replication) Resolved an issue occurring after upgrading which caused an increase in the VPG RPO.
142339, 142509	Resolved an issue which sometimes caused VPGs to appear stuck in sync and subsequently lose journal history.
163573, 168604, 168761	Resolved an issue which caused unusual entries in the vCenter ESXI host Vmkernel log.
156214	Zerto now preserves the order and location of the SCSI controller disks when failing from non-VMware environments back to VMware environments.

Hyper-V - resolved issues

Case Number	Issues Resolved in 8.5
124691, 127917, 127224, 121382, 151892	Resolved an issue that caused large environments in Hyper-V to show as disconnected after ZVM restart.

Azure - resolved issues

Case Number	Issues Resolved in 8.5
148727, 148973	Resolved an issue in which recreate VPG failed after the ZCA IP had changed.
159203	RecoveryDiskType per VM now inherits its values from the VPG settings when creating or updating a VPG over API.
162227	Resolved an issue which caused recovery operations to fail under particular networking configurations where there were VNets without subnets configured.

General - resolved issues

Case Number	Issues Resolved in 8.5
161475	Resolved an issue which caused the upgrade operation to fail when peer sites had the same name.
	Fixed a third party UI package (jQuery v2.2.4) and secured it, as it was found to be vulnerable to Prototype Pollution attacks.
99068	Resolved an issue which sometimes caused the VPG sync process to progress slowly.
153084	Added HTTP headers to all static pages to prevent the ZVM from being exposed to clickjacking.
150744	Resolved an issue in which on disconnected sites, VPGs were incorrectly reported as Meeting SLA.

Case Number	Issues Resolved in 8.5
160947, 160574, 160520, 160389, 158805, 163032, 163252, 164253, 164266	Resolved an issue where installing or upgrading to version 8.0uX failed when Zerto was not installed in the default location.
148024	Resolved an issue which caused the update process to fail the VRAs upgrade on VSAN datastores.

Zerto Analytics

Insight-driven data analytics for a new era of data protection

As IT infrastructures become more complex and demands for performance rise, companies require visibility and control over protected IT environments. Visibility of your entire IT infrastructure (both on-premises or cloud) is imperative to monitor, analyze and plan your environment and resource requirements to ensure zero interruptions. To have confidence that business Service level Agreements (SLAs) are met, you need not only visibility and insights to address existing issues, but also to be able to plan for your future data protection needs.

Zerto Analytics delivers these capabilities through a single interface and one user experience for a comprehensive overview of your entire multi-site, multi-cloud environment. Utilizing metrics such as average recovery point objective (RPO), network performance, and storage consumption, Zerto Analytics delivers real-time and historical insights on the health and protection status of your applications and data. Through Intelligent dashboards you can spot trends, identify anomalies, and troubleshoot issues in network, RPO, and other business SLAs. With these insights, you can eliminate inefficiencies and allocate resources effectively to mitigate data loss, reduce downtime and take control of your data.

See also:

Before Getting Started with Zerto Analytics on page 19

Accessing the Zerto Analytics Portal on page 19

Zerto Analytics APIs on page 20

Zerto Analytics Product Feature Matrix on page 20

Before Getting Started with Zerto Analytics

Verify the following:

- At least 1 ZVM is running Zerto 5.0 or higher.
- **Enable Support notification and product improvement feedback** checkbox is selected This is accessed in the ZVM application in **Settings > About**.
- Internet access.
- A **myZerto** account using your corporate email address.

Accessing the Zerto Analytics Portal

Zerto Analytics can be accessed from https://analytics.zerto.com, or through https://www.zerto.com/myzerto/ and signing in using your myZerto credentials.

You can also access the Zerto Analytics portal from the **ZVM Application Menu tab**: Click 

to open Zerto Analytics in a new browser tab.

> **TIP:**
>
> Use the **What's New** WHAT'S NEW and **Help** features in Zerto Analytics to learn more about each of the features available in Zerto Analytics.

Zerto Analytics APIs

Zerto Analytics is developed with an API first approach, therefore, everything that is presented in the GUI, is also available with APIs. APIs are available the same version as their GUI counterparts.

Zerto Analytics APIs are available in OpenAPI Specification.

The documentation can be accessed via the link: https://docs.api.zerto.com/

Zerto Analytics Product Feature Matrix

The following table lists the available features and from which ZVM version it's supported.

For further details about new features, access the Zerto Analytics portal and click WHAT'S NEW.

Feature	Zerto 7.0	Zerto 7.5	Zerto 8.0	Comments
Dashboard	✓	✓	✓	
VPG Analytics	✓	✓	✓	
VM Analytics	✓	✓	✓	
Storage Analytics	✓	✓	✓	Available from Zerto v6.5 Update 2
Monitoring: Alerts, Tasks, Events	✓	✓	✓	
Reporting: RPO, Journal, Network	✓	✓	✓	
Planning	✓	✓	✓	Available from Zerto v7.0 Update 1

Feature	Zerto 7.0	Zerto 7.5	Zerto 8.0	Comments
ZORG Filter (MSP end user)	✓	✓	✓	Not available for Storage tab
90 Days History	✓	✓	✓	ECE and Cloud licenses Standard 30-day
REST API	✓	✓	✓	

Known Issues

The following are known issues when using Zerto:

Virtual Replication Appliance (VRA)

- You have to wait a few minutes after moving a protected virtual machine to another host before you can forcibly uninstall the VRA ghost on the original host.
- If the VRA IP is allocated via DHCP and the DHCP server at a later date allocates a different IP, the VRA does not change the IP. For this reason it is recommended during production to only use static IPs and use static IPs or DHCP during trials.

- A VRA installed on a host, that is part of a cluster without DRS enabled, will not have affinity rules to that host, and will therefore be migrated off the host once the host enters maintenance mode, and with the condition that the option "migrate vms off the host" in the maintenance mode wizard is selected.

Virtual Protection Group (VPG) and Recovery

- For linux distributions, DNS settings are global, per virtual machine.
- Attempting to create a VPG when the target datastore is unavailable fails.

  Workaround: Try again after the datastore is up.
- Virtual machines with SATA controllers cannot be included in a VPG.
- Exported settings do not populate network settings in the CSV file going into Public Cloud.

VPG Management

- If a VM is removed from the hypervisor inventory, Zerto stops the replication. When adding back this VM to the inventory the ZVR resumes the replication. In Hyper-V environments only, adding back the VM does not resume the replication.
- When the protected site is vCD, initiating "Copy VPG Settings" from the Recovery site is currently not supported.

Failover, Move and Test Failovers

- After stopping a failover test, the checkpoint that was used for the test has the following tag added to identify the test: **Tested at startDateAndTimeOfTest(OriginalCheckpoint_DateAndTime)**. The **Tested at startDateAndTimeOfTest** value is taken from the Zerto Virtual Manager and not from the UI.
- Recovering a VPG using one of the very earliest checkpoints available can fail when the checkpoint specified is moved out of the journal before the recovery operation can commit.
- After a recovery operation, the field **bios.bootOrder** is not passed to the recovered VM. In some cases, not passing the field **bios.bootOrder** can lead to the wrong boot order in the recovered VM.

vCenter Server

- The maximum number of supported volumes protected per site is 32,000.
- In some cases, after updating Zerto software, and after vCenter DB reinitialization, Zerto may not be able to identify some of its entities automatically, due to vCenter MoRef changes.
- When an ESX/ESXi host is disconnected from the vCenter Server but the network connection is still available, the status of any VPG recovering to this host and the status of the VRA on the host are displayed as OK in the Zerto user interface. However, all recovery operations will fail.

- Due to a VMware problem, configuring IPs for the recovery machines is lost when cloning virtual machines with VMXNET3 NIC on Windows 2008 R2 machines. For details and solutions, see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1020078.
- VMware does not identify the IP origin for Linux virtual machines and therefore Zerto cannot know whether it is static or DHCP.
- The boot order defined for a vApp is not reproduced for a cloned vApp.
- Increasing the size of an RDM disk is not reflected in the VPG, nor by the recovery VMDK.

  Workaround: Follow the VMware KB: http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1007021.
- After hibernating a laptop running vSphere Client console, you have to restart the console to reload the Zerto GUI.
- Zerto is not localized. VMware issues alarms where the language is not English with XXX.

  Workaround: Start up the vSphere Client console adding the following argument: -locale en_US, to display all Zerto alerts in English.
- If a host is removed from a site, a ghost VRA is created which you can remove. After the host is added back to the site, a ghost virtual machine is displayed in the vCenter hierarchy.

  Workaround: Remove the ghost virtual machine from the inventory.

VMware Cloud Director

- Re-IP is not supported in Zerto versions 7.5Ux and 8.0Ux, when going from Public Cloud to VCD.
- After updating a VPG, for example by adding a new virtual machine to it, and then immediately moving it or failing it over to vCD, causes the vCD reflection to be out of date and recovery virtual machines are not powered on, resulting in the promotion hanging.

  Workaround: Wait a few minutes between changing the VPG and performing the move or failover operation. If you do not wait, manually power on all recovery virtual machines that are not powered on automatically.
- Recovering a VPG to vCD will fail if the vApp name contains any of the following special characters: ! * ' ( ) ; : @ & = + $, / ? % # [ ].
- When both the recovery site is vCD, if NICs are added to a virtual machine that is included in a VPG and then the VPG is recovered, with reverse protection defined, the VPG for failback needs configuration, but the Zerto User Interface does not enable this configuration.

  Workaround: When adding NICs to a virtual machine that is included in a VPG, edit the VPG to add these NICs to the VPG definition, before performing a recovery operation with reverse protection.

- Storage Policy configuration for VPGs:
  - Preseeding: Browsing the location of the preseeded disk will show only datastores which belong to the VM Storage Policy, and not all Storage Policies in the orgvDC.
  - Zerto does not maintain the Storage Policy per volume of protected VMs upon reverse protection when replicating between vCD<>vCD - the volumes will be aggregated to the VM Storage Policy.

VMware vSphere

- vSphere Web (FLEX) Client 6.7 is not supported.
- Zerto does not support enabling **VMkernel.Boot.execInstalledOnly** on ESXi advanced system settings.
- Datastores which are used by Zerto must not contain special characters in their names.

Hyper-V

- The maximum number of supported volumes protected per site is 4,000.
- Changing the storage used by a VRA from a CSV to non-CSV storage, or from a non-CSV storage to CSV storage, fails.
- You cannot protect virtual machines using storage that is only configured in Hyper-V and not in SCVMM.
- Virtual machines with fixed size disks are always recovered with dynamically expanding disks.
- SCVMM is not automatically refreshed after any recovery operations to or from the SCVMM. This can result in Integration Services not being detected by the Zerto Virtual Manager and this can lead to virtual machines failing to boot and Integration Services functions such as re-IP not working.

  Workaround: Manually refresh the virtual machine in SCVMM.
- All management operations that can be executed from SCVMM, must be executed from SCVMM and not from the Hyper-V host. For example, removing a virtual machine must be done from the SCVMM console and not from the Hyper-V console.
- When Hyper-V Replica is used on a virtual machine protected in a VPG, removing the virtual machine from the VPG is not reflected in the user interface.

  Workaround: Re-edit the VPG to remove the virtual machine and click **DONE**.
- A VRA cannot be installed on a Hyper-V host when the host is attached to a LUN via iSCSI along with other Hyper-V hosts.
- Recovery or replication of Hyper-V virtual machines with shared disks does not work.
- If you mark a disk as shared after the virtual machine to which it is attached is already in a VPG, the virtual machine must be refreshed in the SCVMM console immediately, otherwise the VPG enters an

error state. Then, remove that virtual machine from the VPG since a virtual machine with a shared disk cannot be recovered or replicated by Zerto.

- When a protected Windows VM configured for DHCP is failed over with re-IP set to DHCP, a failed SCVMM job will appear in the SCVMM console.

AWS

- When protecting to AWS, Zerto does not support the following special characters in the VM name: %, {, }, /, \, “, <, >.
- When protecting to AWS, Zerto does not support VMs whose names contain multibyte characters: Traditional Chinese, Simple Chinese, French, Japanese, Spanish, Portuguese, Hindi, Arabic.
- Tagged checkpoints, Force Sync, One-to-Many and Long-term Retention functionalities for VPGs with AWS as the protected site are not supported.
- Preseed to AWS is not supported.
- Restore from retention sets is not supported for VPGs with AWS as their recovery site.
- When using zImport, the disk type is io1 and cannot be configured.
- VMs with EBS volumes using Key Management Service (KMS) to encrypt data cannot be protected.
- The default account limit of the number of c4.8xlarge AWS EC2 instances that can be deployed is 20. To ensure scalability, contact AWS support to request a limit increase.
- The default account limit of the number of m4.large AWS EC2 instances that can be deployed is 20. These instances are used for zSATs and zASAs. To ensure scalability, contact AWS support to request a limit increase.
- GPT cannot be used as the boot disk.
- FOL to AWS fails when the VPG definition contains an invalid entity such as a security group, subnet, VPC or instance type. An invalid entity might be an entity that was removed from the AWS platform.
- AWS rounds up all volumes to the closest 1GB. When failing over/ moving to AWS, with reverse protection, if the VM is with disks that are not a round number of 1GB, the VPG goes into a **Needs Configuration** state after being recovered to AWS. This is due to a volume size mismatch between the protected and recovered sites. After recovery, the user needs to delete this VPG and recreate it, initiating "initial sync".
- Native VMs launched with AWS Marketplace cannot be protected.
- VMs launched through the Community AMIs may be protected depending on the drivers they contain. To find out if these VMs can be protected, Zerto recommends performing a failover test. If the failover test succeeds, then the required drivers are installed and the VMs can be protected.
- Site pairing and replication between AWS sites (AWS to AWS) is currently **not** supported.

Azure

The following limitations apply:

- In some scenarios, when failing out of Azure with reverse protection, or moving the VPG out of Azure and deleting the source VMs, updating the VPG will fail, leaving it in a state of Needs Configuration.

  Editing the VPG without changing anything and then saving again, should solve the problem.

- In environments where the protected site is a VCenter with Zerto v7.5 and the recovery site is Azure with Zerto v8.0, after Failover with reverse protection, the user must use the ZVM on the VCenter site to view, edit or copy settings from the VPG.

- When the recovery site is a Public Cloud with Zerto v7.5Ux, and the protected site is vCenter with Zerto v8.0Ux, after failover with reverse protection, the VPG might become unusable if the sites are unable to sync and will display a disconnection error to the user.

- Zerto's RTO when going to Azure is dependant on the ability to deploy scale-set instances based on a Zerto image in the Market Place. If the subscription does not allow the use of images from the Market Place, contact Zerto Support to work with a different image.

- When failing back to vSphere from Azure, the storage controller drive order is not preserved.

- Usage of General purpose V2 storage accounts (GPv2) is not supported because I/O transaction costs for V2 are substantially higher than V1 storage accounts.

- Although VMs will be recovered to Managed disks (Unmanaged is not supported), VMs will continue to be protected to Unmanaged disks in the storage account defined during ZCA installation.

- Zerto allows protection of VMs up to 8TB. However, there is a 1MB header file that Zerto needs to write to recovered disks. Meaning, that in reality the maximum supported disk size is 1MB less than 8TB. The consequence of this is that you will have a seemingly healthy VPG, but it will be unable to recover. On-prem disks that are 8TB in size must be decreased by 1MB before they are protected to Azure.

  If a failover of a disk with 8TB was already performed, please contact Zerto Support to avoid an initial sync.

- Self replication within a ZCA is not supported.

- Although two ZCAs can share storage accounts (either paired to each other, or each paired to a different site), this is not supported as ZCAs which point to the same storage account are not aware of each other.

- Preseed is not available in Edit or Create VPG flows.

- Disks saved when deleting a VPG or un-pairing sites cannot be used for preseeding in Edit/Create a VPG.

- VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.

- Zerto does not support Role Based Access Control for Active Directory to access the ZCA.

- The protected virtual machines needs to have at least one NIC.
- Azure rounds up all volumes to the closest 1MB. When failing over/ moving to Azure, with reverse protection, if the VM is with disks that are not a round number of 1GB, the VPG goes into a **Needs Configuration** state after being recovered to Azure. This is due to a volume size mismatch between the protected and recovered sites. After recovery, the user needs to delete this VPG and recreate it, initiating "initial sync".
- The supported number of data disks per virtual machine is dependent on the selected instance size. For example, instance size D3_v2 allows up to eight data disks per virtual machine.
- Restore from retention sets is not supported.
- When a VM is recovered to Azure, a temporary drive is automatically created in the drive letter, following the operating system drive. Due to this temp drive, the drives you had set up in your production site may be shifted when recovered to Azure (other than the OS drive) (Azure limitation).
- Use Move operation in order to failback from Azure.
- The minimum RPO from Azure is 1 minute.
- Long-term Retention is not supported for "From Azure" VPGs.
- Reverse protection VM network settings in a VPG are not saved when failing over a VPG from Azure.
- Tag checkpoints, Clone: These operations are not supported for VPGs which have protected VMs in Azure with multiple disks attached.
- For additional limitations, see Azure subscription and service limits, quotas and constraints: https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits.
- After a restart of the ZCA, or a restart of the ZVM service or VRA service on the ZCA, before attempting any of the following, wait for 15 minutes once the ZCA has restarted, or after the ZVM or VRA service on the ZCA is restarted:
  - test failover
  - live failover
  - move operation

Cross-Replication

- When replicating out of Zerto v8.0 Public Cloud (AWS/Azure) to a Hypervisor (VC/vCD/Hyper-V) with Zerto v7.5Ux and below, users will experience an error if their sites disconnect during Failover live. The Failover will succeed, but when the sites reconnect, editing the VPG will fail with a "Communication Problem" error. The user will have to recreate the VPG in order to apply reverse protection.
- NIC configuration in the VPG definition is not applied.

- Recovery of a virtual machine from Hyper-V to vSphere of a generation 1 virtual machine with more than one SCSI controller, fails.
- Under certain conditions, when the declared OS definition does not match the actual installed OS, recovery operations may not work. To prevent this situation, ensure that the declared and installed OS definitions match. If the two definitions cannot match, use the hypervisor guidelines of the protected virtual machine or contact Zerto support.
- You cannot install VMTools on a Hyper-V VM. VMTools on a Hyper-V VM are needed for re-IP to work.

VMware to Hyper-V Cross-Replication

- When protecting from VMware to Hyper-V, the protected volumes must be multiples of 1MB. If you resize a VMDK, the resize must be a multiple of 1GB.
- In VMware, a virtual machine with a guest operating system booting from UEFI firmware can only be protected by Zerto if the guest OS is supported by Hyper-V VM Generation 2.
- SUSE and CentOS Linux machines in VMware cannot be recovered to Hyper-V.
- Recovering a VPG to Hyper-V from vSphere will fail if the name contains any of the following special characters: ! * ' ( ) ; : @ & = + $, / ? % # [ ].

Hyper-V to VMware Cross-Replication

- CentOS 7.3 Linux machines in Hyper-V cannot be recovered to VMware.
- When recovering from Hyper-V to VMware, the virtual machines are recovered with the same number of sockets as CPUs and not the original number of 19035.
- When protecting Windows 2012 R2 virtual machines from Hyper-V to VMware, after a failover test you may need to re-activate the virtual machine.
- Windows XP virtual machines cannot be protected from Hyper-V to VMware.

Remote Upgrade for Cloud Service Providers

- Upgrade of service provider ZVM sites is not supported; only customer DRaaS sites paired to a service provider ZCC are eligible for upgrade.
- Remote upgrade functionality assumes that both the Cloud Service Providers version and the customers Zerto version is v6.0 or above, or v5.5U4.
- VSS installers are not supported. From Zerto v7.5U1 and below remote Upgrade should be used to download only non-VSS versions.

APIs

- Support of VPG Settings APIs when Creating VPGS from vCD to vCD:
  - vCD > VC is not supported.
  - No validations are performed on the inputs provided.
- Invalid Argument Validations:
  - Previously created REST API calls may fail if invalid arguments were used.
- VRA Bulk Upgrade:
  - The upgrade of VRAs provided will halt if one of the VRAs fails to upgrade.
- Copy VPG Settings API:
  - When using the Copy VPG Settings API, Long-term Retention settings cannot be applied to the copied VPG.
- From Zerto v8.5, API help is available only through the PDF or Online Help and is no longer available using /help on the API endpoint (e.g, https://<IP>:9669/v1/flrs/help/ will not work).

File and Folder Level Recovery

- You can only recover files or folders when Long-term Retention is not running.
- You cannot recover files or folders from a virtual machine when a test failover, live failover, move, clone, or retention process is being performed on a VPG that contains the virtual machine.
- You cannot recover files or folders from the Zerto plugin.
- Journal File Level Restore (JFLR) is not supported with the vSphere plugin.
- The Journal File Level Restore workflow is not accessible in the ZSSP.
- File Level Restore (JFLR) cannot be performed on volumes where data de-duplication is enabled on the operating system level.
- **Linux file systems only**: Downloading files larger than 1.5GB is not recommended and may take a long time.
- Zerto will not download files from Linux file systems, when the file name contains the following special characters:

  \ / : * ? " < > |
- When recovering files/folders from Zerto 7.0 to 7.5, the Ide 0:0 disk indication appears as the root folder during browse and as the mounted disk regardless of the selected disk. This does not affect the files/folders selected for mounting.
- **Downloading Files/Folder from Search and Restore**

- The Search and Restore wizard does not filter unsupported files. If an unsupported file is selected for download from Search, a mount session will be executed but the download will fail.
- The user must unmount the VM manually.

- **Search and Restore**
  - Saving indexed meta-data is currently only supported on SMB Repositories which are not PBBA based.
  - When configuring SMB repositories used for indexing, do not use a local user account.
  - Operating Systems, File Systems and Volume Manager that Zerto can index:
    - Operating Systems: Windows Vista and 2008 server and above and Linux
    - File System and Volume Manager: NTFS and EXT2/EXT3/EXT4
    - LVM is not supported for indexing
  - A VM with over 100 million entries (files or folders) cannot be indexed.
  - Rate of entries (files or folders) indexed in NTFS per second: 2000 files.
  - Rate of entries (files or folders) indexed in EXT per second: 1500 files.
  - Supported partitioning methods: GPT, MBR.
  - Zerto can index up to 3 VMs in parallel and no more than one per recovery host.
  - Search and Restore is available only from a recovery ZVM GUI.
  - While indexing, only a Failover operation is allowed and this will stop the indexing process (indexing cannot be resumed).
  - Modified date: displayed in the browser local time.
  - Search is not case sensitive.
  - Support only search according to entry name (not full path).
  - No multi-tenancy support.
  - Search and Restore requires Enterprise Cloud Edition, Cloud One2Many or NFR/Trial license.
  - If the recovery site is 7.0 and the protected is 6.5, the user cannot set File System Indexing. Both the protected and recovery site must be 7.0 and above.
- **Restore File to Production VM**
  - Zerto's Restore File to Production solution is highly secure and agentless and is based on VMware Tools. As such the upload rate is limited and we do not recommend performing restores where the total restore size is large.
  - Both Recovery and Protected sites must run Zerto v8.5 or higher.

- Running a restore operation to a VM in sleep mode will fail, since the VMware Tools are not running when the VM is in this state.

  If the VM enters sleep mode in the middle of a restore operation, the restore might fail, or only partially succeed.
- If the Windows VM with files to be restored uses dynamic disks, files cannot be restored from these disks.
- The Protected site must be vCenter.
- The Protected VM must have VMware Tools running.
- To restore a file to Production, the Protected VM must be powered on.
- The user running the Restore File to Production operation must be assigned an Alias in Guest Services Credentials. The Alias must be an Active Directory user, which has the following permissions: **Modify**, **Read & Execute** and **Write**.
- When used in file names, the special character "**%**" will be replaced with "**&PCT**".
- You cannot run multiple restore operations in parallel on the same VM.
- OS and file system considerations:
  - You can only restore to a Windows VM.
  - You can only restore to NTFS.
  - Zerto's Restore Files/Folders to the production VM is not supported when the protected VM is running Windows Server 2008.
  - If the protected VM is running Windows 8.1, first install KB2999226 before using this feature.

Long-term Retention

- **Upgrade:**
  - Existing 6.5 NFS Repositories will be renamed to deprecated and can be used for Restores only. New repositories must be created for continued Long-term Retention use with Zerto 7.0 and above.
- **Repositories:**
  - **Supported Protocols:**
    - NFS - For list of supported versions, see the Interoperability Matrix.
    - SMB - For list of supported versions, see the Interoperability Matrix.
  - **Amazon AWS S3 Repositories:**
    - The AWS S3 repository can be configured by Region only. Non-default EnpointURLs are not supported.

- The Repository can be configured on top of a single access tier at a given time.
- Supported access tiers are “S3 Standard”, “S3 Standard-IA” and “S3 Standard-OZ”.
- The capacity metrics for the Repository cannot be monitored.
- This Repository type is not eligible for capacity usage alerting.
- Restore can be done to on-premise Recovery sites only.

- **Microsoft Azure Repositories:**
  - The Repository can be configured on top of a single access tier at a given time.
  - The capacity metrics for the Repository cannot be monitored.
  - This Repository type is not eligible for capacity usage alerting.
  - Supported access tiers are “Hot” and “Cool”.
  - The total capacity allocated for the Azure Repository matches the Storage Account capacity limitation.
  - SA key authentication is not supported.
  - Restore can be done to on-premise Recovery site only.
- **HPE StoreOnce Catalyst Repositories:**
  - Catalyst API Server version installed on the appliance should be v9 and above.
  - Prior to defining the HPE StoreOnce Catalyst store as a repository, Client Access should be enabled on the Catalyst store level. This is the only access mode supported for HPE StoreOnce store, which should be configured on the HPE StoreOnce itself.
  - Low-bandwidth (LBW) is the only Transfer Policy supported for a Catalyst store, to allow source side de-duplication by Zerto. This way, only unique data is sent over the wire.
  - High-bandwidth (HBW) Transfer Policy is not supported.
  - Source side de-duplication is enabled by default for this Repository and cannot be disabled.
  - In order to support source side de-duplication for a Catalyst repository, VRA restart is automatically initiated upon the first LTR operation (Retention/Restore) on that VRA to allow sufficient memory allocation. VRA restart is only initiated once running recovery operations are completed.
    - This will fail the first Long-term Retention operation running on this VRA on top of this Repository. Upon Restore, if the VRA is different than the one chosen for Retention, this operation is expected to fail as well.
  - The maximum number of concurrent streams supported when working with Catalyst type of repository is 60.
    - If the number of available streams on the HPE StoreOnce appliance is smaller than 60, an

"Out of Sessions" error will be triggered. (For example, if the HPE StoreOnce appliance supports a smaller number of concurrent streams, or the streams are already utilized by another software).

- Each VRA can support up to 5 concurrent volumes to be processed for Retention or Restore operations, in a given time. Other volumes will be queued and processed once the current ones are completed.

- **Reattached Repository**:
  - Restore of Retention sets created in a Repository in a ZVM running Zerto 8.5 is not supported in a ZVM running an earlier version.
- **Incremental Retention Processes:**
  - Zerto can track up to 40TB of changes per volume.
- **Application-aware :**
  - For Application-aware retention, VMware Tools must be version 10.2.5 and later.
  - Application-aware Retention can only be enabled on Windows VMs.
  - Only a single VM within a VPG can be configured for Application-aware Retention.
  - Application-aware Retention is supported only when both sites are 8.0 and above.
  - In order to retain Application-aware Retention configuration after failing over with reverse protection, the user must ensure the Alias is available and configured with the correct credentials on the Recovery site. If a different Alias should be used, the user must select the correct Alias name with the credentials needed when setting up reverse protection through the Failover wizard. After failover is complete, if the correct Alias is not assigned or is not available in the Guest Services Credentials tab, Edit VPG cannot be performed and a general error to contact Zerto support is displayed.
- **Scheduling and Retention Policy:**
  - All scheduled Retention process periods (Daily, Weekly, Monthly, Yearly) are scheduled to run at the same time of the day.
  - If Full and Incremental Retentions are scheduled for the same day, the system will run a Full Retention process. For example, if a Daily Retention process is set to run an Incremental on Sunday and a Weekly is set to run a Full on Sunday, a Full Retention process will be performed.
  - Retention sets created prior to Zerto 8.5, and their corespondent VPG that was deleted prior to Zerto 8.5 are not managed and their Retention sets are not removed from the repository, even when the retention period has passed.
  - Retention sets created in Zerto 6.5 will not be managed by any Retention policy, even if expired.
  - In some scenarios, the Retention process will wait in queue and will start running only on the following day, resulting in two Retention sets on the same day.

- Retention process can be triggered within 12 hours from scheduled time. After 12 hours the trigger is outdated.
- If the Long-term Retention settings are adjusted to a future time in the day, after the Retention process had already been triggered, the process will be triggered again at the newly set time.
- If the VPG status does not allow for Long-term Retention processes to run due to other recovery operations, and automatic retries for Long-term Retention process are configured (per VPG), the Retention process will wait in queue until the running operation on the VPG completes.
- In rare cases where the time of the Recovery or the Protected sites is out of sync, a Retention process will be considered to have run before its scheduled time, hence will not be taken into account in several metrics in the "Long Term" tab in the ZVM.
- Both Protected and Recovery sites must use the same daylight saving settings - either enabled or disabled.
- When editing a VPG where the protected site runs Zerto 6.5Ux, and the recovery site runs Zerto 7.0 and above, the user will not be able to see updated scheduling settings. Any scheduling configuration done on the Zerto 6.5 GUI will be ignored.

- **Retention Sets Management:**
  - Retention sets created prior to Zerto 8.5 (for existing VPGs) can be managed only by their original ZVM, assuming they are not expired and upon the first successful Retention process in Zerto 8.5
  - Retention sets created prior to Zerto 8.5 and whose VPG was deleted before upgrading to Zerto 8.5 cannot be managed.
  - Retention sets for VPGs that were deleted in Zerto 8.5, can be managed only by their original ZVM, assuming they had at least one successful Retention process in Zerto 8.5.
- **Restore:**
  - Restoring VPGs is allowed for VPGs which currently exist, were deleted, or loaded from a reattached Repository.
  - If one or more volumes are in "initial sync" state during a Retention process, these volumes will be excluded from this Retention process.
- **Performance:**
  - DSS and VRA consume CPU. As such, if the CPU resources on the VRA are saturated, another CPU should be added to the VRA machine.
- **Manual Retention Processes:**
  - If the scheduled Retention process on that day has already executed, manual Retention will either run the last settings used, or run a default incremental with 90 days expiry.
- **Manual Deletion of Retention Sets:**
  - After a recovery operation for a currently protected VPG, if the VPG has Retention sets available,

they will available for manual deletion when accessing "Manage Retention Sets" in the Repository context, from the Recovery site they were created in.

- Retention sets from a reattached Repository that were created on an other Recovery site are not eligible for manual deletion.
- Retention sets marked for manual deletion will be deleted from the Repository in up to 48 hours at most.
- In the “Manage Retention Sets” window, when switching between **VPG** and **Repository** search, all previously selected Retention sets will be automatically deselected.
- Upon triggering manual deletion, the selected Retention sets are not eligible for Restore.
- Upon triggering manual deletion, if a VPG has a running Retention or Restore task, its last Retention sets chain (Full and its subsequent Incrementals) are only eligible for deletion upon the task completion.
- The Retention set size can be determined only for those Retention Sets created in Zerto 8.5 and later.
- “Manage Retention Sets” is not supported via ZSSP.
- In rare cases, when the ZVM time was adjusted (not as part of Daylight saving), the Retention Set dependency can be displayed incorrectly.
- In case the last Retention set was manually deleted, it will be considered as missing. The Long-term Retention tab will report it as such, and an alert will be triggered.

- **Cloud Service Providers and Zerto Cloud Manager Users:**
  - "Extended Recovery" Service profiles are not supported and are removed as part of the upgrade.
  - Extended service profiles are not supported for LTR use. Use Custom Service profiles instead.
- **ZSSP Users**:
  - ZSSP is not supported for Long-term Retention.
- **Compression:**
  - Long-term Compression cannot be set for HPE StoreOnce Catalyst repositories.
  - The Restore process with compressed Retention configured in a ZVM running an earlier Zerto version than 8.5 is not supported.
  - The Compression level is fixed throughout the Retention process.
  - Repositories with Compressed Retention sets can be re-attached to ZVMs running Zerto 8.5 and later.
- **General:**
  - Partial Retention or partial Restore processes are not supported.

- Long-term Retention is not supported where the protected or recovery site is a Public Cloud. Therefore, the SETUP tab in the ZCA was removed.
- Only one Long-term Retention task can run on a VPG concurrently.
- When configuring FreeNAS as Long-term Repository connected via SMB protocol, the “Server minimum protocol” parameter needs to be explicitly set with “3_00."
- A repository previously attached in a ZVM running Zerto 8.5 cannot be re-attached in a ZVM running an earlier version.
- A VPG with Long-term Retention enabled cannot be imported from Zerto 8.0 to Zerto 8.5, due to incompatible Compression settings.

Upgradeability

- **VRA upgrade:** The user is recommended to follow the VRA upgrade via the Zerto Virtual Manager GUI.
- When an update/hotfix installation occurs and the VRA auto upgrade checkbox is still enabled, there is a second event that is presented in the GUI, even though there was no VRA upgrade.

VSS

- VSS checkpoints are only implemented when protecting Windows 2012 generation 2 virtual machines.
- Invoking the Zerto VSS Agent can cause errors to be written to the Windows application log. These errors can be ignored.
- If you use Chrome to download the VSS agent installation, you are warned that the software is malicious. You can ignore this warning.

Zerto Cloud Manager (ZCM)

- MSP administrators with specific roles and permissions defined for them in the ZCM are able to view resources from ZORGs to which they are not assigned in the ZCM.
- When an existing VPG is attached to a ZORG, it is not possible to edit this VPG either after uninstalling the ZCM, or after removing a site from the ZCM.
- If the ZVM access code is not yet input for a site in ZCM, an invalid license alert is displayed. The alert will disappear only after the access code is entered.

General

- Zerto installer certification authority changed to GoDaddy on July 1st, 2020. The installation requires the certification to be installed on the VM. In rare scenarios in Zerto v8.0U3 and above, where Windows did not run a Windows update, or due to strict certification policy that does not allow

GoDaddy certification to be installed, users will get an installation error, and will be required to manually install the GoDaddy root certificate.

- If either the production or recovery sites are protecting over 1000 VMs, then Zerto recommends the ZVM be configured with at least 16GB memory and at least 12 CPUs prior to installing Zerto 8.5. These ZVM requirements will ensure the new features in Zerto 8.5 release will have enough memory and CPU resources to operate properly.
- ZVM initialization is longer than usual when the ZVM site has over 50 peers.
- The backslash character (\) is displayed as **%5c** in the GUI, for example when used in a virtual machine name.
- If the local site Zerto service is down, you can still recover and clone VPGs. When cloning a VPG, the clone progress bar in the VPG Details screen is not updated.
- In a multi-site environment and when masking is not implemented, adding a virtual machine to a VPG by editing the VPG from the recovery site, displays all virtual machines on the protected site, including those protected to a different recovery site.
- Zerto Cloud Connector *.vswp files are not included in the DATASTORES tab, DR Usage value.
- When creating a VPG and there is no available recovery site, the GUI display is corrupted.

  Workaround: Make sure the connection to the replication site is restored and refresh the browser.
- Increasing a protected virtual machine disk size to greater than 2TB causes the VPG to enter a the state, **Needs Configuration**.
- When replication is to a VSAN, disk space used by the journal is not deallocated when the journal size decreases.
- Protecting DVD drives is not supported.

Zerto

Zerto enhances the Zerto the Zerto 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.