RELEASE NOTES FOR ZERTO VIRTUAL REPLICATION 4.5U4

Zerto Virtual Replication 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 and 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 Virtual Replication enables a virtual-aware recovery with low values for both the RTO and RPO. In addition, Zerto Virtual Replication enables protecting virtual machines for extended, longer term, recovery from an offsite backup.

The following topics are described in these Release Notes:

- End-of-Version Support Notice
- Installing Zerto Virtual Replication Version 4.5U4
- Installing Zerto Cloud Manager Version 4.5U4
- Upgrading Zerto Virtual Replication and/or Zerto Cloud Manager to 4.5U4
- Zerto VSS Agent
- New Features and Resolved Issues in 4.5 Update 1
- Known Issues

End-of-Version Support Notice

Zerto is applying the following end-of-version support policy starting with this version of Zerto Virtual Replication:

<table>
<thead>
<tr>
<th>ZERTO/VIRTUAL REPLICATION VERSION</th>
<th>DATE OF GA</th>
<th>END OF SALES AND DISTRIBUTION</th>
<th>END OF STANDARD SUPPORT</th>
<th>END OF TECHNICAL GUIDANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.5</td>
<td>March 7, 2016</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.0</td>
<td>May 5, 2015</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3.5</td>
<td>May 27, 2014</td>
<td>March 31, 2016</td>
<td>September 30, 2016</td>
<td>From the next version after 4.5 release</td>
</tr>
</tbody>
</table>

Zerto will not support customers that use outdated 3rd party software until they upgrade. Zerto will make an effort to help, but no escalations or fixes will be provided.

Installing Zerto Virtual Replication Version 4.5U4

The Zerto Virtual Manager (ZVM) 4.5U4 cannot be installed on Windows 2003 or 2008 32-bit Windows operating systems.

The following platforms are supported for the installation:

- Windows Server 2008 R2 SP1 with KB3033929 and KB2864202
- Windows Server 2012 base and Windows Server 2012 R2

.NET 4.5.2 is required. The .NET 4.5.2 installation package is included with the Zerto Virtual Replication 4.5U4 installation package.

Note: When installing in a Hyper-V environment, you can ignore any warnings about Integration Services not being updated for the VRAs.
Installing Zerto Cloud Manager Version 4.5U4

Zerto Cloud Manager 4.5U4 cannot be installed on Windows 2003. The following platforms are supported for the installation:

- Windows Server 2008 and higher
- Windows 7 and 8

.Net 4.5.2 is required. The .Net 4.5.2 installation package is included with the Zerto Cloud Manager 4.5U4 installation package.

Upgrading Zerto Virtual Replication and/or Zerto Cloud Manager to 4.5U4

If Zerto Cloud Manager is used, upgrade the Zerto Cloud Manager (ZCM) before upgrading the Zerto Virtual Managers. You can use a ZCM running Zerto Virtual Replication 4.5U4 with Zerto Virtual Managers running 4.5, 4.5Ux, 4.0Ux.

For more information, see Upgrading Zerto Virtual Replication.

Notes:

- You do not need to move workloads during an upgrade.
- When upgrading a protected vSphere environment, after the upgrade, a bitmap sync is performed for both incoming and outgoing VPGs.
  When upgrading a protected Hyper-V environment, after the upgrade, the following occurs:
  - If you are upgrading from 4.5 U2 or a later release, a bitmap sync is performed for both incoming and outgoing VPGs.
  - If you are upgrading from 4.5 U1 or an earlier release, a delta sync is performed for outgoing VPGs and a bitmap sync is performed for incoming VPGs.
- Zerto no longer supports protection of vCenter Server vApps. Any VPG protecting a vAPP should be recreated using the virtual machines in the vApp. When upgrading to 4.5U4 from 4.5 or lower, if there is a VPG protecting a vCenter Server vApp, the user will get a warning before the upgrade:
  
  Zerto no longer supports protection of vCenter Server vApps. Create a new VPG with the virtual machines from the vApp added separately to the VPG.

In a Hyper-V environment, if a VRA was configured to use DHCP in a 4.0Ux version, when upgrading to 4.5Ux, the VRA must be configured to a static IP address before upgrading the Zerto Virtual Manager. Otherwise, edit the /etc/network/interfaces file on the VRA as follows:

- Change the iface eth0 inet value from static to dhcp.
- Provide a netmask value.
- Add the gateway.

Resolved Issues in 4.5 Update 4

The following Resolved Issues have been included in 4.5 Update 4.

vCenter Server

- If a user changes the volume type (thick/thin) of a recovery volume by svMotion, the Zerto Virtual Manager (ZVM) will no longer fail to synchronize following an upgrade to 4.5Ux.
- If the user selects virtual machines for the VPG, selects the recovery site, and then clicks BACK to the VMs tab, the previously selected virtual machines no longer disappear.
- Zerto now supports IP reconfiguration for RHEL systems using the legacy network settings under /etc/sysconfig/network in addition to the modern /etc/sysconfig/network-scripts settings.
- Users can successfully re-IP RedHat version 7 and above virtual machines upon failover when using version 6 and below NIC’s naming conventions.
- Re-ip support for oracle Linux virtual machines was fixed.
- It is no longer possible to upgrade with an installer of a different platform.
- When a protected site is disconnected, the Resource Report on the recovery site will run as usual except for the protected host names, which will not be included.
- VRA no longer attempts to access DNS (UDP port 53) when configured with static IP.
- VPGs with a custom service profile can now be managed with the Manage VPG API.
- NLog configuration setting were reverted back to the “discard log lines”, when the ZVM was unable to flush logs fast enough. This prevents high ZVM memory and CPU usage.
- Calls to GetVMs via REST API no longer cause severe ZVM performance issues. In addition, all calls to the API are now properly logged to the ZVM logs.
- It is now possible to perform Zerto Cloud Manager (ZCM) actions when it is disconnected from any paired zerto virtual manager.
- Cloud customers can now use ZSSP through the Cloud Provider portal when a username and password are not set in a ZORG.

vCloud Director
- Running failover live from VC to vCD 8.0.x no longer encounters occasional issues.

Hyper-V
- It is now possible to preseed a recovery volume when preseeding to a Hyper-V recovery site, and the preseeded disk has a file extension name that is in upper case.
- User can see data in the UI when a storage volume has its vmhost.hostcluster.id reported as null.

AWS
- It is now possible to create VPGs with Windows machines recovering to Amazon with up to 22 volumes. Linux machines are still limited to 12 volumes.
- Running failover live from VMware to AWS no longer encounters occasional issues.

Cross-replication
- Protected virtual machines with over 64GB of RAM will no longer cause recovery and move operations to fail when the target site is SCVMM.

Zerto Cloud Manager and Zerto Self-service Portal
- It is no longer necessary to fill in the ZSSP username and password in order to generate the ZSSP URL. It is now possible to add a username in the URL generator to track it in the zerto virtual manager tasks.

General
- Users are now able to use PowerShell’s PSCredentials object to connect to the REST API.
- Messages displayed when login fails are clearer, and the overall understanding of the zerto virtual manager login failure causes has been improved, thus making it easier and faster to solve login issues.
New Features and Resolved Issues in 4.5 Update 3

The following New Features and Resolved Issues have been included 4.5 Update 2:

New Features

- RPO is shown as N/A instead of 0, when creating a VPG, or when an initial or bitmap sync task take longer to complete than the time period of the configured journal history.

Issues Resolved in 4.5 Update 3

The following issues have been resolved in this release.

- Zerto Cloud Connector (ZCC) that have been deleted from vCenter can now be uninstalled using the Zerto Cloud Manager (ZCM).
- Issues when performing recovery operations on a VM with a shared PCI device have been resolved by removing VirtualPCIPassthrough HW devices from recovery VMs.
- In Hyper-V environments, diskbox names longer than 64 characters (due to long host names) will be truncated.
- In Hyper-V environments, zerto virtual manager will handle paths with multiple mount points that have varying capitalization.
- If the Zerto Virtual Manager host IP is changed, Virtual Backup Appliance connectivity is not affected.
- In vCenter to AWS environments, the ampersand character can be part of protected VMs name.
- The certificate password has been added to the Zerto Virtual Manager reconfiguration wizard of the ZertoDiagnostics utility.
- In Hyper-V to vCenter environments Unprotect VM events are no longer triggered when the host has error status in the SCVMM.
- Remote task initiators are correctly reported in VPG Events Monitoring screen.
- Logout and redirect after logging out of ZSSP using the logoutRedirectUrl parameter works correctly.
- When performing Journal File Level Restore (jFLR), in the restore flow, an increased timeout period ensures volume mounts requiring up to ten minutes will succeed. In worst case situations, if a mount fails due to a timeout, VBA restart only is required.
- When specifying an external database name during installation, you can click Next without first having to move to a different input field.
- Undefined system behaviors, no longer occur if removing a single volume does not complete successfully.
- VRA Debian OS was upgraded to latest stable version (8.5) resolving various kernel panic conditions.
- In cases where two different VCs belong to the same vCD and there are two datastores with the same identifier, reflection collection will fail.
- In vCenter to AWS VPC environments where no default subnet is defined, rare occurrences of the inability to create a VPG for recovery operations have been eliminated.
- In Hyper-V to vCD environments, VPGs entering Needs Configuration state caused by missing a reflection cycle have been resolved.
- Following a host restart, VRA driver will not be pushed to a stateless ESXi installed using VIB.
- The user no longer has to enter the password of the vCD, each time a datastore is configured in a Provider Virtual Data Center (PvDC).
- Changing permissions in the ZCM does not affect the cloud sites when ZCM and ZSSP are both open.
- The zerto virtual manager will no longer attempt to collect data for an SCVMM object locked by another operation.
- Upgrade procedure to version 4.5x from version 3.5x via version 4.0x completes without error.
- Credential management during VRA installation has been improved. When a VRA installation incorporates a VIB, the checkbox is unchecked, and the password field is disabled. When a VRA is installed without incorporating a VIB, the checkbox is checked, and the password field is enabled.
- Reverse protection in VPGs created from VCD to VCD no longer experience Missing Configuration error.
- Re-entered correct AWS credentials can now be varified after initially entering incorrect credentials.
- When Use credentials to connect to host is selected when installing a VRA, the password is no longer displayed in the Host Root Password field.
Fields in the vCenter Server Connectivity and zerto virtual manager Site Details dialogs are populated automatically with existing configuration data.

Licenses that have been changed retain their modified value after the zerto virtual manager service restarts.

Upgrades from 4.0Ux to 4.5Ux will complete successfully even if there is a VPG in Needs Configuration state.

In Hyper-V environments, issues have been resolved with VPGs configured with the re-IP option on Linux machines.

Credentials are no longer retained and used in express installation if initial custom installation fails to complete.

Users with permissions over specific ZORGless VPGs retain their permissions after upgrade.

The web UI will now provide a detailed failure message on some VRA installation failures.

In the Advance Journal Settings dialog, when selecting Default in the Default Journal Datastore field, and changing the default value in the Journal Size Hard Limit field, the Journal Datastore field in the Advanced VM Replication Settings dialog is no longer null.

VRA Debian OS was upgraded to latest stable version (8.5). SSH Configuration was also bolstered to address a wide variety of issues.

When having two sites in 4.5 U2, and upgrading a VRA in one of the sites to 4.5 U3, errors no longer appear in the following situations: Pairing the sites. Creating a VPG on one site and recovering to the other site where the VRA was upgraded.

During failover live when pressing commit, and sites are disconnected, the commit popup is no longer locked.

When first installing zerto virtual manager with a custom “Windows Service User”, the zerto virtual manager service no longer requires to be added manually.

Bulk edit of vNICs in the VPG wizard no longer causes the wizard stop to responding.

Adding a virtual machine to a protected vCD vApp no longer causes recovery operations to fail.

In Hyper-V to Hyper-V environments, importing of VPGs exported from 4.5U2 or 4.5U3 into 4.5U3 completes without error.

When creating a ZORG, the option to select a Custom Service Profile is available when using the Cloud zerto virtual manager or ZCM user interfaces to edit the Replication tab of the VPG created in the ZORG.

Installer issue requiring that Repair be run to remove the duplicate zerto virtual manager from ARP has been addressed.

Zerto VSS Agent

Product Change: Zerto VSS Agent is now a separately licensed capability.

Starting July 31st 2016 Zerto will be charging for new deployments of Zerto VSS Agent. It will be licensed on a per VM basis. This license will be required at time of installation of the Zerto VSS agent. Please see the installation guide for further information on license installation. If you have any further questions on this change, please contact your Zerto Account Manager.

Note: Customers that have been using previous versions of the Zerto VSS Agent will need to obtain a license and install a new Zerto VSS agent. Zerto will provide licenses for existing, however installing a new, licensed Zerto VSS Agent is required.

New Features and Resolved Issues in 4.5 Update 2

The following New Features and Resolved Issues have been included 4.5 Update 2:

New Features

The following improvements have been included in this release:

- The AWS Beijing region is supported.
- The AWS Seoul region is supported.
- A single Zerto Virtual Manager can now provide protection for over 2PB of data.
- Any errors during the AWS import process will be reported in the Zerto failure event. This includes, but is not limited to, VMs that aren’t supported by AWS.
Issues Resolved in 4.5 Update 2

The following issues were resolved in this release:

- Users with the Manage VPG privilege can now configure backups when creating or editing a VPG.
- Long file paths in the File and Folder Restore: Download wizard are now correctly displayed.
- When recovering a virtual machine with multiple NICs, to AWS a message is displayed if some of the NICs were not created.
- Exporting the Usage report from the GUI now works.
- If uploading a log bundle via FTP fails, when the user clicks the retry button only the log bundle is uploaded; the logs are no longer collected again.
- When exporting VPGs from the VPG list, the .csv file that is created now includes VPGs protected to AWS.
- In hosting VC to VCD, hosting VC to VC, and VCD to VCD configurations, a customer can now create a VPG to VCD in ZSSP using a custom service profile.
- A failure when upgrading to 4.5U2 does not cause problems with the original installation.
- Checks of the amount of storage available to the journal has been corrected.
- MTU problems in VRA to VRA connections are now checked and detected during the initial connection attempt. VRA to VRA connections with MTU problems will remain disconnected - and a VRA disconnection alert will be displayed in the Zerto Virtual Manager. MTU problems are also reported in the VRA logs.
- In Hyper-V environments, backups via Veeam no longer cause VPGs to enter major error states.
- Static fields are now displayed instead of buttons in the VPG wizard for DRaaS customers that are not permitted to use the Custom Service Profile.
- When using VMware vCloud Director, you can use the Change VM Recovery VRA dialog even if a datastore is removed from the storage profile as long as there is another datastore available to the VRA.
- An appropriate message is now displayed when attempting to log on to Zerto Cloud Manager with insufficient Active Directory permissions.
- Installation logs (MSI) of remote sites are now collected and saved in the installlog folder.
- Re-IP on Ubuntu virtual machines now works correctly during recovery operations.
- In Japanese environments, re-IP during VMware > Hyper-V recovery operation no longer times out while waiting for integration services.
- The journal of a VPG created with a journal size hard limit expressed as a percentage is now configured with the correct amount of storage.
- When editing a virtual machine NICs in a VPG, deleting the contents of the Alternate DNS Server field no longer results in an invalid IP format error.
- The Zerto Cloud Manager no longer crashes when a Zerto Virtual Manager is added to it through the GUI.
- Logging out of ZSSP without the logoutRedirectUrl parameter now closes the session and the URL cannot be re-used.
- Extremely rare system crash of the Hyper-V host when upgrading the VRA from 4.0U6 to 4.5U1 no longer occurs.
Release Notes for Zerto Virtual Replication 4.5U4

New Features and Resolved Issues in 4.5 Update 1

The following New Features and Resolved Issues were included 4.5 Update 1:

New Features

The following improvements have been included in Zerto Virtual Replication version 4.5 Update 1:

- The AWS EU (Frankfurt) region is supported.
- vSphere 6.0U2 is supported, except for VSAN 6.0U2, which is not supported.
- vCloud Director 8.0.1 is supported.
- Monitoring Zerto Self-service Portal is enabled by the addition of an event, EV0070, that is triggered on every login to the Zerto Virtual Manager and Zerto Self-service Portal.
- If role-based access is enabled, users, other than administrators, can perform recovery operations from the recovery site.
- In a VMware environment, virtual machines with a Linux Oracle 6.5 operating system and VM Tools can now be re-IPed.
- Ongoing performance improvements, especially in large environments.

Note: The additional options in the /v1/vpgs API: vpgs/{protectionGroupIdentifier}/forcesync, vpgs/{protectionGroupIdentifier}/pause and vpgs/{protectionGroupIdentifier}/resume are not supported in this release, even though they are displayed as part of the /v1/vpgs/help.

Issues Resolved in 4.5 Update 1

The following types of issues were resolved in this release.

- Creating and Editing a VPG
- Role-Based Access Control
- Zerto Self-service Portal
- vSphere Specific Fixes
- Hyper-V Specific Fixes
- Other Fixes

Upgrade

- When upgrading, the Zerto Virtual Manager service is no longer automatically set to the local account regardless of how it was previously set.

Creating and Editing a VPG

- When you select a vCD vApp with many virtual machines to include in a VPG, the last virtual machine in the list is now visible.
- In a VMware environment:
  - In the STORAGE step of creating a VPG, when the source volume is a preseeded disk, the text at the top of the Browse for file dialog now shows VMDK and not VHDX/VHD.
  - When either the protected or recover site is vCD, creating a VPG with preseeding now works.

Role-Based Access Control

- Using REST APIs does not consider the status of role-based access control, whether it was enabled or disabled.
- When role-based access is enabled, recovery operations from the recovery site can now be performed by all users with valid permissions and not just administrators.
- Implementation of permissions has been hardened:
  - A user with the Manage VRAs privilege can now change the recovery VRA of all virtual machines in VPGs for the site.
  - Users without permission to stop a clone completing, no longer see the Stop Clone button.
  - Only users with an appropriate permission can perform a restore from backup.
  - Users with an appropriate permission can now uninstall a VRA that only manages outgoing VPGs.
■ After a ZORG or VPG with permissions on it enabled, is deleted, the user no longer has access to the Zerto Virtual Manager.
■ Users now only see the buttons, such as the file level recovery UNMOUNT button, and alerts relevant to their permissions.
■ After permissions are updated, the updated set of permissions are now immediately enabled: they do not require logging back in to the Zerto Virtual Manager.

Zerto Self-service Portal
■ When the Zerto Self-service Portal times out, the GUI now automatically redisplay the login screen.

vSphere Specific Fixes
■ When moving VMDK files, for example when changing the datastore, all files related to the VMDK file, such as hidden .lck files are also handled so that Zerto Virtual Replication can efficiently tidy up empty folders.
■ When the protected environment is vCenter Server and the recovery environment is vCD, the user can no longer create a VPG containing virtual machines with a hardware version not supported in the vCD environment.
■ If you add a virtual machine to a protected vCD vApp, and, while the additional virtual machine is still in an initial sync state, fail over the VPG, you are notified that the additional virtual machine will not be recovered because it has not yet been synced to the recovery site. The virtual machine that was added to the vApp is no longer removed from the vApp.
■ A Move operation when one or more of the virtual machines in the VPG includes RDM disks and when the VRA is installed on an ESXi 5.1 now completes successfully.

Hyper-V Specific Fixes
■ When reconfiguring the SCVMM credentials via the Diagnostics utility, you no longer need to stop the Zerto Virtual Manager and Virtual Backup Appliance services.
■ You can now stop a failover test after the Zerto Virtual Manager stopped and was restarted.
■ You can now run Veeam backups while protecting virtual machines.
■ Setting a new MAC address for recovery when the recovery site is vCD now connects the recovered virtual machines to the correct networks.
■ Editing a VRA no longer includes fields required by vSphere only.

Other Fixes
■ After replicating from Hyper-V to vSphere Server and the recovery virtual machine has a write performed that is greater than 4MB, failing back to Hyper-V now succeeds.
■ You can migrate the Zerto Virtual Manager database to an external SQL server 2012 using the Database Migration tool.

New Features in Zerto Virtual Replication 4.5
Zerto Virtual Replication includes the following new features:
■ New Installation
■ File Level Restore
■ Permissions – Role-based Access Control
■ Improved Recovery
■ VRA Enhancements
■ Journal Feature Enhancements
■ API Extensions
■ Cmdlet Enhancements
■ vSphere and Hyper-V Support
■ Additional vCD Functionality
■ Encryption When Recovering to AWS
■ Easier Editing in Tables
New Installation

The Zerto installation has been totally redesigned. As well as a new sharper look, the installation flows have been updated to make them easier to understand.

Silent Installations

You can perform a silent installation of Zerto Virtual Replication in all environments. The silent installation has been changed so you can specify the installation configuration as part of the silent installation command.

File Level Restore

You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto Virtual Replication and running Windows operating systems. You can recover the files and folders from a specific point-in-time.

You can choose to recover one or several files or a folder from the recovery site. Files can be restored from all file systems supported by Windows, such as NTFS, FAT, and ReFS. The operating system of the machine on which the recovery site Zerto Virtual Manager is installed determines the types of file systems from which files and folders can be recovered. When the recovery site Zerto Virtual Manager virtual machine operating system supports a file system, files and folders can be recovered from this file system in virtual machines that this Zerto Virtual Manager will manage the recovery of. For example, if a protected virtual machine running Windows 2012 has files using the ReFS file system and requires one or more of these files to be recovered and the recovery site Zerto Virtual Manager is on a machine with Windows 2008, which does not support ReFS, the protected virtual machine files and folders cannot be recovered.

File level recovery can be performed from vSphere, Hyper-V and AWS recovery sites with the following limitations:

- You can only recover files or folders from Windows machines. You cannot recover files or folders from Linux machines.
- If the Windows virtual machine with files to be restored uses dynamic disks, files cannot be restored from these disks.
- When the Zerto Virtual Manager is installed on a Generation 1 virtual machine, you can only mount disks for file level recovery from a generation 1 virtual machine.
- When the Zerto Virtual Manager is installed on a Generation 2 virtual machine, you can mount disks for file level recovery from a generation 1 virtual machine and from all disks except for the boot disk, normally C:, from a generation 2 virtual machine.
- When the protected virtual machine and the virtual machine of the recovery zerto virtual manager are created from the same template, GPT disks do not support Journal File Level Restore (jFLR).
- When a large number of disks are mounted, when they are unmounted, some of the disks remain mounted and this is not reflected in the user interface.
- You can only recover files or folders when an offsite backup is not running.

To restore files from a protected virtual machine when permissions are set in the Zerto Cloud Manager, described in “Permissions - Role-based Access Control”, below, you user must have both the Manage VPGs and View Only privileges set.

Permissions – Role-based Access Control

Handling permissions has been extended to enable applying permissions to specific entities such as ZORGs, VPGs, and sites.

Roles can be defined with a set of privileges that define an operation or a set of operations that can be performed, such as managing a VPG or VRA. These roles can then be assigned to users and groups of users.

You can then define permissions which determine the roles that apply to a specific user or user group on a specific entity.

The following Active Directory groups are not supported:

- Everyone
- Users
- Pre-Windows 2000 Compatible Access
- Authenticated Users-NT AUTHORITY\Authenticated Users
- This Organization-NT AUTHORITY\This Organization
- Service asserted identity-Service asserted identity
Note: After upgrading the Zerto Cloud Manager to version 4.5 and enabling role-based access, before upgrading any Zerto Virtual Managers, requires that role-based access is disabled and then re-enabled after upgrading the Zerto Virtual Managers.

**Improved Recovery**

**Adding Virtual Machines to a VPG**

After adding virtual machines to a VPG, the additional virtual machines are synchronized with the recovery site. During this synchronization, the original virtual machines in the VPG are still protected and can be failed over. The protection status is Meeting SLA for \( n/m \)

where \( n \) is the number of original virtual machines in the VPG and \( m \) is the total number of virtual machines in the VPG, including the added virtual machines.

When the synchronization for each added virtual machine is complete, Zerto Virtual Manager adds a checkpoint:

VM 'XXX' is fully synced where XXX is the name of the virtual machine that was synced.

When you do a recovery operation using a checkpoints before an added virtual machine was synchronized, only the virtual machines that completed syncing at this checkpoint are recovered.

**More Robust Journal Health**

The journal is automatically reconfigured and journal history increased beyond the configured history SLA, to ensure that the SLA defined for the VPG is maintained during long network outages and other incidents that prevent checkpoints being written to the journal.

**VRA Enhancements**

VRA functionality has been enhanced.

**VRA Deployment (vSphere Environments)**

VRAs can be installed using vSphere Installation Bundle, VIB, so that a password to install the VRA on a host is no longer required. This makes automating the installation of VRAs in a vSphere environment using APIs simple. For API details, refer to “API Extensions”, below.

**Enhanced Handling of Ghost VRAs**

A VRA could enter a ghost state for a few reasons. In Zerto Virtual Replication version 4.5 some of these situations resolve themselves automatically and some require user input.

When a protected disk cannot be accessed by the VRA, only the VPG directly affected is marked as ghost and the user can to do one of the following:

- Remove the affected virtual machines from the VPG, enabling the remaining virtual machines to remain protected. Also, only the relevant VPG is affected and not all VPGs recovering to that VRA.
- Change the recovery datastore. This will result in the VPG being re-synced. All other VPGs recovering to the VRA are unaffected.

**Changing the Recovery Host**

The recovery host can be changed even when the recovery VRA is not accessible, for example, when the host is in maintenance mode.
Journal Feature Enhancements

Journal functionality has been enhanced.

Journal Compression

Data passed from the protected site to the recovery site is saved in the journal in a compressed format. The data is compressed when it is passed over the network to the recovery side and uncompressed when a recovery operation is required. This uses less space without impacting the RTO. Compression is enabled automatically when WAN compression is enabled for a VPG.

Journal Extended to 14 days

Journal history has increased from a maximum of 5 days to 14 days. Also the default journal has changed from 4 hours to 1 day.

Journal Default Sized Changed From Unlimited

When defining the journal size for a VPG, the default has been changed from unlimited to 150GB.

API Extensions

The following changes have been made to the APIs:

Alerts – Enables retrieving information about alerts as well as being able to dismiss or undismiss an alert.

Events – Enhanced to include the ability to retrieve event information by category, entity or type.

Tasks – Enhanced to include the ability to retrieve information by task type.

Virtualizationsites – Enhanced to include the ability to retrieve information to use in the vpgsettings API.

VPGs – Enables deleting a VPG, retrieving event information by VPG priority, retention policy, status or substatus.

VpgSettings – You can manage VPGs using both the VPGs API or the VpgSettings API. Use the VPGs API to perform actions on a VPG, such as failing over a VPG, cloning a VPG or testing a VPG. Use the VpgSettings API to manage the definition of a VPG, including editing the VPG definition and adding or removing virtual machines from a VPG. Although both APIs can be used to create or delete a VPG, the VPGs API can only be used to create a VPG in a VMware vSphere environment and relies on Zerto Virtual Manager defaults for many of the VPG definitions. Using the VpgSettings API, you have full control to specify every field in the VPG definition in both a VMware vSphere and Microsoft Hyper-V environment, although it can only be run to create a VPG from the protected site. Use the vpgSettings API to do the following:

■ Create a new VPG.
■ Display values in an existing VPG.
■ Edit existing values in a VPG.

What is Supported

The vpgSettings API works in the following environments:

■ vCenter Server
■ Hyper-V
■ vCenter Server to Hyper-V and Hyper-V to vCenter Server
■ Running on the protected site

What is Not Supported

The vpgSettings API does not support the following:

■ vCloud Director
■ Preseeding
■ Virtual machines with RDM disks
■ Setting backup
■ Running on the recovery site
**VRAs** – Enables installing, editing and deleting a VRA. Along with the [VRA Deployment (vSphere Environments)](https://www.zerto.com) feature this makes automating the installation of VRAs in a vSphere environment using APIs simple. When installing a VRA on a vSphere ESXi host version 5.5 and higher, Zerto Virtual Manager uses a vSphere Installation Bundle, VIB, to connect to the host. When using VIB and a password is not required in the request body.

**Cmdlet Enhancements**

The export-settings cmdlet can be used to export the VPG settings between the site and a paired when one Zerto Virtual Manager is down, by running the cmdlet from the paired Zerto Virtual Manager.

**vSphere and Hyper-V Support**

Zerto Virtual Replication supports vSphere version 6 and vCloud Director versions 5.6.3 and 5.6.4.

Zerto Virtual Replication supports Microsoft SCVMM and Hyper-V hosts 2012 R2 Rollups 1-9 but recommends using Rollups 5-9.

**Additional vCD Functionality**

**Changing the Recovery Storage Profile**

You can now change the recovery storage profile when recovering to vCD without incurring an initial sync.

**Support for NAT Rules When Recovering to vCD**

When both the protected and recovery sites are vCD environments, NAT rules on source vApp networks can be copied to the recovery vApp during recovery.

**Encryption When Recovering to AWS**

All replicated data from protected virtual machines to AWS can be encrypted in S3. For details, contact Zerto support.

**Easier Editing in Tables**

Values in tables, especially in the VPG wizard, can be edited inline by hovering the mouse over the value and then click the pencil icon to edit the value.

**Known Issues**

The following are known issues when using Zerto Virtual Replication.

**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.
Virtual Protection Group (VPG) and Recovery

- 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.

Modifying the Definition of a Virtual Protection Group (VPG)

- Adding a new volume to a VPG while it is being tested causes the VPG to become corrupted. You cannot stop the test nor perform a failover or move on the VPG.
  
  **Workaround:** Remove the VPG using the `ForceRemove-ProtectionGroup` cmdlet.
- Deleting a VPG can cause the alert status to change temporarily to error and for a ghost VRA to be displayed. This clears up after a few minutes and can be ignored.

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.

vCenter Server

- 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.
- VMware does not identify the IP origin for Linux virtual machines and therefore Zerto Virtual Replication 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.
  
- After hibernating a laptop running vSphere Client console, you have to restart the console to reload the Zerto Virtual Replication GUI.
- Zerto Virtual Replication 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 Virtual Replication 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.

vCloud Director

- A protected VM replicated from vCD to a vCenter Server, that is connected to the `None` network, is recovered with a disconnected NIC, even if configured to connect to a network.
- Adding a new NIC to a protected virtual machine does not update the VPG settings by configuring a network for the NIC, causing an error when setting reverse protection for a Move or Failover operation.
  
  **Workaround:** Manually configure the VPG and add settings for the new NIC.
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.

Deleting a VPG and keeping the target disks when the VPG is recovered to a vCD v5.1 with storage profiles defined, does not move the disks to a datastore that is contained in the recovery storage profile. This means that if the disks are saved to a datastore in the storage profile, these disks cannot be used for preseeding later.

Recovering a VPG to vCD will fail if the vApp name contains any of the following special characters: ! * ' ( ) ; : @ & = + $ , / ? % # [ ].

After importing VPG settings, a volume initial sync is performed on all VPGs replicating to vCD.

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.

Adding disks to a virtual machine being protected to vCD, when the disk size is not a multiple of 1MB will cause recovery operations to fail since vCD cannot handle disks with sizes that are not integers.

---

**Hyper-V**

- Zerto Virtual Replication script parameters use vSphere terminology, even for scripts in a Microsoft Hyper-V environment.
- Re-IP does not work for Linux machines.
- During a storage disaster, if the VRA is shutdown and restarted after the storage is recovered, the journal and recovery volumes managed by the VRA may be deleted.
- In Change VM Recovery VRA, via MORE in the VRAs tab under SETUP, the values in the column VM Size (GB) are not correct.
- 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.
- VSS checkpoints are only implemented when protecting Windows 2012 generation 2 virtual machines.
- Protected virtual machines must have the latest version of Integration Services installed in order for a re-IP to be successfully performed.
- 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.
- A protected virtual machine defined in the VPG to have a static IP address on recovery will switch to a DHCP configuration when recovering.
  
  **Workaround:** Set re-IP options for the virtual machine in the VPG.

- 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.
AWS

- Preseeding is not supported.
- Zerto Virtual Replication APIs are not supported.
- Restore from backup is not supported.
- Not all instance types are available in every region. If the recovery instance type is not supported, recovery operations will fail.
  
  **Workaround:** When defining the VPG make sure that the recovery instance type supported by the recovery site region.
- Windows 7 and Window 8.1 cannot be protected to AWS.

Cross-replication

- 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.

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 Virtual Replication 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.
- A VMware vCenter Server vApp 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

- 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 sockets.
- 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.
- When recovering Windows 7 and Windows 2008 virtual machines from Hyper-V to VMware, at start-up the recovered virtual machine guest operating systems request System Recovery.
  
  **Workaround:** Before attempting recovery operations, update the guest OS registry in Windows 7 and Windows 2008 virtual machines as follows:
  a) Create a blank .reg file.
  b) Copy the following text to the new .reg file:
     ```
     Windows Registry Editor Version 5.00
     [HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services\LSI_SAS] "Start"=dword:00000000
     ```
  c) Copy the .reg file to the protected virtual machines in Hyper-V.
  d) Double-click the file and click Yes to confirm the change.
  e) Delete the .reg file that you copied to the protected virtual machines.
  
  The virtual machines will now start successfully for all recovery operations to VMware. For more details, see VMware KB #1005208.

- Windows XP virtual machines cannot be protected from Hyper-V to VMware.
- After a failover operation, the boot device order may not be replicated to the recovery site. This may lead to a boot failure of those virtual machines. In this event, the boot order of the affected virtual machines must be set manually using the SCVMM Console or the Hyper-V Manager.
Zerto Cloud Manager and Zerto Self-service Portal

- When creating a VPG from a cloud service provider to a Zerto organization, all the cloud virtual machines are displayed to add to the VPG and not just those belonging to the configured resources of the Zerto organization.

General

- Both alerts and events API calls do not return any values instead of the list of most recent events.
- Localization is not supported.
- The backslash character (\) is displayed as %5c in the GUI, for example when used in a virtual machine name.
- If the local site Zerto Virtual Replication 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.
- Invoking the Zerto VSS Agent can cause errors to be written to the Windows application log. These errors can be ignored.
- 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 Needs Configuration state.
- Re-IP does not work when restoring a virtual machine from backup.
- If you use Chrome to download the VSS agent installation, you are warned that the software is malicious. You can ignore this warning.
- When replication is to a VSAN, disk space used by the journal is not deallocated when the journal size decreases.