Zerto Virtual Replication is an IT Resilient platform to provide business continuity (BC) and disaster recovery (DR) 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”, on page 1
- “Prerequisites, Requirements and Installation Instructions”, on page 1
- “Upgrading Zerto Virtual Replication and/or Zerto Cloud Manager”, on page 2
- “What’s New in Zerto Analytics”, on page 2
- “What’s New & Resolved - Zerto Virtual Replication v6.0 Update 1”, on page 3
- “What’s New & Resolved - Zerto Virtual Replication v6.0”, on page 6
- “Known Issues”, on page 16

End-of-Version Support Notice

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

Note: Zerto will not support customers that use outdated 3rd party software until they upgrade.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.

Prerequisites, Requirements and Installation Instructions

- Before installing Zerto Virtual Replication, 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:
  - Microsoft Azure Environments
  - VMware vSphere Environments
  - Microsoft Hyper-V Environments
  - Amazon Web Services (AWS) Environments
- For Zerto Cloud Manager prerequisites and requirements, and for installation instructions, click to open and review Prerequisites & Requirements for Cloud Service Providers
- Zerto Cloud Manager Installation Guide
- For Zerto Cloud Appliance The following platforms are supported for the installation:
  - The following applications are required:
Release Notes for Zerto Virtual Replication v6.0 Update 1

- **.NET 4.5.2.** The .NET 4.5.2 installation package is included with the Zerto Virtual Replication 6.0 installation package.

**Upgrading Zerto Virtual Replication and/or Zerto Cloud Manager**

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

**What’s New in Zerto Analytics**

Zerto Analytics allows you to track, monitor and check the health of your data center from any device. All your alerts, tasks, and information on Virtual Protection Groups (VPGs) can be viewed together. This allows you to monitor your Disaster Recovery and Business Continuity status from any location that has internet connectivity. No VPN is required.

Using Zerto Analytics, you can see aggregated information from the Zerto Virtual Managers, and view the status of your environment.

**Zerto Analytics APIs**

Zerto Analytics information is now also available in OpenAPI Specification. The documentation can be accessed via the link: https://docs.api.zerto.com/

**Zerto Analytics Reporting**

As part of Zerto Analytics, https://analytics.zerto.com, you can now view metrics in the following report formats:

- **RPO:** displays a single VPG’s RPO metrics over a 1 month period.
- **Journal:** displays a single VPG’s Journal History and Journal Size metrics over a 1 month period.
- **Network:** displays network performance metrics over a 1 month period for:
  - **Single VPG:** Network performance at the VPG level (IOPs, Throughput, WAN Traffic over time).
  - **Between 2 Sites:** Total network performance between two sites (IOPs, Throughput, WAN Traffic over time).
  - **Total Outgoing:** Total network outgoing performance from a site (IOPs, Throughput, WAN Traffic over time, Bandwidth throttling).
What’s New & Resolved - Zerto Virtual Replication v6.0 Update 1

“What’s New - Zerto Virtual Replication v6.0 Update 1”, on page 3
“Resolved Issues - Version 6.0 Update 1”, on page 4

What’s New - Zerto Virtual Replication v6.0 Update 1

Zerto Virtual Replication version 6.0 Update 1 includes the following new features and functionalities:

- “Azure”, on page 3
- “vCloud Director”, on page 3
- “AWS”, on page 3
- “API”, on page 3

Azure
- The ZCA installer now filters out any storage account where the account type is set to Blob Storage.

vCloud Director
- vCD organizations configured for Fast Provisioning are now blocked from configuring Storage Policy per volume.
- The default Storage Policy setting for each volume is now ‘Use VM Defaults’.
- Zerto Virtual Replication supports vCloud Director version 9.1.

AWS
- When protecting to AWS, 40 volumes are now supported for Linux machines, and 26 volumes for Windows machines.

API
- Zerto no longer requires setting an authentication method when creating an API session. Authentication is now automatically set, based on the environment and permission settings. Authentication method is still supported in order to maintain existing scripts. However, as of 6.0 U1, the authentication method will be determined automatically, ignoring user specific authentication method.
- We introduced a new API enabling users to add tagged checkpoints, available under: https://zvm_ip:port/v1/vpgs
Resolved Issues - Version 6.0 Update 1

- “Resolved Issues: vCenter”, on page 4
- “Resolved Issues: Hyper-V”, on page 4
- “Resolved Issues: Azure”, on page 4
- “Resolved Issues: AWS”, on page 4
- “Resolved Issues: Cloud”, on page 4
- “Resolved Issues: General”, on page 5

Resolved Issues: vCenter

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>98745, 107073, 107511, 107775, 109704</td>
<td>Resiliency to errors during VRA upgrade has been improved.</td>
</tr>
<tr>
<td>100411</td>
<td>Zerto will no longer fail the reverse protection after failover live, when copying of the recovery disk to the VM folder takes a long time.</td>
</tr>
<tr>
<td>114809, 114960, 115134, 115407, 115200</td>
<td>When upgrading to ZVR 6.0, Zerto no longer fails to connect to vCenter. The failure was caused by ZVR sending the wrong password to vCenter, which caused the connection failure.</td>
</tr>
</tbody>
</table>

Resolved Issues: Hyper-V

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>It is now possible to install the Host (e.g. VRA) when TLS 1.2 is enabled.</td>
</tr>
</tbody>
</table>

Resolved Issues: Azure

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Premium storage accounts are now filtered out from the Select Storage list in the Installation wizard, since Premium storage accounts are currently not supported.</td>
</tr>
</tbody>
</table>

Resolved Issues: AWS

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>113708</td>
<td>Failover Test timeout periods were extended, making Failover Test to AWS more resilient to network failures.</td>
</tr>
<tr>
<td>114431</td>
<td>Fixed an issue which caused many zSAT instances to be created for a single protected volume.</td>
</tr>
</tbody>
</table>

Resolved Issues: Cloud

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>105807</td>
<td>When creating or editing a VPG that recovers to the public cloud, the Subnet setting in Recovery tab of the VPG wizard no longer reverts to the default setting, when moving to another step in the wizard before clicking the Done button.</td>
</tr>
</tbody>
</table>
Resolved Issues: General

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0 UPDATE 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>107427, 110597</td>
<td><strong>Recovery Report:</strong> When running a recovery report and exporting it, the times stated in the report are now consistent, and defined as ZVM local time.</td>
</tr>
<tr>
<td>92965</td>
<td><strong>ZSSP:</strong> When creating a VPG in the ZSSP, and in the recovery site there are two networks with the same display name, the user can now access the advanced create VPG wizard.</td>
</tr>
<tr>
<td>105699, 110940</td>
<td>Issues with the of bitmap sync were fixed, improving its performance.</td>
</tr>
<tr>
<td>105992</td>
<td>When adding a volume to a protected VM, and no default datastore is configured for the VPG, the VPG no longer goes into &quot;Needs configuration&quot; state.</td>
</tr>
<tr>
<td>106873</td>
<td><strong>Performance Report:</strong> The colors of the graph and legends are now correct when running the Performance Report for more than one VPG.</td>
</tr>
<tr>
<td>106861</td>
<td><strong>GET VPG API:</strong> When there’s a problem collecting ActualHistoryinMinutes for the GET VPG API, for example when the sites are disconnected, ActualHistoryinMinutes now shows a value of -1, representing an invalid sample</td>
</tr>
<tr>
<td>111472</td>
<td>Sorting protected VMs by size in the VPG Details tab, takes into account size units as well. The performance of multiple log volumes was improved and can be now be created simultaneously without any issues.</td>
</tr>
<tr>
<td>113348, 113635</td>
<td>Zerto upgrade from 5.5 to 6.0 no longer fails, when SMB backup repository is configured with credentials.</td>
</tr>
<tr>
<td>113812, 114286, 115264</td>
<td>Resolved issues related to editing of VPGs and incorrect RPO values, after importing VPGs from v4.5.</td>
</tr>
</tbody>
</table>
What’s New - In Zerto Virtual Replication v6.0

Zerto Virtual Replication version 6.0 includes the following new features and functionalities:

- “API”, on page 6
- “Azure”, on page 6
- “Replication to, from, and between Azure and AWS”, on page 7
- “AWS”, on page 7
- “Recovery Operations”, on page 7
- “vCloud Director”, on page 8
- “Hyper-V”, on page 8
- “vSphere”, on page 8
- “ZCM”, on page 9
- “Remote Upgrade for Cloud Service Providers”, on page 9
- “Offsite Backup Improvements”, on page 9
- “File Level Restore”, on page 10
- “Scaling”, on page 10
- “VPG”, on page 10

IMPORTANT Notification:

VSS functionality is no longer supported in Zerto Virtual Replication. If you require VSS functionality, see Release Notes for Zerto Virtual Replication with VSS, and Zerto Virtual Replication - VSS Deployment and User Guide.

API

- Added invalid argument validations, ensuring no arguments are misspelled or misused, which might result in unexpected behavior.
- We introduced a new API supporting bulk upgrade of VRAs.
  This allows users to easily and automatically select and upgrade their VRAs after a ZVM upgrade.
- We introduced Datastore Cluster Support in API: The VPG Settings REST API now supports the use of datastore clusters for recovery volumes.

Azure

- “Azure to Azure Replication”, on page 6
- “Failover/Move from Azure with Reverse Protection Using Preseed”, on page 6
- “Export/Import to an Azure VPG Using Delta Sync”, on page 7

Azure to Azure Replication

We now support full replication between different Azure sites.

Failover/Move from Azure with Reverse Protection Using Preseed

To help reduce the amount of data transferred over the network, now, when performing recovery operations from Azure with reverse protection:
■ The original protected disks in Azure can now be saved as recovery disks, instead of being created from scratch.
■ The system now performs delta sync, instead of an initial sync.

Export/Import to an Azure VPG Using Delta Sync
Import or Export of VPGs to Azure now uses delta sync as well as initial sync.

VPG disks can now be saved when un-pairing sites and deleting VPGs, and can later be used for importing VPGs using delta sync.

AWS
■ “Replication Out of AWS for Failback and Migration of Workloads”, on page 7
■ “Prerequisites when Replicating To and From AWS”, on page 7

Replication Out of AWS for Failback and Migration of Workloads
Failover to AWS now includes the option to configure Reverse Protection during or after Failover, allowing for automated reverse replication and failback from AWS. This includes failback and moves back to vSphere, Hyper-V, and Azure environments. EC2 VMs originating in AWS can also be protected to destinations out of AWS.

Features such as Test and live Failover, Move, pre/post scripts, 30-day journal, and many more are also supported when protecting workloads in AWS.
■ Workload Protection is subject to operational costs, as well as additional costs related to protection of those workloads as outlined in Zerto Virtual Replication - Prerequisites & Requirements for Amazon Web Services (AWS). Costs are expected to grow linearly with time as long as the workload runs in AWS.

AWS workload protection is now supported for migration and failback purposes, with the following consideration:
■ Consistent recovery of applications writing to multiple disks is supported with the Move operation only and is not guaranteed with the live or Test Failover operation.

Prerequisites when Replicating To and From AWS

Using Re-IP:
ZertoTools is required for the protection of Windows machines.

In this release, ZertoTools is required for protecting VMs running Windows operating systems in VMware, while AWS is the recovery site platform.

ZertoTools enable Re-IP upon failback to on-premises VMware site. Moreover, it is required for a successful failback to on-premises site when using the “zImport for all volumes” recovery method, when recovering to AWS.

Download the tool from the following location: https://www.zerto.com/myzerto/support/downloads/

AWS quota requirements:
AWS quota requirements are outlined in Zerto Virtual Replication - Prerequisites & Requirements for Amazon Web Services (AWS).

Replication to, from, and between Azure and AWS
Workload mobility between Azure and AWS sites is now supported, meaning workloads can be protected and moved from Azure to AWS, and AWS to Azure.

See Azure and AWS for known issues and considerations.

See myZerto > Technical Documentation for any additional considerations or known issues.

Recovery Operations
■ Failover Test (FOT) Resiliency: In the event of disconnection between the ZVM, VRA or hypervisor when stopping FOT, or rolling back from a Move/FOL before commit operation, the system will no longer hang in an unknown state. Instead, the
Zerto Virtual Replication v6.0 Update 1

ZVM will display a system alert and show a proper state. Once the disconnection is resolved, the user will be able to successfully stop the FOT, or roll-back from a Move/FOL before the commit operation.

- Keep VM UUID: We now allow customers to keep the VM BIOS UUID after failing over.
  - VM UUID preservation is not supported when replicating from or to public cloud.
  - VM UUID preservation is not supported for cross replication, Hyper-V to VMware.
- Zerto now prevents users from taking snapshots and creating clones of test VMs, as a clone of a test VM is not consistent.
- Zerto now prevents users from taking snapshots of VRAs.
- Recovery Commit Policy: The default Commit Policy for recovery operations in "Site Settings" was changed from "Auto Commit with no timeout" to "Auto Commit with 60 minutes timeout".
  In addition, warnings were added to the recovery wizards, specifying the selected commit policy for each VPG.
- Networks with very large latency can now perform faster delta syncs, up to the speed allowed by the disk rate and the rate the CPU calculates the md5 signatures.

vCloud Director

- Enhanced the Storage Policy configuration for VPGs. This allows the user to:
  - Configure Storage Policy per Volume in supported vCD versions.
  - Specify the Journal Storage Policy.
  - Supported between ZVM 6.0 versions and above.
- Improved RTO when Guest Customization is enabled.
  - From Zerto Virtual Replication v5.5 Update 3 we improved the RTO when replicating to vCD 9, when Guest Customization is enabled.
  - In Zerto Virtual Replication v6.0, we also improved the RTO when replicating to vCD versions 8.10.1.1 and 8.20.0.2 and above, when Guest Customization is enabled.
- Zerto is gradually shifting to use vCD APIs instead of vCD SDK. As part of this change we are now collecting the environment information using vCD API.

Hyper-V

- “Hyper-V Events”, on page 8
- “Hyper-V Identifier Mapping”, on page 8
- “Collect Hyper-V Integration Tools Version from the Hyper-V Host”, on page 8

Hyper-V Events

Zerto improved the responsiveness of changes which are done in SCVMM, such as ‘add volume’, from minutes to immediate.

Hyper-V Identifier Mapping

Zerto now maps protected VMs and hosts with a VRA in SCVMM, in order to track cases where the protected VM or the host with the VRA was removed and then re-added.

In these cases, Zerto will recognize that the protected VM or Host with VRA was re-added, and will also resume the VPG from pause and/or resume the VRA from a ghost state.
- We support Host removal and VM removal.
  - Identifier Mapping for Datastore ID and VM Network is not supported in v6.0.
- Depending on the size of the environment, it might take a few minutes to identify that the Host or VM was re-added.

Collect Hyper-V Integration Tools Version from the Hyper-V Host

Zerto now allows users to configure and execute re-IP in Hyper-V, even when SCVMM is not updated with the information, and SCVMM falsely reports that IS (Integration Services) is missing.

vSphere

Up to 96TB per host: The sum of all VMDKs of all virtual machines protected on a particular ESXi was increased from 48TB to 96TB.
ZCM

ZCM now by default, disables the generation of ZSSP URLs. To enable it, in ZCM go to Settings and select Enable ZSSP URL Factory for all Sites.

Remote Upgrade for Cloud Service Providers

- Upgrade Manager: A new feature was introduced in v6.0 which allows Cloud Service Providers to remotely upgrade their end customer sites. This functionality is accessible from MyZerto > Cloud Control > Upgrade Manager tab.
  - Centralized monitoring: Allows Cloud Service Providers an overall view of all their end customers’ ZVR versions.
- Improved service of CSP customers: Cloud Service Providers will be able to keep their customers Zerto Virtual Replication software always up to date.
- Data Protection always-on: Upgrading of Cloud environments is now facilitated by keeping the end customer up-to-date with a compatible version to the provider.
- Recommended Version: The latest version that the customer site can be upgraded to, so it will maintain compatibility with its peer cloud sites.
- Remote upgrade: The Upgrade Manager will enable remote upgrade of end customers Zerto Virtual Replication.
  - Remote upgrade functionality is permitted when:
    - The customers ZVR instance is paired to a CSP-deployed ZCC and does not have a perpetual license applied.
    - Online Services is enabled on both the CSP ZVR instance and the remote customer instance (enabled by default).
    - The end customer ZVR instance has port 443 opened.
  - Prerequisites:
    - The customer’s ZVM is v6.0 or above, or v5.5U4.
  - Considerations:
    - Zerto Recommended Version is based only on the Zerto Virtual Manager version. It does not include VRA versions.
    - Prior to the Remote Upgrade operation, the Cloud Service Provider administrator should verify that the end customer VRAs and ZVMs are the same version.
    - VRAs are automatically upgraded with the Zerto Virtual Manager. Users cannot upgrade the VRAs only via the application.
    - The logged-in Cloud Service Provider needs permissions to preform Remote Upgrade, otherwise the Remote Upgrade option is disabled.
    - Users are unable to stop or rollback the Remote Upgrade operation once it has started; the operation begins following a user clicking Upgrade on the confirmation pop up message.
    - Cloud Service Providers with Zerto Virtual Replication versions 5.0x and 5.5x will be able to benefit from the centralized monitoring view of all their end customers’ Zerto Virtual Replication versions, but Recommended Version details will not appear. In addition, they will not have the option to Remote Upgrade.
    - The end customer site displayed in the new ‘Upgrade Manager’ tab is based on the pairing to the Cloud Provider site. In some cases an end customer will appear without a site. (The details are filled once a VPG is created for the end customer).

Offsite Backup Improvements

Backup resiliency and reliability: Improved backup resiliency and reliability by breaking up the backup file into smaller files, then writing them synchronically while adding a retry mechanism.

Additionally, we removed the compression setting from existing and new repositories.
File Level Restore

“JFLR Installation Optimizations”, on page 10
“File and Folder Restore - Display Unsupported Items”, on page 10
“JFLR Support of Linux VMs”, on page 10

JFLR Installation Optimizations
The Zeus driver was removed from the Zerto Virtual Replication installation.

File and Folder Restore - Display Unsupported Items
Up until now unsupported items were filtered out. Starting from Zerto Virtual Replication version 6.0 unsupported partitions, folders and files are visible in the User Interface, but will be grayed out and disabled for selection. When hovering over unsupported items, additional data will appear with the reason why the item cannot be selected for restore.

JFLR Support of Linux VMs
JFLR now supports Linux based virtual machines, using a file system reader developed explicitly for this purpose.
For more information on The File and Folder Recovery Process, and supported operating and file server systems in Zerto Virtual Replication v6.0, see the Interoperability Matrix.

Scaling
We raised the number VMware VMs that are supported on a single ZVM from 5,000 VMs to 10,000 VMs.

VPG
Zerto has improved performance by optimizing concurrent VPG operations. This is achieved by multiple changes such as:
- Modification to the lock mechanism which replaced some global level locks to being per VPG/VM, and thus increasing rate tasks performed in parallel.
- Performance optimization with the code used to interact with vSphere.
- Increased some ZVM concurrency configuration defaults to enable a higher concurrency rate.

These optimizations result in:
- Reduced duration when VPGs are created concurrently (for example when they are created using import).
- Reduced overall duration when failing over several VPGs to vSphere concurrently.
Resolved Issues - Version 6.0

- “Resolved Issues: Hyper-V", on page 11
- “Resolved Issues: vCenter", on page 11
- “Resolved Issues: Azure", on page 12
- “Resolved Issues: VRA", on page 12
- “Resolved Issues: ZCM", on page 13
- “Resolved Issues: File Level Restore", on page 14
- “Resolved Issues: General", on page 14

Resolved Issues: Hyper-V

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>105884</td>
<td>Collection of SCSI data was optimized to resolve an issue where some of the VMs were not available for protection in large scale environments.</td>
</tr>
<tr>
<td>106030</td>
<td>Fixed an issue where the agent logs successfully collect data from the hosts so that the VM location of its volumes point to the same storage as defined in SCVMM with the same domain.</td>
</tr>
<tr>
<td>106728</td>
<td>Resolved a domain name configuration issue between the Hyper-V host and the SCVMM, which was causing some VMs to not recognize a recovery host or datastore when adding them to a VPG.</td>
</tr>
<tr>
<td>106311</td>
<td>When replicating from Hyper-V, we added support for VMs with Windows Server 2016 operating systems.</td>
</tr>
<tr>
<td>106728</td>
<td>Unavailable hosts caused VRA installation to a Hyper-V host to fail. These hosts are now skipped, and only available hosts are displayed.</td>
</tr>
</tbody>
</table>

Resolved Issues: vCenter

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>00106085</td>
<td>Resolved a synchronization issue between Cloud Providers recovery sites and their peers, where under some circumstances ZCC SSH connection failed.</td>
</tr>
<tr>
<td>105215</td>
<td>Fixed an issue that occurred on VMs with snapshots so that the original VMDK file is always returned after a failover or VPG move operation. This is so that VPG configuration is maintained after the failover or move.</td>
</tr>
<tr>
<td>107715</td>
<td>Resolved an issue where some VMs were not booting during recovery operations in a failover test due to the vm boot disk scsi0 not being the one with the lowest pciSlotNumber.</td>
</tr>
</tbody>
</table>
## Resolved Issues: Azure

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>106821</td>
<td>Resolved an issue which could occur when attempting to delete the auto generated blobs, after the user tried to delete the VM from Azure. This was caused by an incorrect comparison of the storage accounts' location when ZVR filtered the storage accounts in the proper subscription and location.</td>
</tr>
<tr>
<td>106821</td>
<td>Resolved an issue collecting the ZCA storage account information in the reflection, which caused initial sync to fail when performing failover commit from Hyper-V to Azure with reverse protection</td>
</tr>
</tbody>
</table>

## Resolved Issues: VRA

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>98046</td>
<td>Resolved an issue which caused a VRA to disconnect from an active peer VRA. This issue occurred when there were many unreachable peer VRAs.</td>
</tr>
<tr>
<td>100691</td>
<td>Resolved an issue where the ZVM set a critical checkpoint that was older than the earliest checkpoint, which caused the VRA to crash.</td>
</tr>
<tr>
<td>00013220</td>
<td>Resolved an issue where VRA gets stuck when it is restarted during live failover, which was caused by failover live or failover move VMs producing very high IO traffic.</td>
</tr>
<tr>
<td>21235</td>
<td>Corrupt journal data was causing the VRA to crash repeatedly.</td>
</tr>
<tr>
<td>21254</td>
<td>Now when corrupt journal data is detected, the VPG goes into a terminal error state and the other VPGs continue functioning.</td>
</tr>
<tr>
<td>87488</td>
<td>Bitmap sync performance was improved.</td>
</tr>
</tbody>
</table>
## Resolved Issues: ZCM

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>105616</td>
<td>Fixed several issues with the Resource Report not being generated.</td>
</tr>
<tr>
<td>107257</td>
<td></td>
</tr>
<tr>
<td>108711</td>
<td></td>
</tr>
<tr>
<td>110267</td>
<td></td>
</tr>
<tr>
<td>109569</td>
<td>Resolved issues where in some cases the user was unable to edit or remove Service Profiles in ZCM.</td>
</tr>
</tbody>
</table>
### Resolved Issues: File Level Restore

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>105632</td>
<td>File Level Restore issues associated with Zeus driver, such as failure to mount the driver, and some file recovery failures, were resolved. The Zeus driver was removed from the ZVR installation.</td>
</tr>
<tr>
<td>87637</td>
<td>Resolved several issues with dependency on the recovery ZVM operating system version during File Level Restore operations. Issue was resolved by removing dependency on Zeus driver.</td>
</tr>
<tr>
<td>106430</td>
<td>File Level Restore issues related to the Zeus driver were resolved. The Zeus driver was removed from the ZVR installation.</td>
</tr>
</tbody>
</table>

### Resolved Issues: General

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>112998</td>
<td>Fixed an issue that caused the VRA upgrades to fail after upgrading to ZVR 6.0, where different entities in vCenter have duplicate names. <strong>Note:</strong> Relevant from version 6.0P1</td>
</tr>
<tr>
<td>113069</td>
<td>Large scale environments: Resolved an issue where the ZVM's &quot;IO write&quot; to disk is relatively high, due to massive amount of fully occupied journals.</td>
</tr>
<tr>
<td>113018</td>
<td>Added a constraint to the database to avoid two entries for the same ZVM task, which could have caused the ZVM to fail when starting up.</td>
</tr>
<tr>
<td>112926</td>
<td>Resolved an issue which sometimes caused outdated information to be presented in the ZVM Dashboard, and in the VPG details graphs.</td>
</tr>
<tr>
<td>112961</td>
<td>Improved performance when multiple test failovers are running in parallel.</td>
</tr>
<tr>
<td>113049</td>
<td>The Zerto Conversion storage tool was enhanced so that migrating ZVM to an external SQL instance no longer causes issues relating to localization.</td>
</tr>
<tr>
<td>112990</td>
<td>NIC information is now written correctly when exporting a VPG List report.</td>
</tr>
<tr>
<td>113118</td>
<td>Fixed an issue with Remote Log Collector filenames, which was causing the RLC to generate an empty ZIP file.</td>
</tr>
<tr>
<td>84898</td>
<td>Empty and corrupted .FBAK files no longer cause failure to restore other backups in the same repository.</td>
</tr>
</tbody>
</table>
## Issues Resolved in Version 6.0

<table>
<thead>
<tr>
<th>CASE NUMBER</th>
<th>ISSUES RESOLVED IN VERSION 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>106132</td>
<td>Updated the Edit VPG wizard so that if the user changes the vNIC IP configuration, and if there is partial or incorrect data in the text fields, the user will not be able to save the new vNIC IP configuration.</td>
</tr>
<tr>
<td>89360</td>
<td>Clustered environments: Fixed an issue which caused the default target location to be empty, when setting the default target location to a datastore cluster.</td>
</tr>
<tr>
<td>92203</td>
<td>The DB conversion tool no longer shows the password in clear text. In addition, communication problems are detected and reported.</td>
</tr>
<tr>
<td>86561</td>
<td>Updated GUI tooltips to clarify the Bandwidth Regulator feature in the Site Settings window and Edit VRA window. The Bandwidth Regulator lets you assign different VRAs to separate groups, where each VRA group gets its own bandwidth.</td>
</tr>
<tr>
<td>95162</td>
<td>The alerts counter in the ZVM GUI now decreases when alerts are acknowledged.</td>
</tr>
<tr>
<td>6039</td>
<td>Fixed an issue which caused the VPG to go into an error state after Stop Failover Test failure.</td>
</tr>
<tr>
<td>00021174</td>
<td>Resolved an issue where the ZVM disconnected from the VRAs, by adding a timeout to updating port mapping in the ZCC routing table.</td>
</tr>
<tr>
<td>00007913</td>
<td>Resolved several VPG sync issues.</td>
</tr>
</tbody>
</table>
Known Issues

The following are known issues when using Zerto Virtual Replication.

- "Virtual Replication Appliance (VRA)”, on page 16
- "Virtual Protection Group (VPG) and Recovery”, on page 16
- "VPG Management”, on page 16
- "Failover, Move and Test Failovers”, on page 17
- "vCenter Server”, on page 17
- "vCloud Director”, on page 17
- "VMware VSphere”, on page 18
- "Hyper-V”, on page 18
- "AWS”, on page 19
- "Azure”, on page 19
- "Cross-Replication”, on page 20
- "VMware to Hyper-V Cross-Replication”, on page 20
- "Hyper-V to VMware Cross-Replication”, on page 21
- "Remote Upgrade for Cloud Service Providers”, on page 21
- "APIs”, on page 21
- "File Level Restore”, on page 21
- "Offsite Backup Improvements”, on page 22
- "Upgradeability”, on page 22
- "General”, on page 22

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.
- 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.

VPG Management

- If a VM is removed from the hypervisor inventory, Zerto Virtual Replication 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.
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

- 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.
18 Known Issues

Release Notes for Zerto Virtual Replication v6.0 Update 1

- 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.

- Improved RTO when replicating to vCD 9 and Guest Customization is enabled, by avoiding a redundant VM power on and off, which was used by vCD to identify whether VMTools were installed on the VM.

- 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

- If the user restores a VM from a snapshot, Zerto does not automatically synchronize the changes to the recovery site. The user needs to manually Force Sync the VPG.

- The ZVM triggers a warning event for VM restoration from snapshot only in vSphere in all versions except of VC 6.5 and 6.5a.

- vSAN 6.6: When performing Failover or Clone operations, an error appears under Tasks and Events, even though the operation completed successfully.
  The error message that appears is: "Partial success: For VM <vm name>, The disk located in <vmdk path> was not moved to the target location at <vmdk path>.

Hyperl-V

- Zerto Virtual Replication script parameters use vSphere terminology, even for scripts in a Microsoft Hyper-V environment.

- 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.

- 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.
Known Issues

AWS

- If reverse protection is selected on a recovery volume that is larger than the protected volume, the protected volume cannot be used for preseeding during a move or a failover operation. A Delta Sync will also not be possible and an Initial Sync will have to be performed.

- Tagged checkpoints, Force Sync, One-to-Many and Offsite Backup functionalities for VPGs with AWS as the protected site are not supported.
- Preseed to AWS is not supported.
- Restore from backup is not supported for VPGs with AWS as their recovery site.
- When using zImport, the disk type is io1 and cannot be configured.
- Only the ZCA’s Availability Zone (AZ) can be used for faster recovery.
- The instance zASA, and the temporary instances, zImporter and zSATs, require internet access.
- The zImporters, zSATs and zASA are created with a public IP. However, they are connected to a newly created security group.
- When using Zerto import for all volumes, the following Operating Systems are **not** supported:
  - Red Hat Enterprise Linux (RHEL) 7.0
  - CentOS 7
  - Ubuntu 13.10
  - SUSE 12
  - Solaris 11.2
- The default c4.8xlarge AWS EC2 maximum instance quota is 20 (default value). To ensure scalability, you must contact AWS support to increase the maximum relatively to the number of protected volumes.
- The default m4.large AWS EC2, used for zSATs and zASA, maximum instance quota is 20 (default value). To ensure scalability, you must contact AWS support to increase the maximum relatively to the number of protected volumes.
- GPT cannot be used as the boot disk.
- Recovery to AWS using “zImport for all volumes” requires installing drivers on the production VM.
- 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.
- Recovery of Windows VMs will freeze when using AWS import method with the PV driver installed.

Azure

The following limitations apply:

- 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 recommended 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.
- For Virtual Machines to be protected in Azure, the VMs’ volumes must reside in the Standard Storage Account (Zerto Storage Account) that was defined during its installation.
- VMs which are not deployed via the Azure Resource Manager cannot be protected from Azure.
- You cannot protect machines that have a disk larger than 4TB.
- The protected virtual machines needs to have at least one NIC.
- 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 backup is not supported.
- Zerto Virtual Replication APIs are not supported.
- Azure temp drive is not protected by Zerto (Azure limitation).
- Use Move operation in order to failback from Azure.
- The minimum RPO from Azure is 1 minute.
- Offsite Backup is not supported for “From Azure” VPGs.
- Resizing protected disks on Azure is not supported.
- Reverse protection VM network settings in a VPG are not saved when failing over a VPG from Azure.
Known Issues

Release Notes for Zerto Virtual Replication v6.0 Update 1

- Multi-tenant vCenter and vCD environments are not compatible with Azure ZCA.
- 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

For example, see the following default values:
- 20 cores per subscription
- 200 Storage accounts per subscription
- 20 VMs per region per subscription
- VM per series (Dv2, F, etc.) cores per subscription 201 per Region

Additionally, see the following example for maximum values:
- A standard storage account has a maximum total request rate of 20,000 IOPS. The total IOPS across all of your virtual machine disks in a standard storage account should not exceed this limit.

<table>
<thead>
<tr>
<th>VM Tier</th>
<th>Basic Tier VM</th>
<th>Standard Tier VM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk size</td>
<td>1023 GB</td>
<td>1023 GB</td>
</tr>
<tr>
<td>Max 8 KB IOPS per persistent disk</td>
<td>300</td>
<td>500</td>
</tr>
<tr>
<td>Max number of disks performing max IOPS</td>
<td>66</td>
<td>50</td>
</tr>
</tbody>
</table>

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.
- 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 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.
- 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 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.
- 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.

Remote Upgrade for Cloud Service Providers

- Remote upgrade:
  - Upgrade of cloud sites that support Intra-Cloud Disaster recovery is not supported.
  - Remote upgrade functionality assumes that both the Cloud Service Providers version and the customers Zerto Virtual Replication version is v6.0 or above, or v5.5U4.
  - VSS installers are not supported. Remote Upgrade should be used to download only non-VSS versions.

APIs

- Support of VPG Settings APIs when Creating VPGS from vCD to vCD:
  - VC > vCD is not supported
  - 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.

File Level Restore

- In Linux EXT file system, only file and folder names encoded as UTF-8 or 7-bit ASCII are supported.
- If the Windows virtual machine with files to be restored uses dynamic disks, files cannot be restored from these disks.
- You can only recover files or folders when an offsite backup is not running.
- Journal File Level Restore (JFLR) is not supported with the vSphere plugin.
- File Level Restore (JFLR) is not supported on a volume where data deduplication is enabled.
Offsite Backup Improvements

- **Backup resiliency and reliability:**
  - The time it takes to generate a backup, and then to restore it may be slightly slower compared to previous versions.
  - It is recommended to use weekly backups and not daily backups.
  - It is recommended to schedule the backups to start at different days and times to balance the work.

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.

General

- 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.
- 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.
- When replication is to a VSAN, disk space used by the journal is not deallocated when the journal size decreases.
- Protecting CD/DVD drives is not supported.

Known Issues

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. Replacing multiple legacy solutions with a single IT Resilience Platform, Zerto is changing the way disaster recovery, data protection and cloud are managed. With unmatched scale, Zerto’s software platform delivers continuous availability for an always-on customer experience while simplifying workload mobility to protect, recover and move applications freely across hybrid and multi-clouds. Zerto is trusted by over 6,000 enterprise customers globally, and is powering resiliency offerings for Microsoft Azure, IBM Cloud, AWS, Sungard and more than 350 cloud services providers.

Learn more at Zerto.com
Copyright © 2018, Zerto Ltd. All rights reserved.