Zerto

Zerto Analytics

Rev01 U3
Jan 2020
ZVR-ZA-7.5

© 2020 Zerto All rights reserved.

Information in this document is confidential and subject to change without notice and does not represent a commitment on the part of Zerto Ltd. Zerto Ltd. does not assume responsibility for any printing errors that may appear in this document. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without the prior written permission of Zerto Ltd. All other marks and names mentioned herein may be trademarks of their respective companies.

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

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

ZVR-ZA-7.5

Table of Contents

Introduction to the Zerto Solution 4

What is the Zerto Solution? 4
Benefits of using the Zerto Solution 5
The Zerto Solution architecture 10
How Zerto Recovery Works 12

Zerto Analytics - overview and use 14

Before getting started with Zerto Analytics 15
Accessing the Zerto Analytics Portal 15
Accessing Zerto Mobile 15
Accessing Zerto Analytics APIs 16
Navigating the Zerto Analytics Portal 16
End-User Analytics for Service Providers 18
Zerto Analytics product feature matrix 18
Planning your data protection 19
Zerto Analytics secure architecture 20

Zerto Cloud Control - overview 30

Before getting started with Zerto Cloud Control 30
Accessing the Zerto Cloud Control 30
Using Upgrade Manager 30
Using Tenants 31

Introduction to the Zerto Solution

Disaster recovery is the process of preparing for recovery or continuation of IT processing tasks that support critical business processes in the event of a threat to the IT infrastructure. Zerto's Long Term Retention is the additional process of enabling recovery of IT processing tasks after an extended period. This section describes Zerto general concepts to enable replication and recovery in a virtual environment.

The following topics are described in this section:

- What is the Zerto Solution? on page 4
- Benefits of using the Zerto Solution on page 5
- The Zerto Solution architecture on page 10
- How Zerto Recovery Works on page 12
- Zerto Analytics - overview and use on page 14
- Zerto Cloud Control - overview on page 30

What is the Zerto Solution?

IT Resilience Platform™

Zerto's IT Resilience Platform™ converges disaster recovery, backup, and workload mobility whether on-premises or to, from and between hybrid and multi-cloud platforms. The platform is built on a foundation of continuous data protection (CDP) with built-in orchestration and automation providing IT leaders with simplicity, enterprise scale and agile data protection to save time, resources and costs. Analytics, with intelligent dashboards and live reports, provides complete visibility across multi-site and multi-cloud environments, giving organizations confidence that business service levels and compliance needs are met.

Disaster Recovery

Zerto is built from the ground up to be the simplest, most powerful disaster recovery solution for virtualized infrastructures. By including all the replication, recovery orchestration and automation in one simple software platform, users can recover one, all or a subset of virtualized applications, from anywhere to anywhere, maximizing the benefits of virtualization and cloud.

Through native integration into all supported platforms, Zerto not only allows replication and recovery between any storage, but it also protects across and between multiple hypervisors and public cloud platforms. This market-leading technology delivers a best of breed Business Continuity/Disaster Recovery (BC/DR) solution irrespective of underlying hypervisor, public cloud or storage.

Zerto supports replication between VMware vSphere, Microsoft Hyper-V, Microsoft Azure, Amazon Web Services (AWS), and IBM Cloud. Zerto is the underpinning technology of hundreds of Cloud Service Providers (CSPs) globally who are leading the way in delivering Disaster Recovery as a Service (DRaaS) capabilities.

Backup

Elastic Journal

The Zerto Elastic Journal is a new concept in data protection bringing together both short-term retention and long-term retention capabilities. Using unified data protection workflows, powered by intelligent index and search, it enables quick recovery of data - regardless of whether it's from a few seconds ago or a few years ago. Data gets copied from the short-term retention storage into the long-term retention repositories. As the short-term retention is already stored on the target side, moving data to long-term retention has no impact on production, so copies can be taken as often as needed, eliminating the concept of "backup windows".

Workload Mobility

Workload mobility is the ability to move workloads to, from and between multiple platforms, on-premises or cloud, with minimal business impact and no traditional infrastructure constraints. With the recent rise of cloud computing, there is now a plethora of cloud platforms to choose from, with large players such as Microsoft Azure, AWS and IBM Cloud as well as plenty of Cloud Service Providers (CSPs). Each of these platforms have their own attributes which make them suited to certain workloads, whether through compliance, pricing or otherwise. Despite this, the cloud is not always the right option for all workloads, and because of this, the traditional on-premises deployments with VMware vSphere or Microsoft Hyper-V are still prevalent. Ultimately, having all of these options has led to increasing adoption of a multi-cloud and/or hybrid cloud strategy. Organizations are challenged to ensure that workloads, whether in the cloud or on-premises, are not locked into any one platform or vendor, and can be moved around based on where they fit best today, rather than yesterday. This is where workload mobility comes in, removing the traditional lock-in to these platforms and allowing workloads to be moved across platforms seamlessly, on-premises or in the cloud, including the ability to validate mobility prior to the live event without production impact.

Zerto supports any-to-any mobility between VMware vSphere, Microsoft Hyper-V, AWS, IBM Cloud, Microsoft Azure and any of our hundreds of Zerto-powered Cloud Service Providers (CSPs). For a full list of supported platforms and their versions, see our Interoperability Matrix.

Benefits of using the Zerto Solution

Datacenter optimization and virtualization technologies have matured and are now commonly used in IT infrastructure. As more applications are deployed in a virtualized infrastructure, there is a growing need for recovery mechanisms that support mission critical application deployments while providing complete BC and DR.

Traditional replication and disaster recovery solutions were not conceived to deal with the demands created by the virtualization paradigm. For example, most replication solutions are not managed in the hypervisor layer, considering the virtual machines and disks, but at the physical disk level. Hence they are not truly virtualization aware.

The lack of virtualization awareness creates a huge operational and administrative burden. It also results in operational inflexibility. The Zerto solution has been designed to resolve these issues by being fully virtualization aware.

See the following topics:

- (On-premise environments) Fully Virtual – Sits in the Hypervisor or Cloud on page 6
- Hardware Agnostic on page 6
- (On-premise environments) Hypervisor Agnostic on page 7
- Benefits to Using Zerto Enterprise Government Edition on page 7
- Focus is on the Application, Not the Physical Storage on page 7
- Compatibility Across Virtual Environments – Cross-Hypervisor Platform and Version Agnostic on page 7
- (On-premise environments) Fully Scalable on page 8
- Efficient Asynchronous Replication on page 8
- One-Click Failover and Control of the Recovery Process on page 8
- One-Click Migration on page 8
- File and Folder Recovery on page 9
- (On-premise environments) Long Term Retention on page 9
- Policy-based on page 9
- Minimal RPO on page 9
- WAN Optimization Between Protected and Recovery Sites on page 9
- WAN Resilience on Both the Protected and Recovery Sites on page 10
- DR Management Anywhere on page 10

(On-premise environments) Fully Virtual – Sits in the Hypervisor or Cloud

On-Premise Only

Zerto software sits in the hypervisor level. Protection groups are configured with virtual machines and virtual disks, without the need to consider the physical disks.

Hardware Agnostic

ALL Platforms

Because the Zerto solution manages recovery of virtual machines and virtual disks only, it does not matter what hardware is used in either the protected or recovery sites; it can be from the same vendor or different vendors. With the Zerto solution, the logical storage is separated from the physical storage so that the vendor and actual type of storage hardware do not need to be considered.

Zerto provides a workload mobility and protection layer providing seamless connectivity, portability, protection, orchestration, and application encapsulation of workloads across clouds without vendor lock-

in. High scale, mission critical applications, and data are encapsulated, as well as features, specifications, and configurations, and can be seamlessly migrated across different servers, storage, hypervisors, and clouds without any disruption to business services.

With Zerto, IT managers can choose the right infrastructure for the right use case for the right price. One application can leverage several different environments for disaster recovery, bursting, production, retention, testing, and development. With Zerto there is no vendor lock-in to a cloud, technology, or vendor. Any choice, any cloud, any technology, any price, any service level is available in minutes for any workload.

(On-premise environments) Hypervisor Agnostic

On_Premise Only

Zerto runs both in VMware vCenter Server and Microsoft SCVMM. It is compatible with VMware hypervisor management features, such as vMotion and Microsoft hypervisor management features, such as Live Migration.

Benefits to Using Zerto Enterprise Government Edition

The Zerto Enterprise Government Edition (EGE) leverages vSphere APIs for IO (VAIO) framework. The key benefit of vSphere's VAIO framework is certification of the Zerto VAIO VMware Installation Bundle (VIB). With the certified VAIO VIB, Secure Boot can be used for hosts with protected VMs without exposing root credentials. Additionally, cluster level installation of the Zerto VRAs is provided.

> Note: For Zerto Enterprise Government Edition (EGE) documentation, go to the guide *Installing Zerto in On-Premise Environments*, in the section Deploying Zerto Enterprise Government Edition.

Focus is on the Application, Not the Physical Storage

ALL Platforms

By considering the physical disk level and not the virtual disk level, traditional replication is not truly application aware. Even virtual replication recovers block writes at the SCSI level and not at the application level. Zerto is truly application focused, replicating the writes from the application in a consistent manner.

Compatibility Across Virtual Environments – Cross-Hypervisor Platform and Version Agnostic

ALL Platforms

Zerto enables replication across multiple hypervisor managers, such as VMware vCenter Server and Microsoft SCVMM, and to public clouds such as Amazon Web Services (AWS) or Microsoft Azure. You can protect virtual machines in one hypervisor platform and recover to a different hypervisor platform. This feature can also be used to migrate virtual machines to a different hypervisor platform.

Also, virtual machines running in one version a hypervisor can be recovered in a different version of the same type of hypervisor, as long as Zerto supports the hypervisor versions, virtual machines can be protected across versions.

(On-premise environments) Fully Scalable

On-Premise Only

Zerto enables defining software-only Virtual Replication Appliances (VRAs) on each hypervisor host to manage the replication of virtual machines on that host. Increasing the number of hypervisor hosts is handled by defining a new VRA on each new host. There is no need to install additional software to the hypervisor management tool, such as VMware vCenter Server or Microsoft SCVMM, to handle additional hosts or virtual machines and no need to consider additional hardware acquisitions.

Efficient Asynchronous Replication

ALL Platforms

Writes are captured by the Zerto software in the hypervisor level, before they are written to the physical disk at the protected site. These writes are sent to the recovery site asynchronously, thus avoiding long distance replication latency for the production applications.

Also, because these writes are captured and sent to the recovery site, it is only the delta changes and not the whole file or disk that is sent to the recovery site, reducing the amount of network traffic, which reduces WAN requirements and significantly improves the ability to meet both RPO and RTO targets.

One-Click Failover and Control of the Recovery Process

ALL Platforms

When recovery is required, the administrator clicks on a button in the Zerto User Interface to initiate failover. This means that controlling the start of a recovery remains in the hands of the administrator, who can decide when to initiate the recovery and, by selecting a checkpoint, to what point-in-time to recover to.

One-Click Migration

ALL Platforms

Application migrations can be resource intensive projects that take weeks of planning, execution, and downtime. With Zerto migrations are greatly simplified and can be completed without extended outages or maintenance windows and across different types of hardware and even different hypervisors, such as VMware ESXi or Microsoft Hyper-V. Migrations across different versions within a type of hypervisor, such as from a VMware vCenter environment to a vCloud environment or even cross hypervisor migration, such as migration from a vCenter environment to a Hyper-V environment is as easy as a migration from one site to another using the same hypervisor infrastructure.

File and Folder Recovery

ALL Platforms

You can recover specific files and folders from the recovery site for virtual machines that are being protected by Zerto and running Windows or Linux 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 folders from the recovery site.

(On-premise environments) Long Term Retention

Zerto provides a Retention option that enables saving the protected virtual machines for up to one year in a state where they can be easily deployed. Because retention uses the same mechanism used for disaster recovery, there is no performance impact on the production site, since the processing is performed on the recovery site. The data copied for retention are fixed points saved daily, weekly or monthly.

Note: Zerto recommends **weekly** retention sets.

Policy-based

ALL Platforms

In the protected site you define the virtual machines that you want to recover, either individually or as groups, as a virtual protection group (VPG). The virtual machines that you include in the VPG can come from one or more hypervisor hosts. In this way, you can protect applications that run on multiple virtual machines and disks as a single unit, in a single VPG.

Minimal RPO

ALL Platforms

The Zerto solution utilizes continuous data protection, sending a record of every write in the virtual protection group to the recovery site. The transfer of this information is done over an optimized WAN asynchronously. If recovery is required, all the data that was transferred to the recovery site is available resulting in recovery within the requested RPO.

WAN Optimization Between Protected and Recovery Sites

Using compression to minimize bandwidth and other techniques such as throttling to prioritize network traffic to reduce the impact on day-to-day operations, you can make sure that the communication between the protected and recovery sites is fully optimized.

The Zerto solution also uses signature matching to reduce the amount of data sent across the WAN. During synchronization of the protected site and recovery site for every virtual machine in a VPG, Zerto maintains a map of disk sectors so that if there is a need to resynchronize sites, the map signatures can be used to ensure that only data where changes occurred are passed over the WAN.

WAN Resilience on Both the Protected and Recovery Sites

ALL Platforms

The Zerto solution is highly resilient to WAN interruptions. In order to reduce storage overhead used for replication purposes, on WAN failure or when the load over the WAN is too great for the WAN to handle, Zerto starts to maintain a smart bitmap in memory, in which it tracks and records the storage areas that changed. Since the bitmap is kept in memory, Zerto does not require any LUN or volume per VPG at the protected side. The bitmap is small and scales dynamically, but does not contain any actual IO data, just references to the areas of the protected disk that have changed. The bitmap is stored locally on the VRA within the available resources. Once the WAN connection resumes or the load returns to normal traffic, Zerto uses this bitmap to check whether there were updates to the protected disks and if there were updates to the disks, these updates are sent to the recovery site.

DR Management Anywhere

ALL Platforms

With the Zerto solution everything is managed from a standalone browser-base user interface, enabling disaster recovery management from anywhere using any device.

The Zerto Solution architecture

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

Zerto helps customers accelerate IT transformation by eliminating the risk and complexity of modernization and cloud adoption. By replacing multiple legacy solutions with a single IT Resilience Platform™, Zerto is changing the way disaster recovery, retention and cloud are managed. This is done by providing enterprise-class disaster recovery and business continuity software for virtualized infrastructure and cloud environments.

In **on-premise** environments, Zerto Virtual Replication (ZVR) is installed with virtual machines to be protected and recovered.

In **public cloud** environments, Zerto Cloud Appliance (ZCA) is installed in the public cloud site that is to be used for recovery.

The installation includes the following:

- **Zerto Virtual Manager (ZVM)**: The ZVM is a Windows service, running on a dedicated Windows VM, that manages everything required for the replication between the protection and recovery sites, except for the actual replication of data. The ZVM interacts with the hypervisor management user

interface, such as vCenter Server or Microsoft SCVMM, to get the inventory of VMs, disks, networks, hosts, etc. It also monitors changes in the hypervisor environment and responds accordingly. For example, a VMware vMotion operation, or Microsoft Live Migration of a protected VM from one host to another is seen by the ZVM, and the Zerto User Interface is updated accordingly.

  - For the maximum number of virtual machines, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

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

  - For the maximum number of volumes, either being protected or recovered to that site, see Zerto Scale and Benchmarking Guidelines.

- **Virtual Backup Appliance (VBA)**: A Windows service that manages File-Level Recovery operations within the Zerto solution.

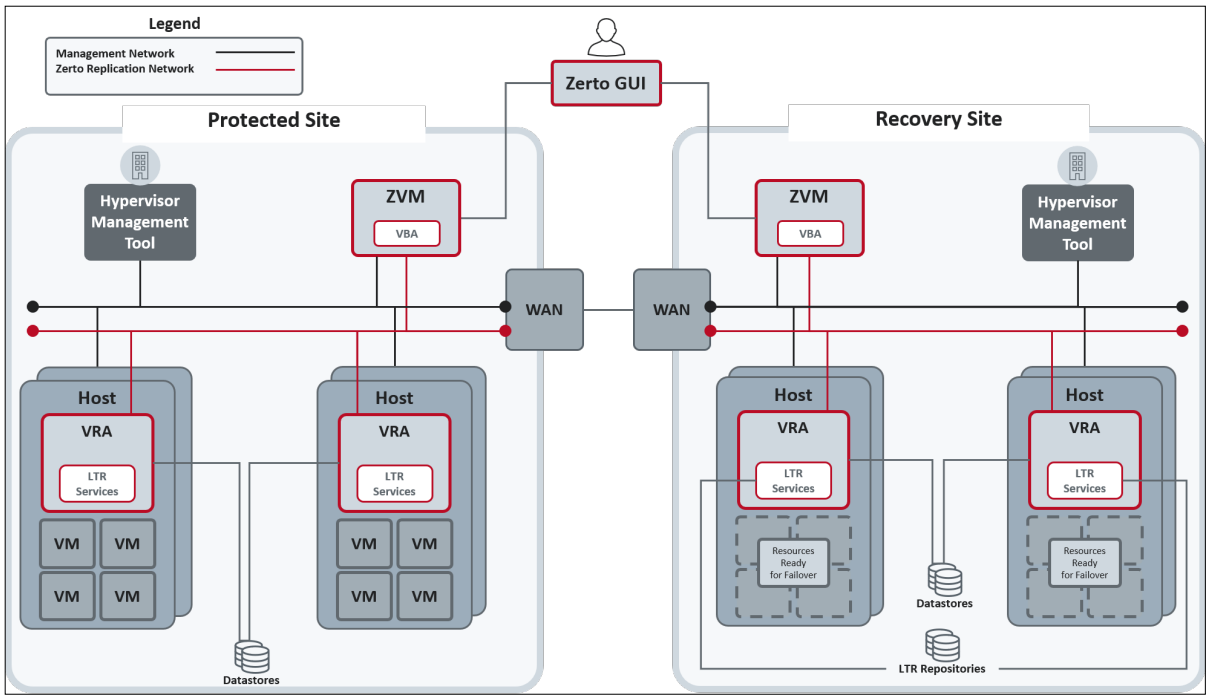
- **Zerto User Interface:** Recovery using the Zerto solution is managed in a browser or, in VMware vSphere Web Client or Client console.

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

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

The following diagram shows how the main Zerto components are deployed across hypervisor-based enterprise sites to provide disaster recovery across these sites.

> Note: For the architecture diagrams when one of the sites is a Cloud Service Providers (CSPs), see *Zerto Cloud Manager Administration Guide*.



When you plan to recover the enterprise site to a public cloud, ZCA is installed in the cloud environment. ZCA comprises the same components but the VRA runs as a service, so that the ZVM, VRA, and VBA all run as services on a single virtual machine instance in the public cloud.

How Zerto Recovery Works

Installing Zerto Virtual Replication installs the Zerto Virtual Manager, which sits in the hypervisor layer on the enterprise site. You manage the Zerto Virtual Manager, one on each of the protected and recovery sites, using the Zerto User Interface.

Zerto also provides a set of RESTful APIs and PowerShell cmdlets to enable incorporating some of the disaster recovery functionality within scripts or programs.

In the protected site you define the virtual machines that you want to replicate, either individually or together, as a virtual protection group (VPG). The virtual machines that you include in the VPG can come from one or more hypervisor hosts. In this way, you can protect applications that run on multiple virtual machines and disks as a single unit – a VPG. An example of an application that runs on multiple virtual machines includes software that requires a web server and database, both of which run on virtual machines different than the virtual machine where the application software runs.

A virtual machine can be included in several VPGs so that you can recover it to several sites, depending on the needs of the organization. For example the same workload can be protected to a local or a remote location as well as to the cloud. Using several recovery sites also enables migrating disaster recovery datacenters from one location to another.

> **Note:** DVD drives cannot be protected.

Every write is copied by Zerto and sent, asynchronously, to the recovery site, while the write continues to be processed on the protected site. For greater efficiency and performance, the write can be compressed before being sent to the recovery site with throttling techniques being used to prioritize network traffic.

On the recovery site the write is written to a journal managed by a Virtual Replication Appliance (VRA). Each protected virtual machine has its own journal. Every few seconds, a checkpoint is also written to each journal. These checkpoints ensure write order fidelity and crash-consistency to each checkpoint. During recovery you pick one of these crash-consistent checkpoints and recover to this point. Additionally, checkpoints can be manually added by the administrator, with a description of the checkpoint. For example, when an event is going to take place that might result in the need to perform a recovery, you can pinpoint when this event occurs as a checkpoint written to each journal.

The VRA manages the journals for every virtual machine that will be recovered to the hypervisor hosting that VRA. It also manages images of the protected volumes for these virtual machines. During a failover, you can specify that you want to recover the virtual machines in the VPG using the last checkpoint or you can specify an earlier checkpoint, in which case the recovery of the mirror images under the VRA are synchronized to this checkpoint. Thus, you can recover the environment to the point before any corruption and ignore later writes in the journal that were corrupted, regardless of the cause of the corruption, such as a crash in the protected site or a virus attack.

To improve the RTO during recovery, the user is able to start working even before the virtual machine volumes on the recovery site have been fully synchronized. Every request is analyzed and the response returned either from the virtual machine directly or from the journal if the information in the journal is more up-to-date. This continues until the recovery site virtual environment is fully synchronized, up until the last checkpoint or an earlier checkpoint, when the integrity of the protected site was assured.

When recovery to a point is required that is further in the past than the time saved in the journal, you can restore from files created during the Retention process. Retention is an extension of disaster recovery, with the virtual machine files, such as the configuration and virtual disk files, saved to a repository for up to one year. These files are then used to restore the virtual machines to the point of the stored retention sets at the recovery site.

Zerto Analytics - overview and use

Zerto Analytics allows you to track and monitor the health of your entire protected environment from browsers and mobile devices.

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

Zerto Analytics also includes **Planning**, allowing you to plan your data protection strategy.

Zerto Analytics is developed with an API first approach, therefore, everything that is presented in the GUI, is also available with APIs. The APIs are delivered with Swagger open source that help you develop and test REST integration using standardized examples. This allows to easily populate custom portals with Zerto Analytic content.

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

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

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

New Resource Planner

With Resource Planner, you can ensure your data protection needs are met as your IT environment grows and diversifies. Use the Resource Planner to monitor and perform analysis of your protected environment to determine the required compute, storage and networking resources for any or all virtual machines (VMs) within your environment, both on-premises or in the cloud. Build out your data protection strategy with 'what-if' scenario modeling to plan for VM protection across clouds or on-premises, or to transition from on premises to cloud, or to protect additional VMs within your environment.

Zerto Analytics is developed with an API first approach, therefore, everything that is presented in the GUI, is also available with APIs. The APIs are delivered with Swagger open source that help you develop and

test REST integration using standardized examples. This allows to easily populate custom portals with Zerto Analytic content.

See the following sections:

Before getting started with Zerto Analytics on page 15

Accessing the Zerto Analytics Portal on page 15

Accessing Zerto Mobile on page 15

Accessing Zerto Analytics APIs on page 16

Navigating the Zerto Analytics Portal on page 16

End-User Analytics for Service Providers on page 18

Zerto Analytics product feature matrix on page 18

Planning your data protection on page 19

Zerto Analytics secure architecture on page 20

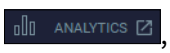
Before getting started with Zerto Analytics

Verify the following:

- At least **1 ZVM** running Zerto**5.0 or higher**.
- **Enable Zerto SaaS applications including Zerto Analytics, Cloud Control, and Mobile App.**check box is selected. This is accessed in the ZVM application in **Settings > About.**
- Internet access.
- A **myZerto** account using your corporate email address.

Accessing the Zerto Analytics Portal

Zerto Analytics is accessed from one of the following locations:

- From a URL: https://analytics.zerto.com
- From myZerto: www.zerto.com/myzerto. Sign in using your credentials and select the **Analytics** tab.
- From the ZVM Application menu tab: Click the Analytics button, 

, to open Zerto Analytics in a new browser tab.

Accessing Zerto Mobile

The Zerto Mobile app is available for both iOS or Android operating systems.

Sign in using your **myZerto** credentials.

Accessing Zerto Analytics APIs

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

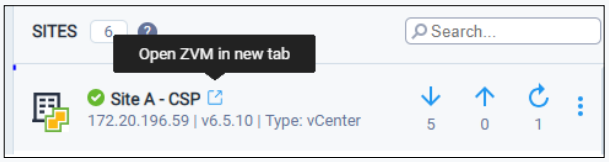
- Zerto Analytics APIs are available in OpenAPI Specification.
- The documentation can be accessed via the link: https://docs.api.zerto.com/

Navigating the Zerto Analytics Portal

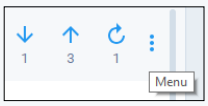
When accessing Zerto Analytics, the **Dashboard** tab opens by default. This tab displays a summary of the entire protected environment, including the average RPO and VPG health, site details and topology, active alerts, running tasks and events.

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

> Tips:
>
> - Use the sites topology to identify sites without remote protection, to identify network issues and to identify cloud issues.
> - To handle any issues in the ZVM site, in the Dashboard tab > SITES area, click the icon Open ZVM in a new tab. This routes you to the specific ZVM site.



> - In the same Sites area, click the Menu button to navigate to the VPGs, Alerts or Tasks for the specified site.



In addition to the Dashboard, there are three additional views that provide details on the overall health of your environment.

See the following sections:

1. Monitoring Alerts, Events and Tasks in Zerto Analytics on page 17
2. Troubleshooting VPGs in Zerto Analytics on page 17
3. Reviewing Reports in Zerto Analytics on page 18

Monitoring Alerts, Events and Tasks in Zerto Analytics

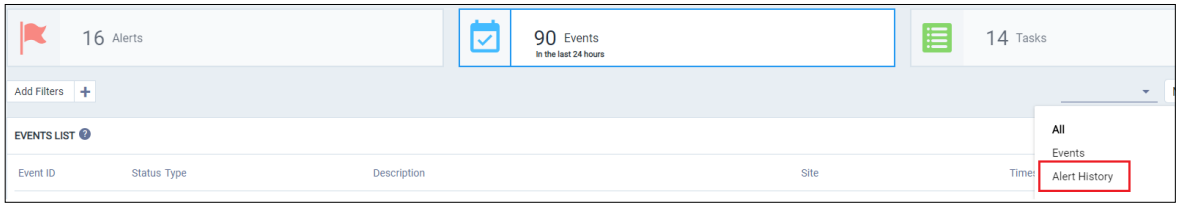
From the **Monitoring** tab review the active alerts, alerts history, running events and tasks.

To see active alerts, events or tasks from a specific ZVM, use the filter in the top left of the screen 

.

Events are displayed for the last 24 hours by default. Use the date selector to filter the Events List by date.

To view a history of alerts, select the **Events** tab and **Alert History** in the sub menu. Inactive alerts are displayed for the selected time range.

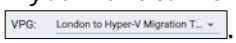


> Tip:
>
> Click the Alert ID and Event ID to open the help and view the full details for that specific alert or event.

Troubleshooting VPGs in Zerto Analytics

From the **VPGs** tab, review the list of VPGs with Errors and Warnings. In the VPGs status area, click either VPGs with Warnings or VPGs with Errors to filter the VPGs list.

To review the status of a VPG, click in the column of the VPG you want to review to open the **VPG Details** page. From here you can view the details of the virtual machines associated with the VPG as well.

If you want to view the details of another VPG, select the VPG from the VPGs drop-down list 

.

> Tip:
>
> To further investigate about a selected VPG, click the VPG History button, and select to view either the RPO, Journal or Network Reports page. (For more details about Reports, see Reviewing Reports in Zerto Analytics on page 18).

Reviewing Reports in Zerto Analytics

The Zerto Analytics reports provide real-time and historical data analysis. ECE and CSP licenses can view up to 90 days of report history. Use the date controller to filter your reports. Statistics are displayed according to the selected time frame.

> Tip:
>
> Zoom in to view more granular data by selecting and dragging your mouse over the selected time frame.

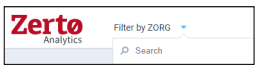
From the **Reports** tab, review the RPO, Journal and Network performance history on the VPGs.

Use the **Network** reports for reviewing the network history for any VPG or Site. You can also view the network summary for a selected time frame, the network performance history and IOPs history.

Use the **RPO** reports for viewing a summary to see if RPO SLAs are being met, the RPO history and the RPO breach table for viewing when the specific time breach occurred and the duration of the SLA breach.

Use the **Journal** reports for understanding if resilience is at risk due to journal storage capacity and plan for storage growth.

End-User Analytics for Service Providers

Service providers can filter their customers in Zerto Analytics using the ZORG filter located at the top of the screen. 

Using the ZORG filter, CSPs can see historical data and status for any individual customer.

Additionally, using the Zerto Analytics **APIs**, CSPs can create custom reports and automate reporting delivery of real-time content to their customers. The APIs can also be used to provide content for customer portals.

Zerto Analytics product feature matrix

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

For further details about new features, access the Zerto Analytics portal and click 

.

Feature	Zerto 6.5	Zerto 7.0	Zerto 7.5	Comments
Dashboard	✓	✓	✓	

Feature	Zerto 6.5	Zerto 7.0	Zerto 7.5	Comments
VPG Analytics	✓	✓	✓	
Storage Analytics	✓	✓	✓	Available from Zerto v6.5 Update 2
Monitoring: Alerts, Tasks, Events	✓	✓	✓	
Reporting: RPO, Journal, Network	✓	✓	✓	
Planning	×	✓	✓	Available from Zerto v7.0 Update 1
ZORG Filter (CSP end user)	✓	✓	✓	Not available for Storage tab
90 Days History	✓	✓	✓	ECE and Cloud licenses Standard 30-day
REST API	✓	✓	✓	

Planning your data protection

Zerto Analytics includes the Zerto Resource Planner; A resource planning capability that performs continuous monitoring and analysis to determine the required storage and networking resources for your data protection. In addition, it provides a recommendation for the required number of ZCAs when replicating to Azure. Analysis can be performed for any or all VMs within your VMware environment. This capability uses data collected from VMware sites and does not require a new installation or license.

The planning capability delivers visibility and forecasting into:

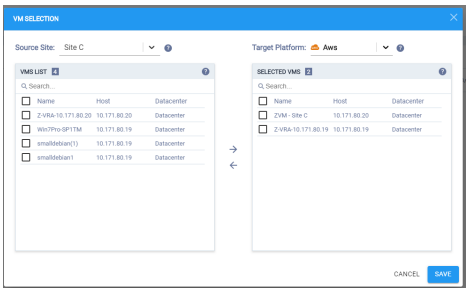
- Zerto protected VMs from vSphere to a public cloud.
- Zerto protected VMs from vSphere to an on-premise site.
- The cost benefit analysis between deciding whether to protect VMs on-premises or in public cloud.

The resource Planning capability provides overall sizing recommendations, including number of **ZCA**s, **WAN**, **Total Journal Size** and **Total Recovery Disk Size**.

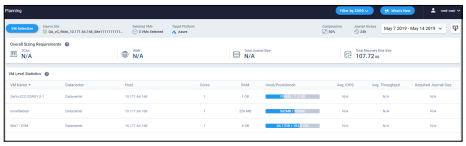
It also includes VM configuration details (CPU, RAM and Total Size) collected from vCenter, per VM calculated performance counters (Avg. Throughput, Avg. IOPS) and the Required Journal Size estimation per VM.

To begin planning your data protection:

1. Click on the **Planning** tab; the VM Selection window opens.
2. From the VM Selection window, select your **Source Site** VMs and **Target Platform** for replication.



3. Click **Save**; The Planning view is displayed.



NOTE:

Use the Help widgets to learn more about each of the features available in Planning.

Zerto Analytics secure architecture

Transmitted Zerto Analytics data is securely stored and can be securely viewed and exported by the user. The data is also used by the analytics engine to provide advanced guidance and analysis. The following section describes the secure architecture that provides the path to transmit, the datastore where the data is housed, and access of that data.

ZVM sends all the data over HTTPS TLS 1.2 only to https://zerto-mobile-data.zerto.com. The data is stored in the Samples Storage in the SaaS backend, located in the public cloud. All communication to and from the cloud are encrypted (HTTPS) using TLS 1.2. Furthermore, the data is isolated in the SaaS backend and accessible only within the backend itself an via VPN from Zerto. End users are authenticated using their myZerto credentials.

See also:

Transmission and Storage of Site Status on page 21

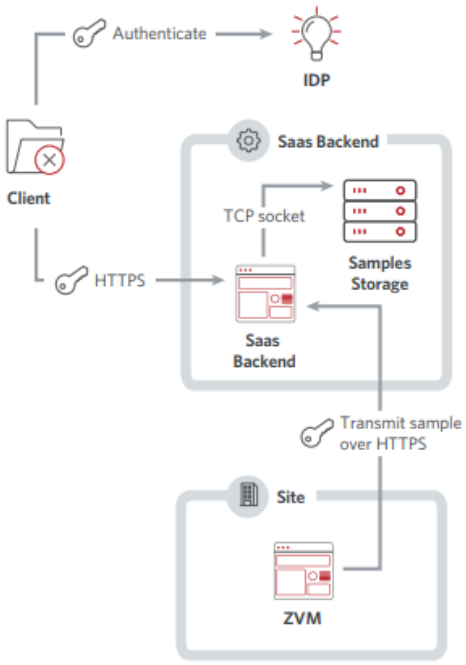
User Authentication and Authorization on page 21

Reporting Historical Data on page 21

Zerto Analytics Collected Data on page 21

Transmission and Storage of Site Status

ZVM transmits current site status over secured HTTPS to the SaaS backend in short (~1 minute) intervals. The SaaS backend collects site status data from all transmitting sites and stores it in the “Samples Storage”. The “Samples Storage” is secured inside an internal protected network and is accessible only within the backend itself and via VPN from Zerto. The samples are kept in the “Samples Storage” of the Zerto Analytics cloud for 30 days to support 30 days of report history.



User Authentication and Authorization

Before sending any request to the backend, a client (browser/mobile/RESTful client) must obtain a security token which securely identifies the user. The security token is achieved by authenticating the user against the Identity Provider (IDP). Each client request contains the security token. For each request, the backend validates the security token and authorizes execution of the request according to the user’s identity which is part of the security token’s payload.

Reporting Historical Data

For each client request, the backend gets the latest data from the relevant samples as stored in the “Samples Storage”. The relevant data is sent to the client.

Zerto Analytics Collected Data

The Zerto Analytics dashboard utilizes several metrics to deliver detailed monitoring and reporting of your multi-site Multi-Cloud environment. The following table was created to address privacy and security issues surrounding data collection.

The following table outlines each piece of information that is collected and sent from the ZVM for Zerto Analytics.

COMPONENT	PARAMETER	DESCRIPTION
Alerts		
	affectedZorgs	List of ZORGs affected by the alert.
	affectedZorgIds	List of ZORG IDs affected by the alert.
	alertIdentifier	Internal alert identifier.
	affectedVpgIds	List of VPG IDs affected by the alert.
	alertType	Help identifier associated with the alert.
	createdDateinUTC	The time the alerts was created.
	description	Alert description.
	entityType	The entity for which the alert applies.
	severity	Alert severity (Warning or Error).
	site	The site which is affected by the alert.

COMPONENT	PARAMETER	DESCRIPTION
Tasks		
	taskName	The task type.
	taskIdentifier	Unique identifier of the task.
	status	The status of the task.
	startedDateInUtc	The time the task started.
	completedDateInUtc	The time the task was completed.
	progress	Progress of the task in percentage of completion.
	sitename	Name of the site.
	protectedDataInMB	Total data protected in the ZVM site.
	siteIdentifier	Internal site identifier.
	transmitterCycleInSec	Number of seconds between two (2) data transmissions.
	type	Site environment.
	initiatedBy	Name of user who initiated task.
	information	Task details.
	relatedVpgsList	List of VPGs related to the task.
	relatedSitesList	List of sites related to the task.

COMPONENT	PARAMETER	DESCRIPTION
Site		
	collectionTimeInUtc	Time the ZVM data was collected.
	documentVersion	Version of the document.
	hashedLicenseKey	ZVM license hashed.
	isTransmissionEnabled	Whether transmission of data was enabled by the user.
	sitename	Name of the site.
	protectedDataInMB	Total data protected in the ZVM site.
	siteIdentifier	Internal site identifier.
	transmitterCycleInSec	Number of seconds between two (2) data transmissions.
	type	Site environment.
	utcOffsetInMinutes	Offset of the site time from UTC, in minutes.
	version	Zerto Virtual Manager version.
	vpgsAlertsCount	Number of active alerts in ZVM.
	zorgsCount	Number of ZORGs in the ZVM site.
	zvmIp	IP of the ZVM

COMPONENT	PARAMETER	DESCRIPTION
VPGs		
	actualJournalHistoryInSeconds	The actual journal history, in seconds.
	actualRpoSeconds	Time since the last checkpoint was written to the journal in seconds.
	configuredJournalHistoryInMinutes	Configured journal history, in minutes.
	configuredRpoSeconds	Configured RPO, in seconds.
	earliestRecoveryPointLocalDateInUtc	Time of the earliest checkpoint in the journal.
	priority	Priority specified for the VPG.
	protectedSite	Protected site details (Site ID, Site Name, Site Type and ZVM version).
	recoverySite	Recovery site details (Site ID, Site Name, SiteType and ZVM version).
	status	Status of the VPG.
	subStatus	Substatus of the VPG.
	vpgIdentifier	Identifier of the VPG.
	vpgName	Name of the VPG.
	zorgName	Name of the Zerto organization set up in the Zerto Cloud Manager, which uses this VPG.

COMPONENT	PARAMETER	DESCRIPTION
VMs		
	IOPS	IO per second between all the applications running on the virtual machine in the VPG and the VRA, that sends a copy to the remote site for replication.
	journalHardLimit	Maximum journal size in MBs, or in a percentage of the virtual machine volume size.
	journalWarningThreshold	Journal size in MBs, or in a percentage of the virtual machine volume size, that generates a warning when the journal is nearing its hard limit.
	outgoingBandWidthInMbps	Bandwidth throttling defined for the virtual machines.
	provisionedStorageMb	The storage provisioned for the virtual machine in the recovery site.
	throughputInMB	MBs of all the applications running on the virtual machine being protected.
	usedJournalStorageMb	Storage used by the virtual machine at the recovery site for Journals.
	usedStorageMb	Storage used by the virtual machine at the recovery site.
	vpgName	The name of the VPG, of which the VM is associated.
	vmIdentifier	ID of the VM.
	vmName	Name of the VM.

COMPONENT	PARAMETER	DESCRIPTION
VRAs		
	vraName	Name of the VRA.
	vraVersion	Version of the VRA.
Events		
	eventIdentifier	The identifier of the event.
	eventCategory	Category of the event. (Possible values: VPG, VRA, Site).
	eventType	The type of event.
	siteIdentifier	The internal site identifier related to the event.
	zorgIdentifier	The identifier of the Zerto organization (ZORG), defined in the Zerto Cloud Manager.
	zorgName	The name of the Zerto organization (ZORG) set up in the Zerto Cloud Manager.
	description	The event description.
	occurredOnInUTC	The date the event occurred.
	eventCode	The event code.
	eventCompletedSuccessfully	Whether the event completed successfully or not.

COMPONENT	PARAMETER	DESCRIPTION
ZORGs		
	zorgIdentifier	The identifier of the Zerto organization (ZORG), defined in the Zerto Cloud Manager.
	zorgName	The name of the Zerto organization (ZORG) set up in the Zerto Cloud Manager.
Datastores		
	datastore	The owning datastore.
	isThisProvisioned	Provision type.
	owningVm	The virtual machine on which the volume is attached.
	path	The volume path.
	protectedVm	The protected virtual machine to which the volume is related.
	size	The volumes used storage.
	volumeType	The volume type.
	vpg	The VPG to which the volume is related.

COMPONENT	PARAMETER	DESCRIPTION
Planning Metrics are collected for all VMs from the source site.		
	WriteKBps - Hourly Avg.	The hourly average data write rate.
	WriteIOPS - Hourly Avg.	The hourly average IO count per second.
	VM ID	The virtual machine identifier.
	Datacenter Name	The datacenter name.
	Datacenter ID	The datacenter identifier.
	Host Name	The host name.
	Host ID	The host identifier.
	Cluster ID	The cluster identifier.
	Cluster Name	The cluster name.
	Folder	The VM folder.
	Configured CPU	The configured CPU.
	Configured RAM	The configured RAM.
	Provisioned Size (GB)	The provisioned storage .
	Used Size (GB)	The used storage.
	Disk Count	Number of virtual disks.

Zerto Cloud Control - overview

The Zerto Cloud Control includes the following features:

- Upgrade Manager
- Tenants

See also:

- Before Getting Started with Zerto Cloud Control on page 1
- Accessing the Zerto Cloud Control on page 1
- Using Upgrade Manager on page 1
- Using Tenants on page 1

Before getting started with Zerto Cloud Control

Verify the following:

- At least **1 ZVM** running Zerto **5.0 or higher**.
- **Enable Zerto SaaS features** check box is selected. This is accessed in the ZVM application in **Settings > About.**
- Internet access.
- A **myZerto** account using your corporate email address.

Accessing the Zerto Cloud Control

Zerto Cloud Control is accessed from one of the following locations:

- From a URL: https://cloudcontrol.zerto.com
- From myZerto: www.zerto.com/myzerto. Sign in using your credentials and select the **Cloud Control** tab.

Using Upgrade Manager

The Upgrade Manager feature allows Cloud Service Providers to remotely upgrade their end customer sites. This allows CSPs to keep their customers Zerto software always up to date. It also allows Cloud Service Providers an overall view of all their end customers' ZVR version.

The remote upgrade functionality has the following pre-requisites:

- The customers ZVR instance is paired to a CSP-deployed ZCC and does not have a perpetual license applied.
- The end customer Zerto instance should be able to transmit over port 443.

Use the **Help** widgets in Upgrade Manager to learn more about each of the features available in the Upgrade Manager.

Using Tenants

The Tenants feature allows Cloud Service Providers to register new and existing enterprise customers to the respective ZORG for that customer. In the ZORG registration, the CSP selects the Product Type. The product type can include features such as One-To-Many and Long Term Retention.

Use the **Help** widgets in Tenants to learn more about each of the features available in the Upgrade Manager.

Zerto

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

Learn more at Zerto.com.

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

© 2020 Zerto Ltd. All rights reserved.