Zerto

# Zerto Platform Architecture Guide

Backup, Disaster Recovery, and Data Mobility

Version 3

## Abstract

The purpose of this document is to provide an architecture guide for anyone designing or implementing an all-encompassing Disaster Recovery, Data Protection solution with Zerto utilizing an on-premises production environment.

It includes a full overview of all design principles, architecture considerations and sizing, as well as an installation overview for anyone looking to, or already utilizing Zerto. In this guide, we also look at common challenges and uses cases that are solved using the Zerto Platform.

The architectures in this guide show only a glimpse of what the Zerto Platform can support. Having a true software-only scale-out architecture and a technology agnostic approach allows you to protect and mobilize your applications in a mix-and-match nature.

## The Zerto Platform

Zerto's software platform delivers disaster recovery (DR), backup, and data mobility across on-premises and multi-cloud environments. The platform is built on a foundation of continuous data protection (CDP), with built-in orchestration and automation to provide IT leaders with simplicity, enterprise scale, and agile data protection to save time, resources, and costs. Analytics, with intelligent dashboards, live reports and resource planning capabilities, provide complete visibility across multi-site and multi-cloud environments, giving organizations confidence that business service levels and compliance needs are met now and in the future.

### Disaster Recovery

Organizations of all sizes that have a virtualized environment use replication for disaster recovery because the impact of not being able to recover successfully and quickly from a disaster can be catastrophic and create systemic risk to the business. Different enterprise-class disaster recovery technologies have been available since the mass adoption of virtualization, but they were typically designed to protect physical servers using storage-based replication and not virtual machines (VMs). This adds significant complexity because the replication is configured on a disk/LUN basis, requiring matching storage and LUN configurations. There is no VM-level granularity and no integration into the virtualization platform. In addition, separate complex software for VM orchestration and automation is required which involves multiple skill sets, resources and does not fully align to the benefits of virtualization.

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.

### Backup

Backup has been an essential part of IT infrastructure since inception, and it is unlikely that will ever change. But with the IT landscape rapidly changing and threats increasing, are we still able to rely on the backup technology we currently use? Organizations today cannot afford to sustain any data loss or downtime. To avoid the impact of data, productivity, and revenue loss, organizations need more granularity in recovery, while maintaining the same level of performance.

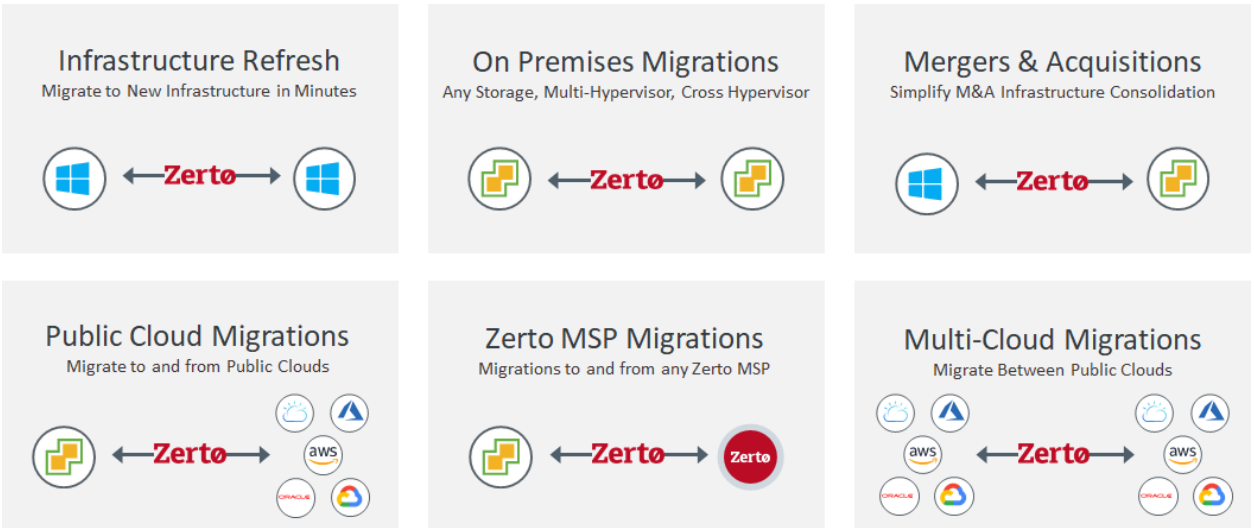
When we look at the backup technology currently protecting our data—one of a company's most valuable assets—not much has changed over the last 35 years. The primary process remains the same: during off-peak hours, take a copy of the data that has changed in our production environments and store it in another, secondary location. This process has a performance impact on the production environment and therefore directly impacts the granularity any backup product can provide.

To ensure granularity without impacting production performance, the future of backup requires the change from periodic or scheduled backups to a continuous backup. By using Zerto's continuous data replication, you can deliver recovery point objectives (RPOs) of seconds by replicating every change that is being generated in near real-time. All these replicated changes are then stored in a journal which allows you to not only recover to the latest point in time but also offers you a granularity of seconds. The outcome of this is the ability to safely rewind to any point in the past, even up to 30 days ago. Recover files, applications, VMs, or even entire datacenters by merely pressing a virtual "rewind" button.

Most recovery use cases that require granular recoveries—such as file deletions, database corruption, or ransomware—only require short-term retention and a 30-day journal supports those requirements. Many organizations have compliance requirements to store data for longer retention periods going back years. Long-term retention data has different requirements as it relates to storage and recovery times but needs to be an integral part of your data protection platform and strategy. As with short-term backups, copies should not come directly from production systems as this impacts performance and often disrupts user experiences.

### Data Mobility & Migrations

Data mobility is the ability to move applications to, from, and between multiple platforms, on-premises or cloud, with minimal business impact and no traditional infrastructure constraints. With the continued increase in cloud adoption, there is now a plethora of cloud platforms to choose from, with large players such as Microsoft Azure, AWS, Google Cloud, Oracle Cloud, and IBM Cloud as well as plenty of managed service providers (MSPs). 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 choice for all workloads, and so, the traditional on-premises deployments with VMware vSphere or Microsoft Hyper-V are still prevalent. Ultimately, all these options have led to increasing adoption of a multi-cloud and/or hybrid cloud strategy. Organizations are challenged to ensure that applications, 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 data mobility comes in, removing the traditional lock-in to these platforms and allowing applications 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.



### Analytics

As data centers become more complex, there is no doubt you need added visibility and control of your protected IT environments across your private, public, and hybrid clouds. Zerto Analytics, included in Zerto's platform, is a secure SaaS-based offering that requires no further configuration and provides a single, 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 analysis of the health and protection status of your applications and data. Built-in intelligent dashboards give you a way to spot trends, identify anomalies, and troubleshoot issues. Provided through a single view across all your environments, whether your data resides on-premises or in the cloud, you can confidently monitor the real-time health and protection status of applications and data. Zerto Analytics informs you to make better decisions to achieve an efficient, resilient mode of operation.

## Core Components of the Zerto Platform

### Zerto Virtual Manager (ZVM)

The ZVM is a Windows service, running on a dedicated Windows VM, that manages everything needed 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.

### Virtual Replication Appliance (VRA)

A VRA is a virtual purpose-built appliance installed on each hypervisor host where VMs are to be protected from or to, delivering a true scale-out architecture. The VRA manages the replication of data from protected virtual machines to its local and/or remote target where it stores the data in the journal. This same scale-out appliance handles copying data from the journal to a long-term retention repository.

### Zerto Cloud Appliance (ZCA)

Used within Amazon Web Services (AWS) and Microsoft Azure deployments, the ZCA is a dedicated Windows VM comprised of the following:

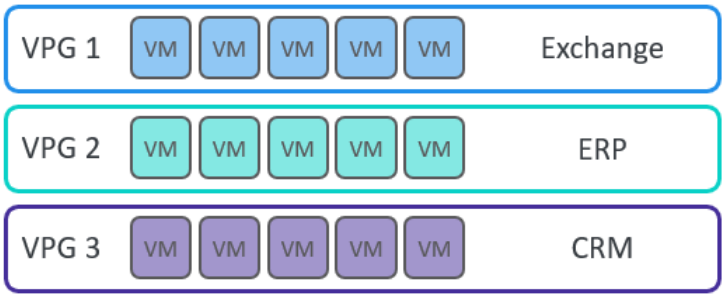
- A Zerto Virtual Manager (ZVM): This is a Windows service that hosts the UI and integrates with the native APIs of Azure/AWS for management and orchestration.
- A Virtual Replication Appliance (VRA): This is a Windows service that performs the replication of data itself from or to Azure/AWS.

The ZCA integrates natively with the platform it is deployed on, allowing you to utilize S3 buckets for journal storage in AWS or blob storage within a Storage Account on Microsoft Azure. This ensures the most cost-efficient deployment on each of these platforms.

### Virtual Protection Group (VPG)

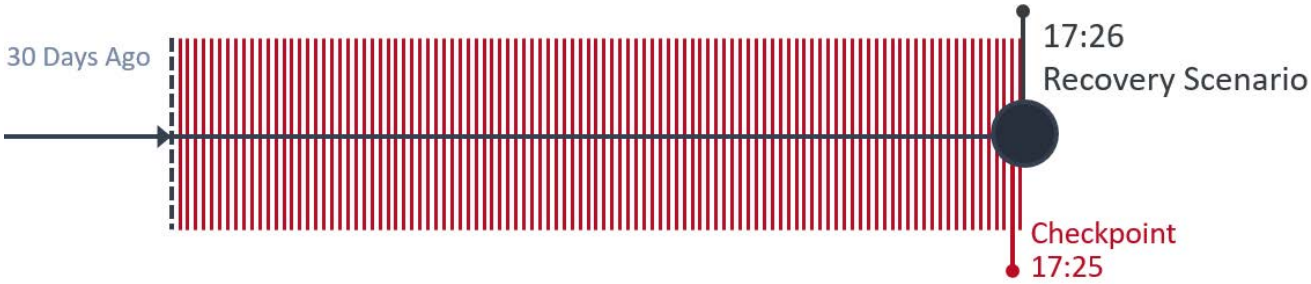
Zerto protection, mobility, and backup are all configured through the creation of Virtual Protection Groups (VPGs). To understand the features of VPGs fully, it is worth covering the traditional approach to protection, where each VM workload is protected individually at different points in time. Today, there are very few scenarios where an application is run on a single VM. Instead, most applications have multiple VM dependencies. Using the traditional method of protecting VMs individually results in significant challenges to recovering your complete application

quickly. You might be able to recover individual VMs quickly, but they will all be recovered to different points in time and it becomes challenging to get them all consistent so that the application is in a usable state. Zerto VPGs differ by allowing you to protect one or more VMs together in a consistent fashion, ensuring every point in time that is inserted into the Zerto journal is from the same point in time for all VMs within the VPG. This allows consistent recovery of an entire application, and all its VM dependencies, to a consistent point in time.




**Journal**

In addition to VPGs, Zerto's continuous data protection (CDP) stores all replicated data in the journal. The journal stores all changes for a user-defined period, up to 30 days, and allows you to recover to any point in time within the journal, ensuring your recovery point objective (RPO) is always as low as possible. Every write to a protected virtual machine is copied by Zerto. These writes are replicated locally and/or remotely and written to a journal managed by a Virtual Replication Appliance (VRA). Each protected virtual machine has its own journal. In addition to the writes, every few seconds all journals within the VPG are updated with a checkpoint timestamp. Checkpoints are used to ensure write order fidelity and crash-consistency. Recovery can be performed to the last checkpoint or a user-selected checkpoint. This enables recovering files, VMs, applications, or entire sites, either to the previous crash-consistent point-in-time or, for example, when the virtual machine is attacked by a virus or ransomware, to a point-in-time before the attack.




**Long-Term Retention (LTR) Repositories**

In addition to flexible options for short-term recovery scenarios using the journal, most organizations that have compliance requirements need long-term retention as an integral part of their data protection platform. Compliance standards often require you to keep and recover data for longer than 30 days. Traditional methods of providing LTR protection have always been performed on the production environment itself, impacting performance and often disrupting user experiences. Long-term retention uses your existing journal to store data from any point in time for days, weeks, months, or even years. Using the data already protected by CDP, combined and stored in a journal on the target side, allows you to offload point-in-time copies to secondary storage targets as often as you want without impacting production workloads.

Zerto supports the use of disk, object, and cloud storage; for a full list of supported repositories and their versions, please see our Interoperability Matrix.

## Reference Architectures

In this section, three example Zerto configurations highlight the different capabilities of Zerto in an easy to understand format. These are intended as guides only to help visualize the benefits that Zerto can provide your organization while also demonstrating the simplicity of the Zerto Platform.

### Use Cases

All three example configurations support the following use cases. Where there are unique differences, they will be highlighted under the relevant architectures.

Outages & Disruptions

Any disruption on the production site, whether it's power, network or otherwise, is protected with recovery of your files and folders, VMs, applications or site within just a few minutes to a point in time just seconds before the issue occurred. *Example: Recovery of your whole site within minutes after a power outage.*

Ransomware Attacks

Recovery from ransomware attacks can be from just seconds before encryption occurred, minimizing data loss and business impact. You can recover your files and folders, VMs, applications or entire sites. E*xample: Recover encrypted files from seconds before they were encrypted.*

Infrastructure Modernization

This same architecture can be used to move your workloads from an end of life platform to your new infrastructure in just minutes, significantly speeding up infrastructure modernization projects. *Example: Move your workloads to a new platform in just minutes with no data loss.*

Consolidations & Migrations

Where multiple sites are to be consolidated or migrated to the same target, this architecture can be used to streamline the process. This enables pre-migration testing and live migration times of just minutes. *Example: Consolidate workloads from diverse hardware, hypervisors and cloud platforms to meet business standards in minutes.*

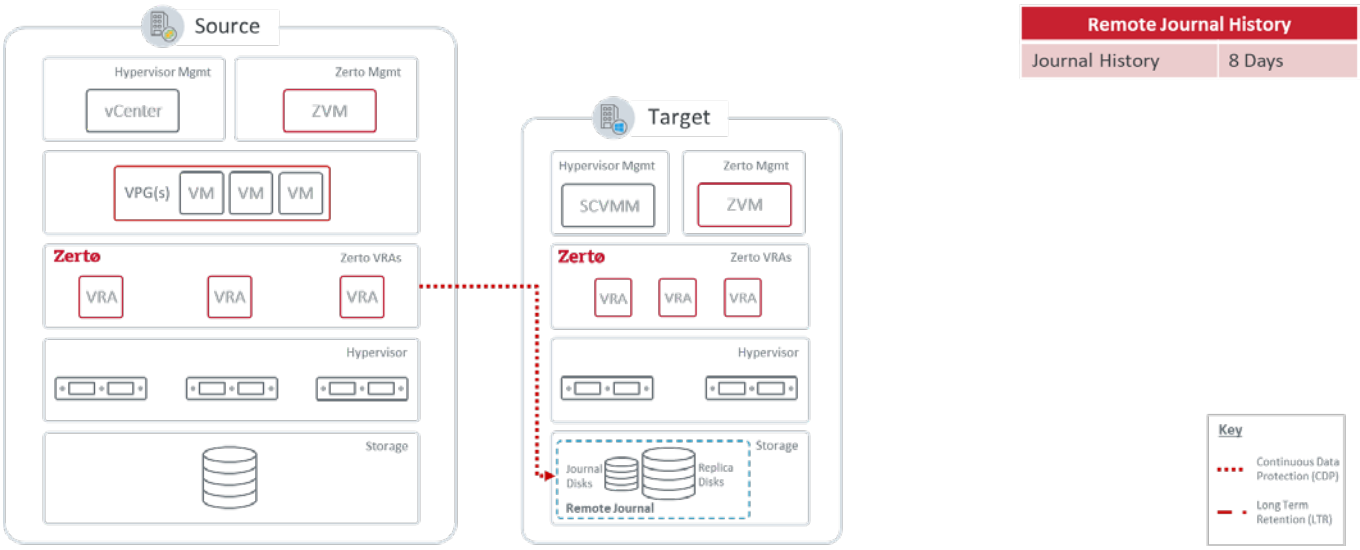
Testing & DevOps

Allows the creation of replicas, at the remote site, of your production environment from any point in time in just minutes. This provides greater flexibility for your development teams and reduces overhead on DevOps teams, as well as enabling DR testing and validation. *Example: Create exact replicas of production applications from seconds ago in just minutes for UAT purposes.*

Analytics Across Clouds

A single SaaS based analytics platform providing complete data analysis across all your sites, both on-premises and in the cloud. This provides a single view that simplifies management and monitoring without added cost. *Example: Identify bandwidth bottlenecks across your entire IT infrastructure through a single portal.*

### Architecture 1: Disaster Recovery



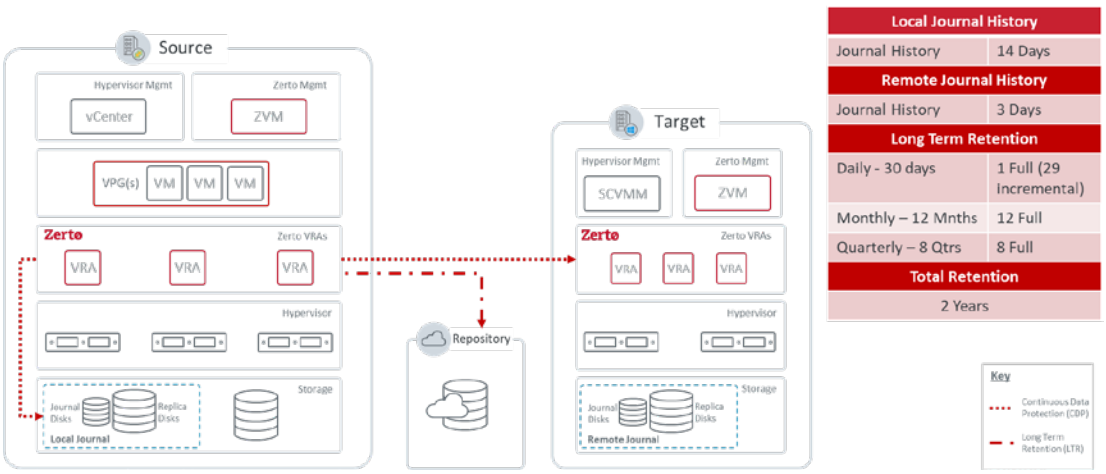

The disaster reference architecture depicted in figure 1 shows a set of proven practices for setting up the platform where a single remote target is being used as the recovery site.

*Description*

Protected VMs are grouped in VPGs with consistency across all the VMs within each VPG. A remote journal is configured on the remote target side and used for short-term recovery scenarios where recovery granularity of just seconds can be achieved. The recommend journal history period for this journal is 8 days as this will cover most recovery scenarios. All changes on the protected VMs are then kept for 8 days before being promoted to the remote replica disk(s).

### Architecture 2: Local Continuous Backup and Disaster Recovery

The reference architecture depicted in figure 2 below shows a set of proven practices for setting up the Zerto Platform just as the previous “disaster recovery” reference architecture, but with the addition of a local journal as well as a long-term retention repository which uses cost-effective public cloud storage. This local journal provides an continuous backup capability, allowing you to recover files, VMs, or applications locally with the granularity of seconds, ensuring minimal data loss in the event of an issue as well as rapid recovery, replacing your legacy backup requirements. The long-term retention repository helps you store the data beyond the journal history for compliance needs.



*Description*

In this configuration, the same VMs exist in two VPGs. The first VPG is for the creation of the journal on the source, and the second VPG is created to provide a journal capability on the remote target. The local journal is configured on the source site and used for backup scenarios where a logical failure occurs, providing recovery granularity of just seconds. The recommended journal history period for this journal is 14 days as this will cover most logical recovery scenarios and with the deduplication capabilities of modern storage arrays will consume minimal storage space. A daily retention process will archive points-in-time from the local journal to the long-term retention repository for compliance needs. In addition to the previous reference architecture, this provides you the ability to recover data directly onto the source site rather than just the remote site. With this architecture, it is recommended that the remote journal history period is 3 days, as this will cover most recovery scenarios where a physical failure has occurred. All changes on the protected VMs are then kept for 3 day before being promoted to the remote replica disk(s).

**Additional Use Cases**

In addition to the standard platform use cases, the below use cases are unique to this architecture or have unique capabilities added to the specific use case.

Outages & Disruptions

The ability to recover files and folders, VMs, applications or site locally in the event of a logical failure is included in this configuration. *Example: If just one application has an issue, recover just this application locally, rather than remotely, to seconds before the issue.*

Ransomware Recovery

The ability to recover files and folders, VMs, applications or site locally in the event of a ransomware attack is included in this configuration. *Example: Recover only impacted Files, VMs or Applications locally, rather than remotely, to seconds before the issue.*

Test/ DevOps

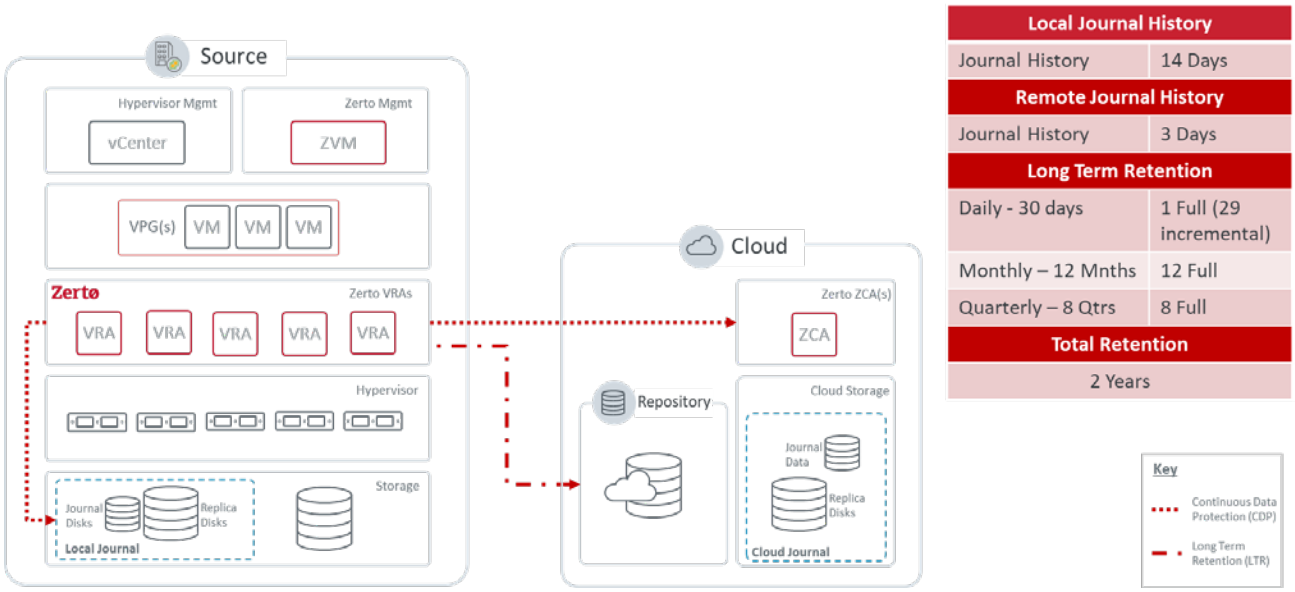
The ability to test recovery or create replicas for DevOps purposes locally is included in this configuration. *Example: Create a replica of a production workload locally, for development purposes.*

Converged DR and backup

Zerto's continuous data protection, with always-on replication and journaling technology, delivers on true convergence of DR and backup providing complete data protection for both short-term and long-term recovery. *Example: One product providing DR and backup with granularity of seconds and no traditional production impact.*

### Architecture 3: Local Continuous Backup and Public Cloud Disaster Recovery

The reference architecture depicted in figure 3 below shows a set of proven practices for setting up the Zerto Platform just as the previous "local continuous backup and disaster recovery" reference architecture, but with the remote target being the public cloud.




| Local Journal History | |
|---|---|
| Journal History | 14 Days |
| **Remote Journal History** | |
| Journal History | 3 Days |
| **Long Term Retention** | |
| Daily - 30 days | 1 Full (29 incremental) |
| Monthly – 12 Mnths | 12 Full |
| Quarterly – 8 Qtrs | 8 Full |
| **Total Retention** | |
| 2 Years | |

*Description*

In this configuration, the same VMs exist in two VPGs. The first VPG is for the creation of the journal on the source, and the second VPG is created to provide a journal capability on the remote public cloud target. This cloud journal is placed on blob storage in Azure or an S3 bucket in AWS and is configured on the cloud side. This reduces cost footprint by having only storage costs incurred and the compute requirements only being spun up in a recovery scenario. The local journal is configured on the source site and used for backup scenarios where a logical failure occurs, providing recovery granularity of just seconds. The recommended journal history period for this journal is 14 days as this will cover most logical recovery scenarios and with the deduplication capabilities of modern storage arrays will consume minimal storage space. A daily retention process will archive points-in-time from the local journal to the long-term retention repository for compliance needs. With this architecture, it is recommended that the remote journal history period is 3 days, as this will cover most recovery scenarios where a physical failure has occurred. All changes on the protected VMs are then kept for 3 day before being promoted to the remote replica which resides on cloud storage.

### Additional Use Cases

In addition to the standard platform use cases, the below use cases are unique to this architecture or have unique capabilities added to the specific use case.

**Cloud Integration & Migration**

Cloud adoption, and the challenges associated with it, can be simplified with this architecture to move workloads to your chosen cloud platform in just minutes with zero data loss. In this use case, long-term retention is likely not needed during the migration. *Example: Move complex applications to the cloud in just 3 steps.*

**Multi-Cloud Hybrid Cloud**

With the increasing adoption of hybrid and multi-cloud strategies, this architecture provides freedom to move workloads around on-demand as requirements change. *Example: Move workloads to, from and across cloud platforms to gain maximum efficiency.*

## Additional Resources

The resources below provide more detailed pre-requisite, guideline, and sizing information.

Zerto - Prerequisites & Requirements for vSphere Environments

Zerto - Prerequisites & Requirements for Microsoft Hyper-V Environments

Zerto - Prerequisites & Requirements for Microsoft Azure Environments

Zerto - Prerequisites & Requirements for Amazon Web Services (AWS)

Interoperability Matrix for All Zerto Software Versions

Zerto Scale & Benchmarking Guidelines

Zerto Journal - Overview, Sizing & Best Practice guide

Zerto Analytics

Please visit https://www.zerto.com/myzerto/technical-documentation for all Zerto's technical documentation.

**About Zerto**

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, data protection and cloud are managed. With enterprise 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. **www.zerto.com**



IS-14437