Zerto

a Hewlett Packard Enterprise company

Disaster Recovery and Data Protection with Zerto and Microsoft Azure

Disaster Recovery and Data Protection with Zerto and Microsoft Azure

SECTION 1

Introduction

Considering the Role of Cloud in Data Protection Strategy

Cloud is playing a key role in nearly every IT infrastructure, whether it's software as a service (SaaS) applications, infrastructure as a service (IaaS), storage, or many other use cases. Cloud is being adopted widely in both hybrid cloud and cloud-only architectures, powering businesses in a 24/7/365 world. Though organizations around the world adopt cloud in different ways, many are adopting cloud specifically for data protection solutions that seamlessly protect on-premises or cloud-based workloads.

Zerto, a Hewlett Packard Enterprise company, helps organizations adopt cloud with disaster recovery, ransomware resilience, and multi-cloud mobility. Whether moving to the cloud for the first time, moving between clouds, protecting on-premises VMs, or protecting cloud VMs to one or more clouds, Zerto has a solution that offers low RPOs and RTOs and seamless orchestration and automation of data and application protection.

Microsoft Azure is a leading public cloud platform with more than 200 products and cloud services designed to build, run, and manage applications across multiple clouds, on-premises, and at the edge. Many organizations choose Azure because it offers flexibility to expand their existing infrastructure to regions around the world, with the capacity for enterprise business operations. Azure supports all industries on a secure, flexible platform that is continuously being innovated.

Zerto and Azure together give organizations world-class data protection with the best RTOs and RPOs in the industry at scale, both on-premises and in the cloud. The multi-cloud capabilities of Zerto enable protection not only to and within Azure but to other clouds as well, giving organizations the freedom to combine multiple clouds in a customized data protection strategy. Whether an organization wants to adopt the cloud as a disaster recovery site, a hybrid cloud for both production and disaster recovery, a cloud-first architecture, or a multi-cloud architecture, Zerto can provide the data protection and cloud-mobility needed.

SECTION 2

Data Protection Defined

There are many concepts and terms in data protection, from business continuity to backup and recovery. Data protection itself is a set of specific use cases centered on the recovery of data. These include backup, disaster recovery, and cyber recovery.

Backup involves slow, regular copying of data, which may be retained for years, to a remote system so that it can be recovered when needed. The amount and kinds of data a backup stores, as well as for how long, are often determined by regulations compliance for the availability of data.

Disaster recovery is the ongoing replication of data to a standby site so that data and applications can be quickly recovered from a disruption in a matter of minutes or hours.

Cyber recovery is similar to disaster recovery, but it focuses specifically on recovering data that has been impacted by cyberattacks, where existing systems may be infected with malware. Data protection focuses on making sure copies of data are available for recovery in any scenario, even catastrophic disasters or cyberevents.

SECTION 3

Isn't Cloud Data Already Protected?

Yes and no. A public cloud usually has redundancies built in, automatically copying data across multiple regional data centers to protect against hardware failures and disasters—these regions are sometimes called "availability zones." These redundancies do make the cloud infrastructure resilient against some data loss and outages, but some outages still occur, and data can be lost in a variety of incidents. There are several ways your cloud data and applications can be affected, including outages, accidental or intentional data loss, and cyberattacks.

Outages

Cloud outages aren't frequent, but they do happen. They often span beyond availability zones to entire regions, leaving cloud customers with no services for hours at a time. Though these outages may or may not cause data loss, they do remove access to data and applications, potentially bringing business to a halt. Because outages can affect entire regions and their availability zones, the high availability redundancies built into the cloud are not effective in these cases. A disaster recovery plan that can fail over to another region or another cloud, or even to an on-premises site, can quickly recover operations if a cloud outage occurs.

Data Loss—Accidental or Intentional

Cloud platforms have redundancies in their infrastructure that protect data against storage failures, but they don't protect data against manmade disasters like deletion or corruption of data, whether accidental or malicious. Anyone with the right access—from an internal employee to an external actor—can delete or corrupt data in your system. The cloud platform is only designed to detect access, not know if actions performed are legitimate or not. When critical data is deleted or corrupted, applications and other services experience downtime. That data can be lost forever without a data protection solution in place to recover it quickly.

Cyberattacks

In recent years, cyberattacks like ransomware have become the leading cause of organizations declaring disaster events. While organizations have taken increased steps to prevent cyberattacks before they happen, attacks are continuing to disrupt. In many cases, recovery from an attack can take days or weeks after data has been maliciously encrypted by malware.

Only 4% of orgs who paid ransom got all their data back, and decryptors are notoriously buggy.

— SOPHOS STATE OF RANSOMWARE 2022

Cyberattacks are not just disasters that cause data loss and downtime—they are disasters with the ill intent of inflicting the most damage possible on your systems to cause disruption. Cloud redundancies do not protect your data or applications from cyberattacks. Having the right solution in place for recovery is crucial to recovering your systems with as little disruption as possible.

SECTION 4

Benefits of Azure

Cloud computing offers a variety of benefits for both production workloads and disaster recovery. Most organizations have adopted cloud in one form or another from cloud-based SaaS, cloud-based storage, IaaS, disaster recovery, backup, and more. Azure is one of the leading public clouds and offers a full range of cloud services. For disaster recovery in particular, clouds like Azure offer some of the following benefits.

Elasticity

One of the key benefits of the cloud is that the infrastructure already exists with nearly unlimited capacity. As an organization needs to add infrastructure, Azure has the advantage of immediate availability to create workloads and applications. Expanding an existing on-premises data center can take months, from ordering hardware to installing, configuring, and networking systems together and then installing and configuring applications.

Azure not only offers ready-made compute, storage, and networking capabilities, but also acts as a remote site especially suitable for disaster recovery. Not every organization has a remote site capable of supporting a disaster recovery data center. Most public clouds, like Azure, have multiple data centers spread across multiple regions, providing many locations for your data and computing workloads. Azure offers 60+ regions in over 140 countries.

As organizations expand, cloud computing allows individual virtual machines to be easily scaled up with more CPU and RAM resources. Scale out is easy too, as you can provision more virtual machines as needed. When setting up disaster recovery in Azure, the resources you need can be deployed within a matter of minutes or hours to begin protecting your production workloads.

Pay As You Go

Cloud computing is an as-a-service model that incurs cost for resources and services consumed, making computing infrastructure an operational expense, not a capital one. This allows organizations to pay for only what they need and nothing more. On-premises data centers, however, are padded with unused compute, storage, and network capacity to allow for growth over time, but this infrastructure has already been paid for even if it is never used.

Cloud expenses vary across providers and can include compute, storage, data ingress, data egress, and other services. Azure, for example, doesn't charge for data ingress but does charge for data egress. Regardless, paying for only what you use can offer a more predictable cost model for expenses when managed well. Buying, managing, maintaining, upgrading, and replacing hardware is non-existent in cloud computing, meaning you can allocate those funds for the operational expense of using only the computing resources and services you need.

Under-Provisioned Disaster Recovery

Under-provisioning disaster recovery resources is a widely used practice that allows an organization to operate during a disaster event by initially recovering only key systems, sometimes at a diminished capacity. This can reduce the cost of disaster recovery infrastructure, which is mostly sitting idle, waiting to be used in a disaster event.

With the pay-as-you-go model and the elasticity of cloud, you have the unique ability to under-provision disaster recovery resources even further. While idle, some disaster recovery solutions don't require virtual machines to run or be provisioned. Only a very small number of compute resources are needed to collect incoming recovery data and store it until it is needed.

With Azure as a disaster recovery site, some or all of the protected workloads can be provisioned to run in the Azure, but the cost of running those workloads is only incurred when that disaster recovery event occurs. When everything is running normally, the disaster recovery resources will have a much smaller cost footprint.

Security

A single cloud platform alone is not necessarily more secure than any other infrastructure, but incorporating the cloud into a multiplatform, multi-cloud architecture can add an extra layer of security. While it is possible to extend an on-premises domain into the cloud, it can make more sense to keep cloud and on-premises separated administratively. Spreading out the accounts and roles can be part of a least-privileged security strategy and make it more difficult for attackers to move laterally between on-premises and cloud infrastructures.

With the cloud as a disaster recovery site, this separation of infrastructures helps prevent recovery data from being impacted by a cyberattack. Azure can provide a secure environment separate from on-premises or other clouds, adding an extra hurdle for attackers to overcome when they target resources across a multisite/multi-cloud environment. Gaining access to production infrastructure does not mean an attacker has access to DR infrastructure, especially if it's on a different operating platform with separate credentials, managed by secure appliances.

SECTION 5

Zerto and Microsoft Azure

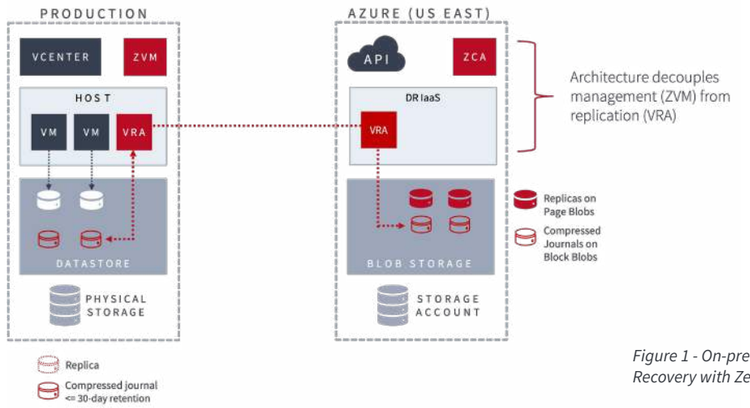


Figure 1 - On-premises to Cloud Disaster Recovery with Zerto and Azure IaaS

Zerto is the gold standard in disaster recovery. It drastically limits your data loss and downtime during natural disasters, hardware failures, or anything else that comes your way. Zerto continuous data protection (CDP) unlocks the lowest RPOs and fastest RTOs to enable recovery of whole clusters, multi-VM applications, or simply a single server. Whether recovering to a secondary site, the public cloud, or a managed service provider, Zerto gives you the confidence to protect, manage, and recover all your critical digital assets.

Zerto CDP technology is well-known in the industry for very fast RPOs and RTOs at scale. You can learn more details about this technology in the white paper "Hypervisor-Based Replication."

Combining Zerto and Azure helps businesses simplify data protection and disaster recovery. Many organizations use Azure as a disaster recovery site or protect across DR regions to eliminate the capital costs associated with owning and operating a data center. Zerto helps organizations keep disaster recovery costs within budget with support for Azure Blob Storage so that recovery data is stored at a low cost until needed for recovery. Zerto is available in the Azure Marketplace, installs in minutes, and is easily integrated with any Azure account.

Zerto and Azure can be used together in a variety of use cases, including on-premises to Azure, native Azure VMs, VMware VMs on Azure, and backup protection for Azure Active Directory. The following sections provide details on the use cases Zerto covers.

Disaster Recovery of VMware Virtual Machines to Microsoft Azure IaaS

Many organizations have deployed Zerto with Azure in a hybrid-cloud configuration that uses the cloud as a disaster recovery site. Azure can be a disaster recovery target site, whether the production site is on-premises VMware or VMware on public cloud, such as Azure VMware Solution, Google Cloud VMware Engine, IBM Cloud for VMware Solutions, or Oracle Cloud VMware Solution. Zerto seamlessly converts VM formats from VMware to Azure IaaS during the recovery process, and back again when they are replicated and recovered back to the production VMware environment.

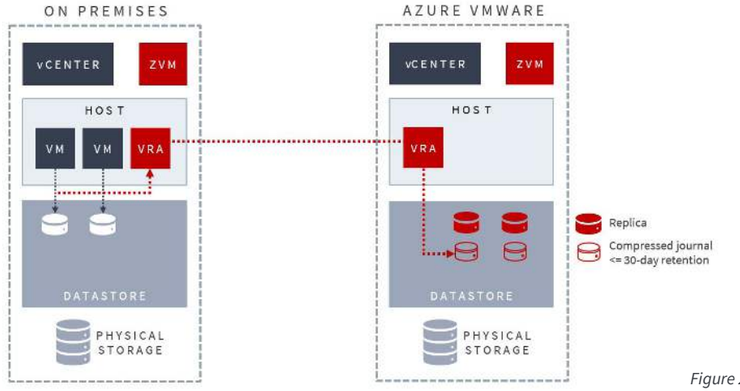


Figure 2 - On-Premises to Azure VMware Service with Zerto

In a VMware environment, Zerto is managed by a Zerto Virtual Manager (ZVM) appliance, purpose built for protecting VMs on VMware. Within Azure, Zerto deploys a Zerto Cloud Appliance (ZCA) for manging the recover and protection of cloud-based VMs. In both environments, Virtual Replication Appliances (VRAs) are deployed to perform the block-level replication, journaling, and recovery or virtual machines at scale. Within Azure, the VRAs also utilize Azure Virtual Machine Scale Sets to further scale out work.

In a VMware environment, Zerto recovery data is simply stored to a datastore of choice defined within vCenter. In Azure, Zerto is stored in Azure Blob storage, a low-cost storage type. Zerto journals are stored on block blobs and replicas are on page blobs. During the recovery process, replica virtual disks that have been stored as page blobs are converted to managed disks and attached to the recovery virtual machines.

This architecture takes advantage of Zerto's award winning CDP technology, extending recovery into the native IaaS architecture of Azure to provide disaster recovery directly to the cloud with RPOs of seconds and RTOs of minutes.

Disaster Recovery of VMware On-Premises to VMware on Microsoft Azure

For organizations that would rather manage all of their workloads from VMware vCenter but still incorporate the public cloud, they can do so by using Azure VMware Solution. With VMware running on Azure, Zerto is installed and managed the same way it is used in on-premises VMware infrastructure. This provides a seamless management experience with vCenter and Zerto across both on-premises and cloud for disaster recovery.

The Zerto Virtual Manager appliance is deployed in the Azure VMware infrastructure, and VRAs are deployed on each virtual host, just as if those hosts were physical. This identical architecture topology makes deploying and managing Zerto more seamless across both on-premises and Azure cloud. All the VMs are managed within vCenter, allowing an organization to make full use of their VMware skills and experience.

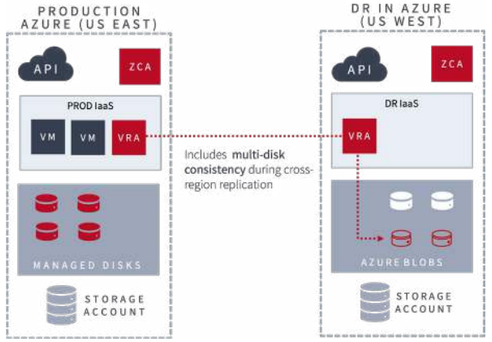


Figure 3 - Region to Region Disaster Recovery with Zerto and Azure IaaS

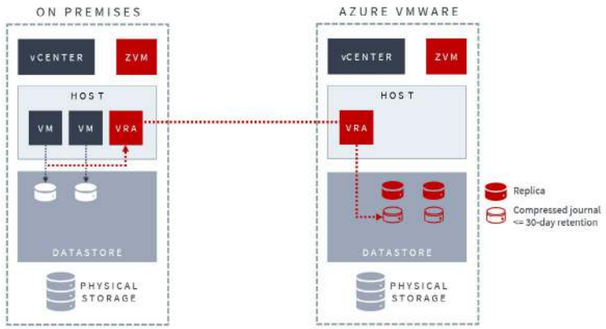


Figure 4 - Region to Region Disaster Recovery with Zerto and Azure VMware Service

When using VMware on Azure as a disaster recovery site, Zerto does not need to convert any VMs at the time of recovery. Instead, Zerto treats VMware on Azure just as it would any VMware site, whether on premises or cloud-based. A Zerto administrator familiar with Zerto on VMware will have a seamless experience using VMware on Azure.

Disaster Recovery within Microsoft Azure: Region to Region

For organizations running production VMs on Azure, Zerto can be deployed within Azure to protect those VMs from region to region, keeping them safe from regional outages and manmade threats like accidental deletion, corruption, or cybercrimes. With Zerto, organizations get world-class protection and orchestration at scale to ensure their workloads can be recovered in the case of disaster.

To protect VMs running on Azure IaaS, Zerto uses a ZCA in each region to manage those regions as sites. Each ZCA deploys VRAs within the region to scale out as needed and perform replication between regions. On Azure IaaS, Zerto uses native Azure snapshot features to perform the replication of Azure VMs and create recovery points in the DR region. The snapshots protect an Azure VM whether it has one or multiple virtual disks attached. This allows Zerto to protect hundreds or thousands of VMs within Azure to another region or regions.

Region to region protection saves resources, reduces cost, and increases flexibility while protecting VMs. As with on-premises to Azure IaaS, this architecture takes advantage of low-cost blob storage. Protected VMs are not provisioned or running until they need to be recovered. And VMs that are failed over from one region to another can be easily failed back to the original region or protected from the new region to a different region.

When using Azure VMware Service, Zerto can also protect VMs between regions where VMware sites have been created. Here, the architecture is the same as on-premises VMware to VMware using the Zerto Virtual Manager and VRAs.

When Zerto protects VMs in Azure from VMware to VMware on Azure VMware Service, it doesn't use native Azure snapshots. Instead, Zerto uses the same CDP replication and journaling that it deploys for VMware on-premises or Zerto on-premises to Azure.

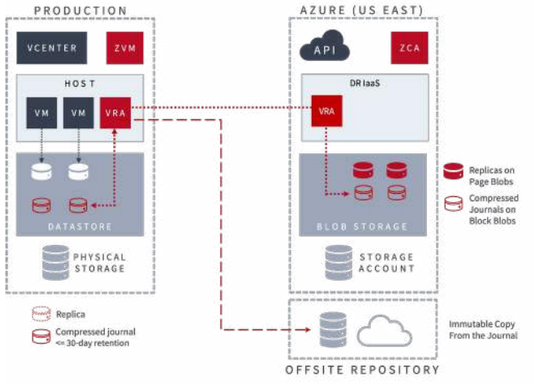


Figure 5 - Immutable Extended Journal Copies with Zerto and Azure

Zerto Immutable Extended Journal Copies

As stated earlier, cyberattacks are a great concern even in cloud environments. Zerto's fast RPOs and RTOs and flexible recovery options enable cyber recovery in most ransomware scenarios. In a worst-case scenario where even Zerto and the recovery journal are compromised, recovery is still possible from an immutable extended journal copy. These extended journal copies are created from a user-specified point in time in the journal and stored on Azure Blob, Amazon S3, or S3-compatible storage.

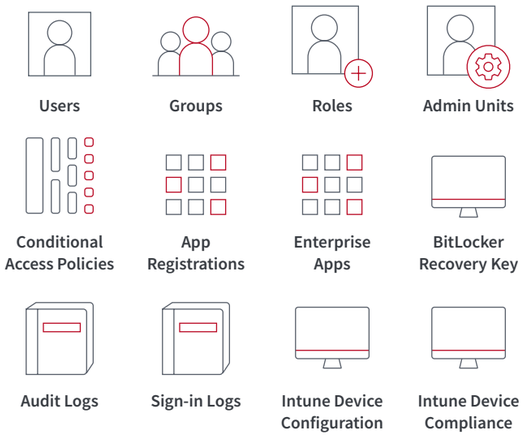
In a worst-case scenario where all other recovery data has been lost, Zerto can recover an immutable extended journal copy into a clean environment, and all VMs including their data and applications can be recovered from that copy. Storing the immutable copy in an offsite repository in Azure Blob, Amazon S3, or on-premises on S3-compatible storage can offer an added layer of protection to your ransomware resilience strategy.

Zerto Backup for SaaS—Azure Active Directory

Organizations who run production workloads in Azure often choose to use Azure Active Directory. When facing a disaster scenario, organizations need to protect their Active Directory domain services as well.

You can recover business-critical data in seconds with Zerto's fully automated backup and recovery solution for Microsoft 365, Microsoft Azure AD, Salesforce, Google Workspace, and Microsoft Dynamics 365. With this offering, Zerto delivers simple, scalable data protection for virtualized, public cloud, and SaaS applications.

Zerto Backup for Microsoft Azure AD is a simple, yet powerful application to protect your Azure AD infrastructure from accidental deletions, ransomware, or other disaster scenarios. Combined with Zerto for Azure, this solution offers protection for:



The Zerto Backup for SaaS for Azure AD security strategy helps you recover business critical identity and application objects that are not protected by Microsoft. Protect against unwanted changes and tackle downtime with continued access to your data. Backup data is stored in a dedicated cloud, providing an isolated and tamperproof second copy so it can be recovered even if Azure is disrupted.

SECTION 6

Benefits of Zerto and Azure

Combining Zerto disaster recovery with Azure cloud services provides a variety of world-class benefits from both solutions. These are several of the key benefits of Zerto and Azure.

The Fastest RPOs and RTOs at Scale—Whether you're protecting dozens or thousands of VMs, Zerto provides RPOs of seconds and RTOs of minutes to your data and applications when protecting to Azure.

Orchestration and Automation—Hundreds or thousands of VMs can be protected in Zerto virtual protection groups (VPGs) and logically orchestrated to be recovered quickly either on-premises or in Azure within minutes. In just a few clicks you have seamless, automated recovery from on-premises to Azure.

Nondisruptive Testing—With Zerto, DR testing can be performed without any disruption to production or protection. Zerto creates an isolated network environment on premises or in Azure to recover VMs for testing and automatically generates a test report on completion.

Immutability Against Ransomware—Zerto immutable extended journal copies protect VMs against worst-case ransomware scenarios and allow full recovery from a point-in-time data copy.

Native Azure VM Support—Zerto supports native Azure VMs, allowing on-premises VMware VMs to automatically convert to Azure VMs during recovery to Azure. Zerto protects native Azure VMs from region to region, Azure to on premises, or between clouds.

VMware to VMware in Cloud—Zerto fully supports Azure VMware Service, so VMware VMs can be protected to VMware on Azure, from VMware to VMware in Azure, or back to on-premises or another VMware environment in the cloud.

Azure Blob Support—Zerto not only waits to provision Azure VMs until recovery is required, but also stores on Azure Blob storage data replicated to Azure for disaster recovery, minimizing the cost of storing the data.

Hybrid Cloud/Multi-Cloud Flexibility—Zerto makes it easy to combine Azure with on-premises infrastructure for disaster recovery or incorporate other supported clouds into a hybrid cloud or multi-cloud strategy.

Backup of Azure AD and SaaS—In addition to disaster recovery for critical VMs, Zerto Backup for SaaS provides protection for cloud-based applications, including Azure AD and a variety of other applications.

Elastic Infrastructure Around the World—Azure provides 60+ regions of cloud infrastructure across 140 countries, giving you data protection with Zerto in the geography of your choice.

SECTION 7

Staying Protected in the Cloud with Zerto and Azure

Going to the cloud has many benefits. Regardless of why data and applications end up in the cloud, they need to be protected from the natural and manmade disasters that threaten downtime and data loss. Although the cloud can be resilient against outages, nothing is infallible. Cloud outages and data loss do happen, especially from cyberattacks targeting specific organizations.

Azure is one of the leading public clouds that organizations choose to enhance their cloud strategy. With Zerto, organizations can move to Azure faster and use a hybrid cloud environment to create a dependable disaster recovery strategy. Zerto brings trusted CDP straight to Azure, and Azure brings a trusted cloud platform to organizations who depend on running a continuous business.

Zerto and Azure make a powerful combination for organizations who need low RPOs and RTOs in this modern, always-on business world. Whether protecting data and applications from on-premises to cloud, from cloud to on-premises, or from cloud to cloud, Zerto for Azure provides world-class disaster recovery on a world-class cloud platform in Azure.

Zerto
a Hewlett Packard Enterprise company

+

Microsoft Azure

About Zerto

Zerto, a Hewlett Packard Enterprise company, empowers customers to run an always-on business by simplifying the protection, recovery, and mobility of on-premises and cloud applications. Zerto eliminates the risk and complexity of modernization and cloud adoption across private, public, and hybrid deployments. The simple, software-only solution uses continuous data protection at scale to solve for ransomware resilience, disaster recovery, and multi-cloud mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Amazon, Google, IBM, Microsoft, and Oracle and more than 350 managed service providers. **www.zerto.com**

RITM0095353