Zerto
a Hewlett Packard Enterprise company

Business Continuity and Disaster Recovery in the Cloud Era

Know Your Options

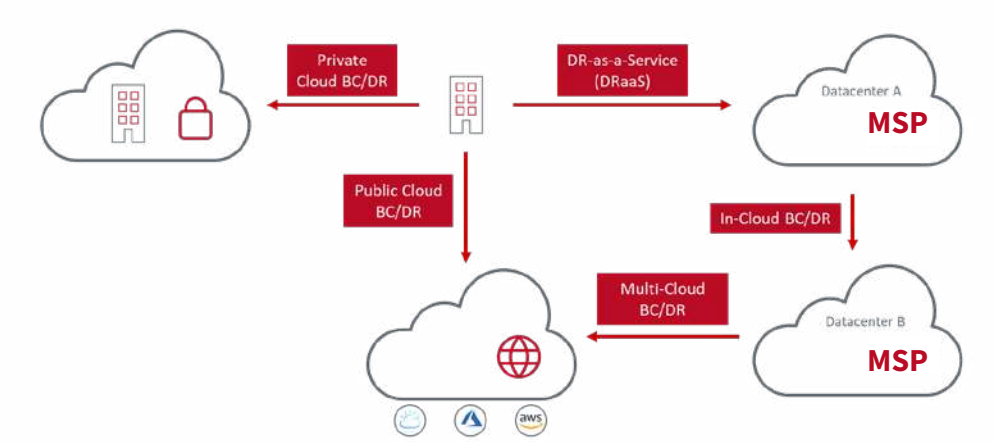
Version 3.0
August 2022

Business Continuity and Disaster Recovery (BC/DR) in the Cloud Era

The benefits of leveraging the cloud and virtualized or containerized environments are many, including greater flexibility and scale without incremental hardware costs coupled with agility to increase availability, business continuity and disaster recovery to protect an "always on" customer experience for digital business. Today, enterprises of all sizes have virtualized their mission-critical applications, either within their own datacenters, or with an external cloud provider. Containers are becoming immensely popular for developing new applications and reducing implementation times for new business-critical applications.

With cloud popularity ever increasing, companies of all sizes are looking for the cloud, be it public, hybrid or private, to become part of their BC/DR solution. However, depending on the tool, these options do not always exist. Virtualization and containerization create the opportunity, but depending on the solution, there can still be a significant technology gap. Mission-critical applications can be effectively virtualized, containerized, and managed, but if you use the wrong solution for BC/ DR, they cannot be effectively protected in a cloud environment.

Zerto, a Hewlett Packard Enterprise company, is the industry's first solution that is multi-hypervisor and public cloud capable, protecting applications within the cloud and moving to the cloud, and has become the standard that all others are measured against.



Overview

In this paper, we'll outline the different types of Cloud BC/DR solutions along with their pros and cons. Then, we'll discuss how Zerto addresses these challenges and improves upon many of the traditional solutions that leave gaps in cloud-based BC/DR.

Different Forms of Cloud BC/DR

Before we discuss the pros and cons, let's briefly define the different forms cloud BC/DR can take:

Cloud	Description
Private Cloud BC/DR	Business continuity and disaster recovery between two or more geographically separate sites, with underlying hardware dedicated to the organization and often all under the control of their own IT team.

Cloud	Description
Public Cloud BC/DR	Business continuity and disaster recovery between one or more sites under the control of the organization's IT team and one or more public cloud platforms utilized as the recovery site. In this deployment the BC/DR implementation is also managed by the organization's IT team internally.
Disaster Recovery-as-a-Service (DRaaS)	The production environment is within the enterprise's datacenter; however, a managed service provider (MSP) is used as the recovery site and replication target.
In-Cloud BC/DR	Production applications have been moved to a public cloud and are protected by the cloud provider with full disaster recovery to another geographical site in the cloud.
Multi-Cloud BC/DR	Production applications have been moved to a public cloud and are protected with full disaster recovery to another public cloud platform in another geographical region.

Private Cloud BC/DR

Private cloud BC/DR is very much the traditional approach from the early days of virtualization, mainly because the original approach to BC/DR here relied upon storage level replication. This typically required identical hardware on both sides. Because all hardware is dedicated to the organization and often managed by it too, capital expenditure is high and speed to scale is slow, with downsizing environments resulting in the writing off hardware. Often a recovery site will exist with the sole purpose of being utilized in a disaster scenario only, creating inefficient spending. With this type of environment, IT teams are geared towards keeping the lights on, through management of the datacenters, hardware, and networks. This being said, there are some key reasons why private cloud BC/DR still exists. At the top of this list is control. With all hardware dedicated to the organization, absolute control is guaranteed and can be beneficial in scenarios where compliance and regulation are tightly managed. Another important factor to consider is performance. Some applications need huge amounts of resources and being able to align these to specific hardware can help provide the performance guarantees these applications require.

Public Cloud BC/DR

Public cloud BC/DR is something that has seen significant uptake as the popularity of public cloud has grown over the past few years. While in this scenario production remains under the control of the organization, often on-premises and with the same caveats around scale and cost as mentioned previously, it provides some significant advantages too. With deployment in the public cloud, the cost of the recovery site can be drastically reduced, with a dedicated environment no longer required and running for the purposes of recovery in the event of any potential disaster. Instead, the benefits of public cloud can be utilized to provide a much more efficient cost for the recovery site. For example, with Zerto, storage is utilized on the target site until a recovery is required, removing the day-to-day cost of compute. One of the main reasons this solution has seen so much growth is because it has delivered enterprise-class BC/DR to smaller organizations who previously couldn't justify the cost of a dedicated second site. There are, however, other considerations to this model. Control is lost as the underlying platform is managed by the cloud provider meaning outages here are out of your hands, albeit this can be a positive attribute depending on your point of view. Public cloud platforms are also multi-tenanted, so "noisy neighbors" do have the potential to impact the platform. All in all, this is often a very effective first step to cloud adoption for many organizations.

Disaster Recovery-as-a-Service

Disaster Recovery-as-a-Service (DRaaS) allows organizations to host and manage their production environment within their own datacenter but use a managed service provider (MSP) to deliver BC/DR as a service to a cloud site. This has a lot of the same benefits as the previous model, with pay as you go compute pricing that eliminates the need for capital expenditure and a managed platform, however it also takes it a step further. With DRaaS, MSPs will provide management of the BC/DR solution providing organizations with SLAs around recovery point objectives (RPOs) and recovery time objectives (RTOs), providing contracted guarantees and removing the overhead of managing this themselves. Because of this, there is often a strong working relationship between the MSP and organization, not to mention the fact that most organizations will choose a local MSP in country.

"We offer many DRaaS solutions but were looking for something that protected data at the VM-level and also offered very aggressive service levels. Zerto delivers RPOs of seconds and RTOs of minutes, with continuous data protection built in. Our DR solution with Zerto, our internal team of experts, and our additional solutions around cloud, connectivity, and security, all give us a clear competitive advantage."—

— Dante Orsini, **Chief Strategy Officer, 11:11 Systems, Inc.**

In-Cloud BC/DR

In-Cloud BC/DR is again an additional step forward from DRaaS. Instead of the organization running and managing their production environment on dedicated hardware in their own datacenter, this too can be moved to a managed provider's platform or to public cloud that remains under the control of the organization's IT team. In the case of the production environment now in the public cloud, a BC/DR Solution can be used to replicate from one public cloud to another public cloud as a BC/DR Target. If using an MSP, the BC/DR is then provided by protecting production from one of the MSP's datacenters to another geographically distant datacenter. BC/DR is then often fully managed by the MSP, as well as potentially providing management where needed for the organization's production environment. This then replicates all the benefits of moving a recovery site to the cloud but applies also to the production site as well. Pay as you go pricing delivers cost efficiencies for production, while the organization's IT teams can focus more on business innovations rather than the day to day running of a datacenter. In addition, MSPs will be delivering SLAs for the production environment as well as BC/DR, with a close, often personal working relationship.

Multi-Cloud BC/DR

Multi-Cloud BC/DR is a model that has grown in popularity recently for a couple of reasons. First, the key driver has been cloud adoption globally, with more and more organizations taking advantage of the cloud. However, it is not unheard of for an organization to maintain a vendor agnostic approach for resilience reasons when looking at their BC/DR strategy. Essentially, rather than taking the in-cloud BC/DR approach, the multi-cloud BC/DR model allows organizations to place their production and recovery site on different cloud platforms. Should an issue ever take one cloud platform provider offline, this solution would still provide the organization the ability to keep on doing business. The other factor driving this approach is the realization that not all cloud platforms suit all applications. Some applications may need greater regulation than others, which not all cloud platforms can meet, so protecting these applications to different cloud platforms can ensure maximum efficiency.

"At Node4 we take an unbiased approach to application hosting and help customers migrate their workloads to the right cloud platform based on suitability. For all its benefits a multi-cloud model can cause operational complexity so when we talk to customers about application resiliency we need standardised tooling that can protect workloads between cloud platforms and Zerto offers us that flexibility."

— Geoff Barlow, **Technology Practice Lead – Strategy, Node4**

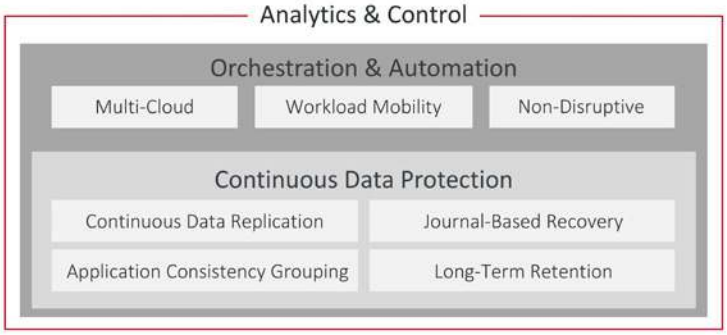
Zerto Overview

Zerto first introduced hypervisor-based replication in 2011 and revolutionized disaster recovery for VMWare vSphere and Microsoft Hyper-V environments. Taking it into the Cloud, Zerto added cloud native support for Microsoft Azure, IBM Cloud, Amazon Web Services (AWS) and VMWare on public cloud. Zerto added support for Kubernetes workloads, supporting Microsoft Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), and IBM Cloud Kubernetes Service as cloud BC/DR targets. The native Zerto for Kubernetes solution drives a "data protection as code" strategy, integrating data protection and disaster recovery operations into the application development life cycle from day one. This means that applications are born protected. Using this approach, organizations can ensure the resilience of their applications without sacrificing the agility, speed, and scale of containerized applications.

Expanding its vision, Zerto now converges disaster recovery, backup, and cloud mobility into a single solution for virtualized, cloud-native and Kubernetes workloads. This allows you to replace multiple legacy solutions with a single, simple, and scalable solution that delivers a continuous, "always on" customer experience. Simplified workload mobility protects, recovers, and moves applications freely across hybrid and multi-cloud environments with over 9,500 customers globally now relying on Zerto's solution.

Zerto Solution

Zerto converges disaster recovery, backup, and workload mobility whether on-premises or to, from and between hybrid and multi-cloud environments. With support for VMware vSphere, Microsoft Hyper-V, Microsoft Azure, AWS, IBM Cloud, Google Cloud, Red Hat OpenShift, VMware Tanzu, Microsoft Azure Kubernetes Service (AKS), Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), IBM Cloud Kubernetes Service and 350+ MSPs globally. Zerto's agnostic approach can deliver on any of the above models. Built on a foundation of continuous data protection (CDP) with built-in orchestration and automation capabilities, Zerto provides you with simplicity, enterprise scale, and agile data protection to save time, resources, and costs. Analytics, with intelligent dashboards and live reports, gives you complete visibility across multi-site and multi-cloud environments and instills confidence that business service levels and compliance requirements are met.



Continuous Data Protection (CDP)

- Continuous Data Replication – Zerto delivers recovery point objectives (RPOs) of seconds by replicating every change that is generated in near real-time. Near-synchronous replication performed at the hypervisor level has no impact on production, delivering granular recovery checkpoints, seconds apart.
- Journal-Based Recovery – All replicated changes are stored in a journal for up to 30 days providing incredible recovery granularity through checkpoints inserted every few seconds. This reduces data loss to just seconds by enabling recovery of files, VMs, applications or entire sites, either to the latest point-in-time or, for example, when attacked by a virus or ransomware, recover to a point-in-time seconds before the attack.

- Application Consistency – Today's applications are rarely run on a single VM, but instead most applications have multiple VM dependencies. Traditional methods of protecting VMs individually result in significant challenges
- to recovering complete applications quickly. Zerto resolves this by using our Virtual Protection Group (VPG) capability. VPGs allow you to protect complex multiple 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.
- Long-Term Retention – Compliance standards often require you to keep, and ultimately recover data, for longer than 30-days. Long-term retention utilizes your existing journal to store data from any point in time for days, weeks, months or even years with no production impact and can be stored into an immutable data store on-premises or cloud for extra protection.
- Scalability – Zerto simplifies scaling the infrastructure to support disaster recovery. As a new virtual host is added, simply install a new virtual appliance. Although Zerto scales to support very large environments, it provides the same granularity for environments of all sizes, with the same capabilities and no production impact.

Orchestration & Automation

Built in orchestration and automation enables faster management of workloads at scale with minimal touch, allowing IT resources to shift their focus toward innovation and services that help your business run more efficiently.

- All recovery settings are configured upfront, such as boot order and re-IP failover, well before any disaster or other event occurs, greatly simplifying the recovery process. It's so simple, any IT team member can perform it in just three clicks.
- Non-disruptive testing allows you to validate recoverability, or test against production replicas, with no production environment or protection impact.
- Flexible REST APIs fully automate the deployment and protection using ready-made examples.

Analytics & Control

Zerto analytics built-into the solution provides one single, comprehensive view of your entire multi-site, multi-cloud environment.

- Provide multi-site, multi-cloud visibility, including a mobile app for monitoring SLAs from anywhere.
- Compliance reporting–pass audits and stay in compliance with built-in reporting and testing with no impact on your environment.
- Forecast future infrastructure needs with a built-in resource planner. Enable accurate infrastructure planning using your own application data. Predict and size your protection needs for protected and unprotected VMs

Zerto Analytics helps you make better informed decisions and plans, in order to achieve an efficient, IT resilient mode of operation.

To learn more, visit the Zerto for Azure on demand lab or request a demo.

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's cloud data management and protection solution eliminates the risks 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 converge disaster recovery, backup, and data mobility. Zerto is trusted by over 9,500 customers globally and is powering offerings for Microsoft Azure, IBM Cloud, AWS, Google Cloud, Oracle Cloud, and more than 350 managed service providers. **www.zerto.com**

IS-15916