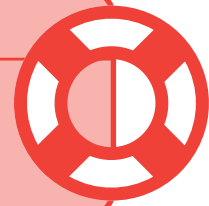


NxtGen Disaster Recovery as a Service

With IT at the core of every business, it is very essential for businesses to focus on IT resilience by planning for and enabling Disaster Recovery. This will also ensure business continuity in case of disasters. NxtGen offers Disaster Recovery as a Service to help enterprises build adequate IT resilience due to any unforeseen events.

NxtGen's Disaster Recovery as a Service is offered in two flavours:

1. Disaster recovery for virtual servers using NxtGen's native cloud platform NG3 (for KVM)
2. Disaster recovery for servers on VMware and Hyper-V using Zerto



DR for virtual servers on NG3 platform

Real-time protection for Virtual Servers

NG3 DRaaS goes far beyond simple snapshot-based DR services. You can get real-time protection for virtual servers in your cloud with high performance Disaster Recovery services with zero data loss guaranteed for most workloads.

Built on our cloud platform

With NG3 DRaaS we can offer real-time protection for your virtual servers, without the cost, because it's built on the integrated storage platform built into the NG3 cloud.

Simply enable a virtual server for NG3 DRaaS, and the system copies all writes to a replication site, in real time.

Industry-leading DR performance

RPO - Recovery Point Objective - measures how up-to-date recovered data is. So an RPO of 2 minutes means you may lose up to 2 minutes of data writes. NG3 DRaaS has an RPO so low that you can guarantee zero data loss for the majority of workloads.

RTO - Recovery Time Objective - measures the time taken for an application to start running again after a failure. NG3 DRaaS has an RTO of less than 5 minutes for most virtual servers

Public DRaaS

In Public DRaaS, NG3 platform provides a selection of remote replication sites across the world to protect your customers' data. Public DRaaS is a fully managed service, and this model supports virtual servers with simple public networks.

Private DRaaS

In Private DRaaS, use our on-premise clouds as remote replication sites. This model supports more complex network setups, including routable private address networks.

Activating protection for virtual servers

Once the zone replication settings are configured, DRaaS can be activated for individual virtual servers in that zone, via the NG3 Control Panel.

When you enable DRaaS for a Virtual Server, a small helper VM is created on the remote replication site, and all data is copied across. Once the data is synchronized, all future Virtual Server writes are copied across at the block level.

The DRaaS dashboard

Once a virtual server has DRaaS activated, it registers on the DRaaS dashboard, which is used to control all DR actions, such as failover and failback. The DRaaS dashboard runs independently of the NG3 control panel, so you can activate DR even in the face of a major outage.

Key Differentiators



Unrivalled Readiness:

Enlist disaster recovery services that are fully cloud-ready



Fastest Recovery:

Leverage any mix of public, private, or hybrid cloud delivery models, to meet your unique business needs



Robust Recovery:

Cloud migration and disaster recovery for multi-tier applications, not just virtual machines

The dashboard shows the status of all of your clouds and highlights any virtual servers that need attention. You can drill down into a virtual server to see details of the replication status of each disk, and to activate failover or failback for that virtual server.

Detecting outages and initiating failover

NG3 DRaaS monitors uptime for each virtual server that has disaster recovery enabled. If a problem is detected, it actively probes to see if any DRaaS-enabled virtual servers are down. Any problems discovered are automatically flagged on your DRaaS dashboard, and an email alert is generated. You can then activate the failover process through the NG3 control panel. You can also activate failover any time you need to, for planned maintenance.

The DRaaS failover process

When failover is initiated, an identical virtual server is deployed at the DRaaS location using the replicated data.

In our public DRaaS service, the new virtual server will have an identical network configuration but will be assigned a different IP address: it will therefore need a minor update to DNS records to maintain a seamless service for end users.

Private DRaaS supports IP address mobility if you have the correct infrastructure.

Real-time restore

Once the outage has been fixed, the failback/restore process is again triggered manually. NG3 DRaaS automatically restores to the original virtual server, or creates a new virtual server in the original cloud. It ensures all live data from the failover VM is replicated back to the source, in real time.

Once the data is in sync, the final stage is to boot the VM on the original site, at which point DRaaS resumes replication from the source back to the DRaaS site.

DR for Virtual Servers using Zerto

Hypervisor-based remote replication technology from Zerto is different from any other DR technology – providing the granularity needed in today's complex enterprise infrastructures, without compromising on performance, simplicity of operation, scalability, reporting, mobility or flexibility. Purpose-built for tier-one applications deployed on a virtual infrastructure, Zerto's virtual replication is the only technology that combines near-continuous replication with block-level, application-consistent data protection across hosts and storage.

This type of replication separates the application from its physical constructs at the data-protection level. It is fully storage vendor and protocol agnostic, protecting data from any source to any target. Simple to install and intuitive to use, this service is ideally suited for cloud infrastructure.

Cloud-Ready Disaster Recovery

Disaster recovery to the cloud is considered by many enterprises as a natural first step in the journey to the cloud, being an effective alternative to in-house DR sites.

Zerto's technology fits perfectly with the specific needs of enterprises

- Replication from any storage to any storage
- Management API
- Built-in WAN optimization
- Native multi-tenancy support
- Software only, highly scalable
- Tier-one protection level

Tier-One Disaster Recovery for Virtual Environments

Tier-one applications need tier-one performance and availability, and Zerto Virtual Replication delivers just that – managed from within the virtual infrastructure:

Tier-One Replication

- Near-synchronous replication
- Scalable management and deployment
- Zero application performance impact
- Recovery Point Objective (RPO) of seconds
- Application recovery enabling a Recovery Time
- Objective(RTO) of a minute
- WAN degradation and outage resiliency
- Compression and WAN optimization

Virtual Protection

- VM and VMDK consistency grouping
- Replication from anything to anything
- Full support for VMotion, storageVMotion, Cluster and HA
- Consistency across hosts and storage

Protect and Recover Multi-Tier Applications

Protecting multi-tier, mission-critical applications means ensuring quick and safe recovery of the entire application, including all components running on different servers and storage. For example, a given CRM application may span across eight VMs deployed on four physical servers using five different data stores located on three different LUNs. To successfully recover such an application, full consistency between all application components is critical.

Zerto's Virtual Protection Groups (VPGs) are a collection of VMs and their related VMDKs, which have dependencies and must be recovered with write-order fidelity. Zerto VPGs ensure applications are replicated and recovered with consistency, regardless of the underlying infrastructure. This enables deployment of the application across different physical devices to maximize performance and capacity, while reducing complexity.

- Group VMs and VMDKs into VPGs
- Maintain all properties of a VPG's VMs
- Test recovery, failover and failback of the entire VPG
- Seamless support for vMotion, DRS and HA while replicating
- Application protection policy and QoS
- Leverage built-in support for VSS and VMware vApp objects

Click-to-Protect – Simplifying Disaster Recovery

Select any VM in vSphere vCenter, click the Zerto tab and it's protected. It's that simple – no storage configuration necessary, no agent installation required. Zerto protects at the VM and VMDK level, which means that protection decisions can be made without any storage constraints.

- Replicate single or multiple VMs
- Protect multiple VMDKs connected to the same VM
- Support replication of RDM devices to a remote VMDK or RDM
- Use an intuitive GUI embedded in vSphere vCenter
- View and manage local and remote sites from the same vCenter

Do It All – Replication, Testing, Recovery, CDP, Migration, Reporting

Zerto eliminates the need to use different solutions for your DR needs. All required work flows are built-in with easy-to-follow and scalable wizards:

- Failover one or more VPGs, including automatic reverse replication
- Recover to a historic point-in-time with journal-based CDP
- Recover volumes instantly, in read-write format
- Test failover, including full remote recovery in a sandboxed zone
- Migrate workloads to a remote data center
- Get comprehensive reporting on all system-wide activities