WHITE PAPER

NEVERFAIL
CONTINUOUS AVAILABILITY

NF CONTINUITY ENGINE VS AZURE SITE RECOVERY

Disaster Recovery (DR) has never been more important than it is now. We are experiencing catastrophic hurricanes, earthquakes, fires, terrorist or cyber attacks and now even pandemics. As such there are many different DR solutions available on the market to help restore business services in the event of a disaster. Many organizations are now leveraging public clouds to ensure the survival of their businesses while improving up-time and reliability of their infrastructure.

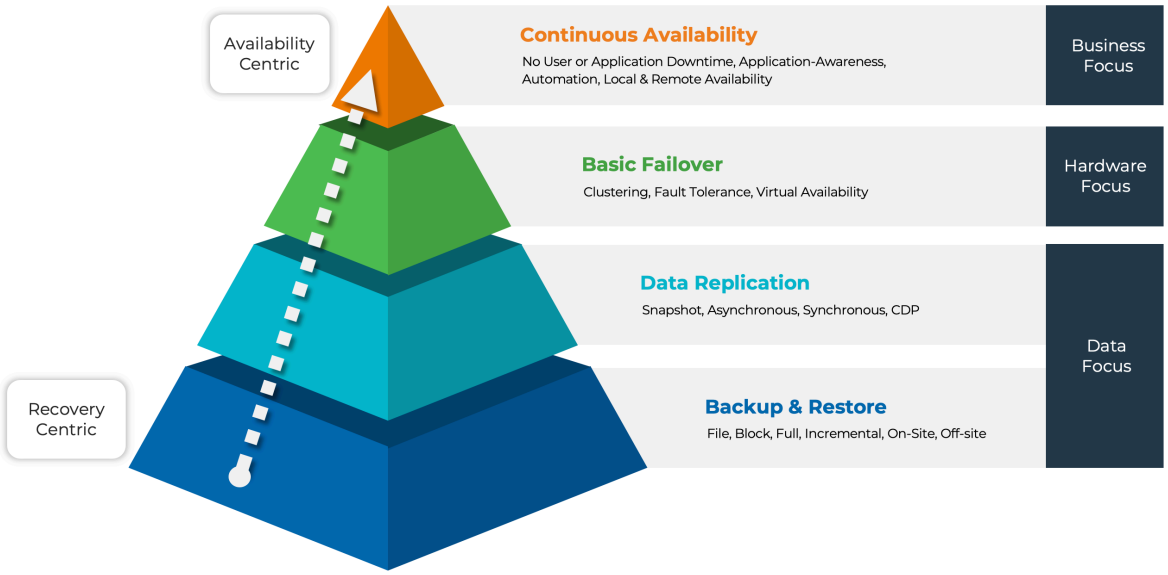
Microsoft Azure is a popular public IaaS offering that has additional services to help their customers recover in the event of a disaster. We will now discuss some differences between Neverfail Continuity Engine and Azure Site Recovery in its self-managed or DRaaS form. This will not be a feature for feature comparison but rather is designed to describe the advantages of using Continuity Engine for your most critical applications and why it adds value.

Neverfail Continuity Engine

Continuity Engine is a business continuity and disaster recovery technology that is built on application aware failover. This provides near-zero downtime for mission critical applications. With over 20 years of maturity, Neverfail has a proven technology for Continuous Availability that is more than just DR; it's an intelligent framework for ensuring critical faults in the application and OS stack are detected in real time, enabling fast recovery.

Continuity Engine is a continuity technology that can run in any environment. The secret to ensuring recovery time objectives (RTOs) of 30-90 seconds is in its "true clone" based architecture. Neverfail takes a clone copy of the original server and is hidden from the network and running real-time replication into the passive clone. The recovery point objective (RPO) is measured in milliseconds and RTO are 30 to 90 seconds regardless of the distance between the production server and its passive clone. Engine also does not require any additional servers to enable replication on premise or premise to cloud. Engine nodes monitor themselves and provide intelligence that is shared by all nodes in the cluster.

Continuous Availability is critical to enabling hands-free failover due to the issues mentioned above. Most protection technologies fall into three categories: Data Protection, Hardware Redundancy, or somewhere in between. These technologies can provide replication and even basic failover capabilities but can not catch all issues that could terminate or interrupt the delivery of the mission critical application services. Neverfail Continuity Engine provides a higher level of protection that is designed for true high availability centric environments. This means that Continuous Availability is designed to focus on full business restoration.



Failover is triggered two ways.

First, Continuity Engine with Continuous Availability uses threshold rules that allows Engine to monitor all aspects of the application server. This is powered by the Application Management Framework (AMFx) that monitors the health of the server, network connectivity, application services, and available compute resources via a set of threshold rules and provides recovery actions that proactively respond to failure events. These rules can trigger automatic failover due to internal application server failures.

Second, Continuity Engine can move workloads on demand between different nodes in the cluster for various reasons.

1. Continuity Engine can be used as a migration tool (similar to Azure SR) from one datacenter to Azure. However, unlike Azure SR which is focused on Azure Cloud, with Continuity Engine, you can migrate regardless if it's on premise or into any private or public clouds transparently in one product.
2. It can be used to offload traditional backups to passive nodes, eliminating backup windows. Backups can be performed during the day with zero impact to mission critical applications and its users.
3. Continuity Engine allows patching of Windows Servers with minimal downtime thus increasing SLAs to true 99.999% availability. There are two major benefits to this approach:
   i. There are times when the windows update process can take from several minutes to several hours to complete. With Continuity Engine, those security updates can be done on the passive nodes first and then users can "switchover" to a passive node (made active) in 30-90 seconds. Then the production server can be patched ensuring the maximum amount of uptime for the application.
   ii. Users can safely test patches on passive nodes thus proving they work. Since these are "true clones", a successful patch update on passive nodes guarantees a successful update on the production server.

Continuity Engine provides a clean process for failover and switchback process. The process is the same regardless if the servers are physical or virtual. It is storage and hardware agnostic so replicating and failing over between any hypervisor is supported.

Continuity Engine supports both HA and DR out of the box. You can choose how you would like to protect your server. Customers also have the option of a three node configuration that allows both HA and DR providing protection from all forms of failures which includes human error, application, OS, networking and even cyber security attacks.

Neverfail provides the most flexible licensing options for enabling perpetual, term and monthly rental for MSPs.

Azure Site Recovery

This product is a native platform integrated continuity solution that provides DR and migration capabilities for both on premise physical or virtual machine infrastructure or Azure to Azure DR. Azure DR functions (similar to Zerto or VMWare SRM) where servers are replicating from premise to cloud or in the Azure cloud to cloud. However, the replicated VMs are stored in the Azure blob storage. These physical or virtual machine assets can be recovered from the Azure blob repository (vault) in the case of a datacenter failure.

Azure Site Recovery requires the use of a configuration server to enable premise to cloud deployments. The configuration server coordinates communications between on-premises VMware or Hyper-V hosts and Azure. It also manages data replication.

When you look at the details of what Azure SR does, it is essentially backup with failover orchestration. It's designed to be a true DR tool but does not have full application awareness. It does integrate with SQL, Exchange and Oracle to provide application consistent recovery. However it does not understand application failure events and what caused it.

The Azure SR UI allows for DR testing and recovery isolation. However, spin up times can take up to 10 minutes per VM as each has to be built on demand and recovered from the vault. This increases tremendously the RTO with large scale recoveries.

Since the replication is very close to real time, RPO is presumed to be low. Reversing replication is supported from Azure to premise VMs. However, reversing replication to physical machines is not supported.

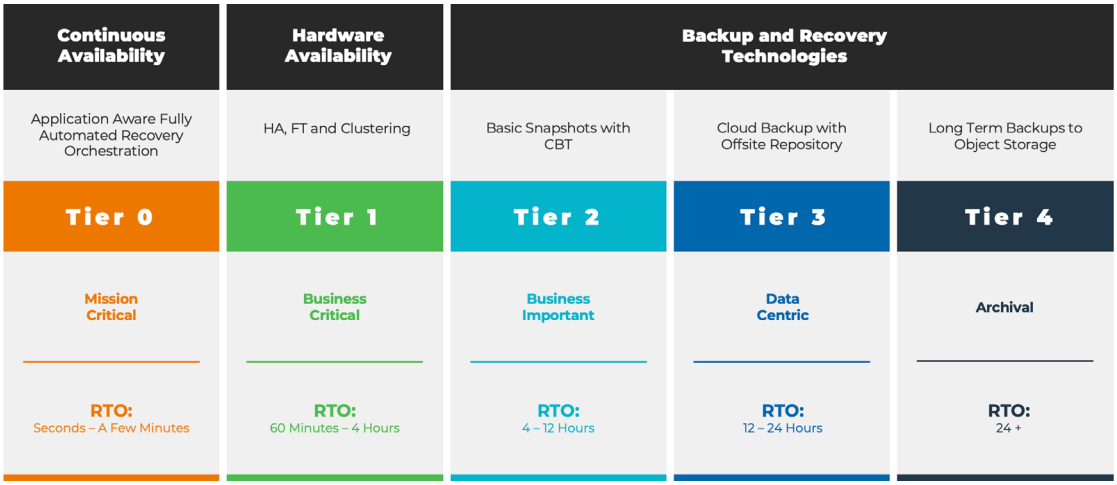
Although the cost is waived for the first 30 days, each protected application server costs about $25 plus storage costs.

Criticality Matters

Clearly understanding the criticality of the application plays a key roll. In the following diagram, you will be able to figure out what technology to use based on its criticality and how you want to recover.

Most applications fall into Tier 2 or lower. These are applications which means that its an application that is needed by the business but organizations could live without them for up to a day or longer. However, if your application is "Business Critical" which means that it needs backing operations in 1 - 4 hours; this is considered a Tier 1 application. A technology like Azure Site Recovery could be sufficient for these needs if it's strictly DR. This would give the user the time they need to spin up the VMs and restore business services from the vault.

Recovery Tiering



When it comes to Tier 0, applications that need to be recovered locally and in the cloud, in order to get to recovery of 30-90 seconds you will need real application aware failover. This is just not possible with Azure SR. This is the only way to ensure your applications can be restored in the event of failure within the SLA. Why? Because of the way Continuity Engine provides failover. Using a true cloned-based architecture, Continuity Engine functions like a HA cluster in an Active/Passive/Passive mode. Users simply see a momentary loss of the application service and then its back online.

Passive nodes do consume compute resources but its minimal and there is no users active on them. The advantage is it provides the fastest recovery to ensure mission critical applications continue operating. Every second counts and for some organizations, waiting for VMs to spin up could cost tens of thousands of dollars per minute. Remember, any application that runs on Windows can be protected at Tier 0 with Continuity Engine. That is not the case with Azure SR.

Conclusion

Continuity Engine is built for Tier 0 applications! With true application awareness, Continuity Engine provides a holistic approach to business continuity and disaster recovery over common disaster recovery tools. Continuity Engine focuses on providing Tier 0 protection for Windows based application servers and Windows 10 physical and virtual desktops. In fact, Continuous Availability provides the highest level of protection which means from a pricing perspective, Azure SR can be a cheaper overall solution but you get what you pay for. Simply put, backup with failover orchestration DR solutions are not designed for the mission critical applications.

About Neverfail

Neverfail enables businesses to achieve 100% uptime through the world's most resilient business continuity and secondary storage solutions. Made for mission-critical businesses, Neverfail solutions mitigate the risk of downtime in the face of any potential outage. By delivering seamless business continuity, we empower our partners and clients to realize their full potential without the risk of downtime.

Honeywell vmware Mitel McKESSON citi Bank of America