WHITE PAPER

NEVERFAIL
CONTINUOUS AVAILABILITY

CONTINUITY ENGINE: PROTECTING VMWARE VCENTER SERVER FROM DOWNTIME

A true clone, host and Continuous Data Protection-based high availability solution provides a simpler, faster and less expensive method of protecting physical and virtual infrastructure, applications and data in the event of a service outage.

Introduction

Applications today don't just support the business, they are the business. Four industry trends are driving the need for business continuity across traditional and cloud deployments.

- **Business applications.** The increasing reliance of business on applications makes downtime and data loss unacceptable. These applications are often hosted on VMware's vSphere virtualization or vRealize cloud suites.
- **Business models.** New SaaS business models are mission critical, always-on and on-demand.
- **Facility and services outages.** Threats to business continuity such as unplanned IT and telecom outages, adverse weather, interruptions to utility supply, fires, security incidents, earthquakes and acts of terrorism.
- **Application outages.** Major outages that are triggered by root causes such as complex unserviceable application architectures, software bugs and failure of underlying infrastructure.

Several high availability, disaster recovery and clustering solutions are available to avoid or protect against downtime, but they each have their limitations and their solutions.

- **High Availability.** VMware vCenter Server Availability protects IT workloads at the hypervisor level but not adequately at the physical server or application levels. vSphere Fault Tolerance and Application HA have limitations on remote operation. An application monitoring system could be integrated with vSphere HA Clusters, so that virtual clusters become application-aware and can remediate sick applications before they fail and cause downtime.
- **Disaster Recovery.** VMware Site Recovery Manager with vSphere Replication is a snap and replicate technology. This means that availability and recovery are not as aggressive as with superior technologies such as Continuous Data Protection (CDP). A CDP based disaster recovery (DR) solution extends vCenter and VMware Site Recovery Manager (SRM) workflows to include physical servers and applications.
- **Clustering.** Windows Server Failover Clustering (WSFC), previously called Microsoft Cluster Server (MSCS) protects the physical server provided it runs Windows. Other operating systems are not protected by WSFC. HA and DR solutions need to be OS and hardware agnostic and versatile, without single points of failure.

A true clone, host and CDP based high availability solution provides a simpler, faster and less expensive method of protecting physical and virtual infrastructure, applications and data in the event of a service outage.

> With relentless expansion of the Internet resulting in 24 by 7 global activities, application and system availability continue to become more and more critical.

Why customers need better BC/DR on virtualized VMware infrastructure

Neverfail has deep, ongoing experience of collaboration with VMware. Our Neverfail HA/DR technology is at the core of VMware® vCenter Server Heartbeat™, VMware's high availability solution for VMware vCenter Server. This experience has afforded Neverfail unparalleled insights into opportunities to deliver solutions that enhance business continuity for customers running VMware vSphere and other products. VMware provides for protection of virtualized infrastructure; however, recent changes enacted in vCenter 6.x and 5.x have created gaps in business continuity planning and operations. Fortunately, Neverfail Continuity Engine can extend the scope of business continuity functionality offered by VMware to fill the following gaps:

- **Architectural Change.** Unlike vCenter 5.x, VMware has split out nearly 40 of the vCenter 6.x services into three distinct component tiers: core, platform and database services. These tiers need individual protection requiring a portfolio of HA software. These services cannot tolerate lengthy downtime that might cause hosted application workloads to fail. Common methods of providing high availability such as snapshot based virtual machine (VM) restart do not shorten downtime in the event of a failure. Host-based high availability focused on Continuous Data Protection (CDP) is a superior solution for shortening the downtime to near zero.
- **No application protection.** While VMware HA provides complete protection from host server failures, it can't detect problems with applications running on those VMs. This is the key limiting factor for customers seeking to protect critical workloads since many threats that cause downtime are due to

application defects or operator error.

Neverfail Continuity Engine provides deep application awareness, proactive monitoring, remediation and multiple levels (that is, local and site-wide) of redundancy protection for superior business continuity protection.

- **Homogeneous only protection.** Current HA solutions such as VMware's hypervisor based solution work best with VMware. They protect either physical, virtual, data or applications well but not all at the same time. Multiple hypervisors, Windows OS and vendor offerings and applications can be protected using Continuity Engine.

  Continuity Engine solves the problems posed by a heterogeneous server landscape by seamlessly integrating physical servers within SRM Recovery Plans. By leveraging Continuity Engine, you can now standardize on SRM to protect your entire server inventory, not just applications deployed on vSphere.

- **Advanced skills required.** Maintaining high availability virtual, physical and applications infrastructure requires advanced skills, training and certifications in various VMware and 3rd party protection technologies. These modules (for example, Microsoft, F5 and Symantec) need to interoperate. This can lead to complex administrative overhead because of multiple protection models to support. Known for being easy to install and use, Continuity Engine provides seamless integration and automated deployment in VMware environments.

- **Too many point solutions.** There are 5 alternative protection technologies but no unified solution for protecting the latest 6.x and 5.x editions in the event of a service outage. [2] Continuity Engine unifies business continuity for Windows applications across the enterprise.

- **Expensive.** VMware solutions are known to have higher total cost of ownership (TCO} because of the complexity of maintaining multiple software components for BC/DR. Alternate competitively priced BC/DR solutions for the small and medium business (SMB) market that work well, such as Continuity Engine's affordable true clone architecture, do not consume additional application licenses. Savings can be achieved on licensing and maintenance costs.

  Continuity Engine, an architecturally superior true clone, host and CDP based high availability solution, provides a simpler, faster and less expensive method of protecting physical and virtual infrastructure, applications and data in the event of a service outage. Both single and multi-site deployments can be protected for business continuity as described in the two sections below.

> Continuity Engine provides a simpler, faster and less expensive method of protecting physical and virtual infrastructure, applications and data in the event of a service outage.

Complementing VMware HA Solutions with Continuity Engine for Single Site Deployment

"VMware only" availability solutions are not adequate for business continuity of VMware vCenter based infrastructure, because of the constraints mentioned above. Continuity Engine provides and complements VMware virtualization based solutions to provide complete protection in at least three single site deployment models:

- Single local vCenter server with embedded or external Platform Services controller
- Clustered local Windows based vCenter Server with external controller
- Load Balanced vCenter Servers with external controllers

Protecting single local vCenter server with embedded controllers

This deployment model works for single standalone sites with VMware virtualization infrastructure which supports only one VMware product or solution. The fault domain is small and local. Replication between embedded Platform Service Controller (PSC) instances is not supported by VMware. Continuity Engine adds high availability of vCenter and platform services in this customer deployment.

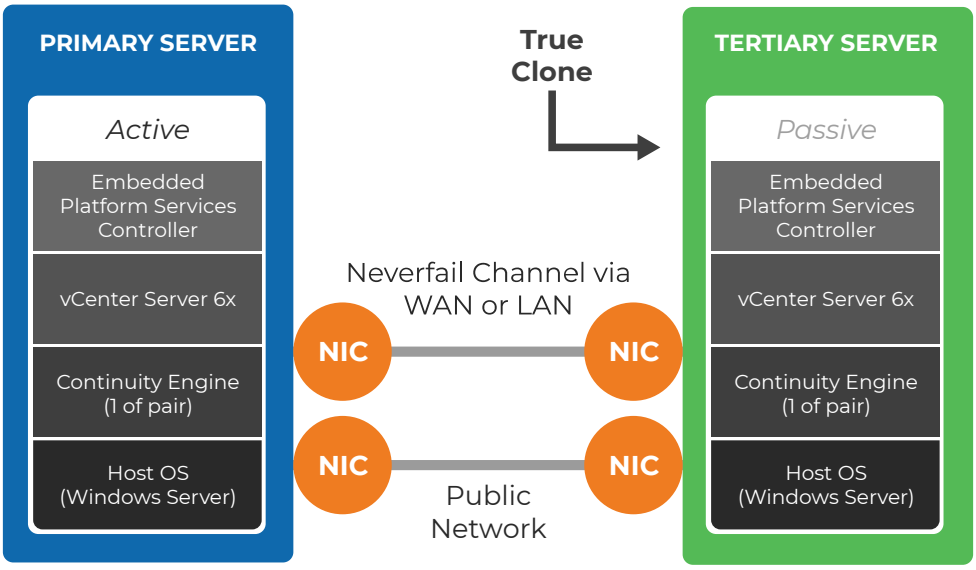

Figure 1: Continuity Engine High Availability protection for a single embedded vCenter server controller

Clustering based high availability for Windows based vCenter Server

With vCenter 6 (and also vCenter 5.5 U3) VMware supports a two node cluster (active/passive) built on Windows Server Failover Cluster for high availability.

- **Benefits.** This solution helps reduce downtime for maintenance operations such as patching or upgrades, on one node in the cluster without taking down the other vCenter Server and database with its shared nothing architecture.
- **Limitations.** Unlike the vSphere HA cluster option, the WSFC option works only for Windows virtual machines and does not support the vCenter Server Appliance. In addition, the back end Microsoft SQL database has to be protected separately with SQL Clustering

Continuity Engine provides a simpler, easier to use and more versatile protection for vSphere environments than using Microsoft WSFC alone.

- **Protection for any application.** Continuity Engine protects any application that runs on windows such as Exchange, SharePoint, MSSQL, File servers, etc. Ensures critical applications are recoverable in seconds to minutes.
- **Simpler protection setup.** Continuity Engine simplifies the ability to protect vCenter complicated Windows File Cluster (WFC) including having file share witness servers. Setup wizards simplify the deployment for protecting critical applications within minutes.
- **Added database protection.** Provides built-in database protection either using vPostgres, SQL Express and/or external SQL Server. Embedded databases can also be protected, unlike with some other solutions.

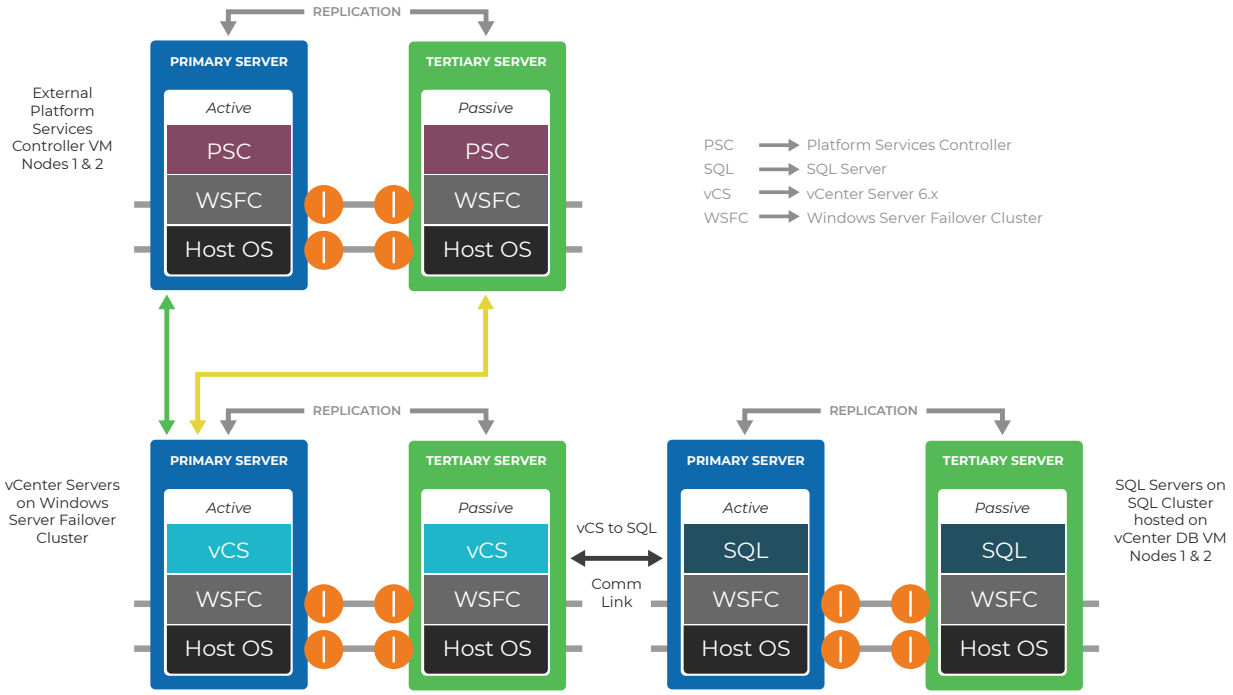

Figure 2: WSFC Clustering based high availability for Windows based vCenter Server

High availability for local vCenter Servers & external PSCs using load balancer

vCenter with an external Platform Services Controller is recommended for bigger and more complex VMware environments. External Platform Services Controllers support replication between them but do not provide any built-in load balancer. It is necessary to use a third party load balancer. Instead of the load balancer, an enhanced alternative architecture that is more beneficial in simplicity and cost is the one using Continuity Engine to add local HA.

This model of deployment protects the external platform service controller service by having multiple instances of PSC locally behind a load balancer. Failure of a PSC does not impact the usage of the infrastructure. The PSCs should also be separated from each other physically using anti-affinity rules. The PSCs replicate state information. vCenter Server nodes are individually clustered with WSFC for HA. The vCenter Servers interact with the PSCs through a load balancer.

- **Advantages of this configuration:** Provides high redundancy locally for all the components.
- **Disadvantages of this configuration:** Inadequate protection at the application level. The load balancer is an added capital and maintenance expense.

Continuity Engine adds the benefits of application monitoring and continuous application and data protection. It eliminates the need for load balancing deployments for the PSC as shown in Figure 4 on the next page.

The combination of VMware HA and Continuity Engine delivers protection from the broadest range of threats in order to keep your critical applications continuously available.

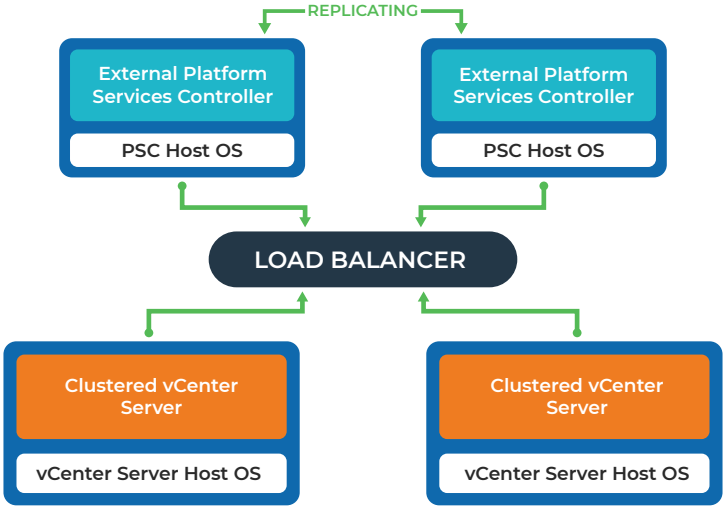

Figure 3: Local vCenter and PSC High Availability with Load Balancer

Reference: VMware blog on vCenter HA [3]

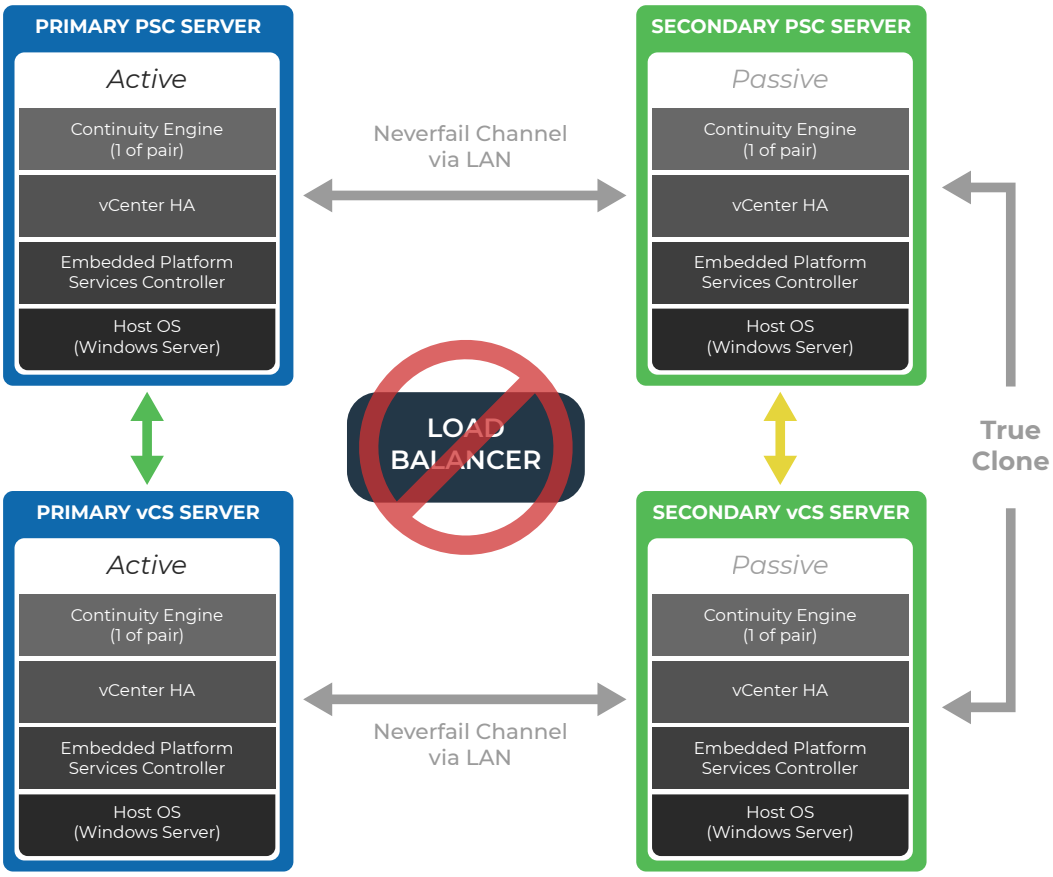

Figure 4: Local vCenter and PSC High Availability without Load Balancer and with Continuity Engine

VMware HA and SRM

VMware vSphere HA minimizes downtime caused by a local host server hardware or operating system failures. It automatically restarts affected VMs on a different host server within a virtual cluster. Like Site Recovery Manager (SRM), its strength lies in its ease-of-use. With a single mouse click, any server can be protected within a virtual cluster. In the basic configuration of VM monitoring, vSphere HA checks for regular heartbeats and I/O activity from the VMware Tools process running inside the guest.

While VMware HA provides some protection from host server or operating system failures, it can't detect application problems running on those VMs without access to VMware application monitoring APIs. Access to these APIs require the additional purchase of modules like vRealize and vSphere Application HA.

In addition, if there is logical corruption of a VM, resetting a VM onto another host server would be problematic since restoration would occur to the same VM. This is the key limiting factor for customers seeking to protect against downtime with critical workloads. Many threats that cause downtime are due to OS or application defects or operator error. Neverfail Continuity Engine does not have this limitation.

Neverfail Continuity Engine Alternative

Continuity Engine deploys a broad range of instruments within the VM to monitor the health of your critical applications without the need for other third party application monitoring products. In real time it determines whether they are running correctly and measures their consumption of system-level resources and application-level behaviors such as response times, service availability and database availability. Monitored parameters are interpreted by a rules-based model that identifies the failure signature of any application component before it actually fails.

When application-level failure events are detected, Continuity Engine leverages multiple recovery options ranging from simple notification of an event, trigger of VMware HA on the production server, restart of the application, restart of a service or failover to a standby passive copy of the server.

A built-in Data Rollback Module (DRM) provides periodic VSS snapshots that enable recovery in the event of logical corruption of the protected data set. This provides a higher level of protection for quick restoration of application data.

Continuity Engine is architected to use a separately managed but cloned copy of the production system. The risk of OS corruption is minimal on the passive nodes since the binary changes are not replicated. It also provides a single availability solution for physical and virtual platforms.

Complementing VMware HA Solutions with Continuity Engine for Multiple Site Deployments

By providing unparalleled protection against any type of downtime, Continuity Engine ensures that critical applications remain available regardless of the source of the threat.

Two multi-site deployment configurations (with and without local HA) where Continuity Engine provides superior availability protection to VMware only solutions are described below.

Multiple Site vCenter Servers and PSCs — Basic Architecture Without Local HA

In this configuration (see Figure 5), each site is independent with PSC replication between sites. Each vCenter Server is aware of the multi-site topologies and uses the local PSC under normal circumstances. This topology supports Enhanced Linked Mode (ELM) operation with interconnected PSCs for redundancy. In vSphere 6 the Windows-based and Virtual Appliance-based vCenter Servers have the same operational maximums and can belong to the same linked mode configuration.

Advantages of this solution. It supports HA from a remote site using VMware Enhanced Linked Mode. Customers are able to seamlessly move the vCenter Servers between PSCs when necessary. This ELM configuration replicates all license, global permissions, tags and roles across all sites. ELM provides a single point of management for all vCenter Servers in the same vSphere domain.

Disadvantages of this solution. It does not provide the best degree of high availability locally.

An alternative architecture (see Figure 6) that adds local HA using Continuity Engine is more beneficial. It is a more cost effective solution for vCenter protection. It enhances ELM based service availability. Continuity Engine provides orchestration of failover for segregated vCenter components running on multiple servers. It significantly reduces the bandwidth requirement for DR.

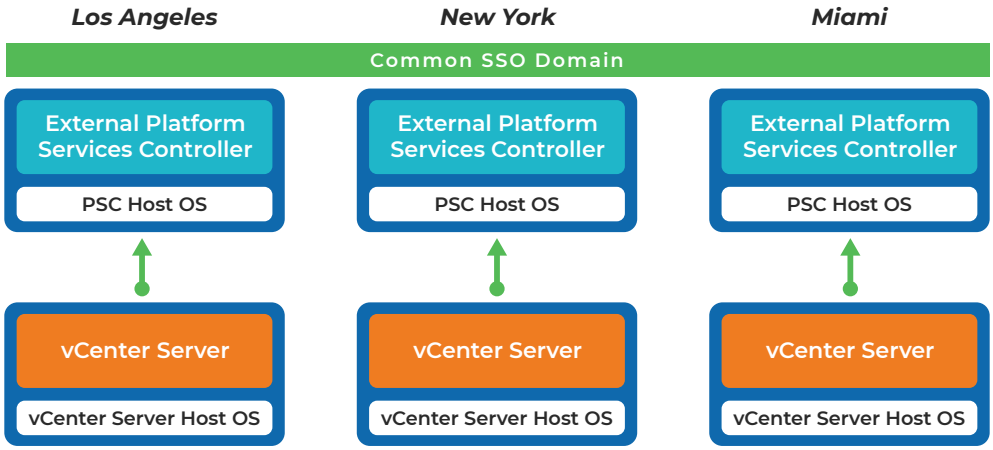

Figure 5: Multi-site vCenter Servers and PSC basic architecture without local HA

Reference: VMware blog on vCenter HA [3]

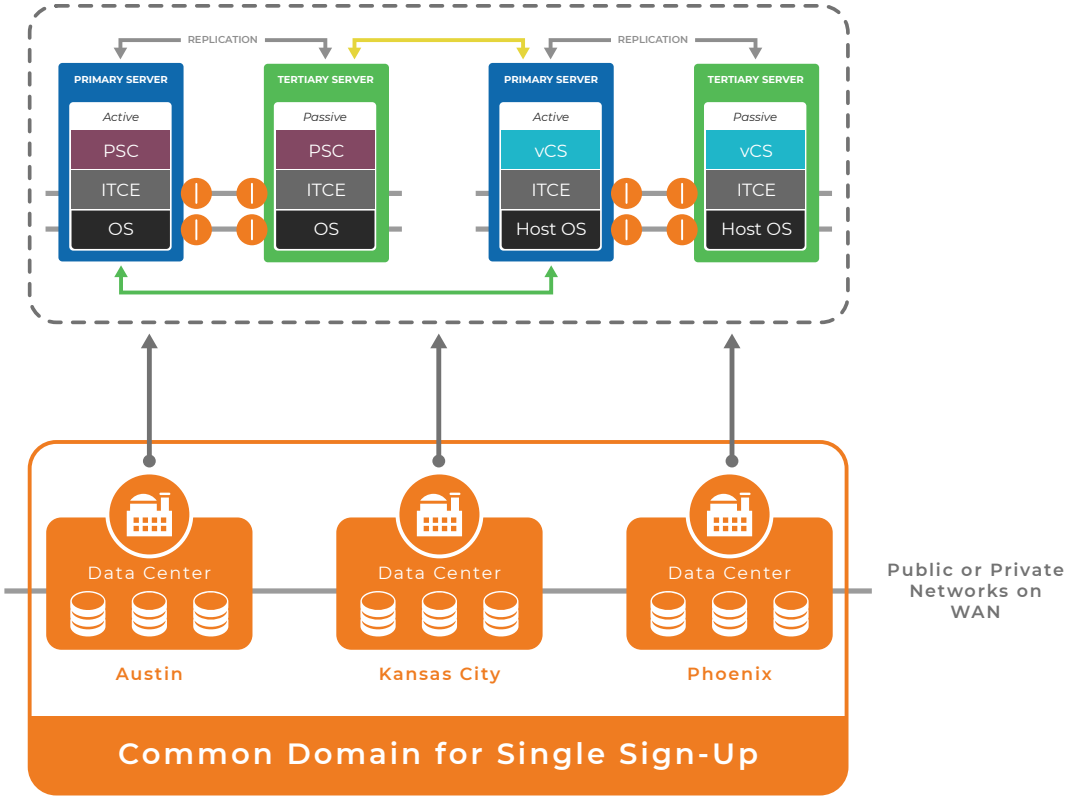

Figure 6: Multi-site vCenter Servers and PSC architecture with Continuity Engine provided local HA

Multiple Site vCenter Server & PSC with High Availability Architecture with Local HA

This deployment option (Figure 7) combines the high availability configuration at a local site with the multi-site configuration. Each site is populated with at least two PSCs for high availability. vCenter Server nodes are individually clustered with WSFC for HA.

- **Advantages of this solution: I**t provides the higher redundancy by combining local and remote HA.
- **Disadvantages of this solution:** It is complex and expensive. It leaves applications and data unprotected.

An alternative architecture (Figure 8) uses Continuity Engine for a simpler, easy to deploy, fully integrated and cost-effective solution.

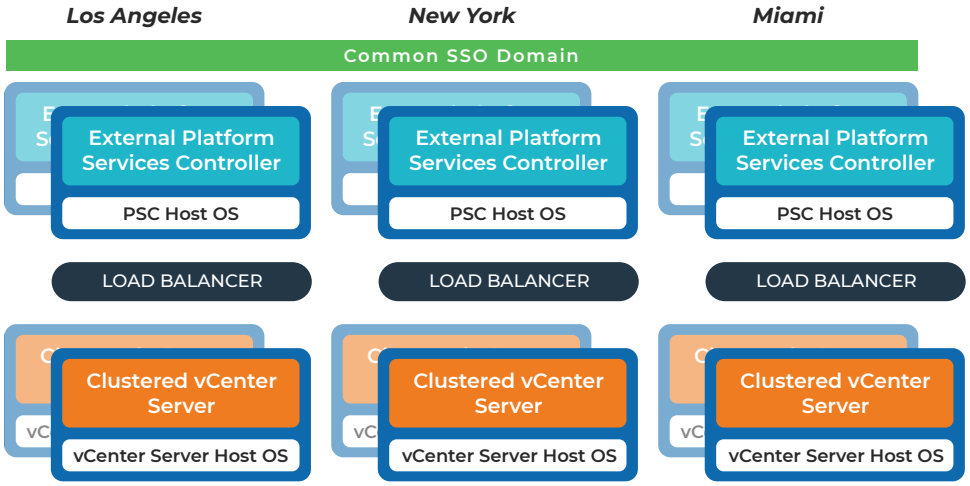

Figure 7: Multi-site vCenter Server and PSC high availability architecture

Reference: VMware blog on vCenter HA [3]

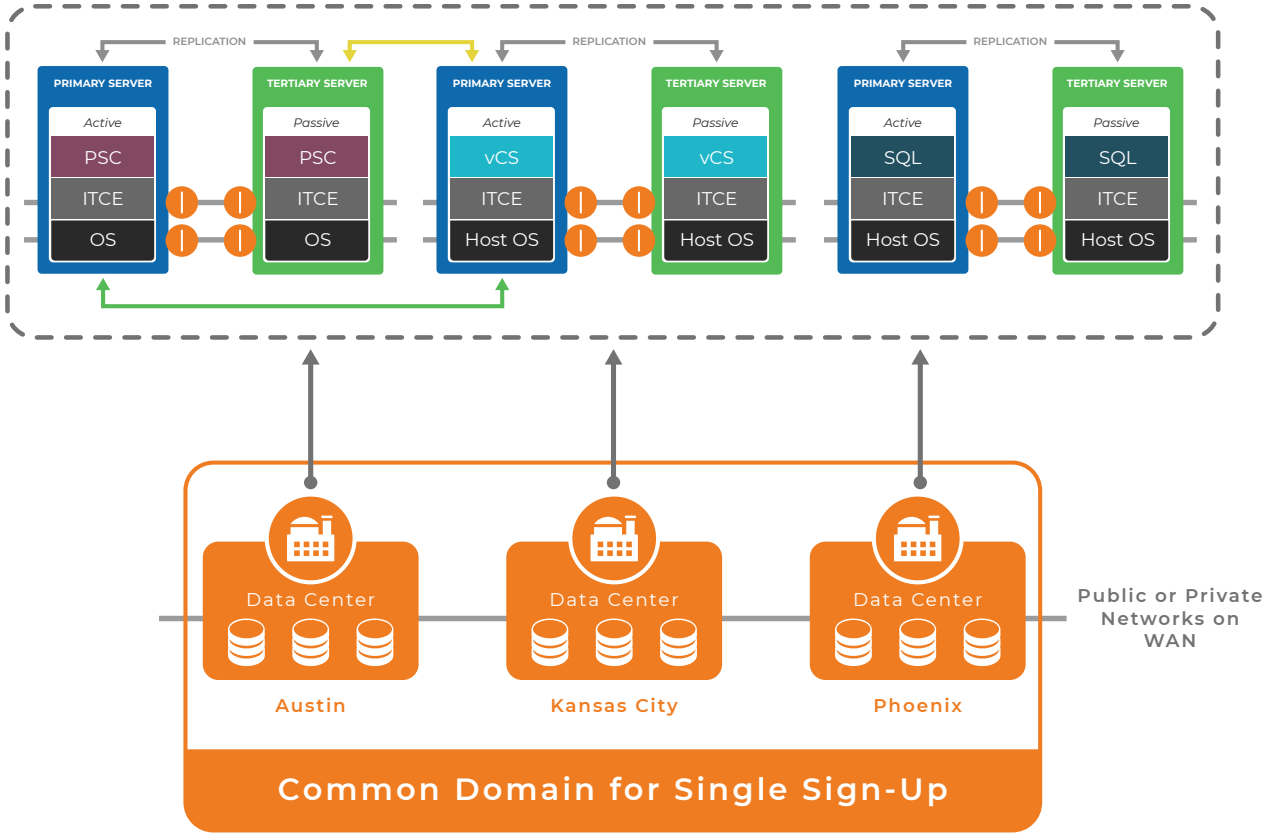

Figure 8: Alternative multi-site deployment with local HA using Continuity Engine

Neverfail Continuity Engine

We have discussed several protection models for vCenter giving you the pros and cons of each approach. Even with the PSC improvements in vCenter 6, it is still compelling to use Continuity Engine to fill in gaps in your protection model and also replace expensive and complex clustering with a simple approach.

Neverfail Continuity Engine is a part of Neverfail's business continuity management product portfolio. Optimized for use in VMware virtualized environments, the product's capabilities are a superset of those found in VMware vCenter Server Heartbeat but with a highly simplified and automated deployment process. Continuity Engine's deep integration with VMware provides complementary add-on HA/DR value in addition to, or an alternative to, the native VMware BC/DR oriented solutions such as HA and SRM. Regardless of the approach you take, consider the following Continuity Engine capabilities for use in your vCenter protection strategy.

- **Native tertiary protection.** Continuity Engine provides combined robust application aware HA and DR (pair) or a Tertiary three node (trio) out of the box. Failover in a tertiary configuration is often configured to provide automatic local failover and push button remote failover. When performing a planned switch over, the operator is given the option of performing a switch over to either the secondary or tertiary machine in the cluster. DR tests can be conducted fast without interrupting production servers.
- **True clone simplicity.** Continuity Engine provides a true clone-based architecture with no boot times, which speeds up Recovery Point Objective (RPO) and Recovery Time Objective (RTO). It keeps recovery architecture Simpler!
- **Application awareness.** Continuity Engine real-time application monitoring system has been integrated with vSphere HA Clusters, so that virtual clusters become application-aware and can re mediate sick applications before they fail and cause downtime.
- **Continuous Data Protection.** Continuity Engine is CDP based and extends vCenter and VMware Site Recovery Manager (SRM) workflows to include physical servers and applications.
- **Hardware agnostic cluster.** HA and DR solutions from Neverfail Neverfail portfolio are hardware agnostic and versatile without the need for a file share witness or use of a cluster quorum; these introduce single points of failure.

Table 1 provides a protection capability comparison that can aid in helping you choose the best vCenter v6 protection strategy.

	vSphere HA	vSphere FT	WSFC for vCenter DB	WSFC for vCenter Server	vCenter Server Watchdog	**Neverfail Continuity Engine**
Continuous Data Protection	Yes with FT and Watchdog	Yes with HA and Watchdog	No	No	No	**Yes with HA. Yes without HA in some cases**
App-aware protection	Yes with add-ons	Yes with add-ons	No	No	No without HA, FT, Watchdog	**Yes**
True clone simplicity	No	Yes. Mirrored resources. 4 CPU limit.	No	No	No	**Yes. Separately managed clones. No CPU limits.**
Hardware agnostic cluster	No	No	Yes	Yes	No	**Yes**
Native tertiary protection	No	No	No	No	No	**Yes**

Table 1: Protection Capability Comparison

Conclusion

For many years, VMware relied on Neverfail's core technology to protect vCenter. VMware vCenter Server Heartbeat was the solution of choice for administrators to protect against infrastructure and application failure or performance degradation. Although VMware has chosen to announce End-of-Availability for this product, it remains a core focus of Neverfail Infrastructure's business continuity product line.

References

[1] VMware vSphere Availability 6.0 (Guide) EN-001435-01

[2] VMware Knowledge Base article 1024051

[3] VMware vSphere blog: vCenter 6 Deployment Topologies and HA

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