WHITE PAPER: HIGH AVAILABILITY AND DISASTER RECOVERY

symantec™

Confidence in a connected world.

Protecting Business-Critical Applications in a VMware Infrastructure 3 Environment Using Veritas™ Cluster Server for VMware ESX

White Paper: High Availability and Disaster Recovery

Protecting Business-Critical Applications in a VMware Infrastructure 3 Environment Using Veritas™ Cluster Server for VMware ESX

Contents

Abstract 4

Executive summary 5

Introduction 5

Overview of VMware HA 6

VMware HA—components 6

VMware HA—architecture 7

Configuration and management *8*

Cluster agents *8*

Shared storage protection *9*

Split-brain protection *9*

VMware HA—licensing *9*

VMware HA—limitations 9

Overview of Veritas Cluster Server for VMware ESX 10

Veritas Cluster Server for VMware ESX—architecture 11

Configuration and management *12*

Cluster agents *12*

Contents *(cont'd)*

Shared storage protection *12*

Veritas Cluster Server for VMware ESX—licensing. 13

Veritas Cluster Server for VMware ESX—disaster recovery and testing disaster recovery plans . . 13

Veritas Cluster Server for VMware ESX—benefits 13

Veritas Cluster Server for VMware ESX—compatibility list 14

Hardware support *14*

Guest operating-system support *14*

Replication agent support. *14*

Application support *15*

Veritas Cluster Server for VMware ESX—use cases 15

Disaster recovery *15*

Management across heterogeneous environments. *15*

Business continuity *16*

Standardization *16*

Summary 16

About Symantec 18

Abstract

This paper begins with a brief overview of the problems of high availability (HA) and disaster recovery (DR) in the virtual environment. Due to server clustering, outages have the potential to affect many servers at once, possibly causing a corresponding failure among many mission-critical applications.

The paper then presents several fundamental criteria for evaluating HA/DR solutions and reviews the components, architecture, and functional characteristics of two that are designed to protect critical applications on VMware ESX: VMware HA and Symantec Veritas™ Cluster Server for VMware ESX. While both VMware HA and Veritas Cluster Server for VMware protect against physical server failures, only Veritas Cluster Server for VMware protects against Virtual Machine (VM) failures, application failures, application failures within VMs, and site-wide disaster recovery—providing high availability and disaster recovery to VMware environments. Using the Cluster Management Console, Veritas Cluster Server for VMware ESX also enables centralized management of all clusters at local and remote locations, as well as clusters running different operating systems.

This white paper concludes by listing other important considerations that make Veritas Cluster Server for VMware ESX a more robust solution—one that is proven to meet the pressing need for both high availability and disaster recovery in the VMware infrastructure.

Executive summary

Veritas™ Cluster Server for VMware ESX provides high availability and disaster recovery to VMware environments.

Veritas Cluster Server for VMware ESX offers the following key advantages over VMware HA:

Veritas Cluster Server for VMware ESX protects against:	VMware HA protects against:
Physical server failures	Physical server failures
Virtual Machine failures	
Application failures within Virtual Machines	
Site-wide disaster recovery	

In addition, Veritas Cluster Server for VMware ESX can work across heterogeneous, multi-platform environments and handle multi-tier applications.

Introduction

Server virtualization is becoming an increasingly common technology in the modern data center. By implementing server virtualization, businesses are able to consolidate the application workload of multiple servers onto a smaller number of physical hosts, which results in improved hardware utilization, fewer physical servers, and considerable cost savings.

With these benefits come some new challenges. Before server virtualization, a physical server failure would likely result in a single application outage. In a consolidated virtual server environment, however, a physical server outage now has the potential to affect tens of virtual servers—and bring down many applications. Thus, virtualization has placed a renewed emphasis on high availability and disaster recovery (HA/DR) in the data center. In the past, a service-level agreement (SLA) for a single application running on a single physical box might not have warranted consideration for HA/DR; however, when many applications are consolidated onto a single physical host, high availability for that host suddenly becomes paramount.

To address the HA/DR needs of their virtual server environments, companies must choose either to adapt existing HA/DR solutions (solutions that were designed for physical server architectures) or to adopt new HA/DR solutions that are designed specifically for virtual server environments.

A production-class HA/DR solution for business-critical applications should provide monitoring of the application and application resources, including the Virtual Machine, network components, storage components, and physical server. It should also provide notification during a failure of any of those resources, as well as automated failure without any manual processes, either within the same data center or to a remote data center.

Ideally, this HA/DR solution should also provide the same functionality across physical and virtual environments—as well as single management across all of a data center's IT platforms to increase operating efficiencies and reduce operating costs.

Moving from a physical server architecture to a highly consolidated virtual server architecture should not compromise the data center's high availability and disaster recovery capabilities. Using Veritas Cluster Server for VMware ESX, tailored specifically for VMware Infrastructure 3 (VI3), organizations can continue to benefit from adopting a single standard for all their high availability and disaster recovery needs across both physical and virtual server environments.

Overview of VMware HA

Recognizing that server consolidation creates more risk of application downtime in virtualized environments, VMware released VMware HA in its launch of VMware Infrastructure 3 (VI3). VMware HA is a server-based clustering technology that runs on the ESX console. It provides high availability for Virtual Machines by detecting the failure of an ESX server and restarting the affected VMs on a different ESX server configured in the same VMware cluster.

VMware HA—components

A VMware HA cluster is composed of the following components:

- **VMware ESX server**—hosts the VMs that run the applications; VMware HA installs and runs on the ESX server
- **VI3 license server**—a centrally located server where all ESX servers participating in a VMware cluster are licensed
- **VirtualCenter Management Server**—the console where all cluster-related configuration and management tasks are accomplished

VMware HA—architecture

Figure 1 depicts a typical four-node VMware HA cluster hosting ten Virtual Machines. Certain characteristics are common to all VMware HA clusters. For example, all nodes in a VMware HA cluster require access to a shared pool of storage where the Virtual Machines files are located. In addition, all nodes in a VMware HA cluster require redundant network connections over which they communicate cluster membership and node status as well as detect hardware failure. A VMware HA cluster also requires two critical services that are located outside of the cluster:

- VMware license server—a Windows®-based server where ESX servers are licensed and VMware HA is enabled
- VMware VirtualCenter server—a Windows-based management server that is used to configure VMware clusters and perform all cluster-related management activities

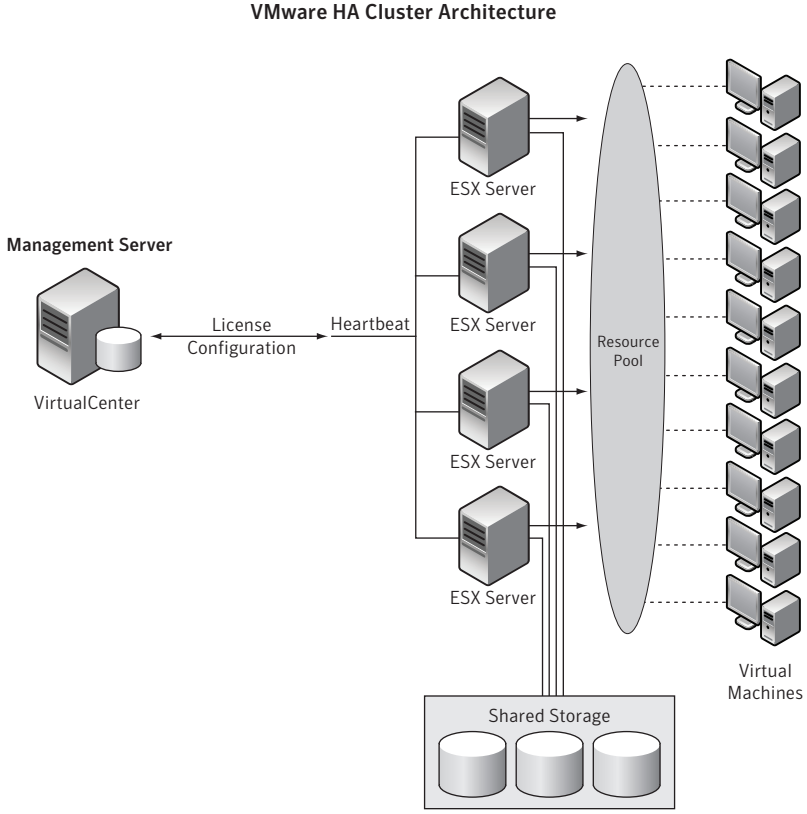

Figure 1. VMware HA cluster

Typically, the license and VirtualCenter servers are configured together on the same physical system. When designing a VMware cluster, it is important that the license and VirtualCenter server always be accessible by all ESX servers participating in the VMware cluster. Additional considerations regarding the availability of the VirtualCenter and license server are discussed under "Configuration and management."

The following are key architectural considerations when implementing VMware HA:

Configuration and management

VMware HA requires a VirtualCenter management server in order to enable and configure VMware HA. The VirtualCenter management server requires an external data store that must be purchased and licensed in addition to VI3.

VMware recommends that customers place the VirtualCenter and license servers together on the same system. In addition, careful consideration must be given to the risks associated with an outage of the VirtualCenter or VMware license server. If the VirtualCenter server goes down, administrators will not be able to make any changes or modifications to the VMware cluster. However, if the license server goes down, the VMware cluster will continue to operate for up to 14 days. If after the 14-day grace period the license server has not been restored, VMware HA will be disabled and it will no longer be possible to power-on the Virtual Machines.

Because of the critical role of the VMware license and VirtualCenter servers, it is recommended that these services be made highly available using a Windows-based clustering solution such as Veritas Cluster Server for Windows.

Cluster agents

When an ESX server is placed in a VMware cluster, an agent is installed on the ESX host. This agent sends a heartbeat over the service console network to the other ESX servers in the cluster. The loss of a heartbeat from an ESX server indicates a failure and triggers a cluster “takeover” of the affected VMs by the other hosts in the cluster. For this reason, it is important to configure redundant network connections between the nodes in a VMware cluster.

Shared storage protection

VMware HA relies on the advanced file-locking capabilities of VMware's VMFS clustered file system to protect against data corruption caused by having multiple ESX servers attempting to access the same VM files at the same time. When a VM is brought online, file-level locks are used to prevent other ESX servers from accessing the same files. In the event of a cluster takeover, the ESX servers performing the takeover must first wait for the VMFS locks to time out and be released before they can perform the takeover.

Split-brain protection

VMware HA allows administrators to define the behavior of an ESX server if it should find itself isolated from the other members in the cluster (a situation commonly referred to as split brain). By default, the ESX server will initiate a graceful shutdown of the VMs and release the VMFS locks, thereby allowing the VMs to be brought online by other nodes in the cluster. Optionally, the administrator can override this behavior and have the ESX server continue to run the Virtual Machines; in this case, the server will maintain its VMFS locks and prevent the other nodes from performing a takeover.

VMware HA—licensing

VMware HA is a separately licensed component of VI3. A VMware HA license is included with the purchase of a VI3 Enterprise license, or it can be purchased as an add-on with a VI3 Starter or Standard edition license.

VMware HA—limitations

VMware HA relies on an external configuration server, which sits outside the VMware cluster, for licensing and configuration. In addition, the configuration server requires a dedicated data store that must be purchased independent of VI3. This design adds hidden cost and creates a potential single point of failure.

VMware HA is focused exclusively on hardware failure. It offers no protection against the failure of an individual VM, the failure of an application running inside the VM, or an outage in a network or storage component.

VMware HA only supports clustering of VMware ESX servers. Other high-availability solutions are needed to protect applications running on physical servers or running in non-VMware virtual server environments (e.g., Solaris™ Zones, IBM® Micro-Pars).

VI3 does not provide an automated DR solution. VMware claims a limited DR capability. They claim that integrating VMware Consolidated Backup with traditional backup and restore technologies such as Veritas NetBackup™ will help customers bring up servers after a site disaster. Reliance on data backup and restore to accomplish DR typically results in long outages and puts heavy demands on highly skilled administrators in order to succeed. In non-critical application environments, it may be acceptable to endure the long outage windows associated with sending copies of backup media to a DR site where they can be restored manually. However, this type of DR solution is not acceptable for mission-critical application environments that cannot afford prolonged periods of downtime. To provide DR for mission-critical applications running inside a VMware virtual server environment, VMware must rely on third-party products such as Veritas Cluster Server for VMware ESX to integrate available replication technologies together with wide-area clustering to provide an automated DR solution.

Also, VMware's VMotion technology is often mistakenly seen as a solution for unplanned downtime. VMotion allows running VMs to move dynamically between physical ESX hosts with no noticeable impact to the applications or end users. However, VMotion requires that the VMware ESX server, the VM, and the applications always be in a running state. If any of these three components fails, VMotion cannot be used to restart the service or recover from the outage.

The value of VMotion comes from its performance of planned maintenance tasks and its ability to balance the workload of many VMs across a small number of ESX hosts. However, the ability to protect against outages requires clustering software that is able to detect a failure and then initiate recovery steps. VMotion has no capability to detect faults and offers no protection against server or application outages.

Overview of Veritas Cluster Server for VMware ESX

To provide protection for mission-critical applications that have stringent SLAs, Symantec offers Veritas Cluster Server for VMware ESX, a new release of the market-leading cross-platform clustering software, Veritas Cluster Server, that has been customized specifically for VMware Infrastructure 3.

Veritas Cluster Server for VMware ESX is a server clustering solution that runs on the ESX server and is designed to protect against outages that affect the availability of applications running inside VMware VMs. Whereas VMware HA protection is limited to protecting against physical ESX server failures, Veritas Cluster Server for VMware ESX adds additional protection for individual VMs, applications running inside the VMs, and the underlying storage and network components.

In addition, Veritas Cluster Server for VMware ESX provides a robust disaster recovery solution by linking geographically dispersed clusters and automating the steps for recovering from a disaster.

Veritas Cluster Server for VMware ESX—architecture

Figure 2 depicts a typical four-node Veritas Cluster Server for VMware ESX cluster. Like VMware HA, Veritas Cluster Server is a server-based clustering solution and shares the same requirements for shared storage and redundant network connections. Veritas Cluster Server for VMware ESX runs on the ESX console and provides high availability for Virtual Machines by detecting failure of an ESX server and restarting VMs elsewhere in the cluster. In addition to protecting against a physical ESX server failure, Veritas Cluster Server for VMware ESX also provides protection for network and storage outages, individual VM outages, and application outages.

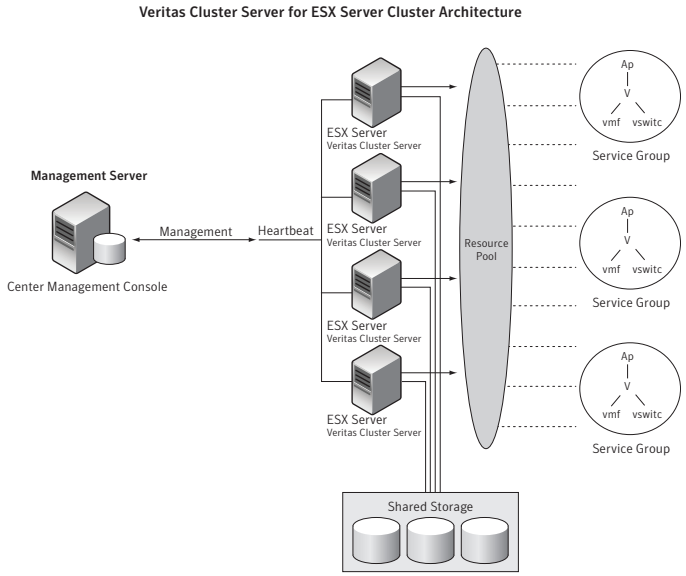

Figure 2. Veritas Cluster Server for VMware ESX

The following architectural components are important factors to consider when implementing high availability with Veritas Cluster Server for VMware ESX:

Configuration and management

Veritas Cluster Server for VMware ESX offers the combination of a command-line interface or a Web-based GUI for configuration and management. The Veritas Cluster Server for VMware ESX Web GUI is configured as a highly available resource. Multiple clusters at both local and remote locations can be centrally managed from a single Veritas Cluster Server management console.

The Veritas Virtualization Manager automates the task of placing Virtual Machines under Veritas Cluster Server control by detecting existing VMs, encapsulating them into Service Groups, and placing them under Veritas Cluster Server control.

Cluster agents

The Veritas Cluster Server engine runs on the ESX servers along with a robust agent framework that enables Veritas Cluster Server to monitor critical hardware components on the ESX host, such as NICs and HBAs. Included in the agent framework is an agent that monitors the VMs running on the ESX server. In addition, a lightweight agent framework can also be installed inside each VM to provide protection against the failure of hosted applications. Application wizards are used to simplify the task of placing applications under cluster control.

Veritas Cluster Server for VMware ESX provides agents for applications such as Oracle®; Apache; Microsoft® SQL, Internet Information Services, and Exchange; and SAP. Symantec will continue to release new application agents for the leading business applications and databases to help companies protect their mission-critical IT operations. For other applications, businesses can create custom scripts that can be integrated into the agent framework.

Shared storage protection

Veritas Cluster Server for VMware ESX relies on the file-locking capabilities of VMFS to provide protection against multiple ESX servers attempting to access the same files located on the shared pool of storage.

Veritas Cluster Server for VMware ESX—licensing

Veritas Cluster Server for VMware ESX does not require a separate license server because all licensing is self-contained within the cluster. The product comes in two licensed versions: Veritas Cluster Server for VMware ESX, which enables local HA and is used in environments where DR is not required; and Veritas Cluster Server HA/DR, which enables local HA plus wide-area DR capability.

Veritas Cluster Server for VMware ESX—disaster recovery and testing disaster recovery plans

Veritas Cluster Server for VMware ESX has a global cluster option that allows a secondary site to be set up anywhere—from a separate region in the same country to the other side of the globe. It provides for automated action during a site-wide disaster—with no manual intervention. It warns administrators of a disaster and makes single-click failover of the entire site possible. The management console provides a consolidated dashboard for monitoring and controlling globally dispersed data centers.

In addition, Veritas Cluster Server for VMware ESX offers the ability to conduct testing of DR plans. Its Fire Drill feature can mount an actual storage snapshot and bring up the application on the secondary site to determine whether a DR failover will be successful. The non-disruptive Fire Drill is conducted in complete isolation from the production system.

Veritas Cluster Server for VMware ESX—benefits

Veritas Cluster Server for VMware ESX provides the following key benefits:

- All the cluster components are self-contained inside the cluster; it is not dependent on an external server to provide licensing or to perform configuration tasks.
- It is virtualization-aware and fully compatible with VMotion and DRS. Veritas Cluster Server for VMware ESX can be used in place of VMware HA with no impact on application availability.
- It is an application-centric clustering solution that protects against failure of the physical server, network and storage components, Virtual Machines, and applications running inside the VMs.
- It enables centralized management of all physical Veritas Cluster Server clusters and Veritas Cluster Server for VMware ESX clusters using the Cluster Management Console. Clusters at both local and remote locations can be managed—even those running different operating systems.

- It eliminates administrative burden and reduces complexity by providing a standard HA solution that spans operating systems and hardware platforms for both physical and virtual server environments.
- It provides disaster recovery with integrated support for hardware-based replication and wide-area clustering.
- It facilitates DR plan testing using the Veritas Cluster Server Fire Drill feature. Fire Drill's functionality makes it easy for customers to conduct DR testing monthly instead of just yearly. This increased frequency prevents configuration drift, which can lead to unsuccessful DR failovers and result in extremely costly downtime.
- It provides simple usability, such as enabling of HA or HA/DR for multiple VMs.

Veritas Cluster Server for VMware ESX—compatibility list

Hardware support

Any server that supports VMware ESX

Guest operating-system support

- Red Hat® Enterprise Linux® version 4 with update 3 (32- and 64-bit versions)
- SUSE Linux Enterprise Server version 9 with SP3 (32- and 64-bit versions)
- SUSE Linux Enterprise Server version 10 with SP1 (32- and 64-bit versions)
- Windows 2003 Standard or Enterprise with SP1 (32- and 64-bit versions)
- Windows 2000 Server or Advanced Server with SP4
- Solaris 10 (x86)

Replication agent support

- Hitachi TruCopy
- EMC Clariion MirrorView
- IBM MetroMirror
- EMC SRDF

Application support

- Microsoft IIS
- Microsoft SQL Server 2000 and 2005
- Apache 1.2, 2.0, and 2.2
- IBM HTTP Server 1.3 and 2.0
- Oracle 10g
- SAP on Linux
- Exchange on Windows

Veritas Cluster Server for VMware ESX—use cases

Key use cases for Veritas Cluster Server for VMware ESX include the following:

- Disaster recovery over wide-area networks
- Centralized management across heterogeneous environments
- Business continuity process and multi-tier applications
- Standardization

Disaster recovery

In the case of an entire site going doing down in a disaster, Veritas Cluster Server for VMware shifts all the site's DR-protected Virtual Machines onto a remote site. This remote site might be in a separate region or in a different part of the world. The failover is automated and requires no manual intervention.

Management across heterogeneous environments

Veritas Cluster Server is available on every major OS platform. As a result, it represents a centralized management framework for managing multiple data centers, regardless of geographical location.

Business continuity

Veritas Cluster Server for VMware ESX can enforce VM dependencies as well as virtual-to-physical-machine dependencies. For example, a resource dependency can be built between two resources—one on a VMware platform protected by Veritas Cluster Server for VMware ESX and another on a Solaris platform protected by Veritas Cluster Server on Solaris. This ability facilitates failover of multi-tier applications and helps meet stringent business continuity demands.

Standardization

Veritas Cluster Server allows the use of a standard set of tools across Windows, UNIX, Linux, and VMware environments. This can have a direct impact on reducing maintenance and training costs.

Summary

As companies implement server virtualization in their data centers and move from a one-application/one-server architecture to a highly consolidated virtual server environment, high availability and disaster recovery become even more important. This renewed emphasis on HA/DR virtualization has led to the inclusion of HA/DR solutions in virtual server products from vendors such as VMware.

Virtualization vendors may provide introductory high availability and disaster recovery solutions, but for business-critical applications, companies need to turn to more robust, proven solutions. With Veritas Cluster Server for VMware ESX, companies will benefit from protection against not only physical server failures, but also outages that affect individual Virtual Machines and the applications running inside them.

In addition to providing local high availability, Veritas Cluster Server for VMware ESX also provides disaster recovery support by allowing geographically dispersed clusters to be linked together. When used in conjunction with replication technologies, Veritas Cluster Server for VMware ESX can provide automated wide-area failover.

With Veritas Cluster Server for VMware ESX, companies can continue to benefit from their adoption of Veritas Cluster Server as a company-standard HA/DR solution. The same industry-leading HA/DR solution that companies have relied on for years to protect their physical server environments can now be used to protect their VMware virtual server environments as well.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 (800) 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

01/08 13584866