



Transforming Business Continuity with VMware Infrastructure and Apani

Current Business Continuity Challenges

Implementing plans to ensure business continuity for key IT services and business critical applications is an essential requirement for organizations today. Downtime of important applications is a costly proposition and extended downtime can even be fatal—industry research finds that a significant number of companies that experience extended interruption to IT services soon go out of business.

While most organizations recognize the importance of business continuity, their ability to provide high availability and disaster recovery for key applications in a physical (non-virtualized) environment is often constrained by the following challenges:

- **High costs.** Many solutions require significant investment in additional hardware, software and services. Disaster recovery plans in particular often require duplicating data center infrastructure, resulting in a proliferation of under-utilized servers.
- **High complexity.** Most traditional business continuity solutions add significant complexity to data center environments. Acquiring and managing additional servers, use of complex cluster tools, implementing and maintaining specialized software and processes all contribute to this complexity.
- **Failure to meet recovery time and availability goals.** Due to the cost and complexity of business continuity solutions, organizations are often forced to compromise on solutions that are unlikely to meet goals for availability and recovery time objectives.
- **Insufficient reliability.** Testing existing complex business continuity solutions is challenging and requires significant equipment, expertise and personnel resources. The complexity of these specialized solutions also makes them difficult to maintain.

Higher Availability with VMware Infrastructure

Industry-leading VMware[®] VMotion[™] technology allows IT administrators to move running virtual machines from one physical server to another without downtime. This capability makes it possible to conduct zero-downtime hardware maintenance by simply using VMotion to move running applications to other physical servers as needed.

VMware Distributed Resource Scheduler (DRS) can reduce unplanned downtime by automating the process of using VMotion to migrate running applications away from servers that cross utilization thresholds or moving virtual machines non-disruptively to servers that have the needed compute resources.

VMware High Availability (HA) provides easy to use, cost effective high availability for applications running in virtual machines. In the event of server failure, affected virtual machines are automatically restarted on other physical servers that have spare capacity.

Better Disaster Recovery with VMware Infrastructure

VMware virtual machines are hardware-independent so any physical server can serve as a recovery target for any virtual machine. Organizations can significantly reduce the cost of hardware for disaster recovery by repurposing underutilized existing servers for recovery targets and disaster recovery testing.

VMware Infrastructure also simplifies and accelerates recovery, helping IT organizations meet their time-to-recovery targets. Complex multi-step procedures using specialized software for bare-metal recovery and operating system recovery can be simplified to single-step file recovery because virtual machines are completely encapsulated in a small number of files and can be restored to any hardware.

Finally, VMware Infrastructure simplifies testing of disaster recovery plans and makes training personnel in disaster recovery procedures easier.

Benefits of VMware Business Continuity Solutions

Customers who use VMware Infrastructure to improve their business continuity plans experience numerous benefits, including:

Downtime reduction by eliminating planned downtime due to maintenance, or reducing un-planned downtime through economical sharing of fault-tolerant hardware features, and automated rapid restart of virtual machines.

Lower costs by implementing better business continuity at a lower cost, eliminating the need for additional hardware and specialized software.

Simplified processes by removing the complexity of maintaining duplicate physical systems for disaster recovery.

Learn More

To learn more about VMware solutions and products, visit <http://www.vmware.com> or call 1-877-4VMWARE.

Apani

Apani
www.apani.com

ISV Overview

Apani provides security software to isolate and protect both virtual and physical machines from a single management point.

Key Business Needs

Large organizations rely on a variety of physical, virtual and legacy servers. Vendors have historically offered a silo approach to protecting them—each with their own management paradigm. Organizations need a way to streamline their data security by protecting virtual environments and heterogeneous hardware with a single management solution.

Key Business Benefits

Only Apani EpiForce VM provides a single solution that secures both virtual and physical machines. Logical security zones isolate machines without reconfiguring the network, while policy-based encryption selectively encrypts data in motion. EpiForce VM fully supports VMotion (hot) and cold migration and offers protection against VM sprawl.

Business Results

By providing robust data center security, Apani EpiForce VM enables organizations to better realize the benefits of server virtualization, including support for multiple platforms, automated migration, reduced unplanned downtime, lower operating expense tied to security policy changes and more flexible management.

VMware and Apani

Only Apani EpiForce VM provides a single solution that secures both virtual and physical machines running VMware ESX Server.

Apani Products

Apani EpiForce VM has been tested with VMware ESX 3.x, VirtualCenter 2.5 and VMotion and supports a broad variety of host operating systems.

Apani® EpiForce® VM Cross-Platform Virtual Security: A Key Element of Business Continuity

High Availability Security for a VMware Environment

Industry Overview

Are you concerned about attaining reliable data security while achieving business continuity through VMware ESX?

The static nature of firewalls and VLANs are inadequate for securing a dynamic VMware ESX virtualization environment. Security solutions designed only for virtual and not physical systems force businesses to take a silo approach to data security, increasing complexity. Finally, firewalls, VLANs, NAC and multi-function virtual security software are bottlenecks and single points of failure that undermine the business continuity benefits of VMware ESX. Organizations are challenged in maintaining reliable security while realizing the business continuity benefits of VMware ESX.

Solution Overview

Apani EpiForce VM delivers reliable security so organizations can fully realize the benefits of business continuity using VMware ESX.

EpiForce VM delivers software-based access control and encryption to virtual servers and endpoints that hardware solutions cannot efficiently manage. It secures both virtual and physical IT assets, simplifying the changes required in a dynamic virtualization environment. All systems can be managed from a central console, which increases administrative flexibility.

EpiForce VM maintains business continuity through a distributed architecture with policy enforced between servers and clients. The EpiForce management system consists of an Admin Console, Admin Server and Database that can be installed in different VMs or physical systems. If a failure occurs in any redundant component, security policies are maintained yielding high availability. This architecture eliminates the bottlenecks and single points of failure common in firewalls, VLANs, NAC and multi-function virtual security solutions.

Also, EpiForce VM enforces security at the endpoint (VM) through agents. It automatically reconfigures security policy if a VM is restarted, preventing a security gap. Each agent has a settable default failure mode that maintains security policy in the event of a catastrophic management system failure. Security policy is also maintained while machines are physically moved or during VMware VMotion or VirtualCenter migration. EpiForce VM delivers reliable security contributing to business continuity.

Solution Benefits

- Enable reliable data security while achieving business continuity through VMware ESX. Deploy consistent, strong security across VMs and physical machines.
- EpiForce VM distributed architecture enforces policy between servers and clients, eliminating the bottlenecks and single points of failure common in firewalls, VLANs, NAC and multi-function virtual security solutions.
- Granular and customizable failover procedures enable EpiForce VM to be a key element in business continuity planning.
- Security policy is automatically reconfigured when a VM is restarted. Security policy deployed by EpiForce remains persistent, regardless of the physical location of a server or endpoint.
- Manage all EpiForce VM-protected machines through a single management console.
- Migrate virtual machines using VMotion or VirtualCenter without compromising security policy.

VMware and Apani

Only Apani EpiForce VM enables organizations to secure both physical machines and VMware ESX environments with a single, centrally managed solution that supports both VMotion and cold migration.