Enhancing Resiliency of VMware Virtual Infrastructures with EMC Layered Applications

Combining VMware® Infrastructure 3 and EMC® layered applications provides powerful high-availability, business continuity, and disaster recovery capabilities that can help organizations create highly resilient IT infrastructures and meet stringent service-level agreements, recovery point objectives, and recovery time objectives for critical systems.

...
organizational needs. Administrators can modify these solutions and templates to help meet enterprise RPOs and RTOs as required.

Understanding business continuity

Business continuity hinges on minimizing downtime and depends on preparation for both planned and unplanned downtime. Administrators use planned downtime to patch, update, or upgrade operating systems, applications, security signature files, and hardware. Performing these operations typically requires a well-planned sequence of administrative tasks carried out after normal operating hours, during which applications are unavailable to users. Taking a system offline for any period of time introduces risks to the organization, users, and IT systems alike.

VMware VMotion and DRS directly address these risks by helping to eliminate application and workload downtime during these periods.

Technologies that address unplanned downtime include clustering, host and SAN replication, and advanced off-site mirrored facilities. These systems and processes, typically referred to as disaster recovery or redundant failover systems, can be very expensive and require extensive IT staff training in traditional physical environments.

A VMware virtual infrastructure, combined with EMC layered applications, is designed to provide a cost-effective, highly resilient infrastructure and minimize unplanned downtime.

Using key business continuity features of VMware Infrastructure 3

Today, VMware Infrastructure 3 is a widely deployed virtualization software suite that incorporates intrinsic business continuity functionality. VMware Infrastructure 3 Enterprise Edition and VMware VirtualCenter Management Server offer high levels of flexibility and manageability to help administrators design and build resilient systems that can meet enterprise SLAs, RPOs, and RTOs.

VMware Infrastructure 3 goes beyond basic server virtualization by aggregating industry-standard x86 or x86-64 processor-based servers, shared storage, and networks into a unified resource pool, or virtual infrastructure (see Figure 1). In a virtual infrastructure, the resource pools of computing power and storage capacity are dynamically provisioned and allocated to match IT resources to specific requirements and organizational needs.

Shared storage is a fundamental component of a virtual infrastructure, enabling VMotion, VMware HA, and VMware DRS features as well as high-performance backup and restore and snapshot functionality through VMware Consolidated Backup. In a VMware virtual infrastructure, shared storage enables secure, robust, and redundant local data stores as well as accessible, duplicative, off-site storage capabilities. VMware virtual infrastructures allow IT organizations to efficiently manage data replication, disaster recovery processes, and dynamic secondary-site expansion based on their needs.

VMware Infrastructure 3 also eases the manageability of IT environments and helps protect critical application workloads and their data through built-in self-healing capabilities from I/O multipathing through network devices and SAN fabrics within a virtual infrastructure.

Key features of VMware Infrastructure 3 include the following:

- **VMware VMotion**: This technology allows the live migration of VMs to help ensure that users and their applications are not disrupted during systems maintenance and planned downtime. VMotion is critically important to providing systems availability during planned downtime in a virtual infrastructure.
- **VMware HA**: This technology delivers high availability across a virtual infrastructure without the cost or complexity of clustering solutions. VMware HA can provide cost-effective high availability for any application running in a VM, regardless of its OS or underlying hardware configuration. It also helps eliminate the need for dedicated standby hardware and additional software.
- **VMware DRS**: VMware DRS is designed to continually monitor utilization across resource pools and intelligently allocate available resources among VMs based on...
<table>
<thead>
<tr>
<th></th>
<th>VMware Virtual Machine File System</th>
<th>Raw device mapping</th>
</tr>
</thead>
</table>
| **Typical applications** | - Microsoft® Active Directory® directory service  
- Application, file and print, and utility servers | - Microsoft Exchange databases and log volumes  
- Microsoft SQL Server® databases and log volumes |
| **Advantages** | - Simplifies implementation and management by using a small number of large VMFS logical units (LUNs)  
- Can provide comprehensive protection when administrators back up entire VMFS LUNs, because all VM files reside on these LUNs | - Supports setting application priorities by recovery plan  
- Allows flexible replication and disaster recovery plans when following the backup best practice of separating data and system images  
- Does not require the replication of large amounts of static data, such as system drives or images  
- Enables low RTOs when using backup VMs at a disaster recovery site that have been preinstalled or that can pull system images from archives  
- Reduces bandwidth demands by allowing the number of VMs to scale without the replication of large amounts of data |
| **Disadvantages** | - Does not support application priorities (for example, SQL Server would have the same priority as a file and print server)  
- Does not discriminate system state—requires restarting service  
- Requires a transactional database to keep changes consistent, which can be bandwidth intensive, especially as the infrastructure scales (large databases and files require large backup targets) | - Increases the complexity of implementation and management by using a greater number of LUNs than are required for VMFS  
- Requires additional disks to host the increased number of LUNs, potentially increasing cost |

Figure 2. Comparison of VMware VMFS and raw device mapping

**Enhancing resiliency of VMware virtual infrastructures with EMC layered applications**

Administrators can use two methods to allow VMware ESX Server to access shared storage: VMware Virtual Machine File System (VMFS) and raw device mapping (RDM). VMFS is typically useful when crash consistency (as opposed to application consistency) is acceptable. RDM, which provides tunable I/O to help optimize performance, is typically useful when application consistency is required. A best practice is to use RDM in conjunction with VMFS by using VMFS for the OS and applications and RDM for databases and logs. EMC layered applications can perform optimally with either of these two methods. Figure 2 summarizes the typical applications, advantages, and disadvantages of these two storage access methods, and Figure 3 illustrates their respective architectures.

In a shared storage environment, the ESX Server systems and their respective VM workloads launch at boot time from the Dell/EMC CX or CX3 storage array. Files representing the encapsulated VMs—the guest OS and its data—launch directly from the SAN, an approach that provides portability and server hardware independence for the VM, OS, workload, and data.

**EMC layered applications: SnapView, MirrorView, and SAN Copy**

VMware VMs encapsulate an OS and its application or workload files into a set of four specific files. These files are easily replicated, and, more importantly, a VM service can be quickly restarted from a targeted remote SAN or replicated volume on a local SAN without

---

dependence on the source hardware platform that originally hosted the files.

EMC SnapView, MirrorView, and SAN Copy are SAN-based replication applications that can help protect VMware ESX Server guest OS images and their associated application and workload files. They offer comprehensive, incremental, and full-site replicas of all files associated with a virtual infrastructure without using host processor or I/O resources, as well as varying degrees of enhanced resiliency for virtual infrastructures that utilize Dell/EMC CX and CX3 storage. Figure 4 summarizes the key features and typical uses of these applications.

**Integrated disaster recovery**

Disaster recovery in an environment not based on a VMware virtual infrastructure can be difficult and complex, and support only long recovery times. Potential problems with this type of disaster recovery include the following:

- **Cost**: Creating a secondary site with a 1:1 server environment identical to the primary production site can be both complex and expensive to implement. And although the disaster recovery systems are often sitting idle, their servers, storage, and networking hardware are still consuming power and cooling resources as well as floor and rack space.

- **Hardware dependencies**: Secondary site requirements are restrictive, and ensuring a viable and rapid recovery at a secondary site depends on maintaining server models, firmware and OS revisions, and hardware and storage configurations identical to those operating in the primary production site.

- **Extensive training**: Properly training IT staff to use the technologies at both the primary production and secondary sites is often impractical.

- **Testing and risks**: Proper testing requires a full shutdown and failover of the primary production site—which can be difficult, because many IT organizations provide critical services to their customers and constituents. And because successful system restarts typically require several attempts and adjustments along the way, this process introduces risks of downtime and lost productivity for enterprises depending on those resources.

Figure 5 illustrates an example physical-to-physical disaster recovery environment incorporating the EMC SnapView, MirrorView, and SAN Copy applications.
environments based on a VMware virtual infrastructure in conjunction with EMC layered applications can help administrators meet SLAs, RPOs, and RTOs efficiently and avoid the physical infrastructure components that introduce complexity. The advantages of this type of environment include the following:

- **Cost-effectiveness:** A secondary site based on a virtual infrastructure often requires fewer network and storage components than a traditional physical infrastructure. More importantly, unlike a traditional physical infrastructure, a virtual infrastructure does not require that the disaster recovery site have a 1:1 server environment identical to the primary production site.
- **Predictable restart times:** Once administrators have replicated VM files to the secondary site using EMC MirrorView or SAN Copy, those systems should provide predictable system restart times (based on the amount of time required to restart VM workloads) and help reduce RTOs.
- **Efficient utilization:** In some cases, enterprises may be able to utilize the virtual infrastructure at a secondary site. Because a virtual infrastructure is built on a pool of shared computing and storage resources, it can provide the operational flexibility to run non-production or noncritical applications, or simply provide additional IT resources. Administrators can also take advantage of the advanced management capabilities and flexibility of SAN storage at both the primary production site and the secondary site to help meet organizational needs.
- **Reduced risk:** A secondary site based on a virtual infrastructure helps minimize the risks of lengthy system outages, reduced productivity, and failures to meet stringent SLAs.

**Creating robust, cost-effective business continuity systems**

VMware Infrastructure 3 provides built-in business continuity features and functionality, and EMC layered applications deliver SAN replication technologies for Dell/EMC CX and CX3 series shared storage systems that provide different levels of performance and functionality. When combined, VMware Infrastructure 3 and EMC layered applications offer powerful capabilities that can enhance the resiliency of IT infrastructures to help minimize risk and enable predictable SLAs, RPOs, and RTOs for organizations of all sizes.

**Eric Pan** manages Dell alliance marketing for VMware. He has held various positions in marketing strategy, alliance management, and product marketing over 18 years in the IT industry. Eric has a B.A. in Management Information Systems and an M.B.A. in Finance.

**Josh Donelson** is a systems engineer for VMware dedicated to the Dell/VMware alliance. He has more than eight years of experience in the IT industry in various fields, including SAN engineering, storage quality assurance, and technical sales. Josh has a B.S. in Electrical Engineering from the University of Texas at Austin.

**Mark Clifton** is an enterprise solutions architect at the Dell Executive Briefing Center working on virtualization strategies and architectures. Mark has a B.B.A. in Management Information Systems from the McCombs School of Business at the University of Texas at Austin.

**Figure 6. Example virtual-to-virtual disaster recovery environment based on VMware Infrastructure 3 and incorporating the EMC SnapView, MirrorView, and SAN Copy applications**

---

Reprinted from Dell Power Solutions, August 2007. Copyright © 2007 Dell Inc. All rights reserved.