LOCATION

Palo Alto, California

KEY CHALLENGES:

- Implement disaster recovery for VMware's most critical business applications
- Document each application's infrastructure dependencies
- Re-design application architecture to house all the most critical applications together to support in-tact failover.
- Deliver disaster recovery for a diverse application environment, including on-premises and SaaS and inclusive of third party integrations.

KEY LESSONS LEARNED:

- DR is best done with a fully virtualized environment
- Failover planning must consider management and monitoring tools as well as applications
- Be willing to adapt and realign organizational roles
- Networking is critical for load balancing

Disaster Recovery: Ensuring High Availability for Mission-Critical Applications

The Challenge: Mapping Applications to Infrastructure

A top priority of any IT organization is to ensure business continuity for the business and its customers. VMware IT began implementing a disaster recovery program a few years ago and has learned along the way the process is one of continual refinement. VMware's rapid growth and demands for high availability from lines of business drove the need to demonstrate that the company's disaster recovery solution could keep pace. The company sought to increase limits for business interruption insurance; doing so required that VMware IT prove it had a solid and executable disaster recovery plan in place.

In the early stages, the challenge was documenting the application footprint for mission-critical applications, including the infrastructure that supported them. Program elements included setting Recovery Point Objective (RPO)—or, the maximum allowable amount of data that might be lost—and Recovery Time Objective—the amount of time it takes to restore an application's availability after an outage. The disaster recovery initiative uses VMware's vCenter Site Recovery Manager (SRM), EMC's RecoverPoint, F5 load balancers, and Cisco's Overlay Transport Virtualization (OTV) protocol, all working in concert to ensure that failovers and failbacks execute seamlessly. Business processes had to be documented as well—and back-up decision makers appointed in the event that the CIO was unavailable after a disaster.

"At the outset of our disaster recovery program, we sought to fully document VMware application and infrastructure dependencies to establish a blueprint against which a disaster recovery plan could be tested and implemented," said Wayne Richards, program manager for resiliency and recovery, IT Operations. "But the target keeps moving—VMware is constantly adding new services and applications, including on-premises and in the cloud. So it's an on-going process."

"When you add a new application, it's rarely as simple as a one-to-one relationship," Richards continued. "We have to look at all new interdependencies that have been introduced and how they change our existing applications and what it means to protect them. We must ask–is everything already protected by virtue of the infrastructure-level solution we deployed, or do we need to make adjustments?"

"One of the strengths of our product set is that it provides reporting features we can use to stay aware of what is being deployed," said Chris Hopkins, VMware solution architect. "We are able to review reports on server build activity across the entire IT organization and stay on top of the incremental changes in how applications consume infrastructure."

Disaster recovery takes everything out to its worst-case scenario—so, while a downed server could be addressed by having an application fail over to a nearby data center, a disaster on the level of a major earthquake or power grid hit is better served by failing over to a data center in a completely different geography, noted Richards. There's a very human side to this as well—for the same reason, you would not designate a back-up decision maker for your CIO who lives in the same area.

"There can be a tendency to view disaster recovery as an 'infrastructure problem.' It goes well beyond that—it's a business problem worthy of attention at the highest levels."

– Alexander Price,
Director, Infrastructure and
Cloud Operations Architecture,
VMware

"Business users often tell us they know where their application is running – but they may think they have resiliency designed-in by having a backup site for that application to fail over, when in fact they don't realize their back-up capability is on the same power grid as the original," explained Richards.

The Solution: Cluster Applications for Disaster Recovery and Require DR Testing as Part of the Application Release Process

In assessing how best to secure VMware's applications and data, the IT team was faced with understanding how DR has to be "designed in" to application architecture and deployment in the first place. And that wasn't the case—once they documented the application ecosystem, they realized that indeed there were applications set to fail over to nearby data centers, and that mission-critical applications were dispersed. It might seem logical that critical applications shouldn't all be in one place, but that also means they all must fail over to different places, increasing complexity instead of simplifying it.

Licensing models can have a tendency to drive clustering by product, while DR requires clustering by application, noted Richards. Securing third party integrations is another consideration, he added.

The decision was made to keep entire data centers intact--that is, every application in a given data center would fail over to one back-up site rather than get dispersed to multiple sites. And all the applications in an affected site would stay together. To implement that decision, a number of applications had to be relocated to ensure that related systems were consolidated into the same data center.

This meant auditing what applications and business processes relied on which data centers the most, reallocating resources to ensure the highest degree of resiliency to the most critical functions, and ensuring that equivalent resources were allocated to the failover site.

"We also considered that an application may have to run out of an alternate data center for a long time, and hence we had to ensure the performance levels in line with the SLAs for that application to ensure the backup site could meet them," said Richards.

Software-Defined Data Center Supports Disaster Recovery

"This is the beauty of the Software-Defined Data Center," said Richards. "It's a platform for services on demand and you gain elasticity on a pay as you go platform."

Application automation is critical to disaster recovery, noted Hopkins.

"Originally we relied on manual startup procedures for our more complex interdependent applications, but for DR we quickly saw this was a major risk," said Hopkins. "Developing intelligent automation—in other words, don't let application A try to start unless B and C are ready – had to be baked into our application release process."

Levels of Resiliency

The most critical applications—Global Services and Support, Finance, the customer and partner portals and VMware.com—are now all run in the same data center and set to fail over to the same alternate data center. Moreover, local resiliency has been added to support these critical business processes. The team has implemented DR for on-premises applications and has in place a process for evaluating SaaS vendors that includes reviewing their DR plans. This application-agnostic solution allowed IT to provide a basic tier of resiliency that all applications could use as a "safety net," and as a starting point towards more customized levels of protection where appropriate. This progression is:

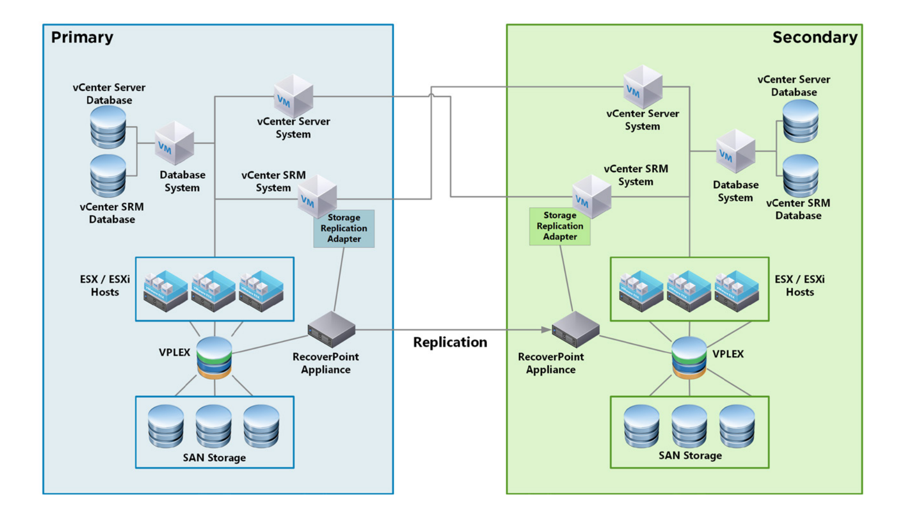
Tier 4: The basic data center-level protection provided by Site Recovery Manager

Tier 3: An SRM solution tailored around the dependencies and infrastructure of a single service

The overarching goal is to bring the most critical applications to more sophisticated, "cloud-native" architectures:

Tier 2: Multi-site application design with manual failover (active/passive)

Tier 1: Multi-site "active/active" application design



Topology of DR components in primary and secondary data centers.

The supporting disaster recovery infrastructure that underlies each application relies on primary and failover VMware vCenters, real-time replicated data, and transport application access handled largely through Site Recovery Manager, RecoverPoint, Load Balancing and Cisco OTV.

The "People Part" of Disaster Recovery

Because the best disaster recovery plan relies on automation but also on people, the team did playbooks to guide executives through the steps of executing disaster recovery. As a best practice, these playbooks exist not only online—the system that hosts them could go down—but distributed directly to appropriate staff across geographies as far away as India.

"Enterprise-class disaster recovery will change how you manage your IT organization," noted Alexander Price, director, IT architecture and strategy, infrastructure architecture, VMware. "It's critical that DR have high level executive support to ensure service-level resiliency for the most critical services. There can be a tendency for DR to be viewed as an 'infrastructure problem.' It goes well beyond that—it's a business problem worthy of attention at the highest levels."

The process involved both technology changes—additional WAN connectivity, real-time replication of all SAN and NAS storage, and virtualization of the few remaining workloads VMware had not yet virtualized—as well as policy changes; these included a mandate that the start-up of all applications be automated, the internationalization of some roles and responsibilities, and back-up methods of storing DR documentation.

Documenting and sharing lessons learned is an important part of disaster recovery.

“Disaster recovery is not a project. Our application suite is always changing and DR must continually adapt to it. One big shift in this phase of our DR maturity is we are now requiring DR testing on all new applications before they are put into production,” said Richards.

To learn more about the earliest phases of VMware IT’s disaster recovery journey, go to http://www.vmware.com/files/pdf/vmware-it-journey/Disaster_Recovery_case_study.pdf

VMWARE ON VMWARE

As the leading proponent of our own products, VMware is committed to passing on the lessons learned by our internal IT group in applying virtualization and cloud management technology to solve business challenges.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com