

SOLUTION NOTE

Business continuity/disaster recovery (BC/DR) is the primary reason companies initiate virtualization projects today. ABI Research 2010 projects that the BC/DR market will grow to \$39 billion by 2014. Cost is a driving factor: both reduced costs in opex and capex, as well as savings in minimizing downtime. While virtualization can dramatically reduce the cost of building out (capex) and maintaining computer infrastructure (opex), the greatest cost efficiency comes from diminishing service interruptions (BC/DR). So what's the drawback in virtualization as a BC/DR solution?

Dangers of BC/DR Virtualization

Three overarching challenges exist when implementing a virtualized BC/DR strategy:

1. Levels of Complexity Increase — Virtualization makes a moving target of network configuration and IP address management.
2. Critical Interdependencies Between Adjacent Systems Increase — A virtualization change in one system must be recognized and understood by a related system or communication between the two breaks down.
3. “Moving” Resource “Stacks” (Applications, Compute, Network, Storage Resources) from One Place to Another Becomes More Complex — Virtual components add flux, so change that needs only local management on a static network requires comprehensive management on a virtual-functioning network.

Protection for BC/DR Virtualization

VMware has developed a comprehensive set of tools to manage, execute and control virtualized BC/DR workloads for its vCenter Site Recovery Manager (SRM). Combined with virtualization, SRM's disaster recovery run-book automation capabilities provide strong disaster recovery capabilities. By adding a set of DNS, DHCP and IP Address Management (DDI), Infoblox has integrated two, key, complementary BC/DR elements into SRM: resource management and infrastructure mobility. Together, VMware and Infoblox have provided the protection needed to implement a virtualized BC/DR solution successfully. Here's how.

The first key element is resource management. Understanding what resources are available before and during a service interruption and restoration cycle is essential. Infoblox IPAM and NiOS DDI solutions together provide visibility into the entire IP address infrastructure.

The second key element is infrastructure mobility. Relocating servers at another location to keep the network running is not a single-step solution; these servers and their position on the network must be correctly and immediately reconfigured to minimize the interruption, tasks the dual solutions from VMware and Infoblox perform in tandem, as shown in Figure 1. The Infoblox solutions that complement SRM also automate the network infrastructure as well as other components on the network to ensure a repeatable recovery, compliance and security.

SOLUTION NOTE

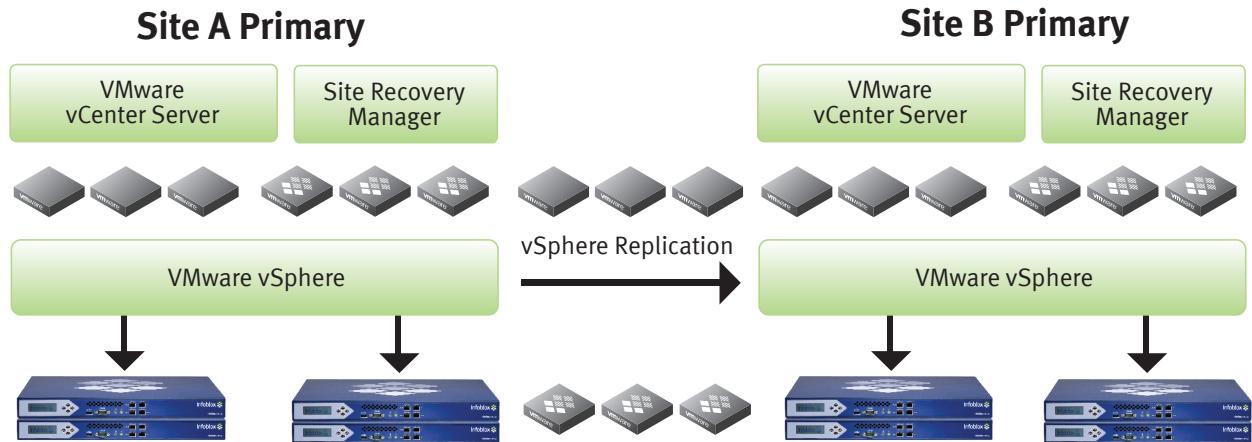


Figure 1. It worked in New York, but will it still work if we move it to London?

Avoidable Challenges to BC/DR Virtualization

Virtualized BC/DR environments bring numerous challenges that the Infoblox additions to VMware’s SRM solve completely, including management of the network, DNS, DHCP and IP address infrastructures.

Virtualized BC/DR environments:

- Cause frequent DNS configuration changes, which make manual DNS run-book updates impossible and result in outages during recovery.
- Need additional IT experts to maintain, thereby consuming IT resources and incurring recovery delays.
- Require significant capital and operational investment to achieve any resiliency/HA.
- Demand additional backup systems/databases for disaster recovery.
- Involve convoluted DR failover processes, often requiring multiple resources and processes.
- Are difficult to test frequently, or even test at all, which begs the question: Will it work during a failure event?
- Entail frequent network reconfiguration, including virtual switch configuration and policy changes.
- Prevent manual recordkeeping of primary site network configuration for rebuilding the data center because of the near-constant changes in networking configuration.
- Make it impossible to correlate security and regulatory policies for servers and applications at both the DR site and at the primary site due to frequent change in networking configuration.

SOLUTION NOTE

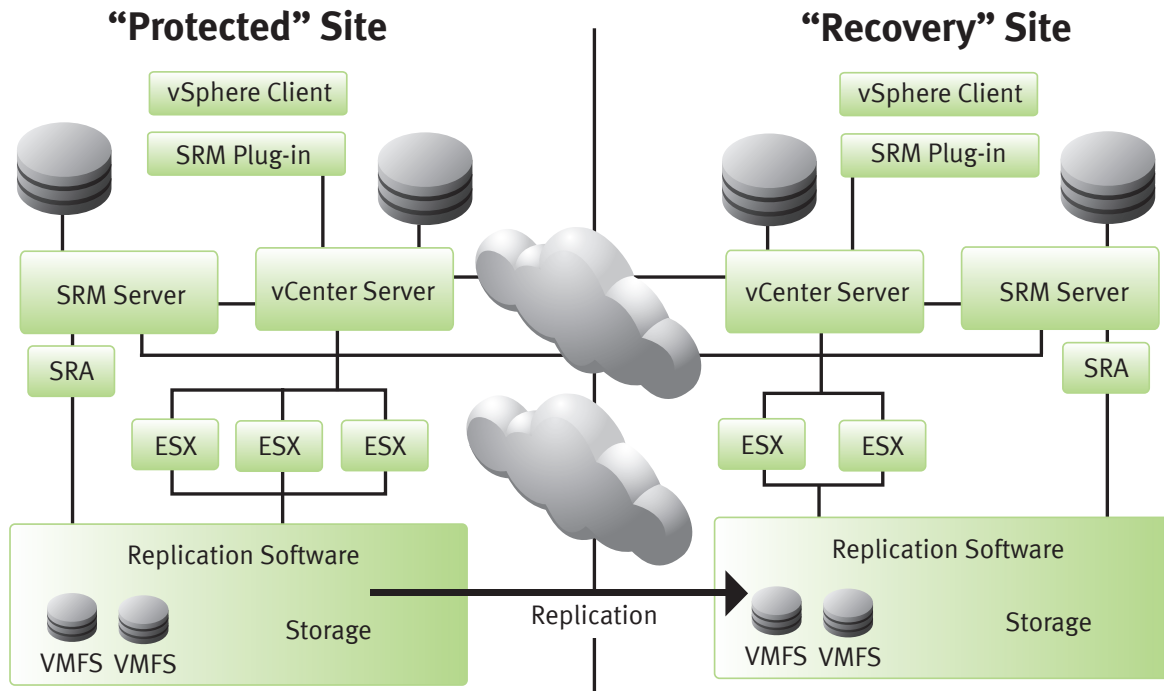


Figure 2. Integration Architecture for BC/DR - Infoblox DDI-to-vCenter Service

By using the VMware SRM with the Infoblox additions as shown in Figure 2, you can avoid all these challenges to implementing a virtualized BC/DR environment. The integrated Infoblox tools automate the disaster recovery process at all stages, and ensure a comprehensive recovery mechanism by testing network infrastructure throughout the process. Infoblox NIOS provides a DNS infrastructure that greatly simplifies the DNS update step of the recovery plan with vCenter SRM, and also delivers an easy way of testing disaster recovery without switching data centers. To ensure a successful recovery, Infoblox NetMRI supplies key network configuration automation capabilities.

How the Infoblox Additions Work for Disaster Recovery

The unique Infoblox Grid™ technology configures a number of always up-to-date appliances as “Grid master candidates” which stand ready to take over in the event of a disaster. In the actual recovery process, these DR site master candidate appliances are “promoted” to serve as Grid masters to replace the non-functioning ones. This always ready, in-place, appliance-based strategy allows enterprises to resume services — and management of those services — in minutes.

Other Grid members throughout the organization then automatically “re-home” to the newly designated DR site master appliances, and the recovery is complete throughout the network, from headquarters to all branch locations.

Unlike conventional systems, this Grid technology-based process can be easily and frequently tested to ensure DR measures are error-free and foolproof. VMware Site Recovery Manager also readily integrates with the Infoblox Grid for recovery, either leveraging DDNS, or, more securely, using Infoblox APIs to update the IP addresses of the recovered applications to point now to the disaster recovery site instances, as shown in Figure 3.

SOLUTION NOTE

• Infoblox DR

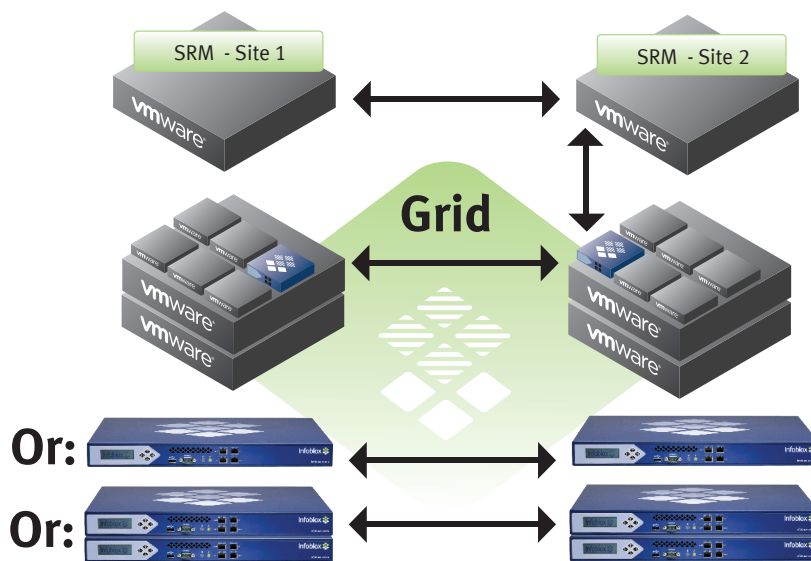


Figure 3. Infoblox DDI Disaster Recovery Architecture

Additionally, the insightful functionality of Infoblox’s “DNS views capability” presents a different view of DNS records to a smaller set of clients as an added troubleshooting tool. This capability is extremely useful for testing disaster recovery scenarios for applications without having to redirect all application traffic to the DR site.

Conclusion

When combined with server virtualization, VMware’s vCenter Site Recovery Manager offers a solid DR infrastructure to meet today’s business continuity needs. Infoblox’s DDI and network management solutions enhance that infrastructure and complete a successful BC/DR solution by providing the missing automation pieces for key network components, such as DNS, DHCP, IPAM, routers, firewalls and load balancers. Together, VMware’s SRM and Infoblox’s complementary additions provide a completely automated BC/DR solution that reduces availability risks and costs while ensuring compliance and security.

Infoblox Product Warranty and Services

The standard hardware warranty is for a period of one year. The system software has a 90-day warranty that will meet published specifications. Optional service products are also available that extend the hardware and software warranty. These products are recommended to ensure the appliance is kept updated with the latest software enhancements and to ensure the security and availability of the system. Professional services and training courses are also available from Infoblox. Information in this document is subject to change without notice. Infoblox Inc. assumes no responsibility for errors that appear in this document.