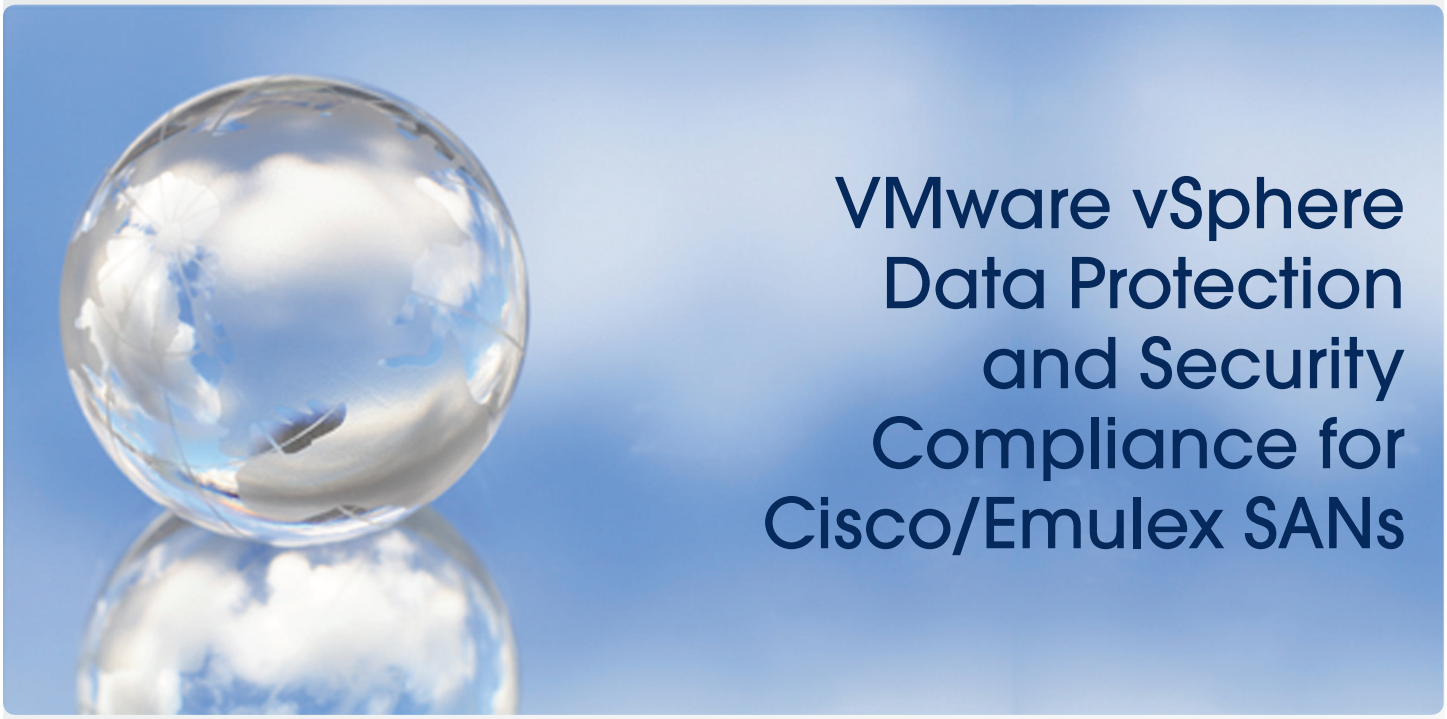


# VMware vSphere Data Protection and Security Compliance for Cisco/Emulex SANs

vmware® cisco™ EMULEX®

## Table of Contents

## Introduction

Protecting enterprise information is a high priority for companies. The flood of records, web content, documents and digital images poses a challenge to enterprises trying to increase IT performance, decrease IT costs and meet IT regulatory and business compliance policies. With so much data at stake, it helps when industry leaders collaborate to provide simplified data center solutions, such as virtualization, that help meet enterprise business needs. VMware,® Cisco® and Emulex® provide such information through the Storage Area Network (SAN) Virtuosity Series (sanvirtuosity.com).

This is the third white paper in the SAN Virtuosity Series sponsored by VMware, Cisco and Emulex. Previous papers focused on maximizing your company's SAN-connected VMware vSphere™-enabled data center with tips for getting started and ensuring high availability (see first two papers listed in "For More Information" at the end of this paper).

This white paper focuses on solutions to common VMware vSphere deployment questions that often delay the planning and implementation process. In particular, this paper explores how to:

- Complete virtual machine (VM) backups in a limited backup window
- Maintain security processes already in place with physical servers (e.g., encryption, backup compliance, intruder threats prevention)
- Maintain Service Level Agreement (SLA) performance
- Allow visibility to SAN and VMware configurations while maintaining management control

## Compliance

Regulatory compliance (e.g., with Health Insurance Portability and Accountability Act [HIPAA], European Union Data Protection Directive [EUDPD] or Payment Card Industry Data Security Standard [PCIDSS]) is an ongoing issue with physical servers. Meeting these requirements should not prevent you from completing your transition to a virtualized environment. Architecting a VMware deployment requires changes to the data protection and security processes in your data center and this white paper addresses those changes. Read on to discover how you will get your VM backups completed, encrypt VM data, secure it, whether in movement or at rest, and control management access to your SAN-connected, VMware-enabled environment.

## Common VMware Deployment Questions

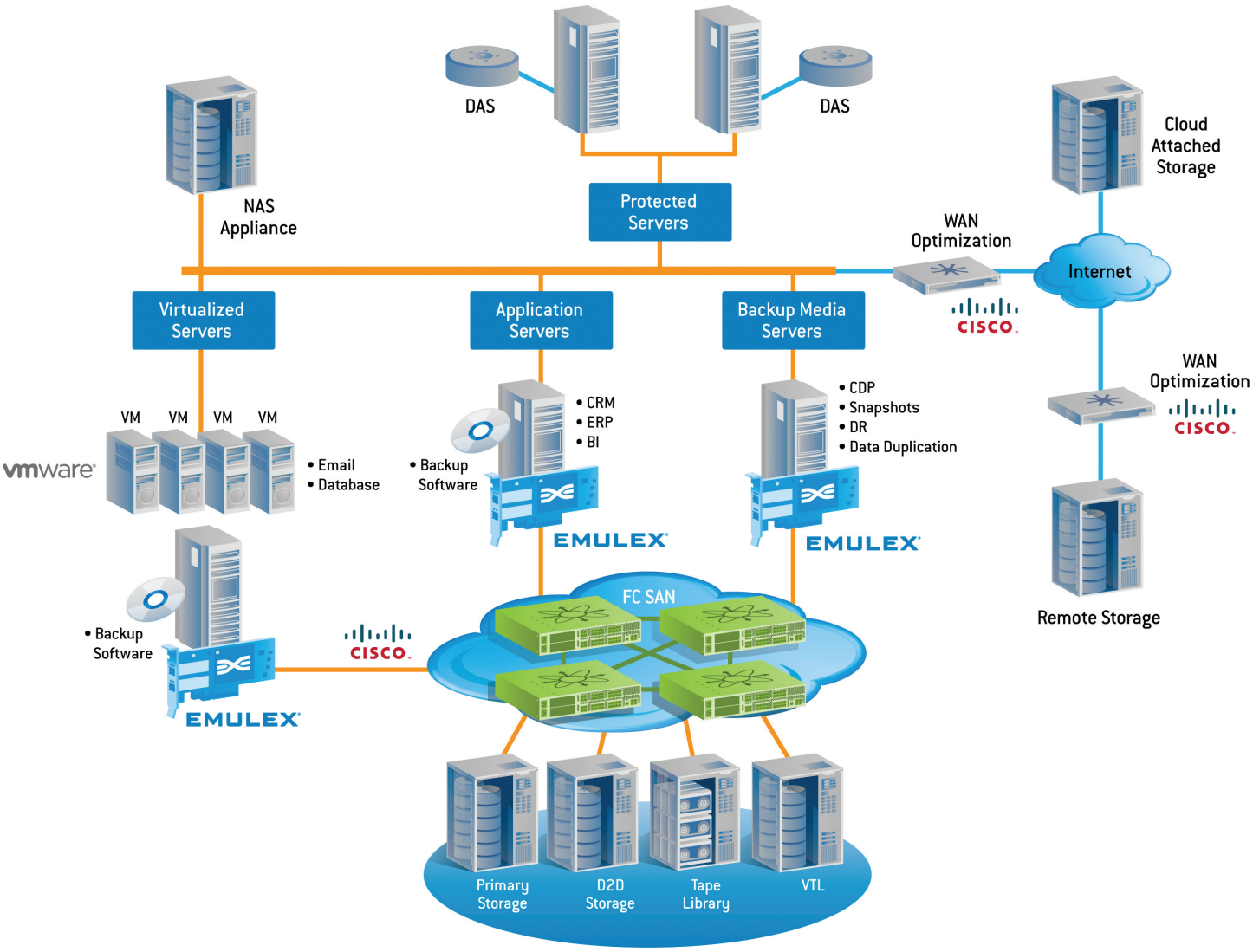
Data center managers architecting a virtualization solution to meet specific business needs are often concerned about how the virtualization deployment will affect key areas of their data center performance and security. This paper explores the questions that arise the most when architecting a VMware deployment.

**1. Limited backup window—I already have a limited backup window on my server. Once I have VMs running on it, how will I get all my backups completed in my limited backup window for that server?**

While virtualization allows all unused CPU and resources (off-shift) to be used for backup operations, virtualization can improve or limit the performance seen with your physical servers. There are many possible options to back up your VMs, ranging from using a guest OS method where each VM is treated as a physical machine, to VMware Consolidated Backup (VCB), which has a backup server proxy, and VMware Data Recovery (snapshot-based). Figure 1 depicts these many options.

It should be noted that customers with similar SAN hardware and backup software achieve different levels of performance. Provided in this white paper topic are tips to achieving maximum VM backup performance.

*Figure 1 VM backup options*

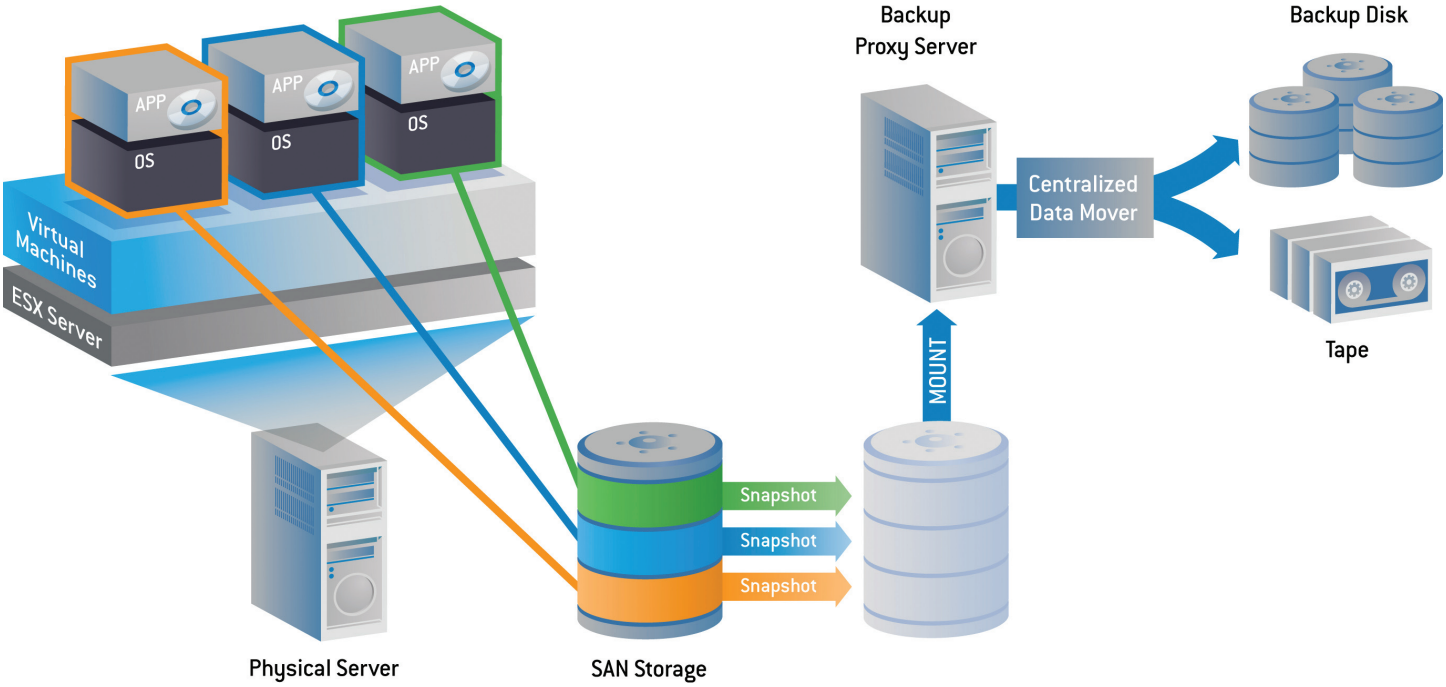



**VMware Consolidated Backup**

VCB performs virtual machine backup at any time by providing a centralized backup facility that reduces the load on production ESX Server hosts by using a centralized proxy server (see Figure 2). Scripts have historically been needed for VCB to complete backups. VMware's latest release, vSphere 4, offers vStorage APIs to eliminate the need for scripts. The new vStorage API for Data Protection delivers direct API-based integration for backups, allowing backup software to query VMs directly, thus resulting is much faster performance.

VCB performance is optimized when the latest Emulex Host Bus Adapter (HBA) or Universal Converged Network Adapter (UCNA) driver is used. Emulex's frame-level multiplexing (a built-in feature that is always on) ensures fairness and predictable performance when mixed loads are active (e.g., backup concurrent with interactive loads). Also SAN multipathing should be turned off (i.e., keep only one path up).

*Figure 2 How VCB works*




VMware Data Recovery (VDR) is another option for protecting data on VMs. It is a disk-based backup option and does not write to tape. With VDR, you can do full or incremental backups of guest VMs. It also supports de-duplication so that only changed data is actually backed up (not duplicate data), allowing you to maintain full point-in-time backups of each VM with only a fraction of the disk space that would be required otherwise. The previous High Availability SAN Virtuosity White Paper provides extensive details on VDR.

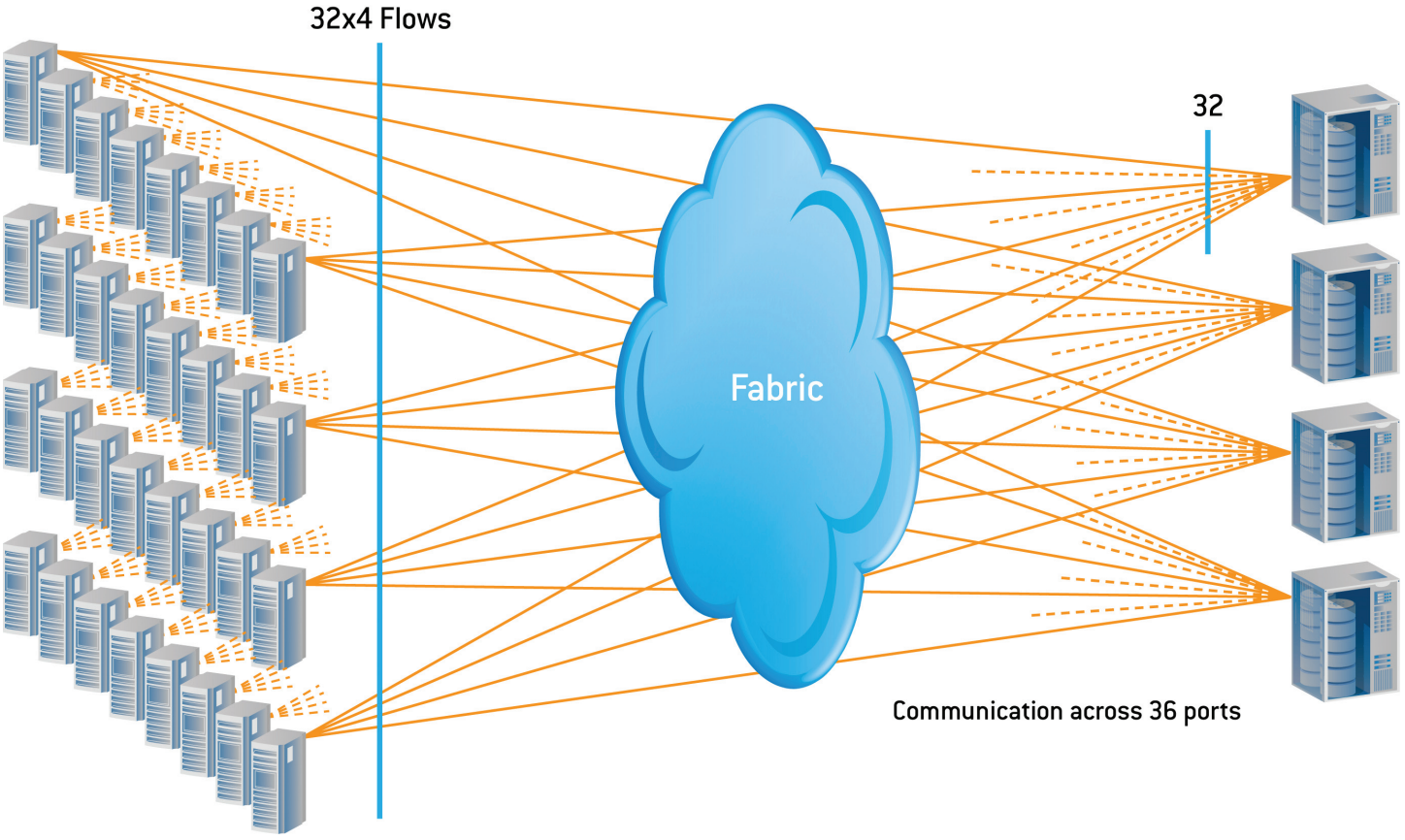
VMware Workstation also provides AutoProtect, allowing you to schedule snapshots of your virtual machine at regular intervals. This ensures that you always have a snapshot available to revert to if needed.

VMs can also be treated like physical servers, using products from backup partners who are storage experts but not virtualization experts. These vendors improve your VM backup performance with data de-duplication to reduce the amount of data requiring backup.

Whichever backup process you use, to make the most of it, you need to ensure that your SAN fabric performance is optimized. Emulex LightPulse® Fibre Channel dual-channel 8 Gigabit per second (Gb/s) HBA delivers the fastest performance across its dual channels. Emulex adapters and drivers are designed to leverage the enhanced storage stack in ESX/ESXi 4.0. Using Emulex OneConnect™ UCNA, you can have your backup traffic flow with your standard networking traffic in a converged network environment. This introduces a whole new topic, Network Convergence, not discussed in this paper.

SAN performance is further optimized using the Cisco MDS 9500 Series Multilayer Director. In nonvirtualized deployments with a large number of physical servers hosting one application per server or cluster, traffic normally is predictable and can be engineered to achieve better performance. In VMware environments with a large number of virtualized servers organized in a hypervisor cluster and any-to-any connectivity, traffic becomes unpredictable, and therefore performance must be predictable across all SAN components regardless of their placement. Figure 3 illustrates the demands that server virtualization places on a SAN infrastructure for consistent performance.

*Figure 3 Traffic pattern: 32-node hypervisor cluster with any-to-any connectivity; predictable performance is essential*




The Cisco MDS 9500 is also designed to provide more efficient utilization of inter-Data Center connections and to move data more quickly between data centers. The Cisco MDS 9500 data compression feature compresses data transmitted over native Fibre Channel and Fibre Channel over Internet Protocol (FCIP) links reducing bandwidth requirements. To increase data replication and backup performance to remote data centers, the Cisco MDS 9500 has a SAN-based intelligent fabric optimizer, called I/O Accelerator (IOA), that enables cost-effective data backup and disaster recovery solutions that are faster, more flexible and deliver mission-critical availability. The IOA service can be extended to either disk or tape, over any transport protocol (FC or FCIP), regardless of the device location (directly attached [e.g., campus distances], Wide Area Network [WAN], or Metropolitan Area Network [MAN]). While Cisco offers data compression for both MAN (native FC) and WAN (FCIP) connections, compression is enabled via different licenses. For MAN links, it is included in the new IOA license. For FCIP, it is in the SAN Extension license.

A final option to improve your VM backup performance is to use VMDirectPath which allows ESX to avoid the emulation of network interface cards (NICs) and map the physical NICs directly to the VMs. This is for operations that can't be virtualized (e.g., direct access to HBA or 10Gb NICs). The VMs are directly connected to an I/O device, bypassing hypervisor storage virtualization. An Emulex HBA port must be fully dedicated to a single VM, so VMDirectPath should be reserved for applications that require maximum I/O.

**2. Management security—I know data needs to be encrypted for different processes, such as when doing backups, when data moves from tier to tier or when VMs move across servers. Where should the data be encrypted?**

It is best to create encrypted virtual disks within the data center. If the virtual disk was encrypted, then it would be possible to bypass all the other layers of encryption possibilities and still maintain data integrity and encryption throughout the process, no matter where the virtual disk image lands. There are other options, however, and encrypting while data is written to tape is one.

Since backup tapes are often targeted by thieves, the only way to be assured that your data is safe is to encrypt it with a complex cipher, treating your data the same way on tape as you would if it was sitting on a public ftp site (with anonymous access enabled). Cisco Storage Media Encryption (SME) encrypts and decrypts your data coming on and off tape. SME allows for the seamless encryption of your data as it flows on and off your backup tapes using AES256 standard encryption. SME protects your data at rest, removing the possibility of an attacker getting access to your critical data.

When the data is moving between data centers, encryption is also required by many compliance and regulatory regimes—and it is a best practice for everyone. However, encrypting data at the source can interfere with operations such as I/O Accelerator and data compression that make transmission over the MAN or WAN more efficient. The switches and modules used by Cisco's SAN Extension over FCIP can encrypt the traffic at the Gigabit Ethernet (GbE) WAN links at full line rate. If the data centers are connected over a MAN or campus link instead of IP, such as dense wavelength division multiplexing (DWDM) or Coarse Wavelength-Division Multiplexing (CWDM), Cisco's current generation of 8Gb/s Fibre Channel switching modules use Cisco TrustSec Fibre Channel Link Encryption to encrypt that traffic at full line rate as well.

Another key item to address is hardening your intermediary devices. You further secure your virtualization environment by following the hardening best practices provided in item 6 below.

**3. Replicated data—I am looking into replicating data to a remote server for disaster recovery. Once I replicate to an offsite server, there is now a new intrusion location. How do I keep that remote copy secure?**

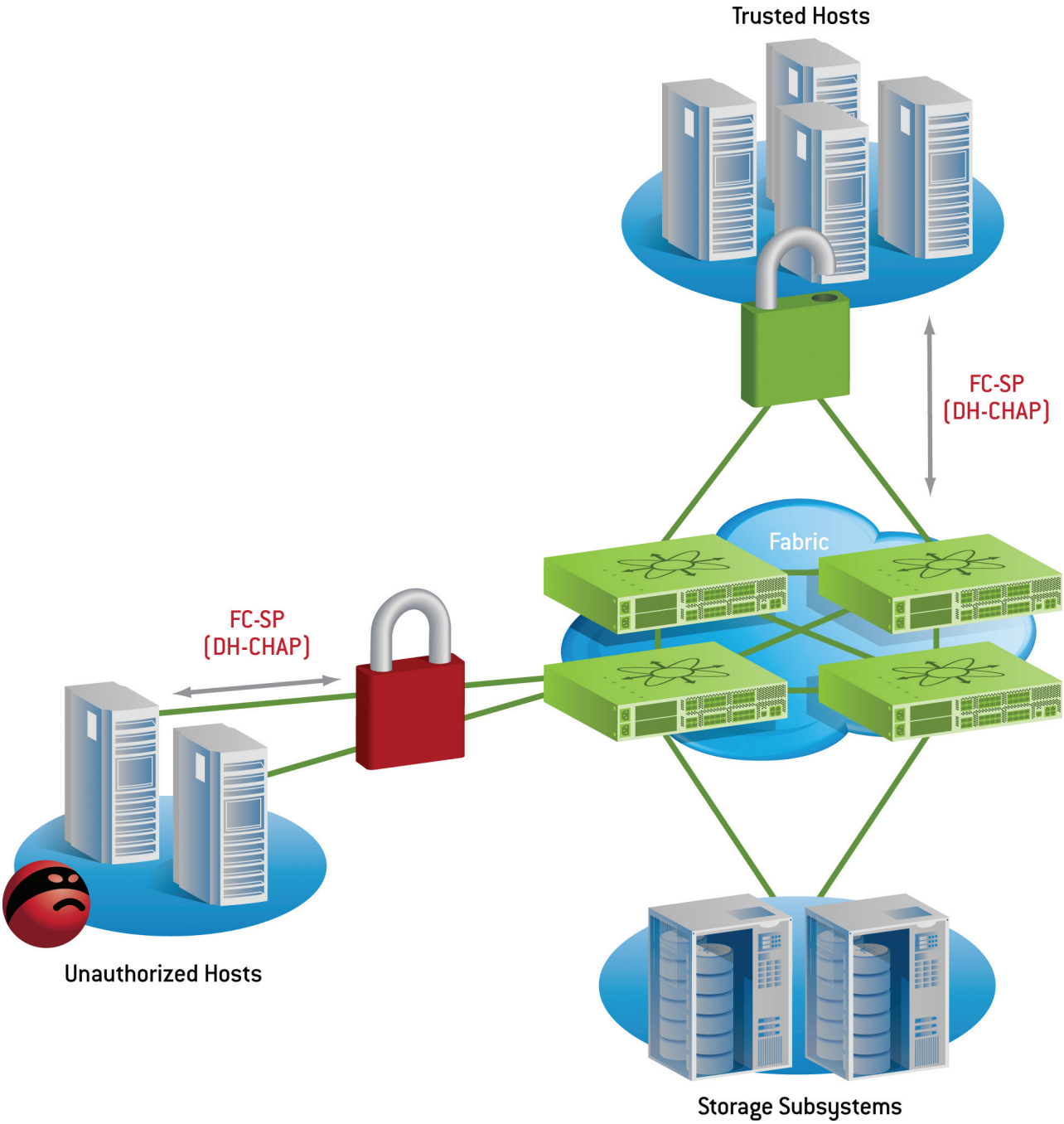
With VDR, you can replicate your VM data to a remote disk location, using your standard encryption technology. If your remote copy is on tape, you can use Cisco SME to encrypt and decrypt your data while it is written or retrieved from tape.

There are two methods to prevent unauthorized access to the Fibre Channel SAN. The first method is to use Cisco MDS 9000 Port Security. This feature grants or denies connections based on the port World Wide Name (pWWN)* of a host/target or switch World Wide Name (sWWN) of a switch trying to connect to a Fibre Channel switch. This security can be done at the switch level or port level for more granular security.

In addition to Port Security, additional access security can be achieved using Fibre Channel Security Protocol (FC-SP) capabilities. FC-SP provides authentication capabilities that overcome security challenges for enterprise-wide fabrics. Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP) is the protocol used by FC-SP to provide authentication between Cisco MDS 9000 Family switches, Emulex adapters and other devices. The authentication allows the switch, HBA or UCNA to prove to the requesting party that it has correctly identified that a particular node is the intended node and communication with that node can be trusted. Depending on the configuration, both the adapter and the switch can independently validate the identity of the other device. DH-CHAP prevents World Wide Name (WWN) spoofing (i.e., impersonation, masquerading attacks) and is designed to withstand replay, offline dictionary password lookup and challenge reflection attacks (see Figure 4).

* Sometimes referred to as Worldwide Port Name (WWPN).

*Figure 4 Host threats prevented by implementation of DH-CHAP authentication by the adapter or switch*




Another way to keep your remote copies secure is by implementing VSAN technology, an ANSI T11 standard, which provides hardware-based network virtualization and traffic isolation. With VSANs, your backup traffic is isolated from the rest of your SAN traffic. VSANs are described in more detail in item 4.

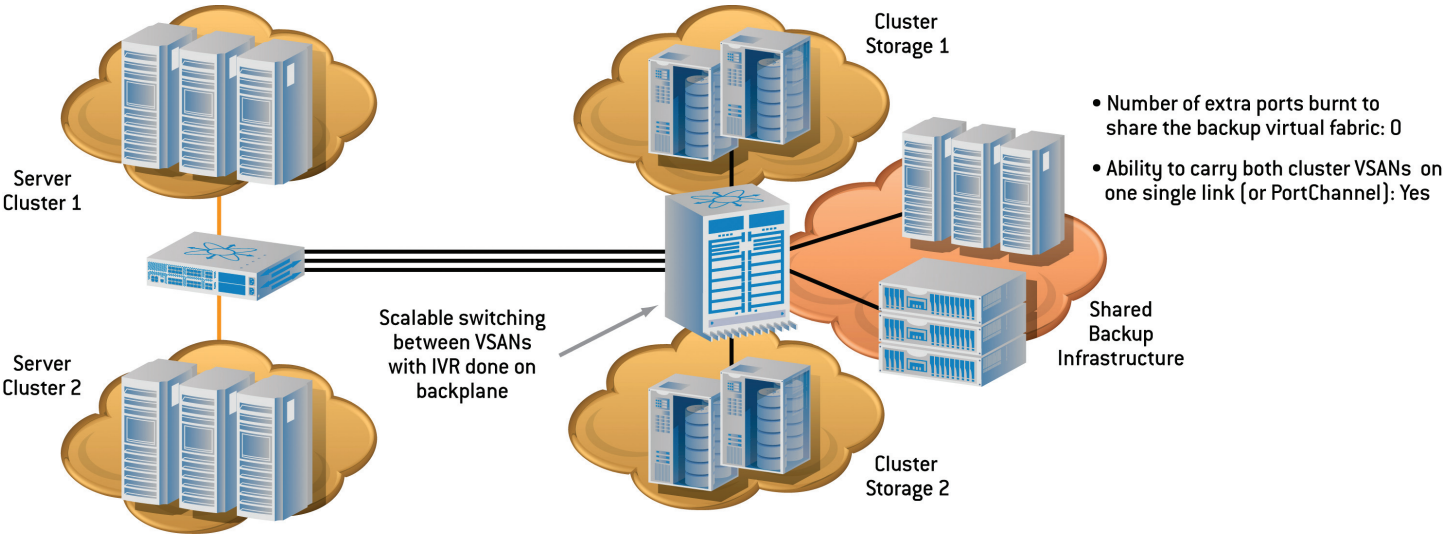
**4. SLAs—What can I do to make sure my SLAs are not adversely affected by my virtualization deployment?**

Different VMs will have different priorities, but setting up a shared infrastructure does not mean that you cannot meet your SLA requirements. VSANs allow you to isolate applications to ensure continued support of SLAs.

Each individual VSAN is regulated by an independent set of fabric services (including zone server, name server, domain manager and Fabric Shortest Path First [FSPF] routing services) in such a way that each VSAN can contain any configuration operation and choice. Thus, it is protected with respect to management, configuration and protocol errors from what happens in a different VSAN. For instance, zoning is a fabric service running on the top of the VSAN infrastructure: a configuration error or a protocol violation, which might lead to a catastrophic zoning misconfiguration, has no effect outside the VSAN where the problem occurred.

Within a VMware infrastructure, VSANs help achieve the best level of availability, but remove the fear of adversely impacting high priority applications and associated SLAs. Emulex adapters and Cisco switches are added to VSANs with no special setup required. Each VSAN is a logically and functionally separate SAN with its own set of Fibre Channel fabric services. Sometimes you need to share resources, such as backup devices, across VSANs. This can be done using Inter-VSAN Routing, also called IVR. IVR lets the SAN administrator create zones that cross VSAN boundaries, as shown in Figure 5.

*Figure 5 VSAN example*




**5. Security processes—My physical servers' security processes are set and working. When I implement VMs, how will the security processes work?**

The SAN zoning you implement with your physical servers determines which server can talk to which storage. As you establish VMs, your SAN zoning remains intact with N_Port ID Virtualization, an ANSI T11 standard developed by Emulex and IBM. NPIV enables a physical adapter port to be logged into a fabric switch with multiple virtual pWWN addresses. Using the Emulex OneCommand™ Manager application, virtual adapter ports (vPorts) can be created with a virtual pWWN. Using this virtualized connection, VMs can then be created with each one having a unique SAN identity and its own zone memberships controlling its access to storage.

The Emulex OneCommand Manager application also enables vPorts for non-virtualized environments, providing a unique SAN identity for applications running on the same server. Since your VMs have their own ID with NPIV, your VM security is very similar to your physical server security. This technology is only available in conjunction with Raw Device Mapping (RDM) for use with applications with demanding isolation or volume management requirements.

NPIV can be combined with Cisco IVR, a switch technology that allows vPorts to be routed to a VSAN that is different than the physical adapter port's VSAN. The routing is configured with the vPort's virtual pWWN, and will be preserved through a VM migration by way of VMotion.

Using NPIV and IVR, a VM or application can be individually routed to a VSAN, providing it with a unique visibility to servers and data in the SAN. NPIV also enables Quality of Service (QoS), backup and other SAN functionality to be managed at the VM or application level.

For further VM security, VMware has a security service called vShield™ Zones as part of its Virtual Data Center Operating System (VDC-OS) platform, which allows enterprises to build their own so-called "internal" cloud in their own data center. The addition of vShield Zones lets users create separate zones in a cloud-based data center. This is similar to the notion of a demilitarized zone in the traditional IT infrastructure, but based on VMs rather than physical devices.

vShield Zones create a protected zone and an unprotected zone. The traffic enters the protected zone from the unprotected zone. As it crosses the zones, the vShield performs traffic analysis, discovery and stateful firewall protection.

**6. VM in motion—Is it possible for an intruder to intercept information off a VM that is in motion from one host to another?**

This is a common misperception that arises from ignoring the fact that virtualization inherently involves a management layer which sits underneath the production VMs. The most basic security best practices dictate that this management layer operate in a dedicated, isolated environment. Only by violating this fundamental rule would an environment open itself up to this kind of problem.

Encryption of all data-in-transit is a well understood mitigation for man-in-the-middle attacks. But the fact that plenty of data flows unencrypted within the enterprise—indeed, perhaps the majority of data—suggests that there are other adequate mitigations. Unencrypted VMotion™ traffic is not a flaw, but allowing VMotion to occur on a compromised network can be. So this is a good time to re-emphasize hardening best practices for VMware Infrastructure and what benefit they serve in this scenario:

1. The most important VMotion best practice is to isolate your VMotion activity from all production network traffic. The current design of VMotion assumes that the VMotion network is secure within a data center, certainly within a rack or set of adjacent racks. In a typical situation, servers in one or more co-located racks would each have one or two network cards dedicated for VMotion; these would be connected to a switch that has no other endpoints connected.

2. You should also tightly restrict access to VI administrative accounts and roles. With VMotion isolated, a virtual rogue presence is more plausible than a physical one, but even a compromised guest VM does not have a virtual NIC on the VMotion network, only on the production network. Therefore the rogue VM must be configured in VI to have a vNIC on the VMotion network.

3. Lastly, don't enable promiscuous mode on vswitches. Unlike a physical network card, someone who has taken over a guest VM cannot configure a vNIC to be promiscuous. Another VI admin setting, promiscuous mode (off by default) is configured on the virtual switch port separately from a VM. Also, to manipulate rather than snoop, the proof-of-concept technique requires traffic actually route through the rogue VM, which would not occur naturally on the vswitch.

**7. VMs turned off—How do I secure my VMs that are turned off?**

Because a VM is encapsulated in a handful of files, making copies of them becomes quite easy. This enables standardization, and also much easier high availability and disaster recovery. However, many security tools, such as Antivirus and Patch Management, require that the server be up and running in order to push out updates, and hence this method does not work for VMs that are turned off, but may come online again in the future. New approaches can address this issue, such as offline patching with VMware vCenter™ Update Manager, or in the future, VMsafe-based host protection without any host-based agents.

**8. Management security—How do I provide shared visibility of my SAN and VMware configurations while ensuring the management security of them?**

In early SAN configurations, multiple administrators could log into different switches on the same fabric and perform fabric-configuration changes concurrently. After enabling and propagating those configuration changes fabric-wide, the fabric configuration could become corrupt due to conflicts. Fabric corruption usually occurs when configuration changes are made through multiple points on a fabric. With VMware, you achieve greater consolidation in your SAN-connected data center, but not at the expense of management controls.

Role Based Access Control (RBAC) for SAN and virtualization management allows users to perform only those functions they are assigned to perform. It allows them to view the many aspects of the SAN and VMware environment, without allowing them to make changes, thus fostering a shared management view, but maintaining control.

RBAC in VMware vCenter restricts VM, hypervisor or pool access to authorized users. Within a virtualization solution, roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles and those roles are then granted to users registered in your directory service. For example, in vCenter, some pre-defined roles are Administrator, Manager, Virtual Machine User, NOC operator or Read-Only. vCenter also allows you to create custom roles.

The Cisco MDS 9000 Family of switches provides RBAC, enabling up to 64 user-defined roles where the scope of the roles can be defined to specific commands and access to specific VSANs. For example, a network administrator role allows configuration of all platform-specific capabilities, while VSAN-administrator roles allow configuration and management of specific VSANs. By adding a layer of security where only administrators can configure switches within specified VSANs, SAN disruptions are reduced by localizing the effects of user errors to the VSANs for which the user has administrative privileges.

Public Key Infrastructures (PKI) technology can also be applied for management-to-fabric security, ensuring that a trusted and secure management console-to-fabric communications layer exists. PKI and other encryption help ensure that the management console or framework used to control the fabric is authentic and authorized. In addition, encryption methodologies can restrict the number of switches on the fabric from which management and configuration changes are propagated to the rest of the fabric. That will create a SAN with a minimal number of security control points.

## Conclusion

Consolidating workloads from underutilized, and often outdated, servers delivers substantial savings in capital expenditures (CapEx) for equipment and operating expenditures (OpEx) for maintenance, power and management resources. When architecting a VMware deployment, there are questions that arise surrounding existing data protection and data security processes. However, moving to virtualized servers does not mean that your data is more at risk than with physical servers.

Many data centers have tackled their data protection and security concerns, coming up with solutions with the assistance of VMware, Cisco and Emulex. With their combined expertise, these companies provide key information to help you design your VMware solution. This white paper answers your data protection and data security questions so that you can move forward with your VMware deployment in your SAN-connected data center.

This document is the third of four papers in the SAN Virtuosity series jointly published by VMware, Cisco and Emulex. To subscribe to the series, visit sanvirtuosity.com.

## For More Information

**Getting Started with VMware vSphere and Emulex/Cisco SANs**
www.emulex.com/artifacts/f6791810-e5b2-417e-a4f3-6ed842249a68/getting-started-with-vsphere-and-sans-cscoelxvmw.PDF

**High Availability with VMware vSphere and Emulex/Cisco**
www.emulex.com/artifacts/69c0fac7-1917-4f49-9877-ec0311efd1b5/elx_wp_sanvirtuosity_ha_cisco_vmware.pdf

**IT Audit for the Virtual Environment**
www.vmware.com/files/pdf/sans_analyst_program_vmware09.pdf

**Achieving Compliance in a Virtualized Environment**
www.vmware.com/files/pdf/technology/compliance_virtualized_environment_wp.pdf

**VMware Consolidated Backup: Best Practices and Deployment Considerations for SAN Environments**
www.vmware.com/files/pdf/vcb_best_practices.pdf

**Storage Media Encryption Key Management**
www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/white_paper_c11-462423_ps6028_Products_White_Paper.html

**Cisco TrustSec Fibre Channel Link Encryption**
www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps5990/white_paper_c11-545124.html

**The Virtual Machine Aware SAN**
www.cisco.biz/en/US/prod/collateral/ps4159/ps6409/ps5989/ps9898/white_paper_c11-494982.html

**Data Center Networking Security - From LAN to SAN**
www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps4358/prod_white_paper0900aecd80281e21_ns513_Networking_Solutions_White_Paper.html

**Cisco MDS 9000 Family Advantages in VMware Environment**
www.cisco.com/en/US/prod/collateral/ps4159/ps6409/ps5990/white_paper_c11-533041.html

**Using Cisco VSANs with Emulex HBAs and UCNAs**
www.emulex.com/artifacts/4f1503e7-47cd-47cc-8381-c178fe16b738/elx_tb_all_ciscovsans.pdf

**Cisco Systems, Inc. 170 West Tasman Drive, San Jose, CA 95134-1706 USA Tel 408-526-4000 www.cisco.com**


---

**Emulex 3333 Susan Street, Costa Mesa, CA 92626 USA Tel 714-662-5600 www.emulex.com**


---

**VMware, Inc. 3401 Hillview Ave. Palo Alto CA 94304 USA Tel 650-427-5000 www.vmware.com**


10-1094 · 3/10