VMware Virtual SAN 6.2

PCI DSS Compliance Guide

Revised February 2016

vmware

Contents

Introduction

VMware, the market leader in powering Hyper-Converged Infrastructure (HCI), enables the lowest cost and highest performance next-generation HCI solutions through proven VMware Hyper-Converged Software. The natively integrated software combines radically simple VMware Virtual SAN™ storage, the marketing-leading VMware vSphere® hypervisor, and the VMware vCenter Server™ unified management solution with the broadest and deepest set of HCI deployment choice.

Virtual SAN delivers the industry's best storage value with radically simple management, high performance, low cost and a future-proof roadmap supporting any app, any scale. Virtual SAN pools server-attached magnetic disks and solid-state flash devices to create a distributed shared datastore that abstracts the storage hardware and provides a hyperconverged storage optimized for virtual machines.

Customers of all industries and sizes trust Virtual SAN to run their mission critical applications such as Microsoft SQL Server, SAP, and Oracle Database. In many sectors such as finance and retail, compliance with security standards is mandated by the card brands and administered by the Payment Card Industry (PCI) Security Standards Council. This guide provides an overview on how Virtual SAN can be utilized successfully in an environment governed by PCI compliance. The following sections discuss the primary PCI Data Security Standard (DSS) goals and requirements as found in the PCI DSS Quick Reference Guide (version 3.1).

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

Build and Maintain a Secure Network and Systems

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Virtual SAN is commonly deployed behind an organization's internal firewall to provide storage services for running virtual machines. Virtual SAN network communication is usually confined to the VMware vSphere® hosts and internal network that make up the Virtual SAN cluster and not routed to a public network.

The exception is when Virtual SAN is deployed in a stretched cluster or 2-node configuration. These configurations require the use of a Virtual SAN witness virtual machine, which is commonly deployed to an alternate location.

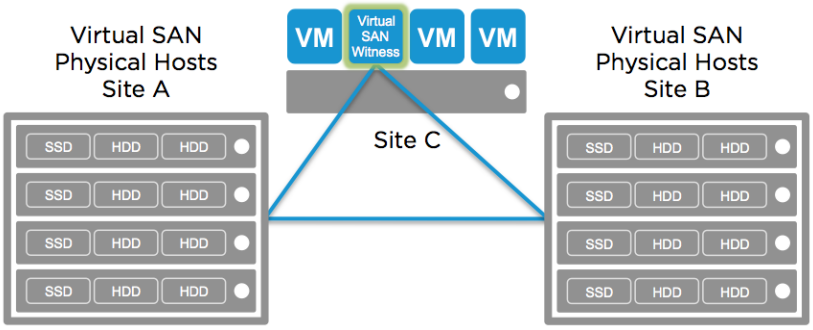

Figure 1. Virtual SAN Stretched Cluster

Communication between physical nodes (vSphere hosts) requires a minimum of 1Gbps or 10Gbps, depending on the Virtual SAN configuration, and a Round Trip Time (RTT) of 5ms or less. These requirements are typically only achieved using private network connections that are not routed across public networks. Communication between physical nodes is not encrypted and should not traverse public network connections.

Communication between the physical nodes and the Virtual SAN witness consists of cluster metadata. Since the witness is typically deployed to an alternate location, it is likely this metadata is transmitted beyond firewalls using a Wide Area Network (WAN) connection. However, data such as customer information, account numbers, and so on that are stored in virtual machine applications and databases are not transmitted to or from the witness or stored in the witness.

Virtual SAN utilizes standard network connectivity architecture along with standard switching, routing, and transport protocols. Therefore, security measures such as physical separation, Virtual Local Area Networks (VLANs), and firewalls can be used to secure a Virtual SAN network.

VMware NSX® is a consideration for enabling specific network access control. NSX brings security inside the data center with automated fine-grained policies tied to the virtual machines, while its network virtualization capabilities let you create entire networks in software. This approach securely isolates networks from each other, delivering an inherently better security model for the data center. However, it is important to note that transmitting Virtual SAN traffic across an NSX VXLAN overlay is not supported.

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

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Virtual SAN runs as a component of the vSphere kernel. Therefore, it relies on the permissions and access control mechanisms built into vSphere and vCenter Server. When these products are deployed, the software installer requires the systems administrator to enter a new password before the installation will proceed. In other words, there are no commonly-known default passwords for vSphere and vCenter Server.

vSphere is a bare metal hypervisor that does not require a general purpose operating system to run. vSphere is deployed with a software firewall enabled and services such as Secure Shell (SSH) disabled by default. Communication can be limited to vCenter Server only to further minimize the attack surface.

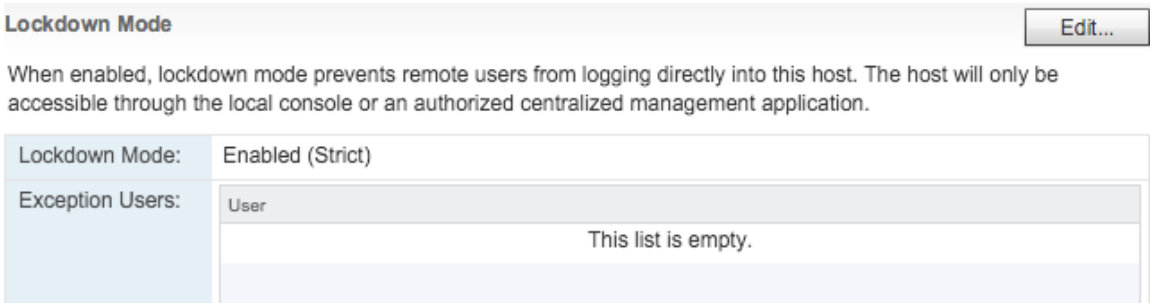

Figure 2. vSphere Lockdown Mode

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

This requirement refers primarily to the management of cardholder data storage, authentication data, and data elements such as a Primary Account Number (PAN) and Card Verification Code (CVC). Compliance including encryption of these items is commonly handled at the application layer before being written to storage.

Virtual SAN includes an end-to-end software checksum mechanism to help protect data against data integrity issues. This feature is on by default, but can be disabled through the use of a storage policy. If encryption at the datastore level is needed, this can be achieved through the use of third-party solutions such as self-encrypting drives and HyTrust DataControl.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

As discussed in “Build and Maintain a Secure Network and Systems - Requirement 1”, Virtual SAN network traffic is commonly limited to private networks. Transmission of application data residing in virtual machines across public networks is not required to utilize Virtual SAN. If a Virtual SAN stretched cluster configuration is implemented, the network connection between the two sites containing data should be a private connection.

Maintain a Vulnerability Management Program

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

vCenter Server runs as a Windows application or in a Linux-based virtual machine appliance. Windows machines (virtual or physical) running vCenter Server can be systematically updated using solutions such as Microsoft Windows Server Update Services. A variety of third-party malware and antivirus solutions are available to address threats to virtual and physical machines running Windows.

VMware provides security-related fixes for vSphere and Linux-based virtual appliances through the VMware Security Advisories web page and email notifications. VMware vSphere Update Manager™ can be utilized to automate the deployment of security patches and other updates to vSphere hosts making it easy to comply with this requirement.

Requirement 6: Develop and maintain secure systems and applications

As discussed on VMware's Security web page, VMware takes customer security and safety very seriously. VMware has well-established programs and practices to identify and remediate security vulnerabilities in our products and to mitigate software security risks to customers. These programs are constantly evolving based on our own experiences, changes in the threat landscape, and our learnings based on industry observation and collaboration. Virtual SAN is no exception to these programs. For more details about VMware product security, please refer to the VMware Product Security White Paper.

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know

While compliance for this requirement is typically handled at the application layer, it is important to point out that access control measures can be implemented at the infrastructure layer, as well. Access control is a key component of vCenter Server. Administrators can utilize existing roles or create new roles with customized privileges for a variety of objects in vCenter Server such as virtual machines, vSphere hosts, and datastores including Virtual SAN.

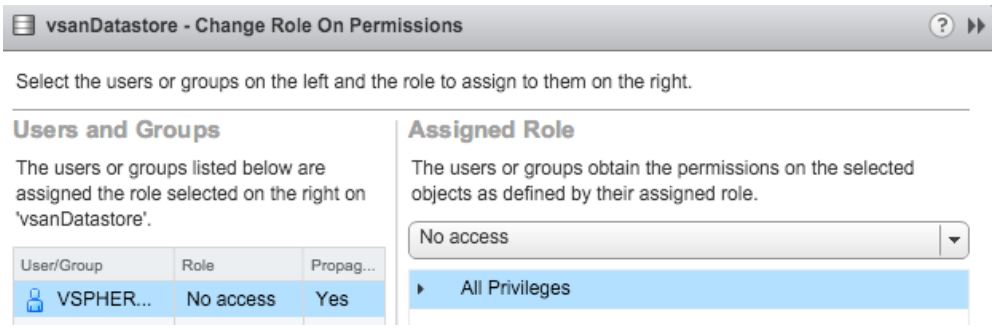

Figure 3. Virtual SAN Datastore Access Control

Requirement 8: Identify and authenticate access to system components

As with any authentication system, users should have individual, password-protected accounts to facilitate access control and proper logging when access is granted or denied. vCenter Server and VMware's Single Sign-On technology enables the creation of individual accounts and groups to implement proper access control. Single Sign-On also integrates with third-party authentication solutions such as Microsoft Active Directory and other Lightweight Directory Access Protocol (LDAP) applications. These controls can be used to limit and monitor access to a Virtual SAN datastore. The following excerpts from vmware-sts-idmd.log in vCenter Server shows an example of a failed login and successful login.

```
2016-02-18T18:58:21.315Z vsphere.local        9bd70d07-dc54-4b57-98ee-c9a03bb04db8 INFO ]
[IdentityManager] Authentication failed for user [jhunter@vsphere.local] in tenant [vsphere.local]
in [14] milliseconds with provider [vsphere.local] of type
[com.vmware.identity.idm.server.provider.vmwdirectory.VMwareDirectoryProvider]
```

```
[2016-02-18T18:58:28.169Z vsphere.local        ac2af3d6-1896-4b6d-93e8-846581875eaa INFO ]
[IdentityManager] Authentication succeeded for user [jhunter@vsphere.local] in tenant
[vsphere.local] in [53] milliseconds with provider [vsphere.local] of type
[com.vmware.identity.idm.server.provider.vmwdirectory.VMwareDirectoryProvider]
```

Requirement 9: Restrict physical access to cardholder data

A Virtual SAN datastore is comprised of storage devices contained within vSphere host servers. Physical access to a Virtual SAN datastore can only be obtained by accessing the vSphere hosts that make up the Virtual SAN cluster. Access to all vSphere hosts and vCenter Server should be controlled in the same many as any other physical asset in a PCI-compliant environment.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Virtual SAN network connectivity utilizes the same standards as other types of network traffic Tools that monitor network access and health can be used with the network connections put in place for Virtual SAN.

When reviewing audit logs, time synchronization is critical to correlating events across multiple networked computer systems. Network Time Protocol (NTP) should be configured on every vSphere host to help ensure time is synchronized across all hosts in a cluster. NTP should also be configured for vCenter Server. Virtual machines can be configured to get the correct time from a vSphere host through VMware Tools or through native NTP services in the guest operating systems of the virtual machines.

Access to cardholder data is commonly controlled at the application layer and proper access control should be implemented at this layer. It is also important to restrict access to vCenter Server, vSphere hosts, and the virtual machines running on Virtual SAN. Virtual machine backup data should also be properly secured with encryption and by limiting access to the physical media on which the backup data resides.

VMware vRealize® Operations™ enables the use of rules to constantly monitor configuration items in the environment for PCI compliance. vRealize Configuration Manager includes a number of predefined templates including PCI DSS that enable an organization to quickly help determine items out of compliance.

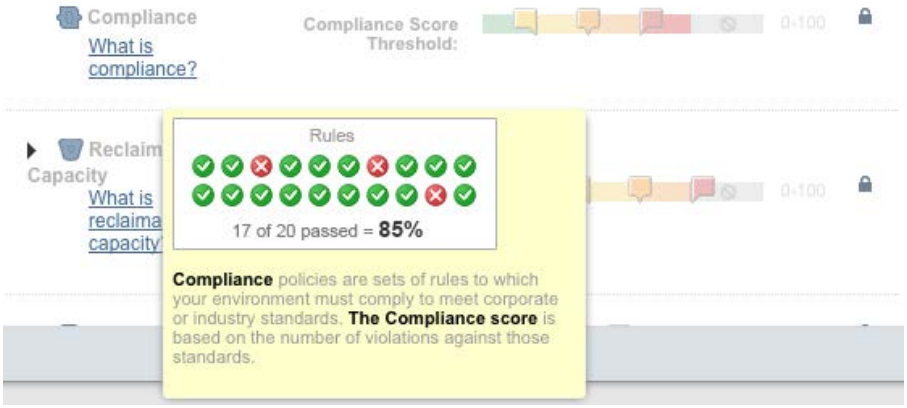

Figure 4. Compliance Reporting in vRealize Operations

Logs available on both the vSphere hosts and in vCenter Server can be used to audit access. VMware vRealize® Log Insight™ should be a consideration to help ease the task of log correlation and auditing.

Requirement 11: Regularly test security systems and processes

As with any networked computer system in an environment subject to PCI compliance, vCenter Server and vSphere hosts in a Virtual SAN cluster should be subject to regular testing for security vulnerabilities. Considering Virtual SAN utilizes standard networking connections and protocols, the same tools used to monitor other networks can be utilized for the Virtual SAN network.

VMware provides vSphere Update Manager to automate the process of deploying security patches and other fixes to vSphere hosts running Virtual SAN. Recommendations for securing a vSphere environment can be found in VMware Documentation and VMware Security Hardening Guides to help pass vulnerability and penetration tests.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security for all personnel

This requirement primarily addresses policies and operating procedures in an organization subject to PCI compliance. Just like other information systems assets in the organization, processes and procedures governing access to and administration of a vSphere environment with Virtual SAN should be clearly defined and well documented. Administrators with full access to a Virtual SAN datastore can potential modify or delete large amounts of data very quickly. This is the case with any storage containing data for multiple applications. These administrators should be carefully screened prior to granting access to datastores including Virtual SAN. Effective backup and disaster recovery methods should also be in place to protect an organization against data loss and corruption and enable quick recovery from a system breech or disaster.

Summary

VMware's Hyperconverged Software consists of vCenter Server, vSphere, and Virtual SAN, which is the market-leading hyperconverged infrastructure solution. These products have the necessary security and controls in place to help organizations easily comply with regulatory standards such as PCI DSS. Virtual SAN's ease of implementation and administration along with outstanding performance make it an attractive storage solution for nearly any organization and use case. Since Virtual SAN runs within the vSphere kernel and it is managed by vCenter Server, it can be secured using the same controls and measures that have been employed for other storage types in PCI-compliant virtualized environments for many years. A number of additional VMware and third-party solutions such as NSX, vRealize Operations, LogInsight, and HyTrust DataControl can be utilized to further enhance security, reduce risk, and help achieve PCI compliance.

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

About the Author

Jeff Hunter is a Staff Technical Marketing Architect at VMware with a focus on storage and availability solutions. He has been with VMware for more than 8 years, prior to which he spent several years implementing and administering VMware virtual infrastructures at two Fortune 500 companies. Follow Jeff Hunter on Twitter: @jhuntervmware

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