TECHNICAL WHITE PAPER
October 2024

VMware vSAN PCI-DSS Compliance Guide

vmware by Broadcom

Table of contents

Introduction 3

Requirement 1: Install and maintain network security controls 4

Requirement 2: Apply secure configurations to all system components 4

Requirement 3: Protect stored account data 5

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks 6

Requirement 5: Protect all systems and networks from malicious software 6

Requirement 6: Develop and maintain secure systems and software 7

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

Requirement 8: Identify users and authenticate access to system components 8

Requirement 9: Restrict physical access to cardholder data 8

Requirement 10: Log and monitor all access to system components and cardholder data 9

Requirement 11: Test the security of systems and networks regularly 10

Requirement 12: Support information security with organizational policies and programs 10

Summary 12

Introduction

VMware Cloud Foundation (VCF) is a comprehensive platform that delivers a high-performance and cost-effective private cloud solution by integrating core VMware technologies. VCF combines the industry-leading vSphere hypervisor, vSAN software-defined storage, NSX network virtualization, vCenter Server for unified management, and VCF Operations for comprehensive monitoring and optimization. This integrated stack provides a robust foundation for modern applications and workloads, simplifying deployment and management while ensuring optimal performance and efficiency.

VMware vSAN delivers the industry's best storage value with simple management, high performance, low cost, and a future-proof roadmap that supports any app on any scale. vSAN 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 vSAN to run mission-critical applications such as Microsoft SQL Server, SAP, and Oracle Database. Sectors such as finance, retail, and card brands mandate compliance with security standards administered by the Payment Card Industry (PCI) Security Standards Council.

This guide provides an overview of how vSAN can be successfully utilized in an environment governed by PCI compliance. The following sections discuss the main goals and requirements of the PCI Data Security Standard (DSS) as outlined in the PCI DSS Quick Reference Guide.

Requirement 1: Install and maintain network security controls

vSAN, a VMware Cloud Foundation (VCF) core component, is commonly deployed behind an organization's internal firewall to provide storage services for virtual machines. This deployment strategy aligns with PCI DSS security requirements, as it helps isolate sensitive data within a protected network environment.

vSAN network communication is typically confined to the VMware vSphere hosts and internal networks that comprise the vSAN cluster. This communication, which includes data replication and synchronization traffic, is generally not routed to a public network, minimizing exposure to external threats.

However, certain vSAN configurations, such as Stretched Clusters and 2-node deployments, require communication with a vSAN Witness virtual machine at an alternate site. This communication, which primarily involves cluster metadata and does not include sensitive cardholder data, may traverse public networks using a secure WAN connection.

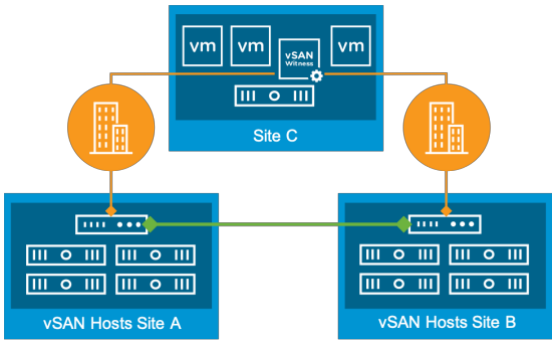

Figure 1. vSAN Stretched Cluster

Communication between physical nodes (vSphere hosts) requires a minimum of 10Gbps and a Round-Trip Time (RTT) latency of 5ms or less. These requirements are typically only achieved using private network connections not routed across public networks. Communication between physical nodes is not encrypted and should not traverse public network connections.

Cluster metadata communicates between the physical nodes and the vSAN witness. Since the vSAN Witness is typically deployed to an alternate location, this metadata is likely transmitted beyond firewalls using a Wide Area Network (WAN) connection. However, data such as customer information, account numbers, and so on stored in virtual machine applications and databases is not transmitted to or from the vSAN Witness or stored in the vSAN Witness.

vSAN utilizes standard network connectivity architecture, 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 vSAN network.

VMware NSX is recommended to enable specific network access control. NSX brings security inside the data center with automated fine-grained policies tied to the virtual machines. 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.

Requirement 2: Apply secure configurations to all system components

While VMware vSphere and vSAN offer robust security features, relying solely on vendor-supplied defaults can leave your environment vulnerable. Customizing security settings and establishing strong passwords is crucial to bolster protection against unauthorized access and potential threats.

vSphere and vCenter Server do not utilize default passwords. The installation process mandates administrators set unique passwords, eliminating the risk associated with commonly known credentials. However, it's essential to go beyond this initial step and configure additional security measures.

vSAN inherits the access control mechanisms of vSphere and vCenter Server, making proper configuration of these systems paramount. Employing the principle of least privilege ensures that users and groups have only the necessary permissions for their roles. Regularly audit and update these permissions as needed.

Despite vSphere's default firewall and disabled SSH, it is crucial to review and fine-tune these settings according to your specific security requirements. Restricting communication to only trusted networks and devices can significantly minimize the attack surface. Implementing multi-factor authentication adds an extra layer of defense against unauthorized access.

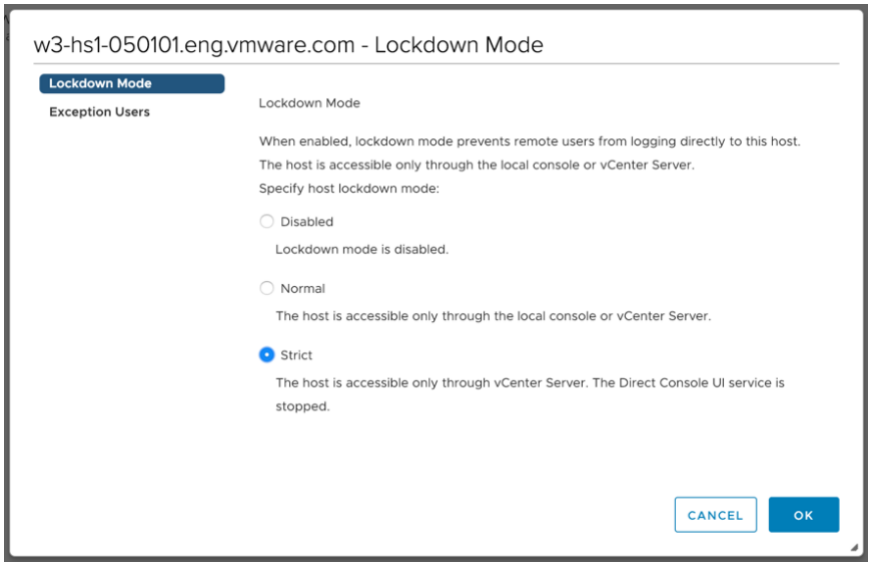

Figure 2. vSphere Lockdown Mode

By proactively customizing security configurations and establishing strong password practices, you can fortify your VMware vSphere and vSAN environment against potential threats and ensure the integrity and confidentiality of your critical data.

Requirement 3: Protect stored account data

Protecting sensitive data like credit card information is paramount in today's environment. The Payment Card Industry Data Security Standard (PCI DSS) outlines stringent requirements for safeguarding cardholder data, including encryption of sensitive elements like the Primary Account Number (PAN) and Card Verification Code (CVC). While PCI DSS compliance often focuses on application-level encryption before data is written to storage, employing additional encryption measures can further enhance data security.

VMware vSAN offers a robust solution with FIPS 140-2 validated encryption for data at rest. This validation ensures that vSAN's encryption mechanisms meet the rigorous standards of the National Institute of Standards and Technology (NIST). By encrypting all data stored on vSAN, this feature provides a comprehensive layer of protection against unauthorized access and data breaches.

One key advantage of vSAN encryption is its ease of use. It doesn't require specialized hardware or complex configurations, making it readily accessible for organizations of all sizes. Enabling vSAN encryption is a straightforward process that can be seamlessly integrated into your existing infrastructure.

The VMware Certifications web page provides information for those seeking more granular details about VMware's FIPS 140-2 validation. This resource offers comprehensive documentation and certificates that attest to the compliance and robustness of VMware's encryption solutions.

Requirement 4: Protect cardholder data with strong cryptography during transmission over open, public networks

VMware vSphere and vSAN provide a robust foundation for securing cardholder data during transmission over open, public networks, a key requirement of PCI DSS. While vSAN primarily operates within private networks, the broader vSphere environment offers tools and capabilities to ensure secure data transmission when traversing public networks.

vSphere's security features, such as its built-in firewall and support for secure protocols like TLS and SSH, enable data encryption in transit. By configuring these features and adhering to security best practices, organizations can effectively protect sensitive cardholder data from unauthorized access while meeting PCI DSS requirements.

For instance, employing a private connection between those sites is crucial when utilizing a vSAN stretched cluster configuration across geographically diverse sites. This dedicated link ensures that sensitive data remains within a secure and controlled environment, minimizing exposure to public networks and potential threats.

Furthermore, organizations can leverage vSphere's network segmentation capabilities to isolate the cardholder data environment (CDE) from other network segments. This isolation adds an extra layer of protection by restricting access to sensitive data and reducing the risk of unauthorized exposure.

Requirement 5: Protect all systems and networks from malicious software

Protecting systems and networks from malicious software is critical to any security strategy, and VMware provides a multi-layered defense system to achieve this. VMware actively releases security patches and updates for its software solutions, addressing vulnerabilities and enhancing security features. These updates are readily available through the VMware Security Advisories web page and email notifications, ensuring your environment remains protected against the latest threats.

VMware vSphere Lifecycle Manager automates the deployment of security updates to vSphere hosts to streamline the patching process. This automation simplifies compliance efforts by applying critical patches promptly and consistently across the environment. vSphere Lifecycle Manager can be configured to scan for missing patches, download updates from VMware repositories, and apply them to ESXi hosts with minimal manual intervention. This helps mitigate the risk of human error and ensures that systems are consistently updated with the latest security fixes.

VMware NSX, a network virtualization and security platform, provides advanced capabilities to enhance malware protection further. With intrusion detection and prevention (IDS/IPS), network traffic analysis, and micro-segmentation, NSX helps identify and mitigate threats before they

compromise systems. NSX's IDS/IPS functionality analyzes network traffic for malicious patterns and signatures, blocking or quarantining suspicious activity. Network traffic analysis provides visibility into network flows, enabling administrators to identify anomalies and potential threats. Micro-segmentation allows for creating granular security policies, isolating sensitive workloads and restricting lateral movement within the network.

Beyond prevention, VMware Live Recovery offers a robust solution for recovering from malware attacks. By providing a secure, isolated environment for recovery, Live Recovery helps ensure that restored systems are clean and free from malware, minimizing downtime and data loss. Live Recovery enables organizations to create isolated recovery environments disconnected from the production network. This isolation prevents malware from spreading and allows for the secure restoration of clean backups. Live Recovery also provides data protection and ransomware recovery capabilities, enabling restoration to specific points in time while minimizing data loss.

Requirement 6: Develop and maintain secure systems and software

VMware Cloud Foundation (VCF) provides a comprehensive platform that significantly aids in meeting the PCI DSS requirement for secure systems and software development. By streamlining the deployment and management of a complete private cloud stack, VCF establishes a secure foundation for applications and workloads, simplifying compliance efforts.

VCF achieves this by incorporating security into its core components, including vSphere, vSAN, and NSX. These components are designed with security in mind, offering features like:

- vSphere: Secure configuration management through vCenter Server, including role-based access control (RBAC) and lockdown mode, enabling granular control over user permissions and system access. vSphere also supports secure boot and trusted platform modules (TPM) to ensure the integrity of the hypervisor and prevent tampering.
- vSAN: Data-at-rest encryption using FIPS 140-2 validated cryptography, safeguarding sensitive cardholder data from unauthorized access. vSAN also supports secure network communication protocols and integrates with NSX for micro-segmentation.
- NSX: Network micro-segmentation capabilities allow for isolating sensitive workloads and creating granular security policies. NSX also provides intrusion detection and prevention (IDS/IPS) functionality to monitor and block malicious network traffic and supports the implementation of virtual firewalls to control network access.

VCF also provides tools for automating security updates and patching, ensuring systems remain protected against the latest threats. vSphere Lifecycle Manager allows for centralized management and automated deployment of patches and updates across the entire vSphere environment, including ESXi hosts and virtual appliances. This automation helps ensure consistent and timely patching, reducing the risk of exploited vulnerabilities.

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

VCF provides a comprehensive platform for managing and securing the entire private cloud environment. At the same time, vSAN offers granular access control mechanisms for securing data at the storage layer.

VCF enables organizations to define and enforce access control policies across a private cloud. By integrating with directory services and role-based access control (RBAC) systems, VCF ensures that only authorized users and groups can access sensitive cardholder data. This centralized management approach simplifies restricting access based on job roles and responsibilities.

vSAN further enhances access control by providing granular permissions at the storage level. Administrators can define specific permissions for individual users and groups, limiting their access to only the necessary data stores and virtual machines. This granular control ensures that sensitive cardholder data is protected from unauthorized access, even within the virtualized environment.

Moreover, vSAN encryption adds another layer of security by encrypting all data at rest. This encryption ensures that the sensitive data remains unreadable even if unauthorized access occurs without the proper decryption keys.

By combining the comprehensive access control capabilities of VCF with the granular permissions and encryption provided by vSAN, organizations can effectively restrict access to cardholder data based on business need-to-know. This layered approach ensures compliance with PCI DSS requirements and safeguards sensitive information from unauthorized access.

Requirement 8: Identify users and authenticate access to system components

VMware Cloud Foundation (VCF) and VMware vSAN provide robust mechanisms to satisfy the PCI DSS requirement for identifying users and authenticating access to system components. VCF offers a centralized platform for managing user accounts and access control policies across the private cloud. At the same time, vSAN integrates with these capabilities to ensure secure authentication and authorization at the storage layer.

VCF utilizes VMware's Single Sign-On (SSO) technology, enabling the creation of individual user accounts and groups with strong password protection. SSO supports a variety of authentication methods, including:

- Password-based authentication: Enforcing strong password policies, including password complexity requirements, minimum length, and regular password changes.
- Certificate-based authentication: Using X.509 certificates for secure user authentication eliminates the need for passwords and provides stronger security.
- Multi-factor authentication (MFA): Integrating with third-party MFA solutions adds an extra layer of security, requiring users to provide multiple forms of identification for authentication.

SSO integrates with existing directory services like Microsoft Active Directory and other LDAP solutions, allowing organizations to leverage their established identity management infrastructure. This centralized approach simplifies user management and ensures consistent authentication across a private cloud. Administrators can manage user accounts, groups, and roles from a single pane of glass, streamlining user provisioning and de-provisioning processes.

vSAN seamlessly integrates with VCF's SSO and access control mechanisms. By enforcing authentication and authorization policies, vSAN ensures that only identified and authenticated users can access sensitive data stored on vSAN datastores. This integration provides a granular level of control, allowing administrators to define specific permissions for individual users and groups based on their roles and responsibilities. Permissions can be set at the datastore, virtual machine, and even individual virtual disk levels, providing fine-grained control over data access.

Furthermore, vSAN leverages vSphere's audit logging capabilities to track all user activity related to vSAN resources. These logs provide a detailed record of user actions, including login attempts, data access, and configuration changes. This audit trail helps meet PCI DSS requirements for logging and monitoring access to sensitive data.

Requirement 9: Restrict physical access to cardholder data

Since a vSAN datastore comprises storage devices within vSphere host servers, controlling access to these hosts is paramount. VCF enables organizations to implement access control measures, such as physical security protocols and surveillance systems, to restrict access to the data center environment where these hosts reside.

vSAN encryption, validated by FIPS 140-2, ensures that data remains unreadable even if physical access to storage devices is compromised without the proper decryption keys. This encryption utilizes strong XTS-AES-256-length keys, further enhancing data security. Moreover, vSAN encryption renders data unrecoverable on retired or removed media devices. Whether through normal lifecycle management or theft, any data on these devices remains encrypted and inaccessible, mitigating the risk of data breaches even if physical devices are compromised.

Requirement 10: Log and monitor all access to system components and cardholder data

VCF provides a robust framework for meeting the PCI DSS requirement to log and monitor all system components and cardholder data access. With its integrated Aria Operations platform, VCF offers a comprehensive approach to logging, monitoring, and auditing, ensuring that organizations can effectively track and analyze access to sensitive data.

VCF Operations, formerly Aria Operations, is crucial in fulfilling this PCI DSS requirement. It provides deep visibility into the entire VCF environment, including vSAN, by collecting and analyzing log data from various sources such as vCenter Server, ESXi hosts, and network devices. This centralized log management capability allows administrators to gain a holistic view of system activity and identify any potential security breaches or compliance violations.

Specifically, VCF Operations offers the following features that contribute to PCI DSS compliance:

- Real-time Monitoring: VCF Operations for Networks continuously monitors network traffic, providing real-time insights into data flows and access patterns. This allows administrators to proactively detect and respond to any anomalies or suspicious activities that could indicate unauthorized access to cardholder data.
- Log Correlation and Analysis: VCF Operations can identify patterns and relationships between events by correlating logs from different sources. This enables security teams to investigate incidents more effectively, helping to identify the root cause of security breaches and prevent future occurrences.
- Customizable Alerts and Notifications: VCF Operations allows administrators to define custom alerts based on specific criteria, such as unauthorized access attempts or changes to sensitive configurations. These alerts can trigger notifications, ensuring that security teams are immediately aware of potential threats and can take appropriate action.
- Compliance Dashboards and Reports: VCF Operations provides pre-built dashboards and reports that offer insights into PCI DSS compliance posture. These dashboards highlight areas of concern and provide actionable recommendations for remediation, simplifying the compliance management process.

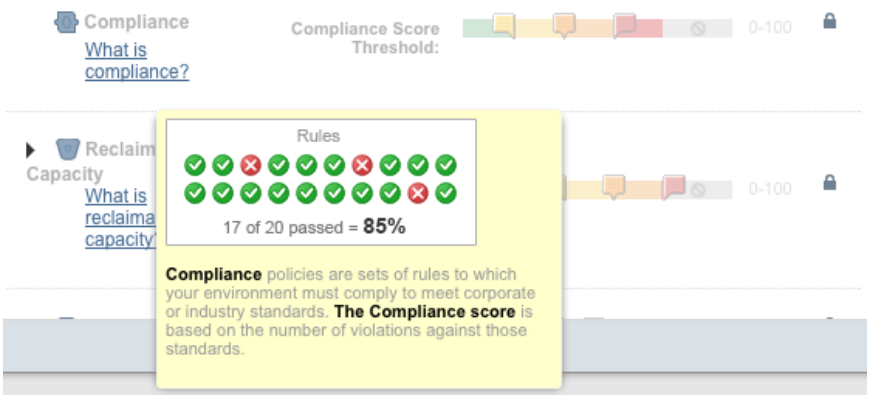

Figure 3. Compliance score

Requirement 11: Test the security of systems and networks regularly

VCF's lifecycle management capabilities play a crucial role by automating the deployment of security patches and updates, ensuring systems are protected against known vulnerabilities. This automation includes creating baselines to define desired states for ESXi hosts, scanning hosts for compliance against those baselines, and automatically remediating discrepancies. vSphere Lifecycle Manager also allows scheduling regular scans and generating reports on compliance status. By streamlining the patching process, vSphere Lifecycle Manager helps organizations adhere to PCI DSS requirements for regular vulnerability management.

Furthermore, VCF leverages standard networking protocols and connections for vSAN, enabling the use of common network security testing tools. Organizations can employ vulnerability scanners, such as Nessus or Qualys, to identify potential weaknesses in the vSAN network configuration. These scanners can detect open ports that attackers could exploit, use outdated or insecure protocols like SSLv3 or TLS 1.0, and misconfigured firewall rules, access control lists, or other network settings that could weaken security.

In addition to automated tools, VCF provides comprehensive security hardening guides and documentation. These resources offer detailed recommendations for configuring vSphere and vSAN to meet PCI DSS security standards. These recommendations cover areas such as network security (configuring firewalls, VLANs, and network access control lists), host security (hardening ESXi hosts by disabling unnecessary services, securing SSH access, and enabling lockdown mode), and data security (implementing vSAN encryption and configuring access control lists for datastores). By following these guidelines, organizations can strengthen their security posture and reduce the risk of vulnerabilities.

Requirement 12: Support information security with organizational policies and programs

VCF supports defining and enforcing security policies across a private cloud environment. Through its integration with directory services and role-based access control (RBAC), VCF enables organizations to implement granular access control policies, ensuring that only authorized personnel can access sensitive systems and data. This granular control helps organizations adhere to PCI DSS requirements for restricting access based on the principle of least privilege.

vSAN further strengthens security by providing data-level protection and access control mechanisms. vSAN encryption ensures that data remains protected even if unauthorized access occurs. Additionally, vSAN's granular permissions allow administrators to define specific access levels for individual users and groups, limiting their ability to modify or delete data.

VCF and vSAN also support the implementation of effective backup and disaster recovery strategies. Regular backups of vSAN datastores and virtual machines help protect against data loss and enable rapid recovery in a security breach or disaster. VCF's disaster recovery capabilities, such as vSphere Replication and Site Recovery Manager, provide robust mechanisms for replicating and recovering critical workloads, ensuring business continuity.

By combining VCF's comprehensive security management capabilities with vSAN's data protection and access control features, organizations can establish and support information security policies and programs that align with PCI DSS requirements. This comprehensive approach helps organizations maintain a secure and compliant environment for cardholder data and other sensitive information.

Summary

VMware Cloud Foundation (VCF) and vSAN provide a robust framework for restricting physical access to cardholder data, a crucial requirement of PCI DSS. VCF facilitates the management of the physical infrastructure underlying the vSAN datastore. Since a vSAN datastore comprises storage devices within vSphere host servers, controlling access to these hosts is paramount. VCF enables organizations to implement access control measures, such as physical security protocols and surveillance systems, to restrict access to the data center environment where these hosts reside. This could include biometric authentication, security guards, and surveillance cameras to monitor and control access to the physical servers.

vSAN complements these physical security measures with data-level protection. vSAN encryption, validated by FIPS 140-2, ensures that data remains unreadable even if physical access to storage devices is compromised without the proper decryption keys. This encryption utilizes strong XTS-AES-256-length keys, further enhancing data security. This means that even if someone physically removed a drive from a vSAN host, the data on that drive would remain encrypted and inaccessible.

Moreover, vSAN encryption renders data unrecoverable on retired or removed media devices. Whether through normal lifecycle management or theft, any data on these devices remains encrypted and inaccessible, mitigating the risk of data breaches even if physical devices are compromised. This ensures that the data they contain cannot be recovered when drives are decommissioned or repurposed, reducing the risk of data breaches. By integrating VCF's physical infrastructure management with vSAN's encryption capabilities, organizations can effectively restrict physical access to cardholder data and comply with PCI DSS requirements. This multi-layered approach safeguards sensitive information from unauthorized physical access and potential data breaches.

Item No: vmw-bc-wp-tech-temp-uslet-word-2024 1/24