This is the final document in the compliance reference architecture for PCI DSS. You can find more information on the framework and download the additional documents from the PCI DSS compliance resources tab on VMware Solution Exchange here.
Table of Contents

Executive Summary ........................................................................................................... 5
For Additional Consideration .......................................................... 5
Implementing PCI DSS 3.2: Use Case Examples .................................................. 6
VMware Compliance Capable Solution for PCI DSS 3.2 ........................................... 7
VMware Validated Design for the SDDC ................................................................. 8
Organization Workload Architecture ........................................................................... 34
VVD VMware Software Components in the Validated Design for SDDC 3.0 ........ 38
Validation Scope and Approach ..................................................................................... 39
Findings and Observations ......................................................................................... 41
Objective: Segmentation .............................................................................................. 41
Objective: Build and Maintain a Secure Network and Systems .................................. 42
Objective: Regularly Monitor and Test Networks ..................................................... 52
Summary ......................................................................................................................... 61
Resources ......................................................................................................................... 62
Acknowledgements ......................................................................................................... 63
About Coalfire ................................................................................................................ 63
Rev 1.0 Jason Macallister First Release Coalfire and VMware SME

The following people provided key input into this whitepaper.

<table>
<thead>
<tr>
<th>Name</th>
<th>Email Address</th>
<th>Role/Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jason Macallister</td>
<td><a href="mailto:jason.macallister@coalfire.com">jason.macallister@coalfire.com</a></td>
<td>Senior Consultant/Principle Author</td>
</tr>
<tr>
<td>Chris Krueger</td>
<td><a href="mailto:chris.krueger@coalfire.com">chris.krueger@coalfire.com</a></td>
<td>Principle/QA to Customer Draft Release</td>
</tr>
<tr>
<td>Anthony Dukes</td>
<td><a href="mailto:adukes@vmware.com">adukes@vmware.com</a></td>
<td>Technology SME, VMware</td>
</tr>
<tr>
<td>Carlos Phoenix</td>
<td><a href="mailto:cpelaez@vmware.com">cpelaez@vmware.com</a></td>
<td>Compliance and Cybersecurity SME, VMware</td>
</tr>
</tbody>
</table>
Trademarks and Other Intellectual Property Notices

The VMware products and solutions discussed in this document are protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their companies.

<table>
<thead>
<tr>
<th>Solution Area</th>
<th>Key Products</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-Defined Compute</td>
<td>VMware ESXi™, VMware vCenter™, VMware vCenter Server®, VMware vCenter Server® Standard™, VMware vCenter™ Single Sign-On, VMware vCenter Server® Appliance™, VMware vCloud Suite®, VMware vSphere® Data Protection™, VMware Tools™, VMware vSphere® Distributed Resource Scheduler™, VMware vSphere® Distributed Power Management™, VMware vSphere® Enterprise Plus Edition™, VMware vSphere® Fault Tolerance, VMware vSphere® Flash Read Cache™, VMware vSphere® High Availability, VMware vSphere® Storage DRS™, VMware vSphere® Storage vMotion®, VMware vSphere® vMotion®, VMware vSphere® Web Client, Platform Services Controller™</td>
</tr>
<tr>
<td>Software-Defined Networking</td>
<td>VMware NSX®, VMware NSX® Manager™, VMware NSX® Edge™, VMware NSX® Controller™, VMware NSX® Services™, VMware NSX® Virtual Switch™, VMware NSX® API™, VMware NSX® for vSphere®</td>
</tr>
<tr>
<td>Management and Automation</td>
<td>VMware vRealize® Suite Enterprise, VMware vRealize® Operations™, VMware vRealize® Operations Manager™, VMware vRealize® Hyperic®, VMware vRealize® Configuration Manager™, VMware vRealize® Infrastructure Navigator™, VMware vRealize® Log Insight™, VMware vRealize® Log Insight™ Content Pack for xxx, VMware vRealize® Operations Insight™, VMware vRealize® Orchestrator™, VMware vRealize® Orchestrator Application™, VMware vRealize® Operations for Horizon®, VMware vRealize® Operations for Published Applications™, VMware vRealize® Operations Manager™ for Horizon®, VMware vRealize® Automation™, VMware vRealize® Business™ Enterprise, VMware vRealize® Operations Management Pack™ for xxx, VMware vSphere® Service Manager™, VMware vSphere® Syslog Collector, VMware vSphere® Update Manager™, VMware vSphere® Update Manager Client™, VMware vSphere® with Operations Management™, VMware Power CLI</td>
</tr>
<tr>
<td>Disaster Recovery Automation</td>
<td>VMware vCenter™ Site Recovery Manager™, VMware vSphere® Replication™</td>
</tr>
</tbody>
</table>
Executive Summary

Per the Payment Card Industry Security Standards Council (PCI SSC), “The Payment Card Industry Data Security Standard (PCI DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally.” (PCI SSC, 2016) The Payment Card Industry Data Security Standard version 3.2 (PCI DSS v3.2) is a proprietary information security standard that was created to reduce credit card fraud by stipulating a series of controls regulating the use of information systems that handle cardholder data (CHD) and sensitive authentication data (SAD). PCI DSS is not an optional standard. As stated, all entities who process, store, or transmit CHD and/or SAD must comply with the standard or they can be fined or refused access to the card brand’s payment system.

VMware recognizes the importance of PCI DSS and understands that the following critical areas must be addressed by each entity (merchants, processors, acquirers, issuers, and service providers) involved in payment card processing: security and compliance, the criticality and vulnerability of the assets needed to manage infrastructures impacting payment card processing, and the risks to which those assets are exposed. By standardizing an approach to compliance and expanding that approach to include technology partners, VMware provides its customers with a proven solution that more fully addresses their compliance needs. This approach provides management, IT architects, administrators, and assessors with a high degree of transparency into risks, solutions, and mitigation strategies for moving critical applications and data to the cloud in a secure and compliant manner in alignment with the recommendations and requirements of PCI DSS in order to protect CHD.

VMware enlisted its assessor partner, Coalfire Systems, Inc. (Coalfire), a QSA company, to engage in a programmatic approach to assess VMware products and solutions for their capabilities to address PCI DSS recommendations and requirements and to document these capabilities as a set of reference architecture documents. This is the second in a series of documents representing Coalfire’s assessment of the different VMware technologies available to organizations that use (or are considering using) VMware Software-Defined Data Center (SDDC), Software Defined Networking (SDN), and End User Computing (EUC) platforms to host PCI SSC regulated information. For this assessment, the SDDC and SDN platforms have been designed and implemented in one of the VMware Centers of Excellence to support demonstration and testing of capabilities to address PCI DSS requirements. The implementation follows a VMware Validated Design approach inclusive of best practices for practical deployment of VMware technologies in real-world installations. Coalfire highlights specific PCI DSS requirements and recommendations that these technologies address and/or support and has applied a testing methodology to validate VMware’s claims of compliance capability in this Compliance Capable Solutions document.

It is Coalfire’s opinion that the assessed VMware Compliance Capable Solution provided sufficient control capabilities in support of the selected PCI DSS requirements and recommendations.

For Additional Consideration

Both VMware and Coalfire understand that no one technical solution or product can enable security and compliance. A strong security posture is best instituted through application of sound security design principles. Organizations are best able to attain compliance through comprehensive governance, risk management, and compliance (GRC) programs and not with a specific product or solution.

For more information on the VMware Reference Architecture Framework documents and VMware’s general approach to compliance issues, please review VMware Compliance Cyber Risk Solutions.
Implementing PCI DSS 3.2: Use Case Examples
For payment entities participating in any part of the payment processing cycle and requiring compliance with PCI DSS 3.2, it was VMware’s intention to demonstrate the capability of VMware solutions to facilitate control capabilities specific to use cases related to PCI DSS 3.2 compliance objectives. The coverage of VMware solutions to address PCI DSS 3.2 requirements was more broadly discussed in the VMware SDDC and EUC PCI DSS 3.2 Product Applicability Guide. From the broader discussion of solution to compliance framework alignment found in the Product Applicability Guide, VMware selected a couple of use cases to showcase for validation of compliance capability.

The use cases selected by VMware include network segmentation for Cardholder Data Environment (CDE) to reduce assessment scope for PCI DSS 3.2, network protection of CHD in a CDE, and accountability through audit, event logging, and analysis. These use cases are supported by the frequency with which inquiries are made to VMware with respect to these topics and relative to VMware capabilities. Additionally, these use cases align with technology capabilities which VMware has chosen to highlight for this validation exercise.

It is essential to enable controls to provide secure enclaves for systems and data to reside whereby the transmission of data can be routed appropriately and protected from unauthorized access. VMware chose to demonstrate the capability of VMware solutions to enable system and communication protection and information integrity. This aligns with PCI DSS Requirement 1. This capability assessment included testing procedures and guidance found for Requirement 1 in PCI DSS 3.2.

PCI DSS 3.2 also makes recommendations for network segmentation. For the payment entity requiring self-assessment or independent assessment of their CDE, some advantages may be gained by isolating the CDE from the remainder of an entity’s general purpose network including:

- Reduction in the scope of the PCI DSS assessment
- Reduction in the cost of the PCI DSS assessment
- Reduction in the cost and difficulty of implementing and maintaining PCI DSS controls
- Reduction in the risk to an organization by consolidating CHD into fewer, more controlled locations

The capability of VMware solutions to support consolidation of CHD into fewer, more controlled locations and providing isolation for CHD using network segmentation techniques was also addressed and validated in this exercise.

It should be noted that the inspection of boundary protection mechanisms was limited to the capabilities supported by VMware technologies. This assessment did not include evaluation of traditional boundary protection measures provided by physical firewall appliances and routers placed at the physical network boundary of the payment entity’s network and the untrusted network provided.
by the payment entity’s Internet Service Provider (ISP). Rather, what was assessed was the effectiveness of the VMware NSX for vSphere Edge Services Gateway to provide edge protection for the virtualized infrastructure and workloads. This capability can be an enhancement to traditional boundary protection mechanisms and may support a defense-in-depth strategy.

Included in the PCI DSS control objectives is the requirement to regularly monitor and test networks. Audit and accountability mechanisms provided by VMware assist the entity with tracking and monitoring of access to network resources and CHD. Testing and assessment included testing procedures and guidance found for Requirement 10 in the PCI DSS 3.2 document.

VMware and partner solutions are not limited in capability to these use cases. There may certainly be many more use cases available to demonstrate the capability of VMware to enable technical controls for the security of CHD in compliance with PCI DSS 3.2.

This document should be considered as an illustration of VMware’s commitment to its clients’ compliance and security requirements as well as VMware’s understanding of the applicability of security and compliance to the technology solutions they provide. Because not every organization is exactly alike regarding their approach to compliance, this document is intended to be an example for entities wanting to achieve compliance.

VMware Compliance Capable Solution for PCI DSS 3.2

The Center of Excellence used for this compliance capable validation exercise was a joint initiative by VMware and Intel. The hardware platform for the lab was inclusive of Intel-equipped solid state drives (SSDs), network controllers, and Intel Xeon based CPUs. The Center of Excellence follows the VMware Validated Design for SDDC. Figure 1 graphically illustrates, at a high level, the conceptual design of the VMware Validated Design for SDDC.

To demonstrate functional control capability for operational workloads, VMware layered on workloads representative of multiple distinct security domains as may exist in a typical organization. In alignment with the topic of PCI DSS 3.2, the security domains were labeled as CDE and non-CDE. Each server workload further represented a multitier server architecture representing web, application, and database.

Figure 1: Conceptual Rendering of the VMware Validated Design for Software-Defined Data Center
This section will provide a high-level summary of the architecture and design elements for the test lab made up of the VMware Validated Design for SDDC. The focus in this section will be primarily on the components that specifically relate to the previously specified use cases. For more complete and detailed information about the VMware Validated Design for SDDC please refer to the VMware Validated Design for SDDC Reference Architecture document.

**VMware Validated Design for the SDDC**

A VMware Validated Design (VVD) provides a comprehensive and extensively-tested design to build and operate the SDDC stack. VMware Validated Designs are based on VMware’s expertise in data center design and further de-risk deployments through extensive product testing to ensure interoperability, availability, scalability, and security. The designs are holistic and span across compute, storage, networking, and management, defining a gold standard for how to deploy and configure the complete SDDC stack with support for a broad set of use cases. Additionally, these designs include detailed guidance that synthesizes best practices for optimally operating the deployed SDDC.

Documents included in each design:

- **Validated SW Software Bill of Materials (BOM)** – Inter-operable versions of software that work together for a given VVD version
- **Release Notes** - Any known issues with the design
- **Design Details** – Design objectives, design decisions and the deep technical aspects of the designs
- **Architecture Diagrams** – Visualization of the architecture and the design
- **Pre-Deployment Checklists** – List of needed items for deployment
- **Deployment Guides** – Detailed instruction on how to deploy the data center
- **Configuration Workbooks** – How to configure the system and components
- **Validation Workbooks** – How to test and validate prior to go-live
- **Operational Guides** – Detailed guidance on Monitoring and Alerting, Backup and Restore, Upgrade, Security and Compliance, Startup and Shutdown, and more operation modules
- **Use Case Guides** – Modular guides that cover use cases like Micro Segmentation, IT Automating IT, and more

http://www.vmware.com/solutions/software-defined-datacenter/validated-designs.html

**Physical Infrastructure Design**

As with any technical solution, whether on premise or in the cloud, the solution starts with physical compute, storage, and network hardware. This lab environment made use of the converged infrastructure of the EMC Dell VxBlock. The VxBlock integrates enterprise-class compute, network, storage, and virtualization technologies from Cisco, Dell EMC, and VMware. This hardware was chosen for its modular design, which simplifies deployment and reduces time to operation. Figure 2, shows the physical wiring diagram of the VxBlock and illustrates the placement of pod components within the VxBlock. The wiring diagram shows both in-band and out-of-band networking. The out-of-band networking supports console access to infrastructure components. This diagram also
illustrates the placement of the management, compute, and edge pods within the physical hardware topology.

**Figure 2: Physical Infrastructure Design of VxBlock**

The VVD for SDDC uses common building blocks called pods. Pods represent the physical grouping of hardware components (network, storage, and compute) that support a certain function. The functions represented by the pods in the test lab for this validation exercise included compute, management, edge and storage. Figure 3 conceptually illustrates the physical components for each pod that makes up the SDDC.

**Figure 3: SDDC Architecture Physical Layer**

**Physical Design Fundamentals**

Figure 4 illustrates the pod architecture of the VVD for SDDC used for The Center of Excellence. This architecture includes two compute pods with 5 ESXi hosts each, 10 total. The compute pods were separated into separate data center racks. The third rack in the illustration shows a shared edge and compute pod, where the compute nodes in this pod may contain DMZ elements of tenant
workloads. The management pod also hosts the infrastructure management elements of the data center. Each rack contains top-of-rack (ToR) or leaf switches in redundant configuration that are connected to spine switches. This pod architecture is scalable and allows for increasing storage, compute and networking resources as necessary.

![Diagram of the VVD for SDDC](image)

Figure 4: Pods in the VVD for SDDC

The compute pods host the tenant or organization workload virtual machines (VMs). In a single subscriber model or private cloud, tenants may represent different departments of the organization. Also, included on the workload cluster are Guest Introspection ESXi Agents to support antivirus/anti-malware for the VMs in the cluster. In the case of this PCI DSS 3.2 validation assessment, the compute pod hosted representative CDE and non-CDE workloads. Table 1 is a listing of the physical ESXi hosts that make up the compute pods in the Center of Excellence used for PCI DSS 3.2 compliance capability testing.

<table>
<thead>
<tr>
<th>Host Name</th>
<th>VMkernel Management IP Address</th>
<th>VLAN ID</th>
<th>Cluster</th>
</tr>
</thead>
<tbody>
<tr>
<td>comp01esx01.ccrsoe02.local</td>
<td>172.19.11.61</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx02.ccrsoe02.local</td>
<td>172.19.11.62</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx03.crcsoe02.local</td>
<td>172.19.11.63</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx04.crcsoe02.local</td>
<td>172.19.11.64</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx05.crcsoe02.local</td>
<td>172.19.11.65</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx06.crcsoe02.local</td>
<td>172.19.11.66</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx07.crcsoe02.local</td>
<td>172.19.11.67</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx08.crcsoe02.local</td>
<td>172.19.11.68</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx09.crcsoe02.local</td>
<td>172.19.11.69</td>
<td>1911</td>
<td>Compute</td>
</tr>
<tr>
<td>comp01esx10.crcsoe02.local</td>
<td>172.19.11.70</td>
<td>1911</td>
<td>Compute</td>
</tr>
</tbody>
</table>

Table 1: Compute Cluster - Physical Compute Nodes of the Compute Pods

The management pod runs the VMs that manage the SDDC. For the PCI DSS 3.2 validation assessment, the management pod contained virtual management layer components, cloud
management layer components, and service management layer components. The management components include vCenter Server(s) and the Platform Services Controller(s), NSX Manager, NSX Controller, vRealize Operations Management, vRealize Log Insight, vRealize Automation, vRealize Orchestrator, and other shared management components as may be needed for the operation. Other shared management components may include, but are not limited to, Microsoft Active Directory Domain Controllers, DNS servers, DHCP servers, and physical infrastructure management. Table 2 provides a listing of ESXi hosts that make up the management pod.

![Table 2: Management Cluster – Physical Compute Nodes of the Management Pod](image)

The edge pods support on-ramp and off-ramp connectivity to the organization’s or service provider’s physical networks, connect VLANs in the physical world, and optionally host centralized physical services. Edge pods also connect virtual networks (overlay networks) provided by NSX for vSphere and the external networks. The edge pods are also the ingress/egress for traffic to and from the Internet. VMware NSX Edge Services Gateway appliances provide an additional layer of security between the untrusted, lower trust, and trusted networks. The edge pod for the PCI DSS 3.2 lab hosts edge services gateway appliances, distributed logical routers, and universal distributed logical routers in support of the overlay networks used to segment CDE from non-CDE resources. NSX Controller appliances are also hosted on the edge pod. Table 3 provides a listing of ESXi hosts that make up the edge pod.

![Table 3: Edge Cluster - Physical Compute Nodes of the Edge Pod](image)
Physical Network Design

The physical network is designed using a leaf and spine design for simplicity and scalability to best support network virtualization architecture. Leaf switches represent top of rack switches and provide network connection points for servers and uplink to spine switches. Leaf switches primarily handle east-west traffic within the environment, while spine switches primarily support north-south and cross-physical VLAN traffic. In this design, the spine represents multiple high-throughput Layer 3 switches with high port density. The leaf switches are made up of Cisco Nexus 9396XP switches. These are wire-rate Layer 2 and Layer 3 switches supporting line rates of 1/10/40 GE with 960 Gbps of switching capacity each. Spine switches in this lab environment are provided by Cisco Nexus 5000 series switches. Figure 5 illustrates the physical network architecture to support the network virtualization architecture.

The architecture supports expansion through the inclusion of additional racks. Each rack contains a pair of top-of-rack Nexus 9396XP switches and additional data center core spine switches as needed to support performance and availability requirements. Figure 5 also illustrates what expansion might look like. These physical switches provide the physical transport support for the organizations data center. It is through the physical switches that interoperability and connectivity can be made between virtual resources and physical resources in the organizations network. Not included in the evaluation for this validation assessment are physical firewall appliances that may sit at the physical boundary of the organization’s internal network and their ISP.

Top-of-rack physical switches are configured with trunk ports that connect with the ESXi hosts. ToR switches are configured to provide all the necessary physical VLANs via an 802.1Q trunk. These connect to virtual distributed switches (vDS) and form the basis for port groups on the vDS. Each ESXi host in the compute rack is connected redundantly to physical switches to support the SDDC network fabric.

Each ESXi host in the compute rack and the management/edge rack uses VLANs and corresponding subnets for internal-only traffic. Leaf switches in each rack act as Layer 3 interface for the corresponding subnet. The following figures and corresponding tables illustrate the connectivity of
ESXi hosts to physical switch infrastructure in each of the pods for compute, management, and edge respectively.

**Compute VLANs**

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Subnet</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1911</td>
<td>172.19.11.0/24</td>
<td>Layer 3 VMkernel Management Interface Network</td>
</tr>
<tr>
<td>1912</td>
<td>172.19.9.0/24</td>
<td>Layer 2 VMkernel network for vMotion operations</td>
</tr>
</tbody>
</table>
| 1916    | 172.19.16/0/24 | Layer 3 VTEP interface for VXLAN transport uplink to physical network. This network supports Edge Services connectivity in support of workload virtual machine network traffic.

**Management VLANs**

**Table 4: Physical to Virtual Networking – Compute Pod**

**Figure 6: VLANs and Subnets within the Compute Pod**

**Figure 7: VLANs and Subnets within the Management Pod**
Table 5: Physical to Virtual Networking – Management Pod

For this lab environment, NFS storage supported management with ISOS, VM images and templates, configuration backup, and so forth. It was also purposed as a vSphere Data Protection (VDP) backup target as well as target storage for vRealize Log Insight logs.

Communications between VLANs is controlled by Layer-3 physical switching infrastructure primarily handled by access control lists on the physical switches.

![Edge VLANs Diagram](image)

Figure 8: VLANs and Subnets within the Edge Pod

In addition to the physical VLANs represented in the previous diagrams and tables above, two additional VLANs existed, one on the Edge vDS and one on the Management vDS. These VLANs supported uplink connectivity to the organization's enterprise network including connectivity to the Internet for the Edge Services Gateways.

Table 6: Physical to Virtual Networking – Edge Pod

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Subnet</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1911</td>
<td>172.19.11.0/24</td>
<td>Layer 3 VMkernel network for host management interface</td>
</tr>
<tr>
<td>1912</td>
<td>172.19.12.0/24</td>
<td>Layer 2 VMkernel network in support of vMotion operations</td>
</tr>
<tr>
<td>1916</td>
<td>172.19.16.0/24</td>
<td>Layer 3 VTEP interface for VXLAN transport and uplink to physical network</td>
</tr>
</tbody>
</table>

Table 7: Edge Services Gateway Uplink Connections.

<table>
<thead>
<tr>
<th>VLAN ID</th>
<th>Subnet</th>
<th>Purpose</th>
<th>ESG Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1917</td>
<td>172.19.17.0/24</td>
<td>vDS-Mgmt01-Uplink01</td>
<td>ccrscoe02-mgmt-esg01-0</td>
</tr>
<tr>
<td>1918</td>
<td>172.19.18.0/24</td>
<td>vDS-Mgmt01-Uplink02</td>
<td>ccrscoe02-mgmt-esg02-0</td>
</tr>
<tr>
<td>1919</td>
<td>172.19.19.0/24</td>
<td>vDS-Edge01-Uplink01</td>
<td>ccrscoe02-edge-esg01-0</td>
</tr>
<tr>
<td>1920</td>
<td>172.19.20.0/24</td>
<td>vDS-Edge01-Uplink02</td>
<td>ccrscoe02-edge-esg02-0</td>
</tr>
</tbody>
</table>
Communications between VLANs is controlled by Layer-3 physical switching infrastructure and primarily handled by access control lists on the physical switch.

**Physical Storage Design**

Physical storage for this Center of Excellence was primarily served by fiber channel (FC) connectivity to an EMC VNX storage array, part of the VxBlock configuration. Cisco UCS B200 blades, through the Cisco Fabric Interconnects, are connected to Cisco MDS switches via FC. The Cisco MDS switches are, likewise, connected to FC ports on the storage array. Zoning is handled by the Cisco MDS fabric switches and LUN masking is handled on the array through alignment of LUNs to the hosts in storage groups. LUNs are presented to the ESXi hosts which formats the presented disk as VMFS volumes. The VMFS volumes are made available to vCenter for virtual machine storage.

Additional physical storage was made available to present NFS volumes as a target to the management pod for VM templates, ISOs, and other management tools. Additionally, the NFS volumes served to provide a target for vSphere Data Protection (vDP) as well as aggregated log storage for vRealize Log Insight. Figure 9 illustrates the layout of the storage from the VxBlock and shows how the storage was provisioned to support the various workloads and functions of the hosted components.
Figure 9: VxBlock Storage

Separate storage pools were created to support separation of CDE and non-CDE elements of the data center. Data stores were carved from the storage pools and presented to ESXi hosts for consumption by the virtual machines hosted within the virtual data center.
Virtual Infrastructure Design

The SDDC components are conceptually made up of a virtual infrastructure layer, cloud management layer, service management layer, business continuity layer, and security layer. Each layer works together to provide resources, management, provisioning, availability, security, and compliance for both the virtual infrastructure and the contained workloads that service the greater payment entity’s purpose. These components are networked together and secured with software-defined networking provided by VMware NSX for vSphere. The following is an overview of the infrastructure management, service management, and cloud management components with the software-defined networking that make up the Center of Excellence that served as a test lab for PCI DSS 3.2 configuration capability testing. The narrative and illustrations to describe the Center of Excellence infrastructure is purposely focused on the benefits that these components bring to the use cases described in a previous section, primarily that of network security. The architecture, design and logical network elements show the intentional boundaries of functional components to support separation of purpose and the implementation of least privilege or least function.

Figure 10 illustrates how the VVD management components are logically combined. This includes the physical and virtual networks that support the interconnectedness of the components. The top of the diagram includes Active Directory which provides a foundation of account and access management for the infrastructure. The data center user object represents the payment entity’s administrators, users, and devices that connect to and interface with the infrastructure, applications, and data hosted within the data center. The Internet/Enterprise Network object is representative of the payment entity’s physical servers and other non-end-user devices, which are not part of the virtual infrastructure, and beyond to the Internet. The physical network was characterized in previous sections. On the physical network VLANs are the infrastructure management layer components. Figure 10 shows the two vCenter servers, vRealize Network Insight, NSX Managers for the compute and management pods, the management pods NSX controllers, and vRealize Identity Management. These components sit on VLAN 1911 along with the ESXi hosts VMkernel network interfaces. The VMware NSX Edge Services Gateways supply a universal transit network for the software-defined network. From the universal transit network on VLAN 1916 sits a Universal Distributed Logical Router. Residing on the VXLAN (MgmtRegion01-VXLAN) are the additional service management layer and cloud management layer components, vRealize Operations and vRealize Automation respectively. The collectors for vRealize Operations, vRealize Log Insight and vRealize Automation sit on an additional VXLAN (Mgmt-0RegionA01-VXLAN). The NSX Edge Services Gateways (MGMT-ESG01 and MGMT-ESG02) also provide network load balancing services to the virtual appliances that are setup for performance and redundancy.
Figure 10: SDDC Management and Operations Networked Together
Virtual Infrastructure Layer

The design of the virtual infrastructure includes the software components that make up the virtual infrastructure layer of the SDDC. The components include the hypervisor, virtualization management or control, and pools of resources (memory, processor, network, and storage) to be provided to workloads in the environment. ESXi hosts are separated into three distinct pods to service management, edge, and compute. The compute pod primarily hosts payment entity workloads. The virtualization management is anchored by vCenter. To support improved separation between management and payment entity workloads, two separate vCenter clusters were used to service the management cluster and the payment entity’s compute and edge clusters. Storage resources are delivered for use by the VMs with VMFS volumes served from the VxBlock Storage Area Network (SAN). Network resources are provided to the VMs through the vDS. vDS ports and VM virtual network interface cards (vNICs) are managed by vCenter, while virtual wires are managed by VMware NSX for vSphere. Finally, pools of compute resources are provided by ESXi. Separate resource pools can be configured within vCenter to define unique service levels for VMs. The resource pools allow for resource consumption limits to be placed for the VMs contained therein. Moreover, resource pools can allow for more granular delegation of management control to specified administrator groups in support of separation of duties. The next few sections will cover the components of the SDDC found in Figure 11.

Figure 11: SDDC Conceptual Virtual Infrastructure Layer

vCenter Server Design

Two vCenter Servers provide infrastructure support for the Center of Excellence. These form the basis for Virtualization Control in the SDDC. As part of the VVD design, one vCenter Server has primary responsibility for the management of the infrastructure. The other vCenter Server services the edge and compute or payment entity’s workload cluster(s). The separation of management, compute, and edge clusters onto their own vCenters helps to provide better functional separation for these distinct purposes. Both vCenter Servers are also served by a pair of platform services controllers. A vCenter Single Sign-On Domain provides single sign-on services for authentication to vCenter. The vCenter Single Sign-On domain is connected to a Microsoft Active Directory Domain to provide user and administrator accounts for access to vCenter. Figure 12 depicts the relationship of the components that make up vCenter.
Figure 12: vCenter for the PCI DSS Lab Center of Excellence

Figure 13 illustrates the relationship of vCenter with the ESXi hosts and the clusters they manage.
Table 8 shows the VMs that make up the core management components of the SDDC including the vCenter servers, platform services controllers, and NSX managers.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Application</th>
<th>Cluster</th>
<th>IP Address</th>
<th>vDS</th>
<th>Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt01vc03</td>
<td>vCenter Server (Mgmt)</td>
<td>Management</td>
<td>172.19.11.111</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>mgmt01psc03</td>
<td>Platform Services</td>
<td>Management</td>
<td>172.19.11.112</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>mgmt01nsx01</td>
<td>NSX Manager (Mgmt)</td>
<td>Management</td>
<td>172.19.11.115</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>comp01vc01</td>
<td>vCenter Server (Comp)</td>
<td>Management</td>
<td>172.19.11.113</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>comp01psc01</td>
<td>Platform Services</td>
<td>Management</td>
<td>172.19.11.114</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>comp01nsx01</td>
<td>NSX Manager (Comp &amp; Ed)</td>
<td>Management</td>
<td>172.19.11.116</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>Mgmt01vum01</td>
<td>vSphere Update Manager</td>
<td>Management</td>
<td>172.19.11.103</td>
<td>vDS-PCI-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
</tbody>
</table>

Table 8: Virtualization Infrastructure Management Components in the PCI DSS Center of Excellence

Virtualized Network Design

Figure 14, at a high level, conceptually represents the architecture of VMware NSX for vSphere. This figure shows the functional separation of components representing the three pods of management, edge, and compute. Moreover, it illustrates the placement of NSX components relative to their integration with the separate vCenter instances. While this diagram illustrates the architecture’s extensibility for multi-region deployments, this Center of Excellence was inclusive of a single region (Region A) as noted by naming conventions found throughout diagrams in this document.
VMware NSX for vSphere creates the network virtualization layer. The virtual networks that are created in this layer are an abstraction between the physical and virtual networks. The network virtualization layer is made up of components of vSphere and NSX including vCenter Server, NSX Manager, NSX Controllers, NSX Virtual Switch, and NSX for vSphere API. These components are separated into different planes to create communications boundaries and provide isolation of workload data from system control communication. The applicable design goals for virtual networking in the VMware Validated Design for SDDC include meeting diverse needs, reducing costs, boosting performance, improving availability, supporting security, and enhancing infrastructure functionality.

Some of the networking best practices applied to the design include separation of networking services from one another, the use of network I/O control and traffic shaping, separating network services on a single vDS, separating vMotion traffic, and separating storage traffic.

Separation of different types of traffic onto different VLANs is useful to reduce contention and latency as well as to provide for network access security. Network access security capability helped meet a functional goal of addressing segmentation of resources by security categorization and, further, meeting security and compliance requirements for PCI DSS 3.2. The virtual networks can support multiple functions in the SDDC and the separation of traffic types should be considered respectful of organizational policies, procedures, and standards.

vSphere operational traffic was segmented and defined by management, vMotion, NFS Storage, and VXLAN. VXLAN(s) were used as overlay networks for virtualized assets for additional isolation and obfuscation of the network where appropriate. The following diagrams, Figure 15 through Figure 17, illustrate the placement of port groups on vCenter managed vDS. These port groups are an extension of the network virtualization conceptual design.
of the physical connections illustrated in Figure 6 through Figure 8 in this document. The port groups represent the vDS interfaces for VMkernel connections, virtual machine vNIC, and virtual appliance vNIC connections.

**Figure 15: Compute Cluster vDS VLAN Extension**

**Figure 16: Management Cluster vDS VLAN Extension**
nic0 through nic3 in Figure 15 and Figure 17 represent the physical network cards on each of the compute and edge pod ESXi hosts. Likewise, vmnic2 through vmnic5 represents the physical network cards on each of the management pod ESXi hosts. These NICs are connected to the physical switch ports that are configured as trunk ports. The NICs are combined as uplink ports on the vDS to support throughput and availability. Each VLAN is tagged from the physical switch and identified by the tag on the vDS. Each vDS is distributed to each of the hosts in the cluster. Among other benefits, this ensures configuration consistency of virtual switching throughout the cluster to support High Availability (HA), vMotion, and Distributed Resource Scheduling (DRS). Beyond the vDS sits the logical components of VMware NSX for vSphere to support logical routing, load balancing, logical firewall, distributed routing, distributed firewall, and logical switches.

Figure 18, conceptually, illustrates the relationship between logical components of VMware NSX for vSphere. Logical switches create logically abstract segments to which virtual machines can connect. A single logical switch is mapped to a unique VXLAN segment ID and is distributed across the ESXi hypervisors within a transport zone. The logical switch allows virtual machine vNICs to connect to the network using virtual extensible wires (vxw) on the designated VXLAN.

The universal distributed logical router provides virtual machine to virtual machine, or east-west routing. The NSX Edge Service Gateway provides north-south connectivity by peering with upstream ToR or leaf switches which allows virtual machines to access physical corporate networks and public networks. The logical firewall provides dynamic security capability for the virtual data center. The edge gateway components help to meet perimeter security requirements for the Center of Excellence in support of PCI DSS 3.2 requirements. This perimeter security capability allows for, among other benefits, the creation of DMZs based on IP/VLAN constructs, workload-to-workload isolation such as between CDE and non-CDE zones, or in a multi-tenant environment between service provider tenants. The edge firewall for each relative security zone also provides network address translation.
(NAT), partner (extranet) VPNs, and user supported SSL VPNs. The virtual distributed firewall allows for micro-segmentation for virtual machines and virtual appliances. Micro-segmentation within the virtual distributed firewall can be configured to apply policy for segmentation based on chosen supported criteria such as VM names, VM attributes, VM metadata, and user identity. It can also apply policy based on vCenter objects like virtual data center membership, virtual cluster membership, resource-pool membership, and host. Policy can also be established using traditional 5-tuple networking attributes of source and destination IP address, source and destination port number, and protocol.

Table 9 shows the software-defined networking components of NSX Controllers, Edge Services Gateways, Universal Distributed Logical Routers, and Load Balancers present in the SDDC.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX_Controller_579d867d-031d-4bc1-adda-e71dd6017081</td>
<td>172.19.11.123</td>
</tr>
<tr>
<td>NSX_Controller_b17b0c18-104a-4d6d-9189-64ab792d07a76</td>
<td>172.19.11.122</td>
</tr>
<tr>
<td>NSX_Controller_7227e9-4d10-453c-a994-1ba0477ac271</td>
<td>172.19.11.121</td>
</tr>
<tr>
<td>PCI-MGMT-ESG01-0</td>
<td>172.19.18.11, 192.168.10.1, 172.19.17.11</td>
</tr>
<tr>
<td>PCI-MGMT-ESG02-0</td>
<td>172.19.20.11, 192.168.100.1, 192.168.110.1, 172.19.19.11</td>
</tr>
<tr>
<td>edge-b1e54948-b403-4279-8331-96fe8cc26d7b-0-UDLR01-MGMT</td>
<td>192.168.11.1, 192.168.31.1, 192.168.10.4, 169.254.1.5</td>
</tr>
<tr>
<td>edge-b1e54948-b403-4279-8331-96fe8cc26d7b-1-UDLR01-MGMT</td>
<td>192.168.11.1, 192.168.31.1, 192.168.10.4, 169.254.1.6</td>
</tr>
<tr>
<td>edge-6d20db72-bcc4-4a15-8a51-800440d8031e-0-UDLR01-EDGE</td>
<td>192.168.100.4, 169.254.1.1</td>
</tr>
<tr>
<td>edge-6d20db72-bcc4-4a15-8a51-800440d8031e-1-UDLR01-EDGE</td>
<td>192.168.100.4, 169.254.1.2</td>
</tr>
<tr>
<td>NSX_Controller_3ed8338e-507c-4e03-8865-dec81e9d7374</td>
<td>172.19.11.127</td>
</tr>
<tr>
<td>NSX_Controller_689799b5-e815-4a14-b0f1-c5b07661362</td>
<td>172.19.11.125</td>
</tr>
<tr>
<td>NSX_Controller_e4c74d0-d357-46dd-895f-6e269e38e7e</td>
<td>172.19.11.127</td>
</tr>
<tr>
<td>PCI-MGMT-LB01-1</td>
<td>192.168.11.1, 169.254.1.2, 192.168.11.22, 192.168.11.24, 192.168.11.25, 192.168.11.27, 192.168.11.26</td>
</tr>
</tbody>
</table>

Table 9: Software-Defined Network Components
In addition to providing network segmentation for the payment entity’s workloads, these virtual network constructs were used in this Center of Excellence, with respect to the VMware Validated Design for vSphere SDDC, to provide segmentation and security for some of the operational and cloud management components of the environment. This includes vSphere Operations Management, vSphere Log Insight, as well as the cloud management and consumption components of vRealize Automation. The following sections and corresponding diagrams represent the architectural, logical, and network design for operations infrastructure and cloud management platform.

**Operations Infrastructure Design**

The remainder of the SDDC conceptual design is represented in this section. These include the service management layer, business continuity layer, and partially the security layer (See Figure 19).
Operations Management is a required element of a SDDC. Infrastructure monitoring operations are supported by vRealize Operations Manager, vRealize Log Insight, and vRealize Network Insight. These components provide capabilities for performance and capacity management for related infrastructure and cloud management components. The VMware Validated Design for SDDC also includes vSphere Data Protection. vSphere Data Protection is primarily used for backup and restore for the management components in the environment to support ongoing operation of the SDDC. To support disaster recovery (DR) in the SDDC, the VMware Validated Design provides protection of vRealize Operations Manager and vRealize Automation by using VMware Site Recovery Manager and VMware vSphere Replication. When failing over to a recovery region, these management applications continue the delivery of operations management, and cloud platform management functionality.

**vRealize Log Insight**

vRealize Log Insight provides a log-management solution for the infrastructure to allow for the ingestion and analysis of logs from various infrastructure components. vRealize Log Insight also includes capability, through content packs, to ingest and digest logs from other sources in the environment, including organizational workloads, to provide a comprehensive analysis capability to identify threats and issues present in the environment. Figure 20 illustrates the architecture of vRealize Log Insight.
Figure 20: vRealize Log Insight Architecture

Figure 21 is a focused view of vRealize Log Insight networking design. To provide context, this illustration is an abstraction from Figure 10.
Figure 22 represents the logical connection of vRealize Log Insight to the components of the infrastructure it serves as well as the storage that supports it.

**Figure 22: Logical Connectivity for vRealize Log Insight**

**vRealize Operations**

vRealize Log Insight and vRealize Operations work together to provide shared visibility into both performance and event-driven analytics to provide greater understanding of the proper function and security of the infrastructure. Where security-driven events impact performance of the systems, vRealize Operations may be used to visually identify the impact by helping to see variations in performance or operations that are out of the ordinary. Figure 23 illustrates the logical connectivity of vRealize Operations in the environment in support of local and remote locations that may serve the organization.
Figure 23: vRealize Operations Logical Design

Figure 24 illustrates an abstract from Figure 10: SDDC Management and Operations Networked Together, specifically showing the vRealize Operations network connectivity and the connection of these components into the Universal Distributed Logical Router, UDLR01. vRealize Operations is served by the Edge Service Gateway instance MGMT-ESG01 and MGMT-ESG02 providing load-balancing services for redundant components of vRealize Operations.

Figure 24: vRealize Operations Network Design
vRealize Network Insight

vRealize Network Insight provides visibility to the network configuration. It includes topology overviews of the currently running network with the ability to visibly identify the flow of information between network endpoints. VMware Network Insight helps network and security administrators to optimize network performance and availability through analytics across virtual and physical networks. The visibility to the network helps security administrators plan and make recommendations for implementing micro-segmentation. Built-in net flow assessment and analysis helps administrators model security groups and firewall rules. On an ongoing basis, vRealize Network Insight can help identify gaps in security compliance postures and quickly address these gaps to improve security. vRealize Network Insight provides an enhanced view of logged network events, including best practice remediation recommendations. Figure 25 illustrates the architecture of vRealize Network Insight including connections to the elements from which it collects and analyzes data. It also illustrates how, using additional proxies and platform servers, it can scale to support greater availability and performance for vRealize Network Insight.

Figure 25: vRealize Network Insight Architecture

Figure 26 is an abstract from Figure 10 and shows more detail relative to the network location of the vRealize Network Insight components.
Table 10 is a listing of the virtual machines that represent the operations management components of the infrastructure.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Application</th>
<th>Cluster</th>
<th>IP Address</th>
<th>vDS</th>
<th>Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrops-mstm-01</td>
<td>vRealize Operations Manager - Master Node</td>
<td>Management</td>
<td>192.168.11.28</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrops-repl-02</td>
<td>vRealize Operations Manager - Replica Node</td>
<td>Management</td>
<td>192.168.11.29</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrops-datan-03</td>
<td>vRealize Operations Manager - Data Node</td>
<td>Management</td>
<td>192.168.11.30</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrops-datan-04</td>
<td>vRealize Operations Manager - Data Node</td>
<td>Management</td>
<td>192.168.11.31</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrops-rmtcol-01</td>
<td>vRealize Operations Manager - Remote Collector</td>
<td>Management</td>
<td>192.168.31.17</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-1-sid-300000-Mgmt-Region01-VXLAN</td>
</tr>
<tr>
<td>vrops-rmtcol-02</td>
<td>vRealize Operations Manager - Remote Collector</td>
<td>Management</td>
<td>192.168.31.18</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-1-sid-300000-Mgmt-Region01-VXLAN</td>
</tr>
<tr>
<td>vli-mstr-01</td>
<td>vRealize Log Insight - Master Node</td>
<td>Management</td>
<td>192.168.31.11, 192.168.31.10</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-1-sid-300000-Mgmt-Region01-VXLAN</td>
</tr>
<tr>
<td>vli-wkr-01</td>
<td>vRealize Log Insight - Worker Node</td>
<td>Management</td>
<td>192.168.31.12</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-1-sid-300000-Mgmt-Region01-VXLAN</td>
</tr>
<tr>
<td>vli-wkr-02</td>
<td>vRealize Log Insight - Worker Node</td>
<td>Management</td>
<td>192.168.31.13</td>
<td>vDS-Mgmt01</td>
<td>vwx-dvs-52-universalwire-1-sid-300000-Mgmt-Region01-VXLAN</td>
</tr>
<tr>
<td>vrniproxy</td>
<td>vRealize Network Insight - Proxy</td>
<td>Management</td>
<td>172.19.11.119</td>
<td>vDS-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
<tr>
<td>vrniplat</td>
<td>vRealize Network Insight - Platform</td>
<td>Management</td>
<td>172.19.11.117</td>
<td>vDS-Mgmt01</td>
<td>vDS-Mgmt01-Management</td>
</tr>
</tbody>
</table>

Table 10: Operations Management Virtual Machines
Cloud Management Platform Design

The Cloud Management Platform (CMP) layer, Figure 27, includes the service catalog, self-service portal, and orchestration engine. The service catalog houses the facilities to be deployed. Orchestration provides the workflows to get the catalog items deployed. The self-service portal empowers the end users to take full advantage of the SDDC. vRealize Automation provides the portal and catalog of services from which a subscriber can deploy and manage. vRealize Orchestrator allows for the orchestration of automated workflows for the creation of new service catalog items that can be made available in the portal.

These components establish tenant or organization departmental self-service and further simplify deployment and management of workloads to the requestor, thus increasing service delivery capability for the organization. Services from the service catalog may be able to be orchestrated to automatically include technical security controls such as distributed firewalls, distributed routers, network creation or placement, and role-based access controls necessary to support an entity’s security and compliance objectives. Table 11 provides a listing of virtual machines that make up the cloud-management platform that support organizational tenant self-service for the deployment and management of workloads.

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Application</th>
<th>Cluster</th>
<th>IP Address</th>
<th>vDS</th>
<th>Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra01svr01a</td>
<td>vRealize Automation Appliance #1</td>
<td>Management</td>
<td>192.168.11.12</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01svr01b</td>
<td>vRealize Automation Appliance #2</td>
<td>Management</td>
<td>192.168.11.13</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01iws01a</td>
<td>vRealize Automation Web Server #1</td>
<td>Management</td>
<td>192.168.11.14</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01iws01b</td>
<td>vRealize Automation Web Server #2</td>
<td>Management</td>
<td>192.168.11.15</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01ims01a</td>
<td>vRealize Automation Manager Server #1</td>
<td>Management</td>
<td>192.168.11.16</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrabc01</td>
<td></td>
<td>Management</td>
<td>192.168.31.16</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vrabus01</td>
<td></td>
<td>Management</td>
<td>192.168.11.23</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01ims01b</td>
<td>vRealize Automation Manager Server #2</td>
<td>Management</td>
<td>192.168.11.17</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
</tbody>
</table>
wo workloads were chosen to demonstrate

and CDE

security zone is segmented from the other using NSX Edge Services Gateways

Figure isolating the CDE from the non controls.

transmission non the compute cluster in the compute pod of the SDDC. The workloads represented

application, and database

Each capabilities of NSX for vSphere were applied to

payment entity’s workloads

infrastructure

This section discusses these workloads and how the security

workloads it serves

Controls can be orchestrated and built into a

workloads it serves

virtually network ports and bandwidth

All of this is designed to support the organization or tenant workload, where a tenant is a consumer

of the cloud pool of resource presented by the previously described infrastructure. VMware NSX for

vSphere goes beyond providing networking resources regarding virtual network ports and bandwidth

to the workloads, but also includes capability to meet security and compliance requirements for the

payment entity workloads it serves. Controls can be orchestrated and built into a service from the
catalog. Controls that can be deployed automatically with the service may include network security

standards, applicable firewall policies, security tagging, appropriate network alignment, access

controls, naming conventions, and more.

**Organization Workload Architecture**

The notional payment entity’s workloads were layered onto the previously described SDDC

infrastructure. The workloads made use of compute, network, and storage resources provided by the

compute pod. VMware NSX for vSphere was utilized to provide security and segmentation for the

payment entity’s workloads. This section discusses these workloads and how the security

capabilities of NSX for vSphere were applied to meet some of the requirements of PCI DSS 3.2.

Each workload was represented by a system composed of three distinct tiers including web, application, and database. For this compliance capability assessment, two workloads were setup on the compute cluster in the compute pod of the SDDC. The workloads represented both CDE and non-CDE (general purpose) security zones. A three-tier system was used to demonstrate untrusted to DMZ, DMZ to internal application server, and application server to database server transmission controls. The two workloads were chosen to demonstrate network segmentation capabilities for isolating the CDE from the non-CDE zones.

Figure 28 shows an overview of the logical network that supports the workloads. Each trusted

security zone is segmented from the other using NSX Edge Services Gateways NON-CDE-EDGE

and CDE-EDGE to represent non-CDE and CDE zones respectively. The NSX distributed logical

<table>
<thead>
<tr>
<th>VM Name</th>
<th>Application</th>
<th>Cluster</th>
<th>IP Address</th>
<th>vDS</th>
<th>Port Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>vra01dem01</td>
<td>vRealize Automation DEM Worker / Agent #1</td>
<td>Management</td>
<td>192.168.11.18</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01dem02</td>
<td>vRealize Automation DEM Worker / Agent #2</td>
<td>Management</td>
<td>192.168.11.19</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01ias01</td>
<td>vRealize Automation Proxy Agent #1</td>
<td>Management</td>
<td>192.168.31.14</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-1-sid-30000-Mgmt-RegionA01-VXLAN</td>
</tr>
<tr>
<td>vra01ias02</td>
<td>vRealize Automation Proxy Agent #2</td>
<td>Management</td>
<td>192.168.31.15</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-1-sid-30000-Mgmt-RegionA01-VXLAN</td>
</tr>
<tr>
<td>vra01sql01</td>
<td>Microsoft SQL Server 2012 (vRA Agent)</td>
<td>Management</td>
<td>172.19.11.18</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-50-universalwire-4-sid-30003-Mgmt-RegionA01-VXLAN</td>
</tr>
<tr>
<td>vra01vro01a</td>
<td>vRealize Orchestrator (Execution)</td>
<td>Management</td>
<td>192.168.11.20</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
<tr>
<td>vra01vro01b</td>
<td>vRealize Orchestrator (Execution)</td>
<td>Management</td>
<td>192.168.11.21</td>
<td>vDS-Mgmt01</td>
<td>vxw-dvs-52-universalwire-2-sid-30001-Mgmt-xRegion01-VXLAN</td>
</tr>
</tbody>
</table>

Table 11: Cloud-Management Virtual Machines
router provided additional segmentation for each tier of the system. Finally, the distributed firewall was applied through NSX Server Composer to provide micro-segmentation between VMs in each segment (web, application, and database) with rules to prevent communications between the VMs east and west on that segment. Load balancing for the web and application tiers was provided by the Edge Services Gateway Load Balancing service. The networks of the CDE and non-CDE environment were obfuscated from each other using distinct VXLANs for each where NAT was used to limit private network discovery.

**CDE / NON-CDE workload**

Figure 28: Workload Logical Network Overview

Figure 29 details one of the security zones (CDE) with more specificity with how the segmentation was provided as well as supporting connectivity for outside services such Active Directory, NTP, DHCP, DNS, certificate services, monitoring, and management from various type 2 systems. This diagram shows the relationship between the distributed logical router and the NSX Edge Services Gateway to provide services for the CDE zone. It also illustrates the connectivity from the CDE zone north bound to the corporate network and external networks through the Edge01 and Edge02 Edge Services Gateways as may be allowed or restricted by policy.

Firewall rules from the edge firewall at Edge01 and Edge02 as well as the PCIDSS01-EDGE01 and EDGE02 provide security services to dictate the flow of information from outside the security zone and within the security zone respectively.
Figure 29: CDE Logical Network Detail

Figure 30 illustrates the flow of user connectivity to an application within the secure CDE zone, where UserA is accessing from outside of the CDE01-3Tier-Apps-Transit. UserA connects to the web client hosted in the web tier. Load balancing to the web client is provided by the Edge Services Gateway. UserA never has direct access to the application or database tier. Web services on the web server can communicate to the application tier as necessary to support the function of the application. Likewise, the application tier can communicate with the database tier through approved ports, protocols, and specified IP addresses. Communication between each tier in the application is provided through the distributed logical router CCRS-CDE01-DLR01 which is distributed by CCRS-CDE01-EDGE01. The Edge Firewall at CCRS-CDE-EDGE01 contains the rules dictating communication between tiers in the application.
Additional control can be provided by setting, policy, specific source IP addresses, IP pools, subnet, or VLAN for access to the payment application front end depending on the organization's specific requirements. Additional considerations and security control capabilities should be applied for ecommerce sites to provide advanced security protection for the CDE. These additional controls could be provided using third-party and partner-integrated solutions inserted in the communication chain through the NSX Service Composer. These advanced security solutions include IDS/IPS, layer 4–7 application firewalls, web proxy servers, and so forth.

Figure 31 illustrates the firewall policy within NSX for providing the connections between segments of one of the three-tiered payment applications.
### VVD VMware Software Components in the Validated Design for SDDC 3.0

Table 12 provides a list of products and their respective versions that were used to build the PCI Center of Excellence. Please confirm functionality of the product or solution where more current versions are available.

<table>
<thead>
<tr>
<th>Product Group and Edition</th>
<th>Product Name</th>
<th>Product Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vSphere Enterprise Plus</td>
<td>ESXi</td>
<td>6.0 Update 2</td>
</tr>
<tr>
<td></td>
<td>vCenter Server Appliance</td>
<td>6.0 Update 2</td>
</tr>
<tr>
<td>VMware Virtual SAN Standard or higher</td>
<td>Virtual SAN</td>
<td></td>
</tr>
<tr>
<td>VMware vSphere Replication</td>
<td>VMware vSphere Replication</td>
<td>6.1.1</td>
</tr>
<tr>
<td>VMware Site Recovery Manager Enterprise</td>
<td>VMware Site Recovery Manager</td>
<td>6.1.1</td>
</tr>
<tr>
<td>VMware NSX for vSphere Enterprise</td>
<td>NSX for vSphere</td>
<td>6.2.4</td>
</tr>
<tr>
<td>VMware vRealize Automation Advanced or higher</td>
<td>vRealize Automation</td>
<td>7.1</td>
</tr>
<tr>
<td></td>
<td>vRealize Orchestrator</td>
<td>7.1</td>
</tr>
<tr>
<td></td>
<td>vRealize Orchestrator Plug-in for NSX</td>
<td>1.0.4</td>
</tr>
</tbody>
</table>

*Figure 31: Firewall Policy Example for CDE 3-Tier Application*
<table>
<thead>
<tr>
<th>Product Group and Edition</th>
<th>Product Name</th>
<th>Product Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware vRealize Business for Cloud Advanced</td>
<td>vRealize Business for Cloud</td>
<td>7.1</td>
</tr>
<tr>
<td>VMware vRealize Operations Manager Advanced or higher</td>
<td>vRealize Operations Manager</td>
<td>6.3</td>
</tr>
<tr>
<td></td>
<td>vRealize Operations Management Pack for NSX for vSphere</td>
<td>3.0.2</td>
</tr>
<tr>
<td></td>
<td>vRealize Operations Management Pack for vRealize Log Insight</td>
<td>1.0.1</td>
</tr>
<tr>
<td></td>
<td>vRealize Operations Management Pack for vRealize Automation</td>
<td>2.1</td>
</tr>
<tr>
<td></td>
<td>vRealize Operations Management Pack for Storage Devices</td>
<td>6.0.4</td>
</tr>
<tr>
<td>VMware vRealize Log Insight</td>
<td>vRealize Log Insight</td>
<td>3.6</td>
</tr>
<tr>
<td></td>
<td>vRealize Log Insight Content Pack for NSX for vSphere</td>
<td>3.5</td>
</tr>
<tr>
<td></td>
<td>vRealize Log Insight Content Pack for Virtual SAN</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>vRealize Log Insight Content Pack for vRealize Automation 7</td>
<td>1.0</td>
</tr>
<tr>
<td></td>
<td>vRealize Log Insight Content Pack for vRealize Orchestrator 7.0.1+</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td>vRealize Log Insight Content Pack for vRealize Operations Manager 6.x</td>
<td>1.7</td>
</tr>
<tr>
<td>VMware vSphere Data Protection</td>
<td>vSphere Data Protection</td>
<td>6.1.2</td>
</tr>
</tbody>
</table>

Table 12: SDDC BoM

Validation Scope and Approach

This validation effort built upon the concepts of compliance capability discussed in the VMware SDDC and EUC PCI DSS 3.2 Product Applicability Guide. Specific use cases were selected to narrow down the scope for this validation engagement. VMware chose to showcase capabilities that may be meaningful to payment entities requiring to be compliant with PCI DSS 3.2. This compliance-capable solutions engagement was limited to the two defined use cases found in the section titled Implementing PCI DSS 3.2: Use Case Examples.

Coalfire considered PCI DSS 3.2 requirement citations for each requirement family included in scope for this assessment. Control determination, examination, tests, and interviews were tailored for this type of vendor solution assessment. For control statements that include organizationally defined variables relative to methods for satisfying the objective, Coalfire endeavored to identify the configuration-capable options available from the technology solution. In many cases, more than one possible option may be available to satisfy the control objective.

Some of the requirements can only be achieved through organizational establishment of policy, procedures, and standards. The test procedures for these requirements involve evaluation of the completeness of these policies, procedures, and standards. Additionally, the testing procedures may include interviews of personnel to determine the level of knowledge and understanding of the same policies and procedures. Because we are not evaluating an actual payments entity, these requirements are not included for this assessment; however, some design considerations and capabilities of the solution may lend support to the establishment and implementation of a standard to meet the requirement. In this case, Coalfire outlines in the findings the technical design
considerations and tested the capability of the solution to produce an outcome specified in the consideration.

Technical design considerations and control decisions found in the following sections are indicative of one example for deployment as defined for the as-built lab environment. This does not exclude other possible design considerations and technical control determinations that may be defined in other deployments of the software-defined data center.

“Additional Consideration” found in the following sections provides thoughtful opinion for additional design consideration that may be applicable to a deployment of the SDDC in support of PCI DSS 3.2 regulated environments.

The testing was performed against a lab environment, hosted in a VMware Center of Excellence, that was built in alignment with the VMware Validated Design for SDDC. Beyond the VVD for SDDC, additional configuration was made to purposefully demonstrate the usefulness of the solution for supporting a payment entity’s workloads. It is also understood that each payment entity must consider, for alignment with its own GRC program, its own organizational policies, procedures, organizational controls, management structure, risk assessment, and technical controls that are pertinent to their mission and environment.

In general, and for each selected test, Coalfire performed the following activities:

1. **Interview:**
   a. Subject matter experts on demonstrated technology capabilities specific to control objectives;
   b. Subject matter experts, architects, and designers of the test lab.

2. **Examine:**
   a. Overall information system design documentation to gain understanding of baseline configuration as part of best practices implementation for foundational components of the test lab.
   b. Information system configuration settings specific to each control decision and associated component configuration documentation to gain understanding of specific configuration settings designed to meet control objectives relative to the PCI DSS 3.2 requirements.
   c. Event and audit logs as a demonstration of activity results supporting control objectives.

3. **Selective Test**
   a. Demonstrate effectiveness of control in place.

Finally, the overall architecture and design of the solution was evaluated for effectiveness in supporting organizational operations in a secure manner.

---

1 Not all controls were tested; tests that were performed were selected to include a specific subset of the controls and to demonstrate specific product capabilities. Some controls capabilities were determined through examination of configuration settings.
Findings and Observations

The PCI DSS 3.2 requirements were chosen based on alignment with the specified use cases. Only requirements that aligned with VMware’s technical capability to address were included in the following narrative. The reader can assume that requirement topics not included in the following narrative are addressable by other means such as payment entity’s documented policies, procedures, standards, other documentation, or technical control implemented by a third party solution not discussed in this paper. The following are the tested objectives and requirements including technical design considerations for the VMware solution, resulting findings, and additional considerations.

Objective: Segmentation

Implement network segmentation to isolate CDE from non-CDE with the goal of achieving reduction in assessment scope with removal of non-CDE assets from scope.

Technical Design Consideration: For the payment entity’s workloads, isolate CDE from non-CDE (general purpose) workloads utilizing software-defined networking mechanisms. Implement distributed virtual routers for network segmentation of CDE onto separate VLAN or VXLAN from non-CDE workloads. Implement virtual distributed firewalls with rules to prevent communication between non-CDE and CDE segments of the environment. Limit access to the CDE for monitoring and administration to only that which is necessary to support regular operational support and awareness. Physically separate CDE and non-CDE workloads onto separate ESXi hosts using vSphere Distributed Resource Scheduling (DRS) affinity rules. For administration and organization purposes, in support of divisions of responsibility, separate CDE and non-CDE into different cluster resource pools and virtual machine folders with explicit permissions placed on each for access and administration.

Findings: It was determined that software-defined network elements of VMware NSX for vSphere sufficiently support segmentation of the virtualized CDE components from non-CDE components. Network transport was not permitted to occur across NSX for vSphere established boundaries. The implemented segmentation, as characterized in the design sections of this document, prohibited transmissions of data to and from the CDE from and to the designated non-CDE segment and assets therein. To further physically segment CDE from non-CDE, the lab environment used DRS affinity rules to separate CDE virtual machines and non-CDE virtual machines onto different cluster hosts.

Additional Consideration: The decision to provide physical separation of CDE and non-CDE virtual machines onto separate hosts using DRS affinity rules was based on guidance from the PCI SSC Special Interest Group (SIG) 2011 publication on virtualization titled PCI DSS Virtualization Guidelines. This guidance paper states, “It is strongly recommended (and a basic security principle) that VMs of different security levels are not hosted on the same hypervisor or physical host; the primary concern being that a VM with lower security requirements will have lesser security controls, and could be used to launch an attack or provide access to more sensitive VMs on the same system.” (PCI Security Standards Council, 2011) Payment entities have historically followed the SIG guidance using several design considerations up to and including separating CDE from non-CDE onto separate workload clusters.

The strong recommendation for this guidance is partially drawn from the conclusion that, “The risk of mixing sensitive data with data of lower trust must be carefully assessed.” (PCI Security Standards Council, 2011) Though PCI DSS 3.2 is predominately considered a prescriptive framework for control and not strictly a risk-based framework of requirements, this SIG guidance seems to provide...
some flexibility for payment entities to evaluate the risk of mixing virtual machines of differing trust levels on the same host and to apply their own standard based on that evaluation of risk.

Segmentation using physical methods may be translatable to virtual environments depending on the technology architecture being used. Starting at the kernel level, vSphere is designed to abstract the virtual plane from the hardware plane, including CPU, memory, network, storage, and other hardware devices of which the virtual environment makes use.

There are many variables that factor into reducing risk and concluding the vSphere ESXi host as a trusted host capable of maintaining workload isolation and the security of the host at the kernel. VMware has published a document, most recently updated January 2014, titled, “Security of the VMware vSphere Hypervisor.” This document outlines built-in security design elements of the vSphere Hypervisor and discusses, in depth, the secure virtual machine isolation in virtualization through virtual extensions, instruction isolation, memory isolation, memory protection, device isolation, resource provisioning, shares, and limits. Beyond this, the paper discusses the built-in network isolation for virtual machine networks as well as VMkernel networking. Also, included in the document are design elements of the vSphere hypervisor for the protection of virtualized storage. Finally, the document outlines the built-in security and configurability of the vSphere hypervisor to provide secure management of the host. As with any system in a regulated environment, it is important that the implementation of technology be secured as much as is possible following recommended hardening and best practices for use of the technology. Secure software packaging, software assurance and integrity protection, and VMware’s software development lifecycle practices all support the trustworthiness of the vSphere hypervisor.

The reader of this and other VMware white papers that outline the effectiveness of security and compliance capability of the VMware solutions presented in this paper must make their own judgement and apply this knowledge in a manner that satisfies their requirements. Having stated this, it is Coalfire’s opinion that there appears to be sufficient isolation for virtual machines on the vSphere hypervisor to support the hosting of workloads of differing trust levels on the same vSphere hypervisor.

While built-in capabilities support the vSphere hypervisor as a trusted host, additional layered-on capabilities from VMware solutions and their solution partners may support additional risk reduction. These include the use of software-defined networking capabilities of VMware NSX for vSphere, the use of log collection and analysis tools, strong identification, authentication and authorization, and other security technologies and principles.

Objective: Build and Maintain a Secure Network and Systems

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

(1.1) “Establish and implement firewall and router configuration standards that include the following.” (PCI SSC, 2016)

Technical Design Consideration: VMware’s intention is to demonstrate how visibility to the network through vRealize Network Insight may provide improved comprehension of the network including identification of network components, visibility and understanding of secure traffic flows, ingress and egress traffic flows, clarification on the use of ports, services, and protocols between endpoints, and so forth. The network visibility provided by vRealize Network Insight could allow for the discovery of present elements of the network including, but not limited to, Internet connections, DMZs, and untrusted network connection points. Moreover, this level of visibility could provide insights to support
the payment entity’s decision-making processes when establishing firewall and router configuration standards in support of securing critical data.

Determine if vRealize Network Insight can provide visibility of the network topology and flow of information through the topology. Determine if vRealize Network Insight helps to identify potential risks and gaps in policy coverage including exposure of possible attack vectors representing increased risk to sensitive application and data. Determine if vRealize Network Insight can help identify policy violations for which standards may need to be improved. Determine if vRealize Network Insight can illustrate network choke points for establishing higher security inspection for the addition of advanced security services insertion.

**Findings:** The testing performed for this assessment was not against an actual payment entity. For this reason, Coalfire did not examine firewall and router configuration standards that would have been documented and implemented by a payment entity. Rather, Coalfire assessed the capability of VMware vRealize Network Insight to provide visibility to an existing network. Furthermore, Coalfire concluded that the information available through the user interfaces and dashboards of vRealize Network Insight may be useful in support of the development of a payment entity’s configuration standards. Additionally, these insights may also be useful for determining whether router and firewall configuration standards have been implemented in a manner that supports the entity’s standards.

vRealize Network Insight could provide visibility of the network which included visibility of existing network routes, location of network devices including network firewalls, and connectivity between networks endpoints. vRealize Network Insights could show, through built-in graphic representation, the unidirectional or bi-directional connection from a network asset to other network assets. It further can show the services, ports, and protocols that are in use for each discovered asset. vRealize Network Insight could also be useful for identifying virtual machines that could benefit from micro-segmentation.

**Summary Result:** Supports Design Objective

(1.1.1) “Establish and implement firewall and router configurations standards that include the following: a formal process for approving and testing all network connections and changes to the firewall and router configurations” (PCI SSC, 2016)

**Technical Design Considerations:** VMware’s intention is to demonstrate the capability of vRealize Network Insight to provide network visibility to firewall and router configuration changes that may allow the entity to review and understand how the change may have impacted the operation and security of the business systems that the network supports. Within the payment entity’s test environment, this insight may facilitate the review processes relative to the testing of connections and changes to the firewall and routers and to identify misconfigurations that may represent policy violations. The payment entity’s review of network changes recorded and reflected in vRealize Network Insight may assist the organization in identifying unauthorized changes and to respond accordingly.

**Findings:** For this requirement, the payment entity must establish and implement firewall and router configuration standards that include a formal process for approving and testing all network connections. Because this assessment did not include the evaluation of an actual payment entity, firewall and router configuration standards were not examined. For the payment entity making changes in a test environment, vRealize Network Insight could be used to help the entity evaluate and review a change’s impact prior to deployment to the production environment.
It was also identified that the logs of changes to network configuration in vRealize Network Insight could be useful for gaining improved visibility to changes that occur on the network. This could be useful for identifying changes that occur outside the payment entity’s change processes. Moreover, this record of changes could be useful for troubleshooting and correcting issues that may occur after network configuration changes are executed.

**Summary Result:** Supports VMware’s Design Objective

1.1.2 “Establish and implement firewall and router configuration standards that include the following: current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The payment entity creates network diagrams to represent the baseline of network configuration. This baseline includes representation of location and purpose of networked devices. The diagram identifies all connections between the CDE and other networks, including any wireless networks. As part of the payment entity’s standards maintenance, the organization must keep diagrams updated with respect to ongoing changes to the network.

VMware’s intention is to illustrate how vRealize Network Insight could be used to identify variances in the current running network from covered-entity created and documented network diagrams. These variances could represent baseline configuration drift from the organization’s creation of baseline documentation and diagrams.

**Findings:** For the tested environment, VMware setup two distinct workloads to be hosted on the SDDC infrastructure. One workload represented a non-CDE or general purpose system including web, application, and database tiers. The other workload represented a CDE system and included a web, application, and database tier. For each of the CDE and non-CDE systems, the tiers included one or more virtual machines that performed the role of the tier. Each of these workloads made use of software-defined networking constructs of VMware NSX. VMware NSX supplied the virtualized network components to support the proper function of the application including routing, switching, and load balancing. Further, NSX provided security features and functions to support network controls for the workload including virtual overlay networks and distributed firewalls. These NSX elements provided the capability to support network access control, segmentation, and micro-segmentation for the workloads. Coalfire examined diagram(s) provided by VMware for the validation lab and observed network configurations to verify that a current network diagram exists and that it documents all connections to and from the notional cardholder data represented in the described notional CDE. Please note that wireless networks were not included in the design of the test lab and, therefore, not part of this validation exercise.

Coalfire observed that vRealize Network Insight could support substantiation of the VMware provided design documentation (network topology and network flow diagrams). The network topology and flow information available from vRealize Network Insight could be useful for identifying the present network connection points and location of network devices as part of the CDE.

The payment entity should create and maintain its own network topology and flow diagrams. vRealize Network Insight should only be used to identify variances between the designed network and the implemented network. Where variances might occur, the payment entity could determine if approved changes are in alignment with the variances or if the variance represents a violation of policy or standard.

**Summary Result:** Partially Supports VMware’s Design Objective
(1.1.3) “Establish and implement firewall and router configuration standards that include the following: current diagrams that shows all cardholder data flows across systems and networks” (PCI SSC, 2016)

Technical Design Consideration and Determination: The payment entity’s diagrams must also illustrate the flow of cardholder data across systems and networks. These diagrams are typically created and maintained manually.

Like requirement 1.1.2, determine if vRealize Network Insight can illustrate the flow of data through the network and between endpoints in support of maintaining network flow diagrams. Determine if vRealize Network Insight can highlight specific segments of the network and show the flow of information to and from the devices in these segments including termination points and Internet connections.

Findings: vRealize Network Insight can illustrate the available network flow between discovered network assets. Flow information includes the services, ports, and protocols that are being used for communications to and from virtual machines in the environment. There are several views that can illustrate the flow. One view may illustrate in a list format the current network traffic that is being transmitted to and from a virtual machine on the network. Another view can allow for visible modeling of the traffic from one asset (VM, VXLAN, VLAN) to another asset on the network. This model includes the placement and use of network security devices between the assets that control the flow of communication. This can include illustration of ingress and egress traffic from and to the Internet.

Summary Result: Supports VMware’s Design Objective

(1.1.4) “Establish and implement firewall and router configuration standards that include the following: requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone” (PCI SSC, 2016)

Technical Design Consideration and Determination: For testing purposes, the Center of Excellence should have at least one Internet connection and at least one established DMZ. VMware Edge Services Gateway(s) with virtual firewall and virtual routers should be used to demonstrate the capability to protect the edge of the virtualized network and to establish a DMZ. The Edge Services Gateways should be placed at or near the boundary of the untrusted network and the notional payment entity’s controlled network as possible.

Determine if as-built diagrams and configuration standards for the Center of Excellence PCI DSS 3.2 test lab include standards for the establishment and placement of firewalls at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone(s). Observe the, as-built lab environment and configurations to verify that a firewall is in place at each Internet connection and between any DMZ and the internal network zones, per the documented standards and network diagrams. Determine what firewall rules exist to control communication between the Internet, DMZ, and internal network zones for both inbound and outbound traffic.

Findings: Coalfire examined VMware produced diagrams that illustrated the placement of both CDE and non-CDE workloads on the SDDC infrastructure. Included in the diagrams were the placement of network routers and firewalls used for the protection of the represented workloads. To support the testing of this requirement, the diagrams and the observed implemented solution included the establishment of a DMZ. Coalfire observed that the Edge Services Gateway firewall was placed at the perimeter boundary of the controlled network and the untrusted network. Two DMZs were established where each of the web component(s) of the CDE and non-CDE applications were placed respectively. Firewall rules were put in place to allow public access to the assets in the DMZ over
port 443. A virtual firewall was also placed between the DMZ components of each the CDE and non-CDE that prevented access from the DMZ to the internal trusted network to only that which was necessary to support proper function of the respective application. The firewall rules were explicit on the allow policies to only include the supported service, port, and protocol with a default deny all rule to disallow all other traffic. Moreover, the distributed firewall that was placed at the vNIC of each virtual machine was configured to disallow east-west traffic between virtual machines on the same network segment.

The observed configuration settings and implemented architecture and design of the network were consistent with provided diagrams. Information obtained with vRealize Network Insight was also consistent with provided diagrams.

**Summary Results:** Supports VMware’s Design Objective

(1.1.5) “Establish and implement firewall and router configuration standards that include the following: description of groups, roles, and responsibilities for management of network components” (PCI SSC, 2016)

**Technical Design Considerations and Determination:** The VMware technical solutions should be able to support the payment entity’s establishment of roles and responsibilities. While this requirement is primarily concerned with the payment entity’s establishment of roles and responsibilities and the understanding from the assigned resources as to performance of the required duties, the technology being deployed for the management and control of the network should be able to support those distinct roles and responsibilities as may be defined by the payment entity.

Determine if, in support of organizations establishment of roles and responsibilities, VMware NSX for vSphere, vRealize Network Insight, vRealize Operations, and vCenter provides both built-in and customizable role definition with permitting capability provided necessary to support common roles and responsibilities.

**Findings:** The SDDC, including the software-defined networking components are primarily accessible through and managed from the vCenter Web Client. VMware provides for infrastructure management built-in roles for enabling role-based access controls. Role templates can also be duplicated and modified to create customized roles. Each of the roles can be modified with a level of granularity to define access rights and permissions for actions that can be performed within the environment. The roles within vCenter for the management of the virtual infrastructure and the network can be integrated with the payment entities identity and access management solution such as Microsoft Active Directory.

**Summary Result:** Supports Requirement Objective

(1.1.6) “Establish and implement firewall and router configuration standards that include the following: documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for these protocols considered to be insecure” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** While documentation of business justification and approvals are an administrative duty for the entity, VMware wanted to demonstrate the value of vRealize Network Insight for illustrating the listing of services, protocols, and ports that are permitted on the network and between interconnected devices. The visibility of the network that vRealize Network Insight provides may be valuable to inform the organization and support identification of required ports, protocols, and services for which a business justification must be
made. Moreover, the network visibility that vRealize Network Insight provides can be useful for determining at which managed interfaces additional security features should be applied.

**Findings:** This requirement is primarily administrative in nature, requiring documented business justification and approval for the use of all services, protocols, and ports allowed on the network. Coalfire examined the capability of vRealize Network Insight to support discovery and illustration of services, ports, and protocols in use on the network for each discovered device. These insights could be useful to provide improved understanding of network communication between devices. This insight may be able to aid the organization in determining the necessity to continue allowing the observed communication and document the purpose and authorization. Likewise, the network visibility provided by vRealize Network Insight may be able to be used for ongoing assessment of network communication in support of identifying and addressing policy violations.

**Summary Result:** Supports Design Objective

**(1.1.7)** “Establish and implement firewall and router configuration standards that include the following: requirement to review firewall and router rule sets at least every six months”  (PCI SSC, 2016)

**Technical Design Consideration and Determination:** While this requirement is primarily procedural and administrative, VMware’s intent was to illustrate how VMware NSX and vRealize Network Insight may be able to support firewall and router configuration and ruleset reviews.

Determine how vRealize Network Insight and VMware NSX may be able to support the payment entity’s six-month firewall and router configuration and ruleset review. Determine how the viewable information in VMware NSX and with vRealize Network Insight may be able to support actionable adjustments in network configuration to address misconfiguration, unauthorized changes, and stale configurations. Determine the capability of vRealize Network Insight to produce reviewable ruleset reports.

**Findings:** VMware NSX provides views to the network configuration that support review of the virtual router and firewall configurations. These views show the rulesets that have been established for the virtualized network. Moreover, NSX allows the reviewer to identify to which assets rulesets are applied. The visibility of the configuration in the user interface can be useful where micro-segmentation has been implemented using the virtual distributed firewall. vRealize Network Insight additionally provides dashboards for viewing the network configuration, including firewall and router rulesets and the impact the rulesets have on the ability for devices to communicate over the network. In both cases, role-based access can be established to provide view-only access to reviewers in support of a regular assessment process.

**Summary Result:** Supports VMware’s Design Objective

**(1.2)** “Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.

Note: An “untrusted network” is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity’s ability to control or manage.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** For demonstration purposes, the design of the network in the test lab included a designated CDE. An Internet connection was also implemented for the test lab. An NSX Edge Services Gateway was placed between the untrusted (Internet) connection and the trusted CDE network. The Edge Services Gateway included services such as load balancer, firewall, router, and SSL VPN plus. The CDE was segmented from the rest of the
internal network using a distributed logical router, where virtual overlay networks (VXLANs) were created to host CDE workload elements.

Determine if the firewall and router configurations restrict connections between untrusted networks and trusted networks.

**Findings:** Coalfire observed the firewall and router configurations, reviewed the firewall rulesets, and examined dashboards in vRealize Network Insight. The firewall was configured to explicitly allow traffic from the untrusted network to the DMZ segment of the CDE over port 443. No direct access was provided from the untrusted network to internal components of the CDE on the trusted network. Likewise, outbound traffic to the Internet was restricted from components in the CDE. Bidirectional access was tested to determine the efficacy of firewall rules to restrict access and Coalfire determined that the in-place firewall and router rules restricted connections between the untrusted network and the trusted network by design.

**Summary Result:** Supports Requirement Objective

(1.2.1) “Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** For this assessment, standards were set to designate which devices in the CDE should allow either or both inbound and outbound connections. The standards included designations for inbound and outbound connections to and from non-CDE elements as well as the Internet. The standard specified that all outbound connections to the Internet or non-CDE initiated from the CDE were to be denied by default. No exception was made to allow for outbound communications. Rules for inbound connections were set to allow only port 443 Https traffic to the designated CDE DMZ web server(s).

Determine that firewall rulesets include an enabled default rule to deny all traffic. Rules and rulesets above this default rule are exceptions and are specifically designed per the identified standard to support a required business function. Determine that the firewall and router configuration limits inbound and outbound traffic to only that which is necessary to properly support a function of the CDE or applications in the CDE.

**Findings:** For this assessment, a notional payment application was established in the CDE with a web (e-commerce), application, and database tier. Each tier of the payment application was segmented onto its own network segment with a virtual logical router. An NSX virtual distributed firewall was distributed to each virtual machine in the CDE. Firewall rulesets explicitly denied all inbound and outbound traffic to and from the CDE. An exception rule allowed port 443 traffic from any address to the DMZ-hosted web component of the payment application. No connection from outside the CDE or from the untrusted network(s) was permitted to the internal components of the payment application. The firewall rules included a rule to allow specific access from the web server in the DMZ to the application server(s) in the application server segment over specific service, port, and protocol assignments. Firewall rules included rules to only allow access to the database element of the payment application from the application server(s) in the application segment. Furthermore, access to the web servers were provided through the Edge Service Gateway load balancers. Rules to permit access pointed to the IP address of the load balancer, which would then direct, based on load, to the appropriate web server.

**Summary Result:** Supports Requirement Objective

(1.2.2) “Secure and synchronize router configuration files.” (PCI SSC, 2016)
**Technical Design Consideration and Determination:** The use of NSX for vSphere includes capabilities to ensure that all router and firewall configurations pertaining to edge gateways and distributed logical routers and firewalls are synchronized and secure. Determine that router configuration is secure and synchronized.

**Findings:** Coalfire examined configuration settings and options and determined that access for configuration can be restricted through role-based access controls. Changes to NSX router or firewall configuration, once saved, is immediately available to the distributed instances of the impacted component and applied to the protected virtual appliance or virtual machine.

**Summary Result:** Supports Requirement Objective

1.3) “Prohibit direct public access between the Internet and any system component in the cardholder data environment.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The NSX Edge Services Gateway with logical edge router and logical edge firewall were placed at the edge of the network, between the core of the entity network and the CDE. An additional NSX Edge Services Gateway was placed between the outside edge and the inside edge of the CDE. The CDE was segmented into web, application, and database network segments using a virtual distributed logical router. A virtual distributed firewall was attached to each virtual machine in the CDE. Direct public access between the Internet and any system component in the CDE was prohibited. Any permitted public access traversed at least one firewall for inspection prior to continued transmission to the web component of the DMZ.

Determine that direct public access between the Internet and any system component in the cardholder data environment was prohibited.

**Findings:** Coalfire reviewed design documents, examined configuration settings, and tested connectivity between the Internet and the elements of the DMZ. Through review of traffic logs and observation of network traffic, it was determined that no direct public access to the CDE was permitted.

**Summary Result:** Supports Requirement Objective

(1.3.1) “Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** VMware established at least one DMZ to host web components of the CDE. An additional DMZ was setup to support non-CDE workloads. Load balancing services were provided by the Edge Service Gateway to proxy and direct traffic to the appropriate DMZ elements of both the CDE and non-CDE environments. Web servers in the DMZ were added to security groups. Rules were applied to the security group and the members thereof which permitted authorized access to the publicly accessible servers. The rules for access specified authorized services, protocols, and ports to be used. No direct access was permitted beyond the DMZ.

Determine that the DMZ network configuration limits access from outside the network to only those specific services, ports, and protocols that are permitted to specific targets within the DMZ. Determine that no direct access is provided through the DMZ to internal elements of the CDE or other in-scope components for P 3.2.

**Findings:** For both CDE and non-CDE environments, Coalfire examined the DMZ configuration and the elements hosted in the DMZ. Coalfire examined rulesets for the DMZ to determine that public
access was limited to specified services, ports, and protocols of listening devices in the DMZ. Coalfire determined that no other access was provided through the DMZ to internal components of the non-CDE or CDE environments. All access to internal elements required programmatic access provided by the application component hosted in the DMZ.

**Summary Result:** Supports Requirement Objective

(1.3.2) “Limit inbound Internet traffic to IP addresses within the DMZ.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** For restriction to access within the DMZ, beyond port, protocol, and service, rules should be established which identify the specific IP address to route inbound Internet traffic to elements hosted in the DMZ.

Determine that the network configuration limits the connectivity from the Internet to specific DMZ components identifiable by IP address. No other access to the DMZ should be allowed.

**Findings:** Coalfire examined the network configuration and determined that direct Internet access to the DMZ was limited to the specified load balancer IP address bound to internal authorized elements of the DMZ. This limited access from the Internet to specific IP addresses specified in the ruleset. Moreover, it was determined that the virtual distributed firewall provided micro-segmentation capabilities to restrict access from one DMZ asset to other adjacent DMZ elements on the same network segment. This helps prevent pivoting from access provided to a single server to gain access to other servers on the same network.

**Summary Result:** Supports Requirement Objective

(1.3.3) “Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** SpoofGuard on VMware NSX should be enabled on the Edge Firewall to prevent attackers from using forged IP addresses to access the network. SpoofGuard should likely be able to prevent spoofing or forging of IP addresses from one network segment to another to provide additional enhanced security from insider attacks.

Determine that SpoofGuard is enabled and preventing the use of forged or spoofed IP addresses.

**Findings:** The configuration was examined and it was determined that SpoofGuard was enabled on NSX. SpoofGuard utilizes information it gathers about elements on the network to tie designated IP addresses to MAC addresses of the virtual machines in each of the networks. This prevents someone from forging an internal IP address and gaining access to a network from outside the same network. The forged IP address will be identified as foreign and the traffic will be denied by the NSX firewall.

**Summary Result:** Supports Requirement Objective

(1.3.4) “Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The network should be setup to prohibit outbound traffic from the CDE to the Internet for both DMZ and internal CDE segments.

Determine that the firewall and router, as configured at the Edge Services Gateway: logical firewall and router, distributed logical router, and distributed firewall prevent traffic outbound from the CDE to the Internet. Determine that authorized connections to the Internet can be filtered and established
to permit connections using 5-tuple rulesets restricted by source and destination IP addresses, source and destination ports, protocols, or blocking of content.

**Findings:** Coalfire examined the configuration capabilities as well as configurations specific to the notional CDE environment established for lab testing to identify restrictions that can be applied to prevent outbound access to the Internet. Coalfire determined that configuration is possible to prohibit outbound connections to the Internet but allow, where authorized, Internet connections specified by source and destination IP addresses, ports, and protocols. NSX is limited in ability to inspect traffic based on content; however, NSX has built-in capability to support service insertion from third-party security solution for deeper Layer 4 – 7 inspection. This service insertion is performed through NSX Service Composer, where routing is setup to direct traffic to additional security sensors and appliances for deeper inspection.

**Summary Result:** Supports Requirement Objective

**Additional Consideration:** Depending on the use case, additional services, above those which are offered by VMware, may need to be included to provide enhanced security.

(1.3.5) “Permit only “established” connections into the network.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The NSX firewall should maintain session state for established sessions.

Determine through examination of configuration, through reviewed documentation, and through testing that the NSX firewall is stateful and capable of blocking packets that are not part of a legitimately established session. The NSX firewall maintains and tracks the operating state and characteristics of the network connections traversing it.

**Findings:** Coalfire identified the NSX firewall as a stateful firewall capable of identifying and verifying legitimate packets as part of already established sessions. Furthermore, the NSX firewall is capable of blocking rogue packets that are not part of a legitimately established session.

**Summary Result:** Supports Requirement Objective

(1.3.6) “Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** Both the CDE and non-CDE environments were populated with multi-tier applications made up of web, application, and database elements. The web component(s) was placed in an established and managed CDE DMZ. The application component(s) was placed in an internal segregated network separate from the DMZ. Finally, the database element was placed in a third network segment segregated from the DMZ and the application segments.

Determine the capability of NSX for vSphere software-defined network firewall and router to segment the network to support separation between the DMZ and internal trusted elements of the network.

**Findings:** Coalfire determined that NSX for vSphere firewall and router capabilities for the software-defined network are capable of being configured to support segmentation between categorized zones of the network. The configuration of the assessment lab included separation of DMZ application and database using separate network segments separated by distributed logical router and protected by distributed firewall. Moreover, CDE and non-CDE zones were further separated by Edge Services Gateways with firewall and router services to prevent unauthorized transmission of traffic between zones.
Summary Result: Supports Requirement Objective

(1.3.7) “Do not disclose private IP addresses and routing information to unauthorized parties.

Note: Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls
- Removal or filtering of route advertisements for private networks that employ registered addressing
- Internal use of RFC1918 address space instead of registered addresses.” (PCI SSC, 2016)

Technical Design Consideration and Determination: For the assessment lab, all private IP addresses, including VXLAN overlay network addresses in use should be obfuscated to prevent disclosure to unauthorized parties.

Determine how NSX supports NAT to prevent disclosure of private IP address space to unauthorized parties. Determine whether NSX is capable of filtering route advertisements to unauthorized or untrusted networks to prevent disclosure.

Findings: NAT was provided at the NSX logical routers to prevent disclosure of private IP addresses to unauthorized parties and prevented route advertisements from being transmitted outside the private network.

Summary Result: Supports Requirement Objective

Objective: Regularly Monitor and Test Networks

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

(10.2) “Implement automated audit trails for all system components to reconstruct the following events.” (PCI SSC, 2016)

(10.2.1) “Implement automated audit trails for all system components to reconstruct the following events: All individual user accesses to cardholder data.” (PCI SSC, 2016)

Technical Design Consideration and Determination: The audit trail production capability should be able to identify access to sensitive systems that may enable regular users or privileged users to access cardholder data. This includes access to underlying systems that host cardholder data including, but not limited to ESXi hosts, vCenter, VM Console access, CLI access, and access to monitoring and management components of the infrastructure.

Determine the capability of VMware systems to generate audit logs through observation of created audit logs and examination of audit log settings.

Findings: The generation of audit logs was observed for each system and audit log settings, where available, were reviewed. VMware systems generate audit trails that can be reviewed for troubleshooting and investigation. Each system can be configured to send logs that it creates to a centralized syslog server. Additionally, logs can be collected and reviewed with vRealize Log Insight; however, the use of vRealize Log Insight is primarily for near real-time troubleshooting.

Summary Result: Partially Supports Requirement Objective
**Additional Consideration:** The payment entity should also include audit trail generation from payment applications, supporting operating systems. While vRealize Log Insight can be configured with connectors to collect and read logs from other systems, it will probably not be fully sufficient to satisfy central syslog requirements.

(10.2.2) "Implement automated audit trails for all system components to reconstruct the following events: All actions taken by any individual with root or administrative privileges." (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The audit trail capability of each system should be able to identify and report when actions are taken by users with privileged access, either root or administrative access. Moreover, the design of the logging mechanisms combined with parsing and alerting may benefit the entity by providing notification when generic root, shell, or administrator accounts are used to access systems as this may be an indication of possible compromise.

Determine if each system is configured to log actions taken by root or administrative privilege accounts.

**Findings:** Each VMware system inspected was determined to be able to generate logs when access or actions are taken by root or administrative privilege accounts. vRealize Log Insight was determined to be capable of aggregating logs from VMware systems. Logs can be reviewed within vRealize Log Insight using querying capability to search for logs specific to root or administrative accounts. Furthermore, alert notifications can be setup to notify when certain accounts are used to logon or access a system.

**Summary Result:** Supports Requirement Objective

(10.2.3) "Implement automated audit trails for all system components to reconstruct the following events: Access to audit trails." (PCI SSC, 2016)

**Technical Design Consideration and Determination:** Design of the logging mechanisms and systems should be able to identify when audit trails are accessed and generate a log of that access. The logged access to audit trails should include access that was obtained through programmatic means, through regular user interfaces, as well as through means available from the underlying operating system where access to audit trails may be attempted directly at the file or database level.

Determine if each system is configured to log access to audit trails.

**Findings:** It was determined that all systems generate logs for each action that is taken against the system; this includes access to audit trails through programmatic means. However, access to audit trails through file systems or databases may require additional configuration of the underlying operating system that supports the application to generate logs for that level of access. vRealize Log Insight does not generate logs for access to vRealize Log Insight and the audit trails being aggregated by this system. There are gaps in capability that prevent vRealize Log Insight from being used as a centralized logging facility to fully meet requirements of PCI DSS.

**Summary Result:** Partially Supports Requirement Objective.

(10.2.4) "Implement automated audit trails for all system components to reconstruct the following events: Invalid logical access attempts." (PCI SSC, 2016)

**Technical Design Consideration and Determination:** Each system should generate audit logs that include invalid logical access attempts. Invalid logical access attempts may include invalid logon...
Determine that each VMware system is configured to log invalid logical access attempts.

**Findings:** Each system in the SDDC is capable of logging invalid logical access attempts. This includes invalid logons as well as invalid access attempts for which the requested action is denied.

**Summary Result:** Supports Requirement Objective

(10.2.5) “Implement automated audit trails for all system components to reconstruct the following events: Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** The systems that make up the assessed VMware SDDC should be capable of logging change to identification and authentication mechanisms where local identification and authentication is provided, even if the local identification and authentication is provided for a select number of user and service accounts, including root and administrative accounts. As such, changes to the local accounts for each system should be logged and be a part of a reviewable audit trail. For both local accounts and authentication provided by integrated authentication mechanisms, elevation of privileges, adding or deleting of users to roles or changes to access control lists should be logged.

Determine whether each system within the VMware SDDC is capable of logging changes to the identification and authentication mechanisms. The applicability of this requirement and the assessment of capability was limited to systems which were provided by VMware including VMware provided infrastructure management and monitoring systems, hypervisor kernels, and VMware provided virtual appliances where the kernel or OS is locked down to support the appliances purpose.

**Findings:** It was determined that the evaluated VMware SDDC components are capable of logging changes to built-in identification and authentication mechanisms.

**Summary Result:** Partially Supports Requirement Objective

**Additional Consideration:** It is recommended that logged additions, changes, or deletions of any account with elevated privilege or for any account that is granted elevated privilege be immediately sent to a central syslog facility where log aggregation and analysis can occur. It is also recommended that alert notification be configured for specific logged events that may indicate the possibility of compromise. Coalfire only evaluated the VMware systems that are outlined in this document and make up the VMware supplied SDDC as part of the Center of Excellence.

(10.2.6) “Implement automated audit trails for all system components to reconstruct the following events: Initialization, stopping, or pausing of the audit logs.” (PCI SSC, 2016)

**Technical Design Consideration and Determination:** For each system, the initialization, stopping, or pausing of audit logs should be logged.

Determine if log entries are generated for VMware system components when associated logging mechanisms are initialized, stopped, or paused.

**Findings:** For most systems, the audit and event logging is built-in and does not provide users with an option for stopping, initializing, or pausing the logs. In some cases, the sudden and unexpected stoppage of logs would most likely coincide with a system outage. The findings for this requirement were inconclusive. It is recommended to use an outside monitoring system for monitoring the state
of the logging services or daemons for each in scope system that generates audit logs. It is also recommended to utilize an outside syslog service or SIEM solution for collections, aggregation, and analysis of logs.

Summary Result: Requirement Objective Gap

(10.2.7) “Implement automated audit trails for all system components to reconstruct the following events: Creation and deletion of system-level objects.” (PCI SSC, 2016)

Technical Design Consideration and Determination: The VMware Systems that are part of the SDDC solution should be capable of logging changes, creation, and deletion of system-level objects which might include changes to configuration files, database tables, stored procedures, database views, scripts, and so forth.

Determine if the VMware SDDC solutions in scope for this assessment are capable of detection and logging of the creation, deletion, or modification of system level objects.

Findings: Changes that occur programmatically through user interfaces or API connections are logged by the systems. This would include, where applicable, the creation and deletion of system level objects. Creation, deletion, or modification that occurs outside of the regular user interfaces may be logged by the underlying operating system or kernel. It is recommended to ship all generated logs to an outside syslog server or SIEM solution for log collection, aggregation, correlation, analysis, and review. Underlying kernels and operating systems should be protected with minimal authorized direct access to limit the possibility for compromise to occur. Where configuration files, databases, tables, or other system level objects are critical, it is recommended to use a file integrity monitoring tool for continuous verification and integrity checking.

Summary Result: Partially Supports Requirement Objective

(10.3) “Record at least the following audit trail entries for all system components for each event:” (PCI SSC, 2016)

(10.3.1) “Record at least the following audit trail entries for all system components for each event: user identification.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for VMware SDDC components include user identification for all recorded events.

Findings: It was determined that each of the assessed systems included the identification of the user, process, or service that performed an action to generate the event. Reviewing logs from the system that generated the logs can be somewhat cumbersome and difficult. For this reason, the use of a centralized log management solution is useful to support regular review, analysis, and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully meet the requirement. It is understood that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis, and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective
(10.3.2) “Record at least the following audit trail entries for all system components for each event: type of event.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for the assessed VMware SDDC components include the type of event for all recorded events.

Findings: It was determined that each of the assessed systems included the type of event that occurred in the recorded log. Reviewing logs from the system that generated the logs can be cumbersome and time consuming. For this reason, the use of a centralized log management solution is useful to support regular review, analysis and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully meet the requirement. It is understood that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective

(10.3.3) “Record at least the following audit trail entries for all system components for each event: date and time” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for the assessed VMware SDDC components include the date and time of the event for all recorded events.

Findings: It was determined that each of the assessed systems included the date and time of the event that occurred in the recorded log. Reviewing logs from the system that generated the logs can be cumbersome and time consuming. For this reason, the use of a centralized log management solution is useful to support regular review, analysis, and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully meet the requirement. It is understood that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective

(10.3.4) “Record at least the following audit trail entries for all system components for each event: success or failure indication” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for the assessed VMware SDDC components include the success or failure indication of the event for all recorded events.

Findings: It was determined that each of the assessed systems included the success or failure indication for the event that occurred in the recorded log. Reviewing logs from the system that generated the logs can be cumbersome and time consuming. For this reason, the use of a centralized log management solution is useful to support regular review, analysis, and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully
meet the requirement. It is understood that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis, and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective

(10.3.5) “Record at least the following audit trail entries for all system components for each event: origination of event” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for the assessed VMware SDDC components include the origination of the event for all recorded events.

Findings: It was determined that each of the assessed systems included the original of event for the event that occurred in the recorded log. Reviewing logs from the system that generated the logs can be cumbersome and time consuming. For this reason, the use of a centralized log management solution is useful to support regular review, analysis, and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully meet the requirement. The assessor found that there the viewable collection of event data was sometimes more complete in vRealize Network Insight than in vRealize Log Insight. It is understood by the assessor that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis, and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective

(10.3.6) “Record at least the following audit trail entries for all system components for each event: identity or name of affected data, system component, or resource” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trail entries for the assessed VMware SDDC components include the identity or name of the affected data, system component, or resource of the event for all recorded events.

Findings: It was determined that each of the assessed systems included the identity or name of the affected data, system component, or resource for the event that occurred in the recorded log. Reviewing logs from the system that generated the logs can be cumbersome and time consuming. For this reason, the use of a centralized log management solution is useful to support regular review, analysis and troubleshooting. While the systems generated the necessary entries for each generated event, the amount of information collected and viewable through vRealize Log Insight was inconsistent to fully meet the requirement. It is understood that vRealize Log Insight’s primary function is for troubleshooting issues and not specifically to support forensic analysis or security event monitoring. Therefore, it is recommended to use a third-party syslog or SIEM solution for log collections, aggregation, correlation, analysis, and review where central logging mechanisms are desired. It is also recommended that the syslog server receive the raw and unaltered logs from the generating system.

Summary Result: Partially Supports Requirement Objective
(10.4) “Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.

Note: One example of time synchronization technology is Network Time Protocol (NTP).” (PCI SSC, 2016)

Technical Design Consideration and Determination: Each system within the SDDC should be capable of being configured to use a centralized time keeping service to ensure synchronization of time across all systems in support of consistency of time stamps generate for events that occur on the systems.

Determine, where applicable, that the VMware SDDC systems are capable of being configured for NTP.

Findings: It was determined that all systems were configured to synchronize time with a domain level internal NTP server. In the case of the Center of Excellence lab, each system was configured to use the domain controllers for NTP. The domain controllers were configured to use an external reliable time source. For applications that generate logs that do not have NTP configuration, it was determined that these applications utilize the time generated by the underlying hosting system. In this case, it is expected that the underlying system, operating system, or kernel are configured to use the same time source for synchronization as the rest of the environment.

Summary Result: Supports Requirement Objective

(10.4.1) “Critical systems have the correct and consistent time.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine that all systems have the correct and consistent time.

Findings: From a sampling of systems that make up the VMware SDDC, it was determined that all systems have the correct and consistent time which was also consistent with the NTP configuration settings and consistent with the configured time source.

Summary Result: Supports Requirement Objective

(10.4.2) “Time data is protected.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if configuration settings are protected through role-based access controls to limit the personnel who can adjust the system time or changing configuration. Determine that any changes to the time configuration or time setting of a system are logged for review.

Findings: For the assessed VMware SDDC solutions, it was determined that role-based access controls could be setup to limit access to time configuration settings. In many cases, the time settings are protected and can only be changed through console access. The payment entity that utilizes these solutions can limit the number of individuals who have access to administrative consoles for these systems to improve security. Changes to the systems, including time changes and time configuration changes are logged by each system. It is recommended to use a central syslog server or log collector or SIEM solution that collects or receives raw logs from the generating system(s) with appropriate retention settings to allow for future forensic review and analysis.

Summary Result: Supports Requirement Objective

(10.4.3) “Time settings are received from industry-accepted time sources.” (PCI SSC, 2016)
Technical Design Consideration and Determination: Determine if time settings can be configured to use industry-accepted time sources.

Findings: Where limitation for external access are required that would prevent access to external "industry-accepted" time sources, the time settings were configured to use a time source local to the VMware SDDC. This internal time source(s) was permitted through explicit firewall rules to communicate to an industry-accepted external time source such as NIST. It was determined that time-source configuration for NTP was not hardcoded and all VMware SDDC systems that were configurable for NTP could be customized to use an approved time source.

Summary Result: Supports Requirement Objective

(10.5) "Secure audit trails so they cannot be altered." (PCI SSC, 2016)

Technical Design Consideration and Determination: The system(s) that create and/or manage audit trails should be designed to prevent unauthorized alteration or tampering of audit trails. Design considerations may include the placement of audit logs on controlled storage within the secure network access list provided with role-based access control to limit direct access to the logs or audit records. User interfaces that allow for interaction with audit logs may be limited to view only, where raw logs are unaltered during log queries, parsing, or log consolidation. Where available, systems should be configured to send logs to a syslog server, log collector, or SIEM solution.

Findings: vRealize Log Insight provides a viewable console for interacting with audit and event logs. Logs are not capable of being altered through programmatic access. Direct console access can be limited to a select number of users and closely monitored. Logs generated by the vRealize Log Insight, however, are not reviewable within vRealize Log Insight. It is recommended to use a third-party syslog server, log collector, or SIEM solution to fully meet the requirement. It is understood by the assessor, that vRealize Log Insight is not intended to be a tool to support forensic security analysis.

Summary Result: Requirement Objective Gap

(10.5.1) “Limit viewing of audit trails to those with a job-related need.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trails can be limited for viewing to those with a job-related need.

Findings: Role-based access controls can be enabled to limit access to audit trails. This can be done at the direct console level, as well as through programmatic access to review audit trails.

Summary Result: Supports Requirement Objective

(10.5.2) “Protect audit trail files from unauthorized modifications.” (PCI SSC, 2016)

Technical Design Consideration and Determination: Determine if audit trails are capable of being protected from unauthorized modification. Protection mechanisms could include access control mechanisms, physical segregation, and or network segregation.

Findings: Access controls can be used with the VMware SDDC systems as well as with vRealize Log Insight to limit or restrict access to the audit trails. Access to the audit trails, either through programmatic means or through direct console access, should be closely logged and monitored. Consideration should be made for the location of storage for logs collected by vRealize Log Insight, where access to the storage is also tightly restricted. Consideration for network segmentation of log collection processes may also be useful to protect the transmission of logs to central logging facilities. Audit trail protection is not a primary objective of vRealize Log Insight; however, mitigating or
compensating controls can be implemented to achieve the level of security for the logs as necessary to meet the requirement.

**Summary Result:** Supports Requirement Objective

**(10.5.3)** “Promptly back up audit trail files to a centralized log server or media that is difficult to alter.”

**(PCI SSC, 2016)**

**Technical Design Consideration and Determination:** Determine if audit trails files are capable of being sent to a centralized log server or media that is difficult to alter.

**Findings:** All VMware SDDC solutions are capable of being configured to send logs to a centralized log server. VMware vRealize Log Insight can back up or archive audit trail files for long-term storage. The location of the backup target can be specified to include secure media or network storage location. Because there is a limitation to the length of time that audit trails can be retained both by VMware SDDC solutions and by vRealize Log Insight specifically, it is recommended to either utilize a purpose-built syslog or SIEM solution. Otherwise, the archive capability of vRealize Log Insight should be utilized to facilitate longer term retention.

**Summary Result:** Partially Supports Requirement Objective

**(10.5.4)** “Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.”

**(PCI SSC, 2016)**

**Technical Design Consideration and Determination:** Determine if logs for external-facing technologies can be written to internal secure, centralized log servers or media devices.

**Findings:** There is nothing from the VMware solution that restricts or prevents logs from being written to a centralized, internal log server or media device.

**Summary Result:** Supports Requirement Objective

**(10.5.5)** “Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).”

**(PCI SSC, 2016)**

**Technical Design Consideration and Determination:** Determine if the VMware SDDC solution utilizes file-integrity monitoring or change-detection software on the logs to ensure that the existing log data cannot be changed without generating alerts.

**Findings:** There is no built-in file integrity or change-detection solution for the VMware SDDC systems or vRealize Log Insight that is capable of detection and generating alerts for already written log data that is changed. This would require an outside, third-party solution that is capable of monitoring and alerting on alterations of the log data. There are, however, VMware Partner solutions for syslog and SIEM that support integrity checking of written logs to ensure consistency and security of logs.

**Summary Result:** Requirement Objective Gap

**(10.7)** “Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).”

**(PCI SSC, 2016)**

**Technical Design Consideration and Determination:** Determine the length of time that logs can be retained in audit trail history and whether VMware solutions support a minimum one-year term retention with three months immediately available for analysis.
Findings: vRealize Log Insight is capable of long-term archive of collected log data. The archived data is not indexed and immediately searchable. To support historical analysis of archived logs, a separate offline instance of Log Insight will be required. The short term indexed and searchable log retention is dependent on the storage pool that Log Insight creates. The size of the storage pool will determine the length of history of log data that will be immediately reviewable. A retention notification threshold can be enabled to notify administrators when the available resources are close to the limit. The threshold is estimated by the rate of collection and input data received to determine how long data can be retained. There are not specific retention settings that can be placed on the logs collected, stored, and archived by vRealize Log Insight. While some mitigating configuration and controls may be setup to achieve, the desired outcome regarding support of this requirement objective, the use of a purpose-built syslog or SIEM to meet compliance objectives may be preferred.

Summary Result: Partially Supports Requirement Objective

Summary
Coalfire performed the assessment of the VMware Validated Design for SDDC, the use cases presented in this document, layering of organizational workloads, and implemented configuration specific to PCI DSS 3.2 requirements. From this assessment, Coalfire concluded that the VMware Validated Design for SDDC with respect to network security as provided by VMware NSX for vSphere may be used to provide controls in alignment for support of requirement 1 of PCI DSS 3.2. The control capability of NSX for vSphere may be useful for segmentation, micro-segmentation, and security of protected workloads both for the infrastructure and for layered payment entity workloads hosted on the infrastructure. Moreover, NSX for vSphere may be able to enhance security for virtualized workloads above that provided by traditional network boundary protection mechanisms.

Payment entities may want to evaluate partner solutions for advanced security (IDS/IPS, next generation application firewalls, web filters, content filters, and so forth) that can be integrated with and work in coordination with NSX for vSphere to further mitigate risk inherent in all networked systems.

Coalfire concluded that VMware components that are part of the VMware Validated Design for SDDC may be used in support of requirement 10 of PCI DSS 3.2. Coalfire also concluded that vRealize Log Insight is primarily a tool for troubleshooting issues that may occur in the VMware SDDC, but that vRealize Log Insight may fall short of meeting necessary capabilities to satisfy centralized logging requirements of PCI DSS 3.2. While mitigating or compensating controls may be possible to augment vRealize Log Insight to achieve the necessary criteria, payment entities should evaluate the costs and benefits of utilizing this solution relative to the degree of difficulty and additional risk that the use of compensating or mitigating controls may present.
Resources

BIBLIOGRAPHY

Acknowledgements
VMware would like to recognize the efforts of the VMware product, marketing, legal, and sales teams that contributed to this paper and to the VMware Compliance and Cyber Risk Solutions Program team. VMware would also like to recognize Coalfire Systems, Inc., www.coalfire.com/Partners/VMware, and Intel Corporation, www.intel.com/vmware, for their industry guidance.

Coalfire Systems, Inc., a leading security and compliance advisory and audit firm, provided the guidance and control interpretation described herein. Intel Corporation and VMware have collaborated for over a decade to bring optimized and trusted solutions to enterprises worldwide.

About Coalfire
Coalfire is a trusted leader in cybersecurity risk management and compliance services. Coalfire integrates advisory and technical assessments and recommendations to the corporate directors, executives, boards, and IT organizations for global brands and organizations in the technology, cloud, healthcare, retail, payments, and financial industries.

Coalfire’s approach addresses each businesses’ specific vulnerability challenges, developing a long-term strategy to prevent security breaches and data theft. With offices throughout the United States and Europe, Coalfire was recently named one of the top 20 Most Promising Risk Management Solution Providers. www.coalfire.com

Disclaimer
*VMware solutions are designed to help organizations address various regulatory compliance requirements. This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address such requirements. VMware encourages any organization that is considering VMware solutions to engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements. It is the responsibility of each organization to determine what is required to meet any and all requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide legal advice and is provided “AS IS”. VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Nothing that you read in this document should be used as a substitute for the advice of an actual Cyber Security auditor or competent legal counsel.