Security and Compliance Configuration for PCI

14 JAN 2019

VMware Validated Design 5.1.1

VMware Validated Design for Software-Defined Data Center 5.1.1

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About VMware Validated Design Security and Compliance Configuration for PCI

VMware Validated Design Security and Compliance Configuration for PCI provides step-by-step configuration for securing a software-defined data center based on the VMware Validated Design for Software-Defined Data Center for compliance with the Payment Card Industry standard.

Legal Disclaimer This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided “AS IS”. VMware makes no claims, promises or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Intended Audience

VMware Validated Design Security and Compliance Configuration for PCI is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to secure and work towards compliance with the PCI framework.

Required VMware Software

The *VMware Validated Design Security and Compliance Configuration for PCI* documentation is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Before You Apply This Guidance

The sequence of the documentation of VMware Validated Design follows the stages for implementing and maintaining an SDDC. See Documentation Map for VMware Validated Design.

To use *VMware Validated Design Security and Compliance Configuration for PCI*, you must be acquainted with the following guidance:

- *Introducing VMware Validated Designs*
- Optionally *VMware Validated Design Architecture and Design*
- *VMware Validated Design Planning and Preparation*

- *VMware Validated Design Deployment of Region A*
- *VMware Validated Design Deployment of Region B*
- *VMware Validated Design for Deployment for Multiple Availability Zones*
- Optionally *Introducing Security and Compliance*
- Optionally *Product Applicability Guide for PCI*

Compliance Considerations with PCI for VMware Validated Design

1

PCI DSS 3.2.1 forms a security baseline for organizations that handle branded credit cards from major credit card brands. The standard was created to increase security around cardholder data and protect consumers. This guide ennumerates security capabilities within the VMware Validated Design to protect cardholder data long the PCI DSS standards.

Payment Card Industry Data Security Standard PCI DSS 3.2.1

PCI DSS v3.2.1 is an updated version of the PCI Data Security Standard originally developed by PCI Standards Council in 2004. This version considers evolving technologies and threat vectors to consumers, merchants and other entities within the transaction chain. This guide addresses configurations that can be applied to the VMware Validated Design to assist in developing capabilities for the PCI DSS 3.2.1 (PCI).

Notice When you apply the guidance from this guide you do not achieve PCI DSS compliance.

This guide can serve as guidance to VMware Validated Design capabilities that have been mapped to PCI DSS 3.2.1 controls. The process to arrive to these mappings is a derivative from the Product Applicability Guide.

An individual business interaction with cardholder data will vary depending on their defined operations. This underscores that there is no one-size fits all recommendation to secure a cardholder data environment (CDE). The responsibility resides with the individual business to ensure they appropriately assess what requirements fit their environment to adequately protect cardholder data along PCI DSS.

As with many security standards, PCI DSS takes a variety of its intentions from NIST 800-53 as guidance for defense in depth security within the cardholder environment.

The PCI DSS standard requires organizations to comply with a robust set of requirements. The criteria are broken down into 6 objective areas and 12 requirements. Each requirement has a set of controls, the necessary testing procedures to ensure that they are implemented appropriately with expert guidance.

The scope of the controls present within each requirement are assessed for applicability and relevance to the VMware Validated Design. In addition, individual controls will be vetted and integrated into the VMware Validated Design based on applicability and relevance, until the full list of applicable PCI DSS requirements are incorporated into the bifurcated model as follows:

Built-in Controls	Security controls based on compliance requirements are included in the VMware Validated Design for Software-Defined Data Center. These may require configuration and adjustment, but by design the capabilities are included in the VMware Validated Design for Software-Defined Data Center.
Enhanced Guidance	Additional guidance on a per regulation, or standard basis includes a set of capabilities that can be added to the VMware Validated Design for Software-Defined Data Center.

Over time, we expect a significant number of enhancement VMware Validated Design controls will be incorporated into the VMware Validated Design for Software-Defined Data Center. However, we do expect that the enhancement guide will always contain some number of PCI controls that are applicable to PCI DSS 3.2.1 but for various reasons, are not included in the VMware Validated Design for Software-Defined Data Center implementation.

Planning and Preparation for Compliance with PCI

2

You must provide a set of external services before you can start the configuration of the SDDC for Compliance with PCI.

- Software Requirements for Compliance with PCI

  To reconfigure your SDDC for compliance with PCI, you must download and license additional VMware and third-party software.

- General Guidance and Security Best Practices for Operating an SDDC for Compliance with PCI

  The PCI framework recommends a number of best practices that you must follow at all times when you operate the SDDC.

Software Requirements for Compliance with PCI

To reconfigure your SDDC for compliance with PCI, you must download and license additional VMware and third-party software.

VMware Validated Design Security and Compliance Configuration for PCI uses scripts and commands based on VMware PowerCLI to reconfigure the SDDC. You must prepare a host with supported OS for running Microsoft PowerShell, set-up Microsoft PowerShell, and install the latest version of VMware PowerCLI. The host must have connectivity to the ESXi management network in the management cluster.

Table 2-1. Third-Party Software Required for *VMware Validated Design Security and Compliance Configuration for PCI*

SDDC Layer	Product Group	Script/Tool	Download Location	Description
Virtual Infrastructure	VMware PowerCLI	Supported OS for VMware PowerCLI	n/a	Operating system that supports Microsoft PowerShell and VMware PowerCLI. For more information on supported operating systems, see VMware PowerCLI User's Guide.
Virtual Infrastructure	VMware NSX® Data Center for vSphere®	FTP server	n/a	Space for NSX Manager backups must be available on an FTP server. The server must support SFTP and FTP. The NSX Manager instances must have connection to the remote FTP server.

Table 2-2. VMware Scripts and Tools Required for *VMware Validated Design Security and Compliance Configuration for PCI*

SDDC Layer	Product Group	Script/Tool	Download Location	Description
Virtual Infrastructure and Operations Management	vSphere, VMware Site Recovery Manager, vRealize Operations Manager	VMware PowerCLI	n/a	VMware PowerCLI contains modules of cmdlets based on Microsoft PowerShell for automating vSphere, VMware Site Recovery Manager, vSphere Automation SDK, vSphere Update Manager, vRealize Operations Manager, NSX-T, and so on. VMware PowerCLI provides a PowerShell interface to the VMware product APIs.

General Guidance and Security Best Practices for Operating an SDDC for Compliance with PCI

The PCI framework recommends a number of best practices that you must follow at all times when you operate the SDDC.

Install Security Patches and updates for ESXi hosts

PCI–VI–ESXI–CFG–00129 You must perform a compliance check on the inventory objects to make sure that you applied all the latest security patches and updates. In the Update Manger tab, you can remediate the non-compliant hosts and virtual machines.

Use Templates to Deploy Virtual Machines

PCI–VI–VC–CFG–00060 Use templates that can contain a hardened, patched, and properly configured operating system to create other, application-specific templates. You can also use the application template to deploy virtual machines.

Verify the Integrity of the installation Media for ESXi

PCI–VI–ESXI–CFG–00134 Always check the SHA1 hash after downloading an ISO, offline bundle, or patch to ensure integrity and authenticity of the downloaded files.

After downloading media, use the MD5 sum value to verify the integrity of the download. Compare the MD5 sum output with the value posted on the VMware Web site. SHA1 or MD5 hash must match.

Add Only System Accounts to the ESXi Exception Users List

PCI–VI–ESXI–CFG–00125 You can add users to the Exception Users list from the vSphere Client. Such users do not lose their permissions when the host enters lockdown mode. Only add service accounts such as backup agents. Do not add administrative users or user groups to that list.

Encrypt VMware vSAN Datastores

PCI–VI–Storage–SDS–CFG–00183 When you enable encryption, vSAN encrypts everything in the vSAN datastore. All files are encrypted, so all virtual machines and their corresponding data are protected. Only administrators with encryption privileges can perform encryption and decryption tasks.

Assigning Roles for vSAN Encryption

PCI–VI–Storage–SDS–CFG–00204 The built-in `Administrator` role has the permission to perform cryptographic operations such as Key Management Server (KMS) functions and encrypting and decrypting virtual machine disks. This role must be reserved for cryptographic administrators where Virtual Machine encryption or vSAN encryption is required. All other vSphere administrators who do not require cryptographic operations must be assigned the `No Cryptography Administrator` role.

vSAN Capacity Sizing Guidelines

PCI–VI–Storage–SDS–CFG–00186 Ensure you have sufficient capacity in the management vSAN cluster for the management virtual machines. You can expand the datastore by adding capacity devices or hosts with capacity devices to the cluster.

NSX Manager Manual Back Up

PCI–VI–NET–CFG–00290 Manually back up the configuration of your NSX Manager nodes after every configuration change. You also configure weekly backups as part of the reconfiguration of the NSX Data Center for vSphere Instances for compliance with PCI.

Business Continuity Guidelines

PCI–VI–VC–CFG–00455 Follow the guidance in the *VMware Validated Design Backup and Restore* document on how to use a vSphere Storage API - Data Protection (VADP) solution for performing backup and restore of the management components in the Software-Defined Data Center. After you deploy the VMware Validated Design for Software-Defined Data Center, backing up management components ensures that you can keep your environment operational in the event of data loss or failure. You implement scheduled backups to prepare for:

- A critical failure of any management component
- An upgrade of any management component
- Updating the certificate of any management component

Region A Virtual Infrastructure Configuration for Compliance with PCI

3

Perform the procedures to secure your virtual infrastructure.

Procedure

1 Configure ESXi Hosts for Compliance with PCI in Region A

Perform the procedures to secure your ESXi hosts.

2 Configure vCenter Server and vSAN for Compliance with PCI in Region A

Perform the procedures to secure your vCenter Server instances.

3 Configure the NSX Data Center for vSphere Instances for Compliance with PCI in Region A

Perform the procedures to secure your NSX Data Center for vSphere instances.

Configure ESXi Hosts for Compliance with PCI in Region A

Perform the procedures to secure your ESXi hosts.

Procedure

1 Configure the SSH Service on the ESXi Hosts for Compliance with PCI in Region A

You must edit the `/etc/ssh/sshd_config` file on all your hosts to reconfigure the SSH service. You also remove the `authorized_keys` file on all ESXi hosts and edit the `/etc/pam.d/passwd` file to configure password settings. Before you can log in to a host and change the configuration file, you must disable lockdown mode.

2 Configure Advanced Settings on the ESXi Hosts for Compliance with PCI in Region A

You perform the procedure on all ESXi hosts to configure firewall settings, password policy, inactivity and availability timeouts, and failed login attempts. Also configure a core dump collector, login banners for the Direct Console User Interface (DCUI) and SSH Connections, disable warnings, and enable Bridge Protocol Data Unit (BPDU) filter by using PowerCLI commands.

3 Restrict the Access to All ESXi Hosts for Compliance with PCI in Region A

You restrict remote access to the host by disabling the SSH service and the shell service and enabling lockdown mode.

Configure the SSH Service on the ESXi Hosts for Compliance with PCI in Region A

You must edit the `/etc/ssh/sshd_config` file on all your hosts to reconfigure the SSH service. You also remove the `authorized_keys` file on all ESXi hosts and edit the `/etc/pam.d/passwd` file to configure password settings. Before you can log in to a host and change the configuration file, you must disable lockdown mode.

You perform the procedure on all ESXi hosts in Region A.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Disable lockdown mode on the sfo01m01esx01.sfo01.rainpole.local host.

   a In the **Hosts and Clusters** inventory, expand the entire **sfo01m01vc01.sfo01.rainpole.local** tree.

   b Under the **sfo01-m01dc** data center, select the **sfo01m01esx01.sfo01.rainpole.local** host object and click the **Configure** tab.

   c Click the **Security Profile** tab on the right.

   d Under **Lockdown Mode**, click **Edit**.

   e In the **Lockdown Mode** dialog box, select **Disabled** and click **OK**.

3 Log in to the `sfo01m01esx01.sfo01.rainpole.local` ESXi host by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo01m01esx01.sfo01.rainpole.local
User name	root
Password	*root_user_password*

4 Rename the existing `sshd_config` file for backup.

```
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
```

5 Create a new `sshd_config` file in the `/etc/ssh` folder with the PCI configurations.

Table 3-1. Configurations to Perform

Configuration ID	Description
PCI-VI-ESXI-CFG-00001	Use only FIPS-approved algorithms for encryption.
PCI-VI-ESXI-CFG-00003	Set the `IgnoreRhosts` option to **yes** to force users to enter a password when authenticating with SSH.
PCI-VI-ESXI-CFG-00004	Set the `HostbasedAuthentication` option to **no** to disable authentication through trusted hosts.
PCI-VI-ESXI-CFG-00005	Set the `PermitRootLogin` option to **no** to disable SSH access for the root user.
PCI-VI-ESXI-CFG-00006	Set the `PermitEmptyPasswords` option to *no* to prevent users with blank password from using SSH.
PCI-VI-ESXI-CFG-00007	Set the `PermitUserEnvironment` option to **no** to forbid users presenting environment options to the SSH deamon.
PCI-VI-ESXI-CFG-00009	Set the `GSSAPIAuthentication` option to **no** to disable GSSAPI authentication.
PCI-VI-ESXI-CFG-00010	Set the `KerberosAuthentication` to **no** to disable the Kerberos protocol.
PCI-VI-ESXI-CFG-00011	Set the `StrictModes` option to **yes** to force permissions checks on keyfiles and directories.
PCI-VI-ESXI-CFG-00012	Set the `Compression` option to **no** to deny compression proir to a successful user authentication.
PCI-VI-ESXI-CFG-00013	Set the `GatewayPorts` option to **no** to prevent connecting to forwarded ports from outside the host.
PCI-VI-ESXI-CFG-00015	Delete all values for `AcceptEnv` to reject environment variables from the client.
PCI-VI-ESXI-CFG-00016	Set the `PermitTunnel` option to **no** to prevent the SSH daemon the ability to create network tunnels over an SSH connection.
PCI-VI-ESXI-CFG-00017	Set the `ClientAliveCountMax` option to **3** as the total number of checkalive messages sent by the SSH server without response by the SSH client.
PCI-VI-ESXI-CFG-00019	Set the `MaxSessions` option to **1** as the maximum number of open sessions permitted per network connection.

a Open the VI editor to add a new `sshd_config` file in `/etc/ssh`.

```
vi /etc/ssh/sshd_config
```

b In the VI editor, enter the configurations to the `sshd_config` file.

```
# Version 6.7.2.0
# running from inetd
# Port 2200

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
```

```
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
Protocol 2
IgnoreRhosts yes
HostbasedAuthentication no
PermitRootLogin no
PermitEmptyPasswords no
PermitUserEnvironment no
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512
GSSAPIAuthentication no
KerberosAuthentication no
StrictModes yes
Compression no
GatewayPorts no
X11Forwarding no
AcceptEnv
PermitTunnel no
ClientAliveCountMax 3
ClientAliveInterval 200
MaxSessions 1
UsePrivilegeSeparation no
SyslogFacility auth
LogLevel info
PrintMotd yes
PrintLastLog no
TCPKeepAlive yes
Banner /etc/issue
```

c Save and close the VI editor.

d Restart the SSH service to apply the new configurations.

```
/etc/init.d/SSH restart
```

6 `PCI-VI-ESXI-CFG-00107` Remove the SSH authorized_keys file from `/etc/ssh/keys-root/`.

```
rm /etc/ssh/keys-root/authorized_keys
```

7 `PCI-VI-ESXI-CFG-00109` Configure the value of the **remember** option to `4` in the `/etc/pam.d/passwd` file to restrict the reuse of the last five passwords.PCI

a Open the VI editor to to edit the `/etc/pam.d/passwd` file.

```
vi /etc/pam.d/passwd
```

b Add **remember=4** at the end of the `password sufficient` line in the file.

```
password sufficient /lib/security/$ISA/pam_unix.so use_authtok nullok shadow
sha512 remember=4
```

c Save and close the VI editor.

8 Repeat the procedure for all remaining hosts in Region A.

Configure Advanced Settings on the ESXi Hosts for Compliance with PCI in Region A

You perform the procedure on all ESXi hosts to configure firewall settings, password policy, inactivity and availability timeouts, and failed login attempts. Also configure a core dump collector, login banners for the Direct Console User Interface (DCUI) and SSH Connections, disable warnings, and enable Bridge Protocol Data Unit (BPDU) filter by using PowerCLI commands.

To perform the procedure, you first connect to the Management vCenter Server and then connect to the Compute vCenter server to perform the procedure on the ESXi hosts that belong to the Compute vCenter server. When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure. Use the values from the table for the respective vCenter Server instance that you configure.

Setting	Value for the Management vCenter Server	Value for the Compute vCenter Server
`esxcli.network.firewall.ruleset.allowedip.add` in step Step 12	172.16.11.0/24	172.16.31.0/24
`vCenterIP` in step Step 13	172.16.11.62	172.16.11.64

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server sfo01m01vc01.sfo01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-ESXI-CFG-00043` Run the command to enable the Bridge Protocol Data Unit filter.

```
Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU | Set-AdvancedSetting -Value 1
```

3 `PCI-VI-ESXI-CFG-00034` Set the maximum number of failed login attempts before an account is locked to 6.

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-AdvancedSetting -Value 6
```

4 `PCI-VI-ESXI-CFG-00022` Configure the ESXi password policy so that passwords contain 4 character classes and no less than 7 characters.

```
Get-VMHost | Get-AdvancedSetting -Name Security.PasswordQualityControl | Set-AdvancedSetting -Value "similar=deny retry=3 min=disabled,disabled,disabled,disabled,7"
```

5 PCI-VI-ESXI-CFG-00038 Configure the inactivity timeout to automatically terminate idle shell sessions to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Set-AdvancedSetting -Value 900
```

6 PCI-VI-ESXI-CFG-00039 When SSH or appliance shell is enabled, allow 900 seconds for a user to log in before the service is automatically disabled.

a Configure timeout to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellTimeOut | Set-AdvancedSetting -Value 900
```

b Restart the SSH service for the changes to take effect.

```
$service = Get-VMHost | Get-VMHostService | where {$_.key -eq 'tsm'}
Restart-VMHostService $service
```

7 PCI-VI-ESXI-CFG-000165 After a user exceeds the maximum allowed failed login attempts, set a lockout timer to temporarily prevent further login attempts.

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime | Set-AdvancedSetting -Value 1800
```

8 PCI-VI-ESXI-CFG-00168 Configure the timeout to automatically terminate idle DCUI connections to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut | Set-AdvancedSetting -Value 900
```

9 PCI-VI-ESXI-CFG-00030 Show warnings in the vSphere Client if local or remote shell sessions are enabled on the ESXi host.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning | Set-AdvancedSetting -Value 0
```

10 PCI-VI-ESXI-CFG-00122 Configure the login banner for the DCUI of the ESXi host.

```
Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage | Set-AdvancedSetting -Value "This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personal may provide the evidence of such monitoring to law enforcement officials."
```

11 PCI-VI-ESXI-CFG-00123 Configure the login banner for the SSH connections.

```
Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue | Set-AdvancedSetting -Value "This system is for the use of authorized users only. Individuals using this computer system without authority
```

```
or in excess of their authority are subject to having all their activities on this system
monitored and recorded by system personnel. Anyone using this system expressly consents to such
monitoring and is advised that if such monitoring reveals possible evidence of criminal activity
system personal may provide the evidence of such monitoring to law enforcement officials."
```

12 `PCI-VI-ESXI-CFG-00028` Configure the ESXi host firewall to only allow traffic from the ESXi management network.

Use the respective value for `esxcli.network.firewall.ruleset.allowedip.add` when you perform the procedure on the Compute vCenter Server.

```
$EsxiHosts = Get-VMHost
foreach($EsxiHost in $EsxiHosts){
$esxcli = Get-EsxCli -VMHost $EsxiHost.Name
#This disables the allow all rule for the target service
$esxcli.network.firewall.ruleset.set($false,$true,"sshServer")
$esxcli.network.firewall.ruleset.allowedip.add("172.16.11.0/24","sshServer")}
```

13 `PCI-VI-ESXI-CFG-00056`, `PCI-VI-Storage-SDS-CFG-00562` Configure a core dump collector.

Use the respective value for `vCenterIP` when you perform the procedure on the Compute vCenter Server.

```
$vCenterIP = '172.16.11.62'
foreach ($VMHost in Get-VMHost) {
$esxcli = Get-EsxCli -VMHost $VMHost.Name
$esxcli.system.coredump.network.set($null,"vmk0",$null,$vCenterIP,6500)
$esxcli.system.coredump.network.set(1)
$esxcli.system.coredump.network.get()
}
```

14 Log in to the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure for the remaining hosts in Region A.

Restrict the Access to All ESXi Hosts for Compliance with PCI in Region A

You restrict remote access to the host by disabling the SSH service and the shell service and enabling lockdown mode.

You perform the procedure on all the ESXi hosts in Region A. To perform the procedure, you first connect to the Management vCenter Server and then connect to the Compute vCenter Server to perform the procedure on all the ESXi hosts that belong to the Computer vCenter Server. When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server sfo01m01vc01.sfo01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-ESXI-CFG-00111` Stop and disable the SSH service.

```
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "SSH"} | Set-VMHostService -Policy Off
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "SSH"} | Stop-VMHostService
```

3 `PCI-VI-ESXI-CFG-00112` Stop and disable the ESXi shell service.

```
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"} | Set-VMHostService -Policy Off
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"} | Stop-VMHostService
```

4 `PCI-VI-ESXI-CFG-00031` Enable `Normal` lockdown mode.

```
$level = "lockdownNormal"
$EsxiHosts = Get-VMHost
foreach($EsxiHost in $EsxiHosts)
{$vmhost = $EsxiHost | Get-View
$lockdown = Get-View $vmhost.ConfigManager.HostAccessManager
$lockdown.ChangeLockdownMode($level) }
```

5 Log in to the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure for the remaining hosts in Region A.

Configure vCenter Server and vSAN for Compliance with PCI in Region A

Perform the procedures to secure your vCenter Server instances.

Procedure

1 Configure Password Policy and Lockout Policy Settings in vCenter Server for Compliance with PCI in Region A

You configure password policy and lockout policy settings on the Management vCenter Server instance in Region A. After you configure the settings, they are populated for the entire `vsphere.local` domain and all regions.

2 Configure the Security Policies for Virtual Switches and Virtual Port Groups for Compliance with PCI in Region A

Restrict port-level configuration overrides on port groups and disable health check on the distributed switches.

3 Configure Advanced Security Settings on the vCenter Server Instances for Compliance with PCI in Region A

You enable SSL for the Network File Copy function and configure the password length for the built-in `vpxuser`.

4 Configure Alerts in vCenter Server for Compliance with PCI in Region A

You configure alerts to system administrators and ISSO personas for all audit failure events and to inform them for every operation that adds, modifies, or deletes permissions in the vsphere.local domain.

5 Configure Sessions Expiration for the vSphere Web Client and the vSphere Client for Compliance with PCI in Region A

You configure sessions in the vSphere Web Client and vSphere Client to expire after 10 minutes of inactivity.

6 Restrict the Use of the Virtual Machine Console for Compliance with PCI in Region A

You configure settings to minimize the use of the Virtual Machine console by removing the privilege to use the virtual machine console for the standard virtual machine user role. You can assign the `Virtual Machine console user` role to a user if they require console access. You configure the privilege on the Management vCenter Server in Region A and the setting is populated for the entire vsphere.local domain.

7 Configure Advanced Settings on All Management Virtual Machines for Compliance with PCI in Region A

Disable unexposed features, drag and drop operations, copy and paste operations, shared salt values, console access, unused display features, sending host information to virtual machines, limit sharing of console connections, limit the VMX configuration file size, and audit all uses of PCI or PCIe passthrough functionalities by using PowerCLI commands.

8 Set SDDC Deployment Details on the vCenter Server Instances for Compliance with PCI in Region A

9 Restrict the Connectivity Between vSAN Health Check and Public Hardware Compatibility List for Compliance with PCI in Region A

You configure a proxy server to restrict the connectivity between vSAN Health Check and public Hardware Compatibility List.

Configure Password Policy and Lockout Policy Settings in vCenter Server for Compliance with PCI in Region A

You configure password policy and lockout policy settings on the Management vCenter Server instance in Region A. After you configure the settings, they are populated for the entire `vsphere.local` domain and all regions.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Configure the password policies.

a From the **Home** menu of the vSphere Client, click **Administration**.

b Under **Single Sign-On**, click **Configuration**.

c On the **Policies** tab, under **Password policy**, click **Edit**.

d In the **Edit password policies** dialog box, configure the settings and click **Save**.

Configuration ID	Setting	Value
PCI–VI–VC–CFG–00410	Minimum length	7

3 Configure the lockout policies.

a On the **Policies** tab, click **Lockout Policy** and click **Edit**.

b In the **Edit lockout policies** dialog box, configure the settings and click **Save**.

Configuration ID	Setting	Value
PCI–VI–VC–CFG–00436	Maximum number of failed login attempts	6
PCI–VI–VC–CFG–00434	Time interval between failuresper	900 Seconds
PCI–VI–VC–CFG–00435	Unlock time	0 seconds

Configure the Security Policies for Virtual Switches and Virtual Port Groups for Compliance with PCI in Region A

Restrict port-level configuration overrides on port groups and disable health check on the distributed switches.

You perform the procedure for all the distributed switches and port groups in Region A. To perform the procedure, you first connect to the Management vCenter Server and then to the Compute vCenter Server.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server sfo01m01vc01.sfo01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00440` Restrict port-level configuration overrides on all existing port groups.

```
$pgs = Get-VDPortgroup | Get-View
ForEach($pg in $pgs){
$spec = New-Object VMware.Vim.DVPortgroupConfigSpec
$spec.configversion = $pg.Config.ConfigVersion
$spec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$spec.Policy.VendorConfigOverrideAllowed = $False
$spec.Policy.BlockOverrideAllowed = $False
$spec.Policy.PortConfigResetAtDisconnect = $True
$pg.ReconfigureDVPortgroup_Task($spec)}
```

3 `PCI-VI-VC-CFG-00411` Disable the health check on all distributed switches.

```
Get-View -ViewType DistributedVirtualSwitch | ?{($_.config.HealthCheckConfig | ?{$_.enable -
notmatch "False"})}| %{$_.UpdateDVSHealthCheckConfig(@((New-Object
Vmware.Vim.VMwareDVSVlanMtuHealthCheckConfig -property @{enable=0}),(New-Object
Vmware.Vim.VMwareDVSTeamingHealthCheckConfig -property @{enable=0})))}
```

4 Log in to the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure to reconfigure the virtual switches and port groups for the shared edge and compute cluster.

Configure Advanced Security Settings on the vCenter Server Instances for Compliance with PCI in Region A

You enable SSL for the Network File Copy function and configure the password length for the built-in `vpxuser`.

When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server sfo01m01vc01.sfo01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00437` Enable SSL for the Network File Copy function.

```
New-AdvancedSetting -Entity  sfo01m01vc01.sfo01.rainpole.local -Name config.nfc.useSSL -Value true
```

3 `PCI-VI-VC-CFG-00427`Change the length of the password for the built-in `vpxuser` account to `32` characters.

```
New-AdvancedSetting -Entity sfo01m01vc01.sfo01.rainpole.local -Name
config.vpxd.hostPasswordLength -Value 32
```

4 Log in to the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure for the shared edge and compute cluster.

Configure Alerts in vCenter Server for Compliance with PCI in Region A

You configure alerts to system administrators and ISSO personas for all audit failure events and to inform them for every operation that adds, modifies, or deletes permissions in the vsphere.local domain.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Hosts and clusters** inventory, select the **sfo01mo1vc01.sfo01.rainpole.local** vCenter Server instance.

3 Click the **Configure** tab and under **More**, select **Alarm Definitions**.

4 PCI-VI-VC-CFG-00412,PCI-VI-VC-CFG-00414,PCI-VI-VC-CFG-00416 Click **Add** to configure alerts for audit failure events for every operation that adds, modifies, or deletes permissions in the vsphere.local domain.

a On the **Name and targets** page, enter the settings and click **Next**.

Setting	Value
Alarm name	vim.event.PermissionsAll
Target type	vCenter Server

b On the **Alarm rule 1** page, under **If**, enter **`vim.event.PermissionAddedEvent`** as a trigger and press Enter.

c Configure the remaining settings for the alarm and click **Add another rule**.

Setting	Value
Trigger the alarm and	Show as warning
Send email notifications	Off
Send SNMP traps	On
Run script	Off

d Configure two more rules and follow the prompts to finish the wizard.

Table 3-2. Alarm Rule 2

Setting	Value
If (trigger)	vim.event.PermissionRemovedEvent
Trigger the alarm and	Show as warning

Table 3-3. Alarm Rule 3

Setting	Value
If (trigger)	vim.event.PermissionUpdatedEvent
Trigger the alarm and	Show as warning

5 PCI-VI-VC-CFG-00442 Configure an alert if an error occurs with the ESXi remote syslog connection.

a Click **Add** to open the **New alarm definition** wizard.

b On the **Name and targets** page, enter the settings and click **Next**.

Setting	Value
Alarm name	esx.problem.vmsyslogd.remote.failure
Target type	vCenter Server

c On the **Alarm rule 1** page, under **If**, enter **esx.problem.vmsyslogd.remote.failure** as a trigger and press Enter.

d Configure the remaining settings for the alarm, click **Next**, and follow the prompts to finish the wizard.

Setting	Value
Trigger the alarm and	Show as warning
Send email notifications	Off
Send SNMP traps	On
Run script	Off

6 Repeat the procedure for the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server in Region A.

Configure Sessions Expiration for the vSphere Web Client and the vSphere Client for Compliance with PCI in Region A

You configure sessions in the vSphere Web Client and vSphere Client to expire after 10 minutes of inactivity.

Procedure

1 Log in to vCenter Server by using a Secure Shell (SSH) client.

Setting	Value
FQDN	sfo01m01vc01.sfo01.rainpole.local
User name	root
Password	*vcenter_server_root_password*

2 `PCI-VI-VC-CFG-00422` Run the commands so that the vSphere Web Client and the vSphere Client terminate sessions after 15 minutes of user inactivity and restart the service.

```
sed -i 's/session.timeout = 120/session.timeout = 15/' /etc/vmware/vsphere-client/
webclient.properties

service-control --stop vsphere-client
service-control --start vsphere-client

sed -i 's/session.timeout = 120/session.timeout = 15/' /etc/vmware/vsphere-ui/webclient.properties

service-control --stop vsphere-ui
service-control --start vsphere-ui
```

3 Log in to the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure.

Restrict the Use of the Virtual Machine Console for Compliance with PCI in Region A

You configure settings to minimize the use of the Virtual Machine console by removing the privilege to use the virtual machine console for the standard virtual machine user role. You can assign the `Virtual Machine console user` role to a user if they require console access. You configure the privilege on the Management vCenter Server in Region A and the setting is populated for the entire vsphere.local domain.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00061`Remove the privilege to use the virtual machine console for the standard virtual machine user role.

a On the **Home** page of the vSphere Client, click **Administration** , and click **Roles**.

b From the **Roles provider** drop-down menu, select **sfo01m01vc01.sfo01.rainpole.local**.

c Select the **Virtual machine user (sample)** role and click **Edit role action**.

d In the **Edit Role** dialog box, select the **Virtual machine** group and under **Interaction**, deselect the **Console interaction** check box.

e Click **Next** and click **Finish**.

Configure Advanced Settings on All Management Virtual Machines for Compliance with PCI in Region A

Disable unexposed features, drag and drop operations, copy and paste operations, shared salt values, console access, unused display features, sending host information to virtual machines, limit sharing of console connections, limit the VMX configuration file size, and audit all uses of PCI or PCIe passthrough functionalities by using PowerCLI commands.

You perform the procedure on all management virtual machines in Region A to comply with multiple configurations. You must also perform the procedure for management virtual machines that you add to the SDDC in the future.

Table 3-4. Configurations to Perform

Configuration ID	Description
`PCI-VI-VC-CFG-00070`	Disable copy operations.
`PCI-VI-VC-CFG-00071`	Disable drag and drop operations.
`PCI-VI-VC-CFG-00072`	Disable all GUI functionalies for copy and paste operations.
`PCI-VI-VC-CFG-00073`	Disable paste operations.

Table 3-4. Configurations to Perform (continued)

Configuration ID	Description
PCI–VI–VC–CFG–00074	Disable virtual disk shrinking.
PCI –VI–VC–CFG–00075	Disable virtual disk erasure.
PCI –VI–VC–CFG–00076	Disable Host Guest File System (HGFS) file transfers.
PCI–VI–VC–CFG–00077	Disable the `isolation.tools.ghi.autologon.disable` feature.
PCI–VI–VC–CFG–00078	Disable the `isolation.bios.bbs.disable` feature.
PCI –VI–VC–CFG–00079	Disable the `isolation.tools.getCreds.disable` feature.
PCI –VI–VC–CFG–00080	Disable the`isolation.tools.ghi.launchmenu.change` feature.
PCI –VI–VC–CFG–00081	Disable the`isolation.tools.memSchedFakeSampleStats.disable` feature.
PCI –VI–VC–CFG–00082	Disable the `isolation.tools.ghi.protocolhandler.info.disable` feature.
PCI –VI–VC–CFG–00083	Disable the `isolation.ghi.host.shellAction.disable` feature.
PCI –VI–VC–CFG–00084	Disable the`isolation.tools.dispTopoRequest.disable` feature.
PCI –VI–VC–CFG–00085	Disable the`isolation.tools.trashFolderState.disable` feature.
PCI –VI–VC–CFG–00086	Disable the `isolation.tools.ghi.trayicon.disable` feature.
PCI –VI–VC–CFG–00087	Disable the`isolation.tools.unity.disable` feature.
PCI –VI–VC–CFG–00088	Configure unexposed feature keyword `isolation.tools.unityInterlockOperation.disable` feature.
PCI –VI–VC–CFG–00089	Disable the `isolation.tools.unity.push.update.disable` feature.
PCI –VI–VC–CFG–00090	Disable the `isolation.tools.unity.taskbar.disable` feature.
PCI –VI–VC–CFG–00091	Disable the `isolation.tools.unityActive.disable` feature.
PCI –VI–VC–CFG–00092	Disable the `isolation.tools.unity.windowContents.disable` feature.
PCI –VI–VC–CFG–00093	Disable the `isolation.tools.vmxDnDVersionGet.disable` feature.
PCI –VI–VC–CFG–00094	Disable the `isolation.tools.guestDnDVersionSet.disable` feature.
PCI –VI–VC–CFG–00095	Disable VIX messages from the VM.
PCI –VI–VC–CFG–00096	Limit the sharing of console connections.
PCI –VI–VC–CFG–00097	Disable console access through the Virtual Network Computing protocol.
PCI –VI–VC–CFG–00098	Disable tools auto install.
PCI –VI–VC–CFG–00099	Limit informational messages from the VM to the VMX file.
PCI –VI–VC–CFG–00101	Prevent unauthorized removal, connection and modification through the `isolation.device.connectable.disable` parameter.

Table 3-4. Configurations to Perform (continued)

Configuration ID	Description
PCI –VI–VC–CFG–00100	Prevent unauthorized removal, connection and modification of devices through the **isolation.device.edit.disable** parameter.
PCI –VI–VC–CFG–00102	Restrict sending host information to guests.
PCI –VI–VC–CFG–00555	Disable unused display features.
PCI –VI–VC–CFG–00561	Audit all uses of PCI or PCIe passthrough functionalities.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server sfo01m01vc01.sfo01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Run the script to configure advanced settings on all management virtual machines.

```
$AdvancedSettingsTrue
=("svga.vgaonly","isolation.bios.bbs.disable","isolation.device.connectable.disable","isolation.de
vice.edit.disable","isolation.ghi.host.shellAction.disable","isolation.tools.autoInstall.disable",
"isolation.tools.diskShrink.disable","isolation.tools.diskWiper.disable","isolation.tools.dispTopo
Request.disable","isolation.tools.dnd.disable","isolation.tools.getCreds.disable","isolation.tools
.ghi.autologon.disable","isolation.tools.ghi.launchmenu.change","isolation.tools.ghi.protocolhandl
er.info.disable","isolation.tools.ghi.trayicon.disable","isolation.tools.guestDnDVersionSet.disabl
e","isolation.tools.hgfsServerSet.disable","isolation.tools.memSchedFakeSampleStats.disable","isol
ation.tools.paste.disable","isolation.tools.copy.disable","isolation.tools.trashFolderState.disabl
e","isolation.tools.unity.disable","isolation.tools.unity.push.update.disable","isolation.tools.un
ity.taskbar.disable","isolation.tools.unity.windowContents.disable","isolation.tools.unityActive.d
isable","isolation.tools.unityInterlockOperation.disable","isolation.tools.vixMessage.disable","is
olation.tools.vmxDnDVersionGet.disable")
$AdvancedSettingsFalse =
("isolation.tools.setGUIOptions.enable","RemoteDisplay.vnc.enabled","tools.guestlib.enableHostInfo
","pciPassthru*.present")
$VMs
=("sfo01m01vc01","sfo01m01psc01","sfo01w01vc01","sfo01w01psc01","vrslcm01svr01a","vrops01svr01a","
vrops01svr01b","vrops01svr01c","sfo01vropsc01a","sfo01vropsc01b","sfo01vrli01a","sfo01vrli01b","sf
o01vrli01c","sfo01umds01","vra01svr01a","vra01svr01b","vra01svr01c","vra01iws01a","vra01iws01b","v
ra01ims01a","vra01ims01b","vra01dem01a","vra01dem01b","sfo01ias01a","sfo01ias01b","vrb01svr01","sf
o01vrbc01","vra01mssql01","sfo01m01srm01","sfo01m01vrms01","sfo01sky01")
Foreach ($vm in $VMs){
    Foreach ($advancedSetting in $AdvancedSettingsTrue) {
        $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -
Property Name, Value
        if(!$setting.Name){
            Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value true -Confirm:$false
        }
        else{
```

```
            Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
true -Confirm:$false
        }
    }
    Foreach ($advancedSetting in $AdvancedSettingsFalse) {
        $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -
Property Name, Value
        if(!$setting.Name){
            Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value false -Confirm:$false
        }
        else{
            Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
false -Confirm:$false
        }
    }
    $advancedSetting = "RemoteDisplay.maxConnections"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -Property
Name, Value
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 1 -Confirm:$false
    }
    else{
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value 1 -
Confirm:$false
    }
    $advancedSetting = "tools.setinfo.sizeLimit"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -Property
Name
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 1048576 -Confirm:$false
    }
    else{
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
1048576 -Confirm:$false
    }
}
```

Set SDDC Deployment Details on the vCenter Server Instances for Compliance with PCI in Region A

Update the identity of your SDDC deployment on vCenter Server. You use this identity as a label in tools for automated SDDC deployment.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Global Inventory Lists** inventory, click **vCenter Servers**.

3 Click the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

4 Under **Settings**, click **Advanced Settings** and click **Edit settings**.

5 In the **Edit advanced vCenter Server Settings** dialog box, enter the settings and click **Add**.

Setting	Value
Name	config.SDDC.Deployed.ComplianceKit
Value	PCI

6 Click **Save** to close the window.

7 Repeat the procedure for the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server in Region A.

Restrict the Connectivity Between vSAN Health Check and Public Hardware Compatibility List for Compliance with PCI in Region A

You configure a proxy server to restrict the connectivity between vSAN Health Check and public Hardware Compatibility List.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 PCI `–VI–VC–CFG–00418,PCI–VI–Storage–SDS–CFG–00207` Configure a proxy for the download of the public Hardware Compatibility List.

   a In the **Hosts and Clusters** inventory, select the **sfo01m01vc01.sfo01.rainpole.local** vCenter Server object.

   b Click the **Configure** tab and under **vSAN**, click **Internet Connectivity**.

   c On the **Internet connectivity** page, click **Edit**.

   d Select **Configure the Proxy Server if your system uses one** check box.

   e Enter the proxy server details and click **Apply**.

3 Repeat the procedure for the `sfo01w01vc01.sfo01.rainpole.local` Compute vCenter Server in Region A.

Configure the NSX Data Center for vSphere Instances for Compliance with PCI in Region A

Perform the procedures to secure your NSX Data Center for vSphere instances.

Procedure

1 Configure the NSX Distributed Firewall to Only Allow Outbound Network Traffic that Contains Legitimate Data for Compliance with PCI in Region A

Configure the NSX Distributed Firewall to deny outbound IP packets that contain an illegitimate address in the source address field. You perform the procedure only for the `172.16.11.66` NSX Manager for the shared edge and compute cluster in Region A.

2 Configure NSX Distributed Firewall to Generate Audit Records for Compliance with PCI in Region A

Configure the NSX Distributed Firewall to generate Audit Records. You perform the procedure for the two NSX Manager nodes in Region A.

3 Disable the SSH Service on the NSX Manager Instances for Compliance with PCI in Region A

You must disable the SSH service on both NSX Manager instances to decrease security risks in your SDDC.

Configure the NSX Distributed Firewall to Only Allow Outbound Network Traffic that Contains Legitimate Data for Compliance with PCI in Region A

Configure the NSX Distributed Firewall to deny outbound IP packets that contain an illegitimate address in the source address field. You perform the procedure only for the `172.16.11.66` NSX Manager for the shared edge and compute cluster in Region A.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Networking and Security** inventory, click **SpoofGuard**.

3 `PCI-VI-NET-CFG-00324` Enable the preconfigured spoof guard default policy.

a On the **SpoofGuard** page, select the **172.16.11.66 Primary** NSX Manager, select the **Default policy**, and click **Edit**.

b In the **Edit Policy** dialog box, turn on the **Enable** toggle switch and click **Finish**.

Configure NSX Distributed Firewall to Generate Audit Records for Compliance with PCI in Region A

Configure the NSX Distributed Firewall to generate Audit Records. You perform the procedure for the two NSX Manager nodes in Region A.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo01m01vc01.sfo01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Networking and Security** inventory, click **Firewall**.

3 `PCI-VI-NET-CFG-00323` Enable logging for all firewall rules.

   a On the **Firewall** page, select the **172.16.11.65 Primary** NSX Manager.

   b On the **General** tab, click **More > Expand all sections** and turn on all toggle switches in the **Log** column to enable logging for all firewall rules.

   c Click the **Ethernet** tab, click **More > Expand all sections**, and turn on all toggle switches in the **Log** column to enable logging for all firewall rules.

   d Click **Publish**.

4 Repeat the procedure for the `172.16.11.66` NSX Manager for the shared edge and compute cluster in Region A.

Disable the SSH Service on the NSX Manager Instances for Compliance with PCI in Region A

You must disable the SSH service on both NSX Manager instances to decrease security risks in your SDDC.

Procedure

1 In a Web browser, log in to the NSX Manager by using the administration interface.

Setting	Value
URL	https://sfo01m01nsx01.sfo01.rainpole.local
User name	admin
Password	*nsx_manager_admin_password*

2 Disable the SSH service on the NSX Manager instance for the management cluster.

   a On the **Home** page, click **View summary**.

   b On the **Summary** tab, under **System-level components**, click **Stop** to disable the SSH service.

3 Repeat the procedure for the `sfo01w01nsx01.sfo01.rainpole.local` NSX Manager for the shared edge and compute cluster in Region A.

Region B Virtual Infrastructure Configuration for Compliance with PCI

4

Perform the procedures to secure your virtual infrastructure.

Configure ESXi Hosts for Compliance with PCI in Region B

Perform the procedures to secure your ESXi hosts.

Configure the SSH Service on the ESXi Hosts for Compliance with PCI in Region B

You must edit the `/etc/ssh/sshd_config` file on all your hosts to reconfigure the SSH service. You also remove the `authorized_keys` file on all ESXi hosts and edit the `/etc/pam.d/passwd` file to configure password settings. Before you can log in to a host and change the configuration file, you must disable lockdown mode.

You perform the procedure on all ESXi hosts in Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Disable lockdown mode on the lax01m01esx01.sfo01.rainpole.local host.

   a In the **Hosts and Clusters** inventory, expand the entire **lax01m01vc01.lax01.rainpole.local** tree.

   b Under the **lax01-m01dc** data center, select the **lax01m01esx01.lax01.rainpole.local** host object and click the **Configure** tab.

   c Click the **Security Profile** tab on the right.

   d Under **Lockdown Mode**, click **Edit**.

   e In the **Lockdown Mode** dialog box, select **Disabled** and click **OK**.

3 Log in to the `lax01m01esx01.sfo01.rainpole.local` ESXi host by using a Secure Shell (SSH) client.

Setting	Value
FQDN	lax01m01esx01.lax01.rainpole.local
User name	root
Password	*root_user_password*

4 Rename the existing `sshd_config` file for backup.

```
mv /etc/ssh/sshd_config /etc/ssh/sshd_config.backup
```

5 Create a new `sshd_config` file in the `/etc/ssh` folder with the PCI configurations.

Table 4-1. Configurations to Perform

Configuration ID	Description
PCI-VI-ESXI-CFG-00001	Use only FIPS-approved algorithms for encryption.
PCI-VI-ESXI-CFG-00003	Set the `IgnoreRhosts` option to **yes** to force users to enter a password when authenticating with SSH.
PCI-VI-ESXI-CFG-00004	Set the `HostbasedAuthentication` option to **no** to disable authentication through trusted hosts.
PCI-VI-ESXI-CFG-00005	Set the `PermitRootLogin` option to **no** to disable SSH access for the root user.
PCI-VI-ESXI-CFG-00006	Set the `PermitEmptyPasswords` option to *no* to prevent users with blank password from using SSH.
PCI-VI-ESXI-CFG-00007	Set the `PermitUserEnvironment` option to **no** to forbid users presenting environment options to the SSH deamon.
PCI-VI-ESXI-CFG-00009	Set the `GSSAPIAuthentication` option to **no** to disable GSSAPI authentication.
PCI-VI-ESXI-CFG-00010	Set the `KerberosAuthentication` to **no** to disable the Kerberos protocol.
PCI-VI-ESXI-CFG-00011	Set the `StrictModes` option to **yes** to force permissions checks on keyfiles and directories.
PCI-VI-ESXI-CFG-00012	Set the `Compression` option to **no** to deny compression proir to a successful user authentication.
PCI-VI-ESXI-CFG-00013	Set the `GatewayPorts` option to **no** to prevent connecting to forwarded ports from outside the host.
PCI-VI-ESXI-CFG-00015	Delete all values for `AcceptEnv` to reject environment variables from the client.
PCI-VI-ESXI-CFG-00016	Set the `PermitTunnel` option to **no** to prevent the SSH daemon the ability to create network tunnels over an SSH connection.

Table 4-1. Configurations to Perform (continued)

Configuration ID	Description
PCI-VI-ESXI-CFG-00017	Set the `ClientAliveCountMax` option to **3** as the total number of checkalive messages sent by the SSH server without response by the SSH client.
PCI-VI-ESXI-CFG-00019	Set the `MaxSessions` option to **1** as the maximum number of open sessions permitted per network connection.

a Open the VI editor to add a new `sshd_config` file in `/etc/ssh`.

```
vi /etc/ssh/sshd_config
```

b In the VI editor, enter the configurations to the `sshd_config` file.

```
# Version 6.7.2.0
# running from inetd
# Port 2200

HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,aes192-cbc,aes256-cbc
Protocol 2
IgnoreRhosts yes
HostbasedAuthentication no
PermitRootLogin no
PermitEmptyPasswords no
PermitUserEnvironment no
MACs hmac-sha1,hmac-sha2-256,hmac-sha2-512
GSSAPIAuthentication no
KerberosAuthentication no
StrictModes yes
Compression no
GatewayPorts no
X11Forwarding no
AcceptEnv
PermitTunnel no
ClientAliveCountMax 3
ClientAliveInterval 200
MaxSessions 1
UsePrivilegeSeparation no
SyslogFacility auth
LogLevel info
PrintMotd yes
PrintLastLog no
TCPKeepAlive yes
Banner /etc/issue
```

c Save and close the VI editor.

d Restart the SSH service to apply the new configurations.

```
/etc/init.d/SSH restart
```

6 `PCI-VI-ESXI-CFG-00107` Remove the SSH authorized_keys file from `/etc/ssh/keys-root/`.

```
rm /etc/ssh/keys-root/authorized_keys
```

7 `PCI-VI-ESXI-CFG-00109` Configure the value of the **remember** option to `4` in the `/etc/pam.d/passwd` file to restrict the reuse of the last five passwords.PCI

a Open the VI editor to to edit the `/etc/pam.d/passwd` file.

```
vi /etc/pam.d/passwd
```

b Add **remember=4** at the end of the `password sufficient` line in the file.

```
password sufficient /lib/security/$ISA/pam_unix.so use_authtok nullok shadow
sha512 remember=4
```

c Save and close the VI editor.

8 Repeat the procedure for all remaining hosts in Region B.

Configure Advanced Settings on the ESXi Hosts for Compliance with PCI in Region B

You perform the procedure on all ESXi hosts to configure firewall settings, password policy, inactivity and availability timeouts, and failed login attempts. Also configure a core dump collector, login banners for the Direct Console User Interface (DCUI) and SSH Connections, disable warnings, and enable Bridge Protocol Data Unit (BPDU) filter by using PowerCLI commands.

To perform the procedure, you first connect to the Management vCenter Server and then connect to the Compute vCenter server to perform the procedure on the ESXi hosts that belong to the Compute vCenter server. When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure. Use the values from the table for the respective vCenter Server instance that you configure.

Setting	Value for the Management vCenter Server	Value for the Compute vCenter Server
`esxcli.network.firewall.ruleset.allowedip.add` in step Step 12	172.17.11.0/24	172.17.31.0/24
`vCenterIP` in step Step 13	172.17.11.62	172.17.11.64

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server lax01m01vc01.lax01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 PCI-VI-ESXI-CFG-00043 Run the command to enable the Bridge Protocol Data Unit filter.

```
Get-VMHost | Get-AdvancedSetting -Name Net.BlockGuestBPDU | Set-AdvancedSetting -Value 1
```

3 PCI-VI-ESXI-CFG-00034 Set the maximum number of failed login attempts before an account is locked to 6.

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-AdvancedSetting
-Value 6
```

4 PCI-VI-ESXI-CFG-00022 Configure the ESXi password policy so that passwords contain 4 character classes and no less than 7 characters.

```
Get-VMHost | Get-AdvancedSetting -Name Security.PasswordQualityControl | Set-
AdvancedSetting -Value "similar=deny retry=3 min=disabled,disabled,disabled,disabled,7"
```

5 PCI-VI-ESXI-CFG-00038 Configure the inactivity timeout to automatically terminate idle shell sessions to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Set-
AdvancedSetting -Value 900
```

6 PCI-VI-ESXI-CFG-00039 When SSH or appliance shell is enabled, allow 900 seconds for log in before the service is automatically disabled.

a Configure timeout to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellTimeOut | Set-AdvancedSetting -Value
900
```

b Restart the SSH service for the changes to take effect.

```
$service = Get-VMHost | Get-VMHostService | where {$_.key -eq 'tsm'}
Restart-VMHostService $service
```

7 PCI-VI-ESXI-CFG-000165 After a user exceeds the maximum allowed failed login attempts, set a lockout timer to temporarily prevent further login attempts.

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountUnlockTime | Set-AdvancedSetting -Value
1800
```

8 PCI-VI-ESXI-CFG-00168 Configure the timeout to automatically terminate idle DCUI connections to 900 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.DcuiTimeOut | Set-AdvancedSetting -Value 900
```

9 PCI-VI-ESXI-CFG-00030 Show warnings in the vSphere Client if local or remote shell sessions are enabled on the ESXi host.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.SuppressShellWarning | Set-AdvancedSetting
-Value 0
```

10 PCI-VI-ESXI-CFG-00122 Configure the login banner for the DCUI of the ESXi host.

```
Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage | Set-AdvancedSetting -Value
"This system is for the use of authorized users only. Individuals using this computer system
without authority or in excess of their authority are subject to having all their activities on
this system monitored and recorded by system personnel. Anyone using this system expressly
consents to such monitoring and is advised that if such monitoring reveals possible evidence of
criminal activity system personal may provide the evidence of such monitoring to law enforcement
officials."
```

11 PCI-VI-ESXI-CFG-00123 Configure the login banner for the SSH connections.

```
Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue | Set-AdvancedSetting -Value "This system
is for the use of authorized users only. Individuals using this computer system without authority
or in excess of their authority are subject to having all their activities on this system
monitored and recorded by system personnel. Anyone using this system expressly consents to such
monitoring and is advised that if such monitoring reveals possible evidence of criminal activity
system personal may provide the evidence of such monitoring to law enforcement officials."
```

12 PCI-VI-ESXI-CFG-00028 Configure the ESXi host firewall to only allow traffic from the ESXi management network.

Use the respective value for `esxcli.network.firewall.ruleset.allowedip.add` when you perform the procedure on the Compute vCenter Server.

```
$EsxiHosts = Get-VMHost
foreach($EsxiHost in $EsxiHosts){
$esxcli = Get-EsxCli -VMHost $EsxiHost.Name
#This disables the allow all rule for the target service
$esxcli.network.firewall.ruleset.set($false,$true,"sshServer")
$esxcli.network.firewall.ruleset.allowedip.add("172.17.11.0/24","sshServer")}
```

13 PCI-VI-ESXI-CFG-00056, PCI-VI-Storage-SDS-CFG-00562 Configure a core dump collector.

Use the respective value for `vCenterIP` when you perform the procedure on the Compute vCenter Server.

```
$vCenterIP = '172.16.11.62'
foreach ($VMHost in Get-VMHost) {
$esxcli = Get-EsxCli -VMHost $VMHost.Name
$esxcli.system.coredump.network.set($null,"vmk0",$null,$vCenterIP,6500)
$esxcli.system.coredump.network.set(1)
$esxcli.system.coredump.network.get()
}
```

14 Log in to the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server and repeat the procedure for the remaining hosts in Region B.

Restrict the Access to All ESXi Hosts for Compliance with PCI in Region B

You restrict remote access to the host by disabling the SSH service and the shell service and enabling lockdown mode.

You perform the procedure on all the ESXi hosts in Region B. To perform the procedure, you first connect to the Management vCenter Server and then connect to the Compute vCenter Server to perform the procedure on all the ESXi hosts that belong to the Computer vCenter Server. When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server lax01m01vc01.lax01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-ESXI-CFG-00111` Stop and disable the SSH service.

```
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "SSH"} | Set-VMHostService -Policy Off
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "SSH"} | Stop-VMHostService
```

3 `PCI-VI-ESXI-CFG-00112` Stop and disable the ESXi shell service.

```
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"} | Set-VMHostService -Policy Off
Get-VMHost | Get-VMHostService | Where {$_.Label -eq "ESXi Shell"} | Stop-VMHostService
```

4 `PCI-VI-ESXI-CFG-00031` Enable `Normal` lockdown mode.

```
$level = "lockdownNormal"
$EsxiHosts = Get-VMHost
foreach($EsxiHost in $EsxiHosts)
{$vmhost = $EsxiHost | Get-View
$lockdown = Get-View $vmhost.ConfigManager.HostAccessManager
$lockdown.ChangeLockdownMode($level) }
```

5 Log in to the `lax01w01vc01.sfo01.rainpole.local` Compute vCenter Server and repeat the procedure for the remaining hosts in Region B.

Configure vCenter Server and vSAN for Compliance with PCI in Region B

Perform the procedures to secure your vCenter Server instances.

Configure Password Policy and Lockout Policy Settings in vCenter Server for Compliance with PCI in Region B

You configure password policy and lockout policy settings on the Management vCenter Server for the entire `vsphere.local` domain.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Configure the password policies.

a From the **Home** menu of the vSphere Client, click **Administration**.

b In the Navigator, under Single Sign-On, click **Configuration**.

c On the **Policies** tab, under **Password policy**, click **Edit**.

d In the **Edit password policies** dialog box, configure the password policies and click **SAVE**.

Configuration ID	Setting	Value
`PCI-VI-VC-CFG-00421`	Maximum lifetime	90
`PCI-VI-VC-CFG-00410`	Minimum length	7

3 Configure the lockout policies.

a On the **Policies** tab, click **Lockout Policy** and click **Edit**.

b In the **Edit lockout policies** dialog box, configure the settings and click **Save**.

Configuration ID	Setting	Value
`PCI-VI-VC-CFG-00436`	Maximum number of failed login attempts	6
`PCI-VI-VC-CFG-00434`	Time interval between failuresper	900 Seconds
`PCI-VI-VC-CFG-00435`	Unlock time	0 seconds

Configure the Security Policies for Virtual Switches and Virtual Port Groups for Compliance with PCI in Region B

Restrict port-level configuration overrides on port groups and disable health check on the distributed switches.

You perform the procedure for all the distributed switches and port groups in Region B. To perform the procedure, you first connect to the Management vCenter Server.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server lax01m01vc01.lax01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00440` Restrict port-level configuration overrides on all existing port groups.

```
$pgs = Get-VDPortgroup | Get-View
ForEach($pg in $pgs){
$spec = New-Object VMware.Vim.DVPortgroupConfigSpec
$spec.configversion = $pg.Config.ConfigVersion
$spec.Policy = New-Object VMware.Vim.VMwareDVSPortgroupPolicy
$spec.Policy.VendorConfigOverrideAllowed = $False
$spec.Policy.BlockOverrideAllowed = $False
$spec.Policy.PortConfigResetAtDisconnect = $True
$pg.ReconfigureDVPortgroup_Task($spec)}
```

3 `PCI-VI-VC-CFG-00411` Disable the health check on all distributed switches.

```
Get-View -ViewType DistributedVirtualSwitch | ?{($_.config.HealthCheckConfig | ?{$_.enable -
notmatch "False"})}| %{$_.UpdateDVSHealthCheckConfig(@((New-Object
Vmware.Vim.VMwareDVSVlanMtuHealthCheckConfig -property @{enable=0}),(New-Object
Vmware.Vim.VMwareDVSTeamingHealthCheckConfig -property @{enable=0})))}
```

4 Log in to the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server and repeat the procedure to reconfigure the virtual switches and port groups for the shared edge and compute cluster.

Configure Advanced Security Settings on the vCenter Server Instances for Compliance with PCI in Region B

You enable SSL for the Network File Copy function and configure the password length for the built-in `vpxuser`.

When you run commands, on the prompts to specify the object of a command, enter `[A] Yes to All` to run a task on all hosts that belong to the vCenter Server instance that you configure.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server lax01m01vc01.lax01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00437` Enable SSL for the Network File Copy function.

```
New-AdvancedSetting -Entity  lax01m01vc01.lax01.rainpole.local -Name config.nfc.useSSL -Value true
```

3 `PCI-VI-VC-CFG-00427`Change the length of the password for the built-in `vpxuser` account to `32` characters.

```
New-AdvancedSetting -Entity lax01m01vc01.lax01.rainpole.local -Name
config.vpxd.hostPasswordLength -Value 32
```

4 Log in to the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server and repeat the procedure for the shared edge and compute cluster.

Configure Alerts in vCenter Server for Compliance with PCI in Region B

You configure alerts to system administrators and ISSO personas for all audit failure events and to inform them for every operation that adds, modifies, or deletes permissions in the vsphere.local domain. Perform the procedure from the vSphere Web Client.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Hosts and clusters** inventory, select the **lax01mo1vc01.lax01.rainpole.local** vCenter Server instance.

3 Click the **Configure** tab and under **More**, select **Alarm Definitions**.

4 PCI-VI-VC-CFG-00412,PCI-VI-VC-CFG-00414,PCI-VI-VC-CFG-00416 Click **Add** to configure alerts for audit failure events for every operation that adds, modifies, or deletes permissions in the vsphere.local domain.

a On the **Name and targets** page, enter the settings and click **Next**.

Setting	Value
Alarm name	vim.event.PermissionsAll
Target type	vCenter Server

b On the **Alarm rule 1** page, under **If**, enter **`vim.event.PermissionAddedEvent`** as a trigger and press Enter.

c Configure the remaining settings for the alarm and click **Add another rule**.

Setting	Value
Trigger the alarm and	Show as warning
Send email notifications	Off
Send SNMP traps	On
Run script	Off

d Configure two more rules and follow the prompts to finish the wizard.

Table 4-2. Alarm Rule 2

Setting	Value
If (trigger)	vim.event.PermissionRemovedEvent
Trigger the alarm and	Show as warning

Table 4-3. Alarm Rule 3

Setting	Value
If (trigger)	vim.event.PermissionUpdatedEvent
Trigger the alarm and	Show as warning

5 PCI-VI-VC-CFG-00442 Configure an alert if an error occurs with the ESXi remote syslog connection.

a Click **Add** to open the **New alarm definition** wizard.

b On the **Name and targets** page, enter the settings and click **Next**.

Setting	Value
Alarm name	esx.problem.vmsyslogd.remote.failure
Target type	vCenter Server

c On the **Alarm rule 1** page, under **If**, enter **esx.problem.vmsyslogd.remote.failure** as a trigger and press Enter.

d Configure the remaining settings for the alarm, click **Next**, and follow the prompts to finish the wizard.

Setting	Value
Trigger the alarm and	Show as warning
Send email notifications	Off
Send SNMP traps	On
Run script	Off

6 Repeat the procedure for the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server in Region B.

Configure Sessions Expiration for the vSphere Web Client and the vSphere Client for Compliance with PCI in Region B

You configure sessions in the vSphere Web Client and vSphere Client to expire after 10 minutes of inactivity.

Procedure

1 Log in to vCenter Server by using a Secure Shell (SSH) client.

Settings	Value
FQDN	lax01m01vc01.lax01.rainpole.local
User name	root
Password	*vcenter_server_root_password*

2 `PCI-VI-VC-CFG-00422` Run the commands so that the vSphere Web Client and the vSphere Client terminate sessions after 15 minutes of user inactivity and restart the service.

```
sed -i 's/session.timeout = 120/session.timeout = 15/' /etc/vmware/vsphere-client/
webclient.properties

service-control --stop vsphere-client
service-control --start vsphere-client

sed -i 's/session.timeout = 120/session.timeout = 15/' /etc/vmware/vsphere-ui/webclient.properties

service-control --stop vsphere-ui
service-control --start vsphere-ui
```

3 Log in to the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server and repeat the procedure.

Restrict the Use of the Virtual Machine Console for Compliance with PCI in Region B

You configure settings to minimize the use of the Virtual Machine console by removing the privilege to use the virtual machine console for the standard virtual machine user role. You can assign the `Virtual Machine console user` role to a user if they require console access.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00061`Remove the privilege to use the virtual machine console for the standard virtual machine user role.

   a On the **Home** page of the vSphere Client, click **Administration** , and click **Roles**.

   b From the **Roles provider** drop-down menu, select **sfo01m01vc01.sfo01.rainpole.local**.

   c Select the **Virtual machine user (sample)** role and click **Edit role action**.

   d In the **Edit Role** dialog box, select the **Virtual machine** group and under **Interaction**, deselect the **Console interaction** check box.

   e Click **Next** and click **Finish**.

3 Repeat the procedure for the lax01w01vc01.lax01.rainpole.local vCenter Server instance.

Configure Advanced Settings on All Management Virtual Machines for Compliance with PCI in Region B

Disable unexposed features, drag and drop operations, copy and paste operations, shared salt values, console access, unused display features, sending host information to virtual machines, limit sharing of console connections, limit the VMX configuration file size, and audit all uses of PCI or PCIe passthrough functionalities by using PowerCLI commands.

You perform the procedure on all management virtual machines in Region B to comply with multiple configurations. You must also perform the procedure for management virtual machines that you add to the SDDC in the future.

Table 4-4. Configurations to Perform

Configuration ID	Description
`PCI-VI-VC-CFG-00070`	Disable copy operations.
`PCI-VI-VC-CFG-00071`	Disable drag and drop operations.
`PCI-VI-VC-CFG-00072`	Disable all GUI functionalies for copy and paste operations.

Table 4-4. Configurations to Perform (continued)

Configuration ID	Description
PCI–VI–VC–CFG–00073	Disable paste operations.
PCI–VI–VC–CFG–00074	Disable virtual disk shrinking.
PCI–VI–VC–CFG–00075	Disable virtual disk erasure.
PCI–VI–VC–CFG–00076	Disable Host Guest File System (HGFS) file transfers.
PCI–VI–VC–CFG–00077	Disable the `isolation.tools.ghi.autologon.disable` feature.
PCI–VI–VC–CFG–00078	Disable the `isolation.bios.bbs.disable` feature.
PCI–VI–VC–CFG–00079	Disable the `isolation.tools.getCreds.disable` feature.
PCI–VI–VC–CFG–00080	Disable the`isolation.tools.ghi.launchmenu.change` feature.
PCI–VI–VC–CFG–00081	Disable the`isolation.tools.memSchedFakeSampleStats.disable` feature.
PCI–VI–VC–CFG–00082	Disable the `isolation.tools.ghi.protocolhandler.info.disable` feature.
PCI–VI–VC–CFG–00083	Disable the `isolation.ghi.host.shellAction.disable` feature.
PCI–VI–VC–CFG–00084	Disable the`isolation.tools.dispTopoRequest.disable` feature.
PCI –VI–VC–CFG–00085	Disable the`isolation.tools.trashFolderState.disable` feature.
PCI–VI–VC–CFG–00086	Disable the `isolation.tools.ghi.trayicon.disable` feature.
PCI–VI–VC–CFG–00087	Disable the`isolation.tools.unity.disable` feature.
PCI–VI–VC–CFG–00088	Configure unexposed feature keyword `isolation.tools.unityInterlockOperation.disable` feature.
PCI–VI–VC–CFG–00089	Disable the `isolation.tools.unity.push.update.disable` feature.
PCI–VI–VC–CFG–00090	Disable the `isolation.tools.unity.taskbar.disable` feature.
PCI–VI–VC–CFG–00091	Disable the `isolation.tools.unityActive.disable` feature.
PCI–VI–VC–CFG–00092	Disable the `isolation.tools.unity.windowContents.disable` feature.
PCI–VI–VC–CFG–00093	Disable the `isolation.tools.vmxDnDVersionGet.disable` feature.
PCI–VI–VC–CFG–00094	Disable the `isolation.tools.guestDnDVersionSet.disable` feature.
PCI–VI–VC–CFG–00095	Disable VIX messages from the VM.
PCI–VI–VC–CFG–00096	Limit the sharing of console connections.
PCI–VI–VC–CFG–00097	Disable console access through the Virtual Network Computing protocol.
PCI–VI–VC–CFG–00098	Disable tools auto install.
PCI–VI–VC–CFG–00099	Limit informational messages from the VM to the VMX file.
PCI–VI–VC–CFG–00101	Prevent unauthorized removal, connection and modification through the `isolation.device.connectable.disable` parameter.

Table 4-4. Configurations to Perform (continued)

Configuration ID	Description
PCI–VI–VC–CFG–00100	Prevent unauthorized removal, connection and modification of devices through the **isolation.device.edit.disable** parameter.
PCI–VI–VC–CFG–00102	Restrict sending host information to guests.
PCI–VI–VC–CFG–00555	Disable unused display features.
PCI–VI–VC–CFG–00561	Audit all uses of PCI or PCIe passthrough functionalities.

Procedure

1 Log in to the Management vCenter Server by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server lax01m01vc01.lax01.rainpole.local -Protocol https
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Run the script to configure advanced settings on all management virtual machines.

```
$AdvancedSettingsTrue
=("svga.vgaonly","isolation.bios.bbs.disable","isolation.device.connectable.disable","isolation.de
vice.edit.disable","isolation.ghi.host.shellAction.disable","isolation.tools.autoInstall.disable",
"isolation.tools.diskShrink.disable","isolation.tools.diskWiper.disable","isolation.tools.dispTopo
Request.disable","isolation.tools.dnd.disable","isolation.tools.getCreds.disable","isolation.tools
.ghi.autologon.disable","isolation.tools.ghi.launchmenu.change","isolation.tools.ghi.protocolhandl
er.info.disable","isolation.tools.ghi.trayicon.disable","isolation.tools.guestDnDVersionSet.disabl
e","isolation.tools.hgfsServerSet.disable","isolation.tools.memSchedFakeSampleStats.disable","isol
ation.tools.paste.disable","isolation.tools.copy.disable","isolation.tools.trashFolderState.disabl
e","isolation.tools.unity.disable","isolation.tools.unity.push.update.disable","isolation.tools.un
ity.taskbar.disable","isolation.tools.unity.windowContents.disable","isolation.tools.unityActive.d
isable","isolation.tools.unityInterlockOperation.disable","isolation.tools.vixMessage.disable","is
olation.tools.vmxDnDVersionGet.disable")
$AdvancedSettingsFalse =
("isolation.tools.setGUIOptions.enable","RemoteDisplay.vnc.enabled","tools.guestlib.enableHostInfo
","pciPassthru*.present")
$VMs
=("lax01m01vc01","lax01m01psc01","lax01w01vc01","lax01w01psc01","vrslcm01svr01a","vrops01svr01a","
vrops01svr01b","vrops01svr01c","lax01vropsc01a","lax01vropsc01b","lax01vrli01a","lax01vrli01b","la
x01vrli01c","lax01umds01","vra01svr01a","vra01svr01b","vra01svr01c","vra01iws01a","vra01iws01b","v
ra01ims01a","vra01ims01b","vra01dem01a","vra01dem01b","lax01ias01b","lax01ias01a","vrb01svr01","la
x01vrbc01","lax01m01srm01","lax01m01vrms01")
Foreach ($vm in $VMs){
    Foreach ($advancedSetting in $AdvancedSettingsTrue) {
        $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -
Property Name, Value
        if(!$setting.Name){
            Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value true -Confirm:$false
        }
        else{
```

```
            Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
true -Confirm:$false
        }
    }
    Foreach ($advancedSetting in $AdvancedSettingsFalse) {
        $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -
Property Name, Value
        if(!$setting.Name){
            Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value false -Confirm:$false
        }
        else{
            Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
false -Confirm:$false
        }
    }
    $advancedSetting = "RemoteDisplay.maxConnections"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -Property
Name, Value
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 1 -Confirm:$false
    }
    else{
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value 1 -
Confirm:$false
    }
    $advancedSetting = "tools.setinfo.sizeLimit"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object -Property
Name
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 1048576 -Confirm:$false
    }
    else{
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting -Value
1048576 -Confirm:$false
    }
}
```

Set SDDC Deployment Details on the vCenter Server Instances for Compliance with PCI in Region B

Update the identity of your SDDC deployment on vCenter Server. You use this identity as a label in tools for automated SDDC deployment.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Global Inventory Lists** inventory, click **vCenter Servers**.

3 Click the **lax01m01vc01.lax01.rainpole.local** vCenter Server object and click the **Configure** tab in the central pane.

4 Under **Settings**, click **Advanced Settings** and click **Edit settings**.

5 In the **Edit advanced vCenter Server Settings** dialog box, enter the settings and click **Add**.

Setting	Value
Name	config.SDDC.Deployed.ComplianceKit
Value	PCI

6 Click **Save** to close the window.

7 Repeat the procedure for the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server in Region B.

Restrict the Connectivity Between vSAN Health Check and Public Hardware Compatibility List for Compliance with PCI in Region B

You configure a proxy server to restrict the connectivity between vSAN Health Check and public Hardware Compatibility List.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 `PCI-VI-VC-CFG-00418`,`PCI-VI-Storage-SDS-CFG-00207` Configure a proxy for the download of the public Hardware Compatibility List.

   a In the **Hosts and Clusters** inventory, select the **lax01m01vc01.lax01.rainpole.local** vCenter Server object.

   b Click the **Configure** tab and under **vSAN**, click **Internet Connectivity**.

   c On the **Internet connectivity** page, click **Edit**.

   d Select **Configure the Proxy Server if your system uses one** check box.

   e Enter the proxy server details and click **Apply**.

3 Repeat the procedure for the `lax01w01vc01.lax01.rainpole.local` Compute vCenter Server in Region B.

Configure the NSX Data Center for vSphere Instances for Compliance with PCI in Region B

Perform the procedures to secure your NSX Data Center for vSphere instances.

Configure the NSX Distributed Firewall to Only Allow Outbound Network Traffic that Contains Legitimate Data for Compliance with PCI in Region B

Configure the NSX Distributed Firewall to deny outbound IP packets that contain an illegitimate address in the source address field. You perform the procedure only for the `172.17.11.66` NSX Manager for the shared edge and compute cluster in Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **Networking and Security** inventory, click **SpoofGuard**.

3 `PCI-VI-NET-CFG-00324` Enable the preconfigured spoof guard default policy.

   a On the **SpoofGuard** page, select the **172.17.11.66 Secondary** NSX Manager, select the **Default policy**, and click **Edit**.

   b In the **Edit Policy** dialog box, turn on the **Enable** toggle switch and click **Finish**.

Configure NSX Distributed Firewall to Generated Audit Records for Compliance with PCI in Region B

Configure the NSX Distributed Firewall to generate Audit Records. You perform the procedure for the two NSX Manager nodes in Region B.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Settings	Value
URL	https://lax01m01vc01.lax01.rainpole.local/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 From the **Menu** of the vSphere Client, select **Networking and Security**.

3 In the **Navigator**, select **Firewall**.

4 `PCI-VI-NET-CFG-00323` Enable the log for each Firewall rule.

   a On the **Firewall** page, select the **172.17.11.65 Secondary** NSX Manager, Under **General**, Expand each Firewall rule's section, turn on the **Enable** toggle switch under **Log** for all the Firewall Rules.

   b Repeat the same step under **Ethernet** and click **PUBLISH**.

5 Repeat this procedure for the `172.17.11.66 Secondary` NSX Manager for the shared edge and compute cluster in Region B.

Disable the SSH Service on the NSX Manager Instances for Compliance with PCI in Region B

You must disable the SSH service on both NSX Manager instances to decrease security risks in your SDDC.

Procedure

1 In a Web browser, log in to the NSX Manager for the management cluster by using the administration interface.

Settings	Value
URL	https://lax01m01nsx01.lax01.rainpole.local
User name	admin
Password	*nsx_manager_admin_password*

2 Disable the SSH service on the NSX Manager instance for the management cluster.

   a On the **Home** page, click **View summary**.

   b On the **Summary** tab, under **System-level components**, click **Stop** to disable the SSH service.

3 Repeat the procedure for the `lax01w01nsx01.lax01.rainpole.local` NSX Manager for the shared edge and compute cluster in Region B.