Security and Compliance Configuration for VMware Cloud Foundation 5.2

23 JUL 2024

VMware Cloud Foundation 5.2

vmware by Broadcom

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

https://docs.vmware.com/

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

Contents

About Security and Compliance Configuration for VMware Cloud Foundation 5.2

Security and Compliance Configuration for VMware Cloud Foundation provides general guidance and step-by-step configuration for securing the management and workload domains in your VMware Cloud Foundation environment towards compliance with the NIST 800-53 standard. This guide is validated for the management workload domain and VI workload domains for VMware Cloud Foundation 5.2.

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

Security and Compliance Configuration for VMware Cloud Foundation 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.

Required VMware Software

The *Security and Compliance Configuration for VMware Cloud Foundation* documentation is compliant and with certain product versions. See *VMware Cloud Foundation Release Notes* for more information about supported product versions.

Update History

This *Security and Compliance Configuration for VMware Cloud Foundation* is updated with each release of the product or when necessary.

Revision	Description
23 JULY 2024	Initial release.

Software Requirements

1

To configure your VMware Cloud Foundation instance for compliance, you must download and license additional VMware and third-party software.

Security and Compliance Configuration for VMware Cloud Foundation 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 1-1. Additional Software Required for *Security and Compliance Configuration for VMware Cloud Foundation*

Product Group	Script/Tool	Description
VMware PowerCLI	Supported OS for VMware PowerCLI	Operating system that supports Microsoft PowerShell and VMware PowerCLI. For more information on supported operating systems, seeVMware PowerCLI User's Guide.
VMware vSAN	Native Key Provider (NKP) or Key Management Server (KMS)	If you are not using Native Key Provider (NKP) for encryption, Deploy and configure Key Management Server (KMS). Key Management Servers are developed and released by security and cloud vendors for encryption in virtualized environments. You use a Key Management Server to activate the encryption of vSAN storage. For a list of supported Key Management Server , see KMS list. Refer to the Key Management Server vendor documentation for setup and configuration instructions. Ensure that all encryption keys are available across regions to activate decryption in case of a region fail over.

Table 1-1. Additional Software Required for *Security and Compliance Configuration for VMware Cloud Foundation* (continued)

Product Group	Script/Tool	Description
VMware vSAN	Proxy server	vSAN uses an external proxy server to connect to the Internet to download the Hardware Compatibility List.
VMware NSX	SFTP server	Space for NSX Manager backups must be available on an SFTP server. The NSX Manager instances must have connection to the remote SFTP server.

Table 1-2. VMware Scripts and Tools Required for *Security and Compliance Configuration for VMware Cloud Foundation*

Product Group	Script/Tool	Download Location	Description
VMware vSphere	VMware PowerCLI	n/a	VMware PowerCLI contains modules of cmdlets based on Microsoft PowerShell for automating vSphere, VMware VMware NSX, and others. VMware PowerCLI provides a PowerShell interface to the VMware product APIs.

Securing ESXi Hosts

2

You perform procedures on the ESXi hosts in all your workload domains by using different interfaces, such as PowerCLI, ESXi Shell, and the vSphere Client.

Procedure

1 Security Best Practices for Securing ESXi Hosts

You must follow multiple best practices at all times when you operate your ESXi hosts.

2 Configure Multiple Security Settings on the ESXi Hosts by Using the ESXi Shell

You activate secure boot on all the ESXi hosts.

3 Configure Multiple Security Settings on the ESXi Hosts by Using PowerCLI

You perform the procedure on all ESXi hosts in all your workload domains to configure firewall settings, password policy, inactivity timeouts, failed login attempts, start up policies, join ESXi hosts to Active Directory domain, and remove ESX Admin group membership. Also, configure login banners for the Direct Console User Interface (DCUI) and SSH connections, deactivate warnings, configure persistent log location, remote logging, implement secure boot enforcement, enable TPM-based configuration encryption, enable audit logging, alocate storage record capacity, and activate bidirectional CHAP authentication by using PowerCLI commands.

4 Configure Multiple Security Settings on Unassigned ESXi Hosts by Using PowerCLI

You perform this procedure on all unassigned ESXi hosts in the SDDC inventory to configure non-native VLAN ID, Virtual Guest Tagging (VGT), and unreserved VLAN ID on all the port groups on the standard switch.

5 Activate Normal Lockdown Mode on the ESXi Hosts

You activate normal lockdown mode on the ESXi hosts.

Security Best Practices for Securing ESXi Hosts

You must follow multiple best practices at all times when you operate your ESXi hosts.

Table 2-1. Security Best Practices for Securing ESXi Hosts

Best Practice	Description
Add only system accounts to the ESXi exception users list. VMW-ESXI-00125	You can add users to the exception users list from the vSphere Client. These user accounts 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 exception users list. Adding unnecessary users to the exception list defeats the purpose of lockdown mode.
Install security patches and updates for ESXi hosts. VMW-ESXI-00129	You install all security patches and updates on the ESXi hosts as soon as the update bundles are available in SDDC Manager. Do not apply patches to ESXi manually or by using vSphere Update Manager or VMware vCenter Lifecycle Manager in a VMware Cloud Foundation environment unless directed to do so by support. If you patch the environment without using SDDC Manager, it can not only lead to a less-secure environment, but may cause issues with automated upgrades or actions in the future.
The ESXi host must protect the confidentiality and integrity of transmitted information by protecting ESXi management traffic. VMW-ESXI-00178	The vSphere management network provides access to the vSphere management interface on each component. Services running on the management interface provide an opportunity for an attacker to gain privileged access to the systems. Any remote attack most likely would begin with gaining entry to this network. The Management VMkernel port group must be on a dedicated VLAN. The Management VLAN must not be shared by any other function and must not be accessible to anything other than management-related functions such as vCenter.
The ESXi host must use approved certificates. VMW-ESXI-01113	The default self-signed, VMCA-issued host certificate must be replaced with a certificate from a trusted Certificate Authority (CA) when the host is accessed directly, such as during a virtual machine (VM) console connection.

Configure Multiple Security Settings on the ESXi Hosts by Using the ESXi Shell

You activate secure boot on all the ESXi hosts.

You perform the procedure from an ESXi Shell session connected to the ESXi host and on all ESXi hosts in the respective workload domain.

Procedure

1 Log in to an ESXi host by using ESXi Shell as **root**.

2 VMW-ESXI-01108 Activate secure boot on the host.

```
/usr/lib/vmware/secureboot/bin/secureBoot.py -c
```

If the output indicates that secure boot cannot be activated, correct the discrepancies and try again. Once all discrepancies are resolved, the server ESXi is installed on can be updated to enable Secure Boot in the firmware.

To enable Secure Boot in the server's firmware, follow the instructions for the specific manufacturer.

3 Perform the procedure on the remaining hosts in the current and any other workload domains.

Configure Multiple Security Settings on the ESXi Hosts by Using PowerCLI

You perform the procedure on all ESXi hosts in all your workload domains to configure firewall settings, password policy, inactivity timeouts, failed login attempts, start up policies, join ESXi hosts to Active Directory domain, and remove ESX Admin group membership. Also, configure login banners for the Direct Console User Interface (DCUI) and SSH connections, deactivate warnings, configure persistent log location, remote logging, implement secure boot enforcement, enable TPM-based configuration encryption, enable audit logging, alocate storage record capacity, and activate bidirectional CHAP authentication by using PowerCLI commands.

To perform the procedure on the ESXi hosts for a workload domain, you connect to the vCenter Server for the respective workload domain. To run a task on all hosts for the domain, when you run commands, on the prompts to specify the object of a command, enter **`[A] Yes to all`**.

Procedure

1 Log in to the vCenter Server for the workload domain you want to reconfigure by using a PowerCLI console.

Setting	Value
Command	Connect-VIServer -Server *management-domain-vcenter-server-fqdn* -Protocol https
User name	administrator@vsphere.local

2 VMW-ESXI-00022 Configure the password complexity policy for the ESXi host.

The requirement is a length of minimum 15 characters (maximum of 64 characters) from 4 character classes that include lowercase letters, uppercase letters, numbers, special characters. Password difference is also mandatory.

```
Get-VMHost | Get-AdvancedSetting -Name Security.PasswordQualityControl | Set-
AdvancedSetting -Value "similar=deny retry=3 min=disabled,disabled,disabled,disabled,15
max=64"
```

3 VMW-ESXI-00028 Configure the ESXi hosts firewall to only allow traffic from the authorized management networks.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
#This disables the allow all rule for the target service.The sshServer service is the
target in this example.
$arguments = $esxcli.network.firewall.ruleset.set.CreateArgs()
$arguments.rulesetid = "sshServer"
$arguments.allowedall = $false
$esxcli.network.firewall.ruleset.set.Invoke($arguments)

#Next add the allowed IPs for the service. Note that executing the "vSphere Web Client"
service this way may disable access but may be done through vCenter or through the console.
$arguments = $esxcli.network.firewall.ruleset.allowedip.add.CreateArgs()
$arguments.rulesetid = "sshServer"
$arguments.ipaddress = "Site-specific networks"
$esxcli.network.firewall.ruleset.allowedip.add.Invoke($arguments)}
```

Note This must be done for each user-configurable enabled service.

4 VMW-ESXI-00034 Set the maximum number of failed login attempts before an account is locked to 3.

```
Get-VMHost | Get-AdvancedSetting -Name Security.AccountLockFailures | Set-AdvancedSetting
-Value 3
```

5 VMW-ESXI-00038 Configure the inactivity timeout to automatically close idle shell sessions to 600 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellInteractiveTimeOut | Set-
AdvancedSetting -Value 600
```

6 VMW-ESXI-00039 Configure the timeout to automatically stop ESXi shell and SSH services to 600 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.ESXiShellTimeOut | Set-AdvancedSetting
-Value 600
```

7 VMW-ESXI-00114 To eliminate the need to create and maintain multiple local user accounts, join ESXi hosts to an Active Directory (AD) domain.

```
Get-VMHost | Get-VMHostAuthentication | Set-VMHostAuthentication -JoinDomain -Domain
"domain name" -User "username" -Password "password"
```

Note If any local user accounts exist, apart from **root** and local service accounts, you can delete the local user accounts by going to the ESXi host UI **Manage > Security & Users > Users**.

8 VMW-ESXI-00122 Configure the login banner for the DCUI of the ESXi host.

```
Get-VMHost | Get-AdvancedSetting -Name Annotations.WelcomeMessage | Set-AdvancedSetting
-Value "Site-Specific banner text"
```

9 VMW-ESXI-00123 Configure the login banner for the SSH connections.

```
Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue | Set-AdvancedSetting -Value "Site-
Specific banner text"
```

10 VMW-ESXI-00136 Configure a persistent log location for all locally stored logs.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logDir | Set-AdvancedSetting -Value
“New Log Location”
```

Note Specify the log location as `[datastorename] path_to_file`, where the path is relative to the root of the volume, backing the datastore. For example, the path `[storage1] /systemlogs` maps to the path `/vmfs/volumes/storage1/systemlogs`.

The new location should not include a subfolder as enabling audit logging will create a folder and will fail if a subfolder is specified.

11 VMW-ESXI-00137 For a host added to Active Directory, use an Active Directory group instead of the default **ESX Admins** group for the *esxAdminsGroup* property on the ESXi hosts.

```
Get-VMHost | Get-AdvancedSetting -Name Config.HostAgent.plugins.hostsvc.esxAdminsGroup |
Set-AdvancedSetting -Value site specifc AD_Group
```

Note Changing the group name does not remove the permissions of the previous group.

12 VMW-ESXI-00164 Configure a remote log server for the ESXi hosts.

Note Use the following format when adding the remote log server. You can enter multiple, comma-separated values.

udp://*<IP/FQDN>*:514

tcp://*<IP/FQDN>*:514

ssl://*<IP/FQDN>*:1514

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logHost | Set-AdvancedSetting -Value
"<site-specific syslog server hostname>"
```

13 VMW-ESXI-00564 Configure idle session timeout for the ESXi host client to 600 seconds.

```
Get-VMHost | Get-AdvancedSetting -Name UserVars.HostClientSessionTimeout | Set-
AdvancedSetting -Value "600"
```

14 VMW-ESXI-01102 Activate bidirectional CHAP authentication for iSCSI traffic.

```
Get-VMHost | Get-VMHostHba | Where {$_.Type -eq "iscsi"} | Set-VMHostHba -ChapType Required
-ChapName chap_name -ChapPassword password -MutualChapEnabled $true -MutualChapName mutual_chap_name
-MutualChapPassword mutual_password
```

15 VMW-ESXI-01121 Activate strict x509 verification for SSL syslog endpoints.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.certificate.strictX509Compliance |
Set-AdvancedSetting -Value "true"
```

16 VMW-ESXI-01122 Activate volatile key destruction on the host.

```
Get-VMHost | Get-AdvancedSetting -Name Mem.MemEagerZero | Set-AdvancedSetting -Value "1"
```

17 VMW-ESXI-01123 Configure the host with an appropriate maximum password age.

```
Get-VMHost | Get-AdvancedSetting -Name Security.PasswordMaxDays | Set-AdvancedSetting
-Value "90"
```

18 VMW-ESXI-01124 Enable TPM-based configuration encryption.

- Ensure the TPM 2.0 chip is enabled in the BIOS and the ESX UI does not show any errors.
- This setting cannot be configured until the TPM is properly enabled in firmware.
- Configuration encryption uses the physical TPM at install or upgrade time. If the TPM is added or enabled later, you must reconfigure the ESXi host to use the newly available TPM. After you enable TPM configuration encryption is enabled, you cannot disable it.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
$arguments = $esxcli.system.settings.encryption.set.CreateArgs()
$arguments.mode="TPM"
$esxcli.system.settings.encryption.set.Invoke($arguments)
}
```

You must evacuate the host and gracefully reboot for changes to take effect.

19 VMW-ESXI-01125 The ESXi host must implement Secure Boot enforcement.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
$arguments = $esxcli.system.settings.encryption.set.CreateArgs()
$arguments.requiresecureboot =$true
$esxcli.system.settings.encryption.set.Invoke($arguments)
}
```

You must evacuate the host and gracefully reboot for changes to take effect.

20 VMW-ESXI-01126 Configure the startup policy for the CIM service on the host to "off".

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

21 VMW-ESXI-01128 Deactivate the startup policy for the SNMP service on the host.

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

22 VMW-ESXI-01152 The ESXi host must disable virtual hardware management network interfaces.

```
Get-VMHost | Get-AdvancedSetting -Name Net.BMCNetworkEnable | Set-AdvancedSetting -Value 0
```

23 VMW-ESXI-01141 The ESXi host must allocate audit record storage capacity to store audit records.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.storageCapacity | Set-
AdvancedSetting -Value 100
```

24 VMW-ESXI-01142 ESXi host must enable audit logging.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.storageEnable | Set-
AdvancedSetting -Value "true"
```

VMW-ESXI-00136 and VMW-ESXI-01141 must be configured and validated before enabling audit logging.

25 VMW-ESXI-01143 ESXi host must off-load audit records via syslog.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.auditRecord.remoteEnable | Set-
AdvancedSetting -Value "true"
```

26 VMW-ESXI-01145 ESXi host must forward audit records containing information to establish what type of events occurred.

```
Get-VMHost | Get-AdvancedSetting -Name Syslog.global.logLevel | Set-AdvancedSetting -Value
"info"
```

27 VMW-ESXI-01150 The ESXi host must deny shell access for the dcui account.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
$arguments = $esxcli.system.account.set.CreateArgs()
$arguments.id = "dcui"
$arguments.shellaccess = "false"
$esxcli.system.account.set.invoke($arguments)
}
```

28 VMW-ESXI-01153 ESXi host must enforce the exclusive running of executables from approved VIBs.

```
Get-VMHost | Get-AdvancedSetting -Name VMkernel.Boot.execInstalledOnly | Set-
AdvancedSetting -Value True
```

29 VMW-ESXI-01154 Configure ESXi host to use approved encryption to protect the confidentiality of network sessions.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
$arguments = $esxcli.system.tls.server.set.CreateArgs()
$arguments.profile = "NIST_2024"
$esxcli.system.tls.server.set.invoke($arguments)
}
```

A reboot is required to complete the process of changing profiles.

Configure Multiple Security Settings on Unassigned ESXi Hosts by Using PowerCLI

You perform this procedure on all unassigned ESXi hosts in the SDDC inventory to configure non-native VLAN ID, Virtual Guest Tagging (VGT), and unreserved VLAN ID on all the port groups on the standard switch.

These controls apply only to unassigned hosts in VMware Cloud Foundation. An unassigned host is a host that is commissioned but not assigned to a workload domain. Once the host is added to a VMware Cloud Foundation workload domain, the standard switch on the host is removed and the host is added to a distributed switch.

The following configurations address ESXi standard switches only. Distributed switches are addressed in the Securing vCenter Server section (see Chapter 3 Securing vCenter Server). If your environment does not have ESXi hosts with standard switches, you can skip this procedure.

Procedure

1 Log in to the unassigned ESXi host you want to reconfigure by using a PowerCLI console and provide the credentials.

```
Connect-VIServer -Server host-fqdn -Protocol https
```

2 VMW-ESXI-01104 Do not configure the port groups on standard switches to VLAN 4095 unless Virtual Guest Tagging (VGT) is required.

```
Get-VirtualPortGroup -Name "portgroup name" | Set-VirtualPortGroup -VLanId "New VLAN#"
```

Activate Normal Lockdown Mode on the ESXi Hosts

You activate normal lockdown mode on the ESXi hosts.

Procedure

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

Setting	Value
URL	https://*vcenter-server-fqdn*/ui
User name	administrator@vsphere.local

2 `VMW-ESXI-00031` Activate normal lockdown mode on a host.

a In the **Hosts and clusters** inventory, select an ESXi host.

b Click **Configure**.

c Under **System**, select **Security profile**.

d In the **Lockdown mode** panel, click **Edit**.

e In the **Lockdown mode** dialog box, select the **Normal** or **Strict** radio button and click **OK**.

Note In strict lockdown mode, the Direct Console User Interface (DCUI) service is stopped. If the connection to vCenter Server is lost and the vSphere Client is no longer available, the ESXi host becomes inaccessible.

3 Repeat the procedure for all ESXi hosts in all workload domains.

Securing vCenter Server

3

You perform procedures on the vCenter Server in all your workload domains using different interfaces: PowerCLI and vSphere Client.

Procedure

1 Security Best Practices for Securing vCenter Server

You must follow multiple best practices at all times when you operate your vCenter Server instances.

2 Configure Security Settings for vCenter Server from the vSphere Client

You perform the procedure on all vCenter Server instances to configure password policies, lockout policies, alarms, proxy, login banners, LDAP, and other configurations.

3 Configure Security Settings for vCenter Server by Using PowerCLI

To configure host password length, native VLAN, reserved VLAN, and VGT, you perform the procedure on all vCenter Servers instances.

4 Configure Security Settings on the vCenter Server Appliance

You configure a syslog server and configure backups for vCenter Server from the vCenter Server Appliance Management Interface.

Security Best Practices for Securing vCenter Server

You must follow multiple best practices at all times when you operate your vCenter Server instances.

Table 3-1. Security Best Practices for Securing vCenter Server

Best Practice	Description
Assign correct roles to vCenter Server users. VMW-VC-00415	Users and service accounts must be assigned only privileges they require. To reduce risk of confidentiality, availability, or integrity loss, the least privilege principle requires that these privileges must be assigned only if needed.
Use unique service accounts for applications that connect to vCenter Server. VMW-VC-00401	Create a service account for each application that connects to vCenter Server. Grant only the required permissions for the application to run.

Table 3-1. Security Best Practices for Securing vCenter Server (continued)

Best Practice	Description
vCenter Server must restrict access to cryptographic permissions. VMW-VC-01211	These permissions must be reserved for cryptographic administrators where VM and/or vSAN encryption is in use. Catastrophic data loss can result from a poorly administered cryptography. Only the Administrator and any site-specific cryptographic group must have the following permissions: ■ **Cryptographic Operations privileges** ■ **Global.Diagnostics** ■ **Host.Inventory.Add host to cluster** ■ **Host.Inventory.Add standalone host** ■ **Host.Local operations.Manage user groups**
The vCenter Server must use LDAPS when adding an SSO identity source. VMW-VC-01229	To protect the integrity of LDAP communications, secure LDAP (LDAPS) must be explicitly configured when adding an LDAP identity source in vSphere SSO. When configuring an identity source and supplying an SSL certificate, vCenter Server enforces secure LDAP.
The vCenter Server must implement Active Directory authentication VMW-VC-01228	The vCenter Server must ensure users are authenticated with an individual authenticator prior to using a group authenticator. Using Active Directory for authentication provides more robust account management capabilities.
Backup the vCenter Native Key Providers with a strong password. VMW-VC-01239	The vCenter Native Key Provider acts as a key provider for encryption based capabilities, such as encrypted virtual machines, without requiring an external KMS solution. When activating this feature, a backup PCKS#12 file is created. If no password is provided during the backup process, the backup file can be used maliciously and compromise the environment.
Restrict access to the cryptographic role. VMW-VC-01210	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 or vSAN encryption is required. All other vSphere administrators, who do not require cryptographic operations, must be assigned the **No cryptography administrator** role.
The vCenter Server Machine SSL certificate must be issued by an appropriate certificate authority. VMW-VC-01205	The default self-signed, VMCA-issued vCenter reverse proxy certificate must be replaced with an approved certificate. The use of an approved certificate on the vCenter reverse proxy and other services assures clients that the service they are connecting to is legitimate and trusted.
Ensure that port mirroring is used legitimately. VMW-VC-01248	The vSphere VDS can mirror traffic from one port to another, allowing observation of traffic. Ensure that port mirroring is used legitimately.

Table 3-1. Security Best Practices for Securing vCenter Server (continued)

Best Practice	Description
Install security patches and updates for vCenter Server. VMW-VC-01253	You install all security patches and updates on vCenter Server instances as soon as possible. An attacker can exploit known vulnerabilities when attempting to attain access or elevate privileges. Mitigate the risk of breaches by updating vCenter Server instances first and then updating ESXi hosts.
Configure Key Encryption Keys (KEKs) to be re-issued at regular intervals for the vSAN encrypted datastores. VMW-VC-01213	Interview the SA to determine whether a procedure exists to perform a shallow re-key of all vSAN encrypted datastores at regular, site-defined intervals. This interval must be defined by the SA and the ISSO. If vSAN encryption is not in use, this is not applicable.
At a minimum, vCenter must provide an immediate, real-time alert to the system administrator (SA) and information system security officer (ISSO) of all audit failure events requiring real-time alerts. VMW-VC-01254	Ensure that the Central Logging Server is configured to alert the SA and ISSO, at a minimum, on any AO-defined events. Otherwise, this is a finding. If there are no AO-defined events, this is not a finding.
Remove unnecessary virtual hardware devices from the VM. VMW-VC-01257	Ensure that no device is connected to a virtual machine if it is not required. For example, serial and parallel ports are rarely used for virtual machines in a datacenter environment, and CD/DVD drives are usually connected only temporarily during software installation. USB devices, sound cards, and other unnecessary hardware may be introduced with migrations from VMware Workstation, Fusion, or through other tools. Any enabled or connected device represents a potential attack channel, through the possibility of device drivers that contain vulnerabilities, by granting the ability to introduce software or exfiltrate data to or from a protected environment. Note: Removing the CD-ROM device may impact VMware Tools installation and maintenance.
vCenter is a version that has not reached End of General Support status. VMW-VC-01256	Ensure that vCenter Server is of a version that has not reached End of General Support status.

Table 3-1. Security Best Practices for Securing vCenter Server (continued)

Best Practice	Description
vCenter must separate authentication and authorization for administrators. VMW-VC-01261	Many organizations do both authentication and authorization using a centralized directory service such as Active Directory. Attackers who compromise an identity source can often add themselves to authorization groups, and simply log into systems they should not otherwise have access to. Additionally, reliance on central identity systems means that the administrators of those systems are potentially infrastructure administrators, too, as they can add themselves to infrastructure access groups at will. The use of local SSO groups for authorization helps prevent this avenue of attack by allowing the centralized identity source to still authenticate users but moving authorization into vCenter itself.
The vCenter Server must configure the firewall to only allow traffic from authorized networks. VMW-VC-01276	Ensures that all incoming and outgoing network traffic is blocked unless explicitly allowed, reducing the attack surface and helping to prevent unauthorized access to the system. Note that outgoing/egress traffic is not blocked, nor are related/established connections, so vCenter Server will still be able to communicate with systems where it initiates the connection. Perimeter firewalls should be used to curtail those types of connections.

Configure Security Settings for vCenter Server from the vSphere Client

You perform the procedure on all vCenter Server instances to configure password policies, lockout policies, alarms, proxy, login banners, LDAP, and other configurations.

Procedure

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

Setting	Value
URL	https://*management-domain-vcenter-server-fqdn*/ui
User name	administrator@vsphere.local

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 **Local accounts** tab, under **Password policy**, click **Edit**.

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

Configuration ID	Setting	Value
VMW-VC-00421	Maximum lifetime	60
VMW-VC-00410	Minimum Length	15
VMW-VC-01269	Maximum Length	64

3 Configure the lockout policies.

a On the **Local accounts** tab, under **Lockout policy**, click **Edit**.

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

Configuration ID	Setting	Value
VMW-VC-00436	Maximum number of failed login attempts	3
VMW-VC-00434	Time interval between failures	900 seconds
VMW-VC-00435	Unlock time	0 seconds

4 VMW-VC-01219 Configure an alert for the appropriate personnel about SSO account actions

a In the **Hosts and clusters** inventory, select the vCenter Server that manages the ESXi host you configure.

b Click the **Configure** tab, select **Alarm definitions** under **Security**.

c Click **Add**.

The **New alarm definition** wizard opens.

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

Setting	Value
Alarm name	SSO account actions - com.vmware.sso.PrincipalManagement
Target type	vCenter Server

e On the **Alarm rule 1** page, under **If**, enter **`com.vmware.sso.PrincipalManagement`** as a trigger and press Enter.

f 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

5 `VMW-VC-01209` Configure a login message.

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

b Navigate to **Single sign-on > Configuration**.

c Click the **Login message** tab and click **Edit**.

d Activate the **Show login message** toggle.

e In the **Login message** text box, enter the login message.

f Activate the **Consent checkbox** toggle.

g In the **Details of login message** text box, enter the site-specific banner text and click **Save**.

6 `VMW-VC-01212` Configure Mutual CHAP for vSAN iSCSI targets.

a In the **Hosts and Clusters** inventory, select the vSAN-enabled cluster.

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

c In the **vSAN iSCSI target service** tile, click **Enable**.

d Activate the service from the toggle switch.

e From the **Authentication** drop-down menu, select **Mutual CHAP**

f Configure the incoming and outgoing users and secrets appropriately and click **Apply**.

7 Set SDDC deployment details on the vCenter Server instances.

a In the **Global inventory lists** inventory, click **vCenter Servers**.

b Click the vCenter Server object and click the **Configure** tab in the central pane.

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

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

Setting	Value
Name	config.SDDC.Deployed.ComplianceKit
Value	VCF-NIST-800-53

8 VMW-VC-00422 vCenter Server must terminate vSphere Client sessions after 10 minutes of inactivity.

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

b Under **Deployment**, click **Client configuration**.

c Click **Edit**, for **Session timeout** , enter **10** minutes, and click **Save**.

9 VMW-VC-01216 vCenter must limit membership to the SystemConfiguration.BashShellAdministrators SSO group.

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

b Under **Single sign-on**, click **Users and Groups** and **Groups**.

c Click **> next page arrow** until **SystemConfiguration.BashShellAdministrators** appears.

d Click **SystemConfiguration.BashShellAdministrators** and click three vertical dots next to the name of each unauthorized account and click **Remove Member** and click **Remove**.

Note By default the Administrator and a unique service account similar to "vmware-applmgmtservice-714684a4-342f-4eff-a232-cdc21def00c2" will be in the group and should not be removed.

10 VMW-VC-01217 vCenter must limit membership to the TrustedAdmins SSO group.

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

b Under **Single sign-on**, click **Users and Groups** and **Groups**.

c Click **> next page arrow** until **TrustedAdmins** appears.

d Click **TrustedAdmins** and click three vertical dots next to the name of each unauthorized account and click **Remove Member** and click **Remove**.

Note These accounts act as root on the Photon operating system and have the ability to severely damage vCenter, inadvertently or otherwise.

11 VMW-VC-01274 The vCenter Server must disable accounts used for Integrated Windows Authentication (IWA).

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

b Under **Single sign-on**, click **Users and Groups** and **Users**.

c Change the domain to **vSphere.local** and

d Select **K/M** and **krbtgt/VSPHERE.LOCAL** accounts and click **More** and select **Disable** and click **OK**.

e Repeat Step d with **krbtgt/VSPHERE.LOCAL** account

12 VMW-VC-01267 vCenter must require authentication for published content libraries.

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

b Click on the target content library and click **Edit Settings** under **Actions**.

c Click the checkbox to **Enable user authentication for access to this content library**, and enter and confirm**password** and click **OK**.

Note Any subscribed content libraries will need to be updated to enable authentication and provide the password.

13 VMW-VC-01268 vCenter must enable the OVF security policy for content libraries.

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

b Click on the target content library and click **Edit Settings** under **Actions**.

c Click the checkbox to **Apply Security Policy**, and click **OK**.

Note If you disable the security policy of a content library, you cannot reuse the existing OVF items.

Configure Security Settings for vCenter Server by Using PowerCLI

To configure host password length, native VLAN, reserved VLAN, and VGT, you perform the procedure on all vCenter Servers instances.

Procedure

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

Setting	Value
Command	Connect-VIServer -Server *management-domain-vcenter-server-fqdn* -Protocol https
User name	administrator@vsphere.local

2 VMW-VC-01201 Configure all port groups to a value different from the value of the native VLAN.

```
Get-VDPortgroup "portgroup name" | Set-VDVlanConfiguration -VlanId "New VLAN#"
```

3 VMW-VC-01202 Configure all port groups to VLAN values not reserved by upstream physical switches

```
Get-VDPortgroup "portgroup name" | Set-VDVlanConfiguration -VlanId "New VLAN#"
```

4 VMW-VC-01227 Do not configure VLAN trunking in vCenter Server unless Virtual Guest Tagging (VGT) is required and authorized.

a (Optional) If you use VLAN ranges, enter VLAN ranges with a comma separated value to configure trunking.

```
Get-VDPortgroup "Portgroup Name" | Set-VDVlanConfiguration -VlanTrunkRange "<VLAN
Range(s) comma separated>"
```

b (Optional) If you use a single VLAN, enter a single VLAN ID to configure trunking.

```
Get-VDPortgroup "Portgroup Name" | Set-VDVlanConfiguration -VlanId "<New VLAN#>"
```

5 VMW-VC-01247 Services that may be unnecessary should be disabled such as CDP or LLDP network discovery protocols.

```
Get-VDSwitch -Name "DSwitch" | Set-VDSwitch -LinkDiscoveryProtocolOperation "Disabled"
```

6 VMW-VC-01265 vCenter must reset port configuration when virtual machines are disconnected.

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

7 VMW-VC-01266 vCenter must not override port group settings at the port level on distributed switches, except for block ports.

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

8 VMW-VC-01275 Configure the vCenter Server login banner text for access via SSH.

```
Get-AdvancedSetting -Entity $VC -Name etc.issue | Set-AdvancedSetting -Value "Authorized
login banner"
```

Configure Security Settings on the vCenter Server Appliance

You configure a syslog server and configure backups for vCenter Server from the vCenter Server Appliance Management Interface.

Procedure

1 In a Web browser, log in to the vCenter Server Management Interface.

Setting	Value
URL	https:///*vcenter-server-fqdn*:5480
User name	administrator@vsphere.local

2 VMW-VC-01218 Configure the appliance to send logs to a central log server.

a In the left pane, click **Syslog**.

b Click **Configure**, configure the address and port of a site-specific syslog aggregator or SIEM with the appropriate protocol, and click **Save**.

Note UDP is discouraged due to it's stateless and unencrypted nature. TLS is recommended.

3 VMW-VC-01220 The vCenter Server configuration must be backed up on a regular basis.

a In the left pane, click **Backup** and click **Configure** or **Edit** for an existing configuration.

b Enter site-specific information for the backup job.

c Ensure that the schedule is set to **Daily** and click **Create**.

4 In a Web browser, log in to the vCenter Server Management Interface.

Setting	Value
URL	https:///*vcenter-server-fqdn*:5480
User name	root

5 VMW-VC-01255 Ensure password expiration for the root user is correct.

a In the left pane, click **Administration** and click **Edit** under Password Expriation Settings.

b Set **Password Validity (days)** to 90 and **Email for expiration warning** to your own email address and click **SAVE**.

Note Configure SMTP on vCenter Server to recieve the notification of expiration warning.

Securing SDDC Manager

4

You perform the procedures on SDDC Manager instances in your environment.

Procedure

1 Security Best Practices for Securing SDDC Manager

You must follow multiple best practices at all times when you operate your SDDC Manager instances.

2 Configure Security Settings for SDDC Manager by Using the SDDC Manager UI

To configure automatic password rotation, you perform the procedure in the SDDC Manager UI .

Security Best Practices for Securing SDDC Manager

You must follow multiple best practices at all times when you operate your SDDC Manager instances.

Table 4-1. Security Best Practices for Securing SDDC Manager

Best Practice	Description
Verify SDDC Manager backup VMW-SDDC-01600	You must back up SDDC Manager regularly to avoid downtime and data loss in case of a system failure. You can back up and restore SDDC Manager with an image-based or a file-based solution. File-based backup is recommended for customers who are comfortable with configuring backups by using APIs, and are not using composable servers or stretched clusters. For image-based backups of SDDC Manager, use a solution compatible with VMware vSphere Storage APIs - Data Protection. For file-based backups, configure an external SFTP server as a target backup location and configure a backup schedule.
The SDDC Manager must sync internal clocks with an authoritative time source. VMW-SDDC-01601	Determining the correct time a particular application event occurred on a system is critical when conducting forensic analysis and investigating system events. Synchronization of system clocks is needed in order to correctly correlate the timing of events that occur across multiple systems. To meet this requirement, the organization will define an authoritative time source and have each system compare its internal clock at least every 24 hours. From the SDDC Manager UI, navigate to Administration >> Network Settings >> NTP Configuration to configure NTP server.
Install security patches and updates for SDDC Manager VMW-SDDC-01602	Install all security patches and updates. To apply patches and updates to SDDC Manager, follow the guidance in the *VMware Cloud Foundation Lifecycle Management* document.
Use SSL certificates issued by a trusted certificate authority for SDDC Manager VMW-SDDC-01603	The use of a trusted certificate on the SDDC Manager appliance assures clients that the service they are connecting to is legitimate and trusted. To update the SDDC Manager certificate, refer the following URL: Install Certificates with External or Third-Party Certificate Authorities.
Do not expose SDDC Manager directly to the internet VMW-SDDC-01604	Allowing external access to the SDDC Manager appliance can expose the server to denial of service attacks or other penetration attempts. System Administrator (SA) should work with the network or boundary team to ensure proper firewall rules are configured or other mechanisms are in place to protect the SDDC Manager appliance.
Assign least privileges to users and service accounts in SDDC Manager VMW-SDDC-01605	Users and groups must be assigned only privileges they require. To reduce risk of confidentiality, availability, or integrity loss, least privilege requires that these privileges must be assigned only if needed. From the SDDC Manager UI, under **Administration > Single Sign On > Users and groups**, review the users and groups assigned a role in SDDC Manager and verify that an appropriate role is assigned.

Table 4-1. Security Best Practices for Securing SDDC Manager (continued)

Best Practice	Description
Dedicate an account for downloading updates and patches in SDDC Manager VMW-SDDC-01607	When access is allowed to download updates online, using a dedicated My VMware account ensures consistent access to updates and security patches in the event of system administrator turnover or account access issues. To configure a dedicated account that is not associated with a particular system administrator, from the SDDC Manager UI, go to **Administration > Depot Settings**.
Deploy SDDC Manager with FIPS security mode activated VMW-SDDC-01608	FIPS mode must be activated during bring-up and cannot be activated post bring-up. Refer to the VCF deployment guide for details on activating FIPS mode on SDDC Manager. **Caution** This option is only available for new VMware Cloud Foundation installations and the setting you apply during bring-up are used for future upgrades. You cannot change the FIPS security mode setting after bring-up.

Configure Security Settings for SDDC Manager by Using the SDDC Manager UI

To configure automatic password rotation, you perform the procedure in the SDDC Manager UI .

If you change the vCenter Server password length using the vSphere Client or the ESXi password length using the VMware Host Client, rotating the password for those components by using SDDC Manager generates a password that complies with the password length that you specified.

Automatic password rotation is currently not supported for ESXi.

SDDC Manager has default password policy settings for automatic password rotation.

Table 4-2. Default Password Settings for Automatic Password Rotation by SDDC Manager

Setting	Value
Minimum length	20 characters
Minimum uppercase characters	1
Minimum numeric characters	1
Minimum special characters	1
Maximum consecutive identical characters	2

Procedure

1 In a Web browser, log in to the SDDC Manager using the SDDC Manager UI.

Setting	Value
URL	https://*sddc_manager-fqdn*/ui
User name	administrator@vsphere.local

2 `VMW-SDDC-01609` Schedule automatic password rotation for vCenter Server, Platform Services Controller (PSC), VMware NSX, and, backup.

a In the left pane, navigate to **Security > Password management**.

b Select a component (such as vCenter).

c Select the username(s), click **Schedule rotation**, and select a rotation schedule (30, 60, or 90 days).

d Click "Yes" to confirm.

Securing Management Virtual Machines

5

You connect to the management domain vCenter Server and use a script to perform multiple configurations on the management virtual machines that belong to the management domain. vSphere Cluster Services (vCLS) nodes are not in scope of this procedure as they are service VMs.

To harden the management VMs, you must power off the VMs one by one and run the script. To harden the vCenter Server VM, follow the instructions below:

1 Disable the lockdown mode on the ESXi host that hosts vCenter Server VM.

2 PowerOff the vCenter Server VM.

3 Run the below script by connecting to ESXi Host using `Connect-VIServer -Server <ESXi host FQDN which hosts vCenter Server VM>` cmdlet.

4 Login to ESXi host client that hosts the vCenter Server VM.

5 Power on the vCenter Server VM.

6 Enable the lockdown mode on the ESXi host.

If ESXi is version 7.0 U3i or above, you can run the script without powering off the management VMs. You must shut down the guest OS and power on (cold boot) the VMs for the advanced settings to take effect. Do not reboot the VMs. To prevent service interruption, cold boot must be performed one virtual machine at a time. Cold boot of vCenter Server and SDDC Manager requires a maintenance window.

Perform cold boot in the following order:

1 NSX Edge nodes

2 NSX Manager nodes

3 vCenter Server

4 SDDC Manager

Configuration ID	Description
VMW-VC-00096	Limit console connection sharing

Procedure

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

Setting	Value
Command	Connect-VIServer -Server *management-domain-vcenter-server-fqdn* -Protocol https
User name	administrator@vsphere.local

2 Configure advanced settings on all management virtual machines by running the script.

You must enter the name of the VM that you are reconfiguring in the first line of the script. For example, `$VMs = ("sddc-manager")`. If ESXi is version 7.0 U3i, you can enter a comma separated list of VMs.

```
$VMs = (management-domain-VM-name)
Foreach ($vm in $VMs){
        $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
    }
    elseif($setting.Value -ne 1){
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value 1 -Confirm:$false
        }
}
```

Securing vSAN

6

You perform procedures on the vCenter Server instance by using the vSphere Client.

Procedure

1 Security Best Practices for Securing vSAN

You must follow multiple best practices at all times when you operate your vSAN storage.

2 Configure a Proxy Server for vSAN from the vSphere Client

You perform the procedure on the respective vCenter Server to configure a proxy server for the download of the public Hardware Compatibility List.

3 Configure vSAN Data-At-Rest and Data-In-Transit Encryption from the vSphere Client

You activate vSAN Data-At-Rest encryption and Data-In-Transit encryption on the vSAN cluster. You can choose Native Key Provider to enable vSAN Encryption or you must set up an external Key Management Server (KMS) and establish a trusted connection between vCenter Server and the KMS.

Security Best Practices for Securing vSAN

You must follow multiple best practices at all times when you operate your vSAN storage.

Table 6-1. Security Best Practice for Securing vSAN

Best Practice	Description
vSAN must reserve space to complete internal maintenance operations. VMW-vSAN-00186	vSAN Operations Reserve capacity setting helps ensure that vSAN always has sufficient free space to maintain the availability and reliability of the vSAN datastore and prevent potential data loss or service disruptions due to insufficient capacity during operations like policy changes. This configuration parameter can be altered while the cluster is operational.
NFS file shares on vSAN File Services must be configured to restrict access. VMW-vSAN-00185	When configuring an NFS file share the "Customize net access" option should be selected with a restrictive set of permissions configured.
SMB file shares on vSAN File Services must accept only encrypted SMB authentication communications. VMW-vSAN-00187	When configuring an SMB file share the Protocol Encryption option must be enabled.

Configure a Proxy Server for vSAN from the vSphere Client

You perform the procedure on the respective vCenter Server to configure a proxy server for the download of the public Hardware Compatibility List.

Procedure

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

Setting	Value
URL	https://*management-domain-vcenter-server-fqdn*/ui
User name	administrator@vsphere.local

2 `VMW-vSAN-00207` Configure a proxy for the download of the public Hardware Compatibility List.

   a In the **Hosts and Clusters** inventory, select the vCenter Server object.

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

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

   d Select the **Configure the proxy server if your system uses one** check box.

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

Configure vSAN Data-At-Rest and Data-In-Transit Encryption from the vSphere Client

You activate vSAN Data-At-Rest encryption and Data-In-Transit encryption on the vSAN cluster. You can choose Native Key Provider to enable vSAN Encryption or you must set up an external Key Management Server (KMS) and establish a trusted connection between vCenter Server and the KMS.

- Do not deploy external KMS server on the same vSAN datastore that you plan to encrypt.
- You cannot encrypt a witness host. The witness host in a stretched cluster does not participate in vSAN encryption. Only metadata is stored on the witness host.

For more information, see vSAN Data-At-Rest Encryption and vSAN Data-In-Transit Enctyption in the vSAN product documentation.

Procedure

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

Setting	Value
URL	https://*management-domain-vcenter-server-fqdn*/ui
User name	administrator@vsphere.local

2 VMW-vSAN-00183 Activate data at rest encryption on the vSAN cluster.

   a In the **Hosts and Clusters** inventory, select the vSphere cluster that uses vSAN as storage.

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

   c Click the Data Services**Edit** button.

   d In the **vSAN Services** dialog box, activate the toggle switch of **Data-At-Rest encryption**, select a Native Key Provider or external KMS cluster, and click **Apply**.

   e Repeat the procedure by selecting the vSphere cluster for the VI workload domain.

3 VMW-vSAN-00184 Activate data in transit encryption on the vSAN cluster.

   a In the **Hosts and Clusters** inventory, select the vSphere cluster that uses vSAN as storage.

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

   c Click the Data Services**Edit** button.

   d In the **vSAN Services** dialog box, activate the toggle switch of **Data-In-Transit encryption**, configure rekey interval and click **Apply**.

   e Repeat the procedure by selecting the vSphere cluster for the VI workload domain.

Securing VMware NSX

7

You perform the procedures on different components of NSX.

Procedure

1 Security Best Practices for Securing VMware NSX

You must follow multiple best practices at all times when you operate your NSX environment.

2 Configure Security Settings for VMware NSX by Using the User Interfaces

You perform the procedure in NSX to configure logging servers, configure logging for distributed and gateway firewall rules, and configure port binding for the spoofguard profile. Configure the settings for all NSX instances in your VMware Cloud Foundation environment.

3 Configure Security Settings for NSX by Using CLI Commands

You configure NSX Manager to back up audit records to a logging server. Also, you configure NSX Edge nodes to back up audit records to a central audit server.

4 Configure Security Settings for VMware NSX by Using NSX API

You configure TLS 1.2 protocol and disable TLS 1.1 for NSX Manager.

5 Optional Security Configurations for VMware NSX

Application Virtual Networks (AVN)s, which include the NSX Edge Cluster and NSX network segments, are no longer deployed and configured during bring-up. Instead they are implemented as a Day-N operations in SDDC Manager, providing greater flexibility. These configurations should be reevaluated if you plan to deploy NSX edges in your environment. Simiarly, Distributed Firewall (DFW) and Gateway Firewall configurations are applicable only if you purchase NSX Firewall Add-On. These configurations are included as optional and site-specific only.

Security Best Practices for Securing VMware NSX

You must follow multiple best practices at all times when you operate your NSX environment.

Table 7-1. NSX

Best Practice and Configuration ID	Description
Use roles and privileges in NSX Manager to limit user privileges. VMW-NSX-01410	Users and service accounts must be assigned the required privileges only. You can create a new role with reduced permissions. Navigate to **System > Settings > User management > Roles**. Click **Add role**, provide a name, the required permissions, and click **Save**. You can reduce permissions to an existing role. Navigate to **System > Settings > User Management > User role assignment**. Click the vertical ellipsis next to the target user or group, select **Edit**, remove the existing role, select the new role, and click **Save**.
Integrate VMware Identity Manager (vIDM) or OpenID Connect (which supports multi factor authenticaiton) with NSX VMW-NSX-01415	Use vIDM or OpenID Connect to meet requirements for authentication, authorization, and access control.
NSX Manager must obtain its public key certificates from an approved certificate authority. VMW-NSX-01466	For user certificates, each organization obtains certificates from an approved, shared service provider, as required by OMB policy. For federal agencies operating a legacy public key infrastructure cross-certified with the Federal Bridge Certification Authority at medium assurance or higher, this Certification Authority will suffice.

Configure Security Settings for VMware NSX by Using the User Interfaces

You perform the procedure in NSX to configure logging servers, configure logging for distributed and gateway firewall rules, and configure port binding for the spoofguard profile. Configure the settings for all NSX instances in your VMware Cloud Foundation environment.

Procedure

1. In a Web browser, log in to the NSX Manager cluster as an administrator by using the user interface.
2. VMW-NSX-01468 You configure NSX Manager to perform backups on an organizational defined schedule.
   a. On the main navigation bar, click **System**.
   b. In the left pane, navigate to **Lifecycle management > Backup and restore**.
   c. Next to **SFTP server**, click **Edit**.
   d. In the **Backup configuration** dialog box, enter the required details and click **Save**.
   e. Next to **Schedule**, click **Edit**.

f In the **Schedule recurring backup** dialog box, click **Recurring backup toggle** and configure an interval between backups.

g To perform backups on detection of configuration changes, activate **Detect NSX configuration change**, specify an interval for detecting changes, and click **Save**.

3 VMW-NSX-01500 The NSX Manager must disable unused local accounts.

a On the main navigation bar, click **System**.

b In the left pane, navigate to **Settings > User management**.

c Click **Local users** and click vertical ellipsis next to the user to modify and click **Deactivate User**.

4 VMW-NSX-01524 NSX Manager must display the Standard Mandatory Notice and Consent Banner before granting access.

a On the main navigation bar, click **System**.

b In the left pane, navigate to **Settings > General Settings**.

c Click **User Interface** and click **Edit** next to **Login Consent Settings**.

d Toggle **Login Consent** to On and **Require Explicit User Consent** to Yes.

e Input **Consent Message Title** with Standard mandatory notice and consent banner and **Consent Message Description** and click **Save**.

Configure Security Settings for NSX by Using CLI Commands

You configure NSX Manager to back up audit records to a logging server. Also, you configure NSX Edge nodes to back up audit records to a central audit server.

Procedure

1 VMW-NSX-01401 Synchronize internal information system clocks using redundant authoritative time sources.

a Open the VM console of the NSX Manager appliance in vCenter Server and log in with credentials authorized for administration.

b Run the following commands:

```
#remove any unknown or nonauthoritative NTP servers
del ntp-server <server-ip or server-name>
#configure ntp server
set ntp-server <server-ip or server-name>
```

2 VMW-NSX-01414 Configure NSX Manager to send logs to a central log server.

You can configure the logging server with one of the following protocols: TCP, LI-TLS, or TLS. If you use the protocls TLS or LI-TLS to configure a secure connection to a log server, the server and client certificates must be stored in the `/image/vmware/nsx/file-store/` folder on each NSX Manager appliance.

a Open the VM console of the NSX Manager appliance in vCenter Server and log in with credentials authorized for administration.

b If you want to configure a TCP or UDP syslog server, run `set logging-server <server-ip_or_server-name> proto <tcp or udp> level info` and press Enter.

c If you want to configure a TLS syslog server, run `set logging-server <server-ip_or_server-name> proto tls level info serverca ca.pem clientca ca.pem certificate cert.pem key key.pem` and press Enter.

d If you want to configure an LI-TLS server, run `set logging-server <server-ip_or_server-name> proto li-tls level info serverca root-ca.crt` and press Enter.

3 VMW-NSX-01421 Enforce a minimum of 15 characters for password length on the NSX Manager nodes.

a Open the VM console of an NSX Manager appliance in vCenter Server and log in with credentials authorized for administration.

b Run the command and press Enter.

```
set password-complexity minimum-password-length 15
```

4 VMW-NSX-01530 NSX Manager must require that when a password is changed, the characters are changed in at least eight of the positions within the password.

a Open the VM console of an NSX Manager appliance in vCenter Server and log in with credentials authorized for administration.

b Run the command and press Enter.

```
set password-complexity max-repeats 8
```

5 Configure login sessions settings for the NSX Manager.

a Open the VM console of the NSX Manager appliance in vCenter Server and log in with credentials authorized for administration.

b VMW-NSX-01416 Configure session lock after a 10-minute period of inactivity.

```
Set service http session-timeout 600
```

c VMW-NSX-01418 Prevent an account from further log in attempts by using the UI or API after three consecutive failed log in attempts.

```
Set auth-policy api max-auth-failures 3
```

d VMW-NSX-01498 Prevent an account from further log in attempts by using CLI after three consecutive failed log in attempts.

```
set auth-policy cli max-auth-failures 3
```

Configure Security Settings for VMware NSX by Using NSX API

You configure TLS 1.2 protocol and disable TLS 1.1 for NSX Manager.

Procedure

- VMW-NSX-01501 Configure an NSX Manager node to only use the TLS 1.2 protocol.

  The change applies to all nodes in the cluster. The API service on each node restarts after the update. A delay of up to a minute between the time this API call completes and when the new configuration applies is possible.

  a Run the GET command and save the output.

  ```
  GET https://<nsx-mgr>/api/v1/cluster/api-service
  ```

  b In the saved output, edit the `protocol_versions` line to disable TLS 1.1.

  ```
  "protocol_versions": [ { "name": "TLSv1.1", "enabled": false }, { "name": "TLSv1.2", "enabled": true } ]
  ```

  c Run the API call using curl or another REST API client with the edited initial output.

  ```
  PUT https://<nsx-mgr>/api/v1/cluster/api-service
  ```

Optional Security Configurations for VMware NSX

Application Virtual Networks (AVN)s, which include the NSX Edge Cluster and NSX network segments, are no longer deployed and configured during bring-up. Instead they are implemented as a Day-N operations in SDDC Manager, providing greater flexibility. These configurations should be reevaluated if you plan to deploy NSX edges in your environment. Simiarly, Distributed Firewall (DFW) and Gateway Firewall configurations are applicable only if you purchase NSX Firewall Add-On. These configurations are included as optional and site-specific only.

Configure Security Settings for NSX Edge Nodes by Using the User Interface

You perform the procedure in NSX to configure traffic logging for Gateway Firewall rules, publish any firewall policy/rule changes, deny traffic by default, flood protection profile, ingress filters, restrict traffic and disable Internet Control Message Protocol (ICMP) unreachable notifications, mask replies, redirects on the external interfaces. Configure the settings for all NSX edge instances in your VMware Cloud Foundation environment.

Procedure

1 In a Web browser, log in to the NSX Manager cluster as an administrator by using the user interface.

2 `VMW-NSX-01429`, `VMW-NSX-01514` Configure the NSX Gateway Firewall on the tier-0 and tier-1 gateways to generate traffic log entries.

Note If the tier-0 gateway is deployed in an active/active high availability mode and no stateless rules exist, this configuration is not applicable.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Gateway Firewall/**

c Click the **Gateway specific rules** tab.

d From the **Gateway** drop-down menu, select the respective gateway.

e For each tier-0 gateway and for each rule with logging disabled, click the gear icon, activate the **Logging** toggle, and click **Apply**.

f On the **Gateway Firewall** page, click **Publish**.

g Repeat the procedure for each tier-1 gateway and for each rule with deactivated logging.

3 `VMW-NSX-01431`, `VMW-NSX-01432` Configure the NSX Gateway Firewall on the tier-0 and tier-1 gateways to deny network traffic by default and allow network traffic by exception.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Gateway Firewall**.

c Click the **Gateway specific rules** tab.

d From the **Gateway** drop-down menu, select the respective gateway.

e Expand the default policy, and from the **Actions** drop-down menu, select **Reject** or **Drop**.

f On the **Gateway Firewall** page, click **Publish**.

g Repeat the procedure for each tier-1 gateway.

4 VMW-NSX-01437 Configure the multicast NSX tier-0 gateway to deactivate Protocol Independent Multicast (PIM) on all interfaces that are not required to support multicast routing.

   a Navigate to **Networking > Connectivity > Tier-0 Gateways** and expand the target Tier-0 gateway.

   b Expand **Interfaces and GRE Tunnels**, click on the number of **External and Service interfaces** present to open the interfaces dialog, and then select "Edit" on the target interface.

   c Expand "Multicast", change PIM to "Deactivated", and then click "Save".

5 VMW-NSX-01438 Remove inactive interfaces on an NSX Tier-0 gateway.

   a Navigate to **Networking > Connectivity > Tier-0 Gateways** and expand the target Tier-0 gateway.

   b Expand **Interfaces and GRE Tunnels**, click on the number of "External and Service interfaces" present to open the interfaces dialog, and then select "Edit" on the target interface.

   c Select "Delete" on the unneeded interface, and then click "Delete" again to confirm.

6 VMW-NSX-01442 Disconnect inactive linked segments for NSX Tier-1 gateways.

   a Navigate to **Neteworking > Connectivity > Segments**and edit the target segment.

   b Under Connected Gateway, change to "None" and click "Save.

   Note The stale linked segment can also be deleted if there are no active workloads attached to it.

   c Naviate to **Networking > Connectivity > Tier-1 Gateways** and edit the target Tier-1 Gateway.

   d Expand Service Interfaces and click on the number to view the Service Interfaces.

   e On the stale service interface, select **Delete** and click **Delete** again to confirm.

7 VMW-NSX-01453, VMW-NSX-01515 Configure flood protection profiles on the NSX Gateway Firewall for the tier-0 and tier-1 gateways to protect against Denial of Service (DDoS) attacks.

   Note If the tier-0 gateway is deployed in an active/active high availability mode and no stateless rules exist, this configuration is not applicable.

   a On the main navigation bar, click **Security**.

   b In the left pane, navigate to **Settings > General Settings**.

   c Click the **Firewall > Flood Protection** under **General Security Settings** tab.

   d Fom the **Add profile** drop-down menu, select **Add Edge Gateway profile**.

e Enter a name and specify appropriate values for the following: **TCP half open connection limit**, **UDP active flow limit**, **ICMP active flow limit**, and **Other active connection limit**.

f Configure the **Applied to** field to contain the tier-0 gateways, and then click **Save**.

g Repeat this step for the tier-1 gateway and set **Applied to** to contain the tier-1 gateways.

8 `VMW-NSX-01460` To protect against route table flooding and prefix de-aggregation attacks, configure the NSX tier-0 gateway to use maximum prefixes.

a On the main navigation bar, click **Networking**.

b In the left pane, navigate to **Connectivity > Tier-0 gateways**.

c Expand the NSX tier-0 gateway.

d Expand the **BGP** section and click **BGP neighbors**.

e In the **Set BGP neighbors** dialog box, click the vertical ellipsis and click **Edit** for the first neighbor.

f Click the number in the **Route filter** column.

g To configure the maximum routes value, specific to your environment, in the **Set route filter** dialog box, click the vertical ellipsis menu and click **Edit**.

h Repeat the step to configure all neighbors.

9 `VMW-NSX-01494`, `VMW-NSX-01495`, `VMW-NSX-01496` Configure the NSX tier-0 gateway to have Internet Control Message Protocol (ICMP) unreachable notifications, mask replies, and disable redirects on all external interfaces.

Note If the tier-0 gateway is deployed in an active/active high availability mode and no stateless rules exist, this configuration is not applicable.

NSX does not come with a pre-configured service for ICMP mask replies. You may need to create this service.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Gateway Firewall**.

c Click the **All shared rules** tab.

d Click **Add rule** (Add a policy first if needed) and, in the **Services** column, click the **Edit** button.

e On the **Set services** dialog box, on the **Services** tab, select the **ICMP destination unreachable** service, and click **Apply**.

f Click the **Settings** icon for the newly added rule and, on the **Settings** dialog box, activate the **Logging** toggle.

g In the **Applied to** column, click the **Edit** icon.

h In the **Applied to** dialog box, select the target NSX tier-0 gateway and click **Apply**.

i On the **Gateway Firewall** page, click **Publish**.

j Repeat the procedure for the **ICMP mask replies** and **ICMP redirect**services.

Note A rule can also be created under Gateway Specific Rules to meet this requirement.

10 VMW-NSX-01532 NSX Tier-1 Gateway Firewall must be configured to inspect traffic at the application layer.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Gateway Firewall** and select **Gateway Specific Rules**.

c From the Gateway drop down choose **Tier-1 Gateway**

d For each rule that should have a Context Profile enabled, click the penci icon in the **Profiles** column. and select **Context profile** under **Select profile** dialog box.

e Select an existing Context Profile or create a custom one then click **Apply**.

f After all the changes are made, click **Publish**.

Note Not all App IDs will be suitable for use in all cases and should be evaluated in each environment before use.

A list of App IDs for application layer rules is available here: https://docs.vmware.com/en/NSX-Application-IDs/index.html

11 VMW-NSX-01469 Unicast Reverse Path Forwarding (uRPF) must be enabled on the NSX Tier-0 Gateway

a On the main navigation bar, click **Networking**.

b In the left pane, navigate to **Connectivity > Tier-0 gateways**.

c Expand the NSX tier-0 gateway.

d Expand the **Interfaces and GRE Tunnels** section and click the number of **External and Service Interfaces**.

e In the **Set Interfaces** dialog box, click the vertical ellipsis and click **Edit** for the first interface.

f From the drop-down set the **URPF Mode** to **Strict** and then click **Save**.

g Repeat the step to configure all interfaces.

12 VMW-NSX-01459 VMW-NSX-01470 The NSX Tier-0 Gateway router must be configured to use encryption for BGP routing protocol authentication and use a unique password for each autonomous system (AS) that it peers with.

a On the main navigation bar, click **Networking**.

b In the left pane, navigate to **Connectivity > Tier-0 gateways**.

c Expand the NSX tier-0 gateway.

d Expand the **BGP** section and click the number next to **BGP neighbors**.

e In the **Set BGP neighbors** dialog box, click the vertical ellipsis and click **Edit** for the first neighbor.

f Under **Timers and Password**, enter a unique password of up to 20 characters that is different from other autonomous systems and then click **Save**.

g Repeat the step to configure all neighbors.

13 `VMW-NSX-01536` The NSX Tier-0 Gateway router must be configured to use encryption for OSPF routing protocol authentication.

a On the main navigation bar, click **Networking**.

b In the left pane, navigate to **Connectivity > Tier-0 gateways**.

c Expand the NSX tier-0 gateway.

d Expand the **OSPF** section and click number next to **Area Definition**.

e In the **Set Area Definition** dialog box, click the vertical ellipsis and click **Edit** for the first Area definition.

f Change the **Authentication** drop-down to MD5 and enter a Key ID and password and then click **Save**.

g Repeat the step to configure all Area definitions.

Note The MD5 password can have a maximum of 16 characters.

Configure Security Settings for NSX Edge Nodes by Using CLI Commands

You configure the NSX Gateway Firewall to send logs to a central log server.

You perform these procedures on the NSX tier-0 and tier-1 gateway only if your environment uses NSX Edges.

Procedure

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

Setting	Value
URL	https://*management-domain-vcenter-server-fqdn*/ui
User name	administrator@vsphere.local

2 In the **VMs and templates** inventory, navigate to the NSX Edge node, right-click the appliance, and select **Open remote console**.

3 VMW-NSX-01430, VMW-NSX-01511 Configure the NSX Gateway Firewall on the tier-0 and tier-1 gateways to send logs to a central log server.

You can configure the logging server with the LI-TLS or TLS protocols. You must store the server and client certificates in the /var/vmware/nsx/file-store/ on each NSX Edge appliance.

a If you want to configure a TCP syslog server, run the command.

```
set logging-server <server-ip or server-name> proto tcp level info
```

b If you want to configure a TLS syslog server, run the command.

```
set logging-server <server-ip_/_server-FQDN> proto tls level info serverca ca.pem
clientca ca.pem certificate cert.pem key key.pem
```

c If you want to configure a LI-TLS syslog server, run the command.

```
set logging-server <server-ip_/_server-FQDN> proto li-tls level info serverca root-
ca.crt
```

Note Configure the syslog or SNMP server to send an alert if the events server is unable to receive events from the NSX Edge node and if DoS incidents are detected.

Configure Security Settings for Distributed Firewall by Using the User Interface

You perform the procedure in NSX to configure traffic logging for Distributed Firewall rules, deny traffic by default and profiles such as spoof guard, flood protection, context, and IP Discovery profile.

Procedure

1 In a Web browser, log in to the NSX Manager cluster as an administrator by using the user interface.

2 VMW-NSX-01409 Configure the NSX Distributed Firewall to generate traffic log entries.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Distributed Firewall**.

c Click the **Category Specific Rules** tab.

d For each rule with logging disabled, click the gear icon, activate the **Logging** toggle, and click **Apply**.

e On the **Distributed Firewall** page, click **Publish**.

3 VMW-NSX-01412 Configure the NSX Distributed Firewall to deny network traffic by default and allow network traffic by exception.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Distributed Firewall**.

c Click the **Category specific rules** tab and select **Application**.

d Expand the **Default Layer3 Section** and for the **Default Layer3 Rule**, select **Reject** or **Drop** from the **Actions** drop-down menu.

e On the **Distributed Firewall** page, click **Publish**.

Caution Before denying, ensure the necessary rules to whitelist approved traffic are created and published or this change may result in a loss of communication for workloads.

4 VMW-NSX-01452 Configure flood protection profiles on the NSX Distributed Firewall to protect against Denial of Service (DDoS) attacks.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Settings > General Settings**.

c Click the **Firewall > Flood Protection** .

d Fom the **Add profile** drop-down menu, select **Add Firewall Profile**.

e Enter a name and specify appropriate values for the following: **TCP half open connection limit**, **UDP active flow limit**, **ICMP active flow limit**, and **Other active connection limit**.

f Enable **SYN Cache** and **RST Spoofing**.

g Configure the **Applied to** field to contain appropriate security groups, and then click **Save**.

5 VMW-NSX-01534 The NSX Distributed Firewall must be configured to inspect traffic at the application layer.

a On the main navigation bar, click **Security**.

b In the left pane, navigate to **Policy Management > Distributed Firewall** and select **Category Specific Rules**.

c For each rule that should have a Context Profile enabled, click the pencil icon in the **Profiles** column. and select **Context profile** under **Select profile** dialog box.

d Select an existing Context Profile or create a custom one then click **Apply**.

e After all the changes are made, click **Publish**.

Note This control does not apply to ethernet rules.

Not all App IDs will be suitable for use in all cases and should be evaluated in each environment before use.

A list of App IDs for application layer rules is available here: https://docs.vmware.com/en/NSX-Application-IDs/index.html

Security Configurations Not Applicable or Not Compatible with VMware Cloud Foundation

8

Typical configuration guidelines apply to standalone implementations of VMware products. When these products are part of VMware Cloud Foundation, some configurations might not be applicable or might not be compatible with VMware Cloud Foundation. Do not implement these configurations. You can find mitigation steps for the configurations in the *VMware Cloud Foundation Audit Guide Appendix*.

Product	Configuration	Context for Excluding Configuration
vCenter Server	vCenter Server must be isolated from the public Internet but must still allow for patch notifications and delivery. VMW-VC-01231	Never apply patches to vCenter Server manually, using VMware vSphere Update Manager, or VMware vCenter Lifecycle Manager in a VMware Cloud Foundation environment, unless directed to do so by support. Patching the environment without using SDDC Manager might cause problems with automated upgrades or actions in the future.
ESXi	ESXi hosts using Host Profiles and/or Auto Deploy must use the vSphere Authentication Proxy to protect passwords when adding themselves to Active Directory. VMW-ESXI-00115	VMware Cloud Foundation does not use host profiles to join ESXi hosts to Active Directory.