Security and Compliance Configuration for VMware Cloud Foundation 4.5

25 MAY 2023

VMware Cloud Foundation 4.5

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

https://docs.vmware.com/

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

Contents

About Security and Compliance Configuration for VMware Cloud Foundation 4.5

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 4.5.

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
25 MAY 2023	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, see VMware 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. Esnure that all encryption keys are available across regions to activate decryption in case of a region failover.

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-T Data Center	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 NSX-T Data Center, 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, join ESXi hosts to Active Directory domain, and remove ESX Admin group membership. Also, stop the ESXi shell service, configure login banners for the Direct Console User Interface (DCUI) and SSH connections, deactivate warnings, activate the Bridge Protocol Data Unit (BPDU) filter, configure persistent log location, remote logging, 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.
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.
Do not provide root or administrator level access to CIM-based hardware monitoring tools or other third-party applications. `VMW-ESXI-01106`	The CIM system provides an interface that activates hardware-level management from remote applications through a set of standard APIs. In environments that implement CIM hardware monitoring, create a limited-privilege, read-only service account for CIM and place this user in the Exception Users list. If a CIM write access is required, create a new role with only the `Host.CIM.Interaction` permission and apply that role to your CIM service account.
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.
Ensure that a TPM 2.0 is installed and activated on the host. `VMW-ESXI-01129`	ESXi can use Trusted Platform Modules (TPM) to activate advanced security features that prevent malware, remove dependencies, and secure hardware life cycle operations. We recommend all servers be configured with a TPM 2.0 and the TPM be activated in the system firmware. **Note** Activating TPM functionality deactivates Quick Boot, making patch cycles longer but forcing the system to go through the process of attestation to help prevent malware loading at boot.

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

Best Practice	Description
Ensure that all system and device firmware is auditable, authentic, and up to date. VMW-ESXI-01130	Hardware firmware is not immune to serious issues affecting confidentiality, integrity, or availability. Vulnerable system management controllers and management engines can provide places for attackers to establish persistence, in order to re-infect and re-compromise hosts after reboots and updates. Ensure that the latest firmware updates are applied to all components of your systems and that the firmware is authentic and supplied by your hardware manufacturer. **Note** If you are a vSAN customer please ensure that storage device & controller firmware versions are certified.
Ensure that integrated hardware management controller internal, emulated, or virtual network interfaces are disabled. VMW-ESXI-01132	Many servers have integrated hardware management controllers with the ability to present virtual network interfaces to ESXi as a management interface. These approaches create potential backdoors for access and are used by adversaries to circumvent network-based/perimeter firewalls, in either direction, and avoid observation by IDS/IPS/threat analysis tools. In many cases this functionality is not strictly necessary to manage hosts.
Ensure that Intel Trusted Execution Technology is enabled in the system firmware, if available. VMW-ESXI-01134	Intel Xeon Scalable Processor platforms have Trusted Execution Technology (TXT), that help harden systems against malware, rootkits, BIOS andfirmware attacks, and more. When enabled, ESXi will take advantage of security benefits offered by this technology. **Note** Enabling early implementations of Intel TXT may cause operations like firmware updates and sudden system shutdowns to trigger attestation alarms in vCenter Server, or cause failures while booting. See VMware Knowledge Base Article 78243.

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

Best Practice	Description
Ensure that integrated hardware management controllers are fully secured. VMW-ESXI-01135	Configure all integrated hardware management components to turn off all unused functionality and all unused access methods, to set passwords and password controlls, and to have firewall and access control in place. Ensure that the only access to the integrated hardware management components is from authorized access workstations for the virtualization administration team. All first boot configuration options must be disabled, especially ones that reconfigure the system through the use of inserted USB devices. Disable or protect USB ports attached to the management controllers. Where possible, USB ports should be set to only permit keyboards. Default passwords for accounts must be changed. Ensure that external information displays are secured to prevent information leaks. Ensure that power and information buttons are secured against unauthorized use. If there are no alternative methods set up in your environment, ensure that you use mechanism embedded in the hardware management controllers to monitor and alert for hardware faults and configuration changes.
Configure NTP servers for the integrated hardware management controllers and ensure NTP servers are authorized per your organization's policies. VMW-ESXI-01136	Configure the integrated hardware management controllers to synchronize internal system clocks by using redundant authoritative time sources. Ensure that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreedupon time standard (such as Coordinated Universal Time—UTC). Cryptography, audit logging, cluster operations, and incident response/forensics depend on synchronized time. Ensure that you have at least four authorized time sources.
Ensure that the use of centralized authentication sources for the integrated hardware management controllers does not create a dependency loop or an attack vector. VMW-ESXI-01137	Connections to centralized authentication sources, like Active Directory, must be disabled or carefully considered as attack vectors and dependency loops (for authentication, authorization, DNS, DHCP, and NTP). Consider managing local accounts on these devices through the provided APIs and CLI interfaces. If you must use Active Directory for authentication, ensure local authorization to deny promotion through group membership for an attacker with access to Active Directory.

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

Best Practice	Description
Ensure that AMD Secure Encrypted Virtualization-Encrypted State is enabled in the system firmware, and is configured for a reasonable number of protected VMs (minimum SEV non-ES ASID), if available. VMW-ESXI-01138	AMD EPYC platforms support Secure Encrypted Virtualization-Encrypted State (SEV-ES), a technology to encrypt memory and CPU register state, and limit visibility to the hypervisor, in order to increase workload security and decrease exposure to certain types of attacks. When configured properly, vSphere supports the use of SEV-ES inside guest virtual machines and containers under vSphere and vSphere with Tanzu. **Note** Use of SEV-ES in a particular VMs requires the guest OS to support it, and will limit some operational features such as vMotion, snapshots, etc.
Ensure that Intel Software Guard Extensions is enabled in the system firmware, if available. VMW-ESXI-01139	Intel Xeon Scalable Processor platforms support Software Guard Extensions (SGX), a technology that helps applications protect data in system memory. When configured properly, vSphere supports the use of SGX inside guest virtual machines. **Note** Use of SGX requires guest OS support, and will limit some operational features inside vSphere, such as vMotion, snapshots, fault tolerance, and suspend/resume.
Ensure that unused external ports are disabled or protected against unauthorized use. VMW-ESXI-01140	Unused ports, especially USB, can be used by attackers to attach storage, networking, and keyboards. Take reasonable steps to control access to these ports through disablement, access control, and/or with other means such as solid rack doors, rack side panels, and flooring that makes the ports inaccessible from outside the rack when the rack door is closed. Cables fit easily through many gaps in and around racks and rack doors, and stiff wires can be used to push them into sockets from outside the rack, as well as to dislodge cables to create a service disruption. Where possible, USB ports should also be set to only permit keyboards. When disabling functionality like this, consider that you may need to access the server using a USB keyboard during an outage or as part of lifecycle operations, and plan accordingly.

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
```

Note If an imaging appliance (VIA) is used to image the ESXi host, the host does not support UEFI, which is a requirement for activating secure boot. ESXi installations done through other methods are supported and can activate UEFI/secure boot.

If the output indicates that secure boot cannot be activated, correct the discrepancies and try again.

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, join ESXi hosts to Active Directory domain, and remove ESX Admin group membership. Also, stop the ESXi shell service, configure login banners for the Direct Console User Interface (DCUI) and SSH connections, deactivate warnings, activate the Bridge Protocol Data Unit (BPDU) filter, configure persistent log location, remote logging, 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 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"
```

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 SSH service.
$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 SSH service.
$arguments = $esxcli.network.firewall.ruleset.allowedip.add.CreateArgs()
$arguments.rulesetid = "sshServer"
$arguments.ipaddress = "Site-specific networks"
$esxcli.network.firewall.ruleset.allowedip.add.Invoke($arguments)}
```

4 VMW-ESXI-00030 Show warnings in the vSphere Client if local or remote shell sessions are activated on the ESXi hosts.

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

5 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
```

6 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
```

7 VMW-ESXI-00043 Activate the Bridge Protocol Data Unit (BPDU) filter.

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

8 VMW-ESXI-00109 Configure the password history setting to restrict the reuse of the last five passwords.

```
Get-VMHost | Get-AdvancedSetting -Name Security.PasswordHistory | Set-AdvancedSetting
-Value 5
```

9 VMW-ESXI-00112 Stop the ESXi shell service and set the startup policy.

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

10 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**.

11 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"
```

12 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"
```

13 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`.

14 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 AD_Group
```

15 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
"<syslog server hostname>"
```

16 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
```

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

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -v2 -VMHost $esxiHost.Name
$arguments = $esxcli.system.syslog.config.set.CreateArgs()
$arguments.x509strict = $true
$esxcli.system.syslog.config.set.Invoke($arguments)
$esxcli.system.syslog.reload.Invoke()
}
```

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

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

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

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

20 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.
- 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.

21 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)
}
```

22 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
```

23 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
```

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 Configure VLAN settings on the standard switch.

Configuration ID	Description
VMW-ESXI-01103	Configure port groups on standard switches to a value other than that of the native VLAN.
VMW-ESXI-01104	Do not configure the port groups on standard switches to VLAN 4095 unless Virtual Guest Tagging (VGT) is required.
VMW-ESXI-01105	Do not configure the port groups on standard switches to VLAN values reserved by upstream physical switches.

```
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** radio button and click **OK**.

Note When performing skip-level upgrade from VMware Cloud Foundation version 4.5 to version 5.0, NSX upgrade pre-check fails if the lockdown mode is enabled on the ESXi hosts. You must disable lockdown mode before upgrading NSX and enable it again after NSX upgrade completes successfully.

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**
Use templates to deploy virtual machines. VMW-VC-01235	To create application-specific templates, use templates that contain a hardened, patched, and properly configured operating system . You can also use the application template to deploy virtual machines.
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.
The vCenter Server must use a limited privilege account when adding an LDAP identity source VMW-VC-01230	When adding an LDAP identity source to vSphere SSO, the account used to bind to the AD must be minimally privileged. This account only requires read rights to the base DN specified. Any other permissions inside or outside of that OU are unnecessary and violate least privilege.
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.

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

Best Practice	Description
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 participation in CDP or LLDP is intentional. VMW-VC-01247	The vSphere VDS can participate in Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP), as a listener, advertiser, or both. This can facilitate improved mapping network topology and troubleshooting, however you must ensure that information sent and received is intentional, as this information can be used by an adversary to gain a better understanding of your environment.
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.
Configure the vCenter Server firewall for additional defense-in-depth. VMW-VC-01251	vCenter Server has its own firewall settings that can be used in conjunction with a network/perimeter firewall for additional defense. Ensure that you configure it with `accept` rules for your workstations prior to configuring `deny` rules.
Remove unnecessary NICs. VMW-VC-01252	In Center Server, you can configure multiple network interfaces connected to different networks. If a system has interfaces on different networks, there is potential to bridge the networks, or create a backdoor that circumvents network-based access controls. Ensure that all NICs are configured properly and are necessary.
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.

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

Best Practice	Description
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.
Consider the risks of using Active Directory groups to authorize vSphere Administrators. VMW-VC-01261	If you are using a centralized directory service such as Active Directory for both authentication and authorization, an attacker can can compromise the service and obtain authorization to other infrastructure services. It also means that the administrators ("Domain Admins") for the directory service are defacto administrators of infrastructure. To help manage risk, where feasible, consider the use of local SSO groups for authorization.

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

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-00418 Configure a proxy for the download of the public Hardware Compatibility List.

a In the **Hosts and Clusters** inventory, select the vCenter Server that you configure.

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**.

6 VMW-VC-01236 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 the vCenter Server that you configure.

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**.

7 VMW-VC-01209 Configure a login message.

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

b Navigate to **Single sing-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**.

8 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**.

9 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

10 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**.

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#>"
```

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 VMW-VC-01250 Limit access to vCenter Server by restricting SSH.

a In the left pane, click **Access** and click **Edit**.

b Deactivate the **Enable SSH login** toggle and click **OK**.

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

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

6 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 9999 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
SDDC Manager backup VMW-SDDC-1600	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.
Install security patches and updates for SDDC Manager VMW-SDDC-1602	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.

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

Best Practice	Description
Use PKI Class 3 or Class 4 certificates issued by a trusted certificate authority for SDDC Manager VMW-SDDC-1603	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-1604	Allowing external access to the SDDC Manager appliance can expose the server to denial of service attacks or other penetration attempts. Security Architect (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-1605	Users and service accounts 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.
Dedicate an account for downloading updates and patches in SDDC Manager VMW-SDDC-1607	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 > Online depot**.
Deploy SDDC Manager with FIPS security mode activated VMW-SDDC-1608	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-1609` Schedule automatic password rotation for vCenter Server, Platform Services Controller (PSC), NSX-T Data Center, and, backup.

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

b Select a filter on the top right (such as vCenter).

c Select the username(s), click **Schedule rotation**, and select a rotation schedule.

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-00070	Deactivate copy operations.
VMW-VC-00071	Deactivate drag and drop operations.

Configuration ID	Description
VMW-VC-00073	Deactivate paste operations.
VMW-VC-00074	Deactivate virtual disk shrinking
VMW-VC-00075	Deactivate virtual disk erasure
VMW-VC-00096	Limit console connection sharing
VMW-VC-00099	Limit informational messages from the VM to the VMX file.
VMW-VC-00101	Prevent unauthorized removal, connection and modification through the `isolation.device.connectable.disable` parameter.
VMW-VC-00102	Restrict sending host information to guests.
VMW-VC-00561	Audit all uses of PCI or PCIe pass-through functionalities.
VMW-VC-01232	Lock the virtual machine guest operating system when the last console connection is closed.
VMW-VC-01233	Deactivate 3D features on the virtual machine when not required.
VMW-VC-01242	Configure Log size on the virtual machine.

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)
$AdvancedSettingsTrue =
("isolation.tools.copy.disable","isolation.tools.dnd.disable","isolation.tools.paste.disabl
e","isolation.device.connectable.disable","tools.guest.desktop.autolock","isolation.tools.d
iskShrink.disable")
$AdvancedSettingsFalse = ("tools.guestlib.enableHostInfo","mks.enable3d")
Foreach ($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
        }
        elseif($setting.Value -ne $true){
            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
        }
        elseif($setting.Value -ne $false){
            Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value false -Confirm:$false
        }
    }
    $advancedSetting = "tools.setinfo.sizeLimit"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object
-Property Name, Value
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 1048576
-Confirm:$false
    }
    elseif($setting.Value -ne 1048576){
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value 1048576 -Confirm:$false
    }
        $advancedSetting = "log.rotateSize"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object
-Property Name, Value
    if(!$setting.Name){
        Get-VM $vm | New-AdvancedSetting -Name $advancedSetting -Value 2048000
-Confirm:$false
    }
    elseif($setting.Value -ne 2048000){
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value 2048000 -Confirm:$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
    }
    elseif($setting.Value -ne 1){
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value 1 -Confirm:$false
        }
    $advancedSetting = "pciPassthru*.present"
    $setting = Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Select-Object
```

```
-Property Name, Value
    if($setting.Name -and $setting.Value -ne $false){
        Get-VM $vm | Get-AdvancedSetting -Name $advancedSetting | Set-AdvancedSetting
-Value false -Confirm:$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 Encryption from the vSphere Client

You activate vSAN Data-At-Rest 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
Plan your vSAN capacity. VMW-vSAN-00186	Ensure you have sufficient capacity in the management vSAN cluster for the management VMs. You can expand the datastore by adding capacity devices or hosts with capacity devices to the cluster.

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 Encryption from the vSphere Client

You activate vSAN Data-At-Rest 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 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 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-At-Rest-Encryption **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.

Securing NSX-T Data Center 7

You perform the procedures on different components of NSX-T Data Center.

Procedure

1 Security Best Practices for Securing NSX-T Data Center

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

2 Configure Security Settings for NSX-T Data Center by Using the User Interfaces

You perform the procedure in NSX-T Data Center 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-T Data Center instances in your VMware Cloud Foundation environment.

3 Configure Security Settings for NSX-T Data Center by Using CLI Commands

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

4 Configure Security Settings for NSX-T Data Center by Using NSX-T API

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

5 Optional Security Configurations for NSX-T Data Center

The use of the NSX-T Data Center gateway firewall requires additional evaluation. This guidance does not cover the use of the gateway firewall to protect components deployed on overlay port groups. You can use the NSX-T Data Center gateway firewall to protect vRealize Automation and vRealize Operations Manager. Such configurations must be additionally evaluated based on your architecture. Similary, the edge configurations must be evaluated if you deploy an NSX-T Edge cluster.

Security Best Practices for Securing NSX-T Data Center

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

Table 7-1. NSX-T Data Center

Best Practice and Configuration ID	Description
Install security patches and updates for NSX-T Data Center. VMW-NSXT-01447	You install all security patches and updates for NSX-T Data Center as soon as the update bundles are available in SDDC Manager. Do not apply patches to NSX-T Data Center manually in a VMware Cloud Foundation environment unless directed to do so by VMware Global Support. If you patch the environment without using SDDC Manager you can cause problems with automated upgrades or actions in the future.
Use roles and privileges in NSX Manager to limit user privileges. VMW-NSXT-01410	Users and service accounts must be assigned the required privileges only. You can create a new role with reduced permissions. Navigate to **System > 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 > 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 VMware Workspace ONE Access with NSX-T Data Center. VMW-NSXT-01415	Use vIDM or Workspace ONE configured to meet requirements for authentication, authorization, and access control.
Validate the integrity of the installation media, patch, or upgrade files in NSX Manager. VMW-NSXT-01408	To validate the integrity of the patch or upgrade received from a vendor, verify the authenticity of the software prior to installation. This ensures the software is not tampered with and is provided by a trusted vendor. Always download VMware software from VMware secure website by using a secure connection. Verify the MD5/SHA1 hash output of the downloaded media with the value posted on the VMware secure website. MD5/SHA1 hashes must match.
Configure NTP servers for the NSX Manager nodes and ensure NTP servers are authorized per your organization's policies. VMW-NSXT-01401	Configure the NSX Manager nodes to synchronize internal system clocks by using redundant authoritative time sources. Ensure that all systems use the same relative time source (including the relevant localization offset), and that the relative time source can be correlated to an agreed-upon time standard (such as Coordinated Universal Time—UTC). This simplifies tracking and correlating the actions of an intruder when reviewing the relevant log files. Incorrect time settings can make it difficult to inspect and correlate log files to detect attacks, and can make auditing inaccurate.
Either use a valid TLS certificate or create a way to specify a self-signed certificate that is used for certificate pinning. VMW-NSXT-01486	NSX-T Data Center admin implicitly receives the Workspace ONE Access admin token because the stored client credentials are not scoped to just RO on Workspace ONE Access. You must modify Workspace ONE Access to provide fine-grained access controls.

Table 7-1. NSX-T Data Center (continued)

Best Practice and Configuration ID	Description
Do not install or use software not supported by VMware on your NSX-T Data Center appliances. VMW-NSXT-01444	To minimize the threat to infrastructure, do not install or use any software not supported by VMware. Do not add other software components to the NSX-T Data Center appliances as it is an untested configuration and could potentially interfere with the operation of the security functions they provide.
Ensure the SFTP server directory that stores the NSX-T backup is secured with proper directory permissions and the backup user has strong password. VMW-NSXT-01406 VMW-NSXT-01482	Dedicate a user for the backup directory on your SFTP server and remove access to the backup directory for all other users. Configure a single user with read and write permissions for the backup directory on your SFTP server. Set a strong password for the backup user.
Ensure that IPv4 DNS server is authorized and secure VMW-NSXT-01405	Mitigate the risk of DNS based vulnerabilities by ensuring that the IPv4 DNS servers are authorized, hardened, and secure.
Isolate virtual network tunnel traffic. VMW-NSXT-01402	To mitigate the risk of tampering with the virtual network, virtual network tunnel traffic must be separated from other traffic. The physical NIC for the virtual tunneling end point (TEP) must be on an isolated network. Physical isolation provides better security than VLAN segment isolation.
Restrict access to the NSX Manager nodes in your vSphere environment. VMW-NSXT-01404	Based on the principle of least privilege, use role-based access control (RBAC) to restrict access to the NSX-T Data Center infrastructure in your environment. Inspect users with access to the NSX Manager nodes. Only intended administrators must have access to the nodes or be able to perform any administrative actions on these nodes.
Monitor the use of APIs. VMW-NSXT-01516	NSX Manager provides management plane protection from denial of service (DoS) attacks by limiting transactions per second and concurrent transactions through the NSX REST API. There is no built-in mechanism to restrict access to the NSX REST API, API access and usage must be monitored through log aggregation.
Monitor any possible port scan attack on NSX manager. VMW-NSXT-01523	NSX manager only opens port which are required for functioning of NSX. Please look at port & protocol requirement in the Installation guide. Review activity logs for any access tried on ports not open. Have mangement network with FW policy to restrict acccess only to required ports on NSX manager appliance.
Use SFTP for backup and restoration. VMW-NSXT-01517	Do not use unecnrypted FTP for backup purposes. Ensure that you scedule regular backups and use encrypted channels to decrease the risks of data breaches.
Harden the SFTP server used for NSX-T Data Center backups. VMW-NSXT-01518	To minimize the threat of tampering or unauthorized access, use an SFTP server for NSX-T Data Center backups that is hardened, patched, and properly configured.

Table 7-1. NSX-T Data Center (continued)

Best Practice and Configuration ID	Description
Ensure that Syslog server is authorized and the configuration is appropriate. VMW-NSXT-01519	After you enable log aggregation through configuring a syslog server, you must ensure that the remote syslog server is authorized and secure. Use a SIEM solution or a syslog server solution such as VMware Log Insight and configure it to securely collect NSX-T Data Center logs.
Ensure the communication between NSX-T Data Center and your identity provider is encrypted. VMW-NSXT-01520	NSX supports both the LDAP and LDAPS protocols. Uses the TLS certificate provided by LDAP server. Use an encrypted channel through LDAPS between the identity provider and NSX-T Data Center.

Configure Security Settings for NSX-T Data Center by Using the User Interfaces

You perform the procedure in NSX-T Data Center 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-T Data Center 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-NSXT-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-NSXT-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**.

Configure Security Settings for NSX-T Data Center by Using CLI Commands

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

Procedure

1 VMW-NSXT-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 syslog server, run `set logging-server <server-ip_or_server-name> proto tcp 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.

2 VMW-NSXT-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 auth-policy minimum-password-length 15
```

3 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-NSXT-01416 Configure session lock after a 15-minute period of inactivity.

```
Set service http session-timeout 900
```

c VMW-NSXT-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-NSXT-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 NSX-T Data Center by Using NSX-T API

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

Procedure

- VMW-NSXT-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 NSX-T Data Center

The use of the NSX-T Data Center gateway firewall requires additional evaluation. This guidance does not cover the use of the gateway firewall to protect components deployed on overlay port groups. You can use the NSX-T Data Center gateway firewall to protect vRealize Automation and vRealize Operations Manager. Such configurations must be additionally evaluated based on your

architecture. Similary, the edge configurations must be evaluated if you deploy an NSX-T Edge cluster.

Caution The following configurations are not officially tested with VMware Cloud Foundation. These configurations are included as optional and site-specific only.

Product	Configuration	Context for Evaluating the Configuration
NSX-T Data Center (Gateway Firewall configurations)	Multiple configurations for the NSX-T Data Center gateway firewall. VI-NET-CFG-01428, VI-NET-CFG-01429, VI-NET-CFG-01431, VI-NET-CFG-01432,VI-NET-CFG-01453,VI-NET-CFG-01456, VI-NET-CFG-01464, VI-NET-CFG-01493, VI-NET-CFG-01494, VI-NET-CFG-01495, VI-NET-CFG-01496, VI-NET-CFG-01513, VI-NET-CFG-01514, VI-NET-CFG-01515	The gateway firewall protects components deployed on overlay port groups such as vRealize Automation or vRealize Operations Manager. The scope of the compliance kit includes ESXi, vCenter Server, vSAN, NSX Manager, and SDDC Manager, which are not deployed on overlay port groups. If you use vRealize Suite products, you must reevaluated this configuration.
NSX-T Data Center (Edge configurations)	VMW-NSXT-01430, VMW-NSXT-01435, VMW-NSXT-01437, VMW-NSXT-01438, VMW-NSXT-01441, VMW-NSXT-01449, VMW-NSXT-01450, VMW-NSXT-01455, VMW-NSXT-01459, VMW-NSXT-01460, VMW-NSXT-01469, VMW-NSXT-01470, VMW-NSXT-01503, VMW-NSXT-01504, VMW-NSXT-01505, VMW-NSXT-01506, VMW-NSXT-01507, VMW-NSXT-01510, VMW-NSXT-01511, VMW-NSXT-01512	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-T edges in your environment.

Security Best Practices for Securing NSX-T Edge Nodes

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

Table 7-2. Security Best Practices for Securing NSX-T Edge Nodes

Best Practice and Configuration ID	Description
You configure the NSX-T tier-0 gateway to reject inbound route advertisements for any prefixes belonging to the local autonomous system (AS). VMW-NSXT-01435	Accepting route advertisements belonging to the local AS can result in traffic looping or being black holed, or at a minimum, using a non-optimized path. For every NSX-T Tier-0 gateway, view route filters for every eBGP neighbor and ensure that the in-filter is configured with a prefix list that rejects prefixes belonging to the local AS.
Deactivate Protocol Independent Multicast (PIM). VMW-NSXT-01437	You configure the multicast NSX-T tier-0 gateway to deactivate PIM on all interfaces that are not required to support multicast routing. If multicast traffic is forwarded beyond the intended boundary, it is possible that it can be intercepted by unauthorized or unintended personnel. Limiting where, within the network, a given multicast group data is permitted to flow is an important first step in improving multicast security.
Deactivate inactive interfaces on an NSX-T Tier-0 gateway. VMW-NSXT-01438	You configure the NSX-T tier-0 gateway to have all inactive interfaces deactivated. An inactive interface is rarely monitored or controlled and might expose a network to an undetected attack on that interface. If an interface is no longer used, the configuration must be deleted and the interface deactivated. For sub-interfaces, delete sub-interfaces that are on inactive interfaces and delete sub-interfaces that are inactive.
Enforce a Quality-of-Service (QoS) policy. VMW-NSXT-01441, NIST800-53-VI-NET-CFG-01512	To limit the effects of packet flooding denial-of-service attacks, you configure the NSX-T tier-0 and tier-1 gateways to enforce a Quality-of-Service policy. Ensure that mechanisms for traffic prioritization and bandwidth reservation exists.
Disconnect inactive linked segments for NSX-T Tier-1 gateways. VMW-NSXT-01442	For each segment attached to an NSX-T Tier-1 gateway that is not in use, edit the segment and set the connectivity to None.
Ensure sufficient password strength and complexity for NSX-T Edge administrators. VMW-NSXT-01450	Ensure that your organization's security policies are enforced for local NSX-T Edge users with administrative rights.

Table 7-2. Security Best Practices for Securing NSX-T Edge Nodes (continued)

Best Practice and Configuration ID	Description
You configure the BGP NSX-T tier-0 gateway to use a unique key for each autonomous system (AS) that it peers with. VMW-NSXT-01459	If the same keys are used between eBGP neighbors, risks of compromising any of the BGP sessions increases. It is possible that a malicious user exists in one autonomous system who can know the key used for the eBGP session. This user would then be able to hijack BGP sessions with other trusted neighbors. For every NSX-T Tier-0 gateway, view timers and password for every external BGP (eBGP) neighbor and configure password with a unique key.
Restrict access to the NSX-T Edge nodes in your vSphere environment. VMW-NSXT-01521	Based on the principle of least privilege, use role-based access control (RBAC) to restrict access to the NSX-T Edge nodes in your vSphere environment. Inspect users with access to the NSX-T Edge nodes. Only intended administrators must have access to the nodes or be able to perform any administrative actions on these nodes.

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

You perform the procedure in NSX-T Data Center 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-T 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-NSXT-01428, VMW-NSXT-01513 Ensure that the NSX-T Gateway Firewall on the tier-0 and tier-1 gateways does not have any unpublished firewall policies or rules.

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

   b In the left pane, navigate to **North South security > 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 with unpublished changes, review any unpublished changes and click either **Revert** or **Publish**.

   f Repeat the procedure for each tier-1 gateway with unpublished changes.

3 VMW-NSXT-01429, VMW-NSXT-01514 Configure the NSX-T 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 **North South security > 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.

4 VMW-NSXT-01431, VMW-NSXT-01432 Configure the NSX-T 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 **North South security > 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**.

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

g Repeat the procedure for each tier-1 gateway.

5 VMW-NSXT-01453, VMW-NSXT-01515 Configure flood protection profiles on the NSX-T 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 Activate **SYN cache** and **RST spoofing**.

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

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

6 VMW-NSXT-01455, VMW-NSXT-01510 Create a spoof guard segment profile with port binding activated and apply the profile to all the segments.

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

b In the left pane, navigate to **Connectivity > Segments**.

c Click the **Segment profiles** tab.

d From the **Add segment profile** drop-down menu, select **Spoof guard**.

e Enter a name for the profile, activate **Port bindings** toggle switch, and click **Save**.

f Click the **Segments** tab.

g Next to the segment you want to configure, click the vertical ellipsis and click **Edit**.

h Expand the **Segment profiles** section, from the **Spoof guard** drop-down menu, select the newly created spoof guard segment profile, click **Save**, and click **Close editing**.

i Repeat this step for the remaining configured segments.

7 VMW-NSXT-01456, VMW-NSXT-01464 Configure ingress filters for inbound traffic through any active external interface on the NSX-T tier-0 and tier-1 Gateway Firewall.

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 **North South security > Gateway firewall**.

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

d From the **Gateway** drop-down menu, select the target NSX-T tier-0 gateway.

e For any rules that have individual interfaces specified in the **Applied to** field, in the **Applied to** column, click **Edit** and deselect the interfaces, leaving only the NSX-T gateway object type selected.

f Click **Apply** and click **Publish**.

g Repeat this step for all NSX-T tier-1 gateways.

8 VMW-NSXT-01460 To protect against route table flooding and prefix de-aggregation attacks, configure the NSX-T 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-T 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-NSXT-01493` Configure the NSX-T tier-0 gateway to restrict traffic destined to itself.

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

b In the left pane, navigate to **North South security > Gateway Firewall**.

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

d From the **Gateway** drop-down menu, select the NSX-T tier-0 gateway.

e Click **Add rule** and, in the **Destination** column, click the **Edit** button.

f On the **Set destination** dialog box, select all IP addresses for external interfaces, and click **Apply**.

g On the **Gateway Firewall** page, in the **Action** column for the new rule, from the **Action** drop-down menu, select **Drop** or **Reject**.

h Click the **Settings** icon and, on the **Settings** dialog box, activate the **Logging** toggle.

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

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

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

l If necessary, you can configure additional rules to allow traffic to external interface IP addresses and place them above this rule.

10 `VMW-NSXT-01494`, `VMW-NSXT-01495`, `VMW-NSXT-01496` Configure the NSX-T 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-T Data Center 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 **North South security > Gateway Firewall**.

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

d From the **Gateway** drop-down menu, select the NSX-T tier-0 gateway.

e Click **Add rule** and, in the **Services** column, click the **Edit** button.

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

g On the **Gateway Firewall** page, click the **Settings** icon and, on the **Settings** dialog box, activate the **Logging** toggle.

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

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

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

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

Configure Security Settings for NSX-T Edge Nodes by Using CLI Commands

You deactivate the SSH service start on boot on the NSX-T edge appliances. You configure the NSX-T Gateway Firewall to send logs to a central log server.

You perform these procedures on the NSX-T tier-0 and tier-1 gateway only if your environment uses NSX-T 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-T Edge node, right-click the appliance, and select **Open remote console**.

3 VMW-NSXT-01430, VMW-NSXT-01511 Configure the NSX-T 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-T Edge appliance.

a 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
```

b 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-T Edge node and if DoS incidents are detected.

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	Terminate shell services on the ESXi host. VI-ESXI-CFG-00039	SDDC Manager requires SSH for bring up and life cycle operations. Deactivating SSH prevents SDDC Manager workflows from accessing requisite hosts and may interfere with long running operations if SSH times out after it is started.
ESXi	The ESXi host must protect the confidentiality and integrity of transmitted information by protecting ESXi management traffic. VMW-ESXI-00178	VMware Cloud Foundation deploys management domain components (vCenter Server, NSX-T Data Center, SDDC Manager) on a shared network across ESXi hosts. This architecture cannot be changed after deployment.
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.

Product	Configuration	Context for Excluding Configuration
NSX-T Data Center	Configure logging for distributed firewall rules. VI-NET-CFG-01409	Users can only configure logging for the default rules available in NSX-T Data Center. VMware Cloud Foundation does not support configuring additional Distributed Firewall rules in the workload domain because most of the management appliances are deployed on Distributed Virtual Portgroups.
NSX-T Data Center	Create a spoof guard segment profile with port binding and apply the profile to all the segments VMW-NSXT-01413	VMware Cloud Foundation does not support configuring additional Distributed Firewall rules in the workload domain because most of the management appliances are deployed on Distributed Virtual Portgroups.
NSX-T Data Center	Multiple configurations for the NSX-T Data Center distributed firewall. VMW-NSXT-01425, VMW-NSXT-01452, VMW-NSXT-01489	VMware Cloud Foundation does not support configuring additional distributed firewall rules in the workload domain because most of the management appliances are deployed on Distributed Virtual Portgroups.
NSX-T Data Center	Deny network communications traffic by default and allow network communications traffic by exception on the distributed firewall. VMW-NSXT-01412	There is no guidance on allowing or denying traffic in NSX Manager used in the workload domain. Therefore, this configuration is not recommended. To avoid the workload domain inadvertently dropping or blocking required packets needed to support workload domain functionality, do not set the Default Layer3 Rule to Reject, which could drop traffic not captured by defined rules in the workload domain.
NSX-T Data Center	Restrict access to NSX Manager. VMW-NSXT-01491	VMware Cloud Foundation deploys NSX Manager nodes on the same management network as vCenter Server. This architecture cannot be changed after deployment.
NSX-T Data Center	The NSX-T Distributed Firewall must verify time based firewall rules. VMW-NSXT-01492	VMware Cloud Foundation does not support configuring additional distributed firewall rules in the workload domain because most of the management appliances are deployed on Distributed Virtual Portgroups.

Product	Configuration	Context for Excluding Configuration
NSX-T Data Center	Harden your VMware vSphere environment. VMW-NSXT-01446	Security for NSX-T Data Center requires a hardened vSphere environment. Due to specifics in the design of VMware Cloud Foundation, you must only use guidance for hardening vSphere as described in this guide. Configurations in other vSphere hardening guides might break VMware Cloud Foundation.
NSX-T Data Center	You configure the NSX-T Distributed Firewall to send traffic log entries to a central audit server. VMW-NSXT-01522	VMware Cloud Foundation does not support configuring additional distributed firewall rules in the workload domain because most of the management appliances are deployed on Distributed Virtual Portgroups.