# Security and Compliance Configuration for VMware Cloud Foundation 4.2

Modified on 10 JAN 2022
VMware Cloud Foundation 4.2
VMware Cloud Foundation 4.2.1

vmware®

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 4.2

*Security and Compliance Configuration for VMware Cloud Foundation* provides general guidance and step-by-step configuration for securing the 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 4.2 and VMware Cloud Foundation 4.2.1.

**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 |
| --- | --- |
| 09 JAN 2022 | ■ The guide is now validated for VMware Cloud Foundation 4.2 and VMware Cloud Foundation 4.2.1.<br>■ The guide is now validated and supports VI workload domains. You can apply the procedures to the management and VI workload domains.<br>■ NIST80053-VI-ESXi-CFG-01109 Configure the ESXi hosts to only run executable files from approved VIBs is now moved to the configurations that must be avoided in VMware Cloud Foundation environments.<br>■ NIST80053-VI-ESXI-CFG-00022 Configure the password complexity policy for the ESXi host is now a required configuration for VMware Cloud Foundation 4.2.1, it is still incompatible with VMware Cloud Foundation 4.2 and must be avoided.<br>■ Added new required configurations:<br>■ NIST80053-VI-ESXi-CFG-00564<br>■ NIST80053-VI-ESXi-CFG-01112<br>■ NIST80053-VI-NET-CFG-01498<br>■ NIST80053-VI-VC-CFG-01205<br>■ NIST80053-VI-VC-CFG-01238<br>■ NIST80053-VI-VC-CFG-01242<br>■ NIST80053-VI-NET-CFG-01445<br>■ NIST80053-VI-NET-CFG-01468<br>■ NIST80053-VI-NET-CFG-01501<br>■ NIST80053-VI-NET-CFG-01508<br>■ Added a new configuration that must be avoided - VI-ESXi-CFG-01109.<br>■ The procedures to configure multiple security settings on the ESXi hosts are now performed by using the ESXi Shell instead of using SSH.<br>■ NIST80053-VI-VC-CFG-01210 Restrict access to the cryptographic role is now part of the configurations for vCenter Server.<br>■ NIST800-53-VI-VC-CFG-00442 The configuration is now removed from the guide. |
| 11 MAY 2021 | vSAN encryption added to the document. |
| 13 APR 2021 | ■ Added a new section Security Configurations for Further Evaluation in the NSX-T Data Center best practices.<br>■ NSX-T distributed firewall configurations are now clarified.<br>■ ESXi login as root configuration added. |
| 16 MAR 2021 | 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 | 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 enable 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, ensuring that all encryption keys are available across regions to enable decryption in the 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-T Manager backups must be available on an SFTP server. The NSX-T 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, vRealize Operations Manager | VMware PowerCLI | n/a | VMware PowerCLI contains modules of cmdlets based on Microsoft PowerShell for automating vSphere, vSphere Automation SDK, vSphere Update Manager, vRealize Operations Manager, 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, SSH, 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 edit the `/etc/ssh/sshd_config` file on all the hosts to disable login as the root user, disallow compression, and disable port forwarding for the SSH daemon. You also enable secure boot and disable the OpenSLP service.

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, disable warnings, enable Bridge Protocol Data Unit (BPDU) filter, configure persistent log location, remote logging, VLAN setting, and enable bidirectional CHAP authentication using PowerCLI commands.

4 Enable Normal Lockdown Mode on the ESXi Hosts

You enable 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. ESXi Hosts

| Best Practice | Description |
|---|---|
| Add only system accounts to the ESXi exception users list.<br>NIST80053-VI-ESXI-CFG-00125 | You can add users to the exception users list from the vSphere Client. Such users do not lose their permissions when the host enters lockdown mode. Only add service accounts such as backup agents. Do not add administrative users or user groups to that list. |
| Install Security Patches and Updates for ESXi hosts.<br>NIST80053-VI-ESXi-CFG-00129 | You install all security patches and updates on the ESXi hosts as soon as the update bundles are available in SDDC Manager.<br>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 can not only lead to a less-secure environment, but may cause problems 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.<br>NIST80053-VI-ESXi-CFG-01106 | The CIM system provides an interface that enables hardware-level management from remote applications through a set of standard APIs. 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.<br>NIST80053-VI-ESXi-CFG-01113 | The default self-signed, VMCA-issued host certificate must be replaced with a certificate from a trusted Certificate Authority (CA). |

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

You edit the `/etc/ssh/sshd_config` file on all the hosts to disable login as the root user, disallow compression, and disable port forwarding for the SSH daemon. You also enable secure boot and disable the OpenSLP service.

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

### Procedure

1 Log in to an ESXi host by using ESXi Shell with the `root` user.

2 Open the VI editor to add or edit the settings in /etc/ssh/sshd_config.

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

a `NIST80053-VI-ESXi-CFG-00005` In the VI editor, add or correct the following line to disable login as the root user.

```
PermitRootLogin no
```

b `NIST80053-VI-ESXi-CFG-00012` In the VI editor, add or correct the following line to disallow compression for the ESXi host SSH daemon.

```
Compression no
```

c `NIST80053-VI-ESXi-CFG-01111` Add or correct the following line to disable port forwarding for the ESXi host SSH daemon.

```
AllowTcpForwarding no
```

d Save and close the VI editor.

e Restart the SSH service to apply the new configurations.

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

3 `NIST80053-VI-ESXi-CFG-01108` Enable secure boot on the host.

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

**Note** If the imaging appliance (VIA) is used to image the ESXi hosts it currently does not support UEFI which is a requirement for enabling secure boot. ESXi installations done through other methods are supported and can enable UEFI/secure boot.

If the output indicates that Secure Boot cannot be enabled, correct the discrepancies and try again.

4 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, disable warnings, enable Bridge Protocol Data Unit (BPDU) filter, configure persistent log location, remote logging, VLAN setting, and enable bidirectional CHAP authentication using PowerCLI commands.

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

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 `NIST80053-VI-ESXI-CFG-00022` If you are configuring VMware Cloud Foundation 4.2.1, configure the password complexity policy for the ESXi host.

This configuration is not compatible with VCF 4.2. The requirement is a length of minimum fifteen characters from four character classes that include lowercase letters, uppercase letters, numbers, special characters, and a 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 `NIST80053-VI-ESXI-CFG-00028` Configure the ESXi hosts firewall to only allow traffic from the ESXi management network.

```
$esxiHosts = Get-VMHost
foreach($esxiHost in $esxiHosts){
$esxcli = Get-EsxCli -VMHost $esxiHost.Name
#This disables the allow all rule for the target 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 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 `NIST80053-VI-ESXI-CFG-00030` Show warnings in the vSphere Client if local or remote shell sessions are enabled on the ESXi hosts.

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

5 NIST80053-VI-ESXI-CFG-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 NIST80053-VI-ESXI-CFG-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 NIST80053-VI-ESXI-CFG-00043 Run the command to enable the Bridge Protocol Data Unit (BPDU) filter.

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

8 NIST80053-VI-ESXI-CFG-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 NIST800-53-VI-ESXI-CFG-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 NIST80053-VI-ESXi-CFG-00114 Join ESXi hosts to an Active Directory (AD) domain to eliminate the need to create and maintain multiple local user accounts.

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

11 NIST80053-VI-ESXI-CFG-00122 Configure the login banner for the DCUI of the ESXi host.

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

12 NIST80053-VI-ESXI-CFG-00123 Configure the login banner for the SSH connections.

```
Get-VMHost | Get-AdvancedSetting -Name Config.Etc.issue | Set-AdvancedSetting -Value "This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their
```

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

13 NIST80053-VI-ESXI-CFG-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 NIST80053-VI-ESXi-CFG-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 NIST80053-VI-ESXi-CFG-00164 Configure a remote log server for the ESXi hosts.

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

16 NIST80053-VI-ESXi-CFG-00168 Set a timeout to automatically close idle DCUI sessions after 600 seconds.

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

17 NIST80053-VI-ESXi-CFG-00564 Set a timeout to automatically close sessions in the host client after 600 seconds of inactivity.

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

18 NIST80053-VI-ESXi-CFG-01102 Enable 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
```

19 NIST80053-VI-ESXi-CFG-01112 Disable the OpenSLP service on the host.

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

# Enable Normal Lockdown Mode on the ESXi Hosts

You enable 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 `NIST80053-VI-ESXI-CFG-00031` Enable 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**.

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, SSH, 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, smart Card configurations, proxy, login banners, LDAP, and other configurations.

3 Configure Security Settings for vCenter Server by Using PowerCLI

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

4 Configure Security Settings for vCenter Server by Using an SSH Client

You perform the procedure on all vCenter Server instances to configure session timeouts and MOB configurations.

5 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. vCenter Server

| Best Practice | Description |
|---|---|
| Assign correct roles to vCenter Server users.<br>NIST80053-VI-VC-CFG-00415 | Users and service accounts must only be assigned privileges they require. Least privilege principle requires that these privileges must only be assigned if needed, to reduce risk of confidentiality, availability, or integrity loss. |
| Use unique service accounts for applications that connect to vCenter Server.<br>NIST80053-VI-VC-CFG-00401 | Create a service account for each application that connects to vCenter Server. Only grant the required permissions for the application to run. |
| Restrict the use of the built-in single sign-on Administrator account.<br>NIST80053-VI-VC-CFG-00439 | Only use the administrator@vsphere.local account for emergencies and situations where no other option exists. The built-in single sign-on account must not be used for daily operations. Set up a policy that restricts the use of the account. |
| vCenter Server must restrict access to cryptographic permissions.<br>NIST80053-VI-VC-CFG-01211 | These permissions must be reserved for cryptographic administrators where VM encryption 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:<br>■ Cryptographic Operations privileges<br>■ Global.Diagnostics<br>■ Host.Inventory.Add host to cluster<br>■ Host.Inventory.Add standalone host<br>■ Host.Local operations.Manage user groups. |
| Use templates to deploy virtual machines<br>NIST80053-VI-VC-CFG-01235 | Use templates that contain a hardened, patched, and properly configured operating system to create other, application-specific templates. You can also use the application template to deploy virtual machines. |
| The vCenter Server must use LDAPS when adding an SSO identity source<br>NIST80053-VI-VC-CFG-01229 | To protect confidentiality 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 will enforce LDAPs. |
| The vCenter Server must implement Active Directory authentication<br>NIST80053-VI-VC-CFG-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<br>NIST80053-VI-VC-CFG-01230 | When adding an LDAP identity source to vSphere SSO the account used to bind to 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. |

Table 3-1. vCenter Server (continued)

| Best Practice | Description |
|---|---|
| Restrict access to the cryptographic role.<br>NIST80053-VI-VC-CFG-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 encryption or vSAN encryption is required. All other vSphere administrators who do not require cryptographic operations must be assigned the `No Cryptography Administrator` role. |
| The vCenter Server Machine SSL certificate must be issued by an appropriate certificate authority.<br>NIST80053-VI-VC-CFG-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. |

# 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, smart Card configurations, 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 |
|---|---|---|
| NIST80053-VI-VC-CFG-00421 | Maximum lifetime | 60 |

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 |
|---|---|---|
| NIST80053-VI-VC-CFG-00436 | Maximum number of failed login attempts | 3 |
| NIST80053-VI-VC-CFG-00434 | Time interval between failures | 900 Seconds |
| NIST80053-VI-VC-CFG-00435 | Unlock time | 0 seconds |

4 NIST80053-VI-VC-CFG-00442 Configure an alert if an error occurs with the ESXi remote syslog connection.

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**.

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

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

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

e On the **Alarm rule 1** page, under **If**, enter **`esx.problem.vmsyslogd.remote.failure`** 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 NIST80053-VI-VC-CFG-01219 Configure an alert to the appropriate personnel about SSO account actions

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

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

| Setting | Value |
|---|---|
| Alarm name | com.vmware.sso.PrincipalManagement |
| Target type | vCenter Server |

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

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

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

6 NIST80053-VI-VC-CFG-00418 Configure a proxy for the download of the public Hardware Compatibility List.

a In the **Hosts and Clusters** inventory, select the 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 **Configure the Proxy Server if your system uses one** check box.

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

7 NIST80053-VI-VC-CFG-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**.

8 NIST80053-VI-VC-CFG-01209 Configure a login message.

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

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

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

d In the **Details of login message** text box, enter **`This system is for the use of authorized users only. Individuals using this computer system without authority or in excess of their authority are subject to having all their activities on this system monitored and recorded by system personnel. Anyone using this system expressly consents to such monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personal may provide the evidence of such monitoring to law enforcement officials.`** and click **Save**.

9 NIST80053-VI-VC-CFG-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 Enable the service from the toggle switch and, from the **Authentication** drop-down menu, select **Mutual CHAP**.

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

10 NIST80053-VI-VC-CFG-01213 Configure Key Encryption Keys (KEKs) to be re-issued at 60 days intervals for the vSAN encrypted datastores.

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 **Data cervices** tile, click **Edit**.

d Turn on **Data-in-transit encryption** and enter a custom interval of **`86400`** minutes that equals 60 days.

e Click **Apply**.

11 NIST80053-VI-VC-CFG-01238 Disable SNMPv1/2 receivers.

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

b Click the **Configure** tab and, under **Settings**, click **General**.

c On the **vCenter Server Settings** page, click **Edit**.

d In the **Edit vCenter general settings** dialog box, click **SNMP receivers**.

e Disable all the enabled receivers and click **Save**.

12 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 |

# Configure Security Settings for vCenter Server by Using PowerCLI

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

### 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 `NIST80053-VI-VC-CFG-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 `NIST80053-VI-VC-CFG-01202` Configure all port groups to VLAN values not reserved by upstream physical switches

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

4 NIST80053-VI-VC-CFG-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 for vCenter Server by Using an SSH Client

You perform the procedure on all vCenter Server instances to configure session timeouts and MOB configurations.

### Procedure

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

| Setting | Value |
|---|---|
| FQDN | sfo01-m01-vc01.sfo.rainpole.io |
| User name | root |

2 Enter **shell** to launch BASH on the appliance.

3 NIST80053-VI-VC-CFG-00422 Run the commands so that vSphere Client sessions expire after 10 minutes of user inactivity and restart the service.

```
sed -i 's/session.timeout = 120/session.timeout = 10/' /etc/vmware/vsphere-ui/
webclient.properties

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

4 NIST80053-VI-VC-CFG-01203 Disable the managed object browser when not required for the purpose of troubleshooting or maintenance of managed objects.

a Navigate to and open **/etc/vmware-vpx/vpxd.cfg**

b Locate the **<vpxd>...</vpxd>** element.

c Add or update the element in the **<vpxd>** section with the **<enableDebugBrowse>false</enableDebugBrowse>** property.

d Run the command to restart the `vpxd` service.

```
service-control --restart vmware-vpxd
```

# 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 Appliance Management Interface.

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

2 `NIST80053-VI-VC-CFG-01218` Configure the appliance to send logs to a central log server.

a Select **Syslog** on the left navigation pane and click **Configure** to configure the address and port of a site-specific syslog aggregator or SIEM with the appropriate protocol and click **Save**.

b Note : UDP is discouraged due to it's stateless and unencrypted nature.

3 `NIST80053-VI-VC-CFG-01220` The vCenter Server configuration must be backed up on a regular basis.

a Select **Backup** on the left navigation pane 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**.

# Securing SDDC Manager

4

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

Table 4-1. SDDC Manager

| Best Practice | Description |
| --- | --- |
| SDDC Manager Backup<br>NIST80053-VI-SDDC-CFG-1600 | You must back up the 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 using APIs, and are not using composable servers or stretched clusters.<br>For image-based backups of SDDC Manager, use a solution compatible with VMware vSphere Storage APIs - Data Protection.<br>For file-based backups, configure an external SFTP server as a target backup location. |
| Install Security Patches and updates for SDDC Manager<br>NIST80053-VI-SDDC-CFG-1602 | Make sure you install all security patches and updates. To apply patches and updates to SDDC Manager, follow the guidance in the *VMware Cloud Foundation Lifecycle Management* document. |
| Use an SSL certificate issued by a trusted certificate authority on the SDDC Manager<br>NIST80053-VI-SDDC-CFG-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 on the Internet<br>NIST80053-VI-SDDC-CFG-1604 | Allowing access to the SDDC Manager appliance from the internet or externally to the organization could expose the server to denial of service attacks or other penetration attempts. Note that this fix refers to an entity outside the scope of SDDC Manager. Security Architect (SA) should work with network or boundary team to ensure proper firewall rules or other mechanisms are in place to protect the SDDC Manager appliance from being accessible externally to the organization. |

Table 4-1. SDDC Manager (continued)

| Best Practice | Description |
| --- | --- |
| Assign least privileges to users and service accounts in SDDC Manager<br>NIST80053-VI-SDDC-CFG-1605 | Users and service accounts must only be assigned privileges they require. Least Privilege requires that these privileges must only be assigned if needed, to reduce risk of confidentiality, availability, or integrity loss.<br>From the SDDC Manager UI, under **Administration > Users**, 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<br>NIST80053-VI-SDDC-CFG-1607 | Using a dedicated My VMware account when access is allowed to pull updates online will ensure consistent access to updates and security patches in the event of system administrator turnover or account access issues.<br>From the SDDC Manager UI, go to **Administration > Repository Settings**, configure a dedicated account that is not associated with a particular system administrator. |

# Securing Management Virtual Machines

5

To perform the procedure, you connect to the management domain vCenter Server and perform multiple configurations on the management virtual machines that belong to the management domain. vSphere Cluster Services (vCLS) nodes are not subject of securing as they are service VMs and not true VMs.

After you run the script, 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. Cold boot must be performed one VM at a time so that service are not interrupted. Cold boot of vCenter Server and SDDC Manager requires a maintenance window.

Perform cold boot in the following order:

1 NSX-T Edge nodes

2 NSX-T Manager nodes

3 vCenter Server

4 SDDC Manager

| Configuration ID | Description |
|---|---|
| NIST80053-VI-VC-CFG-00070 | Disable copy operations. |
| NIST80053-VI-VC-CFG-00071 | Disable drag and drop operations. |
| NIST80053-VI-VC-CFG-00073 | Disable paste operations. |
| NIST80053-VI-VC-CFG-00076 | Disable Host Guest File System (HGFS) file transfers. |
| NIST80053-VI-VC-CFG-00097 | Disable console access through the Virtual Network Computing protocol. |
| NIST80053-VI-VC-CFG-00099 | Limit informational messages from the VM to the VMX file. |
| NIST80053-VI-VC-CFG-00101 | Prevent unauthorized removal, connection and modification through the `isolation.device.connectable.disable` parameter. |
| NIST80053-VI-VC-CFG-00102 | Restrict sending host information to guests. |
| NIST80053-VI-VC-CFG-00561 | Audit all uses of PCI or PCIe pass-through functionalities. |
| NIST80053-VI-VC-CFG-01232 | Lock the virtual machine guest operating system when the last console connection is closed. |

| Configuration ID | Description |
|---|---|
| NIST80053-VI-VC-CFG-01233 | Disable 3D features on the virtual machine when not required. |
| NIST80053-VI-VC-CFG-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 Run the script to configure advanced settings on all management virtual machines.

You must enter the names of the VMs that you reconfigure in the first line of the script. For example, `$VMs = ("edge-node1", "nsx-manager1", "vcenter-server", "sddc-manager")`.

```
$VMs = (list-of-comma-seperated-management-domain-VM-names)
$AdvancedSettingsTrue =
("isolation.tools.copy.disable","isolation.tools.dnd.disable","isolation.tools.paste.disabl
e","isolation.tools.hgfsServerSet.disable","isolation.device.connectable.disable","tools.gu
est.desktop.autolock")
$AdvancedSettingsFalse =
("RemoteDisplay.vnc.enabled","tools.guestlib.enableHostInfo","pciPassthru*.present","mks.en
able3d")
Foreach ($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
    }
}
```

# 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 enable vSAN Data-At-Rest encryption on the vSAN cluster. Before you can enable vSAN encryption, you must set up a 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.<br>NIST80053-VI-Storage-SDS-CFG-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 `NIST80053-VI-Storage-SDS-CFG-00207` Configure a proxy for the download of the public Hardware Compatibility List.

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

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

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

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

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

# Configure vSAN Data-At-Rest Encryption from the vSphere Client

You enable vSAN Data-At-Rest encryption on the vSAN cluster. Before you can enable vSAN encryption, you must set up a Key Management Server (KMS) and establish a trusted connection between vCenter Server and the KMS.

- Do not deploy your 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 `VI-Storage-SDS-CFG-00183` Enable 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, enable the toggle switch of **Data-At-Rest encryption**, select a 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 from User Interfaces

You perform the procedure in NSX-T Data Center to configure logging servers, enable logging for distributed and gateway firewall rules, and enable port binding for Spoofguard profile. Configure the settings for all NSX-T Data Cnter instances in your VMware Cloud Foundation environment.

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

You configure NSX-T Manager to backup audit records to logging server, session timeouts, maximum authentication failures, password length. Also, you configure NSX-T Edge nodes to backup audit records to central audit server.

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

You enable TLS 1.2 protocol and disable TLS 1.1 for NSX-T manager.

## 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.<br>NIST80053-VI-NET-CFG-01447 | You install all security patches and updates for NSX-T Data Center as soon as the update bundles are available in SDDC Manager.<br>Do not apply patches to NSX-T Data Center manually in a VMware Cloud Foundation environment unless directed to do-so by 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-T Manager to limit user privileges.<br>NIST80053-VI-NET-CFG-01410 | Users and service accounts must only be assigned the required privileges.<br>To create a new role with reduced permissions, navigate to **System > Users and Roles > Roles** . Click **Add Role** and provide a name and the required permissions, and click **Save**.<br>You can reduce permissions to an existing role. Navigate to **System > Users and Roles > User Role Assignment**. Click the menu drop-down next to the target user or group, select edit, remove the existing role, select the new role, and click **Save**. |
| Integrate VMware Identity Manager with NSX-T Data Center.<br>NIST80053-VI-NET-CFG-01415 | You integrate NSX-T Data Center with VMware Identity Manager to enforce two-factor authentication. The integration ensures the individuals can be held accountable for the configuration changes they implement (non-repudiation). |
| The BGP NSX-T Tier-0 gateway must be configured to use a unique key for each autonomous system (AS) that it peers with.<br>NIST80053-VI-NET-CFG-01459 | If the same keys are used between eBGP neighbors, risks of a hacker compromising any of the BGP sessions increases. It is possible that a malicious user exists in one autonomous system who would know the key used for the eBGP session. This user would then be able to hijack BGP sessions with other trusted neighbors.<br>For every NSX-T Tier-0 gateway, view timers and password for every external BGP (eBGP) neighbor and configure password with a unique key. |
| Validate the integrity of the installation media or patch or upgrade in NSX-T Manager.<br>NIST80053-VI-NET-CFG-01408 | Verify the authenticity of the software prior to installation to validate the integrity of the patch or upgrade received from a vendor. This ensures the software has not been tampered with and has been provided by a trusted vendor.<br>Always download VMware software from VMware Secure website 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 hash must match. |
| Configure NTP servers for the NSX-T Manager nodes<br>NIST80053-VI-NET-CFG-01401 | Configure the NSX-T Manager nodes to synchronize internal information system clocks using redundant authoritative time sources. |

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

| Best Practice and Configuration ID | Description |
| --- | --- |
| Ensure that any NTP servers you use are authorized as per your own policies.<br>NIST80053-VI-NET-CFG-01445 | 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). It is simpler to track and correlate 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.<br>NIST80053-VI-NET-CFG-01486 | NSX-T Data Center admin implicitly receives Workspace ONE Access admin token due to the fact that the stored client credentials are not scoped to just RO on Workspace ONE Access. This is the risk until modify Workspace ONE Access to offer finer grains access controls. |
| Do not install or use software not supported by VMware on your NSX-T Data Center appliances.<br>NIST80053-VI-NET-CFG-01444 | Do not install or use any software not supported by VMware to minimize the threat to infrastructure. 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. |
| The NSX-T Tier-0 Gateway must be configured to reject inbound route advertisements for any prefixes belonging to the local autonomous system (AS).<br>NIST80053-VI-NET-CFG-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 Filter for every eBGP neighbor and ensure that the In Filter is configured with a prefix list that rejects prefixes belonging to the local AS. |
| The NSX-T Tier-0 Gateway must be configured to use its loopback address as the source address for iBGP peering sessions.<br>NIST80053-VI-NET-CFG-01462 | When the loopback address is used as the source for eBGP peering, the BGP session is harder to hijack as the source address to be used is not known globally—making it more difficult for a hacker to spoof an eBGP neighbor. By using `traceroute`, a hacker can easily determine the addresses for an eBGP speaker when the IP address of an external interface is used as the source address. The routers within the iBGP domain must also use loopback addresses as the source address when establishing BGP sessions.<br>For every NSX-T Tier-0 gateway, view Source Address for every internal BGP (iBGP) neighbor and configure it with an NSX-T Tier-0 gateway loopback address. |
| Disable Protocol Independent Multicast (PIM).<br>NIST80053-VI-NET-CFG-01437 | The multicast NSX-T Tier-0 gateway must be configured to disable 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. |

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

| Best Practice and Configuration ID | Description |
| --- | --- |
| Disable inactive interfaces on an NSX-T Tier-0 gateway.<br>NIST80053-VI-NET-CFG-01438 | An NSX-T Tier-0 gateway must be configured to have all inactive interfaces disabled. 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 disabled. 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.<br>NIST80053-VI-NET-CFG-01441, NIST800-53-VI-NET-CFG-01512 | The NSX-T Tier-0 and Tier-1 gateways must be configured to enforce a Quality-of-Service policy to limit the effects of packet flooding denial-of-service attacks. Ensure that mechanisms for traffic prioritization and bandwidth reservation exists. |
| Implement measures to protect against Denial-of-Service attacks.<br>NIST80053-VI-NET-CFG-01488 | As Bidirectional Forwarding Detection (BFD) might be tied into the stability of the network infrastructure (such as routing protocols), the effects of an attack on a BFD session might be serious. A link might be falsely declared to be down, or falsely declared to be up. In either case, the effect is denial of service. Implementing appropriate measures against DoS attack is critical. Edge checks for max-allowed-hops or TTL check for ingress BFD packets to mitigate spoofing attacks. |
| Disable inactive linked segments for NSX-T Tier-1 gateways.<br>NIST80053-VI-NET-CFG-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 the directory where the NSX-T backup is stored on the SFTP server is secured with proper directory permissions.<br>NIST80053-VI-NET-CFG-01406<br>NIST80053-VI-NET-CFG-01482 | Dedicate a user for the backups directory on your SFTP Server and restrict the access of all other users to that directory. Configure a single user with read and write permissions for the directory that stores backups on your SFTP server. Configure a strong password for the backup user. |
| Ensure that IPv4 DNS is authorized and secure<br>NIST80053-VI-NET-CFG-01405 | By ensuring that the IPv4 DNS servers are authorized and secure would mitigate the risks against DNS based vulnerabilities. Also, ensure that the DNS server is hardened based on the best practice guidelines. |

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

| Best Practice and Configuration ID | Description |
|---|---|
| Isolate Virtual network tunnel traffic.<br>NIST80053-VI-NET-CFG-01402 | Virtual network tunnel traffic (Geneve) must be separated from other traffic to avoid tampering with the tunnel. The Physical NIC for the virtual tunneling end point (TEP) must be on an isolated network with the other TEPs in your data center on trusted ESXi hosts. You can isolate this to a VLAN segment, but for extra safety use physical isolation. Thoroughly review the deployment and ensure that the virtual network is isolated. |
| Restrict access to the NSX-T Manager nodes and NSX-T Edge nodes in your vSphere environment.<br>NIST80053-VI-NET-CFG-01404 | Users that have access to the NSX-T Manager nodes and NSX-T Edge nodes in your vSphere environment could potentially cause harm by intentionally or unintentionally performing power off, suspend, migrate, or other administrative functions. It is important that the access is protected using user access controls or separating and isolating the environment.<br>Log in to the vSphere Client and inspect users that have access permissions to the NSX-T Manager nodes and NSX-T Edge nodes. No user other than the intended administrator should have access to the nodes or be able to perform any administrative actions on these nodes. |

## Security Configurations for Further Evaluation

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 configuration must be additionally evaluated based on your architecture.

| Product | Configuration | Context for Evaluating the Configuration |
|---|---|---|
| NSX-T Data Center | Multiple configurations for the NSX-T Data Center gateway firewall.<br>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-T Manager, and SDDC Manager, which are not deployed on overlay port groups.<br>This configuration should be reevaluated if you use vRealize Suite products. |

# Configure Security Settings for NSX-T Data Center from User Interfaces

You perform the procedure in NSX-T Data Center to configure logging servers, enable logging for distributed and gateway firewall rules, and enable port binding for Spoofguard profile. Configure the settings for all NSX-T Data Cnter instances in your VMware Cloud Foundation environment.

Procedure

1 In a Web browser, log in to an NSX-T Manager by using the user interface and go to **Policy** View.

| Setting | Value |
|---|---|
| URL | https://sfo-m01-nsx01.sfo.rainpole.io |
| User name | administrator@vsphere.local |

2 `NIST80053-VI-NET-CFG-01413`, `NIST80053-VI-NET-CFG-01455`, `NIST80053-VI-NET-CFG-01510` Create a Spoof Guard segment profile with port binding enabled and apply the profile to all the segments.

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

   b In the upper-right corner, switch to the **Policy** tab.

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

   d In the left pane, click **Segments** and click the **Segment Profiles** tab.

   e Click **Add Segment Profile > Spoof Guard**.

   f Enter name for the profile, enable **Port Bindings**, and click **Save**.

   g Click the **Segments** tab.

   h Click the **ellipses** menu and click **Edit** next to the segment you want to configure.

   i Under **Segment profiles**, from the **Spoof guard** drop-down menu, select the newly created Spoof Guard segment profile, click **Save**, and click **Close editing**.

   j Repeat for the remaining configured segments.

3 `NIST80053-VI-NET-CFG-01460` Configure the Tier-0 gateway to use the maximum prefixes setting to protect against route table flooding and prefix de-aggregation attacks.

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

   b In the left pane, click **Tier-0 gateways**.

   c Expand the Tier-0 gateway to see its full configuration.

   d Expand the **BGP** section and click the number for the **BGP Neighbors**.

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

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

g In the **Set Route Filter** dialog box, click the **vertical ellipses** menu and click **Edit** to configure the maximum routes value, specific to your environment.

h Repeat the step as needed to configure all neighbors with a maximum routes value.

4 `NIST80053-VI-NET-CFG-01468` The NSX-T Manager must be configured to perform backups on an organizational defined schedule.

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

b In the left pane, under **Lifecycle Management**, click **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 Enable **Detect NSX configuration change** to perform backups on detection of configuration changes, specify an interval for detecting changes, and click **Save**.

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

You configure NSX-T Manager to backup audit records to logging server, session timeouts, maximum authentication failures, password length. Also, you configure NSX-T Edge nodes to backup audit records to central audit server.

### Procedure

1 `NIST80053-VI-NET-CFG-01414` Configure NSX-T 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-T Manager appliance.

a Open the VM console of the NSX-T 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 a tls 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 `NIST80053-VI-NET-CFG-01421` Enforce a minimum of 15 characters for password length on the NSX-T Manager nodes.

a Open the VM console of an NSX-T 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 `NIST80053-VI-NET-CFG-01430`, `NIST800-53-VI-NET-CFG-01511` Configure the NSX-T Tier-0 and Tier-1 gateway firewall to send logs to a central log server.

You can configure the logging server with one of the following protocols: `li-tls` or `tls`. The server and client certificates must be stored in the `/image/vmware/nsx/file-store` on each NSX-T Edge Gateway appliance.

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

b 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.

c If you want to configure a li-tls syslog server, run `set logging-server <server-ip or server-name> proto li-tls level info serverca root-ca.crt` and press Enter.

4 Configure login sessions settings for the NSX-T manager.

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

b `NIST80053-VI-NET-CFG-01416` Configure session lock after a 15-minute period of inactivity.

```
set service http session-timeout 900
```

c `NIST80053-VI-NET-CFG-01418` Prevent an account from further login attempts by using the UI or API after three consecutive failed login attempts.

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

d `NIST80053-VI-NET-CFG-01498` Prevent an account from further login attempts by using CLI after three consecutive failed login attempts.

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

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

You enable TLS 1.2 protocol and disable TLS 1.1 for NSX-T manager.

### Procedure

1 `NIST80053-VI-NET-CFG-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
```

2 `NIST80053-VI-NET-CFG-01508` Enable the global FIPs compliance mode for load balancers on the NSX-T Manager nodes.

a Run the GET command and save the output.

```
GET https://<nsx-mgr>/policy/api/v1/infra/global-config
```

b In the saved output, edit the `fips` line to enable global FIPs setting for load balancers.

```
{ "fips": { "lb_fips_enabled": true }, "resource_type": "GlobalConfig",
"_revision": 2 }
```

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

Use the global setting when you create new load balancer instances. Changing the setting does not affect existing load balancer instances.

```
PUT https://<nsx-mgr>/policy/api/v1/infra/global-config
```

d To update existing load balancers to use this setting do the following:

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

f In the left pane, click **Load Balancing** under **Network Services**.

g Click **Edit** on the target load balancer.

h In the attachment field click the **X** to detach the load balancer from it's current Gateway and click **SAVE**.

i Click **Edit** on the target load balancer again and reattach it to its Gateway and click **SAVE**.

Detaching a load balancer from the Tier-1 gateway results in a traffic interruption for the load balancer instance.

# 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 | Enforce multiple vCenter Server password complexity rules.<br>`VI-VC-CFG-00410` | When rotating passwords, SDDC Manager does not take into account password complexity configured on the target vCenter Server. This might result in a new password that does not meet SDDC manager password requirements and workflows might fail. |
| vCenter Server | Isolate all management traffic on the vSphere Distributed Switch from other traffic types.<br>`VI-VC-CFG-01223` | VMware Cloud Foundation deploys vCenter Server, NSX-T Data Center, and SDDC Manager on a shared network across ESXi hosts. This architecture cannot be changed after deployment. |
| vCenter Server | vCenter Server must be isolated from the public Internet but must still allow for patch notifications and delivery.<br>`VI-VC-CFG-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 | Disable non-essential capabilities by disabling SSH on the ESXi host.<br>`VI-ESXi-CFG-00111` | SDDC Manager requires SSH for bring up and lifecycle operations. Disabling SSH prevents SDDC Manager workflows from accessing requisite hosts. |
| ESXi | Terminate shell services on the ESXi host.<br>`VI-ESXi-CFG-00039` | SDDC Manager requires SSH for bring up and lifecycle operations. Disabling SSH prevents SDDC Manager workflows from accessing requisite hosts. |
| ESXi | Configure the ESXi hosts to only run executable files from approved VIBs.<br>`VI-ESXi-CFG-01109` | The ExecInstalledOnly policy prevents any executable to run on an ESXi host which was not installed by using a VIB. Update Manager and Lifecycle Manager workflows using baselines require to push an Upgrade-Agent (vua) to the ESXi. If ExecInstalledOnly is enabled, the vua agent is not allowed to be executed that breaks the Update Manager or Lifecycle Manager workflows. |

| | | |
|---|---|---|
| NSX-T Data Center | Enable logging for distributed firewall rules.<br>VI-NET-CFG-01409 | Users can only enable 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 | Multiple configurations for the NSX-T Data Center distributed firewall.<br>VI-NET-CFG-01425, VI-NET-CFG-01452, VI-NET-CFG-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.<br>VI-NET-CFG-01412 | There is no guidance on allowing or denying traffic in NSX-T 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 | Enforce password complexity rules on NSX-T Edge nodes.<br>VI-NET-CFG-1450 | SDDC Manager enforces password complexity rules on the credentials. This could result in a new password that does not meet SDDC manager password requirements and might cause workflows to fail. |
| NSX-T Data Center | Restrict access to NSX Manager.<br>VI-NET-CFG-01491 | VMware Cloud Foundation deploys NSX-T 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.<br>VI-NET-CFG-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. |
| NSX-T Data Center | Harden your VMware vSphere environment.<br>VI-NET-CFG-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. |