VMware ESXi 7 and 8 Hardening Guide

Contents

1. VMware Security Overview

1.1 Enterprise Directory service

Description:

Using an Enterprise Directory service like Active Directory allows for password and role management and single login credential storage, but if the Directory was compromised, an attacker could promote themselves to have permissions to the VMware ESXi servers, or vCenter Server.

For a script to validate the hardening of ESXi hosts, please contact your Security Solutions Architect.

Recommendation:

Do not use an Enterprise Directory service for authentication to integrated hardware management, i.e. iDRAC, ILO, or xClarity. Instead, use long, complex passwords, store them, and only use in emergency cases, or for maintenance. Also, using an Enterprise Directory service could cause issues during emergency access, if the Directory is unreachable.

Do not join vCenter or ESXi servers to an Enterprise Directory service. Instead, use a separate Directory service that is separate from the Corporate Directory service, or use the built-in Platform Service Controller in vCenter Server. Also, use Multi-Factor Authentication (MFA) with the separated Directory service, or with the Platform Service Controller.

1.2 VMware Management Network

Description:

Isolating Network Infrastructure onto its own Management Network is a common security design. This enables isolation and gives flexible control to allow authorized networks' access to the Management Network.

Recommendation:

Isolate the VMware infrastructure to its own Management Network, separate from the Management Network on the common Network Infrastructure. This will allow segmentation for the VMware ESXi Management and vCenter interfaces. Virtual Machine traffic should be split and isolated from the VMware Management Network and the common Management Network. Access lists should be applied to help control access to these Management Networks.

1.3 *Storage Network*

Description:

A Storage Network consists of storage resources, i.e. SAN, NAS, Fiber Channel, etc.

Recommendation:

Isolate the Storage Network with the ESXi hosts, so that only the ESXi hosts can access the network and the storage resources needed.

2. Hardware/Physical

2.1 Device Firmware

Version:

ESXi7, ESXi8

Description:

Hardware firmware can have issues that can affect the availability, integrity, or confidentiality of a system. Ensure the latest firmware updates are installed and verify the firmware is authentic and supplied by the hardware manufacturer.

Rationale:

Ensuring the latest firmware will help the stability and security of a system.

Audit:

Check with the hardware manufacturer for the latest firmware.

Remediation:

Follow the manufacturer's guidance on how to apply the latest firmware.

2.2 UEFI Secure Boot

Version:

ESXi7, ESXi8

Description:

Verify that UEFI Secure Boot is enabled.

Rationale:

Enabling UEFI Secure Boot on an ESXi host helps to prevent malware and untrusted configurations.

Audit:

Ensure UEFI Secure Boot is enabled in the BIOS.

Remediation:

Enable UEFI Secure Boot in the BIOS.

2.3 Verify that TPM 2.0 is installed and enabled on the host.

Version:

ESXi7, ESXi8

Description:

Trusted Platform Modules (TPM) 2.0 is a security feature on boot to prevent malware and secure hardware firmware.

Rationale:

Enabling TPM 2.0 will secure the ESXi boot process and prevent unauthorized software to be loaded at boot.

Audit:

Check the BIOS of the system and ensure TPM 2.0 is enabled.

Remediation:

Enable TPM 2.0 in the BIOS of the system.

3. ESXi OS Base Controls

3.1 Set Image Profile VIB acceptance level

#CIS#1.2

Version:

ESXi7, ESXi8

Description:

Set the vSphere Installation Bundle (VIB) to VMware Certified, VMware Accepted, or Partner Supported.

Rationale:

Setting this value to Partner Supported or VMware Certified will ensure that tested VIBs and trusted modules are installed to the ESXi host.

Audit:

Verify the host image profile acceptance level:

1. From the vSphere Web Client, select the host.
2. Click **Configure**, then under **System,** select **Security Profile**.
3. Under **Host Image Profile Acceptance Level**, ensure it is set to **VMware Certified**, **VMware Accepted**, or **Partner Supported**.

Remediation:

1. From the vSphere Web Client, select the host.
2. Click **Configure**, then under **System**, select **Security Profile**.
3. Under **Host Image Profile Acceptance Level**, select **Edit**.
4. In the drop-down, select one of the following: **VMware Certified**, **VMware Accepted**, or **Partner Supported**.

3.2 No unauthorized kernel modules loaded on host

#CIS#1.3

Version:

ESXi7, ESXi8

Description:

By default, ESXi hosts do not permit the loading of kernel modules that do not have valid digital signatures. Ensure that this has not been overridden.

Rationale:

VMware provides digital signatures for kernel modules. Malicious or untested kernel modules could pose a risk of instability or security to the host.

Audit:

List all loaded kernel modules from either the ESXi shell or vCLI:

```
esxcli system module list
```

Remediation:

Disable unsigned modules and remove the offending VIBs using this PowerCLI command.

*__Note__: Evacuate Virtual Machines and place the host into maintenance mode before performing this command.

```
$ESXCli = Get-EsxCli -VMHost “MyHost_or_IPAddress”

$ESXCli.system.module.set($false, $false, “Module_Name_To_Disable”)
```

3.3 Default value of individual salt per VM

#CIS#1.4

Version:

ESXi7, ESXi8

Description:

VM salting was introduced to address security concerns of Transparent Page Sharing (TPS). TPS allows multiple virtual machines to share pages when the memory content is the same. By default, salting is enabled, ensure the setting has not been overridden.

Rationale:

By enabling each VM to have its own salt, TPS will not share memory pages, so each VM will only page share within itself.

Audit:

:

1. From the vSphere Web Client, select the host.
2. Click **Configure**, expand **System** and select **Advanced System Settings**.
3. Click **Edit** and in the **Filter,** type **Mem.ShareForceSalting**.
4. Verify it is set to **2**.

Remediation:

:

1. From the vSphere Web Client, select the host.
2. Click **Configure**, expand **System** and select **Advanced System Settings**.
3. Click **Edit** and in the **Filter**, type **Mem.ShareForceSalting**.
4. Set the value to **2**.
5. Click **Ok**.

3.4 ESXi Memory Eager Zero

#VMW#Mem.EagerZero

Version:

ESXi7, ESXi8

Description:

ESXi zeroes out pages allocated for virtual machines, userspace applications, and kernel threads at the time of allocation, by default. This will ensure that no non-zero memory pages are exposed to a virtual machine or userspace applications. This is an in-place measure to prevent exposure of cryptographic keys from virtual machines or other virtual machines from another environment.

Rationale:

Using Eager Zero will help prevent memory pages from being allocated that contain existing data from the last time they were used by a process.

Audit:

1. Select the host.
2. Click **Configure**, expand **System** and select **Advanced System Settings**.
3. Click **Edit** and in the **Filter**, type **Mem.MemEagerZero**.
4. Verify it is set to **1**.

Remediation:

1. Select the host.
2. Click **Configure**, expand **System** and select **Advanced System Settings**.
3. Click **Edit** and in the **Filter**, type **Mem.MemEagerZero**.
4. Set the value to **1**.
5. Click **Ok**.

3.5 Network Time Protocol

#CIS#2.1

Version:

ESXi7, ESXi8

Description:

Network Time Protocol (NTP) should be configured on each ESXi host to correctly timestamp system logs. The time servers should utilize the same source and time zone as other network equipment to ensure timestamps can be correlated with other network infrastructure events. There should be at least 3 NTP server sources configured.

Rationale:

NTP needs to be configured properly, so that the logs from the host will have the correct timestamp.

Audit:

Confirm NTP is enabled and NTP Servers are configured.

1. Select the ESXi host.
2. Click **Configure,** then expand **System,** and select **Time Configuration**.
3. Verify that **Time Synchronization** is set to **Automatic**.
4. Verify that the **NTP Client** is set to **Enabled**.
5. Verify that the **NTP Service Status** is **Running**.
6. Verify the time servers are set.

Remediation:

Enable and configure NTP synchronization.

1. Select the ESXi host.
2. Click **Configure**, then expand **System,** and select **Time Configuration**.

3. Select **Edit** next to **Network Time Protocol**.
4. Select the **Enable** box and fill in the **Time Servers**.
5. On the **NTP Service Startup Policy**, select the drop-down and select **Start and stop with host**.
6. Click **Ok**.

3.6 ESXi Firewall

#CIS#2.2

Version:

ESXi7, ESXi8

Description:

ESXi ships with a firewall that is enabled by default, allowing ICMP Ping, DHCP, and DNS. Access to services on the ESXi host should be limited to authorized IP addresses or networks.

Rationale:

Allowing all access to services running on an ESXi host exposes the host to unauthorized access and attacks. Allowing known sources to utilize ESXi services will reduce the risk to the ESXi host.

Audit:

Confirm access to services running on an ESXi host is restricted to authorized IP address or networks.

1. Select the ESXi host.
2. Click **Configure**, then expand **System**, and select **Firewall**.
3. For each enabled service, check to ensure the list of allowed IP addresses or networks match the authorized ones.

Remediation:

To configure the ESXi firewall on an ESXi host:

1. Select the ESXi host.
2. Click **Configure**, then expand **System**, and select **Firewall**.
3. For each service that is enabled, enter a list of IP addresses or networks.
4. Click **Ok**.

3.7 Verify the Managed Object Browser (MOB) is disabled.

#CIS#2.3

Version:

ESXi7, ESXi8

Description:

The Managed Object Browser (MOB) is a web-based service that allows the exploration of objects that exist on the ESXi server. It allows browsing and changing object models used by the VM kernel to manage the host.

Rationale:

The MOB is used for debugging the vSphere software development kit (SDK). Since there are no access controls, MOB can be used to get information about a host with unauthorized access.

Audit:

To confirm if MOB is enabled:

1. Select a host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Click **Edit** and search for **Config.HostAgent.plugins.solo.enableMob.**
4. Verify the value is set to **false**.

Remediation:

To disable MOB:

1. Select a host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Click **Edit** and search for **Config.HostAgent.plugins.solo.enableMob**.
4. Set the value to **false**.
5. Click **Ok**.

3.8 Verify SNMP is disabled.

#CIS#2.5

Version:

ESXi7, ESXi8

Description:

Simple Network Management Protocol (SNMP) is used to manage and monitor network devices and servers. SNMP can be a security risk. If SNMP is needed, use SNMPv3, which has a stronger security than SNMPv1 and SNMPv2.

Rationale:

If SNMP is not being used, make sure it is disabled.

Audit:

From either ESXi shell or vCLI, run the following:

```
esxcli system snmp get
```

Remediation:

To disable SNMP, from either ESXi shell or vCLI, run the following:

```
esxcli system snmp set –enable false
```

3.9 Ensure dvfilter API is not configured if not being used.

#CIS#2.6

Version:

ESXi7, ESXi8

Description:

The dvfilter network API is used by other products, for example, vShields.

Rationale:

If vShields or another product is not being used that uses dvfilter, check to make sure dvfilter is not configured.

Audit:

Check to make sure dvfilter is not configured:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **Net.DVFilterBindIpAddress** in the filter.
5. Verify that **Net.DVFilterBindIpAddress** has an **empty value**.
6. If an appliance or solution is being used, ensure the IP address in this value is correct.

Remediation:

To remove a dvfilter configuration:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **Net.DVFilterBindIpAddress** in the filter.
5. Set **Net.DVFilterBindIpAddress** to **empty**.
6. Click **Ok**.

3.10 Ensure VDS health check is disabled.

#CIS#2.9

Version:

ESXi7, ESXi8

Description:

The VDS Health Check helps to identify and troubleshoot configuration errors in a vSphere Distributed Switch.

Rationale:

The VDS Health Check should be turned on when troubleshooting and turned off after troubleshooting. VDS Heath Check collects packets and information about a host that could aid attackers.

Audit:

In the vSphere Web Client for each vSphere Distributed Switch:

1. Select a vSphere Distributed Switch.
2. Go to **Configure**, expand **Settings**, and select **Health Check**.
3. Ensure that **VLAN and MTU** as well as **Teaming and Failover** are set to **Disabled**.

Remediation:

In the vSphere Web Client for each vSphere Distributed Switch:

1. Select a vSphere Distributed Switch.
2. Go to **Configure**, expand **Settings**, and select **Health Check**.
3. Click on **Edit**.
4. Set **VLAN and MTU** state to **Disabled**.
5. Set **Teaming and Failover** state to **Disabled**.
6. Click **Ok**.

3.11 Host must not suppress warnings about unmitigated hyperthreading vulnerabilities.

#CIS#ESXi8#2.9

Version:

ESXi7, ESXi8

Description:

Do not suppress warning about unmitigated hyperthreading vulnerabilities.

Rationale:

By not suppressing these warnings, it will ensure potential CPU vulnerabilities are not overlooked.

Audit:

Verify HyperthreadWarning is enabled:

1. Select the host.

2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.SuppressHyperthreadWarning** in the filter.
5. Verify that **UserVars.SuppressHyperthreadWarning** has a value of **0**.

Remediation:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.SuppressHyperthreadWarning** in the filter.
5. Set **UserVars.SuppressHyperthreadWarning** to **0**.
6. Click **Ok**.

3.12 Disable SLP

#CIS#ESXi8#3.4

Version:

ESXi7, ESXi8

Description:

The Service Location Protocol (SLP) is used to discover network services in a local area network.

Rationale:

Stopping the SLP service will reduce the attack surface of the ESXi host.

Audit:

Verify the SLP service is disabled:

1. Select the ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. SLPD should be in a **stopped** state.
4. Click on **SSH** and click **Edit Startup Policy**.
5. Verify the **Startup Policy** is set to **Start and Stop Manually**.

Remediation:

1. Select the ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. Click the radio button next to the **SLPD Service** and then click on **Stop**.
4. Click on **SLPD** and click **Edit Startup Policy**.
5. Set **SLPD** to **Start and Stop Manually**.
6. Click **Ok**.

3.13 Host must not suppress warnings that the shell is enabled.

#CIS#ESXI8#3.10

Version:

ESXi7, ESXi8

Description:

Warnings in the ESXi console, or in vCenter that warn about the ESXi shell or SSH being enabled helps to alert administrators that these services are running.

Rationale:

An alert that lets an administrator know SSH or the ESXi shell can help administrators make sure these services are turned back off in use, or that someone has enabled them without their knowledge.

Audit:

Verify shell warnings are enabled:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.SuppressShellWarning** in the filter.
5. Verify that **UserVars.SuppressShellWarning** has a value of **0**.

Remediation:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.SuppressShellWarning** in the filter.
5. Set **UserVars.SuppressShellWarning** to a value of **0**.
6. Click **Ok**.

3.14 Host must have a session timeout for the API.

#CIS#ESXi8#3.16

Version:

ESXi7, ESXi8

Description:

Specifying a session timeout reduces the risk of an active session hijack and ends idle sessions.

Rationale:

A session timeout limits the exposure for any malicious threat. A timeout of 30 seconds is recommended.

Audit:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **Config.HostAgent.vmacore.soap.sessionTimeout** in the filter.
5. Verify that **Config.HostAgent.vmacore.soap.sessionTimeout** has a value of **30**.

Remediation:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **Config.HostAgent.vmacore.soap.sessionTimeout** in the filter.
5. Set **Config.HostAgent.vmacore.soap.sessionTimeout** to a value of **30**.
6. Click **Ok**.

3.15 Host must automatically terminate idle host client sessions.

#CIS#ESXi8#3.17

Version:

ESXi7, ESXi8

Description:

Timing out idle host client sessions helps mitigate security risks used to hijack unattended sessions.

Rationale:

Automatically ending idle sessions helps prevent unauthorized access or exploiting unattended sessions. An idle timeout of 15 minutes is recommended.

Audit:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.HostClientSessionTimeout** in the filter.
5. Verify that **UserVars.HostClientSessionTimeout** has a value of **900**.

Remediation:

1. Select the host.
2. Click **Configure**, then expand **System**.
3. Click on the **Advanced System Setting**, then **Edit**.
4. Search for **UserVars.HostClientSessionTimeout** in the filter.
5. Set **UserVars.HostClientSessionTimeout** to a value of **900**.
6. Click **Ok**.

3.16 Host must deny shell access for the DCUIaccount.

#CIS#ESXi8#3.22

Version:

ESXi8

Description:

The DCUI account is used for process isolation for the Direct Console User Interface (DCUI). By default, this account has shell access.

Rationale:

Disabling shell access for the DCUI account reduces any potential exploitations.

Note: Only on ESXi version 8 can the shell be disabled for a user.

Audit:

Verify shell access for the DCUI user:

1. Logon to the ESXi host ESXi shell either by direct console access or SSH.
2. Run the following command to view users with shell access.

```
esxcli system account list
```

3. Verify that shell access for User ID DCUI is **false**.

Remediation:

Disable shell access for the DCUI user:

1. Logon to the ESXi host ESXi shell either by direct console access or SSH.
2. Run the following command to view users and shell access:

```
esxcli system account list
```

3. If shell access for User ID is **true**, run the following command:

```
esxcli system account set -I dcui -s false
```

4. Run the following command and verify shell access for User ID DCUI is **false**.

```
esxcli system account list
```

3.17 Host must deny shell access for the vpxuser account.

#CIS#ESXi8#3.23

Version:

ESXi8

Description:

Removing shell access for the vpxuser account enhances the security posture for an ESXi 8 host by forcing an “API Only” security stance for predefined non-root ESXi users.

Rationale:

Removing shell access for vpxuser reduces the attack surface by limiting other ways the vpxuser can access an ESXi 8 host. This will align with the Least Privilege security model.

Note: Only on ESXi version 8 can the shell be disabled for a user.

Audit:

Verify shell access for the vpxuser:

1. Logon to the ESXi host ESXi shell either by direct console access or SSH.
2. Run the following command to view users with shell access.

```
esxcli system account list
```

3. Verify that shell access for User ID vpxuser is **false**.

Remediation:

Disable shell access for the vpxuser:

1. Logon to the ESXi host ESXi shell either by direct console access or SSH.
2. Run the following command to view users and shell access:

```
esxcli system account list
```

3. If shell access for User ID is **true**, run the following command:

```
esxcli system account set -I vpxuser -s
```

4. Run the following command and verify shell access for User ID vpxuser is **false**.

```
esxcli system account list
```

3.18 Host must display a login banner for the DCUI and Host Client.

#CIS#ESXi8#3.24

Version:

ESXi7, ESXi8

Description:

Enabling a login banner provides a way to display legal notices at login. Create a banner that meets the policies and legal requirements of the organization.

Rationale:

Login banners serve as the first line legal defense against unauthorized access as well as helping enforcement reminders of the organizational security policies.

Audit:

Verify the DCUI login banner:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Annotations.WelcomeMessage** in the filter.
4. Verify that **Annotations.WelcomeMessage** has a value with the login banner.

Remediation:

Set a login banner for the DCUI:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Annotations.WelcomeMessage** in the filter.
4. Set **Annotations.WelcomeMessage** to the value of the login banner.
5. Click **Ok**.

3.19 Host must display a login banner for SSH sessions.

#CIS#ESXi8#3.25

Version:

ESXi7, ESXi8

Description:

Enabling a login banner provides a way to display legal notices at login. Create a banner that meets the policies and legal requirements of the organization.

Rationale:

Login banners serve as the first line legal defense against unauthorized access as well as helping enforcement reminders of the organizational security policies.

Audit:

Verify the SSH login banner:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Config.Etc.Issue** in the filter.
4. Verify that **Config.Etc.Issue** has a value with the login banner.

Remediation:

Set the SSH login banner:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Config.Etc.Issue** in the filter.
4. Set **Config.Etc.Issue** to the value of the login banner.
5. Click **Ok**.

3.20 Host must enable the highest version of TLS supported.

#CIS#ESXi8#3.26

Version:

ESXi7, ESXi8

Description:

The ESXi host should be configured to use the highest version of TLS supported. TLS 1.2 is enabled by default, and older versions need to be disabled to ensure protection against vulnerabilities in older versions.

Rationale:

Forcing the use of the highest version of TLS improves the security posture and helps to mitigate any future exploits.

Audit:

Verify disabled TLS versions:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **UserVars.ESXiVPsDisabledProtocols** in the filter.
4. Verify that **UserVars.ESXiVPsDisabledProtocols** has a value of **sslv3, tlsv1, tlsv1.1**.

Remediation:

Disable old TLS versions:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **UserVars.ESXiVPsDisabledProtocols** in the filter.
4. Set **UserVars.ESXiVPsDisabledProtocols** to the value of **sslv3, tlsv1, tlsv1.1**.
5. Click **Ok**.

3.21 Ensure persistent logging is configured.

#CIS#3.2

Version:

ESXi7, ESXi8

Description:

ESXi can be configured to store log files in-memory using the /scratch mount point. This is a temporary mount point and will be deleted when rebooted.

Rationale:

Non-persistent logging is a security risk because logs can be overwritten, thus removing any evidence.

Audit:

Verify persistent logging in the vSphere Web Client:

1. Select a host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **Syslog.global.LogDir** in the filter.
4. Ensure the **Syslog.global.LogDir** is not empty or has Null value or not set to a non-persistent datastore, such as /scratch.

Remediation:

Configure persistent logging in the vSphere Web Client:

1. Select a host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **Syslog.global.LogDir** in the filter.
4. Set **Syslog.global.LogDir** to a persistent location.
5. Click **Ok**.

3.22 Ensure remote logging is configured.

#CIS#3.3

Version:

ESXi7, ESXi8

Description:

ESXi logs are stored on a local scratch disk, by default. Storing logs on a persistent disk and additional send logs to a central remote logging host to centralize and keep logs.

Rationale:

Sending logs to a remote host will provide centralized log storage as well as keep logs secured if a system is compromised.

Audit:

Ensure remote logging is configured:

1. Select host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **Syslog.global.logHost** in the filter.
4. Verify that **Syslog.global.logHost** is set to the hostname or IP address of the remote log server.

Remediation:

Configure remote logging:

1. Select host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **Syslog.global.logHost** in the filter.
4. Set **Syslog.global.logHost** to the hostname or IP address of the remote log server.
5. Click **Ok**.

4. Management Access

4.1 Ensure passwords are required to be complex.

#CIS#4.2

Version:

ESXi7, ESXi8

Description:

ESXi uses the pam_passwdqc.so plug-in to set password strength and complexity. The plug-in allows setting a minimum length, requiring characters from dictionaries, and restricting the number of consecutive failed login attempts. These settings should be changed to match the organization's password policies. Note that an uppercase character that begins a password does not count towards the number of character classes used, and neither does a number that ends a password.

Rationale:

All ESXi passwords should be complex to reduce the risk of unauthorized access.

Audit:

Confirm password complexity and strength are set:

1. Logon to the ESXi host shell as a user with administrator privileges.
2. Open the **/etc/pam.d/passwd** file.
3. Locate the following line:

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=N min=N0,N1,N2,N3,N4
```

4. Confirm **N0** is set to **disabled**.
5. Confirm **N1** is set to **disabled**.
6. Confirm **N2** is set to **disabled**.
7. Confirm **N3** is set to **disabled**.
8. Confirm **N4** is set to **14 or greater**.

The value of 14 on N4 requires all passwords to be 14 characters or more and must include at least one character from four distinct character sets.

Remediation:

To set the password complexity and strength:

1. Logon to the ESXi host shell as a user with administrator privileges.
2. Open the **/etc/pam.d/passwd** file.
3. Locate the following line:

```
password requisite /lib/security/$ISA/pam_passwdqc.so retry=N min=N0,N1,N2,N3,N4
```

4. Set **N0** is set to **disabled**.
5. Set **N1** is set to **disabled**.
6. Set **N2** is set to **disabled**.
7. Set **N3** is set to **disabled**.
8. Set **N4** is set to **14 or greater**.
9. Save the changes.

The value of 14 on N4 requires all passwords to be 14 characters or more and must include at least one character from four distinct character sets.

4.2 Host must be configured with an appropriate maximum password age.

#CIS#ESXi8#3.15

Description:

Password aging is a common security best practice which may be required for certain types of policies.

Rationale:

Forcing a password change periodically helps strengthen security hygiene. It is recommended to have a maximum password age of 90 days or less.

Audit:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Security.PasswordMaxDays** in the filter.
4. Verify that **Security.PasswordMaxDays** has a value of **90**.

Remediation:

1. Select the host, click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Security.PasswordMaxDays** in the filter.
4. Set **Security.PasswordMaxDays** to a value of **90**, or as appropriate.

4.3 Ensure the maximum failed login attempts is set to 5

#CIS#4.3

Version:

ESXi7, ESXi8

Description:

An account should be locked out after 5 consecutive failed login attempts.

Rationale:

Multiple failed login attempts could be a brute force login attempt, so setting the maximum failed attempts will stop a brute force attack.

Audit:

Verify the maximum failed login attempts:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.AccountLockFailures** in the filter.
4. Verify **Security.AccountLockFailures** is set to **5**.

Remediation:

Set the maximum failed login attempts:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.AccountLockFailures** in the filter.
4. Set **Security.AccountLockFailures** to **5**.
5. Click **Ok**.

4.4 Ensure account lockout is set to 30 minutes.

#CIS#4.4

Version:

ESXi7, ESXi8

Description:

After the maximum number of failed login attempts, the account should be locked out. The recommended lock out time is 30 minutes.

Rationale:

Locking out an account for a given amount of time will slow down any brute force attempts.

Audit:

Verify the account lockout time is set to 30 minutes:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.AccountUnlockTime** in the filter.
4. Verify that **Security.AccountUnlockTime** is set to **1800**.

Remediation:

Set the account lockout time to 30 minutes:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.AccountUnlockTime** in the filter.
4. Set **Security.AccountUnlockTime** to **1800**.
5. Click **Ok**.

4.5 Ensure the password history is set to previous 5.

#CIS#4.5

Version:

ESXi7, ESXi8

Description:

Prevent users from reusing the previous 5 passwords.

Rationale:

When users change passwords, it is important to use a different password. This recommendation is to keep a password history for the previous 5 and disallow a user to change their password to any of the previous 5.

Audit:

Verify the password history is set to 5:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.PasswordHistory** in the filter.

4. Verify **Security.PasswordHistory** is set to **5**.

Remediation:

Set the password history to 5:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Security.PasswordHistory** in the filter.
4. Set **Security.PasswordHistory** to **5**.
5. Click **Ok**.

4.6 Disable esxAdminsGroup in ESXi advanced settings.

#CIS#4.7

Version:

ESXi7, ESXi8

Description:

ESXi looks for a group in Active Directory named esxAdminsGroup. Any account in this group will be given administrator level access to the ESXi host, if the ESXi host is joined to an Active Directory Domain.

Rationale:

Disabling this check will prevent ESXi from looking for the group in Active Directory. This will help circumvent any misconfigured or malicious use of the group that is out of control of the ESXi host.

Audit:

Check to see if the esxAdminsGroup is configured:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** in the filter.
4. Verify **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** is **Empty**.
5. Enter **stsvc.esConfig.HostAgent.plugins.hoxAdminsGroupAutoAdd** in the filter.
6. Verify **stsvc.esConfig.HostAgent.plugins.hoxAdminsGroupAutoAdd** is set to **false**.
7. Enter **Config.HostAgent.plugins.vimsvc.authValidateInterval** in the filter.
8. Verify **Config.HostAgent.plugins.vimsvc.authValidateInterval** is set to **90**.

Remediation:

To disable the esxAdminsGroup:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** in the filter.
4. Set **Config.HostAgent.plugins.hostsvc.esxAdminsGroup** to **“”** or **blank it out**.
5. Enter **stsvc.esConfig.HostAgent.plugins.hoxAdminsGroupAutoAdd** in the filter.

6. Set **stsvc.esConfig.HostAgent.plugins.hoxAdminsGroupAutoAdd** to **false**.
7. Enter **Config.HostAgent.plugins.vimsvc.authValidateInterval** in the filter.
8. Set **Config.HostAgent.plugins.vimsvc.authValidateInterval** to **90**.

4.7 Ensure proper configuration in the Exception Users list.

#CIS#4.8

Version:

ESXi7, ESXi8

Description:

Users added to the “Exception Users” list do not lose their permissions when the host enters lockdown mode. Service Accounts, such as a backup agent, may need to be added to this list.

Rationale:

Users who need access to the ESXi host should be exempted from the lockdown mode.

Audit:

Verify “Exception Users” list:

1. Select the ESXi host.
2. Click on **Configure**, expand **System**, then select **Security Profile**.
3. Under **Lockdown Mode**, view and verify the list of **Exception Users**.

Remediation:

Add or remove users to the “Exception Users” list:

1. Select the ESXi host.
2. Click on **Configure**, expand **System**, then select **Security Profile**.
3. Select **Edit** next to **Lockdown Mode**.
4. Click on **Exception Users**.
5. **Add/Remove** users as needed.
6. Click **Ok**.

4.8 Ensure DCUI has a trusted users list for lockdown mode.

#CIS#5.10

Version:

ESXi7, ESXi8

Description:

Lockdown mode disables direct host access to the DCUI. Set DCUI access to a list of highly trusted users who will be able to override lockdown mode for access if the ESXi host cannot communicate with vCenter Server for administration.

Rationale:

Have an exception list to only trusted accounts allows admins to access the ESXi console in the event vCenter Server is unavailable, or the ESXi host is unable to communicate with the vCenter Server.

Audit:

Verify the trusted users list for DCUI:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **DCUI.Access** in the filter.
4. Verify that the **DCUI.Access** attribute is set to a **comma-separated list of users** who are allowed to override lockdown mode.

Remediation:

Set a list of trusted users for the DCUI who can override lockdown mode:

1. Select the ESXi host.
2. Click **Configure**, expand **System**, then select **Advanced System Settings** and click **Edit**.
3. Enter **DCUI.Access** in the filter.
4. Set the **DCUI.Access** attribute to a **comma-separated list of users** who are allowed to override lockdown mode.
5. Click **Ok**.

4.9 Ensure Normal Lockdown mode is enabled.

#CIS#5.5

Version:

ESXi7, ESXi8

Description:

Enabling lockdown mode disables direct local access to an ESXi host, requiring the host be managed remotely from the vCenter Server.

There are some operations, such as backup and troubleshooting, that require direct access to the host. In these cases, lockdown mode can be disabled on a temporary basis for specific hosts as needed, and then re-enabled when the task is completed.

Rationale:

Lockdown mode limits ESXi host access to the vCenter Server to ensure the roles and access controls implemented in the vCenter Server are always enforced and users cannot bypass them by logging onto a host directly. By forcing all interaction to occur through the vCenter Server, the risk of someone inadvertently attaining elevated privileges or performing tasks that are not properly audited is greatly reduced.

Audit:

Verify lockdown mode is enabled:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Security Profile**.
3. Verify **Lockdown Mode** is set to **Normal**.

Remediation:

Set lockdown mode to Normal:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Security Profile**.
3. Across from **Lockdown Mode** click on **Edit**.
4. Click the radio button for **Normal**.
5. Click **Ok**.

4.10 Ensure DCUI timeout is set to 600 seconds or less.

#CIS#5.1

Version:

ESXi7, ESXi8

Description:

The Direct Console User Interface (DCUI) is used for directly logging onto an ESXi host and carrying out host management tasks. This setting terminates an idle DCUI session after the specified number of seconds has elapsed.

Rationale:

Terminating idle DCUI sessions helps avoid unauthorized usage of the DCUI originating from residual login sessions.

Audit:

Verify the DCUI timeout setting:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **UserVars.DcuiTimeOut** in the filter.
4. Verify that **UserVars.DcuiTimeOut** is **600 seconds or less**.

Remediation:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **UserVars.DcuiTimeOut** in the filter.

4. Set **UserVars.DcuiTimeOut** to **600 seconds or less**.

4.11 Ensure the ESXi shell is disabled.

#CIS#5.2

Version:

ESXi7, ESXi8

Description:

The ESXi shell is the console command line environment accessible for the DCUI or via SSH. The ESXi shell should only be enabled when performing troubleshooting or diagnostics.

Rationale:

Leaving the ESXi shell disabled greatly reduces the attack surface of an ESXi host.

Audit:

Verify the status of the ESXi shell:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. **ESXi shell** should be in a **stopped** state.
4. Click on **ESXi shell** and click **Edit Startup Policy**.
5. Verify the **Startup Policy** is set to **Start and Stop Manually**.

Remediation:

Disable the ESXi shell:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. Click on **ESXi shell** and click **Edit Startup Policy**.
4. Set the **Startup Policy** to **Start and Stop Manually**.
5. Click **Ok**.

4.12 Ensure SSH is disabled.

#CIS#5.3

Version:

ESXi7, ESXi8

Description:

The ESXi shell can be accessed via SSH. SSH should be stopped and only started when performing troubleshooting or diagnostic operations.

Rationale:

Disabling SSH and only starting it when needed will help reduce the attack surface of the ESXi host.

Audit:

Verify SSH status:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. **SSH** should be in a **stopped** state.
4. Click on **SSH** and click **Edit Startup Policy**.
5. Verify the **Startup Policy** is set to **Start and Stop Manually**.

Remediation:

Disable SSH:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. Click on **SSH** and click **Edit Startup Policy**.
4. Set the **Startup Policy** to **Start and Stop Manually**.
5. Click **Ok**.

4.13 Ensure CIM access is limited.

#CIS#5.4

Version:

ESXi7, ESXi8

Description:

The Common Information Model (CIM) is a service consumed by manufacturers to provide remote hardware monitoring.

Rationale:

If not being utilized, the CIM service should be disabled. If needed, limit the access to the services that use it.

Audit:

Verify the CIM service status:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. **CIM Server** should be in a **stopped** state.
4. Click on **CIM Server** and click **Edit Startup Policy**.
5. Verify the **Startup Policy** is set to **Start and Stop Manually**.

Remediation:

Disable the CIM Server:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Services**.
3. Click on **CIM Server** and click **Edit Startup Policy**.
4. Set the **Startup Policy** to **Start and Stop Manually**.
5. Click **Ok**.

If using the CIM Server for remote hardware monitoring, limit the CIM Server access:

1. Create a limited privileged service account for CIM.
2. This account should access the CIM Server(s) through the vCenter Server.
3. Give the account the CIM Interaction privilege only.

4.14 Ensure the SSH authorized_keys file is empty.

#CIS#5.7

Version:

ESXi7, ESXi8

Description:

ESXi hosts have SSH, which can be configured to use public key authentication. Lockdown mode should be enabled, and only authorized users should be in the exception list. The SSH service should be enabled and disabled when the task needed for SSH is complete.

Rationale:

The presence of keys in /etc/ssh/keys-root/authorized_keys file could allow unauthorized access via SSH to an ESXi host.

Audit:

Verify the authorized_keys file does not contain any keys:

1. Logon to the ESXi shell as root or another admin account.
2. Verify the **/etc/ssh/keys-root/authorized_keys** file is **empty** or contains **known SSH keys**.

Remediation:

Remove keys from the authorized_keys file:

1. Logon to the ESXi shell as root or another admin account.
2. Edit the **/etc/ssh/keys-root/authorized_keys** file.
3. Remove all keys or only unknown keys, if they exist.
4. Save the file.
5. Stop/restart the SSH service.

4.15 Ensure idle ESXi shell and SSH session time out after 900 seconds or less.

#CIS#5.8

#CIS#5.9

Version:

ESXi7, ESXi8

Description:

ESXi allows for the configuration of automated ESXi shell and SSH session timeout. This should be set to 900 seconds or less.

Rationale:

If an ESXi shell or SSH session is not properly terminated, the idle session will continue to run indefinitely. Setting a timeout ensures these sessions are terminated.

Audit:

Verify a timeout is set for ESXiShellInteractiveTimeOut and ESXiShellTimeOut:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **ESXiShellInteractiveTimeOut** in the filter.
4. Verify that **ESXiShellInteractiveTimeOut** is **900 seconds or less**.
5. Select **Edit** and enter **ESXiShellTimeOut** in the filter.
6. Verify that **ESXiShellTimeOut** is **900 seconds or less**.

Remediation:

Set a timeout for ESXiShellInteractiveTimeOut and ESXiShellTimeOut:

1. Select ESXi host.
2. Select **Configure**, expand **System**, then select **Advanced System Settings**.
3. Select **Edit** and enter **ESXiShellInteractiveTimeOut** in the filter.
4. Set **ESXiShellInteractiveTimeOut** to **900 seconds or less**.
5. Select **Edit** and enter **ESXiShellTimeOut** in the filter.
6. Set **ESXiShellTimeOut** to **900 seconds or less**.

5. vNetwork Settings

5.1 Ensure vSwitch Forged Transmit policy is set to reject.

#CIS#7.1

Version:

ESXi7, ESXi8

Description:

Set the vSwitch policy on a standard virtual switch to reject forged transmit packets.

Rationale:

Rejecting forged transmits will not allow a virtual machine to send “fake” MAC addresses, which will protect against MAC address impersonation.

Audit:

1. Select ESXi host.
2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Verify that **Forged Transmits** are set to **Reject** in the drop-down.

Remediation:

1. Select ESXi host.
2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Set **Forged Transmits** to **Reject** in the drop-down.
6. Click **Ok**.

5.2 Ensure vSwitch MAC Address Change policy is set to reject.

#CIS#7.2

Version:

ESXi7, ESXi8

Description:

Set the vSwitch policy on a standard virtual switch to reject MAC address changes.

Rationale:

If a virtual machine operating system changes its MAC address, it can then send frames as another virtual machine and intercept information destined for another virtual machine. Disallowing MAC address changes helps to ensure traffic is going to the intended source.

Audit:

1. Select ESXi host.

2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Verify that **MAC address changes** is set to **Reject** in the drop-down.

Remediation:

1. Select ESXi host.
2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Set **MAC address changes** to **Reject** in the drop-down.
6. Click **Ok**.

5.3 Ensure vSwitch Promiscuous Mode policy is set to reject.

#CIS#7.3

Version:

ESXi7, ESXi8

Description:

Set the vSwitch policy on a standard virtual switch to reject Promiscuous Mode.

Rationale:

Promiscuous Mode allows virtual machines attached to the vSwitch or PortGroup to read all the packets coming in and going out of that vSwitch or PortGroup. Rejecting Promiscuous Mode keeps those packets from only being seen by the destination and source traffic.

Audit:

1. Select ESXi host.
2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Verify that **Promiscuous Mode** is set to **Reject** in the drop-down.

Remediation:

1. Select ESXi host.
2. Click **Configure** and expand **Networking**.
3. Select a **Virtual Switch** and click **Edit**.
4. Click on **Security**.
5. Set **Promiscuous Mode** to **Reject** in the drop-down.

5.4 Ensure PortGroups are not configured with the value of the Native VLAN.

#CIS#7.4

Version:

ESXi7, ESXi8

Description:

ESXi standard vSwitches do not use a native VLAN. If the default native VLAN is 1, then the ESXi standard vSwitch should be configured with a value between 2 and 2094.

Rationale:

Network switches that have ports unconfigured will be put on VLAN 1, by default. These frames could pass through a standard vSwitch if it has a PortGroup configured with the VLAN ID of 1. As a recommended security practice, do not use a VLAN for a PortGroup tagged as 1.

Audit:

Verify the native VLAN ID is not being used for PortGroups:

1. Select ESXi host.
2. Click **Configure**, expand **Networking**, then select **Virtual Switches**.
3. Expand the **Standard vSwitch**.
4. View the topology diagram of the switch and see the PortGroups associated on the vSwitch.
5. For each PortGroup, verify which VLAN IDs are used.

Remediation:

Change the VLAN ID for the PortGroups:

1. Select ESXi host.
2. Click **Configure**, expand **Networking**, then select **Virtual Switches**.
3. Expand the **Standard vSwitch**.
4. View the topology diagram of the switch and see the PortGroups associated on the vSwitch.
5. For each PortGroup, verify which VLAN IDs are used.
6. If a PortGroup has a VLAN ID of **1**:
    a. Click **Edit Settings**.
    b. In the **Properties** section, enter a name in the **Network Label** field.
    c. In the **VLAN ID** drop-down, select an existing VLAN, or if it is a new one, type in the value.
    d. Click **Ok**.

5.5 Ensure PortGroups are not configured to VLAN 4095 or 0.

#CIS#7.6

Version:

ESXi7, ESXi8

Description:

ESXi Standard vSwitches should not be configured with VLAN 4095 or 0, unless Virtual Guest Tagging (VGT) is used. Setting a VLAN ID of 4095 passes all tagged VLANs to the virtual machine, so that the virtual machine will act as a switch.

Rationale:

If VGT is not enabled and configured properly, it could cause a denial of service, or that virtual machine can potentially read unauthorized traffic.

Audit:

1. Select ESXi host.
2. Click **Configure**, expand **Networking**, then select **Virtual Switches**.
3. Expand the **Standard vSwitch**.
4. View the topology diagram of the switch and see the PortGroups associated on the vSwitch.
5. For each PortGroup, verify VLAN ID 0 or 4095 is **not** in use.

Remediation:

1. Select ESXi host.
2. Click **Configure**, expand **Networking**, then select **Virtual Switches**.
3. Expand the **Standard vSwitch**.
4. View the topology diagram of the switch and see the PortGroups associated on the vSwitch.
5. For each PortGroup that is configured with VLAN ID 0 or 4095, change them to another value.

5.6 Ensure Virtual Distributed Switch Netflow traffic is sent to an authorized collector.

#CIS#7.7

Version:

ESXi7, ESXi8

Description:

Netflow can be enabled on a vSphere Distributed Switch (VDS). Netflow will export network traffic passing through the VDS. These exports are unencrypted and contain information. An attacker or a Man in the Middle (MITM) attack would find the information useful.

Rationale:

If Netflow is going to be used or in use, verify that the collector IP address that the VDS is sending the export to is valid and trusted.

Audit:

Check the VDS to verify if Netflow is used and validate the collector:

1. In the vCenter UI, navigate to the **Networking** section.
2. Select a **VDS**, go to **Configure**, expand **Settings**.

3. Click on **Netflow**.
4. Verify the **Collector IP address and port**.

Remediation:

Configure Netflow:

1. In the vCenter UI, navigate to the **Networking** section.
2. Select a **VDS**, go to **Configure**, expand **Settings**.
3. Click on **Netflow**.
4. Enter a valid **Collector IP address** and **Collector port** or delete the address and port to disable Netflow.
5. Click **Ok**.

5.7 Ensure port-level configuration overrides are disabled.

#CIS#7.8

Version:

ESXi7, ESXi8

Description:

Port-level configuration overrides are disabled, by default. Port-level overrides can be used to override the setting of a Standard vSwitch for the PortGroup associated with the Standard vSwitch.

Rationale:

Some scenarios may require an override for a PortGroup, this should be monitored. A Port-level override for a PortGroup could enable a case where the PortGroup has a less secure configuration than the parent Standard vSwitch, or VDS.

Audit:

Verify Switch configuration:

1. In the vCenter UI, navigate to the **Networking** section.
2. Expand each individual **switch** and check each **PortGroup**.
    a. Go to **Configure**, expand **Settings**, then click on **Properties**.
    b. Verify that **Override Port Policies** is set to **Disabled**.

Remediation:

Disable Port-level overrides:

1. In the vCenter UI, navigate to the **Networking** section.
2. Expand each individual **switch** and check each **PortGroup**.
    a. Go to **Configure**, expand **Settings**, then click on **Properties**.
    b. Set **Override Port Policies** to **Disabled**.

c. Click **Ok**.

5.8 Host must filter Bridge Protocol Data Unit (BPDU) packets.

#CIS#ESXi8#5.4

Version:

ESXi7, ESXi8

Description:

Filtering BPDU packets will drop BPDU packets sent from virtual machines to the physical switches. This is important because VMware Standard and Distributed Virtual Switches do not support Spanning Tree Protocol (STP), which could potentially cause network loops if BPDU packets are not filtered.

Rationale:

Filtering BPDU packets helps to prevent potential network loops in the virtual switching.

Audit:

1. Select the host and click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Net.BlockGuestBPDU** in the filter.
4. Verify that **Net.BlockGuestBPDU** has a value of **1**.

Remediation:

1. Select the host and click **Configure**, then expand **System**.
2. Click on the **Advanced System Setting**, then **Edit**.
3. Search for **Net.BlockGuestBPDU** in the filter.
4. Set **Net.BlockGuestBPDU** to a value of **1**.
5. Click **Ok**.