CIS VMware vSphere 8.0 vCenter STIG Benchmark

v1.0.0 – 01-30-2025

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (legalnotices@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

Target Technology Details

VMware vSphere 8.0 vCenter Secure Technical Implementation Guide (STIG)
Version: 2 Release: 2 Benchmark
Date: 30 Jan 2025

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate VMware vSphere 8.0 vCenter and are looking to comply with the STIG guidance

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted, or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations (or rules) for securing a technology or a supporting platform. STIG Benchmark profiles are used to identify which Vulnerability Severity Category Code (CAT) each rule is associated with.

Description

The Rule Title from the STIG.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Additional Information

References from the STIG Rule if applicable.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **SEVERITY: CAT I**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be high severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT II**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be medium severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

- **SEVERITY: CAT III**

  Items in this profile exhibit one or more of the following characteristics:

  - are considered to be low severity
  - are intended for environments or use cases where following STIG based security guidance is paramount.
  - acts as defense in depth measure.
  - may negatively inhibit the utility or performance of the technology.

  This profile is intended for servers and workstations.

Acknowledgements

The Recommendations in this Benchmark are a representation of the Rules in the unclassified DISA STIG for VMware vSphere 8.0 vCenter

Recommendations

1 STIG RULES

VMware vSphere

VMware vSphere 8.0 vCenter Secure Technical Implementation Guide (STIG)

Version: 2 Release: 2 Benchmark

Date: 30 Jan 2025

CLASSIFICATION unclassified

1.1 VCSA-80-000009 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must use DOD-approved encryption to protect the confidentiality of network sessions.

```
GROUP ID: V-265978
RULE ID: SV-265978r1003613
```

Rationale:

Using older unauthorized versions or incorrectly configuring protocol negotiation makes the gateway vulnerable to known and unknown attacks that exploit vulnerabilities in this protocol.

In vCenter 8 Update 3, Transport Layer Security (TLS) Profiles were introduced that allow users to manage and configure TLS parameters for the vCenter server. Several TLS profiles are available by default but not all may be suitable for high security environments.

Audit:

From the vSphere Client, go to Developer Center >> API Explorer.
Select "appliance" from the "Select API" drop down list then scroll down to the "tls/profiles/global" section.
Expand the GET call and click Execute and review the response for the configured global TLS profile.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Invoke-GetTlsProfilesGlobal
If the global TLS profile is not "NIST_2024", this is a finding.

Remediation:

From the vSphere Client, go to Developer Center >> API Explorer.
Select "appliance" from the "Select API" drop down list then scroll down to the "tls/profiles/global" section.
Expand the PUT call and enter the following in the value box:
{
"profile": "NIST_2024"
}
Click Execute and Continue to configure a new global TLS profile.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Invoke-SetProfilesGlobalAsync -TlsProfilesGlobalSetSpec (Initialize-TlsProfilesGlobalSetSpec -VarProfile NIST_2024)
To monitor the status of the operation the task id from the command output can be used with the "Invoke-GetTask" command. For example:
Invoke-GetTask -Task 66b247c2-fe02-4425-9338-1c88eb856138:com.vmware.appliance.tls.profiles.global

Additional Information:

CCI-000068 Implement cryptographic mechanisms to protect the confidentiality of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-000382 Configure the system to prohibit or restrict the use of organization-defined prohibited or restricted functions, system ports, protocols, software, and/or services.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (iii)
- NIST SP 800-53 Revision 4::CM-7 b
- NIST SP 800-53 Revision 5::CM-7 b

CCI-001184 Protect the authenticity of communications sessions.

- NIST SP 800-53::SC-23
- NIST SP 800-53A::SC-23.1
- NIST SP 800-53 Revision 4::SC-23
- NIST SP 800-53 Revision 5::SC-23

CCI-001453 Implement cryptographic mechanisms to protect the integrity of remote access sessions.

- NIST SP 800-53::AC-17 (2)
- NIST SP 800-53A::AC-17 (2).1
- NIST SP 800-53 Revision 4::AC-17 (2)
- NIST SP 800-53 Revision 5::AC-17 (2)

CCI-001941 Implement replay-resistant authentication mechanisms for access to privileged accounts and/or non-privileged accounts.

- NIST SP 800-53 Revision 4::IA-2 (8)
- NIST SP 800-53 Revision 5::IA-2 (8)

CCI-002418 Protect the confidentiality and/or integrity of transmitted information.

- NIST SP 800-53 Revision 4::SC-8
- NIST SP 800-53 Revision 5::SC-8

CCI-002420 Maintain the confidentiality and/or integrity of information during preparation for transmission.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002421 Implement cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.

- NIST SP 800-53 Revision 4::SC-8 (1)
- NIST SP 800-53 Revision 5::SC-8 (1)

CCI-002422 Maintain the confidentiality and/or integrity of information during reception.

- NIST SP 800-53 Revision 4::SC-8 (2)
- NIST SP 800-53 Revision 5::SC-8 (2)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

1.2 VCSA-80-000023 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must enforce the limit of three consecutive invalid login attempts by a user.

```
GROUP ID: V-258905
RULE ID: SV-258905r960840
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
The following lockout policy should be set as follows:
Maximum number of failed login attempts: 3
If this account lockout policy is not configured as stated, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
Click "Edit".
Set the "Maximum number of failed login attempts" to "3" and click "Save".

Additional Information:

CCI-000044 Enforce the organization-defined limit of consecutive invalid logon attempts by a user during the organization-defined time period.

- NIST SP 800-53::AC-7 a
- NIST SP 800-53A::AC-7.1 (ii)
- NIST SP 800-53 Revision 4::AC-7 a
- NIST SP 800-53 Revision 5::AC-7 a

1.3 VCSA-80-000024 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must display the Standard Mandatory DOD Notice and Consent Banner before logon.

```
GROUP ID: V-258906
RULE ID: SV-258906r960843
```

Rationale:

Display of the DOD-approved use notification before granting access to the application ensures privacy and security notification verbiage used is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

System use notifications are required only for access via login interfaces with human users and are not required when such human interfaces do not exist.

The banner must be formatted in accordance with DTM-08-060. Use the following verbiage for applications that can accommodate banners of 1300 characters:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

Use the following verbiage for operating systems that have severe limitations on the number of characters that can be displayed in the banner:

```
"I've read (literal ampersand) consent to terms in IS user agreem't."
```

Satisfies: SRG-APP-000068, SRG-APP-000069, SRG-APP-000070

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Login Message.
If the selection box next to "Show login message" is disabled, "Details of login message" is not configured to the standard DOD User Agreement, or the "Consent checkbox" is disabled, this is a finding.
Note: Refer to vulnerability discussion for user agreement language.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Login Message.
Click "Edit".
Click the "Show login message" slider to enable.
Configure the "Login message" to "DOD User Agreement".
Click the "Consent checkbox" slider to enable.
Set the "Details of login message" to the Standard Mandatory DOD Notice and Consent Banner text.
Click "Save".

Additional Information:

CCI-000048 Display an organization-defined system use notification message or banner to users before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidelines.

- NIST SP 800-53::AC-8 a
- NIST SP 800-53A::AC-8.1 (ii)
- NIST SP 800-53 Revision 4::AC-8 a
- NIST SP 800-53 Revision 5::AC-8 a

CCI-000050 Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system.

- NIST SP 800-53::AC-8 b
- NIST SP 800-53A::AC-8.1 (iii)
- NIST SP 800-53 Revision 4::AC-8 b
- NIST SP 800-53 Revision 5::AC-8 b

CCI-001384 For publicly accessible systems, display system use information with organization-defined conditions before granting further access to the publicly accessible system.

- NIST SP 800-53::AC-8 c
- NIST SP 800-53A::AC-8.2 (i)
- NIST SP 800-53 Revision 4::AC-8 c 1
- NIST SP 800-53 Revision 5::AC-8 c 1

1.4 VCSA-80-000034 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must produce audit records containing information to establish what type of events occurred.

```
GROUP ID: V-258907
RULE ID: SV-258907r960891
```

Rationale:

Without establishing what types of events occurred, it would be difficult to establish, correlate, and investigate the events leading up to an outage or attack.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Verify the "config.log.level" value is set to "info".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name config.log.level and verify it is set to "info".
If the "config.log.level" value is not set to "info" or does not exist, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Click "Edit Settings" and configure the "config.log.level" setting to "info".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name config.log.level | Set-AdvancedSetting -Value info

Additional Information:

CCI-000130 Ensure that audit records contain information that establishes what type of event occurred.

- NIST SP 800-53::AU-3
- NIST SP 800-53A::AU-3.1
- NIST SP 800-53 Revision 4::AU-3
- NIST SP 800-53 Revision 5::AU-3 a

1.5 VCSA-80-000057 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

vCenter Server plugins must be verified.

```
GROUP ID: V-258908
RULE ID: SV-258908r960963
```

Rationale:

The vCenter Server includes a vSphere Client extensibility framework, which provides the ability to extend the vSphere Client with menu selections or toolbar icons that provide access to vCenter Server add-on components or external, web-based functionality.

vSphere Client plugins or extensions run at the same privilege level as the user. Malicious extensions might masquerade as useful add-ons while compromising the system by stealing credentials or incorrectly configuring the system.

Additionally, vCenter comes with a number of plugins preinstalled that may or may not be necessary for proper operation.

Audit:

From the vSphere Client, go to Administration >> Solutions >> Client Plug-Ins.
View the Installed/Available Plug-ins list and verify they are all identified as authorized VMware, third-party (partner), and/or site-specific approved plug-ins.
If any installed/available plug-ins in the viewable list cannot be verified as allowed vSphere Client plug-ins from trusted sources or are not in active use, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Solutions >> Client Plug-Ins, click the radio button next to the unknown plug-in, and click "Disable".
If the plugin will not be needed in the future, proceed to uninstall the plug-in.
To uninstall plug-ins, do the following:
If vCenter Server is in linked mode, perform this procedure on the vCenter Server that is used to install the plug-in initially and then restart the vCenter Server services on the linked vCenter Server:
In a web browser, navigate to "http://vCenter_Server_name_or_IP/mob", where "vCenter_Server_name_or_IP/mob" is the name of the vCenter Server or its IP address.
Click "Content".
Click "ExtensionManager".
Select and copy the name of the plug-in to be removed from the list of values under "Properties".
Click "UnregisterExtension". A new window appears.
Paste the name of the plug-in and click "Invoke Method". This removes the plug-in.
Close the window.
Refresh the Managed Object Type:ManagedObjectReference:ExtensionManager window to verify the plug-in is removed successfully.
Note: If the plug-in still appears, restart the vSphere Client.
Note: The Managed Object Browser (MOB) may have to be enabled temporarily if it was disabled previously.

Additional Information:

CCI-000381 Configure the system to provide only organization-defined mission essential capabilities.

- NIST SP 800-53::CM-7
- NIST SP 800-53A::CM-7.1 (ii)
- NIST SP 800-53 Revision 4::CM-7 a
- NIST SP 800-53 Revision 5::CM-7 a

1.6 VCSA-80-000059 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must uniquely identify and authenticate users or processes acting on behalf of users.

```
GROUP ID: V-258909
RULE ID: SV-258909r1051115
```

Rationale:

To ensure accountability and prevent unauthenticated access, organizational users must be identified and authenticated to prevent potential misuse and compromise of the system.

Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors). Organizational users (and any processes acting on behalf of users) must be uniquely identified and authenticated for all accesses except the following.

(i) Accesses explicitly identified and documented by the organization. Organizations document specific user actions that can be performed on the information system without identification or authentication; and (ii) Accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity.

Using Active Directory or an identity provider for authentication provides more robust account management capabilities and accountability.

Satisfies: SRG-APP-000148, SRG-APP-000153, SRG-APP-000163, SRG-APP-000180, SRG-APP-000234

Audit:

From the vSphere Web Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider.
If the identity provider type is "embedded" and there is no identity source of type "Active Directory" (either Windows Integrated Authentication or LDAP), this is a finding.
If the identity provider type is "Microsoft ADFS" or another supported identity provider, this is NOT a finding.

Remediation:

When using the embedded identity provider type, perform the following:
From the vSphere Web Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider >> Identity Sources.
Click "Add".
Select either "Active Directory over LDAP" or "Active Directory (Windows Integrated Authentication)" and configure appropriately.
Note: Windows Integrated Authentication requires that the vCenter server be joined to Active Directory before configuration via Administration >> Single Sign On >> Configuration >> Identity Provider >> Active Directory Domain.
OR
To change the identity provider type to a third-party identity provider such as Microsoft ADFS, perform the following:
From the vSphere Web Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider.
Click "Change Identity Provider".
Select "Microsoft ADFS" and click "Next".
Enter the ADFS server information and User and Group details and click "Finish".
For additional information on configuring ADFS for use with vCenter, refer to the vSphere documentation.

Additional Information:

CCI-000764 Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

- NIST SP 800-53::IA-2
- NIST SP 800-53A::IA-2.1
- NIST SP 800-53 Revision 4::IA-2
- NIST SP 800-53 Revision 5::IA-2

CCI-004045 Require users to be individually authenticated before granting access to the shared accounts or resources.

- NIST SP 800-53 Revision 5::IA-2 (5)

CCI-003627 Disable accounts when the accounts have expired.

- NIST SP 800-53 Revision 5::AC-2 (3) (a)

CCI-000804 Uniquely identify and authenticate non-organizational users or processes acting on behalf of non-organizational users.

- NIST SP 800-53::IA-8
- NIST SP 800-53A::IA-8.1
- NIST SP 800-53 Revision 4::IA-8

- NIST SP 800-53 Revision 5::IA-8

CCI-001682 Automatically remove or disable emergency accounts after an organization-defined time period for each type of account.

- NIST SP 800-53 Revision 5::AC-2 (2)
- NIST SP 800-53::AC-2 (2)
- NIST SP 800-53 Revision 4::AC-2 (2)
- NIST SP 800-53A::AC-2 (2).1 (ii)

CCI-000770 The organization requires individuals to be authenticated with an individual authenticator when a group authenticator is employed.

- NIST SP 800-53::IA-2 (5) (b)
- NIST SP 800-53A::IA-2 (5).2 (ii)
- NIST SP 800-53 Revision 4::IA-2 (5)

CCI-000795 The organization manages information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

- NIST SP 800-53::IA-4 e
- NIST SP 800-53A::IA-4.1 (iii)
- NIST SP 800-53 Revision 4::IA-4 e

1.7 VCSA-80-000060 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must require multifactor authentication.

```
GROUP ID: V-258910
RULE ID: SV-258910r960864
```

Rationale:

Without the use of multifactor authentication, the ease of access to privileged functions is greatly increased.

Multifactor authentication requires using two or more factors to achieve authentication.

Factors include: (i) something a user knows (e.g., password/PIN); (ii) something a user has (e.g., cryptographic identification device, token); or (iii) something a user is (e.g., biometric).

Satisfies: SRG-APP-000080, SRG-APP-000149, SRG-APP-000150, SRG-APP-000391, SRG-APP-000402

Audit:

From the vSphere Web Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider.
If the embedded identity provider is used, click on "Smart Card Authentication".
If the embedded identity provider is used and "Smart Card Authentication" is not enabled, this is a finding.
If a third-party identity provider is used, such as Microsoft ADFS, and it does not require multifactor authentication to log on to vCenter, this is a finding.

Remediation:

To configure smart card authentication for vCenter when using the embedded identity provider, refer to the vSphere documentation.
For vCenter Servers using a third-party identity provider, consult the product's documentation for enabling multifactor authentication.

Additional Information:

CCI-000166 Provide irrefutable evidence that an individual (or process acting on behalf of an individual) falsely denying having performed organization-defined actions to be covered by non-repudiation.

- NIST SP 800-53::AU-10

- NIST SP 800-53A::AU-10.1
- NIST SP 800-53 Revision 4::AU-10
- NIST SP 800-53 Revision 5::AU-10

CCI-000765 Implement multifactor authentication for access to privileged accounts.

- NIST SP 800-53::IA-2 (1)
- NIST SP 800-53A::IA-2 (1).1
- NIST SP 800-53 Revision 4::IA-2 (1)
- NIST SP 800-53 Revision 5::IA-2 (1)

CCI-000766 Implement multifactor authentication for access to non-privileged accounts.

- NIST SP 800-53::IA-2 (2)
- NIST SP 800-53A::IA-2 (2).1
- NIST SP 800-53 Revision 4::IA-2 (2)
- NIST SP 800-53 Revision 5::IA-2 (2)

CCI-001953 Accept Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-002009 Accept Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

1.8 VCSA-80-000069 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server passwords must be at least 15 characters in length.

```
GROUP ID: V-258911
RULE ID: SV-258911r1015925
```

Rationale:

The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks. Password length is one factor of several that helps to determine strength and how long it takes to crack a password. The shorter the password, the lower the number of possible combinations that need to be tested before the password is compromised.

Use of more characters in a password helps to exponentially increase the time and/or resources required to compromise the password.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Minimum Length" setting.
Minimum Length: 15
If the password policy is not configured with a "Minimum Length" policy of "15" or more, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set the "Minimum Length" to "15" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000205 The information system enforces minimum password length.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (i)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.9 VCSA-80-000070 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must prohibit password reuse for a minimum of five generations.

```
GROUP ID: V-258912
RULE ID: SV-258912r1015267
```

Rationale:

Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

To meet password policy requirements, passwords must be changed at specific policy-based intervals.

If the information system or application allows the user to consecutively reuse their password when that password has exceeded its defined lifetime, the result is a password that is not changed per policy requirements.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Restrict reuse" setting.
Restrict reuse: Users cannot reuse any previous 5 passwords
If the password policy is not configured with a "Restrict reuse" policy of "5" or more, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set the "Restrict reuse" to "5" and click "Save".

Additional Information:

CCI-004061 For password-based authentication, verify when users create or update passwords, that the passwords are not found on the list of commonly-used, expected, or compromised passwords in IA-5 (1) (a).

- NIST SP 800-53 Revision 5::IA-5 (1) (b)

1.10 VCSA-80-000072 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server passwords must contain at least one lowercase character.

```
GROUP ID: V-258914
RULE ID: SV-258914r1015927
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Character requirements" setting.
Character requirements: At least 1 lowercase characters
If the password policy is not configured with "Character requirements" policy requiring "1" or more lowercase characters, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set "lowercase characters" to at least "1" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000193 The information system enforces password complexity by the minimum number of lower case characters used.

- NIST SP 800-53::IA-5 (1) (a)

- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.11 VCSA-80-000071 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server passwords must contain at least one uppercase character.

```
GROUP ID: V-258913
RULE ID: SV-258913r1015926
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password is, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Character requirements" setting.
Character requirements: At least 1 uppercase characters
If the password policy is not configured with "Character requirements" policy requiring "1" or more uppercase characters, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set "uppercase characters" to at least "1" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000192 The information system enforces password complexity by the minimum number of upper case characters used.

- NIST SP 800-53::IA-5 (1) (a)

- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.12 VCSA-80-000073 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server passwords must contain at least one numeric character.

```
GROUP ID: V-258915
RULE ID: SV-258915r1015928
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor of several that determine how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Character requirements" setting.
Character requirements: At least 1 numeric characters
If the password policy is not configured with "Character requirements" policy requiring "1" or more numeric characters, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set "numeric characters" to at least "1" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000194 The information system enforces password complexity by the minimum number of numeric characters used.

- NIST SP 800-53::IA-5 (1) (a)

- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.13 VCSA-80-000074 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server passwords must contain at least one special character.

```
GROUP ID: V-258916
RULE ID: SV-258916r1015929
```

Rationale:

Use of a complex password helps to increase the time and resources required to compromise the password. Password complexity, or strength, is a measure of the effectiveness of a password in resisting attempts at guessing and brute-force attacks.

Password complexity is one factor in determining how long it takes to crack a password. The more complex the password, the greater the number of possible combinations that need to be tested before the password is compromised.

Special characters are not alphanumeric. Examples include: ~ ! @ $ % ^ *.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Character requirements" setting.
Character requirements: At least 1 special characters
If the password policy is not configured with "Character requirements" policy requiring "1" or more special characters, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set "special characters" to at least "1" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-001619 The information system enforces password complexity by the minimum number of special characters used.

- NIST SP 800-53::IA-5 (1) (a)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (a)

1.14 VCSA-80-000077 (Manual)

Profile Applicability:

- SEVERITY: CAT I

Description:

The vCenter Server must enable FIPS-validated cryptography.

```
GROUP ID: V-258917
RULE ID: SV-258917r961029
```

Rationale:

FIPS 140-2 is the current standard for validating that mechanisms used to access cryptographic modules use authentication that meets DOD requirements.

In vSphere 6.7 and later, ESXi and vCenter Server use FIPS-validated cryptography to protect management interfaces and the VMware Certificate Authority (VMCA).

vSphere 7.0 Update 2 and later adds additional FIPS-validated cryptography to vCenter Server Appliance. By default, this FIPS validation option is disabled and must be enabled.

Satisfies: SRG-APP-000172, SRG-APP-000179, SRG-APP-000224, SRG-APP-000231, SRG-APP-000412, SRG-APP-000514, SRG-APP-000555, SRG-APP-000600, SRG-APP-000610, SRG-APP-000620, SRG-APP-000630, SRG-APP-000635

Audit:

From the vSphere Web Client, go to Developer Center >> API Explorer.
From the "Select API" drop-down menu, select appliance.
Expand system/security/global_fips >> GET.
Click "Execute" and then "Copy Response" to view the results.
Example response:
{
"enabled": true
}
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Invoke-GetSystemGlobalFips
If global FIPS mode is not enabled, this is a finding.

Remediation:

From the vSphere Web Client go to Developer Center >> API Explorer.
From the "Select API" drop-down menu, select appliance.
Expand system/security/global_fips >> PUT.
In the response body under "Try it out" paste the following:
{
"enabled": true
}
Click "Execute".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
$spec = Initialize-SystemSecurityGlobalFipsUpdateSpec -Enabled $true; Invoke-SetSystemGlobalFips -SystemSecurityGlobalFipsUpdateSpec $spec
Note: The vCenter server reboots after FIPS is enabled or disabled.

Additional Information:

CCI-000197 For password-based authentication, transmit passwords only over cryptographically-protected channels.

- NIST SP 800-53::IA-5 (1) (c)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (c)
- NIST SP 800-53 Revision 5::IA-5 (1) (c)

CCI-000803 Implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

- NIST SP 800-53::IA-7
- NIST SP 800-53A::IA-7.1
- NIST SP 800-53 Revision 4::IA-7
- NIST SP 800-53 Revision 5::IA-7

CCI-001188 Generate a unique session identifier for each session with organization-defined randomness requirements.

- NIST SP 800-53::SC-23 (4)
- NIST SP 800-53A::SC-23 (4).1 (ii)
- NIST SP 800-53 Revision 4::SC-23 (3)
- NIST SP 800-53 Revision 5::SC-23 (3)

CCI-001199 Protects the confidentiality and/or integrity of organization-defined information at rest.

- NIST SP 800-53::SC-28
- NIST SP 800-53A::SC-28.1
- NIST SP 800-53 Revision 4::SC-28
- NIST SP 800-53 Revision 5::SC-28

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

CCI-002450 Implement organization-defined types of cryptography for each specified cryptography use.

- NIST SP 800-53 Revision 4::SC-13
- NIST SP 800-53 Revision 5::SC-13 b

CCI-003123 Implement organization-defined cryptographic mechanisms to protect the confidentiality of nonlocal maintenance and diagnostic communications.

- NIST SP 800-53 Revision 4::MA-4 (6)
- NIST SP 800-53 Revision 5::MA-4 (6)

1.15 VCSA-80-000080 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must enable revocation checking for certificate-based authentication.

```
GROUP ID: V-258919
RULE ID: SV-258919r1015931
```

Rationale:

The system must establish the validity of the user-supplied identity certificate using Online Certificate Status Protocol (OCSP) and/or Certificate Revocation List (CRL) revocation checking.

Satisfies: SRG-APP-000175, SRG-APP-000392, SRG-APP-000401, SRG-APP-000403

Audit:

If a federated identity provider is configured and used for an identity source and supports smart card authentication, this is not applicable.
From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider >> Smart Card Authentication.
Under Smart Card Authentication settings >> Certificate Revocation, verify "Revocation check" does not show as disabled.
If "Revocation check" shows as disabled, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider >> Smart Card Authentication.
Under Smart Card Authentication settings >> Certificate Revocation, click the "Edit" button.
Configure revocation checking per site requirements. OCSP with CRL failover is recommended.
Note: If FIPS mode is enabled on vCenter, OCSP revocation validation may not function and CRL bay be used instead.
By default, both locations are pulled from the cert. CRL location can be overridden in this screen, and local responders can be specified via the sso-config command line tool.
Refer to the vSphere documentation for more information.

Additional Information:

CCI-000185 For public key-based authentication, validate certificates by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- NIST SP 800-53::IA-5 (2)
- NIST SP 800-53A::IA-5 (2).1
- NIST SP 800-53 Revision 4::IA-5 (2) (a)
- NIST SP 800-53 Revision 5::IA-5 (2) (b) (1)

CCI-001954 Electronically verify Personal Identity Verification-compliant credentials.

- NIST SP 800-53 Revision 4::IA-2 (12)
- NIST SP 800-53 Revision 5::IA-2 (12)

CCI-004068 For public key-based authentication, implement a local cache of revocation data to support path discovery and validation.

- NIST SP 800-53 Revision 5::IA-5 (2) (b) (2)

CCI-002010 Electronically verify Personal Identity Verification-compliant credentials from other federal agencies.

- NIST SP 800-53 Revision 4::IA-8 (1)
- NIST SP 800-53 Revision 5::IA-8 (1)

CCI-001991 The information system, for PKI-based authentication, implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.

- NIST SP 800-53 Revision 4::IA-5 (2) (d)

1.16 VCSA-80-000079 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must enforce a 90-day maximum password lifetime restriction.

```
GROUP ID: V-258918
RULE ID: SV-258918r1043190
```

Rationale:

Any password, no matter how complex, can eventually be cracked. Therefore, passwords must be changed at specific intervals.

One method of minimizing this risk is to use complex passwords and periodically change them. If the application does not limit the lifetime of passwords and force users to change their passwords, there is the risk that the system and/or application passwords could be compromised.

This requirement does not include emergency administration accounts, which are meant for access to the application in case of failure. These accounts are not required to have maximum password lifetime restrictions.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
View the value of the "Maximum lifetime" setting.
Maximum lifetime: Password must be changed every 90 days
If the password policy is not configured with "Maximum lifetime" policy of "90" or less, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Password Policy.
Click "Edit".
Set "Maximum lifetime" to "90" and click "Save".

Additional Information:

CCI-004066 For password-based authentication, enforce organization-defined composition and complexity rules.

- NIST SP 800-53 Revision 5::IA-5 (1) (h)

CCI-000199 The information system enforces maximum password lifetime restrictions.

- NIST SP 800-53::IA-5 (1) (d)
- NIST SP 800-53A::IA-5 (1).1 (v)
- NIST SP 800-53 Revision 4::IA-5 (1) (d)

1.17 VCSA-80-000089 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must terminate vSphere Client sessions after 15 minutes of inactivity.

```
GROUP ID: V-258920
RULE ID: SV-258920r1015932
```

Rationale:

Terminating an idle session within a short time period reduces the window of opportunity for unauthorized personnel to take control of a management session enabled on the console or console port that has been left unattended. In addition, quickly terminating an idle session will also free resources committed by the managed network element.

Satisfies: SRG-APP-000190, SRG-APP-000295, SRG-APP-000389

Audit:

From the vSphere Client, go to Administration >> Deployment >> Client Configuration.
View the value of the "Session timeout" setting.
If the "Session timeout" is not set to "15 minute(s)" or less, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Deployment >> Client Configuration.
Click "Edit" and enter "15" minutes into the "Session timeout" setting. Click "Save".

Additional Information:

CCI-001133 Terminate the network connection associated with a communications session at the end of the session or after an organization-defined time period of inactivity.

- NIST SP 800-53::SC-10
- NIST SP 800-53A::SC-10.1 (ii)
- NIST SP 800-53 Revision 4::SC-10
- NIST SP 800-53 Revision 5::SC-10

CCI-004895 Permit users to invoke the trusted communications path for communications between the user and the organization-defined security functions, including at a minimum, authentication and re-authentication.

- NIST SP 800-53 Revision 5::SC-11 b

CCI-002361 Automatically terminate a user session after organization-defined conditions or trigger events requiring session disconnect.

- NIST SP 800-53 Revision 4::AC-12
- NIST SP 800-53 Revision 5::AC-12

CCI-002038 The organization requires users to reauthenticate upon organization-defined circumstances or situations requiring reauthentication.

- NIST SP 800-53 Revision 4::IA-11
- NIST SP 800-53 Revision 5::IA-11

1.18 VCSA-80-000095 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server user roles must be verified.

```
GROUP ID: V-258921
RULE ID: SV-258921r961095
```

Rationale:

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.

Satisfies: SRG-APP-000211, SRG-APP-000233, SRG-APP-000380

Audit:

From the vSphere Client, go to Administration >> Access Control >> Roles.
View each role and verify the users and/or groups assigned to it by clicking on "Usage".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VIPermission | Sort Role | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto
Application service account and user required privileges should be documented.
If any user or service account has more privileges than required, this is a finding.

Remediation:

To update a user's or group's permissions to an existing role with reduced permissions, do the following:
From the vSphere Client, go to Administration >> Access Control >> Global Permissions.
Select the user or group, click the pencil button, change the assigned role, and click "OK".
Note: If permissions are assigned on a specific object, the role must be updated where it is assigned (for example, at the cluster level).
To create a new role with reduced permissions, do the following:
From the vSphere Client, go to Administration >> Access Control >> Roles.
Click the green plus sign and enter a name for the role and select only the specific permissions required.
Users can then be assigned to the newly created role.

Additional Information:

CCI-001082 Separate user functionality, including user interface services, from system management functionality.

- NIST SP 800-53::SC-2
- NIST SP 800-53A::SC-2.1
- NIST SP 800-53 Revision 4::SC-2
- NIST SP 800-53 Revision 5::SC-2

CCI-001084 Isolate security functions from nonsecurity functions.

- NIST SP 800-53::SC-3
- NIST SP 800-53A::SC-3.1 (ii)
- NIST SP 800-53 Revision 4::SC-3
- NIST SP 800-53 Revision 5::SC-3

CCI-001813 Enforce access restrictions using organization-defined mechanisms.

- NIST SP 800-53 Revision 4::CM-5 (1)
- NIST SP 800-53 Revision 5::CM-5 (1) (a)

1.19 VCSA-80-000110 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must manage excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service (DoS) attacks by enabling Network I/O Control (NIOC).

```
GROUP ID: V-258922
RULE ID: SV-258922r961155
```

Rationale:

DoS is a condition when a resource is not available for legitimate users. When this occurs, the organization either cannot accomplish its mission or must operate at degraded capacity.

Managing excess capacity ensures sufficient capacity is available to counter flooding attacks. Employing increased capacity and service redundancy may reduce the susceptibility to some DoS attacks. Managing excess capacity may include, for example, establishing selected usage priorities, quotas, or partitioning.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to Networking.
Select a distributed switch >> Configure >> Settings >> Properties.
View the "Properties" pane and verify "Network I/O Control" is "Enabled".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDSwitch | select Name,@{N="NIOC Enabled";E={$_.ExtensionData.config.NetworkResourceManagementEnabled}}
If "Network I/O Control" is disabled, this is a finding.

Remediation:

From the vSphere Client, go to Networking.
Select a distributed switch >> Configure >> Settings >> Properties.
In the "Properties" pane, click "Edit". Change "Network I/O Control" to "Enabled". Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
(Get-VDSwitch "VDSwitch Name" | Get-View).EnableNetworkResourceManagement($true)

Additional Information:

CCI-001095 Manage capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.

- NIST SP 800-53::SC-5 (2)
- NIST SP 800-53A::SC-5 (2).1
- NIST SP 800-53 Revision 4::SC-5 (2)
- NIST SP 800-53 Revision 5::SC-5 (2)

1.20 VCSA-80-000123 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must provide an immediate real-time alert to the system administrator (SA) and information system security officer (ISSO), at a minimum, on every Single Sign-On (SSO) account action.

```
GROUP ID: V-258923
RULE ID: SV-258923r1015933
```

Rationale:

Once an attacker establishes initial access to a system, they often attempt to create a persistent method of reestablishing access. One way to accomplish this is for the attacker to create a new account. They may also try to hijack an existing account by changing a password or enabling a previously disabled account. Therefore, all actions performed on accounts in the SSO domain much be alerted on in vCenter at a minimum and ideally on a Security Information and Event Management (SIEM) system as well.

To ensure the appropriate personnel are alerted about SSO account actions, create a new vCenter alarm for the "com.vmware.sso.PrincipalManagement" event ID and configure the alert mechanisms appropriately.

Satisfies: SRG-APP-000291, SRG-APP-000292, SRG-APP-000293, SRG-APP-000294, SRG-APP-000320

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Security >> Alarm Definitions.
Verify there is an alarm created to alert upon all SSO account actions.
The alarm name may vary, but it is suggested to name it "SSO account actions - com.vmware.sso.PrincipalManagement".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AlarmDefinition | Where {$*.ExtensionData.Info.Expression.Expression.EventTypeId -eq "com.vmware.sso.PrincipalManagement"}* | *Select Name,Enabled,@{N="EventTypeId";E={$*.ExtensionData.Info.Expression.Expression.EventTypeId}}
If an alarm is not created to alert on SSO account actions, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Security >> Alarm Definitions.
Click "Add".
Provide the alarm name of "SSO account actions - com.vmware.sso.PrincipalManagement" and an optional description.
From the "Target type" dropdown menu, select "vCenter Server".
Click "Next".
Paste "com.vmware.sso.PrincipalManagement" (without quotes) in the line after "IF" and press "Enter".
Next to "Trigger the alarm and", select "Show as Warning".
Configure the desired notification actions that will inform the SA and ISSO of the event.
Click "Next". Click "Next" again. Click "Create".

Additional Information:

CCI-000015 Support the management of system accounts using organization-defined automated mechanisms.

- NIST SP 800-53::AC-2 (1)
- NIST SP 800-53A::AC-2 (1).1
- NIST SP 800-53 Revision 4::AC-2 (1)
- NIST SP 800-53 Revision 5::AC-2 (1)

CCI-001683 The information system notifies organization-defined personnel or roles for account creation actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

CCI-001684 The information system notifies organization-defined personnel or roles for account modification actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

CCI-001685 The information system notifies organization-defined personnel or roles for account disabling actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53 Revision 4::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)

CCI-001686 The information system notifies organization-defined personnel or roles for account removal actions.

- NIST SP 800-53::AC-2 (4)
- NIST SP 800-53A::AC-2 (4).1 (i and ii)
- NIST SP 800-53 Revision 4::AC-2 (4)

CCI-002132 The information system notifies organization-defined personnel or roles for account enabling actions.

- NIST SP 800-53 Revision 4::AC-2 (4)

1.21 VCSA-80-000145 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must set the interval for counting failed login attempts to at least 15 minutes.

```
GROUP ID: V-258924
RULE ID: SV-258924r961368
```

Rationale:

By limiting the number of failed login attempts, the risk of unauthorized system access via user password guessing, otherwise known as brute forcing, is reduced. Limits are imposed by locking the account.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
View the value of the "Time interval between failures" setting.
Time interval between failures: 900 seconds
If the lockout policy is not configured with "Time interval between failures" policy of "900" or more, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
Click "Edit".
Set the "Time interval between failures" to "900" and click "Save".

Additional Information:

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

1.22 VCSA-80-000148 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must be configured to send logs to a central log server.

```
GROUP ID: V-258925
RULE ID: SV-258925r961395
```

Rationale:

vCenter must be configured to send near real-time log data to syslog collectors so information will be available to investigators in the case of a security incident or to assist in troubleshooting.

Audit:

Open the Virtual Appliance Management Interface (VAMI) by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with a Single Sign-On (SSO) account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Syslog" on the left navigation pane.
On the resulting pane on the right, verify at least one site-specific syslog receiver is configured and is listed as "Reachable".
If no valid syslog collector is configured or if the collector is not listed as "Reachable", this is a finding.

Remediation:

Open the VAMI by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with an SSO account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Syslog" on the left navigation pane.
On the resulting pane on the right, click "Edit" or "Configure".
Edit or add the address and port of a site-specific syslog aggregator or Security Information Event Management (SIEM) system with the appropriate protocol.
User Datagram Protocol (UDP) is discouraged due to its stateless and unencrypted nature. Transport Layer Security (TLS) is preferred.
Click "Save".

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.23 VCSA-80-000150 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must provide an immediate real-time alert to the system administrator (SA) and information system security officer (ISSO), at a minimum, of all audit failure events requiring real-time alerts.

```
GROUP ID: V-258926
RULE ID: SV-258926r961401
```

Rationale:

It is critical for the appropriate personnel to be aware if a system is at risk of failing to process audit logs as required. Without a real-time alert, security personnel may be unaware of an impending failure of the audit capability and system operation may be adversely affected.

Alerts provide organizations with urgent messages. Real-time alerts provide these messages immediately (i.e., the time from event detection to alert occurs in seconds or less).

Satisfies: SRG-APP-000360, SRG-APP-000379, SRG-APP-000510

Audit:

Review the Central Logging Server being used to verify it is configured to alert the SA and ISSO, at a minimum, on any AO-defined events. Otherwise, this is a finding.
If there are no AO-defined events, this is not a finding.

Remediation:

Configure the Central Logging Server being used to alert the SA and ISSO, at a minimum, on any AO-defined events.

Additional Information:

CCI-000172 Generate audit records for the event types defined in AU-2 c that include the audit record content defined in AU-3.

- NIST SP 800-53::AU-12 c
- NIST SP 800-53A::AU-12.1 (iv)
- NIST SP 800-53 Revision 4::AU-12 c
- NIST SP 800-53 Revision 5::AU-12 c

CCI-001744 Implement organization-defined security responses automatically if baseline configurations are changed in an unauthorized manner.

- NIST SP 800-53 Revision 5::CM-3 (5)
- NIST SP 800-53 Revision 4::CM-3 (5)

CCI-001858 Provide an alert in an organization-defined real-time-period to organization-defined personnel, roles, and/or locations when organization-defined audit failure events requiring real-time alerts occur.

- NIST SP 800-53 Revision 4::AU-5 (2)
- NIST SP 800-53 Revision 5::AU-5 (2)

1.24 VCSA-80-000158 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must compare internal information system clocks at least every 24 hours with an authoritative time server.

```
GROUP ID: V-258927
RULE ID: SV-258927r1015934
```

Rationale:

Inaccurate time stamps make it more difficult to correlate events and can lead to an inaccurate analysis. Determining the correct time a particular event occurred on a system is critical when conducting forensic analysis and investigating system events. Sources outside of the configured acceptable allowance (drift) may be inaccurate. Additionally, unnecessary synchronization may have an adverse impact on system performance and may indicate malicious activity.

Synchronizing internal information system clocks to an authoritative time server provides uniformity of time stamps for information systems with multiple system clocks and systems connected over a network.

Audit:

Open the Virtual Appliance Management Interface (VAMI) by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with a single sign-on (SSO) account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Time" on the left navigation pane.
On the resulting pane on the right, verify at least one authorized time server is configured and is listed as "Reachable".
If "NTP" is not enabled and at least one authorized time server configured, this is a finding.

Remediation:

Open the VAMI by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with an SSO account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Time" on the left navigation pane.
On the resulting pane on the right, click "Edit" under "Time Synchronization".
Select "NTP" for "Mode" and enter a list of authorized time servers separated by commas. Click "Save".

Additional Information:

CCI-004923 Compare the internal system clocks on an organization-defined frequency with organization-defined authoritative time source.

- NIST SP 800-53 Revision 5::SC-45 (1) (a)

CCI-001891 The information system compares internal information system clocks on an organization-defined frequency with an organization-defined authoritative time source.

- NIST SP 800-53 Revision 4::AU-8 (1) (a)

1.25 VCSA-80-000195 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server Machine Secure Sockets Layer (SSL) certificate must be issued by a DOD certificate authority.

```
GROUP ID: V-258928
RULE ID: SV-258928r961596
```

Rationale:

Untrusted certificate authorities (CA) can issue certificates, but they may be issued by organizations or individuals that seek to compromise DOD systems or by organizations with insufficient security controls. If the CA used for verifying the certificate is not a DOD-approved CA, trust of this CA has not been established.

The DOD will only accept public key infrastructure (PKI) certificates obtained from a DOD-approved internal or external certificate authority. Reliance on CAs for the establishment of secure sessions includes, for example, the use of Transport Layer Security (TLS) certificates.

The default self-signed, VMware Certificate Authority (VMCA)-issued vCenter reverse proxy certificate must be replaced with a DOD-approved certificate. The use of a DOD certificate on the vCenter reverse proxy and other services assures clients that the service they are connecting to is legitimate and trusted.

Audit:

From the vSphere Client, go to Administration >> Certificates >> Certificate Management >> Machine SSL Certificate.
Click "View Details" and examine the "Issuer Information" block.
If the issuer specified is not a DOD approved certificate authority, this is a finding.

Remediation:

Obtain a DOD-issued certificate and private key for each vCenter in the system following the requirements below:
Key size: 2048 bits or more (PEM encoded)
CRT format (Base-64)
x509 version 3
SubjectAltName must contain DNS Name=<machine_FQDN>
Contains the following Key Usages: Digital Signature, Non Repudiation, Key Encipherment
Export the entire certificate issuing chain up to the root in Base-64 format. Concatenate the individual certificates into one file with the ".cer" extension.
From the vSphere Client, go to Administration >> Certificates >> Certificate Management >> Machine SSL Certificate.
Click Actions >> Import and Replace Certificate.
Select the "Replace with external CA certificate" radio button and click "Next".
Supply the CA-issued certificate , the exported roots file, and the private key.
Click "Replace".

Additional Information:

CCI-002470 Only allow the use of organization-defined certificate authorities for verification of the establishment of protected sessions.

- NIST SP 800-53 Revision 4::SC-23 (5)
- NIST SP 800-53 Revision 5::SC-23 (5)

1.26 VCSA-80-000196 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must enable data at rest encryption for vSAN.

```
GROUP ID: V-258929
RULE ID: SV-258929r961599
```

Rationale:

Applications handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.

Data encryption is a common technique used in environments that require additional levels of security. It consists of a process to ensure that data can only be consumed by systems that have appropriate levels of access. Approved systems must have and use the appropriate cryptographic keys to encrypt and decrypt the data. Systems that do not have the keys will not be able to consume the data in any meaningful way, as it will remain encrypted in accordance with the commonly used Advanced Encryption Standard (AES) from the National Institute of Standards and Technology, or NIST.

vSAN supports Data-At-Rest Encryption and Data-in-Transit Encryption and uses an AES 256 cipher. Data is encrypted after all other processing, such as deduplication, is performed. Data at rest encryption protects data on storage devices in case a device is removed from the cluster.

Audit:

If no clusters are enabled for vSAN, this is not applicable.
From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Select the cluster >> Configure >> vSAN >> Services >> Data Services.
Review the "Data-at-rest encryption" status.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-Cluster | Where-Object {$_.VsanEnabled -eq $true} | Get-VsanClusterConfiguration | Select-Object Name,EncryptionEnabled
If "Data-At-Rest encryption" is not enabled, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Select the target cluster >> Configure >> vSAN >> Services >> Data Services.
Click "Edit".
Enable "Data-At-Rest encryption" and select a pre-configured key provider from the drop down. Click "Apply".
Note: Before enabling, read and understand the operational implications of enabling data at rest encryption in vSAN and how it effects capacity, performance, and recovery scenarios.

Additional Information:

CCI-002475 Implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined system components.

- NIST SP 800-53 Revision 4::SC-28 (1)
- NIST SP 800-53 Revision 5::SC-28 (1)

1.27 VCSA-80-000248 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable the Customer Experience Improvement Program (CEIP).

```
GROUP ID: V-258930
RULE ID: SV-258930r961863
```

Rationale:

The VMware CEIP sends VMware anonymized system information that is used to improve the quality, reliability, and functionality of VMware products and services. For confidentiality purposes, this feature must be disabled.

Audit:

From the vSphere Client, go to Administration >> Deployment >> Customer Experience Improvement Program.
If Customer Experience Improvement "Program Status" is "Joined", this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Deployment >> Customer Experience Improvement Program.
Click "Leave Program".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.28 VCSA-80-000253 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must enforce SNMPv3 security features where SNMP is required.

```
GROUP ID: V-258931
RULE ID: SV-258931r961878
```

Rationale:

SNMPv3 supports commercial-grade security, including authentication, authorization, access control, and privacy. Previous versions of the protocol contained well-known security weaknesses that were easily exploited. SNMPv3 can be configured for identification and cryptographically based authentication.

SNMPv3 defines a user-based security model (USM) and a view-based access control model (VACM). SNMPv3 USM provides data integrity, data origin authentication, message replay protection, and protection against disclosure of the message payload. SNMPv3 VACM provides access control to determine whether a specific type of access (read or write) to the management information is allowed. Implement both VACM and USM for full protection.

SNMPv3 must be disabled by default and enabled only if used. SNMP v3 provides security feature enhancements to SNMP, including encryption and message authentication.

Audit:

At the command prompt on the vCenter Server Appliance, run the following commands:
appliancesh
snmp.get
Note: The "appliancesh" command is not needed if the default shell has not been changed for root.
If "Enable" is set to "False", this is not a finding.
If "Enable" is set to "True" and "Authentication" is not set to "SHA1", this is a finding.
If "Enable" is set to "True" and "Privacy" is not set to "AES128", this is a finding.
If any "Users" are configured with a "Sec_level" that does not equal "priv", this is a finding.

Remediation:

At the command prompt on the vCenter Server Appliance, run the following commands:
appliancesh
snmp.set --authentication SHA1
snmp.set --privacy AES128
To change the security level of a user, run the following command:
snmp.set --users /<auth_password> <priv_password>/priv

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.29 VCSA-80-000265 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must disable SNMPv1/2 receivers.

```
GROUP ID: V-258932
RULE ID: SV-258932r961878
```

Rationale:

SNMPv3 supports commercial-grade security, including authentication, authorization, access control, and privacy. Previous versions of the protocol contained well-known security weaknesses that were easily exploited. Therefore, SNMPv1/2 receivers must be disabled, while SNMPv3 is configured in another control. vCenter exposes SNMP v1/2 in the UI and SNMPv3 in the CLI.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> General.
Click "Edit".
On the "SNMP receivers" tab, note the presence of any enabled receiver.
If there are any enabled receivers, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> General.
Click "Edit".
On the "SNMP receivers" tab, ensure all receivers are disabled.

Additional Information:

CCI-001967 Authenticate organization-defined devices and/or types of devices before establishing a local, remote, and/or network connection using bidirectional authentication that is cryptographically based.

- NIST SP 800-53 Revision 4::IA-3 (1)
- NIST SP 800-53 Revision 5::IA-3 (1)

1.30 VCSA-80-000266 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must require an administrator to unlock an account locked due to excessive login failures.

```
GROUP ID: V-258933
RULE ID: SV-258933r961368
```

Rationale:

By requiring that Single Sign-On (SSO) accounts be unlocked manually, the risk of unauthorized access via user password guessing, otherwise known as brute forcing, is reduced. When the account unlock time is set to zero, a locked account can only be unlocked manually by an administrator.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
View the value of the "Unlock time" setting.
Unlock time: 0 seconds
If the lockout policy is not configured with "Unlock time" policy of "0", this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Local Accounts >> Lockout Policy.
Click "Edit".
Set the "Unlock time" to "0" and click "Save".

Additional Information:

CCI-002238 Automatically lock the account or node for either an organization-defined time period, until the locked account or node is released by an administrator, or delays the next logon prompt according to the organization-defined delay algorithm when the maximum number of unsuccessful logon attempts is exceeded.

- NIST SP 800-53 Revision 4::AC-7 b
- NIST SP 800-53 Revision 5::AC-7 b

1.31 VCSA-80-000267 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable the distributed virtual switch health check.

```
GROUP ID: V-258934
RULE ID: SV-258934r961863
```

Rationale:

Network health check is disabled by default. Once enabled, the health check packets contain information on host, vds, and port, which an attacker would find useful. It is recommended that network health check be used for troubleshooting and turned off when troubleshooting is finished.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Health Check.
View the health check pane and verify the "VLAN and MTU" and "Teaming and failover" checks are "Disabled".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
$vds = Get-VDSwitch
$vds.ExtensionData.Config.HealthCheckConfig
If the health check feature is enabled on distributed switches and is not on temporarily for troubleshooting purposes, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Health Check.
Click "Edit".
Disable the "VLAN and MTU" and "Teaming and failover" checks.
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-View -ViewType DistributedVirtualSwitch | ?{($*.config.HealthCheckConfig* | *?{$*.enable -notmatch "False"})}| %{$_.UpdateDVSHealthCheckConfig(@((New-Object Vmware.Vim.VMwareDVSVlanMtuHealthCheckConfig -property @{enable=0}),(New-Object Vmware.Vim.VMwareDVSTeamingHealthCheckConfig -property @{enable=0})))}

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.32 VCSA-80-000268 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must set the distributed port group Forged Transmits policy to "Reject".

```
GROUP ID: V-258935
RULE ID: SV-258935r961863
```

Rationale:

If the virtual machine operating system changes the Media Access Control (MAC) address, the operating system can send frames with an impersonated source MAC address at any time. This allows an operating system to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.

When the "Forged Transmits" option is set to "Accept", ESXi does not compare source and effective MAC addresses.

To protect against MAC impersonation, set the "Forged Transmits" option to "Reject". The host compares the source MAC address being transmitted by the guest operating system with the effective MAC address for its virtual machine adapter to determine if they match. If the addresses do not match, the ESXi host drops the packet.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Verify "Forged Transmits" is set to "Reject".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy
If the "Forged Transmits" policy is set to accept for a nonuplink port, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "Security" tab.
Set "Forged Transmits" to "Reject".
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits $false
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy | Set-VDSecurityPolicy -ForgedTransmits $false

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.33 VCSA-80-000269 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must set the distributed port group Media Access Control (MAC) Address Change policy to "Reject".

```
GROUP ID: V-258936
RULE ID: SV-258936r961863
```

Rationale:

If the virtual machine operating system changes the MAC address, it can send frames with an impersonated source MAC address at any time. This allows it to stage malicious attacks on the devices in a network by impersonating a network adaptor authorized by the receiving network.

This will prevent virtual machines from changing their effective MAC address and will affect applications that require this functionality. This will also affect how a layer 2 bridge will operate and will affect applications that require a specific MAC address for licensing.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Verify "MAC Address Changes" is set to "Reject".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy
If the "MAC Address Changes" policy is set to accept, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "Security" tab.
Set "MAC Address Changes" to "Reject".
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges $false
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy | Set-VDSecurityPolicy -MacChanges $false

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.34 VCSA-80-000270 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must set the distributed port group Promiscuous Mode policy to "Reject".

```
GROUP ID: V-258937
RULE ID: SV-258937r961863
```

Rationale:

When promiscuous mode is enabled for a virtual switch, all virtual machines connected to the port group have the potential of reading all packets across that network, meaning only the virtual machines connected to that port group.

Promiscuous mode is disabled by default on the ESXi Server, and this is the recommended setting.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Verify "Promiscuous Mode" is set to "Reject".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy
If the "Promiscuous Mode" policy is set to accept, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "Security" tab.
Set "Promiscuous Mode" to "Reject".
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
Get-VDSwitch | Get-VDSecurityPolicy | Set-VDSecurityPolicy -AllowPromiscuous $false
Get-VDPortgroup | ?{$_.IsUplink -eq $false} | Get-VDSecurityPolicy | Set-VDSecurityPolicy -AllowPromiscuous $false

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.35 VCSA-80-000271 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must only send NetFlow traffic to authorized collectors.

```
GROUP ID: V-258938
RULE ID: SV-258938r961863
```

Rationale:

The distributed virtual switch can export NetFlow information about traffic crossing the switch. NetFlow exports are not encrypted and can contain information about the virtual network, making it easier for a man-in-the-middle attack to be executed successfully. If NetFlow export is required, verify that all NetFlow target Internet Protocols (IPs) are correct.

Audit:

If distributed switches are not used, this is not applicable.
To view NetFlow Collector IPs configured on distributed switches:
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> NetFlow.
View the NetFlow pane and verify any collector IP addresses are valid and in use for troubleshooting.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDSwitch | select Name,@{N="NetFlowCollectorIPs";E={$_.ExtensionData.config.IpfixConfig.CollectorIpAddress}}
To view if NetFlow is enabled on any distributed port groups:
From the vSphere Client, go to "Networking".
Select a distributed port group >> Manage >> Settings >> Policies.
Go to "Monitoring" and view the NetFlow status.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup | Select Name,VirtualSwitch,@{N="NetFlowEnabled";E={$_.Extensiondata.Config.defaultPortConfig.ipfixEnabled.Value}}
If NetFlow is configured and the collector IP is not known and documented, this is a finding.

Remediation:

To remove collector IPs, do the following:
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> NetFlow.
Click "Edit".
Remove any unknown collector IPs.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:

```
$dvs = Get-VDSwitch dvswitch | Get-View
ForEach($vs in $dvs){
$spec = New-Object VMware.Vim.VMwareDVSConfigSpec
$spec.configversion = $vs.Config.ConfigVersion
$spec.IpfixConfig = New-Object VMware.Vim.VMwareIpfixConfig
$spec.IpfixConfig.CollectorIpAddress = ""
$spec.IpfixConfig.CollectorPort = "0"
$spec.IpfixConfig.ActiveFlowTimeout = "60"
$spec.IpfixConfig.IdleFlowTimeout = "15"
$spec.IpfixConfig.SamplingRate = "0"
$spec.IpfixConfig.InternalFlowsOnly = $False
$vs.ReconfigureDvs_Task($spec)
}
```

Note: This will reset the NetFlow collector configuration back to the defaults.
To disable NetFlow on a distributed port group, do the following:
From the vSphere Client, go to "Networking".
Select a distributed port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "Monitoring" tab.
Change "NetFlow" to "Disabled".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:

```
$pgs = Get-VDPortgroup | Get-View
ForEach($pg in $pgs){
$spec = New-Object VMware.Vim.DVPortgroupConfigSpec
$spec.configversion = $pg.Config.ConfigVersion
$spec.defaultPortConfig = New-Object VMware.Vim.VMwareDVSPortSetting
$spec.defaultPortConfig.ipfixEnabled = New-Object VMware.Vim.BoolPolicy
$spec.defaultPortConfig.ipfixEnabled.inherited = $false
$spec.defaultPortConfig.ipfixEnabled.value = $false
$pg.ReconfigureDVPortgroup_Task($spec)
}
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.36 VCSA-80-000272 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must configure all port groups to a value other than that of the native virtual local area network (VLAN).

```
GROUP ID: V-258939
RULE ID: SV-258939r961863
```

Rationale:

ESXi does not use the concept of native VLAN. Frames with VLAN specified in the port group will have a tag, but frames with VLAN not specified in the port group are not tagged and therefore will end up belonging to native VLAN of the physical switch.

For example, frames on VLAN 1 from a Cisco physical switch will be untagged, because this is considered as the native VLAN. However, frames from ESXi specified as VLAN 1 will be tagged with a "1"; therefore, traffic from ESXi that is destined for the native VLAN will not be correctly routed (because it is tagged with a "1" instead of being untagged), and traffic from the physical switch coming from the native VLAN will not be visible (because it is not tagged).

If the ESXi virtual switch port group uses the native VLAN ID, traffic from those virtual machines will not be visible to the native VLAN on the switch, because the switch is expecting untagged traffic.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Review the port group VLAN tags and verify they are not set to the native VLAN ID of the attached physical switch.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup | select Name, VlanConfiguration
If any port group is configured with the native VLAN of the ESXi hosts attached physical switch, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "VLAN" tab.
Change the VLAN ID to a nonnative VLAN.
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup "portgroup name" | Set-VDVlanConfiguration -VlanId "New VLAN"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.37 VCSA-80-000273 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must not configure VLAN Trunking unless Virtual Guest Tagging (VGT) is required and authorized.

```
GROUP ID: V-258940
RULE ID: SV-258940r961863
```

Rationale:

When a port group is set to VLAN Trunking, the vSwitch passes all network frames in the specified range to the attached virtual machines without modifying the virtual local area network (VLAN) tags. In vSphere, this is referred to as VGT.

The virtual machine must process the VLAN information itself via an 802.1Q driver in the operating system. VLAN Trunking must only be implemented if the attached virtual machines have been specifically authorized and are capable of managing VLAN tags themselves.

If VLAN Trunking is enabled inappropriately, it may cause a denial of service or allow a virtual machine to interact with traffic on an unauthorized VLAN.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Review the port group "VLAN Type" and "VLAN trunk range", if present.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup | Where {$_.ExtensionData.Config.Uplink -ne "True"} | Select Name,VlanConfiguration
If any port group is configured with "VLAN trunking" and is not documented as a needed exception (such as NSX appliances), this is a finding.
If any port group is authorized to be configured with "VLAN trunking" but is not configured with the most limited range necessary, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "VLAN" tab.
If "VLAN trunking" is not authorized, remove it by setting "VLAN type" to "VLAN" and configure an appropriate VLAN ID. Click "OK".
If "VLAN trunking" is authorized but the range is too broad, modify the range in the "VLAN trunk range" field to the minimum necessary and authorized range. An example range would be "1,3-5,8". Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command to configure trunking:
Get-VDPortgroup "Portgroup Name" | Set-VDVlanConfiguration -VlanTrunkRange "<VLAN Range(s) comma separated>"
or
Run this command to configure a single VLAN ID:
Get-VDPortgroup "Portgroup Name" | Set-VDVlanConfiguration -VlanId "<New VLAN>"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.38 VCSA-80-000275 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must configure the "vpxuser" auto-password to be changed every 30 days.

```
GROUP ID: V-258942
RULE ID: SV-258942r961863
```

Rationale:

By default, vCenter will change the "vpxuser" password automatically every 30 days. Ensure this setting meets site policies. If it does not, configure it to meet password aging policies.

Note: It is very important the password aging policy is not shorter than the default interval that is set to automatically change the "vpxuser" password to preclude the possibility that vCenter might be locked out of an ESXi host.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Verify that "VirtualCenter.VimPasswordExpirationInDays" is set to "30".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name VirtualCenter.VimPasswordExpirationInDays
If the "VirtualCenter.VimPasswordExpirationInDays" is set to a value other than "30" or does not exist, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Click "Edit Settings" and configure the "VirtualCenter.VimPasswordExpirationInDays" value to "30" or if the value does not exist create it by entering the values in the "Key" and "Value" fields and clicking "Add".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
If the setting already exists:
Get-AdvancedSetting -Entity -Name VirtualCenter.VimPasswordExpirationInDays | Set-AdvancedSetting -Value 30
If the setting does not exist:
New-AdvancedSetting -Entity -Name VirtualCenter.VimPasswordExpirationInDays -Value 30

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.39 VCSA-80-000276 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must configure the "vpxuser" password to meet length policy.

```
GROUP ID: V-258943
RULE ID: SV-258943r961863
```

Rationale:

The "vpxuser" password default length is 32 characters. Ensure this setting meets site policies; if not, configure to meet password length policies.

Longer passwords make brute-force password attacks more difficult. The "vpxuser" password is added by vCenter, meaning no manual intervention is normally required. The "vpxuser" password length must never be modified to less than the default length of 32 characters.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Verify that "config.vpxd.hostPasswordLength" is set to "32".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name config.vpxd.hostPasswordLength and verify it is set to 32.
If the "config.vpxd.hostPasswordLength" is set to a value other than "32, this is a finding.
If the setting does not exist, this is not a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Click "Edit Settings" and configure the "config.vpxd.hostPasswordLength" value to "32".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name config.vpxd.hostPasswordLength | Set-AdvancedSetting -Value 32

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.40 VCSA-80-000274 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must not configure all port groups to virtual local area network (VLAN) values reserved by upstream physical switches.

```
GROUP ID: V-258941
RULE ID: SV-258941r961863
```

Rationale:

Certain physical switches reserve certain VLAN IDs for internal purposes and often disallow traffic configured to these values. For example, Cisco Catalyst switches typically reserve VLANs 1001 to 1024 and 4094, while Nexus switches typically reserve 3968 to 4094.

Check with the documentation for the organization's specific switch. Using a reserved VLAN might result in a denial of service on the network.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Review the port group VLAN tags and verify that they are not set to a reserved VLAN ID.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup | select Name, VlanConfiguration
If any port group is configured with a reserved VLAN ID, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Policies.
Click "Edit".
Click the "VLAN" tab. Change the VLAN ID to an unreserved VLAN ID.
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDPortgroup "portgroup name" | Set-VDVlanConfiguration -VlanId "New VLAN"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.41 VCSA-80-000277 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The vCenter Server must be isolated from the public internet but must still allow for patch notification and delivery.

```
GROUP ID: V-258944
RULE ID: SV-258944r961863
```

Rationale:

vCenter and the embedded Lifecycle Manager system must never have a direct route to the internet. Despite this, updates and patches sourced from VMware on the internet must be delivered in a timely manner.

There are two methods to accomplish this: a proxy server and the Update Manager Download Service (UMDS). UMDS is an optional module for Lifecycle Manager that fetches upgrades for virtual appliances, patch metadata, patch binaries, and notifications that would not otherwise be available to an isolated Lifecycle Manager directly.

Alternatively, a proxy for Lifecycle Manager can be configured to allow controlled, limited access to the public internet for the sole purpose of patch gathering. Either solution mitigates the risk of internet connectivity by limiting its scope and use.

Audit:

Check the following conditions:

1. Lifecycle Manager must be configured to use the UMDS.

OR

2. Lifecycle Manager must be configured to use a proxy server for access to VMware patch repositories.

OR

3. Lifecycle Manager must disable internet patch repositories and any patches must be manually validated and imported as needed.

Option 1:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Setup.
Click the "Change Download Source" button.
Verify the "Download patches from a UMDS shared repository" radio button is selected and that a valid UMDS repository is supplied.
Click "Cancel".
If this is not set, this is a finding.
Option 2:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Setup.
Click the "Change Download Source" button.
Verify the "Download patches directly from the internet" radio button is selected.
Click "Cancel".
Navigate to the vCenter Server Management interface at https://:5480 >> Networking >> Proxy Settings.
Verify that "HTTPS" is "Enabled".
Click the "HTTPS" row.
Verify the proxy server configuration is accurate.
If this is not set, this is a finding.
Option 3:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Downloads.
Verify the "Automatic downloads" option is disabled.
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Setup.
Verify any download sources are disabled.
If this is not set, this is a finding.

Remediation:

Option 1:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Setup.
Click the "Change Download Source" button.
Select the "Download patches from a UMDS shared repository" radio button and supply a valid UMDS repository.
Click "Save".
Option 2:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Setup.
Click the "Change Download Source" button.
Select the "Download patches directly from the internet" radio button.
Click "Save".
Navigate to the vCenter Server Management interface at https://:5480 >> Networking >> Proxy Settings.
Click "Edit".
Slide "HTTPS" to "Enabled".
Supply the appropriate proxy server configuration.
Click "Save".
Option 3:
From the vSphere Client, go to Lifecycle Manager >> Settings >> Patch Downloads.
Click "Edit" and uncheck "Download patches".
Under "Patch Setup" select each download source and click Disable.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.42 VCSA-80-000278 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must use unique service accounts when applications connect to vCenter.

```
GROUP ID: V-258945
RULE ID: SV-258945r961863
```

Rationale:

To not violate nonrepudiation (i.e., deny the authenticity of who is connecting to vCenter), when applications need to connect to vCenter they must use unique service accounts.

Audit:

Verify each external application that connects to vCenter has a unique service account dedicated to that application.
For example, there should be separate accounts for Log Insight, Operations Manager, or anything else that requires an account to access vCenter.
If any application shares a service account that is used to connect to vCenter, this is a finding.

Remediation:

For applications sharing service accounts, create a new service account to assign to the application so that no application shares a service account with another.
When standing up a new application that requires access to vCenter, always create a new service account prior to installation and grant only the permissions needed for that application.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.43 VCSA-80-000279 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must protect the confidentiality and integrity of transmitted information by isolating Internet Protocol (IP)-based storage traffic.

```
GROUP ID: V-258946
RULE ID: SV-258946r961863
```

Rationale:

Virtual machines might share virtual switches and virtual local area networks (VLAN) with the IP-based storage configurations.

IP-based storage includes vSAN, Internet Small Computer System Interface (iSCSI), and Network File System (NFS). This configuration might expose IP-based storage traffic to unauthorized virtual machine users. IP-based storage frequently is not encrypted. It can be viewed by anyone with access to this network.

To restrict unauthorized users from viewing the IP-based storage traffic, the IP-based storage network must be logically separated from the production traffic. Configuring the IP-based storage adaptors on separate VLANs or network segments from other VMkernels and virtual machines will limit unauthorized users from viewing the traffic.

Audit:

If IP-based storage is not used, this is not applicable.
IP-based storage (iSCSI, NFS, vSAN) VMkernel port groups must be in a dedicated VLAN that can be on a standard or distributed virtual switch that is logically separated from other traffic types.
The check for this will be unique per environment.
To check a standard switch, do the following:
From the vSphere Client, select the ESXi host and go to Configure >> Networking >> Virtual switches. Select a standard switch.
For each storage port group (iSCSI, NFS, vSAN), select the port group and note the VLAN ID associated with each port group.
Verify it is dedicated to that purpose and is logically separated from other traffic types.
To check a distributed switch, do the following,
From the vSphere Client, go to "Networking".
Select and expand a distributed switch.
For each storage port group (iSCSI, NFS, vSAN), select the port group and navigate to the "Summary" tab.
Note the VLAN ID associated with each port group and verify it is dedicated to that purpose and is logically separated from other traffic types.
If any IP-based storage networks are not isolated from other traffic types, this is a finding.

Remediation:

Configuration of an IP-based VMkernel will be unique to each environment.
To configure VLANs and traffic types, do the following:
Standard switch:
From the vSphere Client, select the ESXi host and go to Configure >> Networking >> VMkernel adapters.
Select the Storage VMkernel (for any IP-based storage). Click "Edit..." and click the "Port properties" tab.
Uncheck everything (unless vSAN).
Click the "IPv4" settings or "IPv6" settings tab.
Enter the appropriate IP address and subnet information.
Click "OK".
From the vSphere Client, select the ESXi host and go to Configure >> Networking >> Virtual switches. Select a standard switch.
For each storage port group (iSCSI, NFS, vSAN), select the port group and click "...".
Click "Edit Settings". On the "Properties" tab, enter the appropriate VLAN ID and click "OK".
Distributed switch:
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Topology.
Select the Storage VMkernel (for any IP-based storage). Click "..." and click "Edit Settings".
On the "Port properties" tab, uncheck everything (unless vSAN).
Click the "IPv4" settings or "IPv6" settings tab.
Enter the appropriate IP address and subnet information.
Click "OK".
From the vSphere Client, go to "Networking".
Select and expand a distributed switch.
For each storage port group (iSCSI, NFS, vSAN), select the port group and navigate to Configure >> Settings >> Properties.
Click "Edit".
Click the "VLAN" tab.
Enter the appropriate VLAN type and ID and click "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.44 VCSA-80-000280 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must be configured to send events to a central log server.

```
GROUP ID: V-258947
RULE ID: SV-258947r961395
```

Rationale:

vCenter server generates volumes of security-relevant application-level events. Examples include logins, system reconfigurations, system degradation warnings, and more. To ensure these events are available for forensic analysis and correlation, they must be sent to the syslog and forwarded on to the configured Security Information and Event Management (SIEM) system and/or central log server.

The vCenter server sends events to syslog by default, but this configuration must be verified and maintained.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Verify that "vpxd.event.syslog.enabled" value is set to "true".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name vpxd.event.syslog.enabled
If the "vpxd.event.syslog.enabled" value is not set to "true", this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> Advanced Settings.
Click "Edit Settings" and configure the "vpxd.event.syslog.enabled" setting to "true".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-AdvancedSetting -Entity -Name vpxd.event.syslog.enabled | Set-AdvancedSetting -Value true

Additional Information:

CCI-001851 Transfer audit logs per organization-defined frequency to a different system, system component, or media than the system or system component conducting the logging.

- NIST SP 800-53 Revision 4::AU-4 (1)
- NIST SP 800-53 Revision 5::AU-4 (1)

1.45 VCSA-80-000281 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable or restrict the connectivity between vSAN Health Check and public Hardware Compatibility List (HCL) by use of an external proxy server.

```
GROUP ID: V-258948
RULE ID: SV-258948r961863
```

Rationale:

The vSAN Health Check is able to download the HCL from VMware to check compliance against the underlying vSAN Cluster hosts. To ensure the vCenter server is not directly downloading content from the internet, this functionality must be disabled. If this feature is necessary, an external proxy server must be configured.

Audit:

If no clusters are enabled for vSAN, this is not applicable.
From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Configure >> vSAN >> Internet Connectivity.
If the HCL internet download is not required, verify "Status" is "Disabled".
If the "Status" is "Enabled", this is a finding.
If the HCL internet download is required, verify "Status" is "Enabled" and a proxy host is configured.
If "Status" is "Enabled" and a proxy is not configured, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Configure >> vSAN >> Internet Connectivity.
Click "Edit".
If the HCL internet download is not required, ensure that "Status" is "Disabled".
If the HCL internet download is required, ensure that "Status" is "Enabled" and that a proxy host is appropriately configured.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.46 VCSA-80-000282 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must configure the vSAN Datastore name to a unique name.

```
GROUP ID: V-258949
RULE ID: SV-258949r961863
```

Rationale:

A vSAN Datastore name by default is "vsanDatastore". If more than one vSAN cluster is present in vCenter, both datastores will have the same name by default, potentially leading to confusion and manually misplaced workloads.

Audit:

If no clusters are enabled for vSAN, this is not applicable.
From the vSphere Client, go to Host and Clusters.
Select a vSAN Enabled Cluster >> Datastores.
Review the datastores and identify any datastores with "vSAN" as the datastore type.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
If($(Get-Cluster | where {$*.VsanEnabled}* | *Measure).Count -gt 0){*
Write-Host "vSAN Enabled Cluster found"
Get-Cluster | *where {$*.VsanEnabled} | Get-Datastore | where {$_.type -match "vsan"}
}
else{
Write-Host "vSAN is not enabled, this finding is not applicable."
}
If vSAN is enabled and a datastore is named "vsanDatastore", this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vSAN Enabled Cluster >> Datastores.
Right-click on the datastore named "vsanDatastore" and select "Rename".
Rename the datastore based on site-specific naming standards.
Click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:

```
If($(Get-Cluster | where {$.VsanEnabled} | Measure).Count -gt 0){
Write-Host "vSAN Enabled Cluster found"
$Clusters = Get-Cluster | where {$.VsanEnabled}
Foreach ($clus in $clusters){
$clus | Get-Datastore | where {$_.type -match "vsan"} | Set-Datastore -Name
$(($clus.name) + "_vSAN_Datastore")
}
}
else{
Write-Host "vSAN is not enabled, this finding is not applicable."
}
```

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.47 VCSA-80-000283 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable Username/Password and Windows Integrated Authentication.

```
GROUP ID: V-258950
RULE ID: SV-258950r961863
```

Rationale:

All forms of authentication other than Common Access Card (CAC) must be disabled. Password authentication can be temporarily reenabled for emergency access to the local Single Sign-On (SSO) accounts or Active Directory user/pass accounts, but it must be disabled as soon as CAC authentication is functional.

Audit:

If a federated identity provider is configured and used for an identity source, this is not applicable.
From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider >> Smart Card Authentication.
Under "Authentication method", examine the allowed methods.
If "Smart card authentication" is not enabled and "Password and windows session authentication" is not disabled, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider >> Smart Card Authentication.
Next to "Authentication method", click "Edit".
Select to radio button to "Enable smart card authentication".
Click "Save".
To re-enable password authentication for troubleshooting purposes, run the following command on the vCenter Server Appliance:
/opt/vmware/bin/sso-config.sh -set_authn_policy -pwdAuthn true -winAuthn false -certAuthn false -securIDAuthn false -t vsphere.local

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b

- NIST SP 800-53 Revision 5::CM-6 b

1.48 VCSA-80-000284 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must restrict access to the default roles with cryptographic permissions.

```
GROUP ID: V-258951
RULE ID: SV-258951r1003606
```

Rationale:

In vSphere, the built-in "Administrator" role contains 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 and/or vSAN encryption is in use.

A new built-in role called "No Cryptography Administrator" exists to provide all administrative permissions except cryptographic operations. Permissions must be restricted such that normal vSphere administrators are assigned the "No Cryptography Administrator" role or more restrictive.

The "Administrator" role must be tightly controlled and must not be applied to administrators who will not be doing cryptographic work. Catastrophic data loss can result from poorly administered cryptography.

Audit:

By default, there are five roles that contain cryptographic related permissions: Administrator, No Trusted Infrastructure Administrator, vCLSAdmin, VMOperator Controller Manager, and vSphere Kubernetes Manager.
From the vSphere Client, go to Administration >> Access Control >> Roles.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VIPermission | Where {$.*Role -eq "Admin" -or $*.Role -eq "NoTrustedAdmin" -or $.*Role -eq "vCLSAdmin" -or $*.Role -eq "VMOperatorController" -or $_.Role -eq "vSphereKubernetesManager"} | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto
If there are any users or groups assigned to the default roles with cryptographic permissions and are not explicitly designated to perform cryptographic operations, this is a finding.
The built-in solution users assigned to the administrator role are NOT a finding.

Remediation:

From the vSphere Client, go to Administration >> Access Control >> Roles.
Move any accounts not explicitly designated for cryptographic operations, other than Solution Users, to other roles such as "No Cryptography Administrator".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.49 VCSA-80-000285 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must restrict access to cryptographic permissions.

```
GROUP ID: V-258952
RULE ID: SV-258952r1003608
```

Rationale:

These permissions must be reserved for cryptographic administrators where virtual machine encryption and/or vSAN encryption is in use. Catastrophic data loss can result from poorly administered cryptography.

Audit:

By default, there are five roles that contain cryptographic related permissions: Administrator, No Trusted Infrastructure Administrator, vCLSAdmin, VMOperator Controller Manager, and vSphere Kubernetes Manager.
From the vSphere Client, go to Administration >> Access Control >> Roles.
Highlight each role and click the "Privileges" button in the right pane.
Verify that only the Administrator, No Trusted Infrastructure Administrator, vCLSAdmin, and vSphere Kubernetes Manager and any site-specific cryptographic roles have the following permissions:
Cryptographic Operations privileges
Global.Diagnostics
Host.Inventory.Add host to cluster
Host.Inventory.Add standalone host
Host.Local operations.Manage user groups
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:

```
$roles = Get-VIRole
ForEach($role in $roles){
$privileges = $role.PrivilegeList
If($privileges -match "Crypto*" -or $privileges -match "Global.Diagnostics" -or
$privileges -match "Host.Inventory.Add*" -or $privileges -match "Host.Local
operations.Manage user groups"){
Write-Host "$role has Cryptographic privileges"
}
}
```

If any role other than the five default roles contain the permissions listed above and is not authorized to perform cryptographic related operations, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Access Control >> Roles.
Highlight the target custom role and click "Edit".
Remove the following permissions from any custom role that is not authorized to perform cryptographic related operations:
Cryptographic Operations privileges
Global.Diagnostics
Host.Inventory.Add host to cluster
Host.Inventory.Add standalone host
Host.Local operations.Manage user groups

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.50 VCSA-80-000286 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must have Mutual Challenge Handshake Authentication Protocol (CHAP) configured for vSAN Internet Small Computer System Interface (iSCSI) targets.

```
GROUP ID: V-258953
RULE ID: SV-258953r961863
```

Rationale:

When enabled, vSphere performs bidirectional authentication of both the iSCSI target and host. When not authenticating both the iSCSI target and host, the potential exists for a man-in-the-middle attack in which an attacker might impersonate either side of the connection to steal data. Bidirectional authentication mitigates this risk.

Audit:

If no clusters are enabled for vSAN or if vSAN is enabled but iSCSI is not enabled, this is not applicable.
From the vSphere Client, go to Host and Clusters.
Select a vSAN Enabled Cluster >> Configure >> vSAN >> iSCSI Target Service.
For each iSCSI target, review the value in the "Authentication" column.
If the Authentication method is not set to "CHAP_Mutual" for any iSCSI target, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vSAN Enabled Cluster >> Configure >> vSAN >> iSCSI Target Service.
For each iSCSI target, select the item and click "Edit".
Change the "Authentication" field to "Mutual CHAP" and configure the incoming and outgoing users and secrets appropriately.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.51 VCSA-80-000287 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must have new Key Encryption Keys (KEKs) reissued at regular intervals for vSAN encrypted datastore(s).

```
GROUP ID: V-258954
RULE ID: SV-258954r1003610
```

Rationale:

The KEK for a vSAN encrypted datastore is generated by the Key Management Server (KMS) and serves as a wrapper and lock around the Disk Encryption Key (DEK). The DEK is generated by the host and is used to encrypt and decrypt the datastore. A shallow rekey is a procedure in which the KMS issues a new KEK to the ESXi host, which rewraps the DEK but does not change the DEK or any data on disk.

This operation must be done on a regular, site-defined interval and can be viewed as similar in criticality to changing an administrative password. If the KMS is compromised, a standing operational procedure to rekey will put a time limit on the usefulness of any stolen KMS data.

Audit:

If vSAN is not in use, this is not applicable.
Interview the system administrator (SA) to determine that a procedure has been put in place to perform a shallow rekey of all vSAN encrypted datastores at regular, site-defined intervals.
VMware recommends a 60-day rekey task, but this interval must be defined by the SA and the ISSO.
If vSAN encryption is not in use, this is not a finding.
If vSAN encryption is in use and a regular rekey procedure is not in place, this is a finding.

Remediation:

If vSAN encryption is in use, ensure a regular rekey procedure is in place.
To generate new encryption keys for vSAN, do the following:
From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Select the cluster >> Configure >> vSAN >> Services >> Data Services.
Select "Generate New Encryption Keys" and optionally generate new DEKs and click "Generate".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.52 VCSA-80-000288 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must use secure Lightweight Directory Access Protocol (LDAPS) when adding an LDAP identity source.

```
GROUP ID: V-258955
RULE ID: SV-258955r961863
```

Rationale:

LDAP is an industry standard protocol for querying directory services such as Active Directory. This protocol can operate in clear text or over a Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encrypted tunnel. To protect confidentiality of LDAP communications, secure LDAP (LDAPS) must be explicitly configured when adding an LDAP identity source in vSphere Single Sign-On (SSO).

When configuring an identity source and supplying an SSL certificate, vCenter will enforce LDAPS. The server URLs do not need to be explicitly provided if an SSL certificate is uploaded.

Audit:

If LDAP is not used as an identity provider, this is not applicable.
From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider.
Click the "Identity Sources" tab.
For each identity source of type "Active Directory over LDAP", if the "Server URL" does not indicate "ldaps://", this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Configuration >> Identity Provider.
Click the "Identity Sources" tab.
For each identity source of type "Active Directory over LDAP" where LDAPS is not configured, highlight the item and click "Edit".
Ensure the primary and secondary server URLs, if specified, are configured for "ldaps://".
At the bottom, click the "Browse" button, select the AD LDAP cert previously exported to your local computer, click "Open", and "Save" to complete modifications.
Note: With LDAPS, the server must be a specific domain controller and its specific certificate or the domain alias with a certificate that is valid for that URL.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.53 VCSA-80-000290 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must limit membership to the "SystemConfiguration.BashShellAdministrators" Single Sign-On (SSO) group.

```
GROUP ID: V-258956
RULE ID: SV-258956r961863
```

Rationale:

vCenter SSO integrates with PAM in the underlying Photon operating system so members of the "SystemConfiguration.BashShellAdministrators" SSO group can log on to the operating system without needing a separate account. However, even though unique SSO users log on, they are transparently using a group account named "sso-user" as far as Photon auditing is concerned. While the audit trail can still be traced back to the individual SSO user, it is a more involved process.

To force accountability and nonrepudiation, the SSO group "SystemConfiguration.BashShellAdministrators" must be severely restricted.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Groups.
Click the next page arrow until the "SystemConfiguration.BashShellAdministrators" group appears.
Click "SystemConfiguration.BashShellAdministrators".
Review the members of the group and ensure that only authorized accounts are present.
Note: By default the Administrator and a unique service account similar to "vmware-applmgmtservice-714684a4-342f-4eff-a232-cdc21def00c2" will be in the group and should not be removed.
If there are any accounts present as members of SystemConfiguration.BashShellAdministrators that are not authorized, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Groups.
Click the next page arrow until the "SystemConfiguration.BashShellAdministrators" group appears.
Click "SystemConfiguration.BashShellAdministrators".
Click the three vertical dots next to the name of each unauthorized account.
Select "Remove Member".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.54 VCSA-80-000291 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must limit membership to the "TrustedAdmins" Single Sign-On (SSO) group.

```
GROUP ID: V-258957
RULE ID: SV-258957r961863
```

Rationale:

The vSphere "TrustedAdmins" group grants additional rights to administer the vSphere Trust Authority feature.

To force accountability and nonrepudiation, the SSO group "TrustedAdmins" must be severely restricted.

Audit:

From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Groups.
Click the next page arrow until the "TrustedAdmins" group appears.
Click "TrustedAdmins".
Review the members of the group and ensure that only authorized accounts are present.
Note: These accounts act as root on the Photon operating system and have the ability to severely damage vCenter, inadvertently or otherwise.
If there are any accounts present as members of TrustedAdmins that are not authorized, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Groups.
Click the next page arrow until the "TrustedAdmins" group appears.
Click "TrustedAdmins".
Click the three vertical dots next to the name of each unauthorized account.
Select "Remove Member".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)

- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.55 VCSA-80-000292 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server configuration must be backed up on a regular basis.

```
GROUP ID: V-258958
RULE ID: SV-258958r961863
```

Rationale:

vCenter server is the control plane for the vSphere infrastructure and all the workloads it hosts. As such, vCenter is usually a highly critical system in its own right. Backups of vCenter can now be made at a data and configuration level versus traditional storage/image-based backups. This reduces recovery time by letting the system administrator (SA) spin up a new vCenter while simultaneously importing the backed-up data.

For sites that implement the Native Key Provider (NKP), introduced in 7.0 Update 2, regular vCenter backups are critical. In a recovery scenario where the virtual machine files are intact but vCenter was lost, the encrypted virtual machines will not be able to boot as their private keys were stored in vCenter after it was last backed up. When using the NKP, vCenter becomes critical to the virtual machine workloads and ceases to be just the control plane.

Audit:

Option 1:
If vCenter is backed up in a traditional manner, at the storage array level, interview the SA to determine configuration and schedule.
Option 2:
For vCenter native backup functionality, open the Virtual Appliance Management Interface (VAMI) by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with a Single Sign-On (SSO) account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Backup" on the left navigation pane.
On the resulting pane on the right, verify the "Status" is "Enabled".
Click "Status" to expand the backup details.
If vCenter server backups are not configured and there is no other vCenter backup system, this is a finding.
If the backup configuration is not set to a proper, reachable location or if the schedule is anything less frequent than "Daily", this is a finding.

Remediation:

Option 1:
Implement and document a VMware-supported storage/image-based backup schedule.
Option 2:
To configure vCenter native backup functionality, open the VAMI by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with an SSO account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Backup" on the left navigation pane.
On the resulting pane on the right, click "Configure" (or "Edit" for an existing configuration).
Enter site-specific information for the backup job.
Ensure "Schedule" is set to "Daily". Limiting the number of retained backups is recommended but not required.
Click "Create".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.56 VCSA-80-000293 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must have task and event retention set to at least 30 days.

```
GROUP ID: V-258959
RULE ID: SV-258959r961863
```

Rationale:

vCenter tasks and events contain valuable historical actions, useful in troubleshooting availability issues and for incident forensics. While vCenter events are sent to central log servers in real time, it is important that administrators have quick access to this information when needed.

vCenter retains 30 days of tasks and events by default, and this is sufficient for most purposes. The vCenter disk partitions are also sized with this in mind. Decreasing is not recommended for operational reasons, while increasing is not recommended unless guided by VMware support due to the partition sizing concerns.

Audit:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> General.
Click to expand the "Database" section.
Note the "Task retention" and "Event retention" values.
If either value is configured to less than "30" days, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Settings >> General.
Click "Edit".
On the "Database" tab, set the value for both "Task retention" and "Event retention" to "30" days (default) or greater, as required by your site.
Click "Save".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.57 VCSA-80-000294 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server Native Key Provider must be backed up with a strong password.

```
GROUP ID: V-258960
RULE ID: SV-258960r1051428
```

Rationale:

The vCenter Native Key Provider feature was introduced in 7.0 U2 and acts as a key provider for encryption-based capabilities such as encrypted virtual machines without requiring an external KMS solution. When enabling this feature, a backup must be taken, which is a PKCS12 formatted file. If no password is provided during the backup process, this presents the opportunity for this to be used maliciously and compromise the environment.

Audit:

If the vCenter Native Key Provider feature is not in use, this is not applicable.
Interview the system administrator and determine if a password was provided for any backups taken of the Native Key Provider.
If backups exist for the Native Key Provider that are not password protected, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select a vCenter Server >> Configure >> Security >> Key Providers.
Select the Native Key Provider, click "Back-up", and check the box "Protect Native Key Provider data with password".
Provide a strong password and click "Back up key provider".
Delete any previous backups that were not protected with a password.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.58 VCSA-80-000295 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must require authentication for published content libraries.

```
GROUP ID: V-258961
RULE ID: SV-258961r1051430
```

Rationale:

In the vSphere Client, you can create a local or a subscribed content library. By using content libraries, you can store and manage content in one vCenter Server instance. Alternatively, you can distribute content across vCenter Server instances to increase consistency and facilitate the deployment workloads at scale. When publishing a content library it can be protected by requiring authentication for subscribers.

Audit:

Note: If Content Libraries are not used, this is not applicable.
From the vSphere Client, go to Content Libraries.
Review the "Password Protected" column.
If a content library is published and is not password protected, this is a finding.

Remediation:

From the vSphere Client, go to Content Libraries.
Select the target content library.
Select "Actions" then "Edit Settings".
Click the checkbox to "Enable user authentication for access to this content library".
Enter and confirm a password for the content library. Click "OK".
Note: Any subscribed content libraries will need to be updated to enable authentication and provide the password.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.59 VCSA-80-000296 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter server must enable the OVF security policy for content libraries.

```
GROUP ID: V-258962
RULE ID: SV-258962r1051432
```

Rationale:

In the vSphere Client, you can create a local or a subscribed content library. By using content libraries, you can store and manage content in one vCenter Server instance. Alternatively, you can distribute content across vCenter Server instances to increase consistency and facilitate the deployment workloads at scale.

You can protect the OVF items by applying default OVF security policy to a content library. The OVF security policy enforces strict validation on OVF items when you deploy or update the item, import items, or synchronize OVF and OVA templates. To make sure that the OVF and OVA templates are signed by a trusted certificate, you can add the OVF signing certificate from a trusted CA.

Audit:

Note: If Content Libraries are not used, this is not applicable.
From the vSphere Client, go to Content Libraries.
Review the "Security Policy" column.
If a content library does not have the "OVF default policy" enabled, this is a finding.

Remediation:

From the vSphere Client, go to Content Libraries.
Select the target content library.
Select "Actions" then "Edit Settings".
Click the checkbox to "Apply Security Policy". Click "OK".
Note: If you disable the security policy of a content library, you cannot reuse the existing OVF items.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.60 VCSA-80-000298 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must separate authentication and authorization for administrators.

```
GROUP ID: V-258963
RULE ID: SV-258963r961863
```

Rationale:

Many organizations do both authentication and authorization using a centralized directory service such as Active Directory. Attackers who compromise an identity source can often add themselves to authorization groups, and simply log into systems they should not otherwise have access to. Additionally, reliance on central identity systems means that the administrators of those systems are potentially infrastructure administrators, too, as they can add themselves to infrastructure access groups at will.

The use of local SSO groups for authorization helps prevent this avenue of attack by allowing the centralized identity source to still authenticate users but moving authorization into vCenter itself.

Audit:

From the vSphere Client, go to Administration >> Access Control >> Roles.
View the Administrator role and any other role providing administrative access to vCenter to verify the users and/or groups assigned to it by clicking on "Usage".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VIPermission | Sort Role | Select Role,Principal,Entity,Propagate,IsGroup | FT -Auto
If any user or group is directly assigned a role with administrative access to vCenter that is from an identity provider, this is a finding.
Note: Users and/or groups assigned to roles should be from the "VSPHERE.LOCAL" identity source.

Remediation:

To add groups from an identity provider to the local SSO Administrators group, as an example, do the following:
From the vSphere Client, go to Administration >> Single Sign On >> Groups.
Select the Administrators group and click "Edit".
In the "Add Members" section, select the identity source and type the name of the target user/group in the search bar.
Select the target user/group to add them and click "Save".
Note: A new SSO group or groups can be created as needed and used to provide authorization to vCenter.
To remove identity provider users/groups from a role, do the following:
From the vSphere Client, go to Administration >> Access Control >> Global Permissions.
Select the offending user/group and click "Delete".
Note: If permissions are assigned on a specific object, then the role must be updated where it is assigned (for example, at the cluster level).

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.61 VCSA-80-000299 (Manual)

Profile Applicability:

- SEVERITY: CAT III

Description:

The vCenter Server must disable CDP/LLDP on distributed switches.

```
GROUP ID: V-258964
RULE ID: SV-258964r961863
```

Rationale:

The vSphere Distributed Virtual Switch can participate in Cisco Discovery Protocol (CDP) or Link Layer Discovery Protocol (LLDP), as a listener, advertiser, or both. The information is sensitive, including IP addresses, system names, software versions, and more. It can be used by an adversary to gain a better understanding of your environment, and to impersonate devices. It is also transmitted unencrypted on the network, and as such the recommendation is to disable it.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Properties.
Review the "Discovery Protocol" configuration.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDSwitch | Select Name,LinkDiscoveryProtocolOperation
If any distributed switch does not have "Discovery Protocols" disabled, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Properties.
Click "Edit".
Select the advanced tab and update the "Type" under "Discovery Protocol" to disabled and click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDSwitch -Name "DSwitch" | Set-VDSwitch -LinkDiscoveryProtocolOperation "Disabled"

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.62 VCSA-80-000300 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must remove unauthorized port mirroring sessions on distributed switches.

```
GROUP ID: V-258965
RULE ID: SV-258965r961863
```

Rationale:

The vSphere Distributed Virtual Switch can enable port mirroring sessions allowing traffic to be mirrored from one source to a destination. If port mirroring is configured unknowingly this could allow an attacker to observe network traffic of virtual machines.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Port Mirroring.
Review any configured "Port Mirroring" sessions.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
Get-VDSwitch | select Name,@{N="Port Mirroring Sessions";E={$_.ExtensionData.Config.VspanSession.Name}}
If there are any unauthorized port mirroring sessions configured, this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Configure >> Settings >> Port Mirroring.
Select the unauthorized "Port Mirroring" session and click "Remove". Click "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.63 VCSA-80-000301 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must not override port group settings at the port level on distributed switches.

```
GROUP ID: V-258966
RULE ID: SV-258966r961863
```

Rationale:

Port-level configuration overrides are disabled by default. Once enabled, this allows for different security settings to be set from what is established at the Port Group level. If overrides are not monitored, anyone who gains access to a VM with a less secure VDS configuration could exploit that broader access.

If there are cases where particular VMs require unique configurations then a different port group with the required configuration should be created instead of overriding port group settings.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Properties.
Review the "Override port policies".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
(Get-VDPortgroup).ExtensionData.Config.Policy
If there are any distributed port groups that allow overridden port policies, this is a finding.
Note: This does not apply to the "Block Ports" or "Configure reset at disconnect" policies.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Properties.
Click "Edit".
Select advanced and update all port policies besides "Block Ports" to "disabled" and click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:

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

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.64 VCSA-80-000302 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must reset port configuration when virtual machines are disconnected.

```
GROUP ID: V-258967
RULE ID: SV-258967r961863
```

Rationale:

Port-level configuration overrides are disabled by default. Once enabled, this allows for different security settings to be set from what is established at the Port Group level. If overrides are not monitored, anyone who gains access to a VM with a less secure VDS configuration could exploit that broader access.

If any unknown or unauthorized per-port overrides exist and are not discarded when a virtual machine is disconnected from that port then a future virtual machine connected to that port may receive a less secure port.

Audit:

If distributed switches are not used, this is not applicable.
From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Properties.
Review the "Configure reset at disconnect" setting.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:
(Get-VDPortgroup).ExtensionData.Config.Policy.PortConfigResetAtDisconnect
If there are any distributed port groups with "Configure reset at disconnect" configured to "disabled" or "False", this is a finding.

Remediation:

From the vSphere Client, go to "Networking".
Select a distributed switch >> Select a distributed port group >> Configure >> Settings >> Properties.
Click "Edit".
Select advanced and update "Configure reset at disconnect" to be enabled and click "OK".
or
From a PowerCLI command prompt while connected to the vCenter server, run the following command:

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

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.65 VCSA-80-000303 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable Secure Shell (SSH) access.

```
GROUP ID: V-258968
RULE ID: SV-258968r961863
```

Rationale:

vCenter Server is delivered as an appliance, and intended to be managed through the VAMI, vSphere Client, and APIs. SSH is a troubleshooting and support tool and should only be enabled when necessary.

vCenter Server High Availability uses SSH to coordinate the replication and failover between the nodes. Use of this feature requires SSH to remain enabled.

Audit:

Open the Virtual Appliance Management Interface (VAMI) by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with a Single Sign-On (SSO) account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Access" on the left navigation pane.
If "SSH Login" is not "Deactivated", this is a finding.

Remediation:

Open the Virtual Appliance Management Interface (VAMI) by navigating to https://<vCenter server>:5480.
Log in with local operating system administrative credentials or with a Single Sign-On (SSO) account that is a member of the "SystemConfiguration.BashShellAdministrator" group.
Select "Access" on the left navigation pane.
Click "Edit" then disable "Activate SSH Login" and click "OK".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.66 VCSA-80-000304 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must enable data in transit encryption for vSAN.

```
GROUP ID: V-258969
RULE ID: SV-258969r961863
```

Rationale:

Transit encryption must be enabled to prevent unauthorized disclosure information and to protect the confidentiality of organizational information.

vSAN data-in-transit encryption has the following characteristics: -vSAN uses AES-256 bit encryption on data in transit. -Forward secrecy is enforced for vSAN data-in-transit encryption. -Traffic between data hosts and witness hosts is encrypted. -File service data traffic between the VDFS proxy and VDFS server is encrypted. -vSAN file services inter-host connections are encrypted. -vSAN uses symmetric keys that are generated dynamically and shared between hosts. Hosts dynamically generate an encryption key when they establish a connection, and they use the key to encrypt all traffic between the hosts. You do not need a key management server to perform data-in-transit encryption.

Each host is authenticated when it joins the cluster, ensuring connections only to trusted hosts are allowed. When a host is removed from the cluster, it is authentication certificate is removed.

vSAN data-in-transit encryption is a cluster-wide setting. When enabled, all data and metadata traffic is encrypted as it transits across hosts.

Audit:

If no clusters are enabled for vSAN, this is not applicable.
From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Select the cluster >> Configure >> vSAN >> Services >> Data Services.
Review the "Data-in-transit encryption" status.
or
From a PowerCLI command prompt while connected to the vCenter server, run the following commands:
$vsanclusterconf = Get-VsanView -Id VsanVcClusterConfigSystem-vsan-cluster-config-system
$vsanclusterconf.VsanClusterGetConfig((Get-Cluster -Name).ExtensionData.MoRef).DataInTransitEncryptionConfig
Repeat these steps for each vSAN enabled cluster in the environment.
If "Data-In-Transit encryption" is not enabled, this is a finding.

Remediation:

From the vSphere Client, go to Host and Clusters.
Select the vCenter Server >> Select the target cluster >> Configure >> vSAN >> Services >> Data Services.
Click "Edit".
Enable "Data-In-Transit encryption" and choose a rekey interval suitable for the environment then click "Apply".

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

1.67 VCSA-80-000305 (Manual)

Profile Applicability:

- SEVERITY: CAT II

Description:

The vCenter Server must disable accounts used for Integrated Windows Authentication (IWA).

```
GROUP ID: V-265979
RULE ID: SV-265979r1003616
```

Rationale:

If not used for their intended purpose, default accounts must be disabled. vCenter ships with several default accounts, two of which are specific to IWA and SASL/Kerberos authentication. If other methods of authentication are used, these accounts are not needed and must be disabled.

Audit:

If IWA is used for vCenter authentication, this is not applicable.
From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Users.
Change the domain to "vsphere.local" and review the "K/M" and "krbtgt/VSPHERE.LOCAL" accounts.
If the "K/M" and "krbtgt/VSPHERE.LOCAL" accounts are not disabled, this is a finding.

Remediation:

From the vSphere Client, go to Administration >> Single Sign On >> Users and Groups >> Users.
Select the "K/M" or "krbtgt/VSPHERE.LOCAL" and click "More" then select "Disable".
Click "Ok" to disable the user account.

Additional Information:

CCI-000366 Implement the security configuration settings.

- NIST SP 800-53::CM-6 b
- NIST SP 800-53A::CM-6.1 (iv)
- NIST SP 800-53 Revision 4::CM-6 b
- NIST SP 800-53 Revision 5::CM-6 b

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**STIG RULES**		
1.1	VCSA-80-000009 (Manual)	☐	☐
1.2	VCSA-80-000023 (Manual)	☐	☐
1.3	VCSA-80-000024 (Manual)	☐	☐
1.4	VCSA-80-000034 (Manual)	☐	☐
1.5	VCSA-80-000057 (Manual)	☐	☐
1.6	VCSA-80-000059 (Manual)	☐	☐
1.7	VCSA-80-000060 (Manual)	☐	☐
1.8	VCSA-80-000069 (Manual)	☐	☐
1.9	VCSA-80-000070 (Manual)	☐	☐
1.10	VCSA-80-000072 (Manual)	☐	☐
1.11	VCSA-80-000071 (Manual)	☐	☐
1.12	VCSA-80-000073 (Manual)	☐	☐
1.13	VCSA-80-000074 (Manual)	☐	☐
1.14	VCSA-80-000077 (Manual)	☐	☐
1.15	VCSA-80-000080 (Manual)	☐	☐
1.16	VCSA-80-000079 (Manual)	☐	☐
1.17	VCSA-80-000089 (Manual)	☐	☐
1.18	VCSA-80-000095 (Manual)	☐	☐
1.19	VCSA-80-000110 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.20	VCSA-80-000123 (Manual)	☐	☐
1.21	VCSA-80-000145 (Manual)	☐	☐
1.22	VCSA-80-000148 (Manual)	☐	☐
1.23	VCSA-80-000150 (Manual)	☐	☐
1.24	VCSA-80-000158 (Manual)	☐	☐
1.25	VCSA-80-000195 (Manual)	☐	☐
1.26	VCSA-80-000196 (Manual)	☐	☐
1.27	VCSA-80-000248 (Manual)	☐	☐
1.28	VCSA-80-000253 (Manual)	☐	☐
1.29	VCSA-80-000265 (Manual)	☐	☐
1.30	VCSA-80-000266 (Manual)	☐	☐
1.31	VCSA-80-000267 (Manual)	☐	☐
1.32	VCSA-80-000268 (Manual)	☐	☐
1.33	VCSA-80-000269 (Manual)	☐	☐
1.34	VCSA-80-000270 (Manual)	☐	☐
1.35	VCSA-80-000271 (Manual)	☐	☐
1.36	VCSA-80-000272 (Manual)	☐	☐
1.37	VCSA-80-000273 (Manual)	☐	☐
1.38	VCSA-80-000275 (Manual)	☐	☐
1.39	VCSA-80-000276 (Manual)	☐	☐
1.40	VCSA-80-000274 (Manual)	☐	☐
1.41	VCSA-80-000277 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.42	VCSA-80-000278 (Manual)	☐	☐
1.43	VCSA-80-000279 (Manual)	☐	☐
1.44	VCSA-80-000280 (Manual)	☐	☐
1.45	VCSA-80-000281 (Manual)	☐	☐
1.46	VCSA-80-000282 (Manual)	☐	☐
1.47	VCSA-80-000283 (Manual)	☐	☐
1.48	VCSA-80-000284 (Manual)	☐	☐
1.49	VCSA-80-000285 (Manual)	☐	☐
1.50	VCSA-80-000286 (Manual)	☐	☐
1.51	VCSA-80-000287 (Manual)	☐	☐
1.52	VCSA-80-000288 (Manual)	☐	☐
1.53	VCSA-80-000290 (Manual)	☐	☐
1.54	VCSA-80-000291 (Manual)	☐	☐
1.55	VCSA-80-000292 (Manual)	☐	☐
1.56	VCSA-80-000293 (Manual)	☐	☐
1.57	VCSA-80-000294 (Manual)	☐	☐
1.58	VCSA-80-000295 (Manual)	☐	☐
1.59	VCSA-80-000296 (Manual)	☐	☐
1.60	VCSA-80-000298 (Manual)	☐	☐
1.61	VCSA-80-000299 (Manual)	☐	☐
1.62	VCSA-80-000300 (Manual)	☐	☐
1.63	VCSA-80-000301 (Manual)	☐	☐

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.64	VCSA-80-000302 (Manual)	☐	☐
1.65	VCSA-80-000303 (Manual)	☐	☐
1.66	VCSA-80-000304 (Manual)	☐	☐
1.67	VCSA-80-000305 (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
09-04-2025	1.0.0	Initial CIS Release