**Using This Master Template**

There are four sections on these first two pages that contain information on using the template:

* **Section 1 (IMPORTANT):** Seven fields immediately below in section 1 allow you to insert information specific to your document and then have that information AUTOMATICALLY populated into corresponding fields within the actual template below. This is a new capability that frees you up from having to update a document’s often-confusing Properties dialog window. Information in these fields is critical for ISO purposes.
* **Section 2:** Information on the Cisco Customer Experience (CX) *Documentation Master Template* and the accompanying *Documentation Style Guide*.
* **Section 3:** Information on updating a document’s security classification, if necessary. In most cases, this will not be necessary.
* **Section 4:** Information on updating a document’s footers, if necessary.
* These two template instruction pages, as well as other additional instructions (**red text**) on other pages of the template, ***must be removed*** before you submit a final document. Drag your mouse across all text and press ***Delete***. Be aware, you may have to press *Delete* twice to delete these first two pages.

**Section 1: Template’s Automatic Fields**

Click on a field below and then click on the small box with three dots appearing at the front of the field. This selects the field for updates. Enter an appropriate title for each of the seven fields. Corresponding fields within the actual template starting with the title page will now be automatically updated.

* [Project Name and Customer Name, e.g., “Cisco ACI for ABC Industries”]
* [Deliverable Name, e.g., “Low-Level Design”]
* [Version, e.g., “0.1”, “1.0”]
* [Author Name, e.g., “John Smith, Customer Experience, Cisco”]
* [Change Authority, e.g., “Customer Experience, Cisco”]
* [DCP Content ID, if applicable (otherwise “n/a”)]
* [Project ID, if applicable (otherwise “n/a”)]

**Section 2**: **Cisco CX Documentation** ***Master Template*** and ***Style Guide***

This Master Template presents a general framework of document sections that should be included in all documents of this type presented to the customer. Add or remove sections that fit your specific customer scenario. However, do not edit or remove the last two sections (Trademarks and Disclaimers, Document Acceptance) under any circumstances. The template is closely governed by instructions in the Cisco CX Documentation Style Guide mentioned below.

This template conforms to documentation style guidelines (fonts, headers, footers, format, graphics, etc.) included in all ICN templates, and it contains the ISO-required document control elements and the Cisco data classification as well. Please send any feedback or requests for style enhancements to the following:

[svt-templates-team@cisco.com](mailto:svt-templates-team@cisco.com)

* Click below to access a page containing a link to a PowerPoint deck on the DCP process as it relates to documentation standards in Cisco CX. It contains information on document requirements, templates, processing, reviews, approvals, versioning, etc.  
  <https://go2.cisco.com/DCP2DailyUse>

The Cisco CX Documentation **Style Guide** contains detailed instructions on document structure, formatting, styles, figures and tables, graphics, trademarks and disclaimers, and customer acceptance. The Style Guide can be found here: <https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-22030275&ver=approved>

It is essential writers review the Style Guide for instructions on properly writing their documents. Instructions in the guide are Cisco CX-approved and ISO-compliant.

**Section 3:** **Changing a Document’s** ***Security Classification*** **in the Footer**

This template allows an author to change the security classification appearing in the footer, from the default of Cisco Highly Confidential to Cisco Public, Cisco Confidential, or Cisco Restricted:

1. Go to **File** > **Info** > **Properties** > **Advanced Properties** > **Custom** tab.
2. In the Properties field, scroll to the bottom and click on **Document Classification.**
3. In the Value field immediately above, type a new classification level and click **Modify**.
4. Click **OK**.
5. See the instructions below for ***Updating a Document’s Page Footers*** to update the document’s classification.

|  |
| --- |
| **For Apple Mac users:**   1. From your Apple Mac’s main toolbar at the top of the screen, click on **File** and select **Properties**. 2. Click on **Custom** tab. 3. In the Properties field, click on **Document Classification.** 4. In the Value field immediately above, type a new classification level and click **Modify**. 5. Click **OK**. See the instructions below for ***Updating a Document’s Page Footers*** to update the document’s classification. |

For more information on *Security Classifications*: <http://wwwin.cisco.com/infosec/policies/classification.shtml>

**Section 4:** **Updating a Document’s** ***Page Footers***

1. Scroll to the first page displaying the standard expanded footer (as opposed to the abbreviated footer on the title page), which should be the first page of the Table of Contents.
2. Double-click anywhere in the footer. The Header and Footer tab automatically opens.
3. If you have changed the document’s default classification from **Cisco Highly Confidential** to one of the other accepted classifications, right-click on the classification field in the footer and select Update Field to update the footer.

Scroll down after the cover page to make sure the footer has been updated on subsequent pages in the document. If not, repeat the process on those pages and then recheck the footers again.



[Project Name and Customer Name, e.g., “Cisco ACI for ABC Industries”]

[Deliverable Name, e.g., “Low-Level Design”]

October 4, 2023

Version [Version, e.g., “0.1”, “1.0”]

Phone: +1 408-526-4000

Toll Free: +1 800-553-NETS (6387)

Fax: +1 408-526-4100

**Document Classification**

**Cisco Highly Confidential**

170 West Tasman Drive

San Jose, CA 95134-1706 USA

Cisco Systems, Inc.

Corporate Headquarters

Contents

[Contents 2](#_Toc95212150)

[List of Figures and Tables 3](#_Toc95212151)

[About This Document 4](#_Toc95212152)

[History 4](#_Toc95212153)

[Review 4](#_Toc95212154)

[Document Conventions 4](#_Toc95212155)

[1 Introduction 5](#_Toc95212156)

[1.1 Preface 5](#_Toc95212157)

[1.2 Audience 5](#_Toc95212158)

[1.3 Scope 5](#_Toc95212159)

[1.4 Assumptions 5](#_Toc95212160)

[1.5 Related Documents 5](#_Toc95212161)

[2 Heading 1 6](#_Toc95212162)

[2.1 Heading 2 6](#_Toc95212163)

[2.1.1 Heading 3 6](#_Toc95212164)

[Heading 1-No Numbers 7](#_Toc95212165)

[Heading 2-No Numbers 7](#_Toc95212166)

[Heading 3-No Numbers 7](#_Toc95212167)

[3 Appendix A: Title 8](#_Toc95212168)

[3.1 Appendix A Sub-Section 8](#_Toc95212169)

[3.1.1 Appendix A Sub-Section 8](#_Toc95212170)

[4 Appendix B: Acronym Listing/Glossary 9](#_Toc95212171)

[Trademarks and Disclaimers 10](#_Toc95212172)

[Document Acceptance 11](#_Toc95212173)

List of Figures and Tables

**No table of figures entries found.**

**No table of figures entries found.**

About This Document

|  |  |
| --- | --- |
| Author | [Author Name, e.g., “John Smith, Customer Experience, Cisco”] |
| Change Authority | [Change Authority, e.g., “Customer Experience, Cisco”] |
| DCP Reference | [DCP Content ID, if applicable (otherwise “n/a”)] |
| Project ID | [Project ID, if applicable (otherwise “n/a”)] |

History

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Status | Change Description |
| 0.1 | YYYY-MM-DD | Pre-draft | Initial creation |
| 0.2 |  |  |  |
| 0.3 |  |  |  |
| … |  | Draft |  |
| 1.0 |  | Final |  |

Review

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Reviewer | Review Description |
| 0.x | YYYY-MM-DD |  |  |
| … |  |  |  |
| … |  |  |  |

Document Conventions

|  |  |
| --- | --- |
|  | Caution: Alerts readers to be careful. In this situation, you might do something that could result in equipment damage or loss of data. |
|  | Note: Alerts readers to take note. Notes contain helpful suggestions or references to material not covered in the document. |
|  | Timesaver: Alerts the reader that they can save time by performing the action described in the paragraph affixed to this icon. |
|  | Tip: Alerts the reader that the information affixed to this icon will help them solve a problem. The information might not be troubleshooting or even an action, but it could be useful information similar to a Timesaver. |
|  | Warning: Alerts readers of a situation that could cause bodily injury. They need to be aware of the hazards involved with electrical circuitry and familiarize themselves with standard practices for preventing accidents. |

# Introduction

## Preface

[Enter appropriate text in this section using style **Normal**.]

## Audience

[Enter appropriate text in this section using style **Normal**.]

## Scope

[Enter appropriate text in this section using style **Normal**.]

## Assumptions

[Enter appropriate text in this section using style **Normal**.]

## Related Documents

[Enter appropriate text in this section using style **Normal**.]

* It is absolutely essential writers review the Cisco CX Documentation Style Guide for instructions on properly writing their documents. Instructions in the guide are Cisco CX-approved and ISO-compliant. Adherence to the Style Guide is mandatory. The Style Guide is available in Doc Central:   
  <https://docs.cisco.com/share/proxy/alfresco/url?docnum=EDCS-22030275&ver=approved>

# Heading 1

[Enter appropriate text in this section using style **Normal**.]

## Heading 2

[Enter appropriate text in this section using style **Normal**.]

### Heading 3

[Enter appropriate text in this section using style **Normal**.]

#### Heading 4

[Enter appropriate text in this section using style **Normal**.]

##### Heading 5

[Enter appropriate text in this section using style **Normal**.]

###### Heading 6

[Enter appropriate text in this section using style **Normal**.]

Heading 7

[Enter appropriate text in this section using style **Normal**.]

Heading 8

[Enter appropriate text in this section using style **Normal**.]

Heading 9

[Enter appropriate text in this section using style **Normal**.]

1. AAA
2. Aaaaa aaaaa Aaaaa Aaaaa Aaaaa Aaaaa Aaaaa aaaaa Aaaaa Aaaaa Aaaaa aaaaa Aaaaa Aaaaa Aaaaa aaaaa Aaaaa Aaaaa

Heading 1-No Numbers

[Enter appropriate text in this section using style **Normal**.]

* In using this Cisco CX Document Master Template, if for some reason you decide to use one of the unnumbered types of headings, you will be unable to set up cross-references from text in other numbered sections in your document to text in these unnumbered sections.

Heading 2-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 3-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 4-No Numbers

[Enter appropriate text in this section using style **Normal**.]

Heading 5-No Numbers

[Enter appropriate text in this section using style **Normal**.]

# Appendix A: Title

[Enter appropriate text in this section using style **Normal**.]

## Appendix A Sub-Section

[Enter appropriate text in this section using style **Normal**.]

### Appendix A Sub-Section

[Enter appropriate text in this section using style **Normal**.]

# Appendix B: Acronym Listing/Glossary

* Adjust the section headline depending on its content   
  (either "Appendix B: Acronym Listing" or "Appendix B: Glossary").

|  |  |
| --- | --- |
| Term | Definition |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Trademarks and Disclaimers

IF THIS DOCUMENT IS PROVIDED AS A DELIVERABLE IN ACCORDANCE WITH THE CISCO TERMS AND CONDITIONS ASSOCIATED WITH A PURCHASED CISCO SERVICE (“TERMS”) THEN THIS DOCUMENT IS PRESENTED SUBJECT TO THOSE TERMS. IN ALL OTHER EVENTS, THIS DOCUMENT IS PROVIDED “AS-IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2022 Cisco and/or its affiliates. All rights reserved.

Document Acceptance

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Name |  | Name |  |
| Title |  | Title |  |
| Company |  | Company |  |
| Signature |  | Signature |  |
| Date |  | Date |  |

# NSO Operating System (RHEL) Security Features Validation

The following tests verify the security configuration that are expected to be implemented on the redhat servers that will host the Cisco NSO application  
 - firewall Service Configrations  
 - autheselect custome profile creation and modifications  
 - PAM Configrations  
 - Password quality modifications Refer to the SCDP documentation to address any failed tests.

Table- NSO Operating System (RHEL) Security Features Validation Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 5 | 6 | 0 |

Table- Verify firewalld service is enabled

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | The firewall service should not be disabled on reboot |
| procedure | 1. Run the command systemctl is-enabled firewalld 2. Verify that the response is 'enabled' |
| status | PASS |
| messages | Run the command systemctl is-enabled firewalld Verify that the response is 'enabled' Running command 'systemctl is-enabled firewalld 2>&1'. ${output} = enabled |

Table- Verify NSO ports are configured in the firewalld

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | Check that the neccesary tcp/udp ports are open for nso the ports are listed in the list "nso\_fw\_ports" defined in the global Variables List includes the following : ['2022', '2024', '8080', '8888'] |
| procedure | 1. Run the command sudo firewall-cmd --list-all 2. Verify that the required ports are configured |
| status | PASS |
| messages | Run the command sudo firewall-cmd --list-all Verify that the required ports are configured Running command 'sudo firewall-cmd --list-all 2>&1'. ${output} = public (active)  target: default  icmp-block-inversion: no  interfaces: ens160  sources:   services: cockpit dhcpv6-client ssh  ports: 22/tcp 2022/tcp 2024/tcp 8888/tcp 4000/udp 1062/udp 20243/t... 2022 2024 8080 8888 |

Table- Verify authselect profile sssd-vf is created

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | Verify that a custom sssd profile has been created |
| procedure | 1. Run the command 'authselect list' 2. Verify that the 'sssd-vf' profile exists |
| status | PASS |
| messages | Run the command 'authselect list' Verify that the 'sssd-vf' profile exists Running command 'authselect list 2>&1'. ${output} = - minimal Local users only for minimal installations - sssd Enable SSSD for system authentication (also for local users only) - winbind Enable winbind for system authenticat... |

Table- Verify expected authselect profile is active

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | This runs the command "authselect current -r" and returns the current active profile the test checks that this matches the expected value of custom/sssd-vf |
| procedure | 1. Run the command 'authselect current -r' 2. Verify that the profile custom/sssd-vf is active |
| status | PASS |
| messages | Run the command 'authselect current -r' Verify that the profile custom/sssd-vf is active Running command 'authselect current -r 2>&1'. ${output} = custom/sssd-vf without-nullok with-faillock ${profile} = custom/sssd-vf Execution passed with message: Current Profile is correct - sssd-vf |

Table- Verify that the required PAM Modules are enabled

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | This test will verify that without-nullok and with-faillock modules are activated the test will run the command "autheselect current" which returns the enabled features in the format:  Profile ID: custom/sssd-vf Enabled features: - with-faillock - without-nullok  Checks made against the following features: ['with-faillock', 'without-nullok'] |
| procedure | 1. Run the command 'authselect current' 2. Validate that the required features, listed above, are enabled |
| status | PASS |
| messages | Run the command 'authselect current' Validate that the required features, listed above, are enabled Running command 'authselect current 2>&1'. ${output} = Profile ID: custom/sssd-vf Enabled features: - without-nullok - with-faillock ${module\_status\_dict} = {} Profile ID: custom/sssd-vf Enabled features: - without-nullok - with-faillock ${regex\_result} = PASS ${regex\_message} = with-faillock ${regex\_result} = PASS ${regex\_message} = without-nullok {'with-faillock': 'PASS', 'without-nullok': 'PASS'} ${status} = PASS ${status\_message} = None PASS |

Table- Check the password-auth file has been updated

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | Read the /etc/authselect/custom/sssd-vf/password-auth file and check that the values have been modified the check takes a dict with the module search string and the expected configuration as a k,v Pairs the check then searches the file for the key and evaluates the value |
| procedure | 1. View the contents of the file: '/etc/authselect/custom/sssd-vf/password-auth' 2. Locate the 'pam\_unix.so' entry in the auth section, verify that the definition includes 'try\_first\_pass' 3. Locate the 'pam\_pwquality.so' entry in the password section, verify that the definition includes 'try\_first\_pass' 4. Locate the 'pam\_unix.so' entry in the password section, verify the definition includes 'try\_first\_pass' |
| status | FAIL |
| messages | View the contents of the file: '/etc/authselect/custom/sssd-vf/password-auth' Locate the 'pam\_unix.so' entry in the auth section, verify that the definition includes 'try\_first\_pass' Locate the 'pam\_pwquality.so' entry in the password section, verify that the definition includes 'try\_first\_pass' Locate the 'pam\_unix.so' entry in the password section, verify the definition includes 'try\_first\_pass' ${check\_dict} = {'auth.\*pam\_unix.so': '{if not "without-nullok":nullok} try\_first\_pass', 'password.\*pam\_pwquality.so': 'try\_first\_pass local\_users\_only', 'password.\*pam\_unix.so sha512 shadow': '{if not "without-nullo... Getting file '<a href="file:///etc/authselect/custom/sssd-vf/password-auth">/etc/authselect/custom/sssd-vf/password-auth</a>'. ${password\_auth} = auth required pam\_env.so auth required pam\_faildelay.so delay=2000000 auth required ... ${error\_list} = [] auth.\*pam\_unix.so : {if not "without-nullok":nullok} try\_first\_pass ${matches} = ['{if not "without-nullok":nullok}'] Length is 1 ${len} = 1 Match Found match auth.\*pam\_unix.so : ['{if not "without-nullok":nullok}'] {if not "without-nullok":nullok} auth.\*pam\_unix.so Not configured as expected password.\*pam\_pwquality.so : try\_first\_pass local\_users\_only ${matches} = ['local\_users\_only'] Length is 1 ${len} = 1 Match Found match password.\*pam\_pwquality.so : ['local\_users\_only'] local\_users\_only password.\*pam\_pwquality.so Not configured as expected password.\*pam\_unix.so sha512 shadow : {if not "without-nullok":nullok} try\_first\_pass use\_authtok ${matches} = ['{if not "without-nullok":nullok} use\_authtok'] Length is 1 ${len} = 1 Match Found match password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok} use\_authtok'] {if not "without-nullok":nullok} use\_authtok password.\*pam\_unix.so sha512 shadow Not configured as expected ['auth.\*pam\_unix.so', 'password.\*pam\_pwquality.so', 'password.\*pam\_unix.so sha512 shadow'] Length is 3 Errors found in the following modules ['auth.\*pam\_unix.so', 'password.\*pam\_pwquality.so', 'password.\*pam\_unix.so sha512 shadow'] |

Table- Check the system-auth file has been updated

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | Read the /etc/authselect/custom/sssd-vf/system-auth file and check that the values have been modified the check takes a dict with the module search string and the expected configuration as a k,v Pairs the check then searches the file for the key and evaluates the value |
| procedure | 1. View the contents of the file: '/etc/authselect/custom/sssd-vf/system-auth' 2. Locate the 'pam\_unix.so' entry in the auth section, verify that the definition matches '{if not "without-nullok":nullok} try\_first\_pass' 3. Locate the 'pam\_pwquality.so' entry in the password section, verify that the definition matches 'try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12' 4. Locate the 'pam\_unix.so' entry in the password section, verify the definition matche '{if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12' |
| status | FAIL |
| messages | View the contents of the file: '/etc/authselect/custom/sssd-vf/system-auth' Locate the 'pam\_unix.so' entry in the auth section, verify that the definition matches '{if not "without-nullok":nullok} try\_first\_pass' Locate the 'pam\_pwquality.so' entry in the password section, verify that the definition matches 'try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12' Locate the 'pam\_unix.so' entry in the password section, verify the definition matche '{if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12' ${check\_dict} = {'auth.\*pam\_unix.so': '{if not "without-nullok":nullok} try\_first\_pass', 'password.\*pam\_pwquality.so': 'try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12', 'password.\*pam\_unix.so sh... Getting file '<a href="file:///etc/authselect/custom/sssd-vf/system-auth">/etc/authselect/custom/sssd-vf/system-auth</a>'. ${password\_auth} = {imply "with-smartcard" if "with-smartcard-required"} auth required pam\_env.so auth required pam\_faildelay.so dela... ${error\_list} = [] auth.\*pam\_unix.so : {if not "without-nullok":nullok} try\_first\_pass ${matches} = ['{if not "without-nullok":nullok}'] Length is 1 ${len} = 1 Match Found match auth.\*pam\_unix.so : ['{if not "without-nullok":nullok}'] {if not "without-nullok":nullok} auth.\*pam\_unix.so Not configured as expected password.\*pam\_pwquality.so : try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12 ${matches} = ['local\_users\_only'] Length is 1 ${len} = 1 Match Found match password.\*pam\_pwquality.so : ['local\_users\_only'] local\_users\_only password.\*pam\_pwquality.so Not configured as expected password.\*pam\_unix.so sha512 shadow : {if not "without-nullok":nullok} try\_first\_pass use\_authtok remember=12 ${matches} = ['{if not "without-nullok":nullok} use\_authtok'] Length is 1 ${len} = 1 Match Found match password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok} use\_authtok'] {if not "without-nullok":nullok} use\_authtok password.\*pam\_unix.so sha512 shadow Not configured as expected ['auth.\*pam\_unix.so', 'password.\*pam\_pwquality.so', 'password.\*pam\_unix.so sha512 shadow'] Length is 3 Errors found in the following modules ['auth.\*pam\_unix.so', 'password.\*pam\_pwquality.so', 'password.\*pam\_unix.so sha512 shadow'] |

Table- Verify that faillock.conf has been modifed

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | We are required to modify the fail\_interval to be = 1800 seconds |
| procedure | 1. View the file /etc/security/faillock.conf 2. Verify that the 'fail\_interval' is set to '1800' |
| status | FAIL |
| messages | View the file /etc/security/faillock.conf Verify that the 'fail\_interval' is set to '1800' ${dict} = {'fail\_interval': '1800'} ${file\_path} = /etc/security/faillock.conf {'fail\_interval': '1800'} /etc/security/faillock.conf Getting file '<a href="file:///etc/security/faillock.conf">/etc/security/faillock.conf</a>'. ${file} = # Configuration for locking the user after multiple failed # authentication attempts. # # The directory where the user files with the failure records are kept. # The default is /var/run/faillock. # di... ${errors\_list} = [] ${match} = [] Length is 0 ${number\_of\_results} = 0 Length is 1 Errors found in values for ['fail\_interval'] |

Table- Verify that pwquality.conf has been modified

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | We are required to modify the /etc/security/pwquality.conf to ensure only complex passwords are allowed following values should be used: - minlen = 8 - dcredit = -1 - ucredit = -1 - lcredit = -1 - ocredit = -1 |
| procedure | 1. View the file '/etc/security/pwquality.conf' 2. Validate that the attributes are assigned the correct values, see above |
| status | FAIL |
| messages | View the file '/etc/security/pwquality.conf' Validate that the attributes are assigned the correct values, see above ${dict} = {'minlen': '8', 'dcredit': '-1', 'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-1', 'dummy': '1'} ${file\_path} = /etc/security/pwquality.conf {'minlen': '8', 'dcredit': '-1', 'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-1', 'dummy': '1'} /etc/security/pwquality.conf Getting file '<a href="file:///etc/security/pwquality.conf">/etc/security/pwquality.conf</a>'. ${file} = # Configuration for systemwide password quality limits # Defaults: # # Number of characters in the new password that must not be present in the # old password. # difok = 1 # # Minimum acceptable size ... ${errors\_list} = [] ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = [] Length is 0 ${number\_of\_results} = 0 Length is 6 Errors found in values for ['minlen', 'dcredit', 'ucredit', 'lcredit', 'ocredit', 'dummy'] |

Table- Verify login.defs has been modifed

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | Password expiration values need to be modified in the /etc/login.defs file the default values need to be modified to meet the following requirements: - PASS\_MIN\_LEN 5 - PASS\_MAX\_DAYS 90 - PASS\_MIN\_DAYS 1 - PASS\_WARN\_AGE 5 |
| procedure | 1. View the file '/etc/login.defs' 2. Validate that the attributes are assigned the correct values, see above |
| status | FAIL |
| messages | View the file '/etc/login.defs' Validate that the attributes are assigned the correct values, see above ${dict} = {'PASS\_MAX\_DAYS': '90', 'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '5', 'dummy': '5'} ${file\_path} = /etc/login.defs {'PASS\_MAX\_DAYS': '90', 'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '5', 'dummy': '5'} /etc/login.defs Getting file '<a href="file:///etc/login.defs">/etc/login.defs</a>'. ${file} = # # Please note that the parameters in this configuration file control the # behavior of the tools from the shadow-utils component. None of these # tools uses the PAM mechanism, and the utilities that... ${errors\_list} = [] ${match} = ['99999'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 99999 99999 != 90 ${status} = FAIL ${status\_message} = 99999 != 90 ${match} = ['0'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = None Argument types are: <class 'NoneType'> <class 'str'> 'None' cannot be converted to an integer: TypeError: int() argument must be a string, a bytes-like object or a number, not 'NoneType' ${status} = FAIL ${status\_message} = 'None' cannot be converted to an integer: TypeError: int() argument must be a string, a bytes-like object or a number, not 'NoneType' ${match} = [] Length is 0 ${number\_of\_results} = 0 ${match} = ['7'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 7 7 != 5 ${status} = FAIL ${status\_message} = 7 != 5 ${match} = [] Length is 0 ${number\_of\_results} = 0 Length is 5 Errors found in values for ['PASS\_MAX\_DAYS', 'PASS\_MIN\_DAYS', 'PASS\_MIN\_LEN', 'PASS\_WARN\_AGE', 'dummy'] |

Table- Verify the user account inavtive days value has been modified

|  |  |
| --- | --- |
| section | s1-s1 |
| Purpose | The default value of INACTIVE in /etc/defaults/useradd is set to -1 which equates to no inactvity time out for user. We need to change this value to 90 as per request from Customer |
| procedure | 1. View the file '/etc/default/useradd' 2. Validate that the attributes are assigned the correct values, see above |
| status | FAIL |
| messages | View the file '/etc/default/useradd' Validate that the attributes are assigned the correct values, see above Getting file '<a href="file:///etc/default/useradd">/etc/default/useradd</a>'. ${useradd\_conf} = # useradd defaults file GROUP=100 HOME=/home INACTIVE=-1 EXPIRE= SHELL=/bin/bash SKEL=/etc/skel CREATE\_MAIL\_SPOOL=yes   ${match} = ['-1'] ${match\_val} = -1 INACTIVE not set to expected value |

# NSO Operating System (RHEL) Validations

The following tests verify the operating system configuration & dependency packages are present in preperation for the Cisco NSO application testing. The checks include:  
 - dependent packages are available  
 - required utilities are present  
 - hostname has been changed  
 - DNS and NTP serviecs are configured and active Refer to the SCDP documentation to address any failed tests.

Table- NSO Operating System (RHEL) Validations Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 8 | 2 | 0 |

Table- Verify dependency packages are installed

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Check the installed packages using the "rpm -q" command against a list of expected packages, add and remove packages form the list to modify the test case. List included : ['ant', 'java-11-openjdk', 'python3', 'openssl', 'pam', 'python3-setuptools'] |
| procedure | 1. Run the command 'rpm -q {package\_name}' and verify the neccessary packages are installed |
| status | PASS |
| messages | Run the command 'rpm -q {package\_name}' and verify the neccessary packages are installed ${command} = rpm -q ${check\_string} = not installed ${errors\_list} = [] ${run\_cmd} = rpm -q ant rpm -q ant Running command 'rpm -q ant 2>&1'. ${output} = ant-1.10.9-7.el9.noarch ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q java-11-openjdk rpm -q java-11-openjdk Running command 'rpm -q java-11-openjdk 2>&1'. ${output} = java-11-openjdk-11.0.18.0.10-2.el9\_1.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q python3 rpm -q python3 Running command 'rpm -q python3 2>&1'. ${output} = python3-3.9.16-1.el9.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q openssl rpm -q openssl Running command 'rpm -q openssl 2>&1'. ${output} = openssl-3.0.7-6.el9\_2.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q pam rpm -q pam Running command 'rpm -q pam 2>&1'. ${output} = pam-1.5.1-14.el9.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q python3-setuptools rpm -q python3-setuptools Running command 'rpm -q python3-setuptools 2>&1'. ${output} = python3-setuptools-53.0.0-12.el9.noarch ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify required package are and package versions

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Check the versions of the packages installed meets the neccessary minimum values the test calls the packages\_dict dictionary which should be populated with k,v pairs representing the required package and the minimum supported value |
| procedure | 1. Using the 'rpm -q' command valdate that the neccesary packages versions meet the minimum requirements |
| status | PASS |
| messages | ${packages\_dict} = {'ant': '1.9.3', 'java-11-openjdk': '1.1', 'python3': '3.7', 'openssl': '0', 'pam': '1.3.1', 'python3-setuptools': '0'} ${error\_list} = [] Using the 'rpm -q' command valdate that the neccesary packages versions meet the minimum requirements Package = ant Version = 1.9.3 Running command 'rpm -q ant 2>&1'. ${package\_rpm} = ant-1.10.9-7.el9.noarch ant-1.10.9-7.el9.noarch ${installed\_version} = ['1.10.9'] Installed Version : 1.10.9 @{installed\_segments} = [ 1 | 10 | 9 ] @{required\_segments} = [ 1 | 9 | 3 ] Length is 3 ${installed\_length} = 3 Length is 3 ${required\_length} = 3 ${max\_length} = 3 ${segments} = ['1', '10', '9'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 1.10.9 ${installed\_version} = 1.10.9 ${segments} = ['1', '9', '3'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 1.9.3 ${required\_version} = 1.9.3 @{installed\_segments} = [ 1 | 10 | 9 ] @{required\_segments} = [ 1 | 9 | 3 ] ${iterator} = 0 ${result} = True ${result} = True Exiting for loop altogether. ${status} = True Package : ant, Version:1.9.3 Package = java-11-openjdk Version = 1.1 Running command 'rpm -q java-11-openjdk 2>&1'. ${package\_rpm} = java-11-openjdk-11.0.18.0.10-2.el9\_1.x86\_64 java-11-openjdk-11.0.18.0.10-2.el9\_1.x86\_64 ${installed\_version} = ['11.0.18.0.10'] Installed Version : 11.0.18.0.10 @{installed\_segments} = [ 11 | 0 | 18 | 0 | 10 ] @{required\_segments} = [ 1 | 1 ] Length is 5 ${installed\_length} = 5 Length is 2 ${required\_length} = 2 ${max\_length} = 5 ${segments} = ['11', '0', '18', '0', '10'] Length is 5 ${segments\_length} = 5 ${pad\_count} = 0 ${padded\_version} = 11.0.18.0.10 ${installed\_version} = 11.0.18.0.10 ${segments} = ['1', '1'] Length is 2 ${segments\_length} = 2 ${pad\_count} = 3 ${padded\_version} = 1.1.0.0.0 ${required\_version} = 1.1.0.0.0 @{installed\_segments} = [ 11 | 0 | 18 | 0 | 10 ] @{required\_segments} = [ 1 | 1 | 0 | 0 | 0 ] ${iterator} = 0 ${result} = True Exiting for loop altogether. ${status} = True Package : java-11-openjdk, Version:1.1 Package = python3 Version = 3.7 Running command 'rpm -q python3 2>&1'. ${package\_rpm} = python3-3.9.16-1.el9.x86\_64 python3-3.9.16-1.el9.x86\_64 ${installed\_version} = ['3.9.16'] Installed Version : 3.9.16 @{installed\_segments} = [ 3 | 9 | 16 ] @{required\_segments} = [ 3 | 7 ] Length is 3 ${installed\_length} = 3 Length is 2 ${required\_length} = 2 ${max\_length} = 3 ${segments} = ['3', '9', '16'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 3.9.16 ${installed\_version} = 3.9.16 ${segments} = ['3', '7'] Length is 2 ${segments\_length} = 2 ${pad\_count} = 1 ${padded\_version} = 3.7.0 ${required\_version} = 3.7.0 @{installed\_segments} = [ 3 | 9 | 16 ] @{required\_segments} = [ 3 | 7 | 0 ] ${iterator} = 0 ${result} = True ${result} = True Exiting for loop altogether. ${status} = True Package : python3, Version:3.7 Package = openssl Version = 0 Running command 'rpm -q openssl 2>&1'. ${package\_rpm} = openssl-3.0.7-6.el9\_2.x86\_64 openssl-3.0.7-6.el9\_2.x86\_64 ${installed\_version} = ['3.0.7'] Installed Version : 3.0.7 @{installed\_segments} = [ 3 | 0 | 7 ] @{required\_segments} = [ 0 ] Length is 3 ${installed\_length} = 3 Length is 1 ${required\_length} = 1 ${max\_length} = 3 ${segments} = ['3', '0', '7'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 3.0.7 ${installed\_version} = 3.0.7 ${segments} = ['0'] Length is 1 ${segments\_length} = 1 ${pad\_count} = 2 ${padded\_version} = 0.0.0 ${required\_version} = 0.0.0 @{installed\_segments} = [ 3 | 0 | 7 ] @{required\_segments} = [ 0 | 0 | 0 ] ${iterator} = 0 ${result} = True Exiting for loop altogether. ${status} = True Package : openssl, Version:0 Package = pam Version = 1.3.1 Running command 'rpm -q pam 2>&1'. ${package\_rpm} = pam-1.5.1-14.el9.x86\_64 pam-1.5.1-14.el9.x86\_64 ${installed\_version} = ['1.5.1'] Installed Version : 1.5.1 @{installed\_segments} = [ 1 | 5 | 1 ] @{required\_segments} = [ 1 | 3 | 1 ] Length is 3 ${installed\_length} = 3 Length is 3 ${required\_length} = 3 ${max\_length} = 3 ${segments} = ['1', '5', '1'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 1.5.1 ${installed\_version} = 1.5.1 ${segments} = ['1', '3', '1'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 1.3.1 ${required\_version} = 1.3.1 @{installed\_segments} = [ 1 | 5 | 1 ] @{required\_segments} = [ 1 | 3 | 1 ] ${iterator} = 0 ${result} = True ${result} = True Exiting for loop altogether. ${status} = True Package : pam, Version:1.3.1 Package = python3-setuptools Version = 0 Running command 'rpm -q python3-setuptools 2>&1'. ${package\_rpm} = python3-setuptools-53.0.0-12.el9.noarch python3-setuptools-53.0.0-12.el9.noarch ${installed\_version} = ['53.0.0'] Installed Version : 53.0.0 @{installed\_segments} = [ 53 | 0 | 0 ] @{required\_segments} = [ 0 ] Length is 3 ${installed\_length} = 3 Length is 1 ${required\_length} = 1 ${max\_length} = 3 ${segments} = ['53', '0', '0'] Length is 3 ${segments\_length} = 3 ${pad\_count} = 0 ${padded\_version} = 53.0.0 ${installed\_version} = 53.0.0 ${segments} = ['0'] Length is 1 ${segments\_length} = 1 ${pad\_count} = 2 ${padded\_version} = 0.0.0 ${required\_version} = 0.0.0 @{installed\_segments} = [ 53 | 0 | 0 ] @{required\_segments} = [ 0 | 0 | 0 ] ${iterator} = 0 ${result} = True Exiting for loop altogether. ${status} = True Package : python3-setuptools, Version:0 Length is 0 [] |

Table- Check library availability

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Cisco NSO requires that the operating system has specific libraries installed the test verifies that the "ldconfig -p" output includes each of the libraries mentioned in the documentation. To adapt modify the list |
| procedure | 1. Run the command 'ldconfig -p' and capture the output 2. Verify that libpam.so.0 is available 3. Verify that libexpat.so.1 is available 4. Verify that libz.so.1 is available |
| status | PASS |
| messages | Run the command 'ldconfig -p' and capture the output Verify that libpam.so.0 is available Verify that libexpat.so.1 is available Verify that libz.so.1 is available ${libraries} = ['libpam.so.0', 'libexpat.so.1', 'libz.so.1'] Running command 'ldconfig -p 2>&1'. ${system\_libraries} = 510 libs found in cache `/etc/ld.so.cache'  p11-kit-trust.so (libc6,x86-64) => /lib64/p11-kit-trust.so  libzstd.so.1 (libc6,x86-64) => /lib64/libzstd.so.1  libz.so.1 (libc6,x86-64) => /lib64/libz.so.1... ${error\_list} = [] ${status} = PASS ${status\_message} = None libpam.so.0 found ${status} = PASS ${status\_message} = None libexpat.so.1 found ${status} = PASS ${status\_message} = None libz.so.1 found Length is 0 |

Table- Check libz library version

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Cisco NSO requires a minimimum version of 1.2.7.1 for the libz library this test will verify that the verison installed satisfies this requirement. |
| procedure | 1. Run the command 'python3 -c "import zlib; print (zlib.ZLIB\_VERSION)"' 2. Verify that the version is >= 1.2.7.1 |
| status | PASS |
| messages | Run the command 'python3 -c "import zlib; print (zlib.ZLIB\_VERSION)"' Verify that the version is >= 1.2.7.1 ${desired\_major\_version} = 1.2 ${desired\_minor\_version} = 7.1 Running command 'python3 -c "import zlib; print (zlib.ZLIB\_VERSION)" 2>&1'. ${libz\_version} = 1.2.11 ${found\_major\_version} = ['1.2'] ${found\_minor\_version} = ['11'] Going to evaluate : 11 > 7.1 ${log} = True True Found 1.2.11 is greater than minimum Execution passed with message: Major meets requirements, and Minor is greater or equal 1.2.11 |

Table- Verify required utilities are available

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Cisco NSO requires some utilities, this test verfies these binaries exist |
| procedure | 1. Using the command 'which' verify that tar, gzip, find, and ssh-keygen utilities are in the the system $PATH |
| status | PASS |
| messages | Using the command 'which' verify that tar, gzip, find, and ssh-keygen utilities are in the the system $PATH ${command} = which ${check\_string} = /usr/bin/which: no ${errors\_list} = [] ${run\_cmd} = which tar which tar Running command 'which tar 2>&1'. ${output} = /usr/bin/tar ${status} = PASS ${status\_message} = None ${run\_cmd} = which gzip which gzip Running command 'which gzip 2>&1'. ${output} = /usr/bin/gzip ${status} = PASS ${status\_message} = None ${run\_cmd} = which find which find Running command 'which find 2>&1'. ${output} = /usr/bin/find ${status} = PASS ${status\_message} = None ${run\_cmd} = which ssh-keygen which ssh-keygen Running command 'which ssh-keygen 2>&1'. ${output} = /usr/bin/ssh-keygen ${status} = PASS ${status\_message} = None Length is 0 |

Table- Verify correct version of Python is active

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | We require a python verison > 3.7 this test will validatre the active python environmnet meets this requirement |
| procedure | 1. Run the command 'python --version' 2. Verify that the verison is >= to 3.8 |
| status | PASS |
| messages | Run the command 'python --version' Verify that the verison is >= to 3.8 Running command 'python --version 2>&1'. ${python\_version} = Python 3.9.16 ${python\_major\_version} = ['3.9'] ${desired\_version} = 3.08 ${status} = True Execution passed with message: Active Version of Python meets the minimum requirements |

Table- Verify Hostname is not set to localhost

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Hostname Should not be localhost |
| procedure | 1. Run the command 'hostnamectl hostname' 2. Verify that the system hostname is not set to 'localhost' 3. Verify taht the hostname is set to the expected value |
| status | PASS |
| messages | Run the command 'hostnamectl hostname' Verify that the system hostname is not set to 'localhost' Verify taht the hostname is set to the expected value Running command 'hostnamectl hostname 2>&1'. ${output} = robot-dev-rhel-9.2 |

Table- Verify DNS servers are Configured

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | DNS Servers should be Configured |
| procedure | 1. View the file '/etc/resolv.conf' 2. Verify that the neccesary DNS hosts are visible |
| status | FAIL |
| messages | View the file '/etc/resolv.conf' Verify that the neccesary DNS hosts are visible Running command 'more /etc/resolv.conf 2>&1'. ${output} = # Generated by NetworkManager search localdomain 2 nameserver 172.16.167.2 '# Generated by NetworkManager search localdomain 2 nameserver 172.16.167.2' does not contain '192.168.1.1' |

Table- Verify NTP servers are Configured

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | NTP Servers should be Configured |
| procedure | 1. Run the command 'chronyc sources' 2. Verify that the neccesary NTP sources are visible |
| status | FAIL |
| messages | Run the command 'chronyc sources' Verify that the neccesary NTP sources are visible Running command 'chronyc sources 2>&1'. ${output} = MS Name/IP address Stratum Poll Reach LastRx Last sample  =============================================================================== ^- ntp4.bit.nl 1 6 ... 'MS Name/IP address Stratum Poll Reach LastRx Last sample  =============================================================================== ^- ntp4.bit.nl 1 6 377 24 +26ms[ +26ms] +/- 308ms ^\* 159.203.82.102 4 6 377 63 -31ms[ -71ms] +/- 48ms ^+ europa.ellipse.net 2 6 377 4 +46ms[ +46ms] +/- 106ms ^+ ns.bgp.co 2 6 377 41 +1279us[+1279us] +/- 98ms' does not contain 'ntp1.trans-ix.nl' |

Table- Verify NTP service is active

|  |  |
| --- | --- |
| section | s1-s2 |
| Purpose | Check that the NTP service is active |
| procedure | 1. Run the command 'timedatectl show' 2. Verify that the system shows NTPSynchronized=yes |
| status | PASS |
| messages | Run the command 'timedatectl show' Verify that the system shows NTPSynchronized=yes Running command 'timedatectl show | grep -Po '(?<=NTPSynchronized=)[^,]+' 2>&1'. ${output} = yes |

# NSO Configuration (ncs.conf) Validations

The following tests validate that the /etc/ncs/ncs.conf file has been correctly configured with the required values. The faile can be viewed by accessing the server and simply using the commands:  
 - cat /etc/ncs/ncs.conf  
 - more /etc/ncs/ncs.conf

Table- NSO Configuration (ncs.conf) Validations Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 5 | 2 | 0 |

Table- Verify ncs-ipc-access-check is enabled

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Verify that ncs-ipc-access-check is enabled |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'ncs-ipc-access-check/enabled' configuration 3. Verify the value is set to true |
| status | FAIL |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'ncs-ipc-access-check/enabled' configuration Verify the value is set to true ${xml} = false 'false' does not contain 'true' |

Table- Verify External Authentication Is enabled

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | External Authentication should be enabled to authenticate users |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'aaa/external-authentication/enabled' configuration 3. Verify the value is set to true |
| status | PASS |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'aaa/external-authentication/enabled' configuration Verify the value is set to true ${xml} = true |

Table- Verify External Authentication Script Exists

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | If External Auth is enabled check the script called Exists |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'aaa/external-authentication/executable' configuration 3. Record the vlaue of the executable 4. Verify the executable exists using the comand 'ls {file\_path}' |
| status | PASS |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'aaa/external-authentication/executable' configuration Record the vlaue of the executable Verify the executable exists using the comand 'ls {file\_path}' ${xpath} = aaa/external-authentication/executable ${auth\_file} = /etc/ncs/my-test-auth.sh Path '<a href="file:///etc/ncs/my-test-auth.sh">/etc/ncs/my-test-auth.sh</a>' exists. |

Table- Verify netconf-north-bound (GLOBAL) is enabled

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Netconf North Bound interface should be enabled |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'netconf-north-bound/enabled' configuration 3. Verify the value is set to true |
| status | PASS |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'netconf-north-bound/enabled' configuration Verify the value is set to true ${xml} = true |

Table- Verify netconf-north-bound (SSH) is enabled

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Netconf North Bound interface should be enabled |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'netconf-north-bound/transport/ssh/enabled' configuration 3. Verify the value is set to true |
| status | PASS |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'netconf-north-bound/transport/ssh/enabled' configuration Verify the value is set to true ${xml} = true |

Table- Verify netconf-north-bound is (TELNET) is disabled

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Netconf North Bound interface should be enabled |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'netconf-north-bound/transport/tcp/enabled' configuration 3. Verify the value is set to false |
| status | PASS |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'netconf-north-bound/transport/tcp/enabled' configuration Verify the value is set to false ${xml} = false |

Table- Verify High-Availability Is Enabled in ncs.conf

|  |  |
| --- | --- |
| section | s1-s3 |
| Purpose | Verify that High-Availability is enabled in the ncs.conf file |
| procedure | 1. View the file '/etc/ncs/ncs.conf' 2. Locate the 'ha/enabled' configuration 3. Verify the value is set to true |
| status | FAIL |
| messages | View the file '/etc/ncs/ncs.conf' Locate the 'ha/enabled' configuration Verify the value is set to true No element matching 'ha/enabled' found. |

# NSO Configuration (Running Config) Validation

Table- NSO Configuration (Running Config) Validation Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 3 | 0 | 4 |

Table- Is the NSO Service (NCS) Running

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | We need to verify that the service is running this test will run the command 'systemctl is-active ncs' and parse the response test passes if the response is 'actve' any other response will fail if the test fails, enable the service using the 'systemctl start ncs' command |
| procedure | 1. Run the command 'systemctl is-active ncs' 2. Verify that the NCS process is active |
| status | PASS |
| messages | Run the command 'systemctl is-active ncs' Verify that the NCS process is active Running command 'systemctl is-active ncs 2>&1'. ${status} = active ${expected\_output} = active |

Table- Is the NSO service (NCS) enabled on boot

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | Insatlling NSO doesn't automatically enable the service to persistantly start on reboot one the system has been deployed we need to ensure that the service will auto restart if the servers is rebooted. The test will verify using the 'systemct is-enabled ncs' command if the repsonse includes the string 'enabled' the test passes, if the match is not fouund the test will fail.  If the test fails enable the service using the command 'systemctl enable ncs' and re-run the test |
| procedure | 1. Run the command 'systemctl is-enabled ncs' 2. Verify that the NCS process is Enabled for auto-start |
| status | PASS |
| messages | Run the command 'systemctl is-enabled ncs' Verify that the NCS process is Enabled for auto-start Running command 'systemctl is-enabled ncs 2>&1'. ${status} = ncs.service is not a native service, redirecting to systemd-sysv-install. Executing: /usr/lib/systemd/systemd-sysv-install is-enabled ncs enabled ${expected\_output} = enabled |

Table- Extract the NSO Application Config

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | The NSO application config will be extarcted to a local file and the subsequent test will be executed against this file. If the test is unable to retrieve the configuration run the command "show running-config | display xml | save ncs\_config.xml" and move the file the test folder, the script will attempt to load a file if the extarction fails as a fallback, make sure the file is recent  The test will also validate that the test user has the neccesary group permissions needed to execute the test, if it fails add the ncsadmin group to the user 'usermod -a -G ncsadmin test\_user' |
| procedure |  |
| status | PASS |
| messages | Running command 'whoami 2>&1'. ${user} = root Running command 'groups 2>&1'. ${groups} = root ncsadmin Running command 'ncs\_cli -C -u ncsadmin <<< "show running-config | display xml" 2>&1'. ${ncs\_conf\_file} = <config xmlns="http://tail-f.com/ns/config/1.0">  <devices xmlns="http://tail-f.com/ns/ncs">  <global-settings>  <trace-dir>/var/log/ncs</trace-dir>  </global-settings>  <authgroups>  ... ${NCS\_CONF} = <config xmlns="http://tail-f.com/ns/config/1.0">  <devices xmlns="http://tail-f.com/ns/ncs">  <global-settings>  <trace-dir>/var/log/ncs</trace-dir>  </global-settings>  <authgroups>  ... ${xpath} = devices/global-settings/ ${response} = ['/var/log/ncs'] ${response} = ['/var/log/ncs'] Length is 1 Successfully Imported NCS\_CONF |

Table- Verify High-Availability is operational

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | Verify that High-Availability is operational by running the command 'show ncs-state ha' and 'show high-availbility' if the state returns errors the high-availbility is not configured correctly and needs to be modified and re-verified. |
| procedure | 1. Run the command 'show ncs-state ha' 2. Verify that the high-avaialbaility status is enabled 3. Verify that the output shows that the high-availability nodes are listed (master and Slave) |
| status | SKIP |
| messages | Run the command 'show ncs-state ha' Verify that the high-avaialbaility status is enabled Verify that the output shows that the high-availability nodes are listed (master and Slave) TODO Create Test |

Table- Verify that the T-SDN Packages are installed in NSO

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | The CNC integration with NSO requires that the T-SDN Core Function Pack (CFP) is installed and present. These packages should be uploaded to the /var/opt/ncs/packages/ folder and then linked to the /opt/ncs/packages/ directory where the system will load them on application startup. This test validates the core packages only, add additional test cases for custom packages validation. If the packages are not found the test fails. To fix, download the neccesary packages bundle and follow the CFP install instructions. |
| procedure |  |
| status | SKIP |
| messages | TODO Create Test |

Table- Verify that the T-SDN startup configurations are loaded

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | In addtion to the T-SDN Core Function Pack packages being installed the system needs start-up configuration to be loaded into the system to operate. These files are provided as XML files in the CFP bundle in the 'config/' folder. Loading these files is achived by using the 'load merge filename.xml' command |
| procedure |  |
| status | SKIP |
| messages | TODO Create Test |

Table- Test Load merge

|  |  |
| --- | --- |
| section | s1-s4 |
| Purpose | Some text |
| procedure |  |
| status | SKIP |
| messages | TODO Create Test |