

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

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

September 29, 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](#_Toc146907012)

[List of Figures and Tables 3](#_Toc146907013)

[About This Document 4](#_Toc146907014)

[History 4](#_Toc146907015)

[Review 4](#_Toc146907016)

[Document Conventions 4](#_Toc146907017)

[1 Ncs Env 6](#_Toc146907018)

[2 Security 9](#_Toc146907019)

[3 System 17](#_Toc146907020)

List of Figures and Tables

**No table of figures entries found.**

[Table-1 Ncs Env Test Results Summary 6](#_Toc146907021)

[Table-2 Verify that the overcommit\_memory value has been updated 6](#_Toc146907022)

[Table-3 Verify the T-SDN system limits have been configured 6](#_Toc146907023)

[Table-4 Verify that the limit changes are applied to the system 8](#_Toc146907024)

[Table-5 Security Test Results Summary 9](#_Toc146907025)

[Table-6 Verify firewalld service is enabled 9](#_Toc146907026)

[Table-7 Verify NSO ports are configured in the firewalld 9](#_Toc146907027)

[Table-8 Verify authselect profile sssd-vf is created 9](#_Toc146907028)

[Table-9 Verify expected authselect profile is active 10](#_Toc146907029)

[Table-10 Verify that the required PAM Modules are enabled 10](#_Toc146907030)

[Table-11 Check the password-auth file has been updated 11](#_Toc146907031)

[Table-12 Check the system-auth file has been updated 12](#_Toc146907032)

[Table-13 Verify that faillock.conf has been modifed 13](#_Toc146907033)

[Table-14 Verify that pwquality.conf has been modified 14](#_Toc146907034)

[Table-15 Verify login.defs has been modifed 15](#_Toc146907035)

[Table-16 Verify the user account inavtive days value has been modified 16](#_Toc146907036)

[Table-17 System Test Results Summary 17](#_Toc146907037)

[Table-18 Verify dependency packages are installed 17](#_Toc146907038)

[Table-19 Verify required utilities are available 18](#_Toc146907039)

[Table-20 Verify Hostname is not set to localhost 19](#_Toc146907040)

[Table-21 Verify DNS servers are Configured 19](#_Toc146907041)

[Table-22 Verify NTP servers are Configured 19](#_Toc146907042)

[Table-23 Verify NTP service is active 19](#_Toc146907043)

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. |

# Ncs Env

This set of tests validates the system envionment changes have been made for  
the Cisco NSO application and the T-SDN Core Function Pack the changes relate to:  
- overcommit\_memory disabled across reboots  
- system limits configured as per T-SDN package documentation

Table-1 Ncs Env Test Results Summary

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

Table-2 Verify that the overcommit\_memory value has been updated

|  |  |
| --- | --- |
| name | Verify that the overcommit\_memory value has been updated |
| doc | The default os value is pre-configured to 0, this needs to be modified  to "2". This can be changed at run-time by "echo 2 > /proc/sys/vm/overcommit\_memmory"  however it should be persistently added to the /etc/sysctl.d/ncs.conf  this test will check both locations |
| section | s1-s1 |
| status | PASS |
| messages | Running command 'cat  /proc/sys/vm/overcommit\_memory 2>&1'. ${run\_time\_overcommit} = 2 Getting file '<a  href="file:///etc/sysctl.d/ncs.conf">/etc/sysctl.d/ncs.conf</a>'. ${sysctl\_d\_ncs\_conf} = # Adding Over  Commit Memmory Changes  # This change keeps overcommit\_memmory (OOM) disbaled across system reboots.  vm.overcommit\_memory = 2  ${error\_list} = [] /proc/sys/vm/overcommit\_memory is  configured correctly ${matches} = ['2'] ['2'] 2 vm.overcommit\_memory assigned to  correct values Length is 0 |

Table-3 Verify the T-SDN system limits have been configured

|  |  |
| --- | --- |
| name | Verify the T-SDN system limits have been configured |
| doc | The T-SDN Core Function Pack requires system limit changes to be made  the test will check the /etc/security/limnits.d/ncs.conf file exists and that the expected  values  have been provided. The expected values are stored in a dict k,v arrangement and can be  extended  if needed   To handle the Regex \* issue we need to preface each key with  \\*s+ should be handled in  the KEywork but thats for the future |
| section | s1-s1 |
| status | PASS |
| messages | Getting file '<a  href="file:///etc/security/limits.d/ncs.conf">/etc/security/limits.d/ncs.conf</a>'. ${file} = # Adding T-SDN System Limits  needed for NSO   \* soft nproc 65535  \* hard nproc 65535  \* soft nofile 65535  \* hard nofile 65535  \* hard memlock 65536  \* soft memlock 65536  ${clean\_file} = # Adding T-SDN System  Limits needed for NSO \* soft nproc 65535  \* hard nproc 65535  \* soft nofile 65535  \* hard nofile 65535  \* hard memlock 65536  \* soft memlock 65536  ${limits\_dict} = {'soft nproc':  '65535', 'hard nproc': '65535', 'soft nofile': '65535', 'hard memlock': '65536', 'soft  memlock': '65536'} ${error\_list} = [] ${matches} = ['65535'] Length is 1 ${len} = 1 soft nproc value found,  and set to the expected value : 65535 ${matches} = ['65535'] Length is 1 ${len} = 1 hard nproc value found,  and set to the expected value : 65535 ${matches} = ['65535'] Length is 1 ${len} = 1 soft nofile value found,  and set to the expected value : 65535 ${matches} = ['65536'] Length is 1 ${len} = 1 hard memlock value found,  and set to the expected value : 65536 ${matches} = ['65536'] Length is 1 ${len} = 1 soft memlock value found,  and set to the expected value : 65536 Length is 0 |

Table-4 Verify that the limit changes are applied to the system

|  |  |
| --- | --- |
| name | Verify that the limit changes are applied to the system |
| doc | This test checks that the variables applied to the /etc/security/limits.d/ncs.conf  have been applied. This typically requires a user to disconnect and reconnect to the  servers |
| section | s1-s1 |
| status | PASS |
| messages | Running command 'ulimit -a  2>&1'. ${ulimit\_settings} = real-time  non-blocking time (microseconds, -R) unlimited  core file size (blocks, -c) 0  data seg size (kbytes, -d) unlimited  scheduling priority (-e) 0  file ... ${ulimit\_dict} = {'max locked memory':  '65536', 'open files': '65535', 'max user processes': '65535'} ${error\_list} = [] max locked memory:65536 ${matches} = ['65536'] Length is 1 ${len} = 1 max locked memory value  found, and set to the expected value : 65536 open files:65535 ${matches} = ['65535'] Length is 1 ${len} = 1 open files value found,  and set to the expected value : 65535 max user processes:65535 ${matches} = ['65535'] Length is 1 ${len} = 1 max user processes value  found, and set to the expected value : 65535 Length is 0 |

# Security

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-5 Security Test Results Summary

|  |  |  |
| --- | --- | --- |
| pass | fail | skip |
| 11 | 0 | 0 |

Table-6 Verify firewalld service is enabled

|  |  |
| --- | --- |
| name | Verify firewalld service is enabled |
| doc | The firewall service should not be disabled on reboot |
| section | s1-s2 |
| status | PASS |
| messages | Running command 'systemctl is-enabled  firewalld 2>&1'. ${output} = enabled |

Table-7 Verify NSO ports are configured in the firewalld

|  |  |
| --- | --- |
| name | Verify NSO ports are configured in the firewalld |
| doc | 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'] |
| section | s1-s2 |
| status | PASS |
| messages | Running command 'sudo firewall-cmd  --list-all 2>&1'. ${output} = public (active)  target: default  icmp-block-inversion: no  interfaces: ens33  sources:  services: cockpit dhcpv6-client ssh  ports: 22/tcp 4570/tcp 2022/tcp 2023/tcp 2024/tcp 8080/tcp 8888/tcp... 2022 2024 8080 8888 |

Table-8 Verify authselect profile sssd-vf is created

|  |  |
| --- | --- |
| name | Verify authselect profile sssd-vf is created |
| doc | Verify that a custom sssd profile has been created |
| section | s1-s2 |
| status | PASS |
| messages | 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-9 Verify expected authselect profile is active

|  |  |
| --- | --- |
| name | Verify expected authselect profile is active |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | Running command 'authselect current -r  2>&1'. ${output} = custom/sssd-vf  with-faillock without-nullok ${profile} = custom/sssd-vf Execution passed with message:  Current Profile is correct - sssd-vf |

Table-10 Verify that the required PAM Modules are enabled

|  |  |
| --- | --- |
| name | Verify that the required PAM Modules are enabled |
| doc | 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'] |
| section | s1-s2 |
| status | PASS |
| messages | Running command 'authselect current  2>&1'. ${output} = Profile ID: custom/sssd-vf  Enabled features:  - with-faillock  - without-nullok ${module\_status\_dict} = {} Profile ID: custom/sssd-vf  Enabled features:  - with-faillock  - without-nullok ${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-11 Check the password-auth file has been updated

|  |  |
| --- | --- |
| name | Check the password-auth file has been updated |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | ${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} try\_first\_pass'] Length is 1 ${len} = 1 Match Found match  auth.\*pam\_unix.so : ['{if not "without-nullok":nullok} try\_first\_pass'] {if not  "without-nullok":nullok} try\_first\_pass 'auth.\*pam\_unix.so'  Configured as expected password.\*pam\_pwquality.so :  try\_first\_pass local\_users\_only ${matches} = ['try\_first\_pass  local\_users\_only'] Length is 1 ${len} = 1 Match Found match  password.\*pam\_pwquality.so : ['try\_first\_pass local\_users\_only'] try\_first\_pass  local\_users\_only 'password.\*pam\_pwquality.so'  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} try\_first\_pass use\_authtok'] Length is 1 ${len} = 1 Match Found match  password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok}  try\_first\_pass use\_authtok'] {if not  "without-nullok":nullok} try\_first\_pass use\_authtok 'password.\*pam\_unix.so  sha512 shadow' Configured as expected [] Length is 0 |

Table-12 Check the system-auth file has been updated

|  |  |
| --- | --- |
| name | Check the system-auth file has been updated |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | ${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} try\_first\_pass'] Length is 1 ${len} = 1 Match Found match  auth.\*pam\_unix.so : ['{if not "without-nullok":nullok} try\_first\_pass'] {if not  "without-nullok":nullok} try\_first\_pass auth.\*pam\_unix.so  Configured as expected password.\*pam\_pwquality.so :  try\_first\_pass local\_users\_only enforce-for-root retry=3 remember=12 ${matches} = ['try\_first\_pass  local\_users\_only enforce-for-root retry=3 remember=12'] Length is 1 ${len} = 1 Match Found match  password.\*pam\_pwquality.so : ['try\_first\_pass local\_users\_only enforce-for-root  retry=3 remember=12'] try\_first\_pass  local\_users\_only enforce-for-root retry=3 remember=12 password.\*pam\_pwquality.so  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} try\_first\_pass use\_authtok remember=12'] Length is 1 ${len} = 1 Match Found match  password.\*pam\_unix.so sha512 shadow : ['{if not "without-nullok":nullok}  try\_first\_pass use\_authtok remember=12'] {if not  "without-nullok":nullok} try\_first\_pass use\_authtok remember=12 password.\*pam\_unix.so  sha512 shadow Configured as expected [] Length is 0 |

Table-13 Verify that faillock.conf has been modifed

|  |  |
| --- | --- |
| name | Verify that faillock.conf has been modifed |
| doc | We are required to modify the fail\_interval to be = 1800 seconds |
| section | s1-s2 |
| status | PASS |
| messages | ${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} = ['1800'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 1800 ${status} = PASS ${status\_message} = None Length is 0 |

Table-14 Verify that pwquality.conf has been modified

|  |  |
| --- | --- |
| name | Verify that pwquality.conf has been modified |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | ${dict} = {'minlen': '8', 'dcredit':  '-1', 'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-1'} ${file\_path} =  /etc/security/pwquality.conf {'minlen': '8', 'dcredit': '-1',  'ucredit': '-1', 'lcredit': '-1', 'ocredit': '-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} = ['8'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 8 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None ${match} = ['-1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = -1 ${status} = PASS ${status\_message} = None Length is 0 |

Table-15 Verify login.defs has been modifed

|  |  |
| --- | --- |
| name | Verify login.defs has been modifed |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | ${dict} = {'PASS\_MAX\_DAYS': '90',  'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '5'} ${file\_path} = /etc/login.defs {'PASS\_MAX\_DAYS': '90',  'PASS\_MIN\_DAYS': '1', 'PASS\_MIN\_LEN': '5', 'PASS\_WARN\_AGE': '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} = ['90'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 90 ${status} = PASS ${status\_message} = None ${match} = ['1'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 1 ${status} = PASS ${status\_message} = None ${match} = ['5'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 5 ${status} = PASS ${status\_message} = None ${match} = ['5'] Length is 1 ${number\_of\_results} = 1 ${match\_val} = 5 ${status} = PASS ${status\_message} = None Length is 0 |

Table-16 Verify the user account inavtive days value has been modified

|  |  |
| --- | --- |
| name | Verify the user account inavtive days value has been modified |
| doc | 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 |
| section | s1-s2 |
| status | PASS |
| messages | Getting file '<a  href="file:///etc/default/useradd">/etc/default/useradd</a>'. ${useradd\_conf} = # useradd defaults  file  GROUP=100  HOME=/home  INACTIVE=90  # INACTIVE=-1  EXPIRE=  SHELL=/bin/bash  SKEL=/etc/skel  CREATE\_MAIL\_SPOOL=yes    ${match} = ['90'] ${match\_val} = 90 |

# System

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-17 System Test Results Summary

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

Table-18 Verify dependency packages are installed

|  |  |
| --- | --- |
| name | Verify dependency packages are installed |
| doc | As above without break on first failure |
| section | s1-s3 |
| status | PASS |
| messages | ${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-11.0.20.0.8-3.el9.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\_2.1.x86\_64 ${status} = PASS ${status\_message} = None ${run\_cmd} = rpm -q openssl rpm -q openssl Running command 'rpm -q openssl  2>&1'. ${output} =  openssl-3.0.7-17.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-19 Verify required utilities are available

|  |  |
| --- | --- |
| name | Verify required utilities are available |
| doc | Cisco NSO requires some utilities, this test verfies these binaries exist |
| section | s1-s3 |
| status | PASS |
| messages | ${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-20 Verify Hostname is not set to localhost

|  |  |
| --- | --- |
| name | Verify Hostname is not set to localhost |
| doc | Hostname Should not be localhost |
| section | s1-s3 |
| status | PASS |
| messages | Running command 'hostnamectl hostname  2>&1'. ${output} = robot-dev-00 |

Table-21 Verify DNS servers are Configured

|  |  |
| --- | --- |
| name | Verify DNS servers are Configured |
| doc | DNS Servers should be Configured |
| section | s1-s3 |
| status | PASS |
| messages | Running command 'more /etc/resolv.conf  2>&1'. ${output} = # Generated by  NetworkManager  search localdomain  nameserver 192.168.1.1  nameserver 8.8.8.8 |

Table-22 Verify NTP servers are Configured

|  |  |
| --- | --- |
| name | Verify NTP servers are Configured |
| doc | NTP Servers should be Configured |
| section | s1-s3 |
| status | PASS |
| messages | Running command 'chronyc sources  2>&1'. ${output} = MS Name/IP address Stratum  Poll Reach LastRx Last sample  ===============================================================================  ^- ntp1.trans-ix.nl 2 10 ... |

Table-23 Verify NTP service is active

|  |  |
| --- | --- |
| name | Verify NTP service is active |
| doc | Check that the NTP service is active |
| section | s1-s3 |
| status | PASS |
| messages | Running command 'timedatectl show |  grep -Po '(?<=NTPSynchronized=)[^,]+' 2>&1'. ${output} = yes |

Some text

Some text