VMware Cloud Foundation – STIG Hardening Overview

NSX Manager/Edge

9.0.0.0

vmware by Broadcom

Table of contents

Revision History 3

Overview 4

Applicability 4

Disclaimer 4

NSX Compliance 5

- Ubuntu 22.04 Compliance: Overall 5
- Ubuntu 22.04 Compliance: Exceptions 5
- Ubuntu 22.04 Compliance: Not Applicable 13

Frequently Asked Questions 15

Appendix: Full Control List 16

Revision History

Date	Description of Change
June 2025	Initial Release

Overview

Broadcom is a trusted partner in highly secure, mission critical systems around the world, including the United States Department of Defense (DoD). In the DoD, all IT systems must adhere to the rigorous Risk Management Framework (RMF) as defined in DoDI 8510.01. A critical component of RMF is the mandatory implementation of Security Technical Implementation Guides (STIGs) and Security Requirements Guidelines (SRGs) as maintained by the Defense Information Systems Agency (DISA).

To support our customers, NSX Manager and Edge appliances are evaluated against the following standards:

- DISA Canonical Ubuntu 22.04 LTS Security Technical Implementation Guide, Version 2 Release 4

This report will document the product's compliance with this guidance, including any deviations.

Applicability

The contents of this document are applicable to the following product versions:

- VMware Cloud Foundation 9.0.0.0

Disclaimer

This document is intended to provide general guidance for organizations that are considering Broadcom solutions. The information contained in this document is for educational and informational purposes only. This document is not intended to provide advice and is provided "AS IS." Broadcom makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of requirements and effectiveness of implementations.

This document may contain statements which are intended to outline the general direction of certain of Broadcom's offerings. It is intended for information purposes only and may not be incorporated into any contract. Any information regarding the pre-release of Broadcom offerings, future updates or other planned modifications is subject to ongoing evaluation by Broadcom and is subject to change. All software releases are on an if and when available basis and are subject to change. This information is provided without warranty of any kind, express or implied, and is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions regarding Broadcom offerings. Any purchasing decisions should only be based on features currently available. The development, release, and timing of any features or functionality described for Broadcom's offerings in this presentation remain at the sole discretion of Broadcom.

NSX Compliance

VMware NSX is a powerful network virtualization solution for VMware Cloud Foundation that enables network connectivity, operations, and scale. NSX takes a software-defined approach to networking that extends across data centers, clouds, and application frameworks. With NSX, network services are brought closer to the application wherever it's running, from virtual machines to containers to physical servers. NSX delivers cloud operational efficiency for the network independent of the underlying hardware. NSX reproduces the entire network model in software, enabling any network topology from simple to complex multitier networks to be created and provisioned in seconds.

To deliver these capabilities, the NSX Manager and Edge virtual appliances are deployed with VCF.

- NSX Edge nodes - VMs that provide network services to all the NSX components. Also known as edge transport nodes.
- NSX Managers - VMs that provide a browser-based GUI for administering the NSX environment.

Ubuntu 22.04 Compliance: Overall

The NSX Manager and Edge appliances are built on the Ubuntu 22.04 OS. The results below are based on auditing the NSX appliances against the latest Canonical 22.04 LTS STIG release.

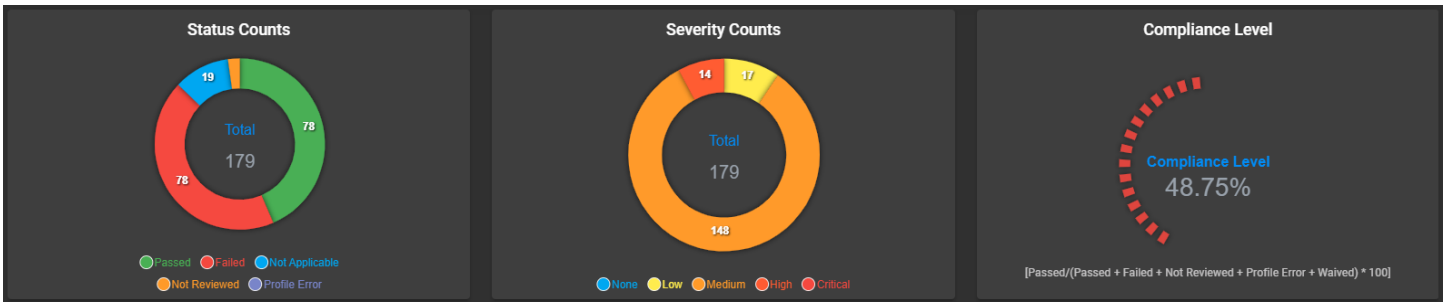

Figure 1: *Overall Compliance for the NSX Manager appliances*

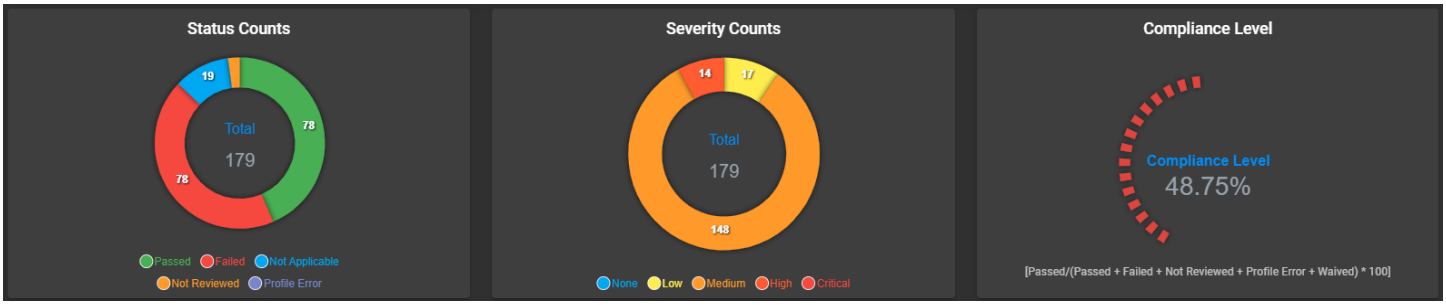

Figure 2: *Overall Compliance for the NSX Edge appliances*

A full list of controls and their statuses is available in the Appendix sections of this document.

Unless otherwise stated the controls listed below and their status are applicable to both NSX Manager and Edge appliances.

Ubuntu 22.04 Compliance: Exceptions

Controls listed in the exceptions table are findings. If post deployment remediation is possible it will be detailed in the justification column.

Control ID	NIST 800-83	Title	Justification
UBTU-22-211015	CM-6 b	Ubuntu 22.04 LTS must disable the x86 Ctrl-Alt-Delete key sequence.	Resolution included in product roadmap.
UBTU-22-214010	CM-14 CM-5 (3)	Ubuntu 22.04 LTS must be configured so that the Advance Package Tool (APT) prevents the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.	Resolution included in product roadmap.
UBTU-22-214015	SI-2 (6)	Ubuntu 22.04 LTS must be configured so that the Advance Package Tool (APT) removes all software components after updated versions have been installed.	Resolution included in product roadmap.
UBTU-22-215010	CM-6 b	Ubuntu 22.04 LTS must have the "libpam-pwquality" package installed.	Resolution included in product roadmap. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-215025	CM-6 b	Ubuntu 22.04 LTS must not have the "ntp" package installed.	The ntp package is used for time synchronization instead of chrony.
UBTU-22-231010	SC-28 SC-28 (1)	Ubuntu 22.04 LTS must implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all information that requires protection at rest.	Data at rest encryption is not implemented locally, however, the NSX virtual machines can reside on storage that provide data at rest encryption such as vSAN.
UBTU-22-232020	CM-5 (6)	Ubuntu 22.04 LTS library files must have mode "755" or less permissive.	Resolution included in product roadmap.
UBTU-22-232025	SI-11 b	Ubuntu 22.04 LTS must configure the "/var/log" directory to have mode "755" or less permissive.	Resolution included in product roadmap.
UBTU-22-232026	SI-11 a	Ubuntu 22.04 LTS must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	Resolution included in product roadmap.
UBTU-22-232027	SI-11 a	Ubuntu 22.04 LTS must generate system journal entries without revealing information that could be exploited by adversaries.	Resolution included in product roadmap.
UBTU-22-232050	CM-5 (6)	Ubuntu 22.04 LTS must have system commands owned by "root" or a system account.	Resolution included in product roadmap.
UBTU-22-232055	CM-5 (6)	Ubuntu 22.04 LTS must have system commands group-owned by "root" or a system account.	Resolution included in product roadmap.
UBTU-22-232060	CM-5 (6)	Ubuntu 22.04 LTS library directories must be owned by "root".	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-232065	CM-5 (6)	Ubuntu 22.04 LTS library directories must be group-owned by "root".	Resolution included in product roadmap.
UBTU-22-232070	CM-5 (6)	Ubuntu 22.04 LTS library files must be owned by "root".	Resolution included in product roadmap.
UBTU-22-232075	CM-5 (6)	Ubuntu 22.04 LTS library files must be group-owned by "root".	Resolution included in product roadmap.
UBTU-22-232140	SI-11 a	Ubuntu 22.04 LTS must be configured so that the "journalctl" command is not accessible by unauthorized users.	Resolution included in product roadmap.
UBTU-22-232145	SC-4	Ubuntu 22.04 LTS must set a sticky bit on all public directories to prevent unauthorized and unintended information transferred via shared system resources.	Resolution included in product roadmap.
UBTU-22-251010	AC-17 (1)	Ubuntu 22.04 LTS must have an application firewall installed in order to control remote access methods.	Iptables is used for firewalling instead of UFW.
UBTU-22-251025	SC-5 a	Ubuntu 22.04 LTS must configure the Uncomplicated Firewall (ufw) to rate-limit impacted network interfaces.	Iptables is used for firewalling instead of UFW.
UBTU-22-251030	CM-7 b	Ubuntu 22.04 LTS must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.	By default, all traffic in and out is dropped by policy unless explicitly allowed. Details on specific ports and protocols used in NSX can be found at: https://ports.broadcom.com/
UBTU-22-252015	SC-45 (1) (b) AU-8 (1) (b)	Ubuntu 22.04 LTS must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.	The ntp package is used for time synchronization instead of chrony.
UBTU-22-255015	SC-8, SC-8 (2)	Ubuntu 22.04 LTS must use SSH to protect the confidentiality and integrity of transmitted information.	By default, the SSH service is not running and disabled. It is recommended to maintain this configuration unless needed for troubleshooting.
UBTU-22-255020	AC-8 a, AC-8 c 1, AC-8 c 2, AC-8 c 3	Ubuntu 22.04 LTS must display the Standard Mandatory DOD Notice and Consent Banner before granting any local or remote connection to the system.	The DOD login banner is not configured out of the box as it is not appropriate for all customers.
UBTU-22-255030	MA-4 e, SC-10	Ubuntu 22.04 LTS must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-255050	AC-17 (2), SC-8 (1), MA-4 (6)	Ubuntu 22.04 LTS must configure the SSH daemon to use FIPS 140-3 approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Resolution included in product roadmap.
UBTU-22-255055	AC-17 (2), SC-8 (1), MA-4 (6)	Ubuntu 22.04 LTS must configure the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-3-approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Resolution included in product roadmap.
UBTU-22-255060	AC-17 (2)	Ubuntu 22.04 LTS SSH server must be configured to use only FIPS-validated key exchange algorithms.	Resolution included in product roadmap.
UBTU-22-291010	IA-3, CM-7 (9) (b)	Ubuntu 22.04 LTS must disable automatic mounting of Universal Serial Bus (USB) mass storage driver.	Resolution included in product roadmap.
UBTU-22-411010	IA-2 (5)	Ubuntu 22.04 LTS must prevent direct login into the root account.	Resolution included in product roadmap.
UBTU-22-411025	IA-5 (1) (d), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce 24 hours/one day as the minimum password lifetime. Passwords for new users must have a 24 hours/one day minimum password lifetime restriction.	Resolution included in product roadmap.
UBTU-22-411030	IA-5 (1) (d), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce a 60-day maximum password lifetime restriction. Passwords for new users must have a 60-day maximum password lifetime restriction.	Resolution included in product roadmap.
UBTU-22-411035	IA-4 e, AC-2 (3) (a), AC-2 (3) (b)	Ubuntu 22.04 LTS must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.	Resolution included in product roadmap.
UBTU-22-411045	AC-7 a, AC-7 b	Ubuntu 22.04 LTS must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts have been made.	Resolution included in product roadmap. This is currently configured to 5.
UBTU-22-412010	CM-6 b	Ubuntu 22.04 LTS must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.	Resolution included in product roadmap.
UBTU-22-412020	AC-10	Ubuntu 22.04 LTS must limit the number of concurrent sessions to ten for all accounts and/or account types.	Resolution included in product roadmap.
UBTU-22-412025	AC-11 a, AC-11 (1)	Ubuntu 22.04 LTS must allow users to directly initiate a session lock for all connection types.	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-412030	AC-12	Ubuntu 22.04 LTS must automatically exit interactive command shell user sessions after 15 minutes of inactivity.	Resolution included in product roadmap.
UBTU-22-412035	CM-6 b	Ubuntu 22.04 LTS default filesystem permissions must be defined in such a way that all authenticated users can read and modify only their own files.	Resolution included in product roadmap.
UBTU-22-432010	SC-11 b, IA-11	Ubuntu 22.04 LTS must require users to reauthenticate for privilege escalation or when changing roles.	Resolution included in product roadmap.
UBTU-22-611010	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring at least one uppercase character be used.	Resolution included in product roadmap. This requirement is currently implemented with the pam_cracklib module. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-611015	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring at least one lowercase character be used.	Resolution included in product roadmap. This requirement is currently implemented with the pam_cracklib module. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-611020	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring that at least one numeric character be used.	Resolution included in product roadmap. This requirement is currently implemented with the pam_cracklib module. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-611025	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring that at least one special character be used.	Resolution included in product roadmap. This requirement is currently implemented with the pam_cracklib module. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-611030	CM-6 b	Ubuntu 22.04 LTS must prevent the use of dictionary words for passwords.	Resolution included in product roadmap.
UBTU-22-611035	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce a minimum 15-character password length.	Resolution included in product roadmap. This is configurable post deployment but must be done via the supported methods and not directly to the underlying OS configuration. A rule exists for this configuration in the NSX Manager STIG.

Control ID	NIST 800-83	Title	Justification
UBTU-22-611040	IA-5 (1) (b), IA-5 (1) (h)	Ubuntu 22.04 LTS must require the change of at least eight characters when passwords are changed.	Resolution included in product roadmap. This is configurable post deployment but must be done via the supported methods and not directly to the underlying OS configuration. A rule exists for this configuration in the NSX Manager STIG.
UBTU-22-611045	CM-6 b	Ubuntu 22.04 LTS must be configured so that when passwords are changed or new passwords are established, pwquality must be used.	Resolution included in product roadmap. The pam_cracklib module is currently used instead of pam_pwquality.
UBTU-22-631010	SC-23 (5)	Ubuntu 22.04 LTS must use DOD PKI-established certificate authorities for verification of the establishment of protected sessions.	Resolution included in product roadmap.
UBTU-22-651010	SI-6 a	Ubuntu 22.04 LTS must use a file integrity tool to verify correct operation of all security functions.	Resolution included in product roadmap.
UBTU-22-651015	SI-6 a	Ubuntu 22.04 LTS must configure AIDE to perform file integrity checking on the file system.	Resolution included in product roadmap.
UBTU-22-651020	CM-3 (5), SI-6 d	Ubuntu 22.04 LTS must notify designated personnel if baseline configurations are changed in an unauthorized manner. The file integrity tool must notify the system administrator when changes to the baseline configuration or anomalies in the operation of any security functions are discovered.	Resolution included in product roadmap.
UBTU-22-651025	SI-6 b	Ubuntu 22.04 LTS must be configured so that the script that runs each 30 days or less to check file integrity is the default.	Resolution included in product roadmap.
UBTU-22-651030	AU-9 (3)	Ubuntu 22.04 LTS must use cryptographic mechanisms to protect the integrity of audit tools.	Resolution included in product roadmap.
UBTU-22-651035	AU-4 (1)	Ubuntu 22.04 LTS must have a crontab script running weekly to offload audit events of standalone systems.	Audit logs are offloaded by configuring log forwarding for NSX. A rule exists for this configuration in the NSX Manager STIG.
UBTU-22-653020	AU-4 (1)	Ubuntu 22.04 LTS audit event multiplexor must be configured to offload audit logs onto a different system from the system being audited.	Audit logs are offloaded by configuring log forwarding for NSX. A rule exists for this configuration in the NSX Manager STIG.
UBTU-22-653030	AU-5 b	Ubuntu 22.04 LTS must shut down by default upon audit failure.	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-653040	AU-5 (1)	Ubuntu 22.04 LTS must immediately notify the system administrator (SA) and information system security officer (ISSO) when the audit record storage volume reaches 25 percent remaining of the allocated capacity.	Resolution included in product roadmap.
UBTU-22-653045	AU-9 a	Ubuntu 22.04 LTS must be configured so that audit log files are not read- or write-accessible by unauthorized users.	Resolution included in product roadmap.
UBTU-22-653055	AU-9 a	Ubuntu 22.04 LTS must permit only authorized groups ownership of the audit log files.	Resolution included in product roadmap.
UBTU-22-653065	AU-12 b	Ubuntu 22.04 LTS must be configured so that audit configuration files are not write-accessible by unauthorized users.	Resolution included in product roadmap.
UBTU-22-654010	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the apparmor_parser command.	Resolution included in product roadmap.
UBTU-22-654015	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chacl command.	Resolution included in product roadmap.
UBTU-22-654025	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chcon command.	Resolution included in product roadmap.
UBTU-22-654045	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful attempts to use the fdisk command.	Resolution included in product roadmap.
UBTU-22-654055	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful attempts to use the kmod command.	Resolution included in product roadmap.
UBTU-22-654065	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the mount command.	Resolution included in product roadmap.
UBTU-22-654075	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the pam_timestamp_check command.	Resolution included in product roadmap.
UBTU-22-654085	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the setfacl command.	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-654095	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the ssh-keysign command.	Resolution included in product roadmap.
UBTU-22-654110	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the sudoedit command.	Resolution included in product roadmap.
UBTU-22-654115	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the umount command.	Resolution included in product roadmap.
UBTU-22-654120	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the unix_update command.	Resolution included in product roadmap.
UBTU-22-654125	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the usermod command.	Resolution included in product roadmap.
UBTU-22-654165	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the creat, open, openat, open_by_handle_at, truncate, and ftruncate system calls.	Resolution included in product roadmap.
UBTU-22-654170	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the delete_module system call.	Resolution included in product roadmap.
UBTU-22-654175	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the init_module and finit_module system calls.	Resolution included in product roadmap.
UBTU-22-654185	AU-12 c	Ubuntu 22.04 LTS must generate audit records for any successful/unsuccessful use of unlink, unlinkat, rename, renameat, and rmdir system calls.	Resolution included in product roadmap.
UBTU-22-654190	CM-6 b	Ubuntu 22.04 LTS must generate audit records for all events that affect the systemd journal files.	Resolution included in product roadmap.
UBTU-22-654225	AU-12 c	Ubuntu 22.04 LTS must generate audit records when successful/unsuccessful attempts to modify the /etc/sudoers.d directory occur.	Resolution included in product roadmap.
UBTU-22-654230	AC-6 (8), AC-6 (9)	Ubuntu 22.04 LTS must prevent all software from executing at higher privilege levels than users executing the software and the audit system must be configured to audit the execution of privileged functions.	Resolution included in product roadmap.

Control ID	NIST 800-83	Title	Justification
UBTU-22-671010	SC-13 b	Ubuntu 22.04 LTS must implement NIST FIPS-validated cryptography to protect classified information and for the following: To provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	The Ubuntu 22.04 kernel FIPS module is not available without an active subscription.

Ubuntu 22.04 Compliance: Not Applicable

Controls listed in the not applicable table were determined to be not applicable in the NSX context.

Control ID	NIST 800-83	Title	Justification
UBTU-22-215015	CM-6 b	Ubuntu 22.04 LTS must have the "chrony" package installed.	The ntp package is used for time synchronization instead of chrony.
UBTU-22-215020	CM-6 b	Ubuntu 22.04 LTS must not have the "systemd-timesyncd" package installed.	The ntp package is used for time synchronization instead of chrony.
UBTU-22-251015	AC-17 (1)	Ubuntu 22.04 LTS must enable and run the Uncomplicated Firewall (ufw).	Iptables is used for firewalling instead of UFW.
UBTU-22-251020	CM-6 b	Ubuntu 22.04 LTS must have an application firewall enabled.	Iptables is used for firewalling instead of UFW.
UBTU-22-252010	SC-45 (1) (a), AU-8 (1) (a)	Ubuntu 22.04 LTS must, for networked systems, compare internal information system clocks at least every 24 hours with a server synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).	The ntp package is used for time synchronization instead of chrony and can be configured to support this requirement.
UBTU-22-271010	AC-8 a	Ubuntu 22.04 LTS must enable the graphical user logon banner to display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.	A GUI is not installed or supported on NSX manager or edge appliances.
UBTU-22-271015	AC-8 a	Ubuntu 22.04 LTS must display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.	A GUI is not installed or supported on NSX manager or edge appliances.

Control ID	NIST 800-83	Title	Justification
UBTU-22-271020	AC-11 b	Ubuntu 22.04 LTS must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.	A GUI is not installed or supported on NSX manager or edge appliances.
UBTU-22-271025	AC-11 a	Ubuntu 22.04 LTS must initiate a graphical session lock after 15 minutes of inactivity.	A GUI is not installed or supported on NSX manager or edge appliances.
UBTU-22-271030	CM-6 b	Ubuntu 22.04 LTS must disable the x86 Ctrl-Alt-Delete key sequence if a graphical user interface is installed.	A GUI is not installed or supported on NSX manager or edge appliances.
UBTU-22-291015	SC-8	Ubuntu 22.04 LTS must disable all wireless network adapters.	Wireless adapters do not exist by default on NSX manager or edge appliances.
UBTU-22-612010	IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (11), IA-2 (6) (a), IA-2 (6) (b)	Ubuntu 22.04 LTS must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612015	IA-2 (12)	Ubuntu 22.04 LTS must accept personal identity verification (PIV) credentials.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612020	IA-2 (1), IA-2 (2), IA-2 (6) (b), IA-2 (3), IA-2 (4)	Ubuntu 22.04 LTS must implement smart card logins for multifactor authentication for local and network access to privileged and nonprivileged accounts.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612025	IA-2 (12)	Ubuntu 22.04 LTS must electronically verify personal identity verification (PIV) credentials.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612030	IA-5 (2) (b) (1), SC-17 b	Ubuntu 22.04 LTS, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612035	IA-5 (2) (d), IA-5 (2) (b) (2)	Ubuntu 22.04 LTS for PKI-based authentication, must implement a local cache of revocation data in case of the inability to access revocation information via the network.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-612040	IA-5 (2) (a) (2)	Ubuntu 22.04 LTS must map the authenticated identity to the user or group account for PKI-based authentication.	Configuring MFA to the local OS on VMware appliances is currently unsupported. MFA to product interface is supported via an identity provider.
UBTU-22-631015	IA-5 (13)	Ubuntu 22.04 LTS must be configured such that Pluggable Authentication Module (PAM) prohibits the use of cached authentications after one day.	Smartcards are not supported for local logins.

Frequently Asked Questions

Can customers make changes to the NSX Manager and Edge appliances?

No it is not supported to remediate the findings listed in this document at this time.

Where can I find the Canonical Ubuntu 22.04 LTS STIG?

The Canonical Ubuntu 22.04 LTS STIG may be found at:

https://public.cyber.mil/stigs/

What is a STIG Readiness Guide?

More information about STIG Readiness Guides can be found at:

https://www.vmware.com/docs/vmw-stig-program-overview

What does the "status" column in the control list tables mean?

Status Definitions	
Passed	The compliance check passed.
Failed	The compliance check failed.
Not Applicable	The control was determined to be N/A in this context.
Not Reviewed	These controls were skipped as the conditions of the test did not exist on the system or require manual review and count as failures unless otherwise attested to manually.

Appendix: Full Control List

Control ID	NIST 800-83	Title	Status
UBTU-22-211015	CM-6 b	Ubuntu 22.04 LTS must disable the x86 Ctrl-Alt-Delete key sequence.	Failed
UBTU-22-212010	AC-3	Ubuntu 22.04 LTS, when booted, must require authentication upon booting into single-user and maintenance modes.	Passed
UBTU-22-212015	AU-14 (1)	Ubuntu 22.04 LTS must initiate session audits at system startup.	Passed
UBTU-22-213010	SC-4	Ubuntu 22.04 LTS must restrict access to the kernel message buffer.	Passed
UBTU-22-213015	SC-24	Ubuntu 22.04 LTS must disable kernel core dumps so that it can fail to a secure state if system initialization fails, shutdown fails or aborts fail.	Passed
UBTU-22-213020	SI-16	Ubuntu 22.04 LTS must implement address space layout randomization to protect its memory from unauthorized code execution.	Passed
UBTU-22-213025	SI-16	Ubuntu 22.04 LTS must implement nonexecutable data to protect its memory from unauthorized code execution.	Passed
UBTU-22-214010	CM-14, CM-5 (3)	Ubuntu 22.04 LTS must be configured so that the Advance Package Tool (APT) prevents the installation of patches, service packs, device drivers, or operating system components without verification they have been digitally signed using a certificate that is recognized and approved by the organization.	Failed
UBTU-22-214015	SI-2 (6)	Ubuntu 22.04 LTS must be configured so that the Advance Package Tool (APT) removes all software components after updated versions have been installed.	Failed
UBTU-22-215010	CM-6 b	Ubuntu 22.04 LTS must have the "libpam-pwquality" package installed.	Failed
UBTU-22-215015	CM-6 b	Ubuntu 22.04 LTS must have the "chrony" package installed.	Not Applicable
UBTU-22-215020	CM-6 b	Ubuntu 22.04 LTS must not have the "systemd-timesyncd" package installed.	Not Applicable
UBTU-22-215025	CM-6 b	Ubuntu 22.04 LTS must not have the "ntp" package installed.	Failed
UBTU-22-215030	CM-7 a	Ubuntu 22.04 LTS must not have the "rsh-server" package installed.	Passed
UBTU-22-215035	IA-5 (1) (c)	Ubuntu 22.04 LTS must not have the "telnet" package installed.	Passed
UBTU-22-231010	SC-28, SC-28 (1), SC-28 (1)	Ubuntu 22.04 LTS must implement cryptographic mechanisms to prevent unauthorized disclosure and modification of all information that requires protection at rest.	Not Reviewed
UBTU-22-232010	AU-9	Ubuntu 22.04 LTS must have directories that contain system commands set to a mode of "755" or less permissive.	Passed
UBTU-22-232015	CM-5 (6)	Ubuntu 22.04 LTS must have system commands set to a mode of "755" or less permissive.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-232020	CM-5 (6)	Ubuntu 22.04 LTS library files must have mode "755" or less permissive.	Failed
UBTU-22-232025	SI-11 b	Ubuntu 22.04 LTS must configure the "/var/log" directory to have mode "755" or less permissive.	Failed
UBTU-22-232026	SI-11 a	Ubuntu 22.04 LTS must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	Failed
UBTU-22-232027	SI-11 a	Ubuntu 22.04 LTS must generate system journal entries without revealing information that could be exploited by adversaries.	Failed
UBTU-22-232030	SI-11 b	Ubuntu 22.04 LTS must configure "/var/log/syslog" file with mode "640" or less permissive.	Passed
UBTU-22-232035	AU-9 a, AU-9	Ubuntu 22.04 LTS must configure audit tools with a mode of "755" or less permissive.	Passed
UBTU-22-232040	AU-9	Ubuntu 22.04 LTS must have directories that contain system commands owned by "root".	Passed
UBTU-22-232045	AU-9	Ubuntu 22.04 LTS must have directories that contain system commands group-owned by "root".	Passed
UBTU-22-232050	CM-5 (6)	Ubuntu 22.04 LTS must have system commands owned by "root" or a system account.	Failed
UBTU-22-232055	CM-5 (6)	Ubuntu 22.04 LTS must have system commands group-owned by "root" or a system account.	Failed
UBTU-22-232060	CM-5 (6)	Ubuntu 22.04 LTS library directories must be owned by "root".	Failed
UBTU-22-232065	CM-5 (6)	Ubuntu 22.04 LTS library directories must be group-owned by "root".	Failed
UBTU-22-232070	CM-5 (6)	Ubuntu 22.04 LTS library files must be owned by "root".	Failed
UBTU-22-232075	CM-5 (6)	Ubuntu 22.04 LTS library files must be group-owned by "root".	Failed
UBTU-22-232080	SI-11 b	Ubuntu 22.04 LTS must configure the directories used by the system journal to be owned by "root".	Passed
UBTU-22-232085	SI-11 b	Ubuntu 22.04 LTS must configure the directories used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-22-232090	SI-11 b	Ubuntu 22.04 LTS must configure the files used by the system journal to be owned by "root".	Passed
UBTU-22-232095	SI-11 b	Ubuntu 22.04 LTS must configure the files used by the system journal to be group-owned by "systemd-journal".	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-232100	SI-11 b	Ubuntu 22.04 LTS must be configured so that the "journalctl" command is owned by "root".	Passed
UBTU-22-232105	SI-11 b	Ubuntu 22.04 LTS must be configured so that the "journalctl" command is group-owned by "root".	Passed
UBTU-22-232110	AU-9 a, AU-9	Ubuntu 22.04 LTS must configure audit tools to be owned by "root".	Passed
UBTU-22-232120	SI-11 b	Ubuntu 22.04 LTS must configure the "/var/log" directory to be owned by "root".	Passed
UBTU-22-232125	SI-11 b	Ubuntu 22.04 LTS must configure the "/var/log" directory to be group-owned by "syslog".	Passed
UBTU-22-232130	SI-11 b	Ubuntu 22.04 LTS must configure "/var/log/syslog" file to be owned by "syslog".	Passed
UBTU-22-232135	SI-11 b	Ubuntu 22.04 LTS must configure the "/var/log/syslog" file to be group-owned by "adm".	Passed
UBTU-22-232140	SI-11 a	Ubuntu 22.04 LTS must be configured so that the "journalctl" command is not accessible by unauthorized users.	Failed
UBTU-22-232145	SC-4	Ubuntu 22.04 LTS must set a sticky bit on all public directories to prevent unauthorized and unintended information transferred via shared system resources.	Failed
UBTU-22-251010	AC-17 (1)	Ubuntu 22.04 LTS must have an application firewall installed in order to control remote access methods.	Failed
UBTU-22-251015	AC-17 (1)	Ubuntu 22.04 LTS must enable and run the Uncomplicated Firewall (ufw).	Not Applicable
UBTU-22-251020	CM-6 b	Ubuntu 22.04 LTS must have an application firewall enabled.	Not Applicable
UBTU-22-251025	SC-5 a	Ubuntu 22.04 LTS must configure the Uncomplicated Firewall (ufw) to rate-limit impacted network interfaces.	Not Reviewed
UBTU-22-251030	CM-7 b	Ubuntu 22.04 LTS must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the PPSM CAL and vulnerability assessments.	Not Reviewed
UBTU-22-252010	SC-45 (1) (a), AU-8 (1) (a)	Ubuntu 22.04 LTS must, for networked systems, compare internal information system clocks at least every 24 hours with a server synchronized to one of the redundant United States Naval Observatory (USNO) time servers, or a time server designated for the appropriate DOD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).	Not Applicable
UBTU-22-252015	SC-45 (1) (b), AU-8 (1) (b)	Ubuntu 22.04 LTS must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.	Failed
UBTU-22-252020	AU-8 b	Ubuntu 22.04 LTS must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC).	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-253010	SC-5 (2)	Ubuntu 22.04 LTS must be configured to use TCP syncookies.	Passed
UBTU-22-255010	SC-8, SC-8 (2), SC-8 (2)	Ubuntu 22.04 LTS must have SSH installed.	Passed
UBTU-22-255015	SC-8, SC-8 (2), SC-8 (2)	Ubuntu 22.04 LTS must use SSH to protect the confidentiality and integrity of transmitted information.	Failed
UBTU-22-255020	AC-8 a, AC-8 c 1, AC-8 c 2, AC-8 c 2, AC-8 c 2, AC-8 c 3	Ubuntu 22.04 LTS must display the Standard Mandatory DOD Notice and Consent Banner before granting any local or remote connection to the system.	Failed
UBTU-22-255025	CM-6 b	Ubuntu 22.04 LTS must not allow unattended or automatic login via SSH.	Passed
UBTU-22-255030	MA-4 e, SC-10	Ubuntu 22.04 LTS must be configured so that all network connections associated with SSH traffic terminate after becoming unresponsive.	Failed
UBTU-22-255035	SC-10	Ubuntu 22.04 LTS must be configured so that all network connections associated with SSH traffic are terminated after 10 minutes of becoming unresponsive.	Passed
UBTU-22-255040	CM-6 b	Ubuntu 22.04 LTS must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.	Passed
UBTU-22-255045	CM-6 b	Ubuntu 22.04 LTS SSH daemon must prevent remote hosts from connecting to the proxy display.	Passed
UBTU-22-255050	AC-17 (2), SC-8 (1), MA-4 (6)	Ubuntu 22.04 LTS must configure the SSH daemon to use FIPSÂ 140-3-approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Failed
UBTU-22-255055	AC-17 (2), SC-8 (1), MA-4 (6)	Ubuntu 22.04 LTS must configure the SSH daemon to use Message Authentication Codes (MACs) employing FIPS 140-3-approved cryptographic hashes to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Failed
UBTU-22-255060	AC-17 (2)	Ubuntu 22.04 LTS SSH server must be configured to use only FIPS-validated key exchange algorithms.	Failed
UBTU-22-255065	MA-4 c	Ubuntu 22.04 LTS must use strong authenticators in establishing nonlocal maintenance and diagnostic sessions.	Passed
UBTU-22-271010	AC-8 a	Ubuntu 22.04 LTS must enable the graphical user logon banner to display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.	Not Applicable
UBTU-22-271015	AC-8 a	Ubuntu 22.04 LTS must display the Standard Mandatory DOD Notice and Consent Banner before granting local access to the system via a graphical user logon.	Not Applicable
UBTU-22-271020	AC-11 b	Ubuntu 22.04 LTS must retain a user's session lock until that user reestablishes access using established identification and authentication procedures.	Not Applicable

Control ID	NIST 800-83	Title	Status
UBTU-22-271025	AC-11 a	Ubuntu 22.04 LTS must initiate a graphical session lock after 15 minutes of inactivity.	Not Applicable
UBTU-22-271030	CM-6 b	Ubuntu 22.04 LTS must disable the x86 Ctrl-Alt-Delete key sequence if a graphical user interface is installed.	Not Applicable
UBTU-22-291010	IA-3, CM-7 (9) (b)	Ubuntu 22.04 LTS must disable automatic mounting of Universal Serial Bus (USB) mass storage driver.	Failed
UBTU-22-291015	SC-8	Ubuntu 22.04 LTS must disable all wireless network adapters.	Not Applicable
UBTU-22-411010	IA-2 (5)	Ubuntu 22.04 LTS must prevent direct login into the root account.	Failed
UBTU-22-411015	IA-2, IA-8	Ubuntu 22.04 LTS must uniquely identify interactive users.	Passed
UBTU-22-411025	IA-5 (1) (d), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce 24 hours/one day as the minimum password lifetime. Passwords for new users must have a 24 hours/one day minimum password lifetime restriction.	Failed
UBTU-22-411030	IA-5 (1) (d), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce a 60-day maximum password lifetime restriction. Passwords for new users must have a 60-day maximum password lifetime restriction.	Failed
UBTU-22-411035	IA-4 e, AC-2 (3) (a), AC-2 (3) (b)	Ubuntu 22.04 LTS must disable account identifiers (individuals, groups, roles, and devices) after 35 days of inactivity.	Failed
UBTU-22-411040	AC-2 (2), AC-2 (2)	Ubuntu 22.04 LTS must automatically expire temporary accounts within 72 hours.	Passed
UBTU-22-411045	AC-7 a, AC-7 b	Ubuntu 22.04 LTS must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts have been made.	Failed
UBTU-22-412010	CM-6 b	Ubuntu 22.04 LTS must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.	Failed
UBTU-22-412020	AC-10	Ubuntu 22.04 LTS must limit the number of concurrent sessions to ten for all accounts and/or account types.	Failed
UBTU-22-412025	AC-11 a, AC-11 (1)	Ubuntu 22.04 LTS must allow users to directly initiate a session lock for all connection types.	Failed
UBTU-22-412030	AC-12	Ubuntu 22.04 LTS must automatically exit interactive command shell user sessions after 15 minutes of inactivity.	Failed
UBTU-22-412035	CM-6 b	Ubuntu 22.04 LTS default filesystem permissions must be defined in such a way that all authenticated users can read and modify only their own files.	Failed

Control ID	NIST 800-83	Title	Status
UBTU-22-431010	CM-7 (2), CM-7 (5) (b), AC-3 (4)	Ubuntu 22.04 LTS must have the "apparmor" package installed.	Passed
UBTU-22-431015	CM-7 (2), CM-7 (5) (b), AC-6 (10)	Ubuntu 22.04 LTS must be configured to use AppArmor.	Passed
UBTU-22-432010	SC-11 b, IA-11	Ubuntu 22.04 LTS must require users to reauthenticate for privilege escalation or when changing roles.	Failed
UBTU-22-432015	SC-3	Ubuntu 22.04 LTS must ensure only users who need access to security functions are part of sudo group.	Passed
UBTU-22-611010	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring at least one uppercase character be used.	Failed
UBTU-22-611015	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring at least one lowercase character be used.	Failed
UBTU-22-611020	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring that at least one numeric character be used.	Failed
UBTU-22-611025	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce password complexity by requiring that at least one special character be used.	Failed
UBTU-22-611030	CM-6 b	Ubuntu 22.04 LTS must prevent the use of dictionary words for passwords.	Failed
UBTU-22-611035	IA-5 (1) (a), IA-5 (1) (h)	Ubuntu 22.04 LTS must enforce a minimum 15-character password length.	Failed
UBTU-22-611040	IA-5 (1) (b), IA-5 (1) (h)	Ubuntu 22.04 LTS must require the change of at least eight characters when passwords are changed.	Failed
UBTU-22-611045	CM-6 b	Ubuntu 22.04 LTS must be configured so that when passwords are changed or new passwords are established, pwquality must be used.	Failed
UBTU-22-611055	IA-5 (1) (d), IA-5 (1) (c)	Ubuntu 22.04 LTS must store only encrypted representations of passwords.	Passed
UBTU-22-611060	CM-6 b	Ubuntu 22.04 LTS must not allow accounts configured with blank or null passwords.	Passed
UBTU-22-611065	CM-6 b	Ubuntu 22.04 LTS must not have accounts configured with blank or null passwords.	Passed
UBTU-22-611070	IA-7	Ubuntu 22.04 LTS must encrypt all stored passwords with a FIPS 140-3-approved cryptographic hashing algorithm.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-612010	IA-2 (1), IA-2 (2), IA-2 (3), IA-2 (4), IA-2 (11), IA-2 (6) (a), IA-2 (6) (b)	Ubuntu 22.04 LTS must implement multifactor authentication for remote access to privileged accounts in such a way that one of the factors is provided by a device separate from the system gaining access.	Not Applicable
UBTU-22-612015	IA-2 (12)	Ubuntu 22.04 LTS must accept personal identity verification (PIV) credentials.	Not Applicable
UBTU-22-612020	IA-2 (1), IA-2 (2), IA-2 (6) (b), IA-2 (3), IA-2 (4)	Ubuntu 22.04 LTS must implement smart card logins for multifactor authentication for local and network access to privileged and nonprivileged accounts.	Not Applicable
UBTU-22-612025	IA-2 (12)	Ubuntu 22.04 LTS must electronically verify personal identity verification (PIV) credentials.	Not Applicable
UBTU-22-612030	IA-5 (2) (b) (1), SC-17 b	Ubuntu 22.04 LTS, for PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	Not Applicable
UBTU-22-612035	IA-5 (2) (d), IA-5 (2) (b) (2)	Ubuntu 22.04 LTS for PKI-based authentication, must implement a local cache of revocation data in case of the inability to access revocation information via the network.	Not Applicable
UBTU-22-612040	IA-5 (2) (a) (2)	Ubuntu 22.04 LTS must map the authenticated identity to the user or group account for PKI-based authentication.	Not Applicable
UBTU-22-631010	SC-23 (5)	Ubuntu 22.04 LTS must use DOD PKI-established certificate authorities for verification of the establishment of protected sessions.	Failed
UBTU-22-631015	IA-5 (13)	Ubuntu 22.04 LTS must be configured such that Pluggable Authentication Module (PAM) prohibits the use of cached authentications after one day.	Not Applicable
UBTU-22-651010	SI-6 a	Ubuntu 22.04 LTS must use a file integrity tool to verify correct operation of all security functions.	Failed
UBTU-22-651015	SI-6 a	Ubuntu 22.04 LTS must configure AIDE to perform file integrity checking on the file system.	Failed
UBTU-22-651020	CM-3 (5), SI-6 d	Ubuntu 22.04 LTS must notify designated personnel if baseline configurations are changed in an unauthorized manner. The file integrity tool must notify the system administrator when changes to the baseline configuration or anomalies in the operation of any security functions are discovered.	Failed
UBTU-22-651025	SI-6 b	Ubuntu 22.04 LTS must be configured so that the script that runs each 30 days or less to check file integrity is the default.	Not Reviewed
UBTU-22-651030	AU-9 (3)	Ubuntu 22.04 LTS must use cryptographic mechanisms to protect the integrity of audit tools.	Failed

Control ID	NIST 800-83	Title	Status
UBTU-22-651035	AU-4 (1)	Ubuntu 22.04 LTS must have a crontab script running weekly to offload audit events of standalone systems.	Failed
UBTU-22-652010	SC-24	Ubuntu 22.04 LTS must be configured to preserve log records from failure events.	Passed
UBTU-22-652015	AC-17 (1)	Ubuntu 22.04 LTS must monitor remote access methods.	Passed
UBTU-22-653010	AU-3 a, AU-3 b, AU-3 c, AU-3 d, AU-3 e, AU-3 (1), AU-6 (4), AU-7 (1), AU-12 a, AU-12 c, CM-5 (1), AU-7 a, AU-7 b, AU-12 (3), CM-5 (1) (b)	Ubuntu 22.04 LTS must have the "auditd" package installed.	Passed
UBTU-22-653015	AU-3 a, AU-3 b, AU-3 c, AU-3 d, AU-3 e, AU-3 (1), AU-6 (4), AU-7 (1), AU-12 a, AU-12 c, CM-5 (1), AU-7 a, AU-7 b, AU-12 (3), CM-5 (1) (b)	Ubuntu 22.04 LTS must produce audit records and reports containing information to establish when, where, what type, the source, and the outcome for all DOD-defined auditable events and actions in near real time.	Passed
UBTU-22-653020	AU-4 (1)	Ubuntu 22.04 LTS audit event multiplexor must be configured to offload audit logs onto a different system from the system being audited.	Failed
UBTU-22-653025	AU-5 a	Ubuntu 22.04 LTS must alert the information system security officer (ISSO) and system administrator (SA) in the event of an audit processing failure.	Passed
UBTU-22-653030	AU-5 b	Ubuntu 22.04 LTS must shut down by default upon audit failure.	Failed
UBTU-22-653035	AU-4	Ubuntu 22.04 LTS must allocate audit record storage capacity to store at least one weeks' worth of audit records, when audit records are not immediately sent to a central audit record storage facility.	Passed
UBTU-22-653040	AU-5 (1)	Ubuntu 22.04 LTS must immediately notify the system administrator (SA) and information system security officer (ISSO) when the audit record storage volume reaches 25 percent remaining of the allocated capacity.	Failed
UBTU-22-653045	AU-9 a, AU-9 a	Ubuntu 22.04 LTS must be configured so that audit log files are not read- or write-accessible by unauthorized users.	Failed
UBTU-22-653050	AU-9 a, AU-9 a, AU-9 a	Ubuntu 22.04 LTS must be configured to permit only authorized users ownership of the audit log files.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-653055	AU-9 a, AU-9 a, AU-9 a	Ubuntu 22.04 LTS must permit only authorized groups ownership of the audit log files.	Failed
UBTU-22-653060	AU-9 a	Ubuntu 22.04 LTS must be configured so that the audit log directory is not write-accessible by unauthorized users.	Passed
UBTU-22-653065	AU-12 b	Ubuntu 22.04 LTS must be configured so that audit configuration files are not write-accessible by unauthorized users.	Failed
UBTU-22-653070	AU-12 b	Ubuntu 22.04 LTS must permit only authorized accounts to own the audit configuration files.	Passed
UBTU-22-653075	AU-12 b	Ubuntu 22.04 LTS must permit only authorized groups to own the audit configuration files.	Passed
UBTU-22-654010	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the apparmor_parser command.	Failed
UBTU-22-654015	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chacl command.	Failed
UBTU-22-654020	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chage command.	Passed
UBTU-22-654025	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chcon command.	Failed
UBTU-22-654030	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chfn command.	Passed
UBTU-22-654035	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chsh command.	Passed
UBTU-22-654040	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the crontab command.	Passed
UBTU-22-654045	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful attempts to use the fdisk command.	Failed
UBTU-22-654050	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the gpasswd command.	Passed
UBTU-22-654055	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful attempts to use the kmod command.	Failed
UBTU-22-654060	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful attempts to use modprobe command.	Passed
UBTU-22-654065	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the mount command.	Failed

Control ID	NIST 800-83	Title	Status
UBTU-22-654070	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the newgrp command.	Passed
UBTU-22-654075	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the pam_timestamp_check command.	Failed
UBTU-22-654080	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the passwd command.	Passed
UBTU-22-654085	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the setfacl command.	Failed
UBTU-22-654090	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the ssh-agent command.	Passed
UBTU-22-654095	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the ssh-keysign command.	Failed
UBTU-22-654100	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the su command.	Passed
UBTU-22-654105	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the sudo command.	Passed
UBTU-22-654110	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the sudoedit command.	Failed
UBTU-22-654115	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the umount command.	Failed
UBTU-22-654120	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the unix_update command.	Failed
UBTU-22-654125	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the usermod command.	Failed
UBTU-22-654130	AC-2 (4), AU-12 c, AC-2 (4), AC-2 (4), AC-2 (4), AC-2 (4)	Ubuntu 22.04 LTS must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/group.	Passed
UBTU-22-654135	AC-2 (4), AU-12 c, AC-2 (4), AC-2 (4), AC-2 (4), AC-2 (4)	Ubuntu 22.04 LTS must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/gshadow.	Passed
UBTU-22-654140	AC-2 (4), AU-12 c, AC-2 (4), AC-2 (4), AC-2 (4), AC-2 (4)	Ubuntu 22.04 LTS must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/opasswd.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-654145	AC-2 (4), AU-12 c, AC-2 (4), AC-2 (4), AC-2 (4), AC-2 (4)	Ubuntu 22.04 LTS must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/passwd.	Passed
UBTU-22-654150	AC-2 (4), AU-12 c, AC-2 (4), AC-2 (4), AC-2 (4), AC-2 (4)	Ubuntu 22.04 LTS must generate audit records for all account creations, modifications, disabling, and termination events that affect /etc/shadow.	Passed
UBTU-22-654155	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chmod, fchmod, and fchmodat system calls.	Passed
UBTU-22-654160	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the chown, fchown, fchownat, and lchown system calls.	Passed
UBTU-22-654165	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the creat, open, openat, open_by_handle_at, truncate, and ftruncate system calls.	Failed
UBTU-22-654170	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the delete_module system call.	Failed
UBTU-22-654175	AU-12 c	Ubuntu 22.04 LTS must generate audit records for successful/unsuccessful uses of the init_module and finit_module system calls.	Failed
UBTU-22-654180	AU-12 c	Ubuntu 22.04 LTS must generate audit records for any use of the setxattr, fsetxattr, lsetxattr, removexattr, fremovexattr, and lremovexattr system calls.	Passed
UBTU-22-654185	AU-12 c	Ubuntu 22.04 LTS must generate audit records for any successful/unsuccessful use of unlink, unlinkat, rename, renameat, and rmdir system calls.	Failed
UBTU-22-654190	CM-6 b	Ubuntu 22.04 LTS must generate audit records for all events that affect the systemd journal files.	Failed
UBTU-22-654195	AU-12 c	Ubuntu 22.04 LTS must generate audit records for the /var/log/btmp file.	Passed
UBTU-22-654200	AU-12 c	Ubuntu 22.04 LTS must generate audit records for the /var/log/wtmp file.	Passed
UBTU-22-654205	AU-12 c	Ubuntu 22.04 LTS must generate audit records for the /var/run/utmp file.	Passed
UBTU-22-654210	AU-12 c	Ubuntu 22.04 LTS must generate audit records for the use and modification of faillog file.	Passed
UBTU-22-654215	AU-12 c	Ubuntu 22.04 LTS must generate audit records for the use and modification of the lastlog file.	Passed
UBTU-22-654220	AU-12 c	Ubuntu 22.04 LTS must generate audit records when successful/unsuccessful attempts to modify the /etc/sudoers file occur.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-22-654225	AU-12 c	Ubuntu 22.04 LTS must generate audit records when successful/unsuccessful attempts to modify the /etc/sudoers.d directory occur.	Failed
UBTU-22-654230	AC-6 (8), AC-6 (9)	Ubuntu 22.04 LTS must prevent all software from executing at higher privilege levels than users executing the software and the audit system must be configured to audit the execution of privileged functions.	Failed
UBTU-22-654235	AU-12 c, MA-4 (1) (a), MA-3 (5)	Ubuntu 22.04 LTS must generate audit records for privileged activities, nonlocal maintenance, diagnostic sessions and other system-level access.	Passed
UBTU-22-671010	SC-13 b	Ubuntu 22.04 LTS must implement NIST FIPS-validated cryptography to protect classified information and for the following: To provision digital signatures, to generate cryptographic hashes, and to protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	Failed

Copyright © 2025 Broadcom. All rights reserved.
The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.
Item No: vmw-bc-wp-tech-temp-uslet-word-2025 Jun-25