STIG Readiness Guide Overview
October 2025

VMware vDefend – Security Services Platform

STIG Readiness Guide Overview

Version 1 Release 1

vmware®
by Broadcom

Table of contents

Overview

Broadcom is a trusted partner in highly secure, mission critical systems around the world, including the US 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). Where a product specific STIG is not available, the relevant SRGs must be used instead.

DoDI 8510.01

"STIGs are product-specific and document applicable DoD policies and security requirements, as well as best practices and configuration guidelines. STIGs are associated with security controls through CCIs, which are decompositions of NIST SP 800-53 security controls into single, actionable, measurable items. SRGs are developed by DISA to provide general security compliance guidelines and serve as source guidance documents for STIGs. When a STIG is not available for a product, an SRG may be used."

To better serve the needs of our DoD partners, and those who wish to meet the bar set by the DoD, Broadcom is providing SRG content that is the source material for an existing STIG, the basis for a future or in-process STIG, or that can be used in the absence of a DISA published STIG.

What does STIG Readiness mean?

Broadcom has published several STIGs with DISA and as such, we are very familiar with the SRGs and what it takes to meet DISA's stringent requirements for risk acceptance and publication. "STIG Readiness" means that we are doing the same level of work as we would do with DISA but self-publishing the content to make it available and usable as soon as possible. The quality is high enough, in our experience, that should a given "STIG Ready" product be put through the DISA process, we are confident that there would be minimal content changes before publication.

This project represents Broadcom's effort to document our compliance against the SRG requirements and nothing more. A published STIG is our eventual goal, in most cases, but this content should not be viewed to be "as good as a STIG". A DISA published STIG includes technical validation, review of requirement fulfillment, accuracy and style, risk acceptance and is digitally signed by the RME and posted on cyber.mil. Except for products that already have published STIGs, there is no explicit or implied DISA approval of the provided content. We also make no guarantee that any STIG(s) will be published from this content in the future.

Other Considerations

It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations as such ensure all steps are taken to back systems up before implementation.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. Furthermore, Broadcom implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is intended for the Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level because some of the settings may not be able to be configured in environments outside the DoD architecture.

Support and Compatibility

The content available in this guide is intended only for VMware vDefend - Security Services Platform 5.1.x. Applicability of this guidance prior to 5.1.0 is not supported.

As previously stated, this content is produced by Broadcom without any DISA ownership. As such, any guidance or technical issues must go through Broadcom support channels and not DISA.

Guidance Details

The STIG Readiness Guide is a collection of documents intended to assist customers that need to comply with DOD security requirements by providing hardening guidance based on DISA Security Requirements Guides.

In the provided guidance there are no Extensible Configuration Checklist Description Format (XCCDF) documents for the listed components.

Product Summary

Security Services Platform for VMware® vDefend™ accelerates and simplifies the journey to Zero Trust security within a VMware Cloud Foundation environment. It is a high-performance and scalable platform that runs vDefend security services, including Security Intelligence, Network Detection and Response, Malware Prevention, and more.

Security Services Platform addresses key challenges that are posed by evolving cyber threats. The platform hosts innovations in VMware® vDefend™ that do not only react to threats but fundamentally change how you build, operate, and secure your enterprise private cloud.

Security Services Platform hosts various innovations for protecting workloads on VCF private cloud:

- Security Intelligence provides real-time application flow discovery and visibility, correlates and analyzes ingested data, and provides ML-based firewall rule recommendations that are aligned with design best practices. It enables accelerated zero trust with built-in automation-driven workflows for multi-stage segmentation and firewall rule analysis to streamline lateral security, making the journey to Zero Trust private cloud faster and more efficient

- Advanced Threat Prevention capabilities identify zero-day threats using behavior-based methods to determine baseline network activity and uses ML models to detect anomalies indicating malicious activities. Its multi-context Network Detection and Response helps quickly triage threat campaigns by automatically correlating multi-context signals into high-fidelity campaigns that are mapped to the MITRE ATT&CK framework. It helps detect and prevent malware using static and AI/ML-based dynamic analysis. This includes protection against zero-day exploits. The solution covers all types of traffic from network devices, virtual machines, containers, and bare-metal systems.

The platform can be configured in the following editions:

- VMware vDefend Firewall

- VMware vDefend Firewall with Advanced Threat Prevention

The platform is comprised of the following components:

- Security Services Platform Installer for VMware vDefend

  Security Services Platform Installer is a VM which deploys and manages the Security Services Platform Instance. The installer also hosts packages needed for the deployment and upgrade of the SSP Instance. The installer has a browser-based user interface to manage the environment.

- Security Services Platform for VMware vDefend

  Security Services Platform consists of a cluster containing controller nodes and worker nodes. You can access the Security Services Platform via its browser-based user interface to manage the SSP instance and the security features.

- Malware Prevention Service – Service Virtual Machine

  Malware Prevention Service – Service Virtual Machine is a VM which is deployed on each host of a cluster when the Distributed Malware Prevention Service is enabled. Its primary function is to detect malicious traffic patterns and analyze files for suspicious behavior.

- NDR Sensor for VMware vDefend

  NDR Sensor for VMware vDefend is a passive, out-of-band virtual appliance that is deployed in data centers to monitor network traffic from non-NSX virtual machines, bare metal servers, and other physical or non-virtualized environments. The sensor analyzes network traffic in real time to detect and respond to security threats.

Applicability

The content contained within this guidance was intended for the following product and versions:

- VMware vDefend – Security Services Platform 5.1.x

Application of this guidance to product versions outside of those listed is not supported.

Component Guidance

Security Services Platform for VMware vDefend is comprised of multiple components that deliver the features and capabilities of VMware vDefend. The Appendix sections will detail the relationship between this guidance and each component.

Product Guidance

- Security Services Platform Installer & Security Services Platform
  - Application – Appendix A

Appliance Guidance

- Security Services Platform Installer
  - Ubuntu 24.04 – Appendix B
  - Kubernetes – Appendix C
- Security Services Platform
  - Ubuntu 24.04 – Appendix B
  - Kubernetes – Appendix D
- Malware Prevention Service – Service Virtual Machine (SVM)
  - Ubuntu 24.04 – Appendix E
- NDR Sensor for VMware vDefend
  - Ubuntu 24.04 – Appendix F

It is not supported for users to make changes to the VMware vDefend appliances (Security Services Platform Installer, Security Services Platform, Malware Prevention Services – Service Virtual Machine, NDR Sensor for VMware vDefend), as these are vendor-hardened appliances.

Refer to the Appendix for details on compliance check status for each of the above components.

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.

Status Definitions	
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.

Frequently Asked Questions

What do the severity codes mean?

As stated in the DISA Security Requirements Guides:

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

DISA Category Code Guidelines	
CAT I	Any vulnerability, the exploitation of which will **directly and immediately** result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which **has a potential to** result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which **degrades measures** to protect against loss of Confidentiality, Availability, or Integrity.

Most of the severity codes in the associated guides are CAT IIs. During STIG development DISA modifies severity codes on a per product and context specific basis.

How do I view a STIG?

STIGs are delivered as an XML file that follows the XCCDF schema as defined by NIST. These XML files can be imported into a tool called STIG viewer which is available from DISA for download here: https://public.cyber.mil/stigs/srg-stig-tools/

Can I import the XCCDF files into STIG Viewer?

Yes, the XCCDF files can be imported into STIG Viewer and then used to create STIG Checklists as necessary.

Are there any scripts or tools to help audit and remediate these controls?

There are currently no example scripts and playbooks to aid in these tasks.

What requirements were considered when developing this content?

All technical NIST SP 800-53 requirements and applicable SRGs were considered while developing this content.

Requirements that are applicable and configurable will be included in the final content.

Appendix A: Application (Security Services Platform Installer + Security Services Platform)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the VMware vDefend Security Services Platform Installer and vDefend Security Services Platform appliances, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
SRG-APP-000001-AS-000001	AC-10 AC-10.1 (ii)	The application server must limit the number of concurrent sessions to an organization-defined number for all accounts and/or account types.	Passed
SRG-APP-000014-AS-000009	AC-17 (2) AC-17 (2).1	The application server must use encryption strength in accordance with the categorization of the management data during remote access management sessions.	Passed
SRG-APP-000015-AS-000010	AC-17 (2) AC-17 (2).1	The application server must implement cryptography mechanisms to protect the integrity of the remote access session.	Passed
SRG-APP-000016-AS-000013	AC-17 (1) AC-17 (1).1	The application server must ensure remote sessions for accessing security functions and security-relevant information are logged.	Passed
SRG-APP-000033-AS-000024	AC-3 AC-3.1	The application server must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies.	Passed
SRG-APP-000086-AS-000048	AU-12 (1) AU-12 (1).1 (iii&v) AU-12 (1)	For application servers providing log record aggregation, the application server must compile log records from organization-defined information system components into a system-wide log trail that is time-correlated with an organization-defined level of tolerance for the relationship between time stamps of individual records in the log trail.	Passed
SRG-APP-000091-AS-000052	AU-12 c AU-12.1 (iv) AU-12 c	The application server must generate log records when successful/unsuccessful attempts to access subject privileges occur.	Passed
SRG-APP-000092-AS-000053	AU-14 (1) AU-14 (1).1	The application server must initiate session logging upon startup.	Passed
SRG-APP-000095-AS-000056	AC-3 AC-3.1	The application server must produce log records containing information to establish what type of events occurred.	Passed
SRG-APP-000096-AS-000059	AC-3 AC-3.1	The application server must produce log records containing sufficient information to establish when (date and time) the events occurred.	Passed
SRG-APP-000098-AS-000061	AC-3 AC-3.1	The application server must produce log records containing sufficient information to establish the sources of the events.	Passed
SRG-APP-000099-AS-000062	AC-3 AC-3.1	The application server must produce log records that contain sufficient information to establish the outcome of events.	Passed
SRG-APP-000100-AS-000063	AC-3 AC-3.1	The application server must generate log records containing information that establishes the identity of any individual or process associated with the event.	Passed
SRG-APP-000116-AS-000076	AU-8 AU-8.1 AU-8 a	The application server must use internal system clocks to generate timestamps for log records.	Passed

Control ID	NIST 800-83	Title	Status
SRG-APP-000118-AS-000078	AU-9 AU-9.1	The application server must protect log information from any type of unauthorized read access.	Passed
SRG-APP-000119-AS-000079	AU-9 AU-9.1	The application server must protect log information from unauthorized modification.	Passed
SRG-APP-000120-AS-000080	AU-9 AU-9.1	The application server must protect log information from unauthorized deletion.	Passed
SRG-APP-000121-AS-000081	AU-9 AU-9.1	The application server must protect log tools from unauthorized access.	Passed
SRG-APP-000122-AS-000082	AU-9 AU-9.1	The application server must protect log tools from unauthorized modification.	Passed
SRG-APP-000123-AS-000083	AU-9 AU-9.1	The application server must protect log tools from unauthorized deletion.	Passed
SRG-APP-000131-AS-000002		The application server must prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate recognized and approved by the organization.	Passed
SRG-APP-000133-AS-000092	CM-5 (6) CM-5 (6).1	The application server must limit privileges to change the software resident within software libraries.	Passed
SRG-APP-000133-AS-000093	SC-24 SC-24.1 (iv)	The application server must be capable of reverting to the last known good configuration in the event of failed installations and upgrades.	Passed
SRG-APP-000141-AS-000095	CM-7 CM-7.1 (ii) CM-7 a	The application server must adhere to the principles of least functionality by providing only essential capabilities.	Passed
SRG-APP-000142-AS-000014	CM-7 CM-7.1 (iii) CM-7 b	The application server must prohibit or restrict the use of non secure ports, protocols, modules, and/or services as defined in the PPSM CAL and vulnerability assessments.	Passed
SRG-APP-000153-AS-000104		The application server must authenticate users individually prior to using a group authenticator.	Passed
SRG-APP-000172-AS-000120	IA-5 (1) (c) IA-5 (1).1 (v)	The application server must transmit only encrypted representations of passwords.	Passed
SRG-APP-000175-AS-000124	IA-5 (2) IA-5 (2).1 IA-5 (2) (a)	The application server must perform RFC 5280-compliant certification path validation.	Passed
SRG-APP-000176-AS-000125	IA-5 (2) IA-5 (2).1	Only authenticated system administrators or the designated PKI Sponsor for the application server must have access to the web servers private key.	Passed
SRG-APP-000178-AS-000127	IA-6 IA-6.1	The application server must obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Passed
SRG-APP-000220-AS-000148	SC-23 (1) SC-23 (1).1	The application server must invalidate session identifiers upon user logout or other session termination.	Passed

Control ID	NIST 800-83	Title	Status
SRG-APP-000223-AS-000150	SC-23 (3) SC-23 (3).1 (ii)	The application server must generate a unique session identifier for each session.	Passed
SRG-APP-000223-AS-000151	SC-23 (3) SC-23 (3).1 (ii)	The application server must recognize only system-generated session identifiers.	Passed
SRG-APP-000225-AS-000153	SC-24 SC-24.1 (iv)	The application server must be configured to perform complete application deployments.	Passed
SRG-APP-000225-AS-000154	SC-24 SC-24.1 (iv)	The application server must provide a clustering capability.	Passed
SRG-APP-000231-AS-000133	SC-28 SC-28.1	The application server must protect the confidentiality and integrity of all information at rest.	Passed
SRG-APP-000231-AS-000156	SC-28 SC-28.1	The application server must employ cryptographic mechanisms to ensure confidentiality and integrity of all information at rest when stored off-line.	Passed
SRG-APP-000251-AS-000165	SI-10 SI-10.1	The application server must check the validity of all data inputs to the management interface, except those specifically identified by the organization.	Passed
SRG-APP-000267-AS-000170	SI-11 c SI-11.1 (iv) SI-11 b	The application server must restrict error messages only to authorized users.	Passed
SRG-APP-000295-AS-000263	AC-12	The application server must automatically terminate a user session after organization-defined conditions or trigger events requiring a session disconnect.	Passed
SRG-APP-000296-AS-000201	AC-12 (1)	The application server management interface must provide a logout capability for user-initiated communication session.	Passed
SRG-APP-000297-AS-000188	AC-12 (1)	The application server management interface must display an explicit logout message to users indicating the reliable termination of authenticated communications sessions.	Passed
SRG-APP-000340-AS-000185	AC-6 (10)	The application server must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.	Passed
SRG-APP-000343-AS-000030	AC-6 (9)	The application server must provide access logging that ensures users who are granted a privileged role (or roles) have their privileged activity logged.	Passed
SRG-APP-000371-AS-000077		The application server must compare internal application server clocks at least every 24 hours with an authoritative time source.	Passed
SRG-APP-000372-AS-000212		The application server must synchronize internal application server clocks to an authoritative time source when the time difference is greater than the organization-defined time period.	Passed
SRG-APP-000428-AS-000265	SC-28 (1)	The application server must implement cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.	Passed
SRG-APP-000429-AS-000157	SC-28 (1)	The application must implement cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.	Passed

Control ID	NIST 800-83	Title	Status
SRG-APP-000435-AS-000069	SC-5	The application server, when a MAC I system, must be in a high-availability (HA) cluster.	Passed
SRG-APP-000435-AS-000163	SC-5	The application server must protect against or limit the effects of all types of Denial of Service (DoS) attacks by employing organization-defined security safeguards.	Passed
SRG-APP-000439-AS-000155	SC-8	The application server must protect the confidentiality and integrity of transmitted information through the use of an approved TLS version.	Passed
SRG-APP-000440-AS-000167	SC-8 (1)	The application server must employ approved cryptographic mechanisms to prevent unauthorized disclosure of information and/or detect changes to information during transmission.	Passed
SRG-APP-000441-AS-000258	SC-8 (2)	The application server must maintain the confidentiality and integrity of information during preparation for transmission.	Passed
SRG-APP-000442-AS-000259	SC-8 (2)	The application server must maintain the confidentiality and integrity of information during reception.	Passed
SRG-APP-000447-AS-000273	SI-10 (3)	The application server must behave in a predictable and documented manner that reflects organizational and system objectives when invalid inputs are received.	Passed
SRG-APP-000454-AS-000268	SI-2 (6)	The application server must remove organization-defined software components after updated versions have been installed.	Passed
SRG-APP-000514-AS-000136	SC-13	Application servers must use NIST-approved or NSA-approved key management technology and processes.	Passed
SRG-APP-000910-AS-000300		The application server must include only approved trust anchors in trust stores or certificate stores managed by the organization.	Passed
SRG-APP-000920-AS-000320		The application server must synchronize system clocks within and between systems or system components.	Passed

Appendix B: Ubuntu 24.04 (Security Services Platform Installer + Security Services Platform)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the VMware vDefend Security Services Platform Installer and vDefend Security Services Platform appliances, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
UBTU-24-100030	IA-5 (1) (c) IA-5 (1).1 (v) IA-5 (1) (c)	Ubuntu 24.04 LTS must not have the telnet package installed.	Passed
UBTU-24-100040	CM-7 CM-7.1 (ii) CM-7 a	Ubuntu 24.04 LTS must not have the rsh-server package installed.	Passed
UBTU-24-100200	SC-24 SC-24.1 (v)	Ubuntu 24.04 LTS must be configured to preserve log records from failure events.	Passed
UBTU-24-100500	AC-3 (4) CM-7 (2) CM-7 (5) (b)	Ubuntu 24.04 LTS must have AppArmor installed.	Passed
UBTU-24-100510	CM-7 (2) AC-6 (10) CM-7 (5) (b)	Ubuntu 24.04 LTS must be configured to use AppArmor.	Passed
UBTU-24-100600	CM-6 b CM-6.1 (iv) CM-6 b	Ubuntu 24.04 LTS must have the "libpam-pwquality" package installed.	Passed
UBTU-24-100700	CM-6 b CM-6.1 (iv) CM-6 b	Ubuntu 24.04 LTS must have the "chrony" package installed.	Passed
UBTU-24-100800	SC-8 SC-8 (2)	Ubuntu 24.04 LTS must have SSH installed.	Passed
UBTU-24-100810	SC-8 SC-8 (2)	Ubuntu 24.04 LTS must use SSH to protect the confidentiality and integrity of transmitted information.	Passed
UBTU-24-100840	AC-17 (2) AC-17 (2).1 AC-17 (2)	Ubuntu 24.04 LTS SSH server must be configured to use only FIPS 140-3 validated key exchange algorithms.	Passed
UBTU-24-102000	AC-3 AC-3.1	Ubuntu 24.04 LTS when booted must require authentication upon booting into single-user and maintenance modes.	Passed
UBTU-24-102010	AU-14 (1) AU-14 (1).1		
UBTU-24-200090	AC-17 (1) AC-17 (1).1 AC-17 (1)	Ubuntu 24.04 LTS must monitor remote access methods.	Passed
UBTU-24-300006	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library files must have mode 0755 or less permissive.	Passed
UBTU-24-300007	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library files must be owned by root.	Passed
UBTU-24-300008	CM-5 (6) CM-5 (6).1 CM-5 (6)	Ubuntu 24.04 LTS library directories must be owned by root.	Passed
UBTU-24-300010	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library directories must be group-owned by root.	Passed
UBTU-24-300011	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands set to a mode of 0755 or less permissive.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-300012	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands owned by root or a system account.	Passed
UBTU-24-300013	CM-5 (6) CM-5 (6).2	Ubuntu 24.04 LTS must have system commands group-owned by root or a system account.	Passed
UBTU-24-300016	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must be configured so that when passwords are changed or new passwords are established, pwquality must be used.	Passed
UBTU-24-300017	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must enforce a delay of at least four seconds between logon prompts following a failed logon attempt.	Passed
UBTU-24-300027	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have accounts configured with blank or null passwords.	Passed
UBTU-24-300028	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not allow accounts configured in Pluggable Authentication Modules (PAM) with blank or null passwords.	Passed
UBTU-24-400000	IA-2 IA-2.1	Ubuntu 24.04 LTS must uniquely identify interactive users.	Passed
UBTU-24-400110		Ubuntu 24.04 LTS must prevent direct login to the root account.	Passed
UBTU-24-400220		Ubuntu 24.04 LTS must store only encrypted representations of passwords.	Passed
UBTU-24-400400	IA-7 IA-7.1	Ubuntu 24.04 LTS must encrypt all stored passwords with a FIPS 140-3 approved cryptographic hashing algorithm.	Passed
UBTU-24-500050	MA-4 c MA-4.1 (iv)	Ubuntu 24.04 LTS must use strong authenticators in establishing nonlocal maintenance and diagnostic sessions.	Passed
UBTU-24-600130	SC-3 SC-3.1 (ii)	Ubuntu 24.04 LTS must ensure only users who need access to security functions are part of sudo group.	Passed
UBTU-24-600140	SC-4 SC-4.1	Ubuntu 24.04 LTS must restrict access to the kernel message buffer.	Passed
UBTU-24-600160		Ubuntu 24.04 LTS must compare internal information system clocks at least every 24 hours with an authoritative time server.	Passed
UBTU-24-600180		Ubuntu 24.04 LTS must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.	Passed
UBTU-24-600190	SC-5 (2) SC-5 (2).1	Ubuntu 24.04 LTS must be configured to use TCP syncookies.	Passed
UBTU-24-600230	SC-8	Ubuntu 24.04 LTS must disable all wireless network adapters.	Passed
UBTU-24-700040	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is owned by "root".	Passed
UBTU-24-700050	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is group-owned by "root".	Passed
UBTU-24-700060	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700070	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700080	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be owned by "root".	Passed
UBTU-24-700090	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be owned by "root"	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-700100	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be group-owned by syslog.	Passed
UBTU-24-700110	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be owned by root.	Passed
UBTU-24-700130	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log/syslog file to be group-owned by adm.	Passed
UBTU-24-700140	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file to be owned by syslog.	Passed
UBTU-24-700150	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file with mode "0640" or less permissive.	Passed
UBTU-24-700300	SI-16	Ubuntu 24.04 LTS must implement nonexecutable data to protect its memory from unauthorized code execution.	Passed
UBTU-24-700310	SI-17	Ubuntu 24.04 LTS must implement address space layout randomization to protect its memory from unauthorized code execution.	Passed
UBTU-24-700400	SI-2 c	Ubuntu 24.04 LTS must be a vendor-supported release.	Passed
UBTU-24-900040	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must be configured so that audit configuration files are not write-accessible by unauthorized users.	Passed
UBTU-24-900050	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized accounts to own the audit configuration files.	Passed
UBTU-24-900060	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized groups to own the audit configuration files.	Passed
UBTU-24-900920	AU-4	Ubuntu 24.04 LTS must allocate audit record storage capacity to store at least one week's worth of audit records, when audit records are not immediately sent to a central audit record storage facility.	Passed
UBTU-24-901220	AU-8 b	Ubuntu 24.04 LTS must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	Passed
UBTU-24-901230	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools with a mode of "0755" or less permissive.	Passed
UBTU-24-901240	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools to be owned by root.	Passed
UBTU-24-901250	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure the audit tools to be group-owned by root.	Passed
UBTU-24-901260	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands set to a mode of "0755" or less permissive.	Passed
UBTU-24-901270	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands owned by root.	Passed
UBTU-24-901280	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands group-owned by root.	Passed
UBTU-24-901300	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured so that audit log files are not read or write-accessible by unauthorized users.	Passed
UBTU-24-901310	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured to permit only authorized users ownership of the audit log files.	Passed
UBTU-24-901380	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured so that the audit log directory is not write-accessible by unauthorized users.	Passed

Appendix C: Kubernetes (Security Services Platform Installer)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the VMware vDefend Security Services Platform Installer, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
CNTR-K8-000190	AC-17 (2) AC-17 (2).1	The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination.	Passed
CNTR-K8-000220	AC-2 (1) AC-2 (1).1	The Kubernetes Controller Manager must create unique service accounts for each work payload.	Passed
CNTR-K8-000270	AC-3 AC-3.1	The Kubernetes API Server must enable Node,RBAC as the authorization mode.	Passed
CNTR-K8-000290	CM-6 b CM-6.1 (iv)	User-managed resources must be created in dedicated namespaces.	Passed
CNTR-K8-000300	AC-3 AC-3.1	The Kubernetes Scheduler must have secure binding.	Passed
CNTR-K8-000310	AC-3 AC-3.1	The Kubernetes Controller Manager must have secure binding.	Passed
CNTR-K8-000330	AC-3 AC-3.1	The Kubernetes Kubelet must have the "readOnlyPort" flag disabled.	Passed
CNTR-K8-000340	AC-3 AC-3.1	The Kubernetes API server must have the insecure bind address not set.	Passed
CNTR-K8-000350	AC-3 AC-3.1	The Kubernetes API server must have the secure port set.	Passed
CNTR-K8-000370	AC-3 AC-3.1	The Kubernetes Kubelet must have anonymous authentication disabled.	Passed
CNTR-K8-000380	AC-3 AC-3.1	The Kubernetes kubelet must enable explicit authorization.	Passed
CNTR-K8-000420	AC-3 AC-3.1	Kubernetes dashboard must not be enabled.	Passed
CNTR-K8-000430	AC-3 AC-3.1	Kubernetes Kubectl cp command must give expected access and results.	Passed
CNTR-K8-000450	AC-3 AC-3.1	Kubernetes DynamicAuditing must not be enabled.	Passed
CNTR-K8-000470	AC-3 AC-3.1	The Kubernetes API server must have Alpha APIs disabled.	Passed
CNTR-K8-000850	CM-5 (6) CM-5 (6).1	Kubernetes Kubelet must deny hostname override.	Passed
CNTR-K8-000860	CM-5 (6) CM-5 (6).1	The Kubernetes manifests must be owned by root.	Passed
CNTR-K8-000880	CM-5 (6) CM-5 (6).1	The Kubernetes KubeletConfiguration file must be owned by root.	Passed
CNTR-K8-000890	CM-5 (6) CM-5 (6).1	The Kubernetes KubeletConfiguration files must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-000900	CM-5 (6) CM-5 (6).1 CM-6 b CM-6.1 (iv) CM-6 b	The Kubernetes manifest files must have least privileges.	Passed

Control ID	NIST 800-83	Title	Status
CNTR-K8-000920	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes API Server must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000930	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes Scheduler must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000940	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes Controllers must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000950	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes etcd must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-001360	SC-2 SC-2.1	Kubernetes must separate user functionality.	Passed
CNTR-K8-001410	SC-23 SC-23.1	Kubernetes API Server must have the SSL Certificate Authority set.	Passed
CNTR-K8-001420	SC-23 SC-23.1	Kubernetes Kubelet must have the SSL Certificate Authority set.	Passed
CNTR-K8-001430	SC-23 SC-23.1	Kubernetes Controller Manager must have the SSL Certificate Authority set.	Passed
CNTR-K8-001440	SC-23 SC-23.1	Kubernetes API Server must have a certificate for communication.	Passed
CNTR-K8-001450	SC-23 SC-23.1	Kubernetes etcd must enable client authentication to secure service.	Passed
CNTR-K8-001490	SC-23 SC-23.1	Kubernetes etcd must have a key file for secure communication.	Passed
CNTR-K8-001500	SC-23 SC-23.1	Kubernetes etcd must have a certificate for communication.	Passed
CNTR-K8-001510	SC-23 SC-23.1	Kubernetes etcd must have the SSL Certificate Authority set.	Passed
CNTR-K8-001520	SC-23 SC-23.1	Kubernetes etcd must have a certificate for communication.	Passed
CNTR-K8-001530	SC-23 SC-23.1	Kubernetes etcd must have a key file for secure communication.	Passed
CNTR-K8-001540	SC-23 SC-23.1	Kubernetes etcd must have peer-cert-file set for secure communication.	Passed
CNTR-K8-001550	SC-23 SC-23.1	Kubernetes etcd must have a peer-key-file set for secure communication.	Passed
CNTR-K8-002010	AC-16 a	Kubernetes must have a pod security policy set.	Passed
CNTR-K8-002600	SC-7 (21)	Kubernetes API Server must configure timeouts to limit attack surface.	Passed
CNTR-K8-002700	SI-4 d	Kubernetes must remove old components after updated versions have been installed.	Passed
CNTR-K8-002720	SI-3 (10) (a)	Kubernetes must contain the latest updates as authorized by IAVMs, CTOs, DTMs, and STIGs.	Passed
CNTR-K8-003110	CM-6 b CM-6.1 (iv)	The Kubernetes component manifests must be owned by root.	Passed
CNTR-K8-003120	CM-6 b CM-6.1 (iv)	The Kubernetes component etcd must be owned by etcd.	Passed
CNTR-K8-003130	CM-6 b CM-6.1 (iv)	The Kubernetes conf files must be owned by root.	Passed

Control ID	NIST 800-83	Title	Status
CNTR-K8-003140	CM-6 b CM-6.1 (iv)	The Kubernetes Kube Proxy kubeconfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003150	CM-6 b CM-6.1 (iv)	The Kubernetes Kube Proxy kubeconfig must be owned by root.	Passed
CNTR-K8-003160	CM-6 b CM-6.1 (iv)	The Kubernetes Kubelet certificate authority file must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003170	CM-6 b CM-6.1 (iv)	The Kubernetes Kubelet certificate authority must be owned by root.	Passed
CNTR-K8-003180	CM-6 b CM-6.1 (iv)	The Kubernetes component PKI must be owned by root.	Passed
CNTR-K8-003190	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet KubeConfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003200	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet KubeConfig file must be owned by root.	Passed
CNTR-K8-003210	CM-6 b CM-6.1 (iv)	The Kubernetes kubeadm.conf must be owned by root.	Passed
CNTR-K8-003220	CM-6 b CM-6.1 (iv)	The Kubernetes kubeadm.conf must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003230	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet config must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003240	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet config must be owned by root.	Passed
CNTR-K8-003260	CM-6 b CM-6.1 (iv)	The Kubernetes etcd must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003270	CM-6 b CM-6.1 (iv)	The Kubernetes admin kubeconfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003330	CM-6 b CM-6.1 (iv)	The Kubernetes PKI CRT must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003340	CM-6 b CM-6.1 (iv)	The Kubernetes PKI keys must have file permissions set to 600 or more restrictive.	Passed
CNTR-K8-002620	SC-12 (3)	Kubernetes API Server must disable basic authentication to protect information in transit.	Passed
CNTR-K8-002630	SC-12 (3)	Kubernetes API Server must disable token authentication to protect information in transit.	Passed
CNTR-K8-002640	SC-12 (3)	Kubernetes endpoints must use approved organizational certificate and key pair to protect information in transit.	Passed

Appendix D: Kubernetes (Security Services Platform for VMware vDefend)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the vDefend Security Services Platform appliances, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
CNTR-K8-000190	AC-17 (2) AC-17 (2).1	The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination.	Passed
CNTR-K8-000220	AC-2 (1) AC-2 (1).1	The Kubernetes Controller Manager must create unique service accounts for each work payload.	Passed
CNTR-K8-000270	AC-3 AC-3.1	The Kubernetes API Server must enable Node,RBAC as the authorization mode.	Passed
CNTR-K8-000290	CM-6 b CM-6.1 (iv)	User-managed resources must be created in dedicated namespaces.	Passed
CNTR-K8-000300	AC-3 AC-3.1	The Kubernetes Scheduler must have secure binding.	Passed
CNTR-K8-000310	AC-3 AC-3.1	The Kubernetes Controller Manager must have secure binding.	Passed
CNTR-K8-000330	AC-3 AC-3.1	The Kubernetes Kubelet must have the "readOnlyPort" flag disabled.	Passed
CNTR-K8-000340	AC-3 AC-3.1	The Kubernetes API server must have the insecure bind address not set.	Passed
CNTR-K8-000350	AC-3 AC-3.1	The Kubernetes API server must have the secure port set.	Passed
CNTR-K8-000370	AC-3 AC-3.1	The Kubernetes Kubelet must have anonymous authentication disabled.	Passed
CNTR-K8-000380	AC-3 AC-3.1	The Kubernetes kubelet must enable explicit authorization.	Passed
CNTR-K8-000420	AC-3 AC-3.1	Kubernetes dashboard must not be enabled.	Passed
CNTR-K8-000430	AC-3 AC-3.1	Kubernetes Kubectl cp command must give expected access and results.	Passed
CNTR-K8-000450	AC-3 AC-3.1	Kubernetes DynamicAuditing must not be enabled.	Passed
CNTR-K8-000470	AC-3 AC-3.1	The Kubernetes API server must have Alpha APIs disabled.	Passed

Control ID	NIST 800-83	Title	Status
CNTR-K8-000850	CM-5 (6) CM-5 (6).1	Kubernetes Kubelet must deny hostname override.	Passed
CNTR-K8-000860	CM-5 (6) CM-5 (6).1	The Kubernetes manifests must be owned by root.	Passed
CNTR-K8-000880	CM-5 (6) CM-5 (6).1	The Kubernetes KubeletConfiguration file must be owned by root.	Passed
CNTR-K8-000890	CM-5 (6) CM-5 (6).1	The Kubernetes KubeletConfiguration files must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-000900	CM-5 (6) CM-5 (6).1 CM-6 b CM-6.1 (iv) CM-6 b	The Kubernetes manifest files must have least privileges.	Passed
CNTR-K8-000920	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes API Server must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000930	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes Scheduler must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000940	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes Controllers must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000950	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes etcd must enforce ports, protocols, and services (PPS) that adhere to the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL).	Passed
CNTR-K8-000960	CM-7 CM-7.1 (iii) CM-7 b	The Kubernetes cluster must use non-privileged host ports for user pods.	Passed
CNTR-K8-001360	SC-2 SC-2.1	Kubernetes must separate user functionality.	Passed
CNTR-K8-001410	SC-23 SC-23.1	Kubernetes API Server must have the SSL Certificate Authority set.	Passed
CNTR-K8-001420	SC-23 SC-23.1	Kubernetes Kubelet must have the SSL Certificate Authority set.	Passed
CNTR-K8-001430	SC-23 SC-23.1	Kubernetes Controller Manager must have the SSL Certificate Authority set.	Passed
CNTR-K8-001440	SC-23 SC-23.1	Kubernetes API Server must have a certificate for communication.	Passed
CNTR-K8-001450	SC-23 SC-23.1	Kubernetes etcd must enable client authentication to secure service.	Passed
CNTR-K8-001460	SC-23 SC-23.1	Kubernetes Kubelet must enable tlsPrivateKeyFile for client authentication to secure service.	Passed

Control ID	NIST 800-83	Title	Status
CNTR-K8-001470	SC-23 SC-23.1	Kubernetes Kubelet must enable tlsCertFile for client authentication to secure service.	Passed
CNTR-K8-001490	SC-23 SC-23.1	Kubernetes etcd must have a key file for secure communication.	Passed
CNTR-K8-001500	SC-23 SC-23.1	Kubernetes etcd must have a certificate for communication.	Passed
CNTR-K8-001510	SC-23 SC-23.1	Kubernetes etcd must have the SSL Certificate Authority set.	Passed
CNTR-K8-001520	SC-23 SC-23.1	Kubernetes etcd must have a certificate for communication.	Passed
CNTR-K8-001530	SC-23 SC-23.1	Kubernetes etcd must have a key file for secure communication.	Passed
CNTR-K8-001540	SC-23 SC-23.1	Kubernetes etcd must have peer-cert-file set for secure communication.	Passed
CNTR-K8-001550	SC-23 SC-23.1	Kubernetes etcd must have a peer-key-file set for secure communication.	Passed
CNTR-K8-002010	AC-16 a	Kubernetes must have a pod security policy set.	Passed
CNTR-K8-002600	SC-7 (21)	Kubernetes API Server must configure timeouts to limit attack surface.	Passed
CNTR-K8-002700	SI-4 d	Kubernetes must remove old components after updated versions have been installed.	Passed
CNTR-K8-002720	SI-3 (10) (a)	Kubernetes must contain the latest updates as authorized by IAVMs, CTOs, DTMs, and STIGs.	Passed
CNTR-K8-003110	CM-6 b CM-6.1 (iv)	The Kubernetes component manifests must be owned by root.	Passed
CNTR-K8-003120	CM-6 b CM-6.1 (iv)	The Kubernetes component etcd must be owned by etcd.	Passed
CNTR-K8-003130	CM-6 b CM-6.1 (iv)	The Kubernetes conf files must be owned by root.	Passed
CNTR-K8-003140	CM-6 b CM-6.1 (iv)	The Kubernetes Kube Proxy kubeconfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003150	CM-6 b CM-6.1 (iv)	The Kubernetes Kube Proxy kubeconfig must be owned by root.	Passed
CNTR-K8-003160	CM-6 b CM-6.1 (iv)	The Kubernetes Kubelet certificate authority file must have file permissions set to 644 or more restrictive.	Passed

Control ID	NIST 800-83	Title	Status
CNTR-K8-003170	CM-6 b CM-6.1 (iv)	The Kubernetes Kubelet certificate authority must be owned by root.	Passed
CNTR-K8-003180	CM-6 b CM-6.1 (iv)	The Kubernetes component PKI must be owned by root.	Passed
CNTR-K8-003190	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet KubeConfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003200	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet KubeConfig file must be owned by root.	Passed
CNTR-K8-003210	CM-6 b CM-6.1 (iv)	The Kubernetes kubeadm.conf must be owned by root.	Passed
CNTR-K8-003220	CM-6 b CM-6.1 (iv)	The Kubernetes kubeadm.conf must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003230	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet config must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003240	CM-6 b CM-6.1 (iv)	The Kubernetes kubelet config must be owned by root.	Passed
CNTR-K8-003260	CM-6 b CM-6.1 (iv)	The Kubernetes etcd must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003270	CM-6 b CM-6.1 (iv)	The Kubernetes admin kubeconfig must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003330	CM-6 b CM-6.1 (iv)	The Kubernetes PKI CRT must have file permissions set to 644 or more restrictive.	Passed
CNTR-K8-003340	CM-6 b CM-6.1 (iv)	The Kubernetes PKI keys must have file permissions set to 600 or more restrictive.	Passed
CNTR-K8-002620	SC-12 (3)	Kubernetes API Server must disable basic authentication to protect information in transit.	Passed
CNTR-K8-002630	SC-12 (3)	Kubernetes API Server must disable token authentication to protect information in transit.	Passed
CNTR-K8-002640	SC-12 (3)	Kubernetes endpoints must use approved organizational certificate and key pair to protect information in transit.	Passed

Appendix E: Ubuntu 24.04 (VMware vDefend – Malware Prevention Service - Service Virtual Machine)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the VMware vDefend – Malware Prevention Service – Service Virtual Machine appliances, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
UBTU-24-100010	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have the "systemd-timesyncd" package installed.	Passed
UBTU-24-100020	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have the "ntp" package installed.	Passed
UBTU-24-100030	IA-5 (1) (c) IA-5 (1).1 (v)	Ubuntu 24.04 LTS must not have the telnet package installed.	Passed
UBTU-24-100040	CM-7 CM-7.1 (ii) CM-7 a	Ubuntu 24.04 LTS must not have the rsh-server package installed.	Passed
UBTU-24-100200	SC-24 SC-24.1 (v)	Ubuntu 24.04 LTS must be configured to preserve log records from failure events.	Passed
UBTU-24-100400	AU-12 a AU-12.1 (ii) AU-12 a AU-12 c AU-12.1 (iv) AU-3 (1) AU-3 (1).1 (ii) AU-3 (1) AU-3 AU-3.1 AU-6 (4) AU-6 (4).1 AU-7 (1) AU-7 (1).1 AU-7 a AU-7 b	Ubuntu 24.04 LTS must have the "auditd" package installed.	Passed
UBTU-24-100410	AU-12 a AU-12.1 (ii) AU-12 a AU-12 c AU-12.1 (iv) AU-3 (1) AU-3 (1).1 (ii) AU-3 (1) AU-3 AU-3.1 AU-6 (4) AU-6 (4).1 AU-7 (1) AU-7 (1).1 AU-7 a AU-7 b	Ubuntu 24.04 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-24-100500	AC-3 (4) CM-7 (2) CM-7 (5) (b)	Ubuntu 24.04 LTS must have AppArmor installed.	Passed
UBTU-24-100510	CM-7 (2) AC-6 (10) CM-7 (5) (b)	Ubuntu 24.04 LTS must be configured to use AppArmor.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-100600	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must have the "libpam-pwquality" package installed.	Passed
UBTU-24-100800	SC-8 SC-8 (2)	Ubuntu 24.04 LTS must have SSH installed.	Passed
UBTU-24-100820	AC-17 (2) AC-17 (2).1 AC-17 (2) MA-4 (6) SC-8 (1)	Ubuntu 24.04 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.	Passed
UBTU-24-100830	AC-17 (2) AC-17 (2).1 MA-4 (6) SC-8 (1)	Ubuntu 24.04 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.	Passed
UBTU-24-100850	AC-17 (2) AC-17 (2).1	Ubuntu 24.04 LTS must configure the SSH client to use FIPS 140-3 approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Passed
UBTU-24-100860	AC-17 (2) AC-17 (2).1	Ubuntu 24.04 LTS SSH client must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-3 validated cryptographic hash algorithms.	Passed
UBTU-24-102000	AC-3 AC-3.1	Ubuntu 24.04 LTS when booted must require authentication upon booting into single-user and maintenance modes.	Passed
UBTU-24-102010	AU-14 (1) AU-14 (1).1	Ubuntu 24.04 LTS must initiate session audits at system startup.	Passed
UBTU-24-200040	AC-11 b AC-11.1 (iii)	Ubuntu 24.04 LTS must retain a user's session lock until the user reestablishes access using established identification and authentication procedures.	Passed
UBTU-24-200090	AC-17 (1) AC-17 (1).1	Ubuntu 24.04 LTS must monitor remote access methods.	Passed
UBTU-24-200580	AC-6 (8) AC-6 (9)	Ubuntu 24.04 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.	Passed
UBTU-24-200610	AC-7 a AC-7.1 (ii) AC-7 b	Ubuntu 24.04 LTS must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts have been made.	Passed
UBTU-24-300006	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library files must have mode 0755 or less permissive.	Passed
UBTU-24-300007	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library files must be owned by root.	Passed
UBTU-24-300008	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library directories must be owned by root.	Passed
UBTU-24-300009	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library files must be group-owned by root or a system account.	Passed
UBTU-24-300010	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS library directories must be group-owned by root.	Passed
UBTU-24-300011	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands set to a mode of 0755 or less permissive.	Passed
UBTU-24-300012	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands owned by root or a system account.	Passed
UBTU-24-300013	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands group-owned by root or a system account.	Passed
UBTU-24-300014		Ubuntu 24.04 LTS must prevent the use of dictionary words for passwords.	Passed
UBTU-24-300016	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must be configured so that when passwords are changed or new passwords are established, pwquality must be used.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-300022	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.	Passed
UBTU-24-300024	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must display the date and time of the last successful account logon upon logon.	Passed
UBTU-24-300027	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have accounts configured with blank or null passwords.	Passed
UBTU-24-300028	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not allow accounts configured in Pluggable Authentication Modules (PAM) with blank or null passwords.	Passed
UBTU-24-300030	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS default filesystem permissions must be defined in such a way that all authenticated users can read and modify only their own files.	Passed
UBTU-24-300031	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not allow unattended or automatic login via SSH.	Passed
UBTU-24-300039	IA-3	Ubuntu 24.04 LTS must disable automatic mounting of Universal Serial Bus (USB) mass storage driver.	Passed
UBTU-24-300041	CM-7 CM-7.1 (iii) CM-7 b	Ubuntu 24.04 LTS must be configured to prohibit or restrict the use of functions, ports, protocols, and/or services, as defined in the Ports, Protocols, and Services Management Category Assurance List (PPSM CAL) and vulnerability assessments.	Passed
UBTU-24-400000	IA-2 IA-2.1 IA-8 IA-8.1	Ubuntu 24.04 LTS must uniquely identify interactive users.	Passed
UBTU-24-400030	IA-2 (1) IA-2 (1).1 IA-2 (2) IA-2 (2).1	Ubuntu 24.04 LTS must implement smart card logins for multifactor authentication for local and network access to privileged and nonprivileged accounts over SSH.	Passed
UBTU-24-400220		Ubuntu 24.04 LTS must store only encrypted representations of passwords.	Passed
UBTU-24-400260		Ubuntu 24.04 LTS must enforce password complexity by requiring that at least one uppercase character be used.	Passed
UBTU-24-400270		Ubuntu 24.04 LTS must enforce password complexity by requiring that at least one lowercase character be used.	Passed
UBTU-24-400280		Ubuntu 24.04 LTS must enforce password complexity by requiring that at least one numeric character be used.	Passed
UBTU-24-400360	IA-5 (2) IA-5 (2).1 IA-5 (2) (a)	Ubuntu 24.04 LTS, for PKI-based authentication, SSSD must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	Passed
UBTU-24-400375	IA-5 (2) IA-5 (2).1 IA-5 (2) (a)	Ubuntu 24.04 LTS, for PKI-based authentication, Privileged Access Management (PAM) must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor.	Passed
UBTU-24-400380		Ubuntu 24.04 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.	Passed
UBTU-24-400400	IA-7 IA-7.1	Ubuntu 24.04 LTS must encrypt all stored passwords with a FIPS 140-3 approved cryptographic hashing algorithm.	Passed
UBTU-24-600030	SC-13	Ubuntu 24.04 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.	Passed
UBTU-24-600060	SC-23 (5)	Ubuntu 24.04 LTS must use DOD PKI-established certificate authorities (CAs) for verification of the establishment of protected sessions.	Passed
UBTU-24-600070	SC-24 SC-24.1 (iv)	Ubuntu 24.04 LTS must disable kernel core dumps.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-600090	SC-28 SC-28.1 SC-28 (1)	Ubuntu 24.04 LTS handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.	Passed
UBTU-24-600130	SC-3 SC-3.1 (ii)	Ubuntu 24.04 LTS must ensure only users who need access to security functions are part of sudo group.	Passed
UBTU-24-600140	SC-4 SC-4.1	Ubuntu 24.04 LTS must restrict access to the kernel message buffer.	Passed
UBTU-24-600150	SC-4 SC-4.1	Ubuntu 24.04 LTS must set a sticky bit on all public directories to prevent unauthorized and unintended information transferred via shared system resources.	Passed
UBTU-24-600180		Ubuntu 24.04 LTS must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.	Passed
UBTU-24-600190	SC-5 (2) SC-5 (2).1	Ubuntu 24.04 LTS must be configured to use TCP syncookies.	Passed
UBTU-24-700010	SI-11 b SI-11.1 (iii) SI-11 a	Ubuntu 24.04 LTS must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.	Passed
UBTU-24-700020	SI-11 b SI-11.1 (iii) SI-11 a	Ubuntu 24.04 LTS must generate system journal entries without revealing information that could be exploited by adversaries.	Passed
UBTU-24-700030	SI-11 b SI-11.1 (iii) SI-11 a	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is not accessible by unauthorized users.	Passed
UBTU-24-700040	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is owned by "root".	Passed
UBTU-24-700050	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is group-owned by "root".	Passed
UBTU-24-700060	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700070	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700080	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be owned by "root".	Passed
UBTU-24-700090	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be owned by "root"	Passed
UBTU-24-700100	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be group-owned by syslog.	Passed
UBTU-24-700110	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be owned by root.	Passed
UBTU-24-700130	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log/syslog file to be group-owned by adm.	Passed
UBTU-24-700140	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file to be owned by syslog.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-700150	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file with mode "0640" or less permissive.	Passed
UBTU-24-700300	SI-16	Ubuntu 24.04 LTS must implement nonexecutable data to protect its memory from unauthorized code execution.	Passed
UBTU-24-700310	SI-16	Ubuntu 24.04 LTS must implement address space layout randomization to protect its memory from unauthorized code execution.	Passed
UBTU-24-700400	SI-2 c	Ubuntu 24.04 LTS must be a vendor-supported release.	Passed
UBTU-24-900040	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must be configured so that audit configuration files are not write-accessible by unauthorized users.	Passed
UBTU-24-900050	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized accounts to own the audit configuration files.	Passed
UBTU-24-900060	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized groups to own the audit configuration files.	Passed
UBTU-24-900920	AU-4	Ubuntu 24.04 LTS must allocate audit record storage capacity to store at least one week's worth of audit records, when audit records are not immediately sent to a central audit record storage facility.	Passed
UBTU-24-901220	AU-8 b	Ubuntu 24.04 LTS must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	Passed
UBTU-24-901230	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools with a mode of "0755" or less permissive.	Passed
UBTU-24-901240	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools to be owned by root.	Passed
UBTU-24-901250	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure the audit tools to be group-owned by root.	Passed
UBTU-24-901260	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands set to a mode of "0755" or less permissive.	Passed
UBTU-24-901270	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands owned by root.	Passed
UBTU-24-901280	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands group-owned by root.	Passed
UBTU-24-901300	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured so that audit log files are not read or write-accessible by unauthorized users.	Passed
UBTU-24-901310	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured to permit only authorized users ownership of the audit log files.	Passed
UBTU-24-901380	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured so that the audit log directory is not write-accessible by unauthorized users.	Passed

Appendix F: Ubuntu 24.04 (NDR Sensor for VMware vDefend)

This appendix covers a list of controls where the Status = Passed.

For controls not listed in this appendix, exception findings are either not applicable, or have resolutions that are targeted in future roadmap. For these control findings, it is not supported for users to make changes to the NDR Sensor for VMware vDefend appliances, as these are vendor-hardened appliances.

Control ID	NIST 800-83	Title	Status
UBTU-24-100010	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have the "systemd-timesyncd" package installed.	Passed
UBTU-24-100020	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have the "ntp" package installed.	Passed
UBTU-24-100030	IA-5 (1) (c) IA-5 (1).1 (v)	Ubuntu 24.04 LTS must not have the telnet package installed.	Passed
UBTU-24-100040	CM-7 CM-7.1 (ii) CM-7 a	Ubuntu 24.04 LTS must not have the rsh-server package installed.	Passed
UBTU-24-100200	SC-24 SC-24.1 (v)	Ubuntu 24.04 LTS must be configured to preserve log records from failure events.	Passed
UBTU-24-100400	AU-12 a AU-12.1 (ii) AU-12 a AU-12 c AU-12.1 (iv) AU-3 (1) AU-3 (1).1 (ii) AU-3 (1) AU-3 AU-3.1 AU-6 (4) AU-6 (4).1 AU-7 (1) AU-7 (1).1 AU-7 a AU-7 b	Ubuntu 24.04 LTS must have the "auditd" package installed.	Passed
UBTU-24-100410	AU-12 a AU-12.1 (ii) AU-12 a AU-12 c AU-12.1 (iv) AU-3 (1) AU-3 (1).1 (ii) AU-3 (1) AU-3 AU-3.1 AU-6 (4) AU-6 (4).1 AU-7 (1) AU-7 (1).1 AU-7 a AU-7 b	Ubuntu 24.04 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-24-100500	AC-3 (4) CM-7 (2) CM-7 (5) (b)	Ubuntu 24.04 LTS must have AppArmor installed.	Passed
UBTU-24-100510	CM-7 (2) AC-6 (10) CM-7 (5) (b)	Ubuntu 24.04 LTS must be configured to use AppArmor.	Passed
UBTU-24-100600	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must have the "libpam-pwquality" package installed.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-100700	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must have the "chrony" package installed.	Passed
UBTU-24-100800	SC-8 SC-8 (2)	Ubuntu 24.04 LTS must have SSH installed.	Passed
UBTU-24-100810	SC-8 SC-8 (2)	Ubuntu 24.04 LTS must use SSH to protect the confidentiality and integrity of transmitted information.	Passed
UBTU-24-100820	AC-17 (2) AC-17 (2).1 AC-17 (2) MA-4 (6) SC-8 (1)	Ubuntu 24.04 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.	Passed
UBTU-24-100830	AC-17 (2) AC-17 (2).1 MA-4 (6) SC-8 (1)	Ubuntu 24.04 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.	Passed
UBTU-24-100840	AC-17 (2) AC-17 (2).1	Ubuntu 24.04 LTS SSH server must be configured to use only FIPS 140-3 validated key exchange algorithms.	Passed
UBTU-24-100850	AC-17 (2) AC-17 (2).1	Ubuntu 24.04 LTS must configure the SSH client to use FIPS 140-3 approved ciphers to prevent the unauthorized disclosure of information and/or detect changes to information during transmission.	Passed
UBTU-24-100860	AC-17 (2) AC-17 (2).1	Ubuntu 24.04 LTS SSH client must be configured to use only Message Authentication Codes (MACs) employing FIPS 140-3 validated cryptographic hash algorithms.	Passed
UBTU-24-102000	AC-3 AC-3.1	Ubuntu 24.04 LTS when booted must require authentication upon booting into single-user and maintenance modes.	Passed
UBTU-24-102010	AU-14 (1) AU-14 (1).1	Ubuntu 24.04 LTS must initiate session audits at system startup.	Passed
UBTU-24-200040	AC-11 b AC-11.1 (iii)	Ubuntu 24.04 LTS must retain a user's session lock until the user reestablishes access using established identification and authentication procedures.	Passed
UBTU-24-200090	AC-17 (1) AC-17 (1).1	Ubuntu 24.04 LTS must monitor remote access methods.	Passed
UBTU-24-300011	CM-5 (6) CM-5 (6).1	Ubuntu 24.04 LTS must have system commands set to a mode of 0755 or less permissive.	Passed
UBTU-24-300022	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must be configured so that remote X connections are disabled, unless to fulfill documented and validated mission requirements.	Passed
UBTU-24-300027	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not have accounts configured with blank or null passwords.	Passed
UBTU-24-300028	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must not allow accounts configured in Pluggable Authentication Modules (PAM) with blank or null passwords.	Passed
UBTU-24-400030	CM-6 b CM-6.1 (iv)	Ubuntu 24.04 LTS must implement smart card logins for multifactor authentication for local and network access to privileged and nonprivileged accounts over SSH.	Passed
UBTU-24-400220		Ubuntu 24.04 LTS must store only encrypted representations of passwords.	Passed
UBTU-24-400400	IA-7 IA-7.1	Ubuntu 24.04 LTS must encrypt all stored passwords with a FIPS 140-3 approved cryptographic hashing algorithm.	Passed
UBTU-24-600000	SC-10 SC-10.1 (ii)	Ubuntu 24.04 LTS must immediately terminate all network connections associated with SSH traffic after a period of inactivity.	Passed
UBTU-24-600010	SC-10 SC-10.1 (ii)	Ubuntu 24.04 LTS must immediately terminate all network connections associated with SSH traffic at the end of the session or after 10 minutes of inactivity.	Passed
UBTU-24-600060	SC-23 (5)	Ubuntu 24.04 LTS must use DOD PKI-established certificate authorities (CAs) for verification of the establishment of protected sessions.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-600070	SC-24 SC-24.1 (iv)	Ubuntu 24.04 LTS must disable kernel core dumps.	Passed
UBTU-24-600090	SC-28 SC-28.1 SC-28 (1)	Ubuntu 24.04 LTS handling data requiring "data at rest" protections must employ cryptographic mechanisms to prevent unauthorized disclosure and modification of the information at rest.	Passed
UBTU-24-600130	SC-3 SC-3.1 (ii)	Ubuntu 24.04 LTS must ensure only users who need access to security functions are part of sudo group.	Passed
UBTU-24-600140	SC-4 SC-4.1	Ubuntu 24.04 LTS must restrict access to the kernel message buffer.	Passed
UBTU-24-600160		Ubuntu 24.04 LTS must compare internal information system clocks at least every 24 hours with an authoritative time server.	Passed
UBTU-24-600180		Ubuntu 24.04 LTS must synchronize internal information system clocks to the authoritative time source when the time difference is greater than one second.	Passed
UBTU-24-600190	SC-5 (2) SC-5 (2).1	Ubuntu 24.04 LTS must be configured to use TCP syncookies.	Passed
UBTU-24-600230	SC-8	Ubuntu 24.04 LTS must disable all wireless network adapters.	Passed
UBTU-24-700040	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is owned by "root".	Passed
UBTU-24-700050	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must be configured so that the "journalctl" command is group-owned by "root".	Passed
UBTU-24-700060	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700070	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be group-owned by "systemd-journal".	Passed
UBTU-24-700080	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the directories used by the system journal to be owned by "root".	Passed
UBTU-24-700090	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the files used by the system journal to be owned by "root"	Passed
UBTU-24-700100	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be group-owned by syslog.	Passed
UBTU-24-700110	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log directory to be owned by root.	Passed
UBTU-24-700130	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure the /var/log/syslog file to be group-owned by adm.	Passed
UBTU-24-700140	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file to be owned by syslog.	Passed
UBTU-24-700150	SI-11 c SI-11.1 (iv) SI-11 b	Ubuntu 24.04 LTS must configure /var/log/syslog file with mode "0640" or less permissive.	Passed
UBTU-24-700300	SI-16	Ubuntu 24.04 LTS must implement nonexecutable data to protect its memory from unauthorized code execution.	Passed
UBTU-24-700310	SI-16	Ubuntu 24.04 LTS must implement address space layout randomization to protect its memory from unauthorized code execution.	Passed

Control ID	NIST 800-83	Title	Status
UBTU-24-700400	SI-2 c	Ubuntu 24.04 LTS must be a vendor-supported release.	Passed
UBTU-24-900040	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must be configured so that audit configuration files are not write-accessible by unauthorized users.	Passed
UBTU-24-900050	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized accounts to own the audit configuration files.	Passed
UBTU-24-900060	AU-12 b AU-12.1 (iii)	Ubuntu 24.04 LTS must permit only authorized groups to own the audit configuration files.	Passed
UBTU-24-900920	AU-4	Ubuntu 24.04 LTS must allocate audit record storage capacity to store at least one week's worth of audit records, when audit records are not immediately sent to a central audit record storage facility.	Passed
UBTU-24-901220	AU-8 b	Ubuntu 24.04 LTS must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	Passed
UBTU-24-901230	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools with a mode of "0755" or less permissive.	Passed
UBTU-24-901240	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure audit tools to be owned by root.	Passed
UBTU-24-901250	AU-9 AU-9.1	Ubuntu 24.04 LTS must configure the audit tools to be group-owned by root.	Passed
UBTU-24-901260	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands set to a mode of "0755" or less permissive.	Passed
UBTU-24-901270	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands owned by root.	Passed
UBTU-24-901280	AU-9 AU-9.1	Ubuntu 24.04 LTS must have directories that contain system commands group-owned by root.	Passed
UBTU-24-901310	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured to permit only authorized users ownership of the audit log files.	Passed
UBTU-24-901380	AU-9 AU-9.1	Ubuntu 24.04 LTS must be configured so that the audit log directory is not write-accessible by unauthorized users.	Passed

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 Oct-25