



VMware Cloud Foundation – STIG Hardening Overview

vSphere Kubernetes Service 3.5+v1.34.1
(Photon OS 5.0)

Table of contents

| | |
|---|----|
| Revision History..... | 3 |
| Overview | 4 |
| Applicability..... | 4 |
| Disclaimer..... | 4 |
| vSphere Kubernetes release Compliance | 5 |
| Photon OS 5.0 Compliance: Overall | 5 |
| Photon OS 5.0 Compliance: Exceptions | 5 |
| Control Plane Kubernetes Compliance: Overall | 5 |
| Control Plane Kubernetes Compliance: Exceptions | 6 |
| Control Plane Kubernetes Compliance: Not Applicable | 6 |
| Worker Node Kubernetes Compliance: Overall | 7 |
| Worker Node Kubernetes Compliance: Exceptions | 8 |
| Worker Node Kubernetes Compliance: Not Applicable | 8 |
| Frequently Asked Questions..... | 9 |
| Appendix: Full Control List – Photon OS 5.0..... | 10 |
| Appendix: Full Control List – Control Plane Kubernetes..... | 15 |
| Appendix: Full Control List – Worker Node Kubernetes..... | 19 |

Revision History

| Date | Description of Change |
|---------------|-----------------------|
| November 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, VCF vSphere Supervisor is evaluated against the following standards:

- DISA Kubernetes Security Technical Implementation Guide, Version 2 Release 3
- VMware Cloud Foundation Photon OS 5.0 STIG Readiness Guide, Version 3 Release 1

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:

- vSphere Kubernetes Service (VKS) 3.5
- VKr 1.34.1 (Photon OS 5.0)/v1.34.1---vmware.1-fips-vkr.4

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.

vSphere Kubernetes release Compliance

vSphere Kubernetes Service (VKS) clusters provides self-service lifecycle management of Kubernetes workload clusters. With VKS, you can provision CNCF certified, upstream conformant Kubernetes clusters, maintaining compatibility and support with the larger Kubernetes ecosystem. For more information, please refer to the VKS Product Documentation.

vSphere Kubernetes release node images have had their operating systems hardened by default. Any security patches, bug fixes, or updates to the hardening will be released as part of the vSphere Kubernetes release image.

Photon OS 5.0 Compliance: Overall

The vSphere Kubernetes Release are built on Photon OS 5.0. The results below are based on auditing the appliances for both control plane and worker nodes against the latest Photon OS 5.0 STIG Readiness Guide release.

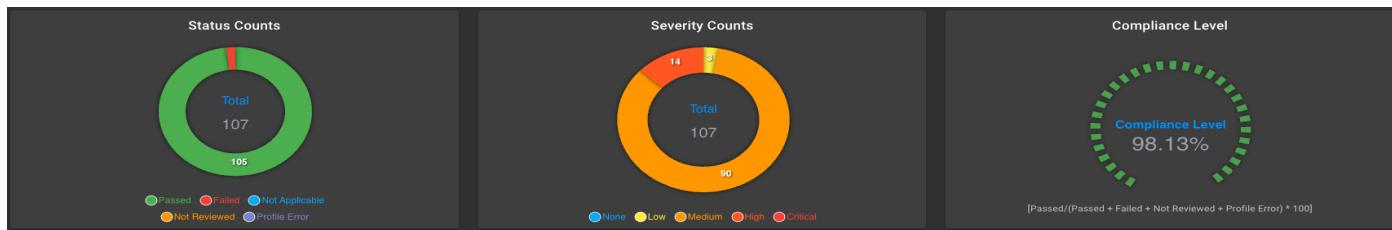


Figure 1: Overall Compliance for Photon OS 5.0

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

Photon OS 5.0 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 |
|----------------|-------------|--|---|
| PHTN-50-000133 | IA-11 | The Photon operating system must require users to reauthenticate for privilege escalation. | There are no users apart from vmware-system-user with sudo privileges and NOPASSWD defined to audit. vmware-system-user is enabled only for internal debugging purpose. |
| PHTN-50-000231 | CM- 6 b | The Photon operating system must not perform IPv4 packet forwarding. | Packet forwarding is required for Kubernetes to route packets for pods. |

Control Plane Kubernetes Compliance: Overall

The results below are based on auditing the control plane node against the latest Kubernetes STIG release.

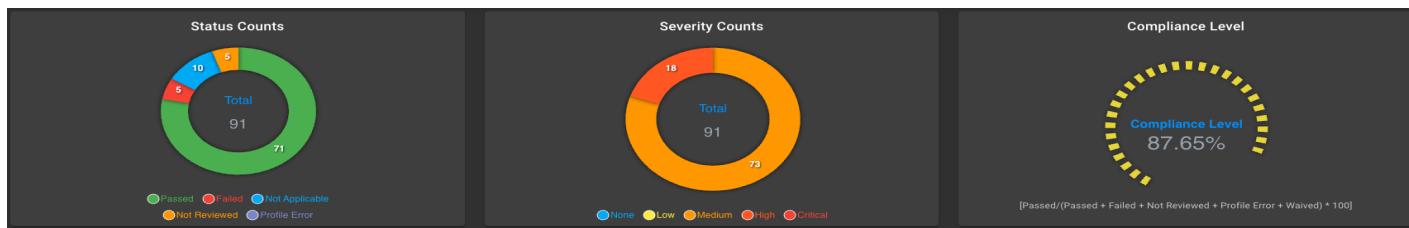


Figure 2: Control Plane Node Compliance for Kubernetes

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

Control Plane Kubernetes 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 |
|----------------|--|--|---|
| CNTR-K8-000290 | CM-6 b | User-managed resources must be created in dedicated namespaces. | 'service/supervisor' is a resources required by the Supervisor and is not a user-managed resource created in a dedicated namespace. |
| CNTR-K8-000360 | AC-3 | The Kubernetes API server must have anonymous authentication disabled. | Anonymous authentication is enabled for health checks and limited to these actions by RBAC policies. |
| CNTR-K8-000700 | AC-2 (4), AU-3 a, AU-3 b, AU-3 c, AU-3 d, AU-3 e, AU-3 (1), AU-12 c, AU-3 f, AU-3 (2), AC-16 a | Kubernetes API Server must generate audit records that identify what type of event has occurred, identify the source of the event, contain the event results, identify any users, and identify any containers associated with the event. | Auditing is enabled but tailored to limit high volume low value records. |
| CNTR-K8-001460 | SC-23 | Kubernetes Kubelet must enable tlsPrivateKeyFile for client authentication to secure service. | The kubelet uses auto generated TLS certificates configured by kubeadm for secure client authentication. While custom certificates are not supported, TLS is enabled by default securing the service. |
| CNTR-K8-001470 | SC-23 | Kubernetes Kubelet must enable tlsCertFile for client authentication to secure service. | The kubelet uses auto generated TLS certificates configured by kubeadm for secure client authentication. While custom certificates are not supported, TLS is enabled by default securing the service. |

Control Plane Kubernetes Compliance: Not Applicable

Controls listed in this Not Applicable table are not applicable in this scenario or require manual review post deployment.

| Control ID | NIST 800-83 | Title | Justification |
|----------------|-------------|--|--|
| CNTR-K8-000320 | AC-3 | The Kubernetes API server must have the insecure port flag disabled. | The Kubernetes API server insecure-port flag is no longer present in any supported Kubernetes version so this control is no longer valid. See: https://github.com/kubernetes/kubernetes/pull/102121 |
| CNTR-K8-000400 | A-3 | Kubernetes Worker Nodes must not have sshd service running. | This control is applicable only to worker nodes and does not apply to the control plane nodes of the cluster. |
| CNTR-K8-000410 | AC-3 | Kubernetes Worker Nodes must not have the sshd service enabled. | This control is applicable only to worker nodes and does not apply to the control plane nodes of the cluster. |
| CNTR-K8-000440 | AC-3 | The Kubernetes kubelet staticPodPath must not enable static pods. | The Kubernetes components run as containers using static pods on the control plane nodes. Workloads are not allowed to run on these nodes. |

| Control ID | NIST 800-83 | Title | Justification |
|----------------|-------------|---|---|
| CNTR-K8-000460 | AC-3 | Kubernetes DynamicKubeletConfig must not be enabled. | DynamicKubeletConfig removed in v1.24 and greater and is not applicable to current version. |
| CNTR-K8-000920 | 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). | No known banned ports in use. Ports and protocols used in the product are available at https://ports.broadcom.com/ and can be used by customers to document against the PPSM CAL. |
| CNTR-K8-000930 | 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). | No known banned ports in use. Ports and protocols used in the product are available at https://ports.broadcom.com/ and can be used by customers to document against the PPSM CAL. |
| CNTR-K8-000940 | 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). | No known banned ports in use. Ports and protocols used in the product are available at https://ports.broadcom.com/ and can be used by customers to document against the PPSM CAL. |
| CNTR-K8-000950 | 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). | No known banned ports in use. Ports and protocols used in the product are available at https://ports.broadcom.com/ and can be used by customers to document against the PPSM CAL. |
| CNTR-K8-001360 | SC-2 | Kubernetes must separate user functionality. | This is a manual review. User workloads are not allowed to run on the control plane nodes and only contain system level pods. |
| CNTR-K8-002001 | AC-16 a | Kubernetes must enable PodSecurity admission controller on static pods and Kubelets. | PodSecurity is no longer a feature gate in 1.28+ and is not applicable to current version. |
| CNTR-K8-002010 | AC-16 a | Kubernetes must have a pod security policy set. | Pod Security Policy is deprecated in version 1.25+ and is not applicable to current version. |
| CNTR-K8-002700 | SI-4 d | Kubernetes must remove old components after updated versions have been installed. | Only a single version of Kubernetes is ever present. When updates are performed they are done in a rolling fashion with new appliances containing only the new Kubernetes version. |
| CNTR-K8-003140 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must have file permissions set to 644 or more restrictive. | Kube Proxy is running as a container and the configuration file does not exist on the host OS. |
| CNTR-K8-003150 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must be owned by root. | Kube Proxy is running as a container and the configuration file does not exist on the host OS. |

Worker Node Kubernetes Compliance: Overall

The results below are based on auditing the worker node against the latest Kubernetes STIG release.

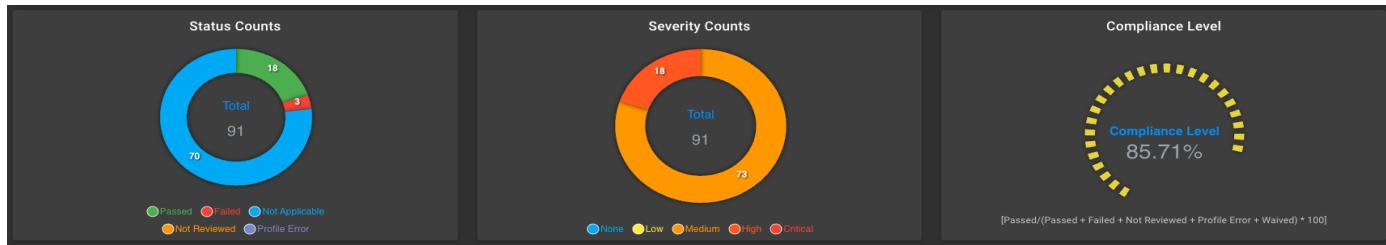


Figure 3: Worker Node Compliance for Kubernetes

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

Worker Node Kubernetes 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 |
|----------------|-------------|---|---|
| CNTR-K8-000400 | AC-3 | Kubernetes Worker Nodes must not have sshd service running. | SSH is currently enabled on worker nodes to support product functionality and is restricted only to privileged users. |
| CNTR-K8-000410 | AC-3 | Kubernetes Worker Nodes must not have the sshd service enabled. | SSH is currently enabled on worker nodes to support product functionality and is restricted only to privileged users. |
| CNTR-K8-000440 | AC-3 | The Kubernetes kubelet staticPodPath must not enable static pods. | There are no static pods running on worker nodes. By default, staticPodPath is set to /etc/kubernetes/manifests. |

Worker Node Kubernetes Compliance: Not Applicable

Not Applicable controls for the worker node are listed in the appendix and not here due to the large number of controls that do not apply to worker nodes.

Frequently Asked Questions

Can customers make changes to the vSphere Kubernetes Release (VKr) images or appliances?

No. Due to the immutable nature of vSphere Kubernetes Release (VKr) images any changes would not be persistent. Modification to images and components is not supported.

Where can I find the Kubernetes STIG?

The Kubernetes STIG may be found at:

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

Where can I find the Photon OS 5.0 STIG Readiness Guide?

The Photon OS 5.0 STIG Readiness guide may be found at:

<https://github.com/vmware/dod-compliance-and-automation/tree/master/photon/5.0/docs>

Is there a compliance report for vSphere Supervisor?

A report will be available in a separate document and those images have a separate lifecycle from vSphere Kubernetes Release (VKr).

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 – Photon OS 5.0

| Control ID | NIST 800-83 | Title | Status |
|----------------|---|---|--------|
| PHTN-50-000003 | AC-2 (4), AU-12 c | The Photon operating system must audit all account creations. | Passed |
| PHTN-50-000004 | AC-7 a | The Photon operating system must enforce the limit of three consecutive invalid logon attempts by a user during a 15-minute time period. | Passed |
| PHTN-50-000005 | AC-8 a, AC-8 c 1, AC-8 c 2, AC-8 c 3 | The Photon operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting local or remote access to the system. | Passed |
| PHTN-50-000007 | AC-10 | The Photon operating system must limit the number of concurrent sessions to ten for all accounts and/or account types. | Passed |
| PHTN-50-000012 | AC-17 (1) | The Photon operating system must monitor remote access logins. | Passed |
| PHTN-50-000013 | AC-17 (2), MA-4 (6), SC-8, SC-8 (2) | The Photon operating system must have the OpenSSL FIPS provider installed to protect the confidentiality of remote access sessions. | Passed |
| PHTN-50-000014 | AU-3 a | The Photon operating system must configure auditd to log to disk. | Passed |
| PHTN-50-000016 | AU-12 a, AU-3 (1), AU-3 c, AU-3 d, AU-3 e, AU-3 f, CM-5 (1) (b) | The Photon operating system must enable the auditd service. | Passed |
| PHTN-50-000019 | AC-6 (8), AU-3 (1) | The Photon operating system must be configured to audit the execution of privileged functions. | Passed |
| PHTN-50-000021 | AU-5 (2), AU-5 a | The Photon operating system must alert the ISSO and SA in the event of an audit processing failure. | Passed |
| PHTN-50-000026 | AU-9 a | The Photon operating system must protect audit logs from unauthorized access. | Passed |
| PHTN-50-000030 | AU-12 b | The Photon operating system must allow only authorized users to configure the auditd service. | Passed |
| PHTN-50-000031 | AU-12 c | The Photon operating system must generate audit records when successful/unsuccessful attempts to access privileges occur. | Passed |
| PHTN-50-000035 | IA-5 (1) (h) | The Photon operating system must enforce password complexity by requiring that at least one uppercase character be used. | Passed |
| PHTN-50-000036 | IA-5 (1) (h) | The Photon operating system must enforce password complexity by requiring that at least one lowercase character be used. | Passed |
| PHTN-50-000037 | IA-5 (1) (h) | The Photon operating system must enforce password complexity by requiring that at least one numeric character be used. | Passed |
| PHTN-50-000038 | IA-5 (1) (h) | The Photon operating system must require the change of at least eight characters when passwords are changed. | Passed |
| PHTN-50-000039 | IA-5 (1) (d) | The operating system must store only encrypted representations of passwords. | Passed |
| PHTN-50-000040 | IA-5 (1) (c) | The Photon operating system must not have the telnet package installed. | Passed |
| PHTN-50-000041 | IA-5 (1) (h) | The Photon operating system must enforce one day as the minimum password lifetime. | Passed |
| PHTN-50-000042 | IA-5 (1) (h) | The Photon operating systems must enforce a 90-day maximum password lifetime restriction. | Passed |
| PHTN-50-000044 | IA-5 (1) (h) | The Photon operating system must enforce a minimum 15-character password length. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|---------------------------------------|---|--------|
| PHTN-50-000046 | AC-3 | The Photon operating system must require authentication upon booting into single-user and maintenance modes. | Passed |
| PHTN-50-000047 | CM-7 a, IA-3 | The Photon operating system must disable unnecessary kernel modules. | Passed |
| PHTN-50-000049 | IA-2 | The Photon operating system must not have duplicate User IDs (UIDs). | Passed |
| PHTN-50-000059 | IA-7 | The Photon operating system must use mechanisms meeting the requirements of applicable federal laws, Executive orders, directives, policies, regulations, standards, and guidance for authentication to a cryptographic module. | Passed |
| PHTN-50-000067 | SC-4 | The Photon operating system must restrict access to the kernel message buffer. | Passed |
| PHTN-50-000068 | SC-5 (2), SC-5 a | The Photon operating system must be configured to use TCP syncookies. | Passed |
| PHTN-50-000069 | MA-4 (7), SC-10 | The Photon operating system must terminate idle Secure Shell (SSH) sessions after 15 minutes. | Passed |
| PHTN-50-000073 | SI-11 a | The Photon operating system /var/log directory must be restricted. | Passed |
| PHTN-50-000074 | SI-11 b | The Photon operating system must reveal error messages only to authorized users. | Passed |
| PHTN-50-000076 | AC-2 (4) | The Photon operating system must audit all account modifications. | Passed |
| PHTN-50-000078 | AC-2 (4) | The Photon operating system must audit all account removal actions. | Passed |
| PHTN-50-000079 | AC-17 (2) | The Photon operating system must implement only approved ciphers to protect the integrity of remote access sessions. | Passed |
| PHTN-50-000080 | AU-14 (1) | The Photon operating system must initiate session audits at system start-up. | Passed |
| PHTN-50-000082 | AU-9, AU-9 a | The Photon operating system must protect audit tools from unauthorized access. | Passed |
| PHTN-50-000085 | CM-5 (6) | The Photon operating system must limit privileges to change software resident within software libraries. | Passed |
| PHTN-50-000086 | IA-5 (1) (h) | The Photon operating system must enforce password complexity by requiring that at least one special character be used. | Passed |
| PHTN-50-000092 | AU-9 (3) | The Photon operating system must use cryptographic mechanisms to protect the integrity of audit tools. | Passed |
| PHTN-50-000093 | AC-12 | The operating system must automatically terminate a user session after inactivity time-outs have expired. | Passed |
| PHTN-50-000105 | AC-6 (10) | The Photon operating system must enable symlink access control protection in the kernel. | Passed |
| PHTN-50-000107 | AC-2 (4), AC-6 (9), AU-12 c, MA-3 (5) | The Photon operating system must audit the execution of privileged functions. | Passed |
| PHTN-50-000108 | AC-7 b | The Photon operating system must automatically lock an account until the locked account is released by an administrator when three unsuccessful logon attempts in 15 minutes occur. | Passed |
| PHTN-50-000110 | AU-4 | The Photon operating system must allocate audit record storage capacity to store audit records when audit records are not immediately sent to a central audit record storage facility. | Passed |
| PHTN-50-000112 | AU-5 (1) | The Photon operating system must immediately notify the SA and ISSO when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. | Passed |
| PHTN-50-000127 | CM-3 (5), SI-6 b | The Photon operating system must install AIDE to detect changes to baseline configurations. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|----------------------|--|--------|
| PHTN-50-000130 | CM-14 | The Photon operating system TDNF package management tool must cryptographically verify the authenticity of all software packages during installation. | Passed |
| PHTN-50-000133 | IA-11 | The Photon operating system must require users to reauthenticate for privilege escalation. | Failed |
| PHTN-50-000160 | SI-16 | The Photon operating system must implement address space layout randomization to protect its memory from unauthorized code execution. | Passed |
| PHTN-50-000161 | SI-2 (6) | The Photon operating system must remove all software components after updated versions have been installed. | Passed |
| PHTN-50-000173 | AU-12 c | The Photon operating system must generate audit records when successful/unsuccessful logon attempts occur. | Passed |
| PHTN-50-000175 | AU-12 c | The Photon operating system must be configured to audit the loading and unloading of dynamic kernel modules. | Passed |
| PHTN-50-000182 | SC-13 b | The Photon operating system must implement NIST FIPS-validated cryptography 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 |
| PHTN-50-000184 | CM-6 b, IA-5 (1) (b) | The Photon operating system must prevent the use of dictionary words for passwords. | Passed |
| PHTN-50-000185 | CM-6 b | The Photon operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt in login.defs. | Passed |
| PHTN-50-000186 | CM-6 b | The Photon operating system must ensure audit events are flushed to disk at proper intervals. | Passed |
| PHTN-50-000187 | CM-6 b | The Photon operating system must define default permissions for all authenticated users in such a way that the user can only read and modify their own files. | Passed |
| PHTN-50-000188 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disallow HostbasedAuthentication. | Passed |
| PHTN-50-000192 | AC-7 a | The Photon operating system must be configured to use the pam_faillock.so module. | Passed |
| PHTN-50-000193 | AC-7 a | The Photon operating system must prevent leaking information of the existence of a user account. | Passed |
| PHTN-50-000194 | AC-7 a | The Photon operating system must audit logon attempts for unknown users. | Passed |
| PHTN-50-000195 | AC-7 a | The Photon operating system must include root when automatically locking an account until the locked account is released by an administrator when three unsuccessful logon attempts occur during a 15-minute time period. | Passed |
| PHTN-50-000196 | AC-7 a | The Photon operating system must persist lockouts between system reboots. | Passed |
| PHTN-50-000197 | IA-5 (1) (h) | The Photon operating system must be configured to use the pam_pwquality.so module. | Passed |
| PHTN-50-000199 | CM-14 | The Photon operating system TDNF package management tool must cryptographically verify the authenticity of all software packages during installation for all repos. | Passed |
| PHTN-50-000200 | AC-17 (1) | The Photon operating system must configure the Secure Shell (SSH) SyslogFacility. | Passed |
| PHTN-50-000201 | AC-17 (1) | The Photon operating system must enable Secure Shell (SSH) authentication logging. | Passed |
| PHTN-50-000203 | SC-10 | The Photon operating system must terminate idle Secure Shell (SSH) sessions. | Passed |
| PHTN-50-000204 | AC-2 (4), AU-12 c | The Photon operating system must audit all account modifications. | Passed |
| PHTN-50-000206 | CM-6 b | The Photon operating system must enforce a delay of at least four seconds between logon prompts following a failed logon attempt. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|---|--------|
| PHTN-50-000207 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disallow authentication with an empty password. | Passed |
| PHTN-50-000208 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disable user environment processing. | Passed |
| PHTN-50-000209 | CM-6 b | The Photon operating system must create a home directory for all new local interactive user accounts. | Passed |
| PHTN-50-000210 | CM-6 b | The Photon operating system must disable the debug-shell service. | Passed |
| PHTN-50-000211 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disallow Generic Security Service Application Program Interface (GSSAPI) authentication. | Passed |
| PHTN-50-000212 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disable X11 forwarding. | Passed |
| PHTN-50-000213 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to perform strict mode checking of home directory configuration files. | Passed |
| PHTN-50-000214 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disallow Kerberos authentication. | Passed |
| PHTN-50-000215 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to disallow compression of the encrypted session stream. | Passed |
| PHTN-50-000216 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to display the last login immediately after authentication. | Passed |
| PHTN-50-000217 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to ignore user-specific trusted hosts lists. | Passed |
| PHTN-50-000218 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to ignore user-specific known_host files. | Passed |
| PHTN-50-000219 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to limit the number of allowed login attempts per connection. | Passed |
| PHTN-50-000220 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to restrict AllowTcpForwarding. | Passed |
| PHTN-50-000221 | CM-6 b | The Photon operating system must configure Secure Shell (SSH) to restrict LoginGraceTime. | Passed |
| PHTN-50-000222 | CM-6 b | The Photon operating system must be configured so that the x86 Ctrl-Alt-Delete key sequence is disabled on the command line. | Passed |
| PHTN-50-000223 | CM-6 b | The Photon operating system must not forward IPv4 or IPv6 source-routed packets. | Passed |
| PHTN-50-000224 | CM-6 b | The Photon operating system must not respond to IPv4 Internet Control Message Protocol (ICMP) echoes sent to a broadcast address. | Passed |
| PHTN-50-000225 | CM-6 b | The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted. | Passed |
| PHTN-50-000226 | CM-6 b | The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) secure redirect messages from being accepted. | Passed |
| PHTN-50-000227 | CM-6 b | The Photon operating system must not send IPv4 Internet Control Message Protocol (ICMP) redirects. | Passed |
| PHTN-50-000228 | CM-6 b | The Photon operating system must log IPv4 packets with impossible addresses. | Passed |
| PHTN-50-000229 | CM-6 b | The Photon operating system must use a reverse-path filter for IPv4 network traffic. | Passed |
| PHTN-50-000231 | CM-6 b | The Photon operating system must not perform IPv4 packet forwarding. | Failed |
| PHTN-50-000232 | CM-6 b | The Photon operating system must send TCP timestamps. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|--|--------|
| PHTN-50-000233 | CM-6 b | The Photon operating system must be configured to protect the Secure Shell (SSH) public host key from unauthorized modification. | Passed |
| PHTN-50-000234 | CM-6 b | The Photon operating system must be configured to protect the Secure Shell (SSH) private host key from unauthorized access. | Passed |
| PHTN-50-000235 | CM-6 b | The Photon operating system must enforce password complexity on the root account. | Passed |
| PHTN-50-000236 | CM-6 b | The Photon operating system must disable systemd fallback DNS. | Passed |
| PHTN-50-000237 | CM-3 (5) | The Photon operating system must configure AIDE to detect changes to baseline configurations. | Passed |
| PHTN-50-000239 | AC-17 (2) | The Photon operating system must implement only approved Message Authentication Codes (MACs) to protect the integrity of remote access sessions. | Passed |
| PHTN-50-000241 | CM-6 b | The Photon operating system must install rsyslog for offloading of audit logs. | Passed |
| PHTN-50-000242 | CM-6 b | The Photon operating system must enable the rsyslog service. | Passed |
| PHTN-50-000244 | CM-6 b | The Photon operating system must enable hardlink access control protection in the kernel. | Passed |
| PHTN-50-000245 | CM-6 b | The Photon operating system must mount /tmp securely. | Passed |
| PHTN-50-000246 | CM-6 b | The Photon operating system must restrict core dumps. | Passed |
| PHTN-50-000247 | CM-6 b | The Photon operating system must not allow empty passwords. | Passed |

Appendix: Full Control List – Control Plane Kubernetes

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|---|----------------|
| CNTR-K8-000150 | AC-17 (2) | The Kubernetes Controller Manager must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Passed |
| CNTR-K8-000160 | AC-17 (2) | The Kubernetes Scheduler must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Passed |
| CNTR-K8-000170 | AC-17 (2) | The Kubernetes API Server must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Passed |
| CNTR-K8-000180 | AC-17 (2) | The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination. | Passed |
| CNTR-K8-000190 | AC-17 (2) | The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination. | Passed |
| CNTR-K8-000220 | AC-2 (1) | The Kubernetes Controller Manager must create unique service accounts for each work payload. | Passed |
| CNTR-K8-000270 | AC-3 | The Kubernetes API Server must enable Node, RBAC as the authorization mode. | Passed |
| CNTR-K8-000290 | CM-6 b | User-managed resources must be created in dedicated namespaces. | Failed |
| CNTR-K8-000300 | AC-3 | The Kubernetes Scheduler must have secure binding. | Passed |
| CNTR-K8-000310 | AC-3 | The Kubernetes Controller Manager must have secure binding. | Passed |
| CNTR-K8-000320 | AC-3 | The Kubernetes API server must have the insecure port flag disabled. | Not Applicable |
| CNTR-K8-000330 | AC-3 | The Kubernetes Kubelet must have the "readOnlyPort" flag disabled. | Passed |
| CNTR-K8-000340 | AC-3 | The Kubernetes API server must have the insecure bind address not set. | Passed |
| CNTR-K8-000350 | AC-3 | The Kubernetes API server must have the secure port set. | Passed |
| CNTR-K8-000360 | AC-3 | The Kubernetes API server must have anonymous authentication disabled. | Failed |
| CNTR-K8-000370 | AC-3 | The Kubernetes Kubelet must have anonymous authentication disabled. | Passed |
| CNTR-K8-000380 | AC-3 | The Kubernetes kubelet must enable explicit authorization. | Passed |
| CNTR-K8-000400 | AC-3 | Kubernetes Worker Nodes must not have sshd service running. | Not Applicable |
| CNTR-K8-000410 | AC-3 | Kubernetes Worker Nodes must not have the sshd service enabled. | Not Applicable |
| CNTR-K8-000420 | AC-3 | Kubernetes dashboard must not be enabled. | Passed |
| CNTR-K8-000430 | AC-3 | Kubernetes Kubectl cp command must give expected access and results. | Passed |
| CNTR-K8-000440 | AC-3 | The Kubernetes kubelet staticPodPath must not enable static pods. | Not Applicable |
| CNTR-K8-000450 | AC-3 | Kubernetes DynamicAuditing must not be enabled. | Passed |
| CNTR-K8-000460 | AC-3 | Kubernetes DynamicKubeletConfig must not be enabled. | Not Applicable |
| CNTR-K8-000470 | AC-3 | The Kubernetes API server must have Alpha APIs disabled. | Passed |
| CNTR-K8-000610 | AU-14 (1) | The Kubernetes API Server must have an audit log path set. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|--|--|--------------|
| CNTR-K8-000700 | AC-2 (4), AU-3 a, AU-3 b, AU-3 c, AU-3 d, AU-3 e, AU-3 (1), AU-12 c, AU-3 f, AU-3 (2), AC-16 a | Kubernetes API Server must generate audit records that identify what type of event has occurred, identify the source of the event, contain the event results, identify any users, and identify any containers associated with the event. | Failed |
| CNTR-K8-000850 | CM-5 (6) | Kubernetes Kubelet must deny hostname override. | Passed |
| CNTR-K8-000860 | CM-5 (6) | The Kubernetes manifests must be owned by root. | Passed |
| CNTR-K8-000880 | CM-5 (6) | The Kubernetes KubeletConfiguration file must be owned by root. | Passed |
| CNTR-K8-000890 | CM-5 (6) | The Kubernetes KubeletConfiguration files must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-000900 | CM-5 (6), CM-6 b | The Kubernetes manifest files must have least privileges. | Passed |
| CNTR-K8-000910 | CM-7 a | Kubernetes Controller Manager must disable profiling. | Passed |
| CNTR-K8-000920 | 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). | Not Reviewed |
| CNTR-K8-000930 | 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). | Not Reviewed |
| CNTR-K8-000940 | 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). | Not Reviewed |
| CNTR-K8-000950 | 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). | Not Reviewed |
| CNTR-K8-000960 | CM-7 b | The Kubernetes cluster must use non-privileged host ports for user pods. | Passed |
| CNTR-K8-001160 | IA-5 (1) (d), IA-5 (1) (c) | Secrets in Kubernetes must not be stored as environment variables. | Passed |
| CNTR-K8-001300 | SC-10 | Kubernetes Kubelet must not disable timeouts. | Passed |
| CNTR-K8-001360 | SC-2 | Kubernetes must separate user functionality. | Not Reviewed |
| CNTR-K8-001400 | SC-23 | The Kubernetes API server must use approved cipher suites. | Passed |
| CNTR-K8-001410 | SC-23 | Kubernetes API Server must have the SSL Certificate Authority set. | Passed |
| CNTR-K8-001420 | SC-23 | Kubernetes Kubelet must have the SSL Certificate Authority set. | Passed |
| CNTR-K8-001430 | SC-23 | Kubernetes Controller Manager must have the SSL Certificate Authority set. | Passed |
| CNTR-K8-001440 | SC-23 | Kubernetes API Server must have a certificate for communication. | Passed |
| CNTR-K8-001450 | SC-23 | Kubernetes etcd must enable client authentication to secure service. | Passed |
| CNTR-K8-001460 | SC-23 | Kubernetes Kubelet must enable tlsPrivateKeyFile for client authentication to secure service. | Failed |
| CNTR-K8-001470 | SC-23 | Kubernetes Kubelet must enable tlsCertFile for client authentication to secure service. | Failed |
| CNTR-K8-001480 | SC-23 | Kubernetes etcd must enable client authentication to secure service. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|---------------|---|----------------|
| CNTR-K8-001490 | SC-23 | Kubernetes etcd must have a key file for secure communication. | Passed |
| CNTR-K8-001500 | SC-23 | Kubernetes etcd must have a certificate for communication. | Passed |
| CNTR-K8-001510 | SC-23 | Kubernetes etcd must have the SSL Certificate Authority set. | Passed |
| CNTR-K8-001520 | SC-23 | Kubernetes etcd must have a certificate for communication. | Passed |
| CNTR-K8-001530 | SC-23 | Kubernetes etcd must have a key file for secure communication. | Passed |
| CNTR-K8-001540 | SC-23 | Kubernetes etcd must have peer-cert-file set for secure communication. | Passed |
| CNTR-K8-001550 | SC-23 | Kubernetes etcd must have a peer-key-file set for secure communication. | Passed |
| CNTR-K8-001620 | SC-3 | Kubernetes Kubelet must enable kernel protection. | Passed |
| CNTR-K8-002000 | AC-16 a | The Kubernetes API server must have the ValidatingAdmissionWebhook enabled. | Passed |
| CNTR-K8-002001 | AC-16 a | Kubernetes must enable PodSecurity admission controller on static pods and Kubelets. | Not Applicable |
| CNTR-K8-002010 | AC-16 a | Kubernetes must have a pod security policy set. | Not Applicable |
| CNTR-K8-002011 | AC-16 a | Kubernetes must have a Pod Security Admission control file configured. | Passed |
| CNTR-K8-002600 | SC-7 (21) | Kubernetes API Server must configure timeouts to limit attack surface. | 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 |
| CNTR-K8-002700 | SI-4 d | Kubernetes must remove old components after updated versions have been installed. | Not Applicable |
| 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 | The Kubernetes component manifests must be owned by root. | Passed |
| CNTR-K8-003120 | CM-6 b | The Kubernetes component etcd must be owned by etcd. | Passed |
| CNTR-K8-003130 | CM-6 b | The Kubernetes conf files must be owned by root. | Passed |
| CNTR-K8-003140 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must have file permissions set to 644 or more restrictive. | Not Applicable |
| CNTR-K8-003150 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must be owned by root. | Not Applicable |
| CNTR-K8-003160 | CM-6 b | The Kubernetes Kubelet certificate authority file must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003170 | CM-6 b | The Kubernetes Kubelet certificate authority must be owned by root. | Passed |
| CNTR-K8-003180 | CM-6 b | The Kubernetes component PKI must be owned by root. | Passed |
| CNTR-K8-003190 | CM-6 b | The Kubernetes kubelet KubeConfig must have file permissions set to 644 or more restrictive. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|--|--------|
| CNTR-K8-003200 | CM-6 b | The Kubernetes kubelet KubeConfig file must be owned by root. | Passed |
| CNTR-K8-003210 | CM-6 b | The Kubernetes kubeadm.conf must be owned by root. | Passed |
| CNTR-K8-003220 | CM-6 b | The Kubernetes kubeadm.conf must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003230 | CM-6 b | The Kubernetes kubelet config must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003240 | CM-6 b | The Kubernetes kubelet config must be owned by root. | Passed |
| CNTR-K8-003260 | CM-6 b | The Kubernetes etcd must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003270 | CM-6 b | The Kubernetes admin kubeconfig must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003280 | CM-6 b | Kubernetes API Server audit logs must be enabled. | Passed |
| CNTR-K8-003290 | CM-6 b | The Kubernetes API Server must be set to audit log max size. | Passed |
| CNTR-K8-003300 | CM-6 b | The Kubernetes API Server must be set to audit log maximum backup. | Passed |
| CNTR-K8-003310 | CM-6 b | The Kubernetes API Server audit log retention must be set. | Passed |
| CNTR-K8-003320 | CM-6 b | The Kubernetes API Server audit log path must be set. | Passed |
| CNTR-K8-003330 | CM-6 b | The Kubernetes PKI CRT must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003340 | CM-6 b | The Kubernetes PKI keys must have file permissions set to 600 or more restrictive. | Passed |

Appendix: Full Control List – Worker Node Kubernetes

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|---|----------------|
| CNTR-K8-000150 | AC-17 (2) | The Kubernetes Controller Manager must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Not Applicable |
| CNTR-K8-000160 | AC-17 (2) | The Kubernetes Scheduler must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Not Applicable |
| CNTR-K8-000170 | AC-17 (2) | The Kubernetes API Server must use TLS 1.2, at a minimum, to protect the confidentiality of sensitive data during electronic dissemination. | Not Applicable |
| CNTR-K8-000180 | AC-17 (2) | The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination. | Not Applicable |
| CNTR-K8-000190 | AC-17 (2) | The Kubernetes etcd must use TLS to protect the confidentiality of sensitive data during electronic dissemination. | Not Applicable |
| CNTR-K8-000220 | AC-2 (1) | The Kubernetes Controller Manager must create unique service accounts for each work payload. | Not Applicable |
| CNTR-K8-000270 | AC-3 | The Kubernetes API Server must enable Node, RBAC as the authorization mode. | Not Applicable |
| CNTR-K8-000290 | CM-6 b | User-managed resources must be created in dedicated namespaces. | Passed |
| CNTR-K8-000300 | AC-3 | The Kubernetes Scheduler must have secure binding. | Not Applicable |
| CNTR-K8-000310 | AC-3 | The Kubernetes Controller Manager must have secure binding. | Not Applicable |
| CNTR-K8-000320 | AC-3 | The Kubernetes API server must have the insecure port flag disabled. | Not Applicable |
| CNTR-K8-000330 | AC-3 | The Kubernetes Kubelet must have the "readOnlyPort" flag disabled. | Passed |
| CNTR-K8-000340 | AC-3 | The Kubernetes API server must have the insecure bind address not set. | Not Applicable |
| CNTR-K8-000350 | AC-3 | The Kubernetes API server must have the secure port set. | Not Applicable |
| CNTR-K8-000360 | AC-3 | The Kubernetes API server must have anonymous authentication disabled. | Not Applicable |
| CNTR-K8-000370 | AC-3 | The Kubernetes Kubelet must have anonymous authentication disabled. | Passed |
| CNTR-K8-000380 | AC-3 | The Kubernetes kubelet must enable explicit authorization. | Passed |
| CNTR-K8-000400 | AC-3 | Kubernetes Worker Nodes must not have sshd service running. | Failed |
| CNTR-K8-000410 | AC-3 | Kubernetes Worker Nodes must not have the sshd service enabled. | Failed |
| CNTR-K8-000420 | AC-3 | Kubernetes dashboard must not be enabled. | Not Applicable |
| CNTR-K8-000430 | AC-3 | Kubernetes Kubectl cp command must give expected access and results. | Passed |
| CNTR-K8-000440 | AC-3 | The Kubernetes kubelet staticPodPath must not enable static pods. | Failed |
| CNTR-K8-000450 | AC-3 | Kubernetes DynamicAuditing must not be enabled. | Passed |
| CNTR-K8-000460 | AC-3 | Kubernetes DynamicKubeletConfig must not be enabled. | Not Applicable |
| CNTR-K8-000470 | AC-3 | The Kubernetes API server must have Alpha APIs disabled. | Passed |
| CNTR-K8-000610 | AU-14 (1) | The Kubernetes API Server must have an audit log path set. | Not Applicable |

| Control ID | NIST 800-83 | Title | Status |
|----------------|--|--|----------------|
| CNTR-K8-000700 | AC-2 (4), AU-3 a, AU-3 b, AU-3 c, AU-3 d, AU-3 e, AU-3 (1), AU-12 c, AU-3 f, AU-3 (2), AC-16 a | Kubernetes API Server must generate audit records that identify what type of event has occurred, identify the source of the event, contain the event results, identify any users, and identify any containers associated with the event. | Not Applicable |
| CNTR-K8-000850 | CM-5 (6) | Kubernetes Kubelet must deny hostname override. | Passed |
| CNTR-K8-000860 | CM-5 (6) | The Kubernetes manifests must be owned by root. | Not Applicable |
| CNTR-K8-000880 | CM-5 (6) | The Kubernetes KubeletConfiguration file must be owned by root. | Passed |
| CNTR-K8-000890 | CM-5 (6) | The Kubernetes KubeletConfiguration files must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-000900 | CM-5 (6), CM-6 b | The Kubernetes manifest files must have least privileges. | Not Applicable |
| CNTR-K8-000910 | CM-7 a | Kubernetes Controller Manager must disable profiling. | Not Applicable |
| CNTR-K8-000920 | 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). | Not Applicable |
| CNTR-K8-000930 | 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). | Not Applicable |
| CNTR-K8-000940 | 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). | Not Applicable |
| CNTR-K8-000950 | 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). | Not Applicable |
| CNTR-K8-000960 | CM-7 b | The Kubernetes cluster must use non-privileged host ports for user pods. | Not Applicable |
| CNTR-K8-001160 | IA-5 (1) (d), IA-5 (1) (c) | Secrets in Kubernetes must not be stored as environment variables. | Not Applicable |
| CNTR-K8-001300 | SC-10 | Kubernetes Kubelet must not disable timeouts. | Not Applicable |
| CNTR-K8-001360 | SC-2 | Kubernetes must separate user functionality. | Not Applicable |
| CNTR-K8-001400 | SC-23 | The Kubernetes API server must use approved cipher suites. | Not Applicable |
| CNTR-K8-001410 | SC-23 | Kubernetes API Server must have the SSL Certificate Authority set. | Not Applicable |
| CNTR-K8-001420 | SC-23 | Kubernetes Kubelet must have the SSL Certificate Authority set. | Not Applicable |
| CNTR-K8-001430 | SC-23 | Kubernetes Controller Manager must have the SSL Certificate Authority set. | Not Applicable |
| CNTR-K8-001440 | SC-23 | Kubernetes API Server must have a certificate for communication. | Not Applicable |
| CNTR-K8-001450 | SC-23 | Kubernetes etcd must enable client authentication to secure service. | Not Applicable |
| CNTR-K8-001460 | SC-23 | Kubernetes Kubelet must enable tlsPrivateKeyFile for client authentication to secure service. | Not Applicable |
| CNTR-K8-001470 | SC-23 | Kubernetes Kubelet must enable tlsCertFile for client authentication to secure service. | Not Applicable |
| CNTR-K8-001480 | SC-23 | Kubernetes etcd must enable client authentication to secure service. | Not Applicable |

| Control ID | NIST 800-83 | Title | Status |
|----------------|---------------|---|----------------|
| CNTR-K8-001490 | SC-23 | Kubernetes etcd must have a key file for secure communication. | Not Applicable |
| CNTR-K8-001500 | SC-23 | Kubernetes etcd must have a certificate for communication. | Not Applicable |
| CNTR-K8-001510 | SC-23 | Kubernetes etcd must have the SSL Certificate Authority set. | Not Applicable |
| CNTR-K8-001520 | SC-23 | Kubernetes etcd must have a certificate for communication. | Not Applicable |
| CNTR-K8-001530 | SC-23 | Kubernetes etcd must have a key file for secure communication. | Not Applicable |
| CNTR-K8-001540 | SC-23 | Kubernetes etcd must have peer-cert-file set for secure communication. | Not Applicable |
| CNTR-K8-001550 | SC-23 | Kubernetes etcd must have a peer-key-file set for secure communication. | Not Applicable |
| CNTR-K8-001620 | SC-3 | Kubernetes Kubelet must enable kernel protection. | Not Applicable |
| CNTR-K8-002000 | AC-16 a | The Kubernetes API server must have the ValidatingAdmissionWebhook enabled. | Not Applicable |
| CNTR-K8-002001 | AC-16 a | Kubernetes must enable PodSecurity admission controller on static pods and Kubelets. | Not Applicable |
| CNTR-K8-002010 | AC-16 a | Kubernetes must have a pod security policy set. | Not Applicable |
| CNTR-K8-002011 | AC-16 a | Kubernetes must have a Pod Security Admission control file configured. | Not Applicable |
| CNTR-K8-002600 | SC-7 (21) | Kubernetes API Server must configure timeouts to limit attack surface. | Not Applicable |
| CNTR-K8-002620 | SC-12 (3) | Kubernetes API Server must disable basic authentication to protect information in transit. | Not Applicable |
| CNTR-K8-002630 | SC-12 (3) | Kubernetes API Server must disable token authentication to protect information in transit. | Not Applicable |
| CNTR-K8-002640 | SC-12 (3) | Kubernetes endpoints must use approved organizational certificate and key pair to protect information in transit. | Not Applicable |
| CNTR-K8-002700 | SI-4 d | Kubernetes must remove old components after updated versions have been installed. | Not Applicable |
| CNTR-K8-002720 | SI-3 (10) (a) | Kubernetes must contain the latest updates as authorized by IAVMs, CTOs, DTMs, and STIGs. | Not Applicable |
| CNTR-K8-003110 | CM-6 b | The Kubernetes component manifests must be owned by root. | Not Applicable |
| CNTR-K8-003120 | CM-6 b | The Kubernetes component etcd must be owned by etcd. | Not Applicable |
| CNTR-K8-003130 | CM-6 b | The Kubernetes conf files must be owned by root. | Not Applicable |
| CNTR-K8-003140 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must have file permissions set to 644 or more restrictive. | Not Applicable |
| CNTR-K8-003150 | CM-6 b | The Kubernetes Kube Proxy kubeconfig must be owned by root. | Not Applicable |
| CNTR-K8-003160 | CM-6 b | The Kubernetes Kubelet certificate authority file must have file permissions set to 644 or more restrictive. | Not Applicable |
| CNTR-K8-003170 | CM-6 b | The Kubernetes Kubelet certificate authority must be owned by root. | Not Applicable |
| CNTR-K8-003180 | CM-6 b | The Kubernetes component PKI must be owned by root. | Passed |
| CNTR-K8-003190 | CM-6 b | The Kubernetes kubelet KubeConfig must have file permissions set to 644 or more restrictive. | Passed |

| Control ID | NIST 800-83 | Title | Status |
|----------------|-------------|--|----------------|
| CNTR-K8-003200 | CM-6 b | The Kubernetes kubelet KubeConfig file must be owned by root. | Passed |
| CNTR-K8-003210 | CM-6 b | The Kubernetes kubeadm.conf must be owned by root. | Passed |
| CNTR-K8-003220 | CM-6 b | The Kubernetes kubeadm.conf must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003230 | CM-6 b | The Kubernetes kubelet config must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003240 | CM-6 b | The Kubernetes kubelet config must be owned by root. | Passed |
| CNTR-K8-003260 | CM-6 b | The Kubernetes etcd must have file permissions set to 644 or more restrictive. | Not Applicable |
| CNTR-K8-003270 | CM-6 b | The Kubernetes admin kubeconfig must have file permissions set to 644 or more restrictive. | Not Applicable |
| CNTR-K8-003280 | CM-6 b | Kubernetes API Server audit logs must be enabled. | Not Applicable |
| CNTR-K8-003290 | CM-6 b | The Kubernetes API Server must be set to audit log max size. | Not Applicable |
| CNTR-K8-003300 | CM-6 b | The Kubernetes API Server must be set to audit log maximum backup. | Not Applicable |
| CNTR-K8-003310 | CM-6 b | The Kubernetes API Server audit log retention must be set. | Not Applicable |
| CNTR-K8-003320 | CM-6 b | The Kubernetes API Server audit log path must be set. | Not Applicable |
| CNTR-K8-003330 | CM-6 b | The Kubernetes PKI CRT must have file permissions set to 644 or more restrictive. | Passed |
| CNTR-K8-003340 | CM-6 b | The Kubernetes PKI keys must have file permissions set to 600 or more restrictive. | Not Applicable |

