



STIG Hardening Overview for vSphere with Tanzu: Tanzu Kubernetes Release

TKR 1.27.6 vSphere 7.x (Photon)

May 2024

Table of contents

Revision History3

Overview4

Applicability4

Disclaimer.....4

Tanzu Kubernetes Release Compliance5

 Photon OS 3.0 Compliance - Overall 5

 Photon OS 3.0 Compliance - Exceptions 5

 Photon OS 3.0 Compliance - N/A Controls 6

 Control Plane Kubernetes Compliance - Overall 6

 Control Plane Kubernetes Compliance - Exceptions 7

 Control Plane Kubernetes Compliance - N/A Controls 8

 Worker Node Kubernetes Compliance - Overall 9

 Worker Node Kubernetes Compliance - Exceptions 9

 Worker Node Kubernetes Compliance – Not Reviewed Controls 9

Frequently Asked Questions 11

Appendix: Tanzu Kubernetes Release Full Control List 13

 TKR Control/Worker Photon OS 3.0 Control List 13

 TKR Control Plane Node Kubernetes Control List 19

 TKR Worker Node Kubernetes Control List 24

Revision History

| Date | Description of Change |
|----------|-----------------------|
| May 2024 | Initial Release |

Overview

VMware 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, vSphere with Tanzu is evaluated and hardened against the following standards:

- DISA Kubernetes STIG Version 1 Release 11
- Photon OS 3.0 STIG Readiness Guide Version 1 Release 9

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:

- TKR 1.27.6 vSphere 7.x (Photon)/v1.27.6---vmware.1-fips.1-tkg.1
- vSphere 7 Update 3p

For more information on TKR compatibility with vSphere see the [TKR Compatibility Matrix](#).

Disclaimer

This document is intended to provide general guidance for organizations that are considering VMware 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." VMware 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 VMware's offerings. It is intended for information purposes only and may not be incorporated into any contract. Any information regarding the pre-release of VMware offerings, future updates or other planned modifications is subject to ongoing evaluation by VMware 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 VMware offerings. Any purchasing decisions should only be based on features currently available. The development, release, and timing of any features or functionality described for VMware's offerings in this presentation remain at the sole discretion of VMware.

Tanzu Kubernetes Release Compliance

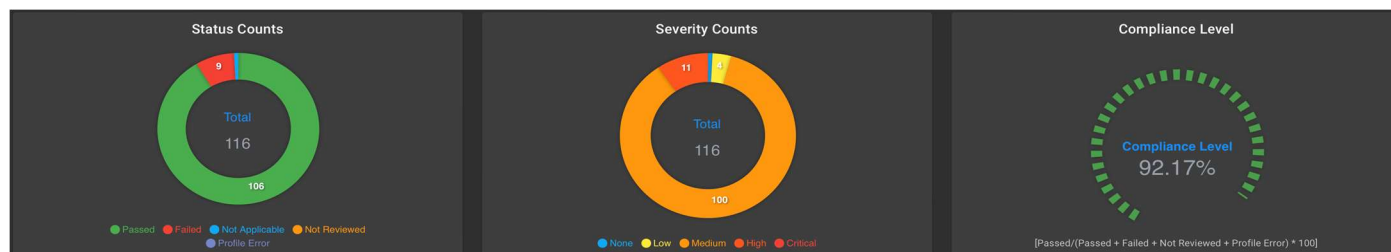
Tanzu Kubernetes Grid (TKG) clusters provide self-service lifecycle management of Kubernetes workload clusters. TKG on Supervisor is optimized for the vSphere with Tanzu environment and integrates with the underlying VMware vSphere infrastructure, as well as virtual networking via VMware NSX, and Cloud Native Storage options. With TKG on Supervisor, you can provision Kubernetes clusters that conform to the upstream Kubernetes open-source project, maintaining compatibility and support with the larger Kubernetes ecosystem.

For more information about the architecture of TKG see the [VMware vSphere with Tanzu Product Documentation](#).

Tanzu Kubernetes Cluster images (TKRs) have had their operating systems hardened by default. TKG Cluster images are not user serviceable. Updates to hardening will be released as part of the standard product update and upgrade processes.

Photon OS 3.0 Compliance - Overall

The results for the Photon OS 3.0 STIG Readiness Guide as it applies to each appliance for both control plane and worker nodes are as follows:



Photon OS 3.0 Compliance - Exceptions

Controls listed in this Exceptions table are either unmet or require post deployment configuration.

| Control ID | NIST 800-53 ¹ | Title | Justification |
|----------------|---|---|---|
| PHTN-30-000003 | AC-8 a, AC-8 c 1 | The Photon operating system must display the Standard Mandatory DoD Notice and Consent Banner before granting SSH access. | The DoD login banner is not configured out of the box as it is not appropriate for all customers. |
| PHTN-30-000039 | SI-11 a, SI-6 d, AC-2 (4), AC-2 (4), AU-4 (1), AU-4 (1), AC-2 (4), AC-2 (4) | The Photon operating system must configure rsyslog to offload system logs to a central server. | Resolution included in product roadmap. |
| PHTN-30-000046 | AU-14 (1) | The Photon operating system must initiate auditing as part of the boot process. | Resolution included in product roadmap. |
| PHTN-30-000058 | AU-8 (1) (a), AU-8 (1) (b) | The Photon operating system must be configured to synchronize with an approved DoD time source. | By default, nodes will sync time with the ESXi host it is running on. |

¹ Duplicate entries may appear in the NIST 800-53 controls column as an artifact of VMware testing, if the control meets multiple requirements.

| | | | |
|----------------|--------------------|--|---|
| PHTN-30-000064 | MA-4 (6), SC-8 (1) | The Photon operating system must configure sshd to use FIPS 140-2 ciphers. | Resolution included in product roadmap. |
| PHTN-30-000088 | CM-6 b | The Photon operating system must configure sshd to limit the number of allowed login attempts per connection. | Resolution included in product roadmap. |
| PHTN-30-000106 | CM-6 b | The Photon operating system must not perform IPv4 packet forwarding. | Packet forwarding is required for Kubernetes to route packets for pods. |
| PHTN-30-000240 | SC-13 | 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. | Resolution included in product roadmap. |
| PHTN-30-000245 | CM-6 b | The Photon operating system must disable systemd fallback DNS. | Resolution included in product roadmap. |

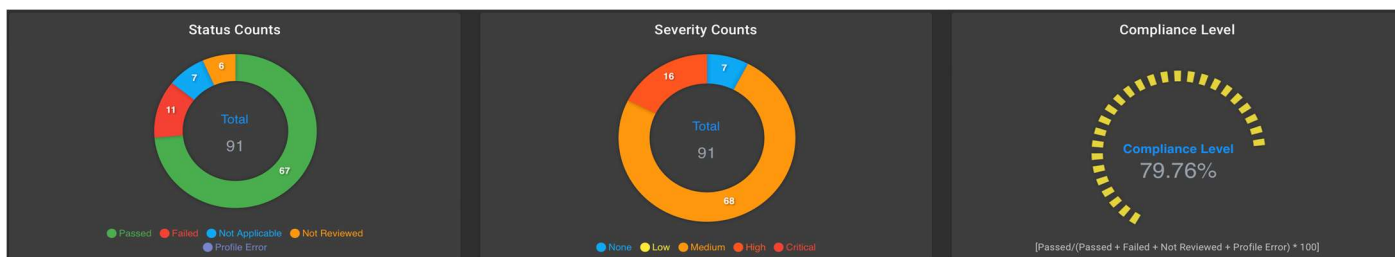
Photon OS 3.0 Compliance - N/A Controls

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

| Control ID | NIST 800-53 ¹ | Title | Justification |
|----------------|--------------------------|--|--|
| PHTN-30-000062 | IA-11 | The Photon operating system must require users to reauthenticate for privilege escalation. | There are no users with sudo privileges and NOPASSWD defined to audit. |

Control Plane Kubernetes Compliance - Overall

The results for the Kubernetes STIG Readiness Guide as it applies to each control plane node are as follows:



Control Plane Kubernetes Compliance - Exceptions

Controls listed in this Exceptions table are either unmet or require post deployment configuration.

| Control ID | NIST 800-53 ¹ | Title | Justification |
|----------------|--|--|--|
| CNTR-K8-000290 | CM-6 b | User-managed resources must be created in dedicated namespaces. | TKG deployments contain a service/supervisor service in the default namespace to provide communication with the supervisor cluster. |
| CNTR-K8-000330 | AC-3 | The Kubernetes Kubelet must have the "readOnlyPort" flag disabled. | The readOnlyPort is disabled but is configured on the kubelet process instead of in the config file and is a finding in V1R10 of the K8s STIG. Resolution included in product roadmap. |
| 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-K8-000440 | 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. |
| 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, AC-2 (4), AC-2 (4), 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-K8-000960 | CM-7 b | The Kubernetes cluster must use non-privileged host ports for user pods. | False positive. A container was used to scan the environment and caused this failure. This container is not present in deployments. |
| CNTR-K8-001300 | SC-10 | Kubernetes Kubelet must not disable timeouts. | Resolution included in product roadmap. |
| CNTR-K8-001460 | SC-23 | Kubernetes Kubelet must enable tls-private-key-file for client authentication to secure service. | Custom certificates are currently not supported for kubelet. |
| CNTR-K8-001470 | SC-23 | Kubernetes Kubelet must enable tls-cert-file for client authentication to secure service. | Custom certificates are currently not supported for kubelet. |
| CNTR-K8-001620 | AC-16 a | Kubernetes Kubelet must enable kernel protection. | The setting protectKernelDefaults is enabled but is configured on the kubelet process instead of in the config file and is a finding in V1R10 of the K8s STIG. Resolution included in product roadmap. |
| CNTR-K8-002011 | AC-16 a | Kubernetes must have a Pod Security Admission control file configured. | Resolution included in product roadmap. |

Control Plane Kubernetes Compliance - N/A Controls

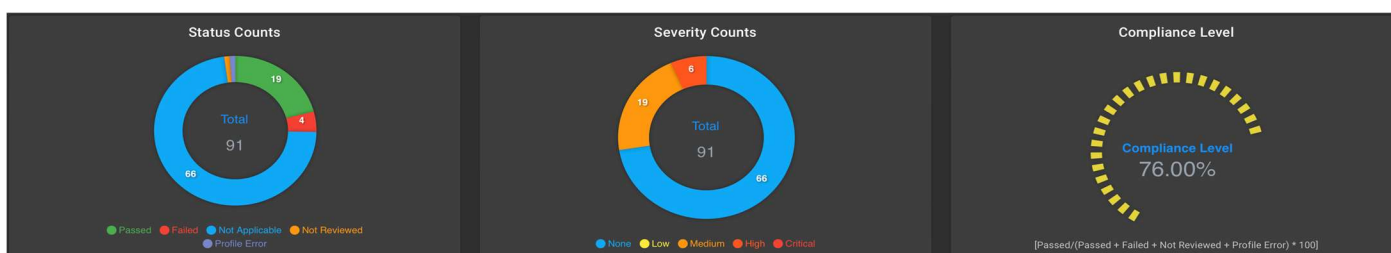
Controls listed in this Not Applicable table are not applicable in this scenario or require manual review post-deployment.

| Control ID | NIST 800-53 ¹ | 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 reference PR |
| CNTR-K8-000400 | AC-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-K8-000460 | AC-3 | Kubernetes DynamicKubeletConfig must not be enabled. | DynamicKubeletConfig is deprecated in Kubernetes versions 1.24 and greater. |
| 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). | Ports and protocols used in the product are available at https://ports.vmware.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). | Ports and protocols used in the product are available at https://ports.vmware.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). | Ports and protocols used in the product are available at https://ports.vmware.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). | Ports and protocols used in the product are available at https://ports.vmware.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-K8-002010 | AC-16 a | Kubernetes must have a pod security policy set. | PSP is deprecated in Kubernetes versions 1.24 and greater. |
| CNTR-K8-002700 | SI-4 d | Kubernetes must remove old components after updated versions have been installed. | This is typically a manual review, but since nodes are completely replaced on upgrades, no older versions of components will exist. |
| CNTR-K8-003140 | CM-6 b | The Kubernetes Kube Proxy 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 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 for the Kubernetes STIG Readiness Guide as it applies to each worker node are as follows:



Worker Node Kubernetes Compliance - Exceptions

Controls listed in this Exceptions table are either unmet or require post deployment configuration.

| Control ID | NIST 800-53 ¹ | Title | Justification |
|----------------|--------------------------|--|--|
| CNTR-K8-000330 | AC-3 | The Kubernetes Kubelet must have the "readOnlyPort" flag disabled. | The readOnlyPort is disabled but is configured on the kubelet process instead of in the config file and is a finding in V1R10 of the K8s STIG. Resolution included in product roadmap. |
| 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. |
| 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. |
| CNTR-K8-000440 | AC-3 | The Kubernetes kubelet static PodPath must not enable static pods. | The embedded registry is run as a container using static pods on the worker nodes. |

Worker Node Kubernetes Compliance – Not Reviewed Controls

Controls listed in this table require manual review post-deployment. 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.

| Control ID | NIST 800-53 ¹ | Title | Justification |
|----------------|--------------------------|---|---|
| CNTR-K8-002700 | SI-4 d | Kubernetes must remove old components after updated versions have been installed. | This is typically a manual review, but since nodes are completely replaced on upgrades, no older versions of components will exist. |

Frequently Asked Questions

Can customers make changes to the vSphere with Tanzu Supervisor or TKr images or appliances?

No. Due to the immutable nature of vSphere with Tanzu deployments any changes would not be persistent. Modification to images and components is not supported. For product improvements please contact your VMware Account Team.

Where can I find the Photon OS 3.0 STIG Readiness Guide?

The Photon OS 3.0 STIG Readiness guide may be found at:

<https://github.com/vmware/dod-compliance-and-automation/tree/master/photon/3.0/docs>

What is a STIG Readiness Guide?

More information about STIG Readiness Guides can be found at:

<https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/docs/vmware-stig-program-overview.pdf>

Is there a compliance report for Tanzu Kubernetes Clusters?

A report for TKCs/TKrs will be available in a separate document and those images have a separate lifecycle from vCenter and the Supervisor nodes.

What do the severity codes mean?

The DISA Security Requirements Guides state:

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.

A description of the category codes are as follows:

| 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 severity codes in the associated guides are CAT II. During STIG development, DISA modifies severity codes on a per product and context specific basis.

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 a manual review. |
|--------------|---|

Appendix: Tanzu Kubernetes Release Full Control List

TKR Control/Worker Photon OS 3.0 Control List

| Control ID | NIST 800-53 ¹ | Title | Status |
|----------------|--|--|--------|
| PHTN-30-000001 | AC-2 (4) | The Photon operating system must audit all account creations. | Passed |
| PHTN-30-000002 | AC-7 a, AC-7 b | The Photon operating system must automatically lock an account when three unsuccessful logon attempts occur. | Passed |
| PHTN-30-000003 | AC-8 a, AC-8 c 1 | The Photon operating system must display the Standard Mandatory DOD Notice and Consent Banner before granting Secure Shell (SSH) access. | Failed |
| PHTN-30-000004 | AC-10 | The Photon operating system must limit the number of concurrent sessions to 10 for all accounts and/or account types. | Passed |
| PHTN-30-000005 | AC-11 a, AC-12, MA-4 e | The Photon operating system must set a session inactivity timeout of 15 minutes or less. | Passed |
| PHTN-30-000006 | AC-17 (1) | The Photon operating system must have the sshd SyslogFacility set to "authpriv". | Passed |
| PHTN-30-000007 | AC-17 (1) | The Photon operating system must have sshd authentication logging enabled. | Passed |
| PHTN-30-000008 | AC-17 (1) | The Photon operating system must have the sshd LogLevel set to "INFO". | Passed |
| PHTN-30-000009 | AC-17 (2), MA-4 (6), SC-13, SC-8 | The Photon operating system must configure sshd to use approved encryption algorithms. | Passed |
| PHTN-30-000010 | AU-3 | The Photon operating system must configure auditd to log to disk. | Passed |
| PHTN-30-000011 | AU-3 | The Photon operating system must configure auditd to use the correct log format. | Passed |
| PHTN-30-000012 | AU-3 (1) | The Photon operating system must be configured to audit the execution of privileged functions. | Passed |
| PHTN-30-000013 | AU-12 a, AU-12 c, AU-3, AU-3 (1), CM-3 (5), CM-5 (1), SI-6 a, SI-6 b | The Photon operating system must have the auditd service running. | Passed |
| PHTN-30-000014 | AU-5 (2), AU-5 a | The Photon operating system audit log must log space limit problems to syslog. | Passed |
| PHTN-30-000015 | AU-5 b | The Photon operating system audit log must attempt to log audit failures to syslog. | Passed |

| | | | |
|----------------|--|--|--------|
| PHTN-30-000016 | AU-9 | The Photon operating system audit log must have correct permissions. | Passed |
| PHTN-30-000017 | AU-9 | The Photon operating system audit log must be owned by root. | Passed |
| PHTN-30-000018 | AU-9 | The Photon operating system audit log must be group-owned by root. | Passed |
| PHTN-30-000019 | AU-12 b | The Photon operating system must allow only the information system security manager (ISSM) (or individuals or roles appointed by the ISSM) to select which auditable events are to be audited. | Passed |
| PHTN-30-000020 | AU-12 c, MA-4 (1) (a) | The Photon operating system must generate audit records when successful/unsuccessful attempts to access privileges occur. | Passed |
| PHTN-30-000021 | IA-5 (1) (a) | The Photon operating system must enforce password complexity by requiring that at least one uppercase character be used. | Passed |
| PHTN-30-000022 | IA-5 (1) (a) | The Photon operating system must enforce password complexity by requiring that at least one lowercase character be used. | Passed |
| PHTN-30-000023 | IA-5 (1) (a) | The Photon operating system must enforce password complexity by requiring that at least one numeric character be used. | Passed |
| PHTN-30-000024 | IA-5 (1) (b) | The Photon operating system must require that new passwords are at least four characters different from the old password. | Passed |
| PHTN-30-000025 | IA-5 (1) (c) | The Photon operating system must store only encrypted representations of passwords. | Passed |
| PHTN-30-000026 | IA-2 (8), IA-2 (9), IA-5 (1) (c), IA-7, MA-4 (7), MA-4 c, SC-8 (2) | The Photon operating system must use an OpenSSH server version that does not support protocol 1. | Passed |
| PHTN-30-000027 | IA-5 (1) (d) | The Photon operating system must be configured so that passwords for new users are restricted to a 24-hour minimum lifetime. | Passed |
| PHTN-30-000028 | IA-5 (1) (d) | The Photon operating system must be configured so that passwords for new users are restricted to a 90-day maximum lifetime. | Passed |
| PHTN-30-000029 | IA-5 (1) (e) | The Photon operating system must prohibit password reuse for a minimum of five generations. | Passed |
| PHTN-30-000030 | IA-5 (1) (a) | The Photon operating system must enforce a minimum eight-character password length. | Passed |
| PHTN-30-000031 | AC-3 | The Photon operating system must require authentication upon booting into single-user and maintenance modes. | Passed |
| PHTN-30-000032 | CM-7 b, IA-3 | The Photon operating system must disable the loading of unnecessary kernel modules. | Passed |

| | | | |
|----------------|-------------------------------------|--|--------|
| PHTN-30-000033 | IA-2 | The Photon operating system must not have duplicate User IDs (UIDs). | Passed |
| PHTN-30-000035 | IA-4 e | The Photon operating system must disable new accounts immediately upon password expiration. | Passed |
| PHTN-30-000036 | SC-5, SC-5 (2) | The Photon operating system must use Transmission Control Protocol (TCP) syncookies. | Passed |
| PHTN-30-000037 | SC-10 | The Photon operating system must configure sshd to disconnect idle Secure Shell (SSH) sessions. | Passed |
| PHTN-30-000038 | SC-10 | The Photon operating system must configure sshd to disconnect idle Secure Shell (SSH) sessions. | Passed |
| PHTN-30-000039 | AC-2 (4), AU-4 (1), SI-11 a, SI-6 d | The Photon operating system must configure rsyslog to offload system logs to a central server. | Failed |
| PHTN-30-000040 | SI-11 b | The Photon operating system "/var/log" directory must be owned by root. | Passed |
| PHTN-30-000041 | SI-11 b | The Photon operating system messages file must have the correct ownership and file permissions. | Passed |
| PHTN-30-000042 | AC-2 (4) | The Photon operating system must audit all account modifications. | Passed |
| PHTN-30-000043 | AC-2 (4) | The Photon operating system must audit all account modifications. | Passed |
| PHTN-30-000044 | AC-2 (4) | The Photon operating system must audit all account disabling actions. | Passed |
| PHTN-30-000045 | AC-2 (4) | The Photon operating system must audit all account removal actions. | Passed |
| PHTN-30-000046 | AU-14 (1) | The Photon operating system must initiate auditing as part of the boot process. | Failed |
| PHTN-30-000047 | AU-9 | The Photon operating system audit files and directories must have correct permissions. | Passed |
| PHTN-30-000048 | AU-9 | The Photon operating system must protect audit tools from unauthorized modification and deletion. | Passed |
| PHTN-30-000049 | CM-5 (6) | The Photon operating system must limit privileges to change software resident within software libraries. | Passed |
| PHTN-30-000050 | IA-5 (1) (a) | The Photon operating system must enforce password complexity by requiring that at least one special character be used. | Passed |
| PHTN-30-000051 | AU-9 (3) | The Photon operating system package files must not be modified. | Passed |
| PHTN-30-000054 | AC-6 (9), AU-12 c | The Photon operating system must audit the execution of privileged functions. | Passed |

| | | | |
|----------------|----------------------------|--|----------------|
| PHTN-30-000055 | AU-4 | The Photon operating system must configure auditd to keep five rotated log files. | Passed |
| PHTN-30-000056 | AU-4 | The Photon operating system must configure auditd to keep logging in the event max log file size is reached. | Passed |
| PHTN-30-000057 | AU-5 (1) | The Photon operating system must configure auditd to log space limit problems to syslog. | Passed |
| PHTN-30-000058 | AU-8 (1) (a), AU-8 (1) (b) | The Photon operating system must be configured to synchronize with an approved DOD time source. | Failed |
| PHTN-30-000059 | CM-5 (3) | The Photon operating system RPM package management tool must cryptographically verify the authenticity of all software packages during installation. | Passed |
| PHTN-30-000060 | CM-5 (3) | The Photon operating system RPM package management tool must cryptographically verify the authenticity of all software packages during installation. | Passed |
| PHTN-30-000061 | CM-5 (3) | The Photon operating system YUM repository must cryptographically verify the authenticity of all software packages during installation. | Passed |
| PHTN-30-000062 | IA-11 | The Photon operating system must require users to reauthenticate for privilege escalation. | Not Applicable |
| PHTN-30-000064 | MA-4 (6), SC-8 (1) | The Photon operating system must configure sshd to use FIPS 140-2 ciphers. | Failed |
| PHTN-30-000065 | SI-16 | The Photon operating system must implement address space layout randomization (ASLR) to protect its memory from unauthorized code execution. | Passed |
| PHTN-30-000066 | SI-2 (6) | The Photon operating system must remove all software components after updated versions have been installed. | Passed |
| PHTN-30-000067 | AU-12 c | The Photon operating system must generate audit records when the sudo command is used. | Passed |
| PHTN-30-000068 | AU-12 c | The Photon operating system must generate audit records when successful/unsuccessful logon attempts occur. | Passed |
| PHTN-30-000069 | AU-12 c | The Photon operating system must audit the "insmod" module. | Passed |
| PHTN-30-000070 | AU-12 c | The Photon operating system auditd service must generate audit records for all account creations, modifications, disabling, and termination events. | Passed |
| PHTN-30-000071 | CM-6 b | The Photon operating system must use the "pam_cracklib" module. | Passed |
| PHTN-30-000072 | CM-6 b | The Photon operating system must set the "FAIL_DELAY" parameter. | Passed |

| | | | |
|----------------|--------|---|--------|
| PHTN-30-000073 | 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 |
| PHTN-30-000074 | CM-6 b | The Photon operating system must ensure audit events are flushed to disk at proper intervals. | Passed |
| PHTN-30-000075 | CM-6 b | The Photon operating system must create a home directory for all new local interactive user accounts. | Passed |
| PHTN-30-000076 | CM-6 b | The Photon operating system must disable the debug-shell service. | Passed |
| PHTN-30-000078 | CM-6 b | The Photon operating system must configure sshd to disallow Generic Security Service Application Program Interface (GSSAPI) authentication. | Passed |
| PHTN-30-000079 | CM-6 b | The Photon operating system must configure sshd to disable environment processing. | Passed |
| PHTN-30-000080 | CM-6 b | The Photon operating system must configure sshd to disable X11 forwarding. | Passed |
| PHTN-30-000081 | CM-6 b | The Photon operating system must configure sshd to perform strict mode checking of home directory configuration files. | Passed |
| PHTN-30-000082 | CM-6 b | The Photon operating system must configure sshd to disallow Kerberos authentication. | Passed |
| PHTN-30-000083 | CM-6 b | The Photon operating system must configure sshd to disallow authentication with an empty password. | Passed |
| PHTN-30-000084 | CM-6 b | The Photon operating system must configure sshd to disallow compression of the encrypted session stream. | Passed |
| PHTN-30-000085 | CM-6 b | The Photon operating system must configure sshd to display the last login immediately after authentication. | Passed |
| PHTN-30-000086 | CM-6 b | The Photon operating system must configure sshd to ignore user-specific trusted hosts lists. | Passed |
| PHTN-30-000087 | CM-6 b | The Photon operating system must configure sshd to ignore user-specific known_host files. | Passed |
| PHTN-30-000088 | CM-6 b | The Photon operating system must configure sshd to limit the number of allowed login attempts per connection. | Failed |
| PHTN-30-000089 | CM-6 b | The Photon operating system must be configured so the x86 Ctrl-Alt-Delete key sequence is disabled on the command line. | Passed |
| PHTN-30-000090 | CM-6 b | The Photon operating system must be configured so the "/etc/skel" default scripts are protected from unauthorized modification. | Passed |

| | | | |
|----------------|--------|---|--------|
| PHTN-30-000091 | CM-6 b | The Photon operating system must be configured so the <code>"/root"</code> path is protected from unauthorized access. | Passed |
| PHTN-30-000092 | CM-6 b | The Photon operating system must be configured so that all global initialization scripts are protected from unauthorized modification. | Passed |
| PHTN-30-000093 | CM-6 b | The Photon operating system must be configured so that all system startup scripts are protected from unauthorized modification. | Passed |
| PHTN-30-000094 | CM-6 b | The Photon operating system must be configured so that all files have a valid owner and group owner. | Passed |
| PHTN-30-000095 | CM-6 b | The Photon operating system must be configured so that the <code>"/etc/cron.allow"</code> file is protected from unauthorized modification. | Passed |
| PHTN-30-000096 | CM-6 b | The Photon operating system must be configured so that all cron jobs are protected from unauthorized modification. | Passed |
| PHTN-30-000097 | CM-6 b | The Photon operating system must be configured so that all cron paths are protected from unauthorized modification. | Passed |
| PHTN-30-000098 | CM-6 b | The Photon operating system must not forward IPv4 or IPv6 source-routed packets. | Passed |
| PHTN-30-000099 | 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-30-000100 | CM-6 b | The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) redirect messages from being accepted. | Passed |
| PHTN-30-000101 | CM-6 b | The Photon operating system must prevent IPv4 Internet Control Message Protocol (ICMP) secure redirect messages from being accepted. | Passed |
| PHTN-30-000102 | CM-6 b | The Photon operating system must not send IPv4 Internet Control Message Protocol (ICMP) redirects. | Passed |
| PHTN-30-000103 | CM-6 b | The Photon operating system must log IPv4 packets with impossible addresses. | Passed |
| PHTN-30-000104 | CM-6 b | The Photon operating system must use a reverse-path filter for IPv4 network traffic. | Passed |
| PHTN-30-000105 | CM-6 b | The Photon operating system must not perform multicast packet forwarding. | Passed |
| PHTN-30-000106 | CM-6 b | The Photon operating system must not perform IPv4 packet forwarding. | Failed |
| PHTN-30-000107 | CM-6 b | The Photon operating system must send Transmission Control Protocol (TCP) timestamps. | Passed |

| | | | |
|----------------|--------------|--|--------|
| PHTN-30-000108 | CM-6 b | The Photon operating system must be configured to protect the Secure Shell (SSH) public host key from unauthorized modification. | Passed |
| PHTN-30-000109 | CM-6 b | The Photon operating system must be configured to protect the Secure Shell (SSH) private host key from unauthorized access. | Passed |
| PHTN-30-000110 | CM-6 b | The Photon operating system must enforce password complexity on the root account. | Passed |
| PHTN-30-000111 | CM-6 b | The Photon operating system must protect all boot configuration files from unauthorized modification. | Passed |
| PHTN-30-000112 | CM-6 b | The Photon operating system must protect sshd configuration from unauthorized access. | Passed |
| PHTN-30-000113 | CM-6 b | The Photon operating system must protect all "sysctl" configuration files from unauthorized access. | Passed |
| PHTN-30-000114 | CM-6 b | The Photon operating system must set the "umask" parameter correctly. | Passed |
| PHTN-30-000115 | CM-6 b | The Photon operating system must configure sshd to disallow HostbasedAuthentication. | Passed |
| PHTN-30-000117 | IA-5 (1) (c) | The Photon operating system must store only encrypted representations of passwords. | Passed |
| PHTN-30-000118 | IA-5 (1) (e) | The Photon operating system must ensure the old passwords are being stored. | Passed |
| PHTN-30-000119 | CM-6 b | The Photon operating system must configure sshd to restrict AllowTcpForwarding. | Passed |
| PHTN-30-000120 | CM-6 b | The Photon operating system must configure sshd to restrict LoginGraceTime. | Passed |
| PHTN-30-000240 | SC-13 | The Photon operating system must implement NIST FIPS-validated cryptography for the following: to provision digital signatures, generate cryptographic hashes, and protect unclassified information requiring confidentiality and cryptographic protection in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. | Failed |
| PHTN-30-000245 | CM-6 b | The Photon operating system must disable systemd fallback Domain Name System (DNS). | Failed |

TKR Control Plane Node Kubernetes Control List

| Control ID | NIST 800-53 ¹ | 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. | Failed |
| 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. | 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. | Passed |
| 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, AC-2 (4), AC-2 (4), 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. | Failed |

| | | | |
|----------------|--------------|---|----------------|
| CNTR-K8-001160 | 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. | Failed |
| 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 |
| 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. | Failed |
| 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. | Passed |
| 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. | Failed |
| 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 Reviewed |
| 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 |
| 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 |

TKR Worker Node Kubernetes Control List

| Control ID | NIST 800-53 ¹ | 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. | Failed |
| 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 |
| 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, AC-2 (4), AC-2 (4), 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. | Passed |
| 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) (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 |

| | | | |
|----------------|-----------|---|----------------|
| 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. | Passed |
| 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 Reviewed |
| 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 |
| 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 |

