ICS 35.040
L 80

团 体 标 准

T/ISEAA XXX-2019

网络安全等级保护容器安全要求

Container security requirement for classified protection of cybersecurity

（征求意见稿）

20XX -XX-XX 发布　　20XX -XX-XX 实施

中关村信息安全测评联盟 发布

目　　次

前言 III
引言 IV
1　范围 1
2　规范性引用文件 1
3　术语和定义 1
4　缩略语 2
5　容器集群概述 2
6　第一级安全要求 3
6.1　安全计算环境 3
6.2　安全管理中心 4
6.3　安全建设管理 4
7　第二级安全要求 4
7.1　安全计算环境 4
7.2　安全管理中心 5
7.3　安全建设管理 5
8　第三级安全要求 5
8.1　安全计算环境 5
8.2　安全管理中心 6
8.3　安全建设管理 7
9　第四级安全要求 7
9.1　安全计算环境 7
9.2　安全管理中心 8
9.3　安全建设管理 8
10　第五级安全要求 9
附录 A（资料性附录）　容器安全场景与安全要求的选择和使用 10
参考文献 15

前　言

本文件按照GB/T 1.1—2009给出的规则起草。

本文件由中关村信息安全测评联盟团体标准委员会提出并归口。

本文件起草单位：

本文件主要起草人：

引　言

为了配合《中华人民共和国网络安全法》的实施，同时适应新技术、新应用情况下网络安全等级保护工作的开展，制定本文件。《网络安全等级保护容器安全要求》将GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》的通用安全保护要求进行细化和扩展，提出容器安全保护技术要求。

本文件是网络安全等级保护相关系列标准之一。

与本文件相关的标准包括：

——GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求。

——GB/T 22240—2020　信息安全技术　网络安全等级保护定级指南。

本文件为评价网络是否符合《网络安全等级保护基本要求》提供了额外的扩展要求，用于指导网络建设单位、测评人员从网络安全等级保护的角度对基于容器技术的网络进行建设和测试评估。

本文件中，**黑体字部分**表示较高等级中增加或增强的要求。

网络安全等级保护容器安全要求

1 范围

本文件规定了采用容器集群技术的等级保护对象的安全要求，包括第一级至第四级网络的要求。

本文件适用于采用容器集群技术的等级保护对象的安全建设、安全整改和安全测试评估。网络安全监管部门依法对采用容器集群技术的等级保护对象监督检查可参照使用。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25069 信息安全技术 术语

GB/T 28448-2019 信息安全技术 网络安全等级保护测评要求

GB/T 28458-2020 信息安全技术 网络安全漏洞标识与描述规范

GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南

3 术语和定义

GB/T 25069、GB/T 22239、GB/T 28448、GB/T 28458、GB/T 30279界定的以及下列术语和定义适用于本文件。

3.1

容器实例 container instance

在应用虚拟化环境中打包和安全运行应用的一种方法。

3.2

容器镜像 container image

包含运行容器所需的所有软件的包文件。

3.3

容器集群 container cluster

采用集群编排工具统一管理的若干个宿主机形成的计算架构。

3.4

容器镜像仓库 container image repository

用于容器镜像分类、标记、存储、下载和版本控制的服务组件

3.5

弹性伸缩 auto scaling

根据用户的业务需求和预设策略，自动调整计算资源，使计算节点数量随业务负载需求自动变化的特性。

3.6

容器逃逸 container escape

从容器内部通过特权配置或者利用网络安全漏洞突破限制获取到宿主机的权限和资源的攻击手段。

3.7

反弹 shell reverse shell

从被控端口发起请求到控制端监听端口，并将其命令行输入输出内容转到控制端的网络攻击行为。

3.8

容器运行时 container runtime

用于保障容器实例运行机制符合特定规范的一组软件集合。

3.9

安全容器运行时 secure container runtime

提供独立的操作系统内核以及虚拟化层的容器运行时。

4 缩略语

下列缩略语适用于本文件。

OCI：开放容器标准（Open Container Initiative）

5 容器集群概述

容器集群是指采用编排软件来统一管理容器形成的集群，容器集群通常由管理平台、计算节点、操作系统、容器镜像、容器运行时、集群网络、容器实例、容器镜像仓库构成。对于未采用集群编排软件进行统一管理，只是将容器作为虚拟化技术使用的场景，不适用于本文件。

图 5.1 给出了容器集群的架构模型。

图 5.1 容器集群架构

——管理平台是用于控制计算节点的管理节点。所有任务分配都来自于管理平台，容器集群提供了一个全局的管理界面，是由相关的管理组件组合共同提供能力，如 Kubernetes 集群有：API Server、CoreDNS、Controller、Scheduler、ETCD 等核心组件，这些管理组件如果配置不当或者出现软件漏洞可能会导致整个集群出现安全风险。

——计算节点是负责执行请求和所分配任务的物理机或者虚拟机，由管理平台负责对计算节点进行控制。每个计算节点上存在容器镜像、容器运行时、集群网络、容器实例等多个角色。

——容器运行时是为了运行容器实例，每个计算节点都需要安装一个容器运行时引擎。比如 Docker，

但 Kubernetes 也支持其他符合 OCI 标准的容器运行时，例如 Containerd 和 CRI-O。

——容器镜像负责给容器实例提供一个虚拟的文件系统，所有需要运行的容器镜像都必须先下载到计算节点上，如果容器镜像中有软件漏洞或者恶意文件可能会导致容器实例出现安全风险，所有容器镜像相关的检测项就是对容器镜像做检查。

——容器镜像运行后即是容器实例，容器实例负责给对应的进程提供一个虚拟的操作系统环境，如果容器实例本身配置不当或者容器实例中有恶意命令执行可能会导致计算节点或者其他容器实例出现安全风险，所有容器实例相关的检测项就是对容器实例做检查。

——容器实例所依赖的容器镜像会集中存储于容器镜像仓库中，如果容器镜像仓库出现配置不当或者软件漏洞可能会导致镜像被恶意篡改，所有容器镜像仓库相关的检测项就是对容器镜像仓库做检查。

根据容器集群的部署位置不同，又分为公有容器集群、物理机部署的私有容器集群和私有云部署的私有容器集群三种场景。通常公有容器集群场景是指企业采用公有云服务商提供的云主机作为部署容器集群的基础设施，或直接采用公有云服务商提供的容器集群托管业务。物理机部署的私有容器集群是指企业在IDC机房使用物理机自建的容器集群。私有云部署的私有容器集群是指企业在自建 IDC 机房的私有云之上部署的容器集群。

6 第一级安全要求

6.1 安全计算环境

6.1.1 身份鉴别

本项要求包括：

a) 应对容器集群的访问请求进行身份标识和鉴别；
b) 应确保容器集群管理平台和容器运行时不被匿名访问；
c) 应对容器镜像仓库的访问请求进行身份标识和鉴别。

6.1.2 访问控制

本项要求包括：

a) 应实现基于角色的访问控制；
b) 应实现对容器镜像仓库访问控制；
c) 应实现容器实例之间的网络访问控制；
d) 应保证当容器实例迁移时，集群用户对资源的访问控制权限随其迁移；
e) 应实现容器实例对宿主机资源的访问控制。

6.1.3 入侵防范

本项要求包括：

a) 应确保容器镜像仅包含必要的软件包或组件；
b) 应确保容器镜像修复有补丁的超危和高危网络安全漏洞；
c) 应实现在容器镜像的持续构建或部署流程中集成扫描功能；
d) 除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行；

6.1.4 恶意代码防范

本项要求包括：

a） 应确保容器镜像内不包含病毒、木马、webshell等恶意代码；
b） 应对容器实例运行过程中发生的恶意代码传播行为进行监测。

6.1.5 容器镜像保护

本项要求包括：
a） 应对容器镜像完整性进行校验；
b） 应实现容器镜像文件的安全加密传输。

6.2 安全管理中心

6.2.1 集中管控

本项要求包括：

a） 应实现以容器集群的方式对容器实例等资源进行统一编排调度管理；
b） 应通过容器镜像仓库对容器镜像进行集中管理；
c） 应对容器实例的各项性能指标进行集中监控。

6.3 安全建设管理

6.3.1 供应链管理

应确保容器集群技术供应商的选择符合国家有关规定。

7 第二级安全要求

7.1 安全计算环境

7.1.1 身份鉴别

本项要求包括：
a） 应对容器集群的访问请求进行身份标识和鉴别；
b） 应确保容器集群管理平台和容器运行时不被匿名访问；
c） 应对容器镜像仓库的访问请求进行身份标识和鉴别。

7.1.2 访问控制

本项要求包括：
a） 应实现基于角色的访问控制；
b） 应实现对容器镜像仓库访问控制；
c） 应实现容器实例之间的网络访问控制；
d） 应保证当容器实例迁移时，集群用户对资源的访问控制权限随其迁移；
e） **应实现容器实例对宿主机资源的访问控制**。

7.1.3 安全审计

本项要求包括：
a） **应实现容器镜像使用情况的审计，包括镜像上传、下载镜像事件审计**；
b） **应实现容器集群事件审计**。

7.1.4 入侵防范

本项要求包括：

a） 应确保容器镜像应只包含必要的软件包或组件；
b） 应确保容器镜像修复有补丁的超危和高危网络安全漏洞；
c） 应实现在容器镜像的持续构建或部署流程中集成扫描功能；
d） 除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行；
e） **应实现容器集群内异常流量监测**。

7.1.5 恶意代码防范

本项要求包括：

a） 应确保容器镜像内不包含病毒、木马、webshell等恶意代码；
b） 应对容器实例运行过程中发生的恶意代码传播行为进行监测。

7.1.6 容器镜像保护

本项要求包括：

a） 应对容器镜像完整性进行校验；
b） 应实现容器镜像文件的安全加密传输。

7.2 安全管理中心

7.2.1 集中管控

本项要求包括：

a） 应实现以容器集群的方式对容器实例等资源进行统一编排调度管理；
b） 应通过容器镜像仓库对容器镜像进行集中管理；
c） 应对容器实例的各项性能指标进行集中监控。

7.3 安全建设管理

7.3.1 供应链管理

本项要求包括：

a） 应确保容器集群技术供应商的选择符合国家有关规定；
b） **应将容器集群供应链安全事件信息或安全威胁信息及时传达到容器集群客户**。

8 第三级安全要求

8.1 安全计算环境

8.1.1 身份鉴别

本项要求包括：

a） 应对容器集群的访问请求进行身份标识和鉴别，**并确保使用安全协议连接**；
b） 应确保容器集群管理平台和容器运行时不被匿名访问；
c） 应对容器镜像仓库的访问请求进行身份标识和鉴别，**并确保使用安全协议连接**。

8.1.2 访问控制

本项要求包括：

a） 应实现基于角色的访问控制，支持设定不同用户对容器集群内各类资源的权限控制；
b） 应实现对容器镜像仓库设定细粒度的访问控制，支持项目级别权限控制；
c） 应实现多用户场景下容器实例之间的网络访问控制；
d） 应保证当容器实例迁移时，集群用户和应用程序对资源的访问控制权限随其迁移；
e） 应实现容器实例对宿主机资源及内核调用的访问控制。

8.1.3 安全审计

本项要求包括：

a） 应实现容器镜像使用情况的审计，包括镜像上传、下载镜像事件审计，记录访问源 IP 并评估风险；
b） 应实现容器集群事件审计，包括各资源创建、更新、销毁等事件并评估风险。

8.1.4 入侵防范

本项要求包括：

a） 应确保容器镜像只使用安全的基础容器镜像，只包含必要的软件包或组件，对不合规的镜像进行告警；
b） 应确保容器镜像修复有补丁的超危、高危和中危网络安全漏洞；
c） 应确保容器镜像内不包含敏感信息、SSH 等证书文件，防止敏感信息泄露；
d） 应实现在镜像的持续构建或部署流程中集成扫描功能，支持对 Dockerfile 和容器镜像的网络安全漏洞扫描，并对不合规镜像进行拦截；
e） 除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行，并进行告警；
f） 应实现对容器集群和容器实例的各类攻击进行实时监测和告警，例如容器逃逸、用户提权、反弹 shell 等等；
g） 应实现容器集群内异常流量实时监测，并进行告警；
h） 应实现对失陷容器进行响应处置，例如重启容器、细粒度隔离容器，避免风险的蔓延。

8.1.5 恶意代码防范

本项要求包括：

a） 应确保容器镜像内不包含病毒、木马、webshell 等恶意代码，并进行告警；
b） 应对容器实例运行过程中发生的病毒、木马、webshell 等恶意代码上传、下载、横向传播等行为进行实时监测，并进行告警。

8.1.6 容器镜像保护

本项要求包括：

a） 应对容器镜像完整性进行校验，提供容器镜像签名功能，防止容器镜像被恶意篡改；
b） 应实现容器镜像文件的安全加密传输；
c） 应确保容器镜像的存储安全，使用国密算法等加密手段，防止容器镜像被非法访问。

8.2 安全管理中心

8.2.1 集中管控

本项要求包括：

a) 应实现以容器集群的方式对容器实例等资源进行统一编排调度管理，**并具备故障自动恢复、弹性伸缩的可用性能力**；
b) 应通过容器镜像仓库对容器镜像进行集中管理，**并实现多个容器镜像仓库数据同步**；
c) **应实现容器集群管理平面与业务平面的流量分离**；
d) 应对容器实例的各项性能指标进行集中**实时**监控，**包括但不限于 CPU 使用信息、内存使用信息、网络带宽信息等**。

8.3 安全建设管理

8.3.1 供应链管理

本项要求包括：
a) 应确保容器集群技术供应商的选择符合国家有关规定；
b) 应将容器集群供应链安全事件信息或安全威胁信息及时传达到容器集群客户；
c) **应将容器集群供应商的重要变更及时传达到容器集群客户，并评估变更带来的安全风险，采取措施对风险进行控制**。

9 第四级安全要求

9.1 安全计算环境

9.1.1 身份鉴别

本项要求包括：
a) 应对容器集群的访问请求进行身份标识和鉴别，并确保使用安全协议连接；
b) 应确保容器集群管理平台和容器运行时不被匿名访问；
c) 应对容器镜像仓库的访问请求进行身份标识和鉴别，并确保使用安全协议连接。

9.1.2 访问控制

本项要求包括：
a) 应实现基于角色的访问控制，支持设定不同用户对容器集群内各类资源**和容器镜像资源的细粒度**权限控制；
b) 应实现对容器镜像仓库设定细粒度的访问控制，支持项目级别权限控制；
c) 应实现多用户场景下容器实例之间基于**网络层和应用层的**访问控制；
d) 应保证当容器实例迁移时，集群用户和应用程序对资源的访问控制权限随其迁移；
e) **应实现基于安全容器运行时技术提供内核级别的强隔离**。

9.1.3 安全审计

本项要求包括：
a) 应实现容器镜像使用情况的审计，包括镜像上传、下载镜像事件审计，记录访问源 IP 并评估风险，**并对容器镜像仓库中长期未被下载使用且存在安全风险的镜像进行统计和删除**；
b) 应实现容器集群事件审计，包括各资源创建、更新、销毁等事件并评估风险，**支持对不同的事件类型开启和关闭，支持开关内置风险策略**。

9.1.4 入侵防范

本项要求包括：

a) 应确保容器镜像只使用安全的基础容器镜像，只包含必要的软件包或组件，对不合规的镜像进行告警，**并实现阻断**；
b) 应确保容器镜像修复有补丁的超危、高危、中危**及低危**网络安全漏洞；
c) 应确保容器镜像内不包含敏感信息、SSH 等证书文件，**环境变量中不包含用户名密码**，防止敏感信息泄露；
d) 应实现在镜像的持续构建或部署流程中集成扫描功能，支持对 Dockerfile 和容器镜像的网络安全漏洞扫描，并对不合规镜像进行拦截；
e) 除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行，并告警，**且能阻止不合规的容器实例运行**；
f) 应实现对容器集群和容器实例的各类攻击进行实时监测和告警，例如容器逃逸、用户提权、反弹 shell 等等，**并能够实时拦截处置**；
g) 应实现对被入侵容器进行响应处置，例如重启容器、**细粒度**隔离容器，避免风险的蔓延；
h) 应实现容器集群内异常流量实时监测，并进行告警**和阻断，且实现阻断策略的发布和撤销**。

9.1.5 恶意代码防范

本项要求包括：

a) 应确保容器镜像内不包含病毒、木马、webshell 等恶意代码，并进行告警**和阻断**；
b) 应对容器实例运行过程中发生的病毒，木马，webshell 等恶意代码上传、下载、横向传播行为进行实时监测，并进行告警**和阻断**。

9.1.6 容器镜像保护

本项要求包括：

a) 应对容器镜像完整性进行校验，提供容器镜像签名功能，防止容器镜像被恶意篡改；
b) 应实现容器镜像文件的安全加密传输；
c) 应确保容器镜像的存储安全，使用国密算法等加密手段，防止容器镜像被非法访问。

9.2 安全管理中心

9.2.1 集中管控

本项要求包括：

a) 应实现以容器集群的方式对容器实例等资源进行统一编排调度管理，以实现故障自动恢复、弹性伸缩的可用性能力；
b) 应通过容器镜像仓库对容器镜像进行集中管理，并实现多个容器镜像仓库数据同步；
c) 应实现容器集群管理平面与业务平面的流量分离；
d) 应对容器实例的各项性能指标进行集中实时监控，包括但不限于容器的 CPU 使用**与限制信息**、内存使用与**限制信息**、网络带宽信息、进程信息等。

9.3 安全建设管理

9.3.1 供应链管理

本项要求包括：

a) 应确保容器集群技术供应商的选择符合国家有关规定；
b) 应将容器集群供应链安全事件信息或安全威胁信息及时传达到容器集群客户；

c） 应将容器集群供应商的重要变更及时传达到容器集群客户，并评估变更带来的安全风险，采取措施对风险进行控制。

10 第五级安全要求

略。

附 录 A

（资料性附录）

容器安全场景与安全要求的选择和使用

A.1 场景与安全要求

在安全建设、整改与等级测评时应考虑上述三种场景有不同的适用要求。

表 A.1 各场景与等级保护技术要求的映射关系

场景	技术要求
公有容器集群	安全通用要求
	云计算安全扩展要求
	容器安全扩展要求
物理机部署的私有容器集群	安全通用要求
	容器安全扩展要求
私有云部署的私有容器集群	安全通用要求
	云计算安全扩展要求
	容器安全扩展要求

表 A.2 要求项与适用场景对照表

安全类	控制点	要求项	物理机部署的私有容器集群	公有容器集群/私有云部署的私有容器集群
安全计算环境	身份鉴别	a)应对容器集群的访问请求进行身份标识和鉴别，并确保使用安全协议连接；	★	★
		b)应确保容器集群管理平台和容器运行时不被匿名访问；	★	★
		c)应对容器镜像仓库的访问请求进行身份标识和鉴别，并确保使用安全协议连接。	★	★
	访问控制	a)应实现基于角色的访问控制，支持设定不同用户对容器集群内各类资源和容器镜像资源的细粒度权限控制；	★	★
		b)应实现对容器镜像仓库设定细粒度的访问控制，支持项目级别权限控制；	★	★
		c)应实现多用户场景下容器实例之间基于网络层和应用层的访问控制；	★	★
		d)应确保当容器实例迁移时，集群用户和应用程序对资源的访问控制权限随其迁移；	★	★

安全类	控制点	要求项	物理机部署的私有容器集群	公有容器集群/私有云部署的私有容器集群
		e)应实现基于安全容器运行时技术提供内核级别的强隔离；	★	★
	安全审计	a)应实现容器镜像使用情况的审计，包括镜像上传、下载镜像事件审计，记录访问源 IP 并评估风险，并对容器镜像仓库中长期未被下载使用且存在安全风险的镜像进行统计和删除；	★	★
		b)应实现容器集群事件审计，包括各资源创建、更新、销毁等事件并评估风险，支持对不同的事件类型开启和关闭，支持开关内置风险策略；	★	★
	入侵防范	a)应确保容器镜像只使用安全的基础容器镜像，只包含必要的软件包或组件，对不合规的镜像进行告警，并实现阻断；	★	★
		b)应确保容器镜像修复有补丁的超危、高危、中危及低危网络安全漏洞；	★	★
		c)应确保容器镜像内不包含敏感信息、SSH 等证书文件，环境变量中不包含用户名密码，防止敏感信息泄露；	★	★
		d)应实现在镜像的持续构建或部署流程中集成扫描功能，支持对 Dockerfile 和容器镜像的网络安全漏洞扫描，并对不合规镜像进行拦截；	★	★
		e)除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行，并告警，且能阻止不合规的容器实例运行；	★	★
		f)应实现对容器集群和容器实例的各类攻击进行实时监测和告警,例如容器逃逸、用户提权、反弹 shell 等等，并能够实时拦截处置；	★	★
		g)应实现对被入侵容器进行响应处置，例如重启容器、细粒度隔离容器，避免风险的蔓延；	★	★
		h)应实现容器集群内异常流量实时监测，并进行告警和阻断，且实现阻断策略的发布和撤销。	★	★
	恶意代码防范	a)应确保容器镜像内不包含病毒、木马、webshell 等恶意代码，并进行告警和阻断；	★	★
		b)应对容器实例运行过程中发生的病毒，木马，webshell 等恶意代码上传、下载、横向传播行为进行实时监测，并进行告警和阻断。	★	★
	容器镜像保护	a)应对容器镜像完整性进行校验，提供容器镜像签名功能，防止容器镜像被恶意篡改；	★	★
		b)应实现容器镜像文件的安全加密传输；	★	★
		c)应确保容器镜像的存储安全，使用国密算法等加密手段，防止容器镜像被非法访问。	★	★
安全管理中心	集中管控	a)应实现以容器集群的方式对容器实例等资源进行统一编排调度管理，以实现故障自动恢复、弹性伸缩的可用性能力；		★

安全类	控制点	要求项	物理机部署的私有容器集群	公有容器集群/私有云部署的私有容器集群
		b)应通过容器镜像仓库对容器镜像进行集中管理，并实现多个容器镜像仓库数据同步；	★	★
		c)应实现容器集群管理平面与业务平面的流量分离；	★	★
		d)应对容器实例的各项性能指标进行集中实时监控，包括但不限于容器的 CPU 使用与限制信息、内存使用与限制信息、网络带宽信息、进程信息等。	★	★
安全建设管理	供应链管理	a)应确保容器集群技术供应商的选择符合国家有关规定；	★	★
		b)应将容器集群供应链安全事件信息或安全威胁信息及时传达到容器集群客户；	★	★
		c)应将容器集群供应商的重要变更及时传达到容器集群客户，并评估变更带来的安全风险，采取措施对风险进行控制。	★	★

A.2 要求项与等级测评对象关系

表A.3 要求项与对象对照表

安全类	控制点	要求项	管理平台	计算节点	容器镜像仓库	容器实例	容器镜像
安全计算环境	身份鉴别	a) 应对容器集群的访问请求进行身份标识和鉴别，并确保使用安全协议连接；	★				
		b) 应确保容器集群管理平台和容器运行时不被匿名访问；	★	★			
		c) 应对容器镜像仓库的访问请求进行身份标识和鉴别，并确保使用安全协议连接。			★		
	访问控制	a) 应实现基于角色的访问控制，支持设定不同用户对容器集群内各类资源和容器镜像资源的细粒度权限控制；	★				
		b) 应实现对容器镜像仓库设定细粒度的访问控制，支持项目级别权限控制；			★		
		c) 应实现多用户场景下容器实例之间基于网络层和应用层的访问控制；				★	
		d) 应确保当容器实例迁移时，集				★	

安全类	控制点	要求项	管理平台	计算节点	容器镜像仓库	容器实例	容器镜像
		群用户和应用程序对资源的访问控制权限随其迁移；					
		e） 应实现基于安全容器运行时技术提供内核级别的强隔离；		★		★	
	安全审计	a） 应实现容器镜像使用情况的审计，包括镜像上传、下载镜像事件审计，记录访问源 IP 并评估风险，并对容器镜像仓库中长期未被下载使用且存在安全风险的镜像进行统计和删除；			★		
		b） 应实现容器集群事件审计，包括各资源创建、更新、销毁等事件并评估风险，支持对不同的事件类型开启和关闭，支持开关内置风险策略；	★				
	入侵防范	a） 应确保容器镜像只使用安全的基础容器镜像，只包含必要的软件包或组件，对不合规的镜像进行告警，并实现阻断；					★
		b） 应确保容器镜像修复有补丁的超危、高危、中危及低危网络安全漏洞；					★
		c） 应确保容器镜像内不包含敏感信息、SSH 等证书文件，环境变量中不包含用户名密码，防止敏感信息泄露；					★
		d） 应实现在镜像的持续构建或部署流程中集成扫描功能，支持对 Dockerfile 和容器镜像的网络安全漏洞扫描，并对不合规镜像进行拦截；					★
		e） 除基础平台组件外，应禁止业务容器实例使用特权用户和特权模式运行，并告警，且能阻止不合规的容器实例运行；				★	
		f） 应实现对容器集群和容器实例的各类攻击进行实时监测和告警，例如容器逃逸、用户提权、反弹 shell 等等，并能够实时拦截处置；	★			★	
		g） 应实现对被入侵容器进行响应				★	

安全类	控制点	要求项	管理平台	计算节点	容器镜像仓库	容器实例	容器镜像
		处置，例如重启容器、细粒度隔离容器，避免风险的蔓延；					
		h） 应实现容器集群内异常流量实时监测，并进行告警和阻断，且实现阻断策略的发布和撤销。				★	
	恶意代码防范	a） 应确保容器镜像内不包含病毒、木马、webshell 等恶意代码，并进行告警和阻断；					★
		b） 应对容器实例运行过程中发生的病毒，木马，webshell 等恶意代码上传、下载、横向传播行为进行实时监测，并进行告警和阻断。				★	
	容器镜像保护	a） 应对容器镜像完整性进行校验，提供容器镜像签名功能，防止容器镜像被恶意篡改；		★	★		★
		b） 应实现容器镜像文件的安全加密传输；					★
		c） 应确保容器镜像的存储安全，使用国密算法等加密手段，防止容器镜像被非法访问。			★		
安全管理中心	集中管控	a） 应实现以容器集群的方式对容器实例等资源进行统一编排调度管理，以实现故障自动恢复、弹性伸缩的可用性能力；	★				
		b） 应通过容器镜像仓库对容器镜像进行集中管理，并实现多个容器镜像仓库数据同步；			★		
		c） 应实现容器集群管理平面与业务平面的流量分离；	★				
		d） 应对容器实例的各项性能指标进行集中实时监控，包括但不限于容器的 CPU 使用与限制信息、内存使用与限制信息、网络带宽信息、进程信息等。	★				

参 考 文 献

[1] CIS Kubernetes Benchmark v1.4.0 - 01-31-2019
[2] CIS Docker Benchmark v1.2.0 - 07-29-2019
[3] NIST.SP.800-190 Application Container Security Guide