CSA 云安全联盟标准

CSA GCR XXXX—XXXX

云原生安全技术规范

Cloud Native Security Technology Specification

（征求意见稿）

2022－XX－XX 发布

云安全联盟大中华区　　发布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本文件由云安全联盟大中华区归口。

本文件主要起草单位：绿盟科技集团股份有限公司、腾讯科技（深圳）有限公司、公安部第三研究所、工商银行云计算实验室、深圳国家金融科技测评中心有限公司、浙江大华技术股份有限公司、北京小佑网络科技有限公司、安易科技(北京)有限公司、北京升鑫网络科技有限公司、北京天融信网络安全技术有限公司、浪潮云信息技术股份公司、中国电信研究院安全技术研究所、北京华云安信息技术有限公司、启明星辰信息技术集团股份有限公司、深信服科技股份有限公司、中孚信息股份有限公司、上海派拉软件股份有限公司、杭州安恒信息技术股份有限公司、北京探真科技有限公司、亚信安全科技股份有限公司、北京山石网科信息技术有限公司、北京雅客云安全科技有限公司、厦门服云信息科技有限公司、新华三技术有限公司、广州赛宝认证中心服务有限公司、北京网御星云信息技术有限公司、北森云计算有限公司。

本文件主要起草人：李雨航、刘文懋、谢奕智、陈妍、浦明、郑剑锋、刘连杰、申屠鹏会、刘强军、应天元、袁曙光、王亮、胡俊、王龑、饶飞、闻剑峰、马维士、郭伟华、朱青、杨文宏、茆正华、金丽慧、李祥乾、张鸣、黄猛、许兆彦、郭嘉伟、李安伦、黄凤贤、刘丕群、郭鹏程、姚凯。

1 范围

本文件主要为了提升云原生类产品技术，帮助更多安全从业人员解决在规划、实施和维护云原生安全体系架构时遇到的问题，针对云原生安全体系中涉及的每类技术制定的标准。

本文件适用于为云原生类产品厂商或甲方构建安全的云原生类产品提供参考和指导。

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，标日期的引用文件，仅该日期所对应的版本适用于本文件；不标注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语
GB/T 35273-2020 信息安全技术 个人信息安全规范
GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
JR/T 0095-2012 中国金融移动支付 应用安全规范
GM/T 0005-2021 随机性检测规范
GM/T 0028-2014 密码模块安全技术要求
GM/T 0054-2018 信息系统密码应用基本要求

3 术语和定义

GB/T 25069—2010、GB/T 35273-2020、ISACA-Glossary界定的下列术语和定义适用于本文件。

3.1
信息技术 Information Technology
用于输入、存储、处理、传输和输出数据的硬件、软件、通信和其他设施的总称。

3.2
角色 Character
在过程或组织的语境中所执行的功能。

3.3
对象 Object
系统中可供访问的实体。例如:数据、资源、进程等。

3.4
入侵 Intrusion
对某一网络或联网系统的未经授权的访问,即对某一信息系统的有意无意的未经授权的访问(包括针对信息的恶意活动)。

3.5
授权 Authorization
赋予某一主体可实施某些动作的权限的过程

3.6
数据保护 Data Protection
采取管理或技术措施,防范未经授权访问数据。

3.7
泄露 Breach
违反信息安全策略,使数据被未经授权的实体使用

4 缩略语

下列缩略语适用于本文件。

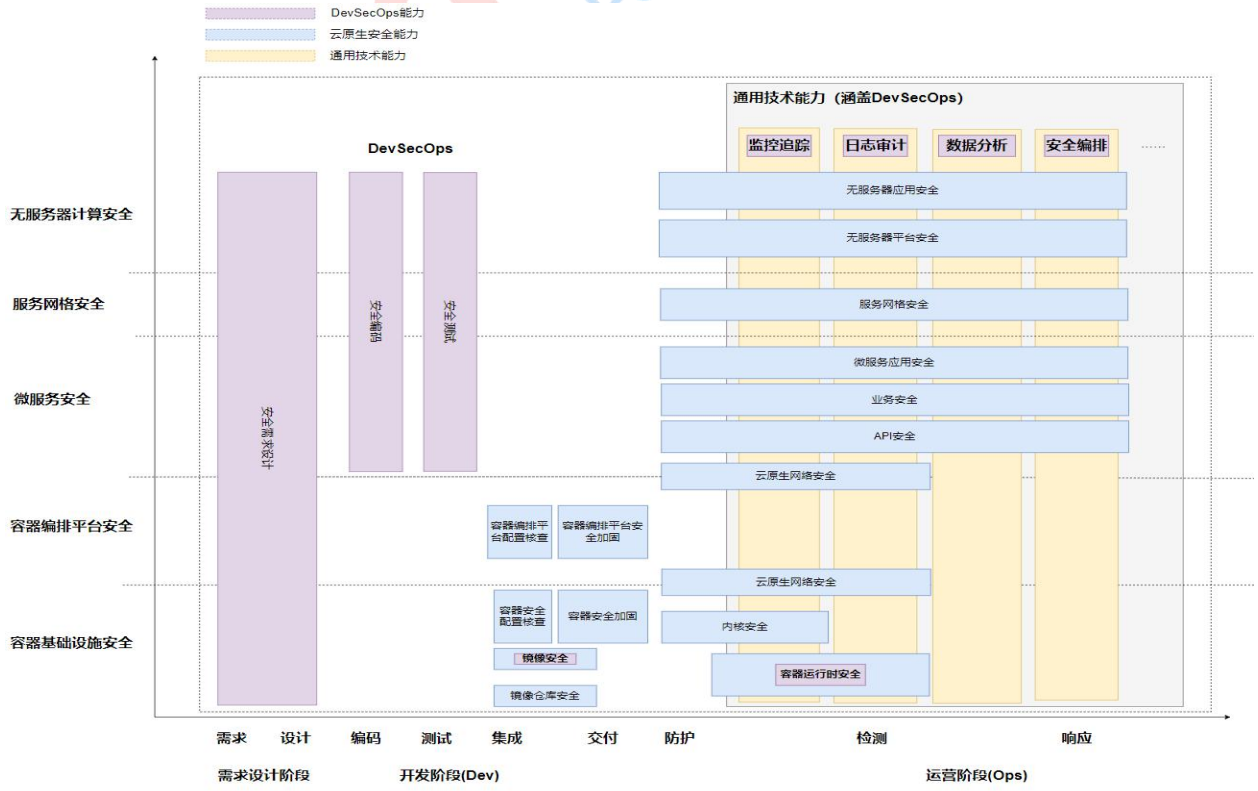
IT	Information Technology	信息技术
DPIA	Data Privacy Impact Assessment	数据隐私影响评估
SDK	Software Development Kit	软件开发工具包
SQL	Structured Query Language	结构化查询语言
KASLR	kernel address-space layout randomization	内核地址空间随机变化
TLS	Transport Layer Security	传输层安全性协议
API	Application Programming Interface	应用程序接口
SELinux	Security-Enhanced Linux	Linux的强制访问控制安全模块
KMS	Key Management Service	密钥管理服务
SSL	Secure Sockets Layer	安全套接字协议
LDAP	Lightweight Directory Access Protocol	轻型目录访问协议
SCIM	System for Cross-domain Identity Management	跨域身份管理介绍
OIDC	OpenId Connect	身份认证
SIEM	Security Information Event Management	安全信息与事件管理
gRPC	gRPC Remote Procedure Calls	远程过程调用系统
XSS	Cross Site Scripting	跨站脚本攻击
SSRF	Server-Side Request Forgery	服务端请求为伪造
XXE	XML External Entity Injection	XML外部实体注入
RCE	remote command/code execute	远程命令/代码执行漏洞
URL	Uniform Resource lLocator	统一资源定位系统
RBAC	Role-Based Access Control	基于角色的访问控制
ABAC	Attribute-Based Access Control	基于属性的访问控制
SIEM	Security Information and Event Management	安全信息和事件管理
KASLR	Kernel Address Space Layout Randomization	内核地址空间布局随机化
SMEP	Supervisor Mode Execution Prevention	管理模式执行保护

SMAP	Supervisor Mode Access Prevention	管理模式访问保护
KPTI	Kernel Page-Table Isolation	内核页表隔离

5 概述

云原生得以迅速发展，一方面得益于开发运营一体化（DevOps）的广泛采用，另一方面在IT基础设施的基础上，出现了更加弹性、敏捷的新型服务支撑体系。同样地，云原生安全也可按照开发运营安全（DevSecOps）和云化系统安全两个维度考虑安全机制。

表1描述了前述的云原生安全框架。其中，横轴是开发运营安全的维度，涉及需求设计（Plan）、开发（Dev）、运营阶段(Ops)，细分为需求、设计、编码、测试、集成、交付、防护、检测和响应阶段；而纵轴则是按照云原生系统和技术的层次划分，包括容器基础设施安全、容器编排平台安全、微服务安全、服务网格安全、无服务器计算安全五个部分，二维象限中列举安全机制（蓝色标注部分）已基本覆盖全生命周期的云原生安全要求。



此外，DevSecOps涉及的能力范围几乎覆盖了横轴和纵轴的各个阶段，可以参考图中紫色标注部分。最后，云原生安全体系中还应支持一些通用技术能力（黄色标注部分），这一部分能力主要体现在检测和响应阶段，并会同时覆盖DevSecOps中Ops阶段的能力。

6 云原生安全能力要求

6.1 容器基础设施安全能力要求

6.1.1 内核安全

【基础要求】

a) 应具备定期检测系统内核漏洞的能力，当发现内核存在漏洞时，发出告警信息；

b) 应具备系统内核升级管理和系统内核自动化批量滚动更新的能力；

c) 应具备内核态 Rootkit 类病毒检测的能力，当发现 Rootkit 时，进行 Rootkit 查杀；

d) 应具备系统内核完整性检测，关键内核数据结构（例如：中断描述符表 IDT、全局描述符表 GDT、系统调用表）完整性校验的能力；

e) 应具备识别内核自我防御模块（例如：GCC_PLUGIN_RANDSTRUCT、GCC_PLUGIN_LATENT_ENTROPY 等）的配置状态，提供安全加固配置建议的能力；

f) 应具备系统内核配置自动检测，内核安全模块（例如：SELinux、SMACK、Tomoyo、AppArmor、Yama、Seccomp）状态识别的能力；

g) 应具备收集内核、系统调用、应用的审计记录和日志的能力；

h) 应具备访问内核模块，阻止非特权用户加载内核模块，只有超级管理员或者物理本地用户才能够触发文件系统的模块加载的能力。

【增强要求】

a) 应具备检测内核堆栈缓冲区溢出等攻击的能力；

b) 应具备保证内存完整性的能力，应具备限制内核内存权限，支持内核内存栈不可执行、内核不能执行用户空间的代码（SMEP）、内核不能访问用户空间的数据（SMAP）的能力；

c) 应具备最小化系统调用访问的能力，只允许可信进程访问特定系统调用；

d) 应启用内核地址空间布局随机化（KASLR）机制；

e) 应支持配置内核页表隔离（KPTI）隔离用户空间与内核空间的内存。

6.1.2 容器安全配置核查

6.1.2.1 主机配置核查

a) 应对容器守护进程的审计能力进行检查；

b) 应对容器文件及目录的审计能力进行检查。

6.1.2.2 容器守护进程配置核查

a) 应禁止容器之间基于默认网桥模式的网络通信；

b) 应具备守护进程的实时恢复的能力；

c) 应具备配置集中和远程日志记录的能力；

d) 应关闭实验特性功能；

e) 应限制容器获取额外的权限。

6.1.2.3 容器守护进程文件配置核查

a) 应严格限制守护进程文件、目录权限；

b) 应严格限制仓库证书文件权限；

c) 应严格限制 TLS CA 证书文件权限；

d) 应严格限制服务器证书文件权限；

e) 应严格限制服务器证书密钥文件权限。

6.1.2.4 容器镜像和 BUILD 文件配置核查

a) 应保证镜像软件包最小化；

b) 支持对镜像进行漏洞扫描，并安装必要的安全补丁；

c) 应禁止配置文件存储账号密码及私钥。

6.1.2.5 容器运行时保护配置核查

a) 应禁止使用特权容器；

b) 应禁止宿主机上的敏感系统挂载在容器上；

c) 应禁止主机特权端口与容器进行映射；

d) 应对容器资源（例如：内存、处理器、网络、存储等）使用进行限制；

e) 应禁止共享主机的进程命名空间、网络命名空间、用户命名空间、IPC 命令空间、UTS 命令空间。

6.1.3 容器安全加固

6.1.3.1 宿主机的安全加固要求

【基础要求】

a) 应及时修复系统漏洞、应用补丁以及更新版本；
b) 应禁用或删除无用账号；
c) 应限制系统管理员账号远程登录；
d) 应关闭不必要的服务和端口；
e) 应设置用户登录的密码强度和使用期限。

【增强要求】

a) 应采用精简的安全的操作系统；
b) 应采用无密码的远程登录方式；
c) 应配置账户登录失败锁定策略。

6.1.3.2 运行环境的安全加固要求

【基础要求】

a) 应将容器平台更新到最新的稳定版本；
b) 应采用低权限用户的权限运行容器；
c) 应具备限制通过特权方式运行容器的能力；
d) 应具备限制每个容器所使用的资源的能力；
e) 应具备使用隔离的网络进行容器间通信的能力。

【增强要求】

a) 应具备容器间隔离的能力；
b) 应将容器的文件系统和挂载卷设为只读权限；
c) 应具备限制容器内部的系统调用的能力。

6.1.3.3 容器自身的安全加固要求

【基础要求】

a) 容器中不应运行无用的进程或服务；

b) 容器中不应包含无用的软件包。

【增强要求】

a) 容器中包含的软件包都应经过安全验证；

b) 容器中不应携带密码等敏感信息。

6.1.4 容器运行时安全

6.1.4.1 安全检测

【基础要求】

应对运行时容器进行安全检测，包括：

a) 应具备对运行时容器的漏洞进行扫描的能力；

b) 应具备对容器内运行程序的异常行为进行检测的能力，如异常登录、恶意反向连接、恶意进程调用、外部暴力破解、特权命令执行等；

c) 应具备对容器内的恶意代码进行检测的能力，包括但不限于二进制病毒木马、webshell 脚本等；

d) 应具备基于安全检测结果和告警策略进行告警的能力，支持对告警规则的配置；

e) 应具备检测、跟踪、汇总和报告来自容器的系统调用的能力，包括检测命名空间修改、制定目录访问，创建符号链接、文件或文件夹权限修改、非法端口启用等；

f) 应具备对容器端口扫描行为进行检测并告警的能力；

g) 应具备对容器启动行为异常检测的能力。

【增强要求】

应对运行时容器进行安全检测，包括：

a) 应具备对容器间的流量进行可视化展现的能力；

b) 应具备对容器逃逸行为进行检测的能力，包括但不限于由于权限不当、敏感挂载产生的逃逸行为，以及利用漏洞导致的逃逸行为;

c) 应具备对容器内访问敏感信息的行为进行检测的能力；

d) 应具备检测无文件攻击的行为的能力，包含但不限于内存级恶意代码检测；

e) 应具备基于创建容器行为模型的未知威胁检测的能力；

f) 应具备自定义的威胁检测能力，例如定义恶意进程、恶意 IP、恶意域名等。

6.1.4.2 安全防护

【基础要求】

应对运行时容器进行安全防护，包括：

a) 应具备对容器系统、容器文件进行访问控制的能力；

b) 应具备对容器间的网络流量进行访问控制的能力；

c) 应具备为容器的运行设置安全策略的能力，如以非超级管理员权限运行、限制使用特权用户运行等；

d) 应具备监控和防止对关键挂载点和文件的改变的能力，能够防止更改二进制文件、证书和远程访问配置；

e) 应具备防护攻击者通过反弹 shell、容器逃逸、本地提权、恶意软件等方式进行恶意入侵的能力；

f) 应具备通过虚拟补丁防护攻击的能力；

g) 应具备对容器运行时防护策略进行自定义配置，并对防护信息进行展示的能力。

【增强要求】

应对运行时容器进行安全防护，包括：

a) 应具备基于黑名单、白名单的容器程序运行控制的能力；

b) 应具备对源于失陷容器或针对正常容器的非法或异常行为进行控制的能力，包括控制容器进程、文件操作或网络访问，隔离失陷容器，暂停容器运行等；

c) 应具备与其他安全产品进行关联分析，联动处置的能力；

d) 应具备提供自动响应方式的能力。

6.1.5 镜像安全

6.1.5.1 镜像构建安全

【基础要求】

a) 应具备对构建环境进行漏洞扫描检查的能力，包括构建工具的安全漏洞，如Jenkins、GitLab 等；

b) 应具备对构建环境进行配置合规检查的能力，包括构建节点的操作系统配置、构建应用的不安全配置等；

c) 应具备对构建镜像的文件进行检查的能力,包括检查镜像标签的版本化管理、不要设置超级管理员等；

d) 应具备识别镜像是否基于基础镜像构建的能力；

- 操作系统基础镜像（busybox、Alpine、CentOS、Ubuntu、Debian）
- 编程语言基础镜像（Java 基础镜像、Python 基础镜像、NodeJs 基础镜像）
- 应用基础镜像（Nginx 基础镜像、Tomcat 基础镜像、Jetty 基础镜像）
- 主要由 Docker 镜像官网（Docker Hub）、Google 镜像（gcr.io）、各开源 OS 厂商官网等机构发布

e) 应具备对构建镜像相关的代码、文件和组件进行安全检查的能力。

【增强要求】

a) 应具备对安全镜像进行签名的能力，以保障镜像的分发安全。

6.1.5.2 镜像脆弱性评估

【基础要求】

a) 应具备对镜像内软件进行漏洞扫描的能力，包括针对二进制等构件和第三方框架的漏洞扫描；

b) 应具备对镜像进行基线合规检查的能力；

c) 应具备对镜像内木马病毒进行检测的能力；

d) 应具备对镜像内敏感文件和敏感信息进行检查的能力；

e) 应具备对镜像内网页后门进行检测的能力；

f) 应具备对镜像是否来自受信仓库进行检查的能力；

g) 应具备根据脆弱性评估结果划分镜像安全风险等级和提供解决方案建议的能力。

【增强要求】

a) 应具备通过原理扫描的方式发现和验证镜像漏洞的能力；

b) 应具备可适配定制化需求的自定义扫描策略能力。

6.1.5.3 高危镜像阻断

【基础要求】

a) 应具备镜像扫描能力可被持续集成系统调用，并根据镜像扫描结果对构建流程进行告警或阻断的能力；

b) 应具备镜像扫描能力可被持续交付系统调用，并根据镜像扫描结果对部署流程进行告警或阻断的能力；

c) 应具备镜像扫描能力与持续集成、持续交付系统联动、记录，并针对所记录的日志进行查阅的能力；

【增强要求】

a) 应具备将特定镜像添加到白名单或黑名单，并对黑、白名单进行策略修改的能力。

6.1.5.4 镜像传输安全

【基础要求】

a) 应具备镜像签名校验的能力，禁止未签名或者签名校验失败的镜像部署或上线。

【增强要求】

a) 应具备镜像签名密钥管理的能力，支持针对不同分类的镜像使用不同密钥。

6.1.6 镜像仓库安全

6.1.6.1 访问控制

a) 应具备主流的鉴权认证方法的能力；

b) 应设置网络访问控制策略以避免私有仓库暴露于互联网。

6.1.6.2 安全通信

a) 应使用有效的镜像仓库证书

b) 应具备镜像上传或下载阶段加密传输的能力

6.1.6.3 仓库镜像扫描

a) 应具备镜像仓库中对指定镜像的软件漏洞、恶意文件、配置等扫描检测的能力；

b) 应具备镜像仓库预设扫描、立即扫描等扫描任务管理的能力；

c) 应具备镜像批量/单项扫描的能力；

d) 应具备镜像仓库中镜像扫描结果信息展示的能力；

e) 应具备镜像仓库扫描策略自定义配置的能力；

f) 应具备对上传镜像进行一致性和完整性检测的能力；

g) 应具备对上传镜像进行风险评估的能力。

6.1.6.4 审计管理

a) 应具备对仓库所有必要操作记录以审计管理的能力。

6.1.6.5 权限管理

a) 应具备对仓库进行权限管理的能力，应保证仅授权用户有权修改、发布、删除相应镜像。

6.1.6.6 事件告警

a) 应具备镜像仓库的扫描告警通知相关方的能力。

6.1.6.7 容灾备份

a) 应具备异地容灾备份的能力。

6.1.7 容器日志审计

【基础要求】

a) 应具备统一的多数据源、多云原生组件的日志收集和处理能力；
b) 应具备多种云原生探针采集器（例如 ：DaemonSet、Sidecar、DockerEngine LogDriver 等）部署的能力；
c) 应具备异构日志格式化、统计分析、可视化的能力；
d) 应具备在日志数据中包含必要云原生资源的信息（例如： Namespace、Pod、Container、Image、Node 等）的能力；
e) 应具备安全策略配置的能力，可根据预先配置的规则检测出违规或异常行为；
f) 应具备出具报表报告的能力，支持 WORD、PDF、EXCEL、HTML 等格式的导出功能；
g) 应具备敏感数据过滤和数据脱敏的能力；
h) 应具备结构化日志输出和第三方对接的能力；
i) 应具备日志数据滚动存储、数据备份、还原的能力；日志数据留存应不少于 6 个月，应可还原指定时间范围的日志数据；
j) 应具备审计日志保护的能力，包括审计日志不应被未授权的访问、修改和破坏。

【增强要求】

a) 应具备多来源相同日志去重的能力；
b) 应具备基于日志以及相关的时序信息，使用机器学习算法，实现智能的告警、预测、根因分析的能力；
c) 应具备将历史日志对接到机器学习框架进行离线训练，并将训练后的结果加载到线上实时的算法库的能力；
d) 应具备基于日志实时计算的业务指标分析和告警的能力。

6.2 容器编排平台安全能力要求

6.2.1 容器编排平台安全配置核查

6.2.1.1 检测规则要求

6.2.1.1.1 组件基础安全配置

【基础要求】

a) 应具备禁止运行特权容器的能力；
b) 应具备禁止容器共享主机进程命名空间的能力；
c) 应具备禁止命名空间中的容器直接访问宿主机的网络资源的能力；
d) 应具备控制以超级管理员权限或超级管理员组成员身份运行容器应用的能力；
e) 应具备禁止容器升级到超级管理员权限的能力；
f) 应具备锁定无写入权限应用的容器文件系统的能力；
g) 应具备编排平台集群控制器设置密码保护的能力；
h) 应支持使用加密通道作为控制台的连接方式；
i) 应禁止将 API 服务绑定到不安全的地址/端口；
j) 应限制系统管理员以外的权限编辑 API 服务器的编排配置文件。

【增强要求】

a) 应具备设置一个只读的根文件系统的能力；
b) 应具备设置容器的强制访问控制机制（例如：SELinux）的能力；
c) 应具备限制容器执行系统调用的能力（例如：seccomp）；
d) 应具备在面向互联网的环境中使用安全容器（例如基于虚拟机技术的容器）的能力；
e) 应具备将控制器管理服务绑定到环回地址上，以最小化攻击面的能力；
f) 应具备配置容器镜像的来源，确保只有安全的镜像才能够部署的能力。

6.2.1.1.2 资源隔离与加固配置

【基础要求】

a) 应将不同的应用部署在不同的命名空间中，而非默认命名空间；
b) 应具备网络流量控制的能力；
c) 应具备限制命名空间或节点的资源使用的能力；

d) 应具备控制对敏感端口的网络访问的能力；

e) 应保护编排平台配置文件，防止非授权的访问。

【增强要求】

a) 应具备将工作节点与其他不需要与工作节点或编排平台服务通信的网络隔离的能力；

b) 应具备加密集群中的所有通信流量的能力；

c) 应具备通过配置静态数据加密或使用外部密钥管理服务来对敏感信息进行加密的能力；

d) 应具备禁止匿名请求的能力；

e) 应具备禁用基本身份认证方式的能力；

f) 应具备使用基于角色的访问控制并使用最小授权原则的能力；

g) 应具备为管理员账号分配最小权限的能力；

h) 应具备确保编排平台配置为只使用强加密密码的能力；

a) 应具备访问编排平台的请求应使用明确授权的能力；

b) 应具备启动编排平台证书认证的能力；

c) 应具备编排平台服务器/客户端证书轮换的能力。

6.2.1.2 安全管理

6.2.1.2.1 安全管理中心

a) 应具备借助第三方安全管理软件设立安全管理中心，对分散在网络中的各类设备、组件进行集中的管控、检测和审计的能力；

b) 应具备制定容器编排平台安全配置核查的工作机制和流程的能力。

6.2.1.2.2 审计日志配置

a) 应具备在主机层面、应用层面和云端进行日志记录的能力；

b) 应具备合理设置日志本地存储，防止因网络通信问题造成的丢失的能力。

6.2.1.2.3 监控配置

a) 应具备各类事件的告警和日志创建的能力；

b) 应具备配置统一的监控告警平台的能力；

c) 应具备设置合理的报警规则的能力；

d) 应具备将必要告警通知相应的人员和部门的能力。

6.2.1.2.4 其他

a) 应具备及时升级编排平台到最新的版本的能力；

b) 应具备在升级编排平台时删除不用的组件的能力。

6.2.2 容器编排平台安全加固

【基础要求】

a) 应具备集群内部组件之间的访问控制机制的能力(例如:Kubernetes 中的 kubelet、API Server、Etcd）；

b) 应具备对集群内组件的身份认证、密钥等敏感信息进行加密保护的能力；

c) 应具备集群内组件使用安全协议传输通信（例如：TSL/SSL 等）的能力；

d) 应具备对集群组件的安全漏洞库实时更新的能力；

e) 应具备限制外部网络访问容器的能力；

f) 应具备对集群共享数据库（例如：Etcd）存储内容加密的能力。

【增强要求】

a) 应具备对集群内组件的身份认证、密钥等敏感信息进行托管保护的能力；

b) 应具备容器编排组件入侵检测的能力

c) 应具备对集群私有数据库存储内容加密的能力。

6.2.3 认证授权

在主体（包括：用户、设备、应用、API 等）访问容器编排平台所管理的资源时，需要对访问主体的身份进行认证，并对访问行为进行授权鉴别；以确保主体身份的合法性和操作行为的合规性。

6.2.3.1 认证要求

【基础要求】

a) 应具备身份认证的能力，包括自然人、设备、应用或 API 等认证，以确保主体可信，可追责；
b) 应具备配置外部身份源（例如：LDAP、SCIM 等）的能力；
c) 应具备有效防止身份信息的泄露及盗用，对用户的身份信息进行安全存储的能力；
d) 应具备认证信息可以设置安全周期范围，超过安全周期需重新认证的能力；
e) 应具备对用户名/密码、数字证书、生物特征等认证凭证的管理，对凭证的签证者的签名、有效性进行验证的能力；
f) 应具备集成外部单点登录服务功能和标准认证协议（例如：OAuth2.0、OIDC 等）的能力；
g) 应使用安全协议完成身份认证过程，认证失败后实施安全控制措施；
h) 应具备客户端证书认证的能力，实现双向认证，支持多种协调通信加密方案；
i) 应具备静态令牌文件认证的能力，用令牌唯一标识请求者，并判定认证是否通过，并减少静态令牌认证范围；
j) 应支持提供多种认证方式（例如: OpenID、Keystone Password、匿名请求等），并减少匿名认证范围；

【增强要求】

a) 应具备认证协议的安全配置的能力，防止篡改、重置、假冒等攻击；
b) 应支持多种认证凭证类型，包括但不限于用户名/密码、动态令牌、数字证书、生物特征等；可根据不同安全需求支持不同认证凭证及多种认证凭证的组合，
c) 应具备对于用户身份敏感信息（例如：邮箱、手机号等）加密存储的能力；
d) 应具备扩展自定义认证方法的能力；
e) 应禁止静态令牌、静态文件、匿名请求等静态认证方式。

6.2.3.2 授权要求

在主体（包括：用户、设备、应用、API 等）访问容器编排平台所管理的资源时，需要对访问行为进行授权鉴别，以最小权限原则控制访问授权，容器编排平台对于访问授权的安全要求包括：

【基础要求】

a) 应具备采用基于角色的访问控制策略的能力，支持跨域授权；
b) 应具备采用基于集群资源的授权管理方式的能力，支持跨域授权；
c) 应具备对用户的授权信息进行安全存储的能力，以有效防止授权信息的泄露及盗用；
d) 应支持检查容器内运行的组件对集群资源的访问操作，并遵照授权策略执行访问控制，拒绝不符合授权的访问，保留授权验证记录；
e) 应具备权限范围配置的能力，以确保权限定义和授权边界清晰；
f) 应具备提供控制访问会话功能的能力，以停止非授权的集群资源访问；
g) 应具备提供永远拒绝（例如：AlwaysDeny）/始终允许（例如：AlwaysAllow）全局访问控制策略的能力。

【增强要求】

a) 应具备基于属性的访问控制策略的能力，应尽量细粒度划分权限范围，以原子化权限配置，以最小权限原则不过度授权；
b) 应具备自动监视的能力，以检测非授权的访问行为，并可以阻止非授权访问行为；
c) 应具备可扩展的第三方授权组件，并提供与容器内置组件的无缝衔接的能力。

6.2.4 密钥管理

编排平台相关的密钥管理应包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档与销毁等环节进行管理和策略制定的全过程。

6.2.4.1 密钥生成

【基础要求】

a) 应具备产生的密钥不重复，并保证其机密性的能力；
b) 密钥应在密码模块内部产生，不以明文方式出现在密码模块之外；

c) 应具备检查和剔除弱密钥的能力；

d) 生成密钥的审计信息应包括：种类、长度、拥有者信息、使用起始时间、使用终止时间。

【增强要求】

a) 密钥生成使用的随机数应符合 GM/T0005 要求，密钥应在符合 GM/T0028 的密码模块中产生；

b) 应使用国家密码管理部门批准的硬件物理噪声源产生随机数。

6.2.4.2 密钥存储

【基础要求】

a) 应具备密钥加密存储的能力，采取必要的安全防护措施，防止密钥被非法获取；

b) 密钥加密密钥应存储在符合 GM/T0028 的二级及以上密码模块中。

【增强要求】

a) 密钥加密密钥，用户签名私钥应存储在符合 GM/T0028 的三级及以上密码模块中或通过国家密码管理部门核准的硬件密码产品；

b) 应具备密钥泄露时的应急处理和响应措施的能力。

6.2.4.3 密钥分发

【基础要求】

a) 应具备密钥分发安全措施的能力，以防止在分发过程中泄露；

b) 应具备身份鉴别的能力，以保障数据完整性、数据机密性；

c) 应具备抗截取、假冒、篡改、重放等攻击的能力，以保障密钥的安全性。

6.2.4.4 密钥导入与导出

【基础要求】

a) 应采取有效的安全措施，保障密钥导入与导出的安全，并保证密钥的正确性，包括采用加密、知识拆分或者使用专用设备等方法。

【增强要求】

a) 应具备保证系统密码服务不间断的能力。

6.2.4.5 密钥使用

【基础要求】

a) 密钥应明确用途，并按用途正确使用；
b) 采取必要的安全防护措施，防止密钥的泄露，以及防止密钥被非法替换和使用；
c) 对于公钥密码体制，在使用公钥之前应对其进行验证；
d) 应按照密钥更换周期要求更换密钥；
e) 应采取有效的安全措施，保证密钥更换时的安全性；
f) 应支持密钥泄露时停止使用，并启动相应的应急处理和响应措施。

6.2.4.6 密钥备份与恢复

【基础要求】

a) 应制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；
b) 应具备密钥备份或恢复应进行记录，并生成审计信息的能力，审计信息包括备份或恢复的主体、备份或恢复的时间等。

6.2.4.7 密钥归档

【基础要求】

a) 应采取有效的安全措施，保证归档密钥的安全性和正确性；
b) 归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；
c) 密钥归档应进行记录，并生成审计信息，审计信息包括归档的密钥归档的时间等；
d) 归档密钥应进行数据备份，并采用有效的安全保护措施。

6.2.4.8 密钥销毁

【基础要求】

a) 应具备在紧急情况下销毁密钥的能力。

6.2.5 网络安全

【基础要求】

a) 应具备包含源 IP、目的 IP 和目的服务端口的部分和全部组合的访问控制能力；
b) 应具备缺省放行和阻断的访问控制能力；
c) 应具备对具体某个网络连接访问放行和阻断动作的控制能力；
d) 应具备对容器应用的访问控制能力；
e) 应具备对宿主机应用的访问控制能力；
f) 应支持对逻辑边界的访问控制能力，逻辑边界包含命名空间和租户；
g) 应具备抵抗绕过能力；
h) 应具备对容器网络或容器端口扫描行为进行检测并告警的能力；
i) 应具备对网络攻击行为进行入侵防御的能力，包括跨站攻击、SQL 注入攻击、拒绝服务攻击、异常报文攻击等。

【增强要求】

a) 应具备基于云资产为对象的访问控制能力，云资产至少包括容器应用、服务与宿主机应用等；
b) 应具备基于域名的访问控制能力；
c) 应具备根据环境内业务访问关系自动生成的能力；
d) 应具备记录网络会话日志能力；
e) 应具备根据协议设置流量隔离能力；
f) 应具备针对租户、节点、以及容器等对象的统一的访问控制能力；
g) 应具备对隔离策略自定义创建、更新、删除和自动推荐的隔离策略管理能力。
h) 应具备对编排平台下的容器最小部署单元的自动隔离能力。
i) 应具备与其他安全产品进行关联分析，联动处置的能力；
j) 应具备多种自动响应方式的能力。

6.2.6 编排系统日志审计

【基础要求】

a) 应支持记录请求过程中的事件 ID，系统运行过程中的操作资源、操作内容、操作结果、账户、角色、时间等多维度信息，以便后期快速定位错误

b) 应支持记录容器编排系统中不同资源（如计算资源，网络资源，存储资源）的创建、更新、删除、访问等操作；

c) 应具备记录容器编排系统中各类资源使用权限变化的能力，以便后期快速定位错误

d) 应具备选择记录日志的级别的能力，以便应对资源开销，具体级别可以包括：

- *不记录日志（例如：None）*
- *记录请求中的元数据（例如：Metadata）*
- *记录请求的全部信息(例如：Metadata、Request Body)*
- *记录请求响应的全部信息（例如：Request Body、Response Body、Metadata）*

e) 应具备选择记录日志类型的能力，例如基本日志、告警日志、错误日志等

f) 应具备在日志收集阶段能覆盖全部的数据来源，并且能保证日志数据连续性的能力。即确保系统收集日志与实际产生日志不存在较大偏差，并且在面对突发流量时能通过一定的缓存机制保证数据的连续性。

g) 应具备针对不同类型的资源分配不同审计策略的能力，此处审计策略可具体指“应记录哪些事件”，“应包含哪些数据”等

h) 应具备针对请求的不同阶段记录日志的能力，例如在容器编排系统中，一次请求的生命周期可简单分为以下阶段：

- *请求接受（例如：RequestReceived）*
- *请求开始（例如：ResponseStarted）*
- *请求处理（例如：RequestHandled）*
- *响应完毕（例如：ResponseCompleted）*

i) 应具备针对收集日志的数据格式进行结构化调整的能力

j) 应具备针对收集日志中的事件进行自动聚合的能力，以便于后期进行分类查询

k) 应具备向外导出日志的能力，以便与外部日志分析系统（例如：SIEM）进行联动

l) 当日志被传送至外部日志服务或系统时，应支持使用加密方式进行传输，如 TLS；

m) 应具备多维日志查询条件的能力，如可根据月、周、日、时、自定义时间范围等条件进行查询

n) 应具备为日志存储提供参数配置的能力

- *需提供日志存储方式的配置*
- *需提供日志存储格式的配置*
- *需提供日志存储路径的配置*
- *需提供日志保留最多天数的配置*
- *需提供日志保留最大数量的配置*
- *需提供日志备份数量的配置*
- *需提供日志文件占用最大磁盘空间的配置*

【增强要求】

a) 应具备将聚合与加工后的日志数据定制为各类图表的能力，以便于实时观察系统的运行状态，找出日志事件可能隐藏的规律和隐患

b) 应具备自动根据冷/热数据采用不同的硬件策略的能力

6.3 微服务安全能力要求

6.3.1 API 安全

6.3.1.1 云原生 API 网关

【基础要求】

a) 应具备对 API 进行认证授权的能力，为未授权的 API 提供保护，具备横向与纵向的权限隔离；

b) 应具备对 API 访问频率与流量带宽限制的能力；

c) 应具备对基本数据类型过滤的能力，包括通过增加规则过滤常规漏洞的攻击；

d) 应具备特定请求（来源 IP、UA 头、特殊路由）封禁的能力；

e) 应具备常见 API 协议与规范（例如：gRPC、GraphQL、Restful、SOAP 等）兼容的能力；

f) 应具备对 API 传输过程中的敏感数据（例如：身份信息、地理位置）进行加密的能力；

g) 应具备 API 调用向第三方审计系统输出日志的能力；

h) 应具备生产环境中隐藏 API 文档的能力，以防止 API 外泄。

【增强要求】

a) 应具备为 API 增加自定义数据头能力；

b) 应具备安全插件扩展能力，包括针对机器流量检测的能力、针对访问行为特征进行分析的能力、反爬虫机制、数据防泄漏的能力；

c) 应具备流量镜像能力，例如 API 网关能将 API 的访问数据镜像至其他安全设备；

d) 应具备数据防篡改的签名机制的能力，以防范中间人攻击。

6.3.1.2 API 脆弱性评估

e) 应具备 API 认证能力，支持多种 API 评估过程中使用的权限认证机制；

f) 应具备针对常规 Web 漏洞检测的能力（例如：SQLi、XSS、SSRF、XXE、RCE 等）；

g) 应具备 API 组件指纹识别的能力；

h) 应具备 API 常用开发组件（例如：fastjson、shiro、log4j、spring 等）漏洞检测的能力；

i) 应具备 API 数据格式处理的能力，生产环境下针对无法处理的数据提供统一处理机制；

j) 应具备 API 脆弱性评估过程中的敏感数据脱敏的能力；

k) 应具备通过流量分析 API 调用的能力，可通过镜像流量分析出可调用的 API，并检测其脆弱性；

l) 应具备 API 脆弱性评估结果可视化和导出的能力。

【增强要求】

a) 应具备 API 调用链全链路分析的能力，以分析 API 之间的调用关系；

b) 应具备 API 自动化模糊测试的能力，以识别未知漏洞。

6.3.2 微服务应用安全

6.3.2.1 认证能力要求

【基础要求】

a）应具备针对不符合认证策略流量预警的能力；

b）应具备面向外部服务访问认证的能力；

c）应具备面向内部服务访问认证的能力；

d）应具备跨集群、混合云环境中的微服务内部与外部访问认证的能力。

【增强要求】

无

6.3.2.2 授权能力要求

【基础要求】

a）应具备配置微服务之间能否访问的策略的能力

b）应具备针对不符合授权策略的流量预警的能力

c）应具备面向外部服务访问授权的能力

d）应具备面向内部服务访问授权的能力

e）应具备以微服务粒度检测与绘制微服务之间访问关系的能力

f）应具备跨集群、混合云环境下的微服务内部与外部授权机制的能力

g）应具备基于角色的访问控制的能力

【增强要求】

a）应具备以微服务 API 粒度检测与绘制微服务间的访问关系的能力

b）应具备配置微服务 API 之间能否访问的策略的能力

c）应具备通过网络访问日志推荐授权策略的能力

d）应具备当微服务访问出现变化时，可配置默认策略，并发出变动预警消息的能力

6.3.2.3 API 安全

【基础要求】

a） 应具备对微服务的 API 进行自动发现的能力。

b） 应具备对微服务的 API 进行标记和管理的能力。

c） 应支持客户端访问服务端的凭证（例如：Token）授权认证机制；

d） 应支持服务端对客户端访问验证时间戳超时机制；

e） 应支持服务访问签名机制保证数据完整性；

【增强要求】

a） 应具备微服务间 API 访问时序分析与上下游分析的能力；

b） 应具备微服务间 API 访问拓扑可视化的能力

c） 应具备 API 调用的访问频率控制能力。

6.3.2.4 通信安全

【基础要求】

a） 应具备微服务间双向通信加密（例如：mTLS）的能力；

b） 应具备对通信安全策略可配置的能力。

【增强要求】

a） 应具备对通信安全策略可配置至 API 级别的能力。

6.3.2.5 凭证管理

【基础要求】

a） 应具备高可用的重要凭证存储与管理的能力，包括密码，密钥等。

【增强要求】

a） 应具备动态修改凭证的能力。

6.4 服务网格安全能力要求

【基础要求】

a) 应具备配置服务设置双向加密通信的能力
b) 应具备遵循最小授权原则，配置服务细粒度认证授权策略的能力
c) 应具备配置专用网关隔离敏感服务的能力
d) 应具备及时应用安全补丁的能力
e) 应具备在应用配置后进行配置有效性检查的能力
f) 应具备生产环境中禁止使用实验性功能的能力
g) 应具备禁止将服务网格控制面组件服务或数据面调试服务暴露至外部网络的能力

【增强要求】

a) 应具备配置应用默认拒绝的授权策略的能力
b) 应具备配置请求路径规范化的能力
c) 应具备支持配置明确的流量协议的能力

6.5 无服务器计算安全能力要求

6.5.1 无服务器应用安全

【基础要求】

a) 应支持应用通信过程中的数据被加密，（如：使用 TLS。确保数据加密被强制执行、使用 HTTP 严格安全传输协议 HSTS ）；禁止缓存包含敏感数据的响应，对于没必要存放的、重要的敏感数据，应当尽快清除；并确保存储的所有敏感数据被加密；
b) 应具备应用接口的安全防护能力。如：注入风险，应避免使用解释器把界面提供的参数直接穿透 ORM 或实体框架；
c) 应具备对于输入参数执行完整性检查的能力。如：任何序列化对象的数字签名，以防止恶意对象创建或数据篡改；
d) 应具备针对特殊字符转义的输入验证的能力，如：应支持白名单，黑名单形式
e) 应具备防护 SQL 注入、XSS 攻击、网页木马、网站扫描、Webshell、跨站请求伪造（CSRF）、系统命令注入、文件包含攻击、目录遍历攻击、信息泄露攻击、Web 漏洞攻击的能力；

f) 应支持 HTTP 方法过滤、HTTP 头部字段 Referer、User-Agent 等注入检测、Host 检测、URL 溢出检测、POST 实体溢出检测、HTTP 头部溢出检测、range 字段防护、multipart 头部字段异常检测、Content-Type 头部字段异常检测，满足 HTTP 协议异常识别方法；

g) 应具备针对自定义文件下载类型过滤，数据防泄漏的能力；

h) 应具备 XML 和 JSON 格式的 API 解析和防护能力；

i) 应具备自定义文件上传类型过滤，防文件上传攻击的能力

j) 应具备针对不同访问类型拥有不同身份验证、访问控制的能力；

k) 应禁止使用含有漏洞的第三方依赖库，转而使用相对安全的依赖库，如：使用云服务商提供的 SDK；

l) 应支持针对具体应用内容进行代码审计的能力；

m) 应具备在应用设计阶段对无服务器资产业务进行梳理的能力，如：

- *确认应用中函数间的逻辑关系*
- *确认应用的数据类型及数据的敏感性*
- *评估无服务器数据的价值*
- *评估可访问数据 API 的安全性*

n) 应支持函数执行顺序发生变化后，再次进行代码安全审计，从而可避免新的输入源带来的风险

6.5.2 无服务器平台安全

【基础要求】

a) 应支持账单告警机制，以便有效对拒绝钱包服务攻击（DoW Denial of Wallet）进行缓解，包括但不限于：

- *应具备为无服务器函数的调用频次设定阈值告警的能力*
- *应具备为无服务器函数的单次调用费用设定阈值告警的能力*

b) 应支持函数资源限额的配置，以便有效对拒绝钱包服务攻击进行缓解，包括但不限于：

- *应具备为函数资源进行内存分配的能力*

- *应具备为函数资源进行临时磁盘容量分配的能力*
- *应具备为函数资源进行进程数和线程数配置的能力*
- *应具备为函数执行时长进行阈值分配的能力*
- *应具备为函数接受载荷大小进行配置的能力*
- *应具备为函数并发执行数进行配置的能力*

c) 应具备无服务器应用监控的能力，以便识别和报告异常行为，如未授权访问、过度执行函数、过长执行时间等

d) 应具备无服务器应用日志审计的能力，以便从日志维度检测异常行为

e) 应具备无服务器应用链路追踪的能力，以便从追踪信息中了解函数的运行状况

f) 应具备无服务器函数间身份认证的能力

g) 应具备无服务器函数间细粒度基于角色的访问控制（RBAC Role Based Acccess Control）的能力

h) 应具备针对已部署但未使用的函数进行追踪的能力，并制定一套机制可以删除他们，从而降低额外风险

i) 应具备无服务器函数执行和访问其他资源权限（AWS S3、DynamoDB、Azure Blob等）的能力，需遵循最小权限的配置原则，以确保每个函数只能访问并操作有限的资源

j) 应具备针对无服务器函数中的开源依赖库漏洞的扫描能力

k) 应具备无服务器函数代码的安全审计能力

l) 应具备安全的函数运行时环境的能力，包括但不限于：

- *应确保函数以非超级管理员权限运行*
- *应确保函数运行时环境中不含有敏感的密钥、令牌等信息*
- *应限制函数运行时环境中目录的写操作*
- *应确保函数运行时环境未启用不安全的配置及挂载*
- *应确保函数运行时自身的安全性，如避免使用含有漏洞的 Docker*

m) 应具备无服务器应用镜像的安全保护的能力，包括但不限于：

- *应禁止应用镜像中使用不安全的第三方组件*
- *应禁止应用镜像中含有恶意软件，如恶意挖矿程序等*

- *应禁止应用镜像中含有易泄漏的敏感信息，如数据库密码、证书和私钥等*

n) 应具备无服务器应用镜像扫描的能力

o) 应支持轮换出口 IP、冷却（禁止重复 IP 的使用）IP、扩大 IP 池、出口 IP 不在租户中共享，以避免攻击者利用出口 IP 进行 DoS 攻击等恶意操作

p) 应具备用户密钥统一纳管的能力

q) 应具备虚拟私有云（VPC）底层资源隔离的能力

r) 应具备无服务器函数在网络层面的隔离的能力

s) 应具备函数即服务（FaaS）平台操作系统软件漏洞修复的能力

t) 应具备无服务器函数代码部署时的有效性和完整性的能力，需要对用户进行授权及代码签名，并且支持签名配置管理等操作。