ICS 35.040
CCS L 80

团　　体　　标　　准

T/ISEAA 004—2023

网络安全等级保护容器安全要求

Container security requirement for classified protection of cybersecurity

2023-04-19 发布　　2023-07-01 实施

中关村信息安全测评联盟　发布
中国标准出版社　出版

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。

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：公安部第三研究所、公安部网络安全保卫局、北京小佑网络科技有限公司、深信服科技股份有限公司、阿里云计算有限公司、广西网信信息技术有限公司、安徽省电子产品监督检验所（安徽省信息安全测评中心）、北京升鑫网络科技有限公司、华为技术有限公司、中移动信息技术有限公司、杭州默安科技有限公司、北京经济管理职业学院。

本文件主要起草人：张振峰、祝国邦、范春玲、刘静、江雷、陈广勇、李明、袁曙光、白黎明、刘斌、杨杜卿、伊玮珑、冯伟、王理冬、陈妍、张艳、王明亮、何坤鹏、李京儒、胡俊、黄敏、刘剑波、孙海青、沈锡镛、袁礼。

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。本文件将 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 GB/T 22239—2019《信息安全技术　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

本文件规定了在云环境中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。

本文件适用于在云环境中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

容器镜像 container image

包含运行容器所需的所有软件的包文件。

3.2

容器实例 container instance

在应用虚拟化环境中运行的容器镜像的具体对象。

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。