# 《网络安全等级保护容器安全要求》
# 编制说明

## 一、工作简况

### 1、任务来源

为配合国家网络安全等级保护制度 2.0 全面推进，加强对采用容器集群技术的等级保护对象的安全保护指导工作，由中关村信息安全测评联盟组织发起，公安部信息安全等级保护评估中心为标准编制牵头单位，中关村信息安全测评联盟为项目归口管理单位，会同小佑科技有限公司、深信服科技有限公司、阿里云计算有限公司、广西网信测评有限公司、安徽省电子信息测评中心共同编制《网络安全等级保护容器安全要求》（简称“容器安全要求”）

### 2、编制背景

等级保护 2.0 核心标准 GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》（简称“基本要求”）自 2019 年修订发布以来，广泛覆盖了云计算、移动互联、物联网、工业控制等各类等级保护对象。按照通用要求加扩展要求的思路，解决了新型等级保护对象安全要求的基础架构问题。近年来，随着微隔离技术的不断成熟以及用户对计算资源复用率需求的进一步提高，容器集群技术逐渐普及，但同时也暴露了一些新的安全威胁，因此需要对《基本要求》进一步扩展，覆盖新暴露的威胁。

本标准将《基本要求》的安全通用保护要求进行细化和扩展，提出容器安全保护技术要求。本标准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，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。

### 3、主要工作过程

2021 年 4 月，受中关村信息安全测评联盟委托，对容器安全相关标准进行预研，标准立项名称为《信息安全技术 网络安全等级保护容器安全评估指引》。

2021 年 6 月，成立标准编制组，研究相关技术和标准框架，完成文档基础

架构、编制成员任务分工。

2021 年 9 月，形成草案第一稿。

2022 年 1 月，讨论调整了标准覆盖对象范围为容器集群，确定标准目标是提出安全扩展要求。调整标准名称为《网络安全等级保护容器安全要求》，形成《容器安全要求》草案第二稿及各级差别对照表。

2022 年 2 月，进一步完善草案第三稿。

2022 年 3 月，组内征求意见，进一步修改完善形成草案第四稿、第五稿和第六稿。

2022 年 4 月，评估中心组织内部专家进行了标准研讨，根据专家意见，对文档的结构、内容进行修订、完善，形成《网络安全等级保护容器安全要求》征求意见稿，与 4 月底提交联盟秘书处。

### 4、标准起草单位和人员

本标准起草单位：公安部第三研究所（公安部信息安全等级保护评估中心）、小佑科技有限公司、深信服科技有限公司、阿里云计算有限公司、广西网信测评有限公司、安徽省电子信息测评中心。

本标准主要起草人：张振峰、李明、袁曙光、白黎明、刘斌、杨杜卿、伊玮珑、冯伟、王理冬、王明亮、何坤鹏、李京儒。

公安部信息安全等级保护评估中心负责组织《容器安全要求》标准文本的起草，按照团体标准报批要求，分阶段完成征求意见稿、送审稿、报批稿和其他相关材料，负责收集各起草单位的指导意见，进行汇总、分析，完成全文的编写、统稿工作。

## 二、标准主要内容及依据

标准编制组前期深入研究容器保护对象的特点，结合容器技术现有技术的发展水平、系统形态和安全防护需求，分析不同形态容器运营者需要对抗的安全威胁，以及应采取的安全机制或措施，明确不同安全保护等级容器保护对象应实现的安全保护目标。通过吸取国际、国内先进的信息安全技术和经验，结合编制组成员单位既有工作经验，编制组确定本标准的范围是采用容器集群技术的等级保护对象，对未采用容器集群技术的等级保护对象，其所用到的容器对象视为普通计算环境对象，适用《基本要求》安全通用要求。

此外，编制组研究构建了采用容器集群技术的等级保护对象抽象化结构，给出了容器集群架构模型及各部分组件的功能说明。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，不适用于本标准。针对以上的抽象结构，本标准给出了一至四级的安全要求。

同时本标准立足使用的便利性和规范性，结合等级保护的特点，以附录形式给出了公有容器集群、物理机部署的私有容器集群以及私有云部署的私有容器集群与适用安全通用要求和扩展要求的对应关系；本标准还给出了要求项与适用场景的对应关系以及要求项与保护对象的映射关系。编制组力求通过以上对应映射，为标准使用者提供可落地的参考建议。

具体内容包括：

1）第一章 范围

本标准规定了采用容器集群技术的等级保护对象的安全扩展要求，包括第一级至第四级网络的要求。

本标准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）第二章 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标准必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本标准；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

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）第三章 术语和定义

本标准充分参考了已有标准的定义，对新的术语进行了定义，对后续章节内

容描述提供了术语支持。

4）第四章 缩略语

本部分给出了标准中的缩略语解释。

5）第四章 概述

对于容器集群架构，给出抽象框架，并给出各部分功能描述。

6）第五章至第九章

本部分为标准的主体内容，根据容器集群技术现状，参照通用要求的级差特点和相应等级保护能力，提出了第一级到第五级的各级别基线要求，包括了采用容器集群技术的等级保护对象应实现的特殊安全保护要求。

6）附录 A（资料性附录）

本部分给出了容器安全场景与安全要求的选择和使用的参考建议。以表格形式给出了不同场景下适用标准的对应关系、不同场景下适用的容器安全要求的要求项以及要求项与保护对象的对应关系。

## 三、与相关法律法规及国家有关规定、国内相关标准的关系

1) 与《基本要求》的关系

本标准定位为《基本要求》的安全扩展要求，需配合《基本要求》共同使用。如等级保护对象为云平台上的容器云，则应同时使用《基本要求》的安全通用要求、云计算安全扩展要求以及本标准《容器安全要求》。

2) 和其他国标的关系

编制组密切关注国标的工作进展，积极参与其他标准的编制工作，已发布和在研国家标准中，目前尚无容器安全相关的其他国标。

## 四、重大分歧意见的处理经过和依据

本标准起草过程中无重大分歧意见。

## 五、其他应予说明的事项

无。