云数据中心安全建设与运维

职业技能等级标准

（2021年1.0版）

深信服科技股份有限公司 制定

2021 年 3 月 发布

目 次

前　言

本标准按照 GB/T1.1-2020 《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》给出的规则起草。

本标准起草单位：深信服科技股份有限公司、暨南大学、北京邮电大学、青岛大学、吉利学院、深圳职业技术学院、深圳信息职业技术学院、天津职业大学、深圳技师职业学院、北京信息职业技术学院、武汉职业技术学院、重庆电子工程职业学院、内蒙古电子信息职业技术学院、许昌职业技术学院、盐城工业职业技术学院、山东商业职业技术学院、河南司法警官职业学院、河南信息工程学校。

本标准主要起草人：魏林锋、雷敏、咸鹤群、吕峻闽、王隆杰、柳伟、张景强、廖银萍、史宝会、杨旭东、武春岭、郝俊寿、孟敏杰、王国军、单锦宝、王惠斌、余飞跃、李文杰、李洋、严波、黄浩、袁泉、石岩、方明理、迟忠旸、吕沐阳、祖少良。

1 范围

本标准规定了云数据中心安全建设与运维职业技能等级对应的工作领域、工作任务及职业技能要求。

本标准适用于云数据中心安全建设与运维职业技能等级培训、考核与评价，相关用人单位的人员聘用、培训与考核可参照使用。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 31167-2014 信息安全技术 云计算服务安全指南

GB/T 31168-2014 信息安全技术 云计算服务安全能力要求

GB/T 25068.1 信息技术 安全技术 IT 网络安全

GB/T 25069-2010 信息安全技术 术语

GB/T 20270-2006 信息安全技术 网络基础安全技术要求

GB/T 20272-2006 信息安全技术 操作系统安全技术要求

GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

GB 17859-1999 计算机信息系统安全保护等级划分准则

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

3 术语和定义

3.1 云计算 cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并可按需自助获取和管理资源的模式。

[GB/T 32400-2015,定义3.2.5]

3.2 云安全 cloud security

根据云计算的服务模式、部署方式以及角色，提供有针对性的安全方案，保护云计算平台及云租户业务应用系统的安全。

[GB/T 32400-2015,定义3.2.7]

3.3 网络安全 cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[GB/T 25069-2010，定义 2.1.53]

3.4 云安全联盟 cloud security alliance CSA

云安全联盟CSA作为业界权威组织，致力于在云计算环境下为业界提供最佳安全解决方案。

[GB/T 32400-2015,定义3.2.23]

3.5 云工作负载保护cloud workload protection platforms CWPP

基于云工作负载的安全解决方案，通过集成的统一安全策略来满足现代混合数据中心架构中，服务器工作负载的保护要求。

[GB/T 20984-2007，定义 3.15]

3.6 微隔离 microsegmentation

微隔离使用策略驱动的防火墙(通常是基于软件的)或网络加密技术，将数据中心和公共云基础设施中的工作负载隔离为服务，并将其放入容器中，其中也包括混合云场景中的工作负载。

[GB/T 20984-2007，定义 3.14]

3.7 数据丢失防护 data loss prevention

数据丢失预防DLP是在操作时基于内容和上下文的策略进行数据丢失防护的动态应用程序。

[GB/T 32400-2015，定义 3.2.32]

3.8 云计算服务 cloud computing service

使用定义的接口，借助云计算提供一种或多种资源的能力。

[GB/T 31167-2014,定义3.2]

3.9 云计算基础设施 cloud computing infrastructure

由硬件资源和资源抽象控制组件构成的支撑云计算的基础设施。

[GB/T 20984-2007，定义 3.14]

3.10 云计算平台 cloud computing platform

云服务商提供的云基础设施及其上的服务软件的集合。

[GB/T 31167-2014,定义3.7]

4 适用院校专业

中等职业学校：网络安防系统安装与维护、计算机应用、计算机网络技术、通信技术、网络信息安全等计算机类相关专业。

高等职业学校：信息安全与管理、计算机网络技术、计算机应用技术、信息网络安全监察等计算机类相关专业。

应用型本科学校：信息安全、通信工程、网络空间安全、网络工程、计算机科学与技术、网络安全与执法等计算机类相关专业。

5 面向职业岗位（群）

【云数据中心安全建设与运维】（初级）：主要面向网络空间安全领域，设备厂商、企事业单位、政府等信息安全部门或技术服务部门，从事网络设备安装、网络设备维护、网络安全运维、云计算基础等岗位工作。

【云数据中心安全建设与运维】（中级）：主要面向网络空间安全领域，设备厂商、企事业单位、政府等信息安全部门或技术服务部门，从事基线检查、安全加固、云安全平台部署与配置等岗位工作。

【云数据中心安全建设与运维】（高级）：主要面向网络空间安全领域，设备厂商、企事业单位、政府等信息安全部门或技术服务部门，从事等级保护、风险评估、应急响应、云安全产品运维等岗位工作。

6 职业技能要求

6.1 职业技能等级划分

云数据中心安全建设与运维职业技能等级分为三个等级：初级、中级、高级，三个级别依次递进，高级别涵盖低级别职业技能要求。

【云数据中心安全建设与运维】（初级）：能根据任务要求完成网络设备安装、网络设备维护、网络安全运维、云计算基础工作等工作。

【云数据中心安全建设与运维】（中级）：能根据任务要求完成基线检查、安全加固、云安全平台部署与配置等工作。

【云数据中心安全建设与运维】（高级）：能根据任务要求完成等级保护、风险评估、应急响应、云安全产品运维等工作。

6.2 职业技能等级要求描述

表1 云数据中心安全建设与运维职业技能等级要求（初级）

工作领域	工作任务	职业技能要求
1.网络安全设备安装与配置	1.1 网络安全基础技能利用与网络安全设备配置	1.1.1 能根据密码学工作任务需求，使用密码学技术 1.1.2 能根据国家相关规定，履行网络安全义务 1.1.3 能根据本地硬件架构安全需求，配置安全设备
2.网络安全运维	2.1 操作系统使用	2.1.1 能根据操作系统使用需求，完成文件与目录管理 2.1.2 能根据操作系统使用需求，完成用户管理 2.1.3 能根据操作系统使用需求，完成程序与进程管理 2.1.4 能根据操作系统使用需求，完成存储管理
	2.2 网络协议基础分析	2.2.1 能根据网络协议分析需求，分析物理层协议 2.2.2 能根据网络协议分析需求，分析数据链路层协议 2.2.3 能根据网络协议分析需求，分析网络层协议 2.2.4 能根据网络协议分析需求，分析传输层协议 2.2.5 能根据网络协议分析需求，分析应用层协议
3.云计算基础运用	3.1 云计算基础技能使用与云安全技术运用	3.1.1 能根据云计算和云安全工作任务需求，分析云计算机制 3.1.2 能根据云计算和云安全工作任务需求，使用虚拟化技术 3.1.3 能根据云计算和云安全工作任务需求，使用分布式系统 3.1.4 能根据云计算和云安全工作任务需求，使用云安全技术

表2 云数据中心安全建设与运维职业技能等级要求（中级）

工作领域	工作任务	职业技能要求
1. 网络安全运维	1.1 路由器与交换机的配置与安全基线检查、安全加固	1.1.1 能根据工作任务需求，配置路由器与交换机 1.1.2 能根据工作任务需求，检查安全基线 1.1.3 能根据工作任务需求，对操作系统、数据库进行安全加固配置

工作领域	工作任务	职业技能要求
2. 云安全产品管理	2.1 云安全资源池平台部署	2.1.1 能根据机柜、服务器设计要求，完成服务器硬件设备安装部署任务 2.1.2 能根据工作任务需求，完成服务器系统安装的安装部署 2.1.3 能根据工作任务需求，完成管理平台部署
	2.2 云安全资源池平台账户管理	2.2.1 能根据工作任务需求，完成平台账户管理 2.2.2 能根据工作任务需求，完成租户账户管理
	2.3 云安全态势感知平台部署	2.3.1 能根据工作任务需求，完成态势感知平台部署 2.3.2 能根据工作任务需求，完成态势感知平台的初始化配置 2.3.3 能根据工作任务需求，完成资产中心配置 2.3.4 能根据工作任务需求，完成云安全设备接入配置
	2.4 云安全资源池开通与管理	2.4.1 能根据工作任务需求，完成云防火墙资源开通与管理 2.4.2 能根据工作任务需求，完成云入侵检测资源开通与管理 2.4.3 能根据工作任务需求， 完成云WAF资源开通与管理 2.4.4 能根据工作任务需求，完成云上网行为管理资源开通与管理 2.4.5 能根据工作任务需求， 完成云VPN资源开通与管理 2.4.6 能根据工作任务需求，完成云堡垒机资源开通与管理 2.4.7 能根据工作任务需求，完成云日志审计资源开通与管理 2.4.8 能根据工作任务需求，完成云数据库审计资源开通与管理 2.4.9 能根据工作任务需求，完成云主机安全资源开通与管理
3. 云安全产品运维	3.1 云安全平台基础运维	3.1.1 能根据工作任务需求，完成平台监控与管理 3.1.2 能根据工作任务需求，完成平台巡检与升级 3.1.3 能根据工作任务需求，完成平台基础排障

表3 云数据中心安全建设与运维职业技能等级要求（高级）

工作领域	工作任务	职业技能要求
1.等级保护	1.1 等级保护标准解读与实施	1.1.1 能根据等级保护标准,对比等级保护的基础及2.0的主要变化 1.1.2 能根据等级保护标准,采用等级保护的基本工作流程 1.1.3 能根据等级保护标准,梳理等级保护要求的基本设计思路 1.1.4 能根据等级保护标准,培养等级保护安全建设的能力 1.1.5 能根据等级保护标准,采用等级保护测评的流程与方法
2.安全服务	2.1 风险评估实施	2.1.1 能根据工作任务需求,依据风险评估标准，完成风险评估工作 2.1.2 能根据工作任务需求,采用风险评估实施流程 2.1.3 能根据工作任务需求,分析风险评估案例
	2.2 应急响应处理	2.2.1 能根据工作任务需求,完成应急响应流程管理 2.2.2 能根据工作任务需求,使用应急响应工具 2.2.3 能根据工作任务需求,分析应急响应案例
3.云安全产品管理与运维	3.1 云安全产品管理与运维	3.1.1 能根据工作任务需求,使用云安全组件 3.1.2 能根据工作任务需求,完成云安全态势感知优化设置 3.1.3 能根据工作任务需求,完成云安全资源管理 3.1.4 能根据工作任务需求,完成云安全风险管理

参考文献

[1] GB/T 1.1-2009 标准化工作导则

[2] 中等职业学校专业目录（含 2019 增补专业）

[3] 普通高等学校高等职业教育（专科）专业目录及专业简介

[4] 普通高等学校本科专业目录（2012 年）

[5] 中等职业学校专业教学标准（试行）

[6] 高等职业学校专业教学标准（2018 年）

[7] 普通高等学校本科专业类教学质量国家标准（2018 年发布）

[8] 国家职业技能标准编制技术规程（2018 年版）

[9] 中华人民共和国职业分类大典（2015 年版）

[10] GB/T 25068.1 信息技术安全技术 IT 网络安全

[11] GB/T 20270-2006 信息安全技术 网络基础安全技术要求

[12] GB/T 20272-2006 信息安全技术 操作系统安全技术要求

[13] GB/T 36626-2018 信息安全技术 信息系统安全运维管理指南

[14] GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

[15] GB/T 25058-2019 信息安全技术 网络安全等级保护实施指南

[16] GB/T 25069-2010 信息安全技术 术语

[17] GB/T 25070 信息安全技术 信息系统等级保护安全设计技术要求

[18] GB/T 20281-2015 信息安全技术 防火墙安全技术要求和测试评价方法

[19] GB 17859-1999 计算机信息系统安全保护等级划分准则

[20] GB/T 25069-2010 信息安全技术术语