



中华人民共和国国家标准

GB/T 47686—2026

网络安全技术 政务云安全配置基线要求

Cybersecurity technology—Requirements for government cloud security
configuration baseline

2026-05-25 发布

2026-12-01 实施

国家市场监督管理总局
国家标准化管理委员会 发布

目 次

前言	V
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 概述	3
5.1 政务云网络参考架构	3
5.2 政务云关键组件架构	4
6 云管理平台安全配置要求	4
6.1 系统虚拟化管理	4
6.2 网络虚拟化管理	5
6.3 存储虚拟化管理	5
6.4 远程访问	5
6.5 通信保护	6
6.6 会话安全	6
6.7 身份鉴别	6
6.8 剩余信息保护	7
6.9 日志与审计	7
6.10 API 访问安全	7
6.11 监控报警	7
6.12 跨云迁移要求	8
6.13 安全配置基线管理	8
7 宿主机操作系统安全配置要求	8
7.1 通用加固	8
7.2 网络服务	9
7.3 账号和口令安全	9
7.4 安全审计	9
7.5 访问控制	10
7.6 用户策略	10
7.7 主机配置	10
7.8 数据保护	10
7.9 备份和故障恢复	11
8 容器安全配置要求	11

8.1	概述	11
8.2	宿主机配置	11
8.3	守护进程配置	11
8.4	容器运行时配置	11
8.5	容器编排配置	12
9	虚拟机安全配置要求	12
9.1	概述	12
9.2	身份鉴别	12
9.3	入侵防范	12
9.4	数据完整性与保密性	12
9.5	数据共享保护	13
9.6	剩余信息保护	13
9.7	最小功能授权	13
9.8	安全审计	13
9.9	镜像安全	13
10	数据库安全配置要求	14
10.1	概述	14
10.2	系统安全	14
10.3	网络安全	14
10.4	账号和口令安全	14
10.5	权限控制	14
10.6	安全审计	15
11	云安全组件安全配置要求	15
11.1	概述	15
11.2	云防火墙配置	15
11.3	云应用防火墙配置	15
11.4	堡垒机配置	15
11.5	网络审计	16
11.6	日志审计	16
11.7	组件自身安全	16
附录 A (资料性)	典型政务业务类型	18
附录 B (资料性)	政务云主要安全风险	19
附录 C (规范性)	宿主机操作系统安全配置项	21
C.1	通用加固配置项	21
C.2	网络服务配置	22
C.3	账号与口令安全配置	23
C.4	安全审计配置	24

附录 D (规范性) 云容器安全配置项	25
D.1 守护进程文件配置项	25
D.2 容器运行时配置项	25
D.3 容器编排配置项	26
参考文献	29

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专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：国家信息中心、中国网络安全审查认证和市场监管大数据中心、北京中关村实验室、浪潮云信息技术股份公司、华为技术有限公司、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、山东省大数据中心、中国信息安全测评中心、中国电子技术标准化研究院、北京国信新网通讯技术有限公司、赛西(深圳)电子信息产品标准化工程中心有限公司、北京邮电大学、浪潮软件集团有限公司、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、北京安信天行科技有限公司、陕西省网络与信息安全测评中心、远江盛邦安全科技集团股份有限公司、北京长亭科技有限公司、中国电力科学研究院有限公司、杭州安恒信息技术股份有限公司、北京神州绿盟科技有限公司、中国电子科技集团公司第十五研究所、中移(苏州)软件技术有限公司、北京卓识网安技术股份有限公司、北京软件产品质量检测检验中心有限公司、公安部第三研究所、中国网络空间研究院、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、国家计算机病毒应急处理中心、国家工业信息安全发展研究中心、中科信息安全共性技术国家工程研究中心有限公司、新华三技术有限公司。

本文件主要起草人：刘蓓、程浩、王啸天、禄凯、刘勇、伍扬、曲平、闫桂勋、饶飞、黄敏、卞建超、王旭东、张静、李鑫、马喆、赵佳璐、董树、赵进延、胡华明、王雨晨、杨斌、石然、王惠莅、马庆栋、符文田、郝沁汾、李小勇、吴思宇、孟建、王杰、张雅昕、安亚鹏、亓泽瑜、张翔、王兆蒙、肖红阳、陈彦羽、周进、刘琛、王肖斌、田海瑞、冯磊、陈妍、翟优、李婧、王胜越、吉磊、胡建勋、郭天奇。

网络安全技术 政务云安全配置基线要求

1 范围

本文件规定了政务云的云管理平台、宿主机操作系统、容器、虚拟机、数据库、云安全组件等关键组件的安全配置基线要求。

本文件适用于指导政务云安全能力建设、运行管理和检测评估。

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 31168—2023 信息安全技术 云计算服务安全能力要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务云 government cloud

专门用于承载政务信息系统和政务数据，统筹提供计算资源、存储资源、服务支撑和安全保障等共性资源的综合服务平台。

3.2

云管理平台 cloud management platform

用于提供资源调度、成本优化、安全合规和自动化运维等能力，统一管理云计算资源的工具平台。

3.3

安全配置基线 security configuration baseline

为符合政务云安全保障要求，政务云关键组件需要达到的最低安全配置要求。

3.4

虚拟机 virtual machine

一种虚拟的数据处理系统，是在某个特定用户的独占使用下，但其功能是通过共享真实数据处理系统的各种资源得以实现的。

[来源：GB/T 35293—2017, 3.1]

3.5

容器 container

操作系统用户空间分割出的多个独立运行的内核单元。

[来源：GB/T 44158—2024, 3.5]

3.6

云安全组件 cloud security components

为政务云提供安全功能和服务的各类软、硬件设备及程序模块等。