



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 发布
国家标准化管理委员会

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。

4 缩略语

下列缩略语适用于本文件。

ACL:访问控制列表(access control list)
API:应用编程接口(application programming interface)
ASLR:地址空间布局随机化(address space layout randomization)
CPU:中央处理器(central processing unit)
CUPS:常见 unix 打印系统(common unix printing system)
DHCP:动态主机配置协议(dynamic host configuration protocol)
DNS:域名系统(domain name system)
FTP:文件传输协议(file transfer protocol)
FTPS:安全文件传输协议(file transfer protocol secure)
HTTP:超文本传输协议(hypertext transfer protocol)
HTTPS:安全超文本传输协议(hypertext transfer protocol secure)
IAM:身份与访问管理(identity and access management)
ICMP:互联网控制消息协议(internet control message protocol)
IOPS:每秒读写次数(input and output per second)
IPC:进程间通信(inter-process communication)
LDAP:轻型目录访问协议(lightweight directory access protocol)
NFS:网络文件系统(network file system)
NIS:网络信息服务(network information service)
OS:操作系统(operating system)
PAM:可插拔认证模块(pluggable authentication modules)
PID:进程标识符(process identifier)
PKI:公开密钥基础设施建设(public key infrastructure)
RBAC:基于角色的访问控制(role-based access control)
RDP:远程桌面协议(remote desktop protocol)
RPM:软件包管理器(red hat package manager)
SCA:软件成分分析(software composition analysis)
SFTP:ssh 文件传输协议(sshfile transfer protocol)
SUID:设置用户标识符(set user id)
SGID:设置组标识符(set group id)
SMB:服务器消息块(server message block)
SMTP:简单邮件传输协议(simple mail transfer protocol)
SMTPS:安全简单邮件传输协议(simple mail transfer protocol secure)
SNMP:简单网络管理协议(simple network management protocol)
SQL:结构化查询语言(structured query language)
SSH:安全外壳(secure shell)
SYN:同步(synchronize)
TLS:传输层安全(transport layer security)
UID:用户标识符(user identifier)
UTS:unix 分时服务(unix timesharing service)

VPN:虚拟专用网(virtual private network)

XSS: 跨站脚本 (cross-site scripting)

5 概述

5.1 政务云网络参考架构

政务云用于承载各级政务部门的门户网站、政务业务应用系统和政务数据,用于政务办公、社会公共服务、数据管理、移动政务、监管执法等政务业务。政务云网络参考架构见图 1。政务云典型政务业务类型见附录 A。

政务云的服务对象主要是各级政务部门,通过政务网络连接到各级政务单位,使用政务云上的计算、网络、存储和安全等资源,承载各类政务信息系统和政务数据,支撑政务人员开展各项政务活动,并为社会公众提供政务服务。

政务云的大规模建设和政务应用在云上集中部署,使得政务云面临的安全风险更为复杂,其主要安全风险见附录 B。通过对政务云关键组件提出安全配置要求,强化各关键组件自身安全强度,减少各组件因缺少配置或配置不当带来的安全风险,从而保障整个政务云以及云上政务应用的安全运行。

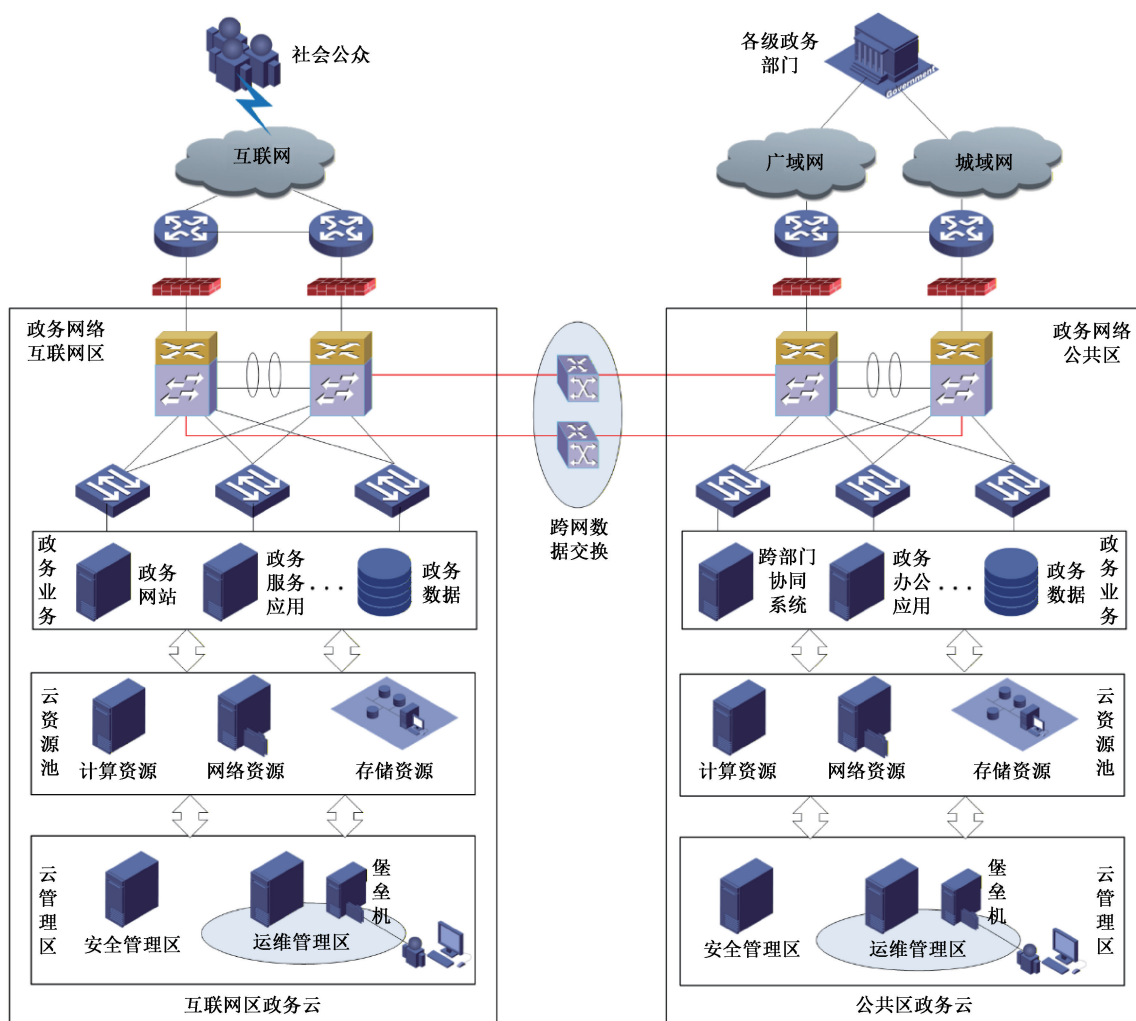


图 1 政务云网络参考架构

5.2 政务云关键组件架构

政务云组件包括云管理侧组件和云租户侧组件,其中云管理侧的云管理平台、宿主机操作系统、容器、虚拟机、数据库、云安全组件等六类组件为政务云关键组件,共同构成政务云核心能力,其关键组件架构见图 2。各关键组件实现政务云的计算、网络、存储等资源的虚拟化,并通过部署管理虚拟机、管理容器和云管理平台实现云资源调度和运行维护,云安全组件提供云平台安全保障能力。

云租户侧组件主要包括虚拟机、容器和数据库,主要承载云租户的业务应用和数据。云租户侧可参照管理侧关键组件的安全配置要求,加强其虚拟机、容器和数据库的安全配置管理。

政务云关键组件的安全配置,原则上至少符合网络安全等级保护三级,云计算安全评估增强级以及商用密码应用安全性评估相关要求。

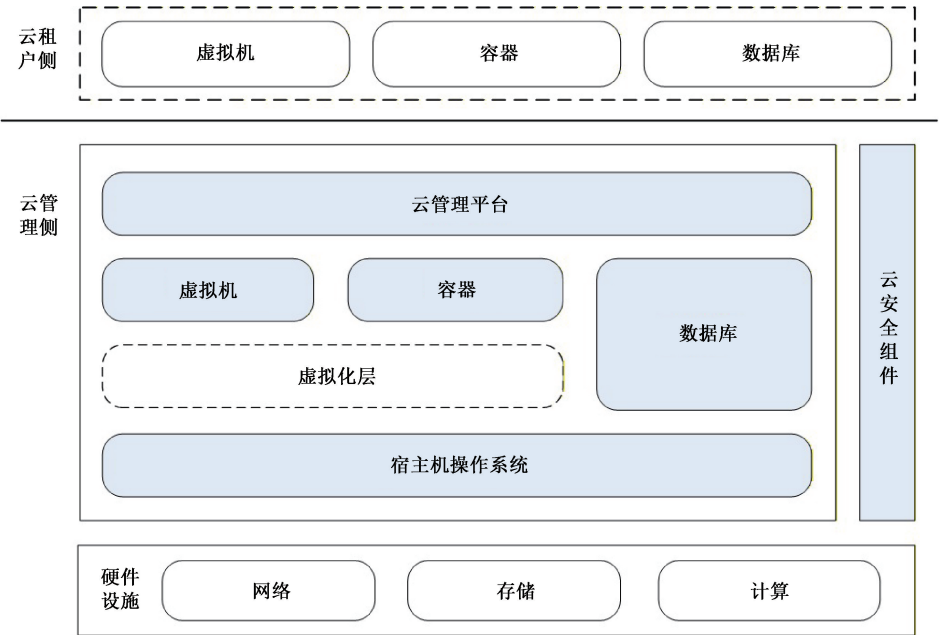


图 2 政务云关键组件架构

6 云管理平台安全配置要求

6.1 系统虚拟化管理

系统虚拟化管理要求包括如下内容。

- a) 应对虚拟机镜像、快照文件设置完整性校验,防止虚拟机镜像被恶意篡改。必要时,可对私有虚拟机镜像设置加密措施。
- b) 应对虚拟机模版文件、配置文件等重要数据配置完整性校验。
- c) 应正确配置虚拟镜像模板,明确模板谱系来源。
- d) 应提供虚拟化平台的资源隔离,虚拟机只能访问分配给该虚拟机的物理存储空间。
- e) 应提供虚拟化平台的资源隔离,实现不同虚拟机之间的虚拟中央处理单元(vCPU)指令隔离和内存隔离,某个虚拟机崩溃后不影响虚拟机监控器及其他虚拟机。
- f) 应提供虚拟机安全隔离,在虚拟机监控器层提供虚拟机与物理机之间的安全隔离措施,控制虚拟机之间以及虚拟机和物理机之间所有的数据通信,防止出现虚拟逃逸。
- g) 应设置告警策略,在资源超出阈值、资源隔离失败时及时告警。

- h) 应对非授权新建虚拟机、非授权配置变更或者重新启用虚拟机进行检测并告警。
- i) 应设置防止虚拟机镜像文件数据被非授权访问的策略。
- j) 应设置虚拟化平台操作管理员权限分离机制,不应出现越权管理、非授权管理等情况。
- k) 应具备虚拟机跨物理机迁移过程中的保护措施,虚拟机迁移时访问控制策略可随其迁移。
- l) 应具备对虚拟机所在物理机范围进行指定或限定的能力。
- m) 应采取措施使虚拟机的内存在被释放或再分配给其他虚拟机前得到完全释放。

6.2 网络虚拟化管理

网络虚拟化管理要求包括如下内容。

- a) 应对不同租户间虚拟网络资源的访问设置网络逻辑隔离,符合不同租户之间的网络隔离要求,并提供访问控制措施。
- b) 对同一租户的不同业务,应设置网络隔离和访问控制措施。
- c) 应对虚拟机网络接口的带宽进行管理。
- d) 应在不同等级的网络区域边界部署访问控制措施,并设置访问控制规则,如采用防火墙、网闸等安全设备进行访问控制,原则上公共区域安全等级高于互联网区域,管理区域安全等级高于业务区域。
- e) 应为租户业务提供虚拟化的负载均衡方案。
- f) 高危端口不应互联网访问,如 SSH(端口 22)、FTP(端口 21)、LDAP(端口 389)、RDP(端口 3389)、SMB(端口 445)、Mysql(端口 3306)、Redis(端口 6379)、Docker(端口 2375)、Elasticsearch(端口 9200)等。
- g) 应配置网络 ACL 规则或安全组,严格限制入方向规则中的高危端口。如确因业务需要开通的,应按最小化开放原则设置。
- h) 应限制云平台上的客户及其他重要信息流向境外。

6.3 存储虚拟化管理

存储虚拟化管理要求包括:

- a) 对存储数据的安全控制,应能应用到逻辑和物理存储实体上,不可因信息在物理存储位置上的改变而导致安全控制措施被旁路;
- b) 应对不同云服务租户所使用的虚拟存储资源进行逻辑隔离;
- c) 应提供虚拟存储数据审计措施,能对用户存储的挂载、操作等进行审计;
- d) 应配置虚拟存储数据访问控制措施,对物理存储实体不应或限制直接访问,如采用身份鉴别、授权访问、安全标签、数据加密等措施;
- e) 应配置虚拟存储冗余备份措施,能通过冗余备份数据进行恢复,如集群部署、镜像恢复等;
- f) 应设置存储协议级数据访问授权策略,如实施互联网小型计算机系统接口(iSCSI)等存储协议级别的安全控制;
- g) 应支持使用第三方加密及密钥管理措施,允许客户部署符合国家密码管理要求的数据加密产品,并应在云平台以密文形式存储客户数据。

6.4 远程访问

远程访问要求包括:

- a) 应使用符合国家密码管理要求的密码措施,保证远程访问会话的保密性、完整性和真实性;
- b) 应限制本地及远程终端设备接入云计算平台;
- c) 所有远程访问应只可经过有限数量的、受管理的访问控制点;

- d) 在远程访问时应使用安全的网络协议,如使用 FTPS/SFTP 代替 FTP、SSH 代替远程登录 (Telnet)、HTTPS 代替 HTTP、SMTPS 代替 SMTP、WebSockets over TLS 代替 WebSockets 等;
- e) 云平台进行远程维护管理时,应防止远程管理设备同时直接连接其他网络资源;
- f) 当远程管理云平台中设备时,管理终端和云计算平台之间应建立双向身份鉴别机制;
- g) 应对远程管理时执行的特权命令进行限制,如虚拟机删除、虚拟机重启等操作,并采取保护措施且进行审计。

6.5 通信保护

通信保护要求包括:

- a) 应对物理资源和虚拟资源按策略进行统一管理调度与分配;
- b) 应将云计算平台管理流量与客户业务流量进行分离,比如通过配置独立的管理网络和业务网络进行网络隔离;
- c) 虚拟化平台的管理命令应采用加密方式进行传输;
- d) 云计算平台应建立独立的运维网络分区,部署资源管理平台、运维管理系统、安全运营中心等实施运维管理;
- e) 应提供集中管控能力,包括系统管理、审计管理、安全管理等;
- f) 应将云平台产生的日志数据和监控流量数据,配置为集中存储;
- g) 应对云平台的计算资源和存储资源进行实时监控,监控指标包括宿主机总数量、虚拟机总数量、虚拟 CPU 总核数、已分配核数、CPU 资源消耗情况、存储总容量、已分配容量、存储消耗情况、内存总容量、已分配容量、内存使用情况、云存储读/写 IOPS、云存储读写使用率、物理硬盘使用率、物理硬盘读/写 IOPS 等内容;
- h) 应对云平台的网络资源进行实时监控,监控项包括网络带宽使用率、网络流量、网络延迟情况、网络入带宽、网络出带宽、带外网流入速率、带外网流出速率、网络连接数等。

6.6 会话安全

会话安全要求包括:

- a) 应在用户注销或会话终止时使会话标识符失效;
- b) 应设置用户会话超时策略,比如用户超过 30 min 未活动,会话将失效,并应重新登录;
- c) 云管理平台的账号 ID 应唯一,同一账号同一时间不可同时在平台上进行多个登录。

6.7 身份鉴别

身份鉴别要求包括:

- a) 云平台应通过统一身份鉴别服务(如 IAM)对账号进行统一管理,能为不同角色分配不同账户权限,如普通管理员、审计管理员、安全管理员等;
- b) 云管理平台应基于口令、硬件令牌或 PKI 进行凭证鉴别,相关密码措施应符合国家密码管理要求;
- c) 口令最小长度不低于 8 位,并至少包括数字、大小写字母和特殊符号;
- d) 用户更新口令时不可修改为过去 5 次使用过的旧口令;
- e) 应使用符合国家密码管理要求的加密算法对存储口令进行加密,并使用 HTTPS、SSH 等方式进行口令传输;
- f) 口令最长使用时间不应超过 90 d 有效期;
- g) 应限制使用默认超级管理员账户,如 Admin、root 等;
- h) 应设置账户锁定策略,比如 5 min 内登录失败次数超过五次,用户会被锁定 10 min;

- i) 应设置账户会话超时策略,如用户在规定会话阈值内未活动,会话将失效,应重新登录。

6.8 剩余信息保护

剩余信息保护要求包括:

- a) 云租户解除存储资源的使用后,所解除的存储资源的所有数据在物理存储上应被完全清除,如镜像文件、快照文件在迁移或删除虚拟机后能被完全清除;
- b) 云租户删除业务应用数据时,应删除云平台中存储的所有副本,包括本地备份和异地备份的副本;
- c) 故障物理存储介质离开云平台(如返厂)前,应采取数据擦除、物理消磁等有效技术手段清除数据,避免数据泄露;
- d) 为防止备份数据误删,可配置开启二次确认策略。

6.9 日志与审计

日志与审计要求包括:

- a) 应在云平台内部配置统一的系统时钟,生成审计记录的时间戳;
- b) 云平台产生的审计记录应包括,事件类型、事件发生的时间和地点、事件来源、事件结果以及与事件相关的用户或主体的身份,以及会话、连接、事务、活动持续期、接收和发出的字节数量、用于诊断或标识事件的附加信息报文、用于描述和标识行动客体或资源的特征等信息;
- c) 云平台产生的审计记录存储时间不应低于 6 个月;其中涉及互联网政务应用相关的日志,留存时间应不少于 1 年;
- d) 应限制非授权账户无法中断审计进程,有效保护审计进程;
- e) 应能对云平台产生的日志数据配置日志转存,便于日志数据的长期存储和大数据分析;
- f) 应为云平台的数据库开启数据库审计策略;
- g) 应对重要审计数据配置完整性校验,防止重要审计数据被篡改;
- h) 应设置审计失败告警策略和审计记录存储容量阈值(如超过 80%)告警策略。

6.10 API 访问安全

API 访问安全要求包括:

- a) 应在服务 API 调用前,配置用户鉴别和鉴权;
- b) 应设置服务 API 的安全传输策略;
- c) 应设置服务 API 的防范重放、代码注入、DoS/DDoS 等安全策略;
- d) 应设置服务 API 过载保护策略,保障不同服务等级用户间业务的公平性和系统资源利用最大化;
- e) 应设置服务 API 的调用日志记录策略,并监控 API 调用频率和异常行为;
- f) 应设置时间阈值,禁用超过阈值未使用的 API 密钥,如超过 180 d 未使用的密钥。

6.11 监控报警

监控报警要求包括:

- a) 应配置触发告警的规则以识别未授权活动和异常事件;
- b) 应设置物理资源和虚拟资源的告警触发条件阈值;
- c) 在创建告警规则时,应设置根据提示符的输入验证策略,防止恶意攻击或输入错误导致的问题。

6.12 跨云迁移要求

跨云迁移要求要求包括：

- a) 应对源云平台的业务全部数据或关键数据进行备份,如虚拟机、数据库、服务列表、账号等;
- b) 应对目标云平台的计算资源、存储资源、网络资源、安全资源和运行情况进行查验,包括但不限于软硬件资源规格、资源配置、网络分配和连接等;
- c) 应对源云平台与目标云平台之间的网络连接(如物理专线或 VPN)进行查验,包括但不限于迁出侧机房和迁入侧机房的接入点、专线网关、专线端口及容量等;
- d) 应根据业务流量模型、负载情况等元素选择合适的时间窗口进行业务切换,如流量波谷期、业务空闲期等;
- e) 应根据业务影响因素,选择业务应用停止服务或不停止服务方式进行迁移;
- f) 应制定业务切换策略和实施规划,包括但不限于业务切换方式(如先切换应用后切换数据,应用和数据同时切换)、数据迁移方式(如全量迁移,增量迁移)、切换时长、回退方案等;
- g) 跨云迁移完成后,应查验目标云平台上应用是否正常运行和数据一致性,并进行连续不间断监控系统运行状况。

6.13 安全配置基线管理

安全配置基线管理要求包括如下内容。

- a) 应制定并实施云管理平台的配置管理计划,包括配置管理员的角色和职责、配置变更管理流程、配置参数及基线配置管理流程、信息系统组件清单管理流程等内容。
- b) 应定期备份云管理平台及软硬件、固件等配置文件和配置记录(如每月一次/变更实施前/更新组件后),必要时能恢复相关配置。
- c) 安全配置基线应通过审核后才能生效。
- d) 应定期开展安全配置基线适用性评估,根据业务架构调整、威胁态势、监管要求等变化及时更新基线内容。
- e) 重大安全事件发生后应触发基线审核。
- f) 应监测基线版本有效期,到期前及时推送预警,失效基线涉及的系统应在过渡期内完成适配或者迁移。
- g) 安全配置基线废止时应评估影响范围,基线被新版本完全替代且无历史系统依赖时,可发起废止申请,经审批后公告废止。
- h) 基线文件应包含版本号、生效日期、修订历史及变更摘要,旧版本基线文档应保留不少于 3 年。
- i) 应明确云管理平台的受控配置列表,并定期变更受控配置列表,如每月更新一次、启动新的扫描前、新规则库发布后等。
- j) 应在实施基线配置变更前,从变更成功率、变更复杂度、安全策略、回退方案、业务影响程度、时间窗口等方面,对受控配置变更进行分析和评审。必要时,应对受控配置变更项进行提前测试和验证。
- k) 在实施变更中,应严格按变更流程和变更方案实施,必要时,可对特权命令操作进行二次审批。
- l) 应在实施变更后,应及时对变更操作进行审计。

7 宿主机操作系统安全配置要求

7.1 通用加固

通用加固要求包括：

- a) 应对通用进程进行加固配置,如启用 ASLR、启用链接文件保护等,符合 C.1 要求;
- b) 应配置访问控制策略,限制保持用户账号信息、密码信息、用户组信息、日志审计等关键系统文件的访问权限;
- c) 应配置普通用户提供口令才能提升权限,防止在不使用口令校验的情况下直接提升权限;
- d) 应及时更新和安装最新的操作系统补丁,修复操作系统已知漏洞;
- e) 应优化系统防火墙的内容;
- f) 应符合 GB/T 31168—2023 中 7.9 中恶意代码防护要求;
- g) 应对系统关键目录进行分区挂载,并根据自身业务特点,将操作系统数据同业务数据进行分区管理,避免将所有数据放在一个磁盘或分区下;
- h) 文件系统配置、软件服务配置、软件升级配置、进程加固配置、系统文件配置、特权命令配置、时钟同步服务配置、定时任务服务配置,应符合 C.1 要求。

7.2 网络服务

网络服务要求包括:

- a) 应对 SSH、RDP 服务进行加固配置,如不使用安全外壳第 1 版(SSHv1)、root、空口令等,配置最大登录尝试次数、配置空闲超时时间、匿名远程连接限制等,并关闭 SSH 端口转发配置项;
- b) 应配置网络服务对可能造成安全风险的报文进行过滤,如安全组、网络 ACLs,来过滤潜在安全风险的网路流量;
- c) 不应使用未加密的 Telnet 进行远程管理;
- d) 应关闭或屏蔽非必要端口,如 135、445、23 等;
- e) 应启用 SYN 攻击保护,防止受到 SYN 攻击;
- f) 应不使用或删除多余的网卡接口;
- g) 系统应使用防火墙实现访问控制,增强系统抵御网络攻击的能力;
- h) 应限制指定每个用户允许的最大会话数;
- i) 内核网络服务配置应符合 C.2.1 要求,网络服务应用配置应符合 C.2.2 要求。

7.3 账号和口令安全

账号和口令安全要求包括:

- a) 应创建具有最小权限的用户账户,禁用默认账户,如 root、guest 等,不应存在空口令账户;
- b) 应配置账户登录失败功能,连续登录失败一定次数后锁定账户;
- c) 应配置登录连接超时自动退出机制,会话超时时间不应为 0 或不配置或时间过长;
- d) 应设置操作系统账号口令,不应使用相同口令,应修改默认口令,账号和口令应不相同;
- e) 口令最小长度不应少于 8 位,并至少包含数字、大小写字母和特殊符号,且采取高强度的加密方式存储;
- f) 应根据业务需要,合理配置口令使用的有效期,最长有效期不宜超过 3 个月;
- g) 应对操作系统账号分配合理权限;
- h) 账号管理配置、口令管理配置、告警提示信息配置应符合 C.3 要求。

7.4 安全审计

安全审计要求包括:

- a) 应在启动阶段启用日志审计机制,配置审计规则,对系统安全相关日志进行记录;
- b) 应合理设置日志审计文件及目录的相应权限,防止审计文件被恶意破坏,并对审计记录进行定期备份,保存时间不少于 6 个月;

- c) 日志审计应包含会话、登陆注销、文件删除、账号信息修改、内核模块变更、环境更改等场景的审计记录；
- d) 应配置系统日志策略配置文件,对系统登录、访问等行为进行审计；
- e) 应设置日志文件大小限值,为审计日志数据分配合理的存储空间或存储时间；
- f) 审计日志限速阈值不应配置过小；
- g) 定期进行审计日志的备份,以防未经预料的信息丢失；
- h) 应对审计进程进行保护,防止未经授权的中断；
- i) 审计 Auditd 服务、日志 Rsyslog 服务配置应符合一定的配置要求,如 Auditd、Rsyslog 配置应符合 C.4 要求。

7.5 访问控制

访问控制要求包括：

- a) 应建立不同权限账户,Linux 中间件、数据库应由非 root 权限账户启动；
- b) 应禁用非必要的默认账户,删除多余的、过期的账户；
- c) 应锁定重要文件权限,如/etc/passwd、/etc/shadow、/etc/group 和/etc/shadow 等；
- d) 应仅限指定网络地址范围的主机可进行远程登录；
- e) 应限制具备超级管理员权限的用户进行远程登录,并远程执行管理员权限操作；
- f) 主机间不应使用公钥登录,部分业务应使用公钥鉴别,根据实际使用情况进行加固；
- g) 凭据管理器不应保存通过域身份验证的密码和凭据,避免用户信息泄露；
- h) 应启用自主访问控制,控制用户对客体的访问,如基于用户的权限表、基于客体的访问控制表；
- i) 可启用基于安全标记的访问控制。

7.6 用户策略

用户策略要求包括：

- a) 应按仅授予管理用户最小权限的原则设置安全管理员、审计管理员、系统管理员,防止用户权限过大；
- b) 应按不同的用户分配不同的账号,避免不同用户间共享账号,避免用户账号和设备间通信使用的账号共享；
- c) 应设置 root 帐户的 UID 为 0；
- d) 当前系统中不应默认帐户 shell；
- e) 当前系统中不应默认帐户密码。

7.7 主机配置

主机配置要求包括：

- a) 系统应使用安全模块,避免造成系统部分安全功能不生效；
- b) 应设置资源限制,如 stack 大小不能设置为 unlimited,避免资源被用户独占；
- c) 应启用访问控制功能,依据安全策略控制用户对资源的访问,防止系统重要数据泄露；
- d) 应去掉文件“系统文件”属性,防止用户滥用及提升权限的可能性。

7.8 数据保护

数据保护要求包括：

- a) 应对系统鉴别数据进行加密存储和传输；
- b) 应对存储在宿主机上的数据进行加密处理,保护数据在静态状态下的安全；

- c) 应采取保护措施保障数据在传输过程中的机密性和完整性,防止数据被窃取或篡改。

7.9 备份和故障恢复

备份和故障恢复要求包括:

- a) 应在系统正常运行时定期实施备份,宜对频繁更新的内容实施每日备份,对相对稳定的数据实施每周备份;
- b) 应在系统重大变化前对系统进行备份,如系统升级、新功能发布等情况。

8 容器安全配置要求

8.1 概述

针对管理侧容器提出安全配置基线要求,可供租户侧云容器参考。

8.2 宿主机配置

宿主机配置要求包括:

- a) 应为容器创建独立的存储空间;
- b) 应更新至最新的稳定版本容器;
- c) 普通用户不应创建、执行和操作容器的权限;
- d) 应定期删除无用镜像;
- e) 应限制宿主机上容器数量;
- f) 应限制宿主机的网络访问范围,仅允许必要的端口通信;
- g) 不应使用特权账户登录宿主机。

8.3 守护进程配置

守护进程配置要求包括:

- a) 不应默认网桥上容器间通信,并启用加密保护;
- b) 不应使用无镜像仓库证书或不使用 TLS 的镜像仓库;
- c) 不应使用已存在的存储驱动程序;
- d) 应启用守护进程的安全配置,如双向身份鉴别、资源限制和资源隔离等;
- e) 应设置容器的默认空间大小;
- f) 应启用容器客户端命令的认证授权机制;
- g) 容器不应通过执行文件提升权限级别;
- h) 不应使用旧仓库版本的交互;
- i) 应启用实时恢复机制;
- j) 不应使用用户态网络代理;
- k) 容器不应以特权模式启动;
- l) 不应以非特权账户运行守护进程,使用非特权用户和安全组运行;
- m) 应对守护进程相关文件、目录的所有权和权限进行配置,符合 D.1 要求。

8.4 容器运行时配置

容器运行时配置要求包括:

- a) 不应以特权身份用户运行容器;
- b) 应限制容器运行时可加载的文件、进程,配置应符合 D.2 要求;

- c) 应设置容器运行的基础参数,如 CPU 优先级、内存使用限制、流量绑定、端口映射等;
- d) 应限制共享配置的使用,如不应共享主机的进程命名空间、IPC 命令空间、用户命名空间和 UTS 命令空间,不应直接共享主机设备给容器,以及不应装载传播共享模式等;
- e) 应对容器运行时相关文件、目录的所有权和权限进行配置,配置应符合 D.2 要求。

8.5 容器编排配置

应设置容器编排相关组件的配置,如 API 服务器、调度程序、控制器、etcd 和 Kubelet 等,配置应符合 D.3 要求。

9 虚拟机安全配置要求

9.1 概述

针对管理侧虚拟机提出安全配置基线要求,供租户侧云虚拟机参考。

9.2 身份鉴别

身份鉴别要求包括:

- a) 对登录的用户进行身份鉴别,用户口令应具有复杂度要求并定期更换,如口令最小长度不低于 8 位,并至少包括数字、大小写字母和特殊符号,口令最长使用时间不超过 90 d 有效期;
- b) 应配置登录失败处理和登录连接超时自动退出等相关策略,如在 5 min 内连续登录失败五次,该账户锁定 10 min,登录连接超时 30 min 自动退出;
- c) 应防止鉴别信息在远程登录过程中被窃听;
- d) 应基于用户权限最小化原则,为不同角色用户设置不同操作权限;
- e) 应对登录的用户逐一分配账户,并重命名或删除默认账户;
- f) 应实现管理用户的权限分离,避免共享账户的存在;
- g) 对账户的网络访问实施多因子鉴别,其中一个因子应由与系统分离的设备提供,以防止多因子鉴别凭证同时遭到破坏或泄露,如基于硬件令牌、基于生物特征。

9.3 入侵防范

入侵防范要求包括:

- a) 应安装恶意代码防护软件,定期更新恶意代码防护软件版本及病毒库,实时监控主机活动,及时发现并响应潜在的恶意代码入侵行为;
- b) 应能检测恶意代码感染及在虚拟机间蔓延的情况,并进行拦截阻断;
- c) 所有用户通信不应绕过恶意代码防护软件的检测;
- d) 应定期对虚拟机进行漏洞扫描,识别并修复已知的安全漏洞,防止恶意代码利用这些漏洞进行攻击;
- e) 应实施应用程序白名单策略,仅允许经过验证和授权的应用程序在主机上运行;
- f) 应关闭程序自动运行机制,避免恶意代码在后台无感运行(应用程序白名单中的程序除外);
- g) 应设置系统定期更新和补丁管理机制。

9.4 数据完整性与保密性

数据完整性与保密性要求包括:

- a) 应采用符合国家密码管理相关要求的密码产品,对重要数据在传输过程中的完整性和保密性进行保护;

- b) 应采用符合国家密码管理相关要求的密码产品,对重要数据在存储过程中的完整性和保密性进行保护。

9.5 数据共享保护

数据共享保护要求包括:

- a) 应设置数据访问限制策略,防止未经授权的增、删、改、查等操作;
- b) 应在数据传输和存储过程中对敏感数据进行加密处理;
- c) 应在数据共享过程中,对需要共享的敏感数据进行脱敏或匿名化处理,以降低数据泄露的风险;
- d) 应建立安全审计机制,记录数据共享过程中的操作日志和访问记录,可及时发现并处理异常数据共享行为。
- e) 应设置虚拟机共享安全访问策略,如采用 HTTPS、SSH 方式访问共享虚拟空间;
- f) 应设置虚拟机网络访问控制策略实现同一物理机上多个虚拟机之间的逻辑隔离;
- g) 应设置远程管理虚拟机的安全通信协议;
- h) 应设置虚拟机的独立存储策略。

9.6 剩余信息保护

剩余信息保护要求包括:

- a) 在删除业务应用数据时,应配置自动删除云平台中存储的所有副本,如在迁移或删除虚拟机后,镜像文件、快照文件应被完全清除;
- b) 在敏感数据的存储空间被释放或重新分配前,应进行数据擦除且数据不能被恢复;
- c) 应定期清理虚拟机中的临时文件和缓存,避免敏感数据残留;
- d) 应建立防止误操作措施,在删除业务应用数据时进行二次确认。

9.7 最小功能授权

最小功能授权要求包括:

- a) 应识别不必要或不安全的功能、端口、协议和服务,严格限制对高风险端口的访问,如不应从互联网访问虚拟机的高风险端口;
- b) 应建立虚拟机的授权软件列表,不应在虚拟机上运行非授权软件;
- c) 应为虚拟机及其用户分配最低必要的权限,不应过度授权;
- d) 应符合最小安装的原则,仅安装必要的组件和应用程序。

9.8 安全审计

安全审计要求包括:

- a) 应启用日志审计机制,对每个用户行为和重要安全事件进行审计;
- b) 审计记录应涵盖事件的日期和时间、涉及的用户、事件的具体类型、事件成功与否的状态,以及其他与审计相关的信息;
- c) 应对审计进程实施保护措施,以防止任何未经授权的访问或中断;
- d) 审计记录存储时间应不低于 6 个月,涉及互联网政务应用相关的日志,留存时间不少于 1 年。

9.9 镜像安全

镜像安全要求包括:

- a) 应使用最新系统镜像,避免使用已经停止服务的版本;

- b) 应对自定义镜像进行安全加固,如关闭不必要的服务与端口、限制账号权限、设置密码安全策略等;
- c) 应定期对虚拟机镜像进行漏洞扫描并对漏洞进行修复;
- d) 应设置镜像和快照的完整性保护策略,防止被恶意篡改。

10 数据库安全配置要求

10.1 概述

针对管理侧数据库提出安全配置基线要求,可供租户侧云数据库参考。

10.2 系统安全

系统安全要求包括:

- a) 不应使用操作系统超级管理员身份登录、启动和运行数据库;
- b) 应使用非系统分区存放数据库。

10.3 网络安全

网络安全要求包括:

- a) 数据库不应使用默认端口号;
- b) 应限制数据库客户端最大连接数;
- c) 应限制数据库连接闲置等待时间;
- d) 会话超时时间不应为 0 或时间过长;
- e) 数据库应仅侦听授权的网络连接,服务监听地址不应为“0.0.0.0”;
- f) 应将管理员用户限制为仅用于本地数据库管理,如需远程访问,应采用加密的通信通道。

10.4 账号和口令安全

账号和口令安全要求包括:

- a) 应启用数据库身份鉴别和权限管理功能;
- b) 应限制默认账户的访问权限,禁用默认账户,避免存在默认口令、空口令账户;
- c) 应配置系统账号口令复杂度要求,口令最小长度不少于 8 位,并至少包含数字、大小写字母和特殊符号;
- d) 应配置口令定期更换策略,至少每 90 d 强制更换一次;
- e) 数据库口令应加密存储;
- f) 应配置口令的不可重用天数或次数,避免用户多次使用相同的密码导致被破解;
- g) 应配置账号登录失败尝试次数,超过规定次数后锁定账户;
- h) 应配置账户锁定后自动解锁时间。

10.5 权限控制

权限控制要求应包括:

- a) 应设置不同角色,为不同角色的用户分配不同的权限;
- b) 授权安全管理员通过安全管理员账户配置访问控制策略;
- c) 授权审计管理员通过审计管理员账户进行审计记录维护。

10.6 安全审计

安全审计要求包括：

- a) 应开启数据库审计日志功能,收集并存储数据库记录的日志;
- b) 应配置日志文件权限,仅对必要用户开放访问权限;
- c) 审计日志应覆盖重要的用户行为,如用户登录注销、数据库启动、停止、恢复和切换、数据库对象的新建、删除、修改;
- d) 应具备不同严重等级的日志,至少包括 Debug, Notice, Warning, Error, Fatal 或同等含义的等级;
- e) 应配置单个审计文件的最大记录时间,如 30 d;
- f) 应配置单个审计日志文件的最大容量,如 20 480 KB;
- g) 审计记录存储时间应最少不低于 6 个月。

11 云安全组件安全配置要求

11.1 概述

针对云管理侧安全组件提出安全配置基线要求,供租户侧云安全组件参考。

11.2 云防火墙配置

云防火墙配置要求包括：

- a) 应开启访问控制功能;
- b) 应对云内虚拟机间的访问设置安全访问控制策略;
- c) 应开启入侵防御功能;
- d) 应设置入侵防御策略,实现对病毒、攻击、漏洞利用的有效防护;
- e) 应设置恶意代码检测与数据过滤策略,及时发现并阻断已知恶意网络地址和攻击特征,以及识别并防御具有已知攻击特征的威胁。

11.3 云应用防火墙配置

云应用防火墙配置要求包括：

- a) 应开启应用系统的访问控制功能;
- b) 应设置应用系统的访问控制策略,控制对应用系统资源的有限访问;
- c) 应设置攻击防护策略,包括但不限于对 XSS 攻击、SQL 注入攻击、目录遍历攻击、LDAP 注入攻击、SSL 注入攻击、XPath 注入攻击等常见网络攻击的防护;
- d) 应设置防盗链、爬虫、暴力登录等策略。

11.4 堡垒机配置

堡垒机配置要求包括：

- a) 应设置针对政务云管理侧各项系统维护的运维审计策略,包括服务器、路由器、交换机、安全组件、虚拟机、应用系统等;
- b) 应开启身份管理功能,设置角色划分,至少包含系统管理员、安全审计员、操作员;
- c) 应设置用户仅能访问授权资源,不应默认“全部允许”策略;
- d) 应设置针对各项系统维护高危命令的审批策略,限制其日常使用。

11.5 网络审计

网络审计要求包括：

- a) 应开启网络审计功能；
- b) 应设置针对政务云管理侧网络访问行为审计策略，至少记录源网络地址、目的网络地址、源端口、目的端口、应用协议、告警级别；
- c) 应设置审计记录存储时间不少于 6 个月。

11.6 日志审计

日志审计要求包括：

- a) 应开启日志审计功能；
- b) 应设置针对政务云管理侧所有系统的日志采集策略，能总览云内所有系统的历史及实时日志；
- c) 应设置日志定时自动备份；
- d) 应设置审计记录存储时间不少于 6 个月。

11.7 组件自身安全

11.7.1 系统安全

系统安全要求包括：

- a) 应禁用不必要或高风险的功能、端口、协议或服务，并将该安全配置作为重新安装或升级时的缺省配置；
- b) 应及时更新系统的基本配置信息库；
- c) 应设置签名验证机制或第三方 SCA 等方式保障组件不含任何盗版软件或者破解程序，并设置系统自动更新或版本检查机制，定期验证合法性；
- d) 应设置合理的 CPU、内存等资源限额，避免过度分配导致政务云业务服务的性能下降；
- e) 应设置资源调度功能，根据负载需求调整资源分配；
- f) 应设置网络接口支持互联网协议第 6 版 (IPv6)，包括地址规划和路由设置。

11.7.2 访问安全

访问安全要求包括：

- a) 应删除或停用多余的、过期的账户；
- b) 不应使用默认口令；
- c) 应设置口令复杂度要求，口令最小长度不少于 8 位，并至少包含数字、大小写字母和特殊符号；
- d) 应设置口令定期更换策略，至少每 90 d 强制更换一次；
- e) 应设置会话超时时间；
- f) 应设置合理的无活动自动退出时间；
- g) 应设置登录来源网络地址范围；
- h) 应设置用户访问时长限制；
- i) 应设置登录失败次数限制和登录失败后的锁定时间；
- j) 应设置双因素鉴别机制；
- k) 应限制安全组件的管理员登录地址范围；
- l) 应设置安全组件特权用户的权限分离；
- m) 远程访问安全组件时，应通过 SSH 或其他加密协议来保护通信内容；

- n) 应设置三权分立机制,如系统管理员,安全管理员和审计管理员。

11.7.3 策略安全

策略安全要求包括:

- a) 应删除多余或无效的策略规则;
- b) 安全策略应根据最小化原则设置,使用时根据实际所需进行开通;
- c) 病毒库、入侵检测规则库、防火墙规则库、漏洞库等重要配置项的配置应符合 GB/T 31168—2023 中 10.3.1 b) 的要求。

11.7.4 安全审计

安全审计要求包括:

- a) 应开启安全组件的日志功能,记录所有关键操作,包括成功和失败事件等;
- b) 应设置审计记录保护功能,避免受到未预期的删除、修改或覆盖等;
- c) 应设置日志备份频率;
- d) 应设置日志加密存储;
- e) 应设置日志留存时间不少于 6 个月。

附 录 A
(资料性)
典型政务业务类型

典型政务业务类型见表 A.1。

表 A.1 典型政务业务类型

业务类型	典型政务业务示例	服务对象
政务办公类业务	a) 公文流转与审批:政府部门内部以及部门之间的公文起草、审核、签发、传递等流程通过政务云平台实现电子化; b) 会议管理:涵盖会议安排、会议通知发送、会议资料共享以及视频会议等功能; c) 日程管理:为政府工作人员提供个人日程安排、任务提醒等功能	政务部门
公共服务类业务	a) 在线政务服务平台:面向公众提供一站式的政务服务,如行政审批事项的在线申报、查询办理进度和结果等; b) 民生服务:社保、医保、公积金等民生领域的业务办理和信息查询; c) 公共事业服务:涉及水、电、气等公共事业费用的缴纳和查询服务	社会公众
数据管理类业务	数据共享与交换:促进政府部门之间的数据共享和交换。通过建立统一的数据标准和交换平台,各部门可按规定的权限和流程共享数据,为协同办公和决策提供数据支持	政务部门
移动政务类业务	移动应用服务:移动办公系统、政务应用程序、政务小程序、移动邮件系统、移动即时通信等	政务部门 社会公众
监管执法类业务	a) 市场监管:市场监管部门利用政务云平台实现对市场主体的注册登记、监管信息录入、执法检查等业务的信息化管理; b) 环境监管:环保部门通过政务云平台实时采集和分析环境监测数据,如空气质量、水质等数据,实时监控和预警; c) 城市管理执法:涵盖城市管理中的违法建设查处、市容市貌管理等执法业务。通过政务云平台,城管执法人员可实时上传执法信息、查询相关法律法规	政务部门

附 录 B
(资料性)
政务云主要安全风险

政务云主要安全风险见表 B.1。

表 B.1 政务云主要安全风险

序号	风险层面	安全风险分类	安全风险描述
1	技术性风险	主机安全风险	a) 主机的操作系统、数据库存在未修复的漏洞,被暴力破解和非法访问等; b) 主机安全配置不当,存在未关闭的高危服务、未限制端口开放等; c) 更新管理滞后,未及时修复操作系统、中间件或应用的安全风险; d) 审计内容覆盖不全面,未开启主机登录日志、操作日志等审计
2		数据安全风险	a) 数据存储风险,敏感数据未加密存储,数据库遭入侵后可被直接窃取; b) 数据传输风险,使用非加密协议、易被破解的弱密码套件传输敏感数据; c) 数据使用与访问控制风险,存在越权访问、共享数据失控等风险; d) 数据备份与恢复风险,备份策略不完善、备份恢复机制失效等
3		应用安全风险	a) 云平台上部署的应用、容器镜像、第三方组件等存在安全漏洞; b) API 未进行身份鉴别、未限制调用频率、存在安全漏洞等; c) 容器配置错误或不当,如特权模式运行容器、使用不可信或过时镜像、资源限制未配置等
4		网络安全风险	a) 网络架构设计存在缺陷,暴露过多攻击面或缺乏冗余性,易被外部攻击者利用; b) 访问控制策略不符合最小化开放原则,允许非授权流量通过,未启用网络隔离等; c) 防火墙规则配置错误,导致攻击面扩大、数据泄露或服务中断等
5		虚拟化层安全风险	a) 虚拟化层存在漏洞,攻击者虚拟机利用突破隔离边界,控制宿主机或其他虚拟机; b) 虚拟化资源(CPU、内存、存储、网络等)分配策略不当,导致资源抢占或隔离失效; c) 虚拟机镜像存在漏洞、后门或敏感信息,导致风险扩散; d) 虚拟化管理平台接口暴露或配置不当,成为攻击入口
6		外部攻击安全风险	a) 恶意程序攻击,如病毒、蠕虫、木马及其他恶意程序等攻击; b) 网络攻击,如 DDoS 攻击、后门植入、漏洞利用、网络扫描等攻击; c) APT 攻击,黑客组织、机构等发起的网络攻击

表 B.1 政务云主要安全风险（续）

序号	风险层面	安全风险分类	安全风险描述
7	管理性风险	制度与流程管理	a) 安全管理制度缺失,租户与云服务商之间的安全责任边界不清,合规管理滞后等; b) 审计与监督管理不完善,如日志留存周期不足,审计流于形式等; c) 变更管理缺失,如系统升级、补丁安装未经过审批和测试
8		人员与权限管理	a) 运维人员安全意识薄弱,导致存在默认口令、弱口令、敏感信息明文存储、特权账号共用、离职人员运维账号没有及时清除等问题; b) 运维工作依赖人力外包服务,外包人员稳定性差,部分人力外包服务存在多层外包,安全责任未有效传递; c) 运维终端缺少有效管控措施,如终端接入无控制、运维终端未做到专用、存在安装非授权软件、使用非受控运维工具、系统补丁及病毒库更新不及时等; d) 不符合最小权限原则,普通用户拥有管理员权限,不同部门共享云资源时权限交叉等
9		数据安全	a) 未对政务数据(如公民个人信息、社保记录)进行分类分级,导致敏感数据未加密存储或传输; b) 未履行数据出境审批(如跨境共享数据未通过国家网信部门安全评估); c) 数据生存周期管理缺失(如未按法规要求留存日志或删除冗余数据)
10	管理性安全风险	供应链管理	a) 供应商管理,如服务器/网络设备固件后门、开源组件漏洞、操作系统未授权代码植入等; b) 云服务商管理,云平台管理接口暴露、运维工具漏洞、超权限访问政务数据等; c) 合作方管理,业务系统代码漏洞、测试数据泄露、外包人员违规操作等; d) 其他关联方管理,网络链路劫持、CA 证书伪造等

附 录 C
(规范性)
宿主机操作系统安全配置项

C.1 通用加固配置项

C.1.1 文件系统配置

文件系统配要求包括：

- a) 应将无需挂载设备的分区以 nodev 方式挂载；
- b) 应将无可执行文件的分区以 noexec 方式挂载,使业务数据盘只用于保存业务执行过程中的数据,并不应在数据盘上执行相关命令；
- c) 应将无需 SUID 和 SGID 的分区以 nosuid 方式挂载。

C.1.2 软件服务配置

软件服务配置要求包括：

- a) 不应安装业务无关软件,如 Telnet 软件、NIS、CUPS、调测类工具、开发编译工具等；
- b) 应关闭不使用的服务,如 SNMP、FTP、DNS、DHCP、NFS 等。

C.1.3 软件升级配置

软件升级配置要求包括：

- a) 应通过签名机制验证 RPM 软件包的完整性,签名算法应符合相关密码标准要求；
- b) 通过 yum 或 dnf 命令安装 RPM 时应校验 rpm 的签名,签名校验不通过不应安装；
- c) 应配置软件仓库源,系统能通过配置软件仓库 yum 源来实现软件包的安装和升级。

C.1.4 进程加固配置

进程加固配置要求包括：

- a) 应启用 ASLR,从而增加缓冲区溢出等攻击利用的难度；
- b) 应将链接文件保护配置正确,避免攻击者以低权限用户伪造的链接文件,被高权限用户执行；
- c) 应将 dmesg 访问权限配置正确,无特权的用户无法查看系统信息；
- d) 内核符号地址应受限访问；
- e) 不应将全局加解密策略配置为 LEGACY。

C.1.5 系统文件权限

系统文件权限要求包括：

- a) 应将/etc/passwd、/etc/shadow、/etc/group、/etc/gshadow 等文件权限配置正确,并给出关键系统文件权限配置表；
- b) 应保障敏感信息不被泄露,定期清理和备份.bash_history 文件,或者配置 history 命令的相关环境变量,如设置 HISTIGNORE 来忽略某些敏感命令的记录；
- c) 全局可写目录应已设置 sticky 位,避免其他用户删除该目录下不属于他的文件和目录；
- d) 不应存在全局可写的文件,避免所有用户都可对文件进行写操作；
- e) 不应存在空链接文件；

- f) 不应存在隐藏的可执行文件；
- g) 应删除文件非必要的 SUID 和 SGID 位；
- h) 默认 umask 应是 027 或更严格。

C.1.6 特权命令配置

特权命令配置要求包括：

- a) 应配置仅允许 wheel 组中的普通用户具有切换用户(su)的使用权限；
- b) su 应受限使用,如/etc/pam.d/su 中是否配置非 wheel 组用户账号禁用 su；
- c) su 命令继承用户环境变量不可引入提权,如/etc/login.defs 中是否配置了自动初始化环境变量 PATH,即 ALWAYS_SET_PATH=yes；
- d) 不应使用 SysRq 键。

C.1.7 时间同步服务配置

时间同步服务配置要求包括：

- a) 应正确配置 ntpd 服务；
- b) 应正确配置 chronyd 服务。

C.1.8 定时任务服务配置

定时任务服务配置要求包括：

- a) cron 服务应启用并正常运行；
- b) 应正确配置 cron 权限配置,如使用白名单管理,只有 root 账号和写在白名单中的账号可使用 cron 命令。

C.2 网络服务配置

C.2.1 内核网络服务配置

内核网络服务配置要求包括：

- a) 系统不应响应 ICMP 广播报文；
- b) 不应接收 ICMP 重定向报文；
- c) 不应转发 ICMP 重定向报文；
- d) 应忽略伪造的 ICMP 报文；
- e) 应启用反向地址过滤；
- f) 不应进行网络地址转发；
- g) 不应接收源路由报文；
- h) 应启用 TCP-SYNcookie 保护；
- i) 不应使用 ARP 代理。

C.2.2 网络服务应用配置

网络服务应用配置要求包括如下内容。

- a) 不应存在端口全零监听。
- b) 应对 SSH 服务进行加固配置,如不应 root 登录、空口令、配置空闲超时时间等。具体包括：
 - 1) 应正确配置/etc/ssh/sshd_config 权限；
 - 2) 应正确配置 SSH 私钥文件权限；

- 3) 应正确配置 SSH 公钥文件权限；
- 4) 应启用 IgnoreRhosts；
- 5) SSH 应使用 PAM 认证；
- 6) 不应 SSHroot 登录；
- 7) 不应 SSH 空口令登录；
- 8) 不应使用 HostbasedAuthentication；
- 9) 应配置 WarningBanner 文件路径；
- 10) 应正确配置 SSH 日志级别；
- 11) 不应使用 X11Forwarding；
- 12) 不应使用 PermitUserEnvironment；
- 13) 应配置 LoginGraceTime 不超过 60 s；
- 14) 应配置空闲超时间隔时间；
- 15) 不应使用 AllowTcpForwarding；
- 16) SSH KexAlgorithms 应配置强算法；
- 17) SSH MACs 应配置强算法；
- 18) SSH Ciphers 应配置强算法；
- 19) 不应配置 SSH 将弃用的选项；
- 20) 应正确配置 MaxAuthTries；
- 21) SSH 服务不应预设置 authorized_keys。

C.3 账号与口令安全配置

C.3.1 账号管理配置

账号管理配置要求包括：

- a) 不应存在 UID 为 0 的非 root 账号；
- b) root 账号不应直接登录系统，应由普通账号 su 之后进行管理员操作；
- c) UID 应唯一；
- d) GID 应唯一；
- e) 账号名应唯一；
- f) 组名应唯一；
- g) /etc/passwd 中的组应都存在；
- h) 关键账号应具有自己的 Home 目录。

C.3.2 口令管理配置

口令管理配置要求包括：

- a) 口令最小长度不少于 8 位，并至少包含数字、大小写字母和特殊符号；
- b) 应限制重用历史口令次数；
- c) 口令过期时间不应超过 90 d；
- d) 口令过期告警时间不低于 15 d；
- e) 应设置口令修改周期为 0 d，避免频繁修改口令；
- f) Grub 应已设置口令保护。

C.3.3 告警提示信息配置

告警提示信息配置要求包括：

- a) 提示信息应包含合理的信息,对应信息不能增加风险,如不应将 OS 发行版、OS 版本、服务器架构类型信息通过/etc/issue 暴露给用户;
- b) motd 文件应包含合理的信息;
- c) 应正确配置/etc/issue 权限,如/etc/issue 文件的 Uid 和 Gid 为 0,且文件权限是 0644;
- d) 应正确配置/etc/issue.net 权限,如/etc/issue.net 文件的 Uid 和 Gid 为 0,且文件权限是 0644;
- e) 应正确配置/etc/motd 权限。

C.4 安全审计配置

C.4.1 Auditd 服务配置

Auditd 服务配置要求包括:

- a) 应启用 auditd 审计服务;
- b) 应启用审计日志 rotate,用于配置日志文件大小到达上限时该如何处理;
- c) 应配置 sudoers 审计规则,如 sudo 命令允许普通用户提权执行 root 管理员权限相关的操作,属于高危操作。

C.4.2 Rsyslog 服务配置

Rsyslog 服务配置要求包括:

- a) 应启用 rsyslog 服务,使得系统日志转储到持久性存储设备,避免系统重启后日志丢失;
- b) 应记录系统认证相关事件日志,用于分析用户登录、root 权限使用以及监测系统的可疑动作等情况;
- c) 应记录 cron 服务日志,当出现恶意操作时,能从日志信息中查看异常,并跟踪系统异常状况;
- d) 应正确配置日志记录,使用 rsyslog 对系统的重要行为及安全相关的信息进行记录;
- e) 应正确配置 rsyslog 默认文件权限,新创建的日志文件权限可在 rsyslog 配置文件中进行配置,并通过设置默认文件权限使新创建的日志文件具有合理安全的权限。

附 录 D
(规范性)
云容器安全配置项

D.1 守护进程文件配置项

守护进程文件配置项要求包括：

- a) 应设置 docker.service 文件的所有权为 root:root；
- b) 应设置 docker.service 文件权限为 644 或更多限制性；
- c) 应设置 docker.socket 文件所有权为 root:root；
- d) 应设置 docker.socket 文件权限为 644 或更多限制性；
- e) 应设置 /etc/docker 目录所有权为 root:root；
- f) 应设置 /etc/docker 目录权限为 755 或更多限制性；
- g) 应设置仓库证书文件所有权为 root:root；
- h) 应设置仓库证书文件权限为 444 或更多限制性；
- i) 应设置 TLS CA 证书文件所有权为 root:root；
- j) 应设置 TLS CA 证书文件权限为 444 或更多限制性；
- k) 应设置 docker 服务器证书文件所有权为 root:root；
- l) 应设置 docker 服务器证书文件权限为 444 或更多限制；
- m) 应设置 docker 服务器证书密钥文件所有权为 root:root；
- n) 应设置 docker 服务器证书密钥文件权限为 400；
- o) 应设置 docker.sock 文件所有权为 root:docker；
- p) 应设置 docker.sock 文件权限为 660 或更多限制性；
- q) 应设置 daemon.json 文件所有权为 root:root；
- r) 应设置 daemon.json 文件权限为 644 或更多限制性；
- s) 应设置 /etc/default/docker 文件所有权为 root:root；
- t) 应设置 /etc/default/docker 文件权限为 644 或更多限制性。

D.2 容器运行时配置项

D.2.1 Docker 运行时安全配置项

Docker 运行时安全配置项要求包括：

- a) 不应使用特权容器；
- b) 不应将敏感的主机系统目录作为容器卷进行挂载，如 /、/boot、/dev、/etc、/lib、/proc、/sys、/usr 等；
- c) 不应在容器中运行 SSH 进程；
- d) 应设置容器的 root 文件系统为只读；
- e) 应设置 on-failure 容器重启策略为 5；
- f) 不应应用 NET_RAW；
- g) 应设置 anonymous-auth 为 false；
- h) 应设置 kubelet-https 为 true；
- i) 应启用 AppArmor 配置文件；

- j) 应设置 SELinux 安全选项；
- k) 应限制使用 PID cgroup。

D.2.2 containerd 运行时安全配置项

containerd 运行时安全配置要求包括：

- a) 应将 containerd 的 socket 文件权限设置为 660 或更严格；
- b) 应将 containerd 的 socket 文件所有权设置为 root:root。

D.2.3 CRI-O 运行时安全配置项

CRI-O 运行时安全配置要求包括：

- a) 不应创建从主机到容器卷的敏感目录映射；
- b) 应将 crio.service 文件的所有权设置为 root:root；
- c) 应将 crio.service 文件的权限设置为 644 或更严格；
- d) 应将 crio.sock 文件的所有权设置为 root:root；
- e) 应将 crio.sock 文件的权限设置为 644 或更严格；
- f) 应将/etc/crio 文件的所有权设置为 root:root；
- g) 应将/etc/crio 文件的权限设置为 755 或更严格；
- h) 应将/etc/sysconfig/crio 文件的所有权设置为 root:root；
- i) 应将/etc/sysconfig/crio 文件的权限设置为 644 或更严格；
- j) 应将 log_level 设置为 INFO 或 WARN 级别；
- k) 应将 disable_checkpoint 设置为 true,以禁用容器检查点功能；
- l) 应将 crio.sock 没有被挂载到任何容器内。

D.3 容器编排配置项

D.3.1 API 服务器配置

API 服务器配置要求包括：

- a) 不应匿名访问,设置 anonymous-auth 参数为 false,并验证 authorization-mode 是否正确配置,如 RBAC；
- b) 不应设置 basic-auth-file 参数；
- c) 不应设置 insecure-allow-any-token 参数；
- d) 应设置 kubelet-https 参数为 true,宜配置 TLS 证书；
- e) 不应设置 insecure-bind-address 参数；
- f) 应设置 insecure-port 参数为 0；
- g) 不应设置 secure-port 参数为 0；
- h) 应设置 profiling 参数为 false；
- i) 应设置 repair-malformed-updates 参数为 false；
- j) 建议对存储在 etcd 中的数据采用 encryption-provider-config 进行加密,保护敏感信息；
- k) 应配置服务器的速率限制防止 API 滥用,如 max-requests-inflight、max-mutating-requests-in-flight。

D.3.2 调度程序配置

调度程序配置要求包括：

- a) 应设置 profiling 参数为 false;
- b) 应设置 address 参数设置为 127.0.0.1;
- c) 应配置 authorization-mode, 限制未授权的调用。

D.3.3 控制器配置

控制器配置要求包括:

- a) 应设置 terminated-pod-gc-threshold 参数设置为适当;
- b) 应设置 profiling 参数设置为 false;
- c) 应设置 use-service-account-credentials 参数设置为 true;
- d) 应设置 service-account-private-key-file 设置为适当值;
- e) 应设置 root-ca-file 参数为适当值;
- f) 应设置 RotateKubeletServerCertificate 参数为 true;
- g) 应设置 address 参数为 127.0.0.1;
- h) 应设置 use-pod-security-policy 使控制器执行 pod 安全策略。

D.3.4 etcd 配置

etcd 配置要求包括:

- a) 应设置 cert-file 和 key-file 参数为适当值;
- b) 应设置 client-cert-auth 参数设置为 true;
- c) 不应设置 auto-tls 参数为 true;
- d) 应设置 peer-cert-file 和 peer-key-file 参数设置为适当值;
- e) 应设置 peer-client-cert-auth 参数设置为 true;
- f) 不应设置 peer-auto-tls 参数为 true;
- g) 应配置绑定 etcd 端点绑定地址, 防止 2379 端口暴露。

D.3.5 Kubelet 配置

Kubelet 配置要求包括:

- a) 应设置 anonymous-auth 参数设置为 false, 或在 config file 文件中配置;
- b) 不应设置 authorization-mode 参数为“始终允许”;
- c) 应设置 client-ca-file 参数为适当值;
- d) 应设置 read-only-port 参数为 0;
- e) 不应设置 streaming-connection-idle-timeout 参数为 0;
- f) 应设置 protect-kernel-defaults 参数为 true;
- g) 应设置 make-iptables-util-chains 参数为 true;
- h) 不应设置 hostname-override 参数;
- i) 应设置 event-qps 参数为 0;
- j) 应设置 tls-cert-file 和 tls-private-key-file 参数为适当值;
- k) 不应设置 rotate-certificates 参数未为 false;
- l) 应设置 RotateKubeletServerCertificate 参数为 true;
- m) 应配置 fail-swap-on 禁用 Swap 功能, 避免 Kubelet 受到影响;
- n) 应设置 service-account-lookup, 避免 Kubelet 获取过高的权限;
- o) 应配置 allow-privileged, 避免 Kubelet 获得容器特权功能;
- p) 应配置 pids-max-pids 容器内进程进程数为适当值。

D.3.6 集群编排配置文件权限

集群编排配置文件权限要求包括：

- a) 应设置 API 服务器 pod 规格文件权限设置为 644 或更严格；
- b) 应设置 API 服务器 pod 规范文件所有权为 root:root；
- c) 应设置控制器管理器 pod 规格文件权限为 644 或更严格；
- d) 应设置控制器管理器 pod 规格文件所有权设置为 root:root；
- e) 应设置调度程序 pod 规格文件权限设置为 644 或更严格；
- f) 应设置调度程序 pod 规格文件所有权设置为 root:root；
- g) 应设置 etcd pod 规格文件权限设置为 644 或更严格；
- h) 应设置 etcd pod 规格文件所有权设置为 root:root；
- i) 应设置容器网络接口文件权限设置为 644 或更严格；
- j) 应设置容器网络接口文件所有权设置为 root:root；
- k) 应设置 etcd 数据目录权限设置为 700 或更严格；
- l) 应设置 admin.conf 文件权限设置为 644 或更严格；
- m) 应设置 admin.conf 文件所有权设置为 root:root；
- n) 应设置 scheduler.conf 文件权限设置为 644 或更严格；
- o) 应设置 scheduler.conf 所有权设置为 root:root；
- p) 应设置 controller-manager.conf 文件权限设置为 644 或更严格；
- q) 应设置 controller-manager.conf 文件所有权设置为 root:root；
- r) 应设置 Kubernetes PKI 目录和文件所有权设置为 root:root；
- s) 应设置 Kubernetes PKI 目录和文件权限设置为 750 或更严格；
- t) 应设置 Kubernetes PKI 密钥文件权限设置为 600。

参 考 文 献

- [1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
 - [2] GB/T 31167—2023 信息安全技术 云计算服务安全指南
 - [3] GB/T 34942—2025 网络安全技术 云计算服务安全能力评估方法
 - [4] GB/T 35293—2017 信息技术 云计算 虚拟机管理通用要求
 - [5] GB/T 37972—2019 信息安全技术 云计算服务运行监管框架
 - [6] GB/T 44158—2024 信息技术 云计算 面向云原生的应用支撑平台功能要求
 - [7] NISTSP800-53 Security and Privacy Controls for Information Systems and Organizations
-

