



中华人民共和国国家标准

GB/T 45409—2025

网络安全技术 运维安全管理产品 技术规范

Cybersecurity technology—Technical specifications for operation and
maintenance security management products

2025-03-28 发布

2025-10-01 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 III

引言 IV

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 通则 2

6 安全技术要求 3

 6.1 安全功能要求 3

 6.2 自身安全要求 6

 6.3 安全保障要求 8

7 测试评价方法 9

 7.1 总体说明与测试环境 9

 7.2 安全功能测评 10

 7.3 自身安全测评 16

 7.4 安全保障测评 23

附录 A（规范性） 运维安全管理产品技术要求等级划分和对应测试评价方法 28

 A.1 安全技术要求等级划分 28

 A.2 测试评价方法 29

附录 B（资料性） 运维安全管理产品典型应用场景 31

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：公安部第三研究所、浙江齐治科技股份有限公司、中国科学院软件研究所、华为技术有限公司、上海辰锐信息科技有限公司、中国网络安全审查认证和市场监管大数据中心、国家工业信息安全发展研究中心、奇安信网神信息技术(北京)股份有限公司、北京天融信网络安全技术有限公司、北京神州绿盟科技有限公司、西安交大捷普网络科技有限公司、北京邮电大学、杭州中尔网络科技有限公司、蓝象标准(北京)科技有限公司、远江盛邦(北京)网络安全科技股份有限公司、深信服科技股份有限公司、长扬科技(北京)股份有限公司、杭州安恒信息技术股份有限公司、北京时代新威信息技术有限公司、北京启明星辰信息技术有限公司、上海三零卫士信息安全有限公司、中电科网络安全科技股份有限公司、上海观安信息技术股份有限公司、广东安创信息科技有限公司、蓝盾信息安全技术股份有限公司、北京智游网安科技有限公司、陕西省网络与信息安全测评中心、河南中科安永科技有限公司、国网区块链科技(北京)有限公司、广东省信息安全测评中心、广电计量检测集团股份有限公司、内蒙古数字经济安全科技有限公司、国网新疆电力有限公司电力科学研究院。

本文件主要起草人：张艳、邹春明、胡津铭、赵戈、沈亮、徐鹏、吴强、蔡永娟、晏敏、杨晨、王峰、王曦、申永波、王冲华、宋小宝、姜威、周进、何建锋、马向亮、葛方隼、张德保、王成义、刘晨、汪义舟、吴焱、王连强、周瑞群、刘彪、鄢昱恒、谢江、钟英南、刘强、韩云、冯燕飞、郭军武、石竹玉、叶劲宏、唐迪、蔡宇渊、加依达尔·金格斯。

引 言

为落实《中华人民共和国网络安全法》第二十三条,GB 42250《信息安全技术 网络安全专用产品安全技术要求》规定了网络安全专用产品及其提供者均需满足的基线要求。

本文件是 GB 42250 的配套标准。GB 42250 与本文件共同用于指导运维安全管理产品的研发、生产、服务、检测和认证工作。

网络安全技术 运维安全管理产品 技术规范

1 范围

本文件规定了运维安全管理产品的安全功能要求、自身安全要求、安全保障要求及测试评价方法，并提出产品等级划分要求。

本文件适用于运维安全管理产品的设计、研发、生产、服务、检测和认证。

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 18336(所有部分) 网络安全技术 信息技术安全评估准则
- GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 36626—2018 信息安全技术 信息系统安全运维管理指南
- GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求
- GB/T 39837—2021 信息技术 远程运维 技术参考模型
- GB 42250—2022 信息安全技术 网络安全专用产品安全技术要求

3 术语和定义

GB/T 18336(所有部分)、GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

运维安全管理产品 operation and maintenance security management product

为运维用户提供统一的身份认证接口、多种远程运维管理方式，对资产及其账号等进行集中管理和授权，监控和审计运维操作过程，并对违规操作行为进行报警、阻断的产品。

3.2

运维对象 operation and maintenance object

受运维安全管理产品保护、通过运维安全管理产品进行远程运维管理的信息资产。

注：常见运维对象包括操作系统、数据库管理系统、网络设备、安全设备等。

3.3

运维用户 operation and maintenance user

通过运维安全管理产品对信息资产进行运行维护和管理用户（人员或自动化运维工具）。

注：运维用户通常以账号作为用户标识，账号由运维安全管理产品进行管理维护。

3.4

授权管理员 authorized administrator

对运维安全管理产品自身进行管理的管理人员。

注：授权管理员包括系统管理员、安全管理员、审计管理员，其职责仅限于对运维安全管理产品自身的管理。

3.5

运维服务协议 operation and maintenance service protocol

对运维对象进行运维操作和管理的网络应用协议。

3.6

统一身份认证系统 unified identity authentication system

专门为用户提供统一的身份标识和鉴别,反馈鉴别结果的系统。

4 缩略语

下列缩略语适用于本文件。

CPU:中央处理单元(Central Processing Unit)

IP:网际协议(Internet Protocol)

IPv4:网际协议版本 4(Internet Protocol version 4)

IPv6:网际协议版本 6(Internet Protocol version 6)

LDAP:轻型目录访问协议(Lightweight Directory Access Protocol)

RADIUS:远程用户拨号认证服务(Remote Authentication Dial In User Service)

RDP:远程桌面协议(Remote Desktop Protocol)

SNMP:简单网络管理协议(Simple Network Management Protocol)

SSH:安全外壳协议(Secure Shell)

5 通则

运维安全管理产品为运维用户提供统一资源访问入口,通过身份认证接口实现对运维用户的身份鉴别,对资产及其管理账户等进行集中管理和授权,监控和审计运维操作过程,并对违规操作行为进行报警、阻断。该类产品保护的对象是操作系统、数据库管理系统、虚拟机、网络设备、安全产品、云平台等信息系统重要资产。此外,运维安全管理产品本身及其内部的重要数据(产品自身及托管的账号和口令、安全配置数据、审计数据等)也是受保护的对象,见图 1。

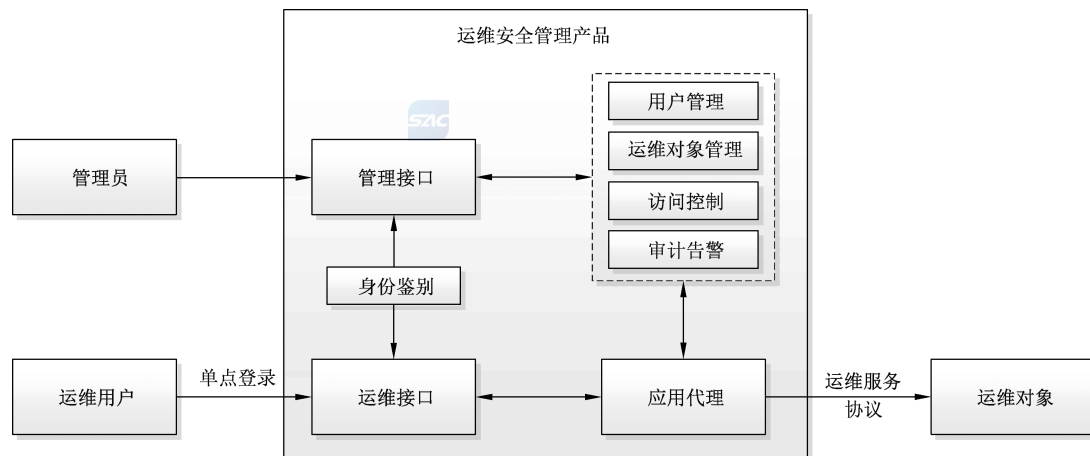


图 1 运维安全管理产品逻辑架构图

本文件将运维安全管理产品的安全技术要求分为安全功能要求、自身安全要求、安全保障要求三类。其中,安全功能要求是对运维安全管理产品应具备的安全功能提出具体要求,包括运维用户管理、运维对象管理、运维服务协议支持、运维访问控制、运维会话管理、运维审计、告警、可用性、虚拟化部署、IPv6 支持、互联互通等;自身安全要求是对运维安全管理产品的自身安全保护提出具体要求,包括通用

要求、标识与鉴别、自身访问控制、自身安全审计、通信安全、配置备份与恢复、时钟同步等；安全保障要求针对运维安全管理产品的开发和使用文档等内容提出具体的要求，包括供应链安全、设计与开发、生产和交付、运维服务保障、用户信息保护等。此外，本文件针对运维安全管理产品的安全技术要求提出了对应的测试评价方法，为使用本文件的人员提供一个测试评价运维安全管理产品的技术准则。

本文件将运维安全管理产品分为基本级和增强级，安全功能与自身安全的强弱，以及安全保障要求的高低是等级划分的具体依据，等级突出安全特性。基本级要求主要支撑 GB/T 22239 第二级安全要求安全计算环境中资产运维安全及资产自身安全的相关要求，增强级要求主要支撑 GB/T 22239 第三级安全要求安全计算环境中资产运维安全及资产自身安全、GB/T 39786 中设备和计算安全中资产运维的密码应用安全相关要求。与基本级内容相比，增强级中要求有所增加或变更的内容在正文中通过“**宋体加粗**”表示。安全技术要求的等级划分和对应测试评价方法应符合附录 A 的要求。

运维安全管理产品在实际应用时，为防止其安全策略被绕过，通常需要结合外部安全措施来保障，在附录 B 中给出了运维安全管理产品的典型应用场景，以及所需采取的外部安全措施。

6 安全技术要求

6.1 安全功能要求

6.1.1 运维用户管理

产品应支持对运维用户进行管理：

- a) 运维用户账户的增加、删除；
- b) 运维用户安全属性定义与修改，包括但不限于账户、用户姓名、联系电话、鉴别信息等；
- c) 本地运维用户账户分组管理；
- d) 与统一身份认证系统对接，由统一身份认证系统对运维用户进行身份鉴别。

6.1.2 运维对象管理

产品应支持对运维对象进行管理：

- a) 运维对象的唯一性标识；
- b) 运维对象的增加、删除、修改；
- c) 运维对象安全属性定义与修改，包括但不限于运维对象的资产类别、IP 地址、运维服务协议、运维对象账户及口令等；
- d) 运维对象分组分类管理；
- e) **运维对象连通性测试；**
- f) **对运维对象账号及鉴别信息进行托管，并支持对鉴别信息进行定期更换，更换周期和鉴别信息复杂度可设置；**
- g) 采用密码技术保障所托管的运维对象管理账户及鉴别信息在存储过程中的保密性和完整性。

6.1.3 运维服务协议支持

产品应至少支持以下运维服务协议对运维对象进行网络运维：

- a) SSH 等命令行方式的运维协议；
- b) RDP 等图形界面方式的运维协议。

6.1.4 运维访问控制

6.1.4.1 用户登录策略

产品应提供统一的身份鉴别功能，实现运维用户的单点登录，运维用户需经过产品的身份鉴别后，

方可访问授权范围内的资产。

6.1.4.2 访问控制策略

产品应支持以下条件对运维过程实施访问控制,且默认禁止:

- a) 主体:运维用户、运维用户组、源地址等;
- b) 客体:运维对象类别、运维对象及其账户等;
- c) 运维服务协议;
- d) 运维时间段。

6.1.4.3 违规操作控制

产品应依据访问控制策略、操作命令,对违规操作进行告警、阻断(操作命令或会话阻断),确保运维用户访问过程的合规性。

6.1.4.4 敏感操作提示

产品应支持敏感操作定义,依据安全策略对敏感操作提请授权人员进行二次确认,确认后才能继续进行运维操作。

6.1.5 运维会话管理

6.1.5.1 会话监视

产品应支持授权人员对运维会话过程进行实时监视。

6.1.5.2 会话回放

产品应提供历史运维会话回放功能:

- a) 通过视频方式对运维会话过程的回放;
- b) 按操作命令或时间进行回放定位。

6.1.6 运维审计

6.1.6.1 运维审计记录

产品应对运维用户的运维操作进行审计,生成审计记录,应至少包括:

- a) 运维操作的起止日期和时间;
- b) 运维用户账号、登录 IP 地址;
- c) 运维对象名称、IP 地址及账户;
- d) 运维服务协议;
- e) 命令行方式运维服务协议:至少包括操作命令、操作时间、返回内容;
- f) 图形界面方式运维服务协议:通用视频格式的录屏文件,并保证清晰度。

6.1.6.2 运维审计查阅

产品应仅允许授权管理员查阅审计记录,支持条件查询并以通用格式导出,查询条件应至少包括:

- a) 操作日期和时间段;
- b) 运维用户、登录 IP 地址;
- c) 运维对象名称、IP 地址及账户;
- d) 运维服务协议;

e) 操作命令等。

6.1.6.3 审计报表

产品应支持基于时间段、运维用户、运维对象等条件生成运维审计报表,并支持一种或者多种通用文本格式,支持自定义报表内容。

6.1.7 告警

6.1.7.1 告警内容

产品应依据告警策略对运维用户的违规操作进行告警,告警信息应至少包括:

- a) 操作时间;
- b) 运维用户;
- c) 源地址;
- d) 运维对象;
- e) 运维服务协议;
- f) 事件描述;
- g) 触发的策略等。

6.1.7.2 告警方式

产品应支持以下方式进行告警:

- a) 屏幕告警;
- b) 短信、邮件或即时通信等至少一种方式告警。

6.1.8 可用性

产品应支持双机或集群方式部署,并保持产品间配置的同步,保证产品的高可用性。

6.1.9 虚拟化部署(有则适用)

产品虚拟化部署要求包括:

- a) 应支持部署于虚拟化环境中,如虚拟机或容器等;
- b) 应支持对虚拟化资源进行运维管理;
- c) 应支持与云管理平台对接。

6.1.10 IPv6 支持(有则适用)

产品应支持在 IPv6 网络环境下正常工作,有效运行其安全功能和自身安全功能:

- a) 支持在 IPv6 网络环境下对运维对象进行管理;
- b) 支持在 IPv6 网络环境下进行自身管理;
- c) 支持 IPv4、IPv6 双协议栈工作模式。

6.1.11 互联互通(有则适用)

产品应符合《网络安全技术 网络安全产品互联互通框架》规定的互联互通信息格式和互联互通功能接口要求。

6.2 自身安全要求

6.2.1 通用要求

产品应符合 GB 42250—2022 中第 5 章规定的标识和鉴别、自身访问控制、自身安全审计、通信安全、支撑系统安全、产品升级、用户信息安全和密码等方面的要求。

注：GB 42250—2022 第 5 章中所述的用户在本文件中包括管理员和运维用户。

6.2.2 标识与鉴别

6.2.2.1 身份标识



产品应为用户提供唯一的身份标识,并将标识与其所有可审计事件相关联。

6.2.2.2 身份鉴别

身份鉴别要求包括:

- a) 产品应在执行任何与安全功能相关操作之前鉴别用户的身份;
- b) 支持两种或两种以上身份鉴别方式,且其中至少一种鉴别技术应使用密码技术实现。

6.2.2.3 鉴别失败处理

当对用户鉴别尝试连续失败达到设定的次数后,产品应阻止进一步的鉴别请求;鉴别失败尝试次数及限制登录时间具有合理的默认值,或仅由授权管理员设定。

6.2.2.4 超时锁定或注销

产品应具有登录连接超时锁定或注销功能,在设定的时间段内没有任何操作的情况下,终止会话,需要再次进行身份鉴别才能够重新操作,最大超时时间具有合理的默认值,或仅由授权管理员设定。

6.2.2.5 鉴别信息安全

产品应采用密码技术保障用户鉴别信息在传输和存储过程中的保密性和完整性。

6.2.3 自身访问控制

6.2.3.1 管理员权限

产品应允许授权管理员对产品进行以下管理:

- a) 创建和删除管理员;
- b) 查阅和修改安全属性;
- c) 制定和修改安全策略。

6.2.3.2 管理员角色

产品应对管理员角色进行区分:

- a) 具有至少三种不同权限的管理员角色,例如系统管理员、安全管理员、审计管理员等;
- b) 根据不同的功能模块,自定义各种不同权限角色,并可对管理员分配角色;
- c) 根据运维对象的分组情况,对管理员可管理的范围进行授权。

6.2.3.3 安全管理

产品应采取措施保障管理安全:

- a) 支持对可远程管理的主机地址范围进行限制；
- b) 应关闭非必要的服务和端口；
- c) 若产品形态为硬件,支持以 SNMP 等标准协议方式对产品的 CPU、内存、存储等资源使用情况进行监测；
- d) 应对产品的重要组件或功能模块运行状态进行监测,出现异常时及时告知管理员；
- e) 支持独立的管理接口,实现运维业务接口与管理接口的分离。

6.2.4 自身安全审计

6.2.4.1 系统日志生成

产品应对产品自身管理相关事件生成系统日志：

- a) 用户的鉴别事件,包括成功和失败,鉴别失败处理；
- b) 安全策略的增加、删除和修改操作；
- c) 用户/角色的增加、删除和属性修改操作；
- d) 配置备份与恢复、安全升级等重要操作；
- e) 管理员的其他操作。

6.2.4.2 系统日志内容

系统日志内容至少应包括事件发生的日期、时间、主体标识、事件描述和结果等。

6.2.4.3 系统日志管理

产品应提供下列系统日志管理功能：

- a) 仅允许授权管理员访问系统日志；
- b) 对系统日志的条件查询功能,查询条件至少包括日期时间范围、主体标识、事件描述关键词等；
- c) 应对系统审计进程进行保护,防止未经授权的中断。

6.2.4.4 审计数据存储

产品应提供以下功能对运维审计记录、系统日志进行安全存储：

- a) 当存储空间达到阈值时,及时通知授权管理员；
- b) 当存储空间达到阈值时,采取防止系统日志丢失的技术措施；
- c) 支持对审计数据进行备份；
- d) 采用密码技术保障审计数据的完整性。

6.2.5 通信安全

产品应采用密码技术保障用户网络运维通道和自身管理通道的数据传输保密性和完整性。



6.2.6 密码要求

本文件中凡要求采用密码技术的相关内容,应符合国家密码管理主管部门的相关要求。

6.2.7 配置备份与恢复

产品应支持配置文件的备份与恢复：

- a) 支持配置文件的备份与恢复,并支持备份文件的导入导出；
- b) 应采用密码技术保障配置文件的完整性；

- c) 支持配置文件的自定义周期备份。

6.2.8 时钟同步

产品应具备时钟同步功能,保证产品系统时间与时钟服务器的一致性。

6.3 安全保障要求

6.3.1 通用要求

产品应符合 GB 42250—2022 中第 6 章规定的供应链安全、设计与开发、生产和交付、运维服务保障和用户信息保护等方面的要求。

6.3.2 设计与开发

6.3.2.1 安全设计

产品提供者应提供产品安全功能和自身安全功能的设计文档,应满足以下要求:

- a) 描述产品安全架构设计,并与产品的安全功能和自身安全功能一致;
- b) 描述产品采取的自我保护、不可旁路的安全机制;
- c) 完整地描述产品的安全功能和自身安全功能;
- d) 描述所有安全功能和自身安全功能接口的目的、使用方法及相关参数;
- e) 标识和描述产品安全功能和自身安全功能的所有子系统,并描述子系统间的相互作用;
- f) 提供子系统和安全功能接口间的对应关系;
- g) 通过实现模块描述安全功能,标识和描述实现模块的目的、相关接口及返回值等,并描述实现模块间的相互作用及调用的接口;
- h) 提供实现模块和子系统间的对应关系。

6.3.2.2 实现表示

产品提供者应为全部安全功能提供实现表示,应满足以下要求:

- a) 实现表示应按详细级别定义产品安全功能,且详细程度达到无需进一步设计就能生成产品安全功能的程度;
- b) 实现表示以开发人员使用的形式提供;
- c) 设计描述与实现表示示例之间的映射能证明它们的一致性。

6.3.2.3 配置管理

产品提供者的配置管理能力应满足以下要求:

- a) 使用配置管理系统对组成产品的所有配置项进行维护;
- b) 建立维护配置项列表,包括产品评估证据和产品组成部分;
- c) 配置管理系统提供一种自动方式来支持产品的生产,通过该方式确保只能对产品的实现表示进行已授权的改变;
- d) 配置管理文档包括一个配置管理计划,配置管理计划描述如何使用配置管理系统开发产品;
- e) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

6.3.2.4 指导性文档

产品提供者应提供操作用户指南和准备程序,应满足以下要求:

- a) 描述用户可访问的功能和特权,包含适当的警示信息;

- b) 描述用户以安全方式使用产品提供的可用接口；
- c) 描述产品安全功能及接口的用户操作方法,包括配置参数的安全值等；
- d) 标识和描述产品运行的所有可能状态,包括操作导致的失败或者操作性错误；
- e) 描述实现产品安全目的所需执行的安全策略；
- f) 描述安全安装产品及其运行环境必需的所有步骤。

6.3.2.5 安全测试

产品提供者对产品进行安全测试,应满足以下要求:

- a) 测试文档描述所有测试项与安全设计文档中所描述产品的安全功能和自身安全功能间的对应性；
- b) 测试文档所标识的测试项与安全设计中产品安全功能接口间的对应性,并证实所有安全功能接口都进行了测试；
- c) 测试文档描述所有测试项的测试计划和执行方案,方案包括如测试条件、测试步骤、预期结果和实际结果等内容；
- d) 基于已标识潜在脆弱性,产品能够抵抗具备基本攻击潜力的攻击者的攻击；
- e) 基于已标识潜在脆弱性,产品能够抵抗具备中等攻击潜力的攻击者的攻击。

7 测试评价方法

7.1 总体说明与测试环境

测试评价方法针对安全技术要求逐项提出,给出的具体测试方法来验证运维安全管理产品是否达到安全技术要求中所提出的要求,主要由测试方法、预期结果和结果判定构成。

运维安全管理产品安全功能和自身安全测评典型环境如图 2 所示。

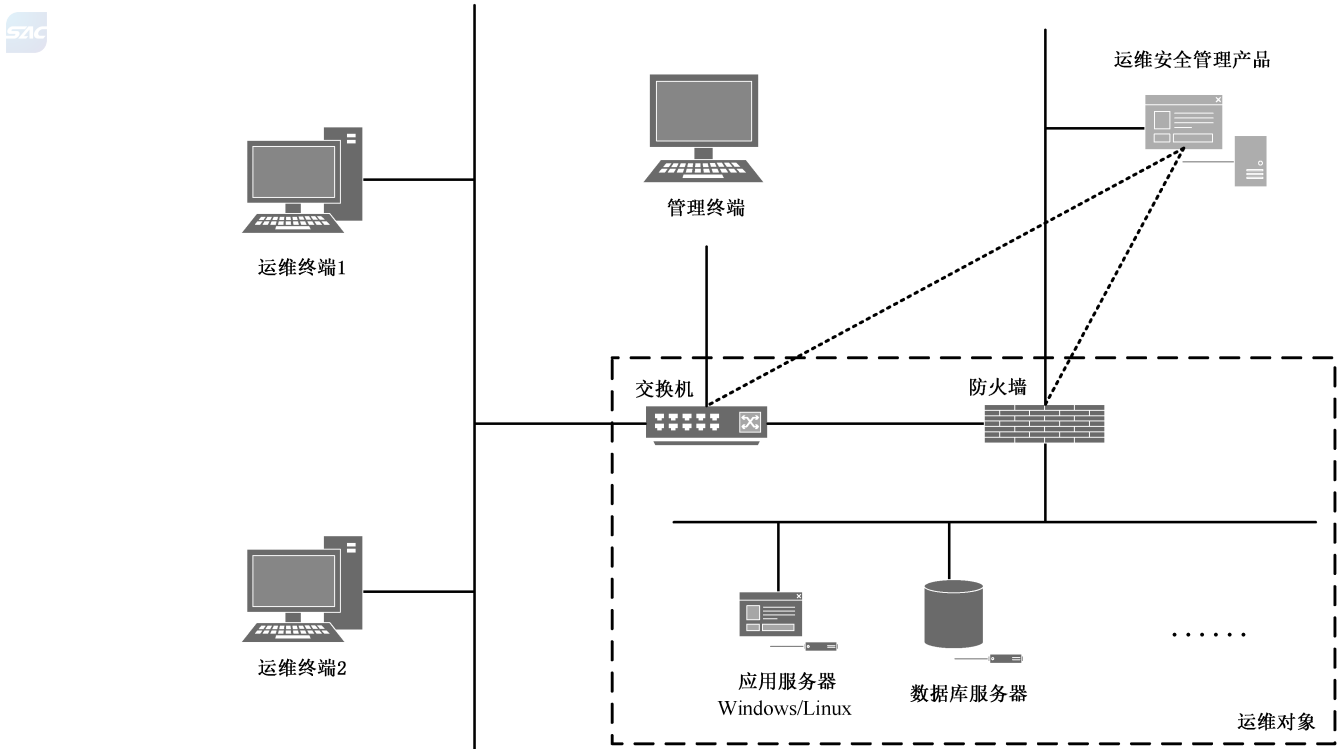


图 2 运维安全管理产品安全功能和自身安全测评典型环境示意图

7.2 安全功能测评

7.2.1 运维用户管理

运维用户管理的测试评价方法如下。

a) 测试方法：

- 1) 尝试增加、删除运维用户账户；
- 2) 检查新增运维用户账号时，检查其安全属性项目情况；
- 3) 检查产品是否支持本地用户账户分组管理；
- 4) 检查是否支持统一身份认证系统对接，如 LDAP、RADIUS 等，尝试配置对接统一身份认证系统，并以统一身份认证系统的账户尝试登录该产品。

b) 预期结果：

- 1) 能够增加、删除运维用户账户；
- 2) 运维用户安全属性至少能包括：账户、用户姓名、联系电话、鉴别信息，并支持用户姓名、联系电话、鉴别信息的修改；
- 3) 支持对本地用户账户分组管理；
- 4) 具有统一身份认证系统对接能力，如 LDAP、RADIUS 等，通过统一身份认证系统正确的鉴别信息可登录该产品。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2 运维对象管理

运维对象管理的测试评价方法如下。

a) 测试方法：

- 1) 尝试增加、删除、修改运维对象；
- 2) 检查运维对象是否具有唯一性标识，并尝试生成或修改为相同标识；
- 3) 新增运维对象时，检查其安全属性项目情况，并尝试对资产类别、IP 地址、运维服务协议、运维对象账户及口令等属性进行修改；
- 4) 检查产品是否支持运维对象的分组分类管理；
- 5) 分别增加可远程访问和不能访问的运维对象，检查其是否支持对连通性进行测试；
- 6) 检查产品是否支持运维对象账号及鉴别信息的托管与代填，运维时无需再次输入运维对象账号和口令；
- 7) 检查是否具有运维对象的账号的鉴别信息管理功能，尝试配置定期更换功能，并检查是否支持鉴别信息复杂度配置；
- 8) 以授权管理员身份查看存储的所托管运维对象账户和鉴别信息，检查是否采用了密码技术进行保密性和完整性保障。

b) 预期结果：

- 1) 能够增加、删除、修改运维对象；
- 2) 运维对象具有唯一性标识，不同的运维对象不会生成相同标识或修改为相同标识；
- 3) 运维对象安全属性至少包括：资产类别、IP 地址、运维服务协议、运维对象账户及口令，并支持对安全属性进行修改；
- 4) 支持运维对象分组分类管理，如网络运维组、安全运维组，Windows 主机类、Linux 主机类、网络设备类等；

- 5) 具有自动或手动方式对运维对象连通性测试能力；
 - 6) 产品能够支持运维对象账号及鉴别信息的托管,运维时无需再次输入运维对象账号和口令；
 - 7) 支持设置鉴别信息的定期更换,并可设置更换周期和鉴别信息复杂度,产品能够依据策略更换符合要求的鉴别信息；
 - 8) 采用密码技术保障所托管的运维对象账户及鉴别信息在存储过程中的保密性和完整性。
- c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.3 运维服务协议支持

运维服务协议支持的测试评价方法如下。

- a) 测试方法：
 - 1) 配置对应的允许运维用户的访问控制策略；
 - 2) 尝试通过该产品采用 SSH 协议对 Linux 操作系统进行网络运维；
 - 3) 尝试通过该产品采用 RDP 协议对 Windows 操作系统进行网络运维。
- b) 预期结果：
 - 1) 运维用户能够通过该产品采用 SSH 等命令行方式协议对 Linux 操作系统等运维对象进行运维；
 - 2) 运维用户能够通过该产品采用 RDP 等图形方式协议对 Windows 操作系统等运维对象进行运维。
- c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.4 运维访问控制

7.2.4.1 用户登录策略

用户登录策略的测试评价方法如下。

- a) 测试方法：
 - 1) 产品以旁路方式部署,通过配置访问控制策略,检查产品是否为运维用户提供统一的身份认证接口；
 - 2) 检查运维用户经过产品的身份鉴别后,是否可访问授权范围内的资产,如网络设备、安全产品、服务器、数据库、应用系统等。
- b) 预期结果：
 - 1) 产品为运维用户提供统一的身份认证接口；
 - 2) 通过产品身份鉴别后,运维用户可访问授权范围内的运维对象资产。
- c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.4.2 访问控制策略

访问控制策略的测试评价方法如下。

- a) 测试方法：
 - 1) 检查产品的运维访问控制策略要素,配置基于主体、客体及运维服务协议的访问控制策略；

- 2) 以主体身份通过相应的运维协议访问被授权的客体资源,检查访问控制策略的正确性;
- 3) 授权管理员根据运维时间段设置控制策略,通过运维账号分别在设置的运维时间段内外尝试登录产品进行运维操作。

b) 预期结果:

- 1) 授权管理员能够根据主体(运维用户、源地址等)、客体(运维对象及其账户等)、运维服务协议(SSH、RDP 等)等设置访问控制策略;
- 2) 仅访问控制策略允许的访问行为可成功执行,且默认禁止其他访问行为;
- 3) 产品支持根据运维时间段配置访问控制策略,只能在策略允许的时间段内进行运维操作。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.4.3 违规操作控制

违规操作控制的测试评价方法如下。

a) 测试方法:

- 1) 检查产品是否支持违规操作控制,配置违规操作控制策略;
- 2) 运维用户执行违规操作,检查产品是否能够对违规操作进行告警或阻断。

b) 预期结果:

- 1) 授权管理员可基于操作命令等设置违规操作告警或阻断控制策略;
- 2) 运维用户执行违规操作时,可对违规操作进行告警、阻断。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.4.4 敏感操作提示

敏感操作提示的测试评价方法如下。

a) 测试方法:

- 1) 检查产品是否具有敏感操作二次确认策略,配置敏感操作清单,如特定运维对象、特定操作命令等,配置授权人员等二次确认策略;
- 2) 运维用户执行敏感操作,检查是否有向授权人员提请二次确认请求操作;
- 3) 授权人员对二次确认请求进行批准或拒绝,检查运维用户是否能执行敏感操作。

b) 预期结果:

- 1) 授权管理员可设置敏感操作二次确认策略;
- 2) 运维用户执行敏感操作,可自动向授权人员提请二次确认请求;
- 3) 授权人员可对二次确认请求进行批准或拒绝;二次确认请求被批准,运维用户可执行敏感操作;二次确认请求被拒绝,运维用户执行敏感操作被阻断。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.5 运维会话管理

7.2.5.1 会话监视

会话监视的测试评价方法如下。

a) 测试方法:

- 1) 运维用户依据访问控制策略访问受保护的客体资源,并执行运维管理操作;

2) 以授权管理员身份登录产品,检查是否提供对访问运维对象会话过程的图形化实时监视功能。

b) 预期结果:

支持对访问运维对象会话过程的图形化实时监视功能。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.5.2 会话回放

会话回放的测试评价方法如下。

a) 测试方法:

1) 运维用户依据访问控制策略访问受保护的客体资源,并执行运维管理操作;

2) 检查是否提供对访问运维会话过程的回放功能;

3) 检查回放功能是否支持按操作命令或时间进行定位。

b) 预期结果:

1) 支持以视频方式回放运维会话;

2) 回放功能支持按操作命令或时间进行定位。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.6 运维审计

7.2.6.1 运维审计记录

运维审计记录的测试评价方法如下。

a) 测试方法:

1) 以运维人员身份登录产品,分别多次以不同的运维协议对不同的运维对象进行运维操作,然后退出运维,尝试生成各种运维审计记录;

2) 以授权管理员身份登录产品,查阅运维审计记录,检查运维审计记录所包括的数据项情况以及与实际操作的一致性。

b) 预期结果:

1) 产品能够对运维过程进行审计,包括命令行方式及图形界面方式运维;

2) 审计记录包括:操作日期和时间,运维用户账号、源登录 IP 地址,运维对象名称、IP 地址及账户,运维方式服务协议,操作内容;

3) 命令行方式运维服务协议:能够记录操作命令、操作时间、返回内容;图形界面方式运维服务协议:能够以通用视频格式进行录屏,视频具有足够的清晰度;

4) 审计记录与实际操作情况基本一致。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.6.2 运维审计查阅

运维审计查阅的测试评价方法如下。

a) 测试方法:

1) 分别以运维用户、各种管理员身份登录产品,尝试查阅运维审计记录;

2) 以授权管理员(具有运维审计记录查阅权限)身份登录产品,查阅审计记录,检查是否支持

条件查询,以及所支持的查询条件情况;

- 3) 检查查询结果是否与查询条件一致;
- 4) 检查审计记录是否支持导出操作,导出格式为通用格式;
- 5) **尝试依据操作命令,对运维审计记录进行查询。**

b) 预期结果:

- 1) 仅授权管理员可查阅审计记录,其他用户无法查阅;
- 2) 支持条件查询,查询条件包括操作日期和时间段,运维用户、源登录 IP 地址,运维对象名称、IP 地址、运维账户,运维服务协议等;
- 3) 查询结果是否与查询条件一致;
- 4) 审计记录支持以通用格式导出功能,如 DOC、PDF 等;
- 5) **审计记录可按操作命令进行查询。**

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.6.3 审计报表

审计报表的测试评价方法如下。

a) 测试方法:

- 1) 以授权管理员身份登录产品,检查是否提供多条件生成审计报表功能,检查支持报表的生成条件;
- 2) 检查是否支持自定义报表内容;
- 3) 生成审计记录报表,检查报表内容的准确性;
- 4) 尝试对报表进行导出,并记录导出格式。

b) 预期结果:

- 1) 支持基于时间段、运维用户、运维对象等条件生成审计报表;
- 2) 支持自定义报表内容,如概要操作报表、详细报表等;
- 3) 审计报表内容准确;
- 4) 支持 DOC、PDF、XLS、WPS、UOF 中的一种或者多种格式生成审计记录报表。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.7 告警

7.2.7.1 告警内容

告警内容的测试评价方法如下:

a) 测试方法:

- 1) 配置违规操作策略,并设置相应的告警方式;
- 2) 运维用户执行违规操作,检查是否产生告警信息,并检查告警内容。

b) 预期结果:

- 1) 产品支持依据告警策略对运维用户的违规操作进行告警;
- 2) 告警信息至少包含操作时间、运维用户、源地址、运维对象、运维服务协议、事件描述、触发的策略等。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.7.2 告警方式

告警方式的测试评价方法如下：

a) 测试方法：

- 1) 配置告警策略,并配置屏幕告警的告警方式;执行相应运维操作,触发告警策略;检查告警情况;
- 2) 分别配置短信、邮件或即时通信的告警方式;配置告警策略,执行对应操作,触发告警策略,检查告警情况。

b) 预期结果：

- 1) 产品支持对违规操作进行屏幕告警;
- 2) 产品至少支持短信、邮件或即时通信至少一种告警方式;
- 3) 触发告警操作时,能够及时以对应的方式进行告警。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.8 可用性

可用性的测试评价方法如下：

a) 测试方法：

- 1) 检查产品是否支持双机或集群方式部署,分别配置将两台产品配置为主备或集群工作模式;
- 2) 通过一台产品进行运维账户、运维对象及访问控制策略,检查另外一台设备的配置情况;
- 3) 关闭主机或断开主机网络,检查是否能通过备机继续进行运维管理操作。

b) 预期结果：

- 1) 产品支持双机或集群方式工作模式;
- 2) 能够及时同步多台设备间的配置信息;
- 3) 当主机出现网络连接断开时,能通过备机进行运维管理操作。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.9 虚拟化部署(有则适用)

虚拟化部署的测试评价方法如下。

a) 测试方法：

- 1) 分别尝试在虚拟化平台部署产品;
- 2) 尝试增加、删除、修改虚拟化运维资源,并添加访问控制策略,检查是否可对虚拟化资源进行运维管理;
- 3) 尝试与云管理平台对接,检查是否支持与云管理平台对接。

b) 预期结果：

- 1) 支持部署于虚拟化平台中,如虚拟机或容器等;
- 2) 支持对虚拟化资源进行运维管理;
- 3) 支持与云管理平台对接。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.10 IPv6 支持(有则适用)

IPv6 支持的测试评价方法如下。

a) 测试方法：

- 1) 模拟 IPv6 网络环境,验证产品及其安全功能是否能在 IPv6 网络环境下正常工作,是否可对运维对象进行管理;
- 2) 模拟 IPv6 网络环境,验证产品是否支持在 IPv6 网络环境下实现自身管理;
- 3) 检测产品是否支持 IPv4、IPv6 双栈方式工作。

b) 预期结果：

- 1) 产品支持在纯 IPv6 网络环境下正常工作,支持对运维对象进行管理;
- 2) 产品支持在 IPv6 网络环境下实现自身管理;
- 3) 产品能够支持 IPv4、IPv6 双栈方式工作。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.2.11 互联互通(有则适用)

互联互通的测试评价方法如下。

a) 测试方法：

- 1) 检查产品相关设计文档,是否提供与第三方产品互联互通的功能和接口;
- 2) 搭建测试环境,验证第三方产品互联互通的功能和接口是否正确执行;
- 3) 验证测试产品是否满足《网络安全技术 网络安全产品互联互通框架》规定的互联互通信息格式和互联互通功能接口要求。

b) 预期结果：

提供了与第三方产品互联互通功能和接口,并符合网络安全产品互联互通的相关标准要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3 自身安全测评

7.3.1 通用要求

通用要求的测试评价方法如下。

a) 测试方法。

- 1) 测试产品是否对其用户(包括管理员和运维用户)进行唯一性标识和鉴别;测试产品对于用户鉴别信息的存储和传输过程中,采取何种措施对其保密性和完整性进行保护;若产品采用口令鉴别机制,测试产品是否提供了口令复杂度校验机制和定期更换设置功能;产品存在默认口令时,检查产品是否强制用户对默认口令进行修改或设置口令。
- 2) 查看管理员和管理员角色列表,检查产品是否至少区分两种管理员角色,并实现管理权限相互制约;验证产品是否由授权主体配置自身访问控制策略,访问控制策略规定主体对客体的访问规则,非授权主体无法配置访问控制策略。
- 3) 以授权用户身份登录产品执行重要操作,查看审计记录,检查产品是否对操作进行了审计记录;检查是否对产品自身运行状态进行审计记录;分别以授权用户和非授权用户身份执行删除审计记录的操作,验证产品是否仅允许授权用户执行对审计记录的操作,是否能够防止修改审计记录;关闭产品电源后重新启动,检查产品是否将审计日志存储于非易失性

存储介质中,检查产品是否支持日志保存时间不少于六个月的相关配置。

- 4) 通过抓包验证产品是否提供安全措施保障产品远程管理以及运维访问网络通信数据的保密性和完整性。
- 5) 对产品进行网络漏洞扫描、WEB 应用安全扫描等安全性测试,检测是否存在已知中、高风险网络安全漏洞。
- 6) 检查产品是否支持更新自身组件的功能,包括但不限于对软件系统的升级以及各种安全能力特征库的升级;验证产品升级过程,通过抓包工具,检查产品是否提供安全措施,避免得到错误的、伪造的升级包和补丁程序。
- 7) 查看产品文档中用户信息收集相关内容,检测收集的用户信息是否是实现产品功能所必需的,检测产品实际收集的用户信息与文档描述是否一致;检测产品是否提供相关授权功能,分别在用户授权前、后尝试处理个人信息;分别在未获得、用户撤回个人信息收集授权的情况下,尝试进行与个人信息无关的安全功能;查看产品文档中个人信息传输相关内容,通过网络抓包等方式截获传输个人信息的报文,检测是否采取传输保密性和完整性保护措施;查看产品文档中个人信息存储相关内容,查看存储个人信息的文件或数据库,检测是否采取存储保密性和完整性保护措施;查看产品文档中个人信息超出保存期限处理方式相关内容,检测实际处理方式是否与文档一致,是否采取删除或匿名化处理措施。

b) 预期结果。

- 1) 产品确保在管理员等用户进行操作之前,对其进行唯一的身份识别和鉴别;鉴别信息在远程传输和本地存储过程中采取了安全措施保证保密性和完整性;产品提供鉴别信息复杂度验证机制和定期更换设置的功能,首次登录产品时,能够强制用户对默认口令进行修改或设置口令。
- 2) 产品对用户分配账户和权限,能够至少区分两种不同权限管理员角色,实现管理权限相互制约;产品由授权主体配置访问控制策略,访问控制策略规定主体对客体的访问规则。
- 3) 产品对支持的事件发生产生了审计记录,包括产品自身运行状态和重要操作;对审计记录进行了保护,只有授权用户才能够对审计记录进行必要的操作;产品将审计日志存储于非易失性存储介质中,支持日志保存时间不少于六个月的功能设置。
- 4) 远程管理产品时,应采取措施确保管理数据在传输过程中不被泄露或篡改,保证数据的保密性和完整性。
- 5) 产品不含已知中、高风险网络安全漏洞。
- 6) 产品支持更新自身组件的能力,包括但不限于对软件系统的升级以及各种安全能力特征库的升级。产品在升级过程中,保障升级数据来源可靠性和完整性,避免得到错误的、伪造的升级包和补丁程序。
- 7) 产品仅收集实现产品功能所必需的用户信息;产品在涉及个人信息处理时提供相关授权功能,仅在获得授权后方能处理个人信息;产品在未获得或撤回个人信息收集授权的情况下,能够提供与个人信息无关的安全功能;产品在涉及个人信息传输和存储的过程中采取技术手段保障个人信息的保密性和完整性;产品在涉及个人信息存储时提供对超出保存期限个人信息的处理功能,如删除或匿名化处理等措施。

c) 结果判定。

实际测试结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.2 标识与鉴别

7.3.2.1 身份标识

标识与鉴别的测试评价方法如下。

- a) 测试方法：
 - 1) 尝试增加相同标识的运维用户和管理员用户；
 - 2) 检查产品的审计日志,是否与该用户的可审计事件关联。
- b) 预期结果：
 - 1) 无法增加具有相同标识的运维用户和管理员用户,用户标识具有唯一性；
 - 2) 用户的可审计事件(如身份鉴别等)关联了用户的唯一性标识。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.2.2 身份鉴别

身份鉴别的测试评价方法如下。

- a) 测试方法：
 - 1) 分别通过管理员界面、运维用户界面在成功进行身份鉴别之前,尝试进行各项操作；
 - 2) 检查产品是否对管理员和运维用户提供两种或两种以上的身份鉴别方式；
 - 3) 检查分析各种身份鉴别方式,是否至少有一种采用了密码技术。
- b) 预期结果：
 - 1) 管理员及运维用户在成功通过身份鉴别之前,无法执行任何与安全功能相关的操作；
 - 2) 产品支持两种或两种以上的身份鉴别方式；
 - 3) 其中至少一种鉴别方式采用了密码技术。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.2.3 鉴别失败处理



鉴别失败处理的测试评价方法如下。

- a) 测试方法：
 - 1) 检查产品指导性文档或管理界面,是否具有可配置或默认的鉴别失败尝试次数及处置措施；
 - 2) 以错误的用户鉴别信息连续尝试登录产品界面,连续失败达到设定的次数后,检查产品是否阻止用户进一步的鉴别请求,如:锁定 IP 或者账号一段时间等,并再次以正确的鉴别信息尝试登录。
- b) 预期结果：
 - 1) 产品具有管理员和运维用户的身份鉴别失败处理措施,鉴别失败的次数及限制登录时间授权管理员可配置,或者具有合理的默认值,如鉴别失败 5 次,锁定 IP 或账号 10 min；
 - 2) 鉴别失败处理措施能够依据策略生效,超过设定次数后,以正确的鉴别信息也无法登录。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.2.4 超时锁定或注销

超时锁定或注销的测试评价方法如下。

- a) 测试方法：
 - 1) 检查产品指导性文档或管理界面,是否具有可配置或默认的超时时间设定;若可配置,设置 3 min 超时；
 - 2) 分别以管理员和运维人员身份登录产品,在设定的时间段内无任何操作的情况下,检查产

品是否终止会话,并尝试重新进行管理和运维操作。

b) 预期结果:

- 1) 产品具有超时退出或注销功能,最大超时时间具有合理的默认值,或仅由授权管理员设定;
- 2) 设定的时间内无任何操作时能够终止会话,需要再次进行身份鉴别后才能重新进行管理和运维操作。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.2.5 鉴别信息安全

鉴别信息安全的测试评价方法如下。

a) 测试方法:

- 1) 通过抓包工具抓取管理员和运维用户鉴别信息的传输过程,检查是否采用密码技术保障鉴别信息传输的保密性和完整性;
- 2) 查看管理员和运维用户鉴别信息的存储文件,检查是否采用密码技术保障鉴别信息存储的保密性和完整性。

b) 预期结果:

- 1) 采用密码技术保障管理员和运维用户鉴别信息的传输保密性和完整性;
- 2) 采用密码技术保障管理员和运维用户鉴别信息的存储保密性和完整性。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.3 自身访问控制

7.3.3.1 管理员权限

管理员权限的测试评价方法如下。

a) 测试方法:

- 1) 以授权管理员身份登录产品,尝试创建和删除管理员,检查是否执行成功;
- 2) 以授权管理员身份登录产品,尝试查阅和修改安全属性,检查是否执行成功;
- 3) 以授权管理员身份登录产品,尝试制定和修改安全策略,检查是否执行成功。

b) 预期结果:

- 1) 支持授权管理员创建和删除管理员;
- 2) 支持授权管理员查阅和删除安全属性;
- 3) 支持授权管理员制定和修改安全策略。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.3.2 管理员角色

管理员角色的测试评价方法如下。

a) 测试方法:

- 1) 检查产品是否至少具备三种不同权限的管理员角色,例如系统管理员、安全管理员、审计管理员等;
- 2) 检查产品是否支持根据不同的功能模块,自定义各种不同权限角色,并可对管理员分配

角色；

3) 检查产品是否支持根据运维对象的分组情况,对管理员的管理范围进行授权。

b) 预期结果:

1) 至少具有三种不同权限的管理员角色;

2) 能够根据功能模块设置不同权限的管理员角色;

3) 能够根据运维对象的分组情况,对管理员可管理的范围进行授权。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.3.3 安全管理

安全管理的测试评价方法如下。

a) 测试方法:

1) 设置远程管理的主机地址范围,分别在设定的地址范围内、外尝试对产品进行远程管理;

2) 结合产品说明文档,查阅产品所开放的端口和服务;查看产品开放的服务,并通过扫描器对产品管理接口和业务接口进行端口扫描,获取其开放的端口信息,并验证开放端口和服务的一致性;

3) 若产品形态为硬件,尝试配置 SNMP 等标准协议对产品运行状态进行监测;

4) 检查产品是否具有重要组件和功能模块的运行状态监测功能,通过后台停止数据库等重要组件和模块的运行;

5) 检查是否提供独立的管理接口,运维业务接口上是否开放了管理服务。

b) 预期结果:

1) 设定的地址范围内主机能够对被测产品进行远程管理,范围外的地址无法访问;

2) 产品管理接口和业务接口上所开放的服务和端口与说明文档一致,且无非必要的服务和端口;

3) 对于硬件产品,支持以 SNMP 等标准协议方式对产品的 CPU、内存、存储的资源使用情况进行监测;

4) 具有重要组件和功能模块的运行状态监测功能,状态变更时,能及时展现;出现停止运行等异常情况时,能通过弹窗等方式及时告知管理员;

5) 产品具有或可配置独立的管理接口,且运维业务接口上未开放管理服务。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.4 自身安全审计

7.3.4.1 系统日志生成

系统日志生成的测试评价方法如下。

a) 测试方法:

1) 以授权管理员身份登录系统,并执行各项操作;

2) 管理员/运维用户的鉴别成功和失败;

3) 对安全策略进行增加、删除和修改的操作;

4) 对用户角色进行增加、删除和属性修改的操作;

5) 对配置进行备份与恢复、安全升级;

6) 管理员的其他操作,如查阅审计记录、生成报表等。

- b) 预期结果：
 - 1) 以授权管理员身份登录系统,查看日志记录,应具有：
 - 2) 管理员/运维用户的鉴别成功和失败记录；
 - 3) 对安全策略进行更改的操作记录；
 - 4) 对角色进行增加、删除和属性修改的操作记录；
 - 5) 对配置进行备份与恢复、安全升级；
 - 6) 运维用户执行的敏感操作记录；
 - 7) **管理员的其他操作记录。**
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.4.2 系统日志内容

系统日志内容的测试评价方法如下。

- a) 测试方法：
 - 1) 以授权管理员身份登录系统,并执行各项安全操作；
 - 2) 检查产品生成的系统日志的内容。
- b) 预期结果：

系统日志的内容至少包括事件发生的日期、时间、主体标识、事件描述和结果。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.4.3 系统日志管理

系统日志管理的测试评价方法如下。

- a) 测试方法：
 - 1) 检查产品是否仅允许授权管理员访问系统日志；
 - 2) 检查产品是否提供系统日志的条件查询功能,分别尝试以日期时间范围、主体标识、事件描述关键词为条件进行查询,查看返回结果；
 - 3) 尝试以非授权方式终止审计进程或关闭审计功能。
- b) 预期结果：
 - 1) 仅允许授权管理员访问系统日志；
 - 2) 支持对系统日志进行条件查询,查询条件包括日期时间范围、主体标识、事件描述关键词；
 - 3) 非授权人员无法终止审计进程或关闭审计功能。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.4.4 审计数据存储

审计数据存储的测试评价方法如下。

- a) 测试方法：
 - 1) 检查产品存储空间达到阈值时,是否能及时通知授权管理员,包括声音、邮件、界面对话框等方式；
 - 2) 当存储空间达到阈值时,检查产品采取的防止系统日志丢失的技术措施；
 - 3) 尝试对审计数据进行备份,查看是否备份成功；
 - 4) 对系统日志进行非授权修改,检查产品是否提供完整性保护措施。

- b) 预期结果：
 - 1) 当存储空间达到阈值时,能及时通知授权管理员,可包括声音、邮件、界面对话框等方式;
 - 2) 当存储空间达到阈值时,具备相应防止系统日志丢失的技术措施;
 - 3) 支持对审计数据进行备份;
 - 4) 产品采用密码技术对系统日志的完整性进行保护。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.5 通信安全

通信安全的测试评价方法如下。

- a) 测试方法：
 - 1) 通过抓包工具抓取管理员对产品进行管理的过程数据,检查是否采用密码技术保障自身管理数据传输的保密性和完整性;
 - 2) 通过抓包工具抓取运维用户从运维终端到产品之间的运维数据,检查是否采用密码技术保障运维数据传输的保密性和完整性。
- b) 预期结果：
 - 1) 采用密码技术保障产品自身管理数据的传输保密性和完整性;
 - 2) 采用密码技术保障运维终端到产品之间运维数据的传输保密性和完整性。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.6 密码要求

密码要求的测试评价方法如下。

- a) 测试方法：

检查本文件中要求采用密码技术的相关条款(运维对象管理、身份鉴别、鉴别信息安全、审计数据存储、通信安全、配置备份与恢复)所采用的密码算法、密钥管理措施等是否符合国家密码主管部门的相关要求。
- b) 预期结果：

本文件中要求采用密码技术的相关条款的具体实现符合国家密码主管部门的相关要求。
- c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.7 配置备份与恢复

配置备份与恢复的测试评价方法如下。

- a) 测试方法：
 - 1) 对产品配置进行备份,并将备份文件导出;
 - 2) 修改产品的各项配置信息,再将备份的配置文件导入并恢复配置,检查配置信息是否对应恢复;
 - 3) 尝试登录产品支撑操作系统,对产品配置信息进行篡改,检查产品是否能够及时发现配置完整性被破坏;
 - 4) 尝试配置周期性备份策略,如每日、每周,检查是否能按策略要求进行配置备份。
- b) 预期结果：
 - 1) 产品具有配置备份功能,并支持将配置文件导出;

- 2) 产品具有配置恢复功能,支持导入配置文件并恢复各项配置;
 - 3) 产品采用密码技术保障配置文件完整性,能够及时发现配置文件遭受篡改的行为;
 - 4) 支持自定义时间周期进行自动备份。
- c) 结果判定:
- 实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.3.8 时钟同步

时钟同步的测试评价方法如下。

- a) 测试方法:
- 1) 配置时间服务器;
 - 2) 修改系统时间、或修改时间服务器时间;
 - 3) 检查被测产品是否能够及时更新时间。
- b) 预期结果:
- 被测产品的系统时间能够及时更新,并与时间服务器保持一致。
- c) 结果判定:
- 实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.4 安全保障测评

7.4.1 通用要求

通用要求的测试评价方法如下。

- a) 测试方法。
- 1) 检查产品提供者是否制定了供应商选择、评定、日常管理等程序;检查产品提供者是否保存对供应商选择、评价和日常管理的记录;检查相应程序是否对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出管理要求,以确保供应商提供的关键部件能够满足安全要求。
 - 2) 检查产品提供者是否建立程序或控制机制,确保供应链各环节核心要素的追溯能力,以保障核心要素供应稳定。
 - 3) 检查产品提供者是否制定持续开展安全意识和技能培训的程序;检查是否保存了相关培训记录。
 - 4) 检查产品提供者是否针对产品制定了安全开发的制度和流程,检查相关内容是否包括产品开发过程的安全策略、安全风险分析和威胁建模;检查是否包括是否至少包括代码编写规范、研发环境安全管理制度、研发人员安全管理制度、研发交付制度等安全开发制度及流程,以确保开发环境安全。
 - 5) 检查产品提供者是否制定了产品的安全设计文档,检查其中是否包括产品安全功能和自身安全功能的设计内容;检查设计文档的描述,是否与安全功能和自身安全功能保持一致。
 - 6) 检查产品提供者提供的配置管理文档和描述,是否制定了产品标识的命名规则,并确认具备唯一性标识;检查内容是否为配置项制定了命名规则,并确定唯一标识;检查是否建立并维护配置项列表。
 - 7) 检查产品提供者的产品相关设计文档或产品指导性文档,是否明确描述产品的功能模块、接口,并阐述未设置恶意程序、隐蔽接口或未明示功能模块等;检查是否通过用户协议、产品说明书等途径将所有功能模块、接口等告知用户。



- 8) 检查产品提供者是否对产品进行了安全性测试并提供相应的测试文档;检查测试文档的内容是否包括漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证等。
 - 9) 检查产品提供者建立和执行了产品完整性检测流程规范,检查是否包括能够防范自制或采购的组件被篡改、伪造等风险的措施。
 - 10) 检查产品提供者是否建立了内部交付程序,如设计到研发、研发到测试、测试到集成等内部交付管理流程以及相关安全措施,以确保产品在交付过程中不被破坏或篡改。
 - 11) 检查产品提供者是否提供了外部交付的控制程序,规定产品交付给客户的控制程序以及安全措施,以确保产品在交付过程中不被破坏或篡改。
 - 12) 检查产品提供者提供的相关文档,是否向用户明示包含在产品中的所有功能模块、外部接口和私有协议,告知用户产品中预置的所有账户和默认口令。
 - 13) 检查产品提供者提供的相关证据(如用户手册、界面提示、用户协议、说明文档等),检查相关证据是否确定了一个满足法律法规规定或与用户约定的期限,检查相关证据是否表明在该期限内产品提供者对产品提供持续的安全维护,声明不会单方面中断或终止安全维护。
 - 14) 检查产品提供者提供的相关证据(如界面提示、用户通知、说明文档等),检查相关证据是否证实了保护用户对软件(包含固件)安装和升级等的知情权和选择权,是否在安装和升级软件时明示用户并获得用户同意。
 - 15) 检查产品提供者是否建立和执行针对产品安全缺陷、漏洞的应急响应机制和流程(如缺陷纠正工具阐述、缺陷纠正文档、应急响应措施程序等),检查相关文档、证据是否包含对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施,是否表明会及时告知用户安全风险和可用的补救措施,是否明确了向有关主管部门报告机制和流程。
 - 16) 检查产品提供者提供的相关文档或声明,是否明示了收集用户信息的目的、方式、范围、种类、存储位置和处理方式。
 - 17) 检查产品提供者提供的相关文档或声明,是否建立和执行用户信息管理制度和流程;检查制度和流程是否明确阐述在产品的设计、生产、升级等各阶段保障用户信息的安全,且不超范围使用用户信息。
- b) 预期结果。
- 1) 产品提供者制定了供应商选择、评定、日常管理等程序;保存了对供应商选择、评价和日常管理的记录;相应程序对供应商的开发环境、规范和人员、开发工具、安全测试和安全验证机制等提出了管理要求。
 - 2) 产品提供者建立了程序或控制机制,确保供应链各环节核心要素的追溯能力;针对产品提供者和产品特点,列举所保障的核心要素(如,核心技术知识产权、工具及部件等)。
 - 3) 产品提供者制定了持续开展安全意识和技能培训的程序;保存了相关培训记录。
 - 4) 产品提供者制定了安全开发的制度和流程,其中内容包括产品开发过程的安全策略、安全风险分析和威胁建模;包括了代码编写规范、研发环境安全管理制度、研发人员安全管理制度、研发交付制度等安全开发制度及流程,以确保开发环境安全。
 - 5) 产品提供者制定了产品安全功能和自身安全功能的设计文档;设计文档的描述,能与安全功能和自身安全功能保持一致。
 - 6) 产品提供者能够提供配置管理文档,并制定了产品标识的命名规则和确定唯一性标识;建立了产品配置项命名规则并确定唯一标识;能够建立并维护配置项列表,配置项至少包括源代码、工具、文档、组件、配置信息等。
 - 7) 产品提供者的产品相关设计文档或指导性文档,能够明确描述产品的功能模块、接口,并阐述未设置恶意程序、隐蔽接口或未明示功能模块等;能够通过用户协议、产品说明书等

途径将所有功能模块、接口等告知用户。

- 8) 产品提供者对产品进行了安全性测试并提供相应的测试文档;测试文档的内容包括漏洞扫描、病毒扫描、代码审计、渗透测试和安全功能验证等。
- 9) 产品提供者建立和执行了产品完整性检测流程规范,具备防范自制或采购的组件被篡改、伪造等风险的措施。
- 10) 产品提供者建立了内部交付程序,包括设计到研发、研发到测试、测试到集成等内部交付管理流程以及相关安全措施,确保产品在交付过程中不被破坏或篡改。
- 11) 产品提供者提供了外部交付的控制程序,规定产品交付给客户的控制程序以及安全措施,确保产品在交付过程中不被破坏或篡改。
- 12) 产品提供者提供文档向用户明示包含在产品中的所有功能模块、外部接口和私有协议,告知用户产品中预置的所有账户和默认口令。
- 13) 产品提供者能够提供相关证据(如用户手册、界面提示、用户协议、说明文档等),相关证据能够确定一个满足法律法规规定或与用户约定的期限,能够表明在该期限内产品提供者对产品提供持续的安全维护,声明不会单方面中断或终止安全维护。
- 14) 产品提供者能够提供相关证据(如界面提示、用户通知、说明文档等),相关证据能够证实保护了用户对软件(包含固件)安装和升级等的知情权和选择权,能在安装和升级软件时明示用户并获得用户同意。
- 15) 建立和执行了针对产品安全缺陷、漏洞的应急响应机制和流程(如缺陷纠正工具阐述、缺陷纠正文档、应急响应措施程序等),相关文档、证据能够包含对发现的产品安全缺陷和漏洞采取修复或替代方案等补救措施,能够表明会及时告知用户安全风险和可用的补救措施,能够明确向有关主管部门报告机制和流程。
- 16) 产品提供者提供了相关文档或声明,明示了收集用户信息的目的、方式、范围、种类、存储位置和处理方式。
- 17) 产品提供者提供了相关文档或声明,能够表明建立和执行了用户信息管理制度和流程;制度和流程能够明确阐述在产品的设计、生产、升级等各阶段保障用户信息的安全,且不超范围使用用户信息。

c) 结果判定:

实际测评结果与相关预期结果一致则判定为符合,其他情况判定为不符合。

7.4.2 设计与开发

7.4.2.1 安全设计

安全设计的测试评价方法如下。

a) 测试方法:

检查安全架构、功能规范或产品设计文档是否准确描述如下内容:

- 1) 描述产品安全架构设计,并与产品的安全功能和自身安全功能一致;
- 2) 描述产品采取的自我保护、不可旁路的安全机制;
- 3) 完整地描述产品的安全功能和自身安全功能;
- 4) 描述所有安全功能和自身安全功能接口的目的、使用方法及相关参数;
- 5) 标识和描述产品安全功能和自身安全功能的所有子系统,并描述子系统间的相互作用;
- 6) 提供子系统和安全功能接口间的对应关系;
- 7) 通过实现模块描述安全功能,标识和描述实现模块的目的、相关接口及返回值等,并描述实现模块间的相互作用及调用的接口;

8) 提供实现模块和子系统间的对应关系。

b) 预期结果：

产品提供者提供的文档内容应满足上述要求。

c) 结果判定：

实际评估结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.2.2 实现表示

实现表示的测试评价方法如下。

a) 测试方法：

产品设计文档是否准确描述如下内容：

- 1) 提供产品设计描述与实现表示实例之间的映射，并证明其一致性；
- 2) 按详细级别定义产品安全功能，详细程度达到无需进一步设计就能生成安全功能的程度；
- 3) 以开发人员使用的形式提供。

b) 预期结果：

产品提供者提供的文档内容应满足上述要求。

c) 结果判定：

实际评估结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.2.3 配置管理



配置管理的测试评价方法如下。

a) 测试方法：

- 1) 检查产品提供者是否建立了配置管理系统对配置项进行了维护；
- 2) 检查配置项列表，确认是否包括产品全部配置项；
- 3) 配置管理系统提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变；
- 4) 配置管理文档包括一个配置管理计划，配置管理计划描述如何使用配置管理系统开发产品。实施的配置管理与配置管理计划相一致；
- 5) 配置管理计划描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

b) 预期结果：

产品提供者提供的文档内容应满足上述要求。

c) 结果判定：

实际评估结果与预期结果一致则判定为符合，其他情况判定为不符合。

7.4.2.4 指导性文档

指导性文档的测试评价方法如下。

a) 测试方法：

检查产品提供者提供的操作用户指南证据，并检查产品提供者提供的信息是否满足证据的内容和形式的所有要求：

- 1) 产品提供者的产品相关文档，能明确描述产品的功能模块、接口，并阐述未设置恶意程序、隐蔽接口或未明示功能模块等；
- 2) 描述用户可访问的功能和特权，包含适当的警示信息；
- 3) 描述如何以安全的方式使用产品提供的可用接口；
- 4) 是否描述产品安全功能及接口的用户操作方法，包括配置参数的安全值；

- 5) 是否标识和描述产品运行的所有可能状态,包括操作导致的失败或者操作性错误;
 - 6) 是否描述实现反垃圾邮件产品安全目的应执行的安全策略;
 - 7) 是否提供准备程序,描述安全安装产品及其运行环境必需的所有步骤。
- b) 预期结果:
- 产品提供者提供的文档内容应满足上述要求。
- c) 结果判定:
- 实际评估结果与预期结果一致则判定为符合,其他情况判定为不符合。

7.4.2.5 安全测试

安全测试的评价方法如下。

- a) 测试方法:
- 1) 检查产品提供者提供的测试覆盖文档,在测试覆盖证据中,是否表明测试文档中所标识的测试与功能规范中所描述的产品安全功能间的对应性;
 - 2) 检查测试文档是否描述所有测试项与安全设计文档中所描述产品的安全功能和自身安全功能间的对应性;
 - 3) 检查测试文档是否描述了所标识的测试项与安全设计中产品安全功能接口间的对应性,并证实所有安全功能接口都进行了测试;
 - 4) 检查测试文档是否描述所有测试项的测试计划和执行方案,方案包括如测试条件、测试步骤、预期结果和实际结果等内容;
 - 5) 对从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对产品进行脆弱性分析,判断产品是否能抵抗基本型攻击;
 - 6) 对从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对产品进行脆弱性分析,判断产品是否能够抵抗中等型攻击。
- b) 预期结果:
- 1) 产品提供者提供的文档内容应满足上述 1)~4) 要求;
 - 2) 脆弱性分析测试结果表明产品能够抵抗基本型攻击;
 - 3) 脆弱性分析测试结果表明产品能够抵抗中等型攻击。
- c) 结果判定:
- 实际评估结果与预期结果一致则判定为符合,其他情况判定为不符合。

附 录 A
(规范性)

运维安全管理产品技术要求等级划分和对应测试评价方法

A.1 安全技术要求等级划分

表 A.1 列出了运维安全管理产品技术要求的等级划分。

表 A.1 运维安全管理产品技术要求等级划分

安全技术要求			基本级	增强级
安全功能要求	运维用户管理		6.1.1 a)~c)	6.1.1
	运维对象管理		6.1.2 a)~d)	6.1.2
	运维服务协议支持		6.1.3	6.1.3
	运维访问控制	用户登录策略	6.1.4.1	6.1.4.1
		访问控制策略	6.1.4.2 a)~c)	6.1.4.2
		违规操作控制	6.1.4.3	6.1.4.3
		敏感操作提示	—	6.1.4.4
	运维会话管理	会话监视	—	6.1.5.1
		会话回放	6.1.5.2 a)	6.1.5.2
	运维审计	运维审计记录	6.1.6.1	6.1.6.1
		运维审计查阅	6.1.6.2 a)~d)	6.1.6.2
		审计报告	6.1.6.3	6.1.6.3
	告警	告警内容	6.1.7.1	6.1.7.1
		告警方式	6.1.7.2 a)	6.1.7.2
	可用性		—	6.1.8
自身安全要求	通用要求		6.2.1	6.2.1
	标识和鉴别	身份标识	6.2.2.1	6.2.2.1
		身份鉴别	6.2.2.2 a)	6.2.2.2
		鉴别失败处理	6.2.2.3	6.2.2.3
		超时锁定或注销	6.2.2.4	6.2.2.4
		鉴别信息安全	—	6.2.2.5
	自身访问控制	管理员权限	6.2.3.1	6.2.3.1
		管理员角色	6.2.3.2 a)	6.2.3.2
		安全管理	6.2.3.3 a)~c)	6.2.3.3

表 A.1 运维安全管理产品技术要求等级划分（续）

安全技术要求			基本级	增强级
自身安全要求	自身安全审计	系统日志生成	6.2.4.1 a)～d)	6.2.4.1
		系统日志内容	6.2.4.2	6.2.4.2
		系统日志管理	6.2.4.3 a)～b)	6.2.4.3
		审计数据存储	6.2.4.4 a)	6.2.4.4
	通信安全		—	6.2.5
	密码要求		—	6.2.6
	配置备份与恢复		6.2.7 a)	6.2.7
	时钟同步		6.2.8	6.2.8
安全保障要求	通用要求		6.3.1	6.3.1
	设计与开发	安全设计	6.3.2.1 a)～f)	6.3.2.1
		实现表示	—	6.3.2.2
		配置管理	6.3.2.3 a)～b)	6.3.2.3
		指导性文档	6.3.2.4	6.3.2.4
		安全测试	6.3.2.5 a)～d)	6.3.2.5

A.2 测试评价方法

表 A.2 列出了运维安全管理产品技术要求对应的测试评价方法。

表 A.2 运维安全管理产品技术要求对应的测试评价方法

测试评价方法			基本级	增强级
安全功能测评	运维用户管理		7.2.1 a)中的 1)～3), b)中的 1)～3), c)	7.2.1
	运维对象管理		7.2.2 a)中的 1)～4), b)中的 1)～4), c)	7.2.2
	运维服务协议支持		7.2.3	7.2.3
	运维访问控制	用户登录策略	7.2.4.1	7.2.4.1
		访问控制策略	7.2.4.2 a)中的 1)、2), b)中的 1)、2), c)	7.2.4.2
		违规操作控制	7.2.4.3	7.2.4.3
		敏感操作提示	—	7.2.4.4
	运维会话管理	会话监视	—	7.2.5.1
		会话回放	7.2.5.2 a)中的 1)、2) b)中的 1), c)	7.2.5.2
	运维审计	运维审计记录	7.2.6.1	7.2.6.1
		运维审计查阅	7.2.6.2 a)中的 1)～4), b)中的 1)～4), c)	7.2.6.2
		审计报表	7.2.6.3	7.2.6.3
	告警	告警内容	7.2.7.1	7.2.7.1
		告警方式	7.2.7.2 a)中的 1), b)中的 1)、3), c)	7.2.7.2

表 A.2 运维安全管理产品技术要求对应的测试评价方法 (续)

测试评价方法			基本级	增强级
安全功能测评	可用性		—	7.2.8
	虚拟化部署(有则适用)		7.2.9	7.2.9
	IPv6 支持(有则适用)		7.2.10	7.2.10
	互联互通(有则适用)		7.2.11	7.2.11
自身安全要求	通用要求		7.3.1	7.3.1
	标识和鉴别	身份标识	7.3.2.1	7.3.2.1
		身份鉴别	7.3.2.2 a)中的 1),b)中的 1),c)	7.3.2.2
		鉴别失败处理	7.3.2.3	7.3.2.3
		超时锁定或注销	7.3.2.4	7.3.2.4
		鉴别信息安全	—	7.3.2.5
	自身访问控制	管理员权限	7.3.3.1	7.3.3.1
		管理员角色	7.3.3.2 a)中的 1),b)中的 1),c)	7.3.3.2
		安全管理	7.3.3.3 a)中的 1)~3),b)中的 1)~3),c)	7.3.3.3
	自身安全审计	系统日志生成	7.3.4.1 a)中的 1)~5),b)中的 1)~6),c)	7.3.4.1
		系统日志内容	7.3.4.2	7.3.4.2
		系统日志管理	7.3.4.3	7.3.4.3
		审计数据存储	7.3.4.4 a)中的 1),b)中的 1),c)	7.3.4.4
	通信安全		—	7.3.5
	密码要求		—	7.3.6
	配置备份与恢复		7.3.7 a)中的 1)~2),b)中的 1)~2),c)	7.3.7
	时钟同步		7.3.8	7.3.8
安全保障要求	通用要求		7.4.1	7.4.1
	设计与开发	安全设计	7.4.2.1 a)中 1)~6),b),c)	7.4.2.1
		实现表示	—	7.4.2.2
		配置管理	7.4.2.3 a)中的 1)~2),b),c)	7.4.2.3
		指导性文档	7.4.2.4	7.4.2.4
		安全测试	7.4.2.5 a)中 1)~5),b)中的 1),2),c)	7.4.2.5

附 录 B
(资料性)

运维安全管理产品典型应用场景

运维安全管理产品典型部署方式如图 B.1 所示,产品通常部署于网络系统的安全管理中心区域,与运维终端区采用防火墙进行隔离,提供一个运维业务接口,与运维对象的管理接口路由可达,运维用户通过该接口实现对各资产的运维管理。

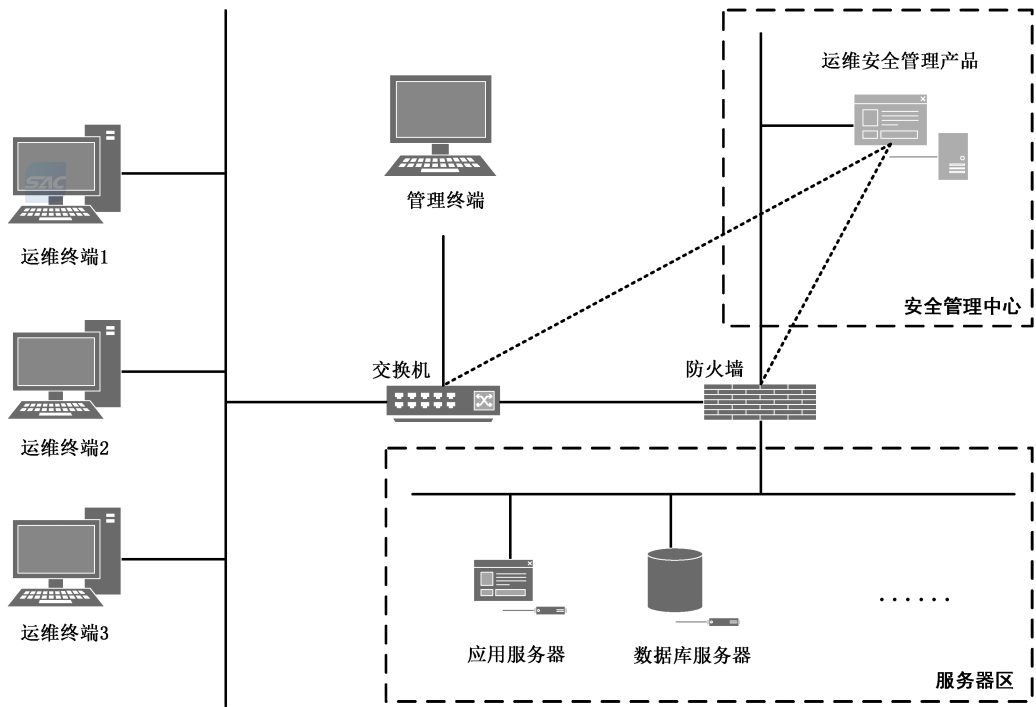


图 B.1 运维安全管理产品典型部署方式示意图

为防止运维终端绕过运维安全管理产品的安全策略,对目标资产进行直接运维,宜对部署环境中相关资产采取必要的安全措施:

- a) 防火墙仅允许运维终端区 IP 地址可远程访问运维安全管理产品运维业务接口上对应的运维服务端口,禁止访问所有运维对象资产的所有运维服务端口;
- b) 为防止运维用户登录受保护资产后,横向越权管理,或直接登录受保护资产进行运维管理,可通过完善运维对象安全配置,限制仅可通过运维安全管理产品进行远程管理。

