

备案号: CNCA/GTS 0051-2007

信息安全产品认证技术规范

ISCCC TS002-2007

信息技术 信息安全 数据备份与恢复产品认证技术规范

Technical specifications

for Data backup and recovery products certification

2008-03-05 发布

2008-03-05 实施

中国信息安全认证中心

发布

目次

前言	1
1 范围.....	2
2 规范性引用文件.....	2
3 术语和定义.....	2
4 技术要求.....	4
4.1 功能要求	4
4.1.1 备份对象.....	4
4.1.2 运行平台.....	4
4.1.3 备份模式.....	4
4.1.4 存储介质.....	5
4.1.5 系统管理功能.....	5
4.1.6 中文化支持.....	5
4.1.7 增强功能.....	5
4.2 性能评价	6
4.2.1 备份速度.....	6
4.2.2 恢复速度.....	6
4.2.3 占用资源.....	6
4.2.4 最大驱动器数.....	6
4.2.5 最大磁带槽位.....	6
4.2.6 最大磁带数.....	6
4.3 安全要求	7
4.3.1 安全审计.....	7
4.3.2 用户数据保护.....	7
4.3.3 标识和鉴别.....	7
4.3.4 功能保护.....	7
4.4 保证要求	8
5 数据备份与恢复产品技术要求的等级划分.....	8
6 测试要求.....	9
6.1 概述	9
6.1.1 测试环境.....	9
6.1.2 标准测试步骤.....	10
6.2 功能测试	10
6.2.1 备份对象.....	10
6.2.2 运行平台.....	11
6.2.3 备份模式.....	11
6.2.4 存储介质.....	12
6.2.5 系统管理功能.....	12
6.2.6 中文化支持.....	13
6.2.7 增强功能.....	13
6.3 性能测试	14
6.3.1 备份速度.....	14

6.3.2	恢复速度.....	14
6.3.3	占用资源.....	15
6.3.4	最大驱动器数.....	15
6.3.5	最大磁带槽位.....	15
6.3.6	最大磁带数.....	15
6.4	安全测试.....	15
6.4.1	安全审计.....	15
6.4.2	用户数据保护.....	16
6.4.3	标识和鉴别.....	16
6.4.4	功能保护.....	16

前 言

本技术规范规定了数据备份与恢复产品的技术要求。

本技术规范由中国信息安全认证中心（ISCCC）提出并归口。

本技术规范起草单位：北京信息安全测评中心、清华威视数据安全研究所、中国信息安全认证中心。

1 范围

本规范规定了数据备份与恢复管理软件产品的技术要求和测试要求。本规范适用于对数据备份与恢复管理软件产品的研制、生产、测试以及评估与认证。

2 规范性引用文件

下列文件中的条款通过本技术规范的引用而成为本技术规范的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本技术规范，然而，鼓励根据本技术规范达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本技术规范。

GB/T18336.2 信息技术 安全技术 信息技术安全性评估准则 第2部分：安全功能要求。

GB/T18336.3 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求。

GB/T20988-2007 信息安全技术 信息系统灾难恢复规范。

3 术语和定义

GB/T 5271.8—2001 和 GB/T 18336 确立的术语和定义适用于本技术规范。

3.1

备份数据 backup(名词)

为保护某一数据集合而存储在非易失性存储介质上的额外数据集合。

3.2

数据备份 backup(动词)

创建备份数据的过程。

3.3

数据恢复 recovery

将数据还原为数据备份前的内容或状态的过程。

3.4

数据卷 volume

用以表示卷管理器控制软件所创建的虚拟磁盘。

3.5

快照 snapshot

关于指定数据集合的一个完全可用拷贝，该拷贝是相应数据在某个时间点的映像。

3.6

备份对象 backup object

需要被备份的数据集合。

3.7

备份介质 backup media

存放备份数据的物理载体。

3.8

备份系统 backup system

实现数据备份与数据恢复的相关软件和硬件集合。

3.9

备份服务器 backup server

备份系统中提供系统管理和控制服务的主机。

3.10

备份客户端 backup client

备份系统中对备份对象进行数据访问和控制的主机。

3.11

备份存储节点 storage node

备份系统中负责访问和控制备份介质服务的主机。

3.12

完全备份 full backup

将所有指定的数据对象进行全部备份的过程。

3.13

增量备份 incremental backup

对所有自上次完全备份或者增量备份操作以来所修改过的数据对象进行备份。

3.14

差量备份(即差分备份) diffirencial backup

自上次完全备份以来所有修改过的数据对象进行备份。

3.15

网络数据管理协议 network data management protocol, NDMP

一种支持数据存储设备、磁带库设备以及备份应用程序之间互相通信以完成备份过程的通信协议。

3.16

存储区域网备份 LAN-free

备份对象的数据流通过存储区域网备份到指定的存储设备中。

4 技术要求

4.1 功能要求

4.1.1 备份对象

数据备份产品应至少支持以下一类备份对象。

4.1.1.1 数据库

对数据库系统的数据和结构进行（在线）备份和恢复。

4.1.1.2 数据卷

以数据卷为备份对象，对数据卷进行整体备份和恢复。

4.1.1.3 文件

以文件为备份对象，对文件系统中的数据进行备份和恢复。

4.1.1.4 操作系统

对操作系统的数据和状态进行备份和恢复。

4.1.2 运行平台

4.1.2.1 备份服务器运行平台

在产品声称的操作系统平台下备份服务器程序的所有功能应能正常运行。

4.1.2.2 备份客户端运行平台

在产品声称的操作系统平台下备份客户端程序的所有功能应能正常运行。

4.1.2.3 存储节点运行平台

在产品声称的操作系统平台下存储节点程序的所有功能应能正常运行。

4.1.3 备份模式

数据备份产品应至少支持以下一种备份模式。

4.1.3.1 基于本机备份

对运行备份服务器程序所在主机的数据进行备份和恢复。

4.1.3.2 基于网络备份

对运行备份客户端主机的数据可以通过网络进行备份和恢复。

4.1.3.3 LAN-free 备份

备份系统支持 LAN-free 备份。

4.1.3.4 NDMP 备份

通过 NDMP 协议进行数据备份和恢复。

4.1.4 存储介质

4.1.4.1 支持备份介质格式

支持不同格式的磁带、光盘等作为备份数据的存储介质。可以通过磁带库、自动加载机、磁带机等设备使用。

4.1.4.2 磁盘支持

支持磁盘作为备份数据的存储介质。

4.1.5 系统管理功能

4.1.5.1 策略定制

应至少能对备份对象、备份介质、备份时间、备份数据保存时间以及备份方式等制定策略。

4.1.5.2 策略管理

应能支持对已配置的策略进行添加、删除、修改、分发、导入、导出等操作。

4.1.5.3 磁带管理

对在线和离线磁带进行管理。应包括以下一项或多项功能：磁带自动标签、标记出错磁带、磁带出入库、磁带自动回收、磁带重用、磁头清洗、磁带离线管理等。

4.1.5.4 提供报表

提供作业状态和设备状态的报表，并支持多种报表格式。

4.1.5.5 管理界面

支持一种或多种形式的管理界面。

4.1.6 中文化支持

应提供中文化管理界面和提示信息。

4.1.7 增强功能

4.1.7.1 备份方式支持

支持完全备份、增量备份和增量备份等备份方式。

4.1.7.2 快照支持

支持快照技术，保证备份对象在备份时间点的数据一致性。

4.1.7.3 恢复重定向

支持将备份数据恢复到与备份对象不同的主机或目录中。

4.1.7.4 恢复时间点选择

支持选择不同备份时间点的备份数据进行恢复。

4.1.7.5 恢复内容选择

支持选择全部或部分备份数据进行恢复。

4.1.7.6 支持磁盘缓存

支持利用磁盘作为备份和恢复过程中的缓冲介质，用以提高备份和恢复作业的性能。

4.1.7.7 压缩传输

支持以减小数据传输量为目标，将备份数据进行压缩编码处理后传输。

4.1.7.8 压缩存储

支持以减小数据存储量为目标，将备份数据进行压缩编码处理后存储。

4.1.7.9 恢复自动化

支持通过恢复过程自动执行的方式，快速恢复备份数据。

4.1.7.10 恢复缺失文件

支持标识出已缺失的备份对象，并能够对缺失的备份对象进行恢复。

4.2 性能评价

4.2.1 备份速度

在单位时间内，完成备份的数据总量，单位 MB/S，该值越大越好。

4.2.2 恢复速度

在单位时间内，完成恢复的备份数据总量，单位 MB/S，该值越大越好。

4.2.3 占用资源

备份或恢复作业相关进程占用主机资源的比例。包括 CPU、系统内存的占用率等。

4.2.4 最大驱动器数

单个存储节点能够管理的最大磁带驱动器数量。

4.2.5 最大磁带槽位

单个存储节点能够管理的最大磁带槽位数量。

4.2.6 最大磁带数

单个存储节点能够管理的最大磁带数量。

4.3 安全要求

4.3.1 安全审计

4.3.1.1 日志审计

应能对各类日志进行审计。

4.3.1.2 审计内容

审计记录中至少包括事件的日期和时间、类型、主体身份、结果（如成功或失败）。

4.3.1.3 日志授权访问

只有授权用户才能访问相应的系统日志。

4.3.1.4 日志格式

日志格式应该标准化，含义便于理解。

4.3.2 用户数据保护

4.3.2.1 数据完整性监视

应能对数据在备份和恢复过程中是否出现完整性错误进行监控。

4.3.2.2 安全传输

备份或恢复数据以安全的格式传输。

4.3.2.3 安全存储

备份数据以安全的格式存储于备份介质上。

4.3.3 标识和鉴别

4.3.3.1 鉴别失败处理

当用户的失败登录次数超过允许的尝试鉴别次数时，应阻止该用户的进一步登录尝试，直至授权管理员恢复对该用户的鉴别能力。

4.3.3.2 安全相关操作访问控制

应能对系统安全相关操作设置访问控制策略。

4.3.4 功能保护

4.3.4.1 失效保护

应提供备份任务失效保护机制。

4.3.4.2 手工恢复

系统关键功能失败应可以人工恢复。

4.3.4.3 系统监控

监控备份系统的运行状态，并以适当方式反馈给管理员，例如电子邮件、手机短信等方式。

4.4 保证要求

数据备份与恢复技术产品的安全保证要求按照《信息技术 安全技术 信息技术安全性评估准则—第三部分：安全保证要求》(GB/T18336.3-2001)中规定的相关等级执行。具体要求参考表 5.1 数据备份与恢复产品等级划分。

5 数据备份与恢复产品技术要求的等级划分

依据数据备份与恢复技术产品的开发、生产现状及实际应用情况，我们将数据备份与恢复技术产品划分成两个等级。

数据备份与恢复产品等级划分如表 5.1 所示：

表 5.1 数据备份与恢复产品等级划分表

		基本要求	增强要求	
4.1 功能要求	4.1.1 备份对象	4.1.1	4.1.1	
	4.1.2 运行平台	4.1.2	4.1.2	
	4.1.3 备份模式	4.1.3.1 基于本机备份	4.1.3.1	4.1.3.1
		4.1.3.2 基于网络备份	4.1.3.2	4.1.3.2
		4.1.3.3 LAN-free 备份		4.1.3.3
		4.1.3.4 NDMP 备份		4.1.3.4
	4.1.4 存储介质	4.1.4	4.1.4	
	4.1.5 系统管理功能	4.1.5.1 策略定制	4.1.5.1	4.1.5.1
		4.1.5.2 策略管理	4.1.5.2	4.1.5.2
		4.1.5.3 磁带管理		4.1.5.3
		4.1.5.4 提供报表	4.1.5.4	4.1.5.4
		4.1.5.5 管理界面	4.1.5.5	4.1.5.5
	4.1.6 中文化支持	4.1.6	4.1.6	
	4.1.7 增强功能	4.1.7.1 备份方式支持	4.1.7.1	4.1.7.1
		4.1.7.2 快照支持		4.1.7.2
		4.1.7.3 恢复重定向	4.1.7.3	4.1.7.3
		4.1.7.4 恢复时间点选择	4.1.7.4	4.1.7.4
4.1.7.5 恢复内容选择		4.1.7.5	4.1.7.5	

		4.1.7.6 支持磁盘缓存		4.1.7.6
		4.1.7.7 压缩传输		4.1.7.7
		4.1.7.8 压缩存储		4.1.7.8
		4.1.7.9 恢复自动化		4.1.7.9
		4.1.7.10 恢复缺失文件		4.1.7.10
4.3 安全要求	4.3.1 安全审计	4.3.1.1 日志审计	4.3.1.1	4.3.1.1
		4.3.1.2 审计内容	4.3.1.2	4.3.1.2
		4.3.1.3 日志授权访问	4.3.1.3	4.3.1.3
		4.3.1.4 日志格式		4.3.1.4
	4.3.2 用户数据保护			4.3.2
	4.3.3 标识和鉴别		4.3.3	4.3.3
	4.3.4 功能保护			4.3.4
4.4 保证要求			EAL1	EAL2

6 测试要求

6.1 概述

6.1.1 测试环境

下图是典型的数据备份与恢复技术产品测试环境，两个局域网、一个 SAN 网络和广域网，各网络的具体配置如下：

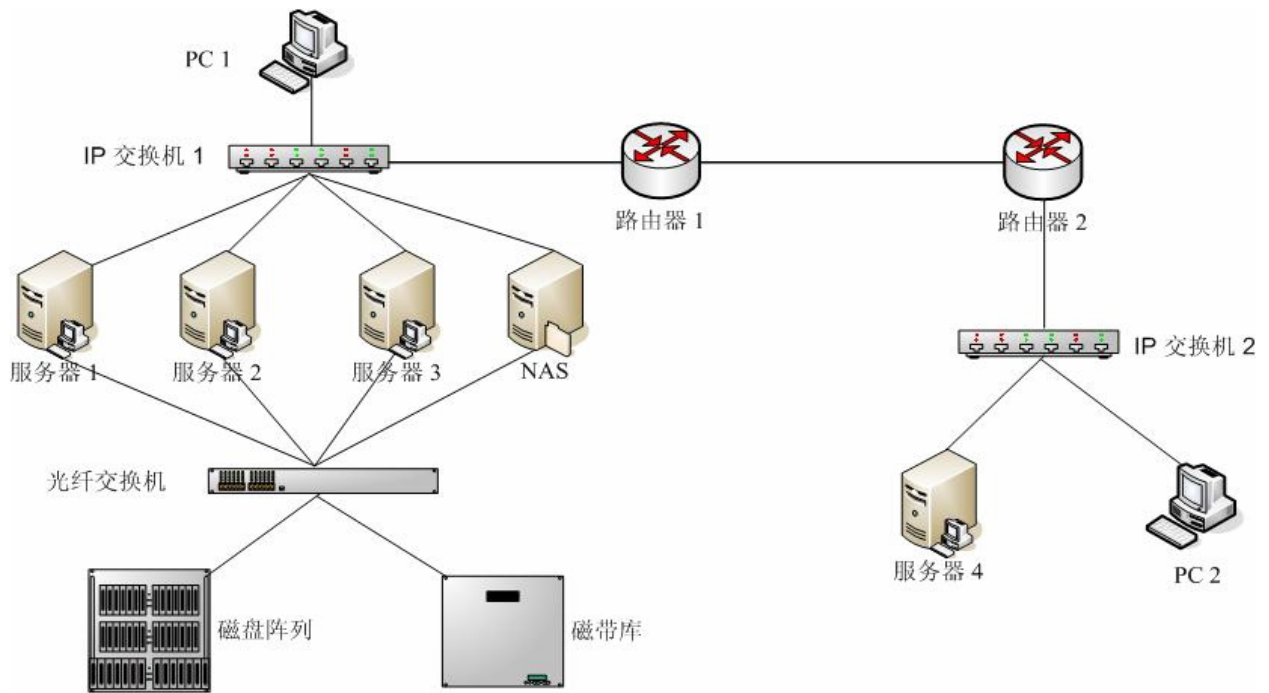


图1 数据备份与恢复产品测试环境

6.1.2 标准测试步骤

下文中所提到的“标准测试步骤”，包括如下内容：

- a) 配置具体项目使测试能够正常执行的各类环境和备份策略；
- b) 执行备份操作，并确认备份成功；
- c) 移除备份对象；
- d) 将备份数据进行恢复；
- e) 验证恢复后的数据是否与备份对象一致、可用。

6.2 功能测试

6.2.1 备份对象

6.2.1.1 数据库

- a) 配置数据库的数据和结构为备份对象，进行数据库备份；
- b) 将数据库恢复至非原主机之外的相同主机环境中；
- c) 将原数据库和恢复后的数据库进行对比。

6.2.1.2 数据卷

- a) 配置待测数据卷所在主机为备份客户端；
- b) 配置备份对象为待测数据卷；

c) 执行标准测试步骤。

6.2.1.3 文件

a) 配置待测文件系统所在主机为备份客户端；

b) 配置备份对象为备份客户端文件系统中的文件；

c) 执行标准测试步骤。

6.2.1.4 操作系统

a) 配置待测操作系统所在主机为备份客户端；

b) 备份对象为操作系统的数据和状态；

c) 执行标准测试步骤；

d) 验证恢复后的操作系统能否正常运行。

6.2.2 运行平台

6.2.2.1 备份服务器运行平台

a) 在待测平台上配置服务器端程序；

b) 配置能够完成服务器端程序所有功能测试的环境；

c) 对服务器端程序的所有功能进行测试，验证每个功能能否实现。

6.2.2.2 备份客户端运行平台

a) 在待测平台上配置备份客户端服务器程序；

b) 配置能够完成客户端程序所有功能测试的测试环境；

c) 对客户端程序的所有功能进行测试，验证每个功能能否实现。

6.2.2.3 存储节点运行平台

a) 在待测平台上配置存储节点程序；

b) 配置能够测试存储节点程序所有功能的测试环境；

c) 对存储节点程序所有功能进行测试，验证每个功能是否能实现。

6.2.3 备份模式

6.2.3.1 基于本机备份

a) 在同一台服务器上配置备份服务器端、备份客户端和存储节点；

b) 配置备份对象为备份服务器本机的数据；

c) 执行标准测试步骤。

6.2.3.2 基于网络备份

- a) 在网络环境中分别配置备份服务器和备份客户端；
- b) 执行标准测试步骤。

6.2.3.3 LAN-free 备份

- a) 配置适用 LAN-free 备份测试的 LAN 和存储区域网络环境；
- b) 使用第三方软件监测备份数据流是否通过 LAN 传输；
- c) 执行标准测试步骤。

6.2.3.4 NDMP 备份

- a) 配置 NDMP 服务器作为备份客户端；
- b) 配置备份对象为 NDMP 服务器中的数据；
- c) 执行标准测试步骤。

6.2.4 存储介质

6.2.4.1 支持备份介质格式

- a) 配置支持待测磁带格式的磁带驱动器；
- b) 配置备份介质为待测格式的磁带；
- c) 执行标准测试步骤。

6.2.4.2 磁盘支持

- a) 配置磁盘作为备份介质；
- b) 执行标准测试步骤。

6.2.5 系统管理功能

6.2.5.1 策略定制

- a) 执行系统的各项策略定制功能；
- b) 验证备份系统能否进行策略定制。

6.2.5.2 策略管理

- a) 执行各项待测策略管理功能；
- b) 验证备份系统策略管理功能是否可用。

6.2.5.3 磁带管理

- a) 配置备份服务器与磁带驱动器以使磁带管理功能测试正常进行；
- b) 测试磁带的管理功能，如磁带自动标签、标记出错磁带、磁带出入库、磁带自动回收、磁带重用、磁头清洗、磁带离线管理等，验证这些功能是否能够实现。

6.2.5.4 提供报表

验证系统是否能提供一种或多种灵活，直观，全面的报表。

6.2.5.5 管理界面

- a) 选取一个或多个待测管理界面对系统进行管理；
- b) 验证系统是否支持此一个或多个管理界面形式。

6.2.6 中文化支持

验证备份系统是否提供中文化的管理界面和提示信息。

6.2.7 增强功能

6.2.7.1 备份方式支持

- a) 配置待测的备份方式；
- b) 执行标准测试步骤；
- c) 验证备份作业是否按既定的备份方式执行。

6.2.7.2 快照支持

- a) 启用快照的相关功能选项；
- b) 确保备份作业进行的同时，备份对象数据有变化；
- c) 执行标准测试步骤；
- d) 验证恢复后的数据是否与开始备份时的备份对象一致。

6.2.7.3 恢复重定向

- a) 配置备份数据恢复至不同于恢复对象所在的主机或目录；
- b) 执行标准测试步骤。

6.2.7.4 恢复时间点选择

- a) 进行数据恢复时，选择创建备份的某个时间点进行恢复；
- b) 执行标准测试步骤；
- c) 验证恢复后的数据与被选时间点的备份对象是否一致。

6.2.7.5 恢复内容选择

- a) 选定备份数据的部分或全部作为恢复对象；
- b) 执行标准测试步骤。

6.2.7.6 支持磁盘缓存

- a) 配置作为缓存的磁盘，并启用该磁盘作为缓存；

- b) 执行标准测试步骤；
- c) 使用第三方软件验证备份数据流是否先写入作为缓存的磁盘再写入备份介质。

6.2.7.7 压缩传输

- a) 选取可行的备份对象测试样本；
- b) 启用压缩传输功能；
- c) 执行标准测试步骤；
- d) 使用第三方软件验证传输的备份数据是否采用了压缩格式进行压缩。

6.2.7.8 压缩存储

- a) 选取可行的备份对象测试样本；
- b) 启动压缩存储功能；
- c) 执行标准测试步骤；
- d) 使用第三方软件验证存储后的备份数据是否采用了压缩格式进行压缩。

6.2.7.9 恢复自动化

- a) 启用恢复自动化相关功能选项；
- b) 按照恢复自动化的要求选择备份对象；
- c) 执行标准测试步骤。

6.2.7.10 恢复缺失文件

- a) 在备份对象完成备份后，删除部分或全部备份对象；
- b) 查看被删除的备份对象是否被有效标示；
- c) 选择被删除的备份对象进行恢复。

6.3 性能测试

6.3.1 备份速度

- a) 根据测试要求选取测试样例，如需要多少文件数量，每个文件数量大小或者数据类型等；
- b) 将测试样例进行备份；
- c) 使用第三方计时设备记录备份测试样例所用的时间。

6.3.2 恢复速度

- a) 根据测试要求选取测试样例，如需要多少文件数量，每个文件数量大小或者数据类型等；
- b) 将测试样例进行备份；
- c) 将测试样例进行恢复；

d) 使用第三方计时设备记录恢复测试样例所用的时间。

6.3.3 占用资源

a) 正常执行数据备份和恢复作业；

b) 使用第三方软件监测备份服务器和客户端服务器在备份和恢复作业执行过程中，备份作业占用系统资源的比例。

6.3.4 最大驱动器数

a) 配置待测磁带库驱动器；

b) 配置必要的备份系统环境以保证最大驱动器数测试能正常进行；

c) 验证备份服务器能管理的最大磁带驱动器数量。

6.3.5 最大磁带槽位

a) 配置待测磁带槽位；

b) 配置必要的备份系统环境以保证最多磁带槽位数测试能正常进行；

c) 验证备份服务器能管理的最大的磁带槽位数量。

6.3.6 最大磁带数

a) 配置待测磁带；

b) 配置必要的备份系统环境以保证最多磁带数测试能正常进行；

c) 验证备份服务器能管理的最大的磁带数量。

6.4 安全测试

6.4.1 安全审计

6.4.1.1 日志审计

a) 使用授权用户登录备份系统；

b) 对各类日志进行审计。

6.4.1.2 审计内容

验证审计记录中是否包括事件的日期和时间，类型，主体身份，结果。

6.4.1.3 日志授权访问

a) 使用授权用户登陆备份系统；

b) 访问相应的系统日志。

6.4.1.4 日志格式

验证系统相应的日志格式是否标准化，含义是否便于理解。

6.4.2 用户数据保护

6.4.2.1 数据完整性监视

- a) 配置备份系统数据完整性监视功能；
- b) 人为破坏数据的完整性；
- c) 验证系统能否对备份数据出现完整性错误进行监控，并给出一定的提示。

6.4.2.2 安全传输

- a) 配置备份系统为网络备份方式；
- b) 启用安全传输功能；
- c) 执行备份作业；
- d) 使用第三方软件验证数据在传输时是否安全。

6.4.2.3 安全存储

- a) 启用安全存储功能，
- b) 执行备份作业；
- c) 使用第三方软件验证数据存储时是否安全。

6.4.3 标识和鉴别

6.4.3.1 鉴别失败处理

- a) 使用同一用户连续多次错误登录系统；
- b) 验证系统是否能检测此类多次登录错误并报警；
- c) 验证系统在规定尝试鉴别次数后是否能阻止该用户的进一步登录尝试，直至授权管理员恢复对该用户的鉴别能力。

6.4.3.2 安全相关操作访问控制

- a) 针对系统安全相关的操作设置访问控制策略；
- b) 验证已设置的访问控制策略在进行系统安全相关操作的时候是否可用。

6.4.4 功能保护

6.4.4.1 失效保护

- a) 人为造成系统关键功能失效；
- b) 验证系统是否提供系统关键功能的失效保护机制。

6.4.4.2 手工恢复

- a) 人为造成系统处于非正常状态；

- b) 使用手工恢复，使系统返回正常状态；
- c) 验证手工恢复是否成功。

6.4.4.3 系统监控

验证备份系统能否提供对备份系统的监控。