ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29765—2013

信息安全技术 数据备份与恢复产品技术要求与测试评价方法

Information security technology—Technical requirements and testing and evaluating method for data backup and recovery products

2013-09-18 发布　　2014-05-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全认证中心、北京信息安全测评中心、清华威视数据安全研究所。

本标准主要起草人:刘海峰、布宁、侯海波、陈晓桦、刘宏、张格、谢文华、李颖涛、段静辉、林森、吴迪。

信息安全技术
数据备份与恢复产品技术要求
与测试评价方法

1 范围

本标准规定了数据备份与恢复产品的技术要求与测试评价方法。

本标准适用于对数据备份与恢复产品的研制、生产、测试、评价。

本标准所指的数据备份与恢复产品是指实现和管理信息系统数据备份和恢复过程的产品，不包括数据复制产品和持续数据保护产品。

2 规范性引用文件

下列文件对于本文件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文件。凡是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 5271.8—2001 信息技术 词汇 第8部分：安全

GB/T 18336.1—2008 信息技术 安全技术 信息技术安全性评估准则 第1部分：简介和一般模型

3 术语和定义

GB/T 5271.8—2001 和 GB/T 18336.1—2008 界定的以及下列术语和定义适用于本文件。

3.1

备份数据 backup data

存储在(通常可移动的)非易失性存储介质上某一时间点的数据集合，用于原数据丢失或不可访问时的数据恢复。

3.2

备份 backup

创建备份数据的过程。

3.3

数据恢复 data recovery

利用备份数据将目标数据还原为某一备份时间点的内容或状态的过程。

3.4

快照 snapshot

指定数据集合的一个完整可用的拷贝，其中包含数据在拷贝启动时间点的映像。

3.5

备份对象 backup object

需要进行备份的数据集合。

3.6

备份介质　backup media

存放备份数据的非易失性储存物理载体。

3.7

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组成的系统。

3.8

备份服务器　backup server

数据备份与恢复产品中提供系统管理和控制服务的部分。

3.9

备份客户端　backup client

数据备份与恢复产品中具体对备份对象进行访问和处理的部分，一般部署在包含备份对象的计算机系统上。

3.10

备份存储节点　backup storage node

数据备份与恢复产品中提供访问和控制备份介质服务的部分。

3.11

完全备份　full backup

备份所有指定的数据对象的过程，不论这些数据自上次备份后是否被更改。完全备份是增量备份的基础。

3.12

增量备份　incremental backup

仅备份自上次备份后更改过的数据对象。

注：包括累积增量备份和差分增量备份。

3.13

累积增量备份　cumulative incremental backup

备份自上次完全备份后更改过的所有数据对象。使用累积增量备份恢复数据时，只需要上次完全备份和自上次完全备份后的累积增量备份。

3.14

差分增量备份　differential incremental backup

备份自上次完全备份或增量备份后更改过的数据对象。使用差分增量备份恢复数据时，需要最新的完全备份和自最新完全备份后的所有差分增量备份。

3.15

存储区域网备份　LAN-free backup

通过存储区域网而不使用局域网(LAN)资源来传输数据的备份方法。

3.16

网络数据管理协议　network data management protocol

一种基于网络的协议和机制，用于控制备份、恢复以及在主要和次要存储器之间的数据传输。

4　数据备份与恢复产品等级划分

根据安全功能要求的不同，将数据备份与恢复产品分为两个等级：基本级和增强级。产品等级划分如表1所示。

第 5 章、第 6 章两章对每一等级的具体要求分别进行描述。其中**“加粗宋体字”**表示所描述的要求仅适用于增强级产品。

在产品等级划分中对产品性能不作要求。产品的性能相关指标和测试方法参见附录 A。

表 1　数据备份与恢复产品等级划分表

技术要求			基本级	增强级
功能要求	备份对象支持		*	*
	运行平台支持	备份服务器运行平台支持	*	*
		备份客户端运行平台支持	*	*
		备份存储节点运行平台支持	*	*
	备份模式支持	基于网络备份	*	*
		基于存储区域网备份		*
		基于网络数据管理协议备份		*
	备份介质支持	离线备份介质支持	*	*
		在线备份介质支持	*	*
	系统管理功能	策略定制	*	*
		策略管理	*	*
		磁带管理		*
		提供报表	*	*
	中文化支持		*	* *
	附加功能	备份方式支持	*	*
		快照支持		*
		恢复重定向	*	*
		恢复时间点选择	*	*
		恢复内容选择	*	*
		磁盘缓存支持		*
		压缩传输		*
		恢复自动化		*
		恢复缺失文件		*
安全功能要求	安全审计	审计事件类型	*	*
		审计记录内容	*	*
		审计记录保护	*	*
	用户数据保护	数据完整性检验	*	*
		传输数据的安全性	*	*
		存储数据的安全性	*	* *
	身份鉴别和访问控制	身份鉴别	*	*
		鉴别失败处理	*	* *

表 1（续）

技术要求			基本级	增强级
安全功能要求	身份鉴别和访问控制	访问控制策略	*	*
		超时锁定	*	*
		会话锁定	*	* *
		访问历史	*	*
	功能保护	功能监控		*
		功能恢复		*
安全保证要求	配置管理			*
	交付与运行		*	*
	开发			*
	指导性文档		*	*
	生命周期支持			*
	测试		*	* *
	脆弱性评定			*
注：在表中，“*”和“* *”表示产品应具备该项技术要求。“*”表示两个级别产品对于该项技术要求相同，“* *”表示增强级产品相对于基本级产品在这项技术要求上进行了增强。				

5 技术要求

5.1 基本级产品要求

5.1.1 功能要求

5.1.1.1 备份对象支持

数据备份与恢复产品应能对数据库、数据卷、文件、操作系统等的数据、结构和状态进行备份和恢复。

5.1.1.2 运行平台支持

5.1.1.2.1 备份服务器运行平台支持

在既定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。

5.1.1.2.2 备份客户端运行平台支持

在既定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。

5.1.1.2.3 备份存储节点运行平台支持

在既定的操作系统平台下备份存储节点程序的所有功能应能正常运行。

5.1.1.3 备份模式支持

5.1.1.3.1 基于网络备份

数据备份与恢复产品应能通过网络备份和恢复客户端主机上的数据。

5.1.1.4 备份介质支持

5.1.1.4.1 离线备份介质支持

应能支持常见格式的磁带等存储介质作为备份数据的离线备份介质。

5.1.1.4.2 在线备份介质支持

应支持磁盘等作为备份数据的在线备份介质。

5.1.1.5 系统管理功能

5.1.1.5.1 策略定制

应至少能对备份对象、备份介质、备份时间、备份数据保存时间和备份方式等制定备份策略。

5.1.1.5.2 策略管理

应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。

5.1.1.5.3 提供报表

应能提供作业状态和设备状态的报表,并支持多种报表格式。

5.1.1.6 中文化支持

应提供中文化的管理界面和提示信息。

5.1.1.7 附加功能

5.1.1.7.1 备份方式支持

应支持完全备份、累积增量备份和差分增量备份等备份方式。

5.1.1.7.2 恢复重定向

应具备将备份数据恢复到与备份对象不同的主机或目录中的功能。

5.1.1.7.3 恢复时间点选择

应能选择不同备份时间点的备份数据进行恢复。

5.1.1.7.4 恢复内容选择

应能选择全部或部分备份数据进行恢复。

5.1.2 安全功能要求

5.1.2.1 安全审计

5.1.2.1.1 审计事件类型

应能对备份系统的身份鉴别、策略管理、备份作业、恢复作业等事件,以及管理员和用户的各类操作

进行审计。

5.1.2.1.2 审计记录内容

审计记录中应至少包括事件的日期和时间、事件类型、主体身份、事件内容、事件的结果(如成功或失败)等内容,且易于阅读。

5.1.2.1.3 审计记录保护

应保证只有授权管理员才能访问相应的审计记录,并对审计记录进行查询、导出和删除操作。

5.1.2.2 用户数据保护

5.1.2.2.1 数据完整性检验

应能对数据在备份、恢复过程中的完整性进行检验。

5.1.2.2.2 传输数据的安全性

应能在备份和恢复过程中利用编码、协议等方式增加数据传输安全性。

5.1.2.2.3 存储数据的安全性

应能以编码等非明文的方式将备份数据存储于备份介质上。

5.1.2.3 身份鉴别和访问控制

5.1.2.3.1 身份鉴别

在管理员或用户进入备份系统之前,产品应鉴别身份。鉴别时应采用口令、证书、生物特征等机制,并在每次进入系统时进行。口令输入应不可回显,并在存储和传输时加密保护。

5.1.2.3.2 鉴别失败处理

当失败登录次数超过三次时,应能阻止该管理员或用户的进一步鉴别尝试。

5.1.2.3.3 访问控制策略

应能对备份系统中与安全相关的所有操作设置访问控制策略,例如,备份作业、日志访问、策略管理等。

5.1.2.3.4 超时锁定

应具有登录超时锁定功能,即,登录后如在设定的时间段内没有任何操作,系统自动终止会话,需要再次进行身份鉴别才能够重新操作。最大超时时间应由授权管理员设定。

5.1.2.3.5 会话锁定

应提供锁定其本身交互会话的功能,锁定后需要再次进行身份鉴别才能够重新管理备份系统。

5.1.2.3.6 访问历史

应具有显示访问历史记录的功能,为登录用户提供登录活动的有关信息,使登录用户识别入侵的企图。用户登录成功后,应显示如下数据:

——上次成功登录系统的日期、时间、来源等情况;

——上次成功登录备份系统以来身份鉴别失败的情况；
——口令距失效日期的天数。

5.1.3 安全保证要求

5.1.3.1 交付与运行

5.1.3.1.1 交付

a) 开发者应使用交付程序给用户交付产品或其部分。
b) 开发者应采用文档的形式描述交付程序，该文档应描述在向用户方分发产品的各个版本时，用以维护其安全性所必需的所有程序。

5.1.3.1.2 安装、生成和启动

开发者应提供文档描述产品安全地安装、生成和启动必需的所有步骤。

5.1.3.2 指导性文档

5.1.3.2.1 管理员指南

a) 开发者应提供针对系统管理员的管理员指南。该指南应说明以下内容：
   1) 管理员可使用的管理功能和接口；
   2) 如何以安全的方式管理产品；
   3) 一些关于安全处理环境中应被控制的功能和特权的警示信息；
   4) 所有关于与产品安全运行有关用户行为的假设；
   5) 所有受管理员控制的安全参数，适当时应指明安全值；
   6) 每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性；
   7) 所有与管理员有关的 IT 环境安全要求。
b) 管理员指南应与供评估的所有其他文档保持一致。

5.1.3.2.2 用户指南

a) 开发者应提供用户指南。该指南应说明以下内容：
   1) 产品的非管理员用户可使用的功能和接口；
   2) 产品所提供的用户可访问安全功能的使用；
   3) 一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
   4) 产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
   5) 所有与用户有关的 IT 环境安全要求。
b) 用户指南应与供评估的所有其他文档保持一致。

5.1.3.3 测试

5.1.3.3.1 测试覆盖

开发者应提供测试覆盖的证据。测试覆盖的证据应说明测试文档中所标识的测试与功能规范中所描述的安全功能之间的对应性。

5.1.3.3.2 功能测试

a) 开发者应测试安全功能，并文档化测试结果。
b) 开发者应提供测试文档，测试文档应包括测试计划、测试程序描述、预期测试结果和实际测试结果。
c) 测试计划应标识要测试的安全功能和描述要执行的测试目标。
d) 测试程序描述应标识要执行的测试，并描述每个安全功能的测试脚本。这些脚本应包括对于其他测试结果的任何顺序依赖性。
e) 预期的测试结果应指出测试成功执行后的预期输出。
f) 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.1.3.3.3 独立测试

a) 开发者应提供用于测试的产品，该产品应适合测试；
b) 开发者应提供一组相当的资源，用于开发者的产品安全功能测试。

5.2 增强级产品要求

5.2.1 功能要求

5.2.1.1 备份对象支持

数据备份与恢复产品应能对数据库、数据卷、文件、操作系统等的数据、结构和状态进行备份和恢复。

5.2.1.2 运行平台支持

5.2.1.2.1 备份服务器运行平台支持

在既定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。

5.2.1.2.2 备份客户端运行平台支持

在既定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。

5.2.1.2.3 备份存储节点运行平台支持

在既定的操作系统平台下备份存储节点程序的所有功能应能正常运行。

5.2.1.3 备份模式支持

5.2.1.3.1 基于网络备份

数据备份与恢复产品应能通过网络备份和恢复客户端主机上的数据。

5.2.1.3.2 基于存储区域网备份

数据备份与恢复产品应能通过存储区域网备份和恢复客户端主机上的数据。

5.2.1.3.3 基于网络数据管理协议备份

数据备份与恢复产品应能通过网络数据管理协议备份和恢复的数据。

5.2.1.4 备份介质支持

5.2.1.4.1 离线备份介质支持

应能支持常见格式的磁带等存储介质作为备份数据的离线备份介质。

5.2.1.4.2 在线备份介质支持

应能支持磁盘等作为备份数据的在线备份介质。

5.2.1.5 系统管理功能

5.2.1.5.1 策略定制

应至少能对备份对象、备份介质、备份时间、备份数据保存时间和备份方式等制定备份策略。

5.2.1.5.2 策略管理

应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。

5.2.1.5.3 磁带管理

应能对在线和离线磁带进行管理，包括以下一项或多项功能：磁带自动标签、出错磁带标记、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。

5.2.1.5.4 提供报表

应能提供作业状态和设备状态的报表，并支持多种报表格式。

5.2.1.6 中文化支持

应提供中文化的管理界面、提示信息和操作手册。

5.2.1.7 附加功能

5.2.1.7.1 备份方式支持

应支持完全备份、累积增量备份和差分增量备份等备份方式。

5.2.1.7.2 快照支持

应支持快照技术，保证备份对象在备份时间点的数据一致性。

5.2.1.7.3 恢复重定向

应具备将备份数据恢复到与备份对象不同的主机或目录中的功能。

5.2.1.7.4 恢复时间点选择

应能选择不同备份时间点的备份数据进行恢复。

5.2.1.7.5 恢复内容选择

应能选择全部或部分备份数据进行恢复。

5.2.1.7.6 磁盘缓存支持

应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。

5.2.1.7.7 压缩传输

应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。

5.2.1.7.8 压缩存储

应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。

5.2.1.7.9 恢复自动化

应支持通过恢复过程自动执行的方式，快速恢复备份数据。

5.2.1.7.10 恢复缺失文件

应标识出已缺失的备份文件，并能够对已缺失的备份文件进行恢复。

5.2.2 安全功能要求

5.2.2.1 安全审计

5.2.2.1.1 审计事件类型

应能对备份系统的身份鉴别、策略管理、备份作业、恢复作业等事件，以及管理员和用户的各类操作进行审计。

5.2.2.1.2 审计记录内容

审计记录中应至少包括事件的日期和时间、事件类型、主体身份、事件内容、事件的结果（如成功或失败）等内容，且易于阅读。

5.2.2.1.3 审计记录保护

应保证只有授权管理员才能访问相应的审计记录，并对审计记录进行查询、导出和删除操作。

5.2.2.2 用户数据保护

5.2.2.2.1 数据完整性检验

应能对数据在备份、恢复过程中的完整性进行检验。

5.2.2.2.2 传输数据的安全性

应能在备份和恢复过程中利用编码、协议等方式增加数据传输安全性。

5.2.2.2.3 存储数据的安全性

应能以编码等非明文的方式将备份数据应存储于备份介质上。只有授权管理员或用户经过身份鉴别后方可访问备份数据。应能对备份数据的被非授权篡改的进行告警提示。

5.2.2.3 身份鉴别和访问控制

5.2.2.3.1 身份鉴别

在管理员或用户进入备份系统之前，产品应鉴别身份。鉴别时应采用口令、证书、生物特征等机制，

并在每次进入系统时进行。口令输入应不可回显，并在存储和传输时加密保护。

5.2.2.3.2 鉴别失败处理

当用户的失败登录次数超过三次时，应能阻止该用户的进一步鉴别尝试，直至授权管理员恢复对该用户的鉴别。

5.2.2.3.3 访问控制策略

应能对备份系统中与安全相关的所有操作设置访问控制策略，例如，备份作业、日志访问、策略管理等。

5.2.2.3.4 超时锁定

应具有登录超时锁定功能，即，登录后如在设定的时间段内没有任何操作，系统自动终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间应由授权管理员设定。

5.2.2.3.5 会话锁定

应为用户提供锁定其本身的交互会话的功能，锁定后需要再次进行身份鉴别才能够重新管理备份系统。同一时间点仅允许同一用户在唯一确定的主机上登录。

5.2.2.3.6 访问历史

应具有显示访问历史记录的功能，为登录用户提供登录活动的有关信息，使登录用户识别入侵的企图。用户登录成功后，应显示如下数据：

——日期、时间、来源和上次成功登录系统的情况；

——上次成功登录备份系统以来身份鉴别失败的情况；

——口令距失效日期的天数。

5.2.2.4 功能保护

5.2.2.4.1 功能监控

应能监控备份产品关键功能的运行状态，并反馈给管理员。

5.2.2.4.2 功能恢复

应提供备份产品关键功能失效时的保护机制，如系统自动恢复、人工干预恢复。

5.2.3 安全保证要求

5.2.3.1 配置管理

5.2.3.1.1 配置管理能力

a) **开发者应为产品提供一个参照号，并在产品上进行标记，该参照号对产品的每一个版本应是唯一的。**

b) **开发者应使用一个配置管理系统。配置管理系统应唯一标识产品所包含的所有配置项，且应提供措施使得只能对配置项进行授权改变。**

c) **开发者应提供配置管理文档。配置管理文档应描述用于唯一标识产品所包含配置项的方法，**

并应提供所有配置项都已经和正在配置管理系统下有效地进行维护的证据。配置管理文档应包括一个配置清单和一个配置管理计划。配置清单应唯一标识组成产品的所有配置项，并应描述组成产品的配置项。配置管理计划应描述配置管理系统是如何使用的，且应提供证实配置管理系统的运行与配置管理计划是一致的证据。

5.2.3.1.2 配置管理范围

开发者应提供一个产品配置项列表。配置项列表应包括：实现表示和安全目标中其他保证组件所要求的评估证据。

5.2.3.2 交付与运行

5.2.3.2.1 交付

a) 开发者应使用交付程序给用户交付产品或其部分。
b) 开发者应采用文档的形式描述交付程序，该文档应描述在向用户方分发产品的各个版本时，用以维护其安全性所必需的所有程序。

5.2.3.2.2 安装、生成和启动

开发者应提供文档描述产品安全地安装、生成和启动必需的所有步骤。

5.2.3.3 开发

5.2.3.3.1 功能规范

开发者应当提供功能规范的设计文档，该文档应满足如下要求：
a) 对产品安全功能及其外部接口进行非形式化描述；
b) 保证其内在一致性；
c) 描述所有外部安全功能接口的用途与使用方法，适当时提供效果、例外情况和出错信息的细节；
d) 完备地表示产品安全功能。

5.2.3.3.2 高层设计

开发者应当提供产品安全功能的高层设计文档，该文档应满足如下要求：
a) 以非形式化方式表述，并且是内在一致的；
b) 按照子系统来描述产品安全功能的结构；
c) 描述每个产品安全功能子系统所提供的安全功能性；
d) 标识产品安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示；
e) 标识产品安全功能子系统的所有接口；
f) 标识产品安全功能子系统的哪些接口是外部可见的；
g) 描述产品安全功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和出错消息的细节；
h) 把产品分成安全策略实施和其他子系统来描述。

5.2.3.3.3 表示对应性

a) **开发者应提供一个所提供产品安全功能表示的所有相邻对之间对应性的分析；**
b) **对于所提供产品安全功能表示的每个相邻对，分析应证实，较为抽象的产品安全功能表示的所有相关安全功能都在较不抽象的安全功能表示中得到正确且完备地细化。**

5.2.3.4 指导性文档

5.2.3.4.1 管理员指南

a) 开发者应提供针对系统管理员的管理员指南。该指南应说明以下内容：
   1) 管理员可使用的管理功能和接口；
   2) 如何以安全的方式管理产品；
   3) 一些关于安全处理环境中应被控制的功能和特权的警示信息；
   4) 所有关于与产品安全运行有关用户行为的假设；
   5) 所有受管理员控制的安全参数，适当时应指明安全值；
   6) 每一种与需要执行的管理功能有关的安全相关事件，包括改变安全功能所控制实体的安全特性；
   7) 所有与管理员有关的 IT 环境安全要求。
b) 管理员指南应与供评估的所有其他文档保持一致。

5.2.3.4.2 用户指南

a) 开发者应提供用户指南。该指南应说明以下内容：
   1) 产品的非管理员用户可使用的功能和接口；
   2) 产品所提供的用户可访问安全功能的使用；
   3) 一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；
   4) 产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；
   5) 所有与用户有关的 IT 环境安全要求。
b) 用户指南应与供评估的所有其他文档保持一致。

5.2.3.5 生命周期支持

5.2.3.5.1 开发安全

开发者应提供开发安全文档，该文档应满足如下要求：

a) **描述在产品的开发环境中，保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施；**
b) **提供在产品的开发和维护过程中执行安全措施的证据。**

5.2.3.6 测试

5.2.3.6.1 测试覆盖

开发者应提供测试覆盖的一**个分析**，该**分析**应满足如下要求：

a) **证实**测试文档中所标识的测试和功能规范中所描述的安全功能之间的对应性；

b) **证实功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是完备的。**

5.2.3.6.2 测试深度

开发者应提供测试深度的分析，深度分析应证实测试文档中所标识的测试足以证实该安全功能是依照其高层设计运行的。

5.2.3.6.3 功能测试

a) 开发者应测试安全功能，并文档化测试结果。
b) 开发者应提供测试文档，测试文档应包括测试计划、测试程序描述、预期测试结果和实际测试结果。
c) 测试计划应标识要测试的安全功能和描述要执行的测试目标。
d) 测试程序描述应标识要执行的测试，并描述每个安全功能的测试脚本。这些脚本应包括对于其他测试结果的任何顺序依赖性。
e) 预期的测试结果应指出测试成功执行后的预期输出。
f) 开发者执行测试所得到的测试结果应证实每个被测试的安全性功能都按照规定运转。

5.2.3.6.4 独立测试

a) 开发者应提供用于测试的产品，该产品应适合测试。
b) 开发者应提供一组相当的资源，用于开发者的产品安全功能测试。

5.2.3.7 脆弱性评定

5.2.3.7.1 脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。该文档满足如下要求：

a) **描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析；**
b) **描述对明显的脆弱性的处置；**
c) **针对所有已标识的脆弱性，说明脆弱性不能在产品的预期使用环境中被利用。**

5.2.3.7.2 误用

开发者应提供指导性文档，该文档应满足如下要求：

a) **标识产品所有可能的运行方式（包括失败和操作失误后的运行），它们的后果以及对于保持安全运行的意义；**
b) **是完备的、清晰的、一致的、合理的；**
c) **列出关于预期使用环境的所有假设；**
d) **列出对外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求。**

6 测试方法

6.1 概述

6.1.1 测试环境

典型的数据备份与恢复产品测试环境由一个局域网和一个存储区域网（SAN）组成，如图 1 所示。

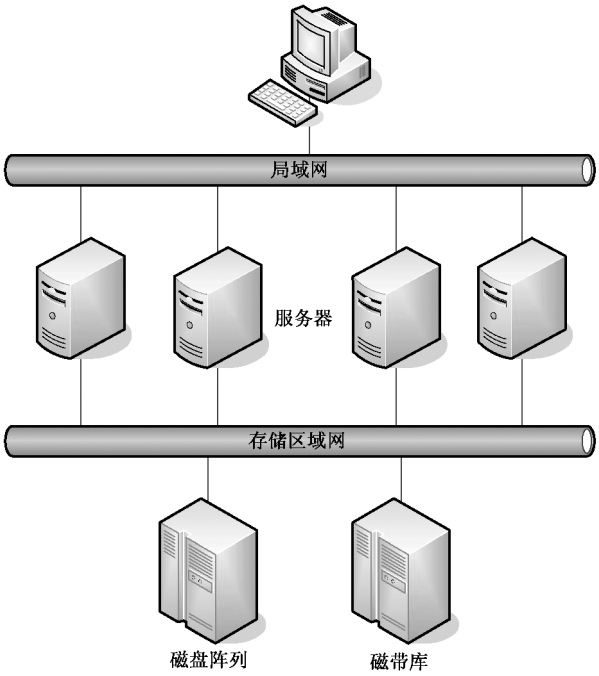

图 1　典型的数据备份与恢复产品测试环境示意图

6.1.2　通用测试步骤

“通用测试步骤”包括如下内容：

a)　配置具体项目以提供使测试能够按照备份策略正常执行的各类环境；

b)　执行备份操作，并确认备份成功；

c)　移除备份对象；

d)　利用备份数据进行恢复；

e)　验证恢复后的数据是否与备份对象一致且可用。

6.2　基本级产品测试

6.2.1　功能测试

6.2.1.1　备份对象支持

6.2.1.1.1　数据库备份

a)　测试方法：

1)　配置待测数据库的数据和结构为备份对象；

2)　执行备份操作；

3)　将数据库恢复至原主机之外的相同主机环境中；

4)　验证恢复后的数据库是否与原数据库一致且可用。

b)　预期结果：

1)　显示数据库备份正常进行；

2)　显示数据库恢复成功；

3)　恢复后的数据库与原数据库一致且可用。

6.2.1.1.2 数据卷备份

a) 测试方法：
   1) 配置待测数据卷所在主机为备份客户端；
   2) 配置待测数据卷为备份对象；
   3) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 数据卷所在主机作为备份客户端配置成功；
   2) 显示备份对象为该主机一个数据卷配置成功；
   3) 恢复后的数据卷与原数据卷一致且可用。

6.2.1.1.3 文件备份

a) 测试方法：
   1) 配置待测文件系统所在主机为备份客户端；
   2) 配置备份客户端文件系统中的文件为备份对象；
   3) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 文件系统所在主机作为备份客户端配置成功；
   2) 显示备份对象为该主机一个或多个文件的配置成功；
   3) 恢复后的文件与原文件一致且可用。

6.2.1.1.4 操作系统备份

a) 测试方法：
   1) 配置待测操作系统所在主机为备份客户端；
   2) 配置操作系统的数据和状态为备份对象；
   3) 执行通用测试步骤(见 6.1.2)；
   4) 验证恢复后的操作系统能否正常运行。
b) 预期结果：
   1) 操作系统所在主机作为备份客户端配置成功；
   2) 显示备份对象为操作系统的数据和状态配置成功；
   3) 恢复后的操作系统正常运行。

6.2.1.2 运行平台支持

6.2.1.2.1 备份服务器运行平台支持

a) 测试方法：
   1) 在既定平台上配置备份服务器程序；
   2) 配置能够完成备份服务器程序所有功能测试的环境；
   3) 对备份服务器程序的所有功能进行测试,验证每个功能能否正常运行。
b) 预期结果：
   1) 既定平台上备份服务器程序的各项待测功能配置成功；
   2) 功能测试所需要的环境配置成功；
   3) 备份服务器程序的所有功能均正常运行。

6.2.1.2.2 备份客户端运行平台支持

a) 测试方法：
   1) 在既定平台上配置备份客户端程序；
   2) 配置能够完成备份客户端程序所有功能测试的测试环境；
   3) 对备份客户端程序的所有功能进行测试，验证每个功能能否正常运行。
b) 预期结果：
   1) 既定平台上备份客户端程序的各项待测功能配置成功；
   2) 功能测试所需要的环境配置成功；
   3) 备份客户端程序的所有功能均正常运行。

6.2.1.2.3 备份存储节点运行平台支持

a) 测试方法：
   1) 在既定平台上配置备份存储节点程序；
   2) 配置能够测试备份存储节点程序所有功能的测试环境；
   3) 对备份存储节点程序的所有功能进行测试，验证每个功能能否正常运行。
b) 预期结果：
   1) 既定平台上备份存储节点程序的各项既定功能配置成功；
   2) 功能测试所需要的环境配置成功；
   3) 备份存储节点程序的所有功能均正常运行。

6.2.1.3 备份模式支持

6.2.1.3.1 基于网络备份

a) 测试方法：
   1) 在网络环境中的不同主机上分别配置备份服务器程序和备份客户端程序；
   2) 配置备份客户端程序所在主机的数据为备份对象；
   3) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 在网络环境中不同主机上的备份服务器程序和备份客户端程序配置成功；
   2) 备份客户端程序所在主机的数据作为备份对象配置成功；
   3) 恢复后的数据与原数据一致且可用。

6.2.1.4 备份介质支持

6.2.1.4.1 离线备份介质支持

a) 测试方法：
   1) 配置支持待测磁带格式的磁带驱动器；
   2) 配置待测格式的磁带为备份介质；
   3) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 磁带驱动器配置成功；
   2) 磁带作为备份介质配置成功；
   3) 恢复后的数据与原数据一致且可用。

6.2.1.4.2 在线备份介质支持

a) 测试方法：
   1) 配置磁盘为备份介质；
   2) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 磁盘作为备份介质配置成功；
   2) 恢复后的数据与原数据一致且可用。

6.2.1.5 系统管理功能

6.2.1.5.1 策略定制

a) 测试方法：
   1) 执行产品的各项待测策略定制功能；
   2) 验证待测策略定制功能是否有效。
b) 预期结果：
   能够有效地进行策略定制。

6.2.1.5.2 策略管理

a) 测试方法：
   1) 执行产品的各项待测策略管理功能；
   2) 验证待测策略管理功能是否有效。
b) 预期结果：
   能够有效地进行策略管理。

6.2.1.5.3 提供报表

a) 测试方法：
   验证产品能否提供一种或多种具有可读性的报表。
b) 预期结果：
   能够提供一种或多种灵活、直观、全面的报表。

6.2.1.6 中文化支持

a) 测试方法：
   验证产品是否提供中文化的管理界面和提示信息。
b) 预期结果：
   能够提供中文化的管理界面和提示信息。

6.2.1.7 附加功能

6.2.1.7.1 备份方式支持

a) 测试方法：
   1) 配置待测的备份方式；
   2) 执行通用测试步骤(见 6.1.2)；
   3) 验证备份作业是否按既定的备份方式执行。

b） 预期结果：

1） 待测备份方式配置成功；

2） 恢复后的数据与原数据一致且可用；

3） 备份作业按照既定的备份方式执行。

6.2.1.7.2 恢复重定向

a） 测试方法：

1） 配置备份数据恢复至不同于其备份对象所在的主机或目录；

2） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：

1） 备份数据恢复至不同于其备份对象所在的主机或目录成功；

2） 恢复后的数据与原数据一致且可用。

6.2.1.7.3 恢复时间点选择

a） 测试方法：

1） 选择创建备份的某个时间点进行数据恢复；

2） 执行通用测试步骤(见 6.1.2)；

3） 验证恢复后的数据与备份对象在所选时间点时的数据是否一致。

b） 预期结果：

1） 数据恢复时间点选择成功；

2） 恢复后的数据与备份对象在所选时间点时的数据一致且可用。

6.2.1.7.4 恢复内容选择

a） 测试方法：

1） 选定备份数据的部分或全部作为恢复对象；

2） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：

1） 恢复对象选择成功；

2） 恢复后的数据与所选恢复对象的原数据一致且可用。

6.2.2 安全功能要求测试

6.2.2.1 安全审计

6.2.2.1.1 审计事件类型

a） 测试方法：

1） 使用授权用户登录备份系统、进行备份作业、恢复作业、策略管理等操作；

2） 查看审计结果。

b） 预期结果：

结果中有上述事件的相应记录。

6.2.2.1.2 审计记录内容

a） 测试方法：

验证审计记录中是否包括事件的日期和时间、事件类型、主体身份、事件内容、事件结果。

b） 预期结果：

审计内容包括了事件的日期和时间、事件类型、主体身份、事件内容、事件结果。

6.2.2.1.3 审计记录保护

a） 测试方法：

1） 使用授权用户和非授权用户分别登录备份系统；

2） 查看产品相应的审计结果。

b） 预期结果：

1） 授权用户能够访问审计记录；

2） 非授权用户查看审计记录被拒绝。

6.2.2.2 用户数据保护

6.2.2.2.1 数据完整性检验

a） 测试方法：

1） 配置备份系统的数据完整性检验功能；

2） 人为破坏备份数据的完整性；

3） 验证产品能否检验出备份数据的完整性已被破坏，并给出相应的警示。

b） 预期结果：

1） 数据完整性检验功能配置成功；

2） 检验出备份数据的完整性已被破坏，并能给出相应的警示。

6.2.2.2.2 传输数据的安全性

a） 测试方法：

1） 配置产品为基于网络备份模式；

2） 启用安全传输功能；

3） 执行备份作业；

4） 使用第三方软件验证数据在传输时是否安全。

b） 预期结果：

1） 基于网络备份模式配置成功；

2） 安全传输功能启用成功；

3） 备份作业正常进行；

4） 数据在传输时有安全措施保障。

6.2.2.2.3 存储数据的安全性

a） 测试方法：

1） 启用安全存储功能；

2） 执行备份作业；

3） 使用第三方软件验证数据存储时是否安全。

b） 预期结果：

1） 安全存储功能启用成功；

2） 备份作业正常进行；

3） 数据在存储时有安全措施保障。

6.2.2.3 身份鉴别和访问控制

6.2.2.3.1 身份鉴别

a) 测试方法：
   1) 验证登录产品之前是否采用口令机制鉴别身份以及该口令是否可见；
   2) 验证管理员口令在存储和传输时是否受加密保护。
b) 预期结果：
   1) 登录产品之前采用口令机制鉴别身份，同时该口令是不可见的；
   2) 口令在存储和传输时受加密保护。

6.2.2.3.2 鉴别失败处理

a) 测试方法：
   1) 使用同一用户连续三次错误登录系统；
   2) 验证产品能否检测三次登录错误并报警；
   3) 验证产品在三次错误登录后能否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。
b) 预期结果：
   1) 拒绝错误登录；
   2) 三次错误登录后报警；
   3) 在三次错误登录后能够阻止用户的进一步登录尝试。

6.2.2.3.3 访问控制策略

a) 测试方法：
   1) 针对产品中与安全相关的操作设置访问控制策略；
   2) 验证已设置的访问控制策略在进行与安全相关的操作时是否可用。
b) 预期结果：
   1) 访问控制策略设置成功；
   2) 在进行与安全相关的操作时已设置的访问控制策略可用。

6.2.2.3.4 超时锁定

a) 测试方法：
   1) 验证产品在管理员设定的时间段内无任何操作时是否自动终止会话，是否需要再次进行身份鉴别才能重新操作；
   2) 验证产品最大超时时间能否由授权管理员设定。
b) 预期结果：
   1) 在设定的时间段内无任何操作时终止会话，需要再次进行身份鉴别才能够重新操作；
   2) 最大超时时间能由授权管理员设定。

6.2.2.3.5 会话锁定

a) 测试方法：
   1) 验证产品是否提供锁定其自身交互会话的功能；
   2) 验证产品锁定后是否需要再次进行身份鉴别才能够重新管理备份系统。

b） 预期结果：

1） 产品提供了锁定其自身交互会话的功能；

2） 锁定后需要再次进行身份鉴别才能够重新管理备份系统。

6.2.2.3.6 访问历史

a） 测试方法：

验证授权用户登录成功后，产品是否显示如下数据：

1） 日期、时间、来源和上次成功登录系统的情况；

2） 上次成功登录备份系统以来身份鉴别失败的情况；

3） 口令距失效日期的天数。

b） 预期结果：

授权用户登录成功后，产品显示如下数据：

1） 日期、时间、来源和上次成功登录系统的情况；

2） 上次成功登录备份系统以来身份鉴别失败的情况；

3） 口令距失效日期的天数。

6.2.3 安全保证要求评估

6.2.3.1 交付与运行

6.2.3.1.1 交付

a） 评估方法：

1） 审查产品的交付文档，查看其是否具有安装文档、产品生成文档、指导用户进行产品运维的文档以及产品培训手册等文档；

2） 审查开发者是否提供了交付程序，该程序是否在文档中得到描述。

b） 预期结果：

交付中的全部要求都能得到满足。

6.2.3.1.2 安装、生成和启动

a） 评估方法：

审查开发者是否提供了文档，描述了产品安全地安装、生成和启动所必要的步骤。

b） 预期结果：

安装、生成和启动中的全部要求都能得到满足。

6.2.3.2 指导性文档

6.2.3.2.1 管理员指南

a） 评估方法：

1） 审查产品的管理员指南，验证其是否：

——描述管理员可使用的管理功能和接口；

——描述如何以安全的方式管理产品；

——包含一些关于安全处理环境中应被控制的功能和特权的警示信息；

——描述所有关于与产品安全运行有关用户行为的假设；

——描述所有受管理员控制的安全参数，合适时指明安全值；

——描述每一种与需要执行的管理功能有关的安全相关事件，包括对改变安全功能所控制的实体的安全特性；

——描述所有与系统管理员有关的 IT 环境安全要求。

2） 审查产品的管理员指南，验证其是否与供评估的所有其他文档保持一致。

b） 预期结果：

管理员指南中的全部要求都能得到满足。

6.2.3.2.2 用户指南

a） 评估方法：

1） 审查产品的用户指南，验证其是否：

——描述非管理员用户可用的功能和接口；

——描述产品所提供的用户可以访问的安全功能的使用；

——包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；

——清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；

——描述所有与用户有关的 IT 环境的安全要求。

2） 审查产品的用户指南，验证其是否与供评估的所有其他文档保持一致。

b） 预期结果：

用户指南中的全部要求都能得到满足。

6.2.3.3 测试

6.2.3.3.1 测试覆盖

a） 评估方法：

审查开发者是否提供了测试覆盖的证据，并验证该证据是否说明了测试文档中所标识的测试和功能规范中所描述的安全功能之间是对应的。

b） 预期结果：

测试覆盖中的全部要求都能得到满足。

6.2.3.3.2 功能测试

a） 评估方法：

1） 审查测试文档是否包括测试计划、测试程序描述、预期测试结果和实际测试结果；

2） 审查测试计划是否标识了要测试的安全功能，描述了要执行的测试目标；

3） 审查测试程序描述是否标识了要执行的测试，并描述了每个安全功能的测试脚本，这些脚本包括对于其他测试结果的任意顺序依赖性；

4） 审查预期的测试结果是否与测试成功执行后的预期输出一致；

5） 审查文档中记录的预期测试结果和实际测试结果，确认每个被测试的安全性功能都按照规定运转。

b） 预期结果：

功能测试中的全部要求都能得到满足。

6.2.3.3.3 独立测试

a） 评估方法：

1） 检查开发者是否提供用于测试的产品，并且产品是否适合测试；
2） 检查开发者是否提供一组相当的资源，用于开发者的产品安全功能测试。

b） 预期结果：
独立测试中的全部要求都能得到满足。

6.3 增强级产品测试

6.3.1 功能测试

6.3.1.1 备份对象支持

6.3.1.1.1 数据库备份

a） 测试方法：
1） 配置待测数据库的数据和结构为备份对象；
2） 执行备份操作；
3） 将数据库恢复至原主机之外的相同主机环境中；
4） 验证恢复后的数据库是否与原数据库一致且可用。

b） 预期结果：
1） 显示数据库备份正常进行；
2） 显示数据库恢复成功；
3） 恢复后的数据库与原数据库一致且可用。

6.3.1.1.2 数据卷备份

a） 测试方法：
1） 配置待测数据卷所在主机为备份客户端；
2） 配置待测数据卷为备份对象；
3） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：
1） 数据卷所在主机作为备份客户端配置成功；
2） 显示备份对象为该主机一个数据卷配置成功；
3） 恢复后的数据卷与原数据卷一致且可用。

6.3.1.1.3 文件备份

a） 测试方法：
1） 配置待测文件系统所在主机为备份客户端；
2） 配置备份客户端文件系统中的文件为备份对象；
3） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：
1） 文件系统所在主机作为备份客户端配置成功；
2） 显示备份对象为该主机一个或多个文件配置成功；
3） 恢复后的文件与原文件一致且可用。

6.3.1.1.4 操作系统备份

a） 测试方法：

1） 配置待测操作系统所在主机为备份客户端；
2） 配置操作系统的数据和状态为备份对象；
3） 执行通用测试步骤(见 6.1.2)；
4） 验证恢复后的操作系统能否正常运行。

b） 预期结果：
1） 操作系统所在主机作为备份客户端配置成功；
2） 显示备份对象为操作系统的数据和状态配置成功；
3） 恢复后的操作系统正常运行。

6.3.1.2 运行平台支持

6.3.1.2.1 备份服务器运行平台支持

a） 测试方法：
1） 在既定平台上配置备份服务器程序；
2） 配置能够完成备份服务器程序所有功能测试的环境；
3） 对备份服务器程序的所有功能进行测试,验证每个功能能否正常运行。

b） 预期结果：
1） 既定平台上备份服务器程序的各项待测功能配置成功；
2） 功能测试所需要的环境配置成功；
3） 备份服务器程序的所有功能均正常运行。

6.3.1.2.2 备份客户端运行平台支持

a） 测试方法：
1） 在既定平台上配置备份客户端程序；
2） 配置能够完成备份客户端程序所有功能测试的测试环境；
3） 对备份客户端程序的所有功能进行测试,验证每个功能能否正常运行。

b） 预期结果：
1） 既定平台上备份客户端程序的各项待测功能配置成功；
2） 功能测试所需要的环境配置成功；
3） 备份客户端程序的所有功能均正常运行。

6.3.1.2.3 备份存储节点运行平台支持

a） 测试方法：
1） 在既定平台上配置备份存储节点程序；
2） 配置能够测试备份存储节点程序所有功能的测试环境；
3） 对备份存储节点程序的所有功能进行测试,验证每个功能能否正常运行。

b） 预期结果：
1） 既定平台上备份存储节点程序的各项既定功能配置成功；
2） 功能测试所需要的环境配置成功；
3） 备份存储节点程序的所有功能均正常运行。

6.3.1.3 备份模式支持

6.3.1.3.1 基于网络备份

a） 测试方法：

1） 在网络环境中的不同主机上分别配置备份服务器程序和备份客户端程序；
2） 配置备份客户端程序所在主机的数据为备份对象；
3） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：
1） 在网络环境中不同主机上的备份服务器程序和备份客户端程序配置成功；
2） 备份客户端程序所在主机的数据作为备份对象配置成功；
3） 恢复后的数据与原数据一致且可用。

6.3.1.3.2 基于存储区域网备份

a） 测试方法：
1） **配置适用存储区域网备份测试的局域网和存储区域网络环境；**
2） **使用第三方软件监测备份数据流是否通过局域网传输；**
3） **执行通用测试步骤(见 6.1.2)。**

b） 预期结果：
1） **备份测试所用的局域网和存储区域网络环境配置成功；**
2） **备份数据流没有通过局域网传输；**
3） **恢复后的数据与原数据一致且可用。**

6.3.1.3.3 基于网络数据管理协议备份

a） 测试方法：
1） **配置支持网络数据管理协议的主机为备份客户端；**
2） **配置该主机中的数据为备份对象；**
3） **执行标准测试步骤。**

b） 预期结果：
1） **支持网络数据管理协议的主机作为备份客户端配置成功；**
2） **该主机中的数据作为备份对象配置成功；**
3） **恢复后的数据与原数据一致且可用。**

6.3.1.4 备份介质支持

6.3.1.4.1 离线备份介质支持

a） 测试方法：
1） 配置支持待测磁带格式的磁带驱动器；
2） 配置待测格式的磁带为备份介质；
3） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：
1） 磁带驱动器配置成功；
2） 磁带作为备份介质配置成功；
3） 恢复后的数据与原数据一致且可用。

6.3.1.4.2 在线备份介质支持

a） 测试方法：
1） 配置磁盘为备份介质；

2） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：

1） 磁盘作为备份介质配置成功；

2） 恢复后的数据与原数据一致且可用。

6.3.1.5 系统管理功能

6.3.1.5.1 策略定制

a） 测试方法：

1） 执行产品的各项待测策略定制功能；

2） 验证待测策略定制功能是否有效。

b） 预期结果：

能够有效地进行策略定制。

6.3.1.5.2 策略管理

a） 测试方法：

1） 执行产品的各项待测策略管理功能；

2） 验证待测策略管理功能是否有效。

b） 预期结果：

能够有效地进行策略管理。

6.3.1.5.3 磁带管理

a） 测试方法：

1） **配置备份服务器和磁带驱动器以提供使磁带管理功能测试能够正常执行的环境；**

2） **测试备份系统的磁带管理功能，例如，磁带自动标签、出错磁带标记、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；**

3） **验证磁带管理功能是否有效**。

b） 预期结果：

1） **备份服务器和磁带驱动器配置成功；**

2） **产品能够有效地进行磁带管理**。

6.3.1.5.4 提供报表

a） 测试方法：

验证产品能否提供一种或多种具有可读性的报表。

b） 预期结果：

能够提供一种或多种灵活、直观、全面的报表。

6.3.1.6 中文化支持

a） 测试方法：

验证产品是否提供中文化的管理界面、提示信息和**操作手册**。

b） 预期结果：

能够提供中文化的管理界面、提示信息和**操作手册**。

6.3.1.7 附加功能

6.3.1.7.1 备份方式支持

a) 测试方法：
   1) 配置支持待测备份方式的测试环境；
   2) 执行通用测试步骤(见 6.1.2)；
   3) 验证备份作业是否按既定的备份方式执行。
b) 预期结果：
   1) 待测备份方式配置成功；
   2) 恢复后的数据与原数据一致且可用；
   3) 备份作业按照既定的备份方式执行。

6.3.1.7.2 快照支持

a) 测试方法：
   1) **启用快照的相关功能选项**；
   2) **确保备份作业进行的同时，备份对象的数据有变化**；
   3) **执行通用测试步骤(见 6.1.2)**。
   4) **验证恢复后的数据与备份对象在备份启动时间点时的数据是否一致且可用**。
b) 预期结果：
   1) **快照功能启用成功**；
   2) **备份作业过程中，备份对象的数据有变化**；
   3) **恢复后的数据与备份对象在备份启动时间点时的数据一致且可用**。

6.3.1.7.3 恢复重定向

a) 测试方法：
   1) 配置备份数据恢复至不同于其备份对象所在的主机或目录；
   2) 执行通用测试步骤(见 6.1.2)。
b) 预期结果：
   1) 备份数据恢复至不同于其备份对象所在的主机或目录成功；
   2) 恢复后的数据与原数据一致且可用。

6.3.1.7.4 恢复时间点选择

a) 测试方法：
   1) 选择创建备份的某个时间点进行数据恢复；
   2) 执行通用测试步骤(见 6.1.2)；
   3) 验证恢复后的数据与备份对象在所选时间点时的数据是否一致。
b) 预期结果：
   1) 数据恢复时间点选择成功；
   2) 恢复后的数据与备份对象在所选时间点时的数据一致且可用。

6.3.1.7.5 恢复内容选择

a) 测试方法：

1） 选定备份数据的部分或全部作为恢复对象；
2） 执行通用测试步骤(见 6.1.2)。

b） 预期结果：
1） 恢复对象选择成功；
2） 恢复后的数据与所选恢复对象的原数据一致且可用。

6.3.1.7.6 磁盘缓存支持

a） 测试方法：
1） **配置作为缓存的磁盘，并启用磁盘缓存功能；**
2） **执行通用测试步骤(见 6.1.2)；**
3） **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。**

b） 预期结果：
1） **磁盘作为缓存配置成功；**
2） **恢复后的数据与原数据一致且可用；**
3） **备份数据流先写入作为缓存的磁盘，再写入备份介质。**

6.3.1.7.7 压缩传输

a） 测试方法：
1） **选取可行的备份对象测试样本；**
2） **启用压缩传输功能；**
3） **执行通用测试步骤(见 6.1.2)；**
4） **使用第三方软件验证传输的备份数据是否经过了压缩。**

b） 预期结果：
1） **压缩传输功能启用成功；**
2） **恢复后的数据与原数据一致且可用；**
3） **传输的备份数据经过了压缩。**

6.3.1.7.8 压缩存储

a） 测试方法：
1） **选取可行的备份对象测试样本；**
2） **启动压缩存储功能；**
3） **执行通用测试步骤(见 6.1.2)；**
4） **使用第三方软件验证存储后的备份数据是否经过了压缩。**

b） 预期结果：
1） **压缩存储功能启用成功；**
2） **恢复后的数据与原数据一致且可用；**
3） **存储的备份数据经过了压缩。**

6.3.1.7.9 恢复自动化

a） 测试方法：
1） **启用恢复自动化的相关功能选项；**
2） **按照恢复自动化的要求选择备份对象；**
3） **执行通用测试步骤(见 6.1.2)。**

b） 预期结果：

1） **恢复自动化的相关功能启用成功；**

2） **恢复后的数据与原数据一致且可用。**

6.3.1.7.10 恢复缺失文件

a） 测试方法：

1） **在对备份对象的数据完成备份后，删除备份对象的部分或全部文件；**

2） **查看被删除的文件是否被有效标示；**

3） **选择被删除的文件进行恢复。**

b） 预期结果：

1） **备份对象的部分或全部文件删除成功；**

2） **被删除的文件被有效标示；**

3） **恢复后的文件与原文件一致且可用。**

6.3.2 安全功能要求测试

6.3.2.1 安全审计

6.3.2.1.1 审计事件类型

a） 测试方法：

1） 使用授权用户登录备份系统、进行备份作业、恢复作业、策略管理等操作；

2） 查看审计结果。

b） 预期结果：

结果中有上述事件的相应记录。

6.3.2.1.2 审计记录内容

a） 测试方法：

验证审计记录中是否包括事件的日期和时间、事件类型、主体身份、事件内容、事件结果。

b） 预期结果：

审计内容至少包括了事件的日期和时间、事件类型、主体身份、事件内容、事件结果。

6.3.2.1.3 审计记录保护

a） 测试方法：

1） 使用授权用户和非授权用户分别登录备份系统；

2） 查看产品相应的审计结果。

b） 预期结果：

1） 授权用户能够访问审计记录；

2） 非授权用户查看审计记录被拒绝。

6.3.2.2 用户数据保护

6.3.2.2.1 数据完整性检验

a） 测试方法：

1） 配置备份系统的数据完整性检验功能；

2） 人为破坏备份数据的完整性；

3） 验证产品能否检验出备份数据的完整性已被破坏，并给出相应的警示。

b） 预期结果：

1） 数据完整性检验功能配置成功；

2） 检验出备份数据的完整性已被破坏，并能给出相应的警示。

6.3.2.2.2 传输数据的安全性

a） 测试方法：

1） 配置产品为基于网络备份模式；

2） 启用安全传输功能；

3） 执行备份作业；

4） 使用第三方软件验证数据在传输时是否安全。

b） 预期结果：

1） 基于网络备份模式配置成功；

2） 安全传输功能启用成功；

3） 备份作业正常进行；

4） 数据在传输时有安全措施保障。

6.3.2.2.3 存储数据的安全性

a） 测试方法：

1） **启用安全存储功能；**

2） **执行备份作业；**

3） **使用第三方软件验证数据存储时是否安全；**

4） **使用非授权管理员或用户访问备份数据；**

5） **非法篡改备份数据，并利用被非法篡改的备份数据进行恢复，验证产品能够对备份数据被篡改进行警告或提示。**

b） 预期结果：

1） **安全存储功能启用成功；**

2） **备份作业正常进行；**

3） **数据在存储时有安全措施保障；**

4） **非授权管理员或用户无法访问备份数据；**

5） **验证产品能够对备份数据被篡改进行警告或提示。**

6.3.2.3 身份鉴别和访问控制

6.3.2.3.1 身份鉴别

a） 测试方法：

1） 验证管理员登录产品之前是否采用口令机制鉴别管理员身份以及该口令是否可见；

2） 验证管理员口令在存储和传输时是否受加密保护。

b） 预期结果：

1） 管理员登录产品之前采用口令机制鉴别管理员身份，同时该口令是不可见的；

2） 管理员口令在存储和传输时受加密保护。

6.3.2.3.2 鉴别失败处理

a) 测试方法：
   1) 使用同一用户连续三次错误登录系统；
   2) 验证产品能否检测三次登录错误并报警；
   3) 验证产品在三次错误登录后能否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。
b) 预期结果：
   1) 拒绝错误登录；
   2) 三次错误登录后报警；
   3) 在三次错误登录后能够阻止用户的进一步登录尝试。

6.3.2.3.3 访问控制策略

a) 测试方法：
   1) 针对产品中与安全相关的操作设置访问控制策略；
   2) 验证已设置的访问控制策略在进行与安全相关的操作时是否可用。
b) 预期结果：
   1) 访问控制策略设置成功；
   2) 在进行与安全相关的操作时已设置的访问控制策略可用。

6.3.2.3.4 超时锁定

a) 测试方法：
   1) 验证产品在管理员设定的时间段内无任何操作时是否自动终止会话，是否需要再次进行身份鉴别才能重新操作；
   2) 验证产品最大超时时间能否由授权管理员设定。
b) 预期结果：
   1) 在设定的时间段内无任何操作时终止会话，需要再次进行身份鉴别才能够重新操作；
   2) 最大超时时间能由授权管理员设定。

6.3.2.3.5 会话锁定

a) 测试方法：
   1) **验证产品是否为管理员提供锁定其自身交互会话的功能；**
   2) **验证产品锁定后是否需要再次进行身份鉴别才能够重新管理备份系统；**
   3) **验证在同一时间点是否可以利用同一用户账号在两台主机上进行登录。**
b) 预期结果：
   1) **为管理员提供了锁定其自身交互会话的功能；**
   2) **锁定后需要再次进行身份鉴别才能够重新管理备份系统。**
   3) **同一用户在同一时间点只能在一台主机上进行登录。**

6.3.2.3.6 访问历史

a) 测试方法：
   验证授权用户登录成功后，产品是否能够显示如下数据：
   1) 日期、时间、来源和上次成功登录系统的情况；

2） 上次成功登录备份系统以来身份鉴别失败的情况；

3） 口令距失效日期的天数。

b） 预期结果：

授权用户登录成功后，产品可以显示如下数据：

1） 日期、时间、来源和上次成功登录系统的情况；

2） 上次成功登录备份系统以来身份鉴别失败的情况；

3） 口令距失效日期的天数。

6.3.2.4 功能保护

6.3.2.4.1 功能监控

a） 测试方法：

1） **在系统正常运行的状态下，人为使其部分功能失效；**

2） **验证产品能否提供对功能失效进行提示和报警。**

b） 预期结果：

能够提供对其自身部分功能的失效进行监控。

6.3.2.4.2 功能恢复

a） 测试方法：

1） **人为造成备份系统部分关键功能失效；**

2） **验证产品是否提供关键功能失效时的保护机制。**

b） 预期结果：

具有关键功能失效时的相应保护机制。

6.3.3 安全保证要求评估

6.3.3.1 配置管理

6.3.3.1.1 配置管理能力

a） 评估方法：

1） **检查每个版本的产品是否具有唯一的参照号；**

2） **检测产品提供的配置管理系统，验证其是否能唯一标识产品所包含的所有配置项，是否提供措施使得对配置项只能进行授权修改；**

3） **审查产品的配置管理文档中是否包括了配置清单和配置计划，审查配置清单是否描述并唯一标识了组成产品的所有配置项，审查配置计划是否描述了配置管理系统使用方法以及配置管理系统的运作和配置管理计划是否相一致，审查配置管理文档是否描述用于唯一标识产品所包含配置项的方法，是否提供所有配置项都已经或正在配置管理系统下有效地进行维护的证据。**

b） 预期结果：

配置管理能力中的全部要求都已经得到满足。

6.3.3.1.2 配置管理范围

a） 评估方法：

审查开发者是否提供了产品配置项列表，且配置项列表包括：实现表示和安全目标中其他保证

组件所要求的评估证据。

b） 预期结果：

配置管理范围中的全部要求都能得到满足。

6.3.3.2 交付与运行

6.3.3.2.1 交付

a） 评估方法：

1） 审查产品的交付文档，查看其是否具有安装文档、产品生成文档、指导用户进行产品运维的文档以及产品培训手册等文档；

2） 审查开发者是否提供了交付程序，该程序是否在文档中得到描述。

b） 预期结果：

交付中的全部要求都能得到满足。

6.3.3.2.2 安装、生成和启动

a） 评估方法：

审查开发者是否提供了文档，描述了产品安全地安装、生成和启动所必要的步骤。

b） 预期结果：

安装、生成和启动中的全部要求都能得到满足。

6.3.3.3 开发

6.3.3.3.1 功能规范

a） 评估方法：

1） 审查产品的开发文档，查看是否具有功能规范设计文档；

2） 审查功能规范设计文档，确认其是否描述了产品的所有安全功能和外部接口，是否包括所有外部安全功能接口的使用方法和用途，是否是内在一致的，是否能完备地表示产品安全功能。

b） 预期结果：

功能规范中的全部要求都能得到满足。

6.3.3.3.2 高层设计

a） 评估方法：

1） 审查产品的开发文档，查看是否具有高层设计文档；

2） 审查高层设计文档，确认其是否按照子系统来描述产品安全功能的结构，是否描述了每个产品安全功能子系统所提供的安全功能性，是否标识了安全功能子系统的所有接口，是否标识了产品安全功能子系统的外部可见的接口，是否标识了产品安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制提供功能的一个表示，是否描述产品安全功能子系统所有接口的用途与使用方法，是否把产品分成安全策略实施和其他子系统来描述，是否以非形式化方式进行描述，是否是内在一致的。

b） 预期结果：

高层设计中的全部要求都能得到满足。

6.3.3.3.3 表示对应性

a) 评估方法：

审查对应性分析报告，确认是否论证了功能规范中所有的相关安全功能都在高层设计中得到正确且完备地细化。

b) 预期结果：

表示对应性中的全部要求都能得到满足。

6.3.3.4 指导性文档

6.3.3.4.1 管理员指南

a) 评估方法：

1) 审查产品的管理员指南，验证其是否：

——描述管理员可使用的管理功能和接口；

——描述如何以安全的方式管理产品；

——包含一些关于安全处理环境中应被控制的功能和特权的警示信息；

——描述所有关于与产品安全运行有关用户行为的假设；

——描述所有受管理员控制的安全参数，合适时指明安全值；

——描述每一种与需要执行的管理功能有关的安全相关事件，包括对改变安全功能所控制的实体的安全特性；

——描述所有与系统管理员有关的 IT 环境的安全要求。

2) 审查产品的管理员指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果：

管理员指南中的全部要求都能得到满足。

6.3.3.4.2 用户指南

a) 评估方法：

1) 审查产品的用户指南，验证其是否：

——描述非管理员用户可用的功能和接口；

——描述产品所提供的用户可以访问的安全功能的使用；

——包含一些关于安全处理环境中应被控制的用户可访问功能和特权的警示信息；

——清晰地阐述产品安全运行所必需的所有用户职责，包括与产品安全环境陈述中可找到的与关于用户行为的假设有关的那些职责；

——描述所有与用户有关的 IT 环境安全要求。

2) 审查产品的用户指南，验证其是否与供评估的所有其他文档保持一致。

b) 预期结果：

用户指南中的全部要求都能得到满足。

6.3.3.5 生命周期支持

6.3.3.5.1 开发安全

a) 评估方法：

1) **审查开发者是否提供了开发安全文档，验证开发文档是否描述了在产品的开发环境中，保护产品设计和实现的保密性和完整性在物理、程序、人员以及其他方面必要的安全措施；**

2） **审查开发安全文档是否提供了产品的开发和维护过程中执行安全措施的证据**。

b） 预期结果：

开发安全中的全部要求都能得到满足。

6.3.3.6 测试

6.3.3.6.1 测试覆盖

a） 评估方法：

审查开发者提供的测试覆盖**分析**，验证该**分析**是否**证实**了测试文档中所标识的测试和功能规范中所描述的安全功能是对应的，**验证功能规范中所描述安全功能和测试文档所标识的测试之间的对应性是否完备**。

b） 预期结果：

测试覆盖中的全部要求都能得到满足。

6.3.3.6.2 测试深度

a） 评估方法：

审查开发者是否提供了测试深度分析文档，验证测试文档中所标识的测试是否足以证明该安全功能是依照其高层设计运行的。

b） 预期结果：

测试深度中的全部要求都能得到满足。

6.3.3.6.3 功能测试

a） 评估方法：

1） 审查测试文档是否包括测试计划、测试程序描述、预期测试结果和实际测试结果；

2） 审查测试计划是否标识了要测试的安全功能，描述了要执行的测试目标；

3） 审查测试程序描述是否标识了要执行的测试，并描述了每个安全功能的测试脚本。这些脚本包括对于其他测试结果的任意顺序依赖性；

4） 审查预期的测试结果是否与测试成功执行后的预期输出一致；

5） 审查文档中记录的预期测试结果和实际测试结果，确认每个被测试的安全性功能都按照规定运转。

b） 预期结果：

功能测试中的全部要求都能得到满足。

6.3.3.6.4 独立测试

a） 评估方法：

1） 检查开发者是否提供用于测试的产品，并且产品是否适合测试；

2） 检查开发者是否提供一组相当的资源，用于开发者的产品安全功能测试。

b） 预期结果：

独立测试中的全部要求都能得到满足。

6.3.3.7 脆弱性评定

6.3.3.7.1 脆弱性分析

a） 评估方法：

1） 检查产品是否提供了脆弱性分析文档；

2） 审查脆弱性文档是否描述为搜索用户能违反产品安全策略的明显方法而执行的产品可交付材料分析；

3） 审查脆弱性文档，确认是否描述了明显的脆弱性的处置方法；

4） 审查脆弱性文档，确认是否针对所有已标识的脆弱性，说明了脆弱性不能在产品的预期使用环境中被利用。

b） 预期结果：

脆弱性分析中的全部要求都能得到满足。

6.3.3.7.2 误用

a） 评估方法：

审查开发者是否提供了指导性文档，该文档是否描述了产品所有可能的运行方式（包括失败和操作失误后的运行），它们的后果以及对于保持安全运行的意义，是否列出关于预期使用环境的所有假设，是否列出外部安全措施（包括外部程序的、物理的或人员的控制）的所有要求，是否是完备的、清晰的、一致的、合理的。

b） 预期结果：

误用中的全部要求都能得到满足。

附 录 A
（资料性附录）
性能指标与测试

A.1 性能指标

A.1.1 备份速度

单位时间内备份的数据总量，单位 MB/s。

A.1.2 恢复速度

单位时间内恢复的数据总量，单位 MB/s。

A.1.3 占用资源

备份或恢复作业相关进程占用主机资源的多少。包括 CPU、系统内存等资源的占用等。

A.1.4 最大磁带驱动器数

单个备份存储节点能够管理的最大磁带驱动器数量。

A.1.5 最大磁带槽位数

单个备份存储节点能够管理的最大磁带槽位数量。

A.1.6 最大磁带数

单个备份存储节点能够管理的最大磁带数量。

A.1.7 稳定性

安装后，产品及其相关系统均能够稳定运行。稳定性可用平均无故障率等指标进行评价。

A.1.8 数据恢复时间

数据受到损坏到数据成功恢复所需要的时间。该指标由数据量、文件大小、数据类型、传输带宽等因素决定。数据恢复时间越短，恢复效率越高。

A.2 性能测试

A.2.1 备份速度

a） 测试方法：

1） 根据测试要求选取测试样例，包括文件的数量，每个文件数量大小和文件类型等并记录测试样例的大小，以 MB 为单位；

2） 对测试样例进行备份，使用第三方计时设备记录备份测试样例所用的时间，记录备份测试样例所使用的时间，以秒(s)为单位；

3） 计算备份速度为测试样例的大小和完成时间的比值，单位为 MB/s。

b） 测试结果：

根据实际测试情况，记录测试所用工具、参数以及测试结果。

A.2.2 恢复速度

a） 测试方法：

1） 根据测试要求选取测试样例，包括文件的数量，每个文件数量大小和文件类型等并记录测试样例的大小，以 MB 为单位；

2） 对测试样例进行恢复，使用第三方计时设备记录恢复测试样例所用的时间，记录恢复测试样例所使用的时间，以秒(s)为单位；

3） 计算恢复速度为测试样例的大小和完成时间的比值，单位为 MB/s。

b） 测试结果：

根据实际测试情况，记录测试所用工具、参数以及测试结果。

A.2.3 占用资源

a） 测试方法：

使用第三方软件监测备份服务器和客户端服务器在备份作业执行过程中，备份作业占用系统资源的多少。

b） 测试结果：

记录第三方软件所显示的资源占用量。

A.2.4 最大磁带驱动器数

a） 测试方法：

1） 配置待测磁带驱动器；

2） 配置必要的备份系统环境以保证最大磁带驱动器数测试能正常进行；

3） 验证备份服务器能够管理的最大磁带驱动器数量。

b） 测试结果：

根据实际测试情况，记录备份服务器能够管理的最大磁带驱动器数量。

A.2.5 最大磁带槽位数

a） 测试方法：

1） 配置待测磁带槽位；

2） 配置必要的备份系统环境以保证最大磁带槽位数测试能正常进行；

3） 验证备份服务器能够管理的最大磁带槽位数量。

b） 测试结果：

根据实际测试情况，记录备份服务器能够管理的最大磁带槽位数量。

A.2.6 最大磁带数

a） 测试方法：

1） 配置待测磁带；

2） 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；

3） 验证备份服务器能够管理的最大磁带数量。

b） 测试结果：

根据实际测试情况，记录备份服务器能够管理的最大磁带数量。

A.2.7 稳定性

a) 测试方法：

1) 根据测试要求持续使用产品；

2) 记录产品的持续无故障率。

b) 测试结果：

能够持续正常使用产品。

A.2.8 数据恢复时间

a) 测试方法：

1) 准备测试用例。包括文件的数量，每个文件数量大小和文件类型等；

2) 准备测试环境，包括网络环境、主机环境等；

3) 进行数据恢复，同时使用第三方计时设备记录从开始恢复到数据成功恢复所需要的时间。

b) 测试结果：

记录数据从受到破坏到成功恢复使用的时间，以秒(s)为单位。

参 考 文 献

[1] GB/T 18336.3—2008 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

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
数据备份与恢复产品技术要求
与测试评价方法
GB/T 29765—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲 2 号(100013)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:010-51780168
010-68522006
2013 年 10 月第一版
*
书号:155066·1-47676

GB/T 29765-2013