GB

中国国家标准汇编

577

GB 29765~29791

（2013年制定）

中国标准出版社

中 国 国 家 标 准 汇 编

577

GB 29765～29791

（2013 年制定）

中国标准出版社　编

中国标准出版社

北　京

图书在版编目(CIP)数据

中国国家标准汇编:2013年制定.577:
GB 29765～29791/中国标准出版社编.—北京:
中国标准出版社,2014.9
ISBN 978-7-5066-7658-8

Ⅰ.①中… Ⅱ.①中… Ⅲ.①国家标准-
汇编-中国-2013 Ⅳ.①T-652.1

中国版本图书馆CIP数据核字(2014)第187383号

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(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 39.25 字数 1 210 千字
2014年9月第一版 2014年9月第一次印刷

*

定价 220.00 元

出 版 说 明

1.《中国国家标准汇编》是一部大型综合性国家标准全集。自1983年起，按国家标准顺序号以精装本、平装本两种装帧形式陆续分册汇编出版。它在一定程度上反映了我国建国以来标准化事业发展的基本情况和主要成就，是各级标准化管理机构，工矿企事业单位，农林牧副渔系统，科研、设计、教学等部门必不可少的工具书。

2.《中国国家标准汇编》收入我国每年正式发布的全部国家标准，分为“制定”卷和“修订”卷两种编辑版本。

“制定”卷收入上一年度我国发布的、新制定的国家标准，顺延前年度标准编号分成若干分册，封面和书脊上注明“20××年制定”字样及分册号，分册号一直连续。各分册中的标准是按照标准编号顺序连续排列的，如有标准顺序号缺号的，除特殊情况注明外，暂为空号。

“修订”卷收入上一年度我国发布的、被修订的国家标准，视篇幅分设若干分册，但与“制定”卷分册号无关联，仅在封面和书脊上注明“20××年修订-1，-2，-3，……”字样。“修订”卷各分册中的标准，仍按标准编号顺序排列(但不连续)；如有遗漏的，均在当年最后一分册中补齐。需提请读者注意的是，个别非顺延前年度标准编号的新制定的国家标准没有收入在“制定”卷中，而是收入在“修订”卷中。

读者配套购买《中国国家标准汇编》“制定”卷和“修订”卷则可收齐由我社出版的上一年度我国制定和修订的全部国家标准。

3.由于读者需求的变化，自1996年起，《中国国家标准汇编》仅出版精装本。

4.2013年我国制修订国家标准共1 979项。本分册为“2013年制定”卷第577分册，收入国家标准GB 29765～29791的最新版本。

中国标准出版社

2014年8月

目　　录

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

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，