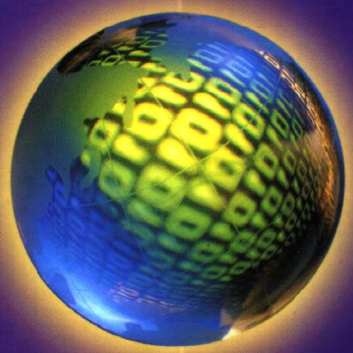
存储技术丛书

Storage Security

Protecting SANs, NAS, and DAS

存储安全技术

——SAN、NAS和DAS的安全保护



[美] John Chirillo　Scott Blaul　著

金甄平　王宝生　洪　平　等译

WILEY

PHEI

電子工業出版社

Publishing House of Electronics Industry

http://www.phei.com.cn

存储技术丛书

存储安全技术

—— SAN、NAS 和 DAS 的安全保护

Storage Security
Protecting SANs, NAS, and DAS

[美] John Chirillo　Scott Blaul　著
金甄平　王宝生　洪　平　等译

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

内 容 简 介

本书内容主要涉及存储网络技术和存储备份技术，着重讨论有关数据安全和数据保护的各种潜在问题，包括各种可能的安全漏洞、DAS/NAS/SAN 框架下的冗余策略、入侵监测、可用性、数据保护、安全监视、测试以及各种应对手段等。数据复制策略和复制技术与网络连接存储(NAS)和存储局域网络(SAN)的体系结构关系密切，也是本书讨论的重点。它的内容包括 RAID 技术、数据克隆、数据快照、远程数据复制、多平台访问安全需求以及数据备份策略和备份技术。为了确保集中数据的完整性，本书给出了一套非常有效的安全规划方法，包括它的流程步骤、不同安全问题的技术答案以及针对来自社会的各种危及数据安全活动的对策方法等。

本书与其他同类书籍的一个最大区别在于本书并不仅限于数据安全的概念和理论的论述，而是采用工业标准的方法学向读者展示一种实用的安全存储网络的实现方法。它对 IT 专业人员、IT 咨询顾问、企业信息主管(CIO)以及技术销售人员具有很高的参考价值。

John Chirillo, Scott Blaul: **Storage Security: Protecting SANs, NAS, and DAS**
ISBN 0-7645-1688-4

版权贸易合同登记号：图字：01-2003-0373

图书在版编目(CIP)数据

存储安全技术：SAN、NAS 和 DAS 的安全保护/(美)奇里洛(chirillo, J.)等著；金甄平等译.
—北京：电子工业出版社，2004.1
(存储技术丛书)
书名原文：Storage Security: Protecting SANs, NAS, and DAS
ISBN 7-5053-9287-5

Ⅰ.存… Ⅱ.①奇…②金… Ⅲ.数据存储-安全技术 Ⅳ.TP333

中国版本图书馆 CIP 数据核字(2003)第 099231 号

责任编辑：周宏敏
印 刷 者：北京兴华印刷厂
出版发行：电子工业出版社 http://www.phei.com.cn
北京市海淀区万寿路 173 信箱 邮编：100036
经 销：各地新华书店
开 本：787×1092 1/16 印张：18.25 字数：467 千字
版 次：2004 年 1 月第 1 版 2004 年 1 月第 1 次印刷
定 价：32.00 元

凡购买电子工业出版社的图书，如有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系。
联系电话：(010)68279077

译 者 序

随着全球信息化的飞速发展，数据已经成为企业的一项最重要的资产。数据存储的可用性、完整性和安全性已不再是一个单纯的技术问题，更是企业生存力和竞争力的重要体现。

本书首先从技术的角度对直接连接存储（DAS）、网络附加存储（NAS）和存储区域网络（SAN）三种基本存储技术的体系结构、技术特点进行了介绍，并重点讨论了它们在数据安全和数据保护方面存在的各种潜在问题；随后，本书围绕数据的可用性、完整性和安全性问题，按照连锁安全逻辑的思想，从系统的基础架构、网络构成、硬件特点、应用软件、磁盘技术、管理工具等各个方面进行了全面的分析，并就 RAID 技术、数据克隆、数据快照、远程数据复制、多平台访问以及数据备份等技术进行了详细讨论；最后，本书结合具体实际案例，对存储解决方案的选用原则、安全规划方法、系统实施方法以及各种安全审计策略和方法进行了讨论。

本书与其他同类书籍相比的一个最大特点在于它的实用性，书中提供的大量案例都是作者长期工作经验的总结；本书所提出安全技术矩阵分析方法具有简单、科学和实用特点，对于我们实际数据安全工作具有一定的参考价值；本书在实际案例分析中所采用的存储安全规划步骤对于我们的实际工作具备一定的指导意义。

本书对于 IT 专业人员、IT 咨询顾问、企业信息主管（CIO）以及技术销售人员具有较高的参考价值。

作者简介

John Chirillo 从 12 岁就开始了他的计算机生涯，当时他用了一年的时间自学了计算机的基础知识，并编写了一些软件予以发表。随后，他又取得了多项编程语言的认证，包括 QuickBasic、VB、C ++ 、Pascal、汇编语言和 Java。他所开发的一个 PC 优化工具曾将当时标准的 Intel 486 芯片的处理速度提高了一倍。

在经营了两家公司(Software Now 和 Geniusware)之后，John 成为一家著名公司的咨询员，专门从事安全分析、嗅探分析、LAN/WAN 设计、实施和故障分析工作。在此期间，John 又取得了一系列网络互连技术的认证资格，包括 Cisco 的 CCNA、CCDA、CCNP、Intel 认证的解决方案咨询师、康柏的 ASE 企业存储认证、UNIX 和 CISSP，现正在申请 CCIE 资格。目前，John 在一家技术管理公司任高级网络工程师。John 曾出版过多部有关计算机安全和网络技术的著作，包括由 John Wiley & Sons 公司出版的黑客攻击(Hack Attacks)系列丛书。

Scott Blaul 于 1981 年开始从事电子行业的工作，并在 United States Marine Corps 担任电子维修工程师。作为 USMC 的一名教师，他曾担任了 5 年的电子课程培训工作。1989 年，Scott 离开 USMC，加入了 Inacomp 计算机公司，该公司最后被 ValCom 公司兼并。他在那里工作了 13 年，参与了许多计算机服务项目的研发，包括各种现场服务(有关台式机的技术服务)和专业服务(有关服务器、大型机、存储系统和安全系统的支持服务)。他所参与服务的许多公司都是名列财富 1000 名的著名企业。Scott 也拥有很多网络技术的资格认证，包括 CNE、ASE、CCNA、CCNP、CISSP 和 CCIE(申请中)。

前　言

有关计算机安全问题的论著已经很多，安全侵害事件层出不穷，触目惊心。本书不打算再重复这方面的内容，而只是想从实用的角度探讨如何应用这些安全理论来建立一种更加安全的集中存储网络，重点讨论如何针对具体情况正确选择安全的存储网络技术。当然，这中间不可避免地会涉及到一些有关存储安全的基本原理，并由此给出特定的安全存储网络解决方案。

我们在考虑存储网络的保护问题时，切不可忘记实施存储网络的基本目的。存储网络类型的选择首先要以基本业务需求为基础。在我们确定了满足这些需求的存储网络技术之后，再根据数据的敏感程度来确定相应的系统安全水平。在本书中，我们将介绍如何利用安全指标的方法来选择最适合特定环境的存储设备。

安全思考： 数据如果过于安全，以致无法被访问，那就等同于没有数据。因此，尽管本书的主题是关于存储和存储网络的，或更确切地说，是关于存储网络安全的，但我们不会因此而忽略数据的访问需求。

目标读者

对于企业来说，集中存储不仅可以节省设备成本和管理费用，而且可以强化企业对数据的控制。但如果我们不能很好地解决存储的安全问题，那将是一件非常可怕的事情。因此，任何一个对于如何建立更加安全的集中存储环境问题感兴趣的人都应该读一下本书。它对 IT 专业人员、IT 咨询顾问、企业信息主管（CIO）以及技术销售人员具有很高的参考价值。

内容提要

本书主要讨论存储网络技术和存储备份技术，着重介绍有关数据安全和数据保护的各种潜在问题，包括各种可能的安全侵害、DAS/NAS/SAN 框架下的冗余策略、入侵监测、数据可用性、数据保护、安全监视、测试以及各种安全应对措施等。本书从微观的角度对所有这些问题进行了深入细致的讨论。数据复制策略和复制技术与网络附加存储（NAS）和存储区域网（SAN）的体系结构关系密切，也是本书讨论的重点，其内容包括 RAID 技术、数据克隆、数据快照、远程数据复制、多平台访问安全需求以及数据备份策略和备份技术。为了确保集中数据的完整性，我们给出了一套非常有效的安全规划方法，包括它的实施步骤、不同安全问题的技术答案以及针对来自社会的各种危及数据俺全活动的对策方法等。

考虑到上述所有因素并以信息系统安全专家认证计划（CISSP）提出的有关计算机安全的十大领域为指导，本书讨论了以下内容：

- ◆ 不同存储技术的通用基础
- ◆ 通用存储网络技术分析
- ◆ 特殊存储网络技术分析
- ◆ 企业存储网络技术的选择评估

- 根据不同安全需求的解决方案选择方法
- 安全备份解决方案的选择方法
- 系统实施过程的安全方法
- 存储网络安全规划的建立、实施和测试框架
- 数据加密技术分析
- 各种安全对策和措施的讨论

对于一个安全存储网络项目来说，它的评估阶段、规划设计阶段以及测试阶段对于该项目的正确选型乃至最终的成功实施都起着至关重要的作用。本书不仅对这方面的内容进行了详细的讨论，而且还提供了具体的案例供读者参考。另外，本书的参考网站（www. wiley. com/compbooks/chirillo）还提供了相应的文档资料，供读者作为对自己的存储网络进行安全需求分析的参考。

本书的一些约定

本书采用以下约定为读者提示一些需要特别强调或有帮助的信息，它们的具体形式和作用如下：

说明： 提供有关当前讨论主题的一些附加的或重要的信息，或是一些技术参考数据。

提示： 给出一些实用的技术提示。

参考： 提示读者获取更多的有关当前讨论内容的信息资料。

安全思考： 主要是告诉读者在从事有关安全事务的过程中需要考虑的一些问题，或提醒读者在进行某项工作时可能对网络或系统带来的负面影响。

目　录

第 1 章　存储技术的发展历史

在正式进入存储安全问题的讨论之前，让我们首先来回顾一下存储技术的发展历史，从中了解存储技术和存储网络安全对于企业生存与发展的重要性。为此，本章从一些关键术语的定义出发，对一些关键的概念以及存储技术的历史进行了详细的讨论，希望以此作为我们对存储与存储网络安全问题讨论的基础。

1.1　常用技术术语

在正式讨论之前，让我们先来了解几个关键术语的定义：

- **存储网络(storage network)**：我们这里之所以采用了存储网络一词并不是偶然的。单就存储而言，它可以采用各种不同的技术和方法(如 DAS、NAS、SAN 和 iSCSI)实现；而存储网络一词通常是指在特定环境下可以提供从多台主机(同构的或异构的)到多台设备访问的存储实现。例如，一个单纯以共享文件访问为目的、采用 SCSI 技术将多个存储子系统与多台(独立的)服务器直接连接起来的系统，都可以像网络附加存储(NAS)或存储区域网(SAN)解决方案那样被视为存储网络。还有一点需要注意的是：本书所说的存储网络一词，它的内容不仅包含存储设备本身，还包含存储网络部件。例如，一个 SAN 存储网络就可能包括主机连接链路、光纤仲裁环路或光纤通道交换技术等。有关存储网络的硬件设备、配置方式、软件组成以及安全组件等，我们将在后面的相应章节中予以讨论。
- **直接连接存储(DAS，direct attached storage)**：就本书而言，直接连接存储主要是指以数据共享为目的而直接配属于某一特定主机的存储。除非特殊说明，本书所提及的所有 DAS 都是指单一主机系统，它们可能带有自己的内置存储设备，或是附接外部存储设备(但不是 NAS 或 SAN)。例如，一台连接在 SCSI 存储子系统上的主机就属于这种情况。
- **网络附加存储(NAS，network attached storage)**：网络附加存储通常是指利用网络连接(典型的是以太网)实现的共享存储。它通过采用通用文件协议的网络连接可以实现异构主机间的文件共享。例如，文件可以在没有文件服务器这样的专用设备的介入下，直接在 TCP/IP 网络下实现共享。
- **存储区域网(SAN，storage area network)**：存储区域网通常是指由多台互连主机通过光纤连接实现共享的存储设施。这些主机可以直接连接到 SAN 上，也可以通过光纤集线器或交换机连接。SAN 是由存储磁盘(或 SAN 磁带库等)组成的一种高速子网，它通常可以提供更多的存储空间供整个 LAN 和 WAN 网络共享，并且不会影响到网络服务或生产效率。

1.2 选择 NAS 或 SAN 的理由

企业采用 NAS 或 SAN 解决方案的一个主要原因是实现数据的“集中”管理，以便更好地控制企业的这部分数据资产。为此，很多设备都需要与 NAS 或 SAN 建立连接通道、访问通道，或是至少能够“看到”这些 NAS 或 SAN 设备。这就如同一滴水落入水池中而形成的连锁反应一样(见图 1.1)，每一个环节(波纹)都可能存在弱点，都必须从安全的角度予以考虑。我们在规划存储网络安全的时候，只有采用连锁安全逻辑才能够最终达到数据安全的目的。因此，连锁逻辑是安全存储的核心。

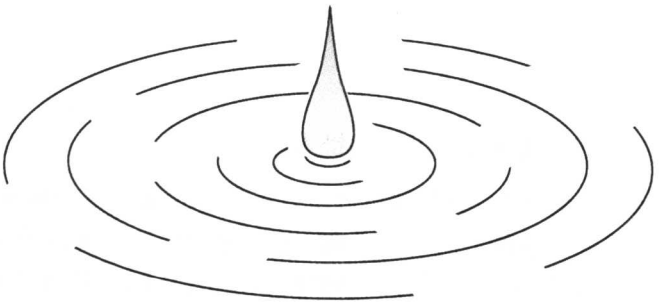


图 1.1 连锁反应

1.3 从大型主机到分布系统

在 20 世纪 80 年代和 90 年代初，业界曾掀起一股分布的潮流，就是将各种计算资源和大型计算机的处理能力进行分散，以实现图 1.2 所示的分布处理结构。在此期间曾经流行的分布网络结构包括：3Com 3Plus Open、Appleshare/Apple Talk、LAN Manager、Novell Netware、Banyan Vines、LANtastic、MS Windows for Workgroups、Windows NT 以及各种 UNIX 的变体版本，包括 AIX、True-64 UNIX、HP-UX、SCO、SUN Solaris 和 Linux 等。但这些操作系统目前大部分已不存在了，仍在使用的分布网络结构只剩下 Novell Netware、Microsoft Windows NT4 和 2000、SUN Solaris、HP-UX、AIX 和 Linux。

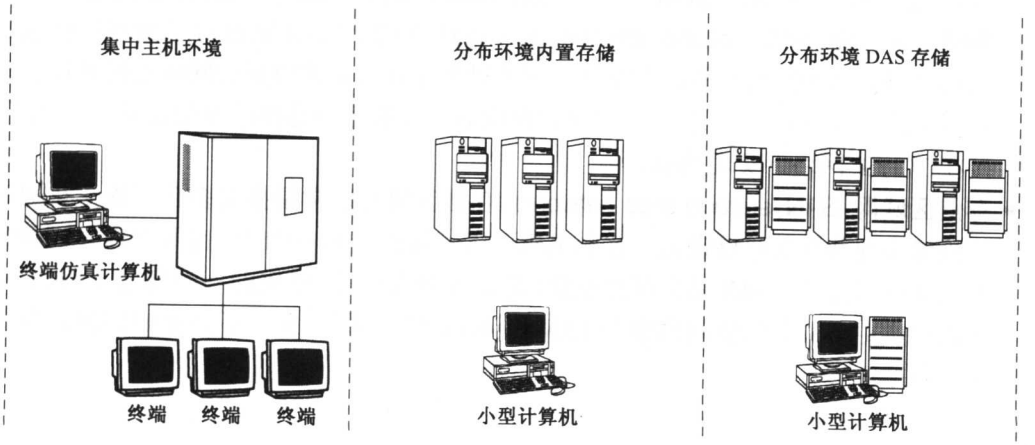


图 1.2 主机系统、分布系统和带 DAS 的分布系统

硬件制造商们在推动分布计算技术的初期是从支持内置和外接两种直接连接的存储设备(DAS)着手的,这主要是考虑到当时的技术限制(也就是 SCSI 的固有距离限制)、DAS 所能提供的速度、以及它的部署简单、成本低廉(与其他技术相比)和市场接受程度高等因素。但随着企业 DAS 系统的能力被不断突破,制造商们开始寻求新的替代方案。而此时的 EMC、IBM 和数据设备公司(DEC)等企业已经以其自己的大型存储设备在大型机市场确立了各自的地位。例如,据 Exodus 报道:

> "1990 年,EMC 以其推出的 Symmetrix 系列产品而一举成为大型机市场中第一个采用小型廉价硬盘阵列构筑智能信息存储系统的厂商。"EMC 也因此确立了 Symmetrix 产品在大型机市场的地位,而且随后又进入了部分分布市场。EMC 之所以能够做到这一点,其中的一个原因就是"EMC 在 1995 年扩展了它的 Symmetrix 技术,创建了第一个平台独立的存储系统,从而具备了同时支持多种主流计算机操作系统的能力。"

但 Symmetrix 产品也存在一个问题,那就是它的初期投资巨大。到了 20 世纪 90 年代末期,数据设备公司(DEC)已经在市场中处于苦苦挣扎的状态。但 DEC 公司所拥有的 VAX 和 Alpha 系列产品技术以及它早在 20 世纪 70 年代就已经着手研究的存储技术吸引了康柏计算机公司(Compaq Computer Corporation),后者于 1998 年 1 月以 96 亿美元购并了 DEC 公司。而在这项购并交易的背后,除了拯救 DEC 公司的产品,包括它的存储技术的目的之外,保持与 HP 和 IBM 的竞争力也是一个重要的原因。这种现象即使是在今天也仍在不断地上演,因为在计算机界中,只有那些实力最强、规模最大、最能适应市场的企业才能够生存。2001 年 9 月康柏被惠普公司收购而成立新惠普的事件又是一个很好的例子。

1.3.1　资源分布

集中计算模式向分布计算模式转移(见图 1.2)的一个原因就是人们相信这种分布方式可以将系统的管理分散到整个组织范围内,从而节省外聘专业公司进行小型机和大型机系统管理的高昂费用。事实上,在某些情况下,它确实可以减轻这种费用的压力,但在更多情况下,它所带来的效果恰恰相反。引起这种费用增加的因素很多,其中最主要的是分布环境下的多地点管理所带来的额外开销。

一般来说,主机应用开发的速度较慢,限制条件较多。为此,很多企业希望寻求一种新的软件开发模式,以便能够在速度上超越自己的竞争对手。而分布计算环境可以让企业在分布平台开发特定的"点应用(point application)"软件,而无需等待主机开发工作的开始。这也是许多企业系统(并不一定是全部)向分布环境转移的一个原因。

如图 1.3 所示,计算资源的分布带来了数据的分散,这给数据的管理(如何控制数据资产)、保护(如何确保故障情况下的数据安全)、远程可用性(如何保证数据的远程使用)和安全性带来了新的问题。而这些问题本身又涉及到企业的财务结构(部门有无自己的预算等)、硬件的限制和企业的政策(资产的控制方式)等因素,因而变得更加复杂。

另外,由于数据都被分散在了企业的各个业务部门和班组中,企业还面临着一个在分布环境下如何更好地控制和管理自己的数据和知识产权的问题。例如,财务部门在拥有了自己的服务器和存储设备之后,他们的数据就与企业的其他数据"分隔"开了。在某些情况下,这种分隔可能是一种很好的数据安全手段。但在更多情况下,它可能形成人们对于数据的"眼不见,

心不烦”的状态，从而更容易导致敏感信息的泄露。但人力资源部倒是这种数据分隔的一个正面的例子。我们知道，企业的员工信息属于企业的保密信息。因此，很多企业也是通过隔离的方式来确保这些资料的安全的。一旦人力资源的数据网络与企业的其他网络分开，我们就可以对流向人力资源部的数据和信息实施更加灵活的控制。

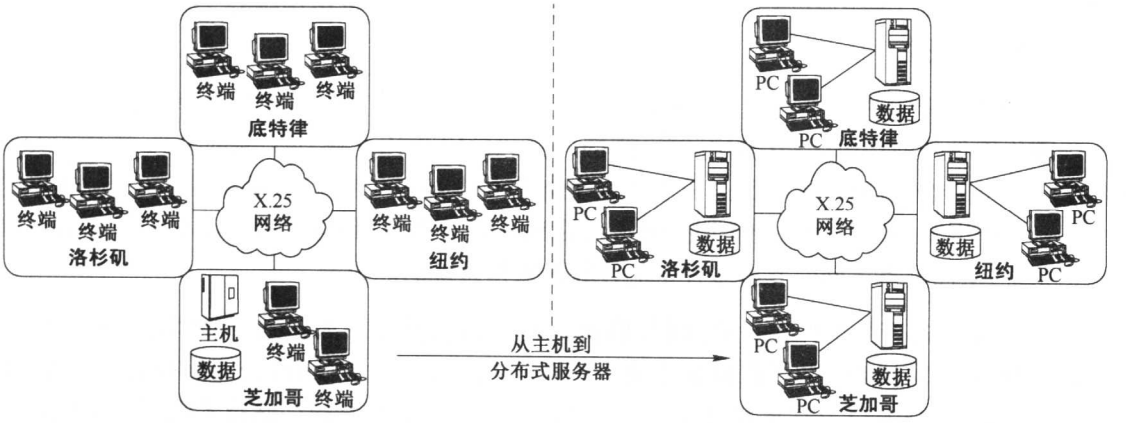


图 1.3 从集中数据向分布数据的转移

集中数据是主机计算模式的副产品，而分布数据存储解决方案又带有其自身的风险。这就带来了一个问题，企业能否同时发挥集中模式和分布模式的优势呢？答案就是采用网络附加存储(NAS)和存储区域网(SAN)。

1.3.2 用 NAS 和 SAN 取代 DAS

随着存储技术的蓬勃发展，加之制造商们为吹嘘自身实力和掩盖自身弱点而大肆鼓噪，因此在一定程度上造成了人们对于 NAS 和 SAN 概念的模糊。换句话说，对于不同的咨询公司、经销商以及制造厂商来说，它们的含义可能是不同的。

有关 DAS、NAS 和 SAN 的技术细节以及它们的安全需求，我们将在第 2、3 和 4 章中分别进行讨论。这里，我们仅就本章开始时给出的定义对 NAS 和 SAN 的概念做一个简要的说明。

- 一般来说，NAS 在两种集中存储方案中的相对费用较低。根据厂商的不同，有些 NAS 可能只支持有限的几种操作系统(例如，有的制造商的设备可能只支持 Windows NT/2000 和 Netware 两种平台)，而其他的 NAS 可能采用标准的访问协议或文件系统(例如 TCP/IP 和 CIFS)来支持任何操作系统。由于制造商之间的这种产品上的差异，详细了解每一种 NAS 设备的特点以及它们的优劣十分重要。
- SAN 一般在成本上要高于 NAS，当然它的系统性能也更加健壮，可以提供更多的冗余特性和选件功能并具备良好的系统伸缩能力。SAN 的实现一般是某种形式的“SAN 网络结构”(最常见的是光纤)，它可以支持多种操作系统。另外，SAN 通常还可以通过配置实现远程数据复制以实现数据的灾害恢复。

以往由于 NAS 和 SAN 的实施费用昂贵，因此超出了许多企业的经济承受能力。但随着近期市场的变化，许多 NAS 设备和部分 SAN 设备的价格已经大幅下降，从而使它们有可能成为许多企业存储系统的替代产品。这种成本的降低不仅使企业能够充分发挥 NAS 和 SAN 解决

方案的特点，而且也使这些存储技术更加普及。在后面的章节中，我们将讨论如何根据安全需求来正确选择此类解决方案。

同任何其他的新技术一样，当企业的原始业务需求得到满足之后，由 NAS 和 SAN 所带来的新特点、新需求以及潜在的安全问题也必须得以解决。正是基于这样一些原因以及我们将在后续各章中讨论的因素，解决数据的安全性和可用性问题已经刻不容缓。由 NAS 和 SAN 引发的主要问题包括：

- **对集中的重新认识**：有人把 NAS 和 SAN 技术比做是“把鸡蛋全部放在了一个篮子里”，以此来否定它们的作用，贬低它们对企业的价值。但是，如果企业在决定采用 NAS 和 SAN 实现数据的重新集中的同时，没有采取适当的措施来解决数据的安全、备份和复制等问题，那么，人们的那句老话就可能成为现实：即把所有的数据都放在了一个没有任何保护措施的破篮子里了。
- **备份窗口问题**：NAS 和 SAN 所带来的另一个问题就是所有数据的可用备份时间问题，专业术语称为备份窗口（Backup Window）。数据集中意味着大量数据存在于单一设备中。如今对于一个企业来说，将几兆兆字节的数据存放在单台设备中的情况并非少见。而这些企业（特别是那些跨国企业）的备份窗口也非常有限。如何正确选取备份工具和备份方法，以便在有限的备份窗口内完成数据备份已经成为一个非常重要的问题。而如何确保备份过程的安全实施也是一个不容忽视的问题。
- **新的分布问题**：2001 年 9 月 11 日发生在美国的震惊全球的 9·11 恐怖袭击事件彻底改变了人们对于信息与技术安全的认识。从那一天起，越来越多的企业开始寻求 NAS/SAN 技术以复制和保护它们的数据。为此，NAS 和 SAN 的实现还必须提供必要的工具来实现数据的本地和远程复制。但这就要求刚刚“集中”的数据现在至少要分散在两个地点，这就带来了额外的安全需求。

1.4　追赶技术潮流

说起来可能会有争议，整个计算机技术的发展以及相关技术的进步似乎并没有什么明显的变化。例如，20 世纪 80 年代的标准 IBM PC/XT 计算机采用的是 4.77 MHz 主频的 8088 处理器、128 ~ 640 KB内存、10 ~ 20 MB 硬盘和一台单色显示器。而我们现在所使用的台式计算机采用的是 2.53 GHz 主频的处理器、3 GB 内存、120 GB 硬盘、AGP 图形卡以及各种附加的外部设备，只是它们的价格更令人望而生畏。我们可以利用一个简单的数学公式来描述这种增长现象。

在 20 世纪 80 年代，一台主频 4.77 MHz 的 PC 主机（不含显示器、图形卡、软驱和硬盘）的售价大约在 1200 美元左右。下面的算式表明，如果以这个价格为基础，那么，今天的系统价格将相当于 60 113 美元。

```
$ 1200/4.77 MHz = $ 25.58 per MHz
$ 25.58 × 2530 MHz = $ 60,113
```

如果制造商们以这样的价格来销售今天的计算机系统，那么，他们的销售量无论如何也不会达到目前的规模。

说明：尽管我们上面是采用处理器速度进行计算的，但如果我们改用内存空间、内存速度、硬盘容量或硬盘速度进行计算，最终的概念基本上仍是相同的。

在20世纪80年代和90年代，技术不仅一直都在进步，而且是以指数形式增长的。随着新的资源的不断出现，低级编程语言（如机器语言）的应用开发越来越少。高级语言编程意味着应用开发和测试时间的缩短，软件产品进入的市场速度更快。而这种软件开发周期的缩短又进一步加速了技术的进步。

人们把这种技术进步亲切地称之为“技术浪潮”。随着这种浪潮进入计算机技术领域，形形色色的计算机服务公司和咨询公司大量涌现。许多这样的公司实际上是在技术浪潮的后期进入市场的，但他们仍以专家自诩。正是这样一些“专家”以低廉的价格和劣质的服务搅乱着市场。许多企业在饱尝了这种服务之苦后，开始有意识地组建自己的技术服务队伍。对于企业系统的日常维护来说，利用自己的技术服务支持不失为一个好主意，但对于新技术和新应用的采用则并非那么理想。

说明：企业内部的技术人员经常会发现，企业的日常维护工作往往要优先于对新技术的跟踪。在这种情况下，一旦涉及诸如存储网络这样的问题，即使是技术能力很强、很有责任心的技术人员也很难做好充分准备。因此，对于一个企业来说，最好选拔自己的技术人员来进行此类系统的实施，而把系统的测试和认证工作委托给外面的专业公司来完成。

随着越来越多的应用被开发出来，人们不断地为这些应用寻找到新的用途，而新的应用开发需求也随之不断涌现。在这些应用中有一条共同的主线，那就是它们对于存储的需求：包括应用自身的安装、配置和管理所需的存储以及应用所创建、评估、管理和操作的数据存储等。在多数情况下，这些应用都是部署在它们自己的分布平台上的。

互联网的发展也为存储需求的增长起到了推波助澜的作用。对于.com公司而言，不管其最终是壮大或是倒闭，他们都会对存储有这样或那样的需求。事实上，对于许多基于互联网业务的企业来说，它们所能拥有的惟一资产就是数据。例如，某些互联网公司大量收集和整理各种有效的电子邮件地址并把它们销售给那些所谓的商人。为了使所销售的电子邮件更具吸引力，这些公司会想尽一切办法来收集电子邮件发信人的资料。对于这些企业来说，数据质量的重要性并不亚于数据本身的重要性，由此我们可以想像出此类企业对于存储的需求。

历史教会了人们许多东西。例如，互联网公司就从中悟出了“数据为王”的道理。谁拥有了最好的数据，谁就可能成为市场的主宰。

为此，企业都在不断地追求最好的数据，这就意味着它们的存储需求将继续不断地增长。但有时由于存储的增长速度过快，导致即使是在分层存储管理的情况下一些简单的数据存档的需求也很难满足。特别是像保险业那样需要频繁进行数据访问或要求数据具备快速响应性的应用更是如此。就目前的发展趋势看，存储需求的增长将无期限地持续下去。

但所有这些对于存储网络的爆炸性增长又有什么关系呢？

众多的制造商、分析家、咨询师和业界专家都在说，集中存储将是未来的发展方向。只有将存储资产尽可能地集中起来，它们才会更加安全，也更便于控制和管理。但作为常识来说，一旦这些存储资产集中起来，企业在灾害面前将会变得更加脆弱。但许多采用集中数据处理的企业往往会忽视这一现实，因为他们把这些数据当做企业的内部数据来考虑。

这里请记住一点，在数据安全的问题上，那些分析家、咨询师或是业界专家并不一定可靠，他们或许就是那些在技术浪潮后期才混入市场的冒牌专家。最好的办法是选择一家具备存储安全经验的知名企业，如果可能的话，还应聘请第三方对其资质进行认证。我们这样做似乎有滥杀无辜的嫌疑。但是，如果我们视数据为企业生命的话，谁又可能拿生命当儿戏呢？

为了让读者更直观地理解上述这些概念，我们将在下面两节中讲一段故事。故事的情节虽然是虚构的，但它在现实生活中也不是不可能发生的。

1.4.1　春风得意

我们假设你正担任着某大公司的 MIS 部经理。该公司的年营业额为 45 亿美元，其中 30% 的营业额来自网上销售，每年网上的交易量达到 45 000 000 笔。目前公司的基础系统采用分布式的数据结构平台（我们假设每台服务器都使用直接连接存储设备，当然，它也可以采用其他形式的分布结构）。鉴于当前系统环境的设计并考虑到 DAS 系统已经处于满负荷运行状态，所以，每当需要扩充存储空间的时候，我们除了需要添置存储设备之外，还需要添置新的服务器、网络操作系统（NOS）、存储子系统、磁带备份系统（以适应备份窗口的需要）、磁带备份软件、防病毒软件以及服务器的专用配套设备和管理软件（如远程访问设备和服务器监视软件等）。在采购了这些设备之后，我们还需要将它们集成到现有的系统环境中并进行必要的配置和测试。这是一项工作量很大的任务，即使是在一个自动化程度很高的系统环境下，它的费用增长速度也是相当快的，还不要说由此所带来的后期维护费用的增加。

为了避免这种重复性的费用投入，同时考虑到你的一个关系不错的设备厂家或咨询顾问一直在向你灌输集中存储是未来发展潮流的观念，你决定将你的数据进行集中管理。在经过一段时间的准备之后，你开始着手寻找满足企业需求的各种可能的技术。你向那家设备厂商或咨询顾问发出求助的信息，于是，各种备选方案如潮水般涌来。

设备供应商与你探讨各种设备的特点、选件、价格、可用性以及相关的安装和维护的问题。咨询顾问则与你讨论一些有关处理速度、供货能力、拓扑结构、兼容性、伸缩性、通用性、备份解决方案以及系统集成方面的问题。如果是一个不错的咨询顾问，他可能还会与你详细讨论有关系统的安全问题。在进行了这些准备工作之后，你现在可以着手制定自己的方案评估计划了。

你已经不止一次地参与过各种技术产品的评估工作，所以对此应该是轻车熟路。于是，你找出过去的一个评估计划作为参考，按照新的存储网络项目的需要加以修改。你工作得十分仔细，所有需要修改的地方、所有需要连接到存储网络的设备以及它们的相关数据都考虑了进去。在修改进行到一半的时候，你突然意识到应该将安全问题也纳入到新的计划中。于是，你又以过去的一份服务器的安全评估计划为蓝本，将相关的安全信息加入到项目计划中。为了确保系统的安全，你考虑最好能得到一些外部的帮助。于是，你又将你的计划发给了那家关系不错的设备供应商（毕竟过去曾与他们有过很好的合作经历），请他们帮助审核和修改。

当该设备供应商将计划返回后，你注意到其中又增加了几项安全方面的内容。现在看来一切都已经十分周密和完备，于是你决定按照这些条件着手方案评估工作。为了对评估问题的答案进行汇总，你准备了评估矩阵表并制定了具体的评分标准，以便对各种产品的优劣进行比较。

你与一家又一家的供应商、制造厂商和咨询商进行接触，逐一对他们进行评估，对他们的问题答案仔细进行分类，每个答案都按照事先制定的标准进行打分。最后，在经过汇总和比较

后,得分排在前面的四家厂商被筛选了出来。

接下来进入第二轮筛选工作。为了确保与现有系统环境的兼容性、可支持性以及易用性等,你再一次对评估准则和评估矩阵做了修改。随后,你逐一拜访了四家竞标厂商,观看他们的解决方案演示,并利用新的评估矩阵表对他们进行重新评估。按照企业当前的需求,结合每个厂家产品的特点、供货能力和进度、系统管理工具等要素,你最终确定 SAN 方案最符合公司的数据集中要求。

假定在价格的问题上不存在异议(这种情况是很少见的),于是你最终选择了 XYZ 公司的"隐形 SAN"产品。该公司不仅产品最接近你的技术要求,而且其设备和安装服务价格也很令人满意。你向该厂商发出了订单和安装条件,并将对培训和文档的要求纳入其中。至此,项目实施进入采购流程。

厂商在接到订单后,通知你设备将在数周后到达并初步确定了开始安装的日期。设备到货之后,安装工作按照计划展开。安装人员的工作十分出色,安装过程中只出现了几个小问题并且马上得到了解决。需要访问 SAN 的每一台设备都逐一进行了设置、连接和测试。用于系统配置和管理的工具软件也进行了安装调试。按照合同订单的要求,厂商不仅提供了相应的培训、系统文挡和维护资料,而且还按照系统验收标准的要求,以文件形式提交了有关系统安全的认证报告和说明。你与属下一起对整个安装过程进行了审核,并确认你的人员已经接受了所有必要的培训,接收了相关的文档。最后,全体人员集体通过了系统的安装验收。现在,我们要向你表示祝贺,祝贺你拥有了新的 SAN 系统。整个系统的实施不仅按时完成,而且所花费用还略低于整个项目的预算。

你是不是该准备一下本年度优秀员工的演讲稿了?你可不要高兴得太早!

1.4.2 如临深渊

公司 CEO、高层领导以及董事会对你的工作给予了充分的肯定。不管怎么讲,对于一个企业来说,SAN 也是一项投资很大的项目,而你不仅按时完成了任务,而且还节省了预算。一切似乎都进展得十分顺利,直到有一天你接到一个 CEO 打来的电话。CEO 告诉你他刚刚接到某个股东的电话,公司的某个竞争对手收到了一封电子邮件,该邮件附带有公司的一些保密数据,其中有公司的客户记录,包括客户的采购习惯、发票要求、支付方式,甚至客户的信用卡资料。CEO 希望你尽快找出他们取得这些信息的原因(请记住,面对这种严重的情况,CEO 是不可能以平静的语气向你下达这样的任务的)。你马上召集你的下属,并邀请了一位安全专家一起来研究造成这一事故的原因。

商业的第一原则就是及时制止损失。但在目前的状况下,你既不知道问题出在哪里,也不知道它产生的原因,你所能采取的惟一行动就是关闭与这些数据相关的服务器。当然,这也就意味着系统的停机。事实上,对于这样一种严重的情况,你少不了要与 CEO 进行磋商,这对于任何人来说都不会是一件轻松的事情。

接下来就是要确定一种最好的方法来寻找产生问题的根源。在安全专家的帮助下,你开始着手制定详细的行动计划。你准备对所有可能涉及相关信息的系统日志进行检查,由于需要查找的日志量非常大,整个过程可能需要耗费数周的时间。

在对系统日志进行检查的同时,你还必须确认是否有特定的账户访问过被窃取的信息,如