数据安全项目案例

存储与备份　SAN与NAS　容错与容灾

康春荣　苏武荣　主编

科学出版社
www.sciencep.com

数据安全项目案例

存储与备份　SAN与NAS　容错与容灾

康春荣　苏武荣　主编

科学出版社

北京

内 容 简 介

本书对计算机系统中数据的安全和保护进行了全面的阐述，内容涉及当前计算机系统在数据安全方面存在的隐患、与数据安全有关的必备知识、计算机系统数据的高可用性存储、系统数据的备份与智能恢复、计算机系统数据的安全部署、当前数据安全流行的解决方案、数据安全防护的高级技巧、计算机系统数据安全管理等。本书内容除了小部分入门的知识之外，大部分素材取自作者的工作日志，内容丰富，与当前流行的数据安全的技术环环相扣，在实用性、知识性、技巧性等方面的表现十分突出。书中还列出了许多具体的数据安全解决方案和成功案例。

本书可作为计算机数据安全工作者、IT 主管、计算管理员的培训教材，也可作为计算机系统集成从业人员的参考手册。

图书在版编目（CIP）数据

数据安全项目案例：存储与备份 SAN 与 NAS 容错与容灾/康春荣，苏武荣主编. —北京：科学出版社，2004

ISBN 7-03-013612-8

Ⅰ.数… Ⅱ.①康…②苏… Ⅲ.电子计算机-数据管理-安全技术 Ⅳ.TP309.2

中国版本图书馆 CIP 数据核字（2004）第 053778 号

策划编辑：李 娜/责任编辑：丁 波

责任印制：吕春珉/封面设计：飞天创意

科学出版社 出版

北京东黄城根北街16号

邮政编码:100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004 年 7 月第 一 版 开本：787×1092 1/16

2004 年 7 月第一次印刷 印张：19 1/2

印数：1—4 000 字数：446 000

定价：32.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

内 容 简 介

本书对计算机系统中数据的安全和保护进行了全面的阐述，内容涉及当前计算机系统在数据安全方面存在的隐患、与数据安全有关的必备知识、计算机系统数据的高可用性存储、系统数据的备份与智能恢复、计算机系统数据的安全部署、当前数据安全流行的解决方案、数据安全防护的高级技巧、计算机系统数据安全管理等。本书内容除了小部分入门的知识之外，大部分素材取自作者的工作日志，内容丰富，与当前流行的数据安全的技术环环相扣，在实用性、知识性、技巧性等方面的表现十分突出。书中还列出了许多具体的数据安全解决方案和成功案例。

本书可作为计算机数据安全工作者、IT 主管、计算管理员的培训教材，也可作为计算机系统集成从业人员的参考手册。

图书在版编目（CIP）数据

数据安全项目案例：存储与备份 SAN 与 NAS 容错与容灾/康春荣，苏武荣主编. —北京：科学出版社，2004

ISBN 7-03-013612-8

Ⅰ.数… Ⅱ.①康…②苏… Ⅲ.电子计算机-数据管理-安全技术 Ⅳ.TP309.2

中国版本图书馆 CIP 数据核字（2004）第 053778 号

策划编辑：李 娜/责任编辑：丁 波

责任印制：吕春珉/封面设计：飞天创意

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

双青印刷厂 印刷

科学出版社发行 各地新华书店经销

*

2004 年 7 月第 一 版 开本：787×1092 1/16

2004 年 7 月第一次印刷 印张：19 1/2

印数：1—4 000 字数：446 000

定价：32.00 元

（如有印装质量问题，我社负责调换〈环伟〉）

前　言

随着计算机和网络等信息技术的飞速发展，近年来在世界范围内掀起了兴建网络环境、传播数据信息的热潮，许多单位的信息化程度越来越高。

在网络应用日益普及的今天，数据悄然成为信息应用的核心，而且已经成为每个单位非常关键的，甚至是最重要的因素。

对于数据的重要性，人们应有以下简单的理解：

- 数据在网络应用中的地位

  ——没有数据的系统，计算机和网络就没有存在的意义。

  ——数据不完整或不可用的系统，计算机和网络仅仅是摆设。

- 数据对 IT 部门领导及员工的意义

  ——网络应用数据的丢失与否将决定领导和员工的职业稳定。

  ——网络数据的可用性优劣将决定领导和员工的业绩和职位的正确评定。

上述对数据的重要性的形象理解显示了一个最简单不过的道理：用户在为计算机系统投入价格不菲的投资后，最终会意识到最为宝贵的财富就是数据，要保证业务的持续运作和成功，就要保护基于计算机的信息。系统中断、信息的泄密、丢失、篡改、毁坏、盗用、意外的天灾人祸等对所有的用户来说都是一种灾难。加大保护数据安全的力度已经成为越来越多用户的共识。

人为的错误、硬盘的损毁、计算机病毒、自然灾难等都有可能造成数据的丢失，给用户造成不可估量的损失。系统数据丢失会导致系统文件、交易资料、客户资料、技术文件、财务账目的丢失，业务将难以正常进行。这时，最关键的问题在于如何尽快恢复计算机系统，使其能正常运行。随着计算机存储信息量的不断增长，对数据稳定的、可靠的和高速的存储，也与数据的安全一样日益成为人们所关注的话题。

由此可见，计算机系统运行的稳定性、连续性及数据安全性是直接关系到用户命运的头等大事。一旦管理或服务系统中断运行，将给整个单位工作的运行带来极大的混乱；而数据一旦丢失，带来的后果（损失）将是灾难性的。

因此，如何确保数据的安全，如何保证计算机系统的连续稳定运行，就成为领导和系统管理人员最关心的问题。而为数据构筑一个有效的存储系统、完整的安全策略以及有效的使用环境是每一个网络的建设者和管理者今天必须考虑的问题，这也是本书的主要关注点。

全书共分为 4 篇，第 1 篇是基础篇，包括第 1～6 章，主要介绍了存储技术、备份技术、双机容错和集群、NAS 与 SAN 等内容；第 2 篇是案例篇，包括第 7～11 章，主要介绍了数据备份、集群容错、NAS 网络存储、异地容灾 SAN 构建等案例；第 3 篇是实战篇，包括第 12～15 章，主要介绍了数据备份和灾难恢复、容错部署、NAS 存储部署等实战案例；第 4 篇是提高篇，包括第 16～17 章，主要介绍了数据安全技巧和数据安全保障等方面的知识。

本书由康春荣、苏武荣主编，参与编写的有康春荣、童丽如、余绍旺、黄健民、刘育琳、杨海燕、李明辉、游明基、陈建平、李初等人。本书作者都是多年从事计算机系统安全管理与 Internet 开发应用的人员，他们的经验融于本书中，一定能带给读者可借鉴的网络安全知识和技能。

由于作者水平有限，加之该领域的技术发展日新月异，书中不妥之处在所难免，希望广大读者批评指正。

作　者

目　录

第 1 篇　基础篇

第 2 篇 案例篇

第 3 篇 实战篇

第 4 篇　提高篇

第 1 篇

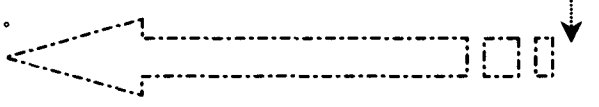
基础篇

本篇主要论述了数据安全的基本知识，如数据的重要性、常规保护措施、数据存储与备份、异地容灾、NAS 与 SAN 等。本篇的结尾还对当前数据安全的发展趋势进行了全面的论述。

对于初学者，掌握本篇的内容可以为以后进一步学习数据安全方面的知识打下坚实的基础；对于已经有一定基础的读者，可以从本篇的内容获益匪浅；而对于数据安全的基本知识已经熟悉的读者也可以跳过本篇内容，直接从第 2 篇开始学习。

本篇的主要内容有：

- 数据安全——一个不容忽视的话题。
- 存储技术快速入门。
- 备份技术快速入门。
- 双机容错和集群。
- NAS 与 SAN。
- 数据安全的“新式武器”。



第1章

数据安全——一个不容忽视的话题

1.1 信 息 安 全

在当今的信息社会，信息技术的发展令人目不暇接。计算机信息主要以数字化形式表现，并存在于每一个二进制数据位中，它在当今社会中扮演着至关重要的角色。随着计算机网络和信息技术的高速发展，数字化信息的快速传递、低成本复制和重复使用等特点，给人们工作和生活带来了很大便捷和好处。

1.1.1 直面信息安全

任何事情都有双面性，计算机信息技术也一样。当人们使用计算机技术提高工作效率、为社会创造更多财富的时候，也有一些人用它做着不道德的事情。他们利用掌握的计算机技术手段非法入侵他人的计算机系统，窃取、篡改、毁坏重要的信息数据，给社会造成难以估量的损失，同时也为信息技术在更广泛领域的应用设定了障碍。即便是在非恶意的情况下，由于组织机构管理的要求，机构间及人员间交流的要求，甚至个人隐私要求等，都要求从技术上保障对应信息只能由有对应权限的本人才能完整保密地获得与使用。因此，信息本身的保密性、完整性、不可否认性以及信息来源与去向的真实性在数字化世界里都显得尤为重要。

随着数字化信息社会的发展，无论是企业管理、日常办公或商务往来，甚至人与人之间的交往等的各个方面都需要信息安全技术的保障。研究数字化信息安全，必须从分析数字化信息社会所依靠的基本技术着手。在早期的计算机发展过程中，信息安全并未得到充分重视，或者说考虑的重点不是针对现在意义的信息安全。20 世纪 90 年代末，计算机发展中由于兼容性的要求，计算机的安全性一直没有完善起来，一方面，由于近年来流行个人计算机的开放性设计，几乎每个人都能知道计算机操作系统的内部结构和工作原理，极易找到攻击漏洞，在 Internet 流行的时代，通过个人计算机在与他人的通信过程中，信息安全问题便充分暴露了出来，且日益严峻，此外，目前使用最广泛的网络协议是 TCP/IP 协议，它的主要设计目标是互联与互通，而不是安全，该协议中已有许多人所共知的安全漏洞和隐患；另一方面，由于软件设计方法本身的发展水平所限，设计人员无法在软件设计过程中考虑到计算机安全的所有方面，从而出现了一些软件公司频频发布安全隐患的补丁，以急堵漏洞的现象。

社会的信息化过程，对计算机的安全又提出了越来越多的新要求，其主要的信息安全问题和需求表现在：权限分工不明、无法确认网络上人员的身份、无法确定收到的消息的可信性、无法防止对所收/发信息的事后抵赖、无法防止篡改信息等方面。

总之，计算机应用的蓬勃发展使我们不得不面对信息安全问题。信息安全技术正逐渐得到越来越多人们的认知。正确掌握信息安全技术并在实践中加以应用，将使人类社会受益匪浅。

1.1.2 信息安全的两个基点

信息安全范围广泛，涉及计算机应用的方方面面。不过，归纳起来，系统安全和数据安全可以称得上是信息安全的两个基点。

1. 系统安全

系统安全确保整个网络系统的安全，使用有效的防范措施和维护措施来阻止或清除带给系统不安全的因素，使得系统成为某种程度上的安全系统，从而保证计算机信息的安全。

系统安全的重点在于防。系统安全基本是一种被动的防范措施，主要是堵塞系统的各种漏洞，限制用户权限，防止非法用户对系统进行破坏和数据窃取。

系统安全保护办法就像修建高高的大堤，堵截防止洪水的袭击。由于原有计算机技术基础有缺陷，同时随着攻击手段的提高，防护“大堤”必须修得越来越高。就这样，还不时发现有新的漏洞，必须不停地堵住所有可能发生危险的小漏洞。否则，一旦被攻击者攻入，得到系统管理员权限，就会导致整个系统的崩溃。

因此，它只能维持危险的现状或拖长危险蔓延的时间，不能从根本上预防或根除危险所在。尽管如此，系统安全在实际应用中也是必不可少的。

系统安全一般采用防火墙（Firewall）、病毒防范、审计防范、入侵检测、漏洞扫描等措施。其中，防火墙、病毒防范和入侵检测就是比较典型和常用的系统防护技术。

（1）防火墙

防火墙是用来防止非法用户和数据进出的一种安全防范措施，是在被保护网络和其他网络之间限制访问的一种设备。它可针对各种应用单独设定，使用灵活，适用于与外网相连的场合。

但是，防火墙存在着安全性较低、适用范围窄、过滤规则是静态的、过滤规则的维护与测试十分复杂、无法进行电子数字签名和身份鉴别等缺点。

防火墙只是保障网络安全的一种必要条件，但绝非充分条件。必须结合其他相关的网络安全产品，如入侵检测产品、漏洞扫描产品、身份认证产品等，才能构成网络安全的综合解决方案。

（2）病毒防范

Internet 正在普及和高速发展，伴随而来的是计算机病毒的泛滥。如每年的 CIH 病毒日、尼姆达（NIMDA）病毒、求职者病毒、冲击波病毒等。各种层出不穷的新病毒和各种恶意代码使人们的工作受到严重影响。计算机病毒的发作往往给受害者造成巨大损失，计算机病毒问题正在成为个人、企业、单位、社会日益关注的问题。如何有效地防范网络病毒，已经成为众多用户所关心的话题。

网络系统与外界的接触，很难杜绝受到计算机病毒的感染。计算机病毒的破坏性程

度是不可预测的，恶性病毒可能会使系统全部瘫痪，就像几年前流行的CIH病毒、红色代码等，所以，计算机病毒的预防和查杀是相当重要的。必须制定一个功能强大，且多层次的反病毒方案，应用有效的病毒防治软件，来预防网络病毒的危害。

通常对病毒防范是选用主流的网络防病毒产品。一般网络防病毒产品都有完整的解决方案，有企业网络个人计算机防毒系统、服务器防毒系统、电子邮件服务器防毒系统等，有些网络防病毒产品还有Internet网关防毒系统和统一的防毒中央控制系统等。

通过在网络上部署防毒解决方案，用户的信息系统（包括重要应用服务器）都提高了抵御病毒侵害的能力，并且还将信息处的工作人员从繁重的日常维护工作中解放出来，使他们把更多的时间和资源投入到业务中。

（3）入侵检测

入侵是指非授权用户试图进入或者滥用用户的系统。其中的“滥用”涉及的范围很广泛，包括从偷窃机密数据，到一些次要的事情，比如滥用用户的电子邮件系统发垃圾邮件。

入侵检测技术是为保证计算机系统的安全而设计与配置的一种能够及时发现并报告系统中未授权或异常现象的技术，是一种用于检测计算机网络中违反安全策略行为的技术。入侵检测系统（Intrusion Detective System，IDS）可以实时监控和检测网络或系统的活动状态，一旦发现网络中的可疑行为或恶意攻击，入侵检测系统可做出及时的报警和响应，甚至可以调整防火墙的配置策略，与其进行联动。

入侵检测系统可以分为基于网络数据包分析和基于主机分析两种基本方式。简单地说，前者就是在网络通信中寻找符合网络入侵模板的数据包，并立即反应；后者是宿主系统审计日志文件，寻找攻击特征，然后给出统计分析报告。它们各有优缺点，互为补充。

网络的动态变化及复杂性使人们对安全风险的控制有了更高的要求，而以入侵检测为基础建立起来的检测和响应基础设施（Detection Response Infrastructure，DRI）是对安全风险进行动态控制和有效管理的最好方法，入侵检测已成为网络安全的基础设施。

2. 数据安全

数据安全有两个方面的内容：一是数据本身的安全，主要是指采用现代密码算法对数据进行主动保护，如数据保密、数据完整性、数据不可否认、双向强身份认证等；二是数据防护的安全，主要是指采用现代信息存储手段对数据进行主动防护，如通过磁盘阵列、数据备份、异地容灾等手段保证数据的安全。

数据安全是一种主动的保护措施。如筑堤防洪，采用系统安全是建大堤堵截洪水，数据安全可以比喻为是抬高了要保护地段的整个标高高度，使洪水无法流入，即使流入，也不能产生大的危害。

数据防护的安全是本书要论述的重点，以后各章节对其有非常详细的介绍，这里只对数据本身的安全进行简单的介绍。

数据本身的安全必须基于可靠的加密算法与安全体系，通常主要有对称算法与公开密钥密码体系两种。