网络安全 – 安全恢复技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

上周回顾

1. 计算机病毒的定义和特征

2. 引导区病毒，文件型病毒，混合型病毒

3. 阐述病毒检测的主要技术

网络灾难

安全恢复的条件

安全恢复的实现

网络灾难

安全恢复的条件

安全恢复的实现

网络灾难 - 1

定义

- 灾难：导致信息系统丧失技术服务能力的事件

自然灾难

- 地震，龙卷风，火灾，洪水，飓风等

人为灾难

- 爆炸，停电，应用系统故障，硬件失效，黑客攻击、分布式拒绝攻击以及病毒攻击，人为破坏等

网络灾难 - 2

网络灾难

- **通信介质、路由器、交换机、服务器等**
- **数据、可靠、信任等**

预防

- **阻止灾难的发生**
- **减小灾难所可能造成的危害**

网络灾难 - 3

灾难恢复

- **灾难恢复技术，也称为业务连续性技术，是对偶然事件的预防计划**
- **通过灾难恢复可有效预防可能出现的数据丢失、感染病毒等问题**

网络灾难 - 4

灾难恢复

- **它能够为重要的计算机系统提供在各种意外事故发生时， 保持持续运行的能力**
- **包括各种备份技术、现场恢复技术等**

网络灾难 - 5

灾难恢复

- **风险评估**
  - **信息安全、业务风险评估**
- **应急措施**
- **数据备份**
- **病毒预防**

网络灾难 - 6

风险评估

- 风险评估需要对信息基础设施运作时存在的风险、系统漏洞对业务活动的影响作出完整的评估
- 包括物理的、环境的、管理的以及技术措施等因素
- 信息安全风险评估、业务风险评估

网络灾难

安全恢复的条件

安全恢复的实现

安全备份的例子

1993年，美国纽约世贸中心大楼发生爆炸，1年后，350加原本在该楼工作的公司只剩150家。其他企业由于数据丢失无法找回，影响业务运行。

2001年美国世贸中心遭受恐怖分子袭击，世贸中心主顾之一，摩根斯坦利并没有遭受数据丢失重大损失

- 远程防灾系统，实时备份，保障公司正常运营

安全备份的误区

用拷贝来代替备份

- **备份等于拷贝加管理**

冗余系统代替备份

只备份数据

- **恢复时如需安全操作系统，需要相当长时间，需要对网络备份**

安全恢复的条件 – 区别

备份与拷贝

- **计划与自动化**

备份与系统冗余

- **系统冗余可以提高系统可用性，但对于人为破坏、恶意攻击、病毒等缺乏保护能力**

安全恢复的条件 - 数据备份与网络系统备份

硬件备份与软件备份相结合

- **硬件容错与存储备份系统**

要求

- **不间断备份**
- **自动/定时备份**
- **自动恢复**

安全恢复的条件 - 网络系统备份

网络数据冷备份

- 将整个网络系统及数据完整备份到存储设备
- 优点
  - 备份介质成本低廉
  - 备份容量巨大
  - 可靠、稳定

安全恢复的条件 - 网络系统备份

网络数据热备份

- 将整个网络系统在两个硬件环境中同时运行。
- 发生问题时，由监控系统切换
- 优点
  - 全自动运行、不间断业务
  - 易于隔离、取证
  - 可以从容修复

安全恢复的条件

备份设备

	硬盘技术	光盘技术	磁带技术
存取速度	快	较快	较慢
备份成本	成本最高，用于在线数据的存储	成本较高，用于数据的运载与文的永久归档。	成本最低，不适于在线备份。
可管理性	由于硬盘的故障发生率较高，不能完全满足要求。	由于光盘是通过拷贝命令来获得系统中的数据，因此无法获得网络系统的完全备份。其次，光盘也难以备份正在使用中的文件。	可对整个系统进行备份。易于保存

存储区域网络技术 - 什么是SAN？

SAN是英文Storage Area Network的缩写，通常译为“存储区域网络”，它是一种在服务器和外部存储资源或独立的存储资源之间实现高速可靠访问的专用网络。

SAN 采用可扩展的网络拓扑结构连接服务器和存储设备，每个存储设备不隶属于任何一台服务器，所有的存储设备都可以在全部的网络服务器之间作为对等资源共享。

SAN备份方式（就数据移动方式而言）

LAN-Based备份方式

LAN-Free备份方式

Server-Free备份方式

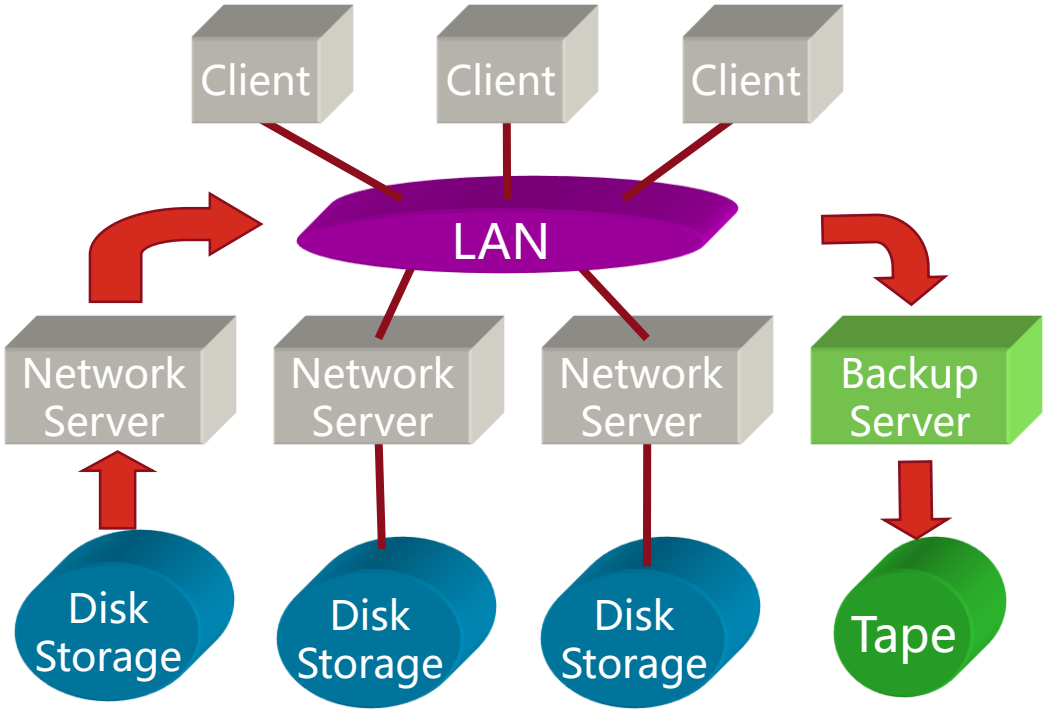
LAN-Based备份 - 1

LAN-Based备份，在该系统中数据的传输是以网络为基础的。其中配置一台服务器作为备份服务器，由它负责整个系统的备份操作。

磁带库则接在某台服务器上，在数据备份时备份对象把数据通过网络传输到磁带库中实现备份的。

LAN-Based备份结构的优点是节省投资、磁带库共享、集中备份管理；它的缺点是对网络传输压力大。

LAN-Based备份 - 2



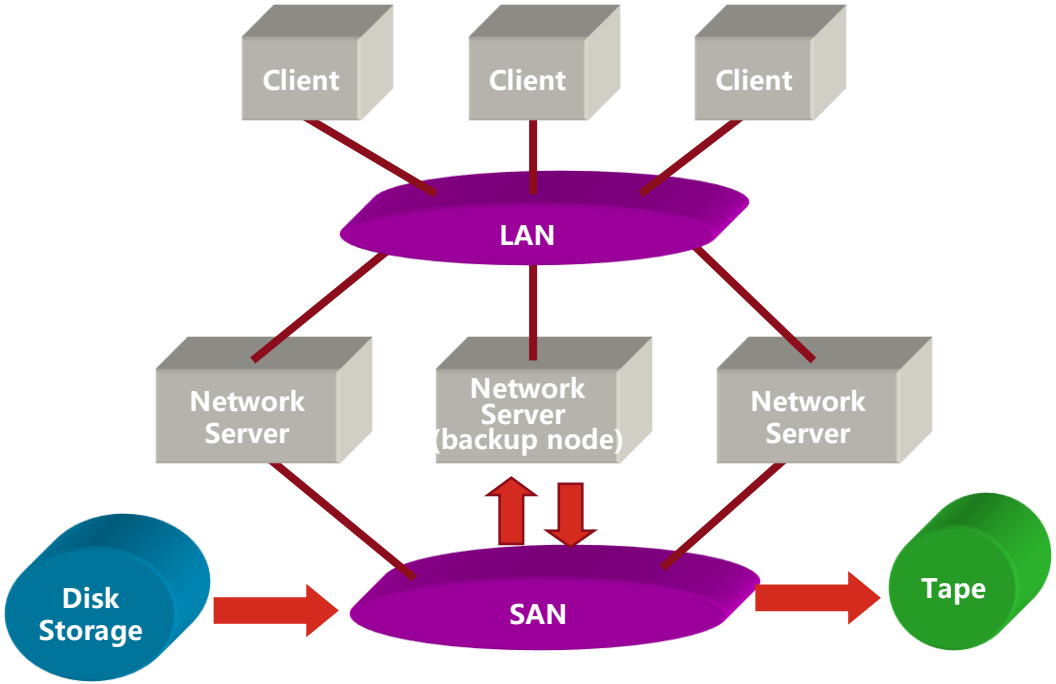
LAN-Free备份方式 - 1

由于数据通过LAN传播，当需要备份的数据量较大，备份时间窗口紧张时，网络容易发生堵塞。在SAN环境下，可采用存储网络的LAN-Free备份，需要备份的服务器通过SAN连接到磁带机上，在LAN-Free备份客户端软件的触发下，读取需要备份的数据，通过SAN备份到共享的磁带机。

这种独立网络不仅可以使 LAN 流量得以转移，而且它的运转所需的CPU 资源低于 LAN 方式，这是因为光纤通道连接不需要经过服务器的 TCP/IP 栈。

有别于传统通过LAN链路的备份方式,这样可以不占用以太网络的带宽

LAN-Free备份方式 - 2



LAN-free备份不足之处

首先，它仍旧让服务器参与了将备份数据从一个存储设备转移到另一个存储设备的过程，在一定程度上占用了宝贵的CPU处理时间和服务器内存。

还有一个问题是，LAN-free技术的恢复能力差强人意，它非常依赖用户的应用。许多产品**并不支持文件级或目录级恢复**，映像级恢复就变得较为常见。映像级恢复就是把整个映像从磁带拷回到磁盘上，如果您需要快速恢复某一个文件，整个操作将变得非常麻烦。

此外，不同厂商实施的LAN-free机制各不相同，这还会导致备份过程所需的系统之间出现**兼容性**问题。

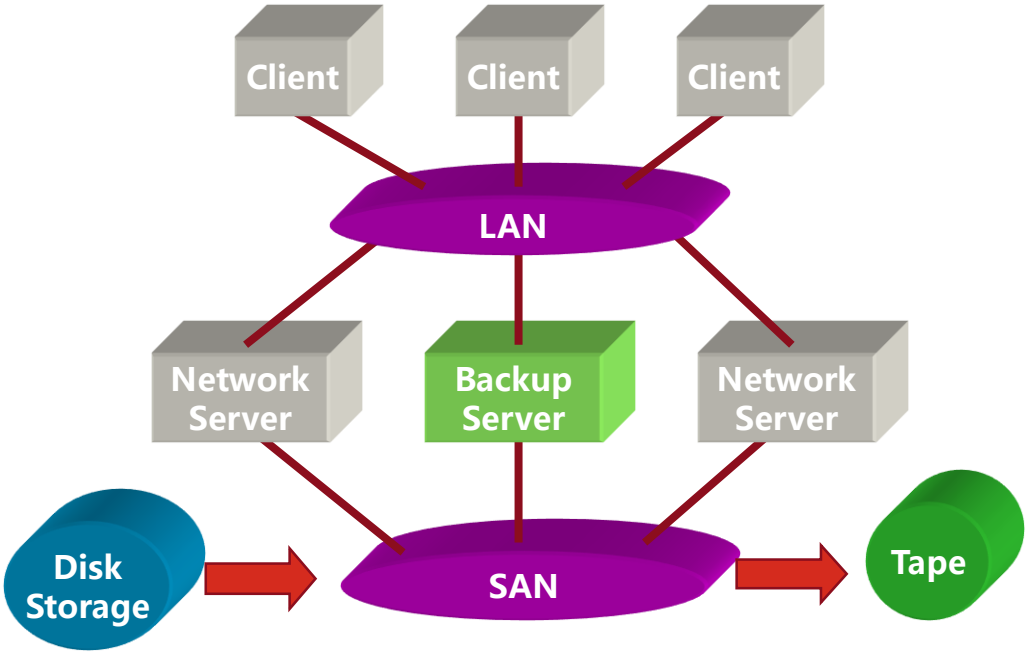
无服务备份 - 1

免服务器的备份和恢复是数据直接在存储设备之间传输，备份过程能够在SAN内部完成，无需服务器干预

提高了备份和恢复速度，缩短了应用主机的CPU周期，释放出的宝贵的CPU周期可用来提高操作的效率并增加工作量。

这种方式是在LAN-free的基础上的进一步改进，克服了LAN-free备份需要服务器参与的问题，从而全面释放网络和服务器资源。

无服务备份 - 2


Client
Client
Client
LAN
Network Server
Backup Server
Network Server
Disk Storage
SAN
Tape

无服务器备份的优势

无服务器备份与LAN-free备份有着诸多相似的优点

- **如果是无服务器备份，源设备、目的设备以及SAN设备是数据通道的主要部件。虽然服务器仍参与备份过程，但负担大大减轻，因为它的作用基本上类似交警，只用于指挥，不用于装载和运输，不是主要的备份数据通道。**

无服务器备份技术具有缩短备份及恢复所用时间的优点

- **因为备份过程在专用高速存储网络上进行，而且决定吞吐量的是存储设备的速度，而不是服务器的处理能力，所以系统性能将大为提升。**

无服务器备份的缺点

虽然服务器的负担大为减轻，但仍需要备份应用软件（以及其主机服务器）来控制备份过程。

元数据必须记录在备份软件的数据库上，这仍需要占用CPU资源。

与LAN-free一样，无服务器备份可能会导致上面提到的同样类型的兼容性问题。而且，无服务器备份可能难度大、成本高。最后，如果无服务器备份的应用要更广泛，恢复功能方面还有待更大改进。

对比

目前主流的备份软件，如IBM Tivoli 、Veritas，均支持上述三种备份方案。

- LAN备份数据量最小，对服务器资源占用最多，成本最低
- LAN free备份数据量大一些，对服务器资源占用小一些，成本高一些
- SAN Server-free备份方案能够在短时间备份大量数据，对服务器资源占用最少，但成本最高

安全恢复的条件 – 容灾系统

为计算机信息系统提供的一个能应付各种灾难（火灾、水灾、地震、战争等不可抗拒的灾难和意外）的环境

数据容灾

- 当计算机在遭受灾害时，容灾系统将保证用户数据的安全性

应用容灾

- 提供不间断的应用服务
- 数据异地 – 数据系统
- 应用异地 – 应用系统

网络灾难

安全恢复的条件

安全恢复的实现

安全恢复的实现 – 安全恢复方法

设定容灾目标

- **考虑各种以外情况、恢复目标**

了解拥有的资源

- **人力、设备、工具、数据等**

制定工作计划

- **备份与恢复**

安全恢复的实现 – 安全恢复计划

安全恢复计划是指当一个机构的计算机网络系统受到灾难性打击或破坏时，对网络系统进行安全恢复所需要的工作过程

主要考虑的问题

- **如何以最快的速度对网络进行恢复**
- **如何将灾难所带来的损失降低到最小**

安全恢复的实现 – 数据备份

完全备份

- **完全备份就是对服务器上的所有文件完全进行归档**

增量备份

- **只把最近新生成的或者新修改的文件拷贝到备份设备上**

差异备份

- **对上次备份后所有发生改变的文件都进行备份(包括删除文件的信息)**

安全恢复的实现 – 安全风险分析

安全风险分析

- **天灾人祸、恶意代码的传入、未经授权发送或访问信息、拒绝接受数据源以及拒绝服务连接等**

导致结果

- **系统可能会丧失信息的完整性、信息的真实性、信息的机密性、服务的可靠性以及交易的责任性等**

什么面临风险？为什么出现问题？可能性多少？

安全恢复的实现 – 安全风险评估

所谓安全风险评估，就是判断维护信息基础设施的安全状况的能力

步骤

- **评定价值**
- **评估威胁（原因、目标）**
- **评估缺陷（弱点）**
- **核实现有安全保障体系（是否已包括必要内容）**
- **评估风险、制定对策**

安全恢复的实现 – 安全恢复过程

确定恢复顺序

确定恢复所需的网络、设备和数据

采用逐步恢复的原则

注意被恢复部分之间的关联关系

安全恢复的实现 - 安全恢复注意事项

恢复文本

测试恢复计划

维护恢复计划

课后习题

1. 比较硬盘、光盘、和磁带三种备份技术,为什么磁带技术才真正适合于备份领域?

2. 什么是容灾系统?

3. 三种备份文件的方法及区别

谢谢!