第七章 网络操作系统与应用服务器配置

7.1 网络操作系统

7.1.1 网络操作系统的基本概念

1. 网络操作系统的功能

网络操作系统应提供单机操作系统的各项功能，除此之外还应具有以下功能：

（1） 网络通信
（2） 共享资源管理
（3） 网络管理
（4） 网络服务
（5） 互操作
（6） 提供网络接口

2. 网络操作系统的特征

NOS 除具备单机操作系统的 4 大特征：并发、资源共享、虚拟和异步性之外，还引入

（1） 开放性
（2） 一致性
（3） 透明性

3. 网络操作系统的安全性

（1）用户帐号安全性
（2）时间限制
（3）站点限制
（4）磁盘空间限制
（5）传输介质的安全性
（6）加密
（7）审计

4. 网络操作系统与 OSI/RM

NOS 主要包换（1）网络驱动程序（2）网络协议软件（3）应用程序接口软件

7.1.2 Windows Server 2003 操作系统

1. WS2003 的主要特点：可靠性、高效性、实用性、经济性
2. WS2003 的新增功能：

（1）配置流程向导
（2）终端服务器——远程桌面连接
（3）Internet 信息服务 6.0
（4）简单的邮件服务器
（5）流媒体服务器 WMS9
（6）系统关闭事件跟踪

7.1.3 Linux 操作系统简介

7.2 网络操作系统的基本配置

7.2.1 Window Server 2003 本地用户与组

用户组可分成：全局组（可以通行所有域的组）、本地组、特殊组

表 7-1　用户权限描述

名　称	权 限 描 述
Administrators	管理员对计算机/域有不受限制的完全访问权
Backup Operators	备份操作员为了备份或还原文件可以替代安全限制
Guests	按默认值，来宾跟用户组的成员有同等访问权，但来宾账户的限制更多
HelpServicesGroup	帮助和支持中心组
Network Configuration Operators	此组中的成员有部分管理权限来管理网络功能的配置
Performance Log Users	此组的成员可以远程访问以计划此计算机上性能计数器的日志
Performance Monitor Users	此组的成员可以远程访问以监视此计算机
Power Users	高级用户（Power Users）拥有大部分管理权限，但也有限制。因此，高级用户可以运行经过验证的应用程序，也可以运行旧版应用程序
Print Operators	成员可以管理域打印机
Remote Desktop Users	此组中的成员被授予远程登录的权限
Replicator	支持域中的文件复制
TelnetClients	本组的成员可以访问此系统上的 Telnet 服务器
Users	用户无法进行有意或无意的改动。因此，用户可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序

7.2.2 Windows Server 2003 活动目录

活动目录服务（Active Directory Service）采用基于 LDAP（Light Directory Access Protocol，轻型目录访问协议）格式的系统设计，包抱两方面：

（1）　目录（Directory）

（2）　目录服务（Directory Service）

1. 对象
2. 架构（Schema）
3. 目录结构
4. 逻辑单元

   Windows 2000 的活动目录逻辑单元包括组织单元（OU）、域（Domain）、域树（Tree）和域森林（Forest）
5. 信任关系

   域间的信任关系分为：

   • 单向信任：域 A（施信域）信任域 B（受信域），但域 B 不信任域 A

   • 双向信任

   • 可传递信任：延伸到一个域的信任关系也自动延伸到该域所信任的任何一个域上

   • 不可传递信任：信任关系只限于施信域和受信域两个域，并且默认单向信任

活动目录中物理结构与逻辑结构是彼此独立的两个概念，物理结构分为：

（1）　站点（Site）

（2）　域控制器

（3）　操作主机

　　按照功能可以划分为 5 个功能角色：架构主机、域名主机、相对 ID 主机、主域控制器住址程序和基础主机

（4）　多主域复制

7.2.3 Windows Server 2003 文件服务器

7.2.4 Windows Server 2003 终端服务

1. 终端服务的安装
2. 终端服务的配置与管理

1）赋予用户权限

2）终端服务高级配置

（1）更改加密级别

（2）允许用户自动登录到服务器

（3）配置终端服务超时和重新连接功能

（4）管理远程控制

7.2.5 Windows Server 2003 远程管理

1. Windows Server 2003 远程管理功能改进

（1）管理远程桌面

（2）远程协助

（3）远程管理的 Web 界面（仅限于 Windows Server 2003 Web Edition 版本）

（4）远程安装服务的改进功能

2. Microsoft 管理控制台（MMC）

3.远程桌面连接

7.2.6 Linux 网络配置

1. 网络配置文件

（1）/etc/sysconfig/network 文件：用来指定服务器上的网络配置信息的文件

（2）/etc/hostname 文件：包含了 Linux 系统的主机名称

（3）/etc/hosts 文件：包含了 IP 地址和主机名之间的映射

重新启动网络：[root@localhost]#/etc/rc.d/init.d/network restart

（4）/etc/host.conf 文件：指定如何解析主机域名。下为 Red Hat Linux 默认内容：

order hosts,bind

multi on

（5）/etc/resolv.conf 文件：配置 DNS 客户，包含主机的域名搜索顺序和 DNS 服务器的地址，例：

Search mydomain.edu.cn

nameserver 210.34.0.14

nameserver 210.34.0.13

（6）/etc/rc.d/init.d/network 文件：Linux 系统可以通过直接编辑此文件内容进行网络主机地址、子网掩码和网关等参数的配置，例：

IPADDR=192.168.0.100

NETMASK=255.255.255.0

BROADCAST=192.168.0.255

GATEWAY=192.168.0.1

2. 安装网卡

（1）设置网上模式，还必须了解网上的 I/O 地址和 IRQ 号

（2）配置网络内核

3. 网络配置命令

（1）网络接口设置命令 ifconfig，基本格式：ifconfig Interface-name ip-address up|down

（2）配置路由命令 route，基本格式：route[-选项]

常用对数和选项说明如下：

- del:删除一个路由表项
- add:增加一个路由表项
  - target:配置的目的网段或者生机。可以是 IP，或者是网络或主机名
  - netmask Nm:用来指明要添加的路由表项的子网掩码
  - gw Gw:任何通往目的地的 IP 分组都要通过这个网关

（3） 网络测试命令 ping

- -t:校验与指定的计算机的连接，直到用户中断
- -a:将地址解析为计算机名
- -n count:发送由 count 指定数量的 ECHO 报文，在发送指定数目（默认 4）的包后停止
- -l length:发送包含由 length 指定数据长度的 ECHO 报文
- -I ttl:将“生存时间”字段设置为 ttl 指定的数值

（4） 网络查询命令 netstat，netstat[-选项][-参数]

- -a:显示所有连接的信息
- -i:显示所有已配置网络设备的统计信息

- -c:持续更新网络状态（每秒一次）直至被人为中止
- -r:显示内核路由表
- -n:以数字（原始）格式而不是已解析的名称显示远程和本地连接

7.2.7 Linux 文件和目录管理

1. Linux 文件组织与结构

1）Linux 文件组织

文件系统组织是指文件存在的物理空间

Linux 文件系统使用索引节点来记录文件信息，可以用 ln 命令对一个已经存在的文件再建立一个新的连接。

连接有软接连和硬连接，软连接又叫符号连接

2）Linux 文件结构

树形结构的最上层是根目录，用“/”表示

3）Linux 文件挂载

挂载是将一个文件系统的顶层目录挂到另一个文件系统的子目录上，使它们成为一个整体，上一层文件系统的子目录就称为挂载点

（1） 挂载点必须是一个目录，而不能是一个文件

（2） 一个分区挂载在一个已存在的目录上，这个目录可以不为空，但挂载后这个目录下以前的内容将不可用

2. Linux 文件类型与访问权限

1）文件名与文件类型：普通文件、目录文件、链接文件、设备文件和管道文件

2）文件和目录访问权限

Linux 对文件访问设定了三级权限：文件所有者、与文件所有者同组的用户及其它用户

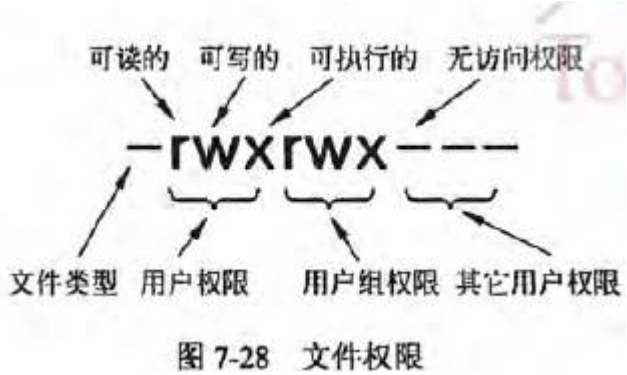

图 7-28 文件权限

3. Linux 文件和目录操作命令

（1）cat 命令：用来在屏幕上滚动显示文件的内容

cat [-选项] filename [filename2]…[fileNameN]

- -n:由 1 开始对文件所有输出的行数编号
- -b:和-n 相似，只不过对于空白行不编号
- -s:当遇到有连续两行以上的空白行，就代换为一行的空白行
- -v:显示非打印字符

（2） more 命令：文体文件较长一屏显示不完可使用此命令将文件内容分屏显示

（3） less 命令：按页显示文件，B 向前翻，P 向后翻，Q 退出，百分比显示指定位置

（4） 文件复制命令 cp：把指定的源文件复制到目标文件或把多个源文件复制到目标目录中

cp [-选项] source filename|directory dest filename|directory

- -a:整个目录拷贝
- -f:删除已经存在的目标文件而不提示
- -i:和 f 选项相反，在覆盖目标文件之前将给出提示要求用户确认
- -p:除复制源文件外还把修改时间以及访问权限也复制到新文件中
- -R:若给出的源文件是一目录文件，此时 cp 将递归复制该目录下所有的子目录和文件
- -l:不作拷贝，只是链接文件

（5） 文件移动命令 mv：为文件或目录改名或将文件由一个目录移入另一个目录中

mv [-选项] source filename|directory dest filename|directory

- -i:交互式操作

- -f:禁止交互式操作

（6） 文件删除命令 rm：删除指定的一个目录中的一个或多个文件或目录

rm [-选项] filename|directory…

- -f:忽略不存在的文件，从不给出提示
- -r:指示 rm 将参数中列出的全部目录和子目录均递归地删除
- -i:进行交互式删除

（7） 创建目录命令 mkdir：在当前目录中建立一个指定的目录

mkdir[-选项] dirName

- -m:对新建目录设置存取权限
- -p:可以是一个路径，加此选项系统将自动建立好那些尚不存在的目录

（8） 删除目录命令 rmdir：功能是从一个目录中删除一个或多个子目录项

rmdir [-选项] dirName

- -p:递归删除目录

（9） 改变目录命令 cd：将当前目录改变到指定的目录，若没有指定目录则显示用户当前所在的主目录路径

cd [directory]

（10） 显示当前目录命令 pwd：显示用户当前所处的目录，且为整个绝对路径

（11） 列目录命令 ls：是 list 的简写，功能为列出当前目录的内容

ls [-选项] filename|directory

- -a:显示指定目录下所有子目录与文件，包括隐藏文件
- -c:按文件的修改时间排序
- -d:如果参数是目录，只显示其名称而不显示其下的各文件
- -i:在输出的第一列显示文件的 i 节点号
- -l:以长格式来显示文件的详细信息

（12） 文件访问权限命令 chmod：用于改变文件或目录的访问权限

chmod[-选项] mode filename…

- -c:若该档案权限确实已经更改，才显示其更改动作
- -v:显示权限变更的详细资料
- -R:对当前目录下所有文件与子目录进行相同的权限变更
- -mode:权限设定字符串。字符串格式为：[ugoa…][[+-=][rwxX]…][,…]

（13） 文件连接命令 ln：功能是在文件之间创建链接

ln[-选项]source filename|directory dest filename|directory

- -f:文件链接时先将与 dest 同文件名的文件删除
- -d:允许系统管理者硬链接自己的目录
- -i:在删除与 dest 同文件名的文件时先进行询问
- -s:进行符号链接（symbolic link）
- -v:在文件链接之前显示其文件名
- -b:将在链接时会被覆盖写或删除的文件进行备份

7.2.8 Linux 用户和组管理

1. 用户管理概述

- 用户标识（UID）：系统中用来标识用户的数字
- 用户主目录：用户的起始工作目录
- 登录 shell：用户登陆后启动以接收用户的输入并执行输入相应命令的脚本程序，即 shell,是用户与 Linux 系统之间的接口
- 用户组/组群：具有相似属性的多个用户被分配到一个组中
- 组标识（GID）：用来表示用户组的数字标识

ROOT 超级用户 ID 和组 ID 都是 0，其它用户 ID 从 500 开始编号

2. 用户管理配置文件

（1）/etc/passwd 文件：对所有可读，每个用户在此中有一行对应的记录，形式如下：

用户名：加密的口令：用户 ID：组 ID：用户的命名或描述：登录目录：登录 shell

（2）/etc/shadow 文件：超级用户可读，包含了系统中所有用户及其口令等相关信息
（3）/etc/group 文件：记录了用户组的基本属性信息，形式如下：
用户组名：加密后的组口令：组 ID：组成员列表
3. 用户和组管理命令
1）用户管理
增加一个新用户的命令格式为：adduser [-选项] username
- -d:指定用于取代默认/home/username 的用户主目录
- -g:用户所属用户组的组名或组 ID（用户组在指定前应存在）
- -m:若指定用户主目录不存在则创建
- -p:使用 crypt 加密的口令
- -s:指定用户登录 shell，默认为/bin/bash
- -u uid:指定用户的 UID，它必须是唯一的，且大于 499

passwd 命令格式：passwd [-选项] [username]
- -l:锁定口令，即禁用帐号
- -u:口令解锁
- -d:使帐号无口令
- -f:强迫用户下次登录时修改口令

临时禁止一个用户的操作：
（1） 把用户的记录从/etc/passwd 文件中注释掉，保留其主目录和其他主文件不变
（2） 在/etc/passwd 文件（或/etc/shadow）中关于该用户的 passwd 域的第一个字符前面加上一个“*”号
删除用户的命令格式为：userdel [-选项] username
- -r:把用户的主目录一起删除

用户在系统使用过程中可以随时使用 su 命令来改变身份，一般格式为：su[username]
Username 是要切换到的用户名，如不指定切换为 root
2）用户组管理
将一个新用户组加入系统的命令是 groupadd，格式一般为：groupadd[-选项] groupname
- -g GID:指定用户组的 GID，它必须是唯一的，且大于 499
- -r:创建小于 500 的系统用户组
- -f:若用户组已存在，退出并显示错误（原用户组不会被改变）

删除一个已有的用户组，命令格式：groupdel groupname，要注意：
（1） 组中的文件不能自行删除，也不能自行改变文件所属的组
（2） 如果组是用户的基本组（即/etc/passwd 文件中显示为该用户的组），则这个组无法删除
（3） 如果组中有用户在系统中处于登录状态就不能删除该组
修改用户组的属性使用 groupmod 命令：groupmod [-选项] groupname
- -g:为用户组指定新的组标识号
- -n:将用户组的名字改为新名字

7.3 Windows Server 2003 IIS 服务的配置
7.3.1 IIS 服务器的基本概念
7.3.2 安装 IIS 服务
7.3.3 配置 Web 服务
1. 网络基本配置
2. 网站的安全性配置
7.3.4 配置 FTP 服务器
1. 修改 IP 地址和端口
2. 限制连接数量
3. 设置主目录
所谓主目录是指映射为 FTP 根目录的文件夹
4. 访问安全设置
（1）禁止匿名访问

（2）限制 IP 地址

5. 客户端访问 FTP 站点

IE 和 DOS 访问

7.4 Linux Apache 服务器的配置

7.4.1 Apache 的安装与配置

1. Apache 的启动与停止

2. Apache 的配置界面

7.4.2 建立基于域名的虚拟主机

所谓虚拟生机服务是指在一台物理机器上提供多个 Web 服务

7.4.3 建立基于 IP 地址的虚拟主机

1.为网卡绑定多个 IP 地址

2.建立基于 IP 地址的虚拟主机

7.4.4 Apache 中的访问控制

7.5 DNS 服务器的配置

7.5.1 DNS 服务器基础

域名系统是一种 TCP/IP 的标准服务，它是一种组织成域层次结构的计算机和网络服务命名系统，负责 IP 地址和域名之间的转换。

（1） 主域名服务器（primary name server）

（2） 辅助域名服务器（secondary name server）

（3） 缓存域名服务器（caching-only server）

（4） 转发域名服务器（forwarding servers）

正向解析表示将域名转换为 IP 地址，反向解析表示将 IP 地址转换为域名

7.5.2 Windows Server 2003 DNS 服务器的安装与配置

1. DNS 服务器的安装

2. 创建 DNS 解析区域

3. 创建域名

4. 设置 DNS 客户端

7.5.3 Linux BIND DNS 服务器的安装

BIND（Berkeley Internet Name Domain）

1. 配置 DNS 解析器

2. 调整缓存服务器的配置

3. 生服务器的配置

4. 从服务器的配置

5. DNS 的测试

7.6 DHCP 服务器的配置

7.6.1 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）服务器基础

7.6.2 Windows Server 2003 DHCP 服务器的配置

1. 创建 DHCP 作用域

2. 设置 DHCP 客户端

3. 备份、还原 DHCP 服务器配置信息

4. DHCP 服务器的 IP 地址与 MAC 地址绑定策略

7.6.3 Linux DHCP 服务器的配置

Linux 下默认安装 DHCP 服务的配置文件为/etc/dhcpd.conf，通常包括三部分：

（1） parameters:用于说明 DHCP 服务工作的网络配置参数

（2） declarations:用来描述网络布局、提供 DHCP 客户的 IP 地址分配策略等信息

（3） option（选项）：用来配置 DHCP 可选参数

7.7 电子邮件服务器的配置

7.7.1 电子邮件服务器的安装

7.7.2 邮箱存储位置设置