# 第八章 系统基础

## Windows常用命令

### Windows系统核心概念

**1. 常见目录结构**

表8.1 Windows常见目录结构

|  |  |
| --- | --- |
| **目录路径** | **作用** |
| C:\Windows\System32 | 系统核心文件（如系统DLL、驱动程序） |
| C:\Program Files | 64位应用程序安装目录 |
| C:\Program Files (x86) | 32位应用程序安装目录 |
| C:\Users\<用户名>\AppData | 用户应用程序数据（隐藏目录） |
| C:\Windows\Temp | 系统临时文件 |

**2. 注册表（Registry）**

作用：存储系统、软件、硬件的配置信息。

关键路径：

* HKEY\_LOCAL\_MACHINE (HKLM)：硬件和系统全局配置。
* HKEY\_CURRENT\_USER (HKCU)：当前用户配置。
* HKEY\_CLASSES\_ROOT：文件关联和COM组件注册。

操作命令：regedit（注册表编辑器）。

**3. 系统启动项**

启动位置：

* 注册表：HKCU\Software\Microsoft\Windows\CurrentVersion\Run
* 系统目录：C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

管理工具：任务管理器 → 启动标签页。

**4. 设备管理器**

作用：查看和管理硬件设备（驱动安装、禁用/启用设备）。

打开方式：

* 右键“此电脑” → 管理 → 设备管理器。
* 命令：devmgmt.msc。

**5. 任务管理器**

功能：

* 查看进程、性能（CPU/内存/磁盘/网络）、启动项、用户会话。

快捷键：Ctrl + Shift + Esc 或 Ctrl + Alt + Del → 任务管理器。

**6. 进程与服务**

进程：运行中的程序实例（.exe）。

服务：后台运行的系统程序（如打印服务、网络服务）。

管理命令：

* 查看进程：tasklist
* 结束进程：taskkill /PID <进程ID> /F

**7. 组策略（Group Policy）**

作用：集中管理用户和计算机的权限、安全策略。

打开方式：gpedit.msc（仅限专业版/企业版）。

**8. 安全组、工作组与域**

表8.2 安全组、工作组与域

|  |  |
| --- | --- |
| **概念** | **说明** |
| 安全组 | 用户权限集合（如管理员组、普通用户组） |
| 工作组 | 对等网络模型，无集中管理（适合小型网络） |
| 域 | 集中管理网络资源（AD域控制器） |

**9. 安全日志**

位置：事件查看器 → Windows日志 → 安全。

作用：记录登录、权限变更、审核事件。

打开方式：eventvwr.msc。

### Windows网络排查命令

**1. ping**

作用：测试网络连通性（ICMP协议）。

常用参数：

ping www.baidu.com # 默认发送4个包

ping -t www.baidu.com # 持续ping（按Ctrl+C停止）

ping -n 10 www.baidu.com # 发送10个包

ping -l 1024 www.baidu.com # 指定数据包大小（字节）

**2. ipconfig**

作用：查看和刷新网络配置（IP地址、DNS、DHCP）。

常用参数：

ipconfig # 显示基础信息

ipconfig /all # 显示详细信息（MAC地址、DNS服务器）

ipconfig /release # 释放IP地址（DHCP客户端）

ipconfig /renew # 重新获取IP地址

ipconfig /flushdns # 清空DNS缓存

**3. route**

作用：查看和修改路由表。

常用参数：

route print # 显示路由表

route add 192.168.2.0 mask 255.255.255.0 192.168.1.1 # 添加路由

route delete 192.168.2.0 # 删除路由

**4. arp**

作用：管理ARP缓存表（IP-MAC映射）。

常用参数：

arp -a # 显示ARP表

arp -d 192.168.1.1 # 删除指定ARP条目

arp -s 192.168.1.1 aa-bb-cc-dd-ee-ff # 添加静态ARP条目

**5. tracert**

作用：追踪数据包路径（通过TTL递增）。

常用参数：

tracert www.baidu.com # 显示路径

tracert -d www.baidu.com # 不解析主机名（加快速度）

**6. telnet**

作用：测试TCP端口连通性（需启用Telnet客户端）。

启用Telnet：控制面板 → 程序 → 启用或关闭Windows功能 → 勾选Telnet客户端。

telnet www.baidu.com 80 # 测试80端口是否开放

### 拓展

**1. 网络诊断工具**

* nslookup：DNS查询。
* netstat：查看网络连接状态。

netstat -ano # 显示所有连接及对应进程PID

netstat -ab # 显示监听端口的程序名称

* netsh：高级网络配置（如防火墙、接口）。

netsh interface show interface # 查看网络接口状态

netsh firewall show state # 查看防火墙状态

**2. 批处理脚本（BAT）**

示例：自动刷新DNS并测试连通性。

@echo off

ipconfig /flushdns

ping www.baidu.com -n 4

pause

**3. PowerShell高级命令**

查看进程：Get-Process

网络测试：Test-NetConnection www.baidu.com -Port 80

**4. IP地址冲突**

现象：网络连接显示“无Internet访问”。

解决：ipconfig /release → ipconfig /renew。

**5. DNS解析失败**

现象：能ping通IP但无法访问域名。

解决：ipconfig /flushdns，检查DNS服务器配置。

**6. 网络连接中断**

排查步骤：

* ping 网关IP → 检查局域网连通性。
* ping 8.8.8.8 → 检查外网连通性。
* tracert 8.8.8.8 → 定位断点。

**7. 为什么ping域名显示“找不到主机”？**

原因：DNS解析失败。

解决：

* 检查网络连接是否正常。
* 运行 ipconfig /flushdns 清空DNS缓存。
* 尝试更换DNS服务器（如 8.8.8.8）。

**8. 删除ARP条目后无法上网怎么办？**

自动恢复：等待1-2分钟，系统会自动重新发送ARP请求。

手动恢复：重启网络适配器（禁用再启用）。

**9. Tracert结果中全是\*怎么办？**

原因：中间节点禁用了ICMP响应。

解决：忽略\*，只要最终到达目标IP即可。

## AD域与LDAP协议

### LDAP协议

**1. LDAP需求背景**

核心问题：企业需集中管理用户、设备、应用等资源信息，但传统文件存储（如Excel）无法满足高效查询和权限控制需求。

解决方案：

* 目录服务：树状结构存储数据（类似电话簿），支持快速检索。
* 标准化协议：不同系统（如Windows、Linux）统一访问目录服务。

**2. LDAP概述**

全称：Lightweight Directory Access Protocol（轻量目录访问协议）。

作用：提供目录服务的访问接口，用于查询和修改目录数据。

关键特性：

* 树状结构（DIT）：根节点 → 组织（O）→ 组织单元（OU）→ 条目（Entry）。
* 条目属性：每个条目由唯一DN（Distinguished Name）标识，包含多个属性（如cn=user1, ou=IT, dc=example, dc=com）。

端口：默认389（明文）/636（LDAPS，加密）。

**3. LDAP报文结构**

操作类型：

* Bind：认证请求（用户名/密码）。
* Search：查询目录条目。
* Modify：修改条目属性。

报文示例（Wireshark抓包）：

LDAP Bind Request

MessageID: 1

ProtocolOp: BindRequest (0)

Version: 3

Name: cn=admin,dc=example,dc=com

Authentication: Simple (密码明文)

### AD域（Active Directory）

**1. AD域需求背景**

企业痛点：

* 用户需在多台设备重复登录，权限分散。
* 缺乏集中式策略管理（如密码复杂度、软件安装）。

AD域作用：

* 统一身份认证：用户一次登录访问域内所有资源。
* 集中策略管理：通过组策略（GPO）控制域内计算机和用户行为。

**2. AD域核心组件**

表8.3 AD域核心组件

|  |  |
| --- | --- |
| **组件** | **说明** |
| 域控制器（DC） | 运行AD DS服务的服务器，存储目录数据库。 |
| 目录数据库 | 存储用户、组、计算机等对象（NTDS.dit文件）。 |
| DNS服务器 | 域内资源定位依赖DNS（如查找域控制器）。 |
| 组策略对象（GPO） | 定义安全策略、软件部署等规则。 |

**3. AD域工作原理**

用户登录流程：

* 用户输入域账号（如user1@example.com）。
* 客户端向DNS查询域控制器地址。
* 域控制器验证用户凭证（Kerberos协议）。
* 颁发票据（TGT），允许访问域内资源。

### AD域信任关系

**1. 信任类型**

单向信任：域A信任域B，但域B不信任域A。

双向信任：域A与域B互相信任（默认同一森林内域间信任）。

跨森林信任：不同AD森林间的信任（需手动配置）。

**2. 信任作用**

资源共享：允许用户跨域访问资源（如文件服务器）。

统一管理：多域环境下集中权限控制。

**3. 信任验证**

示例：域A用户访问域B的文件服务器时，域B的DC验证域A的DC颁发的票据。

### AD域组策略（GPO）

**1. 组策略功能**

* 安全策略：密码复杂度、账户锁定阈值。
* 软件部署：自动安装/卸载应用程序（MSI包）。
* 环境配置：映射网络驱动器、禁用USB存储。

**2. 策略应用流程**

创建GPO：在“组策略管理”控制台（GPMC）中定义策略。

链接GPO：将策略应用到域、OU或站点。

策略生效：客户端定期（默认90分钟）拉取并应用策略。

**3. 常用策略示例**

密码策略：

路径：Computer Configuration → Policies → Windows Settings → Security Settings → Account Policies → Password Policy

策略项：Minimum password length = 8

禁用USB：

路径：Computer Configuration → Policies → Administrative Templates → System → Removable Storage Access

策略项：Deny execute access = Enabled

### 搭建AD域及常用操作

**1. 搭建AD域步骤**

安装AD域服务：

* 服务器管理器 → 添加角色 → 选择“Active Directory域服务”。

提升为域控制器：

* 配置新林（如example.com） → 设置目录还原密码。

配置DNS：确保域控制器安装DNS角色。

验证安装：

* 打开“Active Directory用户和计算机”，确认域结构。

**2. 常用操作命令**

用户管理：

net user user1 P@ssw0rd /add /domain # 创建域用户

dsquery user -name "user1" # 查询用户

组管理：

net group "IT组" /add /domain # 创建域组

net group "IT组" user1 /add /domain # 添加用户到组

### AD域应用场景（SSL VPN结合AD域认证）

**1. 场景需求**

* 企业远程访问：员工通过SSL VPN接入内网，需使用AD域账号认证。

**2. 配置流程**

VPN服务器集成AD域：

* 在VPN设备（如深信服SSL VPN）配置LDAP认证，指向AD域控制器。

配置LDAP参数：

* 服务器地址：AD域控制器IP（如192.168.1.100）。
* 端口：389（LDAP）或636（LDAPS）。
* 绑定DN：cn=admin,dc=example,dc=com。
* 用户搜索库：ou=Users,dc=example,dc=com。

用户登录验证：

* 用户输入域账号密码，VPN设备通过LDAP协议向AD域验证身份。

### 拓展

**1. LDAP安全加固**

使用LDAPS：配置SSL证书加密通信。

匿名访问限制：禁用匿名查询，仅允许授权用户访问。

**2. AD域备份与恢复**

备份工具：Windows Server Backup。

关键数据：NTDS.dit（目录数据库）、SYSVOL（组策略模板）。

**3. AD域与云集成**

Azure AD：微软云目录服务，支持混合部署（本地AD与Azure AD同步）。

**4. 用户无法登录域的可能原因？**

网络不通（检查DNS解析和域控制器可达性）。

用户账号被锁定或密码错误。

**5. 组策略未生效如何排查？**

运行 gpresult /r 查看策略应用结果。

检查GPO链接位置和权限（是否拒绝“应用组策略”）。

**6. LDAP与AD域的关系？**

LDAP是协议，AD域是微软基于LDAP实现的目录服务（扩展了Kerberos、GPO等特性）。

## Linux系统基础与常用命令

### Linux系统介绍

**1. Linux系统组成**

表8.4 Linux系统组成

|  |  |
| --- | --- |
| **组件** | **说明** |
| 内核（Kernel） | 管理硬件资源，提供进程调度、内存管理等核心功能。 |
| Shell | 用户与内核交互的接口（如Bash、Zsh）。 |
| 文件系统 | 树状目录结构（如/, /home, /etc）。 |
| 应用程序 | 用户级软件（如浏览器、编辑器）。 |

**2. Linux特点**

* 开源免费：代码公开，可自由修改和分发。
* 多用户多任务：支持多用户同时操作，进程独立运行。
* 高稳定性：广泛用于服务器环境（如云计算、嵌入式）。
* 丰富的命令行工具：通过命令高效管理系统。

### 查看文件命令

**1. ls - 列出目录内容**

常用参数：

ls -l # 长格式显示（权限、大小、时间）

ls -a # 显示隐藏文件（以`.`开头）

ls -h # 人性化显示文件大小（如KB/MB）

**2. cat - 查看文件内容**

用途：快速显示文件全部内容（适合小文件）。

cat file.txt

cat -n file.txt # 显示行号

**3. more/less - 分页查看文件**

区别：

more：仅支持向下翻页（按空格键）。

less：支持上下翻页（按↑/↓），搜索（/keyword）。

less /var/log/syslog

**4. head/tail - 查看文件头尾**

示例：

head -n 5 file.txt # 显示前5行

tail -f /var/log/nginx/access.log # 实时跟踪日志

### 查找文件或目录命令

**1. find - 按条件查找文件**

语法：find <路径> <条件> <动作>

find /home -name "\*.txt" # 按文件名查找

find /var/log -size +10M # 查找大于10MB的文件

find /etc -type d -mtime -7 # 查找7天内修改的目录

**2. locate - 快速查找文件（依赖数据库）**

更新数据库：sudo updatedb

示例：

locate nginx.conf

### 常用Linux命令及参数

**1. 网络相关命令**

表8.5 Linux网络相关命令

|  |  |  |
| --- | --- | --- |
| **命令** | **作用** | **常用参数** |
| ping | 测试网络连通性 | -c 4（发送4个包） |
| ifconfig | 查看/配置网络接口（旧版） | -a（显示所有接口） |
| ip | 替代ifconfig（新版） | ip addr show |
| netstat | 查看网络连接状态 | -tuln（监听端口） |
| tcpdump | 抓包分析网络流量 | -i eth0 -n port 80 |
| wget | 下载文件 | -O filename（指定保存名称） |
| iptables | 配置防火墙规则 | -A INPUT -p tcp --dport 22 -j ACCEPT |

**2.** **系统管理命令**

表8.6 Linux系统管理命令

|  |  |  |
| --- | --- | --- |
| **命令** | **作用** | **常用参数** |
| ps | 查看进程状态 | aux（显示所有进程） |
| top | 实时监控系统资源（CPU、内存） | -d 2（刷新间隔2秒） |
| free | 查看内存使用情况 | -h（人性化显示） |
| df | 查看磁盘空间 | -hT（显示文件系统类型） |
| du | 查看目录/文件占用空间 | -sh \*（汇总当前目录大小） |
| kill | 终止进程 | -9 PID（强制终止） |
| date | 显示/设置系统时间 | +%Y-%m-%d（格式化输出） |

**3. 文件操作命令**

表8.7 文件操作命令

|  |  |  |
| --- | --- | --- |
| **命令** | **作用** | **示例** |
| cp | 复制文件/目录 | cp -r dir1 dir2（递归复制目录） |
| mv | 移动/重命名文件 | mv old.txt new.txt |
| rm | 删除文件/目录 | rm -rf dir（强制删除目录） |
| chmod | 修改文件权限 | -hT（显示文件系统类型） |
| chown | 修改文件所有者 | chown user:group file.txt |

**4. 硬件与性能工具**

表8.8 硬件与性能工具

|  |  |  |
| --- | --- | --- |
| **命令** | **作用** | **常用参数** |
| ethtool | 查看/配置网卡参数 | ethtool eth0 |
| iperf | 网络带宽测试 | iperf -s（服务器模式） |
| lspci | 列出PCI设备信息 | lspci -v（详细信息） |
| lsusb | 列出USB设备信息 | lsusb -t（树状显示） |

### 拓展

**1. 管道与重定向**

管道：将前一个命令的输出作为后一个命令的输入。

ps aux | grep nginx

重定向：

ls > filelist.txt # 输出重定向到文件

cat file.txt 2>> error.log # 错误追加到文件

**2. 权限管理**

权限符号：

* r（读）：4
* w（写）：2
* x（执行）：1

示例：

chmod 755 script.sh # 所有者：rwx，其他用户：r-x

**3. 服务管理（systemd）**

启动/停止服务：

systemctl start nginx

systemctl stop nginx

systemctl enable nginx # 开机自启

**4. 软件包管理**

Debian/Ubuntu（apt）：

sudo apt update # 更新软件源

sudo apt install nginx # 安装软件

RedHat/CentOS（yum）：

sudo yum install httpd

**5. 命令找不到（Command not found）**

原因：命令未安装或路径未配置。

解决：

which ping # 查看命令路径

sudo apt install iputils-ping # 安装缺失包

**6. 权限被拒绝（Permission denied）**

原因：当前用户无权限执行操作。

解决：

sudo command # 以root权限执行

chmod +x script.sh # 添加执行权限

**7. 磁盘空间不足（No space left on device）**

排查：

df -h # 查看磁盘使用

du -sh /var/log # 检查大目录

## 数字证书

### 证书需求背景

**1. 传统通信的安全问题**

* 明文传输风险：HTTP、FTP等协议数据易被窃听或篡改。
* 身份伪造风险：攻击者可伪装成合法服务器（如中间人攻击）。

**2. 对称加密的局限性**

* 密钥分发难题：如何安全地将密钥传递给通信双方？

**3. 非对称加密的挑战**

* 公钥信任问题：如何确保接收的公钥确实属于目标对象？
* 解决方案：引入受信任的第三方机构（CA）验证公钥身份 → 数字证书。

### 证书的概念及分类

**1. 数字证书定义**

作用：电子“身份证”，绑定公钥与持有者身份（如域名、组织）。

核心内容：

* 持有者信息（Subject）
* 公钥
* 颁发机构（Issuer）
* 有效期
* 数字签名（由CA私钥签发）

**2.** **证书分类**

表8.9 证书分类

|  |  |  |
| --- | --- | --- |
| **类型** | **用途** | **示例** |
| 根证书 | CA自身的证书，预置在操作系统/浏览器中 | DigiCert Global Root CA |
| 中间证书 | 由根证书签发，用于签发终端证书 | Let's Encrypt Intermediate CA |
| 服务器证书 | 验证服务器身份（如HTTPS） | www.example.com的证书 |
| 用户证书 | 验证客户端身份（如VPN登录） | 员工个人证书 |
| 代码签名证书 | 验证软件来源可信（防止篡改） | Microsoft代码签名证书 |

**3. 证书链（Chain of Trust）**

信任传递：客户端通过证书链逐级验证证书合法性。

终端证书 → 中间证书 → 根证书

示例：

www.example.com（终端证书）

↓ 由中间CA签发

Let's Encrypt Intermediate CA

↓ 由根CA签发

ISRG Root X1（根证书）

### 证书的工作原理及流程

**1. 证书申请与签发流程**

生成密钥对：申请者生成公钥（包含在证书中）和私钥（保密）。

创建CSR（证书签名请求）：包含公钥、申请者信息（域名、组织等）。

提交CSR至CA：通过CA网站或API提交请求。

CA验证身份：

* 域名验证（DV）：验证申请者对域名的控制权（如DNS解析、文件验证）。
* 组织验证（OV）：验证企业营业执照等实体信息。
* 扩展验证（EV）：更严格的企业身份审核（显示绿色地址栏）。

签发证书：CA用私钥对证书签名，返回证书文件（如.crt）。

**2. 证书验证流程（以HTTPS为例）**

客户端发起请求：访问https://www.example.com。

服务器返回证书：包含公钥、证书链。

客户端验证证书：

* 有效性检查：证书是否过期？域名是否匹配？
* 签名验证：用CA公钥验证证书签名是否合法（逐级验证证书链）。
* 吊销检查：查询CRL（证书吊销列表）或OCSP（在线证书状态协议）。

建立加密连接：验证通过后，使用证书公钥协商对称加密密钥（如TLS握手）。

### 证书的认证应用场景

**1. HTTPS网站加密**

* 作用：验证服务器身份，建立SSL/TLS加密通道。
* 证书类型：服务器证书（DV/OV/EV）。

**2. VPN身份认证**

* 客户端证书：用户接入VPN时验证身份（如OpenVPN）。
* 服务器证书：验证VPN网关合法性。

**3. 电子邮件加密（S/MIME）**

* 用户证书：签名和加密邮件，确保发件人身份和内容保密。

**4. 代码签名**

* 开发者证书：验证软件发布者身份，防止恶意篡改。

**5. 物联网设备认证**

* 设备证书：确保设备与云平台通信的合法性（如AWS IoT）。

### 拓展

**1. 证书格式**

表8.10 证书格式

|  |  |  |
| --- | --- | --- |
| **格式** | **说明** | **扩展名** |
| PEM | Base64编码的文本格式（含证书/私钥） | .pem, .crt |
| DER | 二进制格式 | .der, .cer |
| PFX/PKCS12 | 包含证书和私钥的加密包（用于Windows） | .pfx, .p12 |

**2. 证书吊销机制**

* CRL（证书吊销列表）：CA定期发布被吊销证书的序列号列表。
* OCSP（在线证书状态协议）：实时查询证书状态（响应更快）。

**3. 自签名证书**

* 用途：内部测试或私有环境，无需CA签发。
* 风险：浏览器提示“不安全”（因未被公共CA信任）。

**4. 浏览器提示“证书不受信任”怎么办？**

* 原因：证书链不完整或根证书未预置。
* 解决：安装中间证书或使用公共CA签发的证书。

**5. 证书过期会有什么影响？**

* 浏览器阻止访问，显示“不安全”警告。
* 需及时续签证书并更新到服务器。

**6. 如何选择证书类型？**

* 个人网站：DV证书（成本低，快速签发）。
* 企业官网：OV/EV证书（显示企业信息，增强信任）。