Windows安全基础上

Windows 操作系统简介

Windows操作系统是由微软公司（Microsoft Corporation）开发的一系列图形化操作系统，自1985年首次发布以来，已成为全球最流行和广泛使用的操作系统之一。它为用户提供了一个直观

的图形用户界面（GUI），简化了计算机的操作方式，使得非专业用户也能够轻松操作电脑。Windows系统广泛应用于个人电脑、企业服务器、移动设备以及嵌入式系统等各类设备中。

Windows操作系统的历史发展

- **Windows 1.0（1985年）**：微软首次发布的图形用户界面操作系统，运行在MS-DOS基础上。Windows 1.0引入了窗口和图标的概念，但由于功能和性能的限制，影响力有限。
- **Windows 3.1（1992年）**：Windows 3.1是第一个广泛普及的Windows版本，支持更多的图形化应用，并且改善了内存管理、打印支持等功能。它标志着Windows开始获得市场关注。
- **Windows 95（1995年）**：Windows 95是一个重要的里程碑，它引入了“开始菜单”和任务栏，这些功能至今仍是Windows操作系统的核心元素。此外，Windows 95具备32位操作能力，支持“即插即用”硬件设备，使得安装和配置硬件更加容易。
- **Windows XP（2001年）**：Windows XP是微软推出的长期支持系统之一，凭借稳定性和兼容性受到用户欢迎。它简化了用户界面，提升了性能，并为家庭和企业用户提供了可靠的系统支持。XP的成功延续了超过十年，许多用户即使在之后的版本发布后仍然坚持使用XP。
- **Windows Vista（2007年）**：Windows Vista对操作系统的视觉效果进行了显著提升，引入了全新的“Aero”界面以及更多安全功能（如用户账户控制UAC）。然而，由于系统资源需求高，导致其表现不如预期。
- **Windows 7（2009年）**：Windows 7在Vista的基础上进行了改进和优化，显著提升了性能、兼容性和用户体验，因此获得了广泛好评。它也是目前许多用户最喜欢的版本之一。
- **Windows 8（2012年）**：Windows 8进行了激进的设计变革，推出了触屏优化的“开始屏幕”，用“平铺”界面替代了传统的“开始菜单”，但因用户习惯的突然改变而饱受争议。
- **Windows 10（2015年）**：Windows 10重新引入了“开始菜单”，融合了传统桌面和现代平板模式，适应触控和非触控设备。Windows 10通过“Windows 作为服务”的模式，定期更新功能和安全补丁，成为目前最主流的操作系统之一。
- **Windows 11（2021年）**：Windows 11进一步简化了用户界面，采用了全新的圆角设计和中置任务栏，并对生产力工具和游戏性能进行了提升，适合现代化办公和家庭娱乐需求。

Windows操作系统的特点

Windows最大的特点是其用户友好的图形用户界面，通过“开始菜单”、任务栏和窗口管理等元素，用户可以直观地在系统中进行操作，而无需依赖命令行。这种界面使得即便是没有技术背景的用户，也能够快速上手操作电脑。

此外，Windows的兼容性极强，支持绝大多数硬件设备，并且拥有庞大的软件生态系统，从办公套件到设计工具，再到开发环境和游戏，都能在Windows系统上流畅运行。这使得Windows不仅适合家庭用户，也成为企业、学校和政府机构的首选操作平台。

多任务处理能力也是Windows的重要功能之一，用户可以在不同应用程序之间无缝切换，通过任务管理器可以监控并管理运行中的进程。对于开发者和高级用户，Windows还提供了丰富的命令行工具和脚本支持。

Windows的安全性

随着信息安全的日益重要，Windows在安全性方面做了大量工作。例如，Windows防火墙（Windows Firewall）、Windows Defender防病毒软件、用户账户控制（User Account Control, UAC）以及文件和磁盘加密技术，都是保护用户数据的重要功能。这些安全措施大大提高了操作系统的抗攻击能力，使得用户在上网和处理敏感信息时更加安全。

此外，Windows系统定期发布安全补丁，通过Windows Update功能自动更新，确保系统始终处于最新状态，减少了安全漏洞被利用的风险。

Windows操作系统在不同设备上的应用

Windows的灵活性使其能够适应多种使用场景。在个人用户方面，Windows常用于日常办公、娱乐和学习。得益于其广泛的软件支持，用户可以通过Windows处理文档、进行视频会议、玩游戏以及进行多媒体创作。

在企业和服务器领域，Windows Server提供了更多针对企业网络环境的功能，例如文件共享、远程桌面、虚拟化支持等，成为企业IT基础设施中的核心组成部分。Windows系统还可以通过Active Directory进行集中管理，便于企业管理用户权限和资源。

嵌入式系统是Windows另一个重要的应用领域。许多ATM机、销售终端（POS）以及工控设备都运行着定制版的Windows系统，提供稳定的操作环境，并且能够通过网络进行远程维护和更新。

Windows版本

Windows的主要版本

- **Windows 家庭版（Home Edition）**：面向个人用户，提供家庭和小型办公室的基础功能，包括媒体播放、文件管理、网络连接和基础办公等功能。
- **Windows 专业版（Professional Edition）**：除了家庭版的功能外，还提供了企业用户常用的高级功能，例如BitLocker磁盘加密、远程桌面连接、企业级网络功能和更多的安全选项。
- **Windows 企业版（Enterprise Edition）**：这是专为大企业设计的版本，具有专业版的所有功能，并添加了更高级的安全功能、虚拟化支持、集中管理能力和企业级软件兼容性。
- **Windows 服务器版（Windows Server）**：用于运行在服务器设备上，提供专为企业网络设计的功能，例如文件共享、网络服务、安全管理和用户管理。

常见的 Windows 版本及其对应的版本号如下，使用该powershell命令可查看本机版本号信息。

```
Plain Text
1  Get-WmiObject -Class win32_OperatingSystem | select Version,BuildNumber
```

Windows 版本	内部版本号	发布日期
Windows 1.0	1.01	1985年11月20日
Windows 3.1	3.1	1992年4月6日
Windows 95	4	1995年8月24日
Windows 98	4.1	1998年6月25日
Windows ME (Millennium Edition)	4.9	2000年9月14日
Windows NT 4.0	4	1996年7月29日
Windows 2000	5	2000年2月17日
Windows XP	5.1	2001年10月25日
Windows Vista	6	2007年1月30日
Windows 7	6.1	2009年10月22日
Windows 8	6.2	2012年10月26日
Windows 8.1	6.3	2013年10月17日
Windows 10	10	2015年7月29日
Windows 11	10	2021年10月5日

Windows 版本号的组成

Windows 的版本号通常由四个部分组成，例如 Windows 10 的初始版本号是 10.0.10240.16384。具体解释如下：

- **主版本号**（Major）：表示大的版本变更，如 Windows 10 的主版本号为 10。
- **次版本号**（Minor）：次版本的更新，通常代表重大功能更新。例如，Windows 7 的次版本号是 1。
- **内部版本号**（Build）：表示编译和构建版本。微软发布的不同功能更新和补丁包会更新这个

数字。

- **修订号**（Revision）：通常用于记录小的功能改动或安全补丁。

在 Windows 操作系统中，根目录（通常是 C:）是整个文件系统的起点，存放系统文件、用户数据、应用程序等。以下是 Windows 根目录中的常见目录及其作用：

Windows

在 Windows 操作系统中，根目录（通常是C:）是整个文件系统的起点，存放系统文件、用户数据、应用程序等。Windows 根目录中的常见目录及其作用如下：

目录名	作用
C:\Program Files	默认安装应用程序的目录，存放系统和第三方软件的应用文件。
C:\Program Files (x86)	32位应用程序的默认安装目录（在64位系统上）。
C:\Windows	这是 Windows 操作系统的核心目录，包含了系统文件、驱动程序、DLL库、服务、以及系统配置文件等。其子目录有重要的系统功能： • System32：该目录存放了 Windows 系统核心的可执行文件、DLL 文件、系统工具（如命令提示符）以及硬件驱动程序等。大多数系统级操作都依赖于这里的文件。 • WinSxS：存储不同版本的系统文件，支持操作系统和应用程序的兼容性管理。 • Fonts：Windows 系统字体目录，存储所有的字体文件。
C:\Users	这是用户数据的存储目录，每个用户都有自己的子目录，包含个人的文件和设置： • Documents：用户的文档文件存放位置。 • Desktop：桌面文件存放位置。 • Downloads：存放下载的文件。 • AppData：存储应用程序的用户特定数据，通常包括应用程序的缓存和配置文件。分为 `Local`、`LocalLow` 和 `Roaming` 三个部分，分别处理本地、低权限和网络漫游数据。

C:\PerfLogs	性能监视工具的日志文件目录，用于系统性能监控。
C:\ProgramData	这个目录用于存储应用程序的公共数据。与 `C:\Users` 下的 `AppData` 不同，`ProgramData` 的数据是对系统所有用户共享的，比如某些应用的配置文件、数据库文件等。
C:$Recycle.Bin	系统的回收站目录，存储删除的文件，直到用户清空回收站。
C:\Temp	临时文件目录，存储安装过程或其他应用生成的临时数据。
C:\hiberfil.sys	系统休眠文件，存储系统进入休眠状态时的内存内容。
C:\Drivers	部分系统可能会包含这个目录，用于存放硬件设备的驱动程序。安装硬件设备时，操作系统可能从该目录读取驱动信息。
C:\Recovery	这个目录用于存放系统恢复相关的文件。在系统发生严重问题时，恢复功能可以通过这些文件将系统恢复到之前的状态。
C:\Boot	存储与操作系统启动相关的文件，如引导配置文件等。对于系统引导过程至关重要。
C:\Temp	此目录主要用于存放系统性能监控工具生成的日志文件，帮助系统管理员或开发者分析和监控系统的运行状态。

Windows 文件系统

Windows 文件系统是操作系统中用于管理文件和目录的核心组件，负责存储、组织、检索和管理硬盘等存储设备上的数据。Windows 支持多种文件系统，其中最常用的是 **NTFS**（New Technology File System）和 **FAT**（File Allocation Table）系列。文件系统在 Windows 中的设计直接影响文件的组织、权限管理、安全性、数据恢复等功能。

NTFS 是目前 Windows 的默认文件系统，自 Windows NT 推出以来成为主流。它不仅支持大容量磁盘，还具备先进的权限管理、加密、文件压缩和磁盘配额等功能。NTFS 设计了强大的日志系统，使系统在崩溃后能够快速恢复数据，保证文件系统的可靠性和稳定性。

相较之下，FAT32 是较旧的文件系统，尽管文件管理较为简单，且不具备复杂的权限控制和日志系统，但由于其广泛的兼容性，依然在 USB 闪存驱动器等设备中被广泛使用。然而，FAT32 文件系统的单个文件大小限制为 4GB，分区最大为 2TB，这在存储大文件时会成为局限。为了应对这一局限，exFAT 文件系统应运而生。exFAT 在保留了 FAT32 跨平台兼容性的同时，支持更大的文件和分区尺寸，因此在便携式存储设备中使用广泛。

NTFS权限

NTFS（New Technology File System）权限是 Windows 操作系统中用于控制对文件和文件夹的访问权限的机制。它使用访问控制列表（ACL，Access Control List）来分配权限，并根据用户或组的身份确定他们对资源的操作能力。

主要的 NTFS 权限类型

NTFS 权限主要分为以下几类：

- **读取（Read）**：允许查看文件或文件夹的内容。
- **写入（Write）**：允许修改文件或文件夹的内容。
- **执行（Execute）**：允许执行文件或文件夹中的程序。
- **删除（Delete）**：允许删除文件或文件夹。
- **修改（Modify）**：允许读取、写入和删除文件或文件夹。
- **完全控制（Full Control）**：允许用户执行所有操作，包括读取、写入、删除、修改、控制权限和所有权。

每个文件或文件夹都可以根据用户或用户组的身份设置不同的权限。例如，管理员可能对某个文件夹拥有“完全控制”权限，而普通用户则只有“读取”权限。

NTFS 权限的层级

NTFS 权限在文件系统中的层级结构上分为**显式权限**和**继承权限**：

- **显式权限（Explicit Permissions）**：直接分配给文件或文件夹的权限，优先级最高。
- **继承权限（Inherited Permissions）**：从上一级文件夹继承来的权限，简化权限管理，但优先级低于显式权限。

NTFS 权限的优先级

- 拒绝的权限比允许的权限优先级高。如果一个用户被显式设置为拒绝访问某个文件，即使他属于一个被允许访问的组，拒绝的权限仍然会生效。

ICACLS

`ICACLS`（Integrity Control Access Control List ）是 Windows 操作系统中的一款命令行工具，用于管理文件和目录的访问控制列表 (ACL)。通过 ACL，系统可以精确控制哪些用户或组对

文件和目录具有哪些权限。`ICACLS` 命令在 Windows 中用于查看、修改、备份和恢复文件的权限。

使用icacls可以查看文件的ACL：

```
C:\Users\Say>icacls Desktop
Desktop NT AUTHORITY\SYSTEM:(I)(OI)(CI)(F)
        BUILTIN\Administrators:(I)(OI)(CI)(F)
        LAPTOP-6882MFSI\Say:(I)(OI)(CI)(F)

已成功处理 1 个文件; 处理 0 个文件时失败
```

常用的权限类型

- **完全控制 (Full Control)**：
  - 允许用户进行任何操作，包括读取、写入、删除文件，以及更改权限设置。
- **修改 (Modify)**：
  - 允许用户读取和写入文件，也可以删除文件和子文件夹，但不能更改权限。
- **读取和执行 (Read & Execute)**：
  - 允许用户查看文件内容和执行可执行文件。
- **读取 (Read)**：
  - 允许用户查看文件内容，但不允许修改。
- **写入 (Write)**：
  - 允许用户修改文件内容，添加新内容或删除现有内容。
- **特殊权限 (Special Permissions)**：
  - 包含一些特定的操作，例如创建文件/文件夹、删除子文件夹和文件等，通常用于提供细粒度的权限控制。

常用的继承类型

- **容器继承 (Container Inherit – CI)**：
  - 该权限将应用于子文件夹。即在目录下创建的所有子文件夹都将继承该权限。
- **对象继承 (Object Inherit – OI)**：
  - 该权限将应用于文件。即在目录下创建的所有文件都将继承该权限。
- **不继承 (No Inherit – NI)**：

    - 表示不允许从父对象继承权限。该权限仅适用于当前对象。
- **继承权限 (Inherited – I)**：
    - 表示该权限是从父目录继承而来的，而不是直接分配给当前对象的。

其他常用命令：

命令	解释
icacls filename	显示指定文件或文件夹的 ACL。
icacls filename /grant UserName:(R)	授予指定用户读取权限。
icacls filename /grant UserName:(F)	授予指定用户完全控制权限。
icacls filename /remove UserName	移除指定用户的所有权限。
icacls filename /inheritance:r	禁止文件夹的权限继承。
icacls filename /setowner UserName	将文件或文件夹的所有者更改为指定用户。
icacls filename /save aclfile	将文件或文件夹的 ACL 保存到指定的文件。
icacls filename /restore aclfile	从指定的 ACL 文件恢复权限设置。
icacls * /T /C /grant UserName:(M)	递归授予指定用户修改权限，包括当前目录及所有子目录和文件。
icacls filename /reset	重置文件或文件夹的 ACL 为默认值。
icacls filename /audit UserName:(OI)(CI)	为指定用户添加审计规则。

Windows服务和进程

Windows服务

Windows服务是一种在后台运行的应用程序，通常不需要用户交互。它们在系统启动时自动启动，负责执行各种任务，例如打印机服务、网络连接和系统更新。服务的设计目标是保持系统的稳定性和安全性。每个服务都有其自己的特定功能，并且可以根据需要被启动、停止、暂停或恢复。

Windows服务是由服务控制管理器（Service Control Manager, SCM）进行管理的。管理员可以使用命令行工具（如 `sc` 命令）或图形用户界面（如“服务”管理工具）来配置这些服务。服务可以通过多种方式被配置，包括启动类型（如自动、手动或禁用）、权限和依赖关系等。常见的服务包括Windows Update、Print Spooler和Event Log等。

进程

进程是操作系统中正在执行的程序的实例。每个进程都有自己的内存空间和系统资源，确保进程之间的独立性。在Windows中，进程由操作系统的内核管理，操作系统通过调度算法来分配CPU时间。进程的生命周期包括创建、运行、等待和终止等状态。Windows提供了多种工具来监视和管理进程，如任务管理器、资源监视器和命令行工具（如 `tasklist` 和 `taskkill`）。

每个进程可以创建一个或多个线程，线程是进程中实际执行任务的单位。Windows通过多线程机制，提高了程序的执行效率，尤其是在进行I/O密集型或计算密集型操作时。

服务与进程的关系

服务通常以进程的形式运行。一个服务可以是一个独立的进程，也可以在 `svchost.exe` 这样的宿主进程中运行。Windows允许多个服务共享同一个宿主进程，从而减少系统资源的消耗。通过这种设计，服务可以独立于用户会话运行，使得它们在用户注销后仍然能够持续执行。

常用的服务和进程：

服务/进程名称	描述
svchost.exe	服务宿主进程，允许多个服务在同一进程中运行，提高资源利用率。
lsass.exe	本地安全授权子系统服务，负责用户身份验证和安全策略的执行。
explorer.exe	Windows资源管理器，负责用户界面的管理，包括桌面和文件浏览。
services.exe	服务控制管理器，管理系统中的所有服务和进程。

winlogon.exe	负责用户登录和注销过程，管理安全验证和用户会话的创建。
wuauserv	Windows更新服务，负责下载和安装操作系统更新。
rpcss.exe	远程过程调用（RPC）服务，允许进程间的通信。
spoolsv.exe	打印机后台处理程序，管理打印任务和打印机队列。
dmwappuserv	DWM应用程序用户服务，管理桌面窗口管理器的窗口和效果。
taskeng.exe	任务调度引擎，执行计划任务和定时任务。

LSASS（Local Security Authority Subsystem Service）是Windows操作系统中的一个关键组件，承担着用户身份验证和安全策略管理的重要职能。作为Windows安全架构的核心，LSASS负责处理用户的登录凭据，确保用户在系统中的身份得到验证。

当用户在Windows系统中输入用户名和密码时，LSASS会检查这些凭据的有效性。这一过程通常涉及与安全帐户管理器（SAM）或Active Directory的交互，以验证用户的身份。一旦验证通过，LSASS会生成一个安全访问令牌，包含用户的权限和安全标识符（SID），并在系统内控制访问权限。LSASS 是一个价值极高的目标，因为存在多种工具可以提取此过程存储在内存中的明文和哈希凭证。

管理服务

可以使用sc.exe和PowerShell的Get-Service查询和管理服务

powershell命令：

```
1   Get-Service | ? {$_.Status -eq "Running"}
```

sc命令使用：

- 列出服务

`sc query state= all`

- 查看服务详细信息

`sc qc wuauserv`

- 开启服务

`sc start wuauserv`

- 关闭服务

`sc stop wuauserv`

- 删除服务

`sc delete wuauserv`

- 修改服务配置

`sc config MyService binPath= "C:\Program Files\MyService\myservice.exe"`

管理进程

在 Windows 中查看和管理进程可以使用多种方法，包括命令行工具和图形化界面。

任务管理器

任务管理器是 Windows 系统中最常用的查看和管理进程的图形工具。你可以通过以下步骤打开它：

- 按 **Ctrl + Shift + Esc**，直接打开任务管理器。
- 或者按 **Ctrl + Alt + Del**，然后选择任务管理器。

任务管理器会显示系统当前运行的所有进程，包括用户进程、系统进程和后台服务。

tasklist

`tasklist` 命令可以在命令提示符或 PowerShell 中列出当前系统中正在运行的所有进程。

查看所有进程：

```
Plain Text
1  tasklist
```

`taskkill` 命令允许你在命令行中终止特定的进程。

根据PID终止进程： `taskkill /PID <ProcessID>`

根据进程名称终止： `taskkill /IM <ProcessName>`

Process Explorer

Process Explorer 是微软 Sysinternals 工具套件中的一款强大工具，主要用于深入了解 Windows 系统中的进程和系统资源的使用情况。它提供了比任务管理器更详细的系统信息，让用户可以查看、分析并管理进程、线程、句柄、DLL、网络连接等。 文件资源管理器键入 `\\live.sysinternals.com\tools` 即可查看 Sysinternals 工具套件，不需要下载可直接运行里面的工具。

拓展资源

https://en.wikipedia.org/wiki/List_of_Microsoft_Windows_components#Services