第三章 用户管理和配置管理

用户管理负责系统中所有用户使用系统资源时的权限管理；
配置管理负责系统中所有软件运行环境的配置。

3.1 用户管理
3.2 配置管理

3.1 用户管理

3.1.1 用户功能
3.1.2 举例

3.1.1 用户功能

- 用户身份：认证通过之后－－生成相应用户身份的shell进程－－在shell中运行的新进程也继承同样的用户身份
- 系统资源中的权限设置（属主和访问权限）：静态资源如文件、设备，动态资源如进程；
- 控制进程对资源的访问控制：进程的用户身份与资源的权限设置比较；

3.1.2 举例

3.1.2.1 UNIX
3.1.2.2 Windows NT

3.1.2.1 UNIX

1. 用户

- 用户的控制台/远程登录(login)：给出用户名和口令；
  - su变为其他用户
- 用户ID(user ID)：是一个整数。Uid为0的是超级用户或特权用户(super-user or privileged user)；
- 用户名(user name)：字符串，通常超级用户是 "root"（对所有资源均有全部访问权，执行所有系统调用）。
- /etc/passwd文件：文本文件，每行对应一个用户，包括：用户名、用户ID、用户组ID、用户全名、用户根目录、默认shell；如："root:x:0:1:Super-User:/:/sbin/sh"为该文件中与root用户对应的行。
  - 有关user的例程：getuid(); setuid();

- 为防止口令失窃，用户口令放在 /etc/shadow文件中，只有超级用户进程可以读取。如："xyong:6YD6YlXYuOAGk:10624::::::"为该文件中对应于用户xyong的加密口令。
- 创建新用户(useradd)：命令"./useradd test1"会对文件"passwd"进行修改，以创建一个新的用户"test1"。
- 删除已有用户(userdel)：命令"./userdel test1"会对文件"passwd"进行修改，以删除已有用户"test1"。

2. 用户组

- 用户组ID(group)：是一个整数。Uid为0的是超级用户组；用户组名：字符串，通常超级用户组是 "root"。
- /etc/group文件：文本文件，每行对应一个用户组，包括：用户组名、用户组ID、组内的各用户。如："sys::3:root,bin,sys,adm,rootc"为该文件中与sys组对应的行。
  - 有关group的例程：initgroups(); getgroups(); setgroups(); getgid(); setgid();
- 创建新用户组(groupadd)：命令"./groupadd test"会对文件"group"进行修改，以创建一个新的用户组"test"。
- 把一个用户加入一个组(usermod)：命令"./usermod -G group user"会对文件"group"进行修改，把用户"user"加入用户组"group"。
- 在文件管理功能中有相应命令进行资源所有者及其所在用户组的控制。如命令"chgrp group directory"可修改目录"directory"所在的用户组为" group"。

3. 资源访问权限

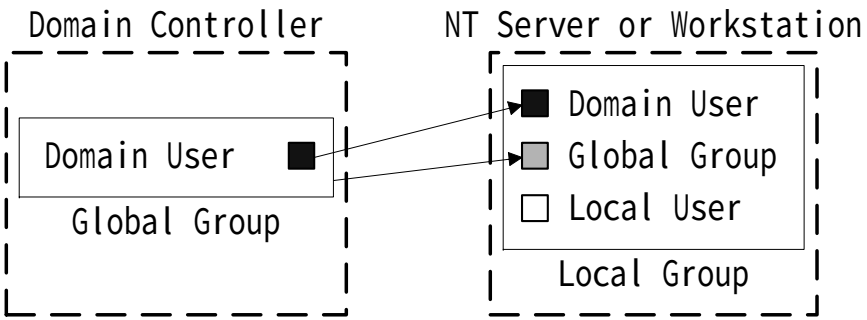
- 资源中的用户信息：
  - 文件：uid, gid——chown()
  - 进程：uid, gid, euid, egid——setuid(), getuid()（real ID对应于调用进程ID，effective ID对应被执行文件的用户ID）
- 资源访问权限对用户的划分：ugoa
  - 资源所有者：the user who owns it (u)
  - 同组用户：other users in the file's group (g)
  - 非同组用户：other users not in the file's group (o)
  - 所有用户：all users (a)（这种情况相当于前三种的组合a=u+g+o）

- 文件访问权限的分类：rwxXstugo前三种是基本权限，中间三种是高级执行权限（在不同系统上会有不同意义），后三种是用户权限的简便描述；
  - 读权限：read (r)，读文件内容或列目录中的文件列表；
  - 写权限：write (w)，修改文件内容或在目录中创建和删除文件；
  - 可执行权限（仅对目录和可执行文件有意义）：execute (or access for directories) (x)，把文件作为程序执行或访问目录中的文件；
  - 仅对目录有效的可执行权限：execute only if the file is a directory or already has execute permission for some user (X)
  - 执行时设置进程的用户或组标识：set user or group ID on execution (s)
  - 对换权限：save the program's text image on the swap device so it will load more quickly when run (called the "sticky bit").为了快速运行程序而在对换区中创建程序映像；
  - 所有者的权限：the permissions that the user who owns the file currently has for it (u)
  - 同组用户权限：the permissions that other users in the file's group have for it (g)
  - 其他用户权限：the permissions that other users not in the file's group have for it (o).

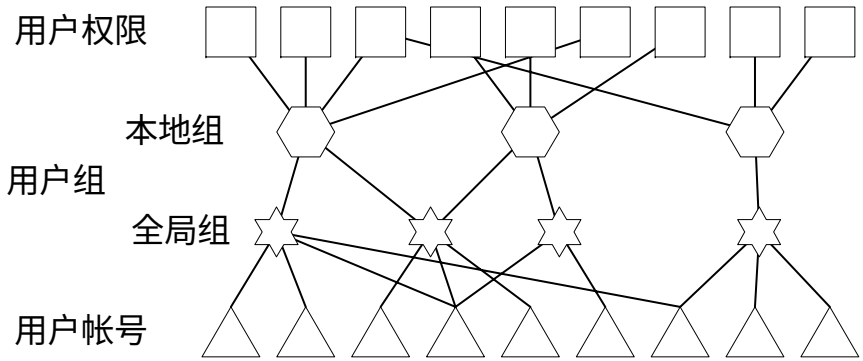
3.1.2.2 Windows NT

1. Windows NT的用户权限

- 用户(account)在控制台/远程登录(logon)：给出用户名、口令和域名
- 域(domain)：由若干计算机组成，包含用户和用户组(group)。域控制器只负责自己一个域，而域控制器和域中成员计算机均可以访问多个域的资源。
- 用户和用户组由安全标识符(SID)识别。SID是在用户或用户组创建时生成的唯一字符串：用户名不同则SID不同，同一用户名的几次创建则SID不同。如：文件A属于用户"user1"，删除用户user1然后重新创建，则A不属于任何用户



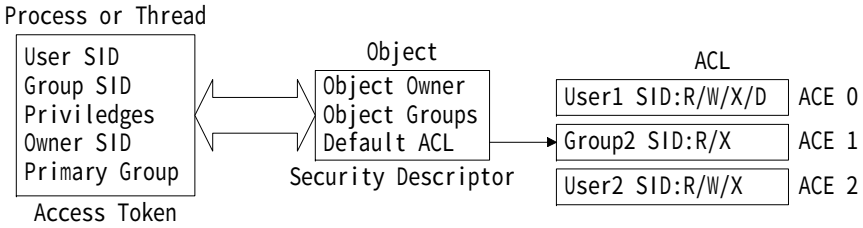
Windows NT的用户帐号



Windows NT的用户帐号和用户权限

2. Windows NT的访问控制

- 进程的用户身份信息：访问令牌(Access Token)
  - LogonUser()：返回一个用户的访问令牌句柄，以便以该用户的身份访问系统资源；
- 系统对象（资源）的用户信息：
  - 安全描述符(Security Descriptor)
  - 访问控制列表(Access Control List)
  - 访问控制条目(Access Control Entry)



Windows NT的对象访问权限认证

3.2 配置管理

3.2.1 配置管理的功能

3.2.2 举例

3.2.1 配置管理的功能

- 系统配置：用户信息、文件系统配置、硬件资源和设备驱动程序、网络配置等
- 应用软件管理：版本、包含的文件、安装时对系统所作的修改（作为将来清除该软件的依据）
- 用户定制信息：用户定制的应用软件配置

3.2.2 举例

1. UNIX
2. Windows NT

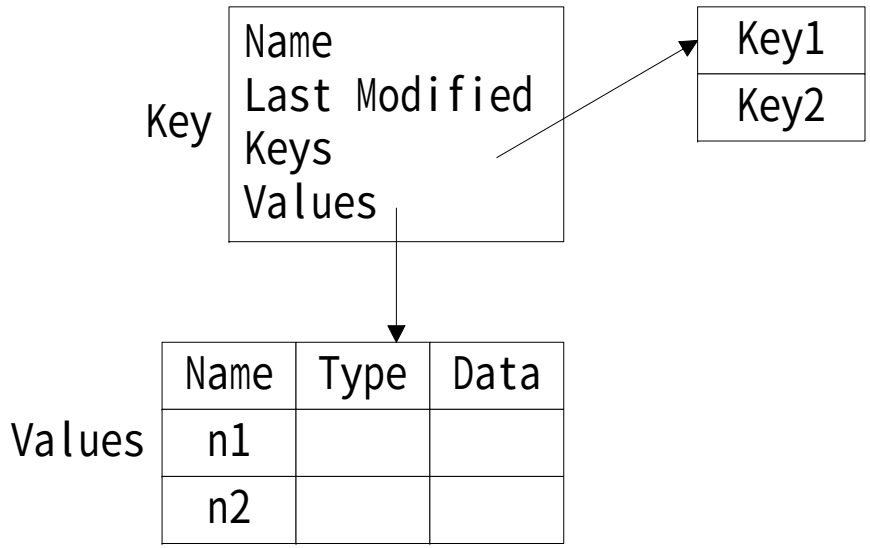
1. UNIX

- 系统配置：通常在 /etc目录下的文本文件，如：
  - 主机名文件(nodename),
  - 安装文件系统(vfstab)本机上各文件系统的设备名、安装目录、文件系统类型等
  - 网络配置(hosts, resolv.conf)：hosts为本机的名字解析列表；resolv.conf为名字解析服务器列表；
- 用户配置信息：每个用户根目录$HOME中的通常有各软件对应的用户配置信息文件。
- 应用软件管理：如Solaris 2.3，可以将应用软件打包成software package形式。各软件的安装信息存放在 /var/sadm/目录下。其操作有：
  - 安装(pkgadd)
  - 清除(pkgrm)
  - 查看软件包信息(pkginfo)
  - 软件打包(pkgmk)

- Linux的软件包管理工具rpm：Red Hat Package Manager，rpm的二进制软件包的命名规则为"<名称><版本>.<结构>.rpm"，其中的"结构"是指软件包的使用硬件环境，如i386, ppc等。
  - 安装和升级软件包：命令"rpm -ivh <软件包>"可安装指定软件包，并用#号表示安装进度；命令"rpm -Uvh <软件包>"可更新已安装的软件包，它会删除所有旧版本；
  - 检查软件包的文件签名：保证软件包的完整性；如：命令"rpm --checksig /usr/bin/telnet"可检查文件"telnet"的完整性；
  - 删除软件包：命令"rpm -e <软件包>"可删除已安装的软件包；
  - 已安装软件包维护：命令"rpm -qa"可列出所有已安装软件包；命令"rpm -q <软件包>"可列出软件包的版本；命令"rpm -ql <软件包>"可软件包中的所有文件；命令"rpm -qf <文件名>"可查询一个文件所属的软件包；
  - 软件包生成：命令"rpm -ba <软件包>"可从源程序开始编译生成新的二进制软件包。
  - 软件包的权限管理：命令"rpm --verify telnet"可检查软件包"Telnet"在安装后是否被改动，如软件包中各文件的时间、权限、大小等变化；

2. Windows NT

- 注册库(Registry)：系统定义的数据库，供系统和应用软件存储和检索配置信息。通过Registry Editor(regedt32.exe)或API编程来访问。注册库可能由多个文件组成。
- 内部采用层次结构（类似于目录和文件）
  - 对某个key中包含的value和下层key进行枚举：RegEnumValue(), RegEnumKey()
    - RegEnumKey：可给出一个注册项的所有子项；
    - RegEnumValue：可给出一个注册项的值；



Windows NT的注册项结构

几个系统预定义的注册项

- HKEY_USERS：计算机上所有用户配置文件。HKEY_CURRENT_USER 为 HKEY_USERS 的子项。
  - HKEY_CURRENT_USER：当前登录用户配置信息；如各软件的配置放在 \HKEY_CURRENT_USER\Software\CompanyName\ProductName\下。
- HKEY_LOCAL_MACHINE：计算机特定的配置信息；
  - HKEY_CLASS_ROOT：HKEY_LOCAL_MACHINE\Software的子项。用户从 Windows NT 资源管理器中打开文件和使用对象链接与嵌入 (OLE) 时，此处保存的信息可用来打开正确的应用程序。如：".zip"中给出要找的项为WinZip；而"WinZip"中给出对应的应用程序为d:\tools\WinZip\winzip32.exe,0
- HKEY_CURRENT_CONFIG：本地计算机在系统启动

- 应用软件管理：
  - 可以在可执行文件（包括DLL）中附加版本信息：公司名称、产品名称、版本号等。如："regedt32.exe"文件的属性中包含一个版本项，说明它是MS的产品。
  - 注册信息写在\HKEY_LOCAL_MACHINE\Software\CompanyName\ProductName\ 如：\HKEY_LOCAL_MACHINE\Software\Visio\Visio 2000\RegisteredSN;
  - 软件安装和清除：可以利用某些软件打包程序，如Install Shield

小结

- 用户管理：
  - 用户帐号
  - 资源访问权限
  - 访问控制
- 配置管理：
  - 系统配置
  - 应用软件管理
  - 用户环境配置信息