

第 3 章 用户登录和退出

3.1 启动 CDE

在一个带有图形接口卡和图形显示器的 RS/6000 上安装 AIX 操作系统 (BOS)，将自动安装下列软件包：

bos.rte (基本操作系统运行库)

bos (基本操作系统)

X11 (AIXwindows)

初始情况下，图形显示器以低功能终端(lft)的方式仿真字符终端，登录界面与字符设备终端没有什么区别，登录进系统后的操作界面是传统的命令行方式，即在带\$或#提示符的 KornShell (KSH, AIX 的标准 SHELL)下执行命令来完成相应管理工作。此时，键入 xinit 命令将启动一个 AIXwindows 界面：

不过，AIX 系统主要的图形用户接口是作为工业标准的“通用桌面环境”(CDE)。在 BOS 安装时不会自动安装 CDE，它包含在 X11.Dt 产品包中。选择安装 X11.Dt 后，同时会把 CDE 设置成为系统的缺省操作界面接口。

要停用 CDE，在命令行键入：

```
$ dtconfig -d
```

要启用 CDE，在命令行键入：

```
$ dtconfig -e
```

3.2 登录

在前一章已提及：机器启动过程中，init 进程从/etc/inittab 文件中读取初始化要执行的命令，运行/etc/rc.dt 脚本，该脚本调用负责登录服务和屏幕管理的 /usr/dt/bin/dtlogin。

dtlogin 取代 UNIX 系统传统的 login 进程，处理用户登录。下列是系统运行 dtlogin 的简要过程：

1. init 启动 dtlogin。
2. 如果必要，dtlogin 启动 X 服务器程序。
3. dtlogin 为它管理的每个显示器启动一新 dtlogin 的进程。
4. 新 dtlogin 进程调用 dtgreet，它显示登录屏幕，并且控制用户登录时的交互动作。

5. 当一个用户从 dtgreet 屏幕登录，如果/usr/dt/config/Xstartup 存在，dtlogin 执行该程序设置缺省的环境变量；然后运行 /usr/dt/bin/Xsession；接着读取 \$HOME/.dtprofile 文件设置用户定义的环境变量；最后调用会话管理器—— /usr/dt/bin/session。

用户登录环境要用到的环境配置文件取决于用户正在使用的界面接口。表 3.1 列出界面接口和相关的配置文件：

表 3.1 各种界面接口下登录用到的环境配置文件

命令行	AIXwindows	CDE
/etc/environment	/etc/environment	/etc/environment
/etc/profile	/etc/profile	\$HOME/.dtprofile
\$HOME/.profile	\$HOME/.profile \$HOME/.Xdefaults \$HOME/.xinitrc \$HOME/.mwmrc	\$HOME/.dt/dtwmrc

/etc/environment 包含通过系统调用 exec()启动的每个进程的缺省环境变量，并且在所有 3 种界面下都有作用。该文件设置的变量包括 PATH(路径)、TZ（时间格式）和 LANG（语言）。/etc/profile 包含环境变量和每次用户登录时调用的命令。这个文件仅仅影响命令行和 AIXwindows 两种界面接口。针对通用桌面环境，起作用的是\$HOME/.dtprofile 和在\$HOME/.dt 目录下的配置文件。除非\$HOME/.dtprofile 文件中的 DTSOURCEPROFILE 变量设置为“TRUE”，通常用户的\$HOME/.profile 文件在 CDE 环境中不起作用。设置 CDE 比较复杂。要深入了解请参考《通用桌面环境：高级的用户和系统管理指南》一书。

在 CDE 登录屏幕上的 Options 菜单允许选择会话类型，例如：有时网络配置错误，用普通的会话类型无法登录，可以选择自动安全保护的会话类型登录 CDE。要登入和退出类型为自动安全保护的会话，先从 Options 菜单选择 session，然后选择 Failsafe Session（自动安全保护会话）登录。一个类型为自动安全保护的会话将简单启动 Motif 和 aixterm 窗口。在 Options 菜单中还能设置的有选择会话的语言类型。

从 Options 菜单选择 Command Line Login（命令行登录），进入非桌面环境。这时将终止 X 服务器程序，并且进入仿真 ASCII 终端的登录界面，从命令行界面退出后，将重启 X 服务器程序。

3.3 退出

如果用户要从登录后的桌面环境（desktop）退出，可从 Workspace Menu（工作区菜单）选择 Log out，或用鼠标点击位于前面板靠着工作区按钮附近的 Exit 控制。

要退出命令行会话，直接输入 exit 或 logout 命令。

3.4 用户属性

系统管理员通过维护用户信息数据库，可以满足特定的系统安全性要求。这些数据库以 ASCII 文件形式保存，按节（stanza）划分不同的用户信息。“default”节中包含了用 mkuser 命令创建一个新用户时的缺省值。例如，当使用 SMIT 创建一个用户时（smit mkuser）将看见包含如下属性设置的一个对话框：

Add a User

Type or select values in entry fields.
Press Enter AFTER making all desired changes.

		[Entry Fields]
[TOP]		
* User NAME		[]
User ID		[]
#		
ADMINISTRATIVE USER?	false	+
Primary GROUP		[]
+		
Group SET		[]
+		
ADMINISTRATIVE GROUPS	[]	+
Another user can SU TO USER?	true	+
SU GROUPS		[ALL]
+		
HOME directory		[]
Initial PROGRAM		[]
User INFORMATION		[]
EXPIRATION date (MMDDhhmmyy)	[0]	
Is this user ACCOUNT LOCKED?	false	+
User can LOGIN?		true
+		
User can LOGIN REMOTELY?	true	+
Allowed LOGIN TIMES		[]
Number of FAILED LOGINS before	[0]	#
user account is locked		
Login AUTHENTICATION GRAMMAR	[compat]	
Valid TTYs		[ALL]
Days to WARN USER before password expires	[0]	#
Password CHECK METHODS	[]	
Password DICTIONARY FILES	[]	
NUMBER OF PASSWORDS before reuse	[0]	#
WEEKS before password reuse	[0]	#
Weeks between password EXPIRATION and LOCKOUT		[-1]
Password MIN. AGE		[0]
#		
Password MIN. LENGTH		[0]
#		

Password MIN. ALPHA characters	[0]	#
Password MIN. OTHER characters	[0]	#
Password MAX. REPEATED characters	[8]	#
Password MIN. DIFFERENT characters	[0]	#
Password REGISTRY		[]
MAX. FILE size		[2097151]
#		
MAX. CPU time		[-1]
MAX. DATA segment		[262144]
#		
MAX. STACK size		[65536]
#		
MAX. CORE file size		[2048]
#		
File creation UMASK		[022]
AUDIT classes		[]
+		
TRUSTED PATH?		nosak
+		
PRIMARY authentication method	[SYSTEM]	
SECONDARY authentication method	[NONE]	

对应的中文界面为：

添加用户

在输入字段中输入或选择值。
进行所有希望的更改之后按 Enter 键。

[顶部]	[输入字段]
* 用户名	[]
用户 ID	[]
#	
管理用户？	假
+	
主组	[]
+	
组集	[]
+	
管理组	[]
+	
另一用户可 SU 至用户	真
SU 组	[ALL]
+	
主目录	[]

初始程序		[]	
用户信息		[]	
到期日期(MMDDhhmmyy)	[0]		
已锁定此用户帐户?	false		+
用户可注册?			真
+			
用户可远程注册?	真		+
允许注册的次数		[]	
在锁定用户帐户之前	[0]		#
失败的注册数			
注册认证语法		[compat]	
有效 TTY		[ALL]	
在口令到期之前提前警告用户的天数			[0]
#			
口令检查方法		[]	
口令字典文件		[]	
在重新使用之前的口令数	[0]		#
在重新使用口令之前的周数	[0]		#
在口令到期和锁定之前的周数	[-1]		
口令最大使用期限			[0]
#			
口令最小使用期限			[0]
#			
口令最小长度			[0]
#			
口令最小字母字符数	[0]		#
口令最小其他字符数	[0]		#
口令最大重复字符数	[8]		#
口令最小不同字符数	[0]		#
口令登记		[]	
软文件大小			[2097151]
#			
软 CPU 时间		[-1]	
软数据段			[262144]
#			
软堆栈大小			[65536]
#			
软磁心文件大小			[2097151]
#			
硬文件大小			[]
#			
硬 CPU 时间		[]	
硬数据段			[]
#			

硬堆栈大小		[]
#		
硬磁心文件大小		[]
#		
文件建立 UMASK	[022]	
审查类		[]
+		
信任的路径?		nosak
+		
主认证方法	[SYSTEM]	
次认证方法	[NONE]	

上面被列出了的属性存储在下面系列文件:

/etc/passwd	包含用户的基本属性
/etc/group	包含组的基本属性
/etc/security/user	包含用户的扩展属性
/etc/security/limits	包含用户的运行资源限制
/etc/security/lastlog	包含用户最后登录属性
/usr/lib/security/mkuser.default	为用户帐户包含缺省值

用 SMIT 能查看、修改用户的属性,或增加、删除用户,对应的命令行命令分别是 `lsuser`、`chuser`、`mkuser` 和 `rmuser`。例如,用 `lsuser` 命令列出用户 `nan` 的属性:

```
# lsuser -f nan
nan :
```

```
id=201
pgrp=roberts
groups=roberts,staff
home=/home/nan
shell=/usr/bin/ksh
login=false
su=false
rlogin=true
daemon=true
admin=false
sugroups=ALL
admgroups=
tpath=nosak
ttys=ALL
```

```
expires=0
auth1=SYSTEM
auth2=NONE
umask=22
SYSTEM=compat
logintimes=
loginretries=0
pwdwarntime=0
account_locked=false
minage=0
maxage=0
maxexpired=-1
minalpha=0
minother=0
mindiff=0
maxrepeats=8
minlen=0
histexpire=0
histsize=0
pwdchecks=
dictionlist=
fsize=2097151
cpu=-1
data=262144
stack=65536
core=4096
rss=65536
time_last_login=839042643
tty_last_login=/dev/pts/0
host_last_login=hpubvwa.nsr.hp.c
unsuccessful_login_count=0
```

要修改 nan 的 SYSTEM 属性，从 compat 改为 NONE，可用 chuser 命令：

```
# chuser SYSTEM=NONE nan
```

如果只想看 chuser 命令是否起作用，可以仅显示用户 nan 的 SYSTEM 属性：

```
# lsuser -a SYSTEM nan
nan SYSTEM=NONE
```

通常一个用户登录，要通过 2 个文件验证该用户的合法性：

/etc/passwd，它验证用户帐号；

/etc/security/passwd，它包含加密的口令及其他与安全相关的数据。

用于用户验证的一个重要属性是用户的 SYSTEM 属性。这属性可以设置成

下列值：

- **DCE**：用户借助于分布式计算环境验证
- **Compat**：用户首先由本地的口令文件验证，如果口令文件中不存在该用户，转由网络信息服务 (NIS) 验证。
- **文件**：用户仅仅由本地的文件证实。
- **NONE**：不需要认证。

注意：如果 **SYSTEM** 属性值为 **NONE**，意味着即使 `/etc/security/passwd` 里面仍然保留用户的加密口令，也不对用户进行认证。