NOVELL 网软件环境的设置

章强　(扬州职业大学 225200)

摘要:本文从一个系统管理员的角度介绍了目前使用广泛的 NOVELL 网络的软件环境的设置,对用户、用户组和系统登录原稿这两个最为关键的问题进行了深入的讨论,并给出应用实例,同时对设置中易碰到的两个常见困难进行了探讨。

关键词:NOVELL 网络　用户组　登录原稿　自动登录

在 NOVELL 集中管理的网络环境下,提供给公用机房联网用户使用的系统,相当于一个带有存储管理的外部存储系统——文件服务器,通过 NETWARE 系统的管理程序如:SYSCON, FILER, FLAG, FLAGDIR 等对用户及文件进行存取权限的划分,保护服务器中的资源。但是目前教学网应用于计算机课程教学和其他教学(如财会电算化)的上机实验逐渐增多,各种上机实验对机器硬盘的众多目录存取权限、使用人员权限的设置又彼此不同,如何恰当地保护硬盘中的用户文件及系统公用软件,已成为机房管理员感到棘手的问题,要充分发挥 NOVELL 网的优越性,就必须对网络软件环境进行良好规划。

一、用户及用户组的设置

NETWARE 的安全管理分以下 4 级,其等级由低而高:

登录安全(LOGIN SECURITY) USERNAME/PASSWORD
权限安全(RIGHTS SECURITY) DIRECTOTY/FILES
属性安全(ATTRIBUTE SECURITY) DIRECTORY/FILES
服务安全(SERVER SECURITY) FILESSERVER CONSOLE

第一点也称入网口令安全管理,主要检查进入的使用者是否被授权以及密码是否正确、过期、失效等;第二点亦称受托者安全性,主要检查某个用户在某个目录或文件上所具有的存取权限,通过访问者权限(TRUSTEE ASSIGNMENT)和继承权屏蔽(INHERITED RIGHTS MASK)来设置;第三点确定目录、子目录或文件能否被读、被改名、被修改、被删除等,属性较前两个高。如某一用户在某一文件上有全部 8 大权限(S、R、W、C、E、M、F、A),但如果文件属性只有 READ ONLY 的权限,那它还是无法更改此文件的内容;第四点 FILE SERVER 的屏幕画面是不可以随便被改动的,只有超级用户(SUPERVISOR)才有权限更改,否则可随意关闭服务器。

我们对用户及用户组的权限主要使用上述前三种安全措施。在网中首先进行简单的用户设置,为具有各种不同权限的用户分别取一个名称(用户名),同时具体对应某一个用户只能使用硬盘中的指定目录和文件,因而不可能对网络中的公用程序及其他用户程序造成破坏。但随着教学内容的不断拓展,广大同学早以不满足五笔字型、WPS、BASIC、FOXBASE、DOS 等一些初级实验内容,进而要求在机器上熟悉 WINDOWS3.1、WINDOWS95、3DS、AUTOCAD、MATHCAD、BORLAND C++等一些大型的实用软件。而原有的所有同类型用户公用一个工作目录的软件环境设置不能适应这种要求(原因有三:(1)由于公用一个工作目录,用户可以互相删除对方使用的文件;(2)有些软件如 BORLAND C++,WINDOWS 要利用磁盘产生一个交换文件,任意时刻,该目录中只能有一个交换文件,所以将导致其他用户无法使用软件;(3)某些软件本不是支持网络的,如果大家同时存取一个文件就会使网络出现碰撞(COLLIDE))。基于这么一个现状笔者提出一个解决方案:建立一个用户组,使每台计算机对应一个用户名,所有用户均属于这个用户组,用户上机时,以对应的用户名上网注册,上网后自动进入相应的用户目录,在这一目录中用户具有写盘权限,其他用户则不能访问这一目录。

具体步骤为:

(1)网络系统建好后,对各工作站进行编号,同时将各工作站的节点地址号(NODE ADDRESS)记下,使工作站编号与工作站地址号对应起来(通过系统提供的程序 USERLIST /A),如下表所示:

工作站编号	工作站节点地址号	用户登录名
1	0000211502FA	USER1
2	0000211503DA	USER2
3	000021000E89	USER3
……	……	……
50	000021150394	USER50

(2)用 SYSCON 程序建立用户组 USER 和属于这一用户组的用户成员(USER1, USER2, USER3……),这些成员共同享有该用户组在其他目录或文件中赋予的权限。这样在进行文件和目录的授权时,就可不必一个用户一个用户地分配,提高了工作效率。在硬盘中对于用户组中的每一个成员还需为其分配一个子目录作为其工作空间,该子目录必须具有排他性,不允许其他用户使用。

但在实际使用中,并非所有磁盘交换文件,临时文件均可以在任意目录存放,这里有两种情况:(1)如 BORLANDC++的交换文件就必须一个用户一个文件(该文件名由系统确定,所有用户的文件都同名),这样就不能将它们放在同一个目录中,这一点如前所述已解决(通过给每个用户一个子目录来实现);(2)AUTOCAD 的交换文件系统要求必须存放在一固定目

录，而且必须从该目录启动，这样又不能将各个用户的主目录作为交换文件、临时文件的存储目录。笔者经过实践，提出了解决方法并在机器上得到了验证，即在卷上设置一个根目录PUB，对该目录赋给所有用户均具有读写权限（象AUTOCAD的交换文件即存于此，同时在PUB子目录下建立若干二级子目录（USER1，USER2，USER3……），一个用户对应一个目录，对这些子目录再分别设定权限，规定其他用户不能访问（象BORLAND C++的交换文件即存放于此）。

下面给出了用SYSCON建立一个用户（下面只列出了一些必须设定的项目）的实例：

①USERNAME（用户名）：USER11

②HOME DIRECTORY（用户主文件）：ZQ/SYS:PUB/USER11

③GROUPS BELONGED TO（所在的组）：EVERYONE，USER

④STATION RESTRICTION（登录站点限制）：0000211502FA；USER1只能从1#工作站上网，该功能再配合后面的自动登录上网程序，可以进行学生上机考试而不会造成学生舞弊。

⑤TRUSTEE DIRECTORY ASSIGNMENT（访问权限设置）：对SYS:PUB设定R，F，W，C，E权，但是到此为止，对用户1的设置仍未达到前面的要求，由于对SYS:PUB设置了R，F，W，C，E权，而用户主目录都在PUB目录之下，根据对NOVELL网络中目录权限的继承关系（缺省继承权为[SRWCEMFA]，任一用户仍然可以对其他用户的主目录进行存取，显然不符合要求。为了解决这个问题，可以利用NOVELL NETWARE提供的继承权限屏蔽功能对有关目录进行处理。

⑥运行FILER程序，在主菜单中选择CURRENT DIRECTORY INFORMATION这一项，此时将弹出一个有关当前目录PUB:\USER1的信息，其中INHERITED RIGHTS MASK（继承权屏蔽）一栏中为[SRWCEMFA]，将其修改为[S]，这样就屏蔽了其他用户在USER1目录中的查看、修改、删除权，同时根据访问权分配原则，用户USER1仍然对目录PUB\USER1有[RMCEF]权。

⑦运行FLAGDIR程序将所有用户主目录（USER1，USER2，USER3……）的目录属性设定为DELETEINHIBIT（禁止删除），RENAMEINHIBIT（禁止更名），防止用户删除、修改自己的工作目录。

二、登录原稿（LOGIN SCRIPT）的建立

登录原稿最主要的目的是为使用者建立网络的环境。当使用者一打开电源，即可由自动批处理文件（AUTOEXEC.BAT）直接进入网中，而所有的网络上的相关设置（例如：路径及环境变量等）都可由登录原稿实现。登录原稿文件相当于DOS系统中的AUTOEXEC.BAT，当某一个用户登录成功后，网络系统就自动执行该用户文件中定义的各种操作，恰当地设置会给以后的操作带来方便。

登录原稿可分为三种类型：

1.系统登录原稿（SYSTEM LOGIN SCRIPT）

该文件名为NET $ LOG.DAT，是一文本文件，存放在SYS:\PUBLIC目录下，这个文件只有Supervisor才能修改和写入，所有用户一进入网络环境中都会自动执行此文件。

2.使用者登录原稿（USER LOGIN SCRIPT）

使用者登录原稿可以由Supervisor或USER在SYSCON的用户信息下建立。建好后存放在SYS:\MAIL目录的USER-ID下，名称为LOGIN，当进入网络后系统会先执行完SYSTEM LOGIN SCRIPT，再执行每一个用户都可以拥有的USER LOGIN SCRIPT（每个用户不同）。这个登录原稿可由使用者自己或Supervisor来规划操作环境。

3.缺省登录原稿（DEFAULT LOGIN SCRIPT）

缺省登录原稿放在LOGIN.EXE文件中，当您安装好网络，第一次进入网络中时，会发现有一些问候信息和磁盘驱动器的设置，这些都是执行缺省登录原稿的结果。如果用户没有建立自己的登录原稿（LOGIN SCRIPT），系统就会自动执行缺省的登录原稿。这个缺省登录原稿无法被看到，所以也无法对此登录原稿做修改。

一般作为系统管理员使用较多的是系统登录原稿，但如果是一个不熟练的使用者最好不要编辑该原稿，否则一不小心会造成整个系统的其他使用者无法使用。这里笔者给出一个系统登录原稿实例来说明如何设计：

```
MAP DISPLAY OFF ;不显示驱动器连接
SET USER = %LOGIN-NAME ;设定DOS环境变量USER，注册完毕后通过该变量获得当前用户名
MAP INS S1:=SYS:LOGIN ;将第一台搜索磁盘驱动器指向目录SYS:LOGIN，让每一位使用者都能方便地使用LOGIN目录下的命令。
MAP INS S2:=SYS:PUBBAT ;将第二台搜索磁盘驱动器指向目录SYS:PUBBAT，让每一位使用者都能方便地使用PUBBAT目录下的公用批处理命令（如UCDOS.BAT，ACIOS.BAT，UP.BAT AC.BAT等）。
MAP INS S3:=SYS:PUBLIC ;将第三台搜索磁盘驱动器指向目录SYS:PUBLIC，让每一位使用者都能方便地使用PUBLIC目录下的命令。
MAP INS S4=SYS:DOS ;将第四台搜索磁盘驱动器指向目录SYS:DOS，其目的为让每一位使用者都能方便地使用DOS目录下的命令。
COMSPEC = S1:COMMAND.COM ;设置COMSPEC到有COMMAND.COM的磁盘驱动器，目的是使用户退出应用程序时不必再从A盘或F盘上读COMMAND.COM，而直接从内存中读取，加快速度，提高执行效率。
```

MAP *1:=SYS:\LOGIN-NAME；将第一台可用的网络驱动器指向用户的主目录。

MAP "%1"="SUPERVISOR" THEN MAP *1:=SYS:\SYSTEM；判断进入网络的使用者为 SUPERVISOR 时，即将第一台网络磁盘驱动器设置到 SYS:SYSTEM 中。

SET TEMP="G:\PUB\&LOGIN-NAME"；设置 DOS 临时环境变量 TEMP。

SET PROMPT="PG"；使用当前路径作为 DOS 的提示符。

MAP DISPLAY ON；登录时显示驱动器连接。

MAP；显示已建立的驱动器连接。

在设计过程中，必须注意：不管是搜索磁盘驱动器或网络磁盘驱动器要用 MAP 映射到某一目录时，必须事先将目录的权限开放给该使用者（至少要有 READ 和 FILE SCAN），否则会出现错误信息－－－"ATTEMPT TO MAP DRIVE INVALID PATH IN MAP COMMAND"。登录结束后，将出现 DOS 提示符 F:\PUB\USER11>，此时用命令 SET 查看 DOS 的环境变量设置，会发现已经有一个变量 USER=USER11，通过在批处理中加入：CD\PUB\%USER%，就可以自动进入用户的用户主目录中。

三、设置过程中常见的几个问题

1.在只有软驱或无盘情况下如何实现第一网驱始终为 F：

这点表面看起来不重要，但实际使用过程中碰到很多麻烦。如果整个网络中使用的均是无盘工作站，但并不是每一台都真正不含软驱，假如出于安全的考虑，在一些工作站的 BIOS 设置中均设定无盘，那么启动成功后（无登录原稿），第一网驱为 A:（映射卷的根目录），另一些工作站的 BIOS 设置为有 A:1.44 软驱，那么这些工作站启动成功后（无登录原稿），第一网驱为 F:（映射卷的根目录），这两种情况中对于同一目录却是不同的驱动器名，引起了混乱，并给一些程序的运行提供了麻烦，诸如 UCDOS 子目录中 UCDOS.BAT 和 UP.BAT 无法执行（命令前含路径），WINDOWS 无法运行（不能在 A 盘运行），WPS NT、一些教学软件、天汇汉字系统无法运行（不能在 A 盘运行）。所以根据上述情况，我们为了系统安全不能将软驱开放，同时为了使第一网驱为 F:又必须将软驱开放，两者似乎很难统一，但笔者经过大量实践，结果找到了一条捷径：将 BIOS 设置中的 B 驱设定为 1.2M，A 驱设定为无，同时将 BIOS 的 ADVANCED SETUP 栏目中的 FLOPPY DRIVE SEEK AT BOOT 设定 DISABLE，即可实现网络启动后第一网驱为 F:。

2.如何实现系统的自动登录

NOVELL 网络用户在登录上网时，都必须要先运行 LOGIN.EXE，然后输入用户名，才能注册上网，有时如果某台机器属于某人专用，或者在教学网上许多老师愿意上机考试已检验学生的动手能力（教师只要让同学在指定机器上做题即可），则可省略登录步骤，就可以让系统自己根据工作站的网络节点地址（Node Address）确定用户名，实现自动登录上网。笔者利用 BORLAND C++3.1 编制了一段小程序如下：

```
//根据网络节点地址读取用户名的 C 程序－－－－GetName.C//
#include <stdio.h>
#include <dos.h>
#include <stdlib.h>
#include <string.h>
//系统主程序//
Void Main(){
char MyNodeAddress[50];//假设该网络中有 50 台工作站//
char UserName[4];//定义一个数组
UserName[1]="user";
GetNodeAddress(MyNodeAddress);//读出上网工作站网络节点地址//
GetUserName(MyNodeAddress, UserName);//通过已读出的上网工作站节点地址计算用户名//
UserName[3]=0x0a;//结束符//
UserName[4]='\0';//结束符//
printf("%s,", UserName);//输出用户名//
}
//对应于每个工作站的网络节点地址存放于 NodeAddress 数组中
char * NodeAddress[]={"0000211502FA","0000211503DA",
"…","000021150394"};
//根据用户使用的机器确定网络节点地址号的子程序
Void GetNodeAddress(char * MyNodeAddress){
    asm{
    mov ah,0xee
    int 0x21}
  sprintf(MyNodeAddress,"%4x%4x%4x",-cx,-bx,-ax);
}
//根据网络节点地址号和用户名的对应关系表和已读出的网络节点地址号确定用户名称//
Void GetUserName(char * MyNodeAddress, char * UserName){
    int xx;
    for (i=0;i<50;i++){
    if (! strcmp(MyNodeAddress, NodeAddress[i])){
      xx=(i/5+1)*10+i%5+1;
      itoa(xx, UserName[2],10);
    }
  }
}
```

该程序利用了 DOS 的管理功能将用户名这一结果作为 LOGIN 程序的输入，实现了自动注册上网。计算机由自启动 EPROM 启动后，将按用户名进入相应的用户主目录。具体使用为：用 GetName|Login 代替 AUTOEXEC.BAT 中的 Login 命令。

（来稿时间：1996 年 10 月）