

操作系统和数据库安全



windows

Sql server

linux

mysql

Windows简介

Microsoft Windows 2000	Windows NT 5.0
Microsoft Windows XP	Windows NT 5.1
Microsoft Windows Server 2003	Windows NT 5.2
Microsoft Windows Vista	Windows NT 6.0
Microsoft Windows Server 2008	Windows NT 6.0
Microsoft Windows 7	Windows NT 6.1
Microsoft Windows Server 2008 R2	Windows NT 6.1
Microsoft Windows 8	Windows NT 6.2
Microsoft Windows Phone 8	Windows NT 6.2
Microsoft Windows Server 2012	Windows NT 6.2

查看系统版本	ver
查看SP版本	wmic os get ServicePackMajorVersion
查看Hotfix	wmic qfe get hotfixid,InstalledOn
查看主机名	hostname
查看网络配置	ipconfig /all
查看用户	net user
查看开放端口	netstat -ano

账户安全

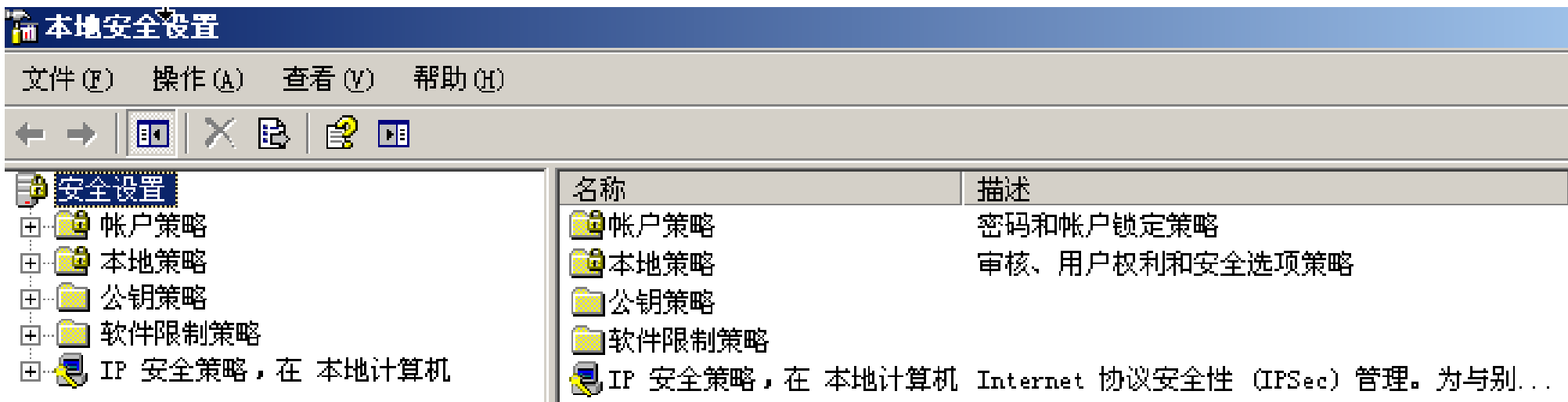
帐号相关命令之net user:

1. 查看账户abc的详细信息: `net user abc`
2. 创建（空密码）[删除] 账户abc: `net user abc /add [del]`
3. 创建普通账户abc，密码为123: `net user abc 123 /add`
4. 把abc加入 [退出] 管理员组: `net localgroup administrators abc /add [del]`
5. 启用[停用]账户abc: `net user abc /active:yes[no]`
6. 新建[删除]组admin: `net localgroup admin /add [del]`

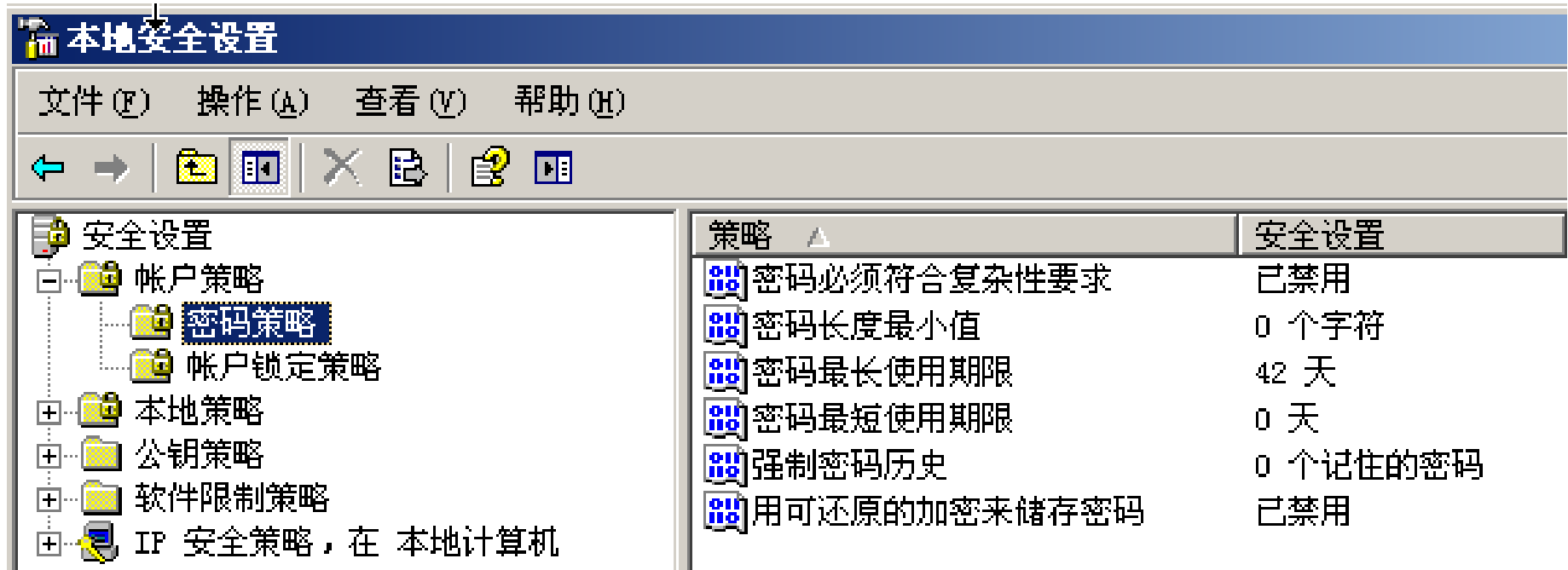
账号安全设置:

设置方法: “开始” -> “运行” 输入secpol.msc

立即启用: gpupdate /force



密码策略:



密码复杂度要求:

密码必须满足：**a**、长度至少为6个字符；**b**、密码字符必须来自大写字母、小写字母、数字、非字母符号中的三个。

帐号策略:

本地安全设置

文件(F) 操作(A) 查看(V) 帮助(H)

← → [Folder Icon] [List Icon] [Close Icon] [Print Icon] [Help Icon] [Full Screen Icon]

安全设置

- 帐户策略
 - 密码策略
 - 帐户锁定策略

策略	安全设置
复位帐户锁定计数器	30 分钟之后
帐户锁定时间	30 分钟
帐户锁定阈值	5 次无效登录

帐号安全选项相关:

安全设置

- 帐户策略
- 本地策略
 - 审核策略
 - 用户权限分配
 - 安全选项
- 公钥策略
- 软件限制策略
- IP 安全策略, 在 本地计算机

策略	安全设置
DCOM: 在安全描述符定义语言 (SDDL)语法...	没有定义
DCOM: 在安全描述符定义语言 (SDDL)语法...	没有定义
Microsoft 网络服务器: 当登录时间用完...	已启用
Microsoft 网络服务器: 数字签名的通信...	已禁用
Microsoft 网络服务器: 数字签名的通信...	已禁用
Microsoft 网络服务器: 在挂起会话之前...	15 分钟
Microsoft 网络客户端: 发送未加密的密...	已禁用
Microsoft 网络客户端: 数字签名的通信...	已启用
Microsoft 网络客户端: 数字签名的通信...	已禁用
故障恢复控制台: 允许对所有驱动器和文...	已禁用
故障恢复控制台: 允许自动系统管理级登录	已禁用
关机: 清除虚拟内存页面文件	已禁用
关机: 允许系统在未登录前关机	已禁用
交互式登录: 不显示上次的用户名	已启用

账户授权：

- 1.在本地安全设置中从远端系统强制关机只指派给Administrators组。
- 2.在本地安全设置中关闭系统仅指派给Administrators组。
- 3.在本地安全设置中取得文件或其它对象的所有权仅指派给Administrators。
- 4.在本地安全设置中配置指定授权用户允许本地登陆此计算机。
- 5.在组策略中只允许授权帐号从网络访问(包括网络共享等，但不包括终端服务)此计算机。

帐户数据库SAM文件:

1. 安全账号管理器的具体表现就是
%SystemRoot%\system32\config\sam文件。
2. sam文件是windows NT的用户帐户数据库,所有2K03/2k/NT用户的登录名及口令等相关信息都会保存在这个文件中。
3. sam文件可以认为类似于unix系统中的shadow文件,不过没有这么直观明了。

我们用编辑器打开这些NT的sam文件,除了乱码什么也看不到。因为NT系统中将这些资料全部进行了加密处理,一般的编辑器是无法直接读取这些信息的。注册表中的

HKEY_LOCAL_MACHINE\SAM\SAM

HKEY_LOCAL_MACHINE\SECURITY\SAM

保存的就是SAM文件的内容,在正常设置下仅对system是可读写的。

弱口令检测:

PWDUMP

```
C:\Documents and Settings\Administrator\桌面\tool\windows_tool\PwDump7>PwDump7.exe
PwDump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:68F86491C924D6A9AAD3B435B51404EE:6924734E3AC652450F514CD2A9590797:::
Guest:501:C2265B23734E0DACAAD3B435B51404EE:69943C5E63B4D2C104DBBCC15138B72B:::
SUPPORT_388945a0:1001:NO PASSWORD*****:437C812DF5B161DDFAD4D2E4C481C768:::
ASPNET:1012:5067E7BA320E1D3181B4B25857150328:A4EBBE833BD4996B24A80E6C43E52E8A:::
IUSR_LUHUI-1C:1022:5CBC9CA3C8BDAF4E3C2721224AD7D5CB:293B970A3FAAA5E66428F81B9C07C791:::
IWAM_LUHUI-1C:1023:0995A8E47E6125328E3EE3ECF90F8C87:6D522DF58094C4ADDB0F875AEA27B43D:::
haha:1025:E983166F205A35F1AAD3B435B51404EE:65589668D933A034BE6CEC5CCB619B45:::
```

LM

NT

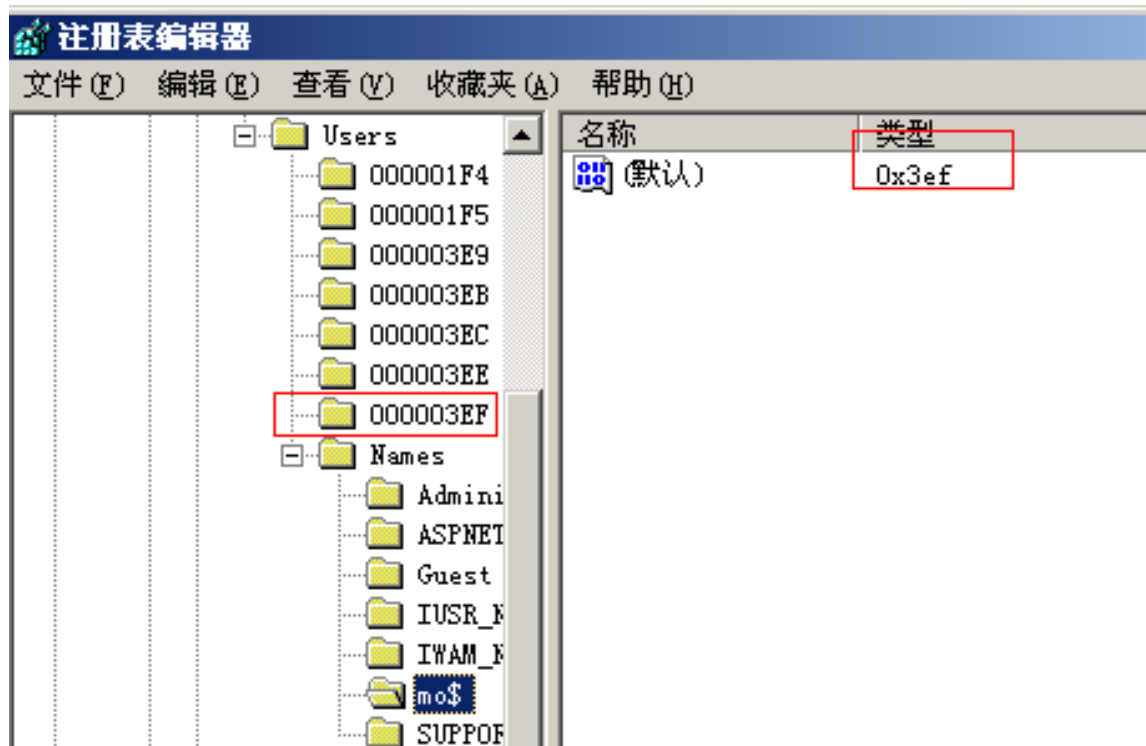
克隆administrator帐号:

1.创建隐藏帐号

2.打开注册表编辑器， 展开HKEY_LOCAL_MACHINE\SAM\SAM，
修改SAM权限为administrator完全控制

3.按F5刷新注册表， 展开

HKEY_LOCAL_MACHINE\SAM\SAM\Domains\account\user\names，
查看要克隆帐号的类型



4. 分别查看administrator的类型的F值和需要克隆的帐号类型的F值，并将administrator的F值复制覆盖要克隆的帐号的F值
5. 注销计算机，用克隆帐号登录，`net localgroup administrators`查看克隆帐号是否在administrators组里
6. 测试是否真实具有administrator的权限，新建用户并将其加入administrator组

```
C:\Documents and Settings\Administrator>net localgroup administrators
别名      administrators
注释      管理员对计算机/域有不受限制的完全访问权

成员

-----
mo$
test1
命令成功完成。
```

快速检查克隆帐号:

```
C:\Documents and Settings\Administrator\桌面\mt>mt.exe -chkuser
```

UserName	ExpectedSID	CheckedSID
Administrator	1F4	1F4
ASPNET	3EE	3EE
Guest	1F5	1F5
IUSR_NSFOCUS-FF23EDB	3EB	3EB
IWAM_NSFOCUS-FF23EDB	3EC	3EC
no\$	3EF	1F4
SUPPORT_388945a0	3E9	3E9
test1	3F0	3F0

Note : If CheckSID is different from ExpectSID, this account has been cloned!








Local Administrator Checker v0.9

Local Administrator Checker

Copyright(C) DragonSoft Security Associates 2002

Important

The scanner check Windows NT/2000/XP local permission, find out shadow administrator/clone administrator.

Account	Permission	Result
 Administrator	Administrators	
 ASPNET	Users	
 Guest	Guests	
 IUSR_NSFOCUS-...	Guests	
 IWAM_NSFOCUS...	Guests	
 mo\$	Users	Shadow Administrator?
 SUPPORT_38894...	Guests	



Windows克隆账号

目标：克隆账号与工具检查

文件权限控制

NTFS分区：

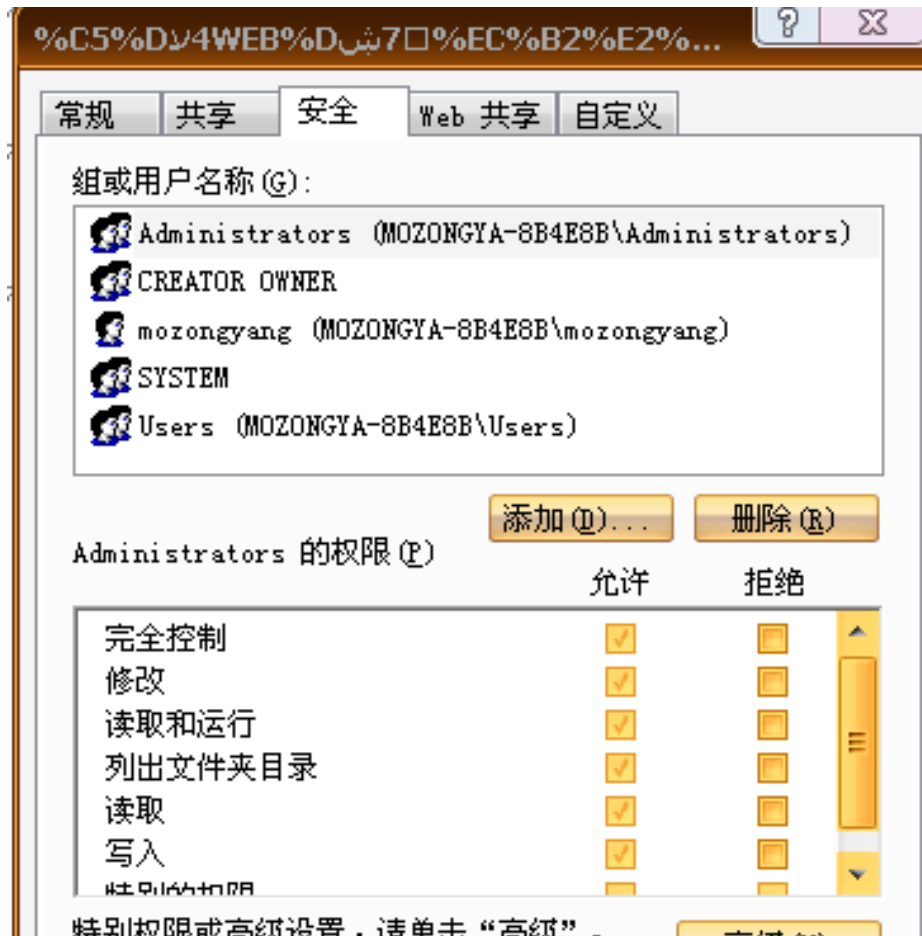
1. NTFS权限既影响网络访问者也影响本地访问者。
2. NTFS权限可以为驱动器、文件夹、注册表键值、打印机等进行设置。
3. 权限可以配置给用户或组，不同用户或组对同一个文件夹或文件可以有不同的权限

分区转换：

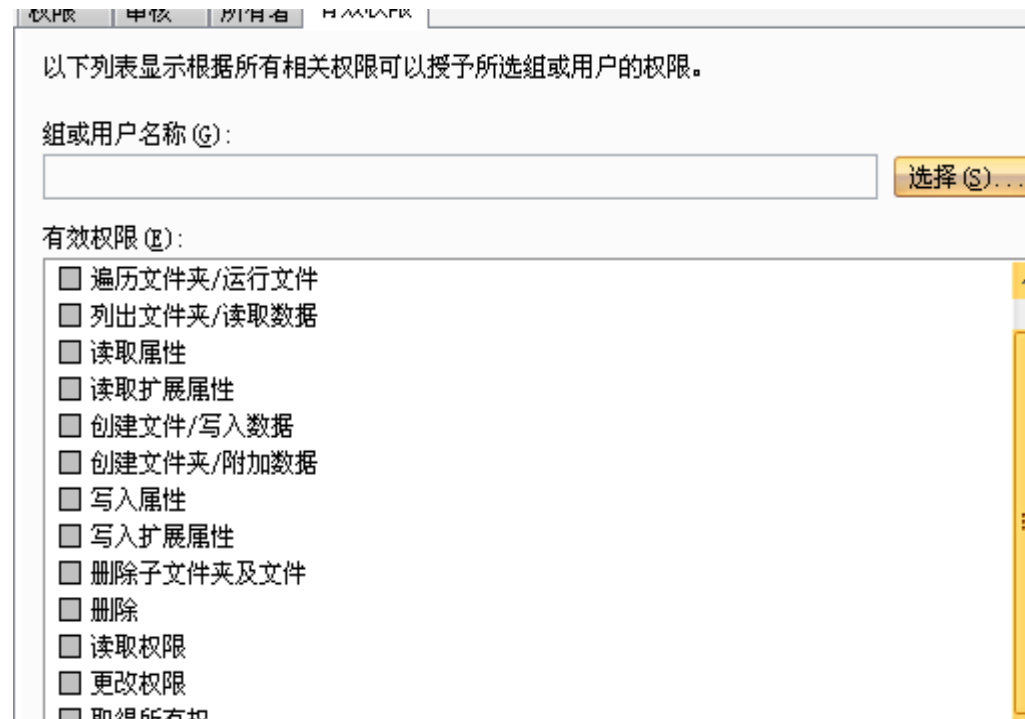
`convert D:/fs:ntfs`

注意：不可逆，只能将 FAT 或 FAT32 系统转换为 NTFS 系统，不能将 NTFS 系统转换成 FAT 或 FAT32 系统。如果必须转换，一般需要重新格式化磁盘。

ACL (access control list) 访问控制列表



ACE (Access control entry) 访问控制记录



权限的优先顺序:

每种权限都有“允许”和“拒绝”两种设置方法。

权限的来源有“直接设置”和“继承”两种。

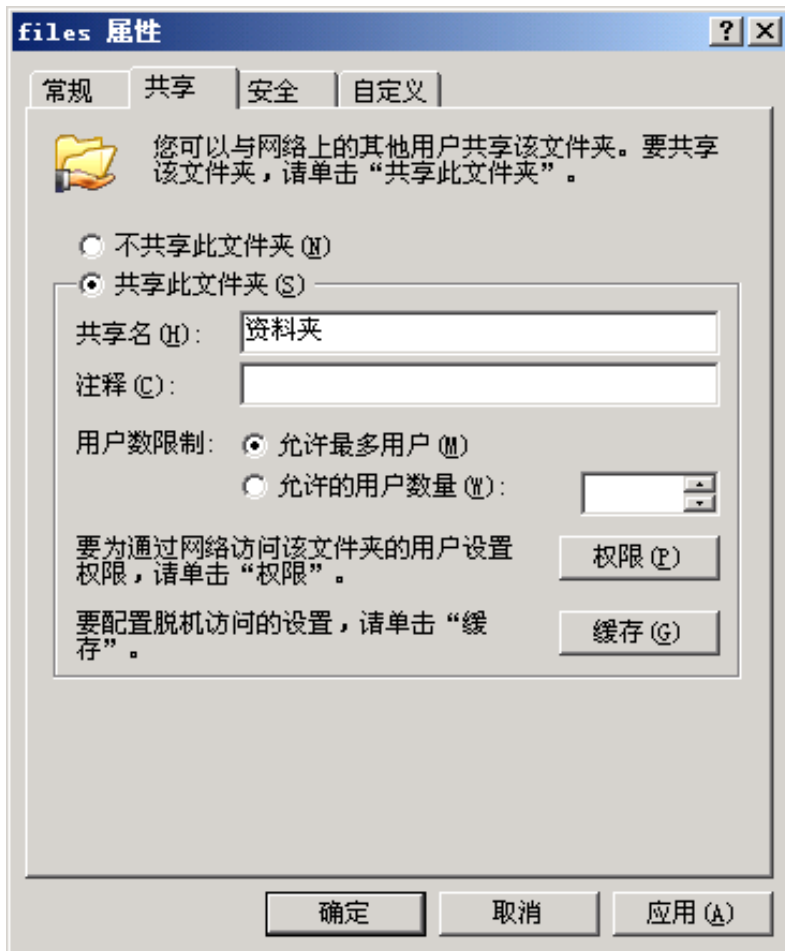
如果权限的设置出现矛盾，系统按下面的优先顺序确定权限：

直接设置的拒绝→直接设置的允许→继承的拒绝→继承的允许

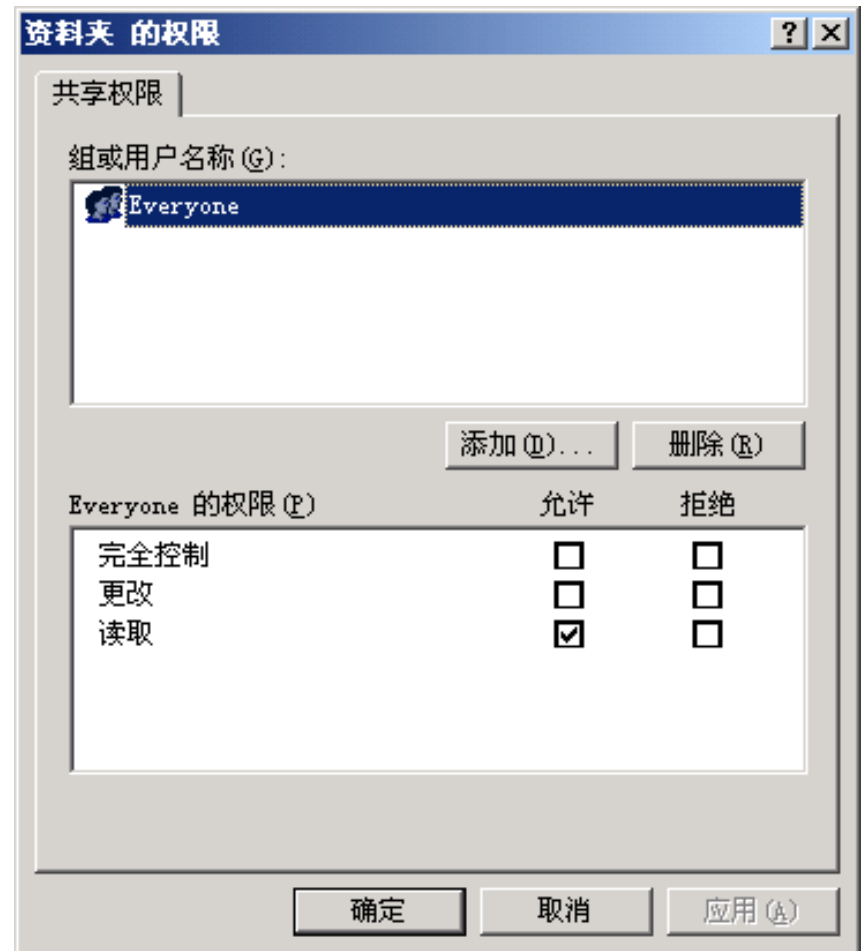
移动、复制对权限继承性的影响:

1. 在同一分区内移动文件或文件夹，权限保持不变。在不同分区间移动文件或文件夹，权限继承新位置的权限。
2. 复制文件或文件夹，权限会继承新位置的权限。
3. 把文件或文件夹移动或复制到FAT分区中时权限会丢失。

“共享”选项卡：



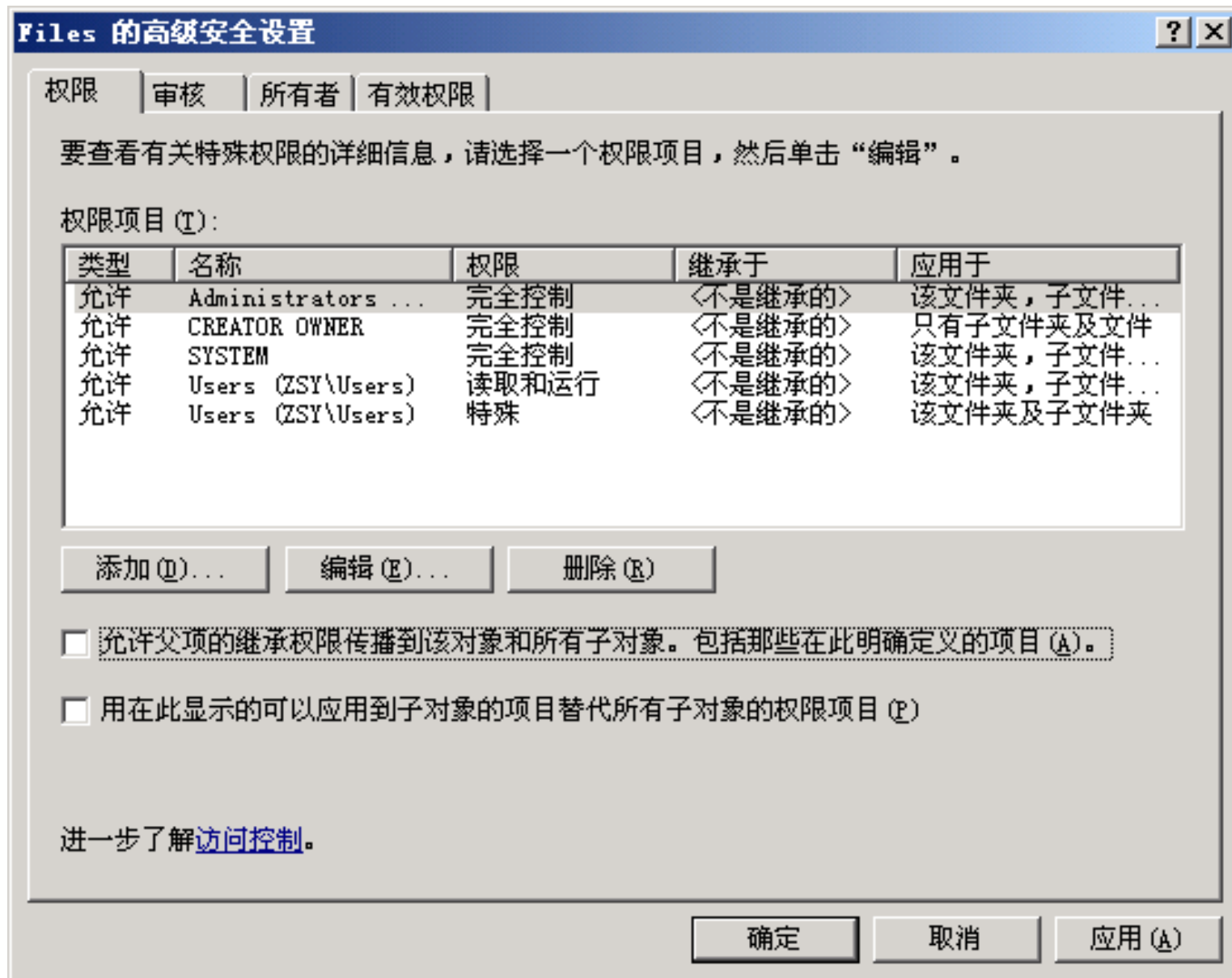
共享权限：



Windows 2003的默认共享权限是Everyone读取；

Windows 2000的默认共享权限是Everyone完全控制。

删除继承权限的方法:

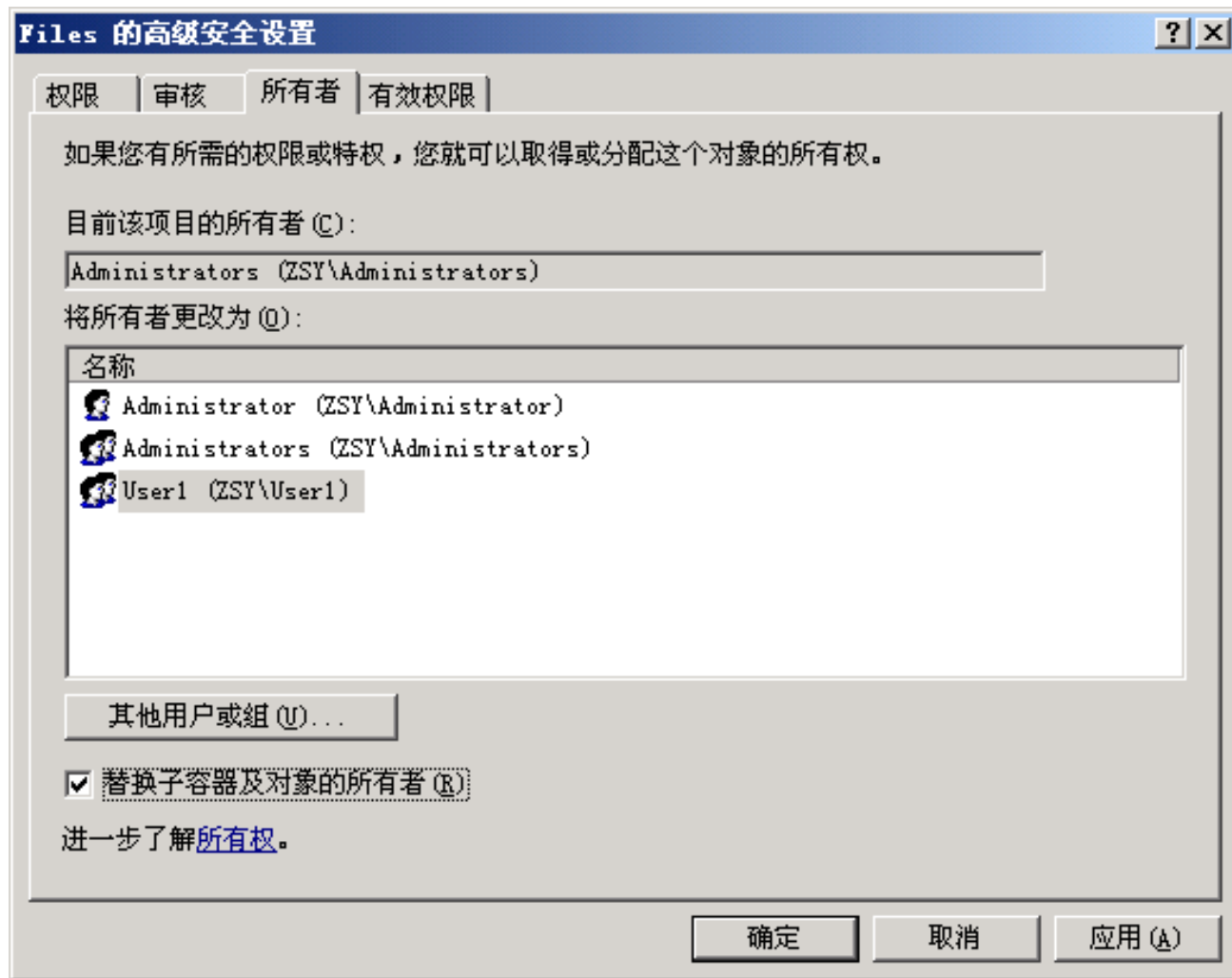


夺权：

只有两种人员可以抢夺所有权：

1、Administrators(管理员)组的用户；

2、拥有“获得所有权”这一特别权限的用户。



Windows系统管理

服务、进程与日志



服务



文件(F) 操作(A) 查看(V) 帮助(H)



服务(本地)



服务(本地)

选择一个项目来查看它的描述。

名称 ▲	描述	状态	启动类型	登录为	
.NET Runtime O...	Mic...		手动	本地系统	
Alerter	通...		禁用	本地服务	
Application Ex...	在...	已启动	自动	本地系统	
Application La...	为 ...		手动	本地服务	
Application Ma...	为 ...		手动	本地系统	
ASP.NET State ...	Pro...		手动	网络服务	
Automatic Updates	允...	已启动	自动	本地系统	
Background Int...	在...	已启动	自动	本地系统	
ClipBook	启...		禁用	本地系统	
COM+ Event System	支...	已启动	自动	本地系统	
COM+ System Ap...	管...	已启动	手动	本地系统	
Computer Browser	维...	已启动	自动	本地系统	
Cryptographic ...	提...	已启动	自动	本地系统	
DCOM Server Pr...	为 ...	已启动	自动	本地系统	
DHCP Client	为...	已启动	自动	网络服务	
Distributed Fi...	将...		手动	本地系统	
Distributed Li...	启...	已启动	自动	本地系统	
Distributed Li...	启...		禁用	本地系统	
Distributed Tr...	协...	已启动	自动	网络服务	
DNS Client	为...	已启动	自动	网络服务	
Error Reportin...	收...	已启动	自动	本地系统	
Event Log	启...	已启动	自动	本地系统	
File Replication	允...		手动	本地系统	
Help and Support	启...	已启动	自动	本地系统	

扩展 / 标准

Apache2.2

常规

登录

服务名称

显示名称

描述 (D):

可执行文

"d:\AppS

启动类型

服务状态

启动 (

当从此处

启动参数

Apache2.2 的

常规

登录

登录身份:

☒ 本地系统
 ☐ 允许

☐ 此帐户 (

密码 (P):

确认密码

您可启用或

硬件配置

Profile 1

Apache2.2 的

常规

登录

选择服务失

第一次失败

第二次失败

后续失败 (

重置失败计

重新启动服

运行程序

程序 (P)

命令行参

☐ 将失

Apache2.2 的属性 (本地计算机)

常规

登录

恢复

依存关系

一些服务依赖于其它服务、系统驱动程序和组的加载顺序。如果系统组件被停止或运行不正常，依赖于它的服务会受到影响。

Apache2.2

此服务依赖以下系统组件 (T)

+

AFD

TCP/IP Protocol Driver

以下系统组件依赖此服务 (F)

i

<无依存关系>

确定

取消

应用 (A)

cms

Docume

Inetpu

inst

Progra

UDiskM

wamp

WINDOW

wmpub

192.168.174.138/shell.php

192.168.174.138 (192.168.174.138)

[Logout](#) | [File Manager](#) | [MySQL Manager](#) | [MySQL Upload & Download](#) | [Execute Command](#) | [PHP Variable](#) | [Eval PHP Code](#)

Execute Program »

Program

c:\windows\system32\cmd.exe

Parameter

/c net start > C:/wamp/www/log.txt

Execute

Execute Command »

Use: phpfunc ▼

Command

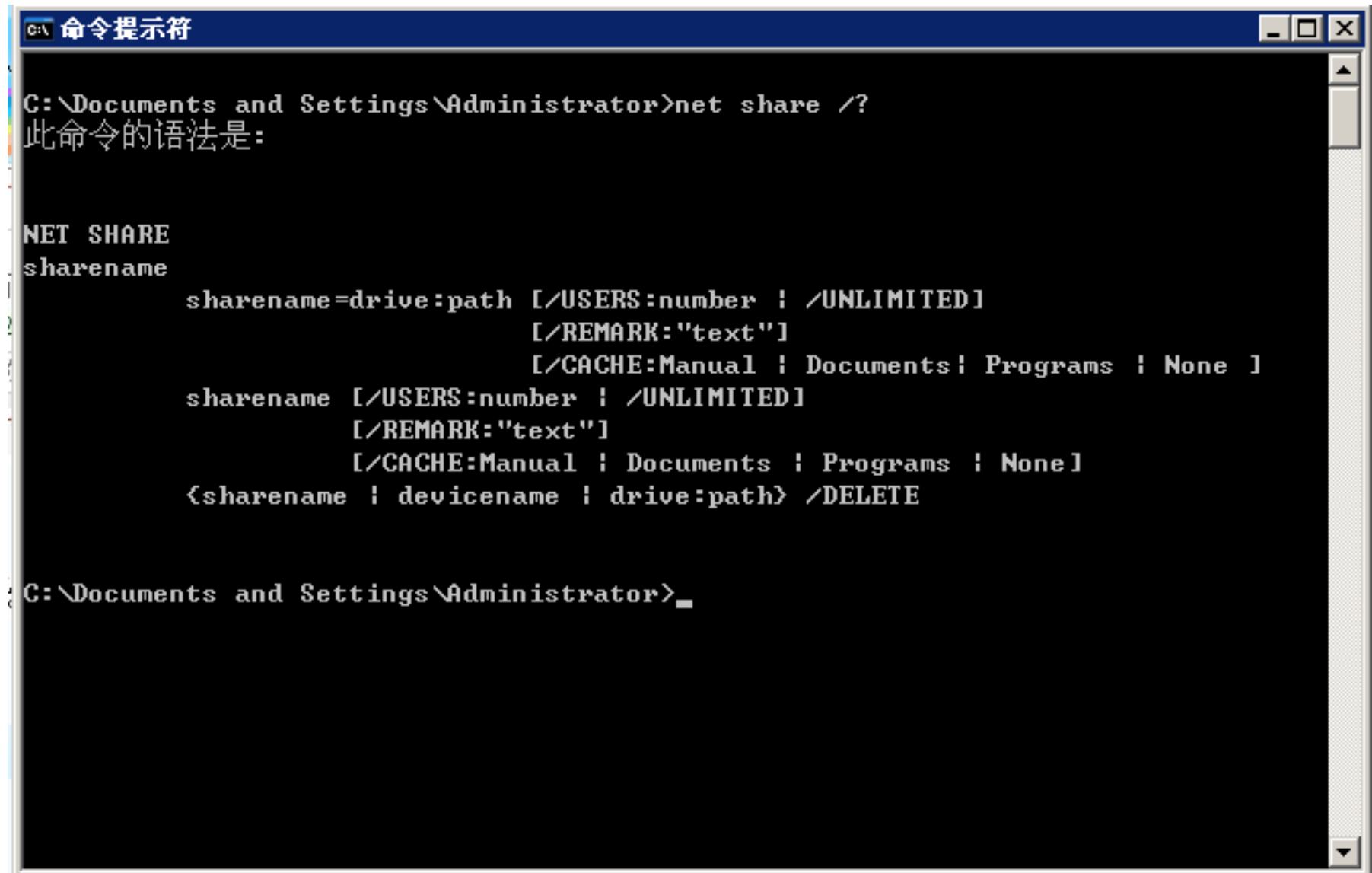
whoami

Execute

nt authority\network service

net share:

功能：文件或目录共享相关设置



```
C:\Documents and Settings\Administrator>net share /?
此命令的语法是:

NET SHARE
sharename
    sharename=drive:path [/USERS:number [/UNLIMITED]
                        [/REMARK:"text"]
                        [/CACHE:Manual | Documents | Programs | None ]
    sharename [/USERS:number [/UNLIMITED]
            [/REMARK:"text"]
            [/CACHE:Manual | Documents | Programs | None]
    {sharename | devicename | drive:path} /DELETE

C:\Documents and Settings\Administrator>
```

小实验：

1. 命令行下在c盘根目录创建文件夹nsfocus，使用net share 查看该共享。
2. 使用net share命令共享该文件夹并设置该文件夹权限为everyone 完全控制。
3. 使用net share命令删除该共享。

- net share nsfocus=c:\nsfocus /grant:everyone,full
- net share nsfocus /delete

query&&logoff:

功能：终端会话控制

```
C:\>query
```

无效参数

```
QUERY < PROCESS : SESSION : TERMSERVER : USER >
```

```
C:\>query user
```

用户名	会话名	ID	状态	空闲时间	登录时间
>administrator	console	0	运行中	.	2011-4-25 1:53
test1	rdp-tcp#2	2	运行中	.	2011-4-25 6:17

```
C:\>query user
```

用户名	会话名	ID	状态	空闲时间	登录时间
>administrator	console	0	运行中	.	2011-4-25 6:38
test1	rdp-tcp#2	2	运行中	2	2011-4-25 6:17

```
C:\>logoff 2
```

```
C:\>query user
```

用户名	会话名	ID	状态	空闲时间	登录时间
>administrator	console	0	运行中	.	2011-4-25 6:38

建议将以下服务停止，并将启动方式修改为手动：

Automatic Updates（不使用自动更新可以关闭）

Background Intelligent Transfer Service（不使用自动更新可以关闭）

DHCP Client

Messenger

Remote Registry

Print Spooler

Server（不使用文件共享可以关闭）

Simple TCP/IP Service

Simple Mail Transport Protocol (SMTP)

SNMP Service

Task Schedule

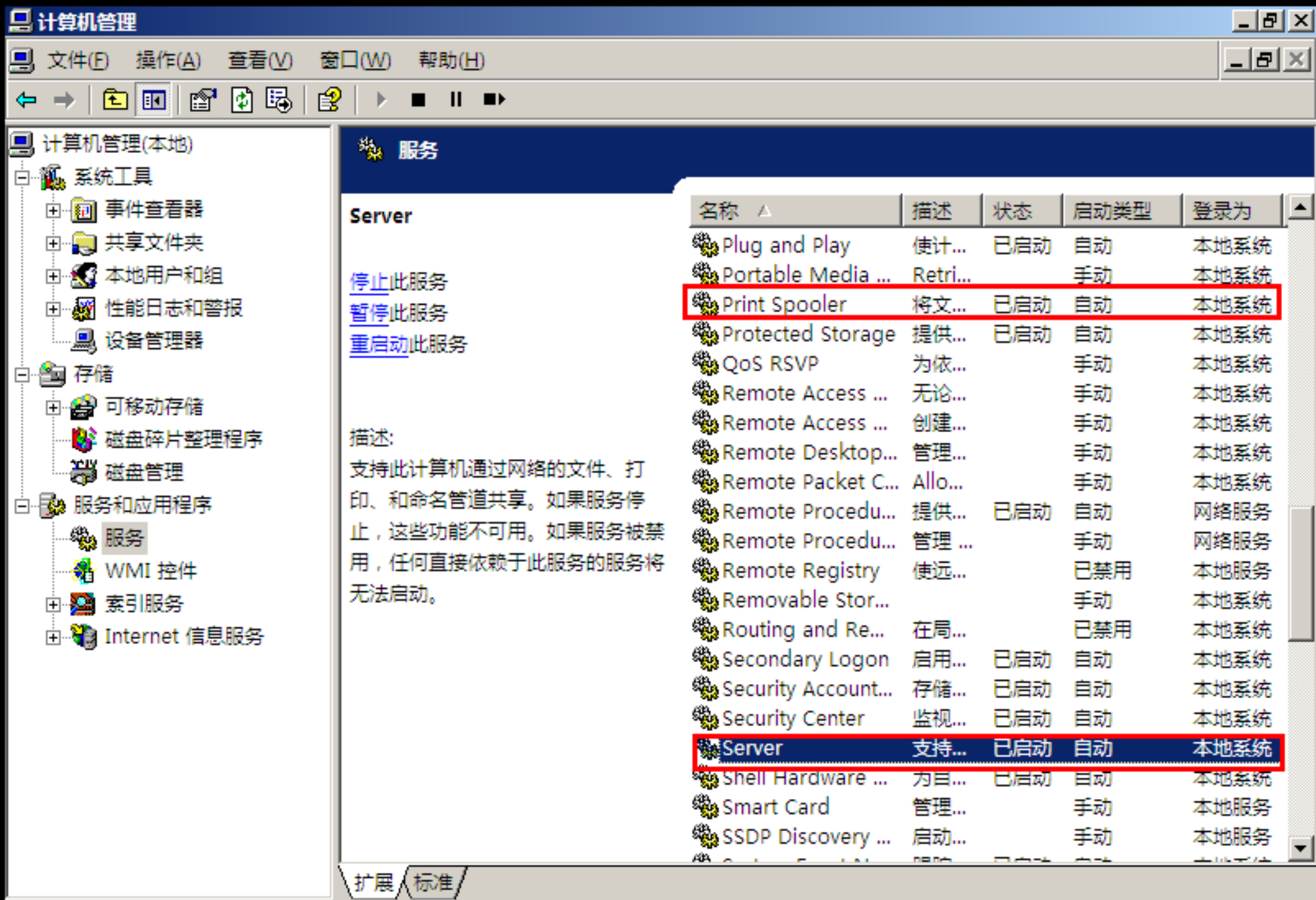
TCP/IP NetBIOS Helper



MS10061

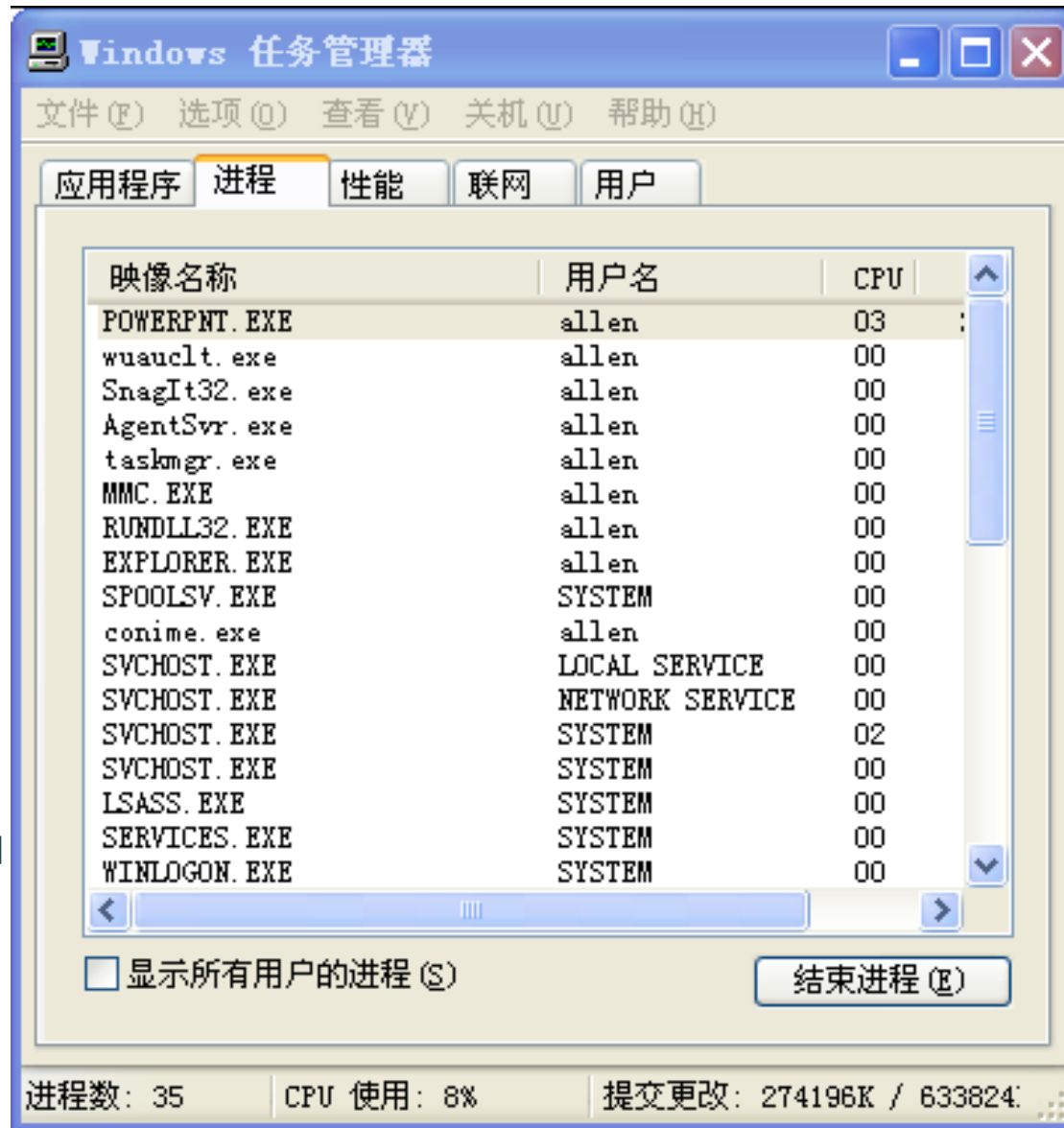


MS06040/MS08067.....



基本的系统进程

1. smss.exe Session Manager
2. csrss.exe 子系统服务器进程
3. winlogon.exe 管理用户登录
4. services.exe 包含很多系统服务
5. lsass.exe 管理 IP 安全策略以及启动 ISAKMP/Oakley (IKE) 和 IP 安全驱动程序。(系统服务)
6. svchost.exe 包含很多系统服务
7. spoolsv.exe 将文件加载到内存中以便迟后打印。(系统服务)
8. explorer.exe 资源管理器
9. internat.exe 输入法



Windows 任务管理器

文件 (F) 选项 (O) 查看 (V) 关机 (U) 帮助 (H)

应用程序 进程 性能 联网 用户

映像名称	PID	用户名	CPU	内存使用
conime.exe	5104		00	3,180 K
POWERPNT.EXE	4964		00	49,956 K
mmc.exe	4840		00	22,312 K
iexplore.exe	4664		02	211,836 K
iexplore.exe	4416		47	180,924 K
explorer.exe	3908		00	38,848 K
regedit.exe	3684		00	888 K
OUTLOOK.EXE	3648		00	13,740 K
QQExternal.exe	3620		01	81,216 K
iexplore.exe	3588		00	219,428 K
QQ.exe	3500		00	89,872 K
QQProtect.exe	3472		00	16,548 K
TTPlayer.exe	3436		01	3,936 K
iexplore.exe	3432		01	231,920 K
taskmgr.exe	3344		01	5,896 K
iexplore.exe	3000		00	14,436 K
wmiprvse.exe	2996		00	5,460 K
TrueCrypt.exe	2876		00	5,496 K
iexplore.exe	2760		02	185,180 K

☒ 显示所有用户的进程 (S)

结束进程 (E)

进程数: 59 CPU 使用: 56% 内存使用: 2193M / 4917M

Process Explorer - Sysinternals: www.sysinternals.com [LUHUI-1C\Administrator]

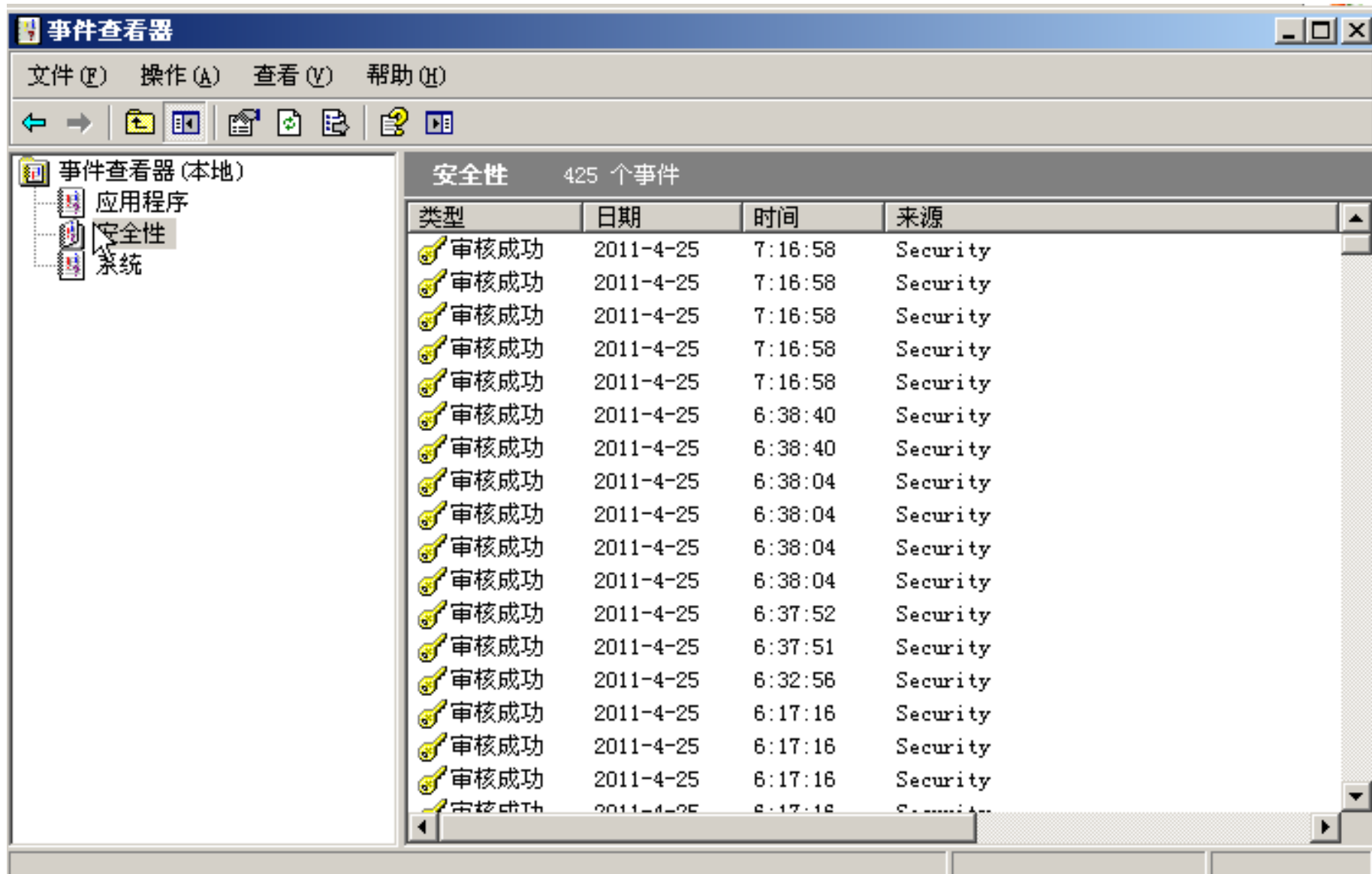
File Options View Process Find Users Help

Process	Private Bytes	Working Set	PID	Description	Company Name
MsDtsSrvr.exe	1,528 K	16,452 K	1264		Microsoft Corporation
sqlservr.exe	3,788 K	75,096 K	1420	SQL Server Windows NT	Microsoft Corporation
svchost.exe	444 K	1,956 K	1464	Generic Host Process ...	Microsoft Corporation
ReportingServices...	3,212 K	35,456 K	1480	Report Scheduling and...	Microsoft Corporation
locator.exe	812 K	2,500 K	1664	Rpc Locator	Microsoft Corporation
tlntsvr.exe	788 K	3,348 K	1720	Telnet	Microsoft Corporation
VMwareService.exe	1,492 K	5,164 K	1744	VMware Tools Service	VMware, Inc.
msftesql.exe	3,632 K	4,076 K	1804	PKM executable	Microsoft Corporation
svchost.exe	2,416 K	4,736 K	2040	Generic Host Process ...	Microsoft Corporation
dllhost.exe	2,480 K	7,452 K	2212	COM Surrogate	Microsoft Corporation
inetinfo.exe	3,416 K	9,180 K	3188	Internet Information ...	Microsoft Corporation
svchost.exe	3,032 K	5,984 K	3488	Generic Host Process ...	Microsoft Corporation
svchost.exe	7,404 K	11,948 K	3692	Generic Host Process ...	Microsoft Corporation
mysqld-nt.exe	3,956 K	13,672 K	3092		
httpd.exe	0,016 K	12,160 K	3264	Apache HTTP Server	Apache Software Fou...
httpd.exe	1,152 K	14,804 K	184	Apache HTTP Server	Apache Software Fou...
lsass.exe	3,020 K	9,504 K	456	LSA Shell	Microsoft Corporation
explorer.exe	1,396 K	26,524 K	3040	Windows Explorer	Microsoft Corporation
UDiskMonitor.exe	1,164 K	4,092 K	2444		
VMwareTray.exe	1,004 K	4,048 K	1200	VMware Tools tray app...	VMware, Inc.
VMwareUser.exe	1,916 K	5,896 K	2476	VMware Tools Service	VMware, Inc.
ctfmon.exe	564 K	3,052 K	3808	CTF Loader	Microsoft Corporation
cmd.exe	1,552 K	796 K	4072	Windows Command Proce...	Microsoft Corporation
conime.exe	500 K	2,652 K	2604	Console IME	Microsoft Corporation
nc.exe	468 K	1,496 K	1280		
cmd.exe	1,544 K	84 K	4076	Windows Command Proce...	Microsoft Corporation

日志在哪？

- Windows 日志文件默认位置是 “%systemroot%\system32\config
- 安全日志文件： %systemroot%\system32\config\SecEvent.EVT
- 系统日志文件： %systemroot%\system32\config\SysEvent.EVT
- 应用程序日志文件：
%systemroot%\system32\config\AppEvent.EVT
- FTP 连接日志和 HTTPD 事务日志：
%systemroot%\system32\LogFiles\

eventvwr.msc



审核策略:

本地安全设置

文件(F) 操作(A) 查看(V) 帮助(H)

安全设置

帐户策略

密码策略

帐户锁定策略

本地策略

审核策略

用户权限分配

安全选项

公钥策略

软件限制策略

IP 安全策略, 在 本地计算机

策略 ▲	安全设置
审核策略更改	无审核
审核登录事件	成功
审核对象访问	无审核
审核过程跟踪	无审核
审核目录服务访问	无审核
审核特权使用	无审核
审核系统事件	无审核
审核帐户登录事件	成功
审核帐户管理	无审核

windows/smb/ms06_040_netapi	2006-08-08	great
Microsoft Server Service NetpwPathCanonicalize Overflow		
windows/smb/ms06_066_nwapi	2006-11-14	good
Microsoft Services MS06-066 nwapi32.dll		
windows/smb/ms06_066_nwwks	2006-11-14	good
Microsoft Services MS06-066 nwwks.dll		
windows/smb/ms06_070_wkssvc	2006-11-14	manual
Microsoft Workstation Service NetpManageIPCCConnect Overflow		
windows/smb/ms07_029_msdns_zonename	2007-04-12	manual
Microsoft DNS RPC Service extractQuotedChar() Overflow (SMB)		
windows/smb/ms08_067_netapi	2008-10-28	great
Microsoft Server Service Relative Path Stack Corruption		
windows/smb/ms09_050_smb2_negotiate_func_index	2009-09-07	good
Microsoft SRV2.SYS SMB Negotiate ProcessID Function Table Dereference		
windows/smb/smb_relay	2001-03-31	excellent
Microsoft Windows SMB Relay Code Execution		
windows/smtp/ms03_046_exchange2000_xexch50	2003-10-15	good
MS03-046 Exchange 2000 XEXCH50 Heap Overflow		
windows/ssl/ms04_011_pct	2004-04-13	average
Microsoft Private Communications Transport Overflow		
windows/wins/ms04_045_wins	2004-12-14	great
Microsoft WINS Service Memory Overwrite		

组策略

文件(F) 操作(A) 查看(V) 帮助(H)

← → 文件夹 打印 帮助 刷新

“本地计算机”策略

- 计算机配置
 - 软件设置
 - Windows 设置
 - 管理模板
 - Windows 组件
 - NetMeeting
 - RSS 提要
 - Internet Exp...
 - 应用程序兼容...
 - 事件查看器
 - Internet 信息
 - 安全中心
 - 任务计划程序
 - 终端服务
 - Windows 资源
 - Windows Inst...
 - Windows Mess...
 - Windows Medi...
 - Windows Mov...
 - Windows Upda...
 - Windows Medi...

Windows Update

选择一个项目来查看它的描述。

设置	状态
不要在“关闭 Windows”对话框显示“安装更新并关机”	未被配置
不要调整“关闭 Windows”对话框里的“安装更新并关机...”	未被配置
配置自动更新	已启用
指定 Intranet Microsoft 更新服务位置	已启用
允许客户端目标设置	未被配置
重新计划自动更新的计划安装	未被配置
对于有已登录用户的计算机，计划的自动更新安装不执行...	未被配置
自动更新检测频率	未被配置
允许自动更新立即安装	已启用
对计划的安装延迟重新启动	未被配置
重新提示计划安装后的重新启动	未被配置
允许非管理员用户接收更新通知	未被配置
通过自动更新启用建议更新	已启用
启用 Windows Update 电源管理以自动唤醒系统来安装计...	未被配置
允许来自 intranet Microsoft 更新服务位置的签名内容	未被配置



windows

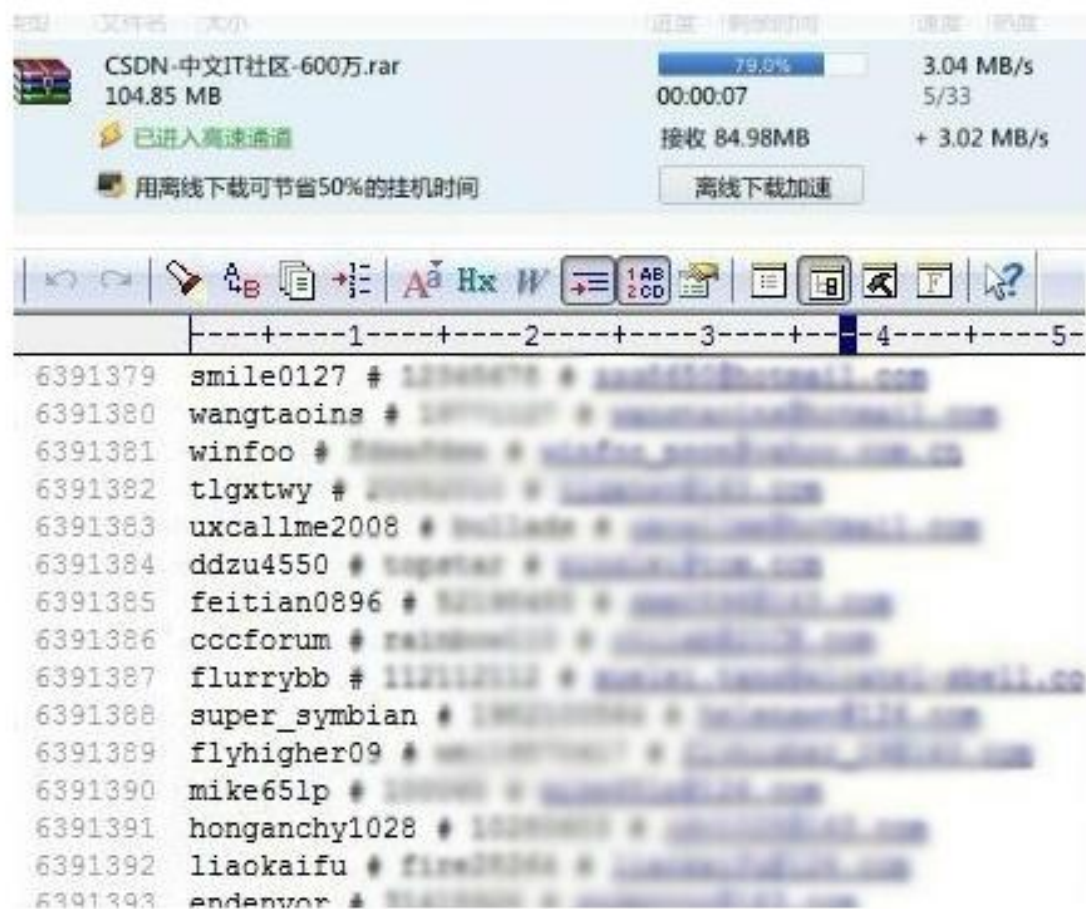
Sql server

linux

mysql

Sql Server 2005

CSDN被黑：600余万个明文的注册邮箱帐号和密码被黑客公开



WIN-ND870N4... dbo.cdsgus													
WIN-ND870N4... dbo.cdsgus													
Name	Ca...	Des...	CtfTp	CtfId	G...	Birthday	Address	Zip	D...	Distr...	Di...	D..	Distri...
陈			OTH	0	Id	QunNum	MastQQ	CreateDate	Title	Class	QunText		
王 兰			OTH	0	2	900007	1	2005-02-01	瞬间		18	VIP	...
陈			OTH	0	3	900009	5	2005-02-13	DotA		398	Dot	...
裴			OTH	0	4	900010	1	2005-02-01	9000		3	901	...
曹			ID	3	5	900012	3	2005-02-01	9000		393		...
孙			ID	3	6	900018	1	2005-02-01	FOR		20	Join	...
jing			ID	4	7	900021	1	2005-05-11	猎豹		3747		...
潘 鹏			ID	3	8	900022	16	2005-08-04	银色		4266		...
徐 鸣			ID	4	9	900023	2	2006-02-12	9000		3499		...
陈			ID	2	10	900024	4	2005-05-11	耿直		2211	dfgc	...
吴 龙			ID	3	11	900025	1	2005-07-06	9000		55		...
王			ID	3	12	900027	1	2005-02-01	深圳		78	内部	...
周 华			ID	3	13	900028	1	2007-05-27	9000		20		...
王 蓉			ID	6	14	900030	9	2005-02-01	伟意		369	详细	...
于			ID	5	15	900031	7	2005-02-01	以人		5	内部	...
袁			ID	5	16	900033	2	2005-05-11	后备		56
胡			OTH	2	17	900035	12	2005-02-01	じ☆		18	照片	...
石			ID	3	18	900036	1	2005-02-01	安兴		395	联系	...
朱 维			ID	3	19	900037	13	2005-05-11	``刘		2814	此群	...
钟			ID	3	20	900040	170	2005-02-01	三码		3507	http	...
徐 峰			ID	3	21	900042	1	2005-05-11	1		1283	1	...
王 蕊			ID	2	22	900043	9	2005-05-11	煙銷		2556	記不	...
					23	900044	20	2006-03-21	临时		161		...
					24	900046	72	2005-05-20	『自		395	此群	...
					25	900048	1	2005-02-01	9000		2		...
					26	900049	3	2005-05-24	123		57		...
					27	900050	31	2005-02-01	彩票		2	承接	...
					28	900051	26	2007-08-17	牵手		1525	杭州	...
					29	900052	2	2005-07-10	9000		305		...

100G的QQ群信息泄露

社工库

89[REDACTED]79

搜

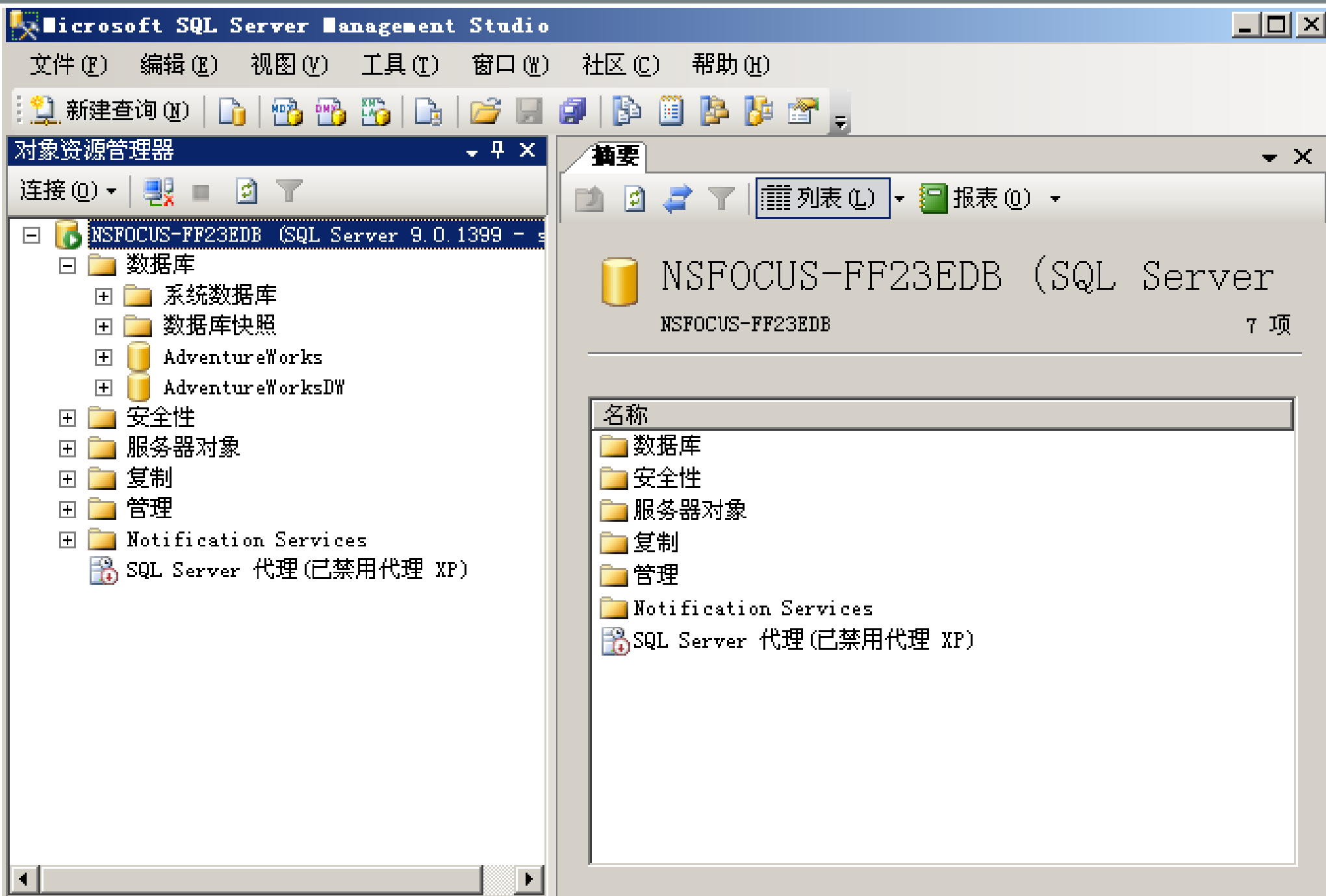
结果

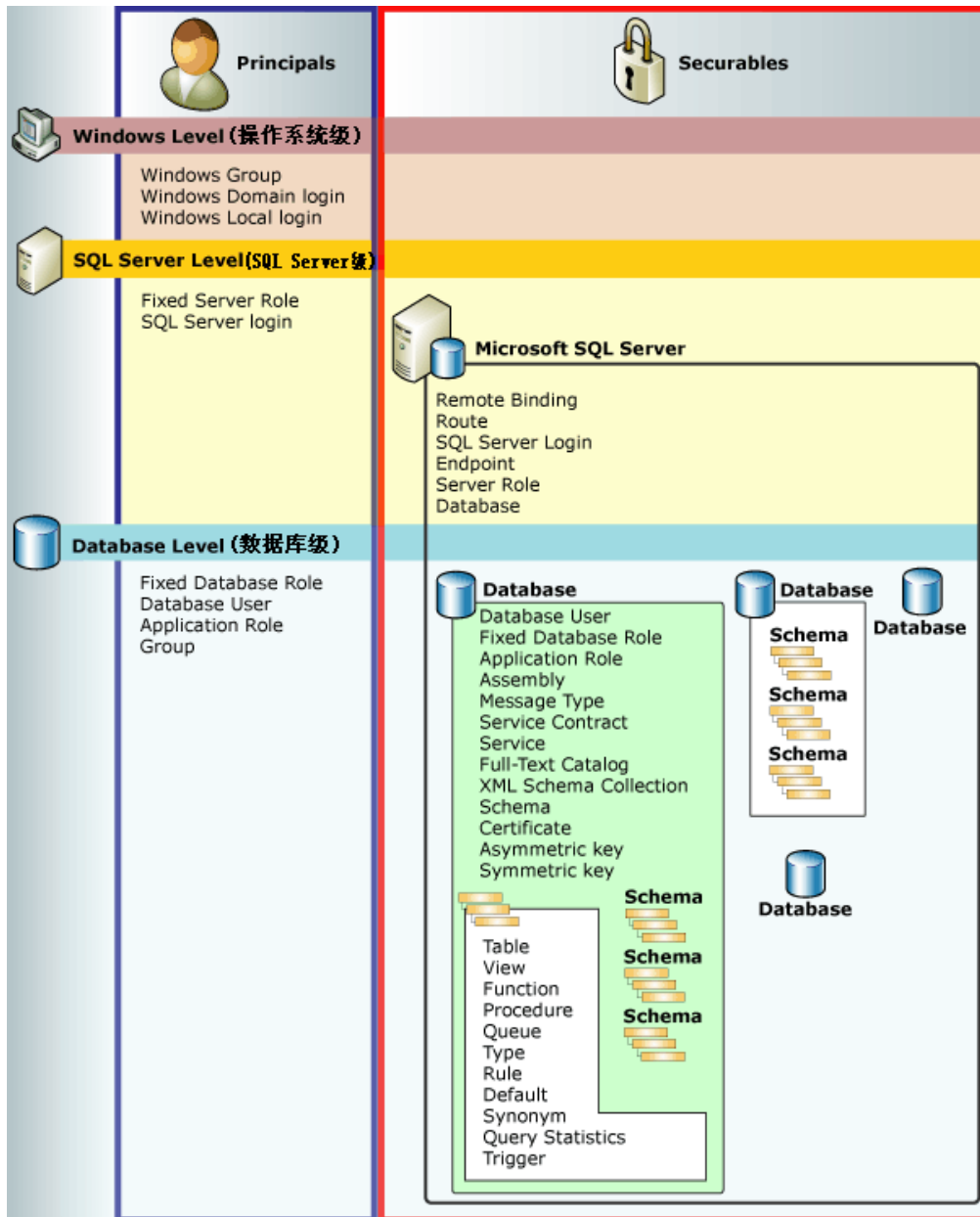
[下一页](#)

893[REDACTED]279, AZJS[REDACTED]#2134

893[REDACTED]279, AZJS[REDACTED]#2134

893[REDACTED]279, AZJS[REDACTED]#2134





操作系统本身的安全

Sqlserver的安全：
管理和设计合理的登录方式

数据库安全：
库、表、列等权限

Sql语句基础

<http://www.w3school.com.cn/sql/>

- SQL 分为两个部分：数据定义语言 (DDL)和数据操作语言 (DML)
 - SQL 的数据定义语言 (DDL) 部分提供了创建或删除表格，也可以定义索引（键），规定表之间的链接，以及施加表间的约束
 - SQL 的操作语言（DML）包含用于更新、插入和删除记录的语法

- 建库 Create database

Create database database_name

例：Create database member

- 进入数据库 use database

例：use member

- 建表 create table table_name

CREATE TABLE 表名称 (列名称1 数据类型, 列名称2 数据类型, 列名称3 数据类型,)

例：create table user(id int, name varchar(255), age int, city varchar(255))

- 删除数据库和表 DROP

例：drop table user

Drop database member

- 增 INSERT

INSERT INTO 表名 (列1, 列2,...) VALUES (值1, 值2,...)

例：insert into user (name,age) values ('xiaowang','20')

- 删 DELETE

DELETE FROM 表名称 WHERE 列名称 = 值

例：delete from user where age='20'

- 改 UPDATE

UPDATE 表名称 SET 列名称 = 新值 WHERE 列名称 = 某值

例：update user set city='beijing' where name='xiaochen'

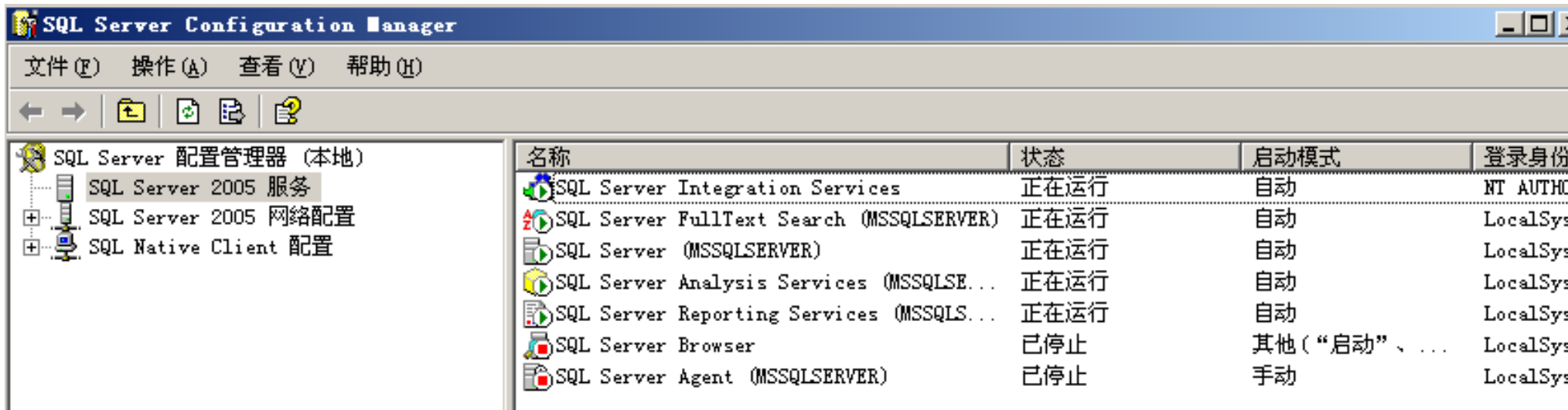
- 查 select

select 字段 from 数据库.表名 where 查询条件。

例：select name from user where name='xiaoli'

Sql Server 2005服务器级管理

服务管理:



The screenshot shows the SQL Server Configuration Manager window. The left pane displays the tree structure under 'SQL Server 配置管理器 (本地)'. The right pane shows a list of services with their status, start mode, and logon identity.

名称	状态	启动模式	登录身份
SQL Server Integration Services	正在运行	自动	NT AUTHO...
SQL Server FullText Search (MSSQLSERVER)	正在运行	自动	LocalSys...
SQL Server (MSSQLSERVER)	正在运行	自动	LocalSys...
SQL Server Analysis Services (MSSQLSE...)	正在运行	自动	LocalSys...
SQL Server Reporting Services (MSSQLS...)	正在运行	自动	LocalSys...
SQL Server Browser	已停止	其他(“启动”、...	LocalSys...
SQL Server Agent (MSSQLSERVER)	已停止	手动	LocalSys...

连接到服务器

Microsoft
SQL Server 2005



服务器类型 (T):

数据库引擎

服务器名称 (S):

LUHUI-1C

身份验证 (A):

SQL Server 身份验证

登录名 (L):

sa

密码 (P):

☐ 记住密码 (M)

连接 (C)

取消

帮助

选项 (O) >>

系统数据库:

Microsoft SQL Server Management Studio

文件(F) 编辑(E) 视图(V) 项目(P) 工具(T) 窗口(W) 社区(C) 帮助(H)

新建查询(N) [Icons]

对象资源管理器

连接(O) [Icons]

NSFOCUS-FF23EDB (SQL Server 9.0.1399 - s)

数据库

系统数据库

- master
- model
- msdb
- tempdb

数据库快照

AdventureWorks

AdventureWorksDW

安全性

服务器对象

复制

管理

Notification Services

SQL Server 代理 (已禁用代理 XP)

摘要

列表(L) 报表(R)

系统数据库

NSFOCUS-FF23EDB\数据库\系统数据库 4 项

名称
master
model
msdb
tempdb

系统库	功能
Master数据库	作用是控制用户数据库和SQL Server的操作，记录SQL Server实例的所有系统信息包括用户帐户、可配置的环境变量、系统错误消息、用户数据库信息等。一旦master数据库被破坏，SQL Server将无法启动。
MsdB数据库	用于SQL Server代理计划警报和作业。
Model数据库	用作SQL Server实例上创建的所有数据库模板。对model进行修改(如数据库大小、排列顺序、恢复模式和其他数据库选项)将用于以后创建的所有数据库。因为SQL Server每次启动时都要创建Tempdb，因此model数据库始终存在于SQL Server系统中。
Tempdb数据库	只是为SQL Server提供一个工作空间，满足临时表及其他临时的工作存储需要，用于保存临时对象或中间结果集。每次启动SQL Server时，都会重新创建tempdb，以便系统启动时，该数据库是空的，在断开连接时会自动删除。

登录帐号:

连接 (U)

NSFOCUS-FF23EDB (SQL Server 9.0.1399 - mo)

数据库

安全性

登录名

BUILTIN\Administrators
mo
NSFOCUS-FF23EDB\SQLServer2005MSFTEUser\$
NSFOCUS-FF23EDB\SQLServer2005MSSQLUser\$
NSFOCUS-FF23EDB\SQLServer2005SQLAgentU\$
NT AUTHORITY\SYSTEM
sa

服务器角色

凭据

服务器对象

复制

管理

维护计划

SQL Server 日志

活动监视器

数据库邮件

分布式事务处理协调器

列表 (L)

报表 (Q)

登录名

NSFOCUS-FF23EDB\安全性\登录名

7 项

名称

BUILTIN\Administrators
mo
NSFOCUS-FF23EDB\SQLServer2005MSFTEUser\$NSFOCUS-
NSFOCUS-FF23EDB\SQLServer2005MSSQLUser\$NSFOCUS-
NSFOCUS-FF23EDB\SQLServer2005SQLAgentUser\$NSFOCUS-
NT AUTHORITY\SYSTEM
sa

Sql server账户登录

用户映射:

设置SQL Server登录名到数据库用户的映射。登录名是登录sql server用的，但是要进入具体的数据库需要数据库用户。默认登录名和数据库用户名一样，首次创建用户默认架构是dbo

选择页

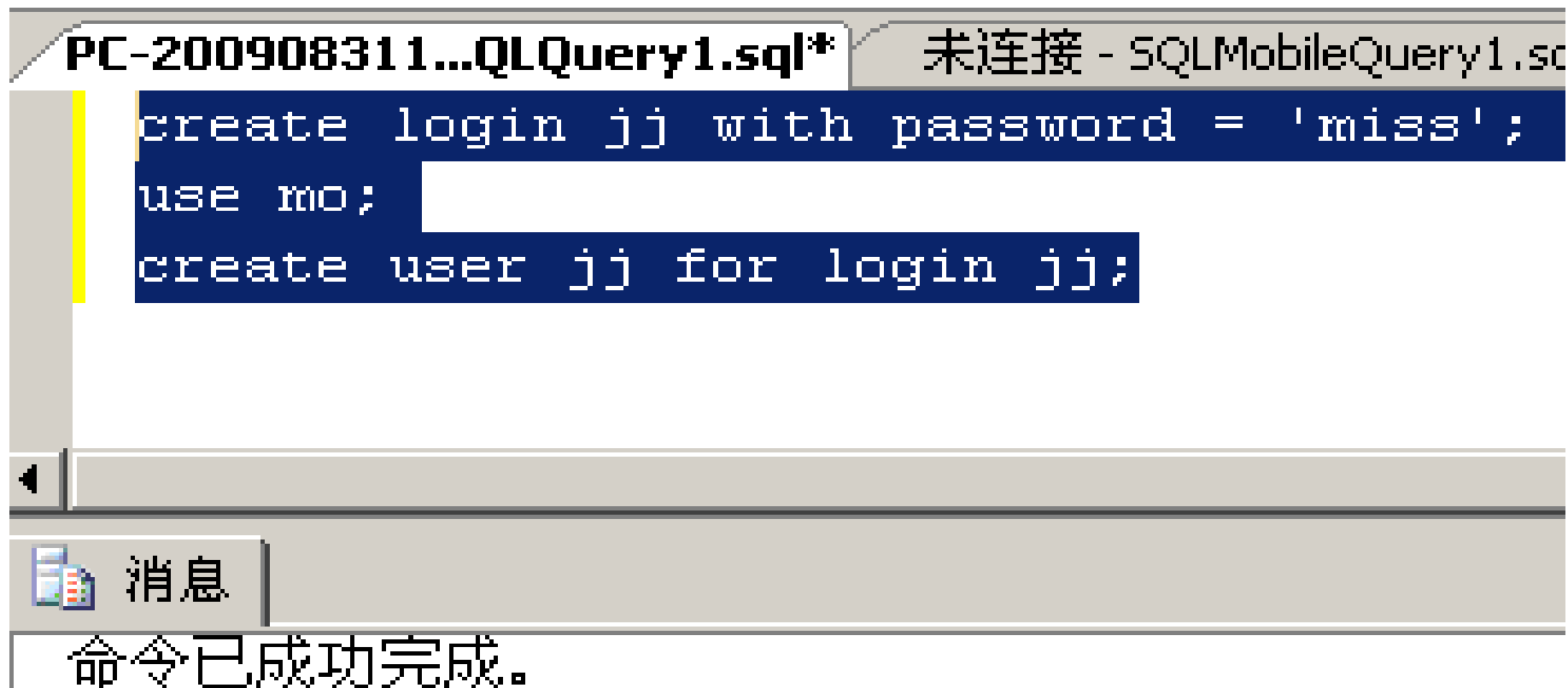
- 常规
- 服务器角色
- 用户映射**
- 安全对象
- 状态

脚本 帮助

映射到此登录名的用户 (U):

映射	数据库	用户	默认架构
<input type="checkbox"/>	AdventureWorks		
<input type="checkbox"/>	AdventureWorksDW		
<input type="checkbox"/>	master		
<input checked="" type="checkbox"/>	mo	mo	dbo
<input type="checkbox"/>	model		
<input type="checkbox"/>	msdb		
<input type="checkbox"/>	tempdb		

创建登陆用户jj，对应mo数据库，创建数据库用户jj对应登陆用户jj



The screenshot shows a SQL Server Enterprise Manager window. The title bar indicates the connection is '未连接 - SQLMobileQuery1.sc'. The active query window is titled 'PC-200908311...QLQuery1.sql*'. The SQL text entered is:

```
create login jj with password = 'miss';  
use mo;  
create user jj for login jj;
```

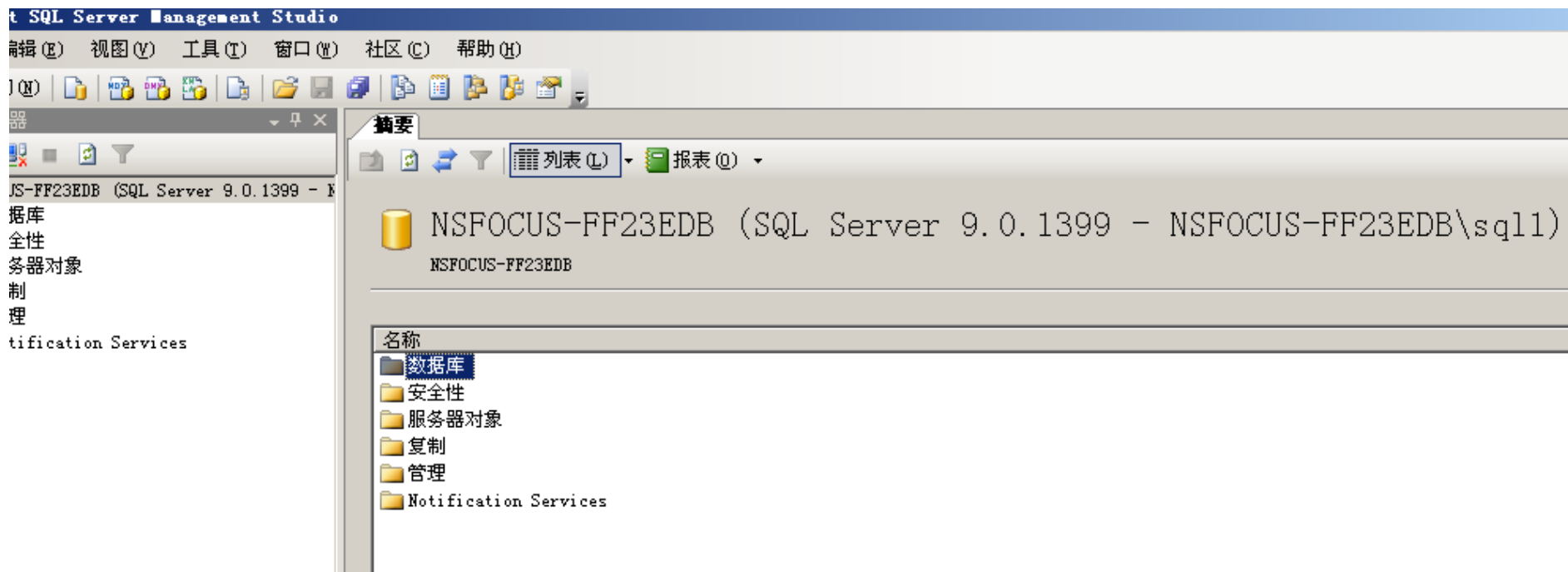
At the bottom of the window, a status bar displays the message: 命令已成功完成。 (Command successfully completed.)

Windows本地登录:

1.创建用户和用户组

2.建立sqlserver登录

3.使用新的用户登录



服务器角色:

The screenshot displays the Microsoft SQL Server Enterprise Manager interface. On the left, the '对象资源管理器' (Object Explorer) pane shows the tree structure of the 'NSFOCUS-FF23EDB' server. The '安全性' (Security) folder is expanded, and the '服务器角色' (Server Roles) folder is selected. The list of roles includes: bulkadmin, dbcreator, diskadmin, processadmin, securityadmin, serveradmin, setupadmin, and sysadmin. On the right, the '摘要' (Summary) pane for '服务器角色' is shown, displaying a list of the same roles. The 'sysadmin' role is currently selected in the list.

Microsoft SQL Server Management Studio

文件(F) 编辑(E) 视图(V) 工具(T) 窗口(W) 社区(C) 帮助(H)

新建查询(N) [Icons]

对象资源管理器

连接(O) [Icons]

NSFOCUS-FF23EDB (SQL Server 9.0.1399 - mo)

- 数据库
- 安全性
 - 登录名
 - 服务器角色
 - bulkadmin
 - dbcreator
 - diskadmin
 - processadmin
 - securityadmin
 - serveradmin
 - setupadmin
 - sysadmin
 - 凭据
- 服务器对象
- 复制
- 管理
- Notification Services
- SQL Server 代理 (已禁用代理 XP)

摘要

服务器角色

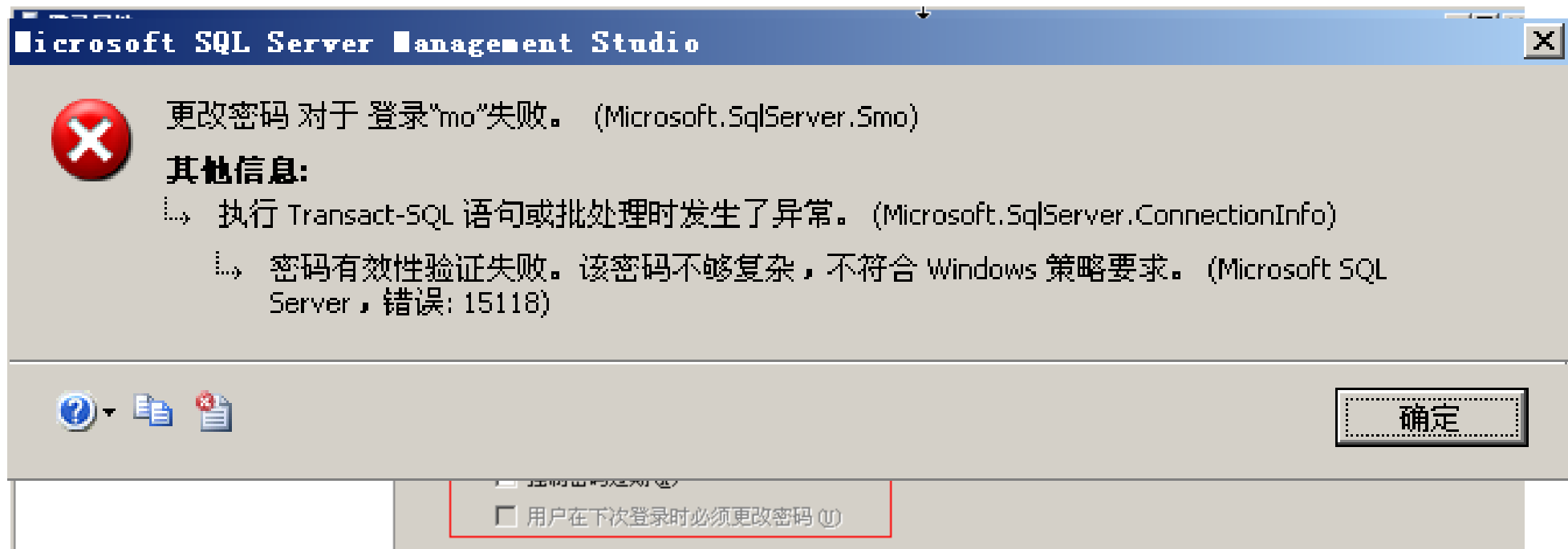
NSFOCUS-FF23EDB\安全性\服务器角色 8 项

名称
bulkadmin
dbcreator
diskadmin
processadmin
securityadmin
serveradmin
setupadmin
sysadmin

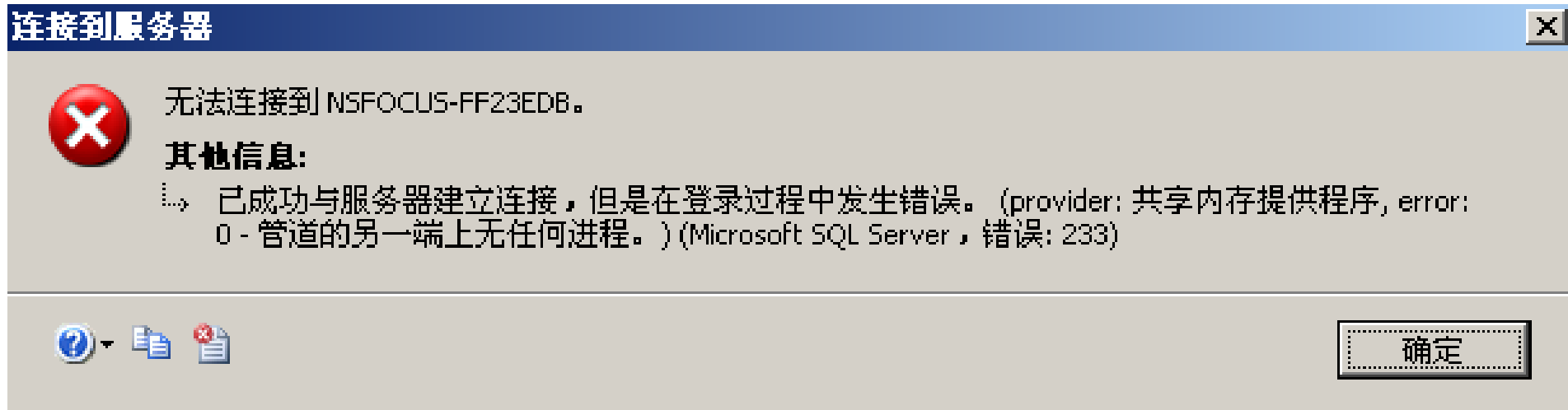
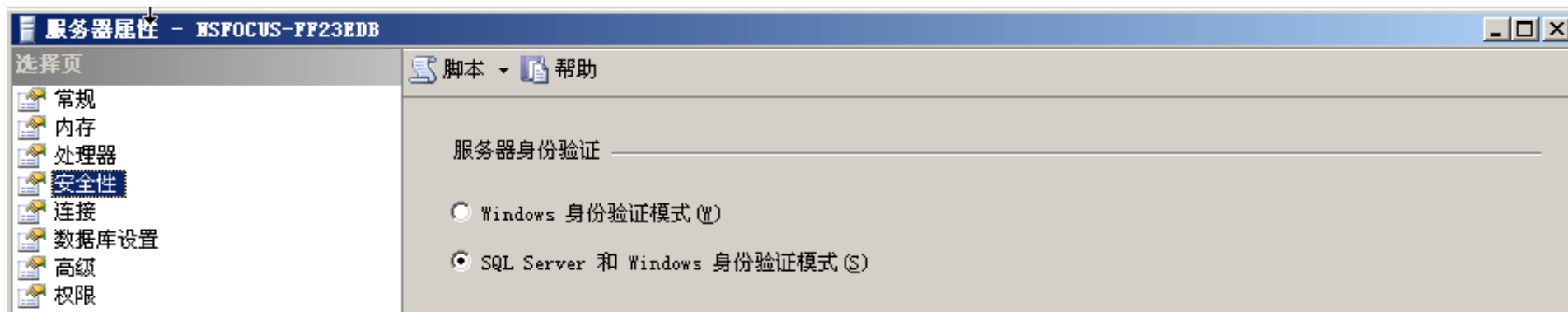
就绪

角色	权限
bulkadmin	可以运行bulkinsert语句
dbcreator	可以创建、更改、删除和还原任何数据库
processadmin	可以终止实例中运行的进程
securityadmin	管理登录名及其属性，可以grant、deny和revoke服务器和数据库级权限，可以重置登录名密码
serveradmin	更改服务器范围的配置选项和关闭服务器
setupadmin	添加和删除链接数据库，并且可以执行某些系统存储过程
sysadmin	可以在服务器任意活动

密码策略:



身份验证:



登录审核:

登录审核

- ☐ 无 (N)
- ☐ 仅限失败的登录 (F)
- ☐ 仅限成功的登录 (U)
- ☒ 失败和成功的登录 (B)

计算机管理									
文件 (F) 操作 (A) 查看 (V) 窗口 (W) 帮助 (H)									
计算机管理 (本地)									
系统工具	事件查看器	应用程序	安全性	系统	Windows PowerShell	共享文件夹	本地用户和组	用户	组
性能日志和警报	设备管理器	存储	可移动存储	磁盘碎片整理程序	磁盘管理	服务和应用程序			
类型	日期	时间	来源	分类	事件	用户	计算机		
审核成功	2011-5-4	23:44:46	MSSQLSERVER	(4)	18454	N/A	NSFOCUS-...		
审核成功	2011-5-4	23:44:46	MSSQLSERVER	(4)	18454	N/A	NSFOCUS-...		
审核成功	2011-5-4	23:44:45	MSSQLSERVER	(4)	18454	N/A	NSFOCUS-...		
审核失败	2011-5-4	23:44:38	MSSQLSERVER	(4)	18456	N/A	NSFOCUS-...		
审核失败	2011-5-4	23:44:29	MSSQLSERVER	(4)	18456	N/A	NSFOCUS-...		
审核成功	2011-5-4	23:43:50	MSSQLSERVER	(4)	18454	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:46	MSSQLSERVER	(2)	9688	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:46	MSSQLSERVER	(2)	9666	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:46	MSSQLSERVER	(2)	9666	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:46	MSSQLSERVER	(2)	3408	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:45	MSSQLSERVER	(2)	17137	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:45	MSSQLSERVER	(2)	8561	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:44	MSSQLSERVER	(2)	8128	N/A	NSFOCUS-...		
审核成功	2011-5-4	23:43:44	MSSQLSERVER	(4)	18454	N/A	NSFOCUS-...		
审核成功	2011-5-4	23:43:44	MSSQLSERVER	(4)	18453	SYSTEM	NSFOCUS-...		
信息	2011-5-4	23:43:43	MSSQLSERVER	(2)	17137	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:43	MSSQLSERVER	(2)	17137	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:43	MSSQLSERVER	(2)	17137	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:43	MSSQLSERVER	(2)	17137	N/A	NSFOCUS-...		
信息	2011-5-4	23:43:43	MSSQLSERVER	(2)	17126	N/A	NSFOCUS-...		

Sql Server 2005数据库级管理

数据库用户：

The screenshot displays the SQL Server Enterprise Manager interface. On the left, the 'mo' database is expanded, showing its structure: 数据库关系图 (Database Diagrams), 表 (Tables), 视图 (Views), 同义词 (Synonyms), 可编程性 (Programmability), Service Broker, 存储 (Stored Procedures), 安全性 (Security), and 用户 (Users). The '用户' folder is expanded, listing the following users: dbo, guest, INFORMATION_SCHEMA, mo, NSFOCUS-FF23EDB\sql, and sys.

On the right, the '用户' (Users) list is shown in a table format. The table has two columns: '名称' (Name) and '创建时间' (Creation Time). The table contains 6 items.

名称	创建时间
dbo	2003-4-8
guest	2003-4-8
INFORMATION_SCHEMA	2005-10-14
mo	2011-5-3
NSFOCUS-FF23EDB\sql	2011-5-5
sys	2005-10-14

dbo是每个数据库的默认用户，具有所有者权限，即DbOwner。通过用DBO作为所有者来定义对象，能够使数据库中的任何用户引用而不必提供所有者名称。

guest 用户:

guest 用户，在SQL Server 2005 中的每个数据库安全性的用户下面均有一个。默认该用户只在master 和 tempdb 数据库下是开启的，其他数据库均为禁用的。该用户在SQL Server 2005中是不允许删除的。

启用Guest:

GRANT Connect TO Guest;

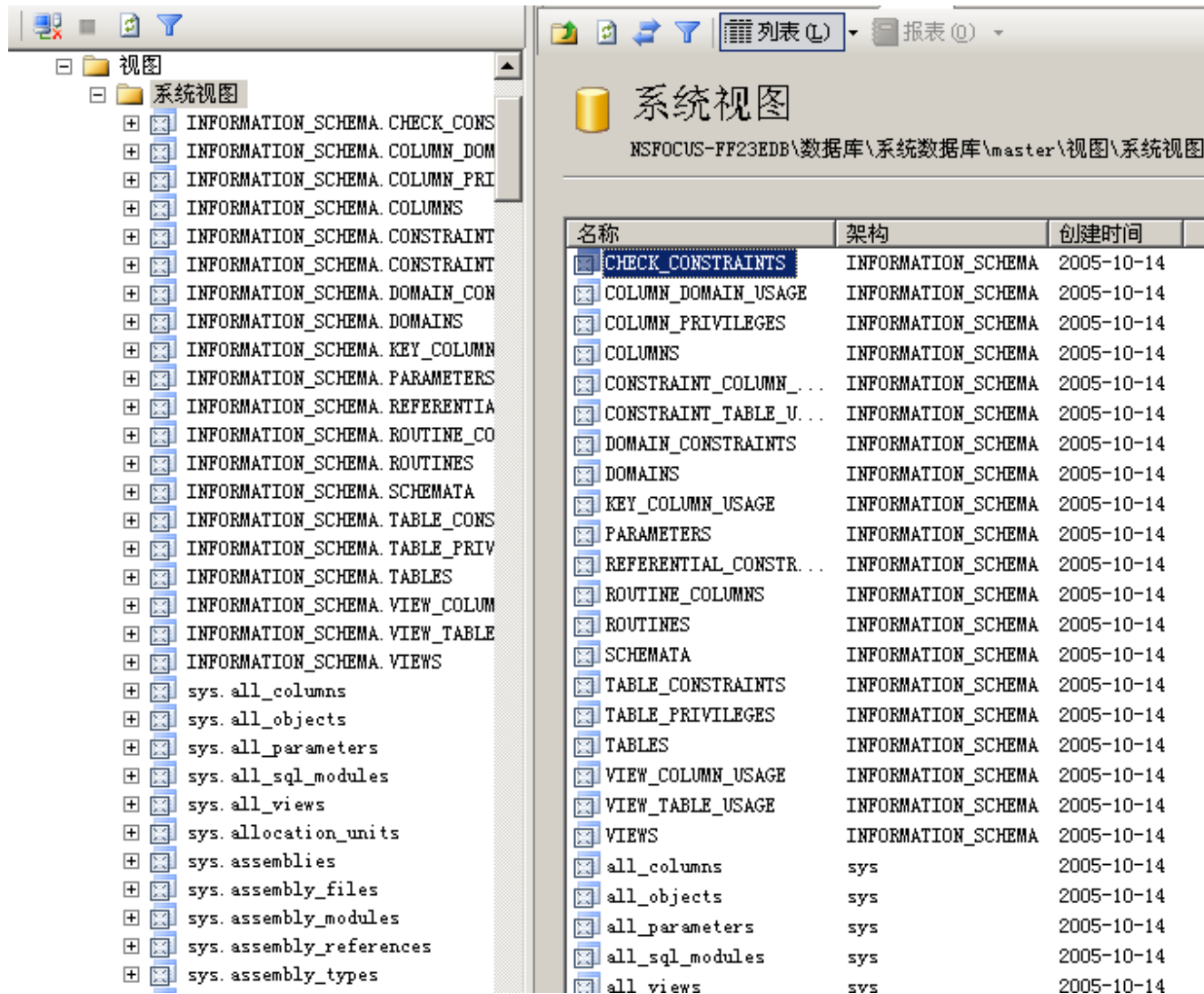
禁用Guest

REVOKE Connect FROM Guest;



INFORMATION_SCHEMA和sys:

它们的登录是<无>，这是系统内置的两个用户。他们拥有自己的视图



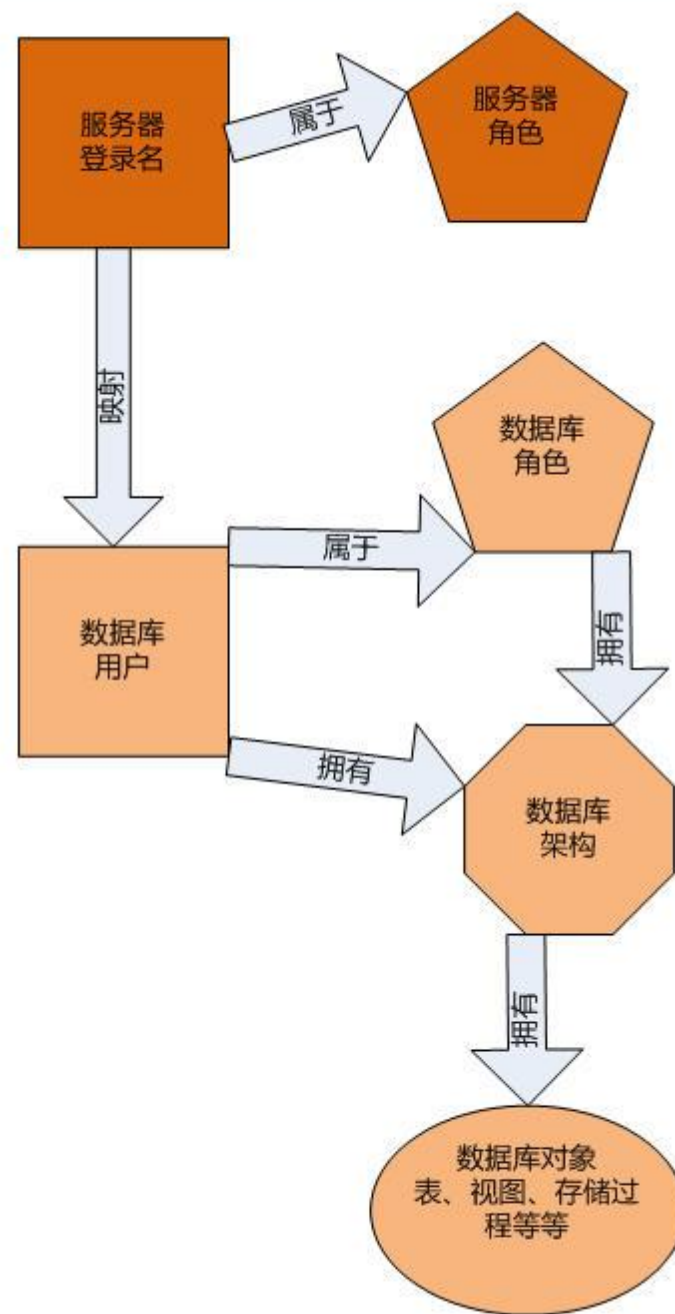
名称	架构	创建时间
CHECK_CONSTRAINTS	INFORMATION_SCHEMA	2005-10-14
COLUMN_DOMAIN_USAGE	INFORMATION_SCHEMA	2005-10-14
COLUMN_PRIVILEGES	INFORMATION_SCHEMA	2005-10-14
COLUMNS	INFORMATION_SCHEMA	2005-10-14
CONSTRAINT_COLUMN...	INFORMATION_SCHEMA	2005-10-14
CONSTRAINT_TABLE_U...	INFORMATION_SCHEMA	2005-10-14
DOMAIN_CONSTRAINTS	INFORMATION_SCHEMA	2005-10-14
DOMAINS	INFORMATION_SCHEMA	2005-10-14
KEY_COLUMN_USAGE	INFORMATION_SCHEMA	2005-10-14
PARAMETERS	INFORMATION_SCHEMA	2005-10-14
REFERENTIAL_CONSTR...	INFORMATION_SCHEMA	2005-10-14
ROUTINE_COLUMNS	INFORMATION_SCHEMA	2005-10-14
ROUTINES	INFORMATION_SCHEMA	2005-10-14
SCHEMATA	INFORMATION_SCHEMA	2005-10-14
TABLE_CONSTRAINTS	INFORMATION_SCHEMA	2005-10-14
TABLE_PRIVILEGES	INFORMATION_SCHEMA	2005-10-14
TABLES	INFORMATION_SCHEMA	2005-10-14
VIEW_COLUMN_USAGE	INFORMATION_SCHEMA	2005-10-14
VIEW_TABLE_USAGE	INFORMATION_SCHEMA	2005-10-14
VIEWS	INFORMATION_SCHEMA	2005-10-14
all_columns	sys	2005-10-14
all_objects	sys	2005-10-14
all_parameters	sys	2005-10-14
all_sql_modules	sys	2005-10-14
all_views	sys	2005-10-14

数据库用户，指有权限能操作数据库的用户

数据库角色，指一组固定的有某些权限的数据库角色

数据库架构，指数据库对象的容器

服务器名.数据库名.架构名.对象名



创建用户:

数据库用户 - mo1

选择页

常规

安全对象

扩展属性

脚本 帮助

用户名 (U):

mo1

☒ 登录名 (L):

mo

...

☐ 证书名称 (C):

☐ 密钥名称 (K):

☐ 无登录名 (N)

默认架构 (D):

sqlc

...

此用户拥有的架构 (O):

设置权限:

数据库属性 - sql1

选择页

常规

文件

文件组

选项

权限

扩展属性

镜像

事务日志传送

脚本 帮助

服务器名称 (S):

NSFOCUS-FF23EDB

查看服务器权限

数据库名称 (U):

sql1

用户或角色 (U):

名称	类型
mol	用户

有效权限 (E)

添加 (A)...

删除 (R)

mol 的显式权限 (E):

权限	授权者	授予	具有授予...	拒绝
Create synonym	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create table	dbo	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create type	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create view	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Create XML schema collection	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Execute	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

连接

服务器:

NSFOCUS-FF23EDB

连接:

sa

查看连接属性

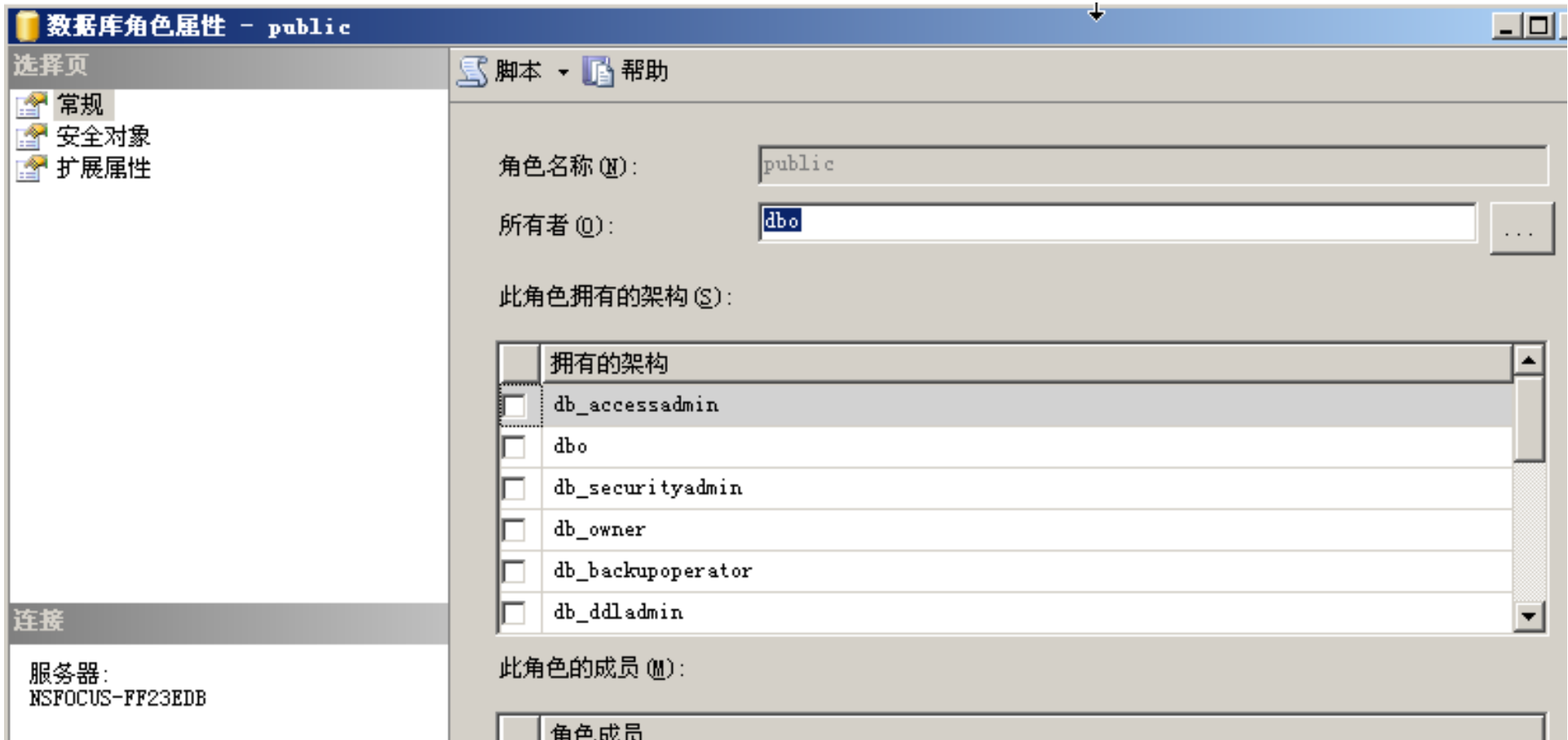
进度

就绪

固定数据库角色	描 述
db_accessadmin	访问权限管理员，具有ALTER ANY USER、CREATE SCHEMA、CONNECT、VIEW ANY DATABASE等权限，可以为Windows登录名、Windows组、SQL Server登录名添加或删除访问权限
db_backupoperator	数据库备份管理员，具有BACKUP DATABASE、BACKUP LOG、CHECKPOINT、VIEW DATABASE等权限，可以执行数据库备份操作
db_datareader	数据检索操作员，具有SELECT、VIEW DATABASE等权限，可以检索所有用户表中的所有数据
db_datawriter	数据维护操作员，具有DELETE、INSERT、UPDATE、VIEW DATABASE等权限，可以在所有用户表中执行插入、更新、删除等操作
db_ddladmin	数据库对象管理员，具有创建和修改表、类型、视图、过程、函数、XML架构、程序集等权限，可以执行对这些对象的管理操作
db_denydatareader	拒绝执行检索操作员，拒绝SELECT权限，具有VIEW ANY DATABASE权限，不能在数据库中对所有对象执行检索操作
db_denydatawriter	拒绝执行数据维护操作员，拒绝DELETE、INSERT、UPDATE权限，不能在数据库中执行所有的删除、插入、更新等操作
db_owner	数据库所有者，具有CONTROL、VIEW ANY DATABASE权限，具有在数据库中的所有操作
db_securityadmin	安全管理员，具有ALTER ANY APPLICATION ROLE、ALTER ANY ROLE、CREATE SCHEMA、VIEW DEFINITION、VIEW ANY DATABASE等权限，可以执行权限管理和角色成员管理等操作

public角色:

除了前面介绍的固定数据库角色之外，Microsoft SQL Server系统成功安装之后，还有一个特殊的角色即public角色。public角色有两大特点，第一，初始状态时没有权限；第二，所有的数据库用户都是它的成员。



表权限:

表属性 - name

选择页

常规

权限

扩展属性

连接

服务器:

NSFOCUS-FF23EDB

连接:

mo

查看连接属性

进度

就绪

脚本 帮助

架构(S):

dbo

查看架构权限

表名(N):

name

用户或角色(U):

名称	类型
mo	用户

有效权限(E)

添加(A)...

删除(R)

mo 的显式权限(E):

权限	授权者	授予	具有授予...	拒绝
Alter	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
References	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

设置用户的表权限

数据库用户 - mo

选择页

常规

安全对象

扩展属性

连接

服务器:

NSFOCUS-FF23EDB

连接:

mo

查看连接属性

进度

就绪

脚本 帮助

用户名 (U):

mo

安全对象 (S):

架构	名称	类型
dbo	name	表
dbo	passwd	表
dbo	sysdiagrams	表

有效权限 (E)...

添加 (A)...

删除 (R)

dbo.name 的显式权限 (P):

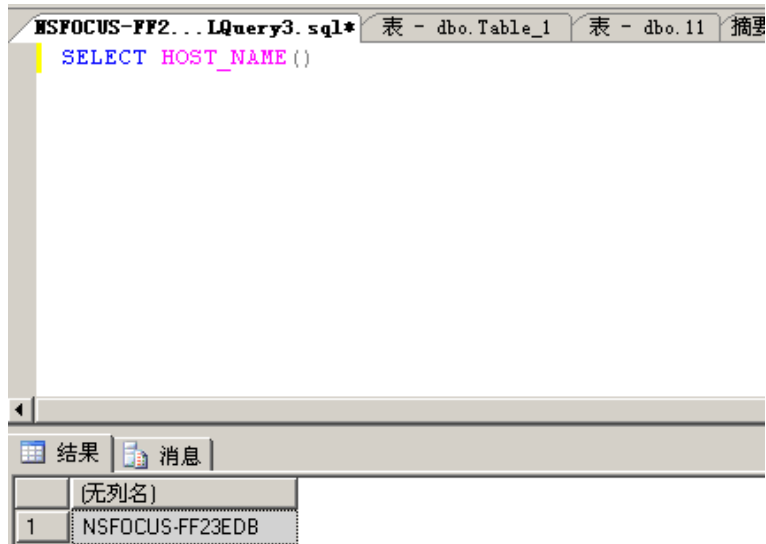
权限	授权者	授予	具有授予...	拒绝
Alter	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Control	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Delete	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Insert	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
References	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Select	dbo	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

列权限 (C)...

Sql Server 2005 安全维护

Sql语句与日志审核

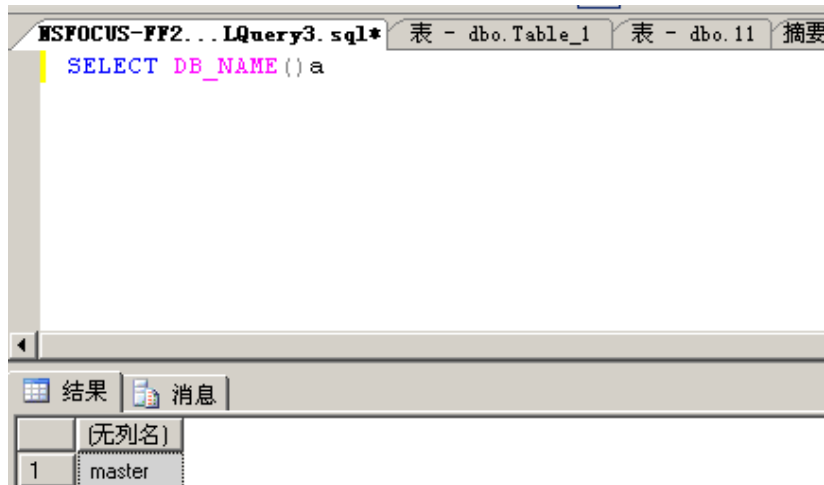
查看主机名:



查看当前用户:



查看当前数据库:



查看当前库所有表:

NSFOCUS-FF2... LQuery3.sql* 摘要

```
Select name from sys.Tables
```

结果 消息

	name
1	spt_fallback_db
2	spt_fallback_dev
3	spt_fallback_usg
4	spt_monitor
5	spt_values
6	MSreplication_options

查看当前库所有存储过程:

NSFOCUS-FF2... LQuery3.sql* 摘要

```
sp_stored_procedures
```

结果 消息

	PROCEDURE_QUALIFIER	PROCEDURE_OWNER	PROCEDURE_NAME
1...	master	sys	sp_verifypublisher;1
1...	master	sys	sp_views_rowset;1
1...	master	sys	sp_views_rowset2;1
1...	master	sys	sp_vupgrade_mergetables;1
1...	master	sys	sp_vupgrade_replication;1
1...	master	sys	sp_vupgrade_replsecurity_metadata;1
1...	master	sys	sp_who;1
1...	master	sys	sp_who2;1
1...	master	sys	sp_xml_schema_rowset;1
1...	master	sys	sp_xml_schema_rowset2;1
1...	master	sys	xp_grantlogin;1
1...	master	sys	xp_logininfo;1
1...	master	sys	xp_repl_convert_encrypt_sysadmin_wre
1...	master	sys	xp_revokellogin;1

查看数据库所有用户名、密码、登录方式:

select name,password,isntname from syslogins

NSFOCUS-FF2... LQuery3. sql* 摘要

```
select name,password,isntname from syslogins
```

结果 消息

	name	password	isnt
1	sa	sa	0
2	##MS_SQLResourceSigningCertificate##	NULL	0
3	##MS_SQLReplicationSigningCertificate##	NULL	0
4	##MS_SQLAuthenticatorCertificate##	NULL	0
5	##MS_AgentSigningCertificate##	NULL	0
6	BUILTIN\Administrators	NULL	1
7	NT AUTHORITY\SYSTEM	NULL	1
8	NSFOCUS-FF23EDB\SQLServer2005MSSQLUser\$NSFOCUS-F...	NULL	1
9	NSFOCUS-FF23EDB\SQLServer2005SQLAgentUser\$NSFOCUS...	NULL	1
10	NSFOCUS-FF23EDB\SQLServer2005MSFTEUser\$NSFOCUS-FF...	NULL	1
11	mo	mo	0
12	NSFOCUS-FF23EDB\sql	NULL	1
13	test1	test1	0

数据库日志:

对象资源管理器

连接 (C) ▾

- NSFOCUS-FF23EDB (SQL Server 9.0.1399 - sa)
 - 数据库
 - 安全性
 - 服务器对象
 - 复制
 - 管理
 - 维护计划
 - SQL Server 日志**
 - 当前 - 2011-5-6 6:25:00
 - 存档 #1 - 2011-5-6 1:19:00
 - 存档 #2 - 2011-5-6 1:13:00
 - 存档 #3 - 2011-5-5 11:44:00
 - 存档 #4 - 2011-5-4 23:43:00
 - 存档 #5 - 2011-5-4 23:42:00
 - 存档 #6 - 2011-5-4 23:39:00

摘要

列表 (L) ▾ 报表 (R) ▾

SQL Server 日志

NSFOCUS-FF23EDB\管理\SQL Server 日志

名称	创建时间
当前 - 2011-5-6 6:...	2011-5-6
存档 #1 - 2011-5-6...	2011-5-6
存档 #2 - 2011-5-6...	2011-5-6
存档 #3 - 2011-5-5...	2011-5-5
存档 #4 - 2011-5-4...	2011-5-4
存档 #5 - 2011-5-4...	2011-5-4
存档 #6 - 2011-5-4...	2011-5-4

日志文件查看器 - HSFOCUS-PP23EDB

选择日志

SQL Server

当前 - 2011-5-6 6:28:00

存档 #1 - 2011-5-6 1:19:00

存档 #2 - 2011-5-6 1:13:00

存档 #3 - 2011-5-5 11:44:00

存档 #4 - 2011-5-4 23:43:00

存档 #5 - 2011-5-4 23:42:00

存档 #6 - 2011-5-4 23:39:00

SQL 代理

Windows NT

数据库邮件

状态

上次刷新:

2011-5-6 6:29:19

筛选器: 无

查看筛选设置

进度

已完成 (77 条记录)。

加载日志

导出

刷新

筛选...

搜索...

帮助

日志文件摘要 (S): 未应用任何筛选器

日期	源	消息
2011-5-6 6:29:22	登录	Login succeeded for user 'NT AUTHORITY\SYSTEM'. Connection:
2011-5-6 6:29:22	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:29:21	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:29:20	登录	Login succeeded for user 'NT AUTHORITY\SYSTEM'. Connection:
2011-5-6 6:29:20	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:28:54	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:28:52	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:28:52	登录	Login succeeded for user 'sa'. Connection: non-trusted. [客
2011-5-6 6:28:39	登录	Login succeeded for user 'NT AUTHORITY\SYSTEM'. Connection:

所选行详细信息 (D):

日期

2011-5-6 6:29:22

日志

SQL Server (当前 - 2011-5-6 6:28:00)

源

登录

消息

Login succeeded for user 'NT AUTHORITY\SYSTEM'. Connection: trusted. [客户端: <local machine>]

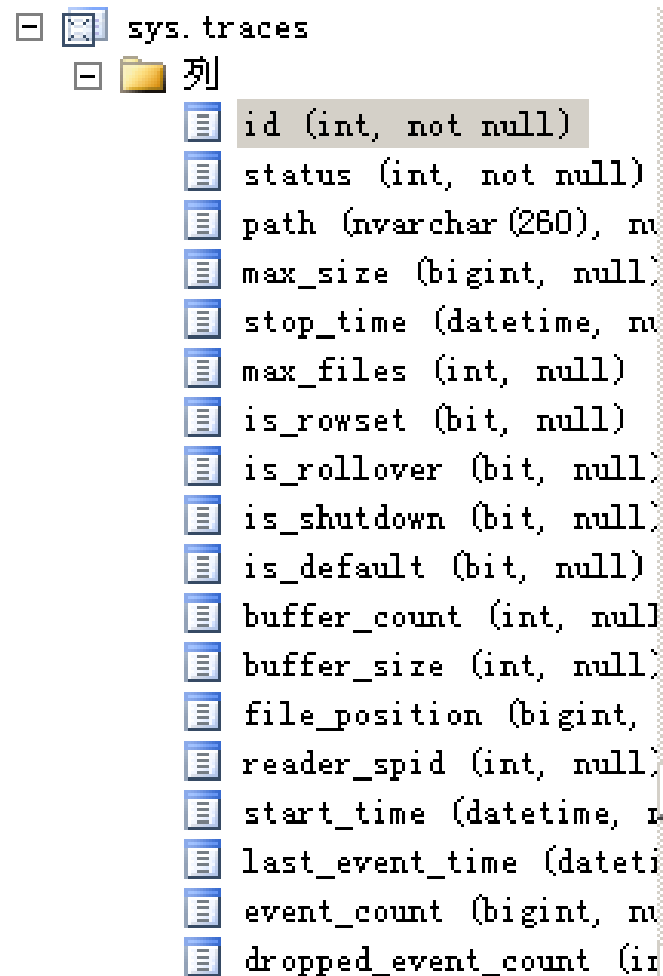
C2审核模式:

作用：选择此选项将配置服务器，以记录对语句和对象的失败和成功的访问尝试。这些信息可以帮助您了解系统活动并跟踪可能的安全策略冲突。

启用C2审计:

```
sp_configure 'show advanced options', 1 ;  
GO  
RECONFIGURE ;  
GO
```


```
sp_configure 'c2 audit mode', 1 ;  
GO  
RECONFIGURE ;  
GO
```



The screenshot shows the SQL Server Enterprise Manager interface. Under the 'sys.traces' folder, the '列' (Columns) folder is expanded, displaying a list of columns for the sys.traces table. The columns are listed with their data types and nullability constraints.

列	数据类型	是否可为空
id	int	not null
status	int	not null
path	nvarchar(260)	not null
max_size	bigint	null
stop_time	datetime	null
max_files	int	null
is_rowset	bit	null
is_rollover	bit	null
is_shutdown	bit	null
is_default	bit	null
buffer_count	int	null
buffer_size	int	null
file_position	bigint	null
reader_spid	int	null
start_time	datetime	null
last_event_time	datetime	null
event_count	bigint	null
dropped_event_count	int	null

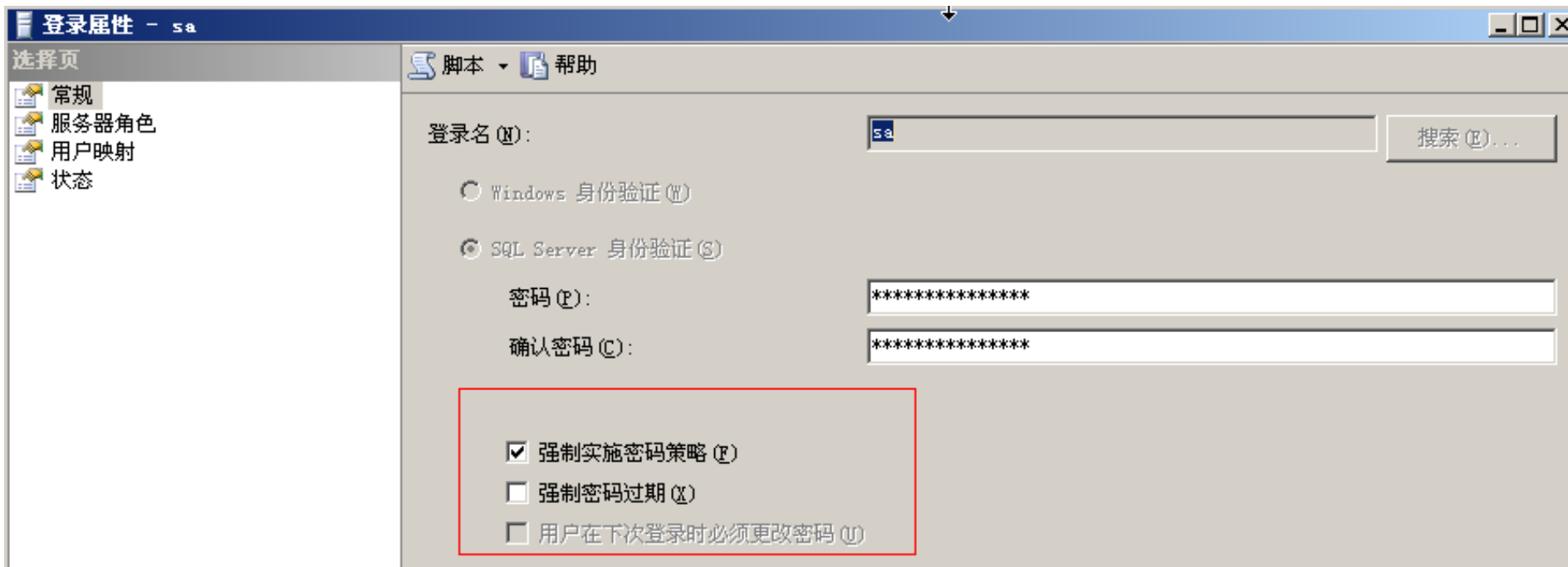
使用profiler打开:



EventClass	TextData
Audit Schema Object Acces...	SELECT ' Server[@Name=' + quotename(CAST(serverproperty(N' Servername') AS sysname),'
Audit Schema Object Acces...	SELECT ' Server[@Name=' + quotename(CAST(serverproperty(N' Servername') AS sysname),'
Audit Schema Object Acces...	SELECT ' Server[@Name=' + quotename(CAST(serverproperty(N' Servername') AS sysname),'
Audit Schema Object Acces...	SELECT ' Server[@Name=' + quotename(CAST(serverproperty(N' Servername') AS sysname),'
Audit Schema Object Acces...	SELECT ' Server[@Name=' + quotename(CAST(serverproperty(N' Servername') AS sysname),'
Audit Schema Object Acces...	sp_configure 'c2 audit mode'
Audit Schema Object Acces...	if (select value_in_use from sys.configurations where configuration_id = 518) = 1
Audit Schema Object Acces...	select @configcount = count(*) from sys.configurations where lower(name collate
Audit Schema Object Acces...	select @configname = name from sys.configurations where lower(name collate Lat
Audit Schema Object Acces...	select name, convert(int, minimum) as minimum, convert(int, maximum) as maxi

sqlserver2005安全威胁与应对

Sqlserver2005



SQL Server 远程访问:



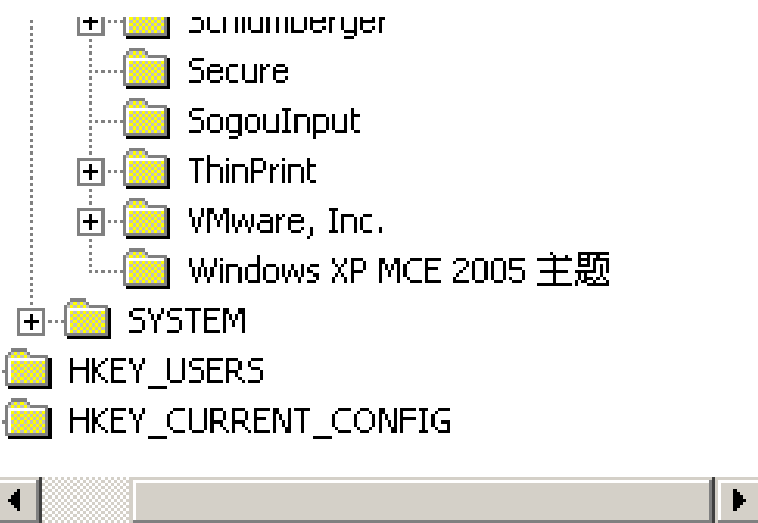
xp_cmdshell:

NSFOCUS-FF2...LQuery3.sql*		摘要
		<code>exec master..xp_cmdShell 'dir c:\'</code>
		结果 消息
output		
1	驱动器 C 中的卷没有标签。	
2	卷的序列号是 3873-AF48	
3	NULL	
4	c:\的目录	
5	NULL	
6	2011-04-25 06:18	<DIR> 1
7	2011-04-29 11:16	9201.cer
8	2011-04-29 10:56	<DIR> 11
9	2011-04-29 11:22	883123.cer
10	2011-04-25 06:23	<DIR> 2
11	2011-04-28 17:03	<DIR> 3
12	2011-04-25 14:34	<DIR> 4
13	2010-10-09 21:34	0 AUTOEXEC.BAT
14	2011-04-29 11:18	1 232 certren.txt

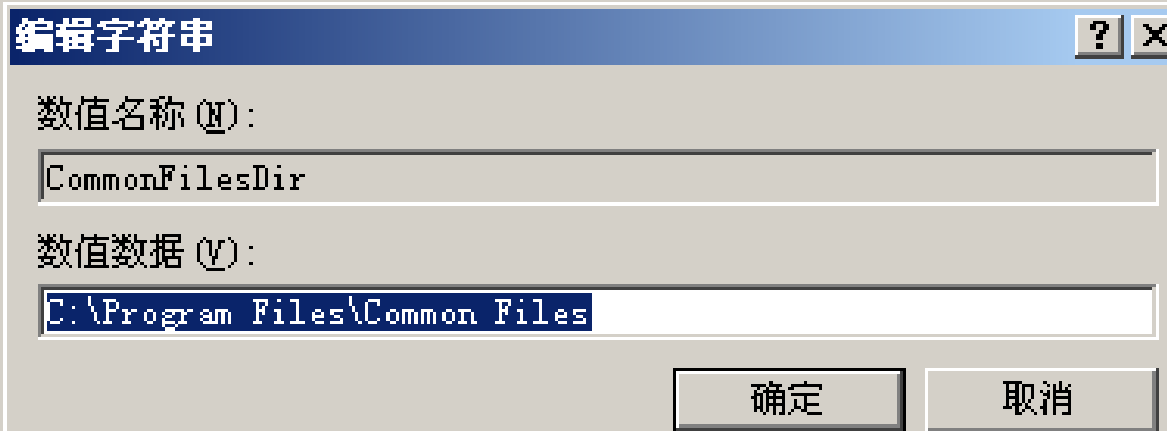
不仅仅是xp_cmdshell:

```

1> xp_regread 'HKEY_LOCAL_MACHINE','SOFTWARE\Microsoft\Windows\CurrentVersion','CommonFilesDir'
2> go
Value                                     Data
-----
CommonFilesDir                           C:\Program Files\Common
Files
    
```



我的电脑\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion



弱口令与扩展存储过程

目标：创建管理员权限账号

破解sql server2005 sa弱口令

利用获得的口令远程连接数据库。

利用xp_cmdshell添加管理员账号nsfoucs1。



启用xp_cmdshell:

```
Exec sp_configure 'show advanced options',1;RECONFIGURE;EXEC  
sp_configure 'xp_cmdshell',1;RECONFIGURE;
```

执行xp_cmdshell命令

```
Exec master.dbo.xp_cmdshell 'net user'
```

禁用xp_cmdshell:

```
Exec sp_configure 'show advanced options',1;RECONFIGURE;EXEC  
sp_configure 'xp_cmdshell',0;RECONFIGURE;
```

- 禁止cmd执行下如何提权？

- declare @o int exec sp_oacreate 'scripting.filesystemobject', @o out exec sp_oamethod @o, 'copyfile',null,'c:\windows\explorer.exe' , 'c:\windows\system32\sethc.exe';
- 开启'sp_oacreate':
- exec sp_configure 'show advanced options', 1;RECONFIGURE;exec sp_configure'Ole Automation Procedures',1;RECONFIGURE;

windows

Sql server

linux

mysql

• 帐号分类

➤ 超级管理员

uid=0、绑定TCP 1024以下端口

➤ 系统默认用户

系统程序使用，从不登录

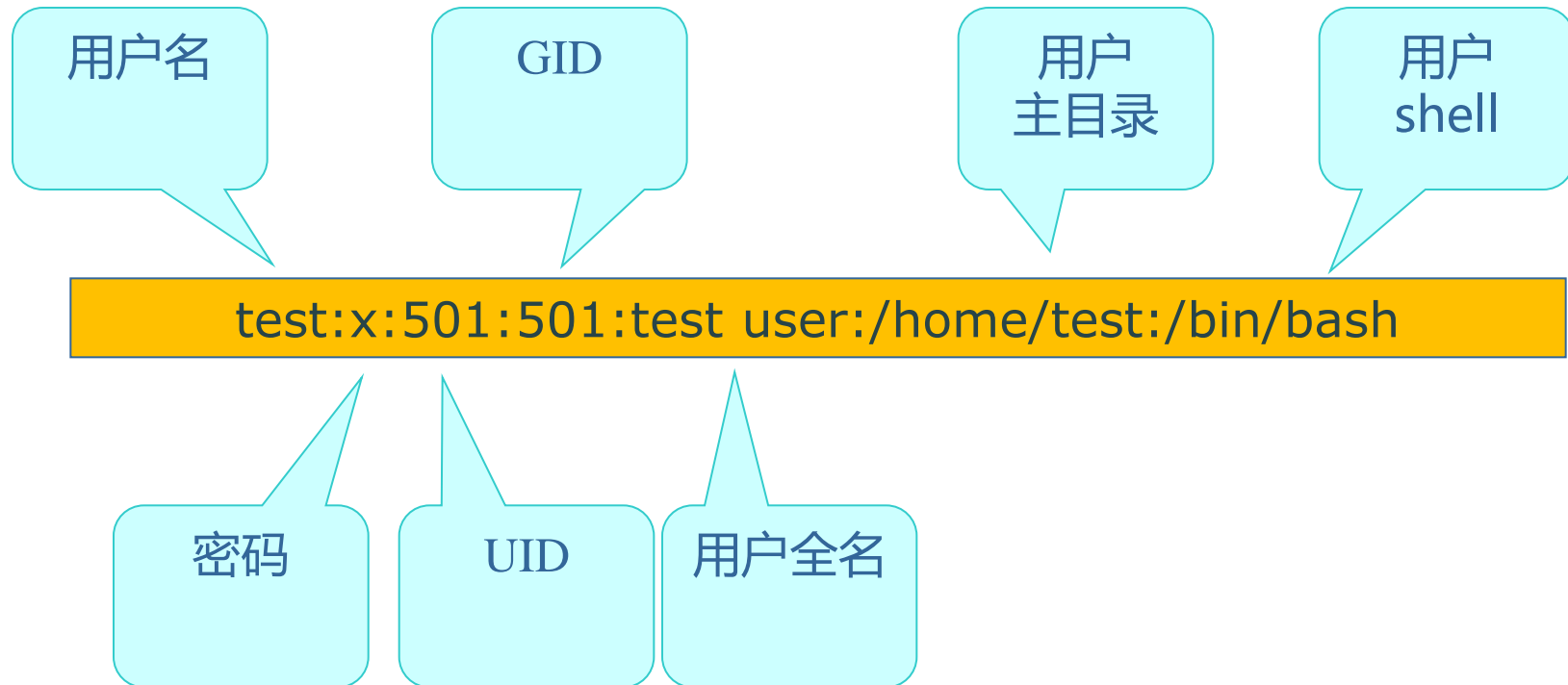
➤ 新建普通用户

uid大于500 (linux)

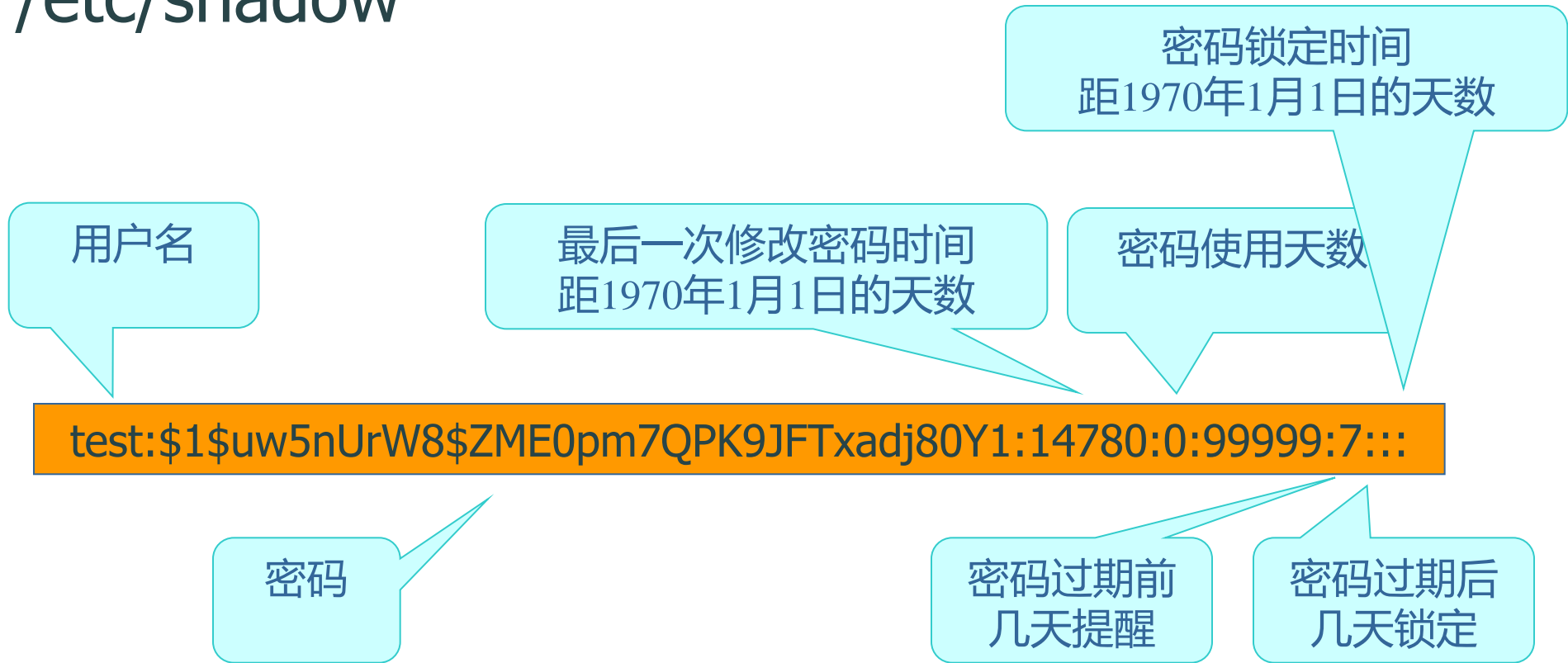
```
smmsp:x:51:51:./var/spool/mqueue:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
haldaemon:x:68:68:HAL daemon:./sbin/nologin
avahi-autoipd:x:100:104:avahi-autoipd:/var/lib/avahi-autoipd:/sbin/nologin
gdm:x:42:42:./var/gdm:/sbin/nologin
nsfocus:x:500:500:nsfocus:/home/nsfocus:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
```

帐号	UID	描述
root	0	管理员
daemon	1	与例行系统任务相关联
bin	2	系统管理任务守护进程帐号，与运行系统二进制文件有关
sys	3	系统管理任务守护进程帐号，与系统日志或更新临时目录中的文件有关
adm	4	系统管理任务守护进程帐号，与系统日志有关
lp	71	行式打印机守护进程
uucp	5	与UUCP有关的守护进程帐号
nuucp	9	远程系统用此帐号来登录到本机并开始文件传输
smmsp	25	sendmail提交消息的守护进程帐号
listen	37	网络监听守护进程帐号
nobody	60001	当一个授权的root用户发出一个请求时，NFS服务器分配的匿名用户帐号，nobody帐号是用来给不需要任何专门权限的软件进程使用
noaccess	60002	该帐号用来给哪些通过某种应用而不是系统登陆步骤来访问系统的用户或进程使用
nobody4	65534	sunos4.0/4.1发布版的匿名用户帐号

- /etc/passwd



- /etc/shadow



- 加密算法

/etc/sysconfig/authconfig

PASSWDALGORITHM=md5

DES加密密文

test:.Q3Vj3F3TS3uY

MD5加密密文

test:\$1\$oBfxIMmF\$fueNkQ1CikG.dsafE.X/

DES只能识别8位密码！

- linux密码复杂度策略：

vi /etc/pam.d/system-auth

```
password requisite pam_cracklib.so try_first_pass retry=3  
minlen=8 ucredit=-2 lcredit=-4 ocredit=-1 remember=5
```

- 解释

minlen=8 最小密码长度为8位

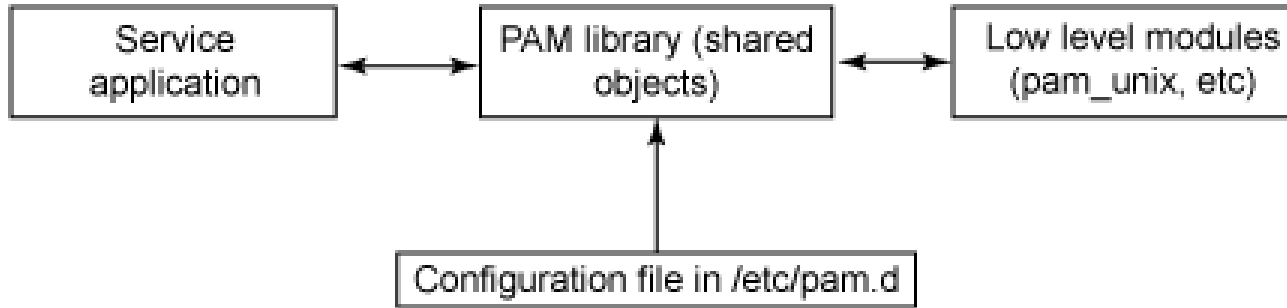
ucredit=-2 最少有2个大写字母

lcredit=-4 最少4个小写字符

ocredit=-1 最少1个符号

remember=5 密码最近5次的不能重用

• PAM(Pluggable Authentication Modules)



类型	含义	控制	含义
auth	检查用户名密码	required	必须通过，否则退出
account	检查用户属性	requisite	有一项通过即可
password	检查修改密码	sufficient	通过后立刻退出
session	检查登录后会话	optional	可选项

- 弱口令审计(john the ripper)

<http://www.openwall.com/john/>

```
john.exe 'shadow' --wordlist='passwd.txt';
```

```
C:\Users\Administrator\Desktop>cd -2016-1-12\tools\john>john.exe 'shadow' --wordlist='passwd.txt'  
Loaded 2 password hashes with 2 different salts (FreeBSD MD5 [$SE2i 12x])  
460143946      (haha)  
nsfocus       (root)  
guesses: 2   time: 0:00:00:01 DONE (Fri Jan 15 14:03:07 2016)  c/s: 19931  trying  
:  
Use the "--show" option to display all of the cracked passwords reliably
```


使用grub修改root密码

```
GNU GRUB  version 0.95  (638K lower / 522176K upper memory)

root (hd0,0)
kernel /vmlinuz-2.6.9-67.EL ro root=/dev/Ur1Group00/LogUr100 rhgb qui→
initrd /initrd-2.6.9-67.EL.img
```

Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.

grub可以修改root密码，那么本身就是不安全的！

➤ 为grub设置密码

```
[root@localhost ~]# /sbin/grub-md5-crypt
Password:
Retype password:
$1$/bd5r0$Lvd6WTaPx7rkahar0wD9y/
[root@localhost ~]#
```

将MD5值写入/etc/grub.conf中

```
#
# kernel /vmlinuz-version ro root=/dev/VolGroup00/LogVol00
# initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
password --md5 $1$ErT5r0$7TRTrnXZlaAMkGj17lwPK1
hiddenmenu
title CentOS (2.6.18-194.el5xen)
```

文件属性

所属用户
组权限所属用户
及用户组最后修改
时间

文件名

```
-rw-r--r-- 1 root root 884 Feb 22 10:04 inittab
```

所属用户
权限其他用户
权限

文件大小

使用数字来代表各个权限，各权限的分数对照表如下：

r:4

w:2

x:1

文件系统安全

➤ 查看权限

ls -l

➤ 修改权限

chmod、chown、chgrp

➤ 关键文件权限

二进制文件、配置文件、日志文件

➤ setuid

```
[root@localhost bin]# find /usr/bin -perm -4000 -type f -print
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/rsh
/usr/bin/staprun
/usr/bin/rlogin
/usr/bin/chage
/usr/bin/Xorg
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/rcp
/usr/bin/crontab
/usr/bin/sudoedit
```

chattr (配置文件隐藏属性)

```
[root@www ~]# chattr [+ -=][ASacdistu] 文件或目录名称
```

选项与参数：

- +** : 添加某一个特殊参数，其他原本存在参数则不动。
- : 移除某一个特殊参数，其他原本存在参数则不动。
- =** : 配置一定，且仅有后面接的参数

- A** : 当配置了 **A** 这个属性时，若你有存取此文件(或目录)时，他的存取时间 **atime** 将不会被修改，可避免I/O较慢的机器过度的存取磁碟。这对速度较慢的计算机有帮助
- S** : 一般文件是非同步写入磁碟的(原理请参考第五章**sync**的说明)，如果加上 **S** 这个属性时，当你进行任何文件的修改，该更动会『同步』写入磁碟中。
- a** : 当配置 **a** 之后，这个文件将只能添加数据，而不能删除也不能修改数据，只有**root** 才能配置这个属性。
- c** : 这个属性配置之后，将会自动的将此文件『压缩』，在读取的时候将会自动解压缩，但是在储存的时候，将会先进行压缩后再储存(看来对于大文件似乎蛮有用的！)
- d** : 当 **dump** 程序被运行的时候，配置 **d** 属性将可使该文件(或目录)不会被 **dump** 备份
- i** : 这个 **i** 可就很厉害了！他可以让一个文件『不能被删除、改名、配置连结也无法写入或新增数据！』对于系统安全性有相当大的助益！只有 **root** 能配置此属性

lsattr (显示文件隐藏属性)

```
[root@www ~]# lsattr [-adR] 文件或目录
```

选项与参数：

- a** : 将隐藏档的属性也秀出来；
- d** : 如果接的是目录，仅列出目录本身的属性而非目录内的档名；
- R** : 连同子目录的数据也一并列出来！

命令档名的搜寻：

which

```
[root@www ~]# which [-a] command
```

选项或参数：

-a : 将所有由 PATH 目录中可以找到的命令均列出，而不止第一个被找到的命令名称

文件档名的搜寻：

whereis (寻找特定文件)

locate (依据 /var/lib/mlocate 内的数据库记载，找出使用者输入的关键字档名。)

find (很好用哦！)

让使用者能进入某目录成为『可工作目录』的基本权限为何？

使用者在某个目录内读取一个文件的基本权限为何？

让使用者可以修改一个文件的基本权限为何？

让一个使用者可以创建一个文件的基本权限为何？

让使用者进入某目录并运行该目录下的某个命令之基本权限为何？

➤ TCP-Wrapper配置

查看libwrap库

```
# ldd /usr/sbin/sshd|grep libwrap
```

```
libwrap.so.0 => /lib/libwrap.so.0 (0x008c5000)
```

```
# ldd /usr/sbin/vsftpd|grep libwrap
```

```
libwrap.so.0 => /lib/libwrap.so.0 (0x00774000)
```

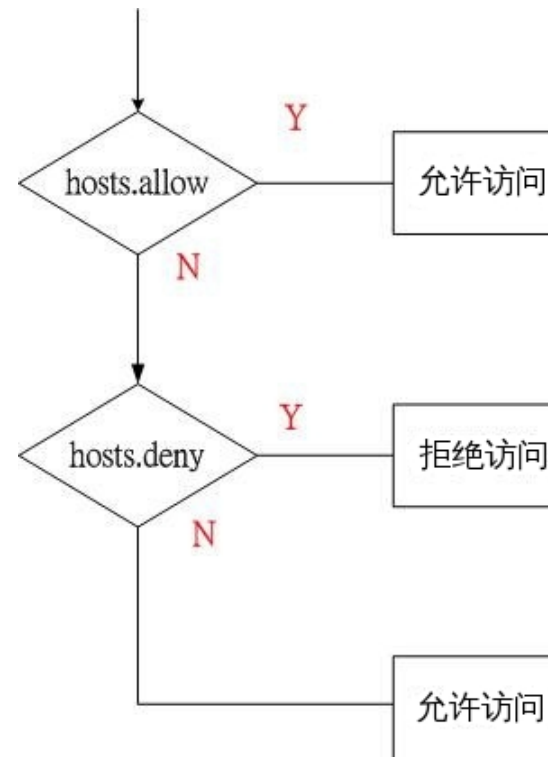
配置访问控制列表

/etc/hosts.allow

sshd:1.1.1.

/etc/hosts.deny

sshd:all



- 禁止root远程登录

- telnet

- Linux、HP-UX: /etc/securetty

- AIX: /etc/security/user, rlogin=false

- Solaris: /etc/default/login, CONSOLE=/dev/console

- SSH

- /etc/ssh/sshd_config, PermitRootLogin=no

- vsftp

- /etc/vsftpd/ftpusers

- 安全远程登录

- 口令嗅探 -> 加密传输 -> SSH、SSL
- 口令管理 -> 密钥登录 -> SSH密钥
- 口令猜解 -> 动态口令 -> RSA SecurID
- 行为审计 -> 统一登录 -> 堡垒主机

iptables 是与 Linux 内核集成的 IP 信息包过滤系统。如果 Linux 系统连接到因特网或 LAN、服务器或连接 LAN 和因特网的代理服务器，则该系统有利于在 Linux 系统上更好地控制 IP 信息包过滤和防火墙配置。

Redhat7.1以上版本，默认安装了iptables工具。/etc/sysconfig/iptables

➤ 限制进入连接

```
iptables -A INPUT -i eth0 -s 192.168.10.0/24 -p tcp --dport 22 -j ACCEPT
```

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -j DROP
```

➤ 限制外发连接

```
iptables -A OUTPUT -o eth0 -p tcp --syn -j DROP
```

```
iptables -A OUTPUT -o eth0 -p udp -j DROP
```

```
[root@localhost log]# ls
anaconda.ifcfg.log      cups
anaconda.log            dmesg
anaconda.program.log    dmesg.old
anaconda.storage.log    dracut.log
audit                   gdm
boot.log                httpd
btmp                    lastlog
ConsoleKit              mail
cron                    maillog
                        messages
                        ntpstats
                        pm-powersave.log
                        ppp
                        prelink
                        sa
                        samba
                        secure
                        spice-vdagentd
                        spooler
                        tallylog
                        wpa_supplicant.log
                        wtmp
                        Xorg.0.log
                        Xorg.0.log.old
                        Xorg.9.log
                        yum.log
```

- boot.log:
该文件记录了系统在引导过程中发生的事件，就是Linux系统开机自检过程显示的信息。
- cron:
该日志文件记录crontab守护进程crond所派生的子进程的动作，前面加上用户、登录时间和PID，以及派生出的进程的动作。
- secure:
该日志文件记录与安全相关的信息,包括用户进行的重启，登陆等动作

➤ lastlog : (重要)

该日志文件记录最近成功登录的事件和最后一次不成功的登录事件，由login生成。在每次用户登录时被查询，该文件是二进制文件，需要使用lastlog命令查看。

➤ wtmp : (重要)

该日志文件永久记录每个用户登录、注销及系统的启动、停机的事件。Last命令就是访问的这个文件。

➤ 进程统计 :

跟踪每个用户运行的每条命令。默认不激活。

```
[root@localhost ~]# lastcomm -f /var/log/pacct
date          root      pts/0      0.00 secs  Tue Feb 19 16:19
ls            root      pts/0      0.00 secs  Tue Feb 19 16:19
lastcomm      root      pts/0      0.00 secs  Tue Feb 19 16:16
lastcomm      root      pts/0      0.00 secs  Tue Feb 19 16:16
fprintd       S        root      _         0.00 secs  Tue Feb 19 16:15
bash          F        root      pts/0     0.00 secs  Tue Feb 19 16:15
..            .         .         .         .         .
```

```
[root@localhost ~]# history | more
  1  mysql -u root -p
  2  service httpd start
  3  service httpd restart
  4  ps aux | grep mysqld
  5  vi /etc/init.d/mysqld
  6  service mysqld status
  7  ps aux | grep mysqld
  8  ll /etc/shadow
  9  mysql -u test1 -p
```

消除痕迹很重要！！

使用命令 “vi /etc/profile”修改配置文件，修改HISTSIZE=5和HISTFILESIZE=5即保留最新执行的5条命令

```
[root@www ~]# dump [-Suvj] [-level] [-f 备份档] 待备份数据
```

```
[root@www ~]# dump -W
```

选项与参数：

- S : 仅列出后面的待备份数据需要多少磁碟空间才能够备份完毕；
- u : 将这次 dump 的时间记录到 /etc/dumpdates 文件中；
- v : 将 dump 的文件过程显示出来；
- j : 加入 bzip2 的支持！将数据进行压缩，默认 bzip2 压缩等级为 2
- level: 就是我们谈到的等级，从 -0 ~ -9 共十个等级；
- f : 有点类似 tar 啦！后面接产生的文件，亦可接例如 /dev/st0 装置档名等
- W : 列出在 /etc/fstab 里面的具有 dump 配置的 partition 是否有备份过？

windows

Sql server

linux

mysql

- 客户端连接MySQL
 - # mysql -h数据库地址 -u用户名 -p密码
- 查看数据库
 - SQL> show databases;
- 创建数据库
 - SQL> create database test;
- 创建和查看表
 - SQL> create table test(data varchar(255));
 - SQL> show tables;

- SELECT

```
SELECT LastName,FirstName FROM Persons
```

"Persons" 表:

LastName	FirstName	Address	City
Adams	John	Oxford Street	London
Bush	George	Fifth Avenue	New York
Carter	Thomas	Changan Street	Beijing

结果：

LastName	FirstName
Adams	John
Bush	George
Carter	Thomas

MySQL可以为不同的用户分配严格的、复杂的权限。这些操作大多都可以用SQL指令Grant（分配权限）和Revoke（回收权限）来实现。

ALTER: 修改表和索引。

CREATE: 创建数据库和表。

DELETE: 删除表中已有的记录。

DROP: 抛弃(删除)数据库和表。

INDEX: 创建或抛弃索引。

INSERT: 向表中插入新行。

REFERENCE: 未用。

SELECT: 检索表中的记录。

UPDATE: 修改现存表记录。

FILE: 读或写服务器上的文件。

PROCESS: 查看服务器中执行的线程信息或杀死线程。

RELOAD: 重载授权表或清空日志、主机缓存或表缓存。

SHUTDOWN: 关闭服务器。

ALL: 所有权限，ALL PRIVILEGES同义词。

USAGE: 特殊的 "无权限" 权限。

- MySQL用户管理

- 新建用户aaa,并设置密码123456 , 允许其在本地访问数据库db1的所有表

```
SQL> use mysql;
```

```
SQL> grant select,insert,update,delete  
      on db1.*  
      to aaa@localhost;
```

```
SQL> update user set password=password ('123456')  
      where user='aaa';
```

```
SQL> flush privileges;
```

- MySQL用户管理（续）
 - 去除用户aaa在db1数据库上的delete权限

```
SQL> use mysql;  
SQL> revoke delete on db1.* from aaa@localhost;  
SQL> flush privileges;
```
 - 查看用户权限

```
mysql> show grants for aaa@localhost;
```

- 设置MySQL远程访问

```
SQL>use mysql;
```

```
SQL>select host,user from user;
```

```
SQL>update user set host='%' where host='localhost';
```

```
SQL>flush privileges;
```

- MySQL备份

- 物理备份

- 复制数据文件

- 逻辑备份

- #mysqldump --database 数据库名 -hlocalhost -uroot -p >备份名.sql

- 注：--all-database参数为备份所有数据库

- 恢复数据

- # mysql -hlocalhost -uroot -p <备份名.sql

- 或者

- SQL> source 备份名.sql

MYSQL连结成功

DLL导出路径: **注意:** MYSQL 5.0以上版本请使用系统目录![导出到此目录](#)

SQL命令:

[执行](#)

回显结果:

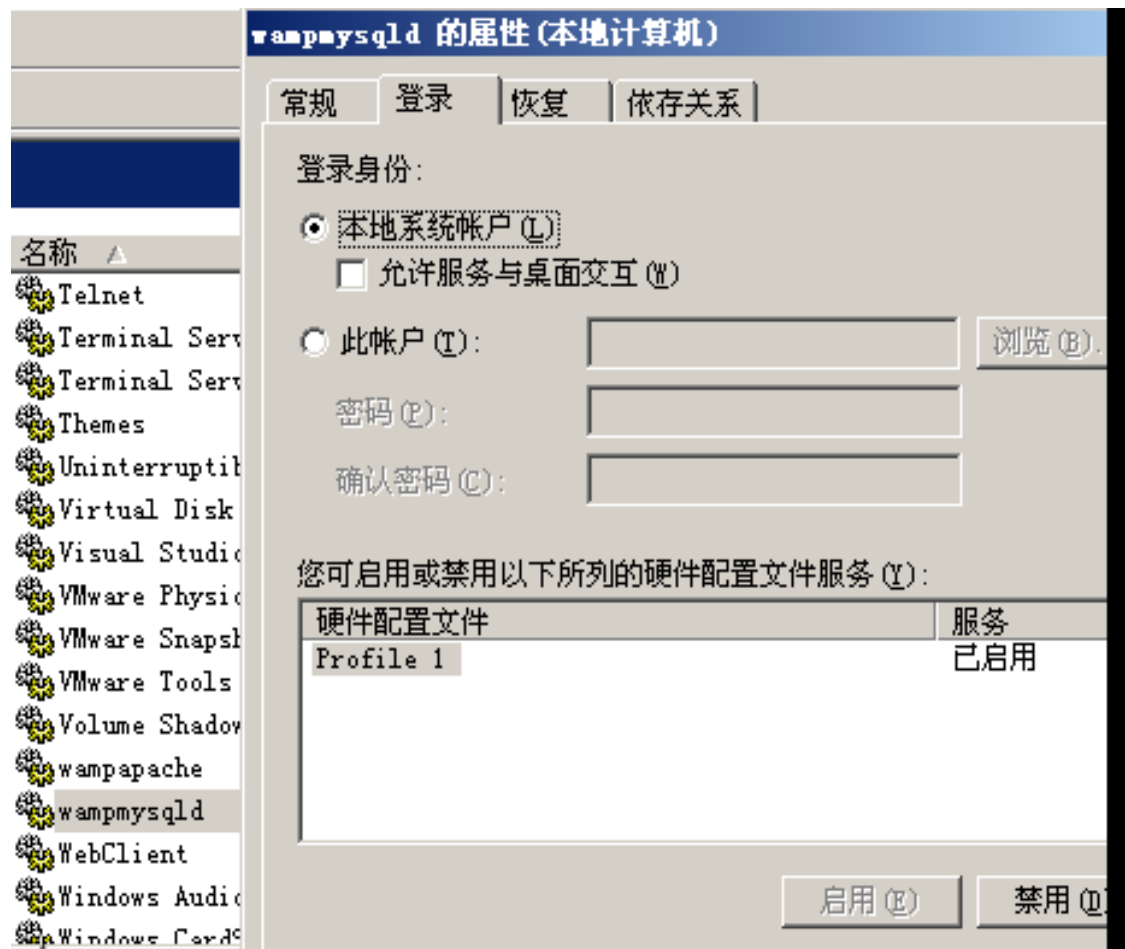
```
cmdshell('netstat -an')
```

Active Connections

Proto	Local Address	Foreign Address	State
TCP	0.0.0.0:23	0.0.0.0:0	LISTENING
TCP	0.0.0.0:80	0.0.0.0:0	LISTENING
TCP	0.0.0.0:135	0.0.0.0:0	LISTENING
TCP	0.0.0.0:445	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3306	0.0.0.0:0	LISTENING
TCP	0.0.0.0:3389	0.0.0.0:0	LISTENING

- MySQL帐号
 - 用户名为空用户
 - 密码为空用户
 - 权限过高用户









- 服务运行帐号











➤ 防护infile

```
mysql> revoke FILE on *.* from test1;
No connection. Trying to reconnect...
Connection id:      2
Current database: mysql

Query OK, 0 rows affected (0.00 sec)
```

 停止
  保存
  载入
  剪切
  复制
  粘贴
  清除
  自动换行

文件(F) 编辑(E) 查看(V) 窗口(W)

 停止
  保存
  载入
  剪切
  复制
  粘贴
  清除
  自动换行

```

mys
Dat
mys
mysql> select data from test into outfile 'c:\\
fi
test2.txt';
104 1045 - Access denied for user 'test1'@'%' (using password: YES)
mysql> select data from test into outfile 'c:\\test2.txt';
```

- Mysql审计
- 查看mysql配置文件my.cnf中log=xxx.log设置，默认未开启审计。
 1. 修改my.cnf，在[mysqld]部分添加行
 2. log = 记录的路径和文件名
 3. 重新启动mysql数据库

➤ 错误日志

包含了当**mysqld**启动和停止时，以及服务器在运行过程中发生任何严重错误时的相关信息。

可以用`--log-error[=file_name]`选项来指定**mysqld**保存错误日志文件的位置。

➤ 通用查询日志

所有连接和语句被记录到日志文件。当你怀疑在客户端发生了错误并想确切地知道该客户端发送给**mysqld**的语句时，该日志可能非常有用。

用`--log[=file_name]`或`-l [file_name]`选项启动它。如果没有给定*file_name*的值，默认名是*host_name.log*。

➤ 二进制日志

包含了所有更新了数据或者已经潜在更新了数据（例如，没有匹配任何行的一个 DELETE）的所有语句。语句以“事件”的形式保存，它描述数据更改。

当用--log-bin[=file_name]选项启动时，mysqld写入包含所有更新数据的SQL命令的日志文件。如果未给出file_name值，默认名为-bin后面所跟的主机名。

➤ 慢速查询日志

可以用来找到执行时间长的查询，可以用于优化。

用--log-slow-queries[=file_name]选项启动时，mysqld写一个包含所有执行时间超过long_query_time秒的SQL语句的日志文件。如果没有给出file_name值，默认未主机名，后缀为-slow.log。

开启错误日志，二进制日志和通用查询日志

--log-error

--log-bin

--log



谢谢！