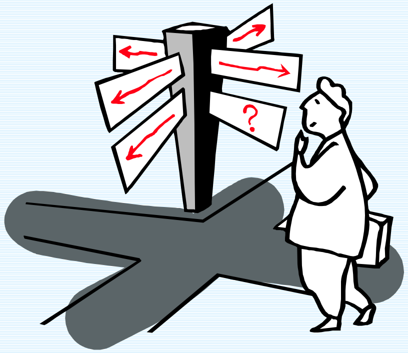
Auditing Windows NT 4.0

Sven Lehmberg

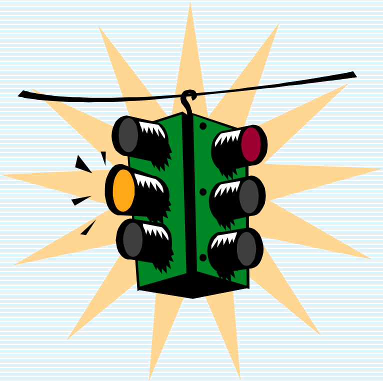


Agenda

- Event Viewer and User Manager
- Analyzing Audit Logs
- Tools

Auditing Step by Step

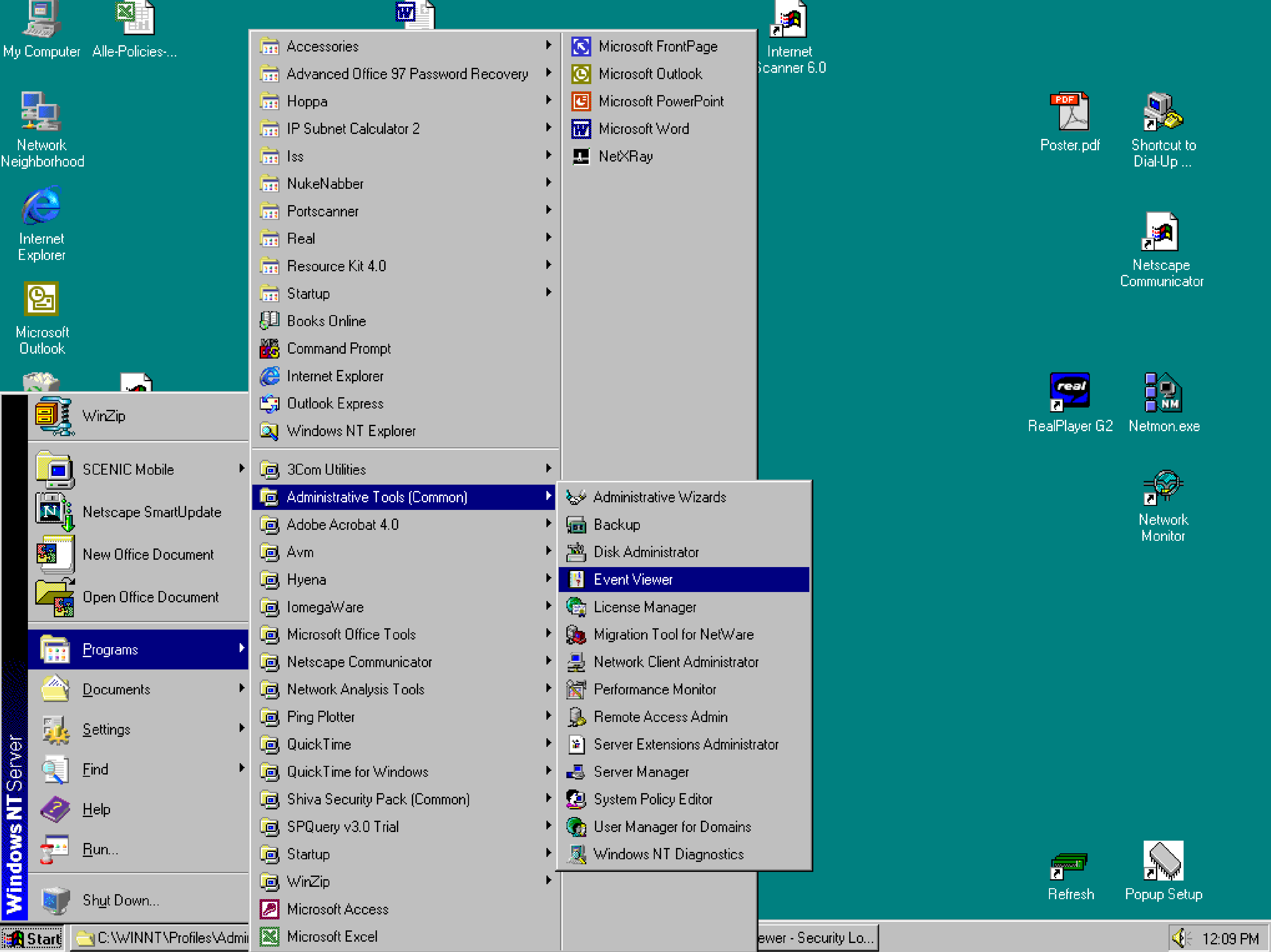
Two important programs in NT 4.0



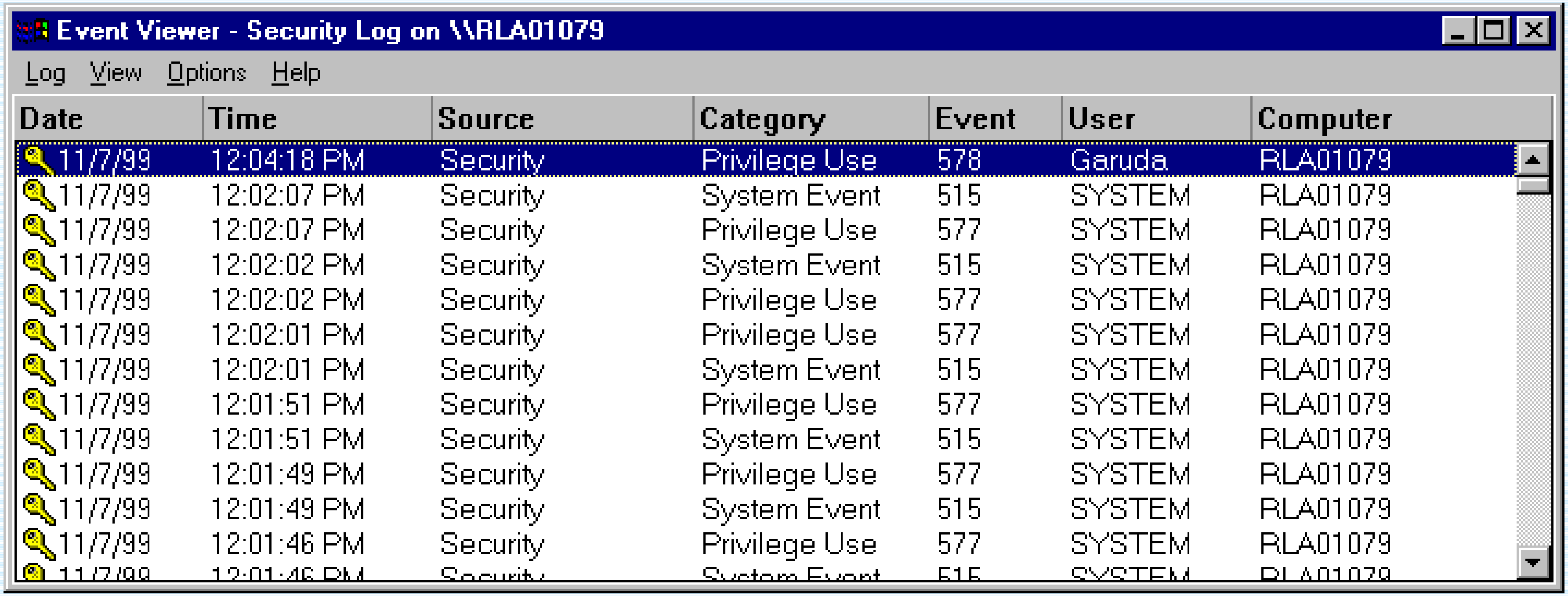
- ***Event Viewer***

and

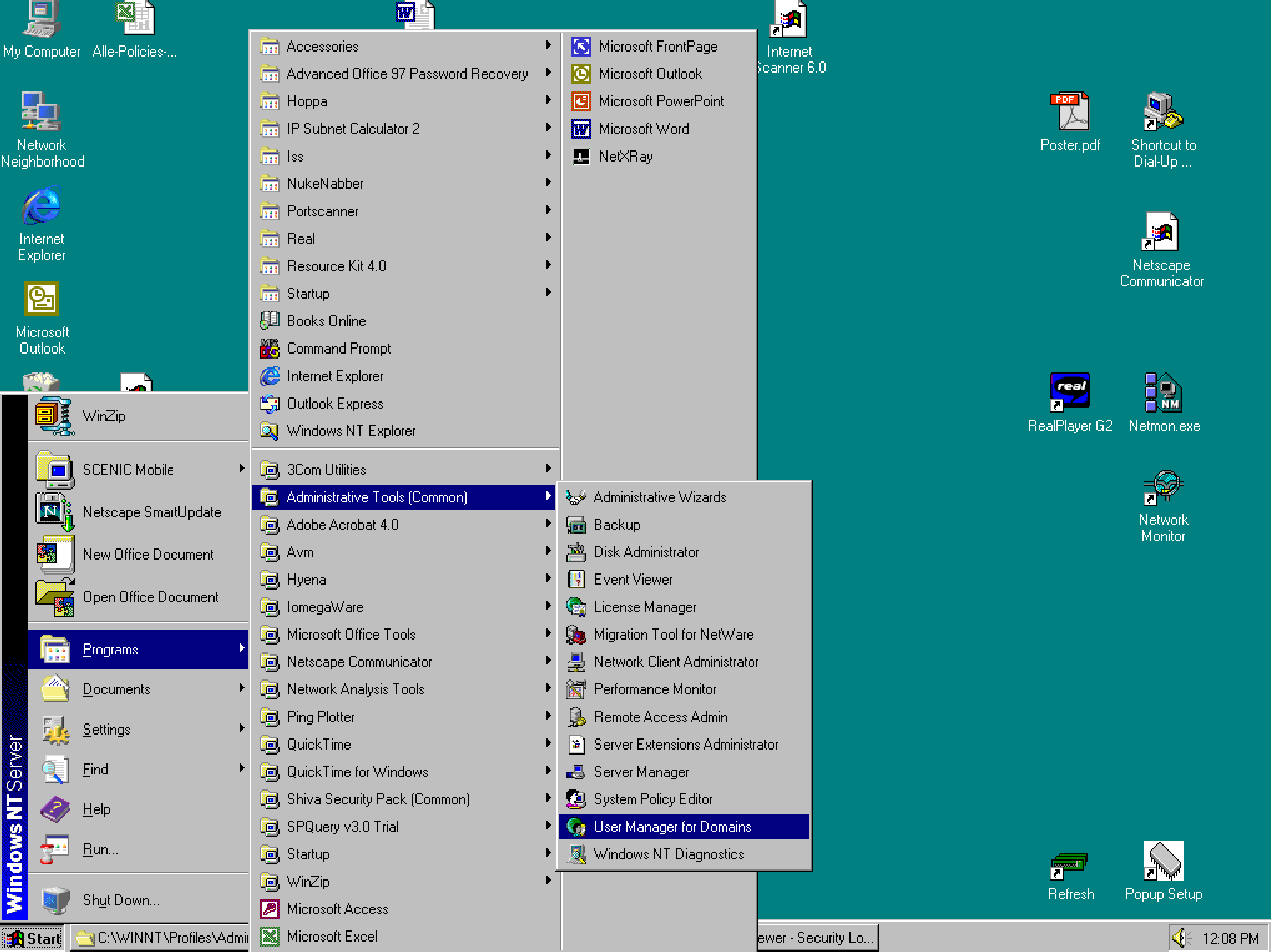
- ***User Manager***
User Manager for Domains


My Computer
Alle-Policies-...
Network Neighborhood
Internet Explorer
Microsoft Outlook
Internet Scanner 6.0
Poster.pdf
Shortcut to Dial-Up ...
Netscape Communicator
RealPlayer G2
Netmon.exe
Network Monitor
Refresh
Popup Setup
WinZip
SCENIC Mobile
Netscape SmartUpdate
New Office Document
Open Office Document
Programs
Documents
Settings
Find
Help
Run...
Shut Down...
Windows NT Server
Accessories
Advanced Office 97 Password Recovery
Hoppa
IP Subnet Calculator 2
Iss
NukeNabber
Portscanner
Real
Resource Kit 4.0
Startup
Books Online
Command Prompt
Internet Explorer
Outlook Express
Windows NT Explorer
3Com Utilities
Administrative Tools (Common)
Adobe Acrobat 4.0
Avm
Hyena
IomegaWare
Microsoft Office Tools
Netscape Communicator
Network Analysis Tools
Ping Plotter
QuickTime
QuickTime for Windows
Shiva Security Pack (Common)
SPQuery v3.0 Trial
Startup
WinZip
Microsoft Access
Microsoft Excel
Microsoft FrontPage
Microsoft Outlook
Microsoft PowerPoint
Microsoft Word
NetXRay
Administrative Wizards
Backup
Disk Administrator
Event Viewer
License Manager
Migration Tool for NetWare
Network Client Administrator
Performance Monitor
Remote Access Admin
Server Extensions Administrator
Server Manager
System Policy Editor
User Manager for Domains
Windows NT Diagnostics
Start
C:\WINNT\Profiles\Admi
ewer - Security Lo...
12:09 PM

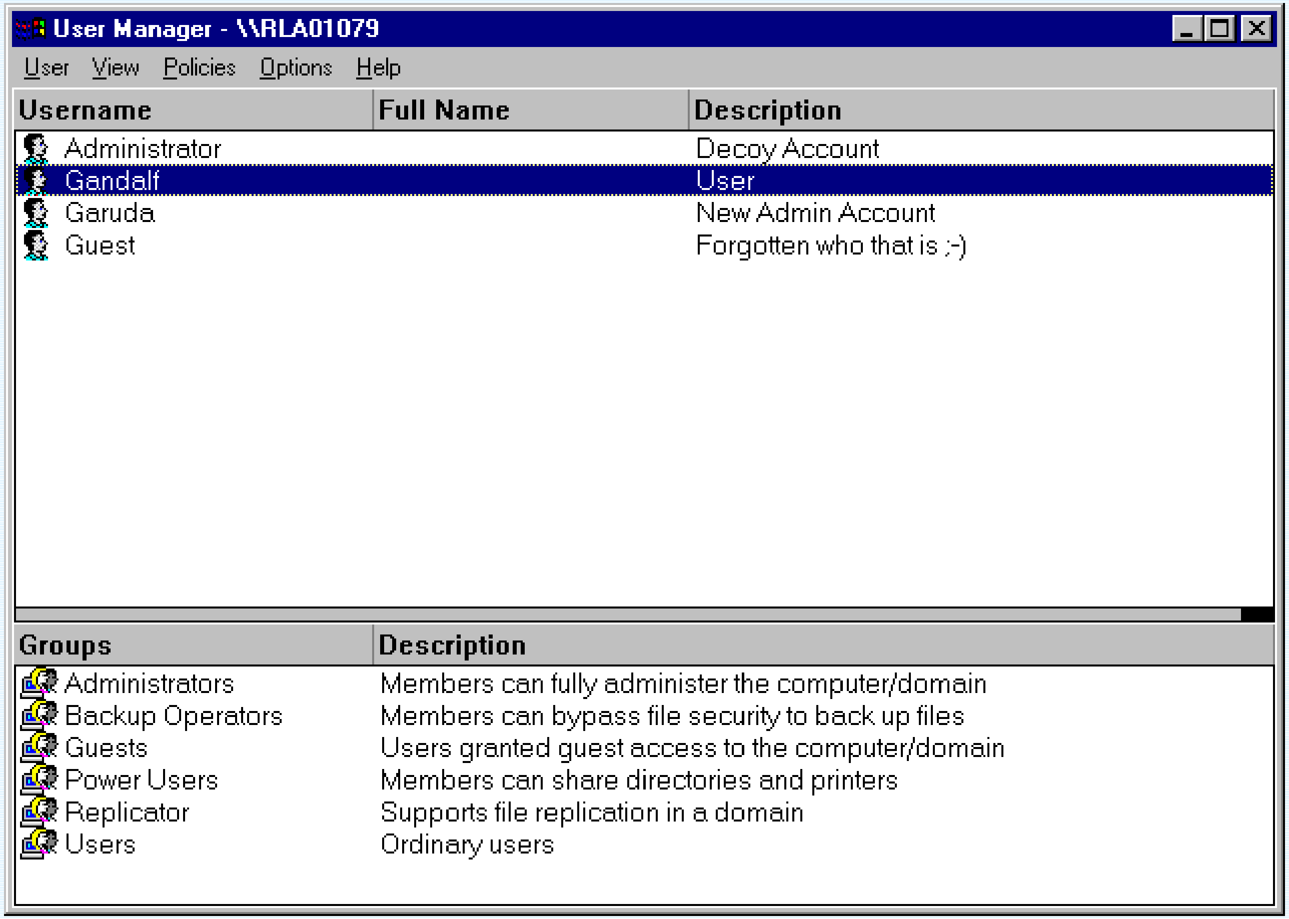
Event Viewer



Date	Time	Source	Category	Event	User	Computer
11/7/99	12:04:18 PM	Security	Privilege Use	578	Garuda	RLA01079
11/7/99	12:02:07 PM	Security	System Event	515	SYSTEM	RLA01079
11/7/99	12:02:07 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:02:02 PM	Security	System Event	515	SYSTEM	RLA01079
11/7/99	12:02:02 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:02:01 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:02:01 PM	Security	System Event	515	SYSTEM	RLA01079
11/7/99	12:01:51 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:01:51 PM	Security	System Event	515	SYSTEM	RLA01079
11/7/99	12:01:49 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:01:49 PM	Security	System Event	515	SYSTEM	RLA01079
11/7/99	12:01:46 PM	Security	Privilege Use	577	SYSTEM	RLA01079
11/7/99	12:01:46 PM	Security	System Event	515	SYSTEM	RLA01079


My Computer
Alle-Policies-...
Internet Scanner 6.0
Network Neighborhood
Internet Explorer
Microsoft Outlook
Poster.pdf
Shortcut to Dial-Up ...
Netscape Communicator
RealPlayer G2
Netmon.exe
Network Monitor
Refresh
Popup Setup
Accessories
Advanced Office 97 Password Recovery
Hoppa
IP Subnet Calculator 2
Iss
NukeNabber
Portscanner
Real
Resource Kit 4.0
Startup
Books Online
Command Prompt
Internet Explorer
Outlook Express
Windows NT Explorer
3Com Utilities
Administrative Tools (Common)
Adobe Acrobat 4.0
Avm
Hyena
IomegaWare
Microsoft Office Tools
Netscape Communicator
Network Analysis Tools
Ping Plotter
QuickTime
QuickTime for Windows
Shiva Security Pack (Common)
SPQuery v3.0 Trial
Startup
WinZip
Microsoft Access
Microsoft Excel
Microsoft FrontPage
Microsoft Outlook
Microsoft PowerPoint
Microsoft Word
NetXRay
Administrative Wizards
Backup
Disk Administrator
Event Viewer
License Manager
Migration Tool for NetWare
Network Client Administrator
Performance Monitor
Remote Access Admin
Server Extensions Administrator
Server Manager
System Policy Editor
User Manager for Domains
Windows NT Diagnostics
WinZip
SCENIC Mobile
Netscape SmartUpdate
New Office Document
Open Office Document
Programs
Documents
Settings
Find
Help
Run...
Shut Down...
Windows NT Server
Start
C:\WINNT\Profiles\Admi
ewer - Security Lo...
12:08 PM

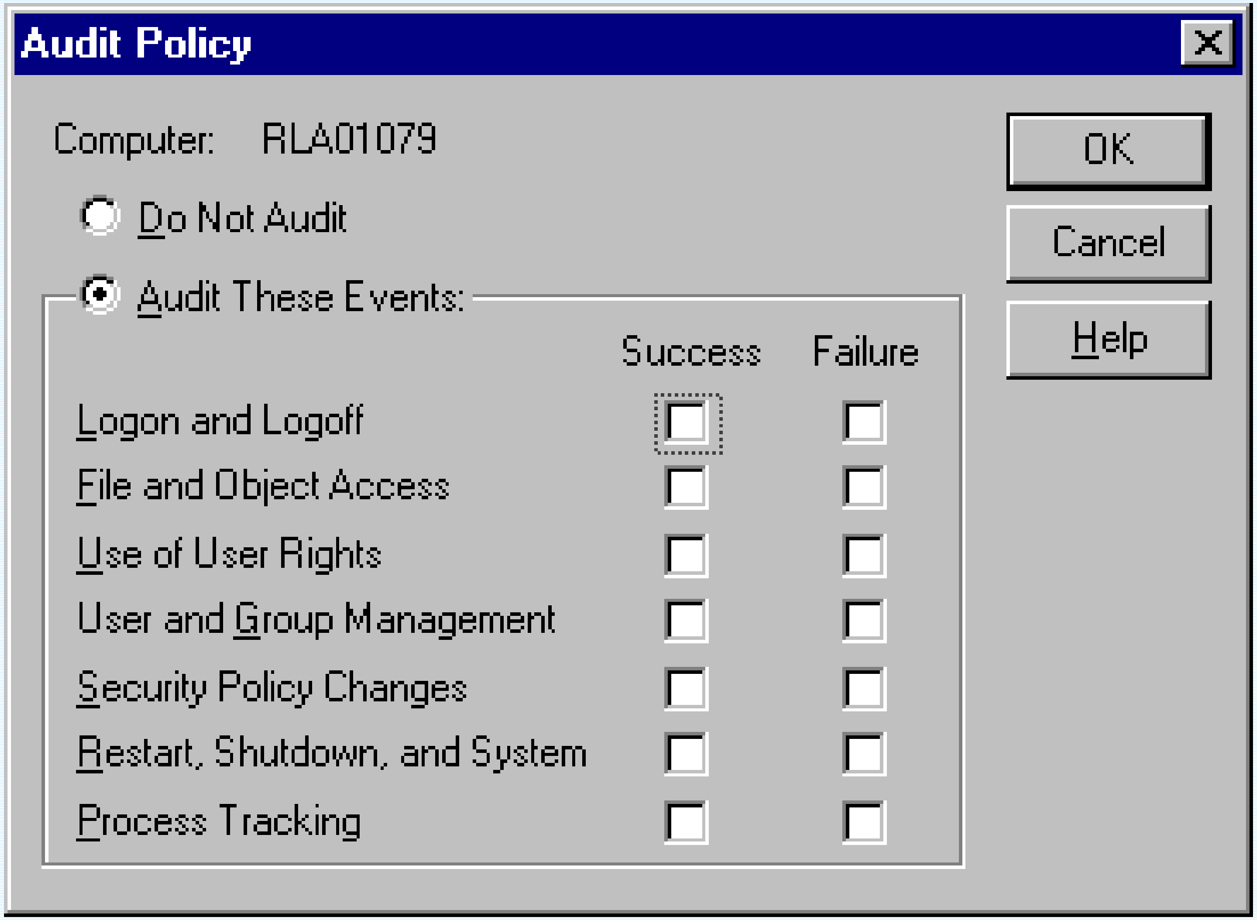
HOWTO Enable Auditing ?



Username	Full Name	Description
Administrator		Decoy Account
Gandalf		User
Garuda		New Admin Account
Guest		Forgotten who that is ;-)

Groups	Description
Administrators	Members can fully administer the computer/domain
Backup Operators	Members can bypass file security to back up files
Guests	Users granted guest access to the computer/domain
Power Users	Members can share directories and printers
Replicator	Supports file replication in a domain
Users	Ordinary users

What to Audit ?



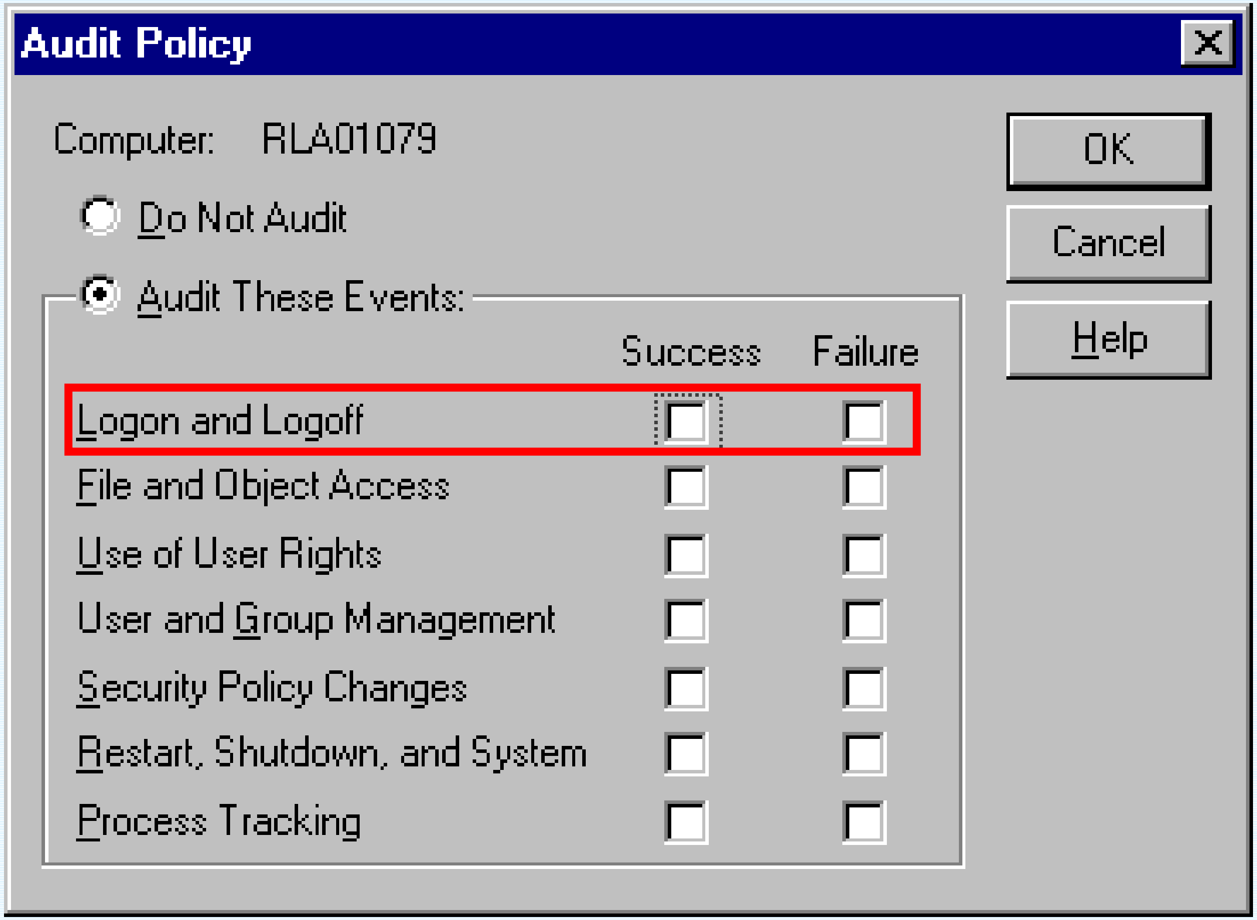
Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Logon and Logoff



Audit Policy

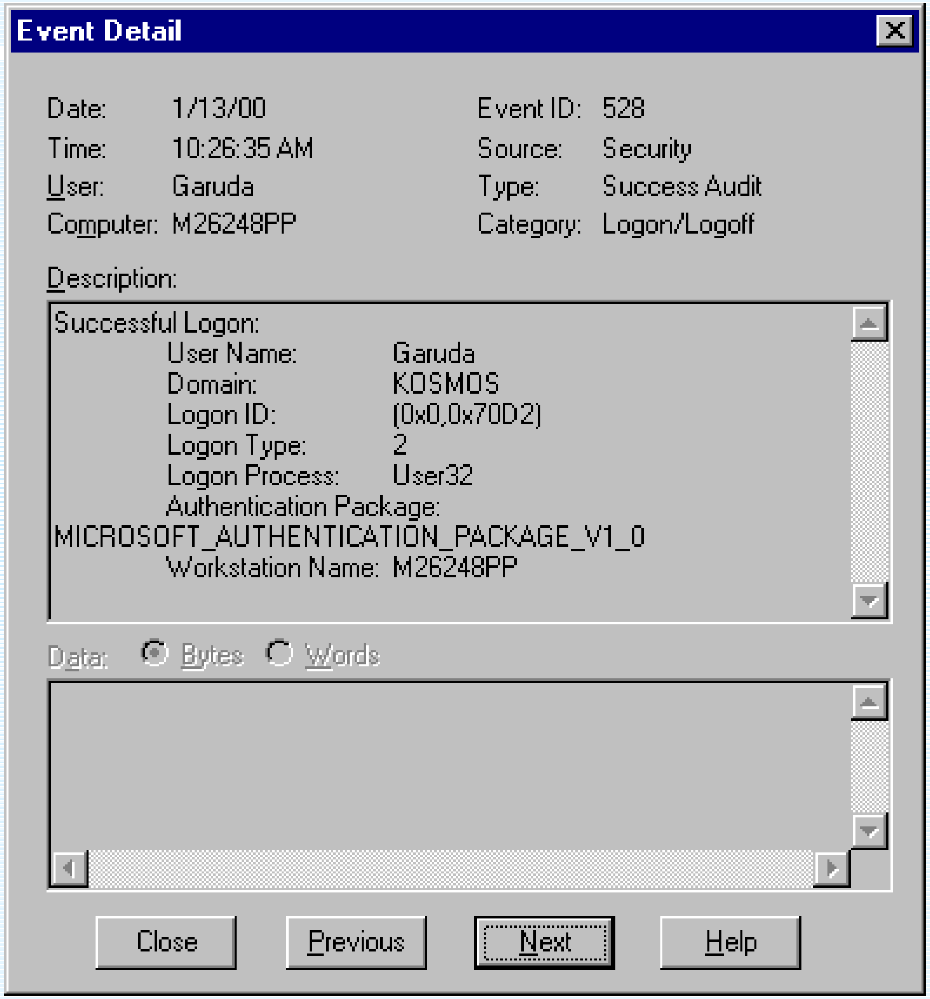
Computer: RLA01079

○ Do Not Audit

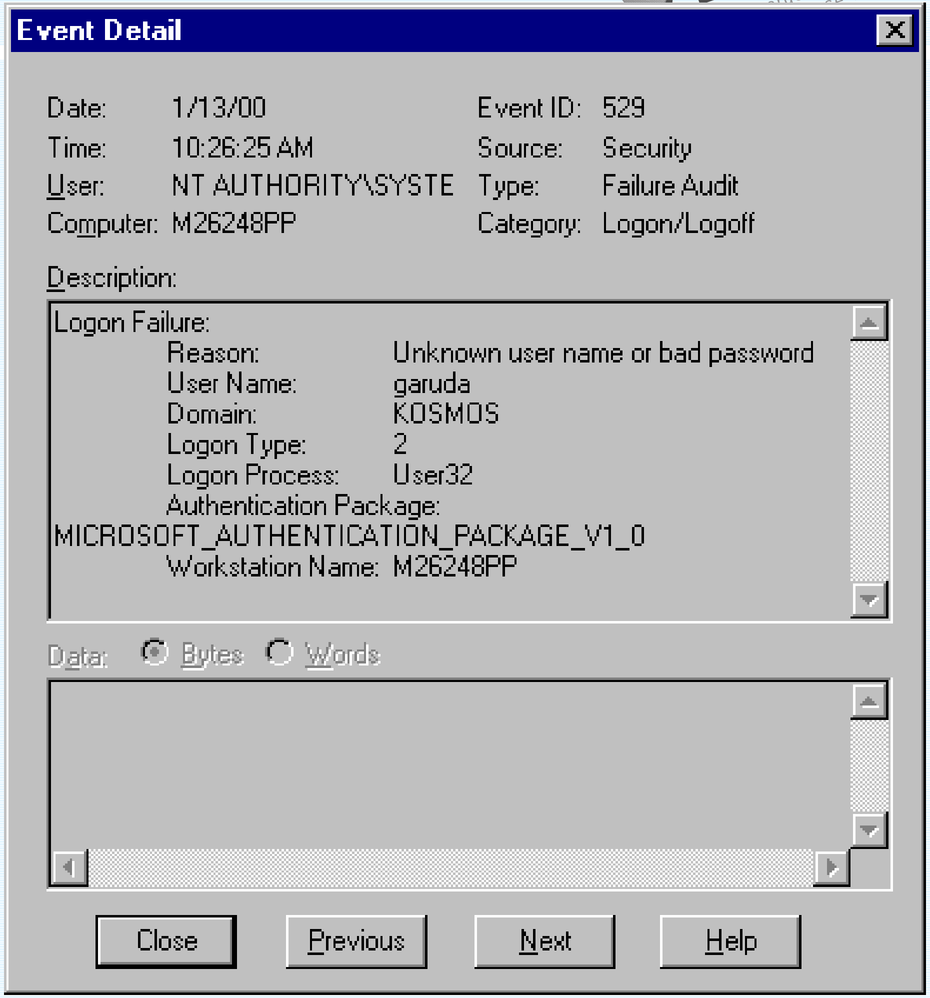
● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Interactive Logon



```
Date:      1/13/00              Event ID:  528
Time:      10:26:35 AM          Source:    Security
User:      Garuda               Type:      Success Audit
Computer:  M26248PP             Category:  Logon/Logoff

Description:
Successful Logon:
         User Name:        Garuda
         Domain:           KOSMOS
         Logon ID:         (0x0,0x70D2)
         Logon Type:       2
         Logon Process:    User32
         Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
         Workstation Name: M26248PP
```



```
Date:      1/13/00              Event ID:  529
Time:      10:26:25 AM          Source:    Security
User:      NT AUTHORITY\SYSTE   Type:      Failure Audit
Computer:  M26248PP             Category:  Logon/Logoff

Description:
Logon Failure:
         Reason:           Unknown user name or bad password
         User Name:        garuda
         Domain:           KOSMOS
         Logon Type:       2
         Logon Process:    User32
         Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
         Workstation Name: M26248PP
```

Logon Type and Processes

Logon Type:

2 : Interactive
3 : Network
4 : Batch
5 : Service
6 : Proxy
7 : Unlock Workstation

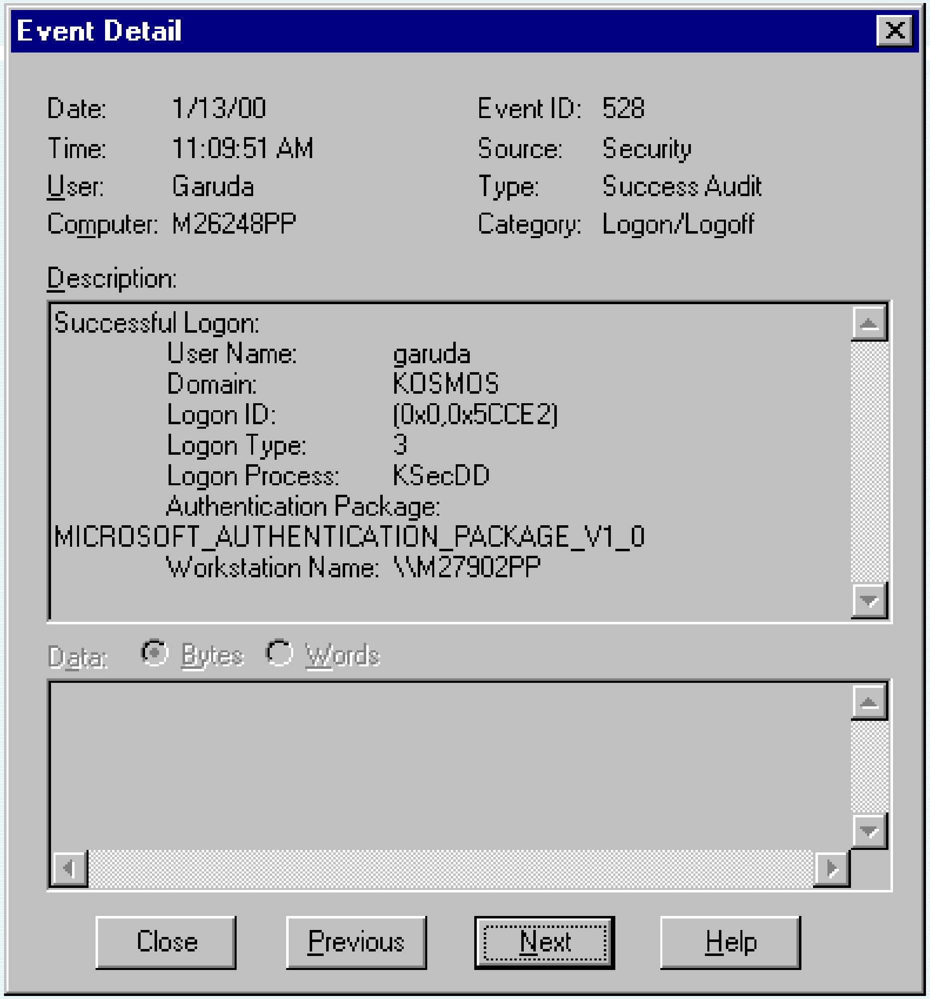
Authentication Package:

MICROSOFT_AUTHENTICATION_PACKAGE_V1_0

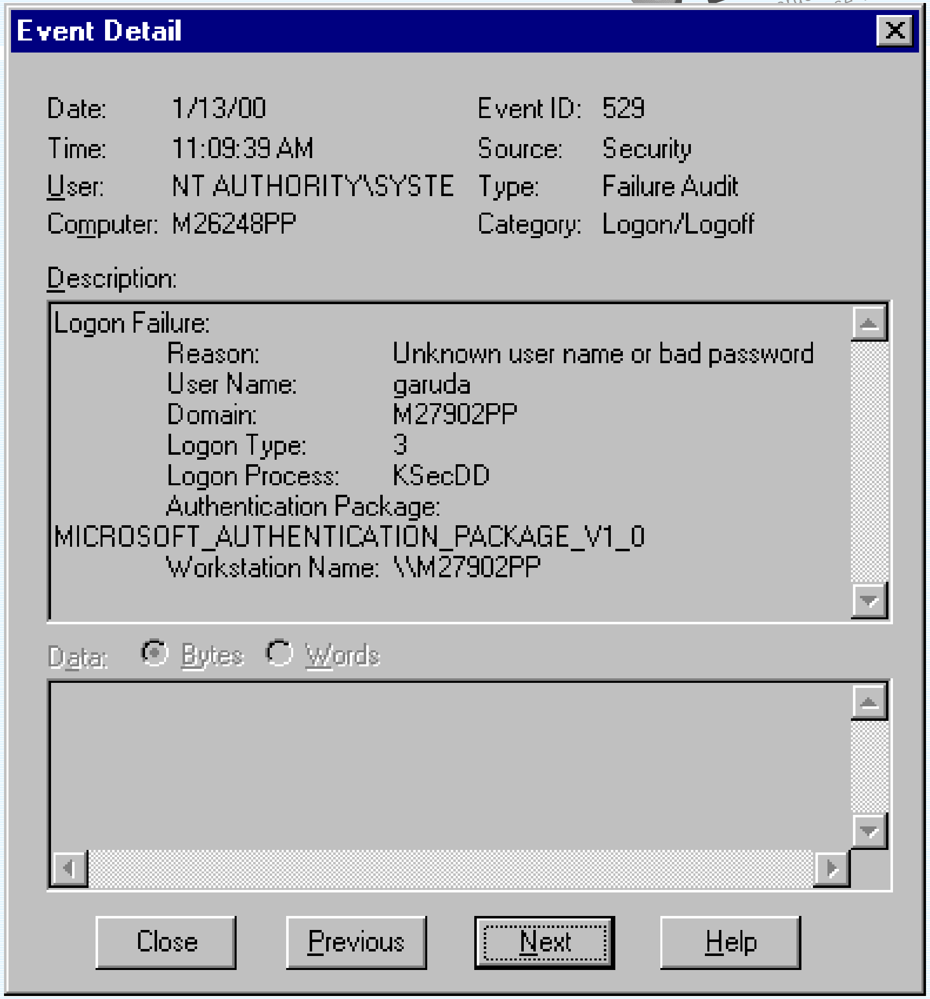
Logon Process:

- KSecDD
- User32 or WinLogon\MSGina
- SCMgr
- LAN Manager Workstation Service
- advapi
- MS.RADIUS

Logon over the Network

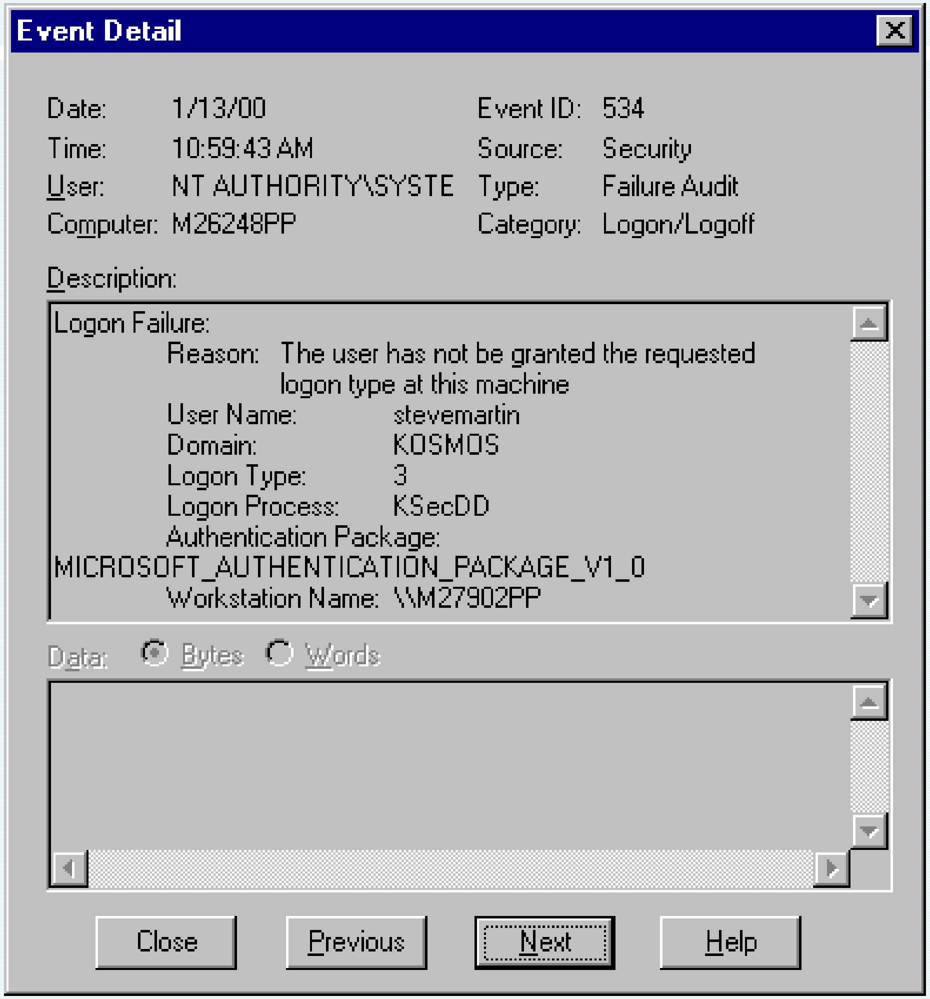


```
Date:      1/13/00              Event ID:  528
Time:      11:09:51 AM          Source:    Security
User:      Garuda               Type:      Success Audit
Computer:  M26248PP             Category:  Logon/Logoff

Description:
Successful Logon:
        User Name:          garuda
        Domain:             KOSMOS
        Logon ID:           (0x0,0x5CCE2)
        Logon Type:         3
        Logon Process:      KSecDD
        Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
        Workstation Name:   \\M27902PP
```



```
Date:      1/13/00                   Event ID:  529
Time:      11:09:39 AM               Source:    Security
User:      NT AUTHORITY\SYSTE        Type:      Failure Audit
Computer:  M26248PP                  Category:  Logon/Logoff

Description:
Logon Failure:
        Reason:             Unknown user name or bad password
        User Name:          garuda
        Domain:             M27902PP
        Logon Type:         3
        Logon Process:      KSecDD
        Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
        Workstation Name:   \\M27902PP
```

Event Detail – No Logon Right over Network



Event Detail

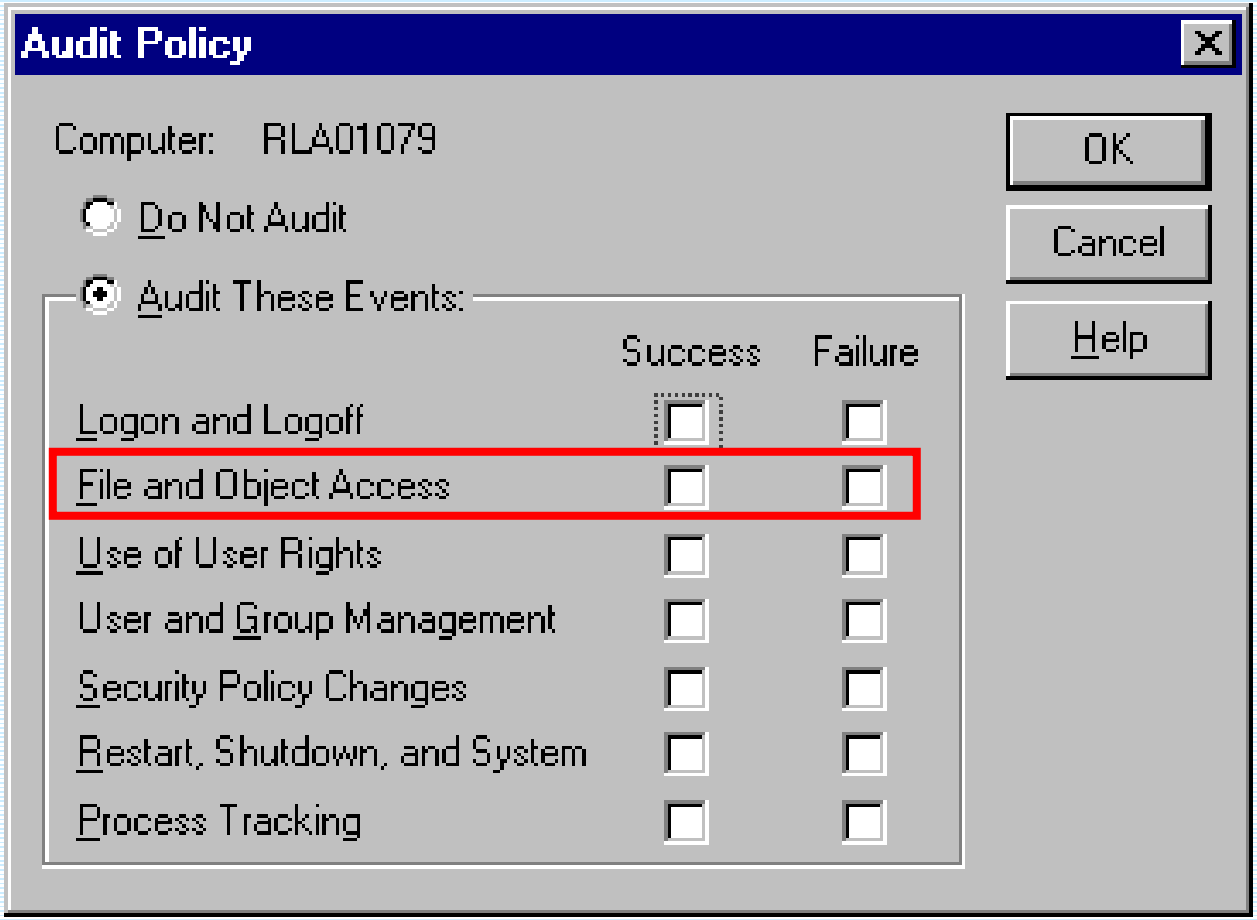
Date: 1/13/00 Event ID: 534
Time: 10:59:43 AM Source: Security
User: NT AUTHORITY\SYSTE Type: Failure Audit
Computer: M26248PP Category: Logon/Logoff

Description:

```
Logon Failure:
		Reason:	The user has not be granted the requested
			logon type at this machine
		User Name:		stevemartin
		Domain:		KOSMOS
		Logon Type:		3
		Logon Process:	KSecDD
		Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
		Workstation Name:	\\M27902PP
```

Data: ● Bytes ○ Words

File and Object Access



Audit Policy

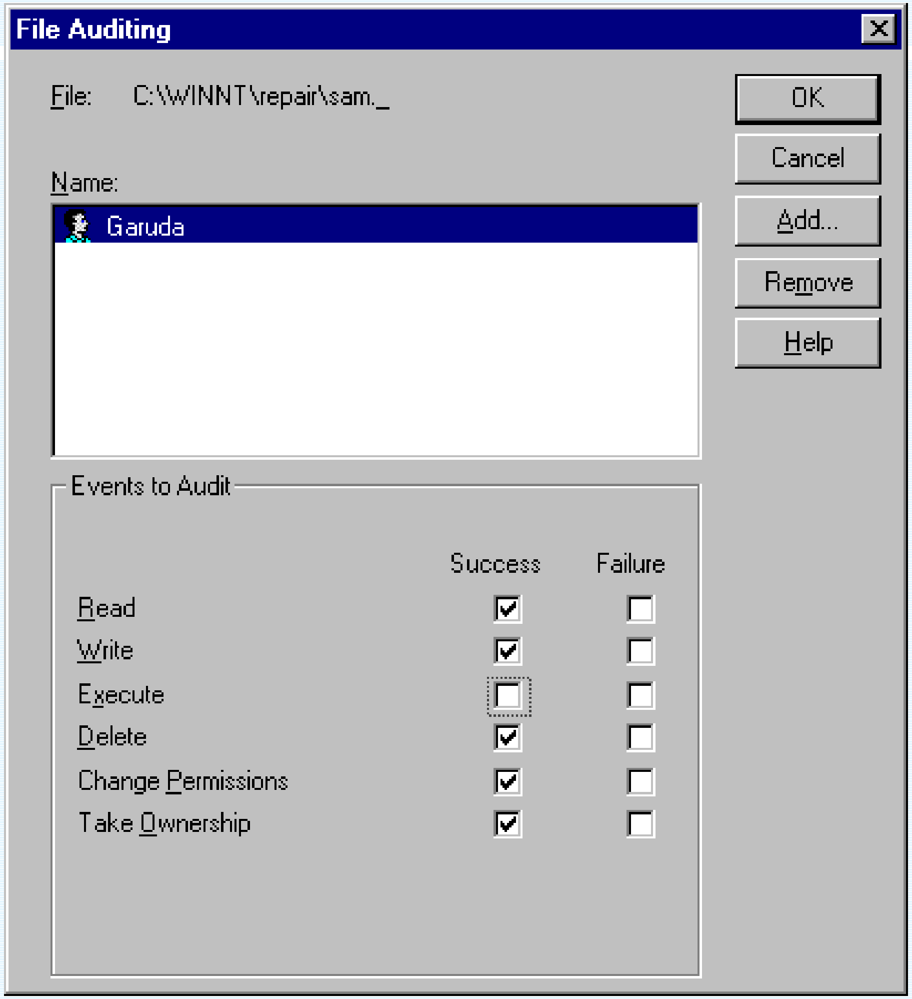
Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

File And Registry Auditing



File Auditing

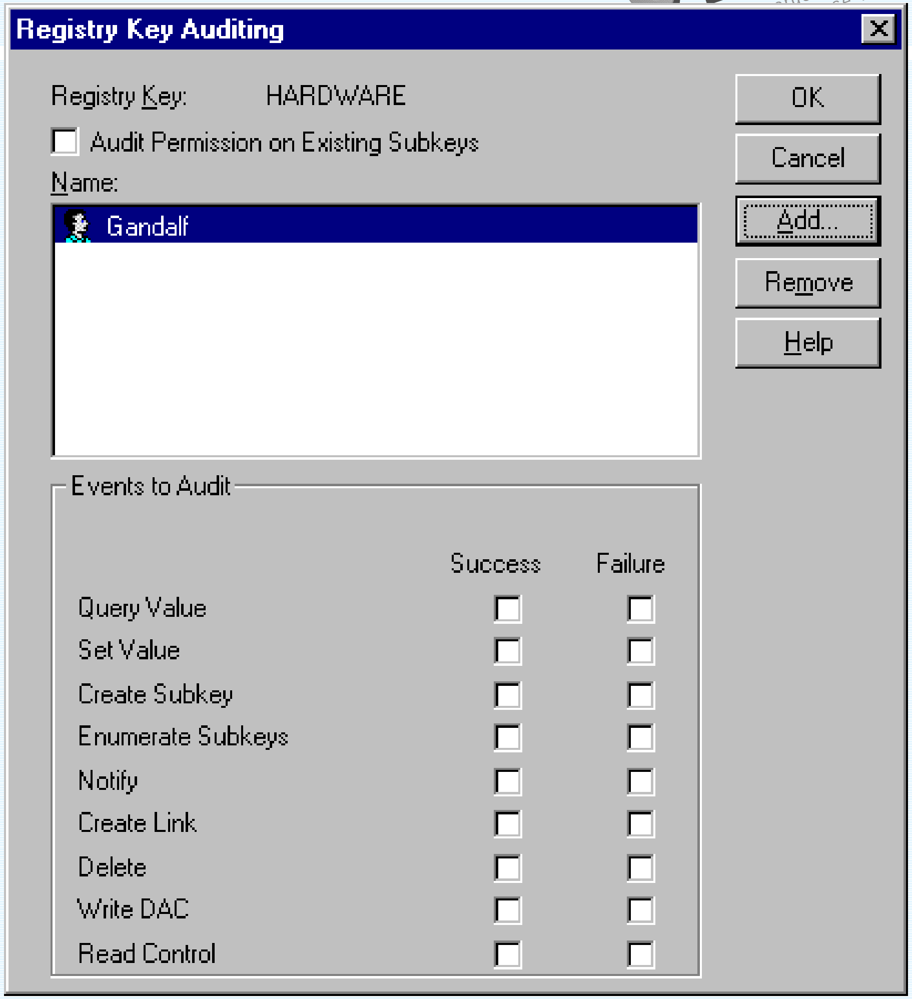
File: C:\WINNT\repair\sam._

Name:

- Garuda

Events to Audit

	Success	Failure
Read	☑	□
Write	☑	□
Execute	□	□
Delete	☑	□
Change Permissions	☑	□
Take Ownership	☑	□



Registry Key Auditing

Registry Key: HARDWARE

□ Audit Permission on Existing Subkeys

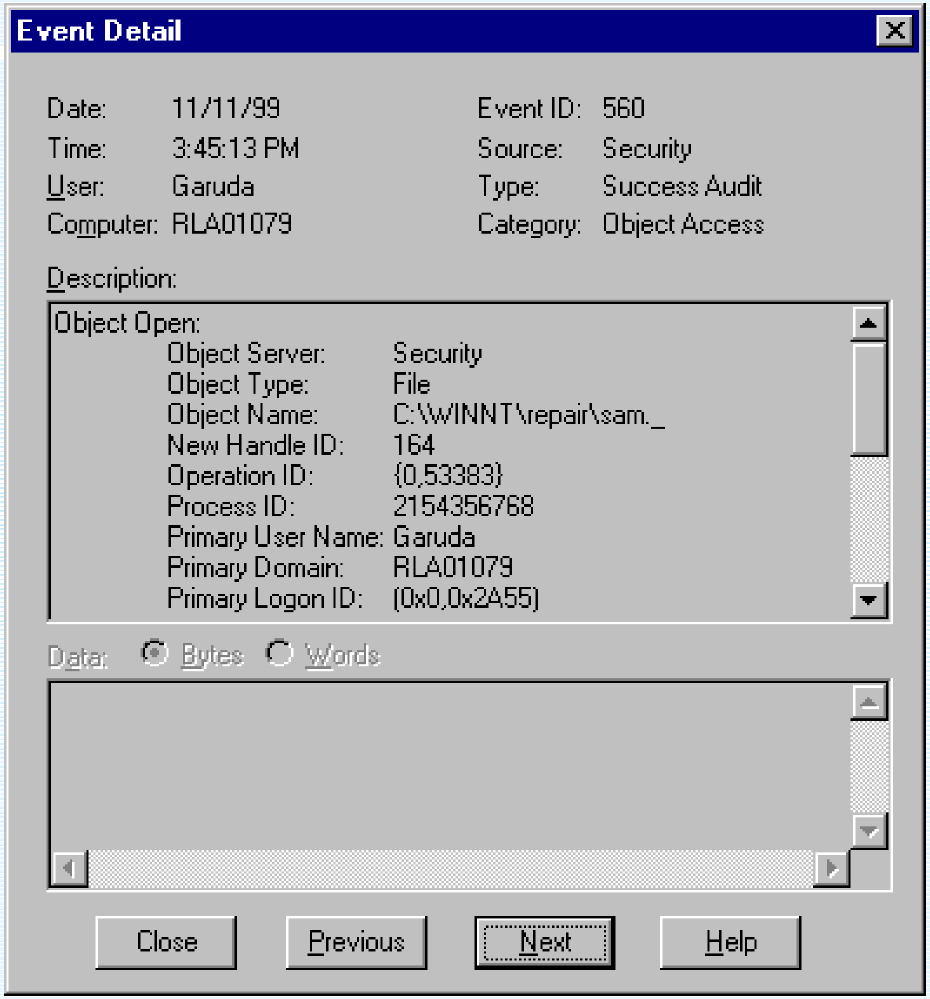
Name:

- Gandalf

Events to Audit

	Success	Failure
Query Value	□	□
Set Value	□	□
Create Subkey	□	□
Enumerate Subkeys	□	□
Notify	□	□
Create Link	□	□
Delete	□	□
Write DAC	□	□
Read Control	□	□

Event Detail – Object Access: File



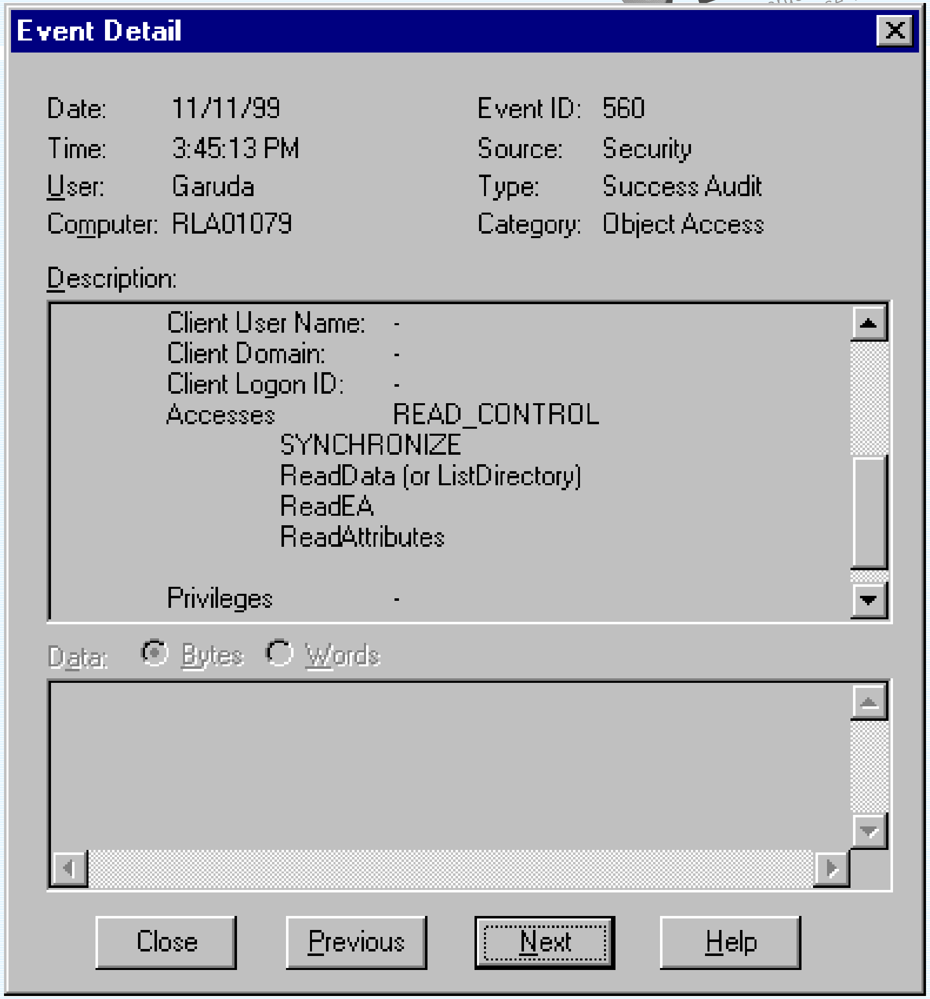
Event Detail

```
Date:      11/11/99         Event ID:  560
Time:      3:45:13 PM       Source:    Security
User:      Garuda           Type:      Success Audit
Computer:  RLA01079         Category:  Object Access
```

Description:

```
Object Open:
        Object Server:       Security
        Object Type:         File
        Object Name:         C:\WINNT\repair\sam._
        New Handle ID:       164
        Operation ID:        {0,53383}
        Process ID:          2154356768
        Primary User Name:   Garuda
        Primary Domain:      RLA01079
        Primary Logon ID:    (0x0,0x2A55)
```

Data: ● Bytes ○ Words



Event Detail

```
Date:      11/11/99         Event ID:  560
Time:      3:45:13 PM       Source:    Security
User:      Garuda           Type:      Success Audit
Computer:  RLA01079         Category:  Object Access
```

Description:

```
        Client User Name:    -
        Client Domain:       -
        Client Logon ID:     -
        Accesses             READ_CONTROL
                SYNCHRONIZE
                ReadData (or ListDirectory)
                ReadEA
                ReadAttributes

        Privileges           -
```

Data: ● Bytes ○ Words

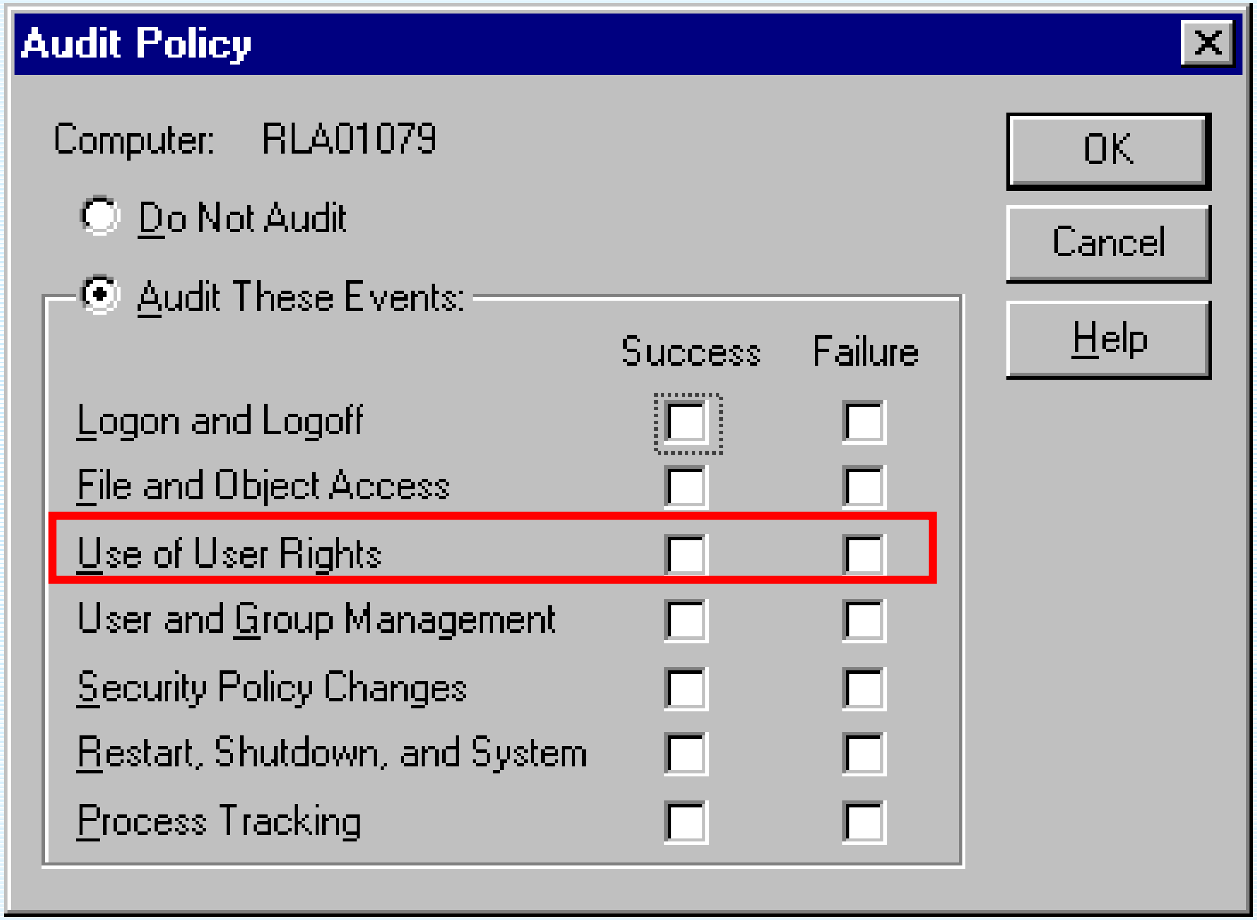
File System Access Types

	Full control	Modify	Read&Execute, List folders	Read	Write
Traverse folder / Execute file	x	x	x		
List folder / Read data	x	x	x	x	
Read attributes	x	x	x	x	
Read extended attributes	x	x	x	x	
Create files / Write data	x	x			x
Create folders / Append data	x	x			x
Write attributes	x	x			x
Write extended attributes	x	x			x
Delete subfolders and files	x				
Delete	x	x			
Read permissions (READ_CONTROL)	x	x	x	x	x
Change permissions (WRITE_DAC)	x				
Take ownership (WRITE_OWNER)	x				
Synchronize	x	x	x	x	x

Registry Access Types

- Query Value
- Set Value
- Create Subkey
- Enumerate Subkeys
- Notify
- Create Link
- Delete
- Write DAC
- Read Control

Use of User Rights



Computer: RLA01079

○ Do Not Audit

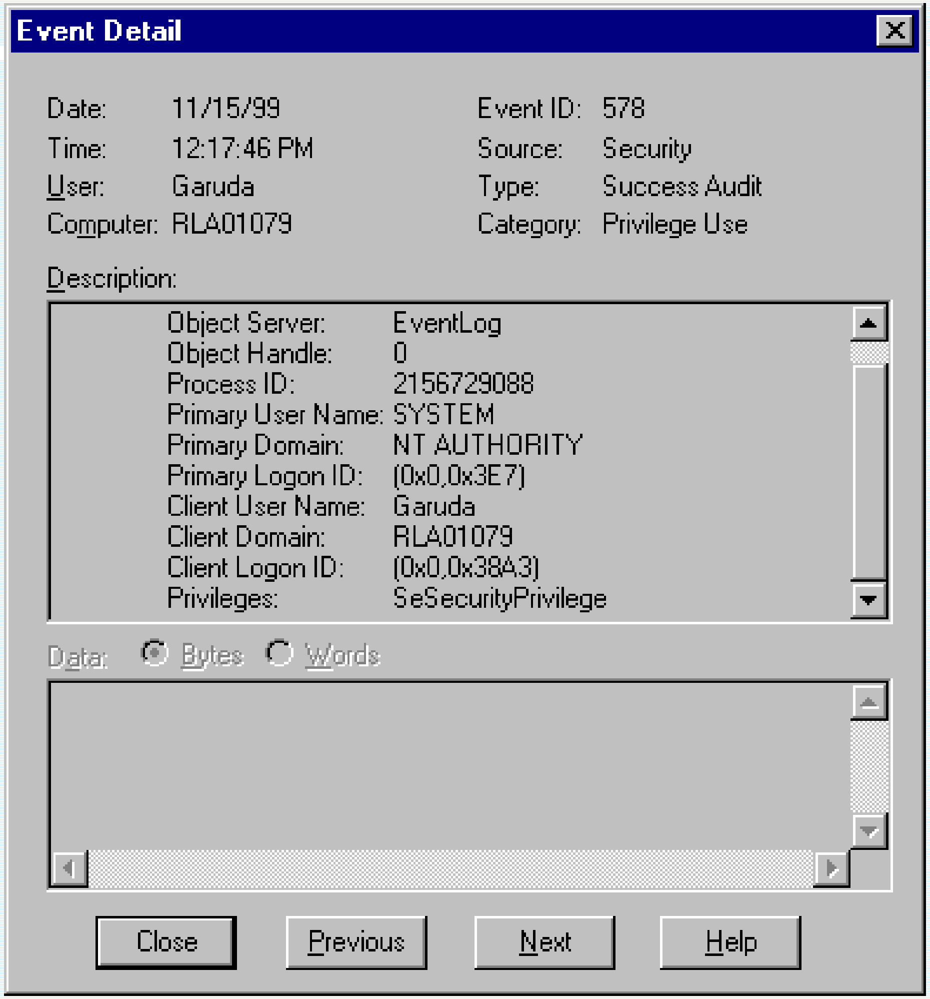
● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

27 User Rights

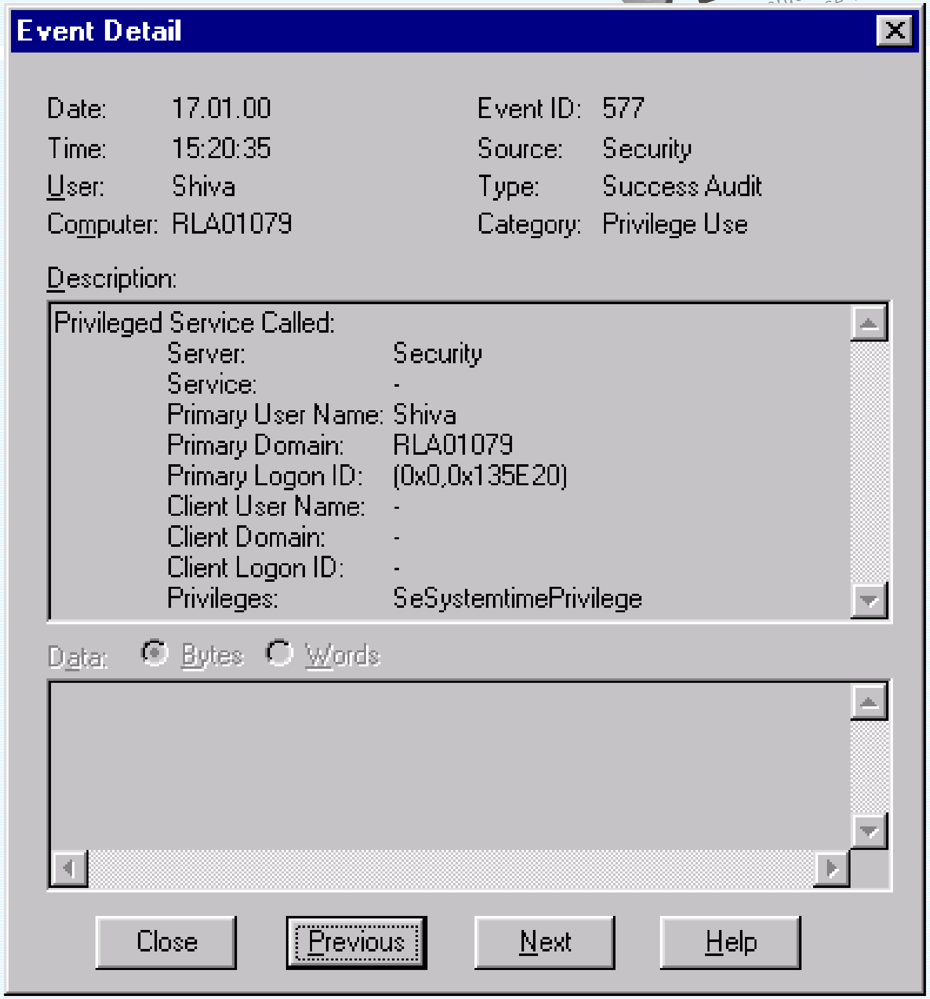
Access this Computer from Network	Debug programs – SeDebugPrivilege	Log on locally
Act as part of the operating system - SeTcbPrivilege	Force shutdown from a remote system – SeRemoteShutdownPrivilege	Manage auditing and security - **SeSecurityPrivilege**
Add workstation to domain – SeMachineAccountPrivilege	Generate security audits – SeAuditPrivilege	Modify firmware environment values – SeSystemEnvironmentPriv.
Backup files and directories – SeBackupPrivilege	Increase quotas – SeIncreaseQuotaPrivilege	Profile single process – SeProfileSingleProcessPriv.
Bypass traverse checking – SeChangeNotifyPrivilege	Increase scheduling priority – SeIncreaseBasePriorityPriv.	Profile system performance – SeSystemProfilePriv.
Change the system time – **SeSystemTimePrivilege**	Load and unload device drivers – SeLoadDriverPrivilege	Replace a process level token – SeAssignPrimaryTokenPriv.
Create a pagefile – SeCreatePagefilePrivilege	Lock pages in memory – SeLockMemoryPriv.	Restore files and directories – SeRestorePriv.
Create a token object – SeCreateTokenPrivilege	Log on as a batch job – SeBatchSID	Shut down the system – SeShutdownPriv.
Create permanent shared objects – SeCreate PermanentPrivilege	Log on as a Service – SeServiceSID	Take ownership of files or other objects – SeTakeOwnershipPriv.

Event Detail – Use of User Rights



Event Detail

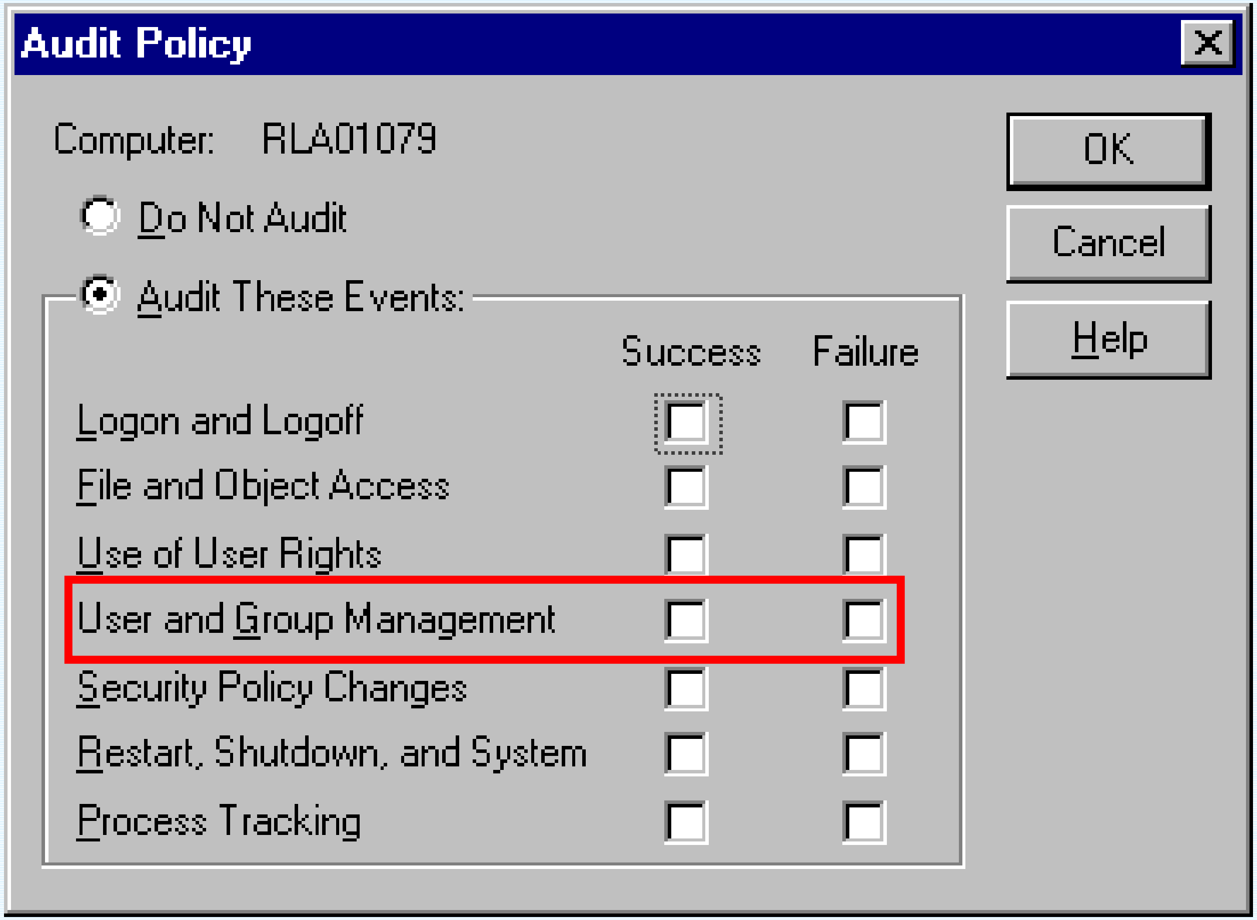
```
Date:      11/15/99          Event ID:  578
Time:      12:17:46 PM       Source:    Security
User:      Garuda            Type:      Success Audit
Computer:  RLA01079          Category:  Privilege Use

Description:
         Object Server:      EventLog
         Object Handle:      0
         Process ID:         2156729088
         Primary User Name:  SYSTEM
         Primary Domain:     NT AUTHORITY
         Primary Logon ID:   (0x0,0x3E7)
         Client User Name:   Garuda
         Client Domain:      RLA01079
         Client Logon ID:    (0x0,0x38A3)
         Privileges:         SeSecurityPrivilege

Data:  ● Bytes  ○ Words
```



Event Detail

```
Date:      17.01.00          Event ID:  577
Time:      15:20:35          Source:    Security
User:      Shiva             Type:      Success Audit
Computer:  RLA01079          Category:  Privilege Use

Description:
Privileged Service Called:
         Server:             Security
         Service:            -
         Primary User Name:  Shiva
         Primary Domain:     RLA01079
         Primary Logon ID:   (0x0,0x135E20)
         Client User Name:   -
         Client Domain:      -
         Client Logon ID:    -
         Privileges:         SeSystemtimePrivilege

Data:  ● Bytes  ○ Words
```

User and Group Management



Audit Policy

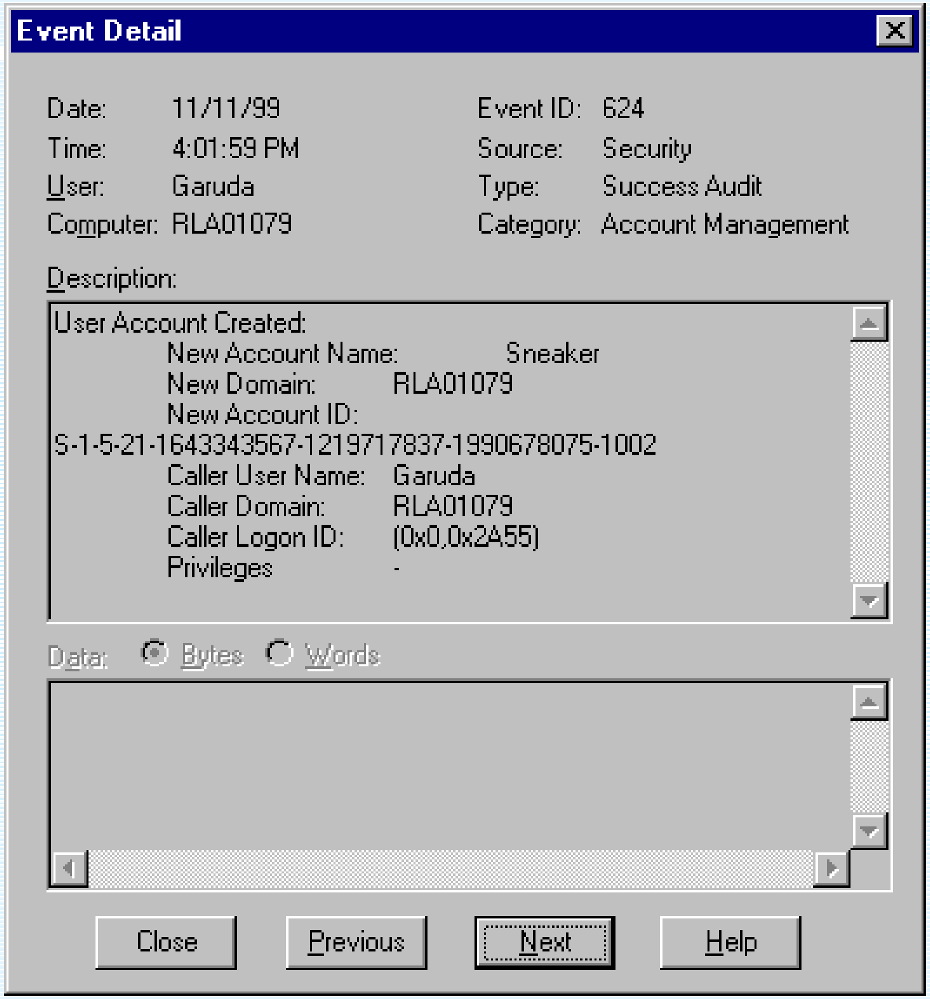
Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Event Detail – User and Group Management



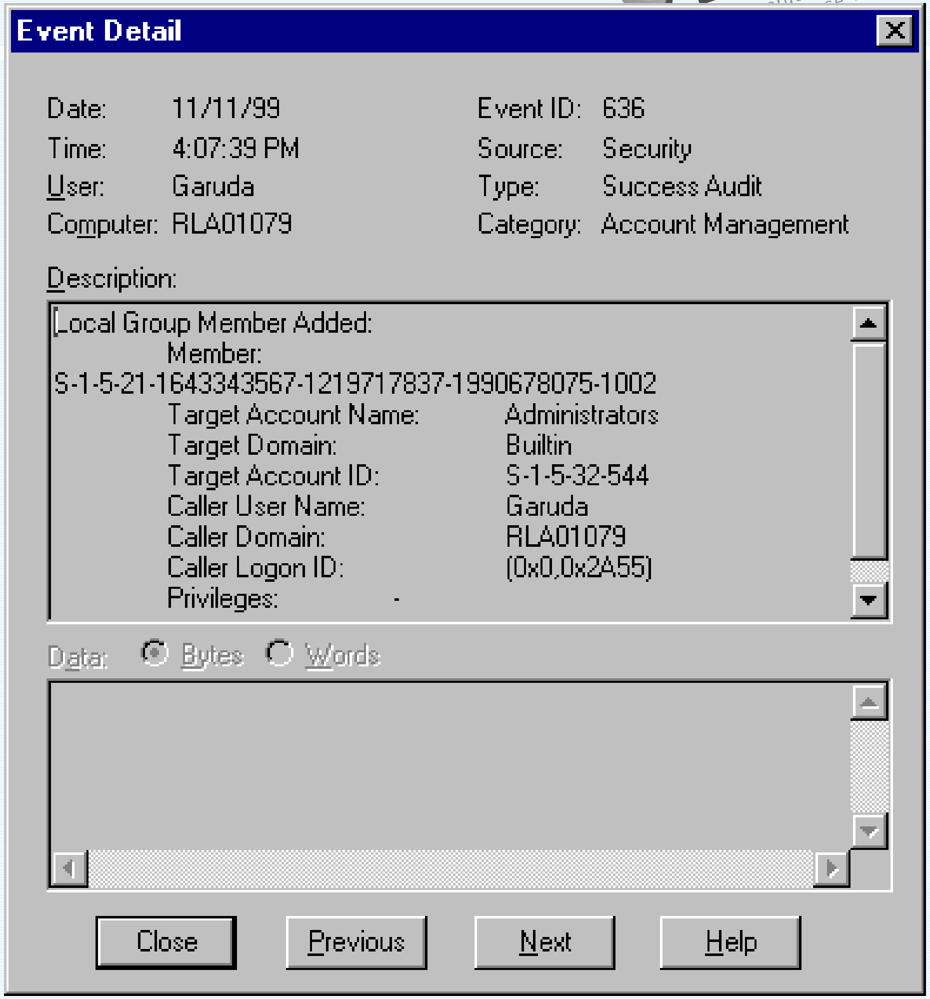
Event Detail

Date: 11/11/99
Time: 4:01:59 PM
User: Garuda
Computer: RLA01079

Event ID: 624
Source: Security
Type: Success Audit
Category: Account Management

Description:

```
User Account Created:
          New Account Name:            Sneaker
          New Domain:         RLA01079
          New Account ID:
S-1-5-21-1643343567-1219717837-1990678075-1002
          Caller User Name:   Garuda
          Caller Domain:      RLA01079
          Caller Logon ID:    (0x0,0x2A55)
          Privileges          -
```



Event Detail

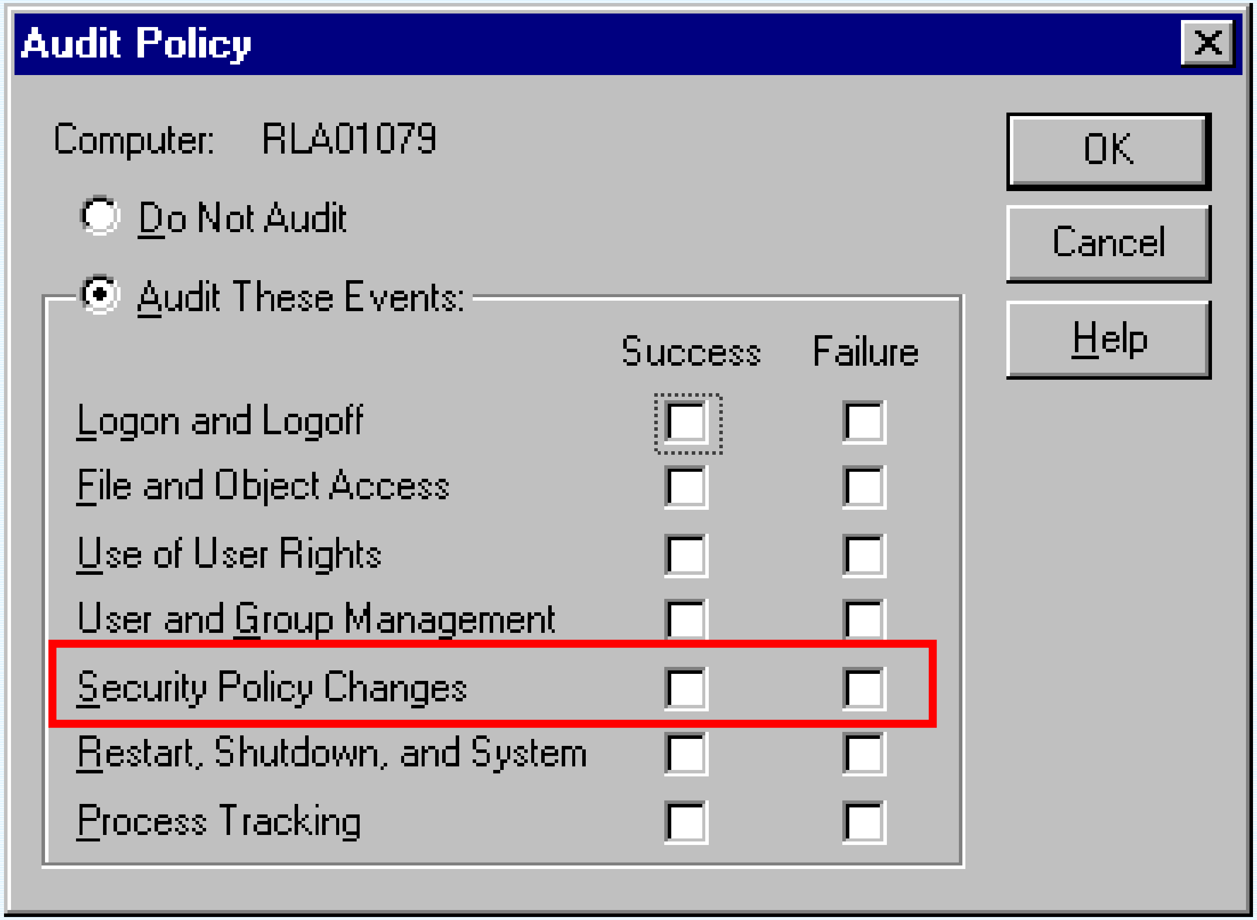
Date: 11/11/99
Time: 4:07:39 PM
User: Garuda
Computer: RLA01079

Event ID: 636
Source: Security
Type: Success Audit
Category: Account Management

Description:

```
Local Group Member Added:
          Member:
S-1-5-21-1643343567-1219717837-1990678075-1002
          Target Account Name:        Administrators
          Target Domain:              Builtin
          Target Account ID:          S-1-5-32-544
          Caller User Name:           Garuda
          Caller Domain:              RLA01079
          Caller Logon ID:            (0x0,0x2A55)
          Privileges:          -
```

Security Policy Changes



Audit Policy

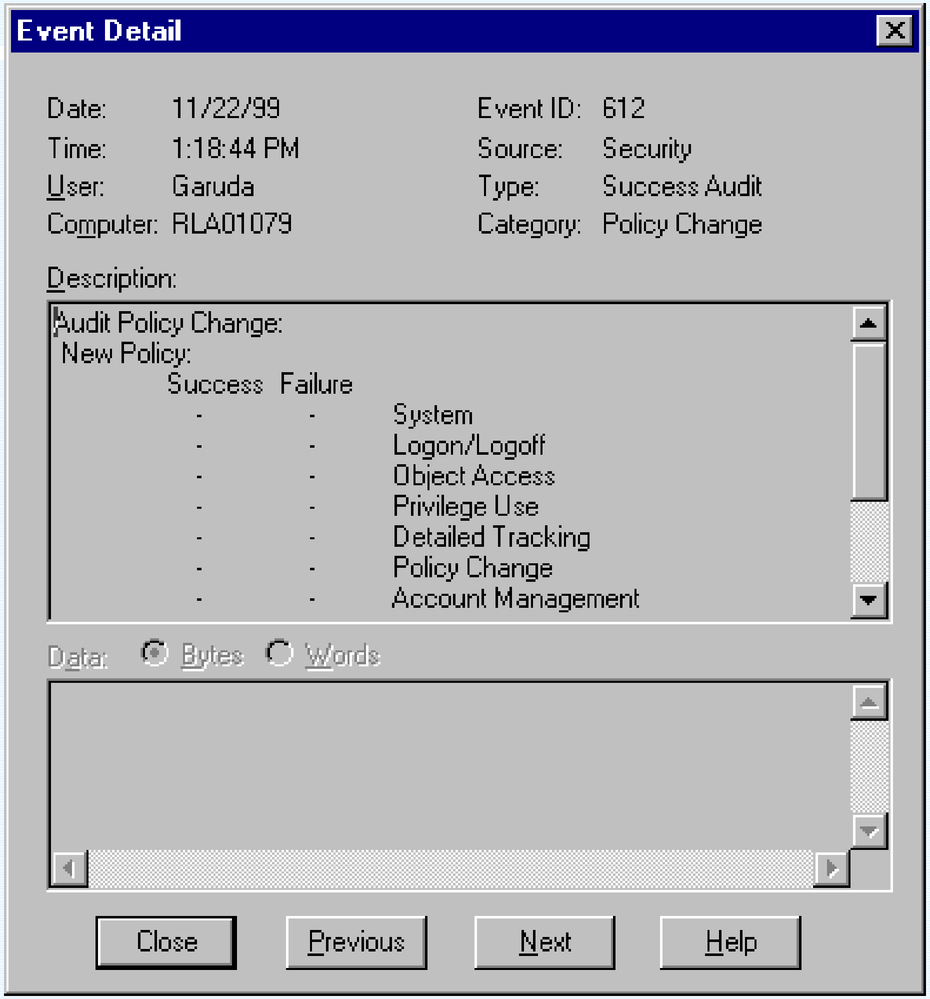
Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

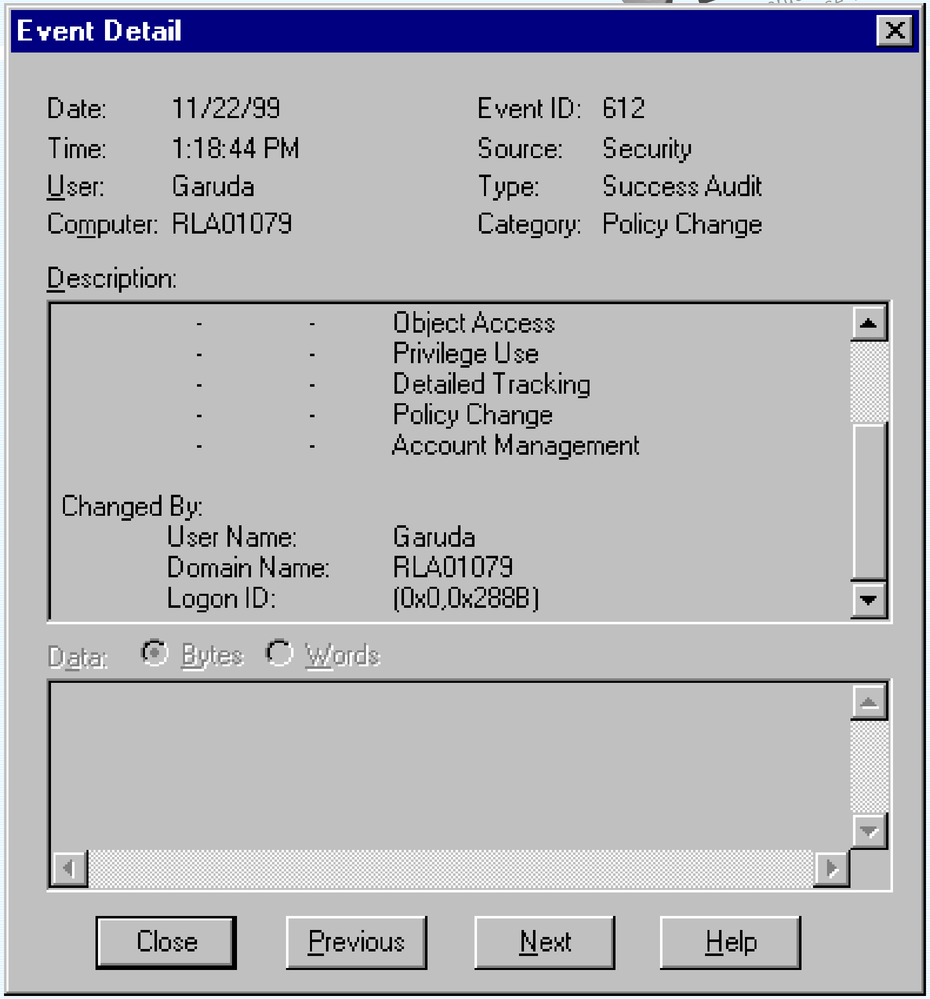
Event Detail - Policy Change



Date: 11/22/99 Event ID: 612
Time: 1:18:44 PM Source: Security
User: Garuda Type: Success Audit
Computer: RLA01079 Category: Policy Change

Description:

```
Audit Policy Change:
 New Policy:
         Success  Failure
            -         -        System
            -         -        Logon/Logoff
            -         -        Object Access
            -         -        Privilege Use
            -         -        Detailed Tracking
            -         -        Policy Change
            -         -        Account Management
```

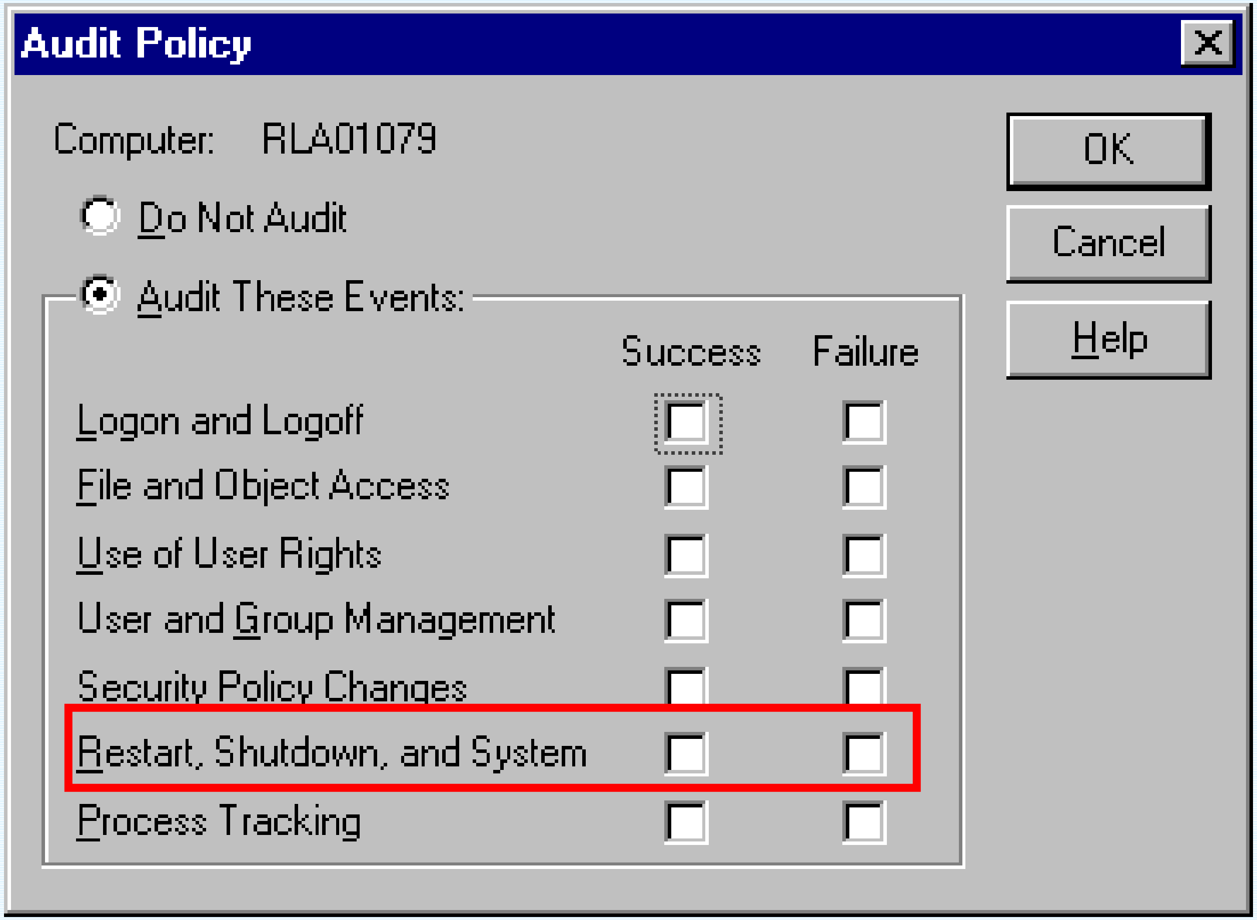


Date: 11/22/99 Event ID: 612
Time: 1:18:44 PM Source: Security
User: Garuda Type: Success Audit
Computer: RLA01079 Category: Policy Change

Description:

```
            -         -        Object Access
            -         -        Privilege Use
            -         -        Detailed Tracking
            -         -        Policy Change
            -         -        Account Management

 Changed By:
         User Name:          Garuda
         Domain Name:        RLA01079
         Logon ID:           (0x0,0x288B)
```

Restart, Shutdown, and System



Audit Policy

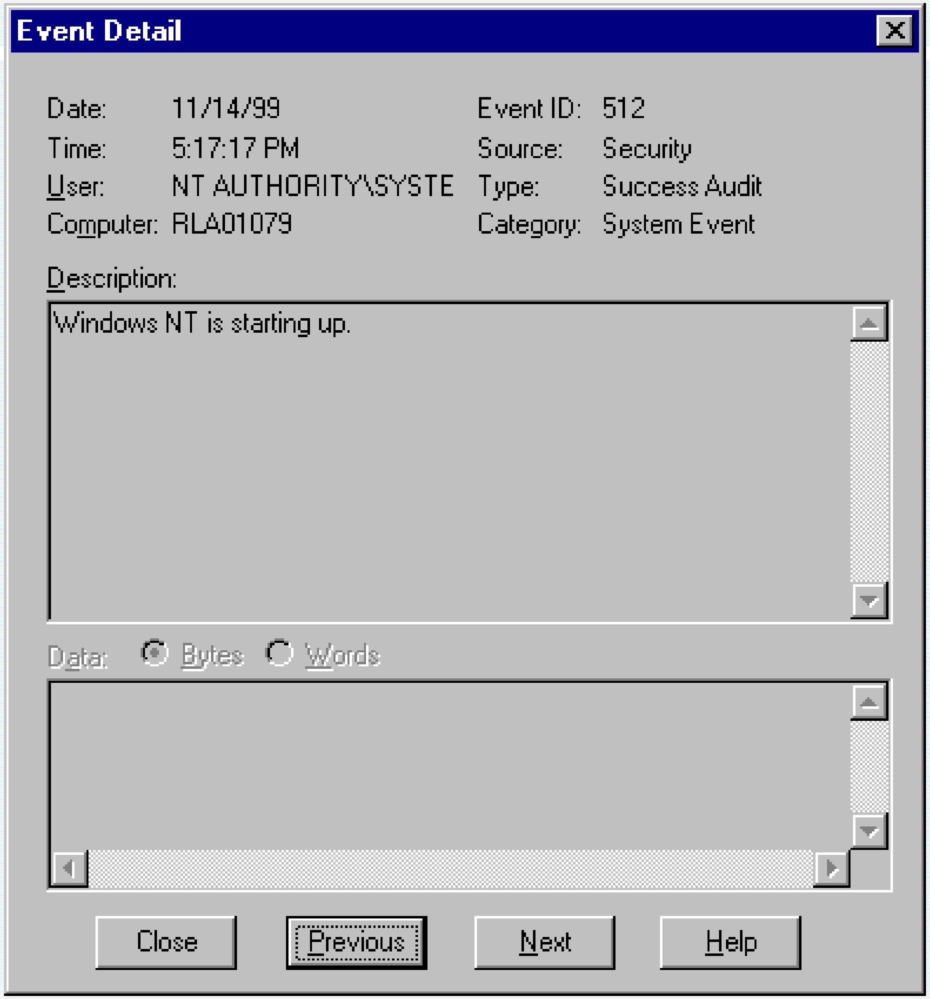
Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

Event Detail: Restart, Shutdown, and System



Date: 11/14/99

Time: 5:17:17 PM

User: NT AUTHORITY\SYSTE

Computer: RLA01079

Event ID: 512

Source: Security

Type: Success Audit

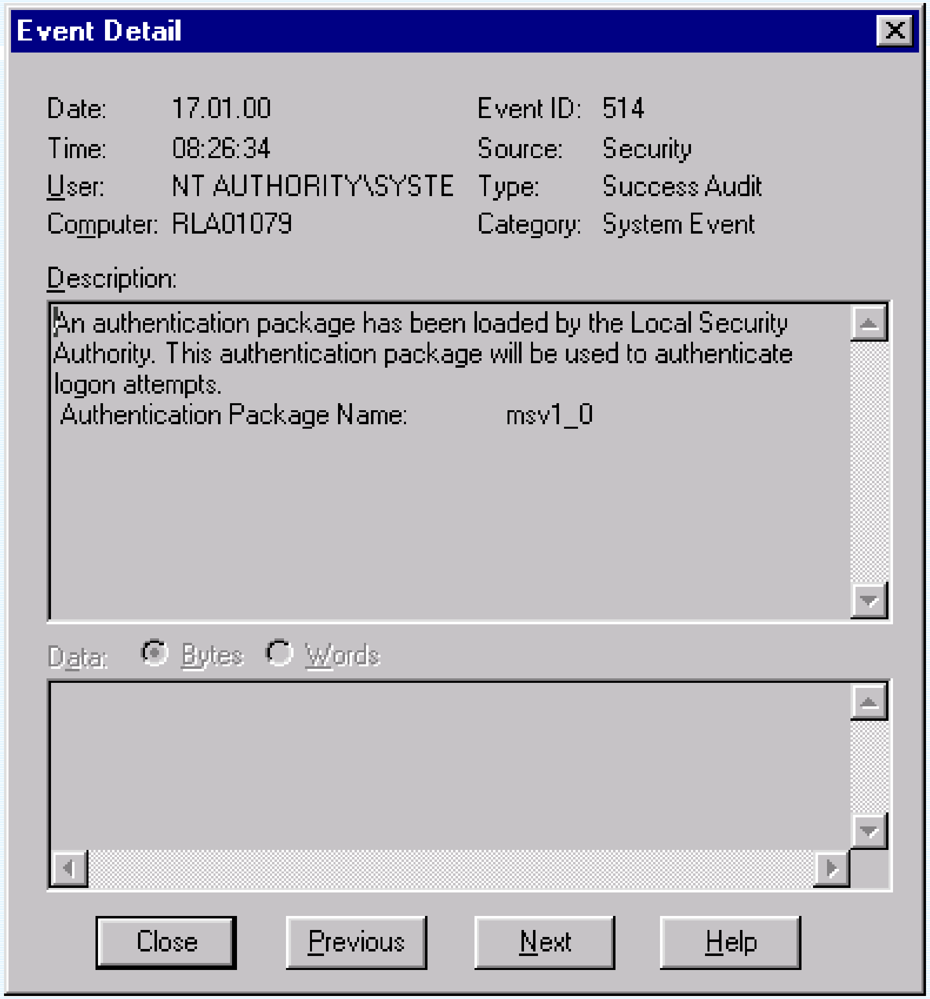
Category: System Event

Description:

Windows NT is starting up.

Data: ● Bytes ○ Words

Starting NT – Authentication and Trusted Logon



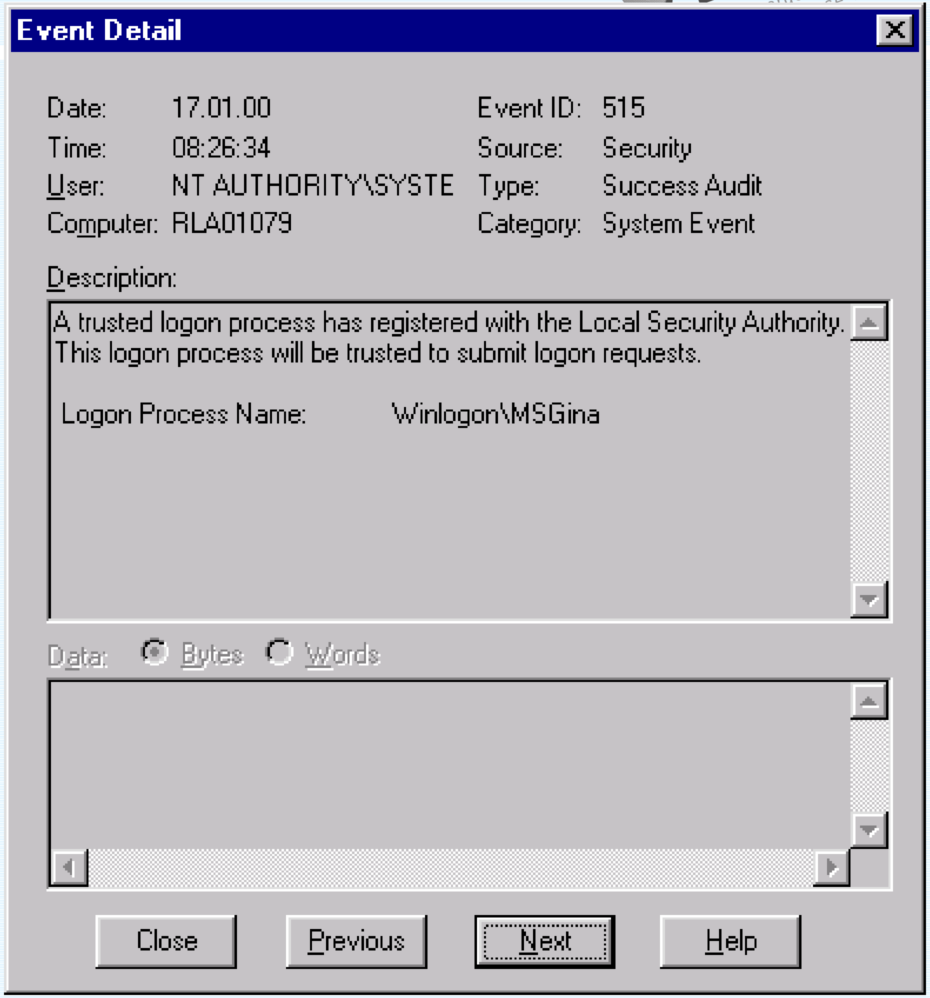
Event Detail

Date: 17.01.00
Time: 08:26:34
User: NT AUTHORITY\SYSTE
Computer: RLA01079

Event ID: 514
Source: Security
Type: Success Audit
Category: System Event

Description:

An authentication package has been loaded by the Local Security Authority. This authentication package will be used to authenticate logon attempts.
Authentication Package Name: msv1_0



Event Detail

Date: 17.01.00
Time: 08:26:34
User: NT AUTHORITY\SYSTE
Computer: RLA01079

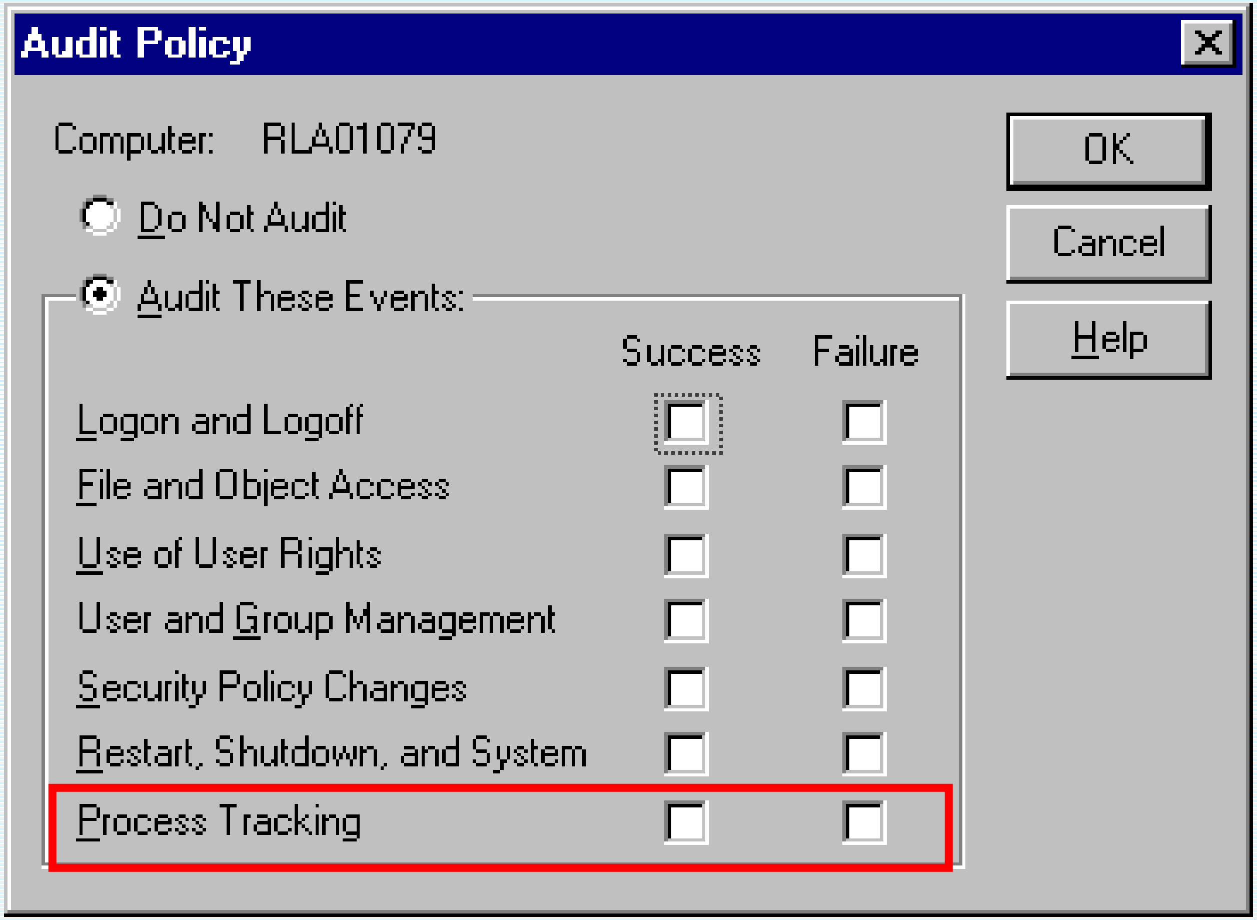
Event ID: 515
Source: Security
Type: Success Audit
Category: System Event

Description:

A trusted logon process has registered with the Local Security Authority. This logon process will be trusted to submit logon requests.

Logon Process Name: Winlogon\MSGina

Process Tracking



Computer: RLA01079

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	□	□
File and Object Access	□	□
Use of User Rights	□	□
User and Group Management	□	□
Security Policy Changes	□	□
Restart, Shutdown, and System	□	□
Process Tracking	□	□

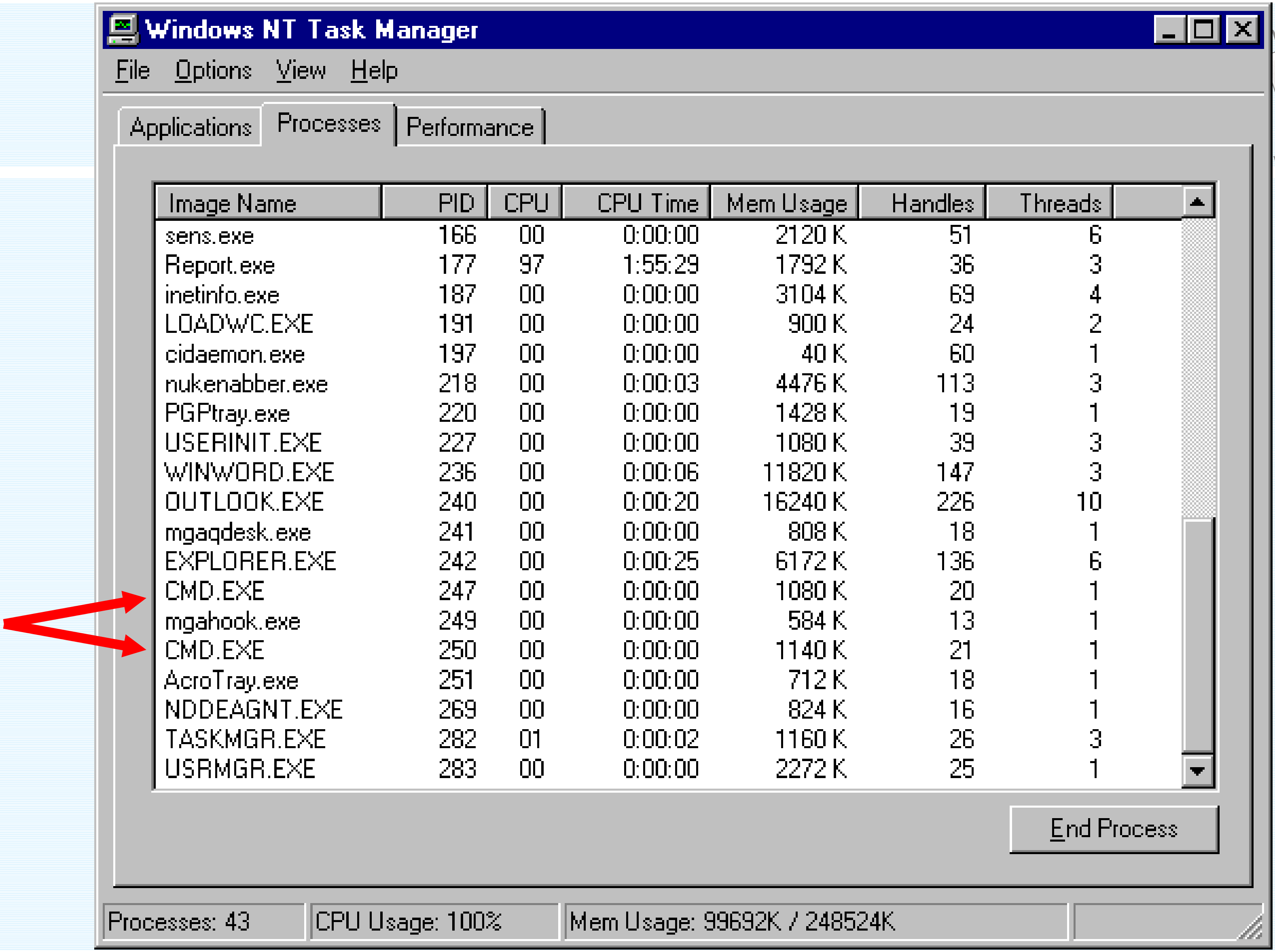
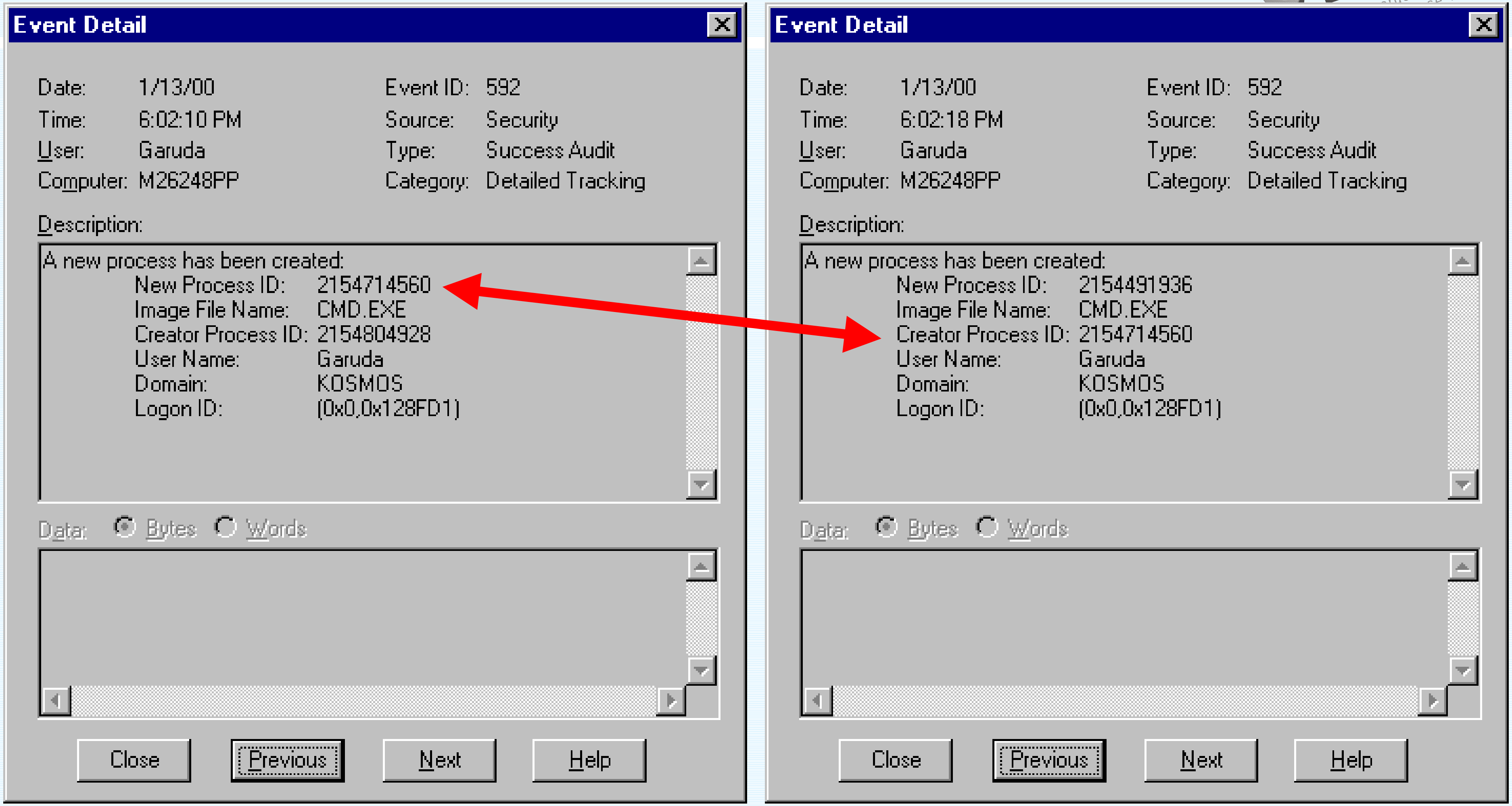


Image Name	PID	CPU	CPU Time	Mem Usage	Handles	Threads
sens.exe	166	00	0:00:00	2120 K	51	6
Report.exe	177	97	1:55:29	1792 K	36	3
inetinfo.exe	187	00	0:00:00	3104 K	69	4
LOADWC.EXE	191	00	0:00:00	900 K	24	2
cidaemon.exe	197	00	0:00:00	40 K	60	1
nukenabber.exe	218	00	0:00:03	4476 K	113	3
PGPtray.exe	220	00	0:00:00	1428 K	19	1
USERINIT.EXE	227	00	0:00:00	1080 K	39	3
WINWORD.EXE	236	00	0:00:06	11820 K	147	3
OUTLOOK.EXE	240	00	0:00:20	16240 K	226	10
mgaqdesk.exe	241	00	0:00:00	808 K	18	1
EXPLORER.EXE	242	00	0:00:25	6172 K	136	6
CMD.EXE	247	00	0:00:00	1080 K	20	1
mgahook.exe	249	00	0:00:00	584 K	13	1
CMD.EXE	250	00	0:00:00	1140 K	21	1
AcroTray.exe	251	00	0:00:00	712 K	18	1
NDDEAGNT.EXE	269	00	0:00:00	824 K	16	1
TASKMGR.EXE	282	01	0:00:02	1160 K	26	3
USRMGR.EXE	283	00	0:00:00	2272 K	25	1

Processes: 43 | CPU Usage: 100% | Mem Usage: 99692K / 248524K

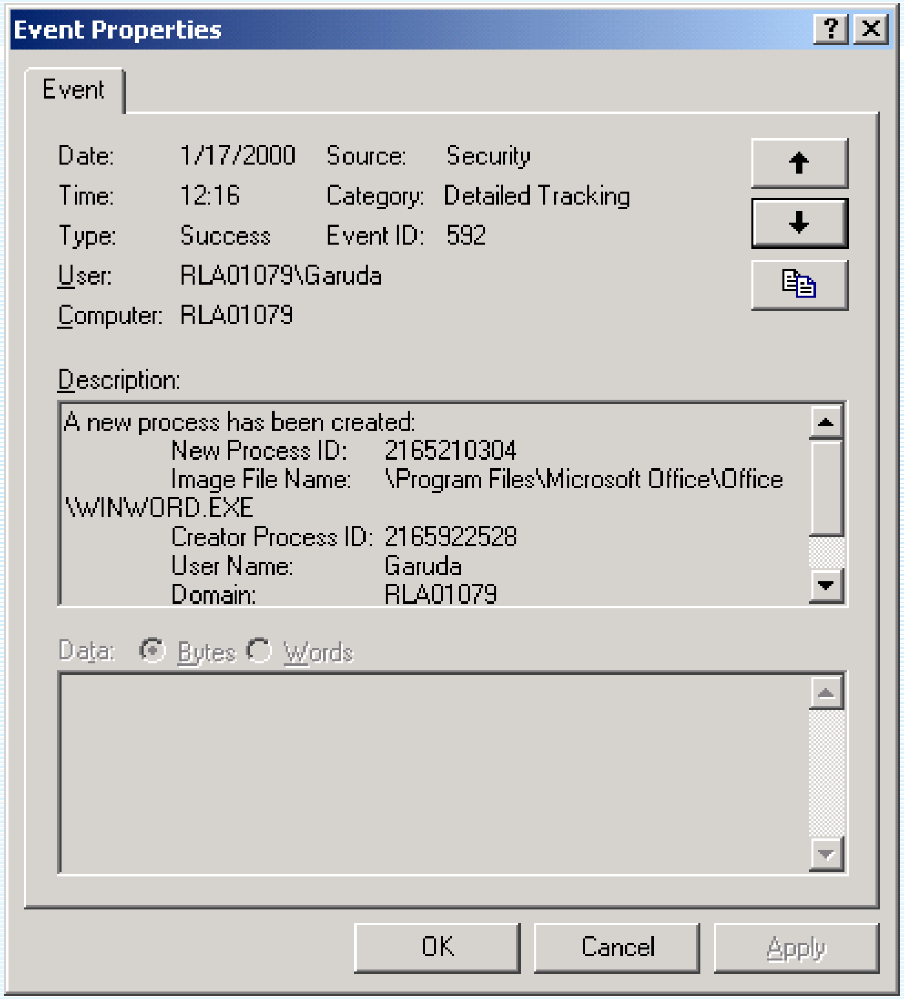
Process IDs II



```
Event Detail

Date:      1/13/00          Event ID:  592
Time:      6:02:10 PM       Source:    Security
User:      Garuda           Type:      Success Audit
Computer:  M26248PP         Category:  Detailed Tracking

Description:
A new process has been created:
        New Process ID:      2154714560
        Image File Name:     CMD.EXE
        Creator Process ID:  2154804928
        User Name:           Garuda
        Domain:              KOSMOS
        Logon ID:            (0x0,0x128FD1)
```

```
Event Detail

Date:      1/13/00          Event ID:  592
Time:      6:02:18 PM       Source:    Security
User:      Garuda           Type:      Success Audit
Computer:  M26248PP         Category:  Detailed Tracking

Description:
A new process has been created:
        New Process ID:      2154491936
        Image File Name:     CMD.EXE
        Creator Process ID:  2154714560
        User Name:           Garuda
        Domain:              KOSMOS
        Logon ID:            (0x0,0x128FD1)
```

Process IDs III – Windows 2000



Date: 1/17/2000 Source: Security
Time: 12:16 Category: Detailed Tracking
Type: Success Event ID: 592
User: RLA01079\Garuda
Computer: RLA01079

Description:

A new process has been created:
New Process ID: 2165210304
Image File Name: \Program Files\Microsoft Office\Office\WINWORD.EXE
Creator Process ID: 2165922528
User Name: Garuda
Domain: RLA01079

Data: ● Bytes ○ Words

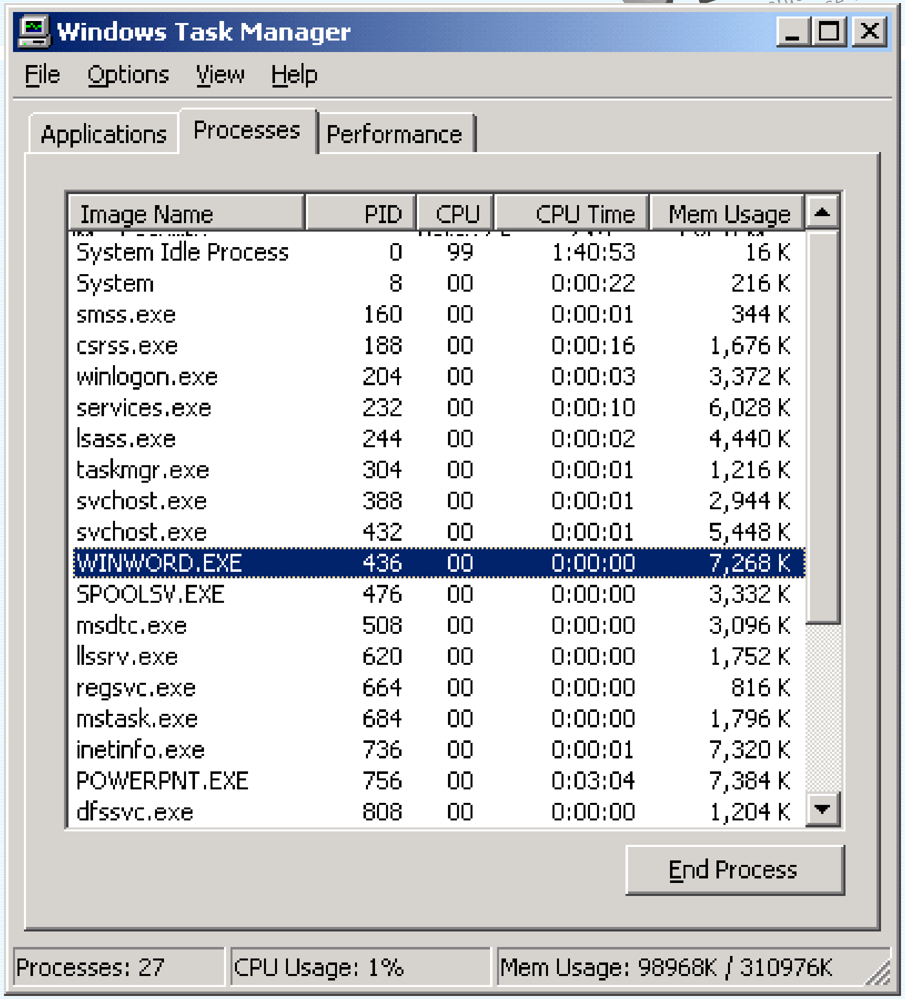
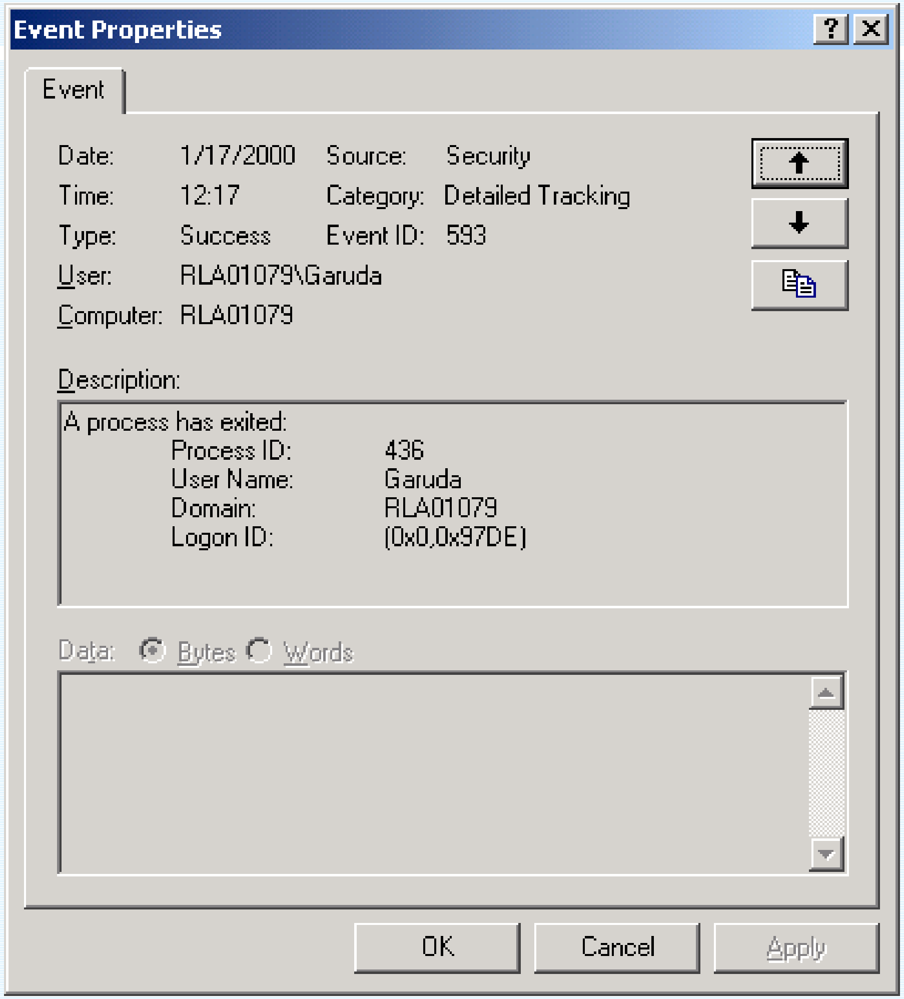


Image Name	PID	CPU	CPU Time	Mem Usage
System Idle Process	0	99	1:40:53	16 K
System	8	00	0:00:22	216 K
smss.exe	160	00	0:00:01	344 K
csrss.exe	188	00	0:00:16	1,676 K
winlogon.exe	204	00	0:00:03	3,372 K
services.exe	232	00	0:00:10	6,028 K
lsass.exe	244	00	0:00:02	4,440 K
taskmgr.exe	304	00	0:00:01	1,216 K
svchost.exe	388	00	0:00:01	2,944 K
svchost.exe	432	00	0:00:01	5,448 K
WINWORD.EXE	436	00	0:00:00	7,268 K
SPOOLSV.EXE	476	00	0:00:00	3,332 K
msdtc.exe	508	00	0:00:00	3,096 K
llssrv.exe	620	00	0:00:00	1,752 K
regsvc.exe	664	00	0:00:00	816 K
mstask.exe	684	00	0:00:00	1,796 K
inetinfo.exe	736	00	0:00:01	7,320 K
POWERPNT.EXE	756	00	0:03:04	7,384 K
dfssvc.exe	808	00	0:00:00	1,204 K

Processes: 27 CPU Usage: 1% Mem Usage: 98968K / 310976K

Process IDs IV – Windows 2000



Date: 1/17/2000 Source: Security
Time: 12:17 Category: Detailed Tracking
Type: Success Event ID: 593
User: RLA01079\Garuda
Computer: RLA01079

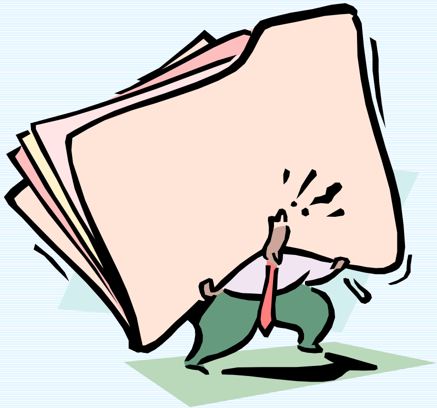
Description:

```
A process has exited:
          Process ID:          436
          User Name:           Garuda
          Domain:              RLA01079
          Logon ID:            (0x0,0x97DE)
```

One Click - Many Security Events

Audit Logs for a new user account:

- Event 632: Global Group Member Added
- Event 624: User Account Created
- Event 642: User Account Changed
- Event 636: Local Group Member Added



Additional Auditing settings

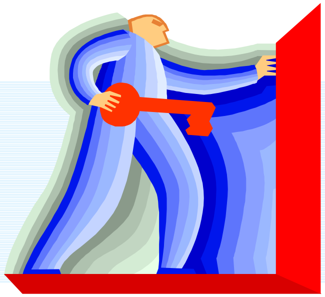
- Auditing Backup and Restore Activities
  Key: HKLM\System\CCS\Control\Lsa\
  Data: FullPrivilegeAuditing
  Type: REG_BINARY
  Value: 1
- Base Object Auditing
  Key: HKLM\System\CCS\Control\Lsa\
  Data: AuditBaseObjects
  Type: REG_DWORD
  Value: 1

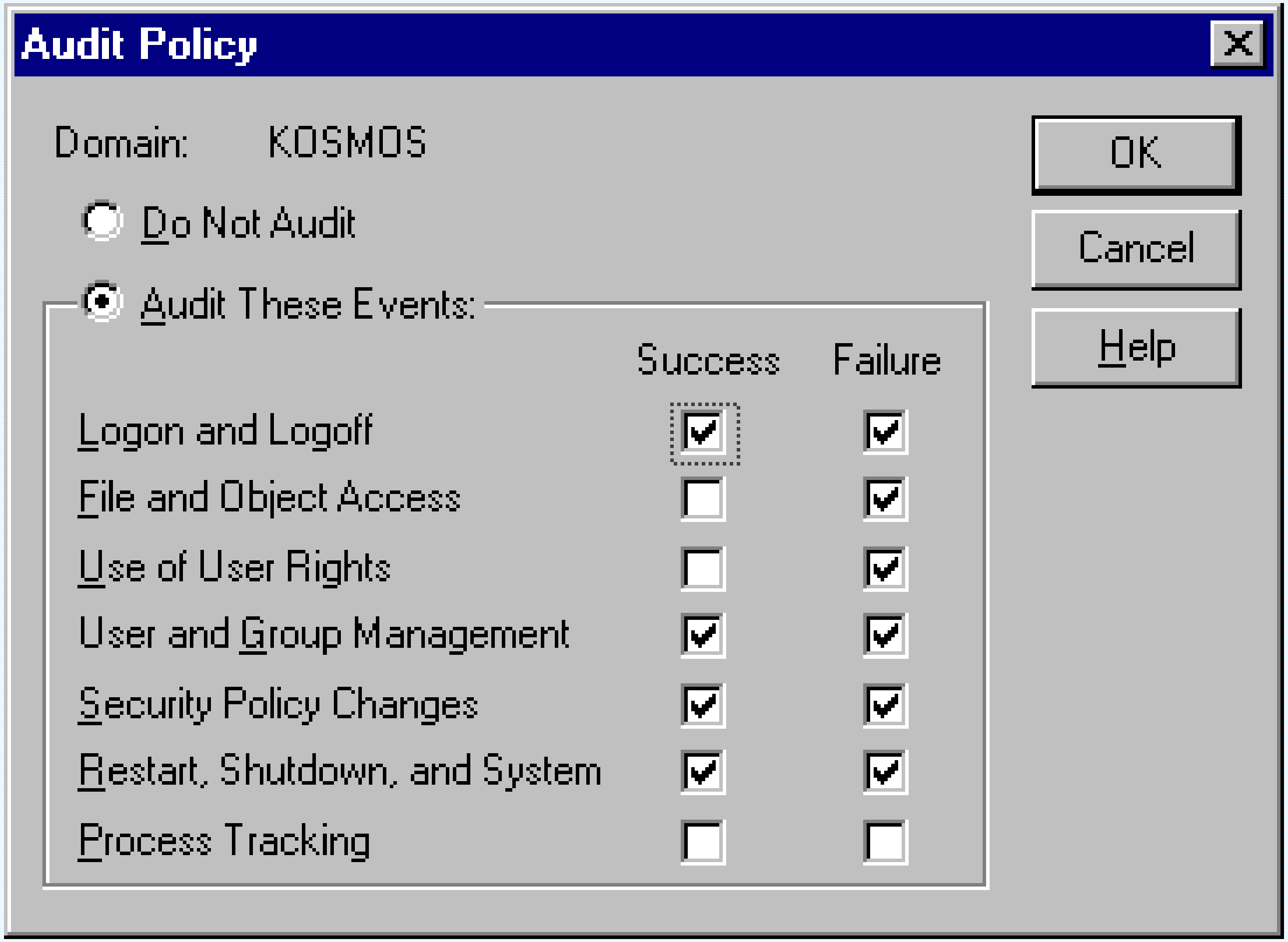
“Account Lockout Event” stored on PDC

- Windows NT 4.0 SP4+

  When a user enters too many incorrect passwords in an attempt to log on to a domain, the account is locked out and an event is written to the workstations security logs (if auditing is enabled here). With SP4 this event is also written to the PDC security log.

Audit Policy





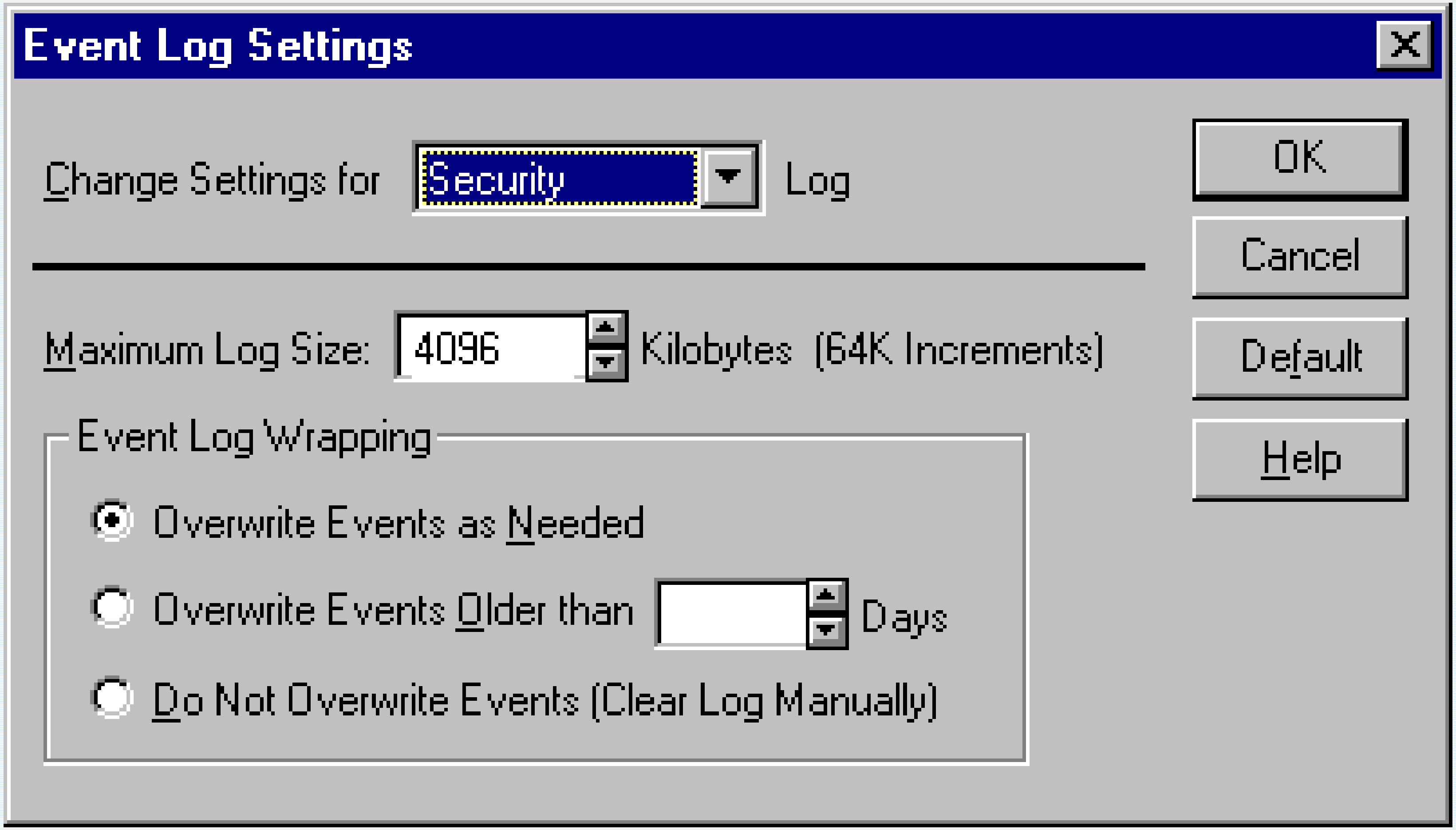
Domain: KOSMOS

○ Do Not Audit

● Audit These Events:

	Success	Failure
Logon and Logoff	☑	☑
File and Object Access	□	☑
Use of User Rights	□	☑
User and Group Management	☑	☑
Security Policy Changes	☑	☑
Restart, Shutdown, and System	☑	☑
Process Tracking	□	□

Event Log Settings



Event Log Settings

Change Settings for Security Log

Maximum Log Size: 4096 Kilobytes (64K Increments)

Event Log Wrapping

● Overwrite Events as Needed

○ Overwrite Events Older than Days

○ Do Not Overwrite Events (Clear Log Manually)

Lesson learnt

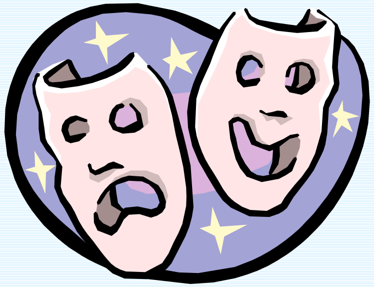
- You can get a lot of information from the logs
- Not all infomation is relevant
- Some information is wrong
- You can‘t get too much information about logging from MS

Filter Suspicious Events from all Events

Event IDs

- 512 - Windows NT is starting up
- 513 - Windows NT is shutting down
- 517 - The audit log was cleared
- 528 - Successful logon
- **529 - Unknown user name or bad password**
- 530 – Account logon time restriction violation
- 531 - Account currently disabled
- 532 - The specified user account has expired
- 533 - User not allowed to log on at this computer
- 534 – User has not been granted the requested logon type
- 535 - The specified account‘s password has expired
- 536 – The NetLogon component is not active
- 537 – An unexpected error occured during logon
- 538 – User Log off
- 539 - Account locked out
- 576 - Special privileges assigned to new logon
- 608 - User Right Assigned
- 609 - User Right Removed
- 612 - Audit Policy Change
- 624 - User Account Created
- 643 - Domain Policy Changed

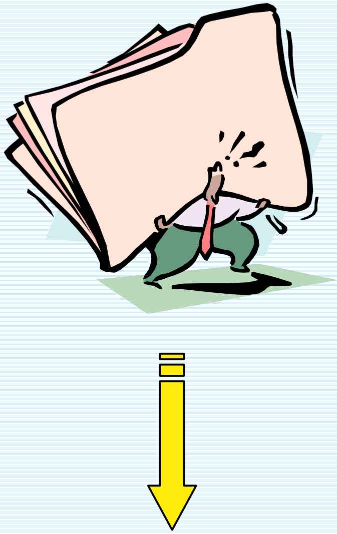
Suspicious Auditing Events

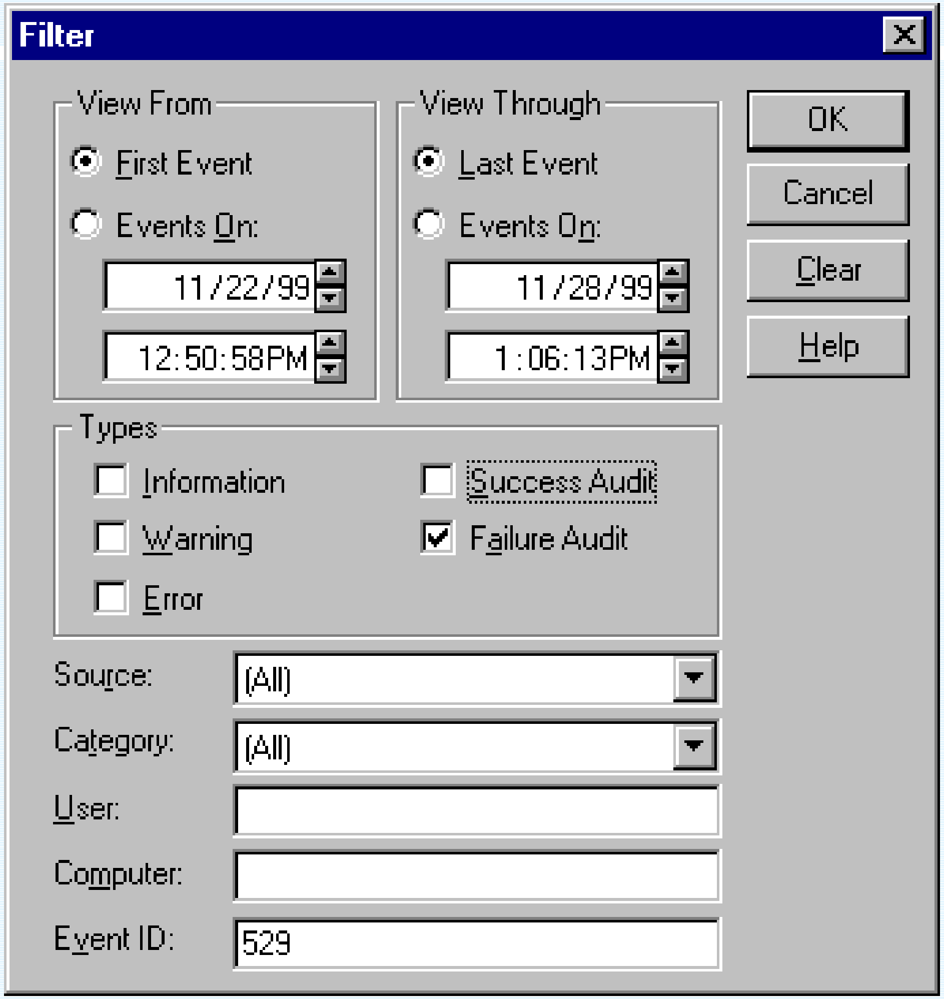


- Failed Logon
  Event ID – 529

Administrator and
„Well Known Accounts“

Filter Suspicious Events from all Events





Filter

View From
● First Event
○ Events On:
11/22/99
12:50:58PM

View Through
● Last Event
○ Events On:
11/28/99
1:06:13PM

Types
□ Information
□ Warning
□ Error
□ Success Audit
☑ Failure Audit

Source: (All)
Category: (All)
User:
Computer:
Event ID: 529

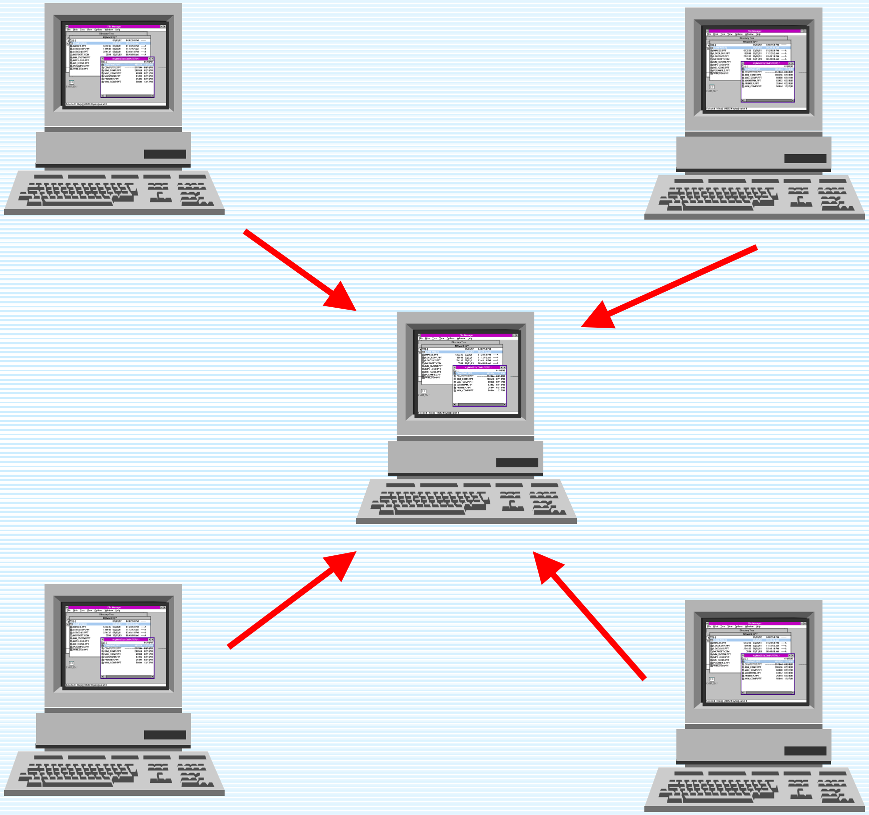
Deficiencies of NT Logging

- Portscans can not be detected
  - BOF – Back Officer Friendly (NFR)
    http://www.nfr.com
  - Nuke Nabber 2.9a (Dynamsol)
    http://www.dynamsol.com/puppet/
  - NetMonitor v0.90 (LeechSoftware)
    http://www.leechsoftware.com
  - BlackICE
    http://advide.networkice.com
- Workstation logs are kept locally
  - See next slide

Logging Host

- EvntSLog 2.0
- NTSlog 1.02, 2.0
- NTOLog

- Siemens CERT



ZT IK 3, Siemens CERT

Further Tools

- Lservers (NT Objectives, Inc.)
- NPList (NT Objectives, Inc.)
- WDumpEvt 1.2
- ELDump 0.12
- ELSaveClr
- NTLast
- Tripwire 2.1 for Windows NT

Literature etc.

- MS Knowledgebase:
  Q174073, Auditing User Authentication
  Q174074, Security Event Descriptions
  Q163905, Auditing User Right Assignment Changes
  Q101366, Definition and List of Windows NT Advanced User Rights
  et al.
  found at http://support.microsoft.com/support/search/c.asp
- Books etc.:
  Microsoft – Windows NT 4.0 Security, Audit and Control
  Microsoft Press – Microsoft Technical ReferenceWindo
  Windows NT Server Resource Kit 4.0
  Visual C++: winnt.h