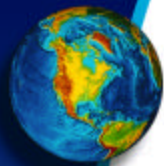


Information Systems Audit & Control Association

Windows 2000/Active Directory Security

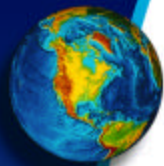
***Presented by: Deloitte & Touche
Raj Mehta – CPA, CITP, CISA, CISSP
Denis Tiouttchev – CIA, CISA, CISSP***

August 21, 2003



Focus

- ◆ Introduction to Windows 2000 and Active Directory
- ◆ Organizational Unit (OU) Concept
- ◆ Group Policy Objects (GPOs)
- ◆ Windows 2000 Groups
- ◆ File System
- ◆ File Permissions / Access Control Lists
- ◆ Registry Permissions
- ◆ Security Templates
- ◆ Rights
- ◆ Demo
- ◆ Audit Checklist

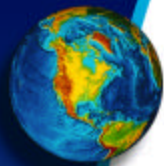


Introduction to Windows 2000

Windows 2000 is essentially Windows NT 5.0

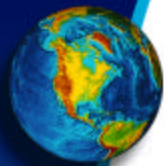
Contains many new security features

- ◆ Active Directory
- ◆ Kerberos Authentication Protocol
- ◆ Encrypting File System
- ◆ IPSec, PKI, & Smartcards



NT versus Win2K (AD)

| NT | Windows 2000 |
|---|---|
| PDC & BDC | Domain Controllers w/Active Directory |
| NTLM Authentication (Weaker Form) | Kerberos (Stronger Authentication) |
| No native file encryption utility | Encrypting File System (EFS) |
| PPTP | IPSec |
| N/A | PKI, Smartcards |
| File System (Share & NTFS Permissions) | Same |
| Trusts Among Domains need to be defined | Automatic two-way trust between Win2K domains and Forests |
| System Policies | Centralized configuration through GPOs |
| N/A | Custom Permissions and Delegation of Authority |
| Syskey not automatically enabled | Syskey automatically enabled |

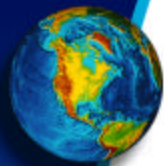


Introduction to Active Directory

Active Directory (AD) is Windows 2000's directory service and is accessed through Lightweight Directory Access Protocol (LDAP).

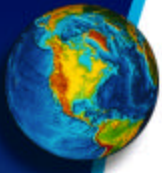
AD is the core policy & configuration repository for each component of Windows 2000 providing most importantly:

- ◆ **Centralized** security configuration of all computers in the domain via **Group Policy Objects**
 - ◆ Local account, lockout and audit policy
 - ◆ Services
 - ◆ File, Registry, & Printer Permissions
 - ◆ User Rights
 - ◆ Event Log Settings



What does AD provide?

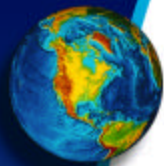
- ◆ Single Sign-on User Database
 - ◆ Windows 2000
 - ◆ Exchange & Lotus Notes
 - ◆ SQL Server
 - ◆ ERP (SAP, Oracle, PeopleSoft)
- ◆ Granular delegation of administrative authority
- ◆ Centralized security configuration of all users and computers in the domain.
 - ◆ Local Account, lockout and audit policy
 - ◆ Services
 - ◆ Registry Permissions
 - ◆ Printer Permissions
 - ◆ User Rights
 - ◆ Event Log settings



AD Concepts

Computers, users, groups, printers, shared file server directories, etc. are organized and controlled according to the enterprise's organizational hierarchy, which are represented through a number of container objects:

- ◆ **Domains** – fundamental container in Active Directory that can hold all of the users, computers, etc for an entire organization
- ◆ **Organizational Units (OU)** – used to subdivide objects within a domain that typically correspond to a division, department, region, etc.
- ◆ **Trees** – used in multiple domain environments to facilitate contiguous DNS name space & automatic trust relationships between domains
- ◆ **Forests** – used in multiple domain environment that do **not** share a contiguous DNS name space
- ◆ **Sites** – used to organize computers based on physical location to efficiently utilize network bandwidth between sites

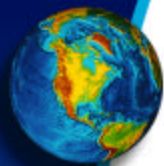


OU Considerations

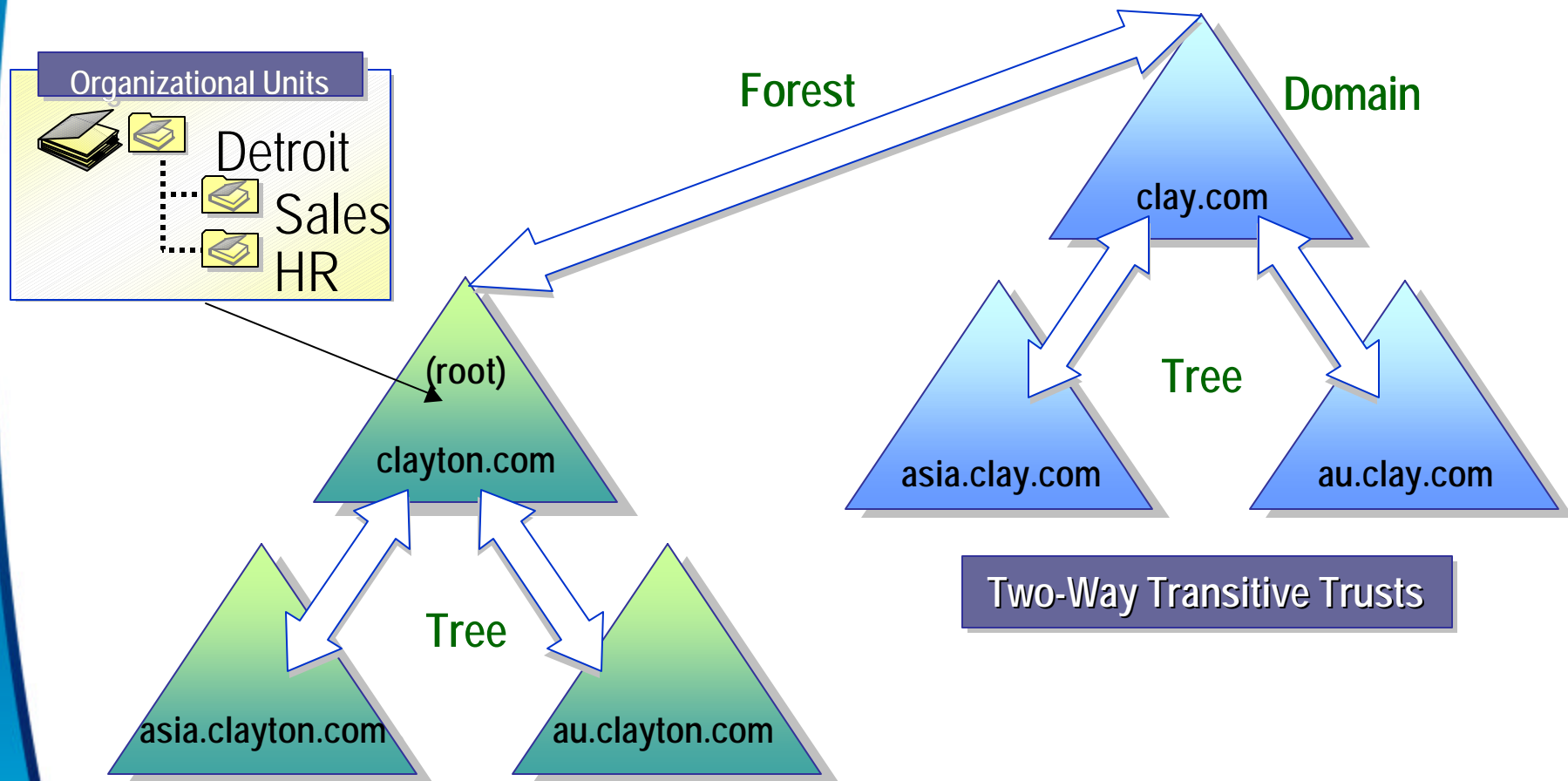
How OU structure is designed is critical in terms of how the AD will be administered. It's very easy to make this a complicated process.

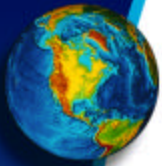
Factors to consider when creating OUs:

- ◆ How objects will be administered – centralized versus decentralized (e.g., HR OU)
- ◆ What type of GPOs will be enforced: User Level (General Users versus Special Users); Machines (Workstation versus Servers)
- ◆ How information needs to be organized

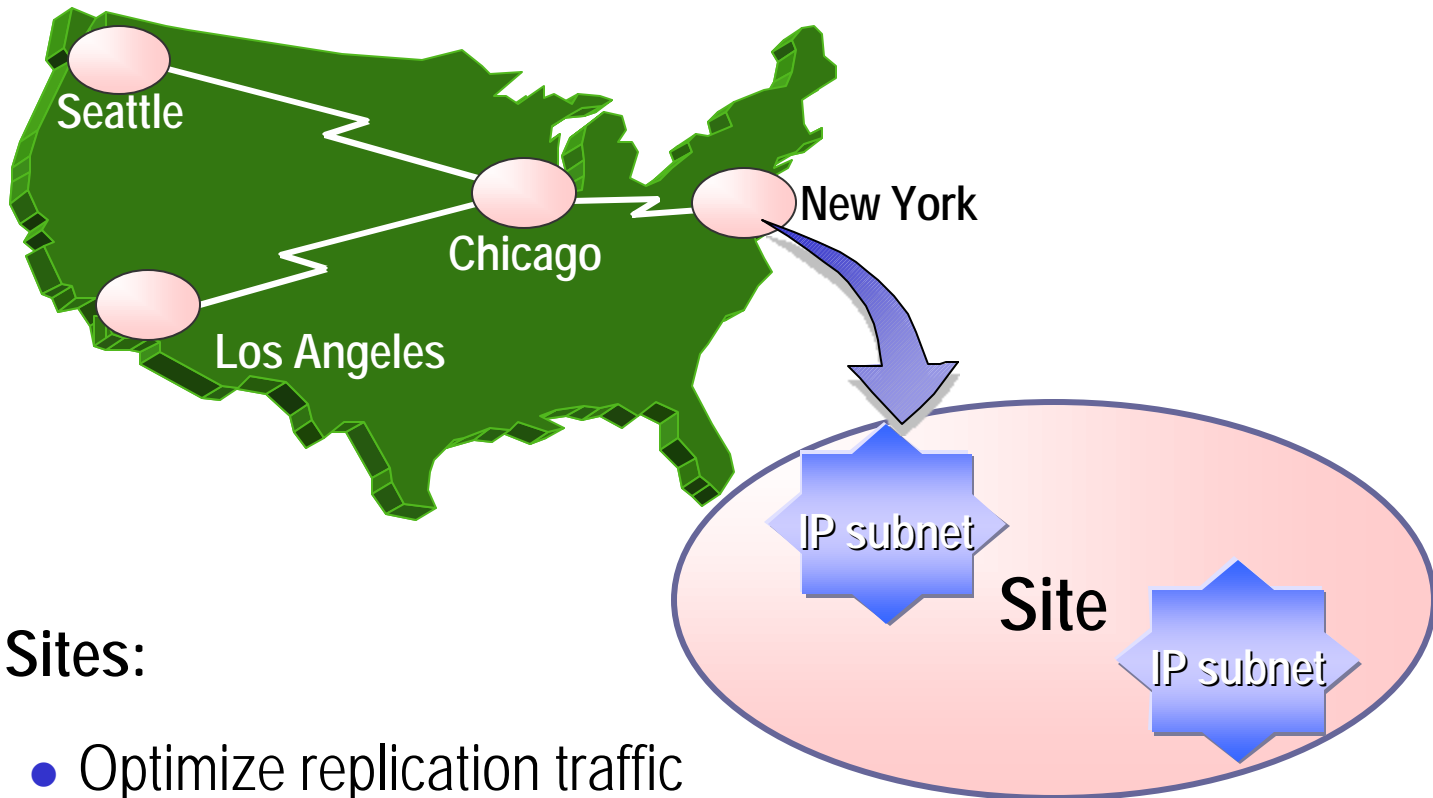


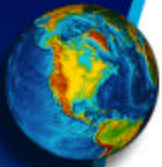
AD Concepts (con't)





AD Concepts (con't)

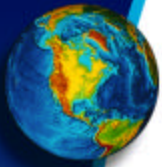




Group Policy Objects

Group Policy Object (GPO) - the avenue for central security configuration within Windows 2000 and Active Directory

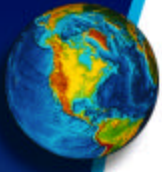
- ◆ GPOs provide a way to manage all of the configuration changes and policy settings utilizing the hierarchy of Active Directory
- ◆ GPOs can be applied to Users and Computers within an OU (e.g. map drives, screen savers, etc.), but can not be applied to Groups within an OU
- ◆ GPO Application Order: L(Local). S(Site). D (Domain). OU(Organizational Unit)
- ◆ If multiple conflicting GPOs within same level, last GPO wins!
- ◆ You can block inheritance from top level GPOs
- ◆ GPO can be defined or undefined



Group Policy Objects (cont.)

- ◆ Example of Computer Configurations:
 - ◆ Account Policies (Password & Account Lockout Policy) – Defined only Once at Domain Level)
 - ◆ Audit Policy
 - ◆ User Rights Assignment
 - ◆ Security Options (e.g., do not display last user name in logon screen)
 - ◆ Setting for Event Logs

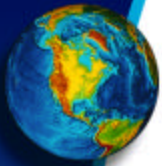
- ◆ Example of User Configurations:
 - ◆ Remove Control Panel Access
 - ◆ Remove Run command Access
 - ◆ Internet Explorer Options
 - ◆ Screen Saver Options



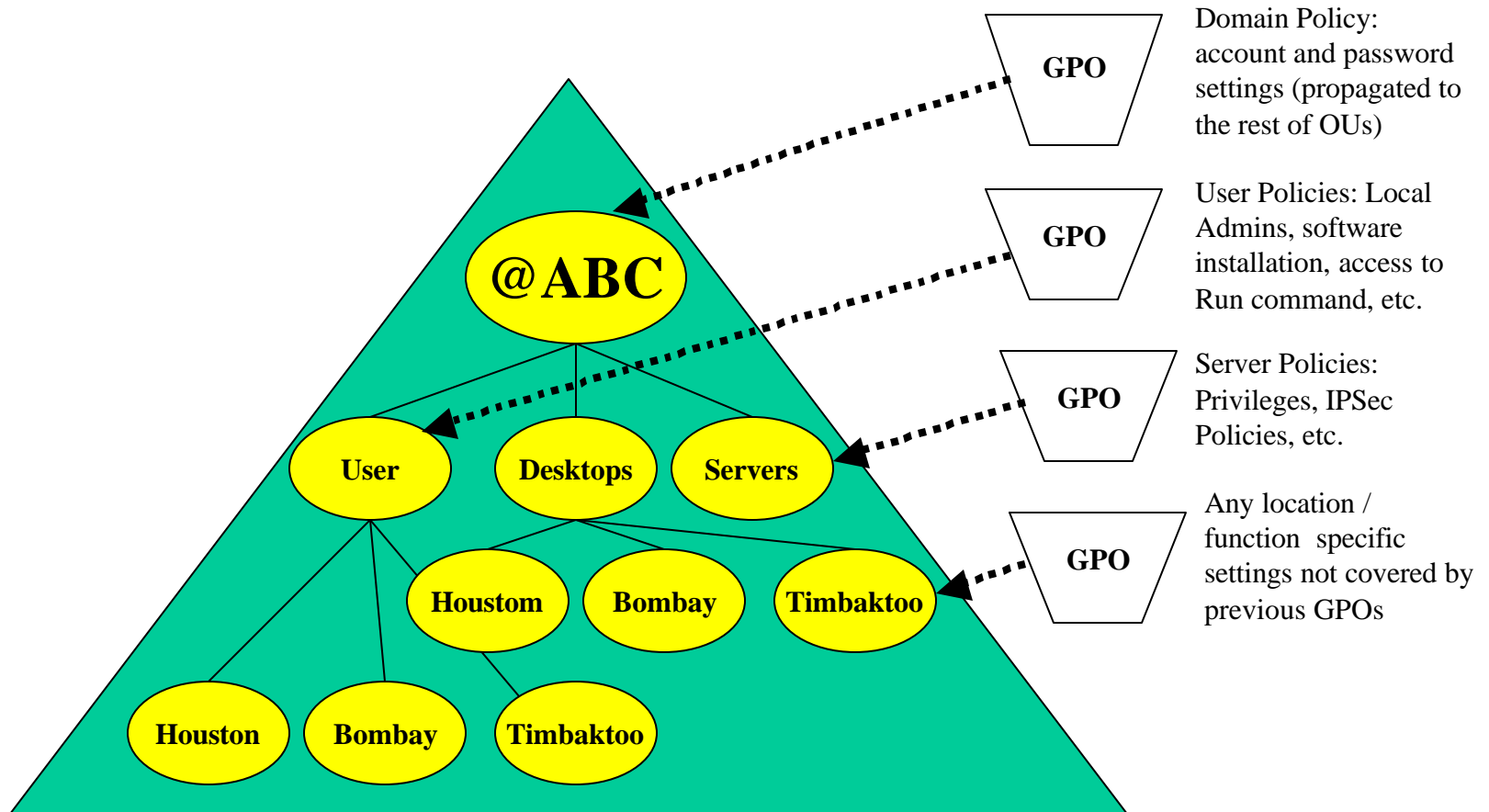
GPO (cont.)

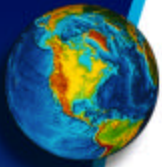
- ◆ Domain Level GPO says -> Enable Start Menu
- ◆ OU Level says -> Disable Start Menu
- ◆ Local Workstation says -> Enable Start Menu

What is the result when the user signs-on to the workstation?



GPOs

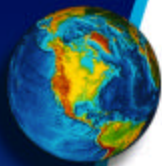




Key Groups

Prior to delegation, check memberships to the following built-in groups:

- ◆ **Member Server/Workstation – Administrator**
- ◆ **Domain Level – Administrators, Domain Admins, Account Operators, Server Operators, Backup Operators, Print Operators, DNSAdmins**
- ◆ **Each Forest – Enterprise Admins, Schema Admins**

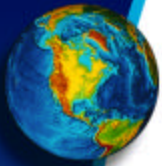


Groups (cont.)

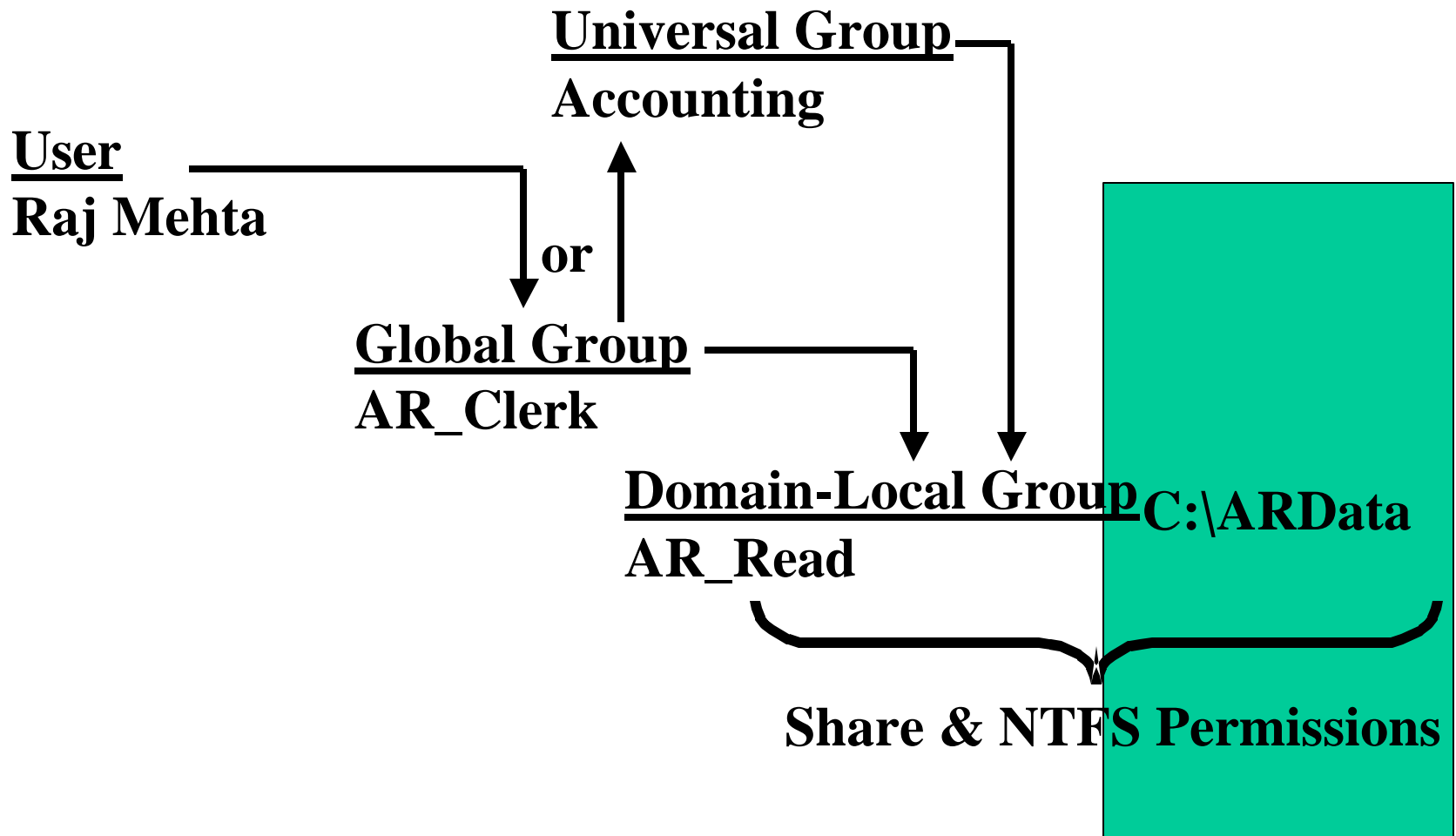
Group Types: Security versus Distribution Groups

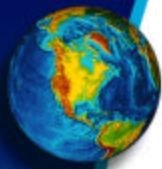
Group Categories for Security Groups:

| Group | Can Contain | Permissions Granted |
|--|--|-------------------------------|
| Universal (Defined at AD) | Users, Global Groups, Universal Groups (any domain in the forest) | Anywhere in the forest |
| Global (Defined at AD) | Users, other Global Groups (from same domain) | Anywhere in the forest |
| Domain Local (Defined at AD) – only on DC | Users, Global Groups, Universal Groups, and Domain Local (from same domain) | Within same domain |



Groups (cont.)

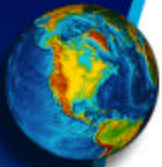




File System

File Systems – how info is stored on a hard drive

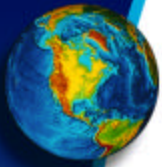
- ◆ NT File System (NTFS)
 - ◆ Security attributes that can be applied to a file or folder via ACLs
 - ◆ Higher performance
 - ◆ Encryption File System
- ◆ File Allocation Table (FAT)
 - ◆ Can't use Encryption or Security
 - ◆ Very Insecure
 - ◆ DOS/WIN95 compatible
- ◆ Typically, Network Administrators have a misperception that FAT file are “Easier to Recover”
- ◆ Issue – Anyone can boot to the server with a Windows 98 startup disk within the Server Driver and gain access to the SAM file



ACL (Access Control Lists)

Access Control List / Permissions –controls access to objects and defines what actions a specific user can perform on a specific object.

- ◆ Files and Folders
 - ◆ Only available on NTFS volumes and administered within the Security tab after right clicking an associated file or folder
- ◆ Printers
 - ◆ Each printer has an ACL accessible through Control Panel/printers that controls access to the printer and the print jobs within the queue
- ◆ Directory Objects
 - ◆ Users, groups, and computers each have an ACL that control who can read properties of the object and perform updates
- ◆ Registry Keys
 - ◆ Access to the registry is managed through the Registry Editor
 - ◆ Similar to folder permissions but different structure (e.g. keys, subkeys, etc.)

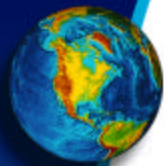


ACL (Access Control Lists)

General Rules:

- ◆ Explicit permissions overrides inherited permissions
- ◆ Deny permission always wins over Allow permissions within same category
- ◆ ACL permissions gained through group membership are cumulative
- ◆ Missing Permissions versus Blank Permissions

NTFS versus Share Permissions



ACL (cont.)

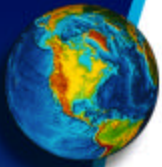
What is John's Access if John is member of Managers?

File Level:

Allow – Finance Clerks – Read
Allow – Managers – Full Control
Allow – Everyone - Modify

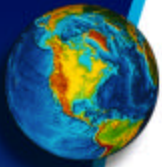
Share Level:

Allow – Everyone - Read



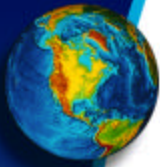
Registry Permissions

- ◆ Access to Registry (security database)
 - ◆ System configuration
 - ◆ Application settings
 - ◆ User preferences and profile settings
 - ◆ Security
 - ◆ Local Users and Groups
 - ◆ Local password, lockout and audit policy
- ◆ The registry attempts to unify and give structure to all configuration data
- ◆ Contains crucial security and system related information, therefore access to the registry should be limited
- ◆ The registry is updated through:
 - ◆ Control Panel
 - ◆ Group Policies
 - ◆ Application setup programs
 - ◆ Registry Editor



Security Templates

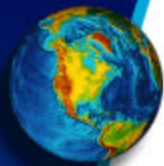
- ◆ Security Configuration and Analysis Tool
- ◆ Security Templates:
 - ◆ C:\Winnt\security\templates
 - ◆ Basicdc.inf
 - ◆ Basicsv.inf
 - ◆ Basicwk.inf
 - ◆ Hisecdc.inf
 - ◆ Hisecwk.inf



Rights

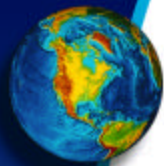
Rights – govern who can use the system and perform specific system management functions

- ◆ Rights do not apply to specific objects
- ◆ Assigned with the “User Rights Assignment” section of the Local Policies within AD
- ◆ Medium - High Risk User Rights:
 - ◆ Act as part of operating system
 - ◆ Backup files and directories
 - ◆ Restore files and directories
 - ◆ Create a token object
 - ◆ Debug programs
 - ◆ Manage auditing and security log
 - ◆ Take ownership of files or other objects
 - ◆ Enable computer and user accounts to be trusted for delegation
 - ◆ Load and unload devices
 - ◆ Shut down the system
 - ◆ Add workstations to domain
 - ◆ Access this computer from the network
 - ◆ Change the system time
 - ◆ Force shutdown from a remote system
 - ◆ Log on as a batch job
 - ◆ Log on as a service
 - ◆ Log on locally

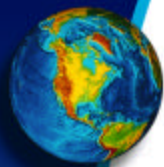


Questions & Answers

DEMO

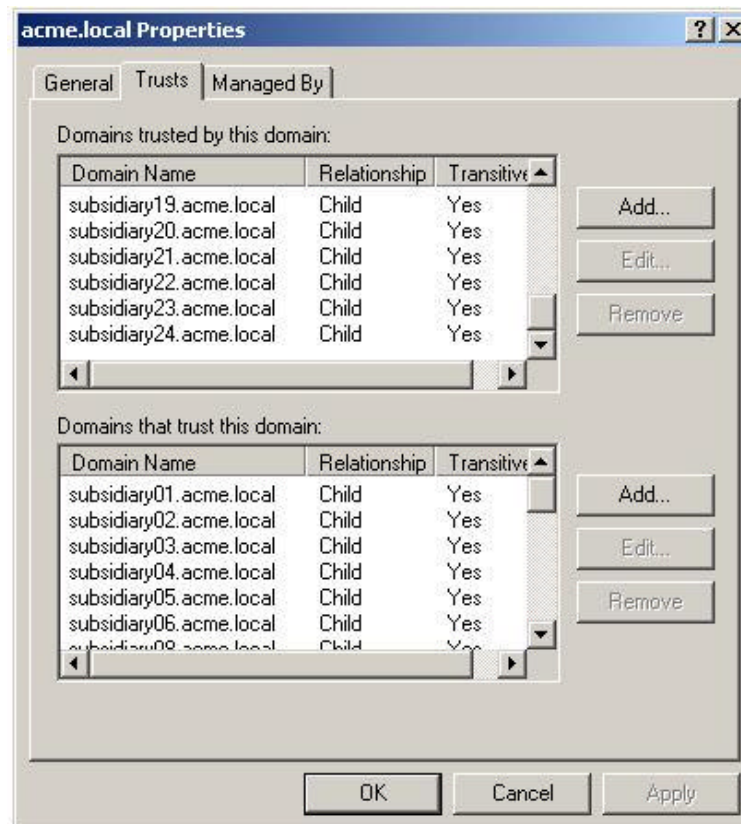


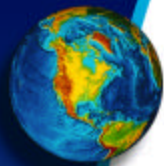
AUDIT CHECKLIST



Audit Checklist

- 1) **DOMAINS, FORESTS, & TRUSTS** – Assess the Domain & Trust structure with a focus on the appropriateness of externally (outside forest) trusted domains. Also, review the physical access of the Domain Controllers & Servers.
 - ◆ Where? – Start, Programs, Administrative Tools, Active Directory Domains & Trusts, right click on the Domain, select Properties, then the Trusts tab

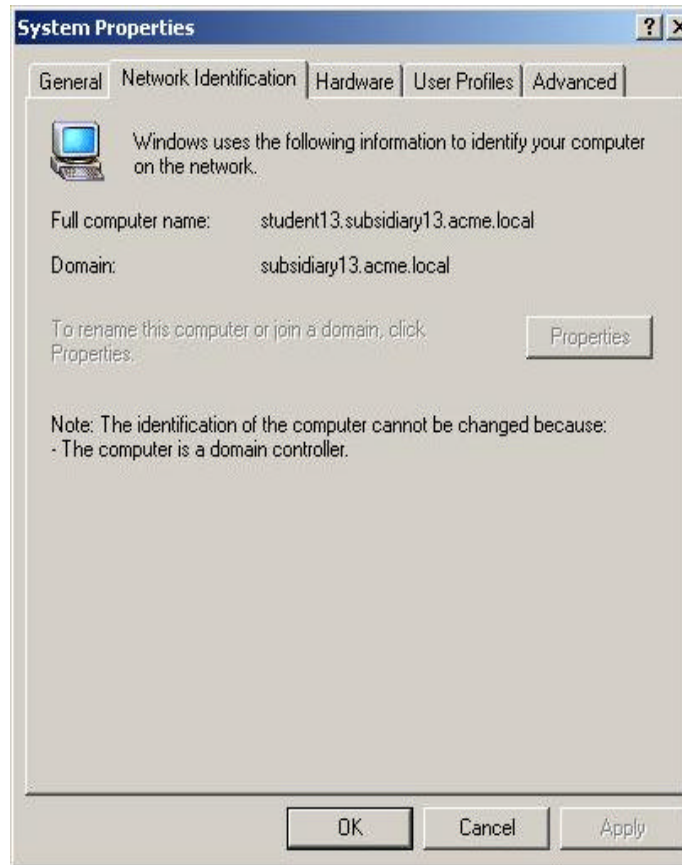


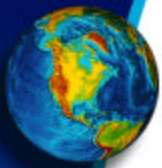


Audit Checklist (con't)

2) **WORKGROUPS & DOMAINS** – Verify that Domains are utilized for security and user administration.

- ◆ Where? – Right Click on My Computer, Properties, Network Identification tab (randomly select a few computers)

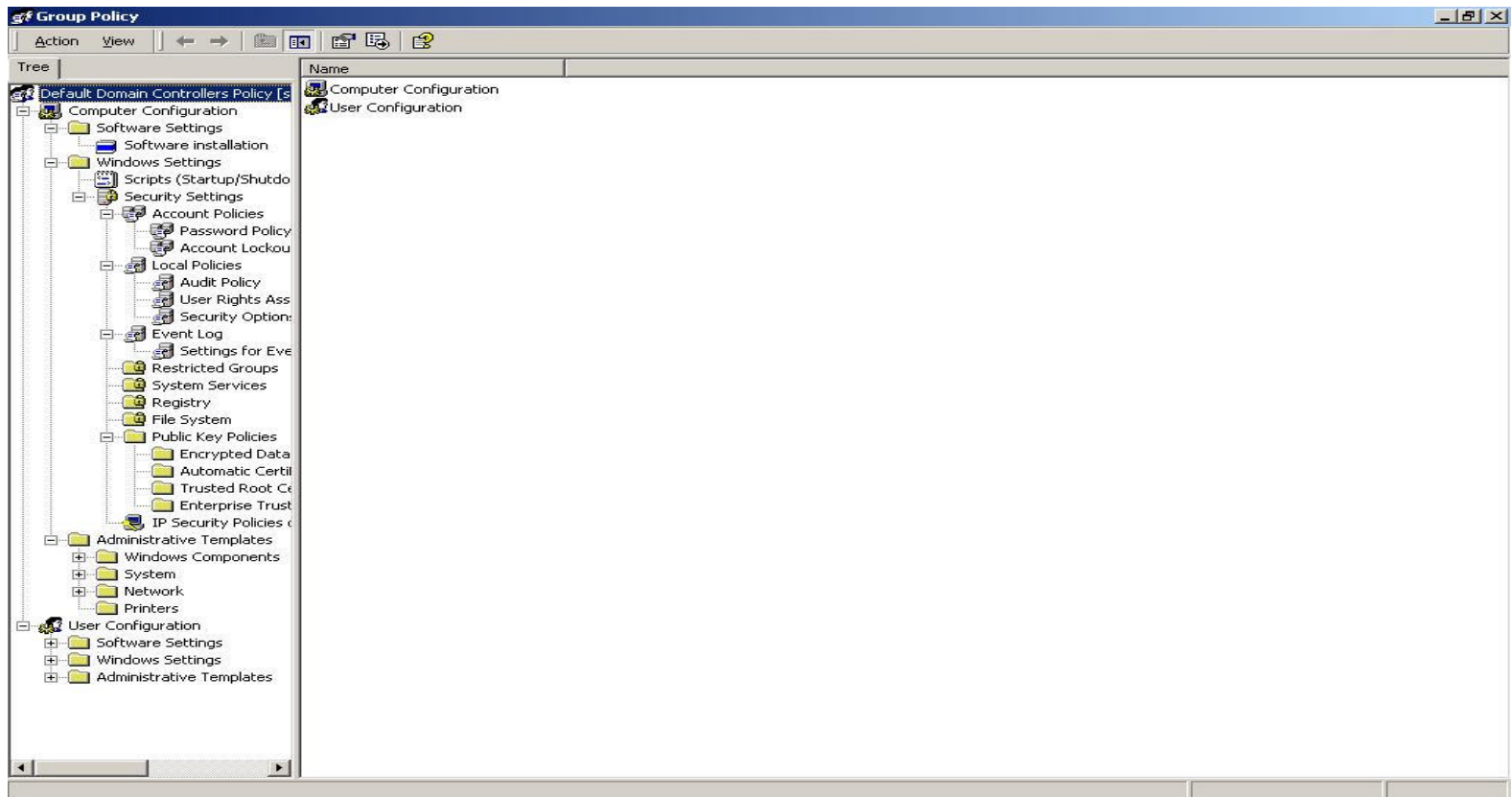


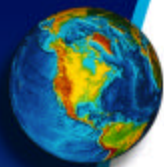


Audit Checklist (con't)

3) **GROUP POLICY OBJECTS** – Obtain an understanding of the methodology for implementation of Group Policies.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, Right Click select Properties then the Group Policy tab





Audit Checklist (con't)

- 4) **PERMISSIONS / ACLs** – Verify that the appropriate groups & users have been granted access to high-risk files, folders, directories, etc.
- ◆ Where? – Right click on resource, properties, security tab, then select the advance tab for each entry, then click view/edit button for each entry

Executive Compensation Properties

General | Web Sharing | Sharing | **Security**

Name: Add... Remove

Curly (Curly@dandt.com)
Guest (SUBSIDIARY13\Guest)
Internal Auditors (SUBSIDIARY13\Internal...
Larry (Larry@dandt.com)
Mo (Mo@dandt.com)

Permissions:

| | Allow | Deny |
|----------------------|-------------------------------------|--------------------------|
| Full Control | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Modify | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read & Execute | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| List Folder Contents | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Advanced...

☐ Allow inheritable permissions from parent to propagate to this object

OK Cancel Apply

Access Control Settings for Executive Compensation

Permissions | Auditing | Owner

Permission Entries:

| Type | Name | Permission | Apply to |
|-------|----------------------------|----------------|-----------------------------------|
| Allow | Curly (Curly@dandt.com) | Full Control | This folder, subfolders and files |
| Allow | Guest (SUBSIDIARY13... | Full Control | This folder, subfolders and files |
| Allow | Internal Auditors (SUBS... | Read & Exec... | This folder, subfolders and files |
| Allow | Larry (Larry@dandt.com) | Full Control | This folder, subfolders and files |
| Allow | Mo (Mo@dandt.com) | Full Control | This folder, subfolders and files |

Add... Remove View/Edit...

This permission is defined directly on this object. This permission is inherited by child objects.

☒ Allow inheritable permissions from parent to propagate to this object
☐ Reset permissions on all child objects and enable propagation of inheritable permissions.

OK Cancel Apply

Permission Entry for Executive Compensation

Object

Name: Change...

Apply onto:

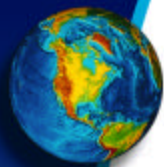
Permissions:

| | Allow | Deny |
|--------------------------------|-------------------------------------|--------------------------|
| Traverse Folder / Execute File | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| List Folder / Read Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Extended Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Create Files / Write Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Create Folders / Append Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write Extended Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Delete Subfolders and Files | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Delete | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Permissions | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Change Permissions | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Take Ownership | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

☐ Apply these permissions to objects and/or containers within this container only

Clear All

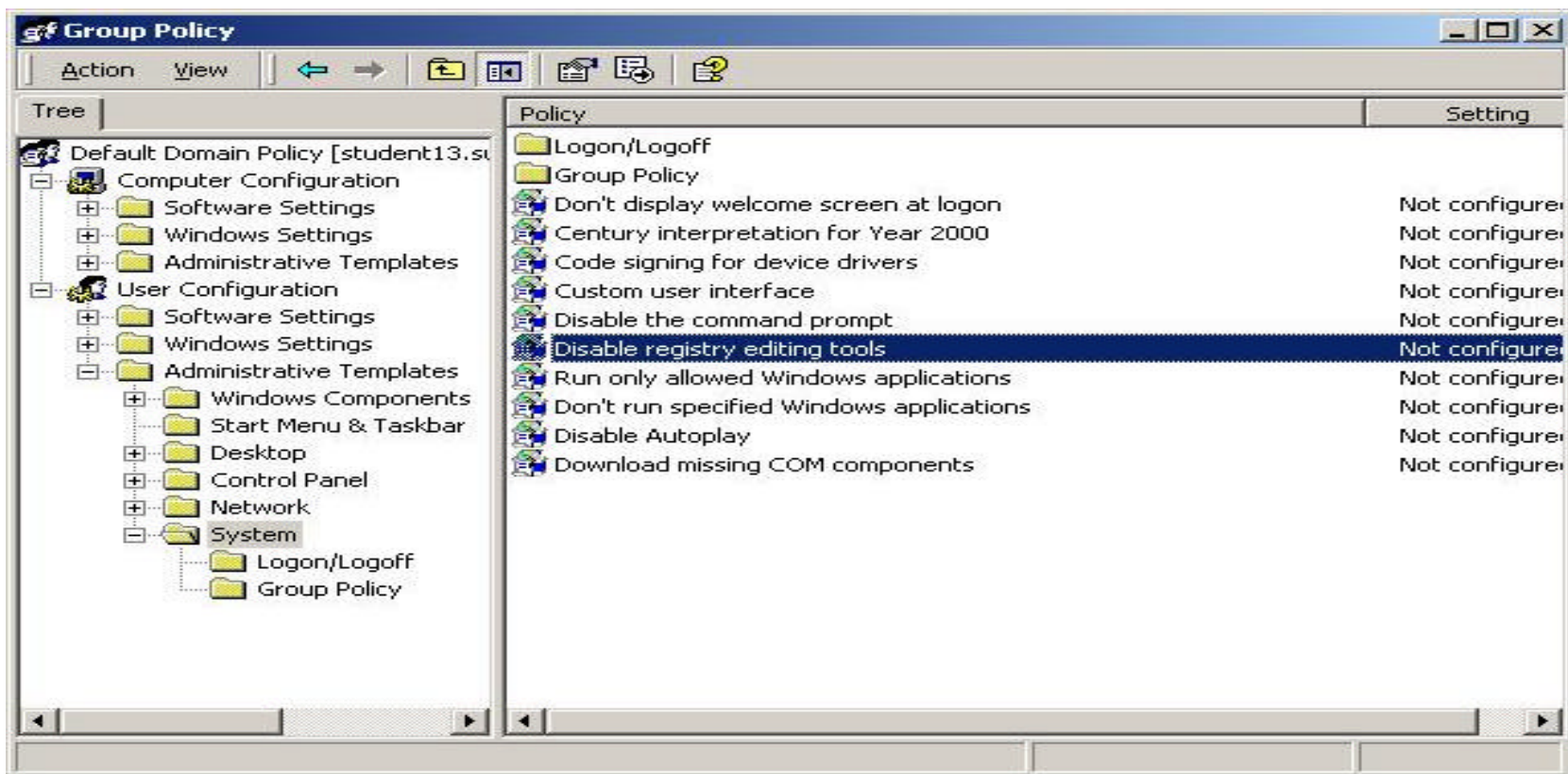
OK Cancel

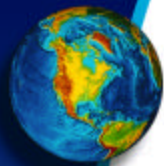


Audit Checklist (con't)

5) **REGISTRY** – Verify which OU has access to update the Registry.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the selected OU select properties then Group Policy. Select the GPO, click on Edit, then review the Disable registry editing tools parameter





Audit Checklist (con't)

6) FILE SYSTEMS - Verify that all disk partitions are formatted with NTFS.

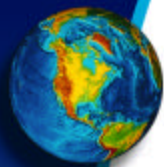
- ◆ Where? – Start, Programs, Administrative Tools, Computer Management

The screenshot shows the Windows Computer Management console. The left pane displays the 'Tree' view with 'Disk Management' selected under 'Storage'. The right pane shows a table of disk partitions.

| Volume | Layout | Type | File System | Status | Capacity | Free Space | % Free |
|--------|-----------|-------|-------------|------------------|----------|------------|--------|
| (C:) | Partition | Basic | FAT | Healthy (System) | 995 MB | 989 MB | 99 % |
| (D:) | Partition | Basic | NTFS | Healthy (Boot) | 1.95 GB | 441 MB | 22 % |

Below the table, the 'Disk 0' section shows a graphical representation of the disk layout. It includes a legend at the bottom: Primary Partition (blue), Extended Partition (green), Free Space (light green), and Logical Drive (dark blue).

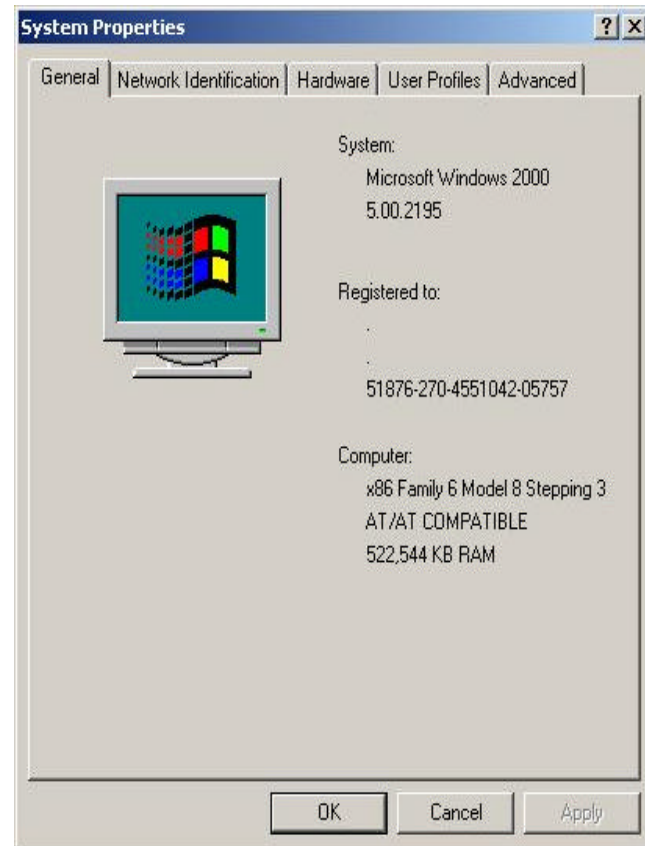
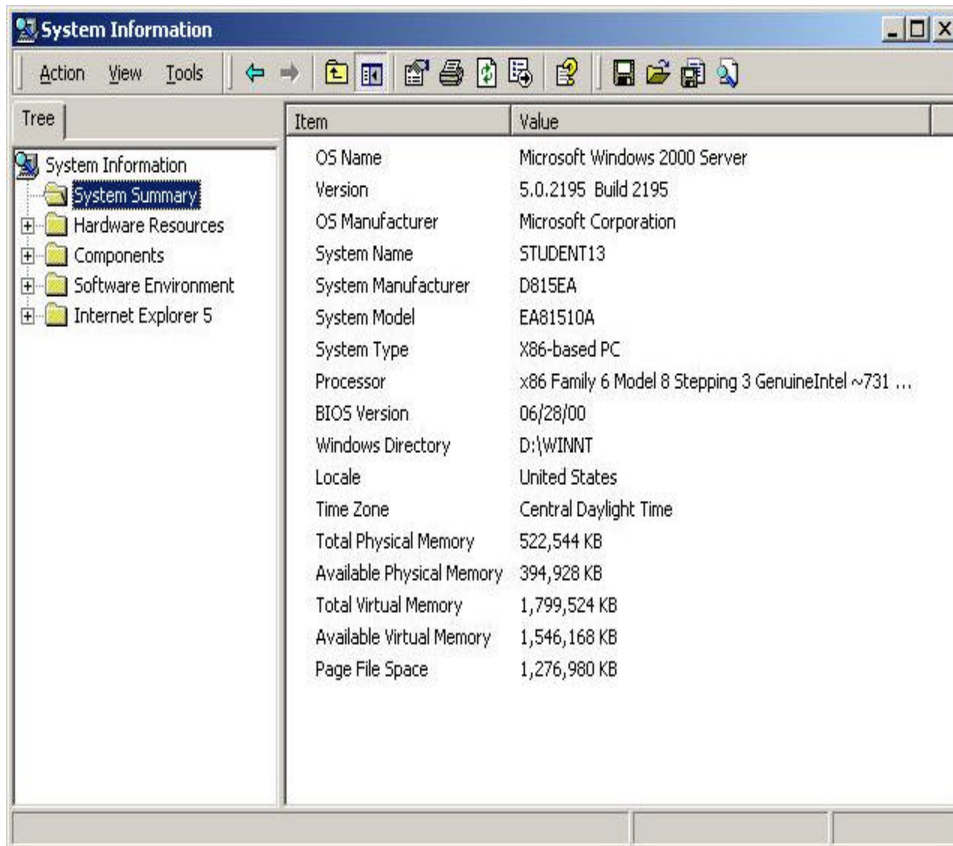
Legend: ■ Primary Partition ■ Extended Partition ■ Free Space ■ Logical Drive

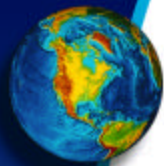


Audit Checklist (con't)

7) **SERVICE PACK / SYSTEM PROPERTIES**- Verify the Windows 2000 system properties and service pack installed

- ◆ Where? – Start, Run, type “MSINFO32” or right click on My Computer and select Properties

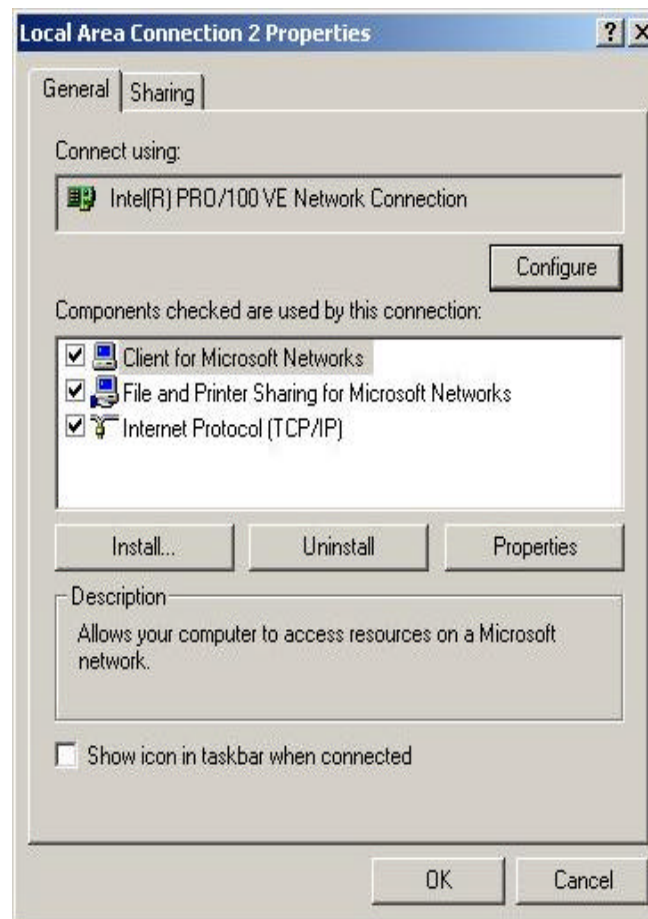


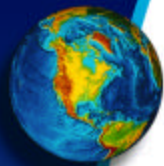


Audit Checklist (con't)

8) **PROTOCOLS** - Verify the network/system protocols installed.

- ◆ Where? – Right click on My Network Places, select Properties, Right click on the applicable Connections, select Properties

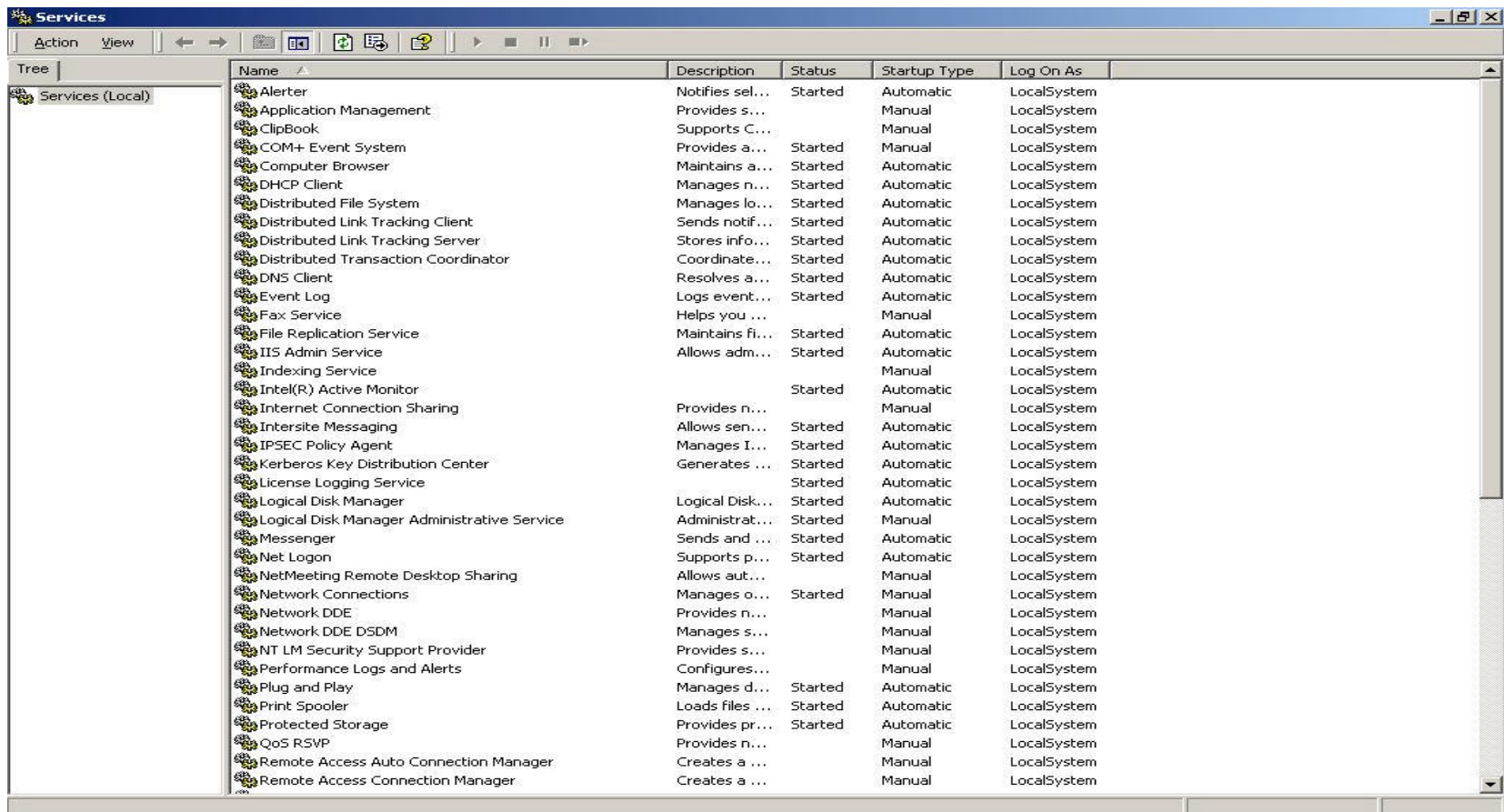




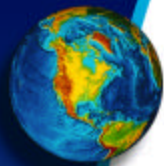
Audit Checklist (con't)

9) **SERVICES** - Examine what services are enabled and ensure that unnecessary and potentially insecure services are disabled (e.g. ftp, telnet, smtp, etc.).

◆ Where? – Start, Programs, Administrative Tools, Services



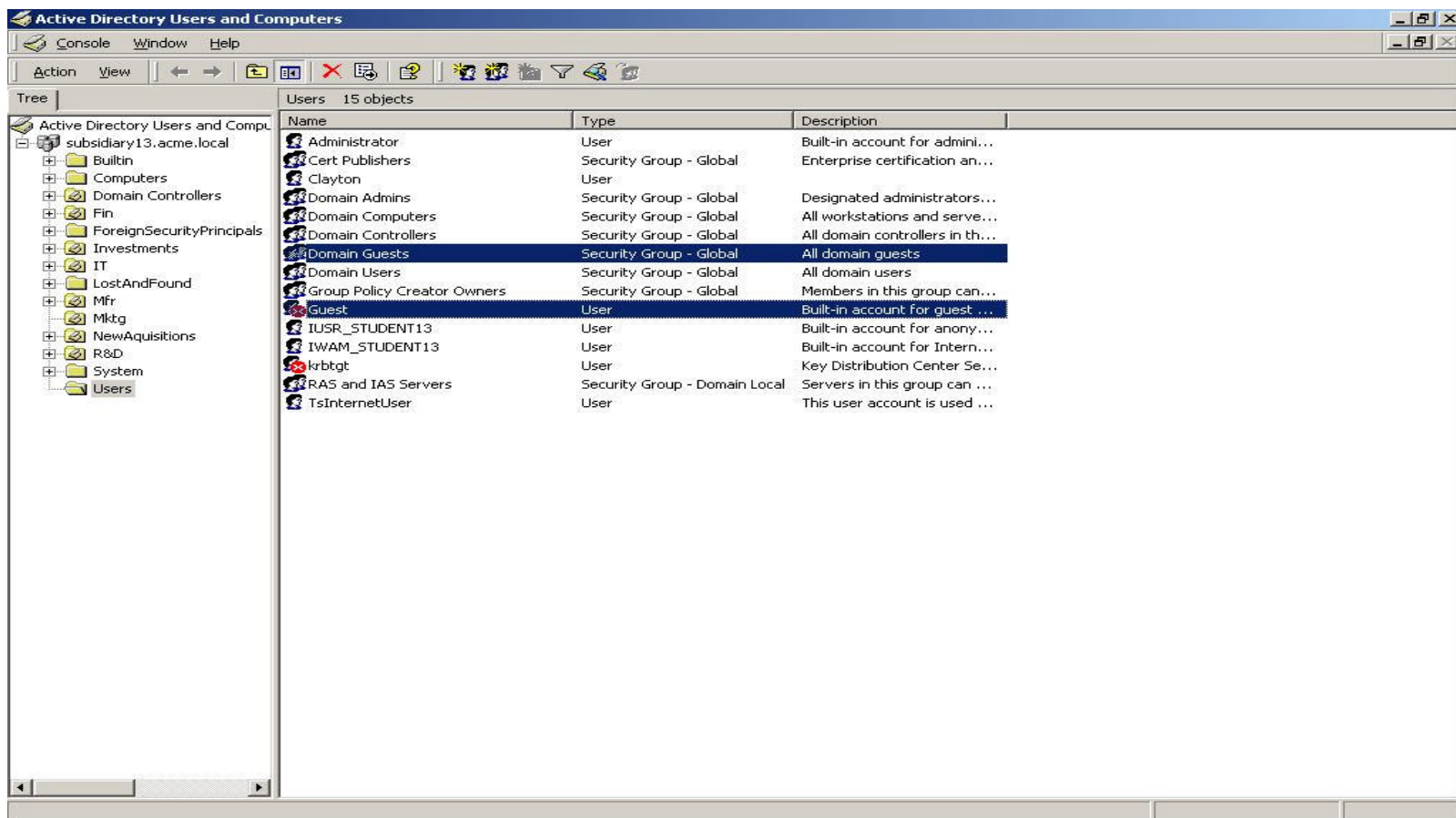
| Name | Description | Status | Startup Type | Log On As |
|---|-----------------|---------|--------------|-------------|
| Alert | Notifies sel... | Started | Automatic | LocalSystem |
| Application Management | Provides s... | | Manual | LocalSystem |
| ClipBook | Supports C... | | Manual | LocalSystem |
| COM+ Event System | Provides a... | Started | Manual | LocalSystem |
| Computer Browser | Maintains a... | Started | Automatic | LocalSystem |
| DHCP Client | Manages n... | Started | Automatic | LocalSystem |
| Distributed File System | Manages lo... | Started | Automatic | LocalSystem |
| Distributed Link Tracking Client | Sends notif... | Started | Automatic | LocalSystem |
| Distributed Link Tracking Server | Stores info... | Started | Automatic | LocalSystem |
| Distributed Transaction Coordinator | Coordinate... | Started | Automatic | LocalSystem |
| DNS Client | Resolves a... | Started | Automatic | LocalSystem |
| Event Log | Logs event... | Started | Automatic | LocalSystem |
| Fax Service | Helps you ... | | Manual | LocalSystem |
| File Replication Service | Maintains fi... | Started | Automatic | LocalSystem |
| IIS Admin Service | Allows adm... | Started | Automatic | LocalSystem |
| Indexing Service | | | Manual | LocalSystem |
| Intel(R) Active Monitor | | Started | Automatic | LocalSystem |
| Internet Connection Sharing | Provides n... | | Manual | LocalSystem |
| InterSite Messaging | Allows sen... | Started | Automatic | LocalSystem |
| IPSEC Policy Agent | Manages I... | Started | Automatic | LocalSystem |
| Kerberos Key Distribution Center | Generates ... | Started | Automatic | LocalSystem |
| License Logging Service | | Started | Automatic | LocalSystem |
| Logical Disk Manager | Logical Disk... | Started | Automatic | LocalSystem |
| Logical Disk Manager Administrative Service | Administrat... | Started | Manual | LocalSystem |
| Messenger | Sends and ... | Started | Automatic | LocalSystem |
| Net Logon | Supports p... | Started | Automatic | LocalSystem |
| NetMeeting Remote Desktop Sharing | Allows aut... | | Manual | LocalSystem |
| Network Connections | Manages o... | Started | Manual | LocalSystem |
| Network DDE | Provides n... | | Manual | LocalSystem |
| Network DDE DSDM | Manages s... | | Manual | LocalSystem |
| NT LM Security Support Provider | Provides s... | | Manual | LocalSystem |
| Performance Logs and Alerts | Configures... | | Manual | LocalSystem |
| Plug and Play | Manages d... | Started | Automatic | LocalSystem |
| Print Spooler | Loads files ... | Started | Automatic | LocalSystem |
| Protected Storage | Provides pr... | Started | Automatic | LocalSystem |
| QoS RSVP | Provides n... | | Manual | LocalSystem |
| Remote Access Auto Connection Manager | Creates a ... | | Manual | LocalSystem |
| Remote Access Connection Manager | Creates a ... | | Manual | LocalSystem |

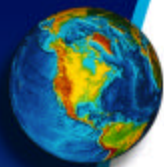


Audit Checklist (con't)

10) **ACCOUNTS** – Verify that the Guest account is disabled.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers

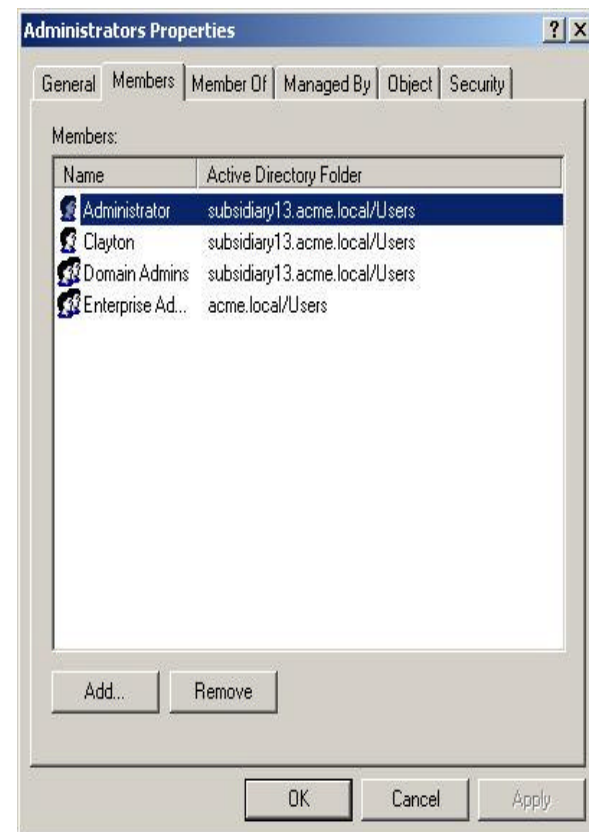
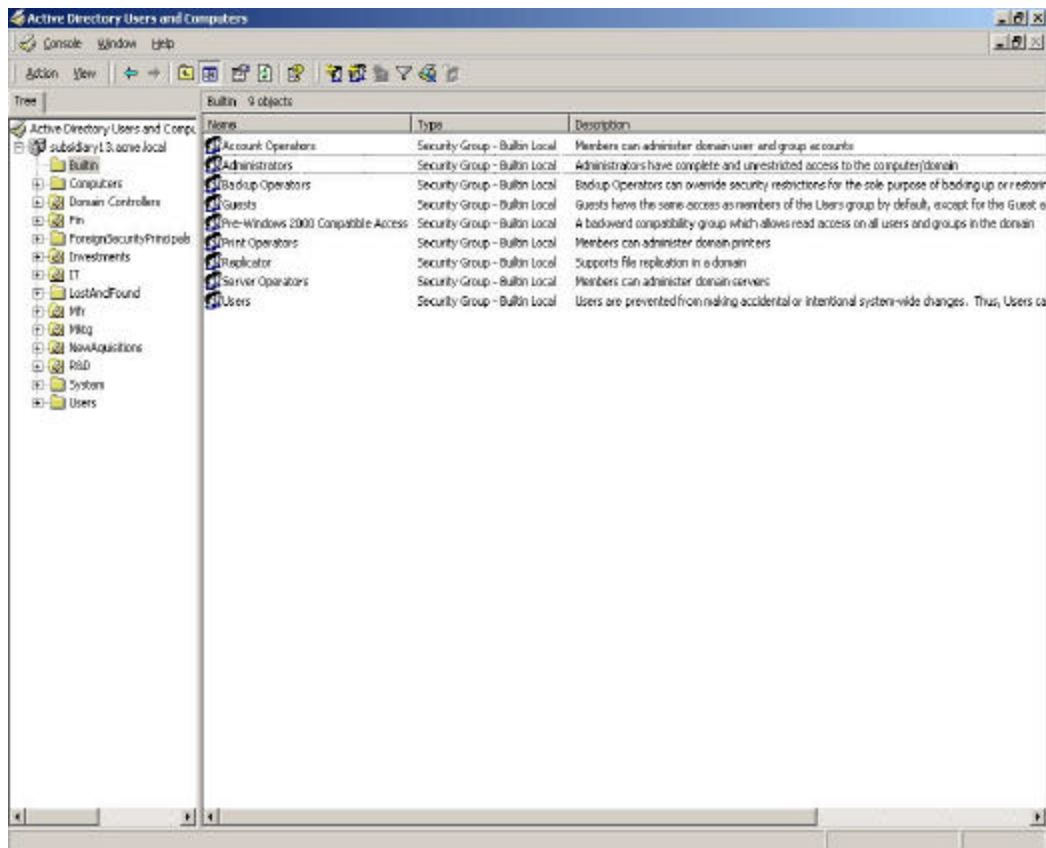


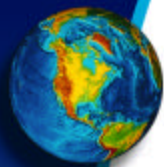


Audit Checklist (con't)

11) ACCOUNTS – Verify the membership of the Built-in Administrative Groups.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, select the Builtin folder, double click on each Group and examine the Members tab





Audit Checklist (con't)

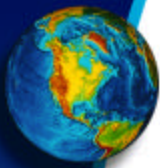
12) **MEMBERSHIP OF GROUPS** – Obtain an understanding of the use of groups and ensure that the assignment of users to the groups is appropriate.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users & Computers, select the applicable groups within the OUs, double click on each Group and examine the Members tab

The screenshot displays the Active Directory Users and Computers console. The left pane shows a tree view of the directory structure, with 'subsidary13.acme.local' expanded. The right pane shows a list of objects under 'InfoSec', including 'PasswordReset-Fin', 'PasswordReset-IT', 'PasswordReset-Mfr', 'PasswordReset-Mktg', and 'PasswordReset-R&D'. The 'PasswordReset-Mktg' group is selected. A 'PasswordReset-Mktg Properties' dialog box is open, showing the 'Members' tab. The 'Members' list contains two entries: 'Jack' and 'Jill', both assigned to the 'subsidary13.acme.local/Mktg' group. The 'Add...' and 'Remove' buttons are visible at the bottom of the dialog.

| Name | Type | Description |
|--------------------|-------------------------|-------------|
| PasswordReset-Fin | Security Group - Global | |
| PasswordReset-IT | Security Group - Global | |
| PasswordReset-Mfr | Security Group - Global | |
| PasswordReset-Mktg | Security Group - Global | |
| PasswordReset-R&D | Security Group - Global | |

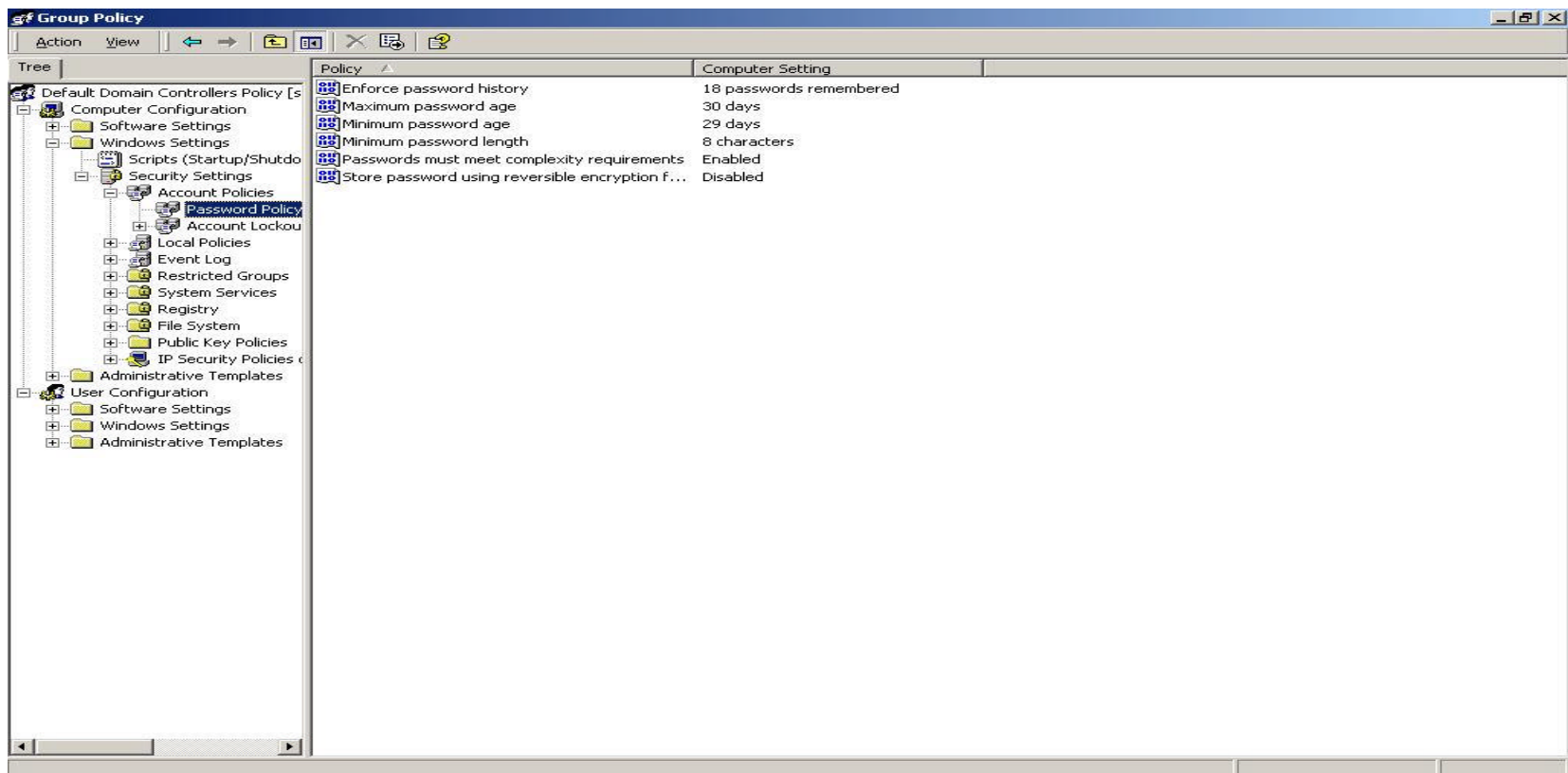
| Name | Active Directory Folder |
|------|-----------------------------|
| Jack | subsidary13.acme.local/Mktg |
| Jill | subsidary13.acme.local/Mktg |

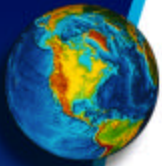


Audit Checklist (con't)

13) **PASSWORD POLICY** – Review the appropriateness of the password parameters within the Account Policies.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Account Policies

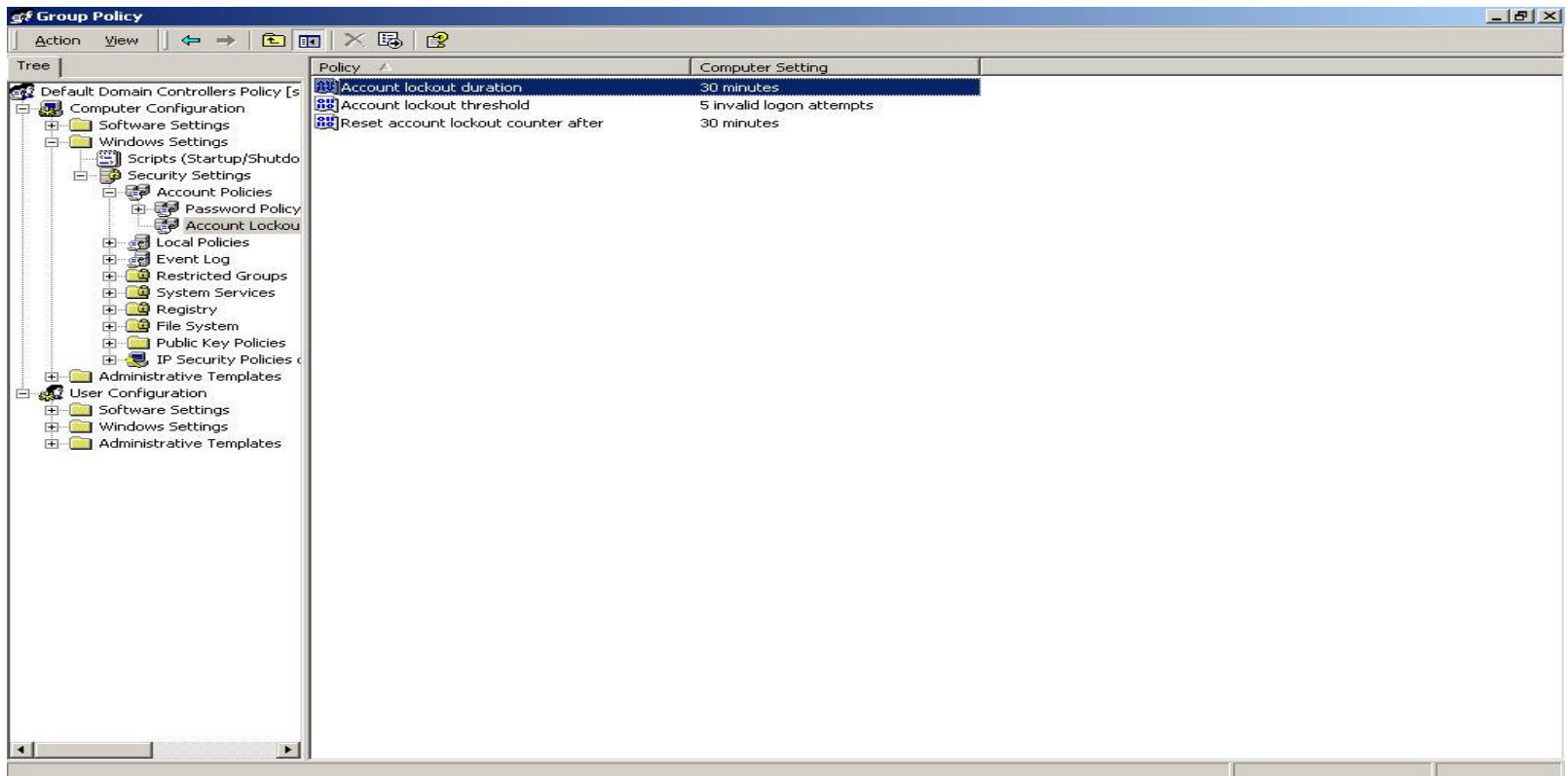


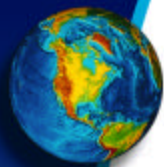


Audit Checklist (con't)

14) **ACCOUNT LOCKOUT** – Review the appropriateness of the account lockout parameters within the Account Policies.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Account Policies





Audit Checklist (con't)

15) **AUDIT POLICY** – Obtain an understanding of the use of auditing and ensure that the appropriate events are logged and reviewed.

- ◆ Where? –Within Group Policy select Windows Settings, Local Policies then Audit Policy. Select your object, right click properties, select security tab, advanced, select auditing tab and View/Edit

The screenshot shows the Windows Local Security Settings console on the left and the 'Permission Entry for Executive Compensation' dialog on the right.

Local Security Settings Console:

| Tree | Policy | Local Setting | Effective Setting |
|-------------------------|--------------------------------|---------------|-------------------|
| Security Settings | Audit account logon events | No auditing | Success, Failure |
| Account Policies | Audit account management | No auditing | Success, Failure |
| Local Policies | Audit directory service access | No auditing | Success, Failure |
| Audit Policy | Audit logon events | No auditing | Success, Failure |
| User Rights Assign | Audit object access | No auditing | Success, Failure |
| Security Options | Audit policy change | No auditing | Success, Failure |
| Public Key Policies | Audit privilege use | No auditing | Success, Failure |
| IP Security Policies on | Audit process tracking | No auditing | Success, Failure |
| | Audit system events | No auditing | Success, Failure |

Permission Entry for Executive Compensation Dialog:

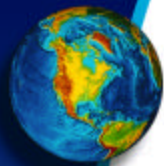
Object: [Curly (Curly@dandt.com)] [Change...]

Apply onto: [This folder, subfolders and files]

| Permissions: | Allow | Deny |
|--------------------------------|-------------------------------------|--------------------------|
| Traverse Folder / Execute file | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| List Folder / Read Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Extended Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Create Files / Write Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Create Folders / Append Data | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write Extended Attributes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Delete Subfolders and Files | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Delete | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read Permissions | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Change Permissions | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Take Ownership | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

☐ Apply these permissions to objects and/or containers within this container only [Clear All]

[OK] [Cancel]

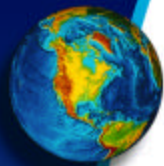


Audit Checklist (con't)

16) **EVENT LOGS** – Inquiry as to the use of the Event Logs and frequency of reviews. Obtain a copy of the event logs.

◆ Where? – Start, Programs, Administrative Tools, Event Viewer

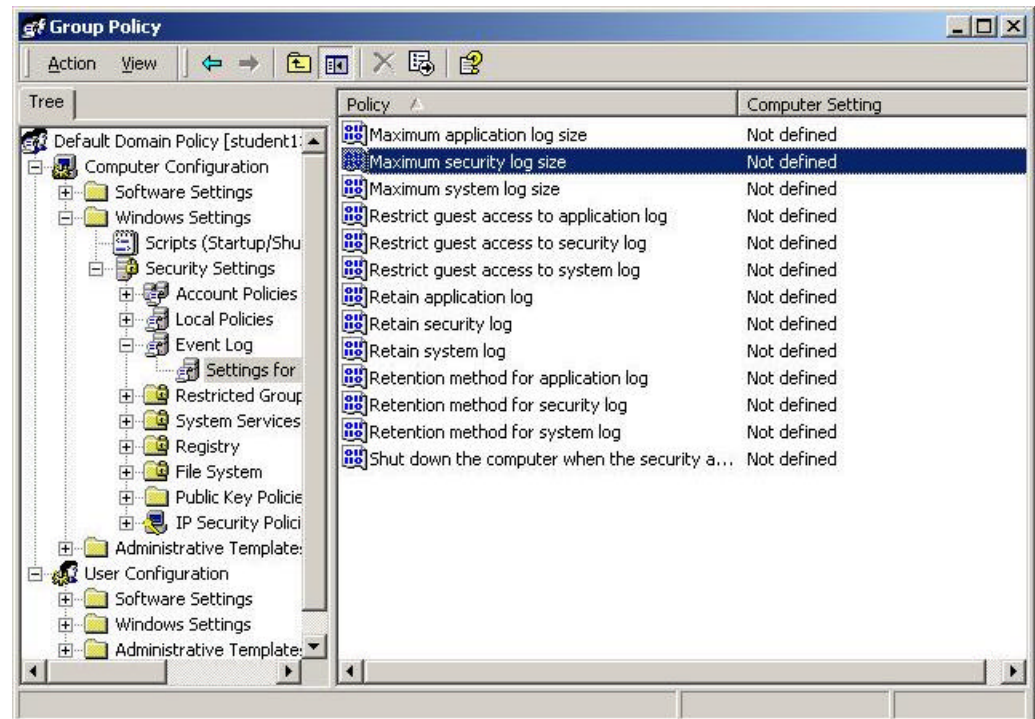
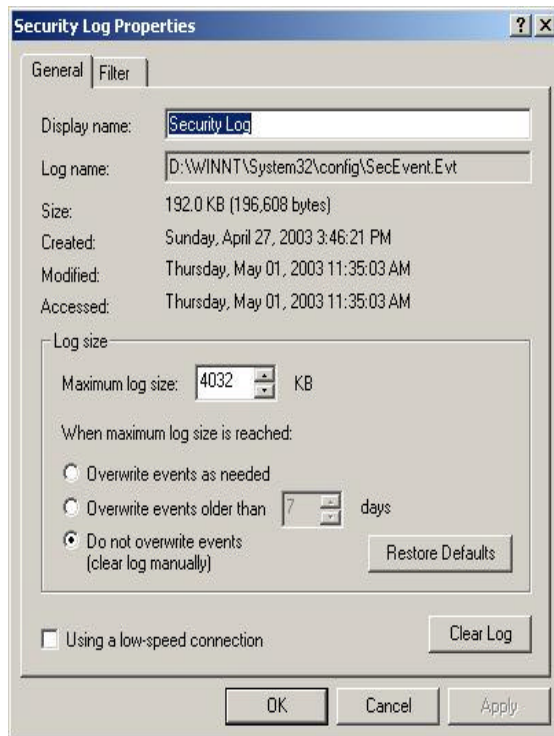
| Type | Date | Time | Source | Category | Event | User | Computer |
|-------------|-----------|--------------|-------------------------|----------|-------|------|-----------|
| Warning | 4/30/2003 | 4:53:12 PM | Netlogon | None | 5781 | N/A | STUDENT13 |
| Information | 4/30/2003 | 4:34:27 PM | Removable Storage Se... | None | 135 | N/A | STUDENT13 |
| Error | 4/30/2003 | 4:33:50 PM | Removable Storage Se... | None | 17 | N/A | STUDENT13 |
| Error | 4/30/2003 | 4:33:35 PM | Removable Storage Se... | None | 17 | N/A | STUDENT13 |
| Information | 4/30/2003 | 4:33:20 PM | Removable Storage Se... | None | 134 | N/A | STUDENT13 |
| Information | 4/30/2003 | 4:33:20 PM | Removable Storage Se... | None | 135 | N/A | STUDENT13 |
| Information | 4/30/2003 | 4:33:19 PM | Removable Storage Se... | None | 134 | N/A | STUDENT13 |
| Information | 4/30/2003 | 4:25:57 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Warning | 4/30/2003 | 3:58:43 PM | Schannel | None | 36872 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:36:54 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:25:23 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:24:20 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:23:36 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:21:35 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 2:06:29 PM | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:42:12 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:42:08 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:41:38 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:39:53 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:37:05 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:36:01 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:35:26 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:23:36 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 11:18:50 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/30/2003 | 10:54:24 ... | Application Popup | None | 26 | N/A | STUDENT13 |
| Information | 4/29/2003 | 11:37:08 ... | Browser | None | 8015 | N/A | STUDENT13 |
| Information | 4/29/2003 | 11:36:52 ... | Browser | None | 8015 | N/A | STUDENT13 |
| Warning | 4/29/2003 | 11:36:20 ... | Dhcp | None | 1007 | N/A | STUDENT13 |
| Information | 4/29/2003 | 11:35:18 ... | eventlog | None | 6005 | N/A | STUDENT13 |
| Information | 4/29/2003 | 11:35:18 ... | eventlog | None | 6009 | N/A | STUDENT13 |
| Error | 4/29/2003 | 11:35:18 ... | eventlog | None | 6008 | N/A | STUDENT13 |
| Warning | 4/29/2003 | 11:35:29 ... | disk | None | 34 | N/A | STUDENT13 |
| Warning | 4/29/2003 | 8:59:29 AM | Schannel | None | 36872 | N/A | STUDENT13 |
| Warning | 4/29/2003 | 1:54:21 AM | W32Time | None | 64 | N/A | STUDENT13 |
| Information | 4/28/2003 | 3:32:09 PM | Browser | None | 8035 | N/A | STUDENT13 |
| Information | 4/28/2003 | 3:27:15 PM | Browser | None | 8015 | N/A | STUDENT13 |
| Warning | 4/28/2003 | 3:27:09 PM | Dhcp | None | 1007 | N/A | STUDENT13 |

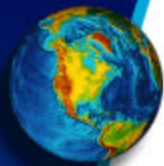


Audit Checklist (con't)

17) **EVENT LOGS** – Verify that the configuration of the event logs will retain an appropriate amount of data (e.g. Max. log size & “Do not overwrite events”, etc.).

- ◆ Where? – Start, Programs, Administrative Tools, Event Viewer, right click on each type of log and select Properties or Group Policy, Windows Settings, Event Log

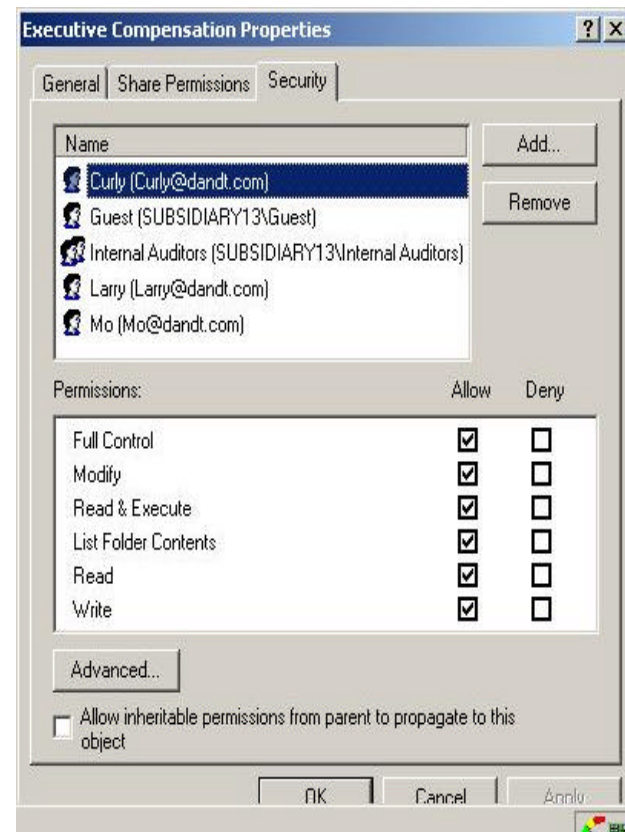
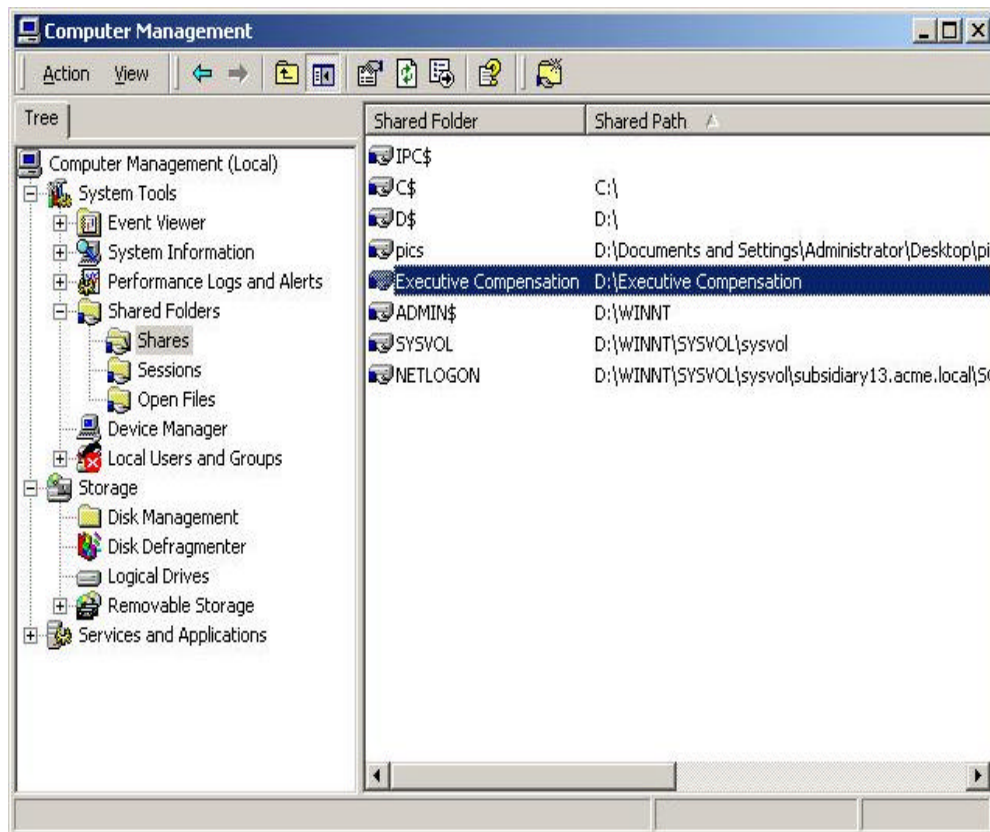


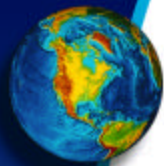


Audit Checklist (con't)

18) **SHARES** – Verify that access to critical shared folders is appropriately controlled through Access Control Lists and Permissions.

- ◆ Where? – Start, Programs, Administrative Tools, Computer Management, double click on the critical shared folders and review the Security tab

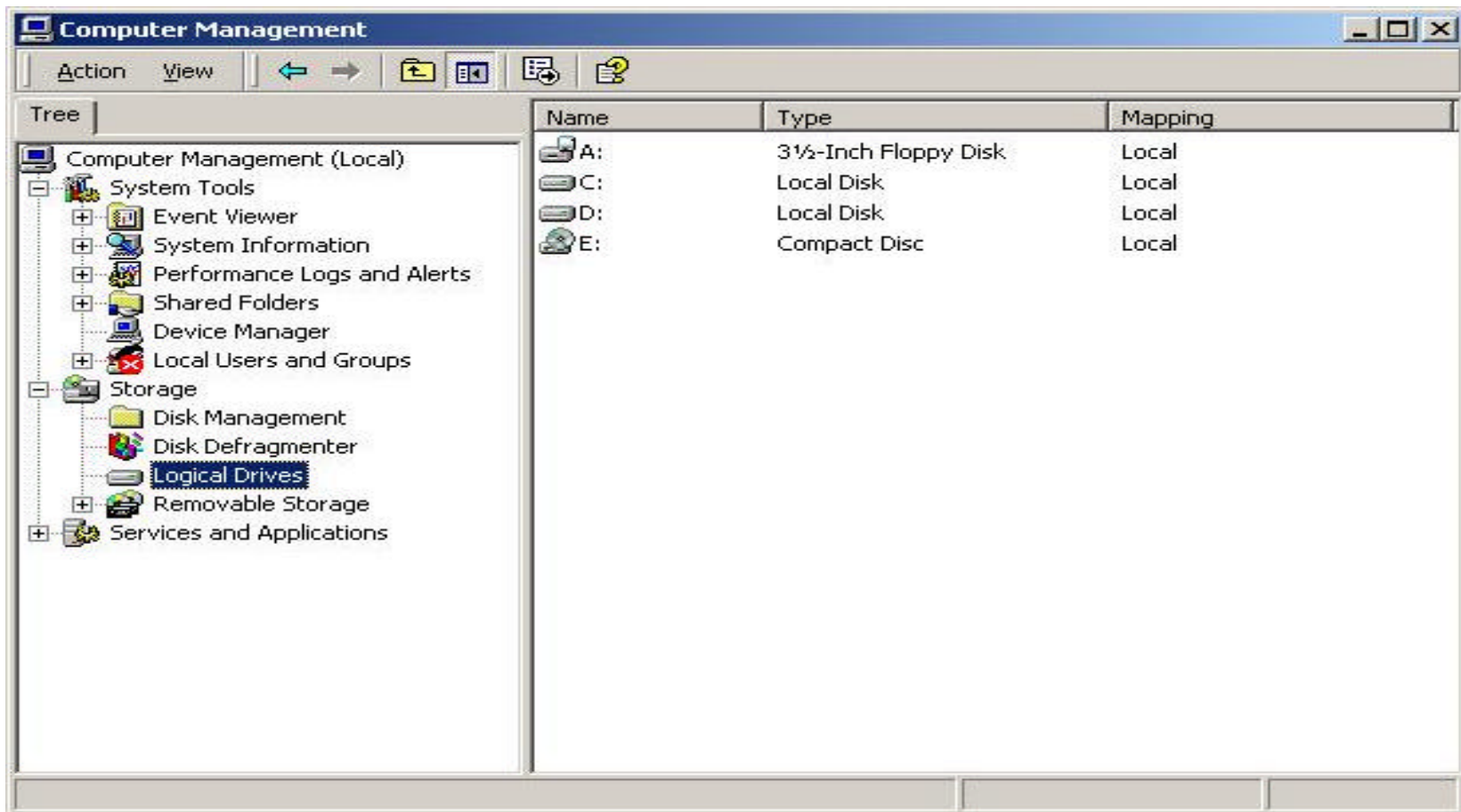


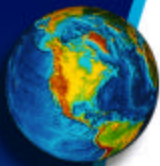


Audit Checklist (con't)

19) **DRIVES MAPPED** – Verify the validity of mapped drives.

- ◆ Where? – Start, Programs, Administrative Tools, Computer Management, select Logical Drives

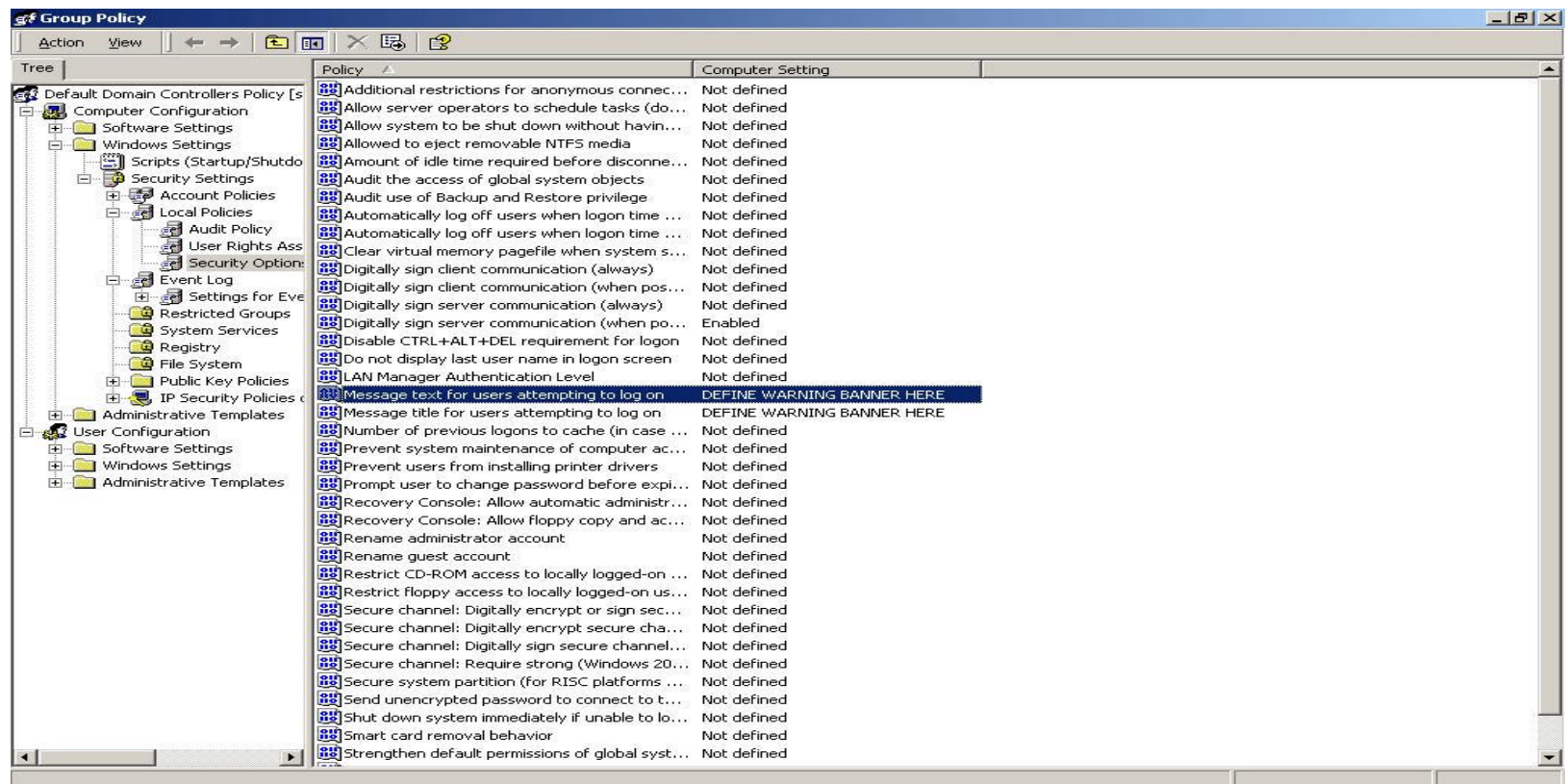


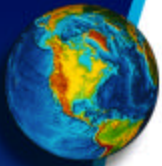


Audit Checklist (con't)

20) **LEGAL NOTICE** – Review the appropriateness of the Legal Notice within the Group Policy.

- ◆ Where? – Start, Programs, Administrative Tools, Active Directory Users and Computers, right click on the Domain Controllers OU select properties then Group Policy. Select the GPO, click on Edit, then review the Security Options.





Tools for Managing & Auditing Security

Checking & Managing Security Configuration Tools

◆ Security Configuration & Analysis Tool Set

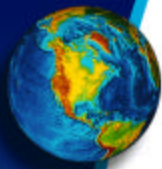
- ◆ Provided by Microsoft to compare current configuration vs. a security template
- ◆ The security template defines almost all security settings for Windows 2000
- ◆ Various templates can be customized per each type of system or level of security

◆ Microsoft Baseline Security Analyser

- ◆ Provided by Microsoft to compare configuration for the latest security related hotfixes, service packs, and performs an analysis of various common security misconfigurations
 - ◆ Windows
 - ◆ IIS
 - ◆ SQL
 - ◆ Desktop application

◆ CIS's Benchmarks and Scoring Tool (www.cisecurity.org)

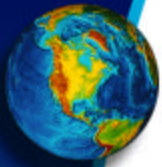
- ◆ A consensus of CIS members (SANS, NSA, DISA, NIST, & GSA)
- ◆ A compilation of security configuration actions and settings that "harden" the Windows O/S
- ◆ "the minimum level of due care"
- ◆ "unlikely to cause an interruption of service"



Tools for Managing & Auditing Security (con't)

Reporting Security Configuration Tools

- ◆ Microsoft doesn't provide built-in reporting capabilities, therefore gathering evidence supporting audit findings is very difficult & time consuming
- ◆ Windows 2000 security management and auditing is impractical without the use of third party reporting tools
- ◆ A few Reporting/Auditing Tools
 - ◆ **DumpSEC** (www.systemtools.com)
 - ◆ A free tool that provides the major security reports needed for auditing users, group policy, services, rights, shares and permission reports
 - ◆ Can only be processed on one domain or system at a time and requires administrator access
 - ◆ **SekCheck**
 - ◆ Endorsed and used by D&T to extract, report, and audit system configurations from Domain Group Policy settings to Home Directories, Logon scripts, and Profiles
 - ◆ Results are processed within 24 hours
 - ◆ Various others Tools



Tools for Managing & Auditing Security (con't)

Security Log Analysis Tools

- ◆ **DumpEL**

- ◆ Part of Windows 2000 resource kit

- ◆ **ELDump**

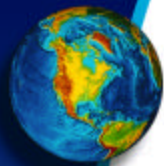
- ◆ Freeware which is more versatile and faster than DumpEL and contains better filtering options
- ◆ Best for reporting directly from the security logs

- ◆ **DumpEVT**

- ◆ Handles special characters better than DumpEL to prevent problems with importing
- ◆ There is no filtering available, therefore it is most commonly used to import into Access

- ◆ **NTLast**

- ◆ Used for analyzing logon activity from the security logs



Useful Resources

Publications

- ◆ **Hacking Windows 2000 Exposed**
 - ◆ Joel Scambray, Foundstone

- ◆ **Hack Proofing Windows 2000 Server**
 - ◆ Chad Todd

Web Sites

- ◆ **MS Security Bulletins**
 - ◆ www.microsoft.com/security
- ◆ www.ntsecurity.net
- ◆ www.win2000mag.com
- ◆ www.websolutions.com
- ◆ www.winnetmag.com
- ◆ www.labmice.net/Security/
- ◆ www.sunbeltsoftware.com

Forums

- ◆ www.ntbugtraq.com
- ◆ www.secadministrator.com/forums/