UNIT 3 SECURITY AND MANAGEMENT - I

Structure **Page Nos.**

3.0 INTRODUCTION

In this unit we will discuss the concepts and configuration required to secure Microsoft Windows computers and also examine everything from the foundational principles of Windows NT Security Management, up to the advanced issues of securing Windows 2000 machines running Active Directory. The unit address is a broad sweep of concepts of Windows Management Architecture and security related issues: Main Issues in Windows Security; Windows Resource Management; Windows 2000 Operating Systems.

Section 3 of this unit deals with "Main Issues in Windows Security and Management" and it covers the following areas; physical security management, logon security management, user/groups management, Windows NT domain model, domain controllers.

Section 4 of this unit deals with Windows resource security management and it covers areas like; files and folder management, files/folder permissions, printer management and Registry Management.

The most important, section 5, deals with the management of Windows 2000 operating system; Windows 2000 features, active directory, logical structure, physical structure, Windows 2000 DNS, Group Policy etc.

3.1 OBJECTIVES

After going through unut you will be able to learn:

- management of Windows NT system, and
- examine the fundamentals of the Management of Windows 2000 system.

The objective of this unit will be:

- examine the various issues of Management of Windows NT 4.0.
- study and manage Windows NT 4.0 Resources
- examine the Windows 2000 Infrastructure.

3.2 MAIN ISSUES IN WINDOWS SECURITY MANAGEMENT

In this section we will point on main issues in windows security management.

3.2.1 Physical Security Management

The main problem or issue of computer security is unauthorized physical access to a secure computer system and it is breech of computer security. If a computer is in a public area it should not contain any sensitive data.

The following steps should be taken to improve physical or local security: computer BIOS must have a password, and computer should be configured to boot from hard drive and not through floppy or any other external media. In Windows NT Server provides options to control local access or right to log on locally and this adds another layer of security on computer.

3.2.2 Logon Security Management

When a user logs on to a Windows NT machine, he is presented with an onscreen message or notice. This message must clearly state the intended use of the computer system. It is suggested that the banner should not have a greeting, or a welcome message. The main steps for creating a user account are given below:

Creating a User Account

1. Log on as an Administrator.
2. Navigate to: User Manager for Domains.
3. Select User -→ New User.
4. Type user name in the Username Field.

5. **Type your first name in the Password Field.** Please note that passwords are case sensitive.
6. Type the exact same password in the Confirm Password Field.
7. Add this user to the Administrators Group.

Steps for Logon Security

1. Creating a Logon Warning Message
2. In the run option, type Regedit to open the Registry editor.
3. In the Registry Editor navigate to:
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogo.
4. Double-click the LegalNoticeCaption value.
5. In the Value Data entry field, Type Unauthorized Access Warning!! Then press OK
6. Double-click the LegalNoticeText value.
7. Type in the Value Data Entry Field.

   "Unauthorized access to this system is punishable by a fine of Rs 7,500 and/or one year in prison. Use of this system indicates that you have read and agree to this warning".
8. Press OK.
9. Close the Registry Editor.
10. Log off and verify the changes.

In addition to logon security management, you can eliminate the name of the previous user logged onto the system. If the last username is not eliminated, then an intruder or hacker can simply look at the screen, or press [Ctrl][Alt][Del] to find out the previous user. By getting a valid username, the intruder has acquired half of what is required to gain access to the system.

3.2.3 Users and Groups Management

In Windows NT every unique user of the system has a unique user account and this account is provided a Security Identifier or SID at the time when account is used. Windows provides multiple levels of user account with the most powerful user account the Administrator (Or Domain Administrator in a domain environment). The Administrator account has the power to manage all the settings on each system and as a result this is the account that must be properly secured. It is suggested that the Administrator account should not be used for day-to-day work at the network. Network administrators should create a separate account for daily routine activities and the Administrator account should be used only when it is absolutely required.

Permissions for resources can be set for individual users but this is not the most efficient way to manage the security of files and folders. It is for this reason that it is necessary to manage the permissions of resources. The function of groups is to assign users who have similar requirements for the use of resources. In this way you will be able to define access to the group rather than to the individual user.

3.2.4 Managing Local and Global Groups

The Administrator can manage the groups in two ways. The two options are Local Groups and Global Groups. Local Groups apply to a single computer and are used to

control access to resources on the local computer. Global Groups apply to an entire domain, or group of computers.

You can combine groups together, local and global. But the only allowed combination is to put a Global Group into a Local Group. This is accomplished by adding new computers or members to the Local Group, and from the list selecting a Global Group as the member.

3.2.5 Managing User Accounts

When securing the Windows System, the standards regarding user passwords should be followed. It must be ensured that users are not using weak, or easy to guess passwords and there should be no user accounts that have a blank password, and none that have a password that is the same as the username.

Please Note: Windows 95/98 and Windows NT support 14 character passwords and remember this as it may be required for backwards compatibility if you are using Windows 2000.

The Windows System provides the required help to an administrator for managing passwords. In User Manager for Domains (or User Manager on workstations or standalone servers), the administrator can define Account Policies. These account policies provide various options such as: how long a password is good, how long the password must be, and how many failed attempts will cause the account to lockout, often set to 3. It is necessary to have the password change often for high security, and for the system to remember passwords, preventing users from using the same password over and over again. The following steps should be followed for defining the account policies.

Steps for Defining Account Policies for disabling last username option.

1. Disabling the Last Username option
2. In the run box. type Regedit to open the Registry Editor.
3. Navigate to: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\Current Version\Winlogon
4. From the drop-down menus choose Edit > New > String Value.
5. Type DontDisplayLastUsername in the Name Field
6. Double-click on your new string.
7. Type 1 in the Value Data entry field, and press OK to close the Edit dialog box.
8. Close the Registry Editor.

Log off and back on again (no need to restart) to verify the changes. Verify that the last user name no longer appears in the logon box.

1. Log on to your Windows NT Server as Administrator.
2. Navigate to: User Manager for Domains.
3. From the drop-down menus select Policies > Account.
4. Halfway down the page select the Account Lockout radio button.
5. Modify the Account Lockout settings to the following:
   a. Lockout: after 5 bad attempts.
   b. Reset count: after 100 minutes.

c. Lockout

d. Duration: Forever (until admin unlocks).

6. Close the Account policy dialog box by pressing OK.
7. Log off as Administrator and try these changes.
8. Log back on as Administrator.
9. Navigate to: User Manager for Domains.
10. Double-click on the user you used above.
11. Verify that the Account Locked Out radio button is checked, and uncheck it. Then press OK.
12. Close User Manager.

It is also necessary to secure the Guest account and this account should never be used in a secure environment. The guest account can be locked down by the following steps:

- Rename the guest account to a difficult - to - guess account name.
- Remove the guest account description.
- Set a very complex 14-character password.
- Change logon hours to never.
- Change the logon to option to a Workstation that is not active.

The concept of user accounts and groups provides an efficient way to manage access to resources, but to define the network itself a larger concept, called the Window NT Domain model, is available.

3.2.6 Windows NT Domain Management

The model of Windows NT Security allows you to control many users, groups, and computers by using a boundary known as a Domain. A server called the Primary Domain Controller (PDC) controls a Domain and there can be only one PDC per domain. But there can be a number of Backup Domain Controllers (BDC) to assist PDC. This Domain model allows for thousands of computers and users under a single management option. When a user logs on to a domain, he is able to access all the computers in the logged domain, with the security of those computers dictating the actual level of permission to objects.

This model also provides for a Single Sign On (SSO) to all resources, that is the user is not required to provide credentials for each computer that s/he wishes to access. While the domain model is useful, it does have limitations: (a) a very large domain would be hard to manage efficiently, and (b) users who are very far apart physically may find a more efficient network experience to have one domain per location.

Regardless of the reason, in order for the network to expand, more than one domain is required. To maintain the SSO across multiple domains a method called trust relationship is used. A trust relationship is an administrative link between two domains. A domain that trusts another domain is called a TRUSTING domain and the other domain is called TRUSTED domain. The TRUSTED domain or Accounts domain holds the user accounts and the TRUSTING domain or RESOURCE domain holds the resources. The trust is only one-way, meaning that if domain A trusts domain B, then domain B does not have to trust domain A. In order to have trust in both directions, two one-way trusts relationship needs to be created. There are four basic domain

models in Windows NT 4.0: (1) the single domain model (no trust created), (2) single master (one Accounts domains (A), one or more Resource domains (R), (3) multiple masters (two or more Accounts domains one or more Resource domain's) shown in *Figure 2*, and (4) complete trust (all domains have direct trusts to all other domain) shown in *Figure 3*.

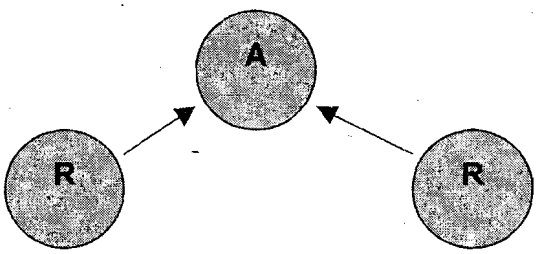


Figure 1: Single Master

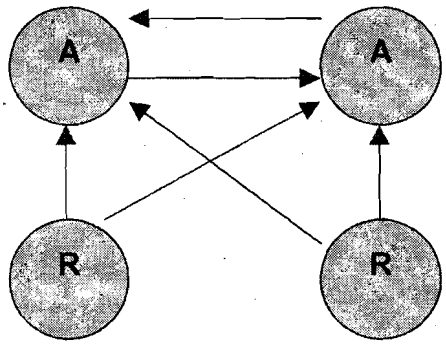


Figure 2: Multiple Master

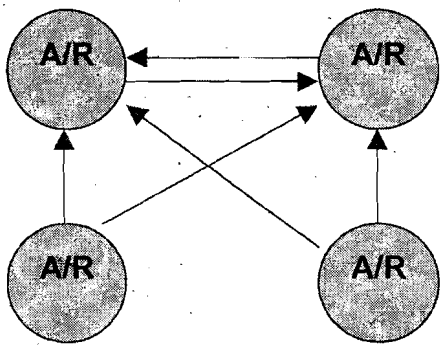


Figure 3: Complete Trust

There is a fifth type of domain structure, but it is not an official model. This type is of a hybrid or mixed layout, shown in *Figure 4* where the trust structure has no specific pattern. In this layout there are some Resource domains as well as some Account domains, spread throughout the network.

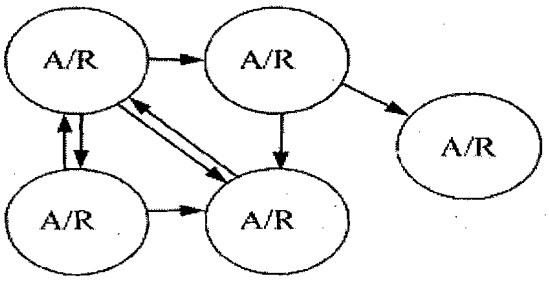


Figure 4: Hybrid or Mixed Layout

☞ **Check Your Progress 1**

1) Create a user account " Testuser" and create a logon warning message:

"Unauthorised access to this system is punishable by a fine of Rs 10,000 and / or one year of imprisonment. Use of this system indicates that you have read and agree to this warning."

.....

.....

.....

.....

2) List the steps for disabling the Last username option.

.....

.....

.....

.....

3.3 DOMAIN CONTROLLER

Windows Server organises groups of computers into domains so that all the machines in a particular domain can share a common database and security policy. Domain controllers are systems that run NT Server and share the centralised directory database that contains user account and security information for a particular domain. When users log on to a particular domain account, the domain controllers authenticate the users username and password, against the information stored in the directory database.

When you perform NT Server installation, you must designate the role that servers will play in a domain. Three choices are available for this role: PDC, BDC, and member server (i.e., a standalone server).

3.3.1 The Primary Domain Controller (PDC)

The first Windows NT Server in the domain is configured as a primary domain controller (PDC). The User Manager for Domains utility is used to maintain user and group information for the domain using the domain security database on the primary controller.

3.3.2 Backup Domain Controllers (BDC)

BDC (Backup Domain Controllers) are the other server after one server has been configured as PDC. BDC stores a copy of the database on the PDC, which is updated periodically to distribute changes made to the main database on the PDC. Such BDC have many advantages:

- If the PDC stops functioning due to a hardware failure, one of the BDC can be promoted to the primary role. Such arrangement provides fault tolerance in the network.

- PDC provides helps in authenticating network logons. When a user logs on to a domain, the logon request can be handled by any PDC or BDC. This provides an automatic mechanism for load distribution and improves logon performance and it is highly useful in domains with large numbers of users.

☞ Check Your Progress 2

1) Fill in the blanks:

   a. The model of Windows NT allows you to control many users, groups, and computers by using a boundary known as a _____.

   b. There can be only _____ PDC per domain. But there can be a number of _____ to assist PDC.

   c. Domain model provides for a _____ to all resources.

   d. A domain that trusts another domain is called a _____ domain and the other domain is called _____ domain.

   e. If PDC stops functioning due to hardware failure, one of the BDC can be promoted to _____

   f. PDC provides help in _____ network logons.

2) What are limitations of the domain model?

.....

.....

.....

2) What do you understand by PDC and BDC?

.....

.....

.....

3.4 WINDOWS RESOURCES SECURITY MANAGEMENT

Files and Folders Management

The following paragraphs explain the management of Windows resources. In Windows there are two levels of security, share level and file level. Share level security is for controlling user access to a resource that has been made available to the network, and functions with any file system on the NT machine. File level security is for controlling user access to an individual file locally on a machine, and functions only on the NTFS file system on an NT machine. The share level permissions on a folder (it cannot be set on a file) have four permissions to choose: No Access, Read, Change, and Full Control. This provides power to an administrator to control access to the shared resource from the minimum of No Access, through to the maximum of Full Control.

The share level permission is helpful in many situations, but when you require further control, or wish to secure resources on the local hard drive, you must use file security. The file level security requires that you must use NTFS file system. When permission is set at the file level, the "Everyone group" has Full Control by default.

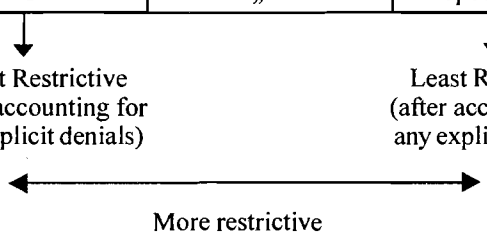
The share level permission could only be applied to a folder; NTFS permissions may be applied to either a folder or a file. Just as you are allowed to set permissions by each user but you can do so by setting the permission for a group to save time and effort, you will normally set permissions by folder, not file, to save time and effort. Setting the file level security one file at a time can take too long on a file server with thousands of files available over the network.

The NTFS file system provides the following permission for resource:

- List - Allows a user to view a field or subdirectory name, but not read the contents of any file or subdirectory.
- No Access - Removes all access rights, and will override any other permission a user may have to this object
- Read - Allows user List permissions, with the added right of reading the contents of a file or subdirectory, and run applications.
- Add - Allows a user the right to add files and subdirectories.
- Read and Add - Allows a user Read permissions, with the added right of adding files and subdirectories to the directory.
- Change - Allows user Read & Add permissions, with the added right of changing data in a file or subdirectory and deleting files and/or subdirectories.
- Full Control - Allows user Change permissions, with the added rights of changing permissions on files and subdirectories and taking ownership of files and Subdirectories.
- Special Access - This permission allows a user to be given access as in *Table 1.*

Table 1 : Assigning Permission for resource

Over the network	**Share permissions**	**NTFS permission local to the machine**	
Access Control List	Corresponding Access Control Entry	Access Control List	Corresponding Access Control Entry
User or Group	No Access	User or Group	No Access
,,		,,	List Holidays
	Read	,,	Add
		,,	Add & Read
		,,	Change
,,	Change	,,	Full Control
,,	Full Control	,,	Special Access



3.5 REGISTRY MANAGEMENT

In older versions of Windows, the Operating System was controlled by multiple files, such as: autoexec.bat, Config.sys, system.ini, and win.ini. In Windows NT, the configuration of the Operating System is stored in what is known as the Registry.

The Registry consists of values, keys, subtree, and hive.

- Values - These contain the information that is stored as part of the Registry. Each value contains three distinct parts: (1) a data type, (2) a name, and (3) a configuration parameter (this contains the actual information).
- Keys (and Sub keys) - These contain the actual Subkeys and values.
- Subtree - These are the highest-level Keys of the Registry. There are five Subtrees in Windows.
- Hive - These are a set of keys, subkeys, and values of the Registry. Each one is stored in its own file in the %systemroot%\System32\Config.

Regedit.exe and regedit32.exe are the two utilities that can be used to manage the REGISTRY. While Regedit.exe provides the ability to view the entire Registry in a single tree, Regedt32.exe on the other hand, allows for managing of individual keys.

3.5.1 Removing Registry Access

The first step to secure Registry is to try to prevent unauthorised users from accessing the Registry. To do this, the operating system files should be installed on an NTFS partition and change the permissions on both the Regedit.exe and the Regedt32.exe so that only members of the Administrators group have Full Control.

3.5.2 Managing Individual Keys

In Registry you can secure individual areas of the Registry as necessary. This option is available in Regedt32.exe which permits you to selectively secure the various keys by using the Security Permissions option. Although the details of securing each key are beyond the scope of this unit, the process is identical to that of securing file resources. You must determine the proper level of access for each key, based on your requirement, and limit permissions accordingly.

3.5.3 Audit Registry Access

After locking down the Registry as per your requirement, you need to make sure that the auditing of critical components of Registry is turned on. This option will help in tracking who accessed the Registry, from where, and when. In order to audit the Registry, the first step is to enable auditing for the computer itself.

The steps for enabling auditing is given below:

1. Logon as Administrators.
2. Go to User Manager for Domains
3. In the Policies menu, select Audit
4. Select Audit These Events to enable these audit choices. Select Failure for the File and Object Access event.
5. Choose OK, and close User Manager for Domains.

There are several options, but for the minimum of registry audits, the Failure for the File and Object Access event is all that is required. Once auditing is turned on for the system itself, you can enable auditing of the Registry. The steps for enabling the auditing registry access is given below:

Steps for enabling the auditing of Registry Access:

1. Log as Administrator
2. Run Regedt32.exe

3. Select the '\Hkey_Local_Machine' Tree

4. Select the Security, Auditing menu option.

5. Add the specific users and/or groups you wish to audit.

6. Choose OK once you have selected all the users and/or groups you wish to add, and confirm your selection.

Some of the Audit events you may wish to use are listed below:

- Write DAC - This audit logs events that try to determine who has access to the key.
- Read Control — This audit logs events that try to determine the owner of a key.
- Delete - This audit logs events that try to delete a key from the Registry.

If you select auditing on all keys for all users this may result in performance hit on the system as it tries to track all these events. Therefore, you should only audit the events you specifically wish to audit. You may view the audited events in the Event Viewer under the Security Log. Events that are audited in the Registry will identify the user, computer, and the event that was audited.

3.6 PRINTER MANAGEMENT

Managing files and folders properly on a Windows machine is just the beginning of setting up the computer's security. Another aspect of computer security is printer management. In Microsoft terminology the printer is a software component, and the hardware device is called the print device. This section will cover this software component in the computer.

Printer permissions are generally overlooked, but in fact it should be taken seriously. If someone has recently purchased an expensive colour laser print device, it should not be used for general print jobs. Print resources are generally the most misused resources in an organisation.

The following four permissions can be set for printers in Windows environment : access, (2) print, (3) manage documents, and (4) full control.

1. No Access -User cannot print to this device or connect to its print queue.

2. Print -User can print documents and manage submitted print jobs, if the owner of those jobs.

3. Manage Documents - Allows a user to manage print jobs, including pausing, restarting, resuming, and deleting queued documents.

4. Full Control -Allows a user to create, manage, and delete printers, as well as all the control of the Manage Documents permission.

The location of the print spooler should not be overlocked. If print documents are sent to the hard drive for processing, and are waiting to be printed, the security of those locations is a big issue. By default this location is in the % systemroot%/systeni32/ spoool folder and, by default that folder has a permission of Everyone Full Control. So, if you have resources that are secured on an NTFS partition, and they are spooled to a FAT folder with lax security, this may become a security breach. You can modify the security spooler location by using "advanced tab" of print server properties.

3.7 MANAGING WINDOWS 2000 OPERATING SYSTEM

In the sub-section we will focus on how to manage windows operating system.

3.7.1 Windows 2000 Features

In Windows 2000 you can create workgroup for multiple to share resources with one another. The workgroup is referred to as peer-to-peer networking, since every machine is equal.

In Windows 2000, a local security database is a list of authorised user accounts and resource access data located on each local computer.

The major advancement in the design of a Windows 2000 is new domain model instead of multiple models of Windows NT 4.0. In this ne new model you still group computers together, but they are controlled differently. In a Windows 2000 domain, you group together computers who share a central directory database. This directory database contains user accounts, security information, service information, and more for the entire domain. Active Directory information includes how each object will interact with other objects in the directory. The Active Directory may start out as a small listing and grow to hold thousands to millions of object listings. This directory forms the database for Active Directory and Active Directory is then known as the Window 2000 directory service. In Active Directory no machine is designated as PDC or BDC instead every system is simply called a Domain Controller. In addition to the information mentioned earlier, the Active Directory holds the information regarding access control. When a user logs on to the network, s/he is authenticated by information that has been stored in the Active Directory. When a user attempts to access an object, the information required to authorise such access is also stored in the Active Directory, and is called the Discretionary Access Control List (DACL). Active Directory objects themselves can be organised into what are known as classes. Classes represent a logical grouping of objects at the discretion of the administrator. Object class examples are: user accounts, computers, omams, groups, an organisation Units (OUs). You also have the ability to create containers, which can hold other objects. Windows 2000 domain is not bounded by location or network configuration, it may be with in a LAN or far apart over a WAN.

3.8 ACTIVE DIRECTORY

Active Directory contains several critical components; these components are logical in nature and have no boundaries. These components are domains, forests, trees, and organisational units (OU). The components of Active Directory that are more physical in nature are the domain controllers and sites, the physical IP subnets of the network. The functionality of Active Directory separates the logical from the physical network structure.

3.8.1 Logical Structure

Active Directory has the ability to build a logical network that mirrors the logical structure of the organisation. As logical structure is more intuitive to users they are able to find and identify resources by logical name, without having to have any knowledge of the physical layout of the network.

The main component behind the structure of Active Directory is the Domain. Active Directory consists of at least, but not limited to, one domain. Microsoft has termed the objects stored inside a domain as interesting objects. These interesting objects are defined as those objects which a user requires in the course of doing their job function. Examples of interesting objects could be printers, databases, email addresses, other

users, and more. Each domain holds information about all the objects in the domain, and only those objects that belong to the domain. Domains are allowed to span one or more physical locations.

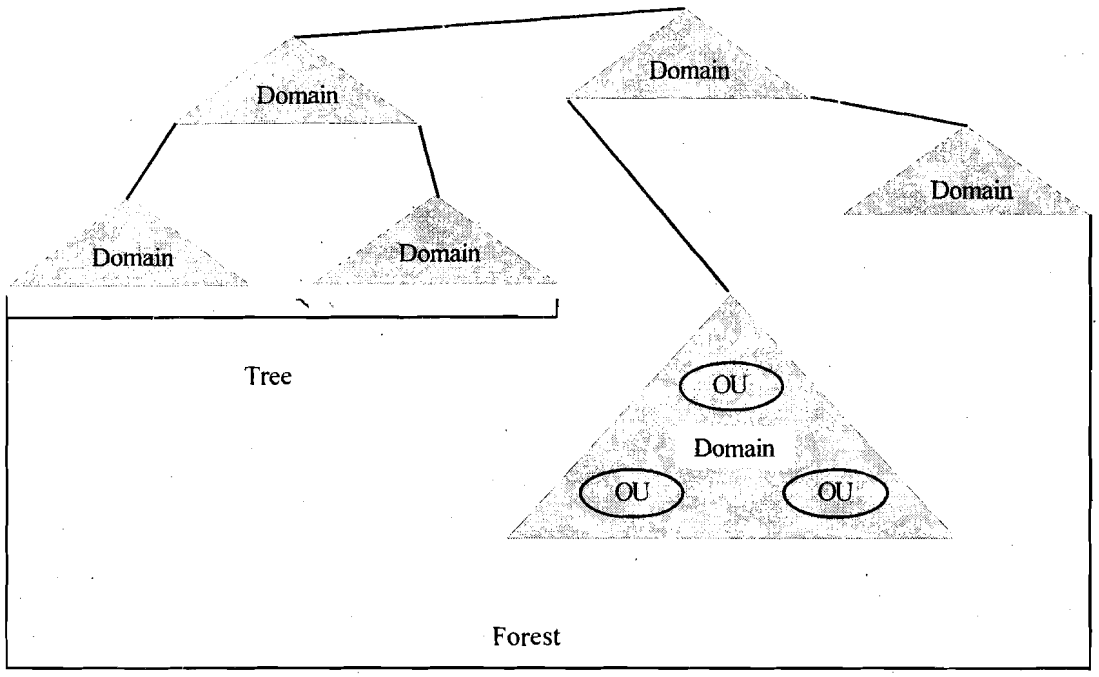


Figure 5 : Logical network layout of a Windows 2000 Active Directory

The domain is used as a boundary by which security controls can be implemented. The Access Control List (ACL) is used to regulate specific access to domain objects, such as shared folders, for defined users. The ACL contains the permissions that are used to grant or deny access for an object, such as a user or group to another object, such as a file, folder, or printer. In the domain it can be called Organisational Units or OUs. An OU is a local holder that is used to further mirror the logical structure of the organisation. An au can contain users, groups, files, folders, printers, and even other OUs from the same domain. Every domain in the network can have a unique OU configuration; as there is no dependency on other domains. Permissions can be granted to an OU as desired. It is possible to assign permissions to each OU, but not required. If there is a permission that you wish all OUs to use in the network, you may assign it to the parent OU of the domain, as the default structure is to allow child objects to inherit permissions from their parent within the Active Directory.

A new concept in Windows 2000 is that of forests and trees *(Figure* 5). A tree is a logical structure created by the network design team of one or more Windows 2000 domains that share a name space. The domains fall in a hierarchical structure and follow the DNS naming standards. A forest in the Windows 2000 Active Directory structure is a collection of completely independent domain trees. These independent trees are tied together with a trust. Each tree in the forest maintains its DNS name system, and there is no requirement for any similar namespace from one tree to another. Each domain functions on its own, but the logical connection of the forest enables organisation wide communication on the network. The implementation of Trust in a Windows 2000 Active Directory network is different from Windows NT 4.0. In Windows 2000 all trusts between domains are called two-way transitive trusts. These trusts, based on Kerberos v5 (a security technique) are created automatically when a new domain is added to the tree. The domain that started the tree is considered the root domain, and each subsequent domain's root will form a Two-Way Transitive trust upon joining.

In the event that older Windows machines are on the network, such as a Windows NT 4.0 machine, a specific trust can be created. This is called an explicit one-way trust such as and it is non-transitive and in this way a Windows 2000 network, running Active Directory, can have communications with an older Windows NT 4.0 Domain. You also have the option of manually creating trusts such as this, so as to connect two Windows 2000 domains that are far down the trees of different forests to improve ? communication speed.

3.8.2 Physical Structure

The majority of the design and implementation of the Active Directory network is on the logical side, but the physical side must be equally addressed. The main components ? of the physical side of Active Directory are sites and the domain controllers.

The site, as defined by Microsoft, "is a combination of one or more Internet Protocol (IP) subnets connected by a highly reliable and fast link to localise as much network traffic as possible." A fast link is reached when the connection speed is at least 512 Kbps. Therefore, the Site is designed to mirror the physical structure of a network, and mayor may not be made up of different IP subnets.

Remember that the domain is designed to mirror the logical needs of the network, and apply that same logic to designing a network using physical aspects. There is no correlation between the site and the domain. It is possible to have multiple domains in a Site, and it is possible to have multiple sites for one domain. A site is also not part of the DNS namespace, which means that when browsing/exploring the directory, you will see user and computer accounts managed by domain and/or OU, but not by site. A site contains only computer objects, and objects relevant to the connection and replication from one site to another.

The other physical component of Active Directory is the actual Domain Controllers (DC) and these machines, which must be running Windows 2000 Server, each have an exact replica of the domain directory. When a change is made on a DC that has an effect on the Active Directory, all other DCs will receive this replicated change. Because any domain controller can authenticate a user to the network, each controller is required to have this directory. Therefore, each DC stores a copy of Active Directory information that is relevant to that domain. Each DC replicates changes, at admin-defined intervals, to all the other DCs to ensure a consistent view of the network at all time? Each DC replicates critical changes to all the other DCs immediately and each DC is able to authenticate user logon requests.

3.9 WINDOWS 2000 DNS MANAGEMENT

For the Active Directory to function, DNS must be running for the network. The implementation of the; DNS namespace will form the foundation on which the Active Directory namespace is created.

A new feature of Windows 2000 is Dynamic DNS (DDNS) which allows clients to receive their IP addresses automatically via a DHCP server and registered with the network. With a DDNS server, the client's machine will automatically communicate with the server, announcing its name and address combination, and will update its DNS information without user information. The advantages of running DNS in a network is the ability to eliminate other protocols and services that may be running to locate resources. For example, the Windows Internet Name Service (WINS) of Windows NT 4.0 is not required, and the use of Net BEUI (Net BIOS Extended User Inferface) as a communication protocol is no longer required.

3.10 MANAGING GROUP POLICY

The final component of the Windows 2000 infrastructur is group policy. A group policy is a logical grouping of user and computer settings that can be inter-connected to computers, domains, OUs, and sites in order to manage a user's desktop environment. For example, a Group Policy is a method of removing objects from the Start Menu.

Group policy consists of GPO (Group Policy Object) and the GPO is then responsible for controlling the application of the policy to Active Directory objects. Once a GPO is configured, it is applied to the AD (Active Directory) object as assigned, and by default the policy will affect all the computers that are in the AD object. The policy can be implemented on all the computers or apply filter how the policy will be implemented for computers and us"ers. The filtering will use Access Control Lists (ACLs), as prepared by you.

Some of the rules for applying a GPO are as follows: a GPO may be associated with more than one domain, a GPO may be associated with more than one OU, A domain may be associated with more than one GPO, and an OU may be associated with more than one GPO. In this section, you have noticed that you are allowed the maximum flexibility in GPO Implememanon. However, Derore getting mto me Implememanon, you must take a step back and look into the GPO itself in more detail.

Policies Options

To configure a GPO open Group Policy Editor via the Microsoft Management Console (MMC). In Group Policy Editor you are provided two options; Users Setting, and Computer Setting. In this you will be able to create the GPO as per your requirements.

In the Computer Settings directory you have the option to manage the behaviour of the a operating system, account policies, IP security policies, etc. The options will be effective once the computer gets restarted.)

The User Settings directory gives the option to manage behaviour that is unique to the user, such as Desktop settings, Control Panel settings, Start Menu settings, etc. These options will be effective once the user logs on to the computer.

Once you create and edit a GPO, it must be enforced to have any impact on the .network and there can be GPOs on Sites, Domains, and OUs. The order of implementation is critical to proper GPO deployment.

The first GPO that is processed is the called Local GPO. Every Windows 2000 computer has a GPO stored locally. However, it is not practical to implement custom configurations on each machine in the network, so often administrators move right past the Local GPO.

After the processing of the Local GPO, the Site GPO is implemented. Since there can be multiple GPOs for one site, it is the administrator's job to deflne the order of .implementation by configuring the Site Properties. After processing the Site GPO, the .Domain GPO is implemented. Just as there can be multiple GPOs for a Site, there can be multiple GPOs for a Domain, so the administrator must take care to define the order .of implementation in this case also.

The last GPO to be processed is the OU. As in the other implementations, more than one GPO may be present for the OU, and as such the administrator is required 10 of; properly plan and implement the GPOs as per the requirements.

In every section with more than one GPO, the place to make the modifications to the order is in the properties of the Site, Domain, or OU (the only exception being the Local GPO). When in the properties of the Site, for example, the GPOs are listed, and the option to move them up or down is present, the system will process the GPOs with the highest on the list having the highest priority, taking precedence over GPOs that are lower down on the list.

The implementation order of the GPOs is critical for the security and management of a Windows 2000 network. By seeing at the implementation order, you can identify that if a Site GPO were to define a password age of 45 days, and a Domain GPO were to define a password age of 30 days, that the final password age would be 30 days, as that GPO was processed last.

☞ **Check Your Progress 3**

1) What is Active Directory?

.....

.....

.....

2) How will you secure guest account?

.....

... .

.....

3) What do you understand by Windows 2000 DNS?

.....

.....

.....

3.11 SUMMARY

This unit describes the broad concepts of Windows Architecture Management and security related issues: Main Issues in Windows Security Management; Windows Resource Management; Windows 2000 Operating Systems. Windows Security specially focuses on Windows NT Management and it covers the areas such as physical security management, logon management, user/groups management, Windows NT domain management, domain controllers. Windows resource management includes areas like: files and folder management, files/folder permissions, printer management, and Registry management. Further, the unit also discusses about the improvement that has been taken up in Windows Architecture, Management with the Management Windows 2000 operating system; Windows 2000 features, active directory, logical structure, physical structure, Windows 2000 DNS management, Group Policy etc. This unit provides detailed concepts and configuration required for management of Microsoft Windows computers and you will be able to examine everything from the foundational principles of Windows NT Management, up to the advanced issues of securing Windows 2000 machines running Active Directory.

3.12 SOLUTIONS/ ANSWERS

Check Your Progress 1

1) • Creating a Logon Warning Message

• In the run option, type Regedit to open the Registry editor.

- In the Registry Editor navigate to:

  HKEY _LOCAL_MACHINE\SOFTW ARE\Microsoft\ WindowsNT\ CurrentV ersion\ Winlogo.5

- Double-click the LegalNoticeCaption value.
- In the Value Data entry field, Type Unauthorised Access Warning!! Then press OK.
- Double-click the LegalNoticeText value.
- Type in the Value Data Entry Field.

  "Unauthorised access to this system is punishable by a fme of Rs 10,000 and / or on , year of imprisonment. Use of this system indicates that you have read and agree to this warning". Press OK.

- Close the Registry Editor.
- Log off and verify the changes :
- Disabling the Last Usemame option
- In the run box. type Regedit to open the Registry Editor.
- Navigate to

  HKEY _LOCAL_MACHINE\SOFTW ARE\Mlcrosoft\ Windows NT\Current Version\Winlogon.

- From the drop-down menus choose Edit> New> String Value.
- Type DontDisplayLastUsemame in the Name Field.
- Double-click on your new string.
- Type 1 in the Value Data entry field, and press OK to close the Edit dialog box.
- Close the Registry Editor.

Check Your Progress 2

1) a) Domain, (b) one, BDC (c) Single Sign On (SSO), (d) TRUSTING, TRUSTED, (e) PDC, (f) authenticating.

2) a) A very large domain would be hard to manage lefficiently, and (b) users who are very far apart physically may find a more efficien\ .network experience to have one domain per location.

3) Primary domain controller and Secondary Domain Controller.

Check Your Progress 3

1) You group together computers who share a central directory database. This directory database contains user accounts, security information, service information, and more for the entire domain.

2) The guest account can be lock down by the following steps:

   - Rename the guest account to a difficult to-guess account name.
   - Remove the guest account description.
   - Set a very complex 14-character password.
   - Change logon hours to never.
   - Change the logon to option to a Workstation that is not active.

3) Windows 2000 is Dynamic DNS (DDNS) and DDNS allows clients, which receive their IP addresses automatically via a DHCP server to have their name IP address registered with the network.

3.13 FURTHER READINGS

1. *Cryptography and Network Security, Principles and Practice,* William Stallings - SE,PE.

2. *Security in Computer,* Charles P. Pfleeger and Shari Lawrence Pfleeger, Third Edition, Pearson Education.

3. *Windows 2000 Commands* by Aleen Frisch.

4. Microsoft Web Site ht!l1://www.microsoft.com.