UNIT 1 CONFIGURING INTRANET

Structure **Page Nos.**

1.0 INTRODUCTION

The next step in setting up an Intranet is to configure it, that is, how to create and host the Web pages and steps to secure the network. There are different types of Web page authoring tools for content creation. Managing the users and granting permission and restriction to them is also an important part of Intranet administration.

The next part of this Unit deals with discovering the vulnerabilities on network. Unfortunately, there are several ways in which a network can be compromised, and the first step towards finding a better solution is to look around the organisation and see how much exposure the organisation can withstand.

1.1 OBJECTIVES

After going through this Unit, you will be able to:

- know the tools for authoring Intranet;
- understand user management issues;
- manage hosting on the Intranet;
- understand Permission and restriction issues;
- understand Network security issues, and
- know the tuning application on Intranet.

1.2 CONFIGURING WEB SERVER

The first step of setting up an Intranet is to configure a Web server. Many Web servers are available. Some of them are commercial and some are free. One of the popular Web servers is Apache. The current version of Apache Web server is 1.3.3-x. It is available free with Red Hat Linux 5.2, and can also be downloaded from *http://www.apache.org*. It sets up and gets ready to run automatically at boot as soon as the Linux installation is completed. The Apache Web server is extremely powerful, and can be configured to handle any kind of environment from a lightly loaded

Intranet to a commercial heavily loaded Internet Web server taking more than 100,000 hits a day.

It is very simple to test the working of the Apache Web server. Simply point the browser to the URL *http://localhost*. The Apache's default "It Worked" page starts up. The *index.html* file in the */home/httpd/html* directory can be changed to start publishing pages on the Intranet. The default configuration file */etc/httpd/conf/httpd.conf* is suitable for simple configurations, though one might want to edit it if there is an unusually heavy load, or wish to configure a different machine name, port, or address to send error messages.

Web Authoring Preview

All that is needed to author a Web page is a word processor, plus attention to detail, common sense and a computer to serve the page where others can access it with Web browsers. Web page can be in any word processing or text editing program. Using a word processor requires knowledge of Web page programming language HTML. Use of software, designed specifically for Web authoring, eliminates the need to know HTML language and makes the creation of a Web site as simple as typing on a word processor. Newer word processors (e.g., MS Word) can even export formatted text to HTML.

Many Web page editing programs also provide for basic editing and placement of graphics and have built-in file transfer protocols to upload Web pages to the server. Web pages consist of text marked with HTML tags that give a Web browser guidelines for how to display or align text and how to link text or graphics to another file on the Internet. For example, to emphasize something, enclose the required text in a pair of tags, such as: <B>. This is a demo text line!!!! It!</B>. A Web browser will then show This is a demo text line!!!! in boldface type, in this example, to make it stand out visually. Attention to detail counts, because HTML tags are picky, and typographical errors can be highly embarrassing even on simple pages.

It is important to see what the Web site looks like on many different browsers and computers, and then edit it appropriately. It is also important to name graphics for people with browsers that cannot view them.

1.2.1 Web Graphics

Most of today's Web browsers support two graphic formats: GIF and JPEG. Both formats use internal compression routines that make the graphics smaller, thus decreasing download times. When it is decided to put a graphic on the Web, it is important to decide whether to use GIF or JPEG.

GIF Versus JPEG: GIF stands for Graphics Interchange Format. It is the only format that all graphics-savvy browsers can display, so it is the format to be used for graphics that is to be seen by everyone. The bad part about GIF graphics is that they are limited to 256 colours and typically do not compress as well as JPEG graphics do. The latest version of the GIF specification (version 89a) supports transparent mode, a nifty option that makes one colour in a graphic transparent. GIF's are shaped like rectangles. To make a GIF's background colour transparent, one can end up with a GIF that looks like an irregularly shaped object.

GIF

GIFs also can be interlaced, that is the image is saved in alternating horizontal bands. Looking at the first half of an interlaced GIF, one would see a low-resolution, striped image, with blank horizontal stripes representing the second half of the image. Some browsers display interlaced GIFs as they read them, first they display every eighth line, then every fourth line, then every second line and then every line. This display method makes the people, waiting for the image to load, to quickly figure out what the final image would look like.

Other browsers bring in a rough version of the graphic and gradually refine it. GIFs also support animation. It is possible to piece together numerous GIFs and create a simple movie.

JPEG

JPEG stands for Joint Photographic Experts Group. It is a graphics compression format that works best for digitized photographs, particularly if they depict photos of natural scenes such as forests or sunsets. JPEG was designed to lose details that the human eye often will not notice, particularly details that would not be noticed from an image with gradual changes in shading and colour. JPEG is most likely to lose too much detail with images that have sudden transitions from one colour to another, so JPEG tends to be a poor format for graphics containing text, line drawings and navigational icons. JPEG images can have millions of colours instead of a just 256. They have better compression, but many older browsers cannot display them without the assistance of a helper application (where the picture displays in a different program's window).

The bottom line: Use of GIF should be made unless one has a photograph requiring very fine details to be exhibited.

1.2.2 Adding Interactivity

Once the construction of basics like text, hypertext links and graphics are over, interactive additions such as image maps, sound, video, search capability, database retrieval, forms and even encryption security is desirable depending on the type of requirement. These advanced functionalities require the help of technologies such as Java programming, Common Gateway Interface (CGI) scripting or the addition of plug-ins. They usually require additions to and modifications of the server software. Such a discussion is beyond the scope of this topic.

Hosting Web Pages on the Internet

Organisations that will host the Web pages can be asked from the Internet Service Provider (ISP) or system administrator. Another option to serve the Web pages is dedicating a computer to run Web server software. The advantage of a dedicated computer is the personal control of Web server software. This option requires a dedicated Internet connection. Some ISPs also provide an option to keep the Web server computer at their site for a direct Internet connection. This usually requires remote control software or many trips to the ISP. Personal server software is becoming popular for small-scale Web sites on office computers with a dedicated Internet connection.

After finding an organisation that will serve the Web pages or choosing own Web server software, some questions can be asked:

1. *What kind of file name extensions are used?* The Web is very particular about file names, the file names must end with an extension that indicates the file type. For example, a Web page coded in HTML needs an .htm or .html extension. The specific extension and the length of the file names depend on the server that serves the files. The beginning Web page may need to be called homepage.html, default.html or index.html depending on the server software.
2. *How to updates pages?* This is usually accomplished by using file transfer protocol (ftp) to transport all the html documents and graphics files to a specific directory on the server. FTP access to the server along with a password is required for this.

HTML code is easily downloaded for review. It is also possible that if some Web site technique that is of interest can be simply saved as HTML from its code. This will provide special techniques that are used in developing own Web pages. Web site graphics are also easily downloaded as HTML files but there is a need to consider infringement of copyright laws, if any, before incorporating them into own Web site.

1.3 INSTALLATION

In order to connect to the Internet or to set up an Intranet, one should plan and layout the physical network, which include the following steps:

- Designing topography
- Planning the connectivity or wiring
- Installing routers and hubs
- Setting up servers
- Establishing security measures such as implementation of firewalls
- Selection and connecting to an ISP.

1.3.1 User Management

In user management Administration, we need to install and configure different issues like user authentication, logon activities and permission, account management, file permission & sharing. In this Section, let us discuss these issues in detail:

Authentication

Authentication is a process that is performed by the system automatically to ensure that the user is genuine. Authentication may be done at a local computer or at a global level for a domain using domain controllers across the network. Windows 2000 supports the following types of authentication:

- Kerberos V5: An Internet standard authentication protocol which is the default protocol for Windows 2000 computers within a domain.
- Windows NT LAN Manager (NTLM): Used to authenticate users from Windows 95, 98, and NT systems. Windows 2000 Active Directory must be operating in mixed mode to use this authentication method.
- Secure Sockets Layer/Transport Layer Security (SSL/TLS): Requires certificate servers and is used to authenticate users that are logging onto secure Web sites.
- Smart card: Contains a chip with information about the user along with the user's private key. A Personal Identification Number (PIN) is normally required for authenticating using a smart card. It requires Extensible Authentication Protocol (EAP) to be enabled for the server to allow smart card authentication. Also some certificate authority must provide keys.

Authentication uses X.509 standard and kerberos.

Process of Logging On

1. As the first step the Ctrl+Alt+Del key combination has been pressed, name and password entered, and local or domain logon is indicated.
2. If the logon is local, the name and password are checked against the local database. If the logon is a domain logon, the name and password are encrypted into a key, and timestamp information is encrypted. This information is sent to the Windows 2000 domain controller with an authentication request.
3. The domain controller decrypts the information and checks for a valid timestamp. If the timestamp is valid, two Kerberos tickets are made and encrypted with the password. The tickets are sent back to the client computer. The tickets are:
    - User session key - Used to log on.
    - User ticket - Used to get other Kerberos tickets for accessing other domain resources.
4. The client decrypts the tickets and uses the session key to log on.

Shares used for logon

NETLOGON/SYSVOL - The Netlogon share is used on Windows NT domain controllers to authenticate users. In Windows 2000, the SYSVOL share carries out these functions. The SYSVOL share includes group policy information which is replicated to all local domain controllers.

Accounts

Accounts defines the actions and permissions, a user can perform in an operating system. As you know there are different types of accounts like administration, guest, etc. Let us discuss about different account types and different user properties in this Section.

Built-In Accounts

The following accounts are created when any Windows 2000 system is installed. These accounts are also created on domain controllers automatically when Active Directory is installed.

- Administrator: Cannot be deleted or disabled and should be renamed.
- Guest - Disabled by default. A password is not required. This account can't be deleted but can be renamed, and should be disabled.

Account Types

- Local : For local computer access.
- Domain : For access to network resources in the domain.

Administrators and power users can create and modify accounts in the domain. Administrators on local computers can create and modify accounts locally. The Windows Scripting Host (WSH) assists administrators in creating many users and groups quickly.

User Properties

In addition to the usage, it is essential to note the following for smooth operation:

- Username - A unique name up to 20 characters excluding:
  " / \ [ ] : ; | , + * ? < >\
- The username may be changed after it is created. Choose a naming convention for large organisations.
- Password - Case sensitive and up to 14 characters.
- User must change password at next logon.
- User accounts can be renamed.

Account Creation and Modification

- Local account: Use the "Local Users and Groups" tool.
  - Right click "My Computer", select "Manage".
  - Click the + next to "Local Users and Groups" in the "Computer Management" box.
  - Enter user information into the "New User" dialog box.

To modify the user properties, right click on the user and select "Properties". User Property tabs include:

- General - Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.
- Member of - Set up local groups the user is a member of.
- Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. The profile includes desktop settings.
- Dial-in (Only on Server computers) - Set remote access permission, callback policy, and IP address and routing information.
- Remote account - Use the "Active Directory Users and Computers" tool.

1. From the Active Directory Users and Computers tool click + next to the domain name.
2. Highlight the “Users” folder and select “Action”, “New”, and “User”.
3. Enter user information into the “New User” dialog box.

To modify the user properties, right click on the user and select "Properties". User Property tabs include:
General: Set up when user must change password (User must change password at next login, User cannot change password, or password never expires) and disable the account here. Indication of account lockout is here.

- Address: Set mail address or physical address information.
- Account: Set hours that the user can logon during and restrict computers the user can use. The following operations are possible:
  - User must change password at next login
  - User cannot change password
  - Password never expires
  - Store password using reversible encryption.
  - Account is disabled
  - Smart card is required for interactive logon
  - Account is trusted for delegation - The user can delegate authority for their privileges or rights to other users.
  - Account is sensitive and cannot be delegated.
  - Use DES encryption types for this account.
  - Do not require Kerberos preauthentication - For systems supporting Kerberos but not preauthorisation.
  - Indication of account lockout is here.
  - Can set when account expires.
- Profile - Set up the environment variables, set a network path to the user profile folder and user home folder. A logon script file can be set. Domain user logon scripts are in the NETLOGON share on the domain controller in the SystemRoot\SYSVOL\sysvol\domainname\SCRIPTS folder. The profile includes desktop settings. Default profile file location is C:\Documents and Settings\username on the computer that the user logged on to.
- Other aspects such as Telephones, mobile, fax phone numbers, etc. and about the organisation consisting of the user title, department, manager, and company could be entered.
- Member Of - Used to assign users to groups and remove users from groups.
- Dial-In - Dial-In privileges can be granted or denied and callback options are set here.
- Published Certificates - Can add or remove user internet certificates.
- Object - View information about the user account object such as when the account was modified last.
- Security - Can set users and groups that can modify this domain user account properties.

The “NET USER” command line tool may be used to create users when used with a batch file.

Permissions

The permissions on Windows 2000 systems are all selectable with two boxes, which are:

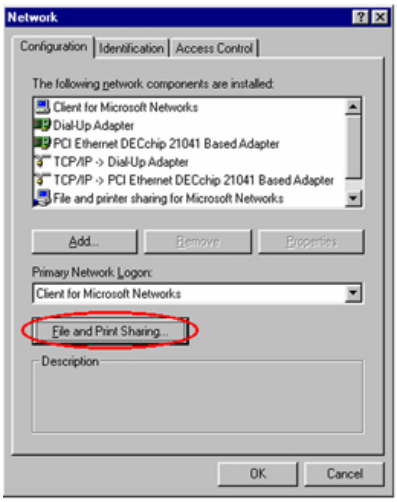
- Allow - Grant the permission.
- Deny - Any denied permission for a group or user will override any allowed permission, even if the user is in a group that has granted that permission.

If neither box is checked, the permission is not granted for the user or group, but if the user is in another group that has the permission, it will not be denied. Normally, if a

user is a member of several groups that have different levels of permissions to an object, the least restrictive permissions apply unless the user, or one of their groups, has the no access box checked for that permission.

Standard File and Folder Permissions

- Read (R) : View attributes, contents, and permissions. Can synchronize.
- Write (W): Can change attributes, and file contents. Can create files or folders. Can synchronize.
- Read (R) and Execute (E): Can change sub folders, perform read operations, and execute a file.
- List Folder Contents : Can perform read and execute permissions on folders. Can view folder contents, attributes, and permissions. Can synchronize and change to subfolders.
- Modify: Perform Read, Execute, and Write permissions along with ability to delete.
- Full Control : Can perform Modify functions (above), take ownership, and modify permissions.



Window NT file sharing option

Permissions assigned to directories are inherited (default) by all files and subdirectories that are contained in the directory. The inheritance option, selected by default, may be deselected. Each file or directory has an Access Control List (ACL). To set permissions for additional users or groups, they are added to the ACL of the file or directory. Windows Explorer or the Cacls command line utility can be used to set permissions.

NTFS File and Share Permissions

When these permissions are different, the most restrictive permissions are applied. The share and NTFS file permissions must overlap in order for the user to have the permission. That means to read a file, the user must have both read share and read NTFS permission.

When a user has full control permission for a folder, the permissions will apply to the files in the folder even though permission for an individual file in the folder may be set to NO ACCESS for that user. When a file or folder is moved, it retains its current permissions, but when it is copied, it inherits the permission of the parent folder or partition it is being copied to.

Ownership

If the owner's user is a member of the administrators group, the owner is the administrators group. Administrators do not have access to all resources, but they may take ownership of any resource. Once ownership is taken, it cannot be given back. Also taking ownership of resources changes all existing permissions for that resource.

Delegated Permissions

Permissions that can be delegated include:

- Create, delete, and manage user groups.
- Create, delete, and manage user accounts.
- Manage group policy links - Group policies assigned by organisational Unit may be modified.
- Modify group membership.
- Read all user information.
- Read user account passwords.

Setting Permissions

1. Right click on the file or folder.
2. Select properties
3. Select the security tab on the properties sheet.
4. Click on the permissions button.

5. If the file selected is a subdirectory there are the following check box choices:
    - Replace permissions on subdirectories: Permission changes are applied to all sub folders.
    - Replace permissions on existing files: Permissions are applied to all files in the folder. If both are selected, permissions are applied to all sub folders and files in all files in the folder and its sub folders.
6. Click on OK to exit the permissions box and OK to exit the properties box.

1.3.2 Disk Quotas

Disk quotas are used to track the use of disk space for each user. They are normally disabled and are only supported on NTFS file systems. Quotas are tracked per partition and per user using ownership information to account for resource use. Compressed file sizes are measured according to the uncompressed file size.

Disk quotas may be viewed and administered by using the "Disk Management" tool to select the properties dialog box of the disk or volume. The "Quota" tab contains quota information and management functions. Quota management must be enabled.

Warning levels may be set and hard limits may also be set. Disk space may be denied to users who exceed their quota limit. The events may be logged when the user exceeds their warning and/or quota limit.

Windows Explorer can be used to set up and monitor disk quotas. The following options are available in Windows Explorer under local disk properties.

- General
- Tools
- Hardware
- Sharing
- Security
- Quota: Used to enable quota management, deny disk space if the quota is exceeded, limit the disk space and set where the disk quota warning is given. The user can also log when the warning level or quota level has been exceeded. The "Quota Entries" selection box is used to view quota utilisation for the volume. To modify the quota levels for any given user, double click the user's entry.
- Web Sharing.

User Rights

User rights are different from access permissions, which allow access to resources such as, read, write or execute. User rights allow system control, which includes the ability to format a hard drive or shut the system down.

Local Users created at installation time

1. Administrators : Used to administer the system. Making a backup of the 'administrator' user would be highly useful during critical situations.
2. Guests : Have minimal privileges. It can be renamed, but cannot be deleted. On NT workstation, disable the guest account or give it a password, since it is enabled upon installation.
3. Initial User - Member of administrators group.

Two levels of security

- Logon
- User Rights.

Adding Accounts

The "Local Users and Groups" tool is used to create user and group accounts locally and the "Active Directory Users and Computers" tool is used to create users remotely.

They are also used to manage functional user rights, security auditing, and account policies. Functional user rights determine what programs the user can run or what system capabilities they have. Passwords are case sensitive, but user names are not. Both can contain spaces.

Two methods of adding user accounts:

- Creation
- Make a copy of an existing account.

When an account is copied from a template the following fields are left blank:

- Username
- Full Name
- Password and confirm password
- User cannot change password
- Account disabled.

User accounts should not be made local on various workstations when using domain user accounts. If a user account is deleted, when it is recreated, even though it may have the same name, it will have a different user ID number and resource access for that account must be set up again.

Passwords are case sensitive and can be up to 14 characters. User names are not case sensitive and can be up to 20 characters. The user's home directory can be specified when the user is created or set later. The home directory is where data from an application is saved by default and where the command prompt will be when a command line session is begun.

User rights are divided into:

- Logon rights
- User privileges.

Setting User Rights

- Organisational Units: In Administrative Tools, select "Active Directory Users and Computers".
- Domain: In Administrative Tools, select "Domain Security Policy". The ADMINPAK must be installed on the computer.
- Domain Controllers : In Administrative Tools, select "Domain Controller Security Policy". The ADMINPAK must be installed on the computer.
- Local Computers: From the Control Panel, "Administrative Tools" applet, double click "Local Security Policy".

Domain controllers do not have a power users group. On the Domain Controllers, Server Operators are similar to the Administrator group on the Workstation with all rights.

1.3.3 Security Configuration and Analysis

The "Security Configuration and Analysis" tool is used to analyze a computer security configuration. To get ready to use this tool, do the following:

- The MMC "Security Templates" snap-in must be previously installed. Once installed, it is the administrative tool called "Security Console".
- The MMC "Security Configuration and Analysis" snap-in must be installed to the "Security Console" by starting it from "Administrative Tools", selecting "Console" and "Add/Remove snap-in".
- A database in the snap-in must be created by selecting "Administrative Tools", "Security Console", select "Action", and "Open database".
- To perform the analysis against a template, open a database, and then select "Action", and "Analyze Computer Now".

- To apply settings from a template, open a database that has the settings users intend to apply to the computer, then select “Action”, and “Configure Computer Now”.

User Profiles

The user’s profile allows the user’s environment to be configured. The User Manager administration tool allows user profiles to be modified when “user properties”, then “profile”are selected. The user profile contains:

- Desktop settings: screen colours, wallpaper, screen saver
- Persistent network and printer connections
- Mouse settings and cursor settings
- Recently edited documents.
- Start-up programs, shortcuts, and personal groups
- Settings for Windows applications: Notepad, Paint, Windows Explorer, Calculator, Clock, and more.
- Start menu settings : Programs that can be selected from the start menu.

The user profile settings are saved on disk. They are loaded when the user logs on. There are two profile types:

- Local profile: Stored in the C:\Documents and Settings\username folder. The profiles file is NTUSER.DAT in the directory called by the user’s name. A mandatory profile which discards any changes the user makes to their profile at logoff time, can be implemented by modifying the name of the user profile file from NTUSER.DAT to NTUSER.MAN. The ntuser.ini file is used to set up the user roaming profile components that are not copied to the server. The ntuser.dat. LOG file is used for NTUSER.DAT file recovery in the case of an error. Additional folders in the C:\Documents and Settings\username folder are:
  - Application Data : Refers to data used by application programs that the user may modify when they change a setting in the application.
  - Cookies
  - Desktop : Refers to desktop and briefcase shortcuts.
  - Favorites: Application favourites such as Web site favourites on IE and favorite programs.
  - FrontPageTempdir : Only on Windows 2000 Servers for files made by Microsoft FrontPage
  - Local Settings: Settings used by applications such as IE.
  - My Documents
  - NetHood: Network servers or shared network folder shortcuts.
  - PrintHood: Network printers.
  - Recent : Shortcuts to documents recently used.
  - SendTo : Shortcuts to places where files are copied.
  - Start Menu: The user’s start menu and shortcuts.
  - Templates: Application templates.
- Roaming - Stored on an NT server and downloaded to the computer that the user logs onto. This way the same user’s profile can be available on any machine.

Profile Creation

- For local users : If no user profile exists when the user logs on, the contents of the Default User profile folder are copied to the C:\Documents and Settings\username folder.
- For domain users : The NETLOGON share on the domain controller is checked for a default user profile. If one does not exist, it copies the contents of the local Default User profile folder to the local computer NETLOGON\username directory.

The default user settings are used to create a new user's profile when the new user logs on for the first time. The administrator may modify the contents of the Default User profile directory to change the settings for first time users of the system. The Control Panel, System applet is used to copy user profiles. The "User Profiles" tab is used. The System applet is also used to delete user profiles. Shortcuts may be added to the Default User profile directory using Windows Explorer.

All Users Profile

Administrators may install applications and place shortcuts in the All Users Profile directory. All users will have access to these shortcuts and applications. These applications appear on users' desktops. The All Users' Profile is not available on a domain wide basis.

Roaming Profiles

Roaming and local profiles may be mandatory which will not allow the user to modify them. Roaming profiles are profiles that have been placed on a central server. When the user logs onto the domain, the roaming profile is copied to the local computer the user logged on from. If the user makes changes to the profile, they are saved to the local computer and the central server. When the user logs on from another computer the most recent of the local or server stored profile is used. If a user's profile is a mandatory profile and that profile is not available when the user attempts to log on, the logon attempt will fail.

To create a roaming user profile:

1. Create a shared directory on a domain controller computer or server.
2. Assign a profile path to the shared directory on domain user accounts. This is done on a domain controller from the "Active Directory Users and Computers" tool.

    - Click + next to the domain the user is in.
    - Highlight the Users folder.
    - Right click the user's account and select properties.
    - Set the path in the Profile path text window.

On a local computer, the user profile path is set using the Computer Management Dialog box which is activated by right clicking on "My Computer" and selecting "Manage":

If a user is deleted, the user profile should first be deleted by using the "User Profile" tab of the User Manager. On Windows NT servers, the System Policy Editor is used to control user profile settings. The authenticating domain controller gets system policies from the file.

WINNT40\SYSTEM32\REPL\IMPORT\SCRIPTS\NTCONFIG.POL.

Therefore, to have policies replicated to all domain controllers, place the NTCONFIG.POL file in the directory.

WINNT40\SYSTEM32\REPL\EXPORT\SCRIPTS.

Roaming profiles can be configured between workstations by setting up a user profile in a shared directory that is accessible to all workstations the user will log on from. Then on each workstation, the user will log in from, the UNC path to the profile file must be set. This is done from the User Manager, "select" "User Properties" for the user, then "Profile", then enter in the UNC path in the "User Profile Path" text box.

1.3.4 Account Policies

The three main groupings are: "Password restrictions", "Account lockout", and "Kerberos". The first four items below are under "Password restrictions".

- Password policy
- Enforce password history: Determines the number of passwords that must be used before an old password can be reused.
- Maximum password age : If 0, passwords never need to be changed.
- Minimum password age: If 0, passwords can be changed whenever the users want to. This can prevent users recycling back to their original password.
- Minimum password length: Values are 0 to 14 characters. If 0, passwords are not required.
- Passwords must meet complexity requirements : Uppercase, lowercase, numeric, and special characters may be required.
- Store password using reversible encryption for all users: One-Way encryption is more secure, and reversible encryption is used for users on Apple computers.

Setting Account Policies

- Organisational Units: In Administrative Tools, select "Active Directory Users and Computers".
- Domain: In Administrative Tools, select "Domain Security Policy". The ADMINPAK must be installed on the computer.
- Domain controllers: In Administrative Tools, select "Domain Controller Security Policy". The ADMINPAK must be installed on the computer.
- Local computers: From the Control Panel, "Administrative Tools" applet, double click: Local Security Policy".

1.3.5 Permissions and Restrictions

Once installed, the server runs constantly, listening for requests and accepting them. If server is running, one would see the icon and its green light (to the left of the server's name) in the Server Administration page. Clicking the icon can start or stop the server. It is also possible to start, restart, and stop the server from the Server Manager.

Stop shuts down the server completely, interrupting service until it is restarted. If the etc/inittab file is set to automatically restart (using "respawn"), it is required to remove the line pertaining to the Web server in etc/inittab before shutting down the server; otherwise the server automatically restarts.

Setting the termination timeout

When the server stops, the server stops accepting new connections. Then it waits for all outstanding connections to complete. The time the server waits before timing out is configurable in the magnus.conf file. By default it is set to 3 seconds. Probably it would not be required to change this value. If required to change the value, add a line in magnus.conf as follows:

TerminateTimeout *seconds* : Where *seconds* represents the number of seconds, user wants to wait before timing out.

The advantage to configuring this value is that if for some reason one would like to wait longer for connections to complete. However, because most servers often have connections open from non-responsive clients, if the time the server waits is increased, usually one has to wait the full time before the server shuts down.

Restarting the server

To restart the server use one of the following methods:
If a version of Unix not derived from System V (such as SunOS 4.1.3), is used it would not be possible to use the inittab file.

- Automatically restart it from the inittab file.
- Automatically restart it with daemons in /etc/rc2.d when the machine reboots.
- Restart it manually.

The server's start script, key pair file, and the key password should be owned by root (or, if a non-root user installed the server, that user account), with only the owner having read and write access to them.

If the security risk is not a concern, these steps to start SSL-enabled server automatically can be followed:

1. Using a text editor, open the start file, which is located in *server_root/https-server_identifier.*
2. In the 10th line counting from the top of the script, insert the following:
   echo "*SSL-enabled_server_ password"*|
   For example, the edited line might look like this:
   echo "MBi12!mo"|./$PRODUCT_BIN -d $PRODUCT_SUBDIR/config $@

Restarting with inittab

To restart the server using inittab, put the following text on one line in the /etc/inittab file:

The -i option prevents the server from putting itself in a background process.
http:2:respawn:*server_root*/*type-identifier*/start -i

Replace *server_root* with the directory where the server has been installed, and replace *type-identifier* with the server's directory.

It is required to remove this line before stopping the server.

1.3.6 Tuning Server Performance

Server's technical options can be configured, including the number of maximum simultaneous requests, listen-queue size, and DNS usage.

Configuring maximum simultaneous requests

The number of maximum simultaneous requests, which is the number of active requests allowed for the server at one time, can be set. However, for general purpose internet or Intranet use, one probably will not need to change the default value (128 requests).

To get the number of simultaneous requests, the server counts the number of active requests, adding 1 to the number when a new request arrives, subtracting 1 when it finishes the request. When a new request arrives, the server checks to see if it is already processing the maximum number of requests. If it has reached the limit, it defers processing new requests until the number of active requests drops below the maximum amount.

In theory, one could set the maximum simultaneous requests to 1 and still have a functional server. Setting this value to 1 would mean that the server could only handle one request at a time, but since HTTP requests generally have a very short duration (response time can be as low as 5 milliseconds), processing one request at a time would still allow the processing up to 200 requests per second.

If it is required to change the number of maximum simultaneous requests, set the number before starting the server. To reset the number, the following steps are followed:
Choose Server Preferences|Performance Tuning.
Type the number of requests.

1. Click OK.
2. Click Save and Apply.

Enabling Domain Name System lookups

The server can be configured to use Domain Name System (DNS) lookups during normal operation. By default, DNS is not enabled. If DNS is enabled, the server looks up the host name for a system's IP address.

Although DNS lookups can be useful for server administrators when looking at logs, they can impact performance. When the server receives a request from a client, the client's IP address is included in the request. If DNS is enabled, the server must look up the hostname for the IP address for every client making a request.

Configuring listen-queue size

The listen-queue size is a socket-level parameter that specifies the number of incoming connections the system will accept for that socket. The default setting is 128 incoming connections.

To manage a heavily used Web site, one should make sure that the system's listen-queue size is large enough to accommodate the listen-queue size setting from the Server Manager form. Before changing the listen-queue size, make sure that system supports the new size. The listen-queue size set from the Server Manager form changes the listen-queue size requested by the server.

Configuring the HTTP persistent connection timeout

With HTTP 1.1, a connection can be set to be persistent (similar to keep alive in HTTP 1.0). However, even if a connection is persistent, it still needs to have a timeout setting, otherwise it may consume system resources.

In order to change the setting, following steps can be taken:

1. From the Server Manager, choose Server Preferences Performance Tuning.
2. Enter a number in seconds in the HTTP Persistent Connection Timeout field.
3. Click OK, and finally, save and apply the changes made.

Configuring MIME types

MIME (Multi-purpose Internet Mail Extension) types control the types of multimedia files the mail system supports. One can also use MIME types to specify what file extensions belong to certain server file types. For example, to designate what files are CGI programs, the following steps are followed.

1. Choose Server Preferences|Mime Types.
2. Select the category and enter the content type and file suffix.
2. Click New Type.

To edit a MIME type

1. Click Edit next to the type user want to edit.
2. Change the category, content type, and file suffix as needed.
3. Click Change MIME Type to update.

To remove a MIME type, click Remove next to the type to be removed.

1.3.7 Configuring Network Settings

Server's network settings can be changed using the Server Manager.

Changing the server's location: To change the server's location

1. Choose Server Preferences|Network Settings.
2. Type the pathname of the server's new location.
3. Click OK and, finally, click Save and Apply for changes to take effect.

Changing the server's user account

The server user specifies a Unix user account that the server uses. All the server's processes run as this user. There is no need to specify a server user if one chooses a port number greater than 1024 and are not running as the ***root*** user (in this case, one does not need to be logged on as ***root*** to start the server).

If user account is not specified here, the server runs with the user account that starts it with. Make sure that when server starts, the correct user account is used.

To change the server's user account:

1. Choose Server Preferences|Network Preferences.
2. Type the new server user account.
3. Click OK and finally, click Save and Apply for changes to take effect.

Changing the server name

The server name is the full hostname of the server machine. When clients access the server, they use this name. The format for the server name is *machinename.yourdomain.domain*. For example, if the full domain name is netscape.com, a server with the name www.netscape.com can be installed.

If the system administrator has set up a DNS alias for the server, use that alias on the Network Preferences form. If not, use the machine's name combined with the domain name to construct the full hostname.

Changing the server port number

On the Network Preferences form, the Server Port Number specifies the TCP port that the server listens. The port number chosen can affect the users-if a nonstandard port is used, then anyone accessing the server must specify a server name and port number in the URL. For example, if port 8090 is used, the user would specify something like this URL:

http://mydomain.com/: 8090/abc/xyz.htm

If it is not sure that if the port number to use is available, look at the /etc/services file on the server machine. Port numbers for the most commonly used network-accessible services are maintained in the file /etc/services.

The standard unsecured Web server port number is 80; the standard secure Web server port number is 443. Technically, the port number can be any port from 1 to 65535.

Changing the server binding address

At times it is required that the server machine answers to two URLs. For example, to answer both http://www.netscape.com/ and http://www.mozilla.com/ from one machine.

If the system is set up to listening to multiple IP addresses and wants to use this feature, on the Network Preferences form use the Bind To Address field to tell the server which IP address is associated with this hostname.

Changing the server's MTA host

To change the MTA (Message Transfer Agent) host, use the MTA Host field on the Network Preferences form to change the name of the SMTP mail server. One must enter a valid MTA host to use the agent email function.

Changing the server's NNTP host

To change the NNTP (Network News Transfer Protocol) host, use the NNTP Host field to change the name of the news server. A valid NNTP host must be entered to use agents with the capability to post to news.

Customising error responses

To specify a custom error response that sends a detailed message to clients when they encounter errors from the server. One can specify a file to send or a CGI program to run.

Instead of sending back the default response file on encountering error, one might want to send a custom error response instead.

What are the errors?

Response to several different kinds of errors can be customised:

- **Unauthorised:** This error occurs when users without access permissions try to access a document on the server that is protected by access control. One might send information on how they can get access.
- **Forbidden:** This error occurs when the server does not have file system permissions to read something, or if the server is not permitted to follow symbolic links.
- **Not Found:** This error occurs when the server can't find a document or when it has been instructed to deny the existence of a document.
- **Server Error:** This error occurs when the server is not configured properly or when a catastrophic error occurs, such as the system running out of memory or producing a core dump.

Setting up the response

Before setting up the response, one needs to write the HTML file to send or create the CGI program to run. After this, set the response by doing the following:

1. From the Server Manager, choose Server Preferences|Error Responses.
2. From the Resource Picker, choose the server resource intended to be configured.
3. Select the error response wanted to be customised.
4. Type the absolute pathname to the file or CGI script that will return for that error code. Check the CGI box if the file is a CGI program that is intended to run. Repeat this process for each of the error responses to be customised
5. Click OK and, finally, click Save and Apply to confirm changes.

To remove a customisation, return to the form and delete the filename from the text box next to the error code.

1.4 NETWORKS AND SECURITY

For a network, whether it is a small home office network or a 5000 node LAN/WAN, security should a top priority. From the smallest to the largest network, steps should be taken to make sure that it is secure from attack or theft. How to protect the integrity of network information can be handled aggressively or casually depending upon what one has and how much one needs to protect. For doing a good job there are specific steps that one should take and in a specific order. Bear in mind that not all steps are necessary for all network situations. Like any major project to be undertaken, one should start with a plan, and a good plan starts with an outline. Given below is a sample outline of the process of providing security to a network.

- Risk Assessment
- Vulnerability
- Budget Analysis
- Security Policy
- Implementation
- Auditing.

SQLBase 7 offers five connectivity interfaces for linking client applications with SQLBase databases. One can choose the connectivity interface that best suits the needs based on the development tool/language users are using and application requirements:

SQL/API is a low level, high performance interface suited for use with C and languages that support external functions in DLLs. It provides complete access to the SQLBase feature set, including "administrative" operations.

- SAL is the 4GL scripting language used in Gupta's development environments for coding business logic.

- SQLBase++ is an object oriented “wrapper” around the SQL/API for use with C++ Applications.
- The SQLBase JDBC driver provides a native interface for Java applications and applets.
- The SQLBase ODBC driver provides a simple and portable interface via ODBC. SQLBase 7 fully supports multi-threaded ODBC applications. It is also fully compatible with the older ODBC 2.0 API.

1.5 TUNING APPLICATIONS OVER INTRANET

As we have already discussed in section 1.3.6 of this Unit, how can we improve server performance. We need different tuning applications with the other required softwares to provide stable database connectivity and simple environment database between clients and server for example, SQL /API is issued to provide functions to perform administrative like database backup’s restoration, ODBC and JDBC provides stable connectivity with Database.

SQL/API

The Structured Query Language/Application Programming Interface (SQL/API) is a function library designed for use with the C programming language, and development environments that support C-style external function calling conventions. SQL/API is a Call Level Interface (CLI) analogous to SQL*Net in Oracle environments and CT-LIB in Sybase environments.

One can make calls to SQL/API functions throughout the application to interact with SQLBase. Typical function calls include connecting and disconnecting to a database, passing SQL statements to the server for compilation and execution, providing bind variable data, and retrieving result sets.

Additionally, the SQL/API provides functions to perform administrative tasks such as performing database backups and restorations.

ODBC (Open Database Connectivity)

Not just an ODBC driver, Recital ODBC Developer provides a complete industry standard ODBC database solution for Unix, Linux, or OpenVMS. Consisting of an ODBC driver, and an Application Server, which has a complete SQL-92 database engine, Recital ODBC Developer can create, query and update Recital databases from Windows applications. If Recital applications are running on Unix, Linux, or OpenVMS, one can provide full read and update access to the databases from Microsoft Windows clients with Recital ODBC Developer. Using Recital ODBC Developer one can use industry standard management reporting tools such as Crystal Reports to generate high quality reports against live data in a Recital based application.

JDBC

Not just a JDBC driver, Recital JDBC Developer provides a complete industry standard JDBC database solution, consisting of an all-Java type 3 driver, and an Application Server that implements a complete SQL-92 database engine. With JDBC Developer, Java applications can query and update data from any data source across Intranets or the Internet.

☞ Check Your Progress 1

1) The first step of setting up the Intranet is to configure a _____.

2) An Internet stands authentication protocol which is the default protocol for Windows 2000 computers within a domain is _____.

3) SQLBase 7 fully supports _____ODBC.

4) SQL/API is a call level interface (CLI) analogous to _____in Sybase environments.

5) _____types control the types of multimedia files the mail system supports.

1.6 SUMMARY

In a world where communication is the key to business process, everyone wants to make use of Intranet technology for business success. While setting up the Intranet, care should be taken to prevent undesired flow of secret business information to competitors.

It is to be always remembered that the foundation of the network depends on the technology that is used to set up the Intranet and the security features that are available with it. The role of a network administrator/Intranet administrator is thus very important. One should judiciously decide who should and should not be allowed certain privileges, privileges which can pose a threat to the network.

Finally, it is desirable for the company to have a proper security policy to curb network security lapses.

1.7 SOLUTIONS/ANSWERS

Check Your Progress 1

1) Web Server

2) Kerberos V5

3) Multi-threaded

4) CT-LIB

5) Multi-Purpose Internet Mail Extension.

1.8 FURTHER READINGS

1) *Empowering Intranets to implement Strategy, Build Teamwork and Manager Change* by D.Keith Denton, Praeger Publisher.
2) *Intranet's Decisions: Creating your organisation's internal network* by Lisa Kimball, Miles River Press.
3) *Internet and Intranet Security Management: Risks and Solutions* by Lech Janczewski, Idea Group Publishing.

Reference Websites

1) http://www.petra.austinc.edu/
2) http://www.javacorporate.com/
3) http://www.tech-noel.com
4) http://www.netscape.com