Course Code	:	**MCS-022**
Course Title	:	**Operating System Concepts and Networking Management**
Assignment Number	:	**MCA (6)/022/Assignment/17-18**
Maximum Marks	:	**100**
Weightage	:	**25%**
Last Date of Submission	:	**15th October, 2017 (For July 2017 Session)**
	:	**15th April, 2018 (For January 2018 Session)**

This assignment has eight questions. Answer all questions. Rest 20 marks are for viva voce. You may use illustrations and diagrams to enhance the explanations. Please go through the guidelines regarding assignments given in the Programme Guide for the format of presentation.

1. (a) What is Active Directory? How can Active Directory connect to other Third-Party Directory Services? Discuss the available options for it. *(5 Marks)*
   (b) What is umask ? How to set the umask permanently for a user in Linux? *(5 Marks)*

2. (a) Compare the features of Windows 2000 Server & Advanced Server? *(5 Marks)*
   (b) Explain SNMP architecture with the help of a diagram. *(5 Marks)*

3. (a) What are the standard user groups in windows 2000? Explain the access privileges of each. *(5 Marks)*
   (b) Explain, how to create partition from the raw disk in Linux? *(5 Marks)*

4. (a) What is the meaning of Global Catalog? How it is related to trust relationship agreement? Explain. *(5 Marks)*
   (b) Describe the installation procedure of Linux operating system. *(5 Marks)*

5. (a) What is DHCP? How we configure DHCP? *(5 Marks)*
   (b) How do you create a new user account? Explain the different options of the command used for it. *(5 Marks)*

6. (a) Explain the significance of each field in the/etc/passwd file in Linux? *(5 Marks)*
   (b) What are application partitions? Explain the process /commands for creating a new application partition in Windows. *(5 Marks)*

7. (a) What is Group Policy object(s) (GPOs)? How is it different from local Group Policy object. *(5 Marks)*
   (b) What is partial backup in Linux? Explain the process of Backup and Restore in Linux using the suitable commands. *(5 Marks)*

8. (a) Explain the different ways to configure DNS & Zones? *(5 Marks)*
   (b) Discuss the security features of Linux? Explain, how the unique authentication module of Linux provides security. *(5 Marks)*

Q.1.
A.1.(a)

Active Directory is a database that keeps track of all the user accounts and passwords in your organization. It allows you to store your user accounts and passwords in one protected location, improving your organization's security.

Active Directory is subdivided into one or more domains. A domain is a security boundary. Each domain is hosted by a server computer called a domain controller (DC). A domain controller manages all of the user accounts and passwords for a domain.

Active Directory is a LDAP compatible directory service and supported by various third party applications like Novell DirXML, and Atlassian Crowd.
Microsoft Identity Integration Server (MIIS) is one of the options you can use to act as an intermediary between two directories (including directories used by SAP, Domino, etc).
MIIS manages information by retrieving identity information from the connected data sources and storing the information in the connector space as connector space objects or CSEntry objects. The CSEntry objects are then mapped to entries in the metaverse called metaverse objects or MVEntry objects. This architecture allows data from dissimilar connected data sources to be mapped to the same MVEntry object. All back-end data is stored in Microsoft SQL Server.

Versions

- Zoomit Via (pre 1999)
- Microsoft Metadirectory Server [MMS] (1999–2003)
- Microsoft Identity Integration Server 2003 Enterprise Edition [MIIS] (2003-2009)
- Microsoft Identity Integration Server 2003 Feature Pack [IIFP] (2003-2009)
- Microsoft Identity Lifecycle Manager Server 2007 ILM (2007-2010)
- Microsoft Forefront Identity Manager 2010 FIM [CR0] (Current)

Supported Data Sources

MIIS 2003, Enterprise Edition, includes support for a wide variety of identity repositories including the following.

- **Network operating systems and directory services:** Microsoft Windows NT, Active Directory, Active Directory Application Mode, IBM Directory Server, Novell eDirectory, Resource Access Control Facility (RACF), SunONE/iPlanet Directory, X.500 systems and other network directory products
- **E-mail:** Lotus Notes and IBM Lotus Domino, Microsoft Exchange 5.5, 2000, 2003, 2007
- **Application:** PeopleSoft, SAP AG products, ERP1, telephone switches PBX, XML- and Directory Service Markup Language DSML-based systems
- **Database:** Microsoft SQL Server, Oracle RDBMS, IBM Informix, dBase, IBM DB2

- **File-based:** DSMLv2, LDIF, Comma-separated values CSV, delimited, fixed width, attribute value pairs

Q.1.

A.1.(b)

When user create a file or directory under Linux or UNIX, she create it with a default set of permissions. In most case the system defaults may be open or relaxed for file sharing purpose. For example, if a text file has 666 permissions, it grants read and write permission to everyone. Similarly a directory with 777 permissions, grants read, write, and execute permission to everyone.

Default umask Value

The user file-creation mode mask (umask) is use to determine the file permission for newly created files. It can be used to control the **default file permission for new files**. It is a four-digit octal number. A umask can be set or expressed using:

- Symbolic values
- Octal values

Procedure To Setup Default umask

You can setup umask in /etc/bashrc or /etc/profile file for all users. By default most Linux distro set it to 0022 (022) or 0002 (002). Open /etc/profile or ~/.bashrc file, enter:

```
# vi /etc/profile
```

OR

```
$ vi ~/.bashrc
```

Append/modify following line to setup a new umask:

```
umask 022
```

Save and close the file. Changes will take effect after next login. All UNIX users can override the system umask defaults in their /etc/profile file, ~/.profile (Korn / Bourne shell) ~/.cshrc file (C shells), ~/.bash_profile (Bash shell) or ~/.login file (defines the user's environment at login).

Q.2.(a)

A.2.(a)

The Windows 2000 Server family currently includes Windows 2000 Server and Windows 2000 Advanced Server. Windows 2000 Server offers core functionality appropriate to small-sized and medium-sized organizations that have numerous workgroups and branch offices and that need essential services including file, print, communications, infrastructure, and Web. Windows 2000 Advanced Server is designed to meet mission-critical needs, such as large data warehouses, online transaction processing (OLTP), messaging, e-commerce, or Web hosting services for medium and large organizations, and Internet service providers (ISPs).

Windows 2000 Advanced Server has evolved from Microsoft® Windows NT® Server 4.0, Enterprise Edition. It provides a comprehensive clustering infrastructure for high availability and scalability of applications and services, including main memory support up to 8 Gigabytes (GB)

on Intel Page Address Extension (PAE) systems. Designed for demanding enterprise applications, Advanced Server supports new systems with up to 8-way symmetric multiprocessingI> (SMP. SMP enables any one of the multiple processors in a computer to run any operating system or application threads simultaneously with the other processors in the system. Windows Advanced Server is well-suited to database-intensive work, and provides high availability server ing and load balancing for excellent system and application availability.

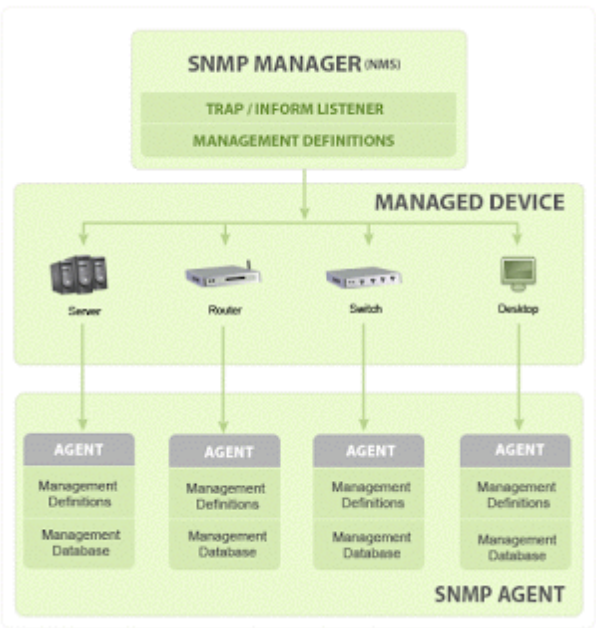
Windows 2000 Advanced Server includes the full feature set of Windows 2000 Server and adds the high availability and scalability required for enterprise and larger departmental solutions. Key features of Advanced Server include:

- Network (TCP/IP) Load Balancing
- Enhanced two-node server clusters based on the Microsoft Windows Cluster Server (MSCS) previously released in the Windows NT Server 4.0 Enterprise Edition
- Up to 8 GB main memory on Intel PAE Systems
- Up to 8-way SMP

A.2.(b)

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control ProtocoIInternet Protocol (TCPIIP) protocol suite.

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

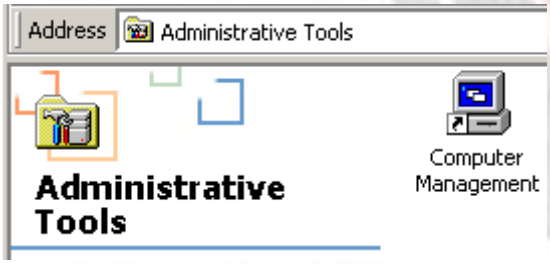


Q.3.

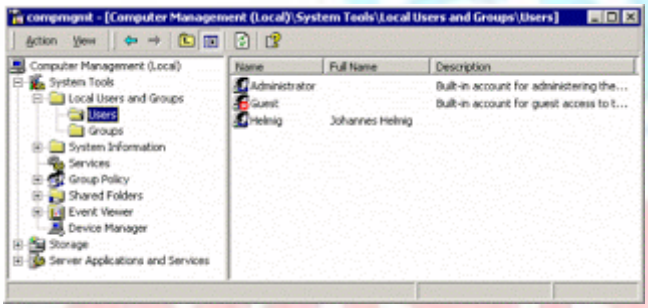
A.3.

When creating new Users in Windows 2000, you define their rights/privileges by defining the users to be a member of a group.
The rights/privileges of a user are based on the rights/privileges of the groups, so a right/privilege is assigned to a user by make the user a member of a group, which has the required right/privilege.
To view/modify these rights/privileges, view the "***Administrative Tools***":

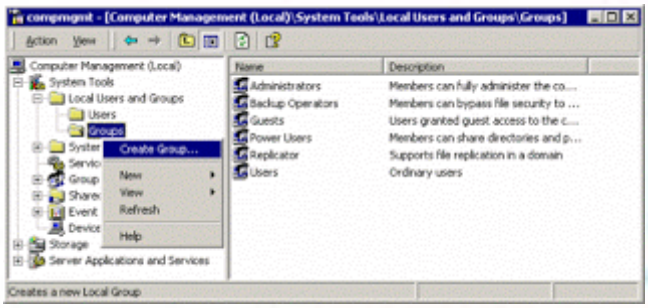
then: "***Computer Management***":

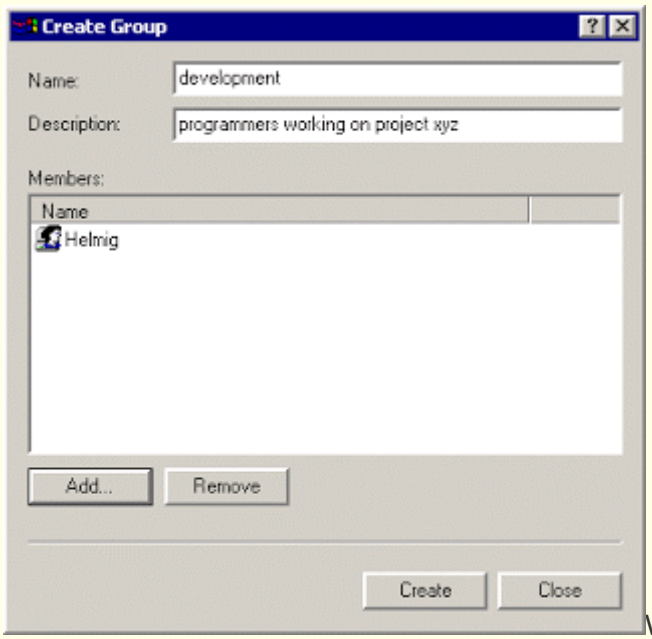


"***Computer Management***" allows also User-Management (add/delete users), but offers some advanced options not available in the more simple User-Applet, for example:
it shows in the overview, that the user-account for "GUEST" is de-activated:



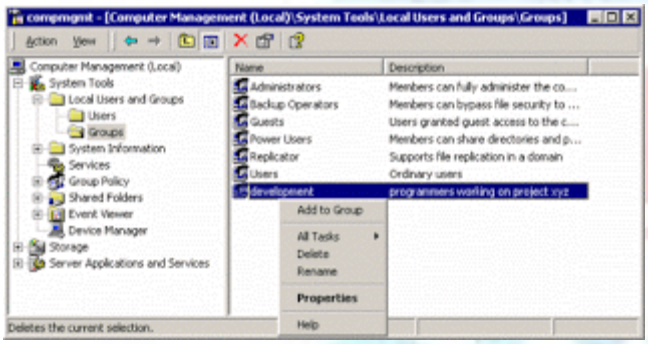
It allows to view the predefined Groups and to add custom-groups:





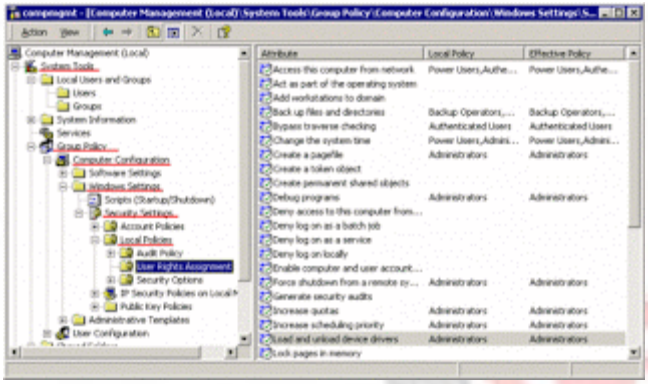
While creating a new group, users can be added immedialety to be a member of the group.
But users can be added later to become a member of a group.

But to see in detail the permission/rights/provileges of a group, you need to "drill down" in the "***Group - Policies***" 4 levels down:

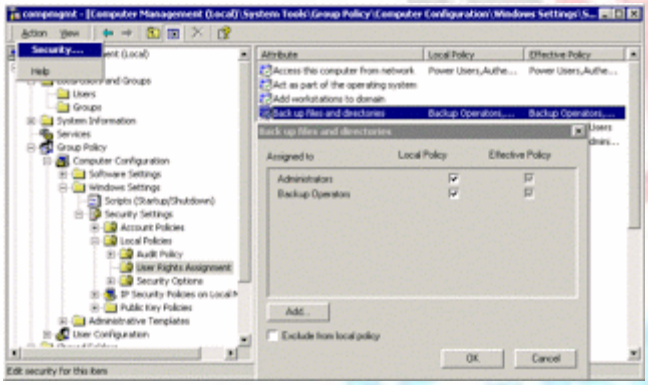


Here you find the list of rights/privileges for all the jobs on your system, from:
- Accessing this computer from the Network
- Backup files and directories
- Restore files and directories (yes, it is a different right/privilege)
- Load and unload device drivers --> Configure hardware, reserved for Administrators.

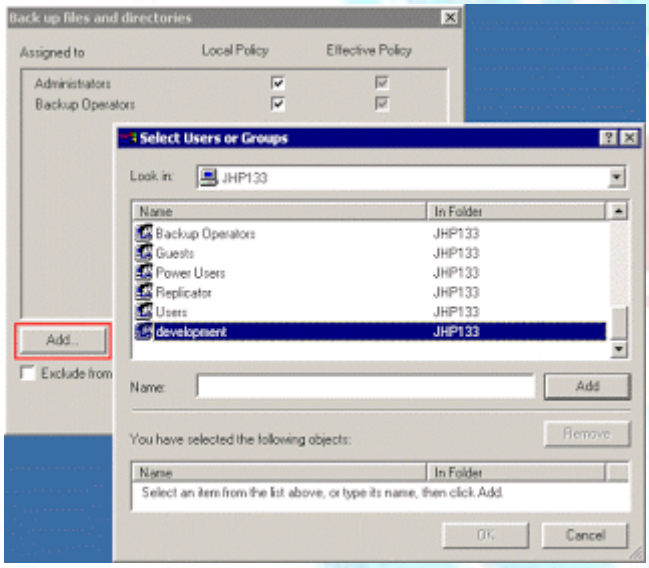
You can view in detail the list of groups with each right/privilege:



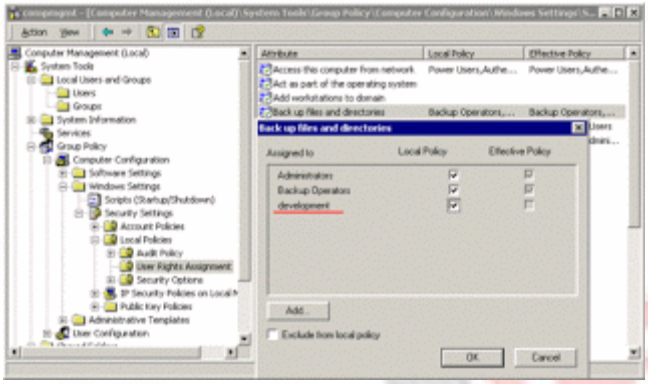
For example: "regular users" do not have the right/permission/privilege to make backups. To enable another group (one of the predefined or our own-defined groups) to have a right/privilege (like: make a backup), you need to add your group to the list:



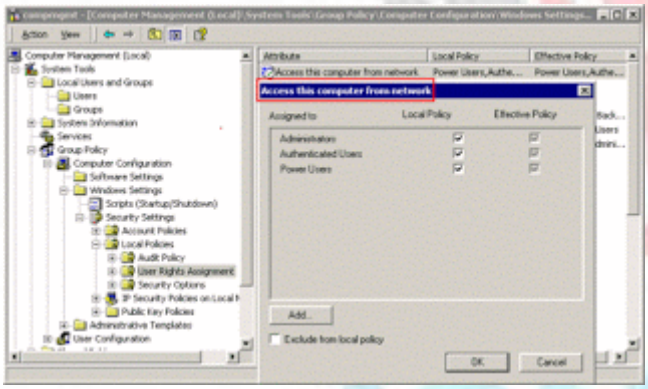
Select from the list of defined groups your group and "add" it:



In summary: everytime, when you are rejected by the system, check here for the groups, which have the right/privilege.
You should check for sure for the "Access this computer from the network", if you intend to use your system as a network server:



A user can be member of MULTIPLE groups, which will give him the combined



A.3.(b)

As root create the /dev/raw directory:

mkdir /dev/raw

Then create the required raw devices using the following sintax:

mknod raw<raw_dev_number> c 162 <raw_dev_number>

i.e.:

mknod raw1 c 162 1

For setting up 12 raw devices use a loop:

```
#!/bin/ksh
x=1
cd /dev/raw
while [ $x -lt 12 ];
do
  mknod raw$x c 162 $x
    x=`expr $x + 1 `
done
```

Once configured create or update the script /etc/udev/scripts/dev-raw.sh to automatize the configuration of raw devices for RAC on each startup

```
# raw-dev.sh
MAKEDEV raw
mv /dev/raw/raw1 /dev/raw/votingdisk
mv /dev/raw/raw2 /dev/raw/ocr.dbf
mv /dev/raw/raw3 /dev/raw/spfile+ASM.ora

chmod 660 /dev/raw/votingdisk
chmod 660 /dev/raw/ocr.dbf
chmod 660 /dev/raw/spfile+ASM.ora

chown oracle:dba /dev/raw/votingdisk
chown oracle:dba /dev/raw/ocr.dbf
chown oracle:dba /dev/raw/spfile+ASM.ora
```

Q.4.

A.4.(a)

A global catalog is a distributed data storage that is stored in domain controllers (also known as global catalog servers) and is used for faster searching. It provides a searchable catalog of all objects in every domain in a multi-domain Active Directory Domain Services (AD DS). A global catalog provides a partial representation of the objects and is distributed using multi-master replication.

A global catalog is a multi-domain catalog that allows for faster searching of objects without the need for a domain name. It helps in locating an object from any domain by using its partial, read-only replica stored in a domain controller. As it uses only partial information and a set of attributes that are most commonly used for searching, the objects from all domains, even in a large forest, can be represented by a single database of a global catalog server.

A global catalog is created and maintained by the AD DS replication system. The predefined attributes that are copied into a global catalog are known as the Partial Attribute Set (PAS).

Users are allowed to add or delete the attributes stored in a global catalog and thus change the database schema.

Some of the common global catalog usage scenarios are as follows:

- Forest-wide searches
- User logon
- Universal group membership caching
- Exchange address book lookups

Q.4.
A.4.(b)

2 Installing the Linux Operating System

2.1 Introduction

The procedure for installing Oracle Enterprise Linux 5.*3* is fully described in the product documentation. This section presents a summary of that procedure, and assumes a sound knowledge of Linux administration.

For information on vendor-specific variations, consult the appropriate documentation. The installation procedure described is based on the use of a DVD media package.

Obtaining the Linux Operating System

The Oracle Enterprise Linux 5.*3* software is available from the Oracle E-Delivery Web site

2.2 Download ISO Image and Burn DVD

1. Download the appropriate ISO image. This guide assumes you are using the DVD version of Oracle Enterprise Linux 5.3.
2. Unzip the files.
3. Burn the ISO file to DVD. Note that this requires the use of a DVD-burning utility (such as UltraISO or Magic ISO Maker).

Note:

According to your corporate policy, the Linux installation procedure may use a different procedure to that described in the following sections.

2.3 Run Installer

Note:

After installing Linux on the first node, repeat the Linux installation procedure for each system.

1. Ensure that server system is able to boot from DVD. Insert the Oracle Enterprise Linux DVD, and power on.
2. When the Oracle Enterprise Linux boot screen appears, press **Enter** to start the installation process.
3. When asked to test the DVD media, select **Skip**. After a short interval, the installer goes into GUI mode. (The media test is not necessary because the DVD burning software would have informed you of any errors on the media).

4. At the Welcome to Oracle Enterprise Linux screen, click **Next**.
5. Select the appropriate options from the Language and Keyboard settings screens.
6. If the installer detects a previous version of Enterprise Linux, you are prompted to "Install Enterprise Linux" or "Upgrade an existing installation". Select "Install Enterprise Linux", and click **Next**.

   Important:

   Oracle recommends that you install the Linux operating system with the default software packages (RPMs), and that you do not customize the RPMs during installation. This installation includes most required packages, and helps you limit manual checks of package dependencies.

2.4 Set up Disk Partitioning

1. When prompted, select the default **Remove Linux partitions on selected drives and create default layout** option, and check the option **Review and modify partitioning layout**. When prompted to confirm your selection, select **Yes**. Click **Next** to continue.

   Note:

   A check box allows you to encrypt the entire system. If selected, for security reasons, a password is required during booting the system.

2. When prompted to confirm the removal of all partitions, click **Yes**.
3. Review and modify (if necessary) the automatically selected disk partitions.

   For most automatic layouts, the installer assigns 100 MB for /boot, 2 GB for swap, and the remainder is assigned to the root (/) partition. Ensure the specified SWAP space is sufficient.

   Required disk space and swap space requirements.

   The installer creates a disk configuration using the Logical Volume Manager (LVM). For example, it will partition the first hard drive (/dev/sda in the described configuration) into two partitions: one for the /boot partition (/dev/sda1), and the remainder of the disk dedicated to a LVM named VolGroup00 (/dev/sda2). The LVM Volume Group (VolGroup00) is then partitioned into two LVM partitions: one for the root file system (/), and another for swap. If you have selected a non-standard layout, ensure that the system meets the required disk space specifications shown in Table 2-1. Ensure enough swap space is allocated for Oracle Enterprise Linux. Its required swap space is shown in Table 2-2.

   Table 2-1 Required Disk Space Specifications

Partition	Minimum Required Disk Space (GB)
/u01/app/	300
/opt/ruei	0.5
/var/opt/ruei/	100

This is the example location of the database used throughout this guide.

Table 2-2 Required Swap Space

Available RAM	Swap Space Required
Up to 8192 MB	Equal to the size of RAM.
More than 8192 MB	0.75 times the size of RAM.

Q.5.(a)

A.5.(a)

What is DHCP?

Dynamic Host Configuration Protocol (DHCP) is a client/server protocol that automatically provides an Internet Protocol (IP) host with its IP address and other related configuration information such as the subnet mask and default gateway. RFCs 2131 and 2132 define DHCP as an Internet Engineering Task Force (IETF) standard based on Bootstrap Protocol (BOOTP), a protocol with which DHCP shares many implementation details. DHCP allows hosts to obtain necessary TCP/IP configuration information from a DHCP server.

The Microsoft Windows Server 2003 operating system includes a DHCP Server service, which is an optional networking component. All Windows-based clients include the DHCP client as part of TCP/IP, including Windows Server 2003, Microsoft Windows XP, Windows 2000, Windows NT 4.0, Windows Millennium Edition (Windows Me), and Windows 98.

Note

- It is necessary to have an understanding of basic TCP/IP concepts, including a working knowledge of subnets before you can fully understand DHCP. For more information about TCP/IP, see "TCP/IP Technical Reference."

Benefits of DHCP

In Windows Server 2003, the DHCP Server service provides the following benefits:

- **Reliable IP address configuration.** DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

- **Reduced network administration.** DHCP includes the following features to reduce network administration:

- Centralized and automated TCP/IP configuration.

- The ability to define TCP/IP configurations from a central location.

- The ability to assign a full range of additional TCP/IP configuration values by means of DHCP options.

- The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.

- The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

Why use DHCP

Every device on a TCP/IP-based network must have a unique unicast IP address to access the network and its resources. Without DHCP, IP addresses must be configured manually for new computers or computers that are moved from one subnet to another, and manually reclaimed for computers that are removed from the network.

DHCP enables this entire process to be automated and managed centrally. The DHCP server maintains a pool of IP addresses and leases an address to any DHCP-enabled client when it starts up on the network. Because the IP addresses are dynamic (leased) rather than static (permanently assigned), addresses no longer in use are automatically returned to the pool for reallocation.

The network administrator establishes DHCP servers that maintain TCP/IP configuration information and provide address configuration to DHCP-enabled clients in the form of a lease offer. The DHCP server stores the configuration information in a database, which includes:

- Valid TCP/IP configuration parameters for all clients on the network.

- Valid IP addresses, maintained in a pool for assignment to clients, as well as excluded addresses.

- Reserved IP addresses associated with particular DHCP clients. This allows consistent assignment of a single IP address to a single DHCP client.

- The lease duration, or the length of time for which the IP address can be used before a lease renewal is required.

A DHCP-enabled client, upon accepting a lease offer, receives:

- A valid IP address for the subnet to which it is connecting.

A.5.(b)

How to Create a New User

CREATE USER 'newuser'@'localhost' IDENTIFIED BY 'password';
Sadly, at this point newuser has no permissions to do anything with the databases. In fact, if newuser even tries to login (with the password, password), they will not be able to reach the MySQL shell.

Therefore, the first thing to do is to provide the user with access to the information they will need.

GRANT ALL PRIVILEGES ON * . * TO 'newuser'@'localhost';
The asterisks in this command refer to the database and table (respectively) that they can access—this specific command allows to the user to read, edit, execute and perform all tasks across all the databases and tables.

Once you have finalized the permissions that you want to set up for your new users, always be sure to reload all the privileges.

FLUSH PRIVILEGES;
Your changes will now be in effect.

How To Grant Different User Permissions

Here is a short list of other common possible permissions that users can enjoy.

- ALL PRIVILEGES- as we saw previously, this would allow a MySQL user all access to a designated database (or if no database is selected, across the system)
- CREATE- allows them to create new tables or databases
- DROP- allows them to them to delete tables or databases
- DELETE- allows them to delete rows from tables
- INSERT- allows them to insert rows into tables
- SELECT- allows them to use the Select command to read through databases
- UPDATE- allow them to update table rows
- GRANT OPTION- allows them to grant or remove other users' privileges

Q.6.(a)
A.6.(a)

/etc/passwd file stores essential information, which is required during login i.e. user account information. /etc/passwd is a text file, which contains a list of the system's accounts, giving for each account some useful information like user ID, group ID, home directory, shell, etc. It should have general read permission as many utilities like ls use it to map user IDs to user names, but write access only for the superuser/root account.

Understanding fields in /etc/passwd

The /etc/passwd contains one entry per line for each user (or user account) of the system. All fields are separated by a colon (:) symbol. Total seven fields as follows. Generally, passwd file entry looks as follows (click to enlarge image):

1. **Username**: It is used when user logs in. It should be between 1 and 32 characters in length.
2. **Password**: An x character indicates that encrypted password is stored in /etc/shadow file. Please note that you need to use the passwd command to computes the hash of a password typed at the CLI or to store/update the hash of the password in /etc/shadow file.
3. **User ID (UID)**: Each user must be assigned a user ID (UID). UID 0 (zero) is reserved for root and UIDs 1-99 are reserved for other predefined accounts. Further UID 100-999 are reserved by system for administrative and system accounts/groups.
4. **Group ID (GID)**: The primary group ID (stored in /etc/group file)
5. **User ID Info**: The comment field. It allow you to add extra information about the users such as user's full name, phone number etc. This field use by finger command.

6. **Home directory**: The absolute path to the directory the user will be in when they log in. If this directory does not exists then users directory becomes /

7. **Command/shell**: The absolute path of a command or shell (/bin/bash). Typically, this is a shell. Please note that it does not have to be a shell.

A.6.(b)

Application directory partitions

Application directory partitions hold the data that is used by your applications. You can create an application partition during AD LDS setup or anytime after installation. Depending on your application, you might extend the schema manually or your application might automatically extend the schema for you. Typically, you manage data in a given application directory partition through your application. After the application directory partition is created, AD LDS holds the application partition reference objects in CN=Partitions,CN=Configuration.

Application Partition Name Space

When you create an application partition, that partition has its own name space, similar to the way that a domain is given its own name space within the Active Directory. An application partition is actually very similar structurally to a domain. The biggest difference is that an application partition can not contain security principles (users, groups, computers, etc.).

Since application directory partitions are so structurally similar to domains, it shouldn't surprise you that they use similar name spaces to domains. An application directory partition can exist as a child of a domain, as a child of an application directory partition, or as a new tree in a forest. For example, if you had an Active Directory consisting of a single domain named brienposey.com, and you wanted to create an application directory partition named application as a child of this domain, then the namespace for the new application directory partition would be application.brienposey.com.

An application directory partition can also exist as a child of another application directory partition. Therefore, if you wanted to create an application directory partition named application2 and make it a child of the partition named application, then the DNS namespace would be application2.application.brienposey.com.

Creating an Application Directory Partition

There are several different tools that can be used to create an application directory partition. You can use the NTDSUTIL command line tool, ADSIEDIT, or LDAP commands. Some application vendors will also include code in their applications to create the application directory partition for you.

If you do have to create the application directory partition yourself, the easiest way of doing so is probably to use the NTDSUTIL command. To do so, open a command prompt window and enter the NTDSUTIL command. When you do, you will see the NTDSUTIL prompt appear. Enter the DOMAIN MANAGEMENT command at the prompt, and you will see the prompt change from NTDSUTIL to domain management.

Q.7.(a)

A.7.(a)

Group Policy Object Editor is a Microsoft Management Console (MMC) snap-in used for configuring and modifying Group Policy settings within Group Policy objects (GPOs).

Administrators need to be able to quickly modify Group Policy settings for multiple users and computers throughout a network environment. The Group Policy Object Editor provides administrators with a hierarchical tree structure for configuring Group Policy settings in GPOs. These GPOs can then be linked to sites, domains, and organizational units (OU) containing computer or user objects.

Group Policy Object Editor consists of two main sections: **User Configuration**, which holds settings that are applied to users (at logon and periodic background refresh), and **Computer Configuration**, which holds settings that are applied to computers (at startup and periodic background refresh). These sections are further divided into the different types of policies that can be set, such as Administrative Templates, Security, or Folder Redirection.

To work efficiently, administrators need to have immediate access to information about the function and purpose of individual policy settings. For Administrative Templates policy settings, Group Policy Object Editor provides information about each policy setting directly in the Web view of the console. This information is called explain text. Explain text shows operating system requirements, defines the policy setting, and includes any specific details about the effect of enabling or disabling the policy setting.

In addition, developers should be able to quickly and easily add Group Policy support to their software products. The Group Policy Object Editor is designed to be extensible. The easiest way for developers to extend Group Policy Object Editor for their applications is to write custom Administrative Template files that “plug in” to Group Policy Object Editor.

Group Policy Object Editor Core Scenarios

There are two core scenarios for Group Policy Object Editor: editing GPOs, and extending the user interface (UI) to accommodate new applications or features. Both of these scenarios are described in detail in the following section.

Editing Group Policy Objects

Group Policy Object Editor is the primary tool used for configuring policy settings within a GPO. Group Policy Object Editor operates as an extension to Group Policy Management Console (GPMC). When an administrator elects to edit a GPO from within GPMC, Group Policy Object Editor appears, displaying the settings for that particular GPO. If GPMC is not available, Group Policy Object Editor operates as an extension to Active Directory management tools, such as the Active Directory Users and Computers snap-in or the Active Directory Sites and Services snap-in. Regardless of the tool an administrator uses to call Group Policy Object Editor, the primary function of Group Policy Object Editor is to edit settings within GPOs.

A.7.(b)

Server Backup Procedures

There are a variety of methods of performing backups with Linux. These include command-line tools included with every Linux distribution, such as ``dd'', ``dump'', ``cpio'', as well as ``tar''. Also available are text-based utilities, such as ``Amanda'' and ``Taper'', which is designed to add a more user-friendly interface to the backup and restore procedures. There are GUI-based utilities as well, such as ``KDat''. Finally, commercial backup utilities are also available, such as ``BRU'' and ``PerfectBackup+''. Any one of these backup solutions can provide protection for your valuable data.

A brief listing of some of the tools available, including where they can be obtained, can be found on the “Linux Applications and Utilities Page”,When deciding on a backup solution, you will need to consider the following factors:

- *Portability* - Is backup portability (ie. the ability to backup on one Linux distribution or implementation of Unix and restore to another; for example from Solaris to Red Hat Linux) important to you? If so, you'll probably want to choose one of the command-line tools (eg. ``dd'', ``dump'', ``cpio'', or ``tar''), because you can be reasonably sure that such tools will be available on any *nix system.
- *Unattended or automated backups* - Is the ability to automate backups so that they can be performed at regular intervals without human intervention important to you? If so, you will need to choose both a tool and a backup medium which will support such a backup scheme.

Backing up with ``tar'':

If you decide to use ``tar'' as your backup solution, you should probably take the time to get to know the various command-line options that are available; type "man tar" for a comprehensive list. You will also need to know how to access the appropriate backup media; although all devices are treated like files in the Unix world, if you are writing to a character device such as a tape, the name of the "file" is the device name itself (eg. ``/dev/nst0'' for a SCSI-based tape drive).
The following command will perform a backup of your entire Linux system onto the ``/archive/'' file system, with the exception of the ``/proc/'' pseudo-filesystem, any mounted file systems in ``/mnt/'', the ``/archive/'' file system (no sense backing up our backup sets!), as well as Squid's rather large cache files (which are, in my opinion, a waste of backup media and unnecessary to back up):

```
tar -zcvpf /archive/full-backup-`date '+%d-%B-%Y'`.tar.gz \
   --directory / --exclude=mnt --exclude=proc --exclude=var/spool/squid .
```

Q.8.

A.8.(a)

Domain Name System is the full form of the abbreviation DNS. It can be configured by clicking the Start button, pointing to the Programs, pointing to Administrative Tools and clicking DNS Manager (which has two zones, namely the Forward Lookup Zone and the Reverse Lookup Zone). When the DNS Server Configuration Wizard starts, click Next. If it does not auto-start, it can be started by right-clicking the user's server name object in the DNS Manager console and choosing the Configure Your Server option.

The next step is to choose to add a forward lookup zone, click Next and ensure whether the new forward lookup zone is a primary zone or not. It can only accept dynamic updates if it is a primary zone. Click Primary, and then click Next. It must be ensured that the zone name must either be the same as the user's Active Directory Domain name or the same as the suffix for all the computers on the network which are to be registered with the DNS server (in case of a stand-alone or workgroup environment). Type the name of the zone and then click Next. The default name is accepted for the new zone file. Then click Next. Choose to add a reverse lookup zone now and click Next.

A.8.(b)

Unix Security – Discretionary Access Control

Linux was initially developed as a clone of the Unix operating system in the early 1990s. As such, it inherits the core Unix security model—a form of Discretionary Access Control (DAC). The security features of the Linux kernel have evolved significantly to meet modern requirements, although Unix DAC remains as the core model.

Briefly, Unix DAC allows the owner of an object (such as a file) to set the security policy for that object—which is why it's called a *discretionary* scheme. As a user, you can, for example, create a new file in your home directory and decide who else may read or write the file. This policy is implemented as permission bits attached to the file's inode, which may be set by the

owner of the file. Permissions for accessing the file, such as *read* and *write,* may be set separately for the owner, a specific group, and other (i.e. everyone else). This is a relatively simple form of access control lists (ACLs).

Programs launched by a user run with all of the rights of that user, whether they need them or not. There is also a *superuser*—an all-powerful entity which bypasses Unix DAC policy for the purpose of managing the system. Running a program as the superuser provides that program with all rights on the system.

Extending Unix Security

Unix DAC is a relatively simple security scheme, although, designed in 1969, it does not meet all of the needs of security in the Internet age. It does not adequately protect against buggy or misconfigured software, for example, which may be exploited by an attacker seeking unauthorized access to resources. Privileged applications, those running as the superuser (by design or otherwise), are particularly risky in this respect. Once compromised, they can provide full system access to an attacker.

Functional requirements for security have also evolved over time. For example, many users require finer-grained policy than Unix DAC provides, and to control access to resources not covered by Unix DAC such as network packet flows.