1) Explain what is Windows Server?

Window server is a series of server operating system developed by Microsoft Corporation.

2) Explain in windows DNS server what is Primary, Secondary and Stub zone?

In windows DNS server,

Primary Zone: In this, the file is saved as normal text file with filename (.dns).

Secondary Zone: It maintains a read-only copy of zone database on another DNS server. Also, it acts as a back-up server to the primary server by providing fault tolerance and load balancing

Stub Zone: It consists of a copy of name server and SOA records which is used for reducing the DNS search orders.

3) Explain what does IntelliMirror do?

IntelliMirror helps to reconcile desktop settings, applications and stored files for users especially for those users who move between workstations or those who works offline

4) In the case when MSI file is not available, how you can install an app?

To add the application using the Software Installer.ZAP text file can be used rather than the windows installer

5) Explain how you can set up remote installation procedure without giving access to user?

To do that, you have to go to,

gponameà User Configuration à Windows Settings à Remote Installation Services à Choice Options

6) What does it mean by “tattooing” the Registry ?

“ Tattooing” the registry means user can modify and view user preference that are not stored in the maintained portions of the Registry. Even if the group policy is changed or removed, the user preference will still persist in the registry.

7) Mention how many types of queries DNS does?

The types of queries DNS does are

Iterative Query

Recursive Query

Window Server

8) Explain what is the primary function of the domain controller?

Primary function of the domain controller is to validate users to the networks, it also provide a catalog of Active Directory Objects.

9) What information is required when TCP/IP is configured on Window Server?

To configure a TCP/PI client for an IPv4 client, you have to provide the IP address and the subnet mask.

10) Explain what does it mean caching only server in terms of DNS?

The caching only DNS server provides information related to queries based on the data it contains in its DNS cache.

11) Explain what is the way to configure the DHCP server such that it allocates the same IP address to certain devices each time the address is removed?

To configure the DHCP server, you can create a reservation for the device. To create a reservation, you must know the MAC hardware address of the device. To determine the MAC address for a network device you can use the ipconfig or nbs tat command line utilities.

12) Explain what is LDAP?

To look up for the information from the server, e-mail and another program follows or uses the internet protocol. This protocol is referred as LDAP or Lightweight Directory Access Protocol.

13) Explain what is SYSVOL folder?

It is a set of files and folders that is stored on the local hard disk of each domain controller in a domain and are replicated by the FRS ( File Replication Service). These files contain group or user policy information.

14) Explain what is the difference between a thread and a computer process?

Computer Process: In computing, a process is an instance of a computer program that is executed sequentially by a computer system which can run several computer programs concurrently.

Thread: A thread is a several executable program that work together as a single process. For instance, one thread might send an error message to the user; another might handle error signals while the third thread might be executing the original action.

15) Explain what is INODE?

INODE holds the metadata of files; INODE is a pointer to a block on the disk, and it is unique.

In simple words, it is a unique number allocated to a file in UNIX-like OS.

16) Explain what is RAID in Windows Server?

For storing same data at a different place RAID or Redundant Array of Independent Disks strategy is used. It is a strategy for building fault tolerance and increase the storage capacity. On separate drives it allows you to combine one or more volumes so that they are accessed by a single drive letter

17) Explain what is the purpose of deploying local DNS servers?

A local DNS server provides the local mapping of fully qualified domain names to IP addresses. To resolve remote requests related to the domains names on your network, local DNS servers can provide record information to remote DNS servers.

18) To check TCP/IP configurations and IP connectivity, what are the two command line utilities that can be used?

Ipconfig: To check the computer’s IP configuration, command ipconfig can be used and also it can be used to renew the client’s IP address if it is provided by a DHCP server.

Ping: To check the connection between the local computer and any of the other computer device on the network Ping command is used

19) Explain if it is possible to connect Active Directory to other 3rd party Directory services?

Yes, you can connect other vendors directory services with Microsoft version. By using dirXML or LDAP to connect to other directories.

20) Explain where is the AD database is held?

AD database is saved in %systemroot%/ntds. Files that controls the AD structure are

ntds.dit

edb.log

res1.log

res2.log

edn.chk

21) Explain what is the major difference between NTFS ( New Technology File System) or FAT (File Allocation Table) on a local server?

For local users FAT (File Allocation Table) and FAT32 provides security, while NTFS ( New Technology File System) provides security for domain users as well as local users. NTFS provides file level security which is not possible through FAT32.

22) Mention what windows server 2008 service is used to install client operating system over the network?

WDE ( Windows Deployment Services ) allows you to install client and server operating systems over the network to any computer with a PXE enabled network interface

Question1. What Is Active Directory?

Answer :

Active Directory (AD) is a directory service developed by Microsoft and used to store objects like User, Computer, printer, Network information, It facilitate to manage your network effectively with multiple Domain Controllers in different location with AD database, able to manage/change AD from any Domain Controllers and this will be replicated to all other DC’s, centralized Administration with multiple geographical location and authenticates users and computers in a Windows domain.

Question2. What Is Tree?

Answer :

Tree is a hierarchical arrangement of windows Domain that share a contiguous name space.

Question3. What Is Domain?

Answer :

Active Directory Domain Services is Microsoft’s Directory Server. It provides authentication and authorization mechanisms as well as a framework within which other related services can be deployed.

Question4. What Is Active Directory Domain Controller (dc)?

Answer :

Domain Controller is the server which holds the AD database, All AD changes get replicated to other DC and vise vase.

Question5. What Is Forest?

Answer :

Forest consists of multiple Domains trees. The Domain trees in a forest do not form a contiguous name space however share a common schema and global catalog (GC)

Question6. What Is Schema?

Answer :

Active directory schema is the set of definitions that define the kinds of object and the type of information about those objects that can be stored in Active Directory

Active directory schema is Collection of object class and there attributes

Object Class = User

Attributes = first name, last name, email, and others

Question7. Can We Restore A Schema Partition?

Answer :

http://www.windowstricks.in/2014/01/can-i-restore-schema-partition.html

Question8. Tel Me About The Fsmo Roles?

Answer :

Schema Master

Domain Naming Master

Infrastructure Master

RID Master

PDC

Schema Master and Domain Naming Master are forest wide role and only available one on each Forest, Other roles are Domain wide and one for each Domain.

AD replication is multi master replication and change can be done in any Domain Controller and will get replicated to others Domain Controllers, except above file roles, this will be flexible single master operations (FSMO), these changes only be done on dedicated Domain Controller so it’s single master replication.

Question9. How To Check Which Server Holds Which Role?

Answer :

Netdom query FSMO.

Question10. Tel Me About Active Directory Database And List The Active Directory Database Files?

Answer :

NTDS.DIT

EDB.Log

EDB.Che

Res1.log and Res2.log

All AD changes didn’t write directly to NTDS.DIT database file, first write to EDB.Log and from log file to database, EDB.Che used to track the database update from log file, to know what changes are copied to database file.

NTDS.DIT: NTDS.DIT is the AD database and store all AD objects, Default location is the %system root%nrdsnrds.dit, Active Directory database engine is the extensible storage engine which us based on the Jet database

EDB.Log: EDB.Log is the transaction log file when EDB.Log is full, it is renamed to EDB Num.log where num is the increasing number starting from 1, like EDB1.Log

EDB.Che: EDB.Che is the checkpoint file used to trace the data not yet written to database file this indicate the starting point from which data is to be recovered from the log file in case if failure

Res1.log and Res2.log: Res is reserved transaction log file which provide the transaction log file enough time to shutdown if the disk didn’t have enough space.

Question11. What Is Active Directory Partitions?

Answer :

Active Directory partition is how and where the AD information logically stored.

Question12. What Are All The Active Directory Partitions?

Answer :

Schema

Configuration

Domain

Application partition

Question13. What Is Use Active Directory Partitions? And How To Find The Active Directory Partitions And There Location?

Answer :

Schema Partition – It store details about objects and attributes. Replicates to all domain controllers in the Forest

DN location is CN=Schema,CN=Configuration,DC=Domainname, DC=com

Configuration Partition – It store details about the AD configuration information like, Site, site-link, subnet and other replication topology information. Replicates to all domain controllers in the Forest

DN Location is CN=Configuration,DC=Domainname,DC=com

Domain Partitions – object information for a domain like user, computer, group, printer and other Domain specific information. Replicates to all domain controllers within a domain

DN Location is DC=Domainname,DC=com

Application Partition – information about applications in Active Directory. Like AD integrated DNS is used there are two application partitions for DNS zones – ForestDNSZones and DomainDNSZones, see more

Question14. How To Configure Active Directory Partitions?

Answer :

You can only configure the Application partition manually to use with AD integrated applications.

Question15. How To Take Active Directory Backup?

Answer :

System state backup will backup the Active Directory, NTbackup can be used to backup active directory.

Question16. Active Directory Restores Types?

Answer :

Authoritative restore

Non-authoritative restore

Question17. Non-authoritative Restore Of Active Directory?

Answer :

Non-authoritative restore is restore the domain controller to its state at the time of backup, and allows normal replication to overwrite restored domain controller with any changes that have occurred after the backup.

After system state restore, domain controller queries its replication partners and get the changes after backup date, to ensure that the domain controller has an accurate and updated copy of the Active Directory database.

Non-authoritative restore is the default method for restoring Active Directory, just a restore of system state is non-authoritative restore and mostly we use this for Active Directory data loss or corruption.

Question18. How Perform A Non-authoritative Restore?

Answer :

Just start the domain controller in Directory Services Restore Mode and perform system state restore from backup

Question19. Authoritative Restore Of Active Directory?

Answer :

An authoritative restore is next step of the non-authoritative restore process. We have do non-authoritative restore before you can perform an authoritative restore. The main difference is that an authoritative restore has the ability to increment the version number of the attributes of all objects or an individual object in an entire directory, this will make it authoritative restore an object in the directory. This can be used to restore a single deleted user/group and event an entire OU.

In a non-authoritative restore, after a domain controller is back online, it will contact its replication partners to determine any changes since the time of the last backup. However the version number of the object attributes that you want to be authoritative will be higher than the existing version numbers of the attribute, the object on the restored domain controller will appear to be more recent and therefore, restored object will be replicated to other domain controllers in the Domain.

Question20. What Are Active Directory Partitions Can Be Restored?

Answer :

You can authoritatively restore only objects from configuration and domain partition. Authoritative restores of schema-naming contexts are not supported.

Question1. What Is Dns?

Answer :

DNS stands for Domain Name System. It is a hierarchical system for identifying hosts on the Internet or on a private, corporate TCP/IP internetwork. It resolves the IP addresses to host names (or friendly internet names) and Host names to IP addresses.

Question2. What Is The Structure Of Dns?

Answer :

The structure of DNS starts with root domain. Then it (root domain) braches to TOP level domains, then second level domains, and so on to the individual host names.

Root Domain –> Top level Domains–> Second level Domains–> So on so forth up to individual host systems

Question3. How To Install Dns?

Answer :

We can install DNS in 3 different ways:

While installing Operating System: While installing Operating System, It asks at Network Settings whether you want Typical settings or Custom Settings. Select Custom Settings–>Select Network Services–>click on Details–>Select DNS–>ok

While installing through Active Directory (DCPROMO): (During installation it asks for CD)

Independently: Programs –>Settings –>Control Panel –Add/Remove Programs –>Add/Remove Windows Components –>Select the Network Services–>Click on properties –>Select DNS –>OK (During the installation it asks for CD)

Question4. How To Open Dns?

Answer :

Start–>Programs–>Administrative Tools–>DNS

Or

Start–>Run–>dnsmgmt.msc

Or

Start–>Run –>cmd –>dnsmgmt.msc

Question5. How To Configure The Dns?

Answer :

Open the DNS Console. Then you will find there

DNS

Server name

Forward Lookup Zone

Reverse Lookup Zone

Note: If you have selected create automatically zones during the setup, then it creates the root zone and domain zone under forward lookup zone. If no zones are there under forward lookup zone first create root zone then create domain zone.

Question6. What Tabs Are There On Properties Of Domain?

Answer :

Domain properties contain the following tabs:

General

Start of Authority (SOA)

Named servers

WINS

Zone transfers

Question7. What Tabs Are There On Properties Of Sever?

Answer :

Server properties contain the following tabs:

Interface

Forwarders

Advanced

Root hints

Logging

Monitoring

Question8. Where To Create The Primary, Secondary, Active Directory Integrated Zones?

Answer :

If you want to create an Active Directory integrated zone, the server must be Domain Controller.

If you want to create the Primary DNS, you can create on Domain Controller or Member server. But if create on member you could not get 4 options under the domain which are meant for Active directory.

You can create Secondary zone on a Member Server or on a Domain Controller. There is no difference between them.

Question9. What Commands Do We Use For Dns?

Answer :

We use the following commands for DNS:

Nslookup (and all interactive mode commands)

Ipconfig /fulshdns

Ipconfig /registerdns

Question10. What Is The Purpose Of Forward Lookup?

Answer :

Forward lookup resolves the Hostnames (Friendly Name) to IP addresses.

Question11. What Is The Purpose Of Reverse Lookup Zone?

Answer :

Reverse lookup resolves the IP addresses to Host names.

Question12. What Is The Difference Between Primary Zone And Secondary Zone?

Answer :

Primary zone has read and write permissions, whereas Secondary zone has read only permission.

Secondary zone is used for Backup and Load balancing.

Question13. How To Check Whether Dns Is Working Or Not?

Answer :

In order to check whether a DNS is working or not, type the command “nslookup” in command prompt. It will give the DNS server name and its IP address.

Question14. What Is Dynamic Updates In Dns?

Answer :

Generally we need to create a host record for newly joined computer (either client or Member server or Domain controller). If you enable dynamic Update option, then DNS itself creates associated host record for newly joined computers.

Question15. How To Get Dynamic Update Option?

Answer :

Right Click on any zone –>properties –>on General tab u will get

Allow Dynamic Updates? [\_Yes/No/Secure Updates]

Note: Put always Dynamic Updates “YES”

Note: If it is Active Directory Integrated zone you will get above three options.

But if it is Primary or Secondary zone you will get only “YES/NO” (You won’t get secure updates)

Question16. What Is Name Resolution?

Answer :

The process of translating the name into some object or information that the name represents is called name resolution. A telephone book forms a namespace in which the names of telephone subscribers can be resolved to the phone numbers.

Question17. What Is A Zone?

Answer :

Also called a zone of authority, zone is a subset of the Domain Name System (DNS) namespace that is managed by a name server. A database of records is called a zone.

Question18. What Is An Iterative Query?

Answer :

The query that has been sent to the DNS server from a Client is called iterative query.

(i. e., iterative query is nothing but gives the answer for my question, don’t ask to contact that person or this person or don’t say something else. Simply just answer to my question. That’s all)

Question19. What Is Recursive Query?

Answer :

Your DNS server requests the root level DNS server for specific IP address. Now DNS server says I don’t know but I can give the address other person who can help you in finding IP address.

Question20. What Type Of Records Do We Find In Dns Database?

Answer :

The most general records found in DNS database are

Host Record (A record)

Mail Exchange Record (MX record)

Canonical name or CNAME record (CNAME)

Question1. What Is Dhcp?

Answer :

Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to a computer from a defined range of numbers (i.e., a scope) configured for a given network.

Question2. What Is The Dhcp Process For Client Machine?

Answer :

A user turns on a computer with a DHCP client.

The client computer sends a broadcast request (called a DISCOVER or DHCPDISCOVER), looking for a DHCP server to answer.

The router directs the DISCOVER packet to the correct DHCP server.

The server receives the DISCOVER packet. Based on availability and usage policies set on the server, the server determines an appropriate address (if any) to give to the client. The server then temporarily reserves that address for the client and sends back to the client an OFFER (or DHCPOFFER) packet, with that address information. The server also configures the client’s DNS servers, WINS servers, NTP servers, and sometimes other services as well.

The client sends a REQUEST (or DHCPREQUEST) packet, letting the server know that it intends to use the address.

The server sends an ACK (or DHCPACK) packet, confirming that the client has a been given a lease on the address for a server-specified period of time.

Question3. What Is Dhcp Scope?

Answer :

DHCP scopes are used to define ranges of addresses from which a DHCP server can assign IP addresses to clients.

Question4. Types Of Scopes In Windows Dhcp?

Answer :

Normal Scope – Allows A, B and C Class IP address ranges to be specified including subnet masks, exclusions and reservations. Each normal scope defined must exist within its own subnet.

Multicast Scope – Used to assign IP address ranges for Class D networks. Multicast scopes do not have subnet masks, reservation or other TCP/IP options.

Multicast scope address ranges require that a Time To Live (TTL) value be specified (essentially the number of routers a packet can pass through on the way to its destination).

Superscope – Essentially a collection of scopes grouped together such that they can be enabled and disabled as a single entity.

Question5. What Is Authorizing Dhcp Servers In Active Directory?

Answer :

If a DHCP server is to operate within an Active Directory domain (and is not running on a domain controller) it must first be authorized.

This can be achieved either as part of the DHCP Server role installation, or subsequently using either DHCP console or at the command prompt using the netsh tool.

If the DHCP server was not authorized during installation, invoke the DHCP console (Start -> All Programs -> Administrative Tools -> DHCP),

right click on the DHCP to be authorized and select Authorize.

To achieve the same result from the command prompt, enter the following command:

netsh dhcp server serverID initiate auth

In the above command syntax, serverID is replaced by the IP address or full UNC name of system on which the DHCP server is installed.

Question6. What Ports Are Used By Dhcp And The Dhcp Clients?

Answer :

Requests are on UDP port 68, Server replies on UDP 67 .

Question7. List Some Benefits Of Using Dhcp?

Answer :

DHCP provides the following benefits for administering your TCP/IP-based network:

Safe and reliable configuration.DHCP avoids configuration errors caused by the need to manually type in values at each computer. Also, DHCP helps prevent address conflicts caused by a previously assigned IP address being reused to configure a new computer on the network.

Reduces configuration management.

Using DHCP servers can greatly decrease time spent to configuring and reconfiguring computers on your network. Servers can be configured to supply a full range of additional configuration values when assigning address leases.

These values are assigned using DHCP options. Also, the DHCP lease renewal process helps assure that where client configurations need to be updated often (such as users with mobile or portable computers who change locations frequently), these changes can be made efficiently and automatically by clients communicating directly with DHCP servers.

The following section covers issues that affect the use of the DHCP Server service with other services or network configurations. Using DNS servers with DHCP Using Routing and Remote Access servers with DHCP Multihomed DHCP servers.

Question8. Describe The Process Of Installing A Dhcp Server In An Ad Infrastructure?

Answer :

Open Windows Components Wizard. Under Components , scroll to and click Networking Services. Click Details . Under Subcomponents of Networking Services , click Dynamic Host Configuration Protocol (DHCP) and then click OK.

Click Next . If prompted, type the full path to the Windows Server 2003 distribution files, and then click Next. Required files are copied to your hard disk.

Question9. How To Authorize A Dhcp Server In Active Directory Open Dhcp?

Answer :

In the console tree, click DHCP

On the Action menu, click Manage authorized servers.

The Manage Authorized Servers dialog box appears. Click Authorize.

When prompted, type the name or IP address of the DHCP server to be authorized, and then click OK.

Question10. What Is Dhcpinform?

Answer :

DHCPInform is a DHCP message used by DHCP clients to obtain DHCP options. While PPP remote access clients do not use DHCP to obtain IP addresses for the remote access connection, Windows 2000 and Windows 98 remote access clients use the DHCPInform message to obtain DNS server IP addresses, WINS server IP addresses, and a DNS domain name.

The DHCPInform message is sent after the IPCP negotiation is concluded. The DHCPInform message received by the remote access server is then forwarded to a DHCP server. The remote access server forwards DHCPInform messages only if it has been configured with the DHCP Relay Agent.

Question11. Describe The Integration Between Dhcp And Dns?

Answer :

Traditionally, DNS and DHCP servers have been configured and managed one at a time. Similarly, changing authorization rights for a particular user on a group of devices has meant visiting each one and making configuration changes.

DHCP integration with DNS allows the aggregation of these tasks across devices, enabling a company’s network services to scale in step with the growth of network users, devices, and policies, while reducing administrative operations and costs. This integration provides practical operational efficiencies that lower total cost of ownership.

Creating a DHCP network automatically creates an associated DNS zone, for example, reducing the number of tasks required of network administrators. And integration of DNS and DHCP in the same database instance provides unmatched consistency between service and management views of IP address-centric network services data.

Question12. What Protocol And Port Does Dhcp Use?

Answer :

DHCP, like BOOTP runs over UDP, utilizing ports 67 and 68.

Question13. Can A Dhcp Server Back Up Another Dhcp Server?

Answer :

You can have two or more servers handing out leases for different addresses. If each has a dynamic pool accessible to the same clients, then even if one server is down, one of those clients can lease an address from the other server. However, without communication between the two servers to share their information on current leases, when one server is down, any client with a lease from it will not be able to renew their lease with the other server.

Such communication is the purpose of the “server to server protocol”. It is possible that some server vendors have addressed this issue with their own proprietary server-to-server communication.

Question14. What Is A Mac Address?

Answer :

A MAC address (also called an Ethernet address or an IEEE MAC address) is a number (typically written as twelve hexadecimal digits, 0 through 9 and A through F, or as six hexadecimal numbers separated by periods or colons, i.e. 0080002012ef, 0:80:0:2:20:ef) which uniquely identifes a computer that has an Ethernet interface.

Unlike the IP number, it includes no indication of where your computer is located. In DHCP’s typical use, the server uses a requesting computer’s MAC address to uniquely identify it.

Question15. Can Dhcp Support Statically Defined Addresses?

Answer :

Yes. At least there is nothing in the protocol to preclude this and one expects it to be a feature of any DHCP server. This is really a server matter and the client should work either way. The RFC refers to this as manual allocation.

Question16. Is A Dhcp Server “supposed To” Be Able To Support A Bootp Client?

Answer :

The RFC on such interoperability (1534) is clear: “In summary, a DHCP server:

MAY support BOOTP clients,” (section 2). The word “MAY” indicates such support, however useful, is left as an option. A source of confusion on this point is the following statement in section 1.5 of RFC 1541: “DHCP must provide service to existing BOOTP clients.”

However, this statement is one in a list of “general design goals for DHCP”, i.e. what the designers of the DHCP protocol set as their own goals. It is not in a list of requirements for DHCP servers.

Question17. How Can I Relay Dhcp If My Router Does Not Support It?

Answer :

A server on a net(subnet) can relay DHCP or BOOTP for that net. Microsoft has software to make Windows NT do this.

Question18. What Is A Client Id?

Answer :

What is termed the Client ID for the purposes of the DHCP protocol is whatever is used by the protocol to identify the client computer. By default, DHCP implementations typically employ the client’s MAC address for this purpose, but the DHCP protocol allows other options. Some DHCP implementations have a setup option to specify the client ID you want. One alternative to the MAC address is simply a character string of your choice.

In any case, in order for DHCP to function, you must be certain that no other client is using the client ID you choose, and you must be sure the DHCP server will accept it.

Question19. Is A Dhcp Client “supposed To” Be Able To Use A Bootp Server?

Answer :

The RFC on such interoperability (1534) is clear: “A DHCP client MAY use a reply from a BOOTP server if the configuration returned from the BOOTP server is acceptable to the DHCP client.”. The word “MAY” indicates such support, however useful, is left as an option.

Question20. How Long Should A Lease Be?

Answer :

A very relevant factor is that the client starts trying to renew the lease when it is halfway through: thus, for example, with a 4 day lease, the client which has lost access to its DHCP server has 2 days from when it first tries to renew the lease until the lease expires and the client must stop using the network.

During a 2- day outage, new users cannot get new leases, but no lease will expire for any computer turned on at the time that the outage commences. Another factor is that the longer the lease the longer time it takes for client configuration changes controlled by DHCP to propogate.

What is Active Directory?

Active Directory (AD) is a directory service developed by Microsoft and used to store objects like User, Computer, printer, Network information, It facilitate to manage your network effectively with multiple Domain Controllers in different location with AD database, able to manage/change AD from any Domain Controllers and this will be replicated to all other DC’s, centralized Administration with multiple geographical location and authenticates users and computers in a Windows domain

What is LDAP and how the LDAP been used on Active Directory(AD)?

http://www.windowstricks.in/ldap-and-ldap-query

What is Tree?

Tree is a hierarchical arrangement of windows Domain that share a contiguous name space

What is Domain?

Active Directory Domain Services is Microsoft’s Directory Server. It provides authentication and authorization mechanisms as well as a framework within which other related services can be deployed

What is Active Directory Domain Controller (DC)?

Domain Controller is the server which holds the AD database, All AD changes get replicated to other DC and vise vase

What is Forest?

Forest consists of multiple Domains trees. The Domain trees in a forest do not form a contiguous name space however share a common schema and global catalog (GC)

What is Schema?

Active directory schema is the set of definitions that define the kinds of object and the type of information about those objects that can be stored in Active Directory

Active directory schema is Collection of object class and there attributes

Object Class = User

Attributes = first name, last name, email, and others

Can we restore a schema partition?

http://www.windowstricks.in/2014/01/can-i-restore-schema-partition.html

Tel me about the FSMO roles?

Schema Master

Domain Naming Master

Infrastructure Master

RID Master

PDC

Schema Master and Domain Naming Master are forest wide role and only available one on each Forest, Other roles are Domain wide and one for each Domain

AD replication is multi master replication and change can be done in any Domain Controller and will get replicated to others Domain Controllers, except above file roles, this will be flexible single master operations (FSMO), these changes only be done on dedicated Domain Controller so it’s single master replication

How to check which server holds which role?

Netdom query FSMO

Which FSMO role is the most important? And why?

Interesting question which role is most important out of 5 FSMO roles or if one role fails that will impact the end-user immediately

Most armature administrators pick the Schema master role, not sure why maybe they though Schema is very critical to run the Active Directory

Correct answer is PDC, now the next question why? Will explain role by role what happens when a FSMO role holder fails to find the answer

Schema Master – Schema Master needed to update the Schema, we don’t update the schema daily right, when will update the Schema? While the time of operating system migration, installing new Exchange version and any other application which requires extending the schema

So if are Schema Master Server is not available, we can’t able to update the schema and no way this will going to affect the Active Directory operation and the end-user

Schema Master needs to be online and ready to make a schema change, we can plan and have more time to bring back the Schema Master Server

Domain Naming Master – Domain Naming Master required to creating a new Domain and creating an application partition, Like Schema Master we don’t cerate Domain and application partition frequently

So if are Domain Naming Master Server is not available, we can’t able to create a new Domain and application partition, it may not affect the user, user event didn’t aware Domain Naming Master Server is down

Infrastructure Master – Infrastructure Master updates the cross domain updates, what really updates between Domains? Whenever user login to Domain the TGT has been created with the list of access user got through group membership (user group membership details) it also contain the user membership details from trusted domain, Infrastructure Master keep this information up-to-date, it update reference information every 2 days by comparing its data with the Global Catalog (that’s why we don’t keep Infrastructure Master and GC in same server)

In a single Domain and single Forest environment there is no impact if the Infrastructure Master server is down

In a Multi Domain and Forest environment, there will be impact and we have enough time to fix the issue before it affect the end-user

RID Master –Every DC is initially issued 500 RID’s from RID Master Server. RID’s are used to create a new object on Active Directory, all new objects are created with Security ID (SID) and RID is the last part of a SID. The RID uniquely identifies a security principal relative to the local or domain security authority that issued the SID

When it gets down to 250 (50%) it requests a second pool of RID’s from the RID master. If RID Master Server is not available the RID pools unable to be issued to DC’s and DC’s are only able to create a new object depends on the available RID’s, every DC has anywhere between 250 and 750 RIDs available, so no immediate impact

PDC – PDC required for Time sync, user login, password changes and Trust, now you know why the PDC is important FSMO role holder to get back online, PDC role will impact the end-user immediately and we need to recover ASAP

The PDC emulator Primary Domain Controller for backwards compatibility and it’s responsible for time synchronizing within a domain, also the password master. Any password change is replicated to the PDC emulator ASAP. If a logon request fails due to a bad password the logon request is passed to the PDC emulator to check the password before rejecting the login request.

Tel me about Active Directory Database and list the Active Directory Database files?

NTDS.DIT

EDB.Log

EDB.Che

Res1.log and Res2.log

All AD changes didn’t write directly to NTDS.DIT database file, first write to EDB.Log and from log file to database, EDB.Che used to track the database update from log file, to know what changes are copied to database file.

NTDS.DIT: NTDS.DIT is the AD database and store all AD objects, Default location is the %system root%\nrds\nrds.dit, Active Directory database engine is the extensible storage engine which us based on the Jet database

EDB.Log: EDB.Log is the transaction log file when EDB.Log is full, it is renamed to EDB Num.log where num is the increasing number starting from 1, like EDB1.Log

EDB.Che: EDB.Che is the checkpoint file used to trace the data not yet written to database file this indicate the starting point from which data is to be recovered from the log file in case if failure

Res1.log and Res2.log: Res is reserved transaction log file which provide the transaction log file enough time to shutdown if the disk didn’t have enough space

What are group policies?

Group policies specify how programs, network resources, and the operating system work for users and computers in an organization. They are collections of user and computer configuration settings that are applied on the users and computers (not on groups). For better administration of group policies in the Windows environment, the group policy objects (GPOs) are used.

What is GPO?

Group policy object (GPO) is a collection of group policy settings. It can be created using a Windows utility known as the Group Policy snap-in. GPO affects the user and computer accounts located in sites, domains, and organizational units (OUs). The Windows 2000/2003 operating systems support two types of GPOs, local and non-local (Active Directory-based) GPOs.

What is Local GPOs/policy?

Local GPOs are used to control policies on a local server running Windows 2000/2003 Server. On each Windows 2000/2003 server, a local GPO is stored. The local GPO affects only the computer on which it is stored. By default, only Security Settings nodes are configured. The rest of the settings are either disabled or not enabled. The local GPO is stored in the %systemroot%SYSTEM32GROUPPOLICY folder.

What is Non-local Policy?

Non-local GPOs are used to control policies on an Active Directory-based network. A Windows 2000/2003 server needs to be configured as a domain controller on the network to use a non-local GPO. The non-local GPOs must be linked to a site, domain, or organizational unit (OU) to apply group policies to the user or computer objects. The non-local GPOs are stored in %systemroot%SYSVOLPOLICIESADM, where is the GPO’s globally unique identifier. Two non-local GPOs are created by default when the Active Directory is installed:

1. Default Domain Policy: This GPO is linked to the domain and it affects all users and computers in the domain.

2. Default Domain Controllers Policy: This GPO is linked to the Domain Controllers OU and it affects all domain controllers placed in this OU.

Multiple GPOs

GPO Apply order

When multiple group policy objects are assigned, the group policies are applied in the following order:

• The local group policy object is applied first

• Then, the group policy objects linked to sites are applied

If multiple GPOs exist for a site, they are applied in the order specified by an administrator

• GPOs linked to the domains are applied in the specified order

• Finally, GPOs linked to OUs are applied

The OU group policy objects are set from the largest to the smallest organizational unit, i.e., first the parent OU and then the child OU.

By default, a policy applied later overwrites a policy that was applied earlier. Hence, the settings in a child OU can override the settings in the parent OU

Group policy settings are cumulative if they are compatible with each other. In case they conflict with each other, the GPO processed later takes precedence.

What is No Override? Block Policy Inheritance?

The following are the exceptions with regard to the above-mentioned settings:

No Override:

Any GPO can be set to No Override. If the No Override configuration is set to a GPO, no policy configured in the GPO can be overridden. If more than one GPO has been set to No Override, then the one that is the highest in the Active Directory hierarchy takes precedence

Block Policy Inheritance:

The Block Policy Inheritance option can be applied to the site, domain, or OU. It deflects all group policy settings that reach the site, domain, or OU from the object higher in the hierarchy. However, the GPOs configured with the No Override option are always applied

What is Loopback policy?

See more on Loopback policy

Is group policy from Parent Domain cab be inherited to child Domain?

Group Policy Inheritance

The group policies are inherited from parent to child within a domain. They are not inherited from parent domain to child domain

Following are the rules regarding group policy inheritance:

A policy setting is configured (Enabled or Disabled) for a parent OU, and the same policy setting is not configured for its child OUs. The child OUs inherit the parent’s policy

A policy setting is configured (Enabled or Disabled) for a parent OU, and the same policy setting is configured for its child OUs. The child OUs settings override the settings inherited from the parent’s OU

If any policy is not configured, no inheritance takes place

Compatible policy settings configured at the parent and child OUs are accumulated

Incompatible policy settings from the parent OU are not inherited

What is security filtering? Filtering Scope of GPOs

Although GPOs are linked to the site, domain, or OUs, and they cannot be linked to the security groups directly, applying permissions to the GPO can filter its scope. The policies in a non-local GPO apply only to users who have the Read and Apply Group Policy permissions set to Allow

What is the SYSVOL folder?

The sysVOL folder stores the server’s copy of the domain’s public files. The contents such as group policy, users etc of the sysvol folder are replicated to all domain controllers in the domain.

The sysvol folder must be located on an NTFS volume.

Que.: What is Active Directory?

Ans. Active Directory is a Meta Data. Active Directory is a data base which store a data base like your user information, computer information and also other network object info. It has capabilities to manage and administor the complite Network which connect with AD.

Que.: What is the Global Catalog?

Ans.: Global Catalog is a server which maintains the information about multiple domain with trust relationship agreement..

Que: What is Active Directory?

Ans: Active Directory directory service is an extensible and scalable directory service that enables you to manage network resources efficiently.

Q01: What is Active Directory?

Ans:Active Directory is directory service that stores information about objects on a network and makes this information available to users and network administrators.

Active Directory gives network users access to permitted resources anywhere on the network using a single logon process.

It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration

3for all network objects.

Q; What is active directory?

Ans: active directory is a domain controller which is use to authenticate and administrate the group of computer,user,server etc. remotely. all the policies and security will be applicable on the client machine which one is join the domain.and all this policies and security is defined in active directory.

Q2: What is LDAP?

Ans2: LDAP(light weight directory accerss protocol) is an internet protocol which Email and other services is used to look up information from the server.

Q 18: What is KCC ?

Ans 18: KCC ( knowledge consistency checker ) is used to generate replication topology for inter site replication and for intrasite replication.with in a site replication traffic is done via remote procedure calls over ip, while between site it is done through either RPC or SMTP.

Q 10: What is Global Catalog Server ?

Ans 10 : Global Catalog Server is basically a container where you put the same type of member ,computer etc and applied the policies and security on the catalog server in place of individual user or computer.

Q; What is active directory?

active directory is a domain controller which is use to authenticate and administrate the group of computer,user,server etc. remotely. all the policies and security will be applicable on the client machine which one is join the domain.and all this policies and security is defined in active directory.

Q 10 : what is Global catalog server GC?

Ans : i m sorry i was given wrong ans of this question above but now im giving the exact ans of this question, and th ans which iwas given previously is the ans of Organisatinal Unit not of GC….. and the ans is

The global catalog is a distributed data repository that contains a searchable, partial representation of every object in every domain in a multidomain Active Directory forest. The global catalog is stored on domain controllers that have been designated as global catalog servers and is distributed through multimaster replication. Searches that are directed to the global catalog are faster because they do not involve referrals to different domain controllers.

Q 4: Where is the AD database held? What other folders are related to AD?

A 4: The AD data base is store in NTDS.DIT.

Q 5 : What is the SYSVOL folder?

A 5; The sysVOL folder stores the server’s copy of the domain’s public files. The contents such as group policy, users etc of the sysvol folder are replicated to all domain controllers in the domain.

Q 19: What is the ISTG? Who has that role by default?

A 19: Windows 2000 Domain controllers each create Active Directory Replication connection objects representing inbound replication from intra-site replication partners. For inter-site replication, one domain controller per site has the responsibility of evaluating the inter-site replication topology and creating Active Directory Replication Connection objects for appropriate bridgehead servers within its site. The domain controller in each site that owns this role is referred to as the Inter-Site Topology Generator (ISTG).

Q :15 What is LDP? What is REPLMON? What is ADSIEDIT? What is NETDOM? What is REPADMIN?

A 15 : LDP : Label Distribution Protocol (LDP) is often used to establish MPLS LSPs when traffic engineering is not required. It establishes LSPs that follow the existing IP routing, and is particularly well suited for establishing a full mesh of LSPs between all of the routers on the network.

Replmon : Replmon displays information about Active Directory Replication.

ADSIEDIT :ADSIEdit is a Microsoft Management Console (MMC) snap-in that acts as a low-level editor for Active Directory. It is a Graphical User Interface (GUI) tool. Network administrators can use it for common administrative tasks such as adding, deleting, and moving objects with a directory service. The attributes for each object can be edited or deleted by using this tool. ADSIEdit uses the ADSI application programming interfaces (APIs) to access Active Directory. The following are the required files for using this tool: ADSIEDIT.DLL

ADSIEDIT.MSCNETDOM : NETDOM is a command-line tool that allows management of Windows domains and trust relationships. It is used for batch management of trusts, joining computers to domains, verifying trusts, and secure channels.

REPADMIN :

This command-line tool assists administrators in diagnosing replication problems between Windows domain controllers.Administrators can use Repadmin to view the replication topology (sometimes referred to as RepsFrom and RepsTo) as seen from the perspective of each domain controller. In addition, Repadmin can be used to manually create the replication topology (although in normal practice this should not be necessary), to force replication events between domain controllers, and to view both the replication metadata and up-to-dateness vectors.

Q 36: how to take backup of AD ?

A 36 : for taking backup of active directory you have to do this :

first go to START -> PROGRAM ->ACCESORIES -> SYSTEM TOOLS -> BACKUP

when the backup screen is flash then take the backup of SYSTEM STATE it will take the backup of all the necessary information about the syatem including AD backup , DNS ETC.

Q 37 : how to restore the AD ?

a 37 : For ths do the same as above in the question 36 but in place of backup you select the restore option and restore the system state .

Q 19: What is the ISTG? Who has that role by default?

A 19: Inter-Site Topology Generator(istg) is responsible for managing the inbound replication connection objects for all bridgehead servers in the site in which it is located. This domain controller is known as the Inter-Site Topology Generator (ISTG). The domain controller holding this role may not necessarily also be a bridgehead server.

Q 29 :What are the DS\* commands

A 29 : You really are spoilt for choice when it comes to scripting tools for creating Active Directory objects. In addition to CSVDE, LDIFDE and VBScript, we now have the following DS commands: the da family built in utility DSmod - modify Active Directory attributesDSrm - to delete Active Directory objectsDSmove - to relocate objectsDSadd - create new accountsDSquery - to find objects that match your query attributesDSget - list the properties of an object

Q 30 :What’s the difference between LDIFDE and CSVDE? Usage considerations?

A 30 : CSVDE is a command that can be used to import and export objects to and from the AD into a CSV-formatted file. A CSV (Comma Separated Value) file is a file easily readable in Excel. I will not go to length into this powerful command, but I will show you some basic samples of how to import a large number of users into your AD. Of course, as with the DSADD command, CSVDE can do more than just import users. Consult your help file for more info.

Like CSVDE, LDIFDE is a command that can be used to import and export objects to and from the AD into a LDIF-formatted file. A LDIF (LDAP Data Interchange Format) file is a file easily readable in any text editor, however it is not readable in programs like Excel. The major difference between CSVDE and LDIFDE (besides the file format) is the fact that LDIFDE can be used to edit and delete existing AD objects (not just users), while CSVDE can only import and export objects.

Q 25 : What is tombstone lifetime attribute?

A 25 : The number of days before a deleted object is removed from the directory services. This assists in removing objects from replicated servers and preventing restores from reintroducing a deleted object. This value is in the Directory Service object in the configuration NIC.

You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that? How it is possibal

(20)What are the requirements for installing AD on a new server?

Ans:1)The Domain structure2)The Domain Name3)storage location of the database and log file4)Location of the shared system volume folder5)DNS config Methode6)DNS configuration

7. What are application partitions? When do I use them.

Ans: AN application diretcory partition is a directory partition that is replicated only to specific domain controller.Only domain controller running windows Server 2003 can host a replica of application directory partition.

Using an application directory partition provides redundany,availabiltiy or fault tolerance by replicating data to specific domain controller pr any set of domain controllers anywhere in the forest

Q:You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that? How it is possibal.

Ans:Login on client as Domain Admin user change whatever you need add printers etc go to system-User profiles copy this user profile to any location by select Everyone in permitted to use after copy change ntuser.dat to ntuser.man and assgin this path under user profile

Q. 8. How do you create a new application partition

ANS:

Use the DnsCmd command to create an application directory partition. To do this, use the following syntax:

DnsCmd ServerName /CreateDirectoryPartition FQDN of partition

Global catalog provides a central repository of domain information for the forest by storing partial replicas of all domain directory partitions. These partial replicas are distributed by multimaster replication to all global catalog servers in a forest.

How do you view all the GCs in the forest?

Ans

C:\>repadmin /showreps

domain\_controller

where domain\_controller is the DC you want to query to determine whether it’s a GC. The output will include the text DSA Options: IS\_GC if the DC is a GC. . . .

Trying to look at the Schema, how can I do that

Ans:

type “adsiedit.msc” in run or command prompt

Q. Can you connect Active Directory to other 3rd-party Directory Services? Name a few options.

Ans. Yes, you can use dirXML or LDAP to connect to other directories

In Novell you can use E-directory

Q 38 :How do you change the DS Restore admin password ?

Ans 38: A. In Windows 2000 Server, you used to have to boot the computer whose password you wanted to change in Directory Restore mode, then use either the Microsoft Management Console (MMC) Local User and Groups snap-in or the command

net user administrator \*

to change the Administrator password. Win2K Server Service Pack 2 (SP2) introduced the Setpwd utility, which lets you reset the Directory Service Restore Mode password without having to reboot the computer. (Microsoft refreshed Setpwd in SP4 to improve the utility’s scripting options.)

In Windows Server 2003, you use the Ntdsutil utility to modify the Directory Service Restore Mode Administrator password. To do so, follow these steps:

1. Start Ntdsutil (click Start, Run; enter cmd.exe; then enter ntdsutil.exe).

2. Start the Directory Service Restore Mode Administrator password-reset utility by entering the argument “set dsrm password” at the ntdsutil prompt:

ntdsutil: set dsrm password

3. Run the Reset Password command, passing the name of the server on which to change the password, or use the null argument to specify the local machine. For example, to reset the password on server thanos, enter the following argument at the Reset DSRM Administrator Password prompt:

Reset DSRM Administrator Password: reset password on server thanos

To reset the password on the local machine, specify null as the server name:

Reset DSRM Administrator Password: reset password on server null

4. You’ll be prompted twice to enter the new password. You’ll see the following messages:

5. Please type password for DS Restore Mode Administrator Account:

6. Please confirm new password:

Password has been set successfully.

7. Exit the password-reset utility by typing “quit” at the following prompts:

8. Reset DSRM Administrator Password: quit

ntdsutil: quit

Q.40: What are Group Policy objects (GPOs)?

A.40: Group Policy objects, other than the local Group Policy object, are virtual objects. The policy setting information of a GPO is actually stored in two locations: the Group Policy container and the Group Policy template. The Group Policy container is an Active Directory container that stores GPO properties, including information on version, GPO status, and a list of components that have settings in the GPO. The Group Policy template is a folder structure within the file system that stores Administrative Template-based policies, security settings, script files, and information regarding applications that are available for Group Policy Software Installation. The Group Policy template is located in the system volume folder (Sysvol) in the \Policies subfolder for its domain.

Q 41 :What is the order in which GPOs are applied ?

A 41: Group Policy settings are processed in the following order:

1.

Local Group Policy object—Each computer has exactly one Group Policy object that is stored locally. This processes for both computer and user Group Policy processing.

2.

Site—Any GPOs that have been linked to the site that the computer belongs to are processed next. Processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the site in Group Policy Management Console (GPMC). The GPO with the lowest link order is processed last, and therefore has the highest precedence.

3.

Domain—Processing of multiple domain-linked GPOs is in the order specified by the administrator, on the Linked Group Policy Objects tab for the domain in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

4.

Organizational units—GPOs that are linked to the organizational unit that is highest in the Active Directory hierarchy are processed first, then GPOs that are linked to its child organizational unit, and so on. Finally, the GPOs that are linked to the organizational unit that contains the user or computer are processed.

At the level of each organizational unit in the Active Directory hierarchy, one, many, or no GPOs can be linked. If several GPOs are linked to an organizational unit, their processing is in the order that is specified by the administrator, on the Linked Group Policy Objects tab for the organizational unit in GPMC. The GPO with the lowest link order is processed last, and therefore has the highest precedence.

This order means that the local GPO is processed first, and GPOs that are linked to the organizational unit of which the computer or user is a direct member are processed last, which overwrites settings in the earlier GPOs if there are conflicts. (If there are no conflicts, then the earlier and later settings are merely aggregated.)

What is LDAP?

Lightweight Directory Access Protocol

This article will tell you how to add your first Windows 2003 DC to an existing Windows 2000 domain. This article is particularly useful if you have Windows 2000 servers that will be replaced by new hardware running Windows Server 2003.

The first step is to install Windows 2003 on your new DC. This is a straighforward process, so we aren’t going to discuss that here.

Because significant changes have been made to the Active Directory schema in Windows 2003, we need to make our Windows 2000 Active Directory compatible with the new version. If you already have Windows 2003 DCs running with Windows 2000 DCs, then you can skip down to the part about DNS.

Before you attempt this step, you should make sure that you have service pack 4 installed on your Windows 2000 DC. Next, make sure that you are logged in as a user that is a member of the Schema Admin and Enterprise Admin groups. Next, insert the Windows 2003 Server installation CD into the Windows 2000 Server. Bring up a command line and change directories to the I386 directory on the installation CD. At the command prompt, type:

Code :

adprep /forestprep

After running this command, make sure that the updates have been replicated to all existing Windows 2000 DCs in the forest.

Next, we need to run the following command:

Code :

adprep /domainprep

The above command must be run on the Infrastructure Master of the domain by someone who is a member of the Domain Admins group.

Once this is complete, we move back to the Windows 2003 Server. Click ’start’ then ‘run” - type in dcpromo and click OK. During the ensuing wizard, make sure that you select that you are adding this DC to an existing domain.

After this process is complete, the server will reboot. When it comes back online, check and make sure that the AD database has been replicated to your new server.

Next, you will want to check and make sure that DNS was installed on your new server. If not, go to the control panel, click on ‘Add or Remove Programs’, and click the ‘Add/Remove Windows Components’ button. In the Windows Components screen, click on ‘Networking Services’ and click the details button. In the new window check ‘Domain Name System (DNS)’ and then click the OK button. Click ‘Next’ in the Windows Components screen. This will install DNS and the server will reboot. After reboot, pull up the DNS Management window and make sure that your DNS settings have replicated from the Windows 2000 Server. You will need to re-enter any forwarders or other properties you had set up, but the DNS records should replicate on their own.

The next 2 items, global catalog and FSMO roles, are important if you plan on decomissioning your Windows 2000 server(s). If this is the case, you need to transfer the global catalog from the old server to the new one.

First, let’s create a global catalog on our new server. Here are the steps:

1. On the domain controller where you want the new global catalog, start the Active Directory Sites and Services snap-in. To start the snap-in, click ‘Start’, point to ‘Programs’, point to ‘Administrative Tools’, and then click ‘Active Directory Sites and Services’.

2. In the console tree, double-click ‘Sites’, and then double-click ’sitename’.

3. Double-click ‘Servers’, click your domain controller, right-click ‘NTDS Settings’, and then click ‘Properties’.

4. On the General tab, click to select the Global catalog check box to assign the role of global catalog to this server.

5. Restart the domain controller.

Make sure you allow sufficient time for the account and the schema information to replicate to the new global catalog server before you remove the global catalog from the original DC or take the DC offline.

After this is complete, you will want to transfer or seize the FSMO roles for your new server. For instructions, read Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller.

After this step is complete, we can now run DCPROMO on the Windows 2000 Servers in order to demote them. Once this is complete, copy over any files you need to your new server and you should have successfully replaced your Windows 2000 server(s) with a new Windows 2003 server(s

Global Catalyst is the one where the authentication happens, by default primary domain controller is Global Catalyst, we can add global catalyst to improve the Netwrk Performance

What is Active Directory?

Its a Directory Service which stores and manages the information of Objects(User,computer,printer shared folder etc)

What are the requirements for installing AD on a new server?

Win2K3 CD

DNS

Static IP

You want to standardize the desktop environments (wallpaper, My Documents, Start menu, printers etc.) on the computers in one department. How would you do that?

go to Start->programs->Administrative tools->Active Directory Users and Computers

Right Click on Domain->click on preoperties

On New windows Click on Group Policy

Select Default Policy->click on Edit

on group Policy console

go to User Configuration->Administrative Template->Start menu and Taskbar

Select each property you want to modify and do the same

What are the required components of Windows Server 2003 for installing Exchange 2003? - ASP.NET, SMTP, NNTP, W3SVC

What must be done to an AD forest before Exchange can be deployed? - Setup /forestprep

What Exchange process is responsible for communication with AD? - DSACCESS

What 3 types of domain controller does Exchange access? - Normal Domain Controller, Global Catalog, Configuration Domain Controller

What connector type would you use to connect to the Internet, and what are the two methods of sending mail over that connector? - SMTP Connector: Forward to smart host or use DNS to route to each address

How would you optimise Exchange 2003 memory usage on a Windows Server 2003 server with more than 1Gb of memory? - Add /3Gb switch to boot.ini

What would a rise in remote queue length generally indicate? - This means mail is not being sent to other servers. This can be explained by outages or performance issues with the network or remote servers.

What would a rise in the Local Delivery queue generally mean? - This indicates a performance issue or outage on the local server. Reasons could be slowness in consulting AD, slowness in handing messages off to local delivery or SMTP delivery. It could also be databases being dismounted or a lack of disk space.

What are the standard port numbers for SMTP, POP3, IMAP4, RPC, LDAP and Global Catalog? - SMTP – 25, POP3 – 110, IMAP4 – 143, RPC – 135, LDAP – 389, Global Catalog - 3268

Name the process names for the following: System Attendant? – MAD.EXE, Information Store – STORE.EXE, SMTP/POP/IMAP/OWA – INETINFO.EXE

What is the maximum amount of databases that can be hosted on Exchange 2003 Enterprise? - 20 databases. 4 SGs x 5 DBs.

What are the disadvantages of circular logging? - In the event of a corrupt database, data can only be restored to the last backup.

19 Responses to “Windows sysadmin interview questions”

1) How windows server will configure?

Tell them that you have 400 pc based network, and you configure a Active Directory domain on windows servers to centralize administration tasks.

1) How windows server will configure?

Its depends on the role of the server. If you installing Active Directory, you have to run DCPROMO on commond prompt, and followed instructions.

Over all its depends on the role.

Simply you can say– there is an option in windows “Manage Server” once you follow the instructions it will guide you to configure your server.

2) How many types of servers?

If they are concern with Hardware server, tell them the hardware configuration and vendor of the server.

If they are asking about the types of windows server, tell them Standard, enterprise, or Small business server etc.

start > Run > Cmd >

Type

net send Computername type ur msg

Question 2: What must be done to an AD forest before Exchange can be deployed? - Setup /forestprep

question 2 is incorrect, in order for ms exchange 2k or 2003 to be sucessfully “deployed” both forestprep and domain prep must successfuly complete first, before the setup.exe of the actual exchange install, or the install and will error out if attempted.

What are main differences between WINS and DNS ???

WINS:- It is used to resolve IP address into netbios Viceversa it is used prior version of win 2000

DNS:-It is used to resolve IP address into host name.Viceversa it is used in 2000, XP, 2003 server

Active Directory

Active Directory is a centralized and standardized system, stores information about objects in a network and makes this information available to users and network administrators.

Domain Controller

In an Active Directory forest, the domain controller is a server that contains a writable copy of the Active Directory database, participates in Active Directory replication, and controls access to network resources.

Global catalog server

A global catalog server is a domain controller that stores information about all objects in the forest. Like all domain controllers, a global catalog server stores full, writable replicas of the schema and configuration directory partitions and a full, writable replica of the domain directory partition for the domain that it is hosting. In addition, a global catalog server stores a partial, read-only replica of every other domain in the forest. Partial replicas are stored on Global Catalog servers so that searches of the entire directory can be achieved without requiring referrals from one domain controller to another.

Partial information of other domains. Partial information nothing but classes and attributes (first name and last name and phones and addresses) attribute level security improvement in 2003….

OU:

"Organizational Units", are administrative-level containers on a computer, it allows administrators to organize groups of users together so that any changes, security privileges or any other administrative tasks could be accomplished more efficiently.

Domain:

Windows Domain is a logical grouping of computers that share common security and user account information.

Forest

A Windows forest is a group of one or more trusted Windows trees. The trees do not need to have contiguous DNS names. A forest shares a schema and global catalog servers. A single tree can also be called a forest.

Tree:

A Windows tree is a group of one or more trusted Windows domains with contiguous DNS domains. “Trusted” means that an authenticated account from one domain isn’t rejected by another domain. “Contiguous DNS domains” means that they all have the same root DNS name.

Site:

Sites are manually defined groupings of subnets. Objects in a site share the same global catalog servers, and can have a common set of group policies applied to them.

Schema:

The schema defines what attributes, objects, classes, and rules are available in the Active Directory.

SID (Security Identifier):

The SID is a unique name (alphanumeric character string) that is used to identify an object, such as a user or a group of users.

Group Policy

Group policy Architecture:

Group Policy objects (GPO):

A GPO is a collection of Group Policy settings, stored at the domain level as a virtual object consisting of a Group Policy container (GPC) and a Group Policy template (GPT).

Password history will store

Computer Configuration\Windows Settings\Security Settings\Account Policies\Password Policy

Group Policy Container (GPC)

The Group Policy container (GPC) is an Active Directory container that contains GPO properties, such as version information, GPO status, plus a list of other component settings.

Group Policy Template (GPT)

The Group Policy template (GPT) is a file system folder that includes policy data specified by .adm files, security settings, script files, and information about applications that are available for installation. The GPT is located in the system volume folder (SysVol) in the domain \Policies sub-folder.

Filtering the Scope of a GPO

By default, a GPO affects all users and computers that are contained in the linked site, domain, or organizational unit. The administrator can further specify the computers and users that are affected by a GPO by using membership in security groups.

Starting with Windows 2000, the administrator can add both computers and users to security groups. Then the administrator can specify which security groups are affected by the GPO by using the Access Control List editor.

Knowledge Consistency Checker (KCC)

The Knowledge Consistency Checker (KCC) is a Windows component that automatically generates and maintains the intra-site and inter-site replication topology.

Intrasite Replication

Replication that happens between controllers inside one site. All of the subnets inside the site should be connected by high speed network wires.

Intersite Replication

Intersite replication is replication between sites and must be set up by an administrator. Simple Mail Transfer Protocol (SMTP) may be used for replication between sites.

Active Directory Replication?

Replication must often occur both (intrasite) within sites and (Intersite) between sites to keep domain and forest data consistent among domain controllers that store the same directory partitions

Adprep.exe

Adprep.exe is a command-line tool used to prepare a Microsoft Windows 2000 forest or a Windows 2000 domain for the installation of Windows Server 2003 domain controllers.

USE:

When Microsoft Exchange Server is deployed in an organization, Exchange Server uses Active Directory as a data store and it extends the Windows 2000 Active Directory schema to enable it to store objects specific to Exchange Server. The ldapDisplayName of the attribute schema ms-Exch-Assistant-Name, ms-Exch-LabeledURI, and ms-Exch-House-Identifier defined by Exchange Server conflicts with the iNetOrgPerson schema that Active Directory uses in Windows Server 2003. When Windows Server 2003 Service Pack 1 is installed, Adprep.exe will be able to detect the presence of the schema conflict and block the upgrade of the schema until the issue has been resolved.

GUID:

When a new domain user or group account is created, Active Directory stores the account's SID in the Object-SID (objectSID) property of a User or Group object. It also assigns the new object a globally unique identifier (GUID), which is a 128-bit value that is unique not only in the enterprise but also across the world. GUIDs are assigned to every object created by Active Directory, not just User and Group objects. Each object's GUID is stored in its Object-GUID (objectGUID) property.

Active Directory uses GUIDs internally to identify objects.

SID:

A security identifier (SID) is a data structure in binary format that contains a variable number of values. When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security Principal SID created in a domain.

Lingering objects

When a domain controller is disconnected for a period that is longer than the TSL, one or more objects that are deleted from Active Directory on all other domain controllers may remain on the disconnected domain controller. Such objects are called lingering objects. Because the domain controller is offline during the time that the tombstone is alive, the domain controller never receives replication of the tombstone

Sysvol

Sysvol is a shared directory that stores the server copy of the domain’s public files, which are replicated among all domain controllers in the domain. The Sysvol contains the data in a GPO: the GPT, which includes Administrative Template-based Group Policy settings, security settings, script files, and information regarding applications that are available for software installation. It is replicated using the File Replication Service (FRS).

File Replication Service (FRS)

In Windows 2000, the SYSVOL share is used to authenticate users. The SYSVOL share includes group policy information which is replicated to all local domain controllers. File replication service (FRS) is used to replicate the SYSVOL share. The "Active Directory Users and Computers" tool is used to change the file replication service schedule.

Win logon

A component of the Windows operating system that provides interactive logon support, Winlogon is the service in which the Group Policy engine runs.

Lightweight Directory Access Protocol (LDAP)

It defines how clients and servers exchange information about a directory. LDAP version 2 and version 3 are used by Windows 2000 Server's Active Directory.

An LDAP URL names the server holding Active Directory services and the Attributed Name of the object. For example:

LDAP://SomeServer.Myco.Com/CN=jamessmith,CN=Sys,CN=Product,CN =Division,DC=myco,DC=domain-controller

USN

Each object has an Update Sequence Number (USN), and if the object is modified, the USN is incremented. This number is different on each domain controller. USN provides the key to multimaster replication.

Universal group membership caching

Due to available network bandwidth and server hardware limitations, it may not be practical to have a global catalog in smaller branch office locations. For these sites, you can deploy domain controllers running Windows Server 2003, which can store universal group membership information locally.

By default, the universal group membership information contained in the cache of each domain controller will be refreshed every 8 hours. Up to 500 universal group memberships can be updated at once. Universal groups couldn't be created in Mixed mode.

What is an ACL or access-control list?

A list of security protections that applies to an object. (An object can be a file, process, event, or anything else having a security descriptor.)

What is an ACE or access-control entry?

ACE contains a set of access rights and a security identifier (SID) that identifies a trustee for whom the rights are allowed, denied, or audited.

Flexible Single Master Operations (FSMO)

MultiMaster Operation:

In Windows 2000 & 2003, every domain controller can receive changes, and the changes are replicated to all other domain controllers. The day-to-day operations that are associated with managing users, groups, and computers are typically multimaster operations.

There is a set of Flexible Single Master Operations (FSMO) which can only be done on a single controller. An administrator determines which operations must be done on the master controller. These operations are all set up on the master controller by default and can be transferred later. FSMO operations types include:

Schema Master: The schema master domain controller controls all updates and modifications to the schema. There can be only one schema master in the whole forest.

Domain naming master: The domain naming master domain controller controls the addition or removal of domains in the forest and responsibility of ensuring that domain names are unique in the forest. There can be only one domain naming master in the whole forest.

Infrastructure Master:

Synchronizes cross-domain group membership changes. The infrastructure master cannot run on a global catalog server (unless all DCs are also GCs.)

The infrastructure is responsible for updating references from objects in its domain to objects in other domains. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

This works when we are renaming any group member ship object this role takes care.

Note: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

Relative ID (RID) Master:

It assigns RID and SID to the newly created object like Users and computers. If RID master is down (u can create security objects up to RID pools are available in DCs) else u can’t create any object one itSDs down

When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security principal SID created in a domain.

PDC Emulator - When Active Directory is in mixed mode, the computer Active Directory is on acts as a Windows NT PDC. The first server that becomes a Windows 2000 domain controller takes the role of PDC emulator by default.

Functions performed by the PDC emulator:

User account changes and password changes.

SAM directory replication requests.

Domain master browser requests

Authentication requests.

GPO

Time synchronization

New Active Directory features in Windows Server 2003

•

Multiple selection of user objects.

•

Drag-and-drop functionality.

•

Efficient search capabilities. Search functionality is object-oriented and provides an efficient search that minimizes

•

Saved queries. Save commonly used search parameters for reuse in Active Directory Users and Computers

•

Active Directory command-line tools.

•

InetOrgPerson class. The inetOrgPerson class has been added to the base schema as a security principal and can be used in the same manner as the user class. The userPassword attribute can also be used to set the account password.

•

Ability to add additional domain controllers using backup media. Reduce the time it takes to add an additional domain controller in an existing domain by using backup media.

•

Universal group membership caching. Prevent the need to locate a global catalog across a WAN when logging on by storing universal group membership information on an authenticating domain controller.

•

Secure LDAP traffic. Active Directory administrative tools sign and encrypt all LDAP traffic by default. Signing LDAP traffic guarantees that the packaged data comes from a known source and that it has not been tampered with.

•

Active Directory quotas. Quotas can be specified in Active Directory to control the number of objects a user, group, or computer can own in a given directory partition. Domain Administrators and Enterprise

Windows Functional levels

In Windows 2000 Active Directory domains is the concept of Mixed and Native Modes. The default mixed mode allows both NT and Windows 2000 domain controllers to coexist. Once you convert to Native Mode, you are only allowed to have Windows 2000 domain controllers in your domain. The conversion is a one-way conversion -- it cannot be reversed. In Windows Server 2003, Microsoft introduced forest and domain functional levels. The concept is rather similar to switching from Mixed to Native Mode in Windows 2000. The new functional levels give you additional capabilities that the previous functional levels didn’t have.

There are four domain functional levels:

Windows 2000 Mixed (supports NT4/2000/2003 DCs)

Windows 2000 Native (supports 2000/2003 DCs)

Windows Server 2003 Interim (supports NT4/2003 DCs)

Windows Server 2003 (supports only 2003 DCs)

And three forest functional levels:

Windows 2000 (supports NT4/2000/2003 DCs)

Windows 2000 Interim (supports NT4/2003 DCs)

Windows Server 2003 (supports only 2003 DCs)

To raise the domain functional level, you go to the properties of your domain in Active Directory Domains and Trusts. To raise the forest functional level you go to the properties of Active Directory Domains and Trusts at the root. Of course, if your domains are not at the correct level, you won’t be able to raise the forest functional level.

Directory partition

A directory partition, or naming context, is a contiguous Active Directory sub tree replicated on one, or more, Windows 2000 domain controllers in a forest. By default, each domain controller has a replica of three partitions: the schema partition the Configuration partition and a Domain partition.

Schema partition

It contains all class and attributes definitions for the forest. There is one schema directory partition per forest.

Configuration partition

It contains replication configuration information (and other information) for the forest. There is one configuration directory partition per forest.

Domain partition

It contains all objects that are stored by one domain. There is one domain directory partition for each domain in the forest.

Application Directory Partition

Application directory partitions are most often used to store dynamic data. An application partition can not contain security principles (users, groups, and computers).The KCC generates and maintains the replication topology for an application directory partition

Application: The application partition is a new feature introduced in Windows Server 2003. This partition contains application specific objects. The objects or data that applications and services store here can comprise of any object type excluding security principles. Security principles are Users, Groups, and Computers. The application partition typically contains DNS zone objects, and dynamic data from other network services such as Remote Access Service (RAS), and Dynamic Host Configuration Protocol (DHCP).

Dynamic Data:

A dynamic entry is an object in the directory which has an associated time-to-live (TTL) value. The TTL for an entry is set when the entry is created.

Security Principles - Objects that can have permissions assigned to them and each contain security identifiers. The following objects are security principles:

o User

Computer

Group

RPC:

Active Directory uses RPC over IP to transfer both intersite and intrasite replication between domain controllers. To keep data secure while in transit, RPC over IP replication uses both the Kerberos authentication protocol and data encryption.

SMTP:

If you have a site that has no physical connection to the rest of your network, but that can be reached using the Simple Mail Transfer Protocol (SMTP), that site has mail-based connectivity only. SMTP replication is used only for replication between sites. You also cannot use SMTP replication to replicate between domain controllers in the same domain—only inter-domain replication is supported over SMTP (that is, SMTP can be used only for inter-site, inter-domain replication). SMTP replication can be used only for schema, configuration, and global catalog partial replica replication. SMTP replication observes the automatically generated replication schedule.

Changing of ntds.dit file from one Drive to another

1.

Boot the domain controller in Directory Services Restore mode and log on with the Directory Services Restore mode administrator account and password (this is the password you assigned during the Dcpromo process).

2.

At a command prompt, type ntdsutil.exe. You receive the following prompt:

ntdsutil:

3.

Type files to receive the following prompt:

file maintenance:

4.

Type info. Note the path of the database and log files.

5.

To move the database, type move db to %s (where %s is the target folder).

6.

To move the log files, type move logs to %s (where %s is the target folder).

7.

Type quit twice to return to the command prompt.

8.

Reboot the computer normally.

DNS

DNS (Domain Name system)

Domain Name System (DNS) is a database system that translates a computer's fully qualified domain name into an IP address.

The local DNS resolver

The following graphic shows an overview of the complete DNS query process.

DNS Zones

Forward lookup zone - Name to IP address map.

Reverse lookup zone - IP address to name map.

Primary Zones - It Holds Read and Write copies of all resource records (A, NS, \_SRV).

Secondary Zones- which hold read only copies of the Primary Zones.

Stub Zones

Conceptually, stub zones are like secondary zones in that they have a read only copy of a primary zone. Stub zones are more efficient and create less replication traffic.

Stub Zones only have 3 records, the SOA for the primary zone, NS record and a Host (A) record. The idea is that if a client queries a record in the Stub Zone, your DNS server can refer that query to the correct Name Server because it knows its Host (A) record.

Queries

Query types are:

Inverse - Getting the name from the IP address. These are used by servers as a security check.

Iterative - Server gives its best answer. This type of inquiry is sent from one server to another.

Recursive - Cannot refer the query to another name server.

Conditional Forwarding

Another classic use of forwards is where companies have subsidiaries, partners or people they know and contact regularly query. Instead of going the long-way around using the root hints, the network administrators configure Conditional Forwarders

Purpose of Resource Records

Without resource records DNS could not resolve queries. The mission of a DNS Query is to locate a server that is Authoritative for a particular domain. The easy part is for the Authoritative server to check the name in the query against its resource records.

SOA (start of authority) record each zone has one SOA record that identifies which DNS server is authoritative for domains and sub domains in the zone.

NS (name server) record An NS record contains the FQDN and IP address of a DNS server authoritative for the zone. Each primary and secondary name server authoritative in the domain should have an NS record.

A (address) record By far the most common type of resource record, an A record is used to resolve the FQDN of a particular host into its associated IP address.

CNAME (canonical name) record A CNAME record contains an alias (alternate name) for a host.

PTR (pointer) record the opposite of an A record, a PTR record is used to resolve the IP address of a host into its FQDN.

SRV (service) record An SRV record is used by DNS clients to locate a server that is running a particular service—for example, to find a domain controller so you can log on to the network. SRV records are key to the operation of Active Directory.

MX (mail exchange) record An MX record points to one or more computers that process SMTP mail for an organization or site.

Where DNS resource records will be stored:

After running DCPROMO, A text file containing the appropriate DNS resource records for the domain controller is created. The file called Netlogon.dns is created in the %systemroot%\System32\config folder and contains all the records needed to register the resource records of the domain controller. Netlogon.dns is used by the Windows 2000 NetLogon service and to support Active Directory for non-Windows 2000 DNS servers.

Procedures for changing a Server’s IP Address

Once DNS and replication are setup, it is generally a bad idea to change a servers IP address (at least according to Microsoft). Just be sure that is what you really want to do before starting the process. It is a bit kin to changing the Internal IPX number of A Novell server, but it can be done.

1. Change the Server’s IP address

2. Stop the NETLOGON service.

3. Rename or delete SYSTEM32\CONFIG\NETLOGON.DNS and NETLOGON.DNB

4. Restart the NETLOGON service and run “IPconfig /registerDNS”

5. Go to one of the other DCs and verify that its DNS is now pointing to the new IP address of the server. If not, change the records manually and give it 15 minutes to replicate the DNS changes out.

6. Run REPLMON and make sure that replication is working now. You may have to wait a little while for things to straighten out. Give it an hour or two if necessary.

If a server shows that it isn’t replicating with one of its partners, there are several issues to address:

A. Check to see that the servers can ping each other.

B. Make sure that both servers’ DNS entries for each other point to the proper IP addresses

C. If server A says it replicated fine, but server B says it couldn’t contact Server A, check the DNS setup on Server B. Chances are it has a record for Server A pointing to the wrong place.

D. Run Netdiag and see if it reports any errors or problems.

Trust Relationship

One way trust - When one domain allows access to users on another domain, but the other domain does not allow access to users on the first domain.

Two way trust - When two domains allow access to users on the other domain.

Trusting domain - The domain that allows access to users on another domain.

Trusted domain - The domain that is trusted, whose users have access to the trusting domain.

Transitive trust - A trust which can extend beyond two domains to other trusted domains in the tree.

Intransitive trust - A one way trust that does not extend beyond two domains.

Explicit trust - A trust that an administrator creates. It is not transitive and is one way only.

Cross-link trust - An explicit trust between domains in different trees or in the same tree when a descendent/ancestor (child/parent) relationship does not exist between the two domains.

Forest trust - When two forests have a functional level of Windows 2003, you can use a forest trust to join the forests at the root.

Shortcut trust - When domains that authenticate users are logically distant from one another, the process of logging on to the network can take a long time. You can manually add a shortcut trust between two domains in the same forest to speed authentication. Shortcut trusts are transitive and can either be one way or two way.

Windows 2000 only supports the following types of trusts:

Two way transitive trusts

One way non-transitive trusts.

Question1. What Is Clustering. Briefly Define & Explain It ?

Answer :

Clustering is a technology, which is used to provide High Availability for mission critical applications. We can configure cluster by installing MCS (Microsoft cluster service) component from Add remove programs, which can only available in Enterprise Edition and Data center edition.

Question2. Types Of Clusters ?

Answer :

In Windows we can configure two types of clusters:

NLB (network load balancing): cluster for balancing load between servers. This cluster will not provide any high availability. Usually preferable at edge servers like web or proxy.

Server Cluster: This provides High availability by configuring active-active or active-passive cluster. In 2 node active-passive cluster one node will be active and one node will be stand by. When active server fails the application will FAILOVER to stand by server automatically. When the original server backs we need to FAILBACK the application.

Question3. What Is Quorum ?

Answer :

A shared storage need to provide for all servers which keeps information about clustered application and session state and is useful in FAILOVER situation. This is very important if Quorum disk fails entire cluster will fails.

Question4. Why Quorum Is Necessary ?

Answer :

When network problems occur, they can interfere with communication between cluster nodes. A small set of nodes might be able to communicate together across a functioning part of a network, but might not be able to communicate with a different set of nodes in another part of the network. This can cause serious issues. In this “split” situation, at least one of the sets of nodes must stop running as a cluster.

To prevent the issues that are caused by a split in the cluster, the cluster software requires that any set of nodes running as a cluster must use a voting algorithm to determine whether, at a given time, that set has quorum. Because a given cluster has a specific set of nodes and a specific quorum configuration, the cluster will know how many “votes” constitutes a majority (that is, a quorum). If the number drops below the majority, the cluster stops running. Nodes will still listen for the presence of other nodes, in case another node appears again on the network, but the nodes will not begin to function as a cluster until the quorum exists again.

For example, in a five node cluster that is using a node majority, consider what happens if nodes 1, 2, and 3 can communicate with each other but not with nodes 4 and 5. Nodes 1, 2, and 3 constitute a majority, and they continue running as a cluster. Nodes 4 and 5 are a minority and stop running as a cluster, which prevents the problems of a “split” situation. If node 3 loses communication with other nodes, all nodes stop running as a cluster. However, all functioning nodes will continue to listen for communication, so that when the network begins working again, the cluster can form and begin to run.

Question5. Different Types Of Quorum In Windows Server 2008 ?

Answer :

Node Majority :Used when Odd number of nodes are in cluster.

Node and Disk Majority :Even number of nodes(but not a multi-site cluster)

Node and File Share Majority : Even number of nodes, multi-site cluster

Node and File Share Majority : Even number of nodes, no shared storage

Question6. Different Types Of Quorum In Windows Server 2003 ?

Answer :

Standard Quorum : As mentioned above, a quorum is simply a configuration database for MSCS, and is stored in the quorum log file. A standard quorum uses a quorum log file that is located on a disk hosted on a shared storage interconnect that is accessible by all members of the cluster.

Standard quorums are available in Windows NT 4.0 Enterprise Edition, Windows 2000 Advanced Server, Windows 2000 Datacenter Server, Windows Server 2003 Enterprise Edition and Windows Server 2003 Datacenter Edition.

Majority Node Set Quorums : A majority node set (MNS) quorum is a single quorum resource from a server cluster perspective. However, the data is actually stored by default on the system disk of each member of the cluster. The MNS resource takes care to ensure that the cluster configuration data stored on the MNS is kept consistent across the different disks.

Majority node set quorums are available in Windows Server 2003 Enterprise Edition, and Windows Server 2003 Datacenter Edition.

Question7. Explain About Each Quorum Type ?

Answer :

Node Majority: Each node that is available and in communication can vote. The cluster functions only with a majority of the votes, that is, more than half.

Node and Disk Majority: Each node plus a designated disk in the cluster storage (the “disk witness”) can vote, whenever they are available and in communication. The cluster functions only with a majority of the votes, that is, more than half.

Node and File Share Majority: Each node plus a designated file share created by the administrator (the “file share witness”) can vote, whenever they are available and in communication. The cluster functions only with a majority of the votes, that is, more than half.

No Majority: Disk Only: The cluster has quorum if one node is available and in communication with a specific disk in the cluster storage.

Question8. How Is The Quorum Information Located On The System Disk Of Each Node Kept In Synch?

Answer :

The server cluster infrastructure ensures that all changes are replicated and updated on all members in a cluster.

Question9. Can This Method Be Used To Replicate Application Data As Well?

Answer :

No, that is not possible in this version of clustering. Only Quorum information is replicated and maintained in a synchronized state by the clustering infrastructure.

Question10. Can I Convert A Standard Cluster To An Mns Cluster?

Answer :

Yes. You can use Cluster Administrator to create a new Majority Node Set resource and then, on the cluster properties sheet Quorum tab, change the quorum to that Majority Node Set resource.

Question11. What Is The Difference Between A Geographically Dispersed Cluster And An Mns Cluster?

Answer :

A geographic cluster refers to a cluster that has nodes in multiple locations, while an MNS-based cluster refers to the type of quorum resources in use. A geographic cluster can use either a shared disk or MNS quorum resource, while an MNS-based cluster can be located in a single site, or span multiple sites.

Question12. What Is The Maximum Number Of Nodes In An Mns Cluster?

Answer :

Windows Server 2003 supports 8-node clusters for both Enterprise Edition and Datacenter Edition.

Question13. Do I Need Special Hardware To Use An Mns Cluster?

Answer :

There is nothing inherent in the MNS architecture that requires any special hardware, other than what is required for a standard cluster (for example, there must be on the Microsoft Cluster HCL). However, some situations that use an MNS cluster may have unique requirements (such as geographic clusters), where data must be replicated in real time between sites.

Question14. Does A Cluster Aware Application Need To Be Rewritten To Support Mns?

Answer :

No, using an MNS quorum requires no change to the application. However, some cluster aware applications expect a shared disk (for example SQL Server 2000), so while you do not need shared disks for the quorum, you do need shared disks for the application.

Question15. Does Mns Get Rid Of The Need For Shared Disks?

Answer :

It depends on the application. For example, clustered SQL Server 2000 requires shared disk for data. Remember, MNS only removes the need for a shared disk quorum.

Question16. What Does A Failover Cluster Do In Windows Server 2008 ?

Answer :

A failover cluster is a group of independent computers that work together to increase the availability of applications and services. The clustered servers (called nodes) are connected by physical cables and by software. If one of the cluster nodes fails, another node begins to provide service (a process known as failover). Users experience a minimum of disruptions in service.

Question17. What New Functionality Does Failover Clustering Provide In Windows Server 2008 ?

Answer :

New validation feature. With this feature, you can check that your system, storage, and network configuration is suitable for a cluster.

Support for GUID partition table (GPT) disks in cluster storage. GPT disks can have partitions larger than two terabytes and have built-in redundancy in the way partition information is stored, unlike master boot record (MBR) disks.

Question18. What Happens To A Running Cluster If The Quorum Disk Fails In Windows Server 2003 Cluster ?

Answer :

In Windows Server 2003, the Quorum disk resource is required for the Cluster to function. In your example, if the Quorum disk suddenly became unavailable to the cluster then both nodes would immediately fail and not be able to restart the clussvc.

In that light, the Quorum disk was a single point of failure in a Microsoft Cluster implementation. However, it was usually a fairly quick workaround to get the cluster back up and operational. There are generally two solutions to that type of problem.

Determine why the Quorum disk failed and repair.

Reprovision a new LUN, present it to the cluster, assign it a drive letter and format. Then start one node with the /FQ switch and through cluadmin designate the new disk resource as the Quorum. Then stop and restart the clussvc normally and then bring online the second node.

Question19. What Happens To A Running Cluster If The Quorum Disk Fails In Windows Server 2008 Cluster ?

Answer :

Cluster continue to work but failover will not happen in case of any other failure in the active node.

1) Differentiate between NTFS & FAT.

NTFS is the current file system used by Windows. It offers features like security permissions (to limit other users' access to folders), quotas (so one user can't fill up the disk), shadowing (backing up) and many other features that help Windows.

FAT32 is the older Microsoft filesystem, primarily used by the Windows 9X line and Window could be installed on a FAT32 parition up to XP. In comparision, FAT32 offers none of what was mentioned above, and also has a maximum FILE (not folder) size of 4GB, which is kind of small these days, especially in regards to HD video.

2) What Is VOIP.

VOIP - Short for Voice Over Internet Protocol, a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions.

3) What is loop back.

Loopback address is 127.0.0.1,

An address that sends outgoing signals back to the same computer for testing.

4) What is Proxy Server.

A proxy server is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security. In some cases, they monitor employees' use of outside resources.

5) Differentiate between FIREWALL/ANTIVIRUS.

Antivirus:

The prime job of an anivirus is protect your system from computer viruses. Your computer may be standalone or part of network or connected to Internet you need an antivirus program. It actively monitors when you are using your system for any virus threat from different sources. if it found one it tries to clean or quarantine the virus ultimately keeping your system and data safe.

Firewall:

Firewall is in other hand a program which protects your system from outsider/intruder/hacker attacks. These attacks may not be virus type. In some cases hackers can take control of your system remotely and steal your data or important information from system. If your system is directly connected to internet or a large network than you can install a software firewall in your PC to protect your self from unauthorized access. Firewall is available either in software or in hardware form. For a single PC you may need a software firewall while a large corporate implements hardware firewall to protect all of their systems from such attacks.

6) Differentiate between Frond end & Back End Server.

Backend server:

A back end server is a computer resource that has not been exposed to the internet. In this regard the computing resource does not directly interact with the internet user. It can also be described as a server whose main function is to store and retrieve email messages.

Frontend server:

A frontend server is a computer resources that has exposed to the internet.

7) What is APIPA.

Stands for Automatic Private IP Addressing

APIPA is a DHCP fail over mechanism for local networks. With APIPA, DHCP clients can obtain IP addresses when DHCP servers are non-functional.

APIPA exists in all modern versions of Windows except Windows NT.

When a DHCP server fails, APIPA allocates IP addresses in the private range 169.254.0.1 to 169.254.255.254.

8) How Release and renew IP address from Command prompt.

Ipconfig / release

ipconfig / renew

9) What is wins server.

Windows Internet Name Service (WINS) servers dynamically map IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of by IP address. If you want this computer to keep track of the names and IP addresses of other computers in your network, configure this computer as a WINS server.

If you do not use WINS in such a network, you cannot connect to a remote network resource by using its NetBIOS name.

10)What is the Windows Registry.

The Windows Registry, usually referred to as "the registry," is a collection of databases of configuration settings in Microsoft Windows operating systems.

11) System Volume Information (SVI) Folder.

Windows XP includes a folder named System Volume Information on the root of each drive that remains hidden from view even when you choose to show system files. It remains hidden because it is not a normally hidden folder you can say it is a Super Hidden Folder. Windows does not shows Super Hidden Folders even when you select "Show Hidden Files."

12 ) What is MBR.

Short form Master Boot Record, a small program that is executed when a computer boots up. Typically, the MBR resides on the first sector of the hard disk. The program begins the boot process by looking up the partition table to determine which partition to use for booting

13) What is Bit Locker.

BitLocker is an encryption feature available in Ultimate and Enterprise versions of Windows 7 and Vista,

To encrypt an entire drive, simply right-click on the drive and select Turn on BitLocker from the context menu.

14) Difference b/w sata and IDE.

IDE and SATA are different types of interfaces to connect storage devices (like hard drives) to a computer's system bus. SATA stands for Serial Advanced Technology Attachment (or Serial ATA) and IDE is also called Parallel ATA or PATA. SATA is the newer standard and SATA drives are faster than PATA (IDE) drives. For many years ATA provided the most common and the least expensive interface for this application. But by the beginning of 2007, SATA had largely replaced IDE in all new systems.

15)Main Difference Between Windows server 2012R2 and 2012

1) New Server Manager: Create, Manage Server Groups

2) Hyper-V Replication : The Hyper-V Replica feature allows you to replicate a virtual machine from one location to another with Hyper-V and a network connection—and without any shared storage required. This is a big deal in the Microsoft world for disaster recovery, high availability and more. VMware does this, too, but the vendor charges new licensees extra for the capability.

3) Expanded PowerShell Capabilities

4) IIS 8.0 and IIS 7 in 2012R2

5) Hyper-V 4.0

6) PowerShell 4.0

16) How Long My Computer Has Been Running? Get to Know My Computer’s Uptime.

Start Task manager, and select Performance tab.

In performance tab we can see system up time

Method 2: By typing systeminfo in command prompt we can find out up time of your server

In system boot time.

17)Event viewer in Windows server

Control panel - Administrative tools - Computer Management - event Viewer

Three types events

Error.

Warning.

Information.

18) Manage Multiple, Remote Servers with Server Manager.

Server Manager is a management console in Windows Server® 2012 R2 Preview and Windows Server® 2012 that helps IT professionals provision and manage both local and remote Windows-based servers from their desktops, without requiring either physical access to servers, or the need to enable Remote Desktop protocol (RDP) connections to each server. Although Server Manager is available in Windows Server 2012R2 R2 and Windows Server 2012R2, Server Manager was updated in Windows Server 2012, to support remote, multi-server management, and help increase the number of servers an administrator can manage.

19) What happens when we type URL in browser.

First the computer looks up the destination host. If it exists in local DNS cache, it uses that information. Otherwise, DNS querying is performed until the IP address is found.

Then, your browser opens a TCP connection to the destination host and sends the request according to HTTP 1.1 (or might use HTTP 1.0, but normal browsers don't do it any more).

The server looks up the required resource (if it exists) and responds using HTTP protocol, sends the data to the client (=your browser)

The browser then uses HTML parser to re-create document structure which is later presented to you on screen. If it finds references to external resources, such as pictures, css files, javascript files, these are is delivered the same way as the HTML document itself.

DHCP:

1) How DHCP work?

DHCP Stands for Dynamic host configuration protocol.

DHCP is a protocol used for automatic configuration IP address in client computers connected to IP networks. DHCP operates on a client server model in four phases.

Discover: A client broadcasts DHCP Discover message when it comes alive on the network.

Offer: When a DHCP server receives the DHCP Discover message from the client, it reserves an I P address for the client and sends a DHCP Offer message to the client offering the reserved IP address.

Request: The client receives the DHCP offer message and broadcasts a DHCP request message to show its consent to accept the offered IP address.

Acknowledge: When the DHCP server receives the DHCP Request message from the client, it sends a DHCP Ack packet to the client. At this point the IP configuration process is complete.

2) What is DHCP Scope?

A range of IP address that the DHCP server can assign to clients that are on one subnet.

3) What protocol and port does DHCP use?

UDP protocol and 67 port in client and 68 port in server.

4) What is a DHCP lease?

A DHCP lease is the amount of time that the DHCP server grants to the DHCP

client permission to use a particular IP address. A typical server allows its

administrator to set the lease time.

5) Can DHCP support statically defined addresses?

Yes.

6) Define Dora Process & why it is used.

Discover, Offer, request and acknowledgement. it is used to assign ip address automatically to client systems.

7) What is Authorizing DHCP Servers in Active Directory?

If a DHCP server is to operate within an Active Directory domain (and is not running on a domain controller) it must first be authorized to Active directory.

8)How to Backup and Restore DHCP in Windows Server 2012R2

In Windows Server 2012R2, backup of DHCP database and settings has gotten simpler. You may want to back up your DHCP server from time to time to prepare for disaster recovery scenarios or when migrating DHCP server role to a new hardware.

Backup DHCP Server

1. Open Server Manager > DHCP role

2. Right click server name, choose Backup..

3. Choose a location for backup, click OK

Restore DHCP Server

1. Open Server Manager > DHCP role

2. Right Click server name, choose Restore

3. Choose the location of the backup, click OK

4. Restart the DHCP Service

DHCP Databse location: C:\WINDOWS\System32\DHCP directory.

DNS

1) Define DNS .

Domain Name System, DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember.

Two types of lookup in DNS.

Forward lookup : it converts Domain name to ip address.

Reverse lookup: it converts ip address to Domain name.

Three types of zone.

Primary zone

secandary zone and stub zone.

what is the port no of DNS.

UDP and port number - 53

What is NSlookup.

Nslookup.exe is a command-line administrative tool for testing and troubleshooting DNS servers. This tool is installed along with the TCP/IP protocol through Control Panel.

MS-DOS utility that enables a user to look up an IP address of a domain or host on a network.

Active directory and Domain

1) What is LDAP? Why it is used.

LDAP is the Lightweight Directory Access Protocol. Its an active directory protocal ,Basically, it's a protocol used to access data from a database

2) What is Active Directory? Why it used.

Active Directory is a Directory Service created by Microsoft. It is included with most Windows Server operating systems.

Active Directory is primarily used to store directory objects like users and groups and computers printers.

Using Active Directory brings a number of advantages to your network,

Centralized user account management

Centralized policy management (group policy)

Better security management

3) What Is Group Policy.

Group Policy is a feature of the Microsoft Windows NT family of operating systems that control the working environment of user accounts and computer accounts. Group Policy provides the centralized management and configuration of operating systems, applications, and users' settings in an Active Directory environment.

4) What is the order in which GPOs are applied .

Local Group Policy object

site ,

Domain and

organizational units.

5) What is the difference between software publishing and assigning.

Assign Users : The software application is advertised when the user logs on. It is installed when the user clicks on the software application icon via the start menu, or accesses a file that has been associated with the software application.

Assign Computers :The software application is advertised and installed when it is safe to do so, s uch as when the computer is next restarted.

Publish to users : The software application does not appear on the start menu or desktop. This means the user may not know that the software is available. The software application is made available via the Add/Remove Programs option in control panel, or by clicking on a file that has been associated with the application. Published applications do not reinstall themselves in the event of accidental deletion, and it is not possible to publish to computers.

6) Can I deploy non-MSI software with GPO.

create the fiile in .zap extension.

7) Name some GPO settings in the computer and user parts.

Computer Configuration, User ConfigurationName

8) Name a few benefits of using GPMC.

Easy administration of all GPOs across the entire Active Directory Forest

View of all GPOs in one single list

Backup and restore of GPOs Migration of GPOs across different domains and forest.

9) How frequently is the client policy refreshed ?

90 minutes give or take.

10) Where are group policies stored ?

C:\Windows\System32\GroupPolicy.

11) Group policy backup

To backup a single GPO, right-click the GPO, and then click Back Up.

To backup all GPOs in the domain, right-click Group Policy Objects and click Back Up All.

12) Define DSRM Mode?

Directory Services Restore Mode (DSRM) is a special boot mode for repairing or recovering Active Directory. It is used to log on to the computer when Active Directory has failed or needs to be restored.

To manually boot in Directory Services Restore Mode, press the F8 key repeatedly. Do this immediately after BIOS POST screen, before the Windows logo appears. (Timing can be tricky; if the Windows logo appears you waited too long.) A text menu menu will appear. Use the up/down arrow keys to select Directory Services Restore Mode or DS Restore Mode. Then press the Enter key.

13) Where is the AD database held? What other folders are related to AD?

The AD data base is stored in c:\windows\ntds\NTDS.DIT.

14 ) Have you ever Installed AD?

To Install Microsoft Active Directory:

Ensure that you log on to the computer with an administrator account to perform installation.

Click electing Start > Administration Tools > Server manager > Configure your Server.

In the Welcome page, click Next.

In the Operating system compatibility panel, click Next.

On the Domain Controller Type panel, select Domain controller for a new domain and click Next.

On the Create New Domain panel, select Domain in a new forest and click Next.

On the New Domain Name panel, enter the DNS suffix for your new Active Directory. This name will be used during Tivoli Provisioning Manager installation, so make a note of it. Click Next.

On the NetBIOS Domain Name panel, enter the NetBIOS name of the domain. The first part of the DNS name is usually sufficient. Click Next.

On the Database and Logs panel, select the desired folders for the Database and Logs.C:\Windows\NTDS is the default. Click Next.

On the Shared System Volume panel, enter a valid directory for the system volume.C:\Windows\Sysvol is the default. Click Next to continue.

If you configured DNS successfully, the Permissions setting panel is displayed. Select Permissions compatible only with Windows 2000 or Windows Server 2003. Click Next.

On the Directory Services Restore Mode Administrator Password panel, enter a valid password to be used when running the Directory Services in Restore Mode. Click Next

Verify the settings and Click Next to begin the Active Directory configuration. The server will be rebooted as part of the process.

15) What is the use of SYSVOL folder

All active directory data base security related information store in SYSVOL folder and it’s only created on NTFS partition.

16) What is global catalog

The Global Catalog is a database that contains all of the information pertaining to objects within all domains in the Active Directory environment

17) What is the difference between local, global and universal groups

Domain local groups assign access permissions to global domain groups for local domain resources. Global groups provide access to resources in other trusted domains. Universal groups grant access to resoures in all trusted domains.

18) What is group nesting.

Adding one group as a member of another group is called 'group nesting'. This will help for easy administration and reduced replication traffic

19) What is Domain control?

A domain controller (DC) is a server that handles all the security requests from other computers and servers within the Windows Server domain

there was a primary domain controller and a backup domain controller. The primary DC focused on domain services only to avoid the possibility of a system slow down or crash due to overtasking from managing other functionality and security requests. In the event of a primary DC going down, a backup DC could be promoted and become the primary DC to keep the rest of the server systems functioning correctly

20) What is domain?

A domain is a set of network resources (applications, printers, and so forth) for a group of users. The user needs only to log in to the domain to gain access to the resources, which may be located on a number of different servers in the network. The ‘domain’ is simply your computer address not to confuse with an URL. A domain address might look something like 211.170.469.

21) What is Forest?

A collection of one or more Active Directory domains that share a common schema, configuration, and global catalog.

22) What is global catalog.

The Active Directory Global Catalog is the central storage of information about objects in an Active Directory forest. A Global Catalog is created automatically on the first domain controller in the first domain in the forest. The Domain Controller which is hosting the Global Catalog is known as a Global catalog server.

23) What is tree.

An Active Directory tree is a collection of Active Directory domains that begins at a single root and branches out into peripheral, child domains. Domains in an Active Directory tree share the same namespace. An Active Directory forest is a collection of Active Directory trees, similar to a real world forest. Catalog Server.

24) What is site.

A Site object in Active Directory represents a geographic location that hosts networks.

25) Flexable Single Master Operation Roles (FSMO)

The 5 FSMO server roles:

Schema Master

Forest Level

One per forest

Domain Naming Master

Forest Level

One per forest

PDC Emulator

Domain Level

One per domain

RID Master

Domain Level

One per domain

Infrastructure Master

Domain Level

One per domain

26) Command to Add client to Domain

NETDOM /Domain:MYDOMAIN /user:adminuser /password:apassword MEMBER MYCOMPUTER /JOINDOMAIN

27) Setting File Permissions on a Folder Using Group Policy

The setting is located under Computer Configuration, Windows Settings, Security Settings, File System. Here's the procedure:

Go to the location in the Group Policy listed above.

Right-click File System.

Click Add File.

In the "Add a file or folder" window, select the folder (or file) for which you want the permissions to be set, and click OK.

In the security box that pops up, you can add a user or a group that needs permission to the folder.

Vertualization

1)Define virtualization.

Hyper-V virtualization will provide an environment in which we can run multiple operating systems at the same time on one physical computer, by running each operating system in its own virtual machine.

2) What are the benefits of virtualization ?

Reduce the number of physical servers

Reduce the infrastructure needed for your data center

3) What is a Hypervisor.

You can think of a Hypervisor as the kernel or the core of a virtualization platform. The Hypervisor is also called the Virtual Machine Monitor. The Hypervisor has access to the physical host hardware.

4) What are a host, guest, and virtual machine.

A host system (host operating system) would be the primary & first installed operating system. If you are using a bare metal Virtualization platform like Hyper-V or ESX, there really isn’t a host operating system besides the Hypervisor. If you are using a Type-2 Hypervisor like VMware Server or Virtual Server, the host operating system is whatever operating system those applications are installed into.

A guest system (guest operating system) is a virtual guest or virtual machine (VM) that is installed under the host operating system. The guests are the VMs that you run in your virtualization platform.

Some admins also call the host & guest the parent and child.

Hyper v Snap shot:

How to create Hyper v Snap shot:

Just select the Virtual machine in Hyper-V Manager and select Snapshot from the Actions pane. The status of the virtual machine will change to “Taking Snapshot” and show the progress of the action using a percentage value.

File extension = .avhd

Virtual Machine files

The first thing to know is what files are used to create a virtual machine:

.XML files

These files contain the virtual machine configuration details. There is one of these for each virtual machine and each snapshot of a virtual machine. They are always named with the GUID used to internally identify the virtual machine or snapshot in question.

.BIN files

This file contains the memory of a virtual machine or snapshot that is in a saved state.

.VSV files

This file contains the saved state from the devices associated with the virtual machine.

.VHD files

These are the virtual hard disk files for the virtual machine

.AVHD files

These are the differencing disk files used for virtual machine snapshots

RAID Interview questions

Question1. What Is Raid?

Answer :

Redundant Array of Independent Drives (or Disks), also known as Redundant Array of Inexpensive Drives (or Disks) (RAID) is an important term for data storage schemes that divide and/or replicate data among multiple hard drives. They offer, depending on the scheme, increased data reliability and/or throughput.

RAID is a way of storing the same data in different drives(thus, redundantly) on multiple hard disks.

Question2. What Are The Advantages Of Raid?

Answer :

Increased redundancy

Increased data availability

Higher READ/Write performance in some RAID levels

Higher Data throughput

better reliability

Higher Data Security: Through the use of redundancy, most RAID levels provide protection for the data stored on the array. This means that the data on the array can withstand even the complete failure of one hard disk (or sometimes more) without any data loss, and without requiring any data to be restored from backup. This security feature is a key benefit of RAID and probably the aspect that drives the creation of more RAID arrays than any other. All RAID levels provide some degree of data protection, depending on the exact implementation, except RAID level 0.

Fault Tolerance: RAID implementations that include redundancy provide a much more reliable overall storage subsystem than can be achieved by a single disk. This means there is a lower chance of the storage subsystem as a whole failing due to hardware failures. (At the same time though, the added hardware used in RAID means the chances of having a hardware problem of some sort with an individual component, even if it doesn't take down the storage subsystem, is increased; see this full discussion of RAID reliability for more.)

Improved Availability: Availability refers to access to data. Good RAID systems improve availability both by providing fault tolerance and by providing special features that allow for recovery from hardware faults without disruption. See the discussion of RAID reliability and also this discussion of advanced RAID features.

Increased, Integrated Capacity: By turning a number of smaller drives into a larger array, you add their capacity together (though a percentage of total capacity is lost to overhead or redundancy in most implementations). This facilitates applications that require large amounts of contiguous disk space, and also makes disk space management simpler. Let's suppose you need 300 GB of space for a large database. Unfortunately, no hard disk manufacturer makes a drive nearly that large. You could put five 72 GB drives into the system, but then you'd have to find some way to split the database into five pieces, and you'd be stuck with trying to remember what was were. Instead, you could set up a RAID 0 array containing those five 72 GB hard disks; this will appear to the operating system as a single, 360 GB hard disk! All RAID implementations provide this "combining" benefit, though the ones that include redundancy of course "waste" some of the space on that redundant information.

Improved Performance: Last, but certainly not least, RAID systems improve performance by allowing the controller to exploit the capabilities of multiple hard disks to get around performance-limiting mechanical issues that plague individual hard disks. Different RAID implementations improve performance in different ways and to different degrees, but all improve it in some way. See this full discussion of RAID performance issues for more.

Question3. What Are Different Levels Of Raid?

Answer :

There are many levels like

RAID 0,RAID 1,RAID 2,RAID 3,RAID 4,RAID 5,RAID 10,RAID 01,RAID 50,RAID 6

But popular are RAID 0,RAID 1,RAID 5,RAID 10,RAID 01,RAID 50,RAID 6

generally used are R0,R1,R5

Question4. Explain Raid 0, Raid 1, Raid 5 ?

Answer :

RAID 0:

The lowest designated level of RAID, level 0, is actually not a valid type of RAID. It was given the designation of level 0 because it fails to provide any level of redundancy for the data stored in the array. Thus, if one of the drives fails, all the data is damaged.

RAID 0 uses a method called striping. Striping takes a single chunk of data like a graphic image, and spreads that data across multiple drives. The advantage that striping has is in improved performance. Twice the amount of data can be written in a given time frame to the two drives compared to that same data being written to a single drive.

RAID 1:

RAID version 1 was the first real implementation of RAID. It provides a simple form of redundancy for data through a process called mirroring. This form typically requires two individual drives of similar capacity. One drive is the active drive and the secondary drive is the mirror. When data is written to the active drive, the same data is written to the mirror drive.

RAID 5:

This is the most powerful form of RAID that can be found in a desktop computer system. Typically it requires the form of a hardware controller card to manage the array, but some desktop operating systems can create these via software. This method uses a form of striping with parity to maintain data redundancy. A minimum of three drives is required to build a RAID 5 array and they should be identical drives for the best performance.

Question5. Whats The Difference Between Raid0 & Raid1 ?

Answer :

RAID 0+1: This is a hybrid form of RAID that some manufacturers have implemented to try and give the advantages of each of the two versions combined. Typically this can only be done on a system with a minimum of 4 hard drives. It then combines the methods of mirroring and striping to provide the performance and redundancy. The first set of drives will be active and have the data striped across them while the second set of drives will be a mirror of the data on the first two.

RAID 10 or 1+0: RAID 10 is effectively a similar version to RAID 0+1. Rather than striping data between the disk sets and then mirroring them, the first two drives in the set are a mirrored together. The second two drives form another set of disks that is are mirror of one another but store striped data with the first pair. This is a form of nested RAID setup. Drives 1 and 2 are a RAID 1 mirror and drives 3 and 4 are also a mirror. These two sets are then setup as stripped array.

Question6. Whats The Difference Between Raid1 And Raid5 ?

Answer :

RAID 1: Minimum 2 drives are required . Gives only 50% disk space.

RAID 5: Minimum 3 drives are required . Gives only (n-1)X Capacity where n is the no. of disks, disk space.

Question7. Whats The Difference Between Raid 3 & Raid 5 ?

Answer :

RAID 3 and RAID 4: Striped Set (3 disk minimum) with Dedicated Parity, the parity bits represent a memory location each, they have a value of 0 or 1, whether the given memory location is empty or full, thus enhancing the speed of read and write. : Provides improved performance and fault tolerance similar to RAID 5, but with a dedicated parity disk rather than rotated parity stripes. The single disk is a bottle-neck for writing since every write requires updating the parity data. One minor benefit is the dedicated parity disk allows the parity drive to fail and operation will continue without parity or performance penalty.

RAID 5 does not have a dedicated parity drive but the parity is rotated across all the drives hence the parity is distributed.

RAID 5: Striped Set (3 disk minimum) with Distributed Parity: Distributed parity requires all but one drive to be present to operate; drive failure requires replacement, but the array is not destroyed by a single drive failure. Upon drive failure, any subsequent reads can be calculated from the distributed parity such that the drive failure is masked from the end user. The array will have data loss in the event of a second drive failure and is vulnerable until the data that was on the failed drive is rebuilt onto a replacement drive.

Question8. Whats The Difference Between Raid01 & Raid10?

Answer :

RAID 0+1: Striped Set + Mirrored Set (4 disk minimum; Even number of disks) provides fault tolerance and improved performance but increases complexity. Array continues to operate with one failed drive. The key difference from RAID 1+0 is that RAID 0+1 creates a second striped set to mirror a primary striped set, and as a result can only sustain a maximum of a single disk loss, whereas 1+0 can sustain multiple drive losses as long as no two drive loss comprise a single pair.

RAID 1+0: Mirrored Set + Striped Set (4 disk minimum; Even number of disks) provides fault tolerance and improved performance but increases complexity. Array continues to operate with one or more failed drives. The key difference from RAID 0+1 is that RAID 1+0 creates a striped set from a series of mirrored drives.

Question9. How Many Minimum Disk Drives Are Needed For R0,r1,r5,r10,r01 ?

Answer :

R0: Minimum 1

R1: Minimum 2

R5: Minimum 3

R10: Minimum 4

R01: Minimum 4

Question10. How Raid 5 Works And How Parity Is Calculated ?

Answer :

The parity calculation is typically performed using a logical operation called "exclusive OR" or "XOR". As you may know, the "OR" logical operator is "true" (1) if either of its operands is true, and false (0) if neither is true. The exclusive OR operator is "true" if and only if one of its operands is true; it differs from "OR" in that if both operands are true, "XOR" is false.

Question11. Other Than Raid Feature What Are The Other Features In Software Management Functionalities?

Answer :

Hot spare

Raid level migration (RLM)

SNMP interaction/management

Question12. What Is Initialization?

Answer :

Initialization is the process of preparing a drive for storage use. It erases all data on the drive & makes way for new file system creation.

Question13. What Is Check Consistency?

Answer :

Consistency check or CC verifies correctness of data in logical drives. This is a feature of some of the RAID hardware controller cards.

Question14. What Is Background Initialization?

Answer :

This is a Consistency check process forced when a new logical drive is created. This is an automatic operation that starts 5 minutes after the new logical drive is created.

Question15. What Is A Raid Array ?

Answer :

RAID array is a group of disks which are configured with RAID. That means they are in a redundant setup to tolerate any disk failures.

Question16. Whats The Difference Between A Jbod & A Raid Array ?

Answer :

Just A Bunch Of Disks (JBOD):-

Hard disks that aren't configured in a RAID configuration. They are just disks piled or connected in one single enclosure.

RAID is having the advantage of bearing a disk failure & still give data availability.

Question17. When Jbod Is Preferred Over Raid Array ?

Answer :

When there is no need for redundancy & when it is ok if there is some hard disk failure or data unavailability in such scenarios JBOD is prefered over RAID because JBOD is inexpensive storage solution. It is also easy to setup & start using compared to RAID.

Question18. What Is A Hot Spare?

Answer :

Hot spare is an extra, unused disk drive that is part of the disk subsystem. It is usually in standby mode ready for service if a drive fails. Whenever there is a drive failure this hot spare kicks in & takes over that failed drive's role.

Question19. What Is A Logical Drive Or Virtual Drive ?

Answer :

The partitioning or division of a large hard drive into smaller units. A single, large Physical Drive can be partitioned into two or more smaller Logical Drives.

Question20. What Is Rebuilding Of Array ?

Answer :

Whenever there is a disk failure in the RAID array the array goes to DOWNGRADED STATE. SO when we plug out the failed drive & insert a new functioning drive the RAID configured array starts regenerating the data to the newer drive. This process is called rebuilding.

RAID Storage Interview Questions & Answers

This set of multiple choice SAN storage questions and answers focuses on RAID technology and various levels of RAID.

1. Which two are advantages of hardware RAID controllers?

a) Volume management is performed by the server

b) Volume management is performed by controller card

c) Dedicated cache memory increases server write performance

d) Parity calculation by the server and cache memory in the RAID controller increases read and write performance

View Answer

2. Which two RAID types use parity for data protection?

a) RAID 1

b) RAID 4

c) RAID 1+ 0

d) RAID 5

View Answer

3. Which one of these is characteristic of RAID 5?

a) Distributed parity

b) No Parity

c) All parity in a single disk

d) Double Parity

View Answer

4. What is the unique characteristic of RAID 6 (Choose one)?

a) Distributed Parity

b) Striping

c) Two independent distributed parity

d) Mirroring

View Answer

5. Which of the following combinations can support RAID 05?

a) 2 sets with 3 disks each

b) 3 sets with 2 disks each

c) 4 sets with 3 disks each

d) 4 sets with 1 disk each

View Answer

6. What is the minimum number of disks required for RAID1?

a) 1

b) 2

c) 4

d) 5

View Answer

7. Which of the following raid levels provides maximum usable disk space?

a) RAID 1

b) RAID 0

c) RAID 5

d) RAID 6

View Answer

8. Can you help decide on the RAID level to use – we are a media house and we use lot of graphics/video applications – we need large throughputs for videos to get played without any jitter and since we are in publishing business we can’t afford downtimes.

Even if there is any downtime we would like our data to be quickly reconstructed and enable us to continue with out work in less time

a) Raid 5

b) Raid 10

c) Raid 6

d) Raid 01

e) Raid 0

View Answer

9. The mean time to failure of a single disk is 200000 hrs. If an array of disks is using 5 such disks, the mttf of the array is

a) 200000 hrs

b) 40000 hrs

c) 1000000 hrs

d) Can not be determined

View Answer

10. An array of disks is more likely to fail compared to a single disk. How is it that RAID arrays still manage to provide more data protection compared to a single disk?

a) Using either mirroring or striping

b) Using either mirroring or parity

c) Using better quality disks

d) Using dedicated hardware

Interview Questions on RAID

Question 1: what is the difference raid 1 and raid 5?

Answer: On most situations you will be using one of the following four levels of RAIDs.

~ RAID 0

~ RAID 1

~ RAID 5

~ RAID 10 (also known as RAID 1+0)

RAID 0

Following are the key points to remember for RAID level 0.

~ Minimum 2 disks.

~ Excellent performance ( as blocks are striped ).

~ No redundancy ( no mirror, no parity ).

~ Don’t use this for any critical system.

In all the diagrams mentioned below:

~ A, B, C, D, E and F – represents blocks

~ p1, p2, and p3 – represents parity

Picture

RAID 1

Following are the key points to remember for RAID level 1.

~ Minimum 2 disks.

~ Good performance ( no striping. no parity ).

~ Excellent redundancy ( as blocks are mirrored ).

Picture

RAID 5

Following are the key points to remember for RAID level 5.

~ Minimum 3 disks.

~ Good performance ( as blocks are striped ).

~ Good redundancy ( distributed parity ).

~ Best cost effective option providing both performance and redundancy. Use this for DB that is heavily read oriented. Write operations will be slow.

Picture

RAID 10

Following are the key points to remember for RAID level 10.

~ Minimum 4 disks.

~ This is also called as “stripe of mirrors”

~ Excellent redundancy ( as blocks are mirrored )

~ Excellent performance ( as blocks are striped )

~ If you can afford the dollar, this is the BEST option for any mission critical applications (especially databases).

Picture

Question 2: Explain Different RAID ?

Answer: However there are several non-standard raids, which are not used except in some rare situations. It is good to know what they are.

This article explains with a simple diagram how RAID 2, RAID 3, RAID 4, and RAID 6 works.

RAID 2

Picture

~ This uses bit level striping. i.e Instead of striping the blocks across the disks, it stripes the bits across the disks.

~ In the above diagram b1, b2, b3 are bits. E1, E2, E3 are error correction codes.

~ You need two groups of disks. One group of disks are used to write the data, another group is used to write the error correction codes.

~ This uses Hamming error correction code (ECC), and stores this information in the redundancy disks.

~ When data is written to the disks, it calculates the ECC code for the data on the fly, and stripes the data bits to the data-disks, and writes the ECC code to the redundancy disks.

~ When data is read from the disks, it also reads the corresponding ECC code from the redundancy disks, and checks whether the data is consistent.

If required, it makes appropriate corrections on the fly.

~ This uses lot of disks and can be configured in different disk configuration. Some valid configurations are 1) 10 disks for data and 4 disks for ECC 2)

4 disks for data and 3 disks for ECC

~ This is not used anymore. This is expensive and implementing it in a RAID controller is complex, and ECC is redundant now-a-days, as the hard disk

themselves can do this.

RAID 3

Picture

~ This uses byte level striping. i.e Instead of striping the blocks across the disks, it stripes the bits across the disks.

~ In the above diagram B1, B2, B3 are bytes. p1, p2, p3 are parities.

~ Uses multiple data disks, and a dedicated disk to store parity.

~ The disks have to spin in sync to get to the data.

~ Sequential read and write will have good performance.

~ Random read and write will have worst performance.

~ This is not commonly used.

RAID 4

Picture

~ This uses block level striping.

~ In the above diagram B1, B2, B3 are blocks. p1, p2, p3 are parities.

~ Uses multiple data disks, and a dedicated disk to store parity.

~ Minimum of 3 disks (2 disks for data and 1 for parity)

~ Good random reads, as the data blocks are striped.

~ Bad random writes, as for every write, it has to write to the single parity disk.

~ It is somewhat similar to RAID 3 and 5, but little different.

~ This is just like RAID 3 in having the dedicated parity disk, but this stripes blocks.

~ This is just like RAID 5 in striping the blocks across the data disks, but this has only one parity disk.

~ This is not commonly used.

RAID 6

Picture

~ Just like RAID 5, this does block level striping. However, it uses dual parity.

~ In the above diagram A, B, C are blocks. p1, p2, p3 are parities.

~ This creates two parity blocks for each data block.

~ Can handle two disk failure

~ This RAID configuration is complex to implement in a RAID controller, as it has to

calculate two parity data for each data block.

P

Software RAID have low performance, because of consuming resource from hosts. Raid software need to load for read data from software raid volumes. Before loading raid software, OS need to get boot to load the raid software. No need of Physical hardware in software raids. Zero cost investment.

Hardware RAID have high performance. They are dedicated RAID Controller which is Physically built using PCI express cards. It won’t use the host resource. They have NVRAM for cache to read and write. Stores cache while rebuild even if there is power-failure, it will store the cache using battery power backups. Very costly investments needed for a large scale.

Hardware RAID Card will look like below:

Hardware RAID

Hardware RAID

Featured Concepts of RAID

Parity method in raid regenerate the lost content from parity saved information’s. RAID 5, RAID 6 Based on Parity.

Stripe is sharing data randomly to multiple disk. This won’t have full data in a single disk. If we use 3 disks half of our data will be in each disks.

Mirroring is used in RAID 1 and RAID 10. Mirroring is making a copy of same data. In RAID 1 it will save the same content to the other disk too.

Hot spare is just a spare drive in our server which can automatically replace the failed drives. If any one of the drive failed in our array this hot spare drive will be used and rebuild automatically.

Chunks are just a size of data which can be minimum from 4KB and more. By defining chunk size we can increase the I/O performance.

RAID’s are in various Levels. Here we will see only the RAID Levels which is used mostly in real environment.

RAID0 = Striping

RAID1 = Mirroring

RAID5 = Single Disk Distributed Parity

RAID6 = Double Disk Distributed Parity

RAID10 = Combine of Mirror & Stripe. (Nested RAID)

RAID are managed using mdadm package in most of the Linux distributions. Let us get a Brief look into each RAID Levels.

RAID 0 (or) Striping

Striping have a excellent performance. In Raid 0 (Striping) the data will be written to disk using shared method. Half of the content will be in one disk and another half will be written to other disk.

Let us assume we have 2 Disk drives, for example, if we write data “TECMINT” to logical volume it will be saved as ‘T‘ will be saved in first disk and ‘E‘ will be saved in Second disk and ‘C‘ will be saved in First disk and again ‘M‘ will be saved in Second disk and it continues in round-robin process.

In this situation if any one of the drive fails we will loose our data, because with half of data from one of the disk can’t use to rebuilt the raid. But while comparing to Write Speed and performance RAID 0 is Excellent. We need at least minimum 2 disks to create a RAID 0 (Striping). If you need your valuable data don’t use this RAID LEVEL.

High Performance.

There is Zero Capacity Loss in RAID 0

Zero Fault Tolerance.

Write and Reading will be good performance.

RAID 1 (or) Mirroring

Mirroring have a good performance. Mirroring can make a copy of same data what we have. Assuming we have two numbers of 2TB Hard drives, total there we have 4TB, but in mirroring while the drives are behind the RAID Controller to form a Logical drive Only we can see the 2TB of logical drive.

While we save any data, it will write to both 2TB Drives. Minimum two drives are needed to create a RAID 1 or Mirror. If a disk failure occurred we can reproduce the raid set by replacing a new disk. If any one of the disk fails in RAID 1, we can get the data from other one as there was a copy of same content in the other disk. So there is zero data loss.

Good Performance.

Here Half of the Space will be lost in total capacity.

Full Fault Tolerance.

Rebuilt will be faster.

Writing Performance will be slow.

Reading will be good.

Can be used for operating systems and database for small scale.

RAID 5 (or) Distributed Parity

RAID 5 is mostly used in enterprise levels. RAID 5 work by distributed parity method. Parity info will be used to rebuild the data. It rebuilds from the information left on the remaining good drives. This will protect our data from drive failure.

Assume we have 4 drives, if one drive fails and while we replace the failed drive we can rebuild the replaced drive from parity informations. Parity information’s are Stored in all 4 drives, if we have 4 numbers of 1TB hard-drive. The parity information will be stored in 256GB in each drivers and other 768GB in each drives will be defined for Users. RAID 5 can be survive from a single Drive failure, If drives fails more than 1 will cause loss of data’s.

Excellent Performance

Reading will be extremely very good in speed.

Writing will be Average, slow if we won’t use a Hardware RAID Controller.

Rebuild from Parity information from all drives.

Full Fault Tolerance.

1 Disk Space will be under Parity.

Can be used in file servers, web servers, very important backups.

RAID 6 Two Parity Distributed Disk

RAID 6 is same as RAID 5 with two parity distributed system. Mostly used in a large number of arrays. We need minimum 4 Drives, even if there 2 Drive fails we can rebuild the data while replacing new drives.

Very slower than RAID 5, because it writes data to all 4 drivers at same time. Will be average in speed while we using a Hardware RAID Controller. If we have 6 numbers of 1TB hard-drives 4 drives will be used for data and 2 drives will be used for Parity.

Poor Performance.

Read Performance will be good.

Write Performance will be Poor if we not using a Hardware RAID Controller.

Rebuild from 2 Parity Drives.

Full Fault tolerance.

2 Disks space will be under Parity.

Can be Used in Large Arrays.

Can be use in backup purpose, video streaming, used in large scale.

RAID 10 (or) Mirror & Stripe

RAID 10 can be called as 1+0 or 0+1. This will do both works of Mirror & Striping. Mirror will be first and stripe will be the second in RAID 10. Stripe will be the first and mirror will be the second in RAID 01. RAID 10 is better comparing to 01.

Assume, we have 4 Number of drives. While I’m writing some data to my logical volume it will be saved under All 4 drives using mirror and stripe methods.

If I’m writing a data “TECMINT” in RAID 10 it will save the data as follow. First “T” will write to both disks and second “E” will write to both disk, this step will be used for all data write. It will make a copy of every data to other disk too.

Same time it will use the RAID 0 method and write data as follow “T” will write to first disk and “E” will write to second disk. Again “C” will write to first Disk and “M” to second disk.

Good read and write performance.

Here Half of the Space will be lost in total capacity.

Fault Tolerance.

Fast rebuild from copying data.

Can be used in Database storage for high performance and availability.

Conclusion

In this article we have seen what is RAID and which levels are mostly used in RAID in real environment. Hope you have learned the write-up about RAID. For RAID setup one must know about the basic Knowledge about RAID. The above content will fulfil basic understanding about RAID.

In the next upcoming articles I’m going to cover how to setup and create a RAID using Various Levels, Growing a RAID Group (Array) and Troubleshooting with failed Drives and much more.

RAID INTERVIEW QUESTIONS

RAID 0 – Striping (Striped Disk Array without Fault tolerance)

It is the Stripped Disk Array with no fault tolerance and it requires at least 2 drives

To be implemented. Due to no redundancy feature, RAID 0 is considered to be the

Lowest ranked RAID level. Striped data mapping technique is implemented for

High performance at low cost. The I/O performance is also improved as it is loaded across many channels.

Recommended Applications

Video production and editing

Image editing

Pre-press applications

Any application requiring high bandwidth

RAID 1 – Mirroring (Mirroring & Duplexing)

It is the Mirroring it is provide high performance. RAID 1 controller is able to perform 2 separate parallel reads or writes per mirrored pair. It also requires at least 2 drives to implement a non-redundant disk array. High level of availability, access and reliability can be achieved by entry-level RAID 1 array. With full redundancy feature available, need of readability is almost negligible. Controller configurations and Storage subsystem design is the easiest and simplest amongst all RAID levels.

Disadvantages

Typically the RAID function is done by system software, loading the CPU/Server and possible degrading throughput at high activity levels. Hardware implementation is strongly recommended

May not support hot swap of failed disk when implemented “software”

Recommended Applications

Accounting

Payroll

Financial

Any application requiring very high availability

RAID 2 (ECC error correcting code) (Hamming Code ECC)

It is the combination of Inherently Parallel Mapping and Protection RAID array.

It's also known as ECC RAID because each data word bit is written to data disk

Which is verified for correct data or correct disk error when the RAID disk is read.

Due to special disk features required, RAID 2 is not very popular since ECC is embedded in almost all modern disk drives.

Disadvantages

Very high ratio of ECC disks to data disks with smaller word sizes – inefficient

Entry level cost very high – requires very high transfer rate requirement to justify

Transaction rate is equal to that of a single disk at best (with spindle synchronization)

No commercial implementations exist / not commercially visible.

RAID LEVEL 3 (Parallel Transfer with Parity)

At least 3 drives we need to implementation in this raid level. Can be used single user environments which access long sequential records to Speed up data transfer. However raid-3 does not allow multiple I/O operation

We can use this raid level for image editing, pre press applications.

Disadvantages

Transaction rate equal to that of a single disk drive at best (if spindles are synchronized)

Controller design is fairly complex

Very difficult and resource intensive to do as a "software" RAID

Recommended Applications

Video Production and live streaming

Image Editing

Video Editing

Prepress Applications

Any application requiring high throughput

RAID Level 4: Independent Data Disk with Shared Parity Disk

Raid 4 does not support multiple simultaneous write operations.

RAID 4 requires a minimum of 3 drives to be implemented. It is composed of independent disks with shared parity to protect the data. Data transaction rate for

Read is exceptionally high and highly aggregated. Similarly, the low ratio of parity

Disks to data disks indicates high efficiency.

Disadvantages

Quite complex controller design

Worst Write transaction rate and Write aggregate transfer rate

Difficult and inefficient data rebuild in the event of disk failure

Block Read transfer rate equal to that of a single disk

RAID Level 5: Independent Data Disk with distributed Parity Blocks

RAIDS 5 is Independent Distributed parity block of data disks with a minimum

Requirement of at least 3 drives to be implemented and N-1 array capacity. It helps in reducing the write inherence found in RAID 4. RAID 5 array offers highest data transaction Read rate, medium data transaction Write rate and good cumulative transfer rate.

Characteristics and Advantages

Highest Read data transaction rate

Medium Write data transaction rate

Low ratio of ECC (Parity) disks to data disks means high efficiency

Good aggregate transfer rate

Disadvantages

Disk failure has a medium impact on throughput

Most complex controller design

Difficult to rebuild in the event of a disk failure (as compared to RAID level 1)

Individual block data transfer rate same as single disk

Recommended Applications

File and Application servers

Database servers

Web, E-mail, and News servers

Intranet servers

Most versatile RAID level

RAID Level 6:

RAIDS 6 are Independent Data Disk array with Independent Distributed parity. It is known to be an extension of RAID level 5 with extra fault tolerance and distributed parity scheme added. RAID 6 is the best available RAID array for mission critical

Applications and data storage needs, though the controller design is very complex

And overheads are extremely high.

Disadvantages

More complex controller design

Controller overhead to compute parity addresses is extremely high

Write performance can be brought on par with RAID Level 5 by using a custom

ASIC for computing Reed-Solomon parity

Requires N+2 drives to implement because of dual parity scheme

Recommended Applications

File and Application servers

Database servers

Web and E-mail servers

Intranet servers

Excellent fault-tolerance with the lowest overhead

RAID Level 10:

RAID 10 is classified as the futuristic RAID controller with extremely high Reliability and performance embedded in a single RAID controller. The minimum

Requirement to form a RAID level 10 controller is 4 data disks. The implementation

Of RAID 10 is based on a striped array of RAID 1 array segments, with almost the

Same fault tolerance level as RAID 1. RAID 10 controllers and arrays are suitable

For uncompromising availability and extremely high throughput required systems

And environment. With all the significant RAID levels discussed here briefly, another important point to add is that whichever level of RAID is used regular and consistent data backup maintenance using tape storage is must as the regular tape storage is best media to recover from lost data scene.

Disadvantages

Very expensive / high overhead

All drives must move in parallel to proper track lowering sustained performance

Very limited scalability at a very high inherent cost

Recommended Applications

Database server requiring high performance and fault tolerance

RAID Level 0+1:

It is the RAID array providing high data transference performance with at least 4 disks needed to implement the RAID 0+1 level. It's a unique combination of stripping

and mirroring with all the best features of RAID 0 and RAID 1 included such as fast

data access and fault tolerance at single drive level. The multiple stripe segments

have added high I/O rates to the RAID performance and it is the best solution for maximum reliability.

Disadvantages

RAID 0+1 is NOT to be confused with RAID 10. A single drive failure will cause the whole array to become, in essence, a RAID Level 0 array

Very expensive / high overhead

All drives must move in parallel to proper track lowering sustained performance

Very limited scalability at a very high inherent cost

Recommended Applications

Imaging applications

General Fileserver

RAID LEVEL 50

RAID Level 50 requires a minimum of 6 drives to implement

Characteristics and Advantages

RAID 50 should have been called "RAID 03" because it was implemented as a striped

(RAID level 0) array whose segments were RAID 3 arrays (during mid-90s)

Most current RAID 50 implementation is illustrated above

RAID 50 is more fault tolerant than RAID 5 but has twice the parity overhead

High data transfer rates are achieved thanks to its RAID 5 array segments

High I/O rates for small requests are achieved thanks to its RAID 0 striping

Maybe a good solution for sites that would have otherwise gone with RAID 5 but need some additional performance boost

Disadvantages

Very expensive to implement

All disk spindles must be synchronized, which limits the choice of drives

Failure of two drives in one of the RAID 5 segments renders the whole array unusable.