MCITP Interview Questions

What is Active Directory Domain Services 2008?

Active Directory Domain Services (AD DS), formerly known as Active Directory Services, is thecentral location for configuration information, authentication requests, and information aboutall of the objects that are stored within your forest. Using Active Directory, you can efficientlymanage users, computers, groups, printers, applications, and other directory-enabled objectsfrom one secure, centralized location.

****

Domain Functional Level

Domain functionality activates features that affect the whole domain and that domain only.The four domain functional levels, their corresponding features, and supported domainControllers are as follows:Windows 2000 mixed (Default)Supported domain controllers: Microsoft Windows NT 4.0, Windows 2000, WindowsServer 2003Activated features: local and global groups, global catalog support

****

What is DNS:-

Domain Name Service/Domain Name System

Provides resolution of name to IP addressing and resolution of IP addresses to names

****

What is DHCP:-

It gives Addresses automatically to the client who is requesting for an IP address

Centralized IP Address management

DHCP prevent IP address conflict and help conserve the use of client IP Address onthe on the network

DHCP reduces the complexity and amount of administrator work by assigningTCP/IP configuration automatically to the clients.

****

What is the Global Catalog?

A global catalog server is a domain controller. It is a master searchable database that containsinformation about every object in every domain in a forest. The global catalog contains acomplete replica of all objects in Active Directory for its host domain, and contains a partialreplica of all objects in Active Directory for every other domain in the forest.It has two important functions:Provides group membership information during logon and authenticationHelps users locate resources in Active Directory

****

Read-Only Domain Controllers (RODCs):-

RODC address some of the problems that are commonly found in branch offices.These locations might not have a DC, Or they might have a writable DC but no physicalsecurity to that DC, low network bandwidth, or inadequate expertise to support that DC.

****

Functionality of RODCs:-

Read-Only DS database

Uni-directional replication

Credential caching

Administrator role separation

****

Read-only AD DS Database:-

Except for accounts password, an RODC holds all the Active Directory objects andattributes that a writable domain controller holds.

However, changes cannot be made to the database that is stored on the RODC. Changesmust be made on a writable domain controller and then replicated back to the RODC.

****

What are FMSO Roles? List them.

FSMO roles are server roles in a Forest

There are five types of FSMO roles

1-Schema master

2-Domain naming master

3-Rid master

4-PDC Emulator

5-Infrastructure master

****

The schema master

domain controller controls all updates and modifications to theschema. Once the Schema update is complete, it is replicated from the schema master to allother DCs in the directory. To update the schema of a forest, you must have access to theschema master. There can be only one schema master in the whole forest.

****

The domain naming master

domain controller controls the addition or removal of domainsin the forest. This DC is the only one that can add or remove a domain from the directory. Itcan also add or remove cross references to domains in external directories. There can beonly one domain naming master in the whole forest.

****

Infrastructure Master:

When an object in one domain is referenced by another object in another domain, itrepresents the reference by the GUID, the SID (for references to security principals), andthe DN of the object being referenced. The infrastructure FSMO role holder is the DCresponsible for updating an object's SID and distinguished name in a cross-domain objectreference. At any one time, there can be only one domain controller acting as theinfrastructure master in each domain.

****

The RID master

is responsible for processing RID pool requests from all domain controllersin a particular domain. When a DC creates a security principal object such as a user orgroup, 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 eachsecurity principal SID created in a domain. Each DC in a domain is allocated a pool of RIDsthat it is allowed to assign to the security principals it creates. When a DC's allocated RIDpool falls below a threshold, that DC issues a request for additional RIDs to the domain'sRID master. The domain RID master responds to the request by retrieving RIDs from thedomain's unallocated RID pool and assigns them to the pool of the requesting DC. At any one time, there can be only one domain controller acting as the RID master in the domain.PDC Emulator

****

The PDC emulator

is necessary to synchronize time in an enterprise. Windows 2000/2003Includes the W32Time (Windows Time) time service that is required by the KerberosAuthentication protocol. All Windows 2000/2003-based computers within an enterpriseUse a common time. The purpose of the time service is to ensure that the Windows TimeService uses a hierarchical relationship that controls authority and does not permit loops toEnsure appropriate common time usage.

****

Basic Disk Storage

Basic storage uses normal partition tables supported by MS-DOS, Microsoft Windows 95,Microsoft Windows 98, Microsoft Windows Millennium Edition (Me), Microsoft WindowsNT, Microsoft Windows 2000, Windows Server 2003 and Windows XP. A disk initialized forBasic storage is called a basic disk. A basic disk contains basic volumes, such as primaryPartitions, extended partitions, and logical drives. Additionally, basic volumes includemultidisk volumes that are created by using Windows NT 4.0 or earlier, such as volumesets, stripe sets, mirror sets, and stripe sets with parity. Windows XP does not supportthese multidisk basic volumes. Any volume sets, stripe sets, mirror sets, or stripe sets withparity must be backed up and deleted or converted to dynamic disks before you installWindows XP Professional.

****

Dynamic Disk Storage

Dynamic storage is supported in Windows XP Professional, Windows 2000 and WindowsServer 2003. A disk initialized for dynamic storage is called a dynamic

disk. A dynamic diskcontains dynamic volumes, such as simple volumes, spanned volumes, striped volumes,mirrored volumes, and RAID-5 volumes. With dynamic storage, you can perform disk andvolume management without the need to restart Windows.

****

Dynamic Storage Terms

A volume is a storage unit made from free space on one or more disks. It can be formattedwith a file system and assigned a drive letter. Volumes on dynamic disks can have any of the following layouts: simple, spanned, mirrored, striped, or RAID-5.

A simple volume

uses free space from a single disk. It can be a single region on a disk orconsist of multiple, concatenated regions. A simple volume can be extended within thesame disk or onto additional disks. If a simple volume is extended across multiple disks, itbecomes a spanned volume.

A spanned volume

is created from free disk space that is linked together from multipledisks. You can extend a spanned volume onto a maximum of 32 disks. A spanned volumecannot be mirrored and is not fault-tolerant.

A striped volume(RAID-0)

is a volume whose data is interleaved across two or more physicaldisks.The data on this type of volume is allocated alternately and evenly to each of the physicaldisks. A striped volume cannot be mirrored or extended and is not fault-tolerant.

A mirrored volume (RAID-1)

is a fault-tolerant volume whose data is duplicated on two physicaldisks. All of the data on one volume is copied to another disk to provide data redundancy. If one of the disks fails, the data can still be accessed from the remaining disk. A mirroredvolume cannot be extended.

A Striping With Parity (RAID-5)

volume is a fault-tolerant volume whose data is striped acrossan array of threeor more disks. Parity (a calculated value that can be used to reconstruct data after a failure)is also striped across the disk array. If a physical disk fails, the portion of the RAID-5volume that was on that failed disk can be re-created from the remaining data and theparity. A RAID-5 volume cannot be mirrored or extended.

The system volume

contains the hardware-specific files that are needed to load Windows(for example, Ntldr, Boot.ini, and Ntdetect.com). The system volume can be, but does not have to be, the same as the boot volume.

The boot volume

contains the Windows operating system files that are located in the%Systemroot% and %Systemroot%System32 folders. The boot volume can be, but doesnot have to be, the same as the system volume.

RAID 0 Striping

RAID 1- Mirroring (minimum 2 HDD required)

RAID 5 Striping With Parity (Minimum 3 HDD required)

RAID levels 1 and 5 only gives redundancy

****

What is the SYSVOL folder?

The Sysvol folder on a Windows domain controller is used to replicate file-based data amongdomain controllers. Because junctions are used within the Sysvol folder structure, Windows NTfile system (NTFS) version 5.0 is required on domain controllers throughout a Windowsdistributed file system (DFS) forest.This is a quote from Microsoft themselves basically the domain controller info stored in files likeyour group policy stuff is replicated through this folder structure.

****

What's New in Windows Server 2008 Active Directory Domain Services?

Active Directory Domain Services in Windows Server 2008 provides a number of enhancementsover previous versions, including these

:Auditing - AD DS auditing has been enhanced significantly in Windows Server 2008. Theenhancements provide more granular auditing capabilities through four new auditingcategories: Directory Services Access, Directory Services Changes, Directory ServicesReplication, and Detailed Directory Services Replication. Additionally, auditing now provides thecapability to log old and new values of an attribute when a successful change is made to thatattribute

Fine-Grained Password Policies - AD DS in Windows Server 2008 now provides the

capability tocreate different password and account lockout policies for different sets of users in a domain.User and group password and account lockout policies are defined and applied via a PasswordSetting Object (PSO). A PSO has attributes for all the settings that can be defined in the DefaultDomain Policy, except Kerberos settings. PSOs can be applied to both users and groups.

Read-Only Domain Controllers — AD DS in Windows Server 2008 introduces a new type of domain controller called a read-only domain controller (RODC). RODCs contain a read-only copyof the AD DS database. ROD

Cs are covered in more detail in Chapter 6, "Manage Sites and Replication."

Restartable Active Directory Domain Services —AD DS in Windows Server 2008 can now bestopped and restarted through MMC snap-ins and the command line. The restartable AD DSservice reduces the time required to perform certain maintenance and restore operations.Additionally, other services running on the server remain available to satisfy client requestswhile AD DS is stopped.

AD DS Database Mounting Tool — AD DS in Windows Server 2008 comes with a AD DS databasemounting tool, which provides a means to compare data as it exists in snapshots or backupstaken at different times. The AD DS database mounting eliminates the need to restore multiplebackups to compare the AD data that they contain and provides the capability to examine anychange made to data stored in AD DS.

****

What is REPADMIN?

Repadmin.exe: Replication Diagnostics ToolThis command-line tool assists administrators in diagnosing replication problems betweenWindows domain controllers.Administrators can use Repadmin to view the replication topology (sometimes referred to asRepsFrom and RepsTool) as seen from the perspective of each domain controller. In addition,Repadmin can be used to manually create the replication topology (although in normal practicethis should not be necessary), to force replication events between domain controllers, and toview both the replication metadata and up-to-dateness vectors.

****

What is NETDOM?

NETDOM is a command-line tool that allows management of Windows domains and trustrelationships. It is used for batch management of trusts, joining computers to

domains,verifying trusts, and secure channels

KCC

The KCC is a built-in process that runs on all domain controllers and generates replicationtopology for the Active Directory forest. The KCC creates separate replication topologiesdepending on whether replication is occurring within a site (intrasite) or between sites(intersite). The KCC also dynamically adjusts the topology to accommodate new domain controllers, domain controllers moved to and from sites, changing costs and schedules, anddomain controllers that are temporarily unavailable.

****

How do you view replication properties for AD?

By using Active Directory Replication Monitor.Start

> Run > Replmon

****

What are sites What are they used for?

One or more well-connected (highly reliable and fast) TCP/IP subnets. A site allowsadministrators to configure Active Directory access and replication topology to take advantage of the physical network.