Active Directory - Cheatsheet

- Active Directory Details

Active Directory Details

Active Directory components in Windows Server 2008

The range of Active Directory (AD) has expanded in Windows Server 2008 and has become an essential part of many information technology (IT) environments. Active Directory has become an umbrella for a multitude of technologies surpassing what AD was in Windows Server 2000 and 2003. Check out the new uses for Active Directory:

- **Active Directory Domain Services:** An X.500-based directory service that provides integrated authentication and authorization services for a Windows computing environment.
- **Active Directory Lightweight Directory Services:** A stripped down version of Active Directory Domain Services that focuses on providing just the directory services functionality.
- **Active Directory Federation Services:** A Web Services–based technology for providing Web single sign-on authentication services between different organizations.
- **Active Directory Certificate Services:** Provides digital certification enrollment and revocation services in the support of a public key infrastructure (PKI).
- **Active Directory Rights Management Services:** Provides a solution for managing how users can use documents that they're authorized to access.

Roles of the Active Directory domain controllers

Active Directory uses a multiple-master model, and usually, domain controllers (DCs) are equal with each other in reading and writing directory information. However, certain roles cannot be distributed across all the DCs, meaning that changes can't take place on more than one domain controller at a time. Some domain controllers, therefore, do assume a single-master operations role — known as operations masters in Active Directory.

The five categories of operations master roles are:

- **Schema master** (one per forest): Maintains the master copy of the schema.

- **PDC emulator** (one per domain): Emulates a primary domain controller for backward compatibility with Windows NT.
- **Domain naming master** (one per forest): Tracks object names throughout a forest to ensure that they’re unique. Also tracks cross-references to objects in other directories.
- **Infrastructure master** (one per domain): Tracks object references among domains and maintains a list of deleted child objects.
- **Relative identifier (RID) master** (one per domain): Tracks the assignment of SIDs (security identifiers) throughout the domain.

Usually, the first domain controller that you create in the first domain assumes the operations master roles. You can assign these roles to other domain controllers in the domain or forest, but only one domain controller at a time can hold each role.

1. What is Active Directory?

It is a database and set of services that contain critical information about users and computers, including the environment and who is allowed to do what. All this information stored under the AD database makes it easy for the administration and users to find and easy to use.

2. Define Kerberos.

Kerberos is a widely used computer network authentication protocol that provides security to the service requests between two or more trusted hosts across untrustworthy networks(like the Internet). It is widely used because of the below-listed benefits:

- Single sign-on.
- Secure.
- Mutual authentication.
- Trusted third party.

3. What is a domain in Active Directory?

An Active Directory domain is a grouping of network resources that share common administration and services. Each domain contains a database that will store the object identity information. Domains are grouped in a tree structure; the group of trees is known as an Active Directory forest.

4. What is the SYSVOL folder.

The SYSVOL(System volume) folder is an essential part of AD found on each domain controller (DC). The log files and Active Directory database are stored in the SysVOL folder on the server.

The SYSVOL folder is located at `C:\Windows\SYSVOL`.

5. What is RID Master?

RID is one of the FSMO roles in AD forest. It is responsible for allocating a unique RID sequence or relative IDs to all the domain controllers in its domain. Only one domain controller in each domain will be there that holds this role.

6. Where is the location of the AD database?

Microsoft Windows has a centralized database known as AD(Active Directory). It stores information about the user, computers, and other things in the network. The location of the Active Directory is not fixed. It is dependent on various things like the Operating System version, network configuration, etc. Although, in many cases, it is stored in the form of a file named NTDS.DIT, which is on a domain controller in the following location `C:\Windows\NTDS\`.

7. Name the three ports used by Active Directory.

The three ports used by the AD are:

- **DNS:** port 53 TCP, UDP
- **LDAP:** port 389 TCP, UDP
- **Kerberos:** port 88 TCP, UDP

8. Compare domain local, global, and universal groups in Active Directory.

The domain local, global, and universal groups are used to manage user access.

- **Domain local groups:** Permissions are granted to users inside a single domain using domain local groups
- **Global groups:** Permissions are given to users across multiple domains using global groups

- **Universal groups:** Permissions are given to users across multiple domains and forests using universal groups

9. Name the different components of the active directory schema.

The three components of active directory schema are:

1. Classes: Attributes are organized into object classes in an Active Directory Schema. In an Active Directory structure, there are three different classes:

- Structural class
- Abstract class
- Auxilliary class

2. Objects: Objects is the basic element of Active Directory that represents resources present in the AD network, such as users, printers, applications, a group, or a computer.
3. Attributes: In the Active Directory environment, attributes are the entities that are used to hold data/information about the objects.

Various Questions

What's the difference between a UPN and SAMAccountName.

> **The samAccountName is the User Logon Name in Pre-Windows 2000 (this does not mean samAccountName is not being used as Logon Name in modern windows systems). The userPrincipalName is a new way of User Logon Name from Windows 2000 and later versions.**

What is the KCC what does it do?

> The Knowledge Consistency Checker (KCC) **creates connection objects automatically, but they can also be created manually**. Connection objects created by the KCC appear in the Active Directory Sites and Services snap-in as <automatically generated> and are considered adequate under normal operating conditions.

What is the ISTG what does it do?

>

> The Inter-Site Topology Generator is an Active Directory process that **defines the replication between Active Directory sites on a network**. A single domain controller in each site is automatically designated to be the Inter-Site Topology Generator.

What is a bridgehead server? Which DCs are bridgeheads by default? Why would you want to designate a specific bridgehead(s)?

> A bridgehead server is **a server that is mainly used for intersite replication**. You can configure a bridgehead server for every site that is created for each intersite replication protocol. This helps to control the server that is used to replicate information to other servers.

What is the KRBTGT account? What does it do why is it important? How would you recover from a KRBTGT compromise?

> The KRBTGT (Key Distribution Center Service Account) is a hidden account in AD that acts as the authentication service for the domain. It encrypts the Ticket Granting Ticket (TGT) with a secret key to ensure secure authentication throughout the domain.

Explain to me how ad sites and services weighting works?

>

Explain to me replciation intervals, intersite vs intrasite? How can you improve this?

>

Explain your current AD S&S config. Are you hub and spoke? Are you full mesh? What is bridge all site links?

>

Explain to me DNS delegation? Why would you use it?

>

Explain to me forwarding? Types? When or why would you use it?

>

What is the role of an SPN? Why are they necessary?

>

Explain to me Kerberos delegation? What types of Kerberos delegation are there? What are the risks with delegation?

Explain to me golden ticket, silver ticket, kerberoasting are and protections against them?

What is adminsdholder, sdprop and admincount =1? What does it do and why is it important?

When sizing a domain controllers memory what is the key metric that should determine server memory?