Cram Guide for Exam 70-294 - Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure

Created by Yu Chak Tin Michael, Sept 2004

Planning and Implementing an Active Directory Infrastructure

Plan a strategy for placing global catalog servers.

1. The global catalog (GC) is used during the logon process and during the location of directory objects in different domains. By increasing the number of Global Catalog Servers (GCS) response time can be improved. However, with too many of them network traffic will become excessive.
2. Try to have at least one GCS in each local location so that traffic can be localized as much as possible.

Plan flexible operations master role placement.

3. The PDC emulator and RID master should be kept on the same domain controller.
4. The Domain Naming Master should be stored on a Global Catalog server.
5. A single master role cannot occur simultaneously at different locations on the network.

Implement an Active Directory directory service forest and domain structure.

6. A forest can consist of either a single domain or multiple domains.
7. A tree is a contiguous namespace.
8. Domains are entities that can be combined into trees and forests. They act as the administrative and security boundaries.

Implement an Active Directory site topology.

9. Sites are based on the network's physical structure and can include Active Directory domain controllers from the same or different Active Directory domain(s).
10. Sites are deployed mainly for localizing traffic.
11. You use site links to specify how Active Directory will connect different sites through favorable replication links.

Plan an administrative delegation strategy.

12. You may use the Delegation wizard to specify to whom you want to delegate authority, the objects to which these users should gain authority, and the permissions the designated users have over these objects.
13. Effective admin often involves delegation! However, do NOT delegate EVERYTHING to your subordinates.
14. If a user is a member of the administrators group, there is no way to limit his/her access.

Managing and Maintaining an Active Directory Infrastructure

Manage an Active Directory forest and domain structure.

15. You seldom need multiple forests unless you are merging two companies into one.
16. You use single domain when your network is small and simple.
17. You use multiple domains to isolate replication traffic, to support decentralized administration and to support more than one domain policy. Note that more domains mean more overhead.
18. You can move Active Directory objects such as users, groups, and OUs from one location to another through the use of Active Directory Users and Computers.
19. You may also use MoveTree.exe at the command-line to move Active Directory objects between domains in a single forest. Not everything is movable though.

Manage an Active Directory site.

20. Within a site, replication traffic is carried out via Remote Procedure Calls.
21. Knowledge Consistency Checker (KCC) generates a replication topology for both intra-site and inter-site replication.
22. You use the REPADMIN command-line utility to check the KCC status and configure replication options.

Monitor Active Directory replication failures.

23. Replication occurs between sites over manually created links based on predefined replication schedule.
24. When Active Directory is installed, a default site link known as DEFAULTIPSITELINK is created.
25. When multiple paths are available, cost value determines which site link is to be used.
26. Transport used for transferring data between sites are either RPC or SMTP. You use SMTP when the network links are less stable.

Restore Active Directory directory services.

27. The Active Directory replication system uses the Update Sequence Number (USN) to detect and replicate changes to Active Directory to all the domain controllers on the network.
28. During a typical file restore operation, Windows Backup operates in non-authoritative restore mode. That means, Windows Backup will restore all files, including Active Directory objects, with their original USN. The effect is that the Active Directory replication system will update the restored data with newer data from other domain controllers.
29. On the other hand, an authoritative restore replicates all objects that are marked authoritative to every domain controller hosting the naming contexts that the objects are in.
30. You use the Ntdsutil.exe tool to make the necessary USN changes to the Active Directory database and perform an authoritative restore on the computer.
31. To restore deleted user accounts, computer accounts, or security groups, you either restore the deleted accounts and then add the restored accounts back to their groups, or authoritatively restore the deleted accounts and the deleted account' security groups two times.

Troubleshoot Active Directory.

32. Each Active Directory object must be uniquely identified.
33. Domain Name System (DNS) is required for Active Directory to run. No DNS, No AD. In particular, the Active Directory DNS records must be registering in DNS.
34. You must configure specific network components properly so that computers will be able to join the domain.
35. If pre-W2K clients will participate in the Active Directory domain, NetBIOS name resolution must be enabled.

Planning and Implementing User, Computer, and Group Strategies

Plan a security group strategy.

36. You should organize domain users based on administrative needs. Create a global group and add the appropriate user accounts into the group as members. Then create a domain local group and add all global groups from the other domain that needs the same access to a resource in your domain. Finally, assign the required permissions on the shared resource to the domain local group.
37. Universal groups are seldom used.

Plan a user authentication strategy.

38. When planning a user authentication strategy, the goal is to minimize admin overhead without sacrificing security.
39. One suggested practice is to hold all resources in one domain and all users in another domain.

Plan an OU structure.

40. An OU is a logical container for organizing objects within a domain into sub-groups.
41. You cannot create an OU in a parent domain with the same name as a child domain because a name conflict is created.
42. Too many OUs may complicate your admin work. However, multiple OUs allow separation of duties when you have multiple subordinates to share your admin work load.

Implement an OU structure.

43. You use multiple OUs to control access to resources, to create group policy objects, to delegate administration, and to group commonly used objects.
44. You may choose to delegate admin duties on a per OU basis.

Planning and Implementing Group Policy

Plan Group Policy strategy.

45. You use Group Policy to restrict users and enforce limitations. Operating systems prior to W2K must utilize system policies instead.

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.

46. The goal of group policy is to reduce Total Cost of Ownership (TCO) by easing network administration.
47. Group policies are implemented first by Site, then by Domain, and finally by OU.

Configure the user environment by using Group Policy.

48. Possible policy settings are Not Configured, Enable and Disabled.
49. You may assign Disk quotas via group policies to restrict how much space a user can consume in specific folders.

Deploy a computer environment by using Group Policy.

50. You may assign a software so that the software can be installed regardless of whether it is used.
51. You may publish a software to make it available to your users or machines when it is in need.
52. Software can be assigned to users or computers.
53. Software can be published only to users, not to computers.

Managing and Maintaining Group Policy

Troubleshoot issues related to Group Policy application.

54. You may use GPUPDATE for group policy updates.
55. You may use the Gpotoole.exe Utility to check GPO and GPO replication.
56. Proper connectivity and DNS resolution must be in place for proper group policy application.
57. Examine the log file Userenv.log (generated by verbose debug logging on the client) to find out the root cause of a general failure to enumerate the list of GPOs that apply to the user.

Maintain installed software by using Group Policy.

58. The Configure Automatic Updates policy allows you to specify whether the computer receives security updates and other important downloads through the Windows Automatic Updates feature.

Troubleshoot the application of Group Policy security settings.

59. You may restrict group membership by using group policy. Do remember that changes to restricted groups remain in effect until the group policy is refreshed.
60. You may use RSoP (Resultant Set of Policy) to show how permissions and policies overlap.
61. You may use the Group Policy Results tool (Gpresult.exe) to display information about how Group Policy affects both the currently logged-on user and the computer.
62. You may delay the security policy from being applied when no changes have been made in the GPO by editing the registry.

© Copyright 2004 CertTalk.com/Adaptive Learning Systems, Inc. All Rights Reserved.