The MCSE Windows® 2000 Directory Services Cram Sheet

This Cram Sheet contains the distilled, key facts about the Directory Services Infrastructure exam. Review this information last thing before entering the testing center, paying special attention to those areas where you feel you need the most review. You can transfer any of the facts onto a blank piece of paper before beginning the exam.

INSTALLING, CONFIGURING, AND TROUBLESHOOTING ACTIVE DIRECTORY

1. Active Directory can be installed in one of two ways:
   - With the **dcpromo.exe** command
   - By using the Configure Your Server administrative tool
2. Verify Active Directory installation by checking for SRV and A records on the DNS server for the new domain controller.
3. Active Directory initially installs in mixed mode; if you want to change it to native mode, you must do so manually.
4. Once converted to native mode, a domain cannot revert to mixed mode to support NT 4 domain controllers.
5. Perform an authoritative restore by booting the computer in Directory Services Repair Mode and running ntdsutil.exe.
6. New sites are configured through Active Directory Sites and Services.
7. After creating a new site, the following tasks must be completed:
   - Add appropriate IP subnets to the site.
   - Install or move a domain controller or controllers into the site. Although a domain controller is not required for a site, it is strongly recommended.
   - Connect the site to other sites with the appropriate site link.
   - Select a server to control and monitor licensing within the site.
8. All site links are bridged by default.
9. Site link bridges can be explicitly defined if a network is not fully routed.
10. Inbound replication can be configured through connection objects.
11. The KCC (Knowledge Consistency Checker) maintains schedules and settings for default site links and bridges. Administrator-configured connection objects require manual configuration and maintenance.
12. Cost is used to determine which path to take between sites when multiple links exist.
13. Global Catalog (GC) servers maintain a read-only subset of information in the complete Active Directory database.
14. To configure a server as a GC server, use Active Directory Sites and Services. Select the desired domain controller, then right-click on NTDS settings and choose properties. Check the box for Global Catalog.
15. Use the Windows 2000 Backup utility to back up the AD system state data.
16. Use authoritative restore when you want your restored settings to overwrite existing AD settings on other domain controllers, such as if an object (OU, user account, and so on) is accidentally deleted from the database.
17. Use nonauthoritative restore when you are restoring out-of-date information and want the restored data to be overwritten by newer data stored in Active Directory on other domain controllers. For example, you would do this if you were recovering a DC from a failed hard drive and restored the server.
18. All domains in a tree automatically establish two-way trust relationships called Kerberos trusts.
19. Trust relationships between Windows 2000 domains and NT 4 domains must be configured manually, just as you would configure a trust relationship between two NT 4 domains.

INSTALLING, CONFIGURING, MANAGING, MONITORING, AND TROUBLESHOOTING DNS FOR ACTIVE DIRECTORY

20. Caching servers do not store an editable copy of the zone database.
21. Active Directory integrated zones can reside only on domain controllers, not member servers or non-Windows 2000 servers of any kind (NT 4, Unix, and so on).
22. If a user who is trying to log on gets an error that a domain controller cannot be found, check for the presence of SRV records in the DNS database for domain controllers.
23. Secure dynamic updates allow only computers and users who have been given permission to update their records into the DNS database.
24. Secure dynamic update is supported only for Active Directory integrated zones.
25. DNS replication is accomplished through Active Directory replication for AD integrated zones and zone transfer for standard zones.
26. A reverse lookup zone must be configured in order to perform reverse lookup queries.
27. Installing AD through Configure Your Server does *not* create a reverse lookup zone in DNS.
28. Windows 2000 DHCP can act as a proxy for non-Windows 2000 clients to support dynamic updates into the DNS database.
29. DHCP is required to support dynamic updates

INSTALLING, CONFIGURING, MANAGING, MONITORING, OPTIMIZING, AND TROUBLESHOOTING CHANGE AND CONFIGURATION MANAGEMENT

30. The No Override setting takes precedence over Block Policy Inheritance.
31. Group Policy settings are applied in the following order:
    - Local
    - Site
    - Domain
    - OU
32. Local policy will always override global policy settings.
33. Unless modified through Block Policy Inheritance or No Override, OU policies overwrite domain policies and domain policies overwrite site policies.
34. Group Policy Objects are linked to sites, domains, and OUs, never directly to security groups.
35. The policies configured in a GPO cannot be selectively applied—it's all or nothing.
36. Create GPOs through Active Directory Users and Computers; edit GPOs with the Group Policy Editor (MMC snap-in).
37. Apply Group Policy and Read are the required permissions to receive the effects of a GPO.
38. Scripts are processed in the following order:
    - Startup
    - Logon
    - Logoff
    - Shutdown
39. Create a RIS boot disk for supported network adapters through the rbfg.exe utility.
40. RIPrep is used to create custom installation images. Run it on a Windows 2000 Professional system from a Windows 2000 RIS server (that is, \\server\riprep.exe from the Run line on a workstation).

41. An active DHCP server must exist on the same subnet as a RIS client for RIS to work.
42. Running RISetup after installing the RIS service creates a CD-based RIS installation image.
43. If you need to support a few Windows 2000 systems that have hardware not contained by the majority of RIS clients, simply use a CD-based image in the appropriate language.
44. RIS clients must either have a network adapter that supports PXE or be directly supported by the RIS boot disk.
45. Deploy software through the Software Installation extension in the Group Policy Editor.
46. Published applications are available for the user to install through Add/Remove Programs.
47. Published applications by default are not configured to auto-install, though they can be configured to auto-install through the package properties.
48. Assigned applications appear in the user's Start menu and/or desktop and automatically install when launched.
49. Assigned applications can be uninstalled by the user but will reinstall themselves after the user logs off and logs back in. Assigned applications are said to be "sticky" applications.
50. Published applications can be uninstalled by the user if so desired.
51. Software deployment problems are almost always attributable to permissions or missing, corrupt, or unavailable source files.
52. Delegate authority for nonadministrators to create GPOs through the Active Directory Users and Computers administrative tool.
53. The following are facts about system policies:
    - They are applied only to domains.
    - They are limited to Registry-based settings an administrator configures.
    - They are not written to a secure location of the Registry; hence, any user with the ability to edit the Registry can disable the policy settings.
    - They often last beyond their useful life spans. System policies remain in effect until another policy explicitly reverses an existing policy or a user edits the Registry to remove a policy.
    - They can be applied through NT domain security groups.
54. The following are facts about Group Policy:
    - It can be applied to sites, domains, or OUs.
    - It can be applied through domain security groups and can apply to all or some of the computers and users in a site, domain, or OU.
    - It is written to a secure section of the Registry, thereby preventing users from being able to remove the policy through the regedit.exe or regedt32.exe utility.
    - It is removed and rewritten whenever a policy change takes place. Administrators can set the length of time between policy refreshes, ensuring that only the current policies are in place.
    - It provides a more granular level of administrative control over a user's environment.

MANAGING, MONITORING, AND OPTIMIZING THE COMPONENTS OF ACTIVE DIRECTORY

55. Active Directory log files should be stored on a separate physical disk from the database for best performance.
56. Delegate administrative control of AD objects through the Active Directory Users and Computers snap-in. Right-click on the object and choose Delegate Control to start the Delegation of Control Wizard.
57. ACLs are used to control access to AD resources. These are configured on the Security tab of an object's property sheet.
58. For AD replication, there can be IP or SMTP transports. SMTP is used for unreliable WAN links between sites. IP is used when a LAN or WAN connection is considered reliable.
59. SMTP replication works only intersite. IP replication can be intersite or intrasite.
60. When replicating among multiple sites, there must be a schedule overlap so that replication can complete. Otherwise, replication will either fail completely or changes will not appear in other sites until the next scheduled replication period.
61. Offline defragmentation of the Active Directory database can be performed only while the computer is booted in Directory Service Repair Mode (run ntdsutil). It is also the only way to reduce the size (compact) the database.

CONFIGURING, MANAGING, MONITORING, AND TROUBLESHOOTING ACTIVE DIRECTORY SECURITY SOLUTIONS

62. Security templates can be used to provide a default security level on a Windows 2000 system. They are applied through Group Policy, and the important ones to know are:
    - *basicdc.inf*—Default security settings for a domain controller
    - *basicsv.inf*—Default security settings for a standalone (or member) server
    - *basicwk.inf*—Default security settings for a Windows 2000 Professional system
    - *compatws.inf*—Security settings that make Server or Professional backwardly compatible with Microsoft Windows NT 4
    - *hisecdc.inf*—High security settings for a domain controller
    - *hisecws.inf*—High security settings for a Windows 2000 Professional system
    - *securedc.inf*—Secure domain controller settings
    - *securews.inf*—Secure Windows 2000 Professional settings
63. The Security Configuration and Analysis tool is used to configure security on *local* systems only. Group Policy is used to configure security in Active Directory.
64. Auditing is not enabled by default. To enable it, use the Group Policy Editor.
65. Select object to audit through the advanced security settings in the object's property sheet (click on the Advanced button on the Security tab, then select the Audit tab).
66. Audited events appear in the Security log in the event viewer.
67. Universal groups are available only when a domain is in native mode.
68. The recommended order of applying permissions to access resources is:
    - Place user accounts into global groups.
    - Place global groups into universal groups (if in native mode).
    - Place universal groups into local groups.
    - Apply access permissions to the local groups.

CORIOLIS™
Certification Insider Press
© 2000 The Coriolis Group. All rights reserved.