Cram Guide for Exam 70-290 - Managing and Maintaining a Microsoft Windows Server 2003 Environment

Created by Yu Chak Tin Michael, Sept 2004

Managing and Maintaining Physical and Logical Devices

Manage basic disks and dynamic disks.

1. Logical Disk Manager (LDM) handles disk drive operations.
2. Basic disks can support up to 4 primary partitions or up to 3 primary partitions and 1 extended partition (which can hold many logical drives).
3. Basic disks can be extended without conversion to dynamic disks.
4. Dynamic Disks are volume-oriented and have much less limitations than Basic Disks.
5. The Disk Management console is the GUI for performing most disk operations.
6. The Disk Quota management feature allows you to limit users to a certain amount of disk space on a volume by volume basis.

Monitor server hardware.

7. You use System Monitor to graphically display performance of various real-time statistics.
8. You use Performance Logs and Alerts to record data for creating and comparing with a baseline.
9. You use the Hardware Troubleshooting Wizard to walk through solutions to common hardware related problems.

Optimize server disk performance.

10. Striped volume means RAID 0. Mirrored volume means RAID 1. RAID 5 refers to striping with parity.
11. You use the Disk Defragmenter to analyze the amount of fragmentation that exists on your disks and rewrite files back to the disks in contiguous units.

Install and configure server hardware devices.

12. With Driver Signing, you have the option to install only drivers that have been digitally signed, receive a warning for drivers haven't been signed, or never allow unsigned drivers to be installed.
13. You can use SIGVERIF.EXE to look for files that are not signed.
14. You rely on Windows Update to maintain a list of known bad drivers (which is kept in the drv_protect.htm file).
15. Hardware connected to a laptop computer often changes, which leads to the need for multiple hardware profiles (a menu will show up during the boot process).

Managing Users, Computers, and Groups

Manage local, roaming, and mandatory user profiles.

16. Profiles can exist for users and hardware.
17. A roaming profile allows you to use the same desktop regardless of the computer you use.
18. A mandatory profile does not allow a user to make permanent changes to the desktop settings.
19. A mandatory profile can be created by changing the user profile filename from NTUSER.DAT to NTUSER.MAN.

Create and manage computer accounts in an Active Directory environment.

20. You may use the Active Directory Users and Computers snap-in to manage computer accounts.

Create and manage groups.

21. The available types of groups are Machine local, Domain local, Global, Universal and Pre-Windows 2000 Compatible.
22. The Pre-Windows 2000 Compatible Access group is solely for backward compatibility with computers running NT 4.0 and earlier. Members of this group have Read access on all users and groups in the domain.
23. Default groups that cannot be deleted are: Administrators, Backup Operators, Guests, Network Configuration Operators, Power Users, Print Operators, Remote Desktop Users, Replicator, and Users.

Create and manage user accounts.

24. You may use the Active Directory Users and Computers snap-in to manage user accounts.
25. Account Policies are always set at the domain level.

Troubleshoot computer accounts.

26. You may use Netdom.exe (which is included in Windows Server 2003 Support Tools) to rename a computer that is a member of a Windows Server 2003 domain. Renaming can be performed either locally or remotely on the computer that is being renamed.
27. You may also use Netdom.exe to reset machine account passwords of a Windows Server 2003 domain controller.

Troubleshoot user accounts.

28. You may recover deleted security principals and restore their group memberships but each security principal must exist in Active Directory before you restore its group membership.

Troubleshoot user authentication issues.

29. Settings in the Account Lockout and Password Policy nodes of the Default Domain policy settings allows you to configure account lockout and mitigate the threat of brute force guessing of account passwords.
30. Lockout count determines how many invalid attempts are allowed before locking the account. Lockout reset time refers to the amount of time that is allowed between invalid attempts. Lockout duration determines the time period the account is locked for.
31. Remote Access Authentication Protocols supported include: CHAP (highly secure), EAP (mainly for smart cards), MS-CHAP (highly secure but client communication must be between two MS operating systems), MS-CHAP v2 (implements two-way authentication), PAP (clear text passwords), and SPAP (medium security).

Managing and Maintaining Access to Resources

Configure access to shared folders.

32. Share permissions apply only when a user is accessing a file or folder non-locally.
33. With Share Level Permissions, the Everyone group is given read permission automatically when a file is shared.
34. The primarily available share permissions include Full Control, Change and Read.
35. Share level permissions can be applied on a user or on a group level, although assigning permissions on a group basis is always recommended.
36. Individual permissions and group permissions can be combined to form the user's effective permissions.
37. You can share a file from the command line via the NET SHARE command.

Troubleshoot Terminal Services.

38. Terminal Services functionality is included in the Windows Server 2003 license, although a Windows CAL is required for each client.
39. The conventional Terminal Server deployment is for Terminal Server to accept simultaneous access by multiple remote clients to Windows-based programs that run on the server.
40. Remote Desktop for Administration allows you to remotely manage Windows Server 2003-based servers from any Terminal Services client.
41. If Terminal Services does not run as expected, check the IP address and make sure that it is valid. Also check the encryption level for Terminal Services sessions (the default is set to Client Compatible to provide the highest encryption level that is supported by the client).

Configure file system permissions.

42. NTFS permissions (does not work with FAT32 partitions) allow you to assign permissions more granularly at the folder and file level (while Share permissions are limited to the folder level).
43. File permissions always take precedence over folder permissions.
44. When copying folders or files from one NTFS partition to another (or on the same partition), the NTFS permissions will be inherited from the target folder. When moving files to another NTFS partition, the NTFS permissions will also be inherited from the target folder. When moving files or folders on the same NTFS partition, the NTFS permissions will remain intact.

Troubleshoot access to files and shared folders.

45. To find out the effective permissions for a user: first pick the

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

least restrictive share permission and the least restrictive NTFS permission, then pick the most restrictive of the two.
46. Always remember that any time a user is explicitly denied access, this overrides all other permissions.

Managing and Maintaining a Server Environment

Monitor and analyze events.
47. You use Event Viewer for viewing the log files of Application, System, Security, Directory Services, File Replication Service and DNS.
48. You may use System Monitor to view the performance of the various real-time statistics in the form of objects and counters.

Manage software update infrastructure.
49. You use the Software Update Service (SUS) for centralized distribution of hotfixes and security updates. With SUS, your client can update software from the internal network server rather than from Microsoft over the internet.
50. You need to use Group Policies to target update servers.

Manage software site licensing.
51. Microsoft licenses software as Full Packaged Product, Original Equipment Manufacturer, or Volume Licenses.
52. Select License is designed for organizations with mixed software and acquisition requirements.
53. Enterprise Agreement is designed for organizations that prefer to standardize their Microsoft software throughout their organization based on the Microsoft enterprise products. At the end of the agreement the customer can continue to use the software.
54. Enterprise Subscription Agreement is designed for organizations that prefer to standardize their Microsoft software throughout their organization based on the Microsoft enterprise products. At the end of the subscription the rights to use the software end.
55. Per Device or Per User basis of licensing requires every computer to have a separate Client Access License (CAL).
56. The per-server licensing mode permits a server to allow a certain number of concurrent connections.

Manage servers remotely.
57. Terminal Services allows remote serever management. Session Directory technology allows you to reconnect to a Terminal Services session from which you have disconnected.
58. You may use the Windows Server 2003 Administration Tools package (Adminpak.msi, available on product CD or download from MS) to remotely administer 2003 servers.
59. Windows 2003 include a command-line utility known as Wmic.exe to access Windows Management Instrumentation (WMI). When you run the Wmic.exe utility for the first time, the utility will compile its .mof files as necessary.
60. You may configure the Remote Assistance tool to enable an expert user to initiate a Remote Assistance session by using the Offer Remote Assistance feature. Note that the Remote Assistance feature requires the computer of the expert user as well as the computer of the novice user to be members of the same domain or members of trusted domains.

Troubleshoot print queues.
61. Printing problems can occur because of problems with the printing device, the connection between the printer and the network, other printing components in Server 2003, as well as the network, protocols, and other communication services in Server 2003.
62. To troubleshoot printing problems, you should verify that:
    a. the physical printer is operational.
    b. the print server is operational.
    c. the printer that is on the print server is using the correct printer driver.
    d. the client computer has the correct printer driver.
    e. on the print server you should check disk space for spooling and may try to change an Enhanced Metafile (EMF) data type print job to the RAW data type to see if it solves the problem.

Monitor system performance.
63. Performance data collected is defined in terms of objects, counters, and instances. A performance object is any resource, program, or service that can be measured.
64. You use System Monitor and performance logs and alerts to select performance objects, counters, and instances to collect and display data about the performance of system components or installed software.
65. You may want to set an alert on a counter so that a message is sent, a program starts, or a log starts when the selected counter's value is above or below a specified level.

Monitor file and print servers.
66. The best tool to use is still the System Monitor.
67. You may also use Performance Logs and Alerts to monitor the relevant counters.

Monitor and optimize a server environment for application performance.
68. By default, Server 2003 caches all disk read and disk write operations for faster application performance.
69. You should use System Monitor to monitor and identify performance bottlenecks.
70. Disk and memory are the commonly identified source of performance problems.

Manage a Web server.
71. IIS 6.0 is the web service on Server 2003. It is locked down by default for limiting the attack surface area through aggressive security defaults. It also includes a plain text XML configuration file that can be modified without having to stop the server, and command-line scripting.
72. IIS 6.0 provides full support for Windows Management Instrumentation as well as command-line and script-based administration.
73. You may optimize your web service performance through the following means:
    a. Disable Nonessential Services
    b. Optimize Data Throughput for Network Applications
    c. Optimize Performance for Background Services
    d. Disable IIS 6.0 Logging
    e. Enable Bandwidth Throttling
    f. Enable CPU Monitoring
    g. Limit Web Site Connections
    h. Use HTTP Keep-Alives

Managing and Implementing Disaster Recovery

Perform system recovery for a server.
74. You may use the command line based Recovery Console to repair Windows if the computer does not start correctly. You can start the Recovery Console from the Windows Server 2003 CD or at startup (if you previously installed the Recovery Console on the computer). Do note that you must be logged on as Administrator or as a member of the Administrators group in order to perform this procedure.
75. You may use the System control panel to configure system failure and recovery options.
76. You may also modify system failure and recovery settings on local or remote computers by modifying the registry key of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\CrashControl

Manage backup procedures.
77. You use the Windows Server 2003 Backup Utility to backup and restore system data.
78. You may also perform backup operations from the command prompt or from a batch file via the ntbackup backup command.
79. A normal/full backup includes all files. Slowest backup but fastest restore. Incremental backup has the fastest backup but slowest restore. Differential backup is in between the two. In any case you must start with a full backup the very first time you backup your data.
80. You may choose to produce either Detailed (includes the name of every file backed up) or Summary (includes a file count and indicates the files skipped) backup logs.

Recover from server hardware failure.
81. If your system has a startup problem immediately after you make a change to the computer, try to start the computer by using the Last Known Good Configuration feature which can restore registry information and driver settings that were in effect the last time the computer started successfully.
82. Safe mode allows you to start the system with a minimal set of device drivers and services. To start Windows Server 2003 in Safe mode, you need to press F8 when the Please Select The Operating System To Start message appears.
83. You may need to use the Recovery Console, which is not installed by default. To install the Recovery Console, boot from the Windows Server 2003 CD and choosing Repair, or running winnt32.exe /cmdcons from the I386 directory of the CD.

Restore backup data.
84. You use the Windows Server 2003 Backup Utility to restore backup data. Note that different backup methods require the use of different restore methods.

Schedule backup jobs.
85. You use the Windows Server 2003 Backup Utility to schedule backup jobs.
86. Timing is important – during backups the server will run slower than usual, therefore you should schedule the backup to take place at night or on weekends when no one is working in the office.

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