Cram Guide for Exam 70-293 - Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Created by Yu Chak Tin Michael, Sept 2004

Planning and Implementing Server Roles and Server Security

Plan and configure security for servers that are assigned specific roles .

1. PDC (Primary Domain Controller) emulator is used for backward compatibility.
2. RID (Relative ID) Master is for holding the pool of ID numbers to be used.
3. Infrastructure Master is for handling updates and name changes.
4. Domain Naming Master is (by default) the first domain controller in a forest.
5. Schema Master is responsible for overseeing all schema operations.
6. PDC emulator and RID master should be kept on the same domain controller
7. Domain Naming Master should be stored on a Global Catalog server for optimal performance.

Plan a secure baseline installation.

8. You may use the Microsoft Baseline Security Analyzer tool (MBSA) to centrally scan Windows-based computers for common security misconfigurations and generates individual security reports.
9. You may also use MBSA to scan for missing security updates
10. The command line version of the tool is mbsacli.exe.
11. You may use the Hfnetchk tool to centrally assess the security update status of computers.

Evaluate and select the operating system to install on computers in an enterprise.

12. The four different versions of Windows Server 2003 available are the Web edition (which supports max two processors), the Standard Edition (which supports max two processors), the Enterprise Edition (which supports max 8 processors) and Datacenter Edition (which supports max 32 processors).
13. The Web edition is for server hosting web sites in a low cost way.

Planning, Implementing, and Maintaining a Network Infrastructure

Plan a TCP/IP network infrastructure strategy.

14. Server computer should always use static IP address for itself. For other computers, you may configure DHCP server to use DDNS (Dynamic DNS).
15. You may use MADCAP (Multicast Address Dynamic Client Allocation Protocol) for issuing multicast addresses.
16. You need to segment the network by configuring the subnet masks (which divide the total number of hosts available for one network into a smaller number available for more networks).

Plan and modify a network topology.

17. Always remember, dynamic addresses allocation is best for frequently changing network topology.
18. Major concerns for selecting a topology include performance, security and scalability.

Plan an Internet connectivity strategy.

19. You need to determine the number of WAN links to deploy.
20. Multiple WAN links allow fault tolerance and load balancing.
21. Demand dial type of WAN interface allows reduced cost.

Plan network traffic monitoring.

22. Bandwidth control may be implemented to allow for more effective internet use.
23. When you capture traffic make sure there isn't much performance impact. The point of traffic capture may become a bottleneck.

Troubleshoot connectivity to the Internet.

24. Portqry.exe is a command-line utility for troubleshooting TCP/IP connectivity issues. It reports the status of a TCP/IP port in one of the following three ways: Listening, Not Listening, and Filtered.
25. You may download and use DNSLint to diagnose common DNS name resolution issues.
26. You may use Tracert to verify the route used from the local host to the remote host.

Troubleshoot TCP/IP addressing.

27. Most problems are the results of incorrect subnet mask or default gateway settings.
28. You may use IPCONFIG to verify your machine's TCP/IP information.

Plan a host name resolution strategy.

29. DDNS is the way to go. It is the marriage of DHCP and DNS – now you no longer need to manually update the DNS records when the IP addresses were changed.
30. Unix computers and other non-MS OS may require static name entries.

Plan a NetBIOS name resolution strategy.

31. WINS (Windows Internet Naming Service) is responsible for resolving NetBIOS names to IP addresses.
32. Multiple WINS servers are desired for fault tolerance.
33. You may setup several WINS servers to replicate data to each other through pull or push type of partnership arrangement. Note that WINS replication does degrade network performance.
34. Use WINS only if the network is MS only and is consisting of many pre-W2003 clients.

Troubleshoot host name resolution.

35. You may use NSlookup to examines entries in the DNS database pertaining to a particular host or domain.
36. You may also manage DNS from the command line via the DNSCMD tool.
37. For load balancing purpose, consider mechanisms such as Round Robin which rotates type A resource records among servers.
38. For MS clients not supporting DNS, you may use hosts file instead to create static name resolution entries.

Planning, Implementing, and Maintaining Routing and Remote Access

Plan a routing strategy.

39. To configure Windows Server 2003 as a router for a LAN, you must enable RRAS and LAN routing.
40. Static routing involves manually configuring the routing table through the use of the route command in the command prompt.
41. Static routing is acceptable for small network only.
42. Dynamic routing involves the use of routing protocols such as Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).
43. RIP is the most popular routing protocol for small to mid size Windows based network. OSPF is more complicated to setup but have better scalability.
44. RIP has a hop count limit – be sure to check and ensure that the limit is not exceeded.
45. Older Netware computers rely on IPX/SPX rather than TCP/IP. RIP for IPX and SAP for IPX. are supported by RRAS. Newer Netware computers can natively support IP.

Plan security for remote access users.

46. You use remote access policy to define actions that can be undertaken for a user or group who connect remotely.
47. In a Windows Server 2003-based native-mode domain, you can use the following three remote access policies: Explicit allow, Explicit deny and Implicit deny.
48. You are encouraged to use IAS (Internet Authentication Service) to centrally enforce remote access policies.
49. Remote Access Dial-in Profiles allow you to define Dial-in Constraints, IP Address Assignment Policy, Multilink, Authentication and Encryption.
50. To setup and use RADIUS, you need to setup a third party RADIUS server.
51. For remote access via modem, call back security is still the most secure authentication method.

Implement secure access between private networks.

52. Secure connection between two private networks is implemented through VPN tunneling.
53. Windows Server 2003 supports IPSec tunneling for situations where both endpoints deploy static IP addresses (which is common for gateway-to-gateway

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

implementations).
54. The computers acting as VPN gateways must be equipped with fast processors and sufficient RAMs, or they will become the bottlenecks.
55. Connection to the Internet should use dedicated line. WAN adapters on both sides should be configured with the IP address and subnet mask assigned by an ISP and be configured as the default gateway of the ISP router.

Troubleshoot TCP/IP routing.
56. You may use the "route print" command to display the routing table.
57. You may use the "route change" or "route delete" command to manage the existing routing entries.
58. Manually configured routing entries (through the route add command) are not permanent unless you explicitly specify so.
59. If RIP and/or other routing protocols are to be used, make sure that the ports they use are not filtered nor blocked.

Planning, Implementing, and Maintaining Server Availability

Plan services for high availability.
60. These are two different types of cluster servers: the fail-over cluster and the load-balancing cluster.
61. The available types of fail-over clusters include the shared-everything cluster and the shared-nothing cluster.
62. In a shared-nothing cluster model, all servers or cluster nodes in the cluster can own the shared cluster resources but only one node may own and manage these resources at any one time.

Identify system bottlenecks.
63. You use the System Monitor tool to identify performance bottlenecks.

Implement a cluster server.
64. Clustering is not available with the Standard edition or Web edition of Windows Server 2003.
65. 2003 Enterprise edition can support a cluster of max four nodes, while the Datacenter edition can support max eight nodes.
66. MS supports a cluster configuration only if that configuration appears on the HCL.
67. Windows Clustering makes no distinction between the nodes during a failover and will not change the failover policy.
68. The best way to move a cluster server from one domain to another is to rebuild the cluster in the new domain.
69. You may control which nodes own which disk resources via the Cluster Administrator utility or Cluster.exe. You may view the disks' ownership with the Windows Server 2003 disk administration tools.

Manage Network Load Balancing.
70. Network Load Balancing allows you to distribute incoming TCP/IP traffic to multiple servers for processing.
71. With the Microsoft Cluster service (MSCS) you may bind multiple NetBIOS network names to one physical server to create a virtual server.

Plan a backup and recovery strategy.
72. Timing is important – backing up large chunk of data is time and resource consuming. It can be bandwidth exhaustive too.
73. 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.

Planning and Maintaining Network Security

Plan for and configure network protocol security.
74. On a production server, the following ports deserve your attention: FTP (data), FTP (session), Telnet, SMTP, HTTP, POP3, and IMAP. You need to decide whether to filter them or not.
75. TCP/IP packet filters can be used to prevent certain types of packets from hitting your network. You can have them configured through the Advanced button of the TCP/IP protocol properties.
76. Filters can be set for TCP or UDP or based on IP protocol numbers. You can configure them to accept or deny packets under specified conditions.
77. TCP/IP filtering works in kernel mode and is considered to be relatively reliable. However, the functionalities offered are for very basic protection only.
78. In fact, TCP/IP filtering cannot block ICMP messages regardless of the settings that are configured in the Permit Only IP Protocols column or whether you do not permit Internet Protocol 1.
79. For advanced security functions, consider the use of full blown package like the ISA Server.

Plan and configure security for data transmission.
80. The major encryption protocols supported by Windows 2003 with VPNs are MPPE + PPTP and IPSec + L2TP.
81. Pre-W2K computers support PPTP.
82. W2K and Windows 2003 computers can use L2TP.
83. L2TP uses UDP port 1701. PPTP uses TCP port 1723.
84. IPSec negotiates secure connection through the use of DES (Data Encryption Standard/ 56-bit) and 3DES (Triple DES) for securing packets between two hosts.
85. DES is no longer secure under today's standard.

Plan secure network administration methods.
86. Procedure-wise, always require authentication and secure (encrypted) connections.
87. You may secure Terminal Services communications by configuring the Terminal server to demand for varying degrees of encryption.
88. Apart from using Terminal Services you may also install and use the original-released version of Windows Server 2003 Administration Tools Pack (Adminpak.msi)

Plan security for wireless networks.
89. IEEE 802.1X allows authenticated network access to wired Ethernet networks and wireless 802.11 networks. It supports the following Extensible Authentication Protocol (EAP) authentication methods for wireless clients and servers: EAP-TLS, EAP, EAP-MS-CHAP v2 and PEAP.
90. The Wireless Network Policies feature allows you to apply Active Directory-based Group Policy settings to your Wi-Fi Protected Access (WPA) wireless network. You may add, edit, or remove wireless network policy settings, define preferred wireless networks, and define 802.1X authentication.

Troubleshoot security for data transmission.
91. You may use the IP Security Monitor console to show IPSec statistics and active security associations (SA).
92. You may also use Network Monitor to capture traffic for further analysis.
93. If the server requires encryption, make sure your clients are capable of supporting the requested encryption standard.

Planning, Implementing, and Maintaining Security Infrastructure.

Configure Active Directory directory service for certificate publication.
94. An Enterprise CA requires Active directory. A Stand-Alone CA, on the other hand, does not require Active Directory.
95. You may not be able to use automatic system provisioning or conventional certificate enrollment if a server has no relationship to any Active Directory domain or that there are firewalls running to block the required communication ports.
96. MS supports the use of third-party domain controller certificates with smart card logon only. It does not support the use of certificates from third-party CAs to support SMTP replication between domain controllers.

Plan a public key infrastructure (PKI) that uses Certificate Services.
97. A Certificate Authority (CA) is responsible for assigning the keys for encryption, decryption and authentication.
98. There are 2 types of CA's, which are Enterprise CA and Stand-Alone CA. Each CA type can have a root CA and multiple subordinate CA.
99. You should work with an outside established commercial CA if your site is to be made public for e-commerce purpose. In fact, MS maintains a list of trusted third-party commercial CAs to validate the identity and entitlement of an applicant.

Plan a framework for planning and implementing security.
100. A framework for security planning and implementation is a must for organization. Within such a framework there must be detailed procedures for network administrators to follow along their security planning and implementation activities. The framework should become the basis for all security related tasks within the organizational network environment.

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