



www.chinatag.com

CHINATAG

70-296

Planning, Implementing, and Maintaining
a Microsoft Windows Server 2003 Environment
for an MCSE Certified on Windows 2000

Q&A

DEMO Version

Copyright (c) 2003 Chinatag LLC. All rights reserved.

Important Note Please Read Carefully

For demonstration purpose only, this free version Chinatag study guide contains **10** full length questions selected from our full version products which have more than **200** questions each.

This Study guide has been carefully written and compiled by Chinatag certification experts. It is designed to help you learn the concepts behind the questions rather than be a strict memorization tool. Repeated readings will increase your comprehension.

For promotion purposes, all PDF files are **not** encrypted. Feel free to distribute copies among your friends and let them know Chinatag website. Our IT certification products start at only **\$7.99**.

Study Tips

This product will provide you questions and answers along with detailed explanations carefully compiled and written by our experts. Try to understand the concepts behind the questions instead of cramming the questions. Go through the entire document at least twice so that you make sure that you are not missing anything.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 180 days after the purchase. You should check the products page on the <http://www.chinatag.com> website for an update 3-4 days before the scheduled exam date.

Please tell us what you think of our products. We appreciate both positive and critical comments as your feedback helps us improve future versions. Feedback on specific questions should be send to feedback@chinatag.com.

Thanks for purchasing our products and look forward to supplying you with all your Certification training needs.

Good studying!

Technical and Support Team
Chinatag LLC.

70-296
Planning, Implementing, and Maintaining
a Microsoft Windows Server 2003 Environment
for an MCSE Certified on Windows 2000

Q&A

Part 1

1. You administer an Active Directory domain that contains the **SRV** organizational unit (OU). There are 10 Windows Server 2003 member server accounts in the **SRV** OU. The domain also contains Windows 2000 Professional and Windows XP Professional computers.

You have reviewed log files on the computers in the **SRV** OU, and you have determined that a malicious user is attempting to gain access to resources on some of the servers in the OU. You want to provide the maximum possible security for the computers in the **SRV** OU while maintaining compatibility with other computers in the domain. You create a Group Policy object (GPO) named **S_Sec** and link it to the **SRV** OU.

Which of the following predefined security templates should you import into the **S_Sec** GPO? (Select the best choice.)

- a. **Setup security.inf**
- b. **Compatws.inf**
- c. **Securedc.inf**
- d. **Hisecws.inf**

Answer: d

Section: 1. Planning and Implementing Server Roles and Server Security

Choice d is correct. You should import the **Hisecws.inf** template into the **S_Sec** GPO. Of the available choices the **Hisecws.inf** template will configure the member servers in the **SRV** OU with the maximum possible security. This security template will remove backward compatibility features; consequently, after the template is applied, member servers in the **SRV** OU will only be able to communicate with Windows 2000 and later computers.

The **Setup security.inf** template is the default security template for Windows Server 2003 computers. The **Setup security.inf** template is applied to Windows Server 2003 computers during installation. The **Securedc.inf** template is designed for domain controllers, not member servers.

The **Compatws.inf** template will reduce security on Windows Server 2003 and Windows 2000 computers; consequently, members of the **Users** group can run applications that are not certified for Windows 2000. You should use the **Compatws.inf** template if you need to configure computers to run legacy applications that will not otherwise run in Windows Server 2003 or Windows 2000 under the security context of a member of the **Users** group.

Reference:

2. You are the network administrator for your organization. You manage a member server named WEB1 that runs Windows Server 2003, Web Edition. WEB1 is located on a perimeter network segment and hosts your organization's public Web site.

You want to ensure that WEB1 is protected by the highest level of operating system security. This is especially important because WEB1 has been the victim of a recent Denial-of-Service (DoS) attack by a malicious Internet user.

Which of the following actions should you perform? (Select 2 choices.)

- a. Apply the **compatws.inf** security template to WEB1.
- b. Apply the **hisecws.inf** security template to WEB1.
- c. Enable IP packet filtering on WEB1.
- d. Enable DFS on WEB1.

Answer: bc

Section: 1. Planning and Implementing Server Roles and Server Security

Choices b and c are correct. In order to ensure that WEB1 is protected by the highest level of operating system security, you should apply the **hisecws.inf** security template, and you should enable IP packet filtering on WEB1. The **hisecws.inf** security template is a predefined security template that provides several high-security options to a Windows Server 2003 domain controller or member server, including disabling the use of the LAN Manager and unsigned Server Message Block (SMB) protocols and limiting the membership of the local **Administrators** group. The **hisecws.inf** security template provides a higher level of security than the **compatws.inf** predefined security template.

IP packet filtering allows an administrator to expressly permit or deny certain types of incoming or outgoing IP traffic on a Windows Server 2003 computer. Because WEB1 has recently been a victim of DoS attacks, it is especially important that you enable IP packet filters on incoming traffic on WEB1. Distributed File System (DFS) is a technology that allows a Windows Server 2003 computer to host a virtual directory tree of shared folder resources from multiple Windows computers. Enabling DFS on WEB1 would not improve the security configuration of the computer.

Reference:

WS3KOH, Contents, "Security," "Internet Protocol Security (IPSec)," "Concepts," "Internet Protocol Security Overview," "Security Information for IPSec."

WS3KOH, Contents, "Security," "Internet Protocol Security (IPSec)," "How To...," "Define IPSec Policies," "Define IPSec Rules," "Define IP Filter Lists," "Add, edit, or remove IPSec filters."

3. You are the network administrator for a corporation named Omnipresence, which is a business consulting firm with clients that are located worldwide. The Omnipresence network consists of an internal network segment and a demilitarized zone (DMZ) segment, both of which are connected by a hardware

firewall. A third interface on the firewall is connected to the Internet.

The private internal Omnipresence network is organized as a single Active Directory domain named `omnipresence.com`. The internal network consists of four Windows Server 2003 domain controllers, eight Windows Server 2003 member servers, and 200 Windows XP Professional client computers.

You have recently installed three Windows Server 2003-based FTP servers on the DMZ segment. These FTP servers will allow your company's clients to upload their data to your network. None of the three FTP servers belongs to the `omnipresence.com` domain. You want to deploy customized security settings to the three FTP servers by using the least amount of administrative effort. You create a custom security template named **`ftp-security.inf`**.

Which of the following should you do next? (Select the best choice.)

- a. Apply the **`ftp-security.inf`** security template to each FTP server by using the Security Configuration and Analysis MMC snap-in.
- b. Apply the **`ftp-security.inf`** security template to each FTP server by using the **`Secedit.exe /refreshpolicy`** command.
- c. Create an OU named **`FTP-SRV`**. Place the three FTP server computer accounts into the **`FTP-SRV`** OU. Import the **`ftp-security.inf`** security template into the OU by using Group Policy.
- d. Use the Local Security Policy MMC snap-in to manually configure the settings that are stored in the **`ftp-security.inf`** security template.

Answer: a

Section: 1. Planning and Implementing Server Roles and Server Security

Choice a is correct. To deploy the **`ftp-security.inf`** customized security template to your three Windows Server 2003 File Transfer Protocol (FTP) servers, you should apply the **`ftp-security.inf`** security template to those servers by using the Security Configuration and Analysis Microsoft Management Console (MMC) snap-in. Because the three FTP servers in question do not belong to the `omnipresence.com` domain, Active Directory and domain-based Group Policy cannot be used to apply the settings contained in the **`ftp-security.inf`** template to the FTP server computers. Although the **`Secedit.exe /import`** command could be used to apply the **`ftp-security.inf`** template to the FTP server computers, the command **`Secedit.exe /refreshpolicy`** can be used only to refresh security settings on the local computer. Theoretically, you could use the Local Security Policy MMC snap-in to copy the security settings stored in **`ftp-security.inf`** to each FTP server computer; however, by doing so, you would fail to meet the scenario's requirement for using the least administrative effort.

Reference:

WS3KOH, Contents, "Security," "Security Configuration Manager," "Concepts," "Security Configuration Manager Overview," "Security Configuration and Analysis overview."

4. You manage an Active Directory domain. All of the servers in your network run Windows Server 2003, and all client workstations run Windows XP Professional. You want to apply a security template to your domain controllers that will enhance security settings while minimally impacting application compatibility.

Which of the following security templates should you apply to your domain controllers? (Select the best

choice.)

- a. **Securedc.inf**
- b. **DC security.inf**
- c. **Setup security.inf**
- d. **Hisecdc.inf**

Answer: a

Section: 1. Planning and Implementing Server Roles and Server Security

Choice a is correct. A *security template* is a collection of security settings that store information related to account policies, local policies, event log settings, restricted groups, system services, the Registry and the file system. Security templates can be applied to individual computers by using Local Security Policy, the **Secedit.exe** tool or the Security Configuration and Analysis Microsoft Management Console (MMC) snap-in. Security templates can be applied to groups of computers by configuring a Group Policy object (GPO). In this scenario, the **Securedc.inf** Windows Server 2003 security template should be applied to a domain controller to enhance security settings while minimally impacting application compatibility.

The **DC security.inf** security template can be used to reinstate factory default security settings for a newly promoted Windows Server 2003 domain controller. The **Setup security.inf** security template can be used to reinstate factory default security settings for any Windows Server 2003, Windows 2000 or Windows XP Professional computer. The **Hisecdc.inf** security template contains high-security settings for Windows Server 2003 domain controllers; however, these security settings may impact application compatibility on the domain controller.

Reference:

WNITK, Chapter 10, Deploying Security Configurations, p. 10-14.

5. You want to use the Security Configuration and Analysis (SCA) Microsoft Management Console (MMC) snap-in to compare the security settings of a Windows Server 2003 domain controller named SERVER02 to the settings contained in the **Hisecdc.inf** security template. You have opened the SCA snap-in, created a database file and loaded **Hisecdc.inf**.

Which of the following actions should you perform next? (Select the best choice.)

- a. Load the Security Templates MMC snap-in.
- b. Right-click **Security Configuration and Analysis** in the SCA MMC window, and select **Configure Computer Now** from the shortcut menu.
- c. Right-click **Security Configuration and Analysis** in the SCA MMC window, and select **Import Template** from the shortcut menu.
- d. Right-click **Security Configuration and Analysis** in the SCA MMC window, and select **Analyze Computer Now** from the shortcut menu.

Answer: d

Section: 1. Planning and Implementing Server Roles and Server Security

Choice d is correct. In order to compare the currently active security settings on SERVER02 with the

security settings that are stored in a security template, you should first create a database file and load the appropriate template. Then, right-click **Security Configuration and Analysis** in the SCA MMC window and select **Analyze Computer Now** from the shortcut menu. The **Analyze Computer Now** command performs a comparison between the local computer's settings and the settings stored in the database file and reports the findings both in the **database.log** log file and directly in the SCA MMC console interface. An administrator can then interpret the results by examining any disparities between the two settings.

The Security Templates MMC snap-in can be used to view and edit the security template files that are shipped with Windows Server 2003. You cannot use the Security Templates console to analyze the security configuration of a computer. Right-clicking **Security Configuration and Analysis** in the SCA MMC window and selecting **Configure Computer Now** from the shortcut menu will not perform a security analysis; instead, all of the settings that are stored in the database file will be applied automatically to the local computer. Right-clicking **Security Configuration and Analysis** in the SCA MMC window and selecting **Import Template** from the shortcut menu will allow you to import the settings from another security template file into the database.

Reference:

WS3KOH, Contents, "Security," "Security Configuration Manager," "Concepts," "Security Configuration Manager overview," "Security Configuration and Analysis overview."

6. You are in charge of administering security on a Windows Server 2003 domain controller named DC01. You want to configure DC01 to require a password in order to successfully start Windows on DC01. You also want to configure the server to refuse LAN Manager responses from other client or server computers.

Which of the following actions should you perform? (Select 2 choices.)

- a. Apply the **DC Security.inf** security template to DC01 by using the Security Configuration and Analysis MMC snap-in.
- b. Apply the **Securedc.inf** security template to DC01 by using the **Secedit.exe** utility.
- c. Run the **Syskey.exe** utility on DC01, and specify the **Password Startup** option.
- d. Run the **Syskey.exe** utility on DC01, and specify the **Store Startup Key on Floppy Disk** option.
- e. Run the **Syskey.exe** utility on DC01, and specify the **Store Startup Key Locally** option.

Answer: bc

Section: 1. Planning and Implementing Server Roles and Server Security

Choices b and c are correct. In order to configure DC01 to require a password during each system startup and to cause LAN Manager responses from other computers to be refused by DC01, you should apply the **Securedc.inf** security template to DC01 and run the **Syskey.exe** utility with the **Password Startup** option. On a Windows Server 2003 member server, either the Security Configuration and Analysis Microsoft Management Console (MMC) snap-in or the **Secedit.exe** utility can be used to apply a security template to a computer. In this scenario, only the **Securedc.inf** default security template enforces the use of the NTLM v2 authentication protocol with downlevel clients by restricting LAN Manager responses from other computers. The **DC Security.inf** default security template is used to restore factory default security settings on a Windows Server 2003 computer.

The **Syskey.exe** utility can be run on a Windows Server 2003 or a Windows 2000 computer to encrypt the

Security Accounts Manager (SAM) user account database and to configure a startup password and startup key options. Specifically, the **Password Startup** option allows an administrator to specify a password that must be entered to successfully start Windows Server 2003. The **Store Startup Key on Floppy Disk** option stores a system-generated password on a floppy disk; the floppy disk must be inserted into the target computer in order to start that computer. The **Store Startup Key Locally** option stores the user accounts database encryption key on the local computer; this is the default option in **Syskey.exe**.

Reference:

WS3KOH, Contents, "Security," "Authentication," "Passwords," "Concepts," "The system key utility."

WS3KOH, Contents, "Security," "Security Configuration Manager," "Concepts," "Using Security Configuration Manager," "Predefined security templates."

7. You have been contracted to design an Active Directory domain for a client. The client's current network is configured as a workgroup. The network consists of a Web server farm that contains two servers running Windows Server 2003, Web Edition; one server running Windows Server 2003, Standard Edition; and one server running Windows Server 2003, Enterprise Edition.

You want to promote at least two of these computers to domain controllers in order to provide fault tolerance for directory services.

Which computers should you promote? (Select the best choice.)

- a. both of the Web Edition computers
- b. one Web Edition computer and the Standard Edition computer
- c. one Web Edition computer and the Enterprise Edition computer
- d. the Standard Edition computer and the Enterprise Edition computer

Answer: d

Section: 1. Planning and Implementing Server Roles and Server Security

Choice d is correct. You should promote the Standard Edition computer and the Enterprise Edition computer to domain controllers. Although a Windows Server 2003, Web Edition computer can be configured as a member server in an Active Directory domain, a Web Edition computer cannot be configured as a domain controller. Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; and Windows Server 2003, Datacenter Edition can all be configured as domain controllers. Only Enterprise Edition and Datacenter Edition computers can be run on 64-bit Intel Itanium processor platforms. All four editions of Windows Server 2003 support Network Load Balancing (NLB).

Reference:

WNITK, Chapter 8, Choosing Server Operating Systems, p. 8-10.

8. Your company is using a Windows Server 2003-based network. All computers on the network are configured to use the DNS server on the internal network for name resolution. Your company's contract with its current ISP expires, and you sign an agreement with another ISP. Users then report that they

cannot access any Internet sites by using the sites'URLs. You check with the new ISP and learn that their DNS server is functioning properly. You must enable computers on your corporate LAN to resolve the URLs of Internet hosts.

Which of the following should you do? (Select the best choice.)

- a. Change the address of the forwarder that your internal DNS server is configured to use.
- b. Specify the internal DNS server as the preferred DNS server on all computers on your corporate LAN.
- c. Configure your DNS server not to use recursion.
- d. Configure your DNS server to allow zone transfers to the DNS server that is maintained by the new ISP.

Answer: a

Section: 2. Planning, Implementing, and Maintaining a Network Infrastructure

Choice a is correct. Based on the scenario and available choices, it appears that your company's internal DNS server is configured not to use recursion and to use the original ISP's DNS server as a forwarder. When a computer on your LAN submits a name resolution request to the internal DNS server and the server cannot resolve the name from the zones that it hosts, it forwards the request to the ISP's DNS server and does not attempt to resolve that name itself if the ISP's server is unavailable or cannot resolve it. When you switched to another ISP, the communications link between your corporate LAN and the original ISP's network must have been reconfigured to connect to the new ISP's network. As a result, the DNS server on the original ISP's network must have become inaccessible. To enable users on your corporate network to resolve names of hosts on the Internet, you should change the address of the forwarder on your internal DNS server to point to the DNS server or servers on the new ISP's network.

Multiple DNS servers can be specified on a client computer: one preferred server and several alternate servers on each network interface. If the original ISP's DNS server were specified as the preferred server and the internal DNS server were specified as an alternate, then you would not have to specify the internal DNS server as the preferred one because the clients would automatically direct their name resolution queries to the alternate server once the preferred server became unavailable. If such a configuration were indeed used, then you might want to change the address of the preferred DNS server to the address of the new ISP's DNS server. Zone transfers are used to synchronize the information between multiple instances of the same zone hosted on different DNS servers. It is highly unlikely that you would want your ISP to host the zone for your internal corporate LAN; this would be unreasonable and would present a substantial security risk. Even if the new ISP's DNS server did host the zone for your internal LAN, configuring zone transfers between your internal DNS server and the ISP's DNS server would still be irrelevant to the ability of computers on your corporate LAN to resolve names of hosts on the Internet.

Reference:

TechNet, Contents, "Products & Technologies," "Windows Server 2003," "Product Documentation," "Windows Server 2003 Enterprise Edition," "Network Services," "Managing Core Network Services," "DNS," "Concepts," "Understanding DNS," "Understanding forwarders."

9. You administer your organization's single Active Directory domain. A Windows Server 2003 member server named DNS1 provides DNS host name resolution for all users in the domain.

You find that name resolution queries are taking an inordinate amount of time to resolve. You want to troubleshoot the problem by examining individual DNS queries on DNS1.

Which of the following should you do? (Select the best choice.)

- a. Audit DNS queries by using Local Security Policy on DNS1.
- b. Load the **Total Query Received/sec** counter in System Monitor on DNS1.
- c. Perform automatic testing by using the **Monitoring** tab of the **Server Properties** dialog box on DNS1.
- d. Enable DNS debug logging on DNS1.

Answer: d

Section: 2. Planning, Implementing, and Maintaining a Network Infrastructure

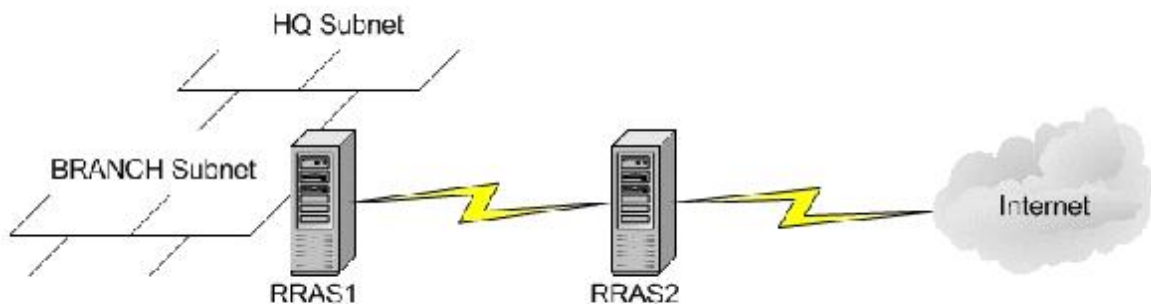
Choice d is correct. You should enable DNS debug logging on DNS1. DNS debug logging will enable you to view detailed information about every query that the Windows Server 2003 DNS server handles. Both incoming and outgoing DNS query packets can be logged; all data is logged to a file that can be analyzed after the logging session is completed. To enable DNS debug logging on a Windows Server 2003 computer, open the DNS console, right-click the DNS server object and select **Properties** from the shortcut menu. In the **Server Properties** dialog box, navigate to the **Debug Logging** tab. On the **Debug Logging** tab, enable **Log packets for debugging** and select the appropriate logging options.

DNS cannot be explicitly audited by using Local Security Policy in Windows Server 2003. Loading the **Total Query Received/sec** counter in System Monitor on DNS1 will display the total number of DNS queries that are received by the DNS server; this counter will not enable you to view the contents of each query packet. The **Monitoring** tab of the **Server Properties** dialog box for a Windows Server 2003 DNS server allows you to perform simple and recursive queries on a DNS server for diagnostic purposes; however, this action will not enable you to view detailed information about the queries that are processed by the DNS server.

Reference:

WS3KOH, Contents, "Network Services," "Managing Core Network Services," "DNS," "Concepts," "Administering DNS," "Monitoring and Optimizing Servers," "Using server debug logging options."

10. Consider the following network diagram, which depicts your organization's network topology:



Users in the HQ subnet are able to access the Internet connection that is configured on the Windows Server 2003 RRAS server named RRAS2. However, users in the BRANCH subnet are not able to access the Internet connection. You want your solution to minimize the amount of inter-router network traffic.

Which of the following actions should you take in order to enable users in the BRANCH subnet to access the Internet? (Select the best choice.)

- a. Configure a default route on RRAS1 that points to RRAS2.
- b. Configure a default route on RRAS2 that points to RRAS1.
- c. Configure RIPv2 on RRAS1 and RRAS2.
- d. Configure OSPF on RRAS1 and RRAS2.

Answer: a

Section: 2. Planning, Implementing, and Maintaining a Network Infrastructure

Choice a is correct. In order to enable users in the BRANCH subnet to access the Internet connection that is configured on the Windows Server 2003 Routing and Remote Access Service (RRAS) router that is located on the HQ subnet, you should configure a default route on RRAS1 that points to RRAS2. A *default route* is a routing table entry that is used to direct frames for which a next hop is not explicitly listed in the routing table. In this scenario, any traffic that is destined for the Internet or any other remote network should be forwarded to RRAS2. Therefore, configuring a default route on RRAS1 that points to RRAS2 will allow you to accomplish your goal.

An alternative to using static routes is using a routing protocol such as Routing Information Protocol version 2 (RIPv2) or Open Shortest Path First (OSPF). Routing protocols simplify a router administration by allowing routers to store dynamically changing routing tables. However, routing protocols are unnecessary in this scenario because the internetwork is very small, involving only two subnetworks. In addition, the scenario calls for keeping inter-router network traffic to a minimum. All routing protocols involve some degree of route information sharing that occurs on a periodic basis.

Reference:

WS3KOH, Contents, "Network Services," "Managing Remote Connections," "Routing and Remote Access," "Routing," "Concepts," "Using Routing," "Deploying Routing," "Setting up a Static Routed IP Internetwork," "Static routing design considerations."

11. You manage an Active Directory forest that consists of two domain trees that span six geographical sites. You want to maximize the performance of your internal DNS namespace and minimize the amount of unnecessary network traffic among domains.

Which of the following actions should you take to accomplish your goals? (Select the best choice.)

- a. Implement conditional forwarding on all internal DNS servers.
- b. Configure all internal DNS servers with stub zones.
- c. Disable the use of root hints on all internal DNS servers.
- d. Ensure that all internal DNS zones are Active Directory-integrated.