


Microsoft

Windows Server 2003 Planning Network Infrastructure

70-293 70-293 70-293 70-293 70-293 70-293 70-293 70-293

STUDY
PRINTABLES

PRINTABLE PRACTICE QUESTIONS
QUESTIONS, ANSWERS, AND
DETAILED EXPLANATIONS IN AN
EASY-TO-USE PRINTABLE FORMAT

 LearnSmart™

Chapter 1

Planning and Implementing Server Roles and Server Security

1. You are one of the Web hosting administrators for your company's e-commerce environment. You are trying to configure a Web server called WEBSRV01 running Windows Server 2003 Standard Edition. WEBSRV01 currently hosts three different Web sites, two of which only offer static content and one that uses Active Server Pages. How can you enable Web services for your server so that it will allow you to offer up the different types of content as required on each of the Web sites hosted on the server, using the least amount of administrative effort and maintaining a high level of security on the base OS of the server? Select the best answer.
 - A. Use the Configure Your Server Wizard to configure the server in the Web server role by using the default settings provided.
 - B. Use the Configure Your Server Wizard to configure the server in the Application Server role by using the default settings provided.
 - C. Add the IIS service via the Control Panel and Add/Remove Windows Components. Then, install the service and dynamic content using the default settings provided when prompted.
 - D. Add the IIS service via the Control Panel and Add/Remove Windows Components. Then, install the service and dynamic content by manually configuring all of the required settings.
 - E. Use the Configure Your Server Wizard to configure the server in the Application Server role, and manually choose the options for dynamic content.

[Find the Answer](#) p. 253



2. You are the systems administrator for preplologic.com. Domain controllers in the domain include Windows 2003 Server systems that were both newly installed and others that were upgraded to server 2003 from NT4 and 2000. All of the domain controllers have security settings applied at the domain controllers OU, as well as at the domain container level. DC4.preplologic.com, DC5.preplologic.com, and DC9.preplologic.com are three domain controllers that have been upgraded from Windows NT4 BDCs. You need to ensure that all of the Windows Server 2003 DCs are running using at least the default security settings for a Windows Server 2003 system. Specifically with regard to the default NTFS permission settings on the systems, you need to ensure as best as possible that all of the proper NTFS settings are enabled for the %Windir% and "Program Files" folders. You need to verify that these DCs are using the default security settings, and you need to complete this action using the least amount of administrative effort. You must also ensure that your actions do not affect other member servers unnecessarily. What is the best way to complete your task from the following choices? Select the best answer.
- A. Configure a GPO to apply the Setup security.inf template at the domain controllers OU.
 - B. Configure a GPO to apply the Basicsv.inf template at the domain object in the Active Directory.
 - C. Configure a GPO to apply the Setup security.inf template at the domain object in the Active Directory.
 - D. Configure a GPO to apply the Defltsv.inf template at the domain controllers OU.
 - E. Configure a GPO to apply the Defltsv.inf template at the domain object in the Active Directory.
 - F. Configure a GPO to apply the Setup security.inf template as a local policy on the three servers.

[Find the Answer](#) p. 253



3. You are a systems administrator for your company. You have been tasked with comparing your standard desktop build currently in use on the desktop systems in your enterprise against the default configuration security settings that are applied during a new installation of the Windows XP Professional operating system. What is the easiest way to accomplish this task by using a script? Select the best answer.
- A. Use the Security Configuration and Analysis tool against all of the systems.
 - B. Use MBSA against all of the systems.
 - C. Use SIGVERIF.exe against all of the systems.
 - D. Use SFC.exe against all of the systems.
 - E. Use Secedit against all of the systems.

[Find the Answer](#) p. 253

4. You are the Web hosting administrator for your company. You have been asked to compare the new security settings configured locally on two Web servers in the DMZ against the default configuration security settings that were originally applied during the default installation, as well as comparing those settings to the settings that are found in the hisecsv.inf template. Which tools can be used to successfully accomplish this task? Select all that apply.
- A. Use the Security Configuration and Analysis tool.
 - B. Use the MBSA utility.
 - C. Use the SIGVERIF.exe tool.
 - D. Use the SFC.exe tool.
 - E. Use the Secedit command-line tool.

[Find the Answer](#) p. 253



5. You are a domain administrator. You have been asked to review the domain controllers Baseline Policy (domain controller.inf) to verify some of the settings that are enabled when the template is in use. Under this template, which of the following default users/groups can access the systems from the network if none of the defaults have been changed? Each answer presents part of the solution. Select the two best answers.

- A. Administrators
- B. Domain Users
- C. Everyone
- D. Authenticated Users
- E. Anonymous
- F. Windows Authorization Access Group

[Find the Answer](#) p. 253

Answers: Chapter 1

1. E	Review Question p. 2	Detailed Explanation p. 267
2. A	Review Question p. 3	Detailed Explanation p. 267
3. E	Review Question p. 4	Detailed Explanation p. 268
4. A, E	Review Question p. 4	Detailed Explanation p. 269
5. A, D	Review Question p. 5	Detailed Explanation p. 269
6. D, E, F	Review Question p. 6	Detailed Explanation p. 270
7. A	Review Question p. 7	Detailed Explanation p. 271
8. C, D, E	Review Question p. 8	Detailed Explanation p. 271
9. A	Review Question p. 9	Detailed Explanation p. 272
10. C, E	Review Question p. 10	Detailed Explanation p. 272
11. A	Review Question p. 11	Detailed Explanation p. 273
12. C, E	Review Question p. 12	Detailed Explanation p. 275
13. C, E	Review Question p. 12	Detailed Explanation p. 275
14. B, C	Review Question p. 13	Detailed Explanation p. 276
15. B	Review Question p. 15	Detailed Explanation p. 277
16. C	Review Question p. 17	Detailed Explanation p. 277
17. A, B	Review Question p. 17	Detailed Explanation p. 278
18. B	Review Question p. 18	Detailed Explanation p. 279
19. A	Review Question p. 19	Detailed Explanation p. 279
20. A, C, E	Review Question p. 20	Detailed Explanation p. 280
21. E	Review Question p. 21	Detailed Explanation p. 281
22. A	Review Question p. 22	Detailed Explanation p. 282
23. F	Review Question p. 24	Detailed Explanation p. 283

Explanations: Chapter 1

1. [Review Question](#) p. 2

Answers: E

Explanation A. IIS6 is not installed by default. When you initially enable it by using the Configure Your Server Wizard, the service is locked down by default, which means that it will offer up only static Web content.

Explanation B. Using the default settings will not enable dynamic content. IIS6 is not installed by default. When you initially enable it by using the Configure Your Server Wizard, the service is locked down by default, which means that it will offer up only static Web content.

Explanation C. Using the default settings will not enable dynamic content. IIS6 is not installed by default. When you initially enable it by using the Configure Your Server Wizard, the service is locked down by default, which means that it will offer up only static Web content.

Explanation D. This is not the least amount of administrative effort. IIS6 is not installed by default. When you initially enable it by using the Configure Your Server Wizard, the service is locked down by default, which means that it will offer up only static Web content.

Explanation E. This is the least amount of administrative effort. IIS6 is not installed by default. When you initially enable it by using the Configure Your Server Wizard, the service is locked down by default, which means that it will offer up only static Web content.

PrepLogic Question: [1123-100](#)

2. [Review Question](#) p. 3

Answers: A

Explanation A. The Setup security.inf template is the initial template created that is applied to any Windows Server 2003 system during installation, and it can also be used at a later time via the Security Configuration and Analysis tool to re-apply default security settings to Windows Server 2003 and Windows 2000 systems, as well as the default NTFS settings.

Explanation B. Basicsv.inf provides a basic level of security for file and print servers on the Windows 2000 platform, but it should not be used on Windows Server 2003 systems. Also, applying it at the domain level would affect all of the workstations and



servers in the domain.

Explanation C. Applying the Setup security.inf at the domain level would affect all of the servers and workstations in the domain.

Explanation D. The Defltsv.inf template is used on Windows 2000 Server systems that are not configured as domain controllers to restore the default NTFS file system permissions in Windows 2000.

Explanation E. The Defltsv.inf template is used on Windows 2000 Server systems that are not configured as domain controllers to restore the default NTFS file system permissions in Windows 2000.

Explanation F. This is not the least amount of administrative effort. You would have to configure three systems individually. Also, settings from local policies will most likely be overwritten by domain level and OU level GPOs.

PrepLogic Question: [1123-101](#)

3. [Review Question](#) p. 4

Answers: E

Explanation A. Although the Security Configuration and Analysis is a tool for analyzing and configuring local system security settings, it is a GUI-based tool. It would not be the easiest way to accomplish the required task because it would require you to run the tool on each system, one at a time.

Explanation B. MBSA is a GUI tool (it can also be run from the command line) that allows an administrator to perform local or remote scans of Windows systems in an effort to scan for missing security updates and Service Packs for Windows, IE, IIS, SQL, Exchange, and Windows Media Player. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.

Explanation C. The File Signature Verification tool, SIGVERIF.exe, can be used to identify unsigned drivers on your system. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.

Explanation D. The System File Checker tool (SFC.exe) allows an administrator to scan all of the protected files on a computer to verify if they are the correct versions. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.



Explanation E. Secedit can be used to analyze and configure the security settings of computers by comparing your current configuration to at least one template from the command line. Using this tool as part of a script allows you to run it against all of the systems with less effort than most GUI tools.

PrepLogic Question: [1123-102](#)

4. [Review Question](#) p. 4

Answers: A, E

Explanation A. The Security Configuration and Analysis is a tool for analyzing and configuring local system security settings. It can be used successfully for this task.

Explanation B. MBSA is a GUI tool (it can also be run from the command line) that allows an administrator to perform local or remote scans of Windows systems in an effort to scan for missing security updates and Service Packs for Windows, IE, IIS, SQL, Exchange, and Windows Media Player. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.

Explanation C. The File Signature Verification tool, SIGVERIF.exe, can be used to identify unsigned drivers on your system. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.

Explanation D. The System File Checker tool (SFC.exe) allows an administrator to scan all of the protected files on a computer to verify if they are the correct versions. It would not allow you to compare your standard desktop build's security settings against the default configuration security settings that are applied.

Explanation E. Secedit can be used to analyze and configure the security settings of computers by comparing your current configuration to at least one template from the command line.

PrepLogic Question: [1123-103](#)

5. [Review Question](#) p. 5

Answers: A, D

Explanation A. This answer is correct. By default, Administrators, Authenticated Users, and Enterprise Domain Controllers have the "Access this computer from the network" right. This allows these users and groups to connect to the computer over the network, and is specifically required by many network protocols.



Explanation B. Domain Users do not have this right by default.

Explanation C. The Everyone group does not have this right by default.

Explanation D. By default, Administrators, Authenticated Users, and Enterprise Domain Controllers have the "Access this computer from the network" right. This allows these users and groups to connect to the computer over the network, and is specifically required by many network protocols.

Explanation E. Anonymous does not have this right by default.

Explanation F. The Windows Authorization Access Group does not have this right by default.

PrepLogic Question: [1123-104](#)

6. [Review Question](#) p. 6

Answers: D, E, F

Explanation A. Because this is part of a security account policy and it is applied at the OU level and not at the domain level, it will not be correctly applied to the systems. Security account policies need to be applied at the domain level to be effective against domain logins.

Explanation B. Because this is part of a security account policy and it is applied at the OU level and not at the domain level, it will not be correctly applied to the systems. Security account policies need to be applied at the domain level to be effective against domain logins.

Explanation C. Because this is part of a security account policy and it is applied at the OU level and not at the domain level, it will not be correctly applied to the systems. Security account policies need to be applied at the domain level to be effective against domain logins.

Explanation D. This is correct. This setting will be configured on all of the systems whose computer accounts are homed within the SETUP OU.

Explanation E. This is correct. This setting will be configured on all of the systems whose computer accounts are homed within the SETUP OU.

Explanation F. This is correct. This setting will be configured on all of the systems whose computer accounts are homed within the SETUP OU.

PrepLogic Question: [1123-105](#)

