

70-291 Managing Windows Server 2003 Network Infrastructure

1

You are the network administrator for your company. The network consists of a single Active Directory domain. The domain contains 25 Windows Server 2003 computers and 6,000 Windows XP Professional computers.

The written company security policy states that network traffic to Web servers must be audited on a regular basis. A server named Server1 is configured as a Web server on the company's intranet. You install Network Monitor Tools from a Windows Server 2003 product CD-ROM on Server1.

You run Network Monitor on Server1 for three hours. When you stop the network capture, you see that Network Monitor captured over 40,000 frames. As you look at the captured frames, you notice that an extremely large number of TCP connection requests have all come from the 131.107.0.1 IP address.

In Network Monitor, you need to view only the frames for network traffic that are captured between Server1 and the 131.107.0.1 IP address.

What should you do?

- A. Create an Address Capture filter for all network traffic between Server1 and the 131.107.0.1 IP address.
- B. Create a Find Frame Expression filter for network traffic captured between Server1 and the 131.107.0.1 IP address.
- C. Create an Address Display filter for all network traffic captured between Server1 and the 131.107.0.1 IP address.
- D. Create a Pattern Match capture trigger for the 131.107.0.1 IP address.

2

You are the network administrator for your company.

On a Windows Server 2003 computer named Server3, you use the Backup program to automatically back up eight servers. You use a scheduled task named AutoBack. The task runs in the security context of a domain account named NightBackup.

The Default Domain Policy Group Policy object (GPO) is configured with the following account policies settings:

- Minimum password length: 8 characters
- Password expiration: 30 days
- Enforce password history: 12 passwords remembered
- Account lockout threshold: 3 invalid logon attempts
- Account lockout duration: 30 minutes

The Backup program runs successfully for four weeks. After four weeks, you notice that nightly backups no longer occur. A successful backup occurs when you log on to Server3 with your own user account and perform a local backup. Your user account is a member of the Domain Admins group.

You want the AutoBack scheduled task to perform unattended backups every night at 11:00 P.M.

Which two actions should you perform in order to resume the nightly backups by using the AutoBack scheduled task? (Each correct answer presents part of the solution. Choose two.)

- A. Unlock the NightBackup user account.
- B. Enable the NightBackup user account.
- C. On the properties sheet for the AutoBack.job scheduled task, reset the password.
- D. Reset the password for the NightBackup user account.
- E. Configure the local security policy on Server3 to grant the service account the **Logon locally** right.
- F. Configure the local security policy on Server3 to grant the service account the **Logon as a service** right.

3

You are the administrator of a Windows Server 2003 computer named Server1. Server1 is an FTP server located in the company's internal network.

Administrators report an increased amount of FTP traffic to Server1.

You need to configure Server1 to achieve the following goals:

- Identify the media access control (MAC) address of any computer that is performing FTP transfers from Server1.
- Find out the exact FTP commands that were executed.
- Ensure that you do not disrupt the operation of Server1.

What should you do?

- A. Configure a performance alert to write an event to the application event log whenever the number of established FTP connections exceeds 1.
- B. Use a Network Monitor filter to capture IP traffic from any computer to Server1.
- C. Run the **finger** command on Server1 to identify the source of the FTP requests.
- D. Run the **arp** command on Server1 to identify the source of the FTP requests.

4

You are the administrator of an Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. The network is configured as shown in the exhibit. (Click the **Exhibit** button.)

DC1 is configured as a DNS server for the domain named contoso.com. DC1 is configured to use ISP-DNS as a forwarder.

A computer named NAT1 is a Network Address Translation (NAT) server. NAT1 provides Internet access for the entire company. You recently created a subnet named Subnet 10.

You are configuring a DHCP server to support Subnet 10. You need to configure the DHCP server options for Subnet 10 to ensure that all users can access the Internet and internal resources.

What should you do?

To answer, drag the appropriate IP address or addresses to the correct location or locations in the work area.

IP Addresses	Work Area
131.107.2.50	<input type="text" value="IP address"/> 003 Router
131.107.3.254	<input type="text" value="IP address"/> 006 DNS
192.168.1.1	
192.168.2.5	
192.168.10.1	

The diagram illustrates a network topology. On the left, the Internet is connected to NAT1 (192.168.1.1). NAT1 is connected to a Router (192.168.2.1). The Router is connected to Subnet 10 (192.168.10.0/24) and Subnet 2 (192.168.2.0/24). Subnet 2 contains two Domain Controllers, DC1 (192.168.2.5) and DC2 (192.168.2.6). Client computers are connected to Subnet 10. An ISP-DNS server (131.107.3.254) is also connected to the Internet.

5

You are the network administrator for Margie's Travel. The network consists of a single Active Directory forest that contains two domains named europe.margiestravel.com and namerica.margiestravel.com.

The network contains Windows Server 2003 computers and Windows XP Professional computers. All client computers and 25 servers are dynamically assigned IP addresses by DHCP.

All company computers are registered in either the europe.margiestravel.com DNS zone or the namerica.margiestravel.com DNS zone. All DNS servers contain copies of all zones. The written company network management policy states that computers cannot have duplicate host names. Client computers always connect to other computers by specifying only the name of the target computer. A fully qualified domain name (FQDN) is not required.

You need to configure the client computers to ensure that all computer names can be resolved by using DNS without the domain name being specified. The configuration of client computers must be automated so that they do not need to be manually reconfigured if an additional domain is added to the forest.

What should you do?

- A. Configure the **Append these DNS suffixes** option in the DNS client configuration of each client computer.
- B. Configure the **015 DNS Domain Name** option on all DHCP scopes.
- C. Configure the Default Domain Policy Group Policy object (GPO) in each domain. Enable the **DNS Suffix Search List** policy setting in the GPO.
- D. Configure the Default Domain Policy Group Policy object (GPO) in each domain. Enable the **Primary DNS Suffix** policy setting in the GPO.

6

You are the administrator of an Active Directory domain. The domain contains a Windows Server 2003 computer named Server1. Server1 functions as a domain controller and a DNS server. The domain also contains a Windows XP Professional client computer named Client1.

You need to establish a detailed record of all of the communications that occur when a typical member of the Domain Users group named User1 logs on to the Active Directory domain from Client1. You might need to use this information as a troubleshooting tool if communications between Client1 and Server1 are disrupted or degraded. You want to use Network Monitor to obtain this baseline information.

What should you do?

To answer, move the appropriate actions from the list of actions to the answer area, and arrange them in the correct order.

List of Actions	Answer Area
Start a capture.	
Enable TCP/IP filtering on Client1.	
Start Network Monitor on Server1 and select Local Area Network .	
Configure a capture filter to capture all traffic between Server1 and Client1.	
Configure a display filter to display all traffic between Server1 and Client1.	
Configure a display filter to display all traffic between Server1 and *ANY.	
Log on to Client1 as User1 and allow the logon process to complete.	
Log on to Server1 as User1 and allow the logon process to complete.	
Stop the capture and save it in a secure, reliable location.	

7

You are the network administrator for your company. All servers run Windows Server 2003.

The company is setting up a sales booth at a large trade show. Twelve company sales representatives will be working in the booth. The sales representatives each have a portable computer that runs Windows XP Professional.

You configure a server named Server2 with a LAN connection and a dial-up connection to the Internet. All of the sales representatives' computers are also connected to the LAN.

The 12 sales representatives report that they cannot connect to the Internet. You view the IP configuration on one of the portable computers as shown in the exhibit. (Click the **Exhibit** button.)

You need to provide the 12 sales representatives' portable computers with Internet access.

What should you do?

- A. Configure Internet Connection Sharing (ICS) on Server2.
- B. Install the DHCP service on Server2. Create a scope for subnet 169.254.0.0/16.
- C. Modify the Internet Explorer properties on the 12 sales representatives' computers to specify 169.254.0.1 as the proxy server.
- D. Install the Connection Manager Administration Kit (CMAK) on Server2.

