Vendor: Microsoft

Exam Code: 70-291

Exam Name: Implementing, Managing, and Maintaining a Microsoft Windows Server 2003 Network Infrastructure

Version: Demo

Question: 1.

You have a stand-alone server that runs Windows Server 2003 Service Pack 2 (SP2). You run the Runas command and receive the following error message:
"1058: The service cannot be started, either because it is disabled or has no enabled devices associated with it." You need to ensure that you can use Runas successfully. What should you do?

A. Enable the Remote Registry service.
B. Enable the Secondary Logon service.
C. Join the server to an Active Directory domain.
D. From Device Manager, scan for hardware changes.

Answer: B

Question: 2.

You are the network administrator for your company. All servers run Windows Server 2003. All servers are configured with static IP addresses. All client computers run Windows XP Professional. All client computers are configured as DHCP clients. The company has a main office and one branch office. The offices are separated by a router. A DHCP server is deployed in each office. One of the DHCP servers shuts down unexpectedly. It takes four hours to repair the server. During that time, several mobile users connect their portable computers to the network and report that they cannot connect to share resources on the network. After the server is repaired, you create a new scope on each DHCP server that includes IP addresses for the other office. You activate the scopes. You test the new DHCP configuration by shutting down the DHCP server in the main office. You find out that the client computers in the main office are not receiving IP addresses from the DHCP server in the branch office. You need to ensure that when the DHCP server in one office fails, the client computers will receive a correct IP address configuration from the DHCP server in the other office. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Configure the router between the offices to forward BOOTP broadcasts.
B. Configure the DHCP server in each office with a DHCP scope that includes the same IP addresses as the DHCP server in the other office. Activate the scope.
C. Configure the DHCP server in each office with an additional network adapter. Connect each new network adapter to the local network. Assign an IP address from the other office's network to each new network adapter.
D. Install and configure a DHCP relay agent in each office.

Answer: DA

Question: 3.

You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. The network contains a Web server named Server1 that runs IIS 6.0 and hosts a secure Web site. The Web site is accessible from the intranet, as well as from the Internet. All users must authenticate when they connect to Server1. All users on the Internet must use a secure protocol to connect to the Web site. Users on the intranet do not need to use a secure protocol. You need verify that all users are using a secure protocol to connect to Server1 from the Internet. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. Monitor the events in the application log on Server1.
B. Monitor the events in the security log on Server1.
C. Monitor the Web server connections on Server1 by using a performance log.
D. Monitor network traffic to Server1 by using Network Monitor.
E. Monitor the IIS logs on Server1.

Answer: ED

Question: 4.

You are the administrator of an Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are members of the domain. The Secure Server (Require Security) IPSec policy is assigned to a file server named Server6. The policy is configured as shown in the exhibit. Users report that they cannot access shared folders on Server6. Users were able to access shared folders on Server6 prior to the implementation of the IPSec policy. You need to ensure that all client computers in the domain can access the shared folders on Server6. You must ensure that all communications between client computers and Server6 be encrypted. What should you do?

A. On Server6, enable the All ICMP Traffic IP Security rule in the properties of the Secure Server (Require Security) IPSec policy.
B. On Server6, enable the <Dynamic> IP Security rule in the properties of the Secure Server (Require Security) IPSec policy.
C. On all client computers, assign the Client (Respond Only) IPSec policy.
D. On all client computers, install an IPSec communication certificate in the local machine store.

Answer: C

Question: 5.

You are a network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. The company has a main office and one branch office. The perimeter networks for each office are configured as shown in the exhibit. You configure an L2TP/IPSec VPN tunnel between Server1 and Server2. You also configure and assign an IPSec policy named RAS IPSec that requires secure communications. You need to ensure that no unsecured traffic from the Internet reaches the internal network through this VPN. You also need to ensure that access to the VPN servers from their respective internal networks is not disrupted. What should you do?

A. Configure input and output L2TP/IPSec packet filters on the internal interfaces of Server1 and Server2.
B. Configure input and output L2TP/IPSec packet filters on the external interfaces of Server1 and Server2.
C. In the properties of RAS IPSec, edit the All IP Traffic IP Filter list to include the IP addresses for only Server1 and Server2.
D. In the properties of RAS IPSec, edit the All ICMP Traffic IP Filter list to include the IP addresses for only Server1 and Server2.

Answer: B

Question: 6.

You are the administrator of an Active Directory domain. The network contains a Windows Server 2003 domain controller named Server1. Users report that they experience intermittent delays when they log on to Server1. Administrators report that replication attempts between Server1 and other domain controllers are occasionally delayed. You need to verify the cause of the intermittent connection delays to Server1. You also need to find out whether the problem is related to a hardware deficiency on Server1. You need to track these delays over a period of one day. What should you do first?

A. Run the netdiag /verbose command to perform a network diagnostic test on Server1.
B. Run the replmon command to view the Active Directory replication status on Server1.
C. Use Network Monitor to view the network traffic packet contents between Server1 and all other computers.
D. Create a System Monitor counter to track the queue lengths on the network adapter on Server1.

Answer: D

Question: 7.

You are the administrator of a Windows Server 2003 computer named Server1. Server1 has a third-party application installed on it. The third-party application runs as a service that is named Service1. Service1 fails periodically. You need to configure the recovery options for Service1 to meet the following requirements: If Service1 runs successfully for a day or more, you need to ensure that only the service is immediately restarted upon failure. If, after this failure, Service1 does not run successfully for another day, you must ensure the entire server is immediately restarted. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Configure the Reset fail count after value for Service1 to 1 day.
B. Configure the Restart service after value for Service1 to 1,440 minutes.
C. Configure the response to the first failure to be to restart Service1.
D. Configure the response to the first failure to be to restart Server1.
E. Configure the response to the second failure to be to restart Service1.
F. Configure the response to the second failure to be to restart Server1.

Answer: FCA

Question: 8.

You are the administrator of a Windows Server 2003 computer named Server1. Server1 is a domain member server that has the DNS service installed. Server1 is configured with two network interfaces named NIC1 and NIC2. Routing is not enabled between the two network interfaces.NIC1 and NIC2 are configured as shown in the following table.

Network interface	IP address	Subnet mask	Preferred DNS server	Purpose
NIC1	192.168.2.10	255.255.255.0	192.168.2.10	Connect to production network
NIC2	192.168.3.10	255.255.255.0	192.168.3.2	Connect to isolated preproduction network segment

Resources on the preproduction network segment use the same fully qualified domain names (FQDNs) as resources in the production network. The TCP/IP properties on client computers in the preproduction environment are controlled by individual testers. You need to ensure that the users in the preproduction environment cannot resolve FQDNs from the production network. You want to accomplish this goal by using the DNS console on Server1. What should you do?

A. Configure the interfaces properties on Server1 to listen on 192.168.2.10 only.
B. Configure the forwarders on Server1 to refer requests to 192.168.3.2.
C. Configure Server1 to disable recursion.
D. Configure Server1 to disable round robin.

Answer: A

Question: 9.

You are a network administrator for A . Datum Corporation. The network consists of a single Active Directory domain named adatum.net. Users regularly browse the internal network and the Internet from their client computers. All Web and e-mail hosting for a separate DNS domain named adatum.com is outsourced to an ISP. All name resolution requests for adatum.com are resolved by the ISP. You have no administrative control over the DNS servers at the ISP. You cannot list the contents of adatum.com by using the nslookup command on the DNS servers at the ISP. A Windows Server 2003 computer named Server1 is configured with a primary zone for adatum.net. All root hints have been removed from Server1. All client computers refer to this DNS server for name resolution. You need to configure DNS resolution to ensure that all client computers can locate and access resources in adatum.net, adatum.com, and the Internet. What should you do?

A. Configure a secondary zone for adatum.com on Server1.
B. Configure a primary zone for adatum.com on Server1.
C. Configure conditional forwarding for adatum.com with the IP address of the DNS server at the ISP.
D. Configure simple forwarding with the default settings with the IP address of the DNS server at the ISP.

Answer: D

Question: 10.

You have a Web server that runs Windows Server 2003 Service Pack 2 (SP2). You attempt to start the World Wide Publishing Service and receive the following error message.

You need to identify which services must be started before you can start the World Wide Web Publishing Service. What should you do?

A. From Event Viewer, view the application log.
B. From Windows Explorer, open the %systemroot%\system32\drivers\etc\services file.
C. From the Services snap-in, view the properties of the World Wide Web Publishing Service.
D. From the command prompt, run Net config server /srvcomment:"World Wide Web Publishing Service".

Answer: C

Question: 11.

You have an DNS server that runs Windows Server 2003 Service Pack 2 (SP2). You need to ensure that an e-mail message is sent to the administrator if the DNS server service stops. You create a script that sends e-mail when the script is executed. What should you do next?

A. Install the POP3 service on the DNS server.
B. Modify the DNS Server service dependencies.
C. Modify the DNS Server service Recovery options.
D. Install the Universal Description, Discovery, and Integration (UDDI) services on the DNS server.

Answer: C

Question: 12.

You are the network administrator for your company. The network consists of a single Active Directory domain. The functional level of the domain is Windows Server 2003. All client computers in the domain run Windows XP Professional. An application named Inventory.exe is installed on all computers in the domain to remotely gather software inventory information. The application runs as a service in the security context of the Local System. The startup type of the service is set to Automatic. In the Default Domain Policy Group Policy object (GPO), the security administrator has configured a software restriction policy that is applied to all computers in the domain. The policy contains a hash rule for the Inventory.exe application, and the hash rule is configured with a security level of Unrestricted. The client computers on the network are attacked by a worm that is distributed by e-mail messages received over the Internet. The worm detects the presence of Inventory.exe on a computer, then starts a new instance of the application in the security context of the logged-on user. The worm exploits a bug in the application to cause the computer to fail. You need to ensure that Inventory.exe cannot be started by the worm, while still allowing the application to run as a service. What should you do?

A. In the computer settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a zone rule for the Internet zone.Configure the zone rule with a security level of Disallowed.

B. In the user settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a zone rule for the Internet zone. Configure the zone rule with a security level of Disallowed.

C. In the user settings section of the Default Domain Policy GPO, configure a software restriction policy that contains a hash rule for the Inventory.exe application. Configure the hash rule with a security level of Disallowed.

D. In the computer settings section of the Default Domain Policy GPO, modify the existing software restriction policy hash rule for the Inventory.exe application so that the hash rule has a security level of Disallowed.

Answer: D

Question: 13.

You are the network administrator for your company. The network consists of a single Active Directory domain. The domain contains an organizational unit (OU) named Web servers. The Web servers OU contains the computer accounts of 12 Windows Server 2003 computers that function as intranet Web servers. A Group Policy object (GPO) named Web servers Policy is linked to the Web servers OU. The GPO is used to configure various settings on the computers in the OU.A global group named Web server Admins is a member of the Administrators local group on each intranet Web server. You plan to install a security scanning application on each intranet Web server. The documentation for the application states that it uses a service account, which must be able to modify the HKEY_LOCAL_MACHINE\SYSTEM key in the registry of every computer on which the application is installed. You create the service account in the domain. The company's written security policy states that service accounts must be assigned only the minimum rights and permissions that they require to function. You need to configure the intranet Web servers so that they comply with the installation requirements of the security scanning application. You also need to comply with the company's security policy. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

A. Add the service account to the WebserverAdmins global group.

B. Configure the required permissions as registry security settings in the WebserversPolicy GPO.

C. Run the regedit.exe command to add the required permissions to the registry of each intranet Web server.

D. Run the explorer.exe command to modify NTFS permissions on the Systemroot\System32\Config\System file.Assign the service account the Allow - Change permission.

E. Configure file system security settings in the WebserversPolicy GPO to modify NTFS permissions on the Systemroot\System32\Config\System file.Assign the service account the Allow - Change permission.

Answer: D

Question: 14.

You are the network administrator for your company. The network contains a Windows Server 2003 computer named Server1. Three administrators are members of the Administrators local group on Server1. Twelve other administrators are members of the Domain Admins group. The Domain Admins group is also a member of the Administrators local group on Server1. Someone makes an unauthorized change to the HKEY_LOCAL_MACHINE\SYSTEM key in the registry on Server1, which causes the computer to fail. You fix the problem. You need to log all attempts to access the HKEY_LOCAL_MACHINE\SYSTEM key in the registry on Server1. You decide to enable auditing in the local security policy on Server1. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Enable auditing in the local security policy on Server1. Select the Audit object access (success and failure) option in the audit policy.
B. Enable auditing in the local security policy on Server1. Select the Audit privilege use (success and failure) option in the audit policy.
C. Enable auditing in the local security policy on Server1. Select the Audit system events (success and failure) option in the audit policy.
D. Configure the SACL on the HKEY_LOCAL_MACHINE\SYSTEM key in the registry. Specify auditing of the Full Control permission for Everyone.
E. Configure the SACL on the HKEY_LOCAL_MACHINE\SYSTEM key in the registry. Specify auditing of the Set Value permission for Everyone.

Answer: D A

Question: 15.

You are the network administrator for your company. The network consists of a single Active Directory domain. The domain contains 35 Windows Server 2003 computers; 3,000 Windows XP Professional computers;
and 2,000 Windows 2000 Professional computers.
Windows Server Update Services (WSUS) is installed on a server named Server1. The necessary Group Policy object (GPO) is configured. You need to confirm whether all computers in the domain have received all approved updates from Server1. What should you do on Server1?

A. Install and configure Urlscan.exe.
B. At the command prompt, type gpresult /scope COMPUTER.
C. Open the WSUS console.Run the Status of Computers report.
D. Open the WSUS console.Run the Synchronization Results report.

Answer: C

Question: 16.

You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. You need to implement a new software update infrastructure. You discover that security patches, critical updates, and service packs have never been installed on any client computer on the network. You install Windows Server Update Services (WSUS) on a Windows Server 2003 computer named Server5. You synchronize and approve all of the current security patches, critical updates, and service packs. You need to ensure that all client computers receive all Microsoft security patches, critical updates, and service packs. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Open the WSUS console. Select the option to automatically approve WSUS updates.
B. Install the Automatic Updates client on all client computers.
C. Modify the Microsoft Update settings of the Default Domain Controller organizational unit (OU) Group Policy object (GPO) to point client computers to http ://server5.
D. Modify the Microsoft Update settings of the Default Domain Policy Group Policy object (GPO) to point client computers to http: //server5.
E. Open the WSUS console. Create a target group and assign all client computers to the group.

Answer: B D

Question: 17.

You are the network administrator for your company. The network consists of a single Active Directory domain. All servers run Windows Server 2003. All client computers run Windows XP Professional. You install Windows Server Update Services (WSUS) on a network server named Server1. When you attempt to synchronize Server1 with the Windows Update servers, you receive an error message. You open Internet Explorer and verify that you can communicate with an external Web site by using the proxy server. You need to ensure that Server1 can communicate with the Windows Update servers. What should you do on Server1?

A. Restart the IIS administration tool.
B. Configure the Internet Explorer settings to bypass the proxy server.
C. In the WSUS options, configure authentication to the proxy server.
D. Install the ISA Firewall Client.

Answer: C

Question: 18.

Your network consists of a single Active Directory domain. The network contains two servers named Server1 and Server2 that run Windows Server 2003 Service Pack 2 (SP2). You log on to Server1 by using the Administrator account for the domain. You open Event Viewer and attempt to connect to Server2 but receive the following error message.

You verify that you can connect to Server2 by using Windows Explorer and that Windows Firewall is disabled on Server2. You open the Services snap-in on Server2 as shown in the exhibit. You need to ensure that you can connect to Server2 remotely by using Event Viewer. What should you do on Server2?

A. Add the Administrator account to the HelpServicesGroup.
B. Set the Startup Type for the Remote Registry service to Automatic and then start the service.
C. Set the Startup Type for the Secondary Logon service to Disabled and then stop the service.
D. Set the Startup Type for the Special Administration Console Helper service to Automatic and then start the service.

Answer: B

Question: 19.

You are the network administrator for your company. The network consists of a single subnet. A Windows Server 2003 computer named Server1 functions as a DHCP server. Server1 leases IP addresses in the 10.1.1.0/24 range to desktop client computers. There are 12 client reservations for other servers and network printers. You have configured several detailed scope and server options. If Server1 fails, you want to have a contingency plan that will allow you to use a domain controller named DC2 as a DHCP server as quickly as possible. You install DHCP on DC2 without any configuration and stop the DHCP Server service. You want to list the tasks that are required to back up Server1 and the tasks that are required to restore the backup to DC2. A backup age of 24 hours or less is acceptable. If Server1 fails, which set of tasks is required to enable DC2 to replace Server1 as the DHCP server?

A. On Server1: Schedule the Backup utility to back up the System State data to tape every 24 hours. On DC2: Perform a non-authoritative System State restore. Using the Services console, start the DHCP Server service. Authorize DHCP. Reconcile the database.
B. On Server1: Use the Backup utility to schedule a tape backup of the DHCP database every 24 hours. On DC2: Restore the tape backup of the DHCP database to a folder. Using the DHCP console,

restore the backup from the same folder. From the command prompt, type net start dhcpserver. Authorize DHCP.

C. On Server1: Schedule the Backup utility to back up the System State data to tape every 24 hours. On DC2: Perform an authoritative System State restore. Manually re-create the server and scope options that were on Server1. From a command prompt, type net start dhcpserver. Authorize DHCP.

D. On Server1: Use the DHCP console to perform a DHCP backup every 24 hours.Copy the backup on a network share that is accessible by DC2. On DC2:

Copy the backup to a local folder. Using the DHCP console, restore the backup from the local folder. From a command line, type net start dhcp. Authorize DHCP.Re-create the 12 client reservations.

<div style="text-align:right; color:red;">Answer: B</div>

Question: 20.

You are a network administrator for Alpine Ski House. The network consists of a single Active Directory domain named alpineskihouse.com. Your company acquires a company named Adventure Works. The Adventure Works network consists of a single Active Directory domain named adventure-works.com. A server named Server32 is a network-management application server in the adventure-works.com domain.Server32 accesses all of the desktop client computers to perform automated software upgrades and hardware inventory. The network-management software on Server32 references desktop computers by unqualified host names, which are resolved to clientname.adventure-works.com by using a DNS server. You join Server32 to your domain to become server32.alpineskihouse.com.The Server32 IP address is 10.10.10.90. You are gradually migrating all adventure-works.com desktop client computers to your domain to become clientname.alpineskihouse.com. You do not have access to the adventure-works.com DNS server. When Server32 attempts to apply an update to the client computers, the network-management software returns many alerts that say that desktop computers cannot be found. You want to allow the network-management software on Server32 to resolve unqualified client computer host names in adventure-works.com or alpineskihouse.com, and you want to use the minimum amount of administrative effort. What should you do?

A. On the DNS server for alpineskihouse.com, add a zone for adventure-works.com. Create a host (A) record for server32.adventure-works.com that points to 10.10.10.90.

B. On Server32, in System Properties, type adventure-works.com in the Primary DNS suffix of this computer field in the DNS Suffix and Netbios Computer Name setting.

C. On Server32, configure a Hosts file that contains the name and IP address of every network computer.

D. On Server32, in Advanced TCP/IP Settings, add adventure-works.com and alpineskihouse.com to the Append these DNS suffixes (in order) setting.

<div style="text-align:right; color:red;">Answer: D</div>

Question: 21.

You are the network administrator for A . Datum Corporation. The company uses the adatum.com namespace for its internal network. The company network consists of two networks that are connected by a WAN link. The 10.9.9.0 network uses the 10.9.9.0/24 address. The 10.9.8.0 network uses the 10.9.8.0/24 address. The relevant portion of the network is shown in the exhibit. The network contains the DNS servers that are configured as shown in the following table.

Server name	IP address	Local DNS zones	Forwarding
DNS1	10.9.8.6	adatum.com, delegation to sales.adatum.com	131.107.5.1
DNS2	10.9.9.3	sales.adatum.com	None
DNS3	10.9.9.7	None	Conditional forwarding to DNS1 for adatum.com. Forwarding to 131.107.5.1 for all other namespaces.

In the 10.9.9.0/24 network, a server named Server1 frequently needs to resolve names in the adatum.com namespace and on the Internet. You need to configure the TCP/IP properties of Server1 to use the most efficient server as its preferred DNS server. The number of hops required to resolve any name must be kept to a minimum. You also need to minimize the amount of network traffic that is caused by name resolution. On Server1, which DNS server should you configure as the preferred DNS server?

A. DNS1
B. DNS2
C. DNS3
D. 131.107.5.1

Answer: C

Question: 22.

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.

Answer: C

Question: 23.

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory domain named contoso.com. The network topology is shown in the exhibit. The configurations of the DNS servers that host the zone named contoso.com are shown in the following table.

Server	Zone type	Server role	Location
Server1	Active Directory-integrated	Domain controller	New York
Server2	Active Directory-integrated	Domain controller	Chicago
Server3	Secondary	Member server	Caracas

The refresh interval for the zone is one hour. The zone contains 10,000 records. The network connection to Caracas is operating at 90 percent of capacity. You remove Server3 from the network to perform hardware maintenance. Two hours later, you bring Server3 back on the network. You need to ensure that Server3 can immediately provide accurate responses to client computer requests for data. You also need to ensure that no unnecessary network traffic is generated by the DNS servers. What should you do on Server3?

A. Transfer the zone from the master server.
B. Reload the zone from the master server.
C. Update server data files.
D. Scavenge stale resource records.

Answer: A

Question: 24.

You are the network administrator for Contoso, Ltd. The network consists of a single Windows Server 2003 DNS zone named contoso.com. The network topology is shown in the exhibit. All network servers run Windows Server 2003. All IP addresses are statically assigned. The primary DNS zone for contoso.com is hosted on a server at the company's main office in Cairo. Secondary zones for contoso.com are hosted on servers in the branch offices. Another administrator reports that network utilization is at 90 percent of capacity. You reconfigure the refresh interval and the minimum default Time to Live (TTL) interval for the contoso.com zone, as shown in the following table.

Refresh interval	3 hours
Minimum default Time to Live (TTL)	1 day

You need to configure the start of authority (SOA) resource record properties for the contoso.com zone. You also need to ensure that the server in the Cairo office will continue to attempt zone transfers if an initial attempt fails. What should you do?

A. Configure the contoso.com zone to expire after 1 hour.
B. Configure the contoso.com zone to expire after 4 hours.
C. Configure the contoso.com zone to expire after 20 seconds.
D. Configure the retry interval to be 1 hour.
E. Configure the retry interval to be 4 hours.
F. Configure the retry interval to be 20 seconds.

Answer: E

Question: 25.

You are the network administrator for Contoso, Ltd. The network consists of two Active Directory domains named contoso.com and corp.contoso.com. All DNS zones are configured to be Active Directory-integrated zones. You create a global security group named ConsoleAdmins in corp.contoso.com. You add a member of the Domain Users global group named Anne to ConsoleAdmins. Anne logs on to her Windows XP Professional computer named Computer1. Anne runs the nslookup command and receives the output shown in the exhibit. You need to configure the zone properties to ensure that Anne can list the contents of corp.contoso.com from Computer1. What should you do?

A. Allow zone transfers to 192.168.2.47.
B. Allow zone transfers to 192.168.2.45.
C. Allow zone transfers to 192.168.2.27.
D. Allow zone transfers to 169.254.25.142.
E. Assign the ConsoleAdmins group the Allow - Full Control permisson.
F. Assign the ConsoleAdmins group the Allow - List Contents permission.

Answer: C

Question: 26.

You are the DNS administrator for Adventure Works. Adventure Works is an Internet service provider (ISP) that hosts Web sites for many companies. Each Adventure Works DNS server hosts multiple DNS zones for customers. Several Adventure Works administrators are allowed to add DNS zones. You want to produce a weekly report that will list all the zones that are hosted on each DNS server. What should you do?

A. Use the dnslint utility to query each DNS server.
B. Use the dnscmd utility to query each DNS server.
C. Use the nslookup utility to query each DNS server.
D. Use the adsiedit utility to query Active Directory for a list of DNS zones.

Answer: B

Question: 27.

You are the network administrator for Humongous Insurance. The network consists of a single Active Directory domain named humongous.com. The domain contains Windows Server 2003 computers and Windows XP sProfessional computers. You configure several Group Policy objects (GPOs) to enforce the use of IPSec for certain types of communication between specified computers. A server named Server2 runs the Telnet service. A GPO is supposed to ensure that all Telnet connections to Server2 are encrypted by using IPSec. However, when you monitor network traffic, you notice that Telnet connections are not being encrypted. You need to view all of the IPSec settings that are applied to Server2 by GPOs. Which tool should you use?

A. the IP Security Policy Management console
B. the IP Security Monitor console
C. the Resultant Set of Policy console
D. Microsoft Baseline Security Analyzer (MBSA)

Answer: C

Question: 28.

Your network consists of a single Active Directory domain. The network contains a server that runs Windows erver 2003 Service Pack 2 (SP2).The server has an application that runs as a service. The application uses a domain service account to access other servers in the domain. Security policies require that users reset their passwords every 30 days. After the application runs for a month, the application fails. You need to ensure that the application starts and can access the remote servers. What should you do?

A. In the Services snap-in, set the service to log on as the Local System account and start the service.
B. In the Services snap-in, set the service to log on as the Local Administrator account and start the service.
C. In Active Directory Users and Computers, reset the server's computer account. In the Services snap-in, start the service.
D. In Active Directory Users and Computers, set the Account Expires option to Never. In the Services snap-in, start the service.

Answer: D

Question: 29.

You are the network administrator for your company. A Windows Server 2003 computer named Router11 is used to connect the network to the Internet. You find out that some computers on the network are infected with a worm, which occasionally sends out traffic to various hosts on the Internet. This traffic always uses a certain source TCP port number. You need to identify which computers are infected with the worm. You need to configure a solution on Router11 that will perform the following two tasks:
Detect and identify traffic that is sent by the worm.
Immediately send a notification to a network administrator that the infected computer needs to be repaired. What should you do?

A. Configure a WMI event trigger.
B. Configure a Network Monitor capture filter.
C. Configure a Network Monitor trigger.
D. Configure a System Monitor alert.

Answer: C

Question: 30.

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.

Answer: C

Question: 31.

You are the network administrator for Alpine Ski House. The network consists of two Active Directory domains. One domain is named alpineskihouse.com. A subsidiary company named Adventure Works has a domain named adventure-works.com. Both domains are in a single forest. A primary DNS server for alpineskihouse.com is located in the company's Seattle office. A primary DNS server for adventure-works.com is located in the company's Portland office. Both DNS servers are Windows Server 2003 computers.
Each domain has three regional offices. Each regional office contains the following computers:
a secondary DNS server in its respective domain a DHCP server a recently installed Microsoft Internet Security and Acceleration (ISA) Server computer that connects the LAN to the Internet Company sales representatives visit the Seattle office, the Portland office, and all regional offices several times each month. All sales representatives use Windows XP Professional portable computers that are members of the alpineskihouse.com domain. You create an appropriate wpad.dat script file on each of the ISA servers in each regional office. On each DHCP server, you configure the 252 Proxy Auto discovery option and the corresponding http://ISAServerName/wpad.dat string value. Sales representatives report that they cannot access the Internet by using Internet Explorer when they visit an office that is in the adventure-works.com domain. You need to ensure that all users can access the Internet at all times. You want to use the minimum amount of administrative effort. What should you do?

A. Configure Windows XP Professional portable computers with the primary DNS suffix of adventure-works.com.
B. Configure the Advanced TCP/IP Settings setting on the Windows XP Professional portable computers with a DNS suffix for this connection setting of adventure-works.com.
C. On each DHCP server that is a member of the adventure-works.com domain, configure the 15 DNS Domain Name option to be adventure-works.com.
D. On the primary DNS server for the adventure-works.com domain, add an _http service service locator (SRV) resource record for each ISA server in the adventure-works.com domain.

Answer: C

Question: 32.

You are the network administrator for your company. The network contains 100 Windows XP Professional computers.
You configure a Windows Server 2003 computer named Dev1 as a DNS server.Dev1 has the IP address 192.168.1.2 and contains host (A) resource records for all network client computers that are located in the branch office.
You install a Windows Server 2003 computer named Dev2 as a DHCP server.Dev2 is configured as shown in the following table.
You install a DSL connection for Internet access. You configure a server named Dev3 as an Internet Connection Sharing (ICS) host with two network adapters. The network adapter that has the IP

address 131.107.96.21 connects to the DSL modem, and the network adapter that has the IP address 192.168.0.1 connects to the LAN.The ISP's
DNS server has the IP address 131.107.62.9.
Your users report that they cannot access the Internet. You need to ensure that all users in the company can access the Internet through the ICS host. What should you do?

A. Remove DHCP from Dev2.
B. Replace the DHCP scope on Dev2 with one that has a subnet mask of 255.255.255.192.
C. Change the DHCP scope option 003 Default Gateway on Dev2 to 131.107.96.21.
D. Install the DNS service on Dev3, and configure 131.107.62.9 as a forwarder.

Answer: A

Question: 33.

You are a network administrator for your company. The network consists of five Windows Server 2003 computers and 50 Windows XP Professional computers on a single subnet. On Sunday, another administrator installs a new firewall between the LAN and the company's T1 Internet connection. The network is configured as shown in the exhibit. Local host names are resolved on the network by using a WINS server. All client computers are configured to use ISP1 for DNS name resolution. On Monday morning, users report that they are no longer able to access secure and nonsecure Internet Web sites. From a Windows XP Professional computer, you are able to succesfully perform the following tasks: Ping the IP addresses of Web servers on the Internet.
Use Internet Explorer to open both secure and nonsecure Web sites by using an IP address in place of the URL. You run the nslookup command and attempt to resolve an Internet fully qualified domain name (FQDN).You receive the following error message:
*** [131.107.100.200] can't find www.microsoft.com:
No response from server >
You need to use the minimum amount of administrative effort to provide users with the ability to browse Web sites on the Internet. What should you do?

A. Configure the firewall to allow traffic on TCP ports 80 and 443.
B. Configure the firewall to allow traffic on TCP port 53 and UDP port 53.
C. Install and configure the DNS service on one of the local servers.
D. Install and configure Microsoft Internet Security and Acceleration (ISA) Server on one of the local servers.

Answer: B

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:

Guarantee & Policy | Privacy & Policy | Terms & Conditions