Examskey Microsoft 70-293 exam demo product is here for you to test the quality of the product. This Microsoft 70-293 demo also ensures that we have this product ready unlike most companies, which arrange the product for you as you order. These 70-293 exam questions are prepared by Microsoft subject matter specialists. Hence these are most accurate version of the 70-293 exam questions that you can get in the market.

We also offer bundle discount packages for every Microsoft certification track, so you can buy all related exam questions in one convenient bundle. And for corporate clients we also offer bundles for Microsoft certification exams at huge discount.

Check out our 70-293 Exam Page and Microsoft Certification Page for more details of these bundle packages.
Question: 1

You are a network administrator for your company. The network consists of a single Active Directory domain. The network contains 80 Web servers that run Windows 2000 Server. The IIS Lockdown Wizard is run on all Web servers as they are deployed. Your company is planning to upgrade its Web servers to Windows Server 2003. You move all Web servers into an organizational unit (OU) named Web Servers. You are planning a baseline security configuration for the Web servers. The company’s written security policy states that all unnecessary services must be disabled on servers. Testing shows that the server upgrade process leaves the following unnecessary services enabled: SMTP, Telnet. Your plan for the baseline security configuration for Web servers must comply with the written security policy. You need to ensure that unnecessary services are always disabled on the Web servers. What should you do?

A. Create a Group Policy object (GPO) and import the Hisecws.inf security template. Link the GPO to the Web Servers OU.
B. Create a Group Policy object (GPO) to apply a startup script to stop the unnecessary services. Link the GPO to the Web Servers OU.
C. Create a Group Policy object (GPO) to apply a logon script that disables the unnecessary services. Link the GPO to the Web Servers OU.
D. Create a Group Policy object (GPO) to set the startup type of the unnecessary services to Disabled. Link the GPO to the Web Servers OU.

Answer: D

Explanation:
Windows Server 2003 installs a great many services with the operating system, and configures quite a few with the Automatic startup type, so that these services load automatically when the system starts. Many of these services are not needed in a typical member server configuration, and it is a good idea to disable the ones that the computer does not need. Services are programs that run continuously in the background, waiting for another application to call on them. Instead of controlling the services manually, using the Services console, you can configure service parameters as part of a GPO. Applying the GPO to a container object causes the services on all the computers in that container to be reconfigured. To configure service parameters in the Group Policy Object Editor console, you browse to the Computer Configuration\Windows Settings\Security Settings\System Services container and select the policies corresponding to the services you want to control.

Incorrect Answers:
* The logon script would only run when someone logs on to the web servers. It’s likely that the web servers will be running with no one logged in.
* The Hisecws.inf security template is designed for workstations, not servers.
* The startup script would only run when the servers are restarted. A group policy would be refreshed at regular intervals.

Reference:
Question: 2

SIMULATION

You are the network administrator for your company. You are configuring security on the Windows Server 2003 computers in the human resources (HR) department. All servers for the HR department are located in the HR Servers organizational unit (OU). You need to configure security for these servers by using existing Group Policy objects (GPOs). Company policy dictates that you should not create additional GPOs. You have been instructed to use GPO1 to configure these settings. In addition, you must ensure the following requirements are met. Web hosting services should not be installed on these servers. Web hosting components should not be installed on these servers in the future. Other services on these servers should not be affected. You need to configure settings by using the minimal amount of configurations on the GPO. What should you do? To answer, click the Simulation button and then perform the appropriate actions.

Answer:

Step #1.
In Group Policy Management, expand the tree until you can see the Organizational Units.

Step #2.
Right click on the HRServers OU and select “Link an Existing GPO…”

Step #3.
Select GPO1 and click OK.
Step #4.
Right click on GPO1 and select Edit.

Step #5.
Expand Computer Configuration > Administrative Templates and select Internet Information Services. In the right pane, double click “Prevent IIS installation”.
Step #6.
Select "Enabled" and click OK.

Question: 3
You are the network administrator for your company. All servers run Windows Server 2003. You configure a baseline security template named Baseline.inf. Several operations groups are responsible for creating templates containing settings that satisfy operational requirements. You receive the templates shown in the following table.

<table>
<thead>
<tr>
<th>Operations group</th>
<th>Template name</th>
<th>Applies to</th>
</tr>
</thead>
<tbody>
<tr>
<td>File and Print</td>
<td>File.inf</td>
<td>File servers</td>
</tr>
<tr>
<td>Database</td>
<td>Db.inf</td>
<td>Database servers</td>
</tr>
<tr>
<td>Security</td>
<td>Sec.inf</td>
<td>All resource servers</td>
</tr>
</tbody>
</table>

The operations groups agree that in the case of conflicting settings, the priority order listed in the following table establishes the resultant setting:

<table>
<thead>
<tr>
<th>Template</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sec.inf</td>
<td>1</td>
</tr>
<tr>
<td>Baseline.inf</td>
<td>2</td>
</tr>
<tr>
<td>Specific server role template</td>
<td>3</td>
</tr>
</tbody>
</table>

You need to create one or more Group Policy objects (GPOs) to implement the security settings. You want to minimize the amount of administrative effort required when changes are requested by the various operations groups. What should you do?

A. Create a GPO and import the following templates in the following order: Sec.inf, Db.inf, File.inf, Baseline.inf.
B. Create a GPO and import the following templates in the following order: Baseline.inf, Sec.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
C. Create a GPO and import the following templates in the following order: Sec.inf, Baseline.inf. Create a GPO for each server role and import only the specific template for that role into each respective GPO.
D. Create a GPO for each server role and import the following templates in the following order: Baseline.inf, specific server role template, Sec.inf.

Answer: B

Explanation:
Windows Server 2003 processes GPOs from the bottom of the list to the top of the list, with the topmost GPO having the final authority. Because policies contained in GPOs will, by default, overwrite policies of previously applied, we would need to import the Baseline.inf before the ServerSec.inf template.

Incorrect Answers:
* Because policies contained in GPOs will, by default, overwrite policies of previously applied; we would need to import the Baseline.inf before the ServerSec.inf template.
A, * Because we need to import templates specific to each of two server roles, we need a separate GPO for each server role.

Reference:
You are the network administrator for your company. The network consists of a single Active Directory domain. The company has a main office in San Francisco and branch offices in Paris and Bogota. Each branch office contains a Windows Server 2003 domain controller. All client computers run Windows XP Professional. Users in the Bogota office report intermittent problems authenticating to the domain. You suspect that a specific client computer is causing the problem. You need to capture the authentication event details on the domain controller in the Bogota office so that you can find out the IP address of the client computer that is the source of the problem. What should you do?

A. Configure Network Monitor to record the authentication events.
B. Configure System Monitor to monitor the authentication events.
C. Configure Performance Logs and Alerts with a counter log to record the authentication events.
D. Configure Performance Logs and Alerts with an alert to trigger on authentication events.

**Answer: A**

**Explanation:**
The question states that you find out the IP address of the client computer that is the source of the problem. Using Network Monitor to capture traffic is the only way to do this.

**Incorrect Answers:**
* This will not display the IP address of the client computer that is the source of the problem.
* This will not display the IP address of the client computer that is the source of the problem.
* This will not display the IP address of the client computer that is the source of the problem.

**Reference:**
http://support.microsoft.com/default.aspx?scid=kb;en-us;175062
Question: 5

You are a network administrator for your company. You need to test a new application. The application requires two processors and 2 GB of RAM. The application also requires shared folders on the application server and requires the installation of software on the client computers. You create the test plan. You assemble a server in the test lab. You install Windows Server 2003, Web Edition on the server. You install the application on the server. You install the client software components for the application on 20 client computers in the test lab. You test the application. You discover that only some of the client computers can run the application. You turn off the client computers that ran the application successfully, and you test again. The client computers that failed in the first test now run the application successfully. You need to identify the cause of the failure and update your test plan. What should you do?

A. Change the Application pool identity to Local Service for the default application pool.
B. Use Add or Remove Programs to add the Application Server Windows component.
C. Increase the Maximum number of worker processes to 20 for the default application pool.

Answer: D

Question: 6

You are the security analyst for your company. The company's written security policy does not allow direct dial-in connections to the network. During a routine security audit, you discover a Windows Server 2003 server named Server1 that has a modem installed and is connected to an outside analog phone line. You investigate and discover that Server1 is also running Routing and Remote Access and is used by the sales department. The modem supports the caller ID service. This remote access connection is used by an application at a partner company to upload product and inventory information to Server1. Each day at midnight, the partner application connects to Server1 and uploads the information. The connection never lasts longer than 30 minutes. The application is currently using the sales manager's domain user account to make the connection. The partner application does not support incoming connections. The partner company has no plans to update this application to support your written security policy, and the sales department requires this updated product and inventory information to be available each morning. Company management directs you to design a solution that provides the highest level of security for this connection until a more secure solution can be developed by the two companies. You need to design and implement a solution that will ensure that only the partner's application can connect to your network over the dial-up connection. Your solution must prevent the connection from being used by unauthorized users, and it must allow only the minimum amount of access to the network. Which two actions should you take? (Each correct answer presents part of the solution. Choose two.)
A. Configure a remote access policy on Server1 that allows the connection for only the specified user account between midnight and 1:00 A.M. Configure the policy to require callback authentication to the partner company's server.
B. Create a local account named PartnerDialup on Server1, and add this account to the local Users group. Grant this user account permissions for the folder to which the sales information is uploaded. Direct the partner company to use this account for remote access.
C. Create an account named PartnerDialup in the domain, and add this account to the Domain Guests group. Grant this user account permissions for the folder to which the sales information is uploaded. Direct the partner company to use this account for remote access.
D. Configure a remote access policy on Server1 that allows the connection for only the specified user account between midnight and 1:00 A.M. Configure the policy to allow only the specific calling station identifier of the partner company's computer.

Answer: B,D

Explanation: A local user account for Microsoft Windows Server 2003 is a user account a domain provides for a user whose global account is not in a trusted domain. A local account is not required where trust relationships exist between domains.

IP address A 32-bit address assigned to Transmission Control Protocol/Internet Protocol (TCP/IP) client computers and other network equipment that uniquely identifies that device on the network. For a computer to be accessible from the Internet, it must have an IP address containing a network identifier registered with the Internet Assigned Numbers Authority (IANA).

Thus options B and D will prevent the connection from being used by unauthorized users and with the minimum amount of access to the network.

Incorrect answers:
* This option will result in unnecessary exposure on the network by allowing more than the minimum amount of access to the network.
* There is no need to make use of require callback authentication. This implies that more than the minimum amount of access to the network needs to be allowed for.

Reference:

Question: 7

DRAG DROP

You are a network administrator for Contoso, Ltd. The network consists of two Active Directory forests. No trust relationships exist between the two forests. All computers in both forests are configured to use a common root certification authority (CA). Each forest contains a single domain. The domain named hr.contoso.com contains five Windows Server 2003 computers that are used exclusively to host confidential human resources applications and data. The domain named contoso.com contains all other servers and client computers. A firewall separates the human resources servers from the other computers on the network. Only VPN traffic from contoso.com to a remote access server in hr.contoso.com is allowed through the firewall. Managers need to access data on the servers in hr.contoso.com from their Windows XP Professional computers. The company's written security policy requires that all communication containing human resources data must be secured by using the strongest IPSec encryption available. You need to configure an IPSec policy for the servers that host the human resources data that complies with the written security
policy and gives the managers in contoso.com access to the data they need. What should you do? To answer, drag the appropriate configuration settings to the IPSec Policy Configuration.

Answer:
Explanations:

We cannot use Kerberos because there is no trust between the forests; we must use certificates, we must affect all traffic, and the server must require security. The security of a VPN is based on the tunneling and authentication protocols that you use and the level of encryption that you apply to VPN connections. For the highest level of security, use a remote access VPN based on L2TP/IPSec with certificate-based IPSec authentication and Triple-DES for encryption. If you decide to use a PPTP-based VPN solution to reduce costs and improve manageability and interoperability, use Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2) as the authentication protocol.

Reference:
You are the systems engineer for Contoso, Ltd. The network consists of a single Active Directory domain named contoso-ad.com. All servers run Windows Server 2003. A Windows Server 2003 computer named DNSSRV1 functions as the internal DNS server and has zones configured as shown in the exhibit. (Click the Exhibit button.) The network is not currently connected to the Internet. The company maintains a separate network that contains publicly accessible Web and mail servers. These Web and mail servers are members of a DNS domain named contoso.com. The contoso.com zone is hosted by a UNIX-based DNS server named UNIXDNS, which is running the latest version of BIND. The company plans to allow users of the internal network to access Internet-based resources. The company’s written security policy states that resources located on the internal network must never be exposed to the Internet. The written security policy also states that the internal network’s DNS namespace must never be exposed to the Internet. To meet these requirements, the design specifies that all name resolution requests for Internet-based resources from computers on the internal network must be sent from DNSSRV1. The current design also specifies that UNIXDNS must attempt to resolve any name resolution requests before sending them to name servers on the Internet. You need to plan a name resolution strategy for Internet access. You need to configure DNSSRV1 so that it complies with company requirements and restrictions. What should you do?

A. Add a name server (NS) resource record for UNIXDNS to your zone. Configure UNIXDNS with current root hints.
B. On DNSSRV1, configure a secondary zone named contoso.com that uses UNIXDNS as the master server. Configure UNIXDNS to forward requests to your ISP’s DNS servers.
C. Delete the root zone from DNSSRV1. Configure DNSSRV1 to forward requests to UNIXDNS.
D. Copy the Cache.dns file from the Windows Server 2003 installation CD-ROM to the C:\Windows\System32\Dns folder on DNSSRV1.

Answer: C

Explanation:
We need to delete the root zone from the internal DNS server. This will enable us to configure the server to forward internet name resolution requests to the external DNS server (UNIXDNS). A DNS server configured to use a forwarder will behave differently than one that is not configured to use it. A DNS server configured to use a forwarder behaves as follows: When the DNS server receives a query, it attempts to resolve this query using the primary and secondary zones that it hosts and its cache. If the query cannot be resolved using this local data, then it will forward the query to the DNS server designated as a forwarder. The DNS server will wait briefly for an answer from the forwarder before attempting to contact the DNS servers specified in its root hints.

Incorrect Answers:
* The Cache.dns file contains the IP addresses of the internet root DNS servers. We don’t want the internal DNS server to query the root DNS servers, so we don’t need the cache.dns file.
* Unixdnss already has root hints. An NS record on the internal DNS server won’t fulfill the requirements of the question.
* We do not need a secondary zone on the internal DNS server. All external resolution requests must be forwarded to the external DNS server.

Reference:

Question: 9

SIMULATION

You are the network administrator for Fabrikam, Inc. The network contains a Windows Server 2003 computer named Server1. Server1 is used as a domain controller, file server, and print server. In the past, Server1 was also used to host intranet content, including streaming media. However, Server1 is no longer used to host intranet content. You need to configure Server1 to remove unnecessary components and services. Your solution must not prevent Server1 from functioning in its assigned server roles or increase the vulnerability of Server1 to security threats. What should you do? To answer, click the Simulation button and then perform the appropriate actions.

Answer:
We need to uninstall IIS.
Step #1.
Open the Add or Remove Programs applet in Control Panel then click “Add/Remove Windows Components”.

Step #2.
Clear the Application Server checkbox and click Next.
Step #3.
Click Finish when Windows Components Wizard finishes.
Question: 10

SIMULATION

You are the network administrator for Contoso, Ltd. The network contains a Windows Server 2003 computer that runs Certificate Services and serves as an enterprise certification authority (CA). You need to achieve the following goals:
Configure Certificate Services to issue code-signing certificates
Use the Certificate Services Web interface to request a code-signing certificate for yourself
Ensure that only a user named Bruno has the authority to add certificates to Active Directory
What should you do? To answer, click the Simulation button and then perform the appropriate actions.

Answer:
*****************************************************************************
- Open Active Directory User and Computer
- Users -> Cert Publishers group -> Members tab ->Add Bruno
  note: You will find only server1 in the Cert Publishers group. Don’t remove it. You will not find extra users, you need to add only Bruno
*****************************************************************************

REQUIREMENT:1 Configure Certificate Services to issue code-signing certificates

Step #1.
Open Certificate authority
Step #2.
In Certificate Authority window Right click on "Certificate Templets" ->select new -> certificate Templets to issue
Step #3.
Select code Signing.

**REQUIREMENTS**
Use the Certificate Services Web interface to request a code-signing certificate for yourself
Step#1.
Open Certificate Services Web interface using http://localhost/certsrv/ in web browser and click request a certificate
Step #2.
In Request a Certificate Page Click Advanced Certificate request

Step #3.
Step #3.

REQUIREMENTS Ensure That only a user name Bruno has the authority to add certificates to active directory.
Step #1.
In Certificate Authority window Right Click on Root CA and Select Properties

Step #2.
In Security Tab of Root CA Properties select Burno and Check Allow "Issue and Manage certificates" and "Manage CA"
Question: 11

SIMULATION
You are the network administrator for Fabrikam, Inc. You have recently deployed a new Active Directory domain. All domain controllers run Windows Server 2003. The network contains Windows NT Workstation, Windows 98 client computers, and Windows XP client computers. You discover that the Windows NT Workstation client computers and Windows 98 client computers cannot communicate with the domain controllers. You do not experience this problem with the Windows XP client computers. You have verified that there are no network connectivity issues. You need to configure Group Policy objects (GPOs) to ensure that all client computers can communicate with the domain controllers. You want to ensure that the domain controllers support IP packet encryption where possible. You need to accomplish these configurations by configuring as few settings as possible. You cannot create new GPOs or GPO links. What should you do? To answer, click the Simulation button and then perform the appropriate actions.

Answer:
Edit GPO of Default Domain Controller:
Disable: Microsoft network server: Digitally sign communications (always)
Enable: Microsoft network server: Digitally sign communications (if client agrees)
Disable: Microsoft network client: Digitally sign communications (always)
Enable: Microsoft network client: Digitally sign communications (if client agrees)
Assign Server(Request Security) for IPSec policy.
Edit GPO of Default Domain policy:
Assign Client(Respond Only) for IPSec policy.
**************************************************************************
We need to disable the requirement for digitally signed communications with servers.
Step #1.
In Group Policy Management, expand the tree and select the Group Policy Objects folder.
Step #2.
Right click the Default Domain Policy and select Edit.

Step #3.
Expand the Computer Configuration section to show Local Policies / Security Options.
Step #4.
Double click “Microsoft Network Server: Digitally sign communications (always)”. Select Disabled and click ok.

Step #5.
Double click “Microsoft Network Server: Digitally sign communications (if client agrees)”. Select the checkbox to “Define this policy setting” and select Enabled.
You are the network administrator for your company. The network consists of a single Active Directory domain. All computers on the network are members of the domain. The domain contains a Windows Server 2003 computer named Server1. You are planning a public key infrastructure (PKI) for the company. You want to deploy an enterprise certification authority (CA) on Server1. You create a new global security group named Cert Approvers. You install an enterprise CA and configure the CA to issue Key Recovery Agent certificates. The company's written security policy states that issuance of a Key Recovery Agent certificate requires approval from a member of the Cert Approvers group. All other certificates must be issued automatically. You need to ensure that members of the Cert Approvers group can approve pending enrollment requests for a Key Recovery Agent certificate. What should you do?

A. Assign the Cert Approvers group the Allow - Issue and Manage Certificates permission for the CA.
B. Add the Cert Approvers group to the existing Cert Publishers group in the domain.
C. For all certificate managers, add the Cert Approvers group to the list of managed subjects.
D. Assign the Cert Approvers group the Allow - Enroll permission for the Key Recovery Agent certificate template.
E. Assign the Cert Approvers group the Allow - Full Control permission for the Certificate Templates container in the Active Directory configuration naming context.

Answer: A

Explanation:
In order to approve certificates you need certificate manager rights. In order to get those rights you need Issue and Manage Certificates rights. The option to enable auto enroll or wait for approval is made at the certificate template (in this case, the key recovery template).
Incorrect Answers:
* Will allow enroll only.
* Will allow all certificate managers.
* Cert publisher group is meant to include the CA servers only.
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. The domain contains an organizational unit (OU) named Servers that contains all of the company's Windows Server 2003 resource servers. The domain also contains an OU named Workstations that contains all of the company's Windows XP Professional client computers. You configure a baseline security template for resource servers named Server.inf and a baseline security template for client computers named Workstation.inf. The Server.inf template contains hundreds of settings, including file and registry permission settings that have inheritance propagation enabled. The Workstation.inf template contains 20 security settings, none of which contain file or registry permissions settings. The resource servers operate at near capacity during business hours. You need to apply the baseline security templates so that the settings will be periodically enforced. You need to accomplish this task by using the minimum amount of administrative effort and while minimizing the performance impact on the resource servers. What should you do?

A. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command. Create a Group Policy object (GPO) and link it to the Workstations OU. Import the Workstation.inf template into the GPO.

B. Import both the Server.inf and the Workstation.inf templates into the Default Domain Policy Group Policy object (GPO).

C. On each resource server, create a weekly scheduled task to apply the Server.inf settings during off-peak hours by using the secedit command. Import the Workstation.inf template into the Default Domain Policy Group Policy object (GPO).

D. Create a Group Policy object (GPO) and link it to the domain. Import both the Server.inf and the Workstation.inf templates into the GPO.

Answer: A

Explanation: The question states that you need to apply the baseline security templates so that the settings will be periodically enforced. To accomplish this you must create a scheduled task so that the performance impact on resource servers is minimized. Furthermore, the question also states that Workstation.inf is a baseline security template for client computers. Therefore, the GPO has to be linked to the OU that contains the client computers, and the Workstation.inf template must be imported to the said GPO so that it can be applied. Secedit.exe is a command line tool that performs the same functions as the Security Configuration And Analysis snap-in, and can also apply specific parts of templates to the computer. You can use Secedit.exe in scripts and batch files to automate security template deployments. You can create a baseline security configuration in a GPO directly, or import a security template into a GPO. Link the baseline security GPO to OUs in which member servers’ computer objects exist.

Incorrect Answers:
* GPOs process security templates from the bottom up; therefore, by import both the Server.inf and the Workstation.inf templates into a single GPO, we would ensure that the settings in the security template imported last are applied in cases where there are conflicting settings. If we apply this to the domain, then all computers would have the same settings.
* The Default Domain Policy Group Policy object (GPO) is applied only to the Domain Controllers group.

Reference:
Craig Zacker, MCSE Self-Paced Training Kit (Exam ): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Redmond, Washington, Chapter 10

Question: 14

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. The domain contains a Windows Server 2003 computer named Server1 that is running Routing and Remote Access. The domain contains a universal group named Managers and a global group named Operations. User accounts in the Managers group require remote access between the hours of 8:00 AM and 8:00 P.M. User accounts in the Operations group require remote access 24 hours per day. You configure a remote access policy on Server1 named RA_Managers with the appropriate settings for the Managers group, and you configure a second remote access policy named RA_Operations on Server1 with the appropriate settings for the Operations group. The default remote access policies on Server1 remain unmodified. Members of the Managers group report that they can establish a remote access connection to Server1, but members of the Operations group report that they cannot establish a remote access connection to Server1. You open the Routing and Remote Access administrative tool and note that the remote access policies are in the order presented in the following table.

<table>
<thead>
<tr>
<th>Remote access policy name</th>
<th>Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>RA_Managers</td>
<td>1</td>
</tr>
<tr>
<td>Connections to Microsoft Routing and remote Access server</td>
<td>2</td>
</tr>
<tr>
<td>RA_Operations</td>
<td>3</td>
</tr>
<tr>
<td>Connections to other access servers</td>
<td>4</td>
</tr>
</tbody>
</table>

You need to enable the appropriate remote access for the members of the Managers and Operations groups while restricting remote access to all other users. What should you do?
A. Delete the Connections to other access servers policy.
B. Move the RA_Operations policy up so that it is the second policy in the order.
C. Re-create the Operations global group as a universal group.
D. Move the Connections to Microsoft Routing and Remote Access server policy up so that it is the first policy in the order.

**Answer: B**

Explanation: The remote access policies are processed in order. If a user meets a condition in a policy, the user is allowed or denied access according to that policy. No other policies are checked. The Connections to Microsoft Routing and Remote Access server policy is being processed before the RA-Operations policy. The users meet the condition in the Connections to Microsoft Routing and Remote Access server policy and are being denied access. The RA-Operations policy isn’t being checked. Therefore, we need to move the RA-Operations policy above the Connections to Microsoft Routing and Remote Access server policy.

Incorrect Answers:
* This policy is not preventing the remote access. The Connections to Microsoft Routing and Remote Access server policy is preventing the access.
* The global group is fine. Changing it will not help.
* The Connections to Microsoft Routing and Remote Access server policy is preventing the access. The RA-Operations policy is not being checked. Therefore, we need to move the RA-Operations policy above the Connections to Microsoft Routing and Remote Access server policy.

Reference:

**Question: 15**

You are a network administrator for your company. The network contains a perimeter network. The perimeter network contains four Windows Server 2003, Web Edition computers that are configured as a Network Load Balancing cluster. The cluster hosts an e-commerce Web site that must be available 24 hours per day. The cluster is located in a physically secure data center and uses an Internet-addressable virtual IP address. All servers in the cluster are configured with the Hisecws.inf template. You need to implement protective measures against the cluster's most significant security vulnerability. What should you do?

A. Use packet filtering on all inbound traffic to the cluster.
B. Use Security Configuration and Analysis regularly to compare the security settings on all servers in the cluster with the baseline settings
C. Use intrusion detection on the perimeter network.
D. Use Encrypting File System (EFS) for all files that contain confidential data stored on the cluster.

**Answer: A**

Explanation: The most sensitive element in this case is the network card that uses an Internet-addressable virtual IP address. The question doesn’t mention a firewall implementation or an intrusion detection system (Usually Hardware). Therefore, we should set up packet filtering. You
can configure packet filtering to accept or deny specific types of packets. Packet headers are examined for source and destination addresses, TCP and UDP port numbers, and other information.

Incorrect Answers:
* In the case of EFS, you can’t use it on cluster storage.
* Security Configuration and Analysis enables you to work with security templates in a database, where you can analyze them before applying them to your computers.
* IDS will (if properly maintained and updated with new signatures) look for certain activity on the network and check this against a signature database it carries. If a match occurs, then an alert is sent to an administrator or logged.

Reference:
Thank You for Trying Our Product

Microsoft

70-293

Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure Exam

TYPE: DEMO

http://www.examskey.com/70-293.html

View list of All certification exams:
http://www.examskey.com/all_certifications.php

- Average 100% Success Rate.
- 100% Money Back Guarantee
- Study Material Updated On Regular Basis.
- Instant Download Access! After Purchased
- Services Of Professional & Certified Experts Available Via Support
- Round-The-Clock Client Support, Safe Website For Shopping

Besides money back guarantee, we also offer 3 months free updates to the 70-293 exam questions to reflect the changes as (& if) they are introduced by the Microsoft.