70-299

Microsoft

Implementing and Administering Security in a Microsoft Windows 2003 Network

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 70-299 exam in first attempt and also get high scores to acquire Microsoft certification.

If you use OfficialCerts 70-299 Certification questions and answers, you will experience actual 70-299 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Microsoft exam prep covers over 95% of the questions and answers that may be appeared in your 70-299 exam. Every point from pass4sure 70-299 PDF, 70-299 review will help you take Microsoft 70-299 exam much easier and become Microsoft certified.

Here's what you can expect from the OfficialCerts Microsoft 70-299 course:

** Up-to-Date Microsoft 70-299 questions as experienced in the real exam.*
** 100% correct Microsoft 70-299 answers you simply can't find in other 70-299 courses.*
** All of our tests are easy to download. Your file will be saved as a 70-299 PDF.*
** Microsoft 70-299 brain dump free content featuring the real 70-299 test questions.*

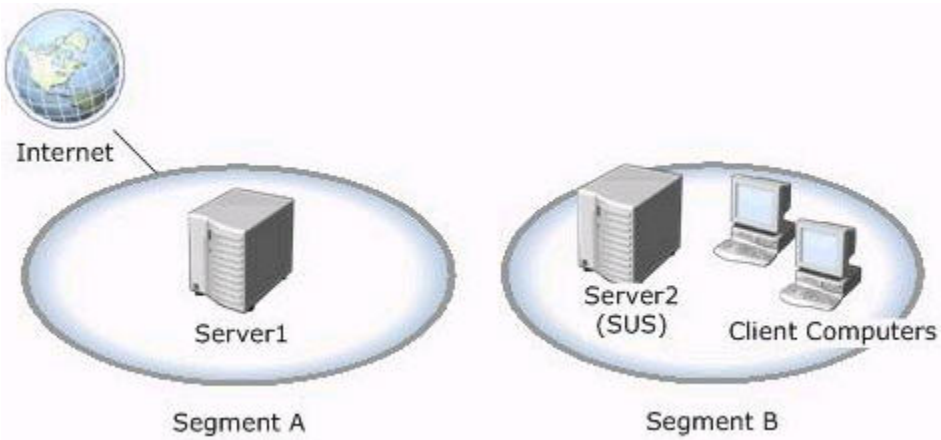
Microsoft 70-299 certification exam is of core importance both in your Professional life and Microsoft certification path. With Microsoft certification you can get a good job easily in the market and get on your path for success. Professionals who passed Microsoft 70-299 exam training are an absolute favorite in the industry.
You will pass Microsoft 70-299 certification test and career opportunities will be open for you.

http://news.ift.org/?newsid=exams.asp?examcode=70-299

A	Implementing, Managing, and Troubleshooting Security Policies
B	Implementing, Managing, and Troubleshooting Patch Management Infrastructure
C	Implementing, Managing, and Troubleshooting Security for Network Communications
D	Planning, Configuring, and Troubleshooting Authentication, Authorization, and PKI

Relevant objective of each question is mentioned along with question number.

Question: 1. (C)
You are the security administrator for Company. The network consists of two segments named Segment A and Segment B. The client computers on the network run Windows XP Professional. The servers run Windows Server 2003. Segment A contains a single server named Server1. Segment B contains all other computers, including a server named Server2. Company's written security policy states that Segment B must not be connected to the Internet. Segment A is allowed to connect to the Internet. There is no network connection between Segment A and Segment B. You can copy files from Segment A to Segment B only by using a CD-ROM to transport the files between the two segments. The network topology is displayed in the exhibit.



You are planning a patch management infrastructure. On Segment B, you install Software Update Services (SUS) on Server2. You configure Automatic Updates on all computers in Segment B to use http://Server2 and to install security patches. You need to ensure that all computers in Segment B automatically install security patches. What should you do?

A. Install SUS on Server1.
Periodically copy the files in the Content folder and in the SUS root folder from Server1 to Server2.
B. Install SUS on Server1.
Periodically copy the files in the Content folder from Server1 to Server2. Copy the Approveditems.txt file from Server1 to the Windows folder on Server2.
C. On Server1, periodically connect to the Microsoft Windows Update Catalog Web site and download new security patches. Copy the files to the Content folder on Server2.
D. On Server1, configure Automatic Updates to use the URL of the Microsoft Windows Update Web site. Periodically copy the downloaded files and the Mssecure.xml file to the Content folder on Server2.

Answer: A

Explanation:
B – You must copy all items in the Content and SUS root folder.
C – This is possible, but you would have to install the patches manually.
D – Turning on AU would update Server1 does not provide files for Server2. The MBSA uses an XML-based catalog file, MSSecure.xml, to determine the security updates that are available. The catalog file is compressed and is stored in the MSSecure.cab file.
If SUS is used to approve updates, it retrieves the Approveditems.txt file from the root of the IIS/SUS default website (http://server2) not the Windows folder.
If you do not install SUS on Server1 there will be no Content folder (distribution point) on Server1.

Automatic Updates should not be turned on, on the SUS servers.
SUS is a server component that, when installed on a server running Windows 2000, allows small and medium enterprises to bring critical updates from Windows Update inside their firewalls to distribute to Windows 2000 and Windows XP computers. The same Automatic Updates component that can direct Windows 2000 and Windows XP computers to Windows Update can be directed to a SUS server inside your firewall to install critical updates.
Automatic Updates retrieves all critical updates and Microsoft Security Response Center security updates that are classified as moderate or important.
Automatic Updates scans only for critical updates, but if its server that runs SUS contains updates other than critical ones, Automatic Updates receives and applies those as well. SUS receives critical and moderate security updates.
Creating Distribution Points When you install a server that runs SUS, a distribution point is created on that server. When you synchronize the server with a parent server or with an external Web site, all the content on the Web site is downloaded to the distribution point. If new updates are downloaded, this distribution point is updated during every synchronization. During Setup, the distribution point is created in a virtual root (Vroot) named /Content.
If you choose to maintain content on the public Web site instead of downloading the patches to the local server running SUS, this distribution point is empty except for the AUCatalog.cab file. AUCatalog.cab defines the updates that have been approved for deployment to clients.
You can also create a distribution point on a server that is not running SUS. Such a server must be running IIS 5.0 or later. You can download and test packages on servers running SUS, and then download approved and tested packages to distribution points for client access.
If your SUS design includes distribution points, perform the following tasks to create a distribution point:
1. Confirm that IIS is present.
2. Create a folder named \Content.
3. Copy all of the following items from the source server running SUS to the newly created \Content folder:
• <root of the SUS Web site>\Aucatalog1.cab
• <root of the SUS Web site>\Aurtf1.cab
• <root of the SUS Web site>\approveditems.txt
• All the files and folders under the \Content\cabs
4. Create an IIS Vroot called http://<Servername>/Content that points to the \content folder.

Question: 2. (B)
You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. All servers run Windows Server 2003. Company's written security policy states that security patches must be manually installed on servers by administrators. You need to configure the network to comply with the written security policy. You need to maintain security patches by using the minimum amount of administrative effort. What should you do?

A. Create a new organizational unit (OU) to contain all server computers.
Create a new Group Policy object (GPO) and link it to the OU. Configure the GPO to disable Automatic Updates. Allow only administrators to start Automatic Updates.
B. Create a new organizational unit (OU) to contain all server computers. Create a new Group Policy object (GPO) and link it to the OU. Configure the GPO to automatically download updates and notify when they are ready to be installed.
C. Create a new organizational unit (OU) named Admins to contain all administrators.
Create a second OU named Servers to contain all server computers. Create a new
Group Policy object (GPO) and link it to the Admins OU. Configure the GPO to disable Automatic Updates.
D. Modify the Default Domain Policy Group Policy object (GPO) to disable Windows

Update and to disable Automatic Updates. Create a new organizational unit (OU) named Admins. Place all administrator accounts in the Admins OU. Block GPO inheritance on the Admins OU.

Answer: B

Explanation:
A – Cannot be done using Network Neighborhood.
C – Scanning the finance subnet would report on all computers on the subnet, including non-finance computers.
D – This option again would scan all systems in the domain, not just the finance once. The scan should be done from an administrative machine, not a users' machine.
Objective: Implementing, Managing, and Troubleshooting Security for Network Communications
Sub-Objective: 3.4.1 Monitor IPSec policies by using IP Security Monitor.
1. Planning a Host Name Resolution Strategy MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7,
The correct syntax is mbsacli /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses.
The mbsacli /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names.
The mbsacli /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned.
http://support.microsoft.com/default.aspx?scid=KB;EN-US;Q320454&ID=KB;EN-US;Q320454&&FR=1
Switches available with /hf flag
mbsacli /hf [-h hostmane] [-fh filename] [-i ipaddress] [-fip filename] [-r ipaddressrange] [-d domainname] [-n]
[-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc]
[-o option] [-f filename] [-unicode] [-t] [-u username] [-p password] [-x] [-?]
To Select Which Computer to Scan
-h hostname - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (,).
-fh filename - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the .txt file, to a maximum of 256 names.
-i xxx.xxx.xxx.xxx - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma.
-fip filename - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the .txt file, with a maximum of 256 IP addresses.
-r xxx.xxx.xxx.xxx - xxx.xxx.xxx.xxx - Scans a specified range of IP addresses.
Note You can use the previous switches in combination. For example, you can use a command-line with the following format:mbsacli /hf –h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz
-d domainname - Scans a specified domain.
-n - Scans all the computers on the local network. All computers from all domains in Network Neighborhood (or My Network Places) are scanned

Question: 3. (B)
You are a security administrator for Company. The network consists of a single Active Directory domain named Company.com. The Company.com Active Directory domain contains 150 Windows Server 2003 computers and 7,500 Windows XP Professional client computers. The network is made up of 64 class C IP subnets t hat range from 172.16.0.0 through 172.16.63.0.

The finance department uses 135 computers on the 172.16.9.0 /24 IP subnet. This subnet also contains computers that belong to other departments in the company. All finance department computers are members of the Company.com Active Directory domain. You need to produce a report that identifies which Microsoft security patches are not installed on the computers in the finance department. The report must contain information about only the finance department computers. You want to achieve this goal by using the minimum amount of administrative effort. What should you do?

A. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Network Neighborhood.
B. Run Mbsacli.exe on a finance department computer with the option to scan computers by using a list of individual IP addresses on the finance department computers.
C. Run Mbsacli.exe on a finance department computer with the option to scan computers on the finance department IP subnet.
D. Run Mbsacli.exe on a finance department computer with the option to scan computers in the Company.com Active Directory domain.

Answer: B

Explanation:
Since there are non-accounting computers on the subnet, the scan needs to be performed by individual IP. Objective: Implementing, Managing, and Troubleshooting Security for Network Communications Sub-Objective: 3.4.1 Monitor IPSec policies by using IP Security Monitor.

1. Planning a Host Name Resolution Strategy

MCSA/MCSE Self-Paced Training Kit (Exams 70-292 and 70-296): Upgrading Your
Certification to Microsoft Windows Server 2003, Microsoft Press Chapter 7,
The correct syntax is mbsacli /hf -fh hosts.txt. The -fh flag causes the tool to scan the NetBIOS computer names specified in the named text file. You must specify one computer name on each line in the .txt file, up to a maximum of 256 names. You should not use the mbsacli /hf -i hosts.txt syntax. The -i flag is used to scan one or more Internet Protocol (IP) addresses. You should not use the mbsacli /hf -r hosts.txt syntax. The -r flag is used to specify a range of IP addresses to be scanned. Switches available with /hf flag mbsacli /hf [-h hostmane] [-fh filename] [-i ipaddress] [-fip filename] [-r ipaddressrange] [-d domainname] [-n] [-sus SUS server|SUS filename] [-b] [-fq filename] [-s 1] [-s 2] [-nosum] [-sum] [-z] [-v] [-history level] [-nvc] [-o option] [-f filename] [-unicode] [-t] [-u username] [-p password] [-x] [-?] To Select Which Computer to Scan -h hostname - Scans the named NetBIOS computer name. The default location is the local host. To scan multiple hosts, separate the host names with a comma (,). -fh filename - Scans the NetBIOS computer names that are specified in the text file that you named. Specify one computer name on each line in the .txt file, to a maximum of 256 names. -i xxx.xxx.xxx.xxx - Scans the named IP address. To scan multiple IP addresses, separate each IP address with a comma. -fip filename - Scans the IP addresses that you specified in the text file that you named. Specify one IP address on each line in the .txt file, with a maximum of 256 IP addresses. -r xxx.xxx.xxx.xxx xxx.xxx.xxx.xxx - Scans a specified range of IP addresses. Note You can use the previous switches in combination. For example, you can use a command-line with the following format:mbsacli /hf –h hostname1,hostname2 -i xxx.xxx.xxx.xxx -fip ipaddresses.txt -r yyy.yyy.yyy.yyy-zzz.zzz.zzz.zzz -d domainname - Scans a specified domain. -n - Scans all the computers on the local network. All computers from all domains in Network Neighborhood
(or My Network Places) are scanned

Reference:
Microsoft Baseline Security Analyzer (MBSA) version 1.2 is available, Microsoft Knowledge Base Article – 320454

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google