70-646 Q&As

Pro: Windows Server 2008

Pass Microsoft 70-646 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/70-646.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your network consists of an Active Directory domain. The domain controllers run Windows Server

2008 R2. Client computers run Windows 7.

You need to implement Encrypting File System (EFS) for all client computers.

You want to achieve this goal while meeting the following requirements:

- You must minimize the amount of data that is transferred across the network when a user logs on to or off from a client computer.

-Users must be able to access their EFS certificates on any client computers.

-

If a client computer\\'s disk fails, EFS certificates must be accessible. What should you do?

A.

Enable credential roaming.

B.

Enable roaming user profiles.

C.

Enable a Data Recovery Agent.

D.

Issue smart cards to all users.

Correct Answer: A

Configuring Credential Roaming

Credential roaming allows for the storage of certificates and private keys within Active Directory.

For example, a user\\'s encrypting file system certificate can be stored in Active Directory and provided to the user when she logs on to different computers within the domain. The same EFS certificate will always be used to encrypt files.

This means that the user can encrypt files on an NTFS-formatted USB storage device on one computer and then decrypt them on another, because the EFS certificate will be transferred to the second computer\\'s certificate store during the

logon process.Credential roaming also allows for all of a user\\'s certificates and keys to be removed when he logs off of the computer.

Credential roaming is enabled through the Certificate Services Client policy, located under User Configuration\Policies\Windows Settings\Security Settings\Public Key Policies and shown in

Figure 10-4.

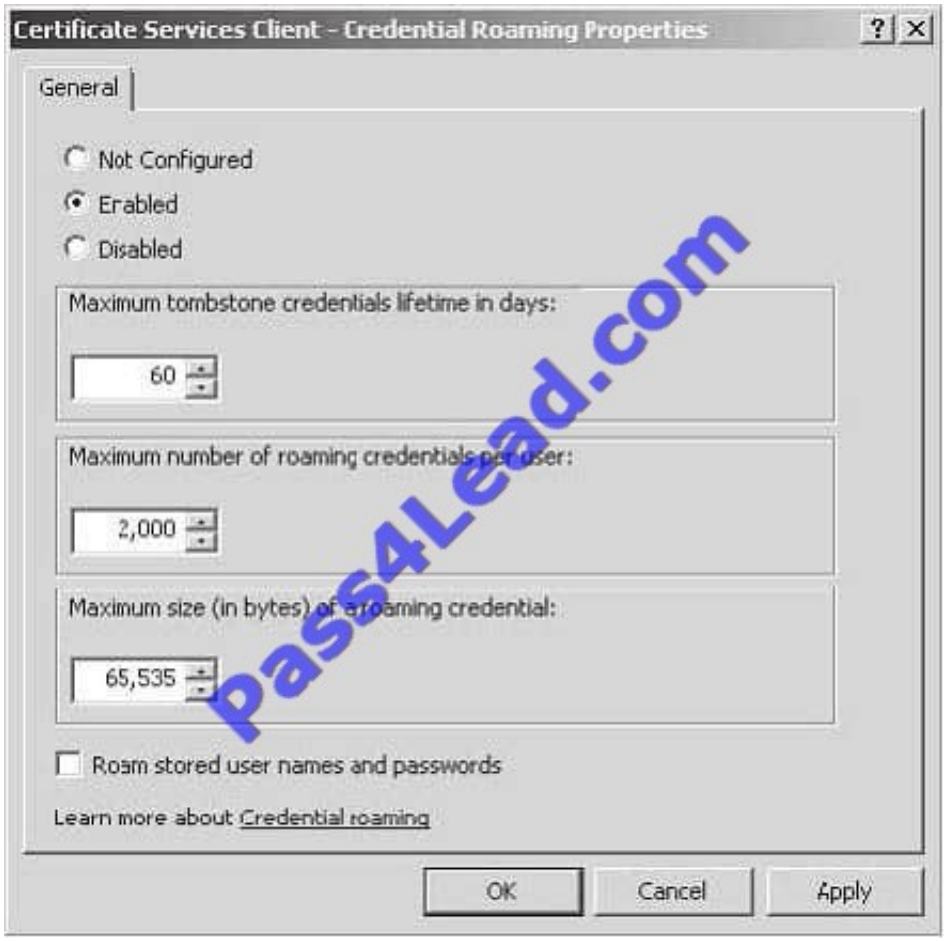

Figure 10-4Credential Roaming Policy

Credential roaming works in the following manner. When a user logs on to a client computer in a domain where the Credential Roaming Policy has been enabled, the certificates in the user\\'s store on the client computer are compared to

certificates stored for the user within Active Directory.

If the certificates in the user\\'s certificate store are up to date, no further action is taken.

If more recent certificates for the user are stored in Active Directory, these credentials are copied to the client computer.

If more recent certificates are located in the user\\'s store, the certificates stored in Active Directory are updated.

Credential roaming synchronizes and resolves any conflicts between certificates and private keys from any number of client computers that a user logs on to, as well as certificates and private keys stored within Active Directory. Credential

roaming is triggered whenever a private key or certificate in the local certificate store changes, whenever the user locks or unlocks a computer, and whenever Group Policy refreshes. Credential roaming is supported on Windows Vista,

Windows Server 2008, Windows XP SP2, and Windows Server 2003

SP1.

MORE INFO More on credential roaming

For more information on configuring credential roaming, consult the following TechNet

link:http://technet2.microsoft.com/windowsserver2008/en/library/fabc1c44-f2a2-43e1-b52e-9b12a1f19a331033.mspx?mfr=true

QUESTION 2

Which NAP enforcement method should you recommend?

A. 802.1x

B. DHCP

C. IPSec

D. VPN

Correct Answer: C

Requirements/information:

Implement Network Access Protection (NAP) for all of the client computers on the internal network and for all of the client computers that connect remotely

Some users work remotely. To access the company\\'s internal resources, the remote users use a VPN connection to NPAS1.

The network contains network switches and wireless access points (WAPs) from multiple vendors Some of the network devices are more than 10 years old and do not support portbased authentication.

Network Access Protection (NAP) is a feature in Windows Server 2008 that controls access to network resources based on a client computer\\'s identity and compliance with corporate

governance policy. NAP allows network administrators to define granular levels of network access based on who a client is, the groups to which the client belongs, and the degree to which that client is compliant with corporate governance

policy. If a client is not compliant, NAP provides a mechanism to automatically bring the client back into compliance and then dynamically increase its level of network access.

NAP Enforcement Methods

When a computer is found to be noncompliant with the enforced health policy, NAPenforces limited network access. This is done through an Enforcement Client (EC). Windows Vista,

Windows XP Service Pack 3, and Windows Server 2008 include NAPEC support for IPsec, IEEE 802.1X, Remote Access VPN, and DHCP enforcement methods. Windows Vista and Windows Server 2008 also support NAP enforcement for

Terminal Server Gateway connections.

NAP enforcement methods can either be used individually or can be used in conjunction with each other to limit the network access of computers that are found not to be in compliance with configured health policies. Hence you can apply the

remote access VPN and IPsec enforcement methods to ensure that internal clients and clients coming in from the Internet are only granted access to resources if they meet the appropriate client health benchmarks.

802.1X step-by-step guide.

http://www.microsoft.com/downloads/en/details.aspx?FamilyID=8a0925ee-ee06-4dfbbba2-07605eff0608anddisplaylang=en

802. 802.1X Enforcement

When 802.1X is used--over either wired or wireless networks--the client device\\'s access is restricted by network infrastructure devices such as wireless connection points and switches. Until the device has demonstrated its compliance, client

access is restricted.

Restriction is enforced on the network access device using an access control list (ACL) or by placing the client device on restricted virtual local area networks (VLANs). The 802.1X standard is more complex to deploy than DHCP, but it

provides a high degree of protection.

as a requirement of 802.1 is port authentication and some of the devices ate 10+ years old and do not support this then then this rules out this method

IPSEC ENFORCEMENT

IPsec enforcement works by applying IPsec rules. Only computers that meet health compliance requirements are able to communicate with each other. IPsec enforcement can be applied on a per-IP address, per-TCP port number, or per-

UDP port number basis. For example: You can use IPsec enforcement to block RDP access to a web server so that only computers that are healthy can connect to manage that server but allow clients that do not meet health requirements to

connect to view Web pages hosted by the same web server.

IPsec is the strongest method of limiting network access communication through NAP. Where it might be possible to subvert other methods by applying static addresses or switching ports, the IPsec certificate used for encryption can be

obtained by a host only when it passes the health check. No IPsec certificate means that communication with other hosts that encrypt their communications using a certificate issued from the same CA is impossible.

VPN Enforcemement

VPN enforcement is used on connecting VPN clients as a method of ensuring that clients granted access to the internal network meet system health compliance requirements. VPN enforcement works by restricting network access to

noncompliant clients through the use of packet filters.

Rather than being able to access the entire network, incoming VPN clients that are noncompliant have access only to the remediation server group.

As is the case with 802.1X enforcement, the health status of a connected client is monitored continuously. If a client becomes noncompliant, packet filters restricting network access will be applied. If a noncompliant client becomes compliant,

packet filters restricting network access will be removed. VPN enforcement requires an existing remote access infrastructure and an NPS server. The enforcement method uses the VPN EC, which is included with Windows 7, Windows Vista,

Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

DHCP NAP Enforcement

DHCP NAP enforcement works by providing unlimited-access IPv4 address information to compliant computers and limited-access IPv4 address information to noncompliant computers.

Unlike VPN and 802.1X enforcement methods, DHCP NAP enforcement is applied only when a client lease is obtained or renewed. Organizations using this method of NAP enforcement should avoid configuring long DHCP leases because

this will reduce the frequency at which compliance checks are made.

To deploy DHCP NAP enforcement, you must use a DHCP server running Windows Server 2008 or Windows Server 2008 R2 because this includes the DHCP Enforcement Service (ES). The DHCP EC is included in the DHCP Client service

on Windows 7, Windows Vista, Windows Server 2008, Windows Server 2008 R2, and Windows XP SP3.

The drawback of DHCP NAP enforcement is that you can get around it by configuring a client\\'s IP address statically. Only users with local administrator access can configure a manual IP, but if your organization gives users local administrator

access, DHCP NAP enforcement may not be the most effective method of keeping these computers off the network until they are compliant.

QUESTION 3

You need to recommend a strategy for managing Windows Firewall that meets the company\\'s technical requirements. What should you include in the recommendation?

A. domain-based Group Policy objects (GPOs)

B. local Group Policy objects (GPOs)

C. Starter Group Policy objects (GPOs)

D. System Starter Group Policy objects (GPOs)

Correct Answer: A

http://technet.microsoft.com/en-us/library/ee461027.aspx The Windows PowerShell command-line and scripting language can be used to automate many Group Policy tasks, including configuring registry-based policy settings and various Group Policy Management Console (GPMC) tasks. To help

you perform these tasks, the Group Policy module for Windows PowerShell provides the cmdlets covered in this section. You can use these Group Policy cmdlets to perform the following tasks for domain-based Group Policy objects (GPOs): Maintain GPOs: GPO creation, removal, backup, reporting, and import.

Associate GPOs with Active Directory Directory Services (AD DS) containers: Group Policy link creation, update, and removal.

Set inheritance and permissions on AD DS organizational units (OUs) and domains.

Configure registry-based policy settings and Group Policy Preferences Registry settings.

Topic 11, Fabrikam Inc Scenario COMPANY OVERVIEW Fabrikam Inc. is a manufacturing company that has a main office and a branch office. PLANNED CHANGES You plan to deploy a failover cluster named Cluster1 in the branch

office. Cluster1 will be configured to meet the following requirements:

-

The cluster will host eight virtual machines (VMs).

-

The cluster will consist of two nodes named Node1 and Node2.

-

The quorum mode for the cluster will be set to Node and Disk Majority.

-A user named Admin1 will configure the virtual switch configuration of the VMs.

-The cluster nodes will use shared storage on an iSCSI Storage Area Network (SAN).

You plan to configure a VM named File2 as a file server. Users will store confidential files on File2.

You plan to deploy a Microsoft Forefront Threat Management Gateway (TMG) server in each site.

The Forefront TMG server will be configured as a Web proxy.

EXISTING ENVIRONMENT

The research department is located in the branch office. Research users frequently travel to the main office.

Existing Active Directory/Directory Services

The network contains a single-domain Active Directory forest named fabrikam.com. The functional level of the forest is Windows Server 2008.

The relevant organizational units (OUs) for the domain are configured as shown in the following

table.

OU name	OU description
Main Office Users	Users in the main office
Main Office Computers	Computers in the main office
Main Office Servers	Servers in the main office
Branch Office Users	Users in the branch office
Branch Office Computers	Computers in the branch office
Branch Office Servers	Servers in the branch office
Domain Controllers	Domain controllers

The relevant sites for the network are configured shown in the following table.

Active Directory site name	Site description
MainOfficeSite	Main office
BranchOfficeSite	Branch office

The relevant group policy objects (GPOs) are configured as shown in the following table.

GPO name	Linked to
Default Domain Policy	Fabrikam.com domain
Default Domain Controllers Policy	Domain Controllers OU
GPO1	Fabrikam.com domain
GPO2	Main Office Computers OU
GPO3	Branch Office Computers OU
GPO4	MainOfficeSite site
GPO5	BranchOfficeSite site

Existing Network Infrastructure

All users run windows server 2008 R2. The relevant servers are configured as shown in following table.

Server name	Role service	Server site
File1	File Services	MainOfficeSite
DC1	Active Directory Domain Services (AD DS)	MainOfficeSite
DC2	Active Directory Domain Services (AD DS)	MainOfficeSite
WSUS1	Windows Server Update Services (WSUS)	MainOfficeSite
WSUS2	Windows Server Update Services (WSUS)	MainOfficeSite

WSUS2 is configured as a downstream replica server.

File1 contains a share named Templates. Users access the Templates share by using the path \\fabrikam.com\dfs\templates.

File1 has the Distributed File System (DFS) Replication role service and the DFS Namespaces role service installed.

TECHNICAL REQUIREMENTS

-Fabrikam must meet the following requirements:

-

Minimize the cost of IT purchases.

-

Minimize the potential attack surface on the servers.

-

Minimize the number of rights assigned to administrators.

-

Minimize the number of updates that must be installed on the servers.

-

Ensure that Internet Explorer uses the local ForeFront TMG server to connect to the Internet.

-

Ensure that all client computers continue to receive updates from WSUS if a WSUS server fails.

-Prevent unauthorized users from accessing the data stored on the VMs by making offline copies of the VM files.

Fabrikam must meet the following requirements for the Templates share:

-Ensure that users access the files in the Templates share from a server in their local site.

- Ensure that users always use the same UNC path to access the Templates share, regardless of the site in which the users are located.

QUESTION 4

You need to recommend a solution for the file servers that meets the company\\'s technical requirements. What should you include in the recommendation?

A. Storage Manager for SANs

B. Network Load Balancing (NLB)

C. TCP/IP offload services

D. the Multipath I/O feature

Correct Answer: D

Multipath I/O Multipath I/O (MPIO) is a feature of Windows Server 2008 that allows a server to use multiple data paths to a storage device. This increases the availability of storage resources because it provides alternate paths from a server or cluster to a storage subsystem in the event of path failure. MPIO uses redundant physical path components (adapters, switches, cabling) to create separate paths between the server or cluster and the storage device. If one of the devices in these separate paths fails, an alternate path to the SAN device will be used, ensuring that the server is still able to access critical data. You configure failover times through the Microsoft iSCSI Software initiator driver or by modifying the Fibre Channel HBA driver parameter settings, depending on the SAN technology deployed in your environment.

QUESTION 5

Your network consists of a single Active Directory domain. Your network contains 10 servers and 500 client computers. All domain controllers run Windows Server 2008 R2.

A Windows Server 2008 R2 server has Remote Desktop Services installed. All client computers run Windows XP Service Pack 3.

You plan to deploy a new line of business Application. The Application requires desktop themes to be enabled.

You need to recommend a deployment strategy that meets the following requirements:

-Only authorized users must be allowed to access the Application.

-Authorized users must be able to access the Application from any client computer.

-

Your strategy must minimize changes to the client computers.

-

Your strategy must minimize software costs. What should you recommend?

A.

Migrate all client computers to Windows 7. Deploy the Application to all client computers by using a Group Policy object (GPO).

B.

Migrate all client computers to Windows 7. Deploy the Application to the authorized users by using a Group Policy object (GPO).

C.

Deploy the Remote Desktop Connection (RDC) 7.0 software to the client computers. Install the Application on the Remote Desktop Services server. Implement Remote Desktop Connection Broker (RD Connection Broker).

D.

Deploy the Remote Desktop Connection (RDC) 7.0 software to the client computers. Enable the Desktop Experience feature on the Remote Desktop Services server. Install the Application on the Remote Desktop Services server.

Correct Answer: D

Desktop Experience

Configuring a Windows Server 2008 server as a terminal server lets you use Remote Desktop Connection 6.0 to connect to a remote computer from your administrator workstation and reproduces on your computer the desktop that exists on the remote computer. When you install Desktop Experience on Windows Server 2008, you can use Windows Vista features such as Windows Media Player, desktop themes, and photo management within the remote connection.

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try 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 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications.
You can view Vendor list of All Certification Exams offered:

https://www.pass4lead.com/allproducts

Need Help

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