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

You need to recommend changes to the DFS infrastructure that meet the company\\'s security requirements. What should you recommend?

A. Modify the NTFS permissions and the share permissions of the DFS targets.

B. Modify the referrals settings of the DFS namespace and the NTFS permissions of the DFS targets.

C. Migrate the namespace to Windows Server 2008 mode and modify the referrals settings.

D. Migrate the namespace to Windows Server 2008 mode and enable accessbased enumeration (ABE).

Correct Answer: D

ABE is enabled by default and lets you hide files and folders from users who do not have access to them.

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 using managed service accounts on the Web servers.

How many managed service accounts should you recommend?

A. 1

B. 2

C. 3

D. 5

Correct Answer: D

There are 5 web servers in total, 3 in the forest root domain and 1 in each child domain. Q 9 in this exam actually confirms the answer is 5 Service Account Vulnerability The practice of configuring services to use domain accounts for

authentication leads to potential security exposure. The degree of risk exposure is dependent on various factors, including:

The number of servers that have services that are configured to use service accounts. The vulnerability profile of a network increases for every server that has domain account authenticated services that run on that server. The existence of

each such server increases the odds that an attacker might compromise that server, which can be used to escalate privileges to other resources on a network.

The scope of privileges for any given domain account that services use. The larger the scope of privileges that a service account has, the greater the number of resources that can be

compromised by that account.

Domain administrator level privileges are a particularly high risk, because the scope of vulnerability for such accounts includes any computer on the network, including the domain

controllers. Because such accounts have administrative privileges to all member servers, the compromise of such an account would be severe and all computers and data in the domain would be suspect.

The number of services configured to use domain accounts on any given server. Some services have unique vulnerabilities, which make them somewhat more susceptible to attacks. Attackers will usually attempt to exploit known

vulnerabilities first. Use of a domain account by a vulnerable service presents an escalated risk to other systems, which could have otherwise been isolated to a single server.

The number of domain accounts that are used to run services in a domain. Monitoring and managing the security of service accounts requires more diligence than ordinary user accounts, and each additional domain account in use by

services only complicates administration of those accounts. Given that administrators and security administrators need to know where each service account is used to detect suspicious activity highlights

The need to minimize the number of those accounts.

The preceding factors lead to several possible vulnerability scenarios that can exist, each with a different level of potential security risk. The following diagram and table describe these scenarios.

For these examples it is assumed that the service accounts are domain accounts and each account has at least one service on each server using it for authentication. The following

information describes the domain accounts shown in the following figure.

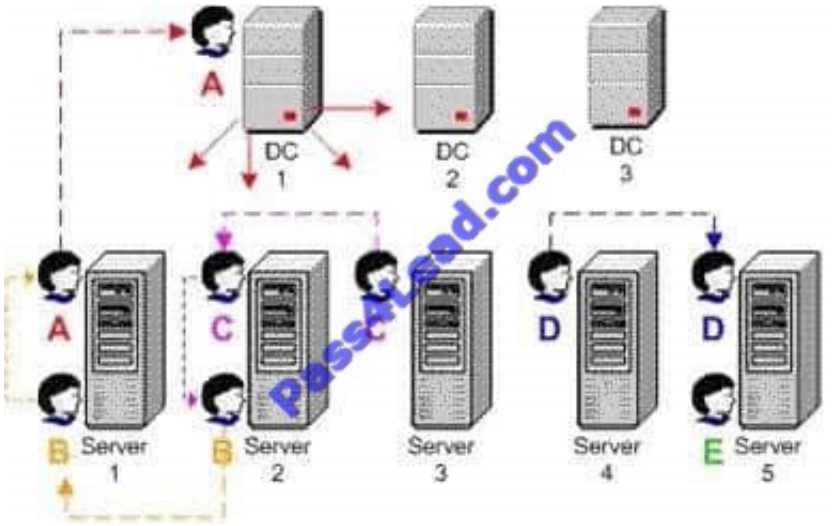
Account A has Administrator-equivalent privileges to more than one domain controller.

Account B has administrator-equivalent privileges on all member servers.

Account C has Administrator-equivalent privileges on servers 2 and 3.

Account D has Administrator-equivalent privileges on servers 4 and 5.

Account E has Administrator-equivalent privileges on a single member server only.



QUESTION 4

You need to recommend changes to the intranet site that meet the company\\'s technical requirements. What should you include in the recommendation?

A. additional Application pools

B. additional worker processes

C. Failover Clustering

D. Network Load Balancing (NLB)

Correct Answer: D

http://technet.microsoft.com/en-us/library/cc725691.aspx

The Network Load Balancing (NLB) feature in Windows Server 2008 R2 enhances the availability and scalability of Internet server applications such as those used on Web, FTP, firewall, proxy, virtual private network (VPN), and other mission-critical servers. A single computer running Windows Server 2008 R2 provides a limited level of server reliability and scalable performance.

However, by combining the resources of two or more computers running one of the products in Windows Server 2008 R2 into a single virtual cluster, NLB can deliver the reliability and performance that Web servers and other mission-critical servers need.

QUESTION 5

You need to recommend a solution for deploying the custom Word dictionary. What should you include in the recommendation?

A. Distributed File System (DFS)

B. Group Policy preferences

C. Offline servicing

D. WDS

Correct Answer: B

http://support.microsoft.com/kb/943729

This article discusses the Group Policy preferences that are new in Windows Server 2008 and how to enable down-level computers to process these new items. Group Policy preferences are made up of more than 20 new Group Policy client-side extensions (CSEs) that expand the range of configurable settings in a Group Policy object (GPO). These new preference extensions are included in the Group Policy Management Editor window of the Group Policy Management Console (GPMC). The kinds of preference items that can be created by using each extension are listed when New is selected for the extension. Examples of the new Group Policy preference extensions include the following:

Folder Options Drive Maps Printers Scheduled Tasks Services Start Menu

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: