70-646$^{\text{Q\&As}}$

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 are designing a Windows Server 2008 R2 deployment strategy for the Austin campus servers.

Which deployment strategy should you recommend?

A. Enable an Auto-Add Policy in WDS.

B. Create a discover image in WDS.

C. Deploy the images by using multicast transmission in WDS.

D. Deploy the images by using unicast transmission in WDS.

Correct Answer: C

Topic 19, Tailspin Toys

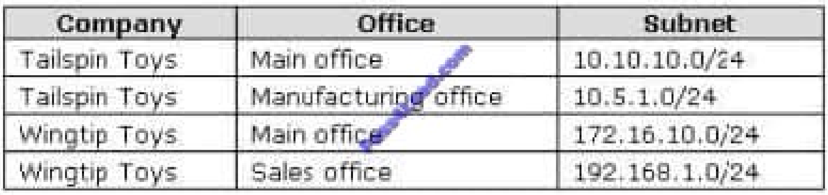
Scenario

General Background

You are the Windows server administrator for Tailspin Toys. Tailspin Toys has a main office and a manufacturing office.

Tailspin Toys recently acquired Wingtip Toys and is in the beginning stages of merging the IT environments. Wingtip Toys has a main office and a sales office.

Technical Backgroundthe companies use the network subnets indicated in the following table.

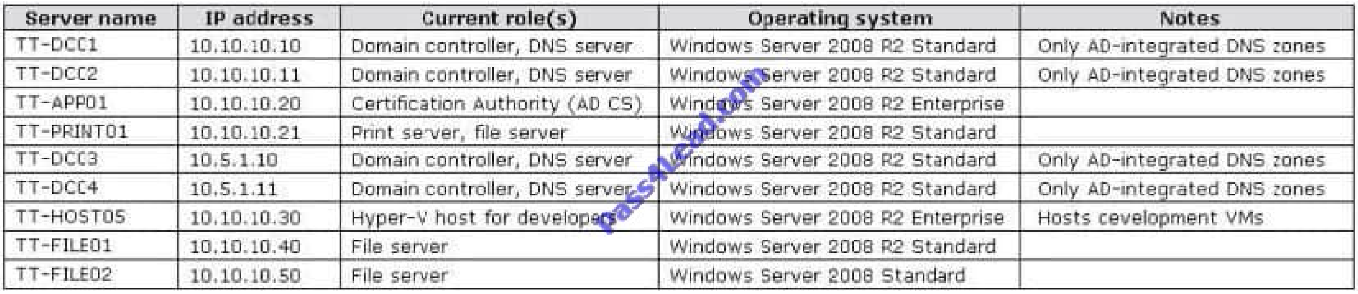


Company	Office	Subnet
Tailspin Toys	Main office	10.10.10.0/24
Tailspin Toys	Manufacturing office	10.5.1.0/24
Wingtip Toys	Main office	172.16.10.0/24
Wingtip Toys	Sales office	192.168.1.0/24

The Tailspin Toys network and the Wingtip Toys network are connected by a point-to-point dedicated 45 Mbps circuit that terminates in the main offices.

Tailspin toys

The current Tailspin Toys server topology is shown in the following table.



Server name	IP address	Current role(s)	Operating system	Notes
TT-DCC1	10.10.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DCC2	10.10.10.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-APP01	10.10.10.20	Certification Authority (AD CS)	Windows Server 2008 R2 Enterprise	
TT-PRINT01	10.10.10.21	Print server, file server	Windows Server 2008 R2 Standard	
TT-DCC3	10.5.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DCC4	10.5.1.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-HOST05	10.10.10.30	Hyper-V host for developers	Windows Server 2008 R2 Enterprise	Hosts cevelopment VMs
TT-FILE01	10.10.10.40	File server	Windows Server 2008 R2 Standard	
TT-FILE02	10.10.10.50	File server	Windows Server 2008 Standard	

The Tailspin Toys environment has the following characteristics:

-All servers are joined to the tailspintoys.com domain.

-In the Default Domain Policy, the Retain old events Group Policy setting is enabled.

-

An Active Directory security group named "Windows system administrators" is used to control all files and folders on TT-PRINT01.

-

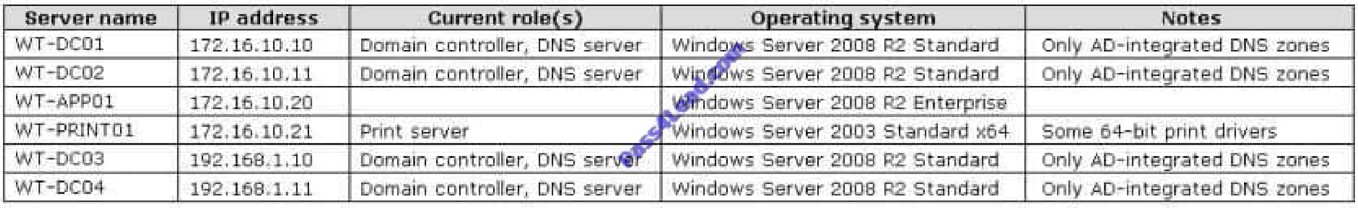
A Tailspin Toys administrator named Marc has been delegated rights to multiple organizational units (OUs) and object in the tailspintoys.com domain.

-

Tailspin Toys developers use Hyper-V virtual machines (VMs) for development. There are 20 development VMs named TT-DEV01 through TT-DEV20.

Wingtip Toys

The current Wingtip Toys server topology is shown in the following table.



Server name	IP address	Current role(s)	Operating system	Notes
WT-DC01	172.16.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-DC02	172.16.10.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-APP01	172.16.10.20		Windows Server 2008 R2 Enterprise	
WT-PRINT01	172.16.10.21	Print server	Windows Server 2003 Standard x64	Some 64-bit print drivers
WT-DC03	192.168.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
WT-DC04	192.168.1.11	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones

All servers in the Wingtip Toys environment are joined to the wingtiptoys.com domain.

Infrastructure Services

You must ensure that the following infrastructure services requirements are met:

-All domain zones must be stored as Active Directory-integrated zones.

-

Only DNS servers located in the Tailspin Toys main office may communicate with DNS servers at Wingtip Toys.

-

Only DNS servers located in the Wingtip Toys main office may communicate with DNS servers at Tailspin Toys.

-

All tailspintoys.com resources must be resolved from the Wingtip Toys offices.

-

All wingtiptoys.com resources must be resolved from the Tailspin Toys offices.

-Certificates must be distributed automatically to all Tailspin Toys and Wingtip Toys computers.

Delegated Administration

You must ensure that the following delegated administration requirements are met:

-

Tailspin Toys IT security administrators must be able to create, modify, and delete user objects in the wingtiptoys.com domain.

-

Members of the Domain Admins group in the tailspintoys.com domain must have full access to the wingtiptoys.com Active Directory environment.

-A delegation policy must grant minimum access rights and simplify the process of delegating rights.

-Minimum permissions must always be delegated to ensure that the least privilege is granted for a job or task.

-

Members of the TAILSPINTOYS\Helpdesk group must be able to update drivers and add printer ports on TT-PRINT01.

-

Members of the TAILSPINTOYS\Helpdesk group must not be able to cancel a print job on TT-PRINT01.

-Tailspin Toys developers must be able to start, stop, and Apply snapshots to their development VMs.

IT Security

You must ensure that the following IT security requirements are met:

- Server security must be automated to ensure that newly deployed servers automatically have the same security configuration as existing servers.

-Auditing must be configured to ensure that the deletion of user objects and OUs is logged.

- Microsoft Word and Microsoft Excel files must be automatically encrypted when uploaded to the Confidential document library on the Tailspin Toys Microsoft SharePoint site.

-Multifactor authentication must control access to Tailspin Toys domain controllers.

-

All file and folder auditing must capture the reason for access.

-

All folder auditing must capture all delete actions for all existing folders and newly created folders.

-New events must be written to the Security event log in the tailspintoys.com domain and retained indefinitely.

-Drive X:\ on TT-FILE01 must be encrypted by using Windows BitLocker Drive Encryption and must automatically unlock.

QUESTION 2

A company has a single Active Directory Domain Services (AD DS) domain. Each department within the company has its own organizational unit (OU). All client computers run Windows 7 Enterprise Edition and Microsoft Office 2010.

The company wants to restrict access to some Office 2010 features. They develop a standard list of corporate restrictions.

You have the following requirements:

-Apply the corporate restrictions to all existing and future departments.

-

Ensure that specific restrictions can be added or removed for individual departments.

-

Ensure that the corporate restrictions are not App1ied to users and computers in the built-in Active Directory containers.

-Minimize administrative effort for Applying restrictions to future departments.

You need to recommend a Group Policy object (GPO) deployment that meets the requirements.

What should you recommend? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Create a GPO that contains the corporate restrictions and link it to the domain. Install the Office 2010 Group Policy Administrative Template settings. Create a separate GPO for each department that deploys and configures Office 2010.

B. Install the Office 2010 Group Policy Administrative Template settings. Create a Starter GPO that contains the corporate restrictions. Create a separate GPO based on the Starter GPO for each department that deploys and configures Office 2010.

C. Install the Office 2010 Resource Kit and create a custom transform (.mst) file for each department. Create a Starter GPO that contains the corporate restrictions. Create a separate GPO based on the Starter GPO for each department that deploys Office 2010 by using the transform file.

D. Install the Office 2010 Resource Kit and create custom installer files for each department. Create a GPO that contains the corporate restrictions and link it to the domain. Create a separate GPO for each department that deploys the installer files,

Correct Answer: B

Starter GPOs are used as a base template to build other GPOs from. admin templates (ADMX and ADML files) need to be applied so that the settings specific to Office 2010 can be applied

QUESTION 3

Your network contains an Active Directory domain. You have a server that runs Windows Server 2008 R2 and has the Remote Desktop Services server role enabled. All client computers run Windows 7.

You need to plan the deployment of a new line of business application to all client computers.

The deployment must meet the following requirements:

-

Users must access the application from an icon on their desktops.

-

Users must have access to the application when they are not connected to the network.

What should you do?

A. Publish the application as a RemoteApp.

B. Publish the application by using Remote Desktop Web Access (RD Web Access).

C. Assign the application to the Remote Desktop Services server by using a Group Policy object (GPO).

D. Assign the application to all client computers by using a Group Policy object (GPO).

Correct Answer: D

http://support.microsoft.com/kb/816102

Assign a Package

To assign a program to computers that are running Windows Server 2003, Windows 2000, or Microsoft Windows XP Professional, or to users who are logging on to one of these workstations:

1.

Start the Active Directory Users and Computers snap-in. To do this, click Start, point to Administrative Tools, and then click Active Directory Users and Computers.

2.

In the console tree, right-click your domain, and then click Properties.

3.

Click the Group Policy tab, select the group policy object that you want, and then click Edit.

4.

Under Computer Configuration, expand Software Settings.

5.

Right-click Software installation, point to New, and then click Package.

6.

In the Open dialog box, type the full Universal Naming Convention (UNC) path of the shared installer package that you want. For example, \\file server\share\file name.msi. Important Do not use the Browse button to access the location. Make sure that you use the UNC path to the shared installer package.

7.

Click Open.

8.

Click Assigned, and then click OK. The package is listed in the right pane of the Group Policy window.

9.

Close the Group Policy snap-in, click OK, and then quit the Active Directory Users and Computers snap-in.

10.

When the client computer starts, the managed software package is automatically installed.

QUESTION 4

You are designing a Windows Server 2008 R2 deployment strategy for the Minneapolis campus servers.

Which deployment strategy should you recommend?

A. install from media.

B. Use a discover image in WDS.

C. Deploy a VHD image.

D. Deploy a WIM image.

Correct Answer: D

Requirements - Bitlocker is needed on all disks in Minneapolis and installations must be done remotely

VHD Image

- according to the official MS courseware book 6433A - a VHD can not contain more than one partition. so if true that rules VHD Images out because you need bitlocker and bitlocker requires 2 partitions. so if this is true then answer C is wrong.also http://technet.microsoft.com/en-us/library/dd363560.aspx

A supported .vhd image. The only supported operating systems are Windows Server 2008 R2, Windows 7 Enterprise, and Windows 7 Ultimate. Fixed, dynamic, and differencing .vhd images are supported. However, note that a supported

image cannot contain the following:

More than one operating system.

More than one partition.

Applications or data (instead of an operating system).

A 64-bit operating system that is partitioned with a GUID partition table (GPT).

So again further evidence that C is not the right answer as Bit locker needs 2 partitions.

I\\'m leaning toward Answer B because

WDS Images

WDS uses two different types of images: install images and boot images. Install images are the operating system images that will be deployed to computers running Windows Server 2008 R2, Windows Server 2008, Windows 7, or Windows

Vista. A default installation image named Install.wim is located in the \Sources directory of the installation DVD. If you are using WDS to deploy Windows 7 to computers with different processor architectures, it will be necessary to add

separate installation images for each architecture to the WDS server.

Architecture-specific images can be found on the architecture-specific installation media; for example, the Itanium image is located on the Itanium installation media, and the x64 default installation image is located on the x64 installation

media. Although it is possible to create custom images, it is necessary to have only one image per processor architecture. For example, deploying Windows Server 2008 R2 Enterprise edition x64 to a computer with two x64 processors and to

a computer with eight x64 processors in SMP configuration only requires access to the default x64 installation image. Boot images are used to start a client computer prior to the installation of the operating system image. When a computer

starts off a boot image over the network, a menu is presented that displays the possible images that can be deployed to the computer from the WDS server. The Windows Server 2008 R2 Boot.wim file allows for advanced deployment options,

and this file should be used instead of the Boot.wim file that is available from other sources.

In addition to the basic boot image, there are two separate types of additional boot images that can be configured for use with WDS. The capture image is a boot image that starts the WDS capture utility. This utility is used with a reference

computer, prepared with the Sysprep utility, as a method of capturing the reference computer\\'s image for deployment with WDS. The second type of additional boot image is the discover image. Discover images are used to deploy images to

computers that are not PXE-enabled or on networks that don\\'t allow PXE. These images are written to CD, DVD, or USB media and the computer is started off the media rather than off the PXE network card, which is the traditional method of

using WDS.

I\\'m gonna make a huge assumption that the Minneapolis servers are on a different subnet, which makes sense because they are all different campuses for a college. but if there is a DHCP Server or IP Helper is enabled then that wont be a

problem. So B may not be the answer

Media Install

It specifically says they use WDS for deployment. WDS is all about using images so would that not rule out media install? You can do media installs that are unattended but it requires sending a DVD and corresponding USB key with an

answer file to the site and it being inserted into the server. But GDI uses PXE enabled network cards so that would imply media is not used as images would be stored centrally.

QUESTION 5

You need to recommend a strategy for using managed service accounts on the Web servers.

Which managed service accounts should you recommend?

A. One account for all the web servers.

B. One account for each web server.

C. One account for the parent domain and one account for both child domains.

D. One account for the parent domain and one account for each child domain.

Correct Answer: B

There are 5 web servers in total, 3 in the forest root domain and 1 in each child domain.

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.

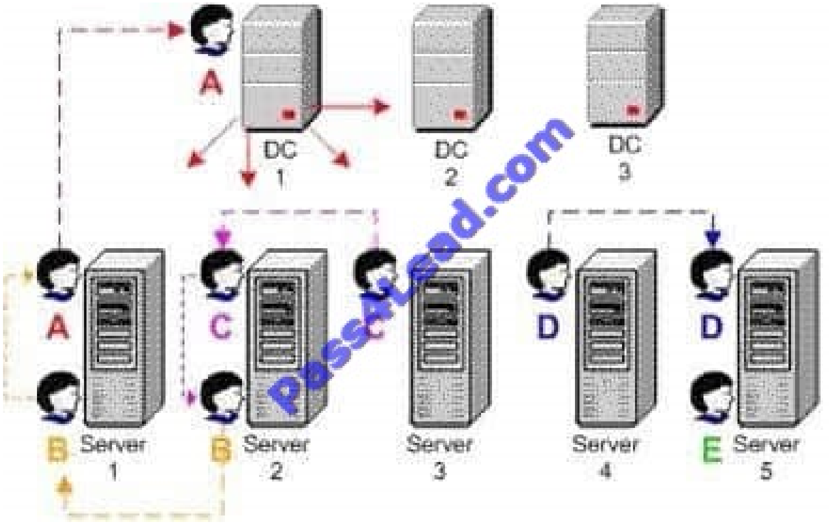
Account A has Administrator-equivalent privileges to more than one domain controller.

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

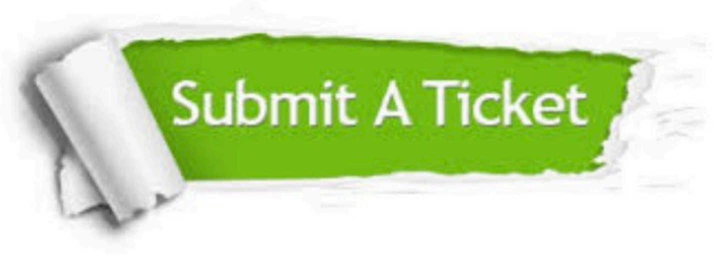
Account C has Administrator-equivalent privileges on servers 2 and 3.

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

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



[Latest 70-646 Dumps](#) [70-646 Practice Test](#) [70-646 Braindumps](#)


Submit A Ticket