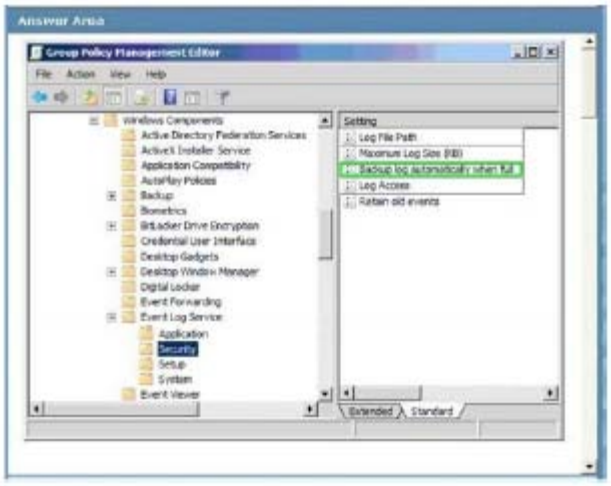
Microsoft

70-646

Pro: Windows Server 2008, Server Administrator



Backup log automatically when full

This policy setting controls Event Log behavior when the log file reaches its maximum size and takes effect only if the Retain old events policy setting is enabled. If you enable this policy setting and the Retain old events policy setting is enabled, the Event Log file is automatically closed and renamed when it is full. A new file is then started. If you disable this policy setting and the Retain old events policy setting is enabled, new events are discarded and the old events are retained. When this policy setting is not configured and the Retain old events policy setting is enabled, new events are discarded and the old events are retained.

Possible values:

Enabled

Disabled

Not Configured

Normally you need RETAIN OLD EVENTS enabled also But this is already set in the default domain policy per the exhibit for the testlet

QUESTION: 32

You need to recommend a solution that meets the following requirements:

- Log access to all shared folders on TT-FILE02.
- Minimize administrative effort.
- Ensure that further administrative action is not required when new shared folders are added to TT-FILE02.

Which actions should you perform in sequence?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order. (Use only actions that apply.)

tailspin1 (exhibit):

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 ha
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.

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

Server name	IP address	Current role(s)	Operating system	Notes
TT-DC01	10.10.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC02	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-DC03	10.5.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC04	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 development 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-PRI
- 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-DE\ through TT-DEV20.

tailspin2 (exhibit):

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:

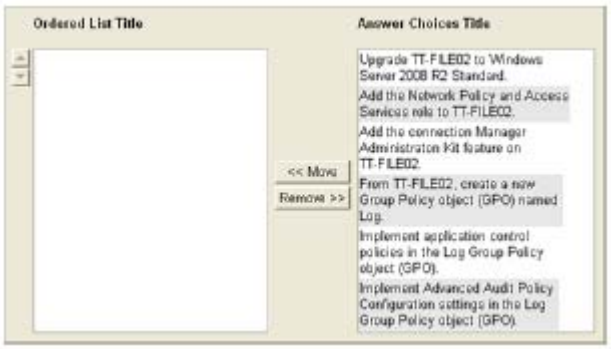
- Tailspin Toys IT security administrators must be able to create, modify, and delete user objects in the wingtiptoys.com domai
- Members of the Domain Admins group in the tailspintoys.com domain must have full access to the wingtiptoys.com Active Di
- A delegation policy must grant minimum access rights 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:

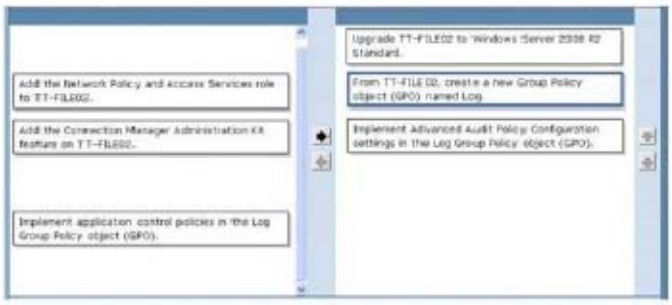
- Server security must be automated to ensure that newly deployed servers automatically have the same security configuration
- Auditing must be configured to ensure that the deletion of user objects and OUs is logged.
- Microsoft Word and Microsoft Excel files must be automatically encrypted when uploaded to the Confidential document library 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.

Build List and Reorder:



Answer:

Explanation:



QUESTION: 33
You need to recommend a solution to meet the following requirements:
- Meet the company auditing requirements.
- Ensure that further administrative action is not required when new folders are added to the file server.
What should you recommend? (Choose all that apply.)
tailspin1 (exhibit):

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
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.

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

Server name	IP address	Current role(s)	Operating system	Notes
TT-DC01	10.10.10.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC02	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-DC03	10.5.1.10	Domain controller, DNS server	Windows Server 2008 R2 Standard	Only AD-integrated DNS zones
TT-DC04	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 development 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-PRIN
- 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-DEV through TT-DEV20.

tailspin2 (exhibit):

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 x64-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 Di
- 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
- 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 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.

A. Enable the Audit File System Group Policy setting for Success.
B. Enable the Audit object access Group Policy setting for Success.
C. Enable the Audit File System Group Policy setting for Failure.
D. Enable the Audit Handle Manipulation Group Policy setting for Success.
E. Enable the File system option of the Global Object Access Auditing Group Policy setting.
F. Enable the Audit Handle Manipulation Group Policy setting for Failure.

Answer: B, D, E

Explanation:

We need to ensure that we have the following Audit scenario covered :

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

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

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

4. - Ensure that further administrative action is not required when new folders are added to the file server.

To cover # 1. - We do Enable the Audit object access Group Policy setting for Success.

The Audit object access Policy category includes the following subcategories:

Audit Application Generated
Audit Certification Services
Audit Detailed File Share
Audit File Share
Audit File System
Audit Filtering Platform Connection
Audit Filtering Platform Packet Drop
Audit Handle Manipulation
Audit Kernel Object
Audit Other Object Access Events
Audit Registry
Audit SAM

As you see below - enabling the Audit object access gives you all the above including the File System audit.

Auditing Windows Server 2008 File and Folder Access

Enabling File and Folder Auditing

File and folder auditing is enabled and disabled using either Group Policy (for auditing domains, sites and organizational units) or local security policy (for single servers).

To enable file and folder auditing for a single server, select Start -> All Programs -> Administrative Tools
-> Local Security Policy.

In the Local Security Policy tool, expand the Local Policies branch of the tree and select Audit Policy.

Double click on the Audit Object Access item in the list to display the corresponding properties page and choose whether successful,

failed, or both types of access to files or folders may be audited:

Once the settings are configured click on Apply to commit the changes and then OK to close the properties.

With file and folder auditing enabled the next task is to select which files and folders are to be audited.

To cover # 2. - We do Enable the Audit Handle Manipulation Group Policy setting for Success.

To configure, apply, and validate a reason for object access policy, you must:

Configure the file system audit policy. (done via Audit object access Group Policy setting)

Enable auditing for a file or folder. (choose your files/folders)

Enable the handle manipulation audit policy. (We have Just Enabled it)

Ensure that Advanced Audit Policy Configuration settings are not overwritten.

Update Group Policy settings.

Review and verify reason for access auditing data

To cover # 3 and # 4. - We do Enable the File system option of the Global Object Access Auditing Group
Policy setting.

Global Object Access Auditing policy settings allow administrators to define computer system access control lists (SACLs) per object type for either the file system or registry.

The specified SACL is then automatically applied to every object of that type.

So that means that new file/folders will automatic be enrolled and no further administrative action is required.

Security auditing allows you to track the effectiveness of your network defenses and identify attempts to circumvent them. There are a number of auditing enhancements in Windows Server 2008 R2 and Windows 7 that increase the level of detail in security auditing logs and simplify the deployment and management of auditing policies.

Auditing policy

Before you implement auditing policy, you must decide which event categories you want to audit. The auditing settings that you choose for the event categories define your auditing policy. On member servers and workstations that are joined to a domain, auditing settings for the event categories are undefined by default. On domain controllers, auditing is turned on by default. By defining auditing settings for specific event categories, you can create an auditing policy that suits the security needs of your organization.

Audit Object Access

This security setting determines whether to audit the event of a user accessing an object--for example, a file, folder, registry key, printer, and so forth--that has its own system access control list (SACL) specified.

If you define this policy setting, you can specify whether to audit successes, audit failures, or not audit the event type at all. Success audits generate an audit entry when a user successfully accesses an object that has an appropriate SACL specified. Failure audits generate an audit entry when a user unsuccessfully attempts to access an object that has a SACL specified.

To set this value to No auditing, in the Properties dialog box for this policy setting, select the Define these policy settings check box and clear the Success and Failure check boxes.

Note that you can set a SACL on a file system object using the Security tab in that object's Properties dialog box.

http://technet.microsoft.com/en-us/library/cc776774%28v=ws.10%29.aspx

Audit Handle Manipulation Group Policy setting

This policy setting determines whether the operating system generates audit events when a handle to an object is opened or closed. Only objects with configured SACLs generate these events, and only if the attempted handle operation matches the SACL. Event volume can be high, depending on how SACLs are configured. When used together with the Audit File System or Audit Registry policy settings, the Audit Handle Manipulation policy setting can provide an administrator with useful "reason for access," audit data detailing the precise permissions on which the audit event is based. For example, if a file is configured as a read-only resource but a user attempts to save changes to the file, the audit event will log not just the event itself but the permissions that were used, or attempted to be used, to save the file changes.

Global Object Access Auditing Group Policy setting.

Global Object Access Auditing. In Windows Server 2008 R2 and Windows 7, administrators can define computer-wide system access control lists (SACLs) for either the file system or registry. The specified SACL is then automatically applied to every single object of that type. This can be useful both for verifying that all critical files, folders, and registry settings on a computer are protected, and for identifying when an issue with a system resource occurs.

Pass your exam at First Attempt....Guaranteed!