Vendor: Microsoft

Exam Code:70-646

Exam Name: Pro: Windows Server 2008

Version: Demo

QUESTION 1

Your network consists of a single Active Directory domain. The network contains five Windows Server 2008 R2 servers that host Web Applications. You need to plan a remote management strategy to manage the Web servers. Your plan must meet the following requirements:

-Allow Web developers to configure features on the Web sites

-

Prevent Web developers from having full administrative rights on the Web servers What should you include in your plan?

A.

Configure request filtering on each Web server.

B.

Configure authorization rules for Web developers on each Web server.

C.

Configure the security settings in Internet Explorer for all Web developers by using a Group Policy.

D.

Add the Web developers to the Account Operators group in the domain.

Correct Answer: B

http://mscerts.programming4.us/windows_server/windows%20server%202008%20%20%20contro lling%20access%20to%20web%20services%20%28part%205%29%20-%20managing%20url%20authorization%20rules.aspx Managing URL Authorization Rules Authorization is a method by which systems administrators can determine which resources and content are available to specific users Authorization relies on authentication to validate the identity of a user. Once the identity has been proven,

authorization rules determine which actions a user or computer can perform IIS provides methods of securing different types of content using URL-based authorization. Because Web content is generally requested using a URL that includes a

full path to the content being requested, you can configure authorization settings easily, using IIS Manager

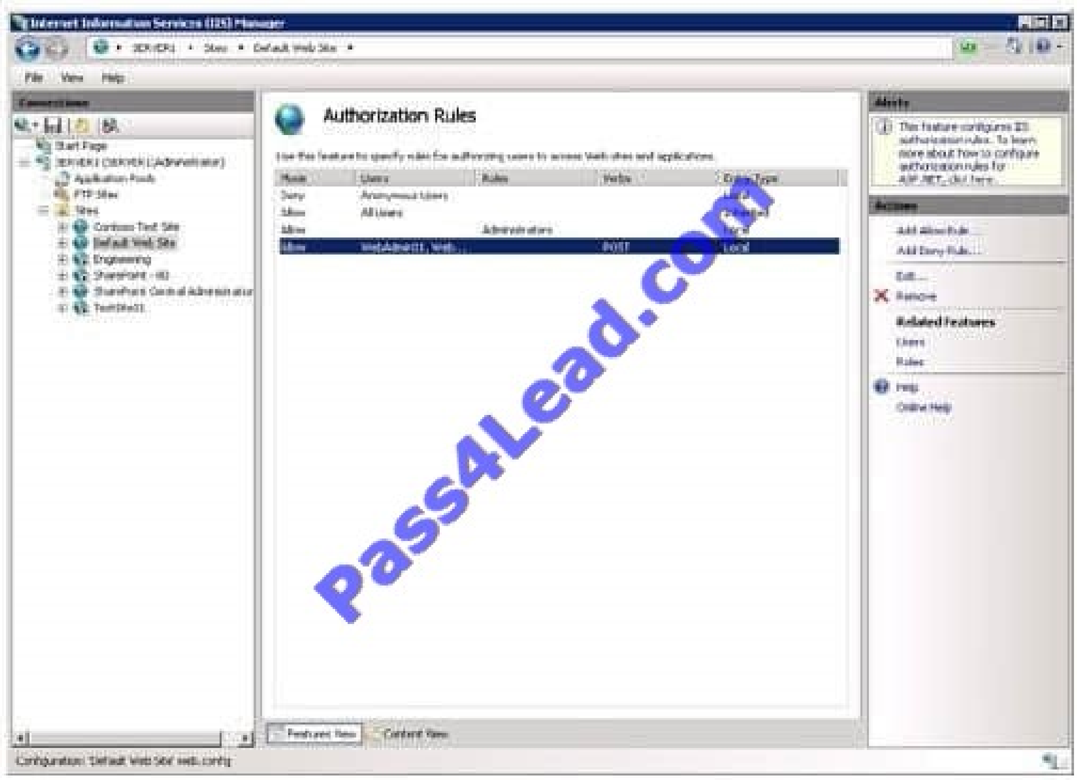
Creating URL Authorization Rules

To enable URL authorization, the UrlAuthorizationModule must be enabled Authorization rules can be configured at the level of the Web server for specific Web sites, for specific Web applications, and for specific files (based on a complete

URL path). URL authorization rules use inheritance so that lower-level objects inherit authorization settings from their parent objects (unless they are specifically overridden).

To configure authorization settings, select the appropriate object in the left pane of IIS Manager, and then select Authorization Rules in Features View. Figure 6 shows an example of multiple rules configured for a Web site.

Figure 6. Viewing authorization rules for a Web site



Authorization Rules

Use this feature to specify rules for authorizing users to access Web sites and applications.

Mode	Users	Roles	Verbs	Entry Type
Deny	Anonymous Users			Local
Allow	All Users			Inherited
Allow		Administrators		Local
Allow	WebAdmin01, Web...		POST	Local

This feature configures IIS authorization rules. To learn more about how to configure authorization rules for ASP.NET, click here.

Configuration: 'Default Web Site' web.config

There are two types of rules: Allow and Deny. You can create new rules by using the Add Allow Rule and Add Deny Rule commands in the Actions pane The available options for both types of rules are the same. (See Figure 7) When creating a new rule, the main setting is to determine to which users the rule applies. The options are:

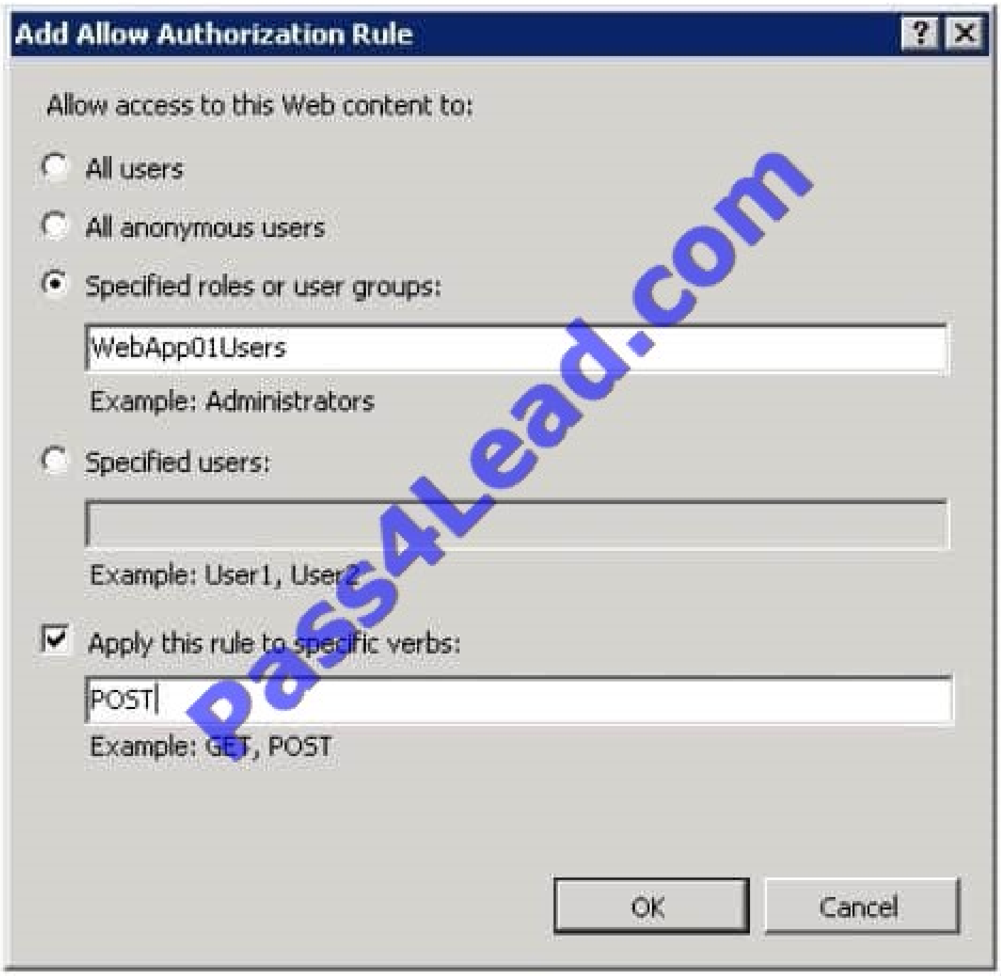
All Users

All Anonymous Users

Specific Roles Or User Groups

Specific Users

Figure 7. Creating a new Allow Rule for a Web application



Add Allow Authorization Rule

Allow access to this Web content to:

○ All users

○ All anonymous users

● Specified roles or user groups:

WebApp01Users

Example: Administrators

○ Specified users:

Example: User1, User2

☑ Apply this rule to specific verbs:

POST

Example: GET, POST

When you choose to specify users or groups to which the rule applies, you can type the appropriate names in a command-separated list. The specific users and groups are defined using NET role providers. This is a standard feature that is available to ASP NET Web developers.

Developers can create their own roles and user accounts and can define permissions within their applications. Generally, information about users and roles is stored in a relational database or relies on a directory service such as Active Directory.

In addition to user and role selections, you can further configure an authorization rule based on specific HTTP verbs. For example, if you want to apply a rule only for POST commands (which are typically used to send information from a Web browser to a Web server), add only the POST verb to the rule

Managing Rule Inheritance As mentioned earlier in this section, authorization rules are inherited automatically by lower-level objects This is useful when your Web site and Web content is organized hierarchically based on intended users or groups The Entry Type column shows whether a rule has been inherited from a higher level or whether it has been defined locally IIS Manager automatically will prevent you from creating duplicate rules. You can remove rules at any level, including both Inherited and Local entry types

---

QUESTION 2

You are planning to deploy new servers that will run Windows Server 2008 R2. Each server will have 32 GB of RAM.

The servers must support installation of the following role services:

-Routing and Remote Access

-Remote Desktop Services Gateway

-Minimize CPU and RAM usage

You need to deploy the minimum edition of Windows Server 2008 R2 that meets the requirements.

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

A. A Server Core installation of Windows Server 2008 R2 Datacenter.

B. A Full Installation of Windows Server 2008 R2 Enterprise.

C. A Full Installation of Windows Server 2008 R2 Standard.

D. A Server Core installation Windows Server 2008 R2 Web.

Correct Answer: C

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.

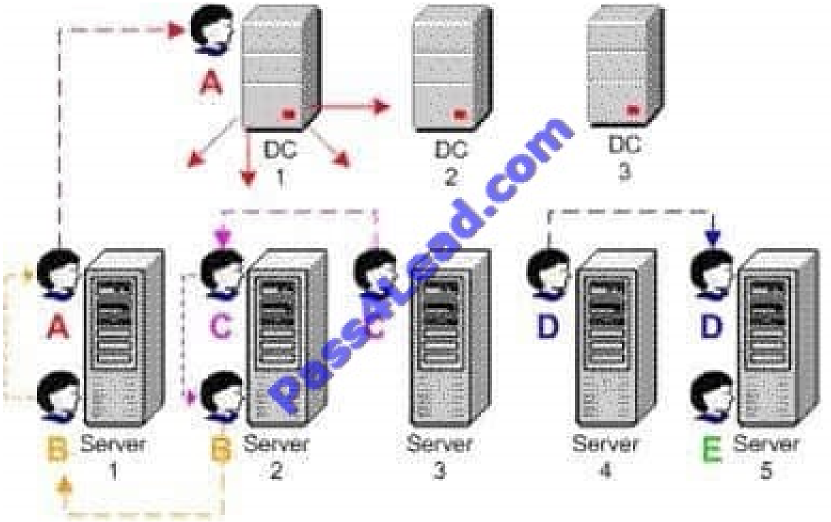
Account A has Administrator-equivalent privileges to more than one domain controller.

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 network that address the user problems statement. What should you recommend?

A. Deploy DirectAccess.

B. Configure folder redirection.

C. Create a volume mount point.

D. Implement additional DFS targets.

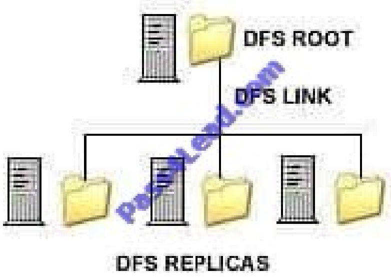
Correct Answer: D

Direct Access is a remote access solution and does not address the problem. Folder redirection does not address the problem Volume mount point would not solve this problem either

The Distributed File System is used to build a hierarchical view of multiple file servers and shares on the network. Instead of having to think of a specific machine name for each set of files, the user will only have to remember one name; which will be the \\'key\\' to a list of shares found on multiple servers on the network. Think of it as the home of all file shares with links that point to one or more servers that actually host those shares.

DFS has the capability of routing a client to the closest available file server by using Active Directory site metrics

Dfs target (or replica): This can be referred to as either a root or a link. If you have two identical shares, normally stored on different servers, you can group them together as Dfs Targets under the same link.



QUESTION 5

Your network contains a single Active Directory domain. All domain controllers run Windows Server 2008 R2. There are 1,000 client computers that run Windows 7 and that are connected to managed switches. You need to recommend a strategy for network access that meets the following requirements:

-Users are unable to bypass network access restrictions.

-Only client computers that have uptodate service packs installed can access the network.

-Only client computers that have uptodate antimalware software installed can access the network.

What should you recommend?

A. Implement Network Access Protection (NAP) that uses DHCP enforcement.

B. Implement Network Access Protection (NAP) that uses 802.1x enforcement.

C. Implement a Network Policy Server (NPS), and enable IPsec on the domain controllers.

D. Implement a Network Policy Server (NPS), and enable Remote Authentication DialIn User Service (RADIUS) authentication on the managed switches.

Correct Answer: B

MCITP Self-Paced Training Kit Exam 70-646 Windows Server Administration:

Integration with network access protection (NAP)System Center Configuration Manager 2007 lets your organization enforce compliance of software updates on client computers. This helps protect the integrity of the corporate network through

integration with the Microsoft Windows Server 2008 NAP policy enforcement platform. NAP policies enable you to define which software updates to include in your system health requirements. If a client computer attempts to access your

network, NAP and System Center Configuration Manager 2007 work together to determine the client\\'s health state compliance and determine whether the client is granted full or restricted network access. If the client is noncompliant, System

Center Configuration Manager 2007 can deliver the necessary software updates so that the client can meet system health requirements and be granted full network access.

Restrict network accessSystem Center Configuration Manager 2007 NAPenables you to include software updates in your system health requirements.NAP policies define which software updates need to be included, and the System Center

Configuration Manager 2007 System Health Validator point passes the client\\'s compliant or noncompliant health state to the Network Policy Server, which determines whether to grant the client full or restricted network access. Noncompliant

clients can be automatically brought into compliance through remediation. This requires the System Center Configuration Manager 2007 software updates feature to be configured and operational.

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 NAP Enforcement

802.1X enforcement makes use of authenticating Ethernet switches or IEEE 802.11 Wireless Access Points.

These compliant switches and access points only grant unlimited network access to computers that meet the compliance requirement. Computers that do not meet the compliance requirement are limited in their communication by a restricted

access profile. Restricted access profiles work by applying IP packet filters or VLAN (Virtual Local Area Network) identifiers. This means that hosts that have the restricted access profile are allowed only limited network communication. This

limited network communication generally allows access to remediation servers. You will learn more about remediation servers later in this lesson.

An advantage of 802.1X enforcement is that the health status of clients is constantly assessed. Connected clients that become noncompliant will automatically be placed under the restricted access profile. Clients under the restricted access

profile that become compliant will have that profile removed and will be able to communicate with other hosts on the network in an unrestricted manner. For example, suppose that a new antivirus update comes out. Clients that have not

installed the update are put under a restricted access profile until the new update is installed. Once the new update is installed, the clients are returned to full network access. A Windows Server 2008 computer with the Network Policy Server

role is necessary to support 802.1X NAP enforcement. It is also necessary to have switch and/or wireless access point hardware that is 801.1xcompliant.

Client computers must be running Windows Vista, Windows Server 2008, or Windows XP Service Pack 3 because these operating systems include the EAPHost EC.

MORE INFO 802.1X enforcement step-by-step For more detailed information on implementing 802.1X NAP enforcement, consult the following Step-by-Step guide on TechNet: http://go.microsoft.com/fwlink/?LinkId=86036.

QUESTION 6

Your network consists of a single Active Directory domain. The network contains a file server that runs Windows Server 2008 R2. All servers use internal storage only. You plan to deploy a client/server Application.

You need to deploy the Application so that it is available if a single server fails. You must achieve this goal while minimizing costs.

What should you do?

A. Deploy RemoteApp.

B. Deploy a failover cluster that uses No Majority: Disk Only.

C. Deploy a failover cluster that uses Node and File Share Disk Majority.

D. Deploy Distributed File System (DFS) and configure replication.

Correct Answer: C

Understanding Cluster Quorum Models

Quorums are used to determine the number of failures that can be tolerated within a cluster before the cluster itself has to stop running. This is done to protect data integrity and prevent problems that could occur because of failed or failing communication between nodes.

Quorums describe the configuration of the cluster and contain information about the cluster components such as network adapters, storage, and the servers themselves. The quorum exists as a database in the registry and is maintained on the witness disk or witness share. The witness disk or share keeps a copy of this configuration data so that servers can join the cluster at any time, obtaining a copy of this data to become part of the cluster.

One server manages the quorum resource data at any given time, but all participating servers also have a copy.

You can use the following four quorum models with Windows Server 2008 Failover Clusters:

Node Majority Microsoft recommends using this quorum model in Failover Cluster deployments that contain an odd number of cluster nodes. A cluster that uses the Node Majority quorum model is called a Node Majority cluster and remains up and running if the number of available nodes exceeds the number of failed nodes--that is, half plus one of its nodes is available. For example, for a seven-node cluster to remain online, four nodes must be available. If four nodes fail in a seven-node Node Majority cluster, the entire cluster shuts down. You should use Node Majority clusters in geographically or network-dispersed cluster nodes. To operate successfully this model requires an extremely reliable network, high-quality hardware, and a third-party mechanism to replicate back-end data.

Node and Disk Majority Microsoft recommends using this quorum model in clusters that contain even numbers of cluster nodes. Provided that the witness disk remains available, a Node and Disk Majority cluster remains up and running when one-half or more of its nodes are available. A six-node cluster will not shut down if three or more nodes plus its witness disk are available. In this model, the cluster quorum is stored on a cluster disk that is accessible to all cluster nodes through a shared storage device using Serial Attached SCSI (SAS), Fibre Channel, or iSCSI connections. The model consists of two or more server nodes connected to a shared storage device and a single copy of the quorum data is maintained on the witness disk. You should use the Node and Disk Majority quorum model in Failover Clusters with shared storage, all connected on the same network and with an even number of nodes. In the case of a witness disk failure, a majority of the nodes need to remain up and running. For example, a six-node cluster will run if (at a minimum) three nodes and the witness disk are available. If the witness disk is offline, the same six-node cluster requires that four nodes are available.

Exam Tip If the 70-646 examination asks which quorum model is the closest to the traditional single-quorum device cluster configuration model, the answer is the Node and Disk Majority quorum model.

Node and File Share Majority This configuration is similar to the Node and Disk Majority model, but the quorum is stored on a network share rather than on a witness disk. A Node and File Share Majority cluster can be deployed in a similar fashion to a Node Majority cluster, but as long as the witness file share is available the cluster can tolerate the failure of half its nodes. You should use the Node and File Share Majority quorum model in clusters with an even number of nodes that do not utilize shared storage.

No Majority: Disk Only Microsoft recommends that you do not use this model in a production environment because the disk containing the quorum is a single point of failure. No Majority: Disk Only clusters are best suited for testing the deployment of built-in or custom services and applications on a Windows Server 2008 Failover Cluster. In this model, provided that the disk containing the quorum remains available, the cluster can sustain the failover of all nodes except one.

MORE INFO Quorum models webcast Four quorum models are available with Windows Server 2008. For more information on the models, view the TechNet webcast at http://msevents.microsoft.com/CUI/WebCastEventDetails .aspx? EventID=1032364841andEventCategory=4andculture=en-USandCountryCode=US

QUESTION 7

You need to recommend a security strategy for WebApp2 that meets the company\\'s Application requirements. What should you include in the recommendation?

A. Basic authentication and connection security rules

B. Basic authentication and SSL

C. Digest authentication and connection security rules

D. Digest authentication and SSL

Correct Answer: B

QUESTION 8

You need to recommend a security strategy for WebApp2 that meets the company\\'s Application requirements. What should you include in the recommendation?

A. Basic authentication and SSL

B. Digest authentication and SSL

C. Digest authentication and SSL VPN

D. Basic authentication and SSL VPN

Correct Answer: A

You must support multiple browsers and one advantage of the basic access authentication is all web browsers support it. But due to the fact that the username and password are passed in cleartext, it is rarely used by itself on publicly accessible Internet web sites. However, it is somewhat commonly found on publicly accessible sites if combined with SSL/TLS (HTTPS). The use of SSL/TLS to encrypt the entire connection mitigates the fact that the Basic passwords themselves are not encrypted. Most browsers will actually display an alert of some kind if a site uses Basic Auth without SSL/TLS, but will not display an alert when Basic Auth is used on a connection that has SSL/TLS enabled.

QUESTION 9

You need to ensure that Web1, Web2, and Web3 download updates from WSUS1.

What should you do?

A. Modify the Default Domain Policy Group Policy object (GPO).

B. Modify the local computer policy on Web1, Web2, and Web3.

C. Import a security policy template toWeb1, Web2, and Web3.

D. Create a service location (SRV) record in the _msdcs.graphicsdesigninstitute.com DNS zone.

Correct Answer: B

Servers belong to a work group so WSUS policy cant be applied using AD GPO. but the local security policy can be modified to point to the WSUS server

---

QUESTION 10

You are evaluating whether to add an additional hard disk drive to each file server and create a striped volume for the data files. Which storage requirement is met by adding the hard disk drive and creating the striped volume?

A. Improve data availability on the file servers.

B. Improve the performance of the file servers.

C. Provide additional storage on the file servers without causing downtime.

D. Enable users to access the previous versions of all the files stored on the file servers.

Correct Answer: B

http://technet.microsoft.com/en-us/library/cc732422.aspx

A striped volume is a dynamic volume that stores data in stripes on two or more physical disks. Data in a striped volume is allocated alternately and evenly (in stripes) across the disks. Striped volumes offer the best performance of all the

volumes that are available in Windows, but they do not provide fault tolerance. If a disk in a striped volume fails, the data in the entire volume is lost.

You can create striped volumes only on dynamic disks. Striped volumes cannot be extended. You can create a striped volume onto a maximum of 32 dynamic disks.

QUESTION 11

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.

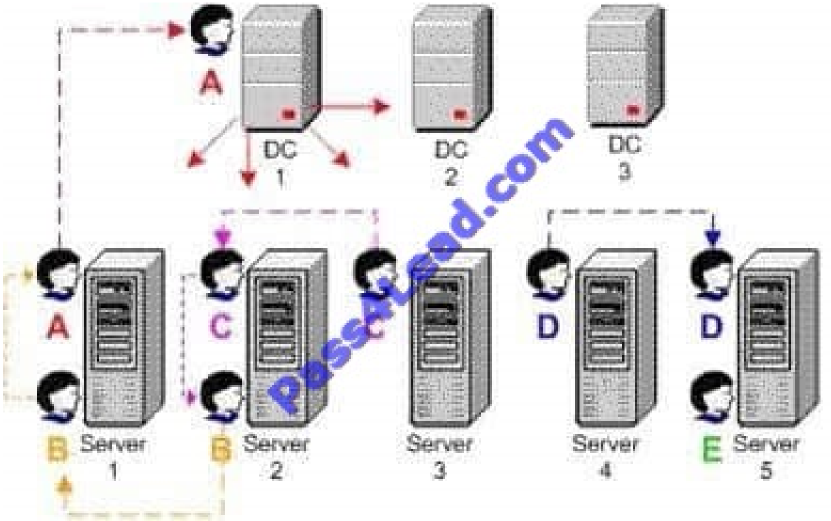
Account A has Administrator-equivalent privileges to more than one domain controller.

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.



QUESTION 12

You need to recommend a data management solution that meets the company\\'s technical requirements.

What should you include in the recommendation?

A. DFS Management

B. File Server Resource Manager (FSRM)

C. Share and Storage Management

D. Storage Explorer

Correct Answer: C

http://technet.microsoft.com/en-us/library/cc753175.aspx

Share and Storage Management provides a centralized location for you to manage two important server resources:

Folders and volumes that are shared on the network

Volumes in disks and storage subsystems

Shared resources management

You can share the content of folders and volumes on your server over the network using the Provision a Shared Folder Wizard, which is available in Share and Storage Management. This wizard guides you through the necessary steps to

share a folder or volume and assign all applicable properties to it. With the wizard, you can:

Specify the folder or volume that you want to share or create a new folder to share.

Specify the network sharing protocol used to access the shared resource.

Change the local NTFS permissions for the folder or volume you will be sharing.

Specify the share access permissions, user limits, and offline access to files in the shared resource.

Publish the shared resource to a Distributed File System (DFS) namespace.

If Services for Network File System (NFS) has been installed, specify NFS-based access permissions for the shared resource.

If File Server Resource Manager is installed on your server, apply storage quotas to the new shared resource, and create file screens to limit the type of files that can be stored in it.

Using Share and Storage Management, you can also monitor and modify important aspects of your new and existing shared resources. You can:

Stop the sharing of a folder or volume.

Change the local NTFS permissions for a folder or volume.

Change the share access permissions, offline availability, and other properties of a shared resource.

See which users are currently accessing a folder or a file and disconnect a user if necessary.

If Services for Network File System (NFS) has been installed, change the NFS-based access permissions for a shared resource.

For more information about using Share and Storage Management to manage shared resources, see Provisioning Shared Resources.

Storage management With Share and Storage Management, you can provision storage on disks that are available on your server, or on storage subsystems that support Virtual Disk Service (VDS). The Provision Storage Wizard guides you

through the process of creating a volume on an existing disk, or on a storage subsystem attached to your server. If the volume is going to be created on a storage subsystem, the wizard will also guide you through the process of creating a

logical unit number (LUN) to host that volume. You also have the option of only creating the LUN, and using Disk Management to create the volume later.

Share and Storage Management also helps you monitor and manage the volumes that you have created, as well as any other volumes that are available on your server. Using Share and Storage Management you can:

Extend the size of a volume.

Format a volume.

Delete a volume.

Change volume properties like compression, security, offline availability and indexing.

Access disk tools for error checking, defragmentation, and backup.