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.pass4itsure.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 a management solution for Server1 that meets the company\\'s security requirements. What should you include in the recommendation?

A. accessbased enumeration (ABE)

B. Authentication Mechanism Assurance

C. Authorization Manager

D. HyperV Manager

Correct Answer: C

http://technet.microsoft.com/en-us/library/cc732290%28WS.10%29.aspx What does Authorization Manager do? Authorization Manager is a role-based security architecture for Windows that can be used in any application that needs role-based authorization, including ASP.NET Web applications, ASP.NET Web services, and client/server systems based

on .NET Remoting. The role-based management model enables you to assign users to roles and gives you a central place to record permissions assigned to each role. This model is often called rolebased access control.

QUESTION 2

You need to recommend changes to the infrastructure to ensure that DFS meets the company\\'s security requirements. What should you include in the recommendation?

A. Upgrade DFS2 to Windows Server 2008 R2.

B. Implement accessbased enumeration (ABE).

C. Implement Authentication Mechanism Assurance.

D. Configure the DFS namespace to use Windows Server 2008 mode.

Correct Answer: A

Users must only be able to modify the financial forecast reports on DFSl. DFS2 must contain a read-only copy of the financial forecast reports. Both servers are part of the same replication group and it is in Windows 2000 server mode http://blogs.technet.com/b/filecab/archive/2009/04/01/configuring-a-read-only-replicated-folder.aspx Please read the following notes carefully before deploying the read-only replicated folders feature. a) Feature applicability: The read-only replicated folders feature is available only on replication member servers which are running Windows Server 2008 R2. In other words, it is not possible to configure a replicated folder to be read-only on a

member server running either Windows Server 2003 R2 or Windows Server 2008.

b) Backwards compatibility: Only the server hosting read-only replicated folders needs to be running Windows Server 2008 R2. The member server that hosts a read-only replicated folder can replicate with partners that are on Windows Server 2003 or Windows Server 2008. However, to configure and administer a replication group that has a read-only replicated folder, you need to use the DFS Management MMC snap-in on Windows Server 2008 R2. c) Administration of read-only replicated folders: In order to configure a replicated folder as read-only replicated folder, you need to use the DFS Management MMC snap-in on Windows Server 2008 R2. Older versions of the snap-in (available

on Windows Server 2003 R2 or Windows Server 2008) cannot configure or manage a read-only replicated folder. In other words, these snap-ins will not display the option to mark a replicated folder \\'read-only\\'.

d) Schema updates: If you have an older version of the schema (pre-Windows Server 2008), you will need to update your Active Directory schema to include the DFS Replication schema extensions for Windows Server 2008.

http://blogs.technet.com/b/filecab/archive/2009/01/21/read-only-replicated-folders-on-windows-server-2008-r2.aspx

Why deploy read-only replicated folders?

Consider the following scenario. Contoso Corporation has a replication infrastructure similar to that depicted in the diagram below. Reports are published to the datacenter server and these need to be distributed to Contoso\\'s branch offices.

DFS Replication is configured to replicate a folder containing these published reports between the datacenter server and branch office servers.

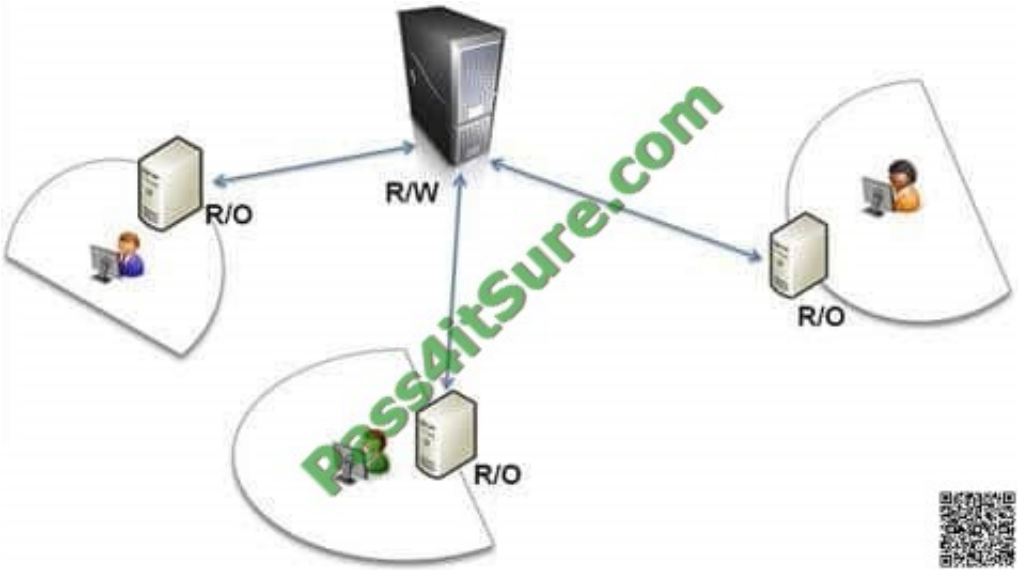
The DFS Replication service is a multi-master file replication engine ?meaning that changes can be made to replicated data on any of the servers taking part in replication. The service then ensures that these changes are replicated out to all

other members in that replication group and that conflicts are resolved using `last-writerwins\\' semantics.

Now, a Contoso employee working in a branch office accidentally deletes the `Specs\\' sub-folder from the replicated folder stored on that branch office\\'s file server. This accidental deletion is replicated by the DFS Replication service, first to the datacenter server and then via that server to the other branch offices. Soon, the `Specs\\' folder gets deleted on all of the servers participating in replication. Contoso\\'s file server administrator now needs to restore the folder from a previously taken backup and ensure that the restored contents of the folder once again replicate to all branch office file servers.

Administrators need to monitor their replication infrastructure very closely in order to prevent such situations from arising or to recover lost data if needed. Strict ACLs are a way of preventing these accidental modifications from happening, but managing ACLs across many branch office servers and for large amounts of replicated data quickly degenerates into an

administrative nightmare. In case of accidental deletions, administrators need to scramble to recover data from backups (often up-to-date backups are unavailable) and in the meantime, end-users face outages leading to loss of productivity.



This situation can be prevented by configuring read-only replicated folders on branch office file servers. A readonly replicated folder ensures that no local modifications can take place and the replica is kept in sync with a read-write enabled

copy by the DFS Replication service. Therefore, read-only replicated folders enable easyto-deploy and low-administrative-overhead data publication solutions especially for branch office scenarios.

How does all this work?

For a read-only replicated folder, the DFS Replication service intercepts and inspects every file system operation. This is done by virtue of a file system filter driver that layers above every replicated folder that is configured to be read-only.

Volumes that do not host read-only replicated folders or volumes hosting only readwrite replicated folders are ignored by the filter driver.

Only modifications initiated by the service itself are allowed ?these modifications are typically caused by the service installing updates from its replication partners. This ensures that the read-only replicated folder is maintained in sync with a

read-write enabled replicated folder on another replication partner (presumably located at the datacenter server).

All other modification attempts are blocked ?this ensures that the contents of the read-only replicated folder cannot be modified locally. As shown in the below figure, end-users are unable to modify the contents of the replicated folder on

servers where it has been configured to be read-only. The behavior is similar to that of a read-only SMB share ?contents can be read and attributes can be queried for all files, however, modifications are not possible.

QUESTION 3

Your network consists of a single Active Directory domain. All servers run Windows Server 2008

R2. You plan to publish a Web site on two Web servers.

You need to deploy an availability solution for your Web servers that meets the following requirements:

-Supports the addition of more Web servers without interrupting client connections

-Ensures that the Web site is accessible even if a single server fails

What should you do?

A. Configure a failover cluster.

B. Configure a Web garden on each Web server.

C. Create a Network Load Balancing cluster.

D. Create two Application pools on each Web server.

Correct Answer: C

Windows Web Server 2008

Windows Web Server 2008 is designed to function specifically as a Web applications server.

Other roles, such as Windows Deployment Server and Active Directory Domain Services, are not supported on Windows Web Server 2008. You deploy this server role either on a screened subnet to support a Web site viewable to external

hosts or as an intranet server. As appropriate given its stripped-down role, Windows Web Server 2008 does not support the high-powered hardware configurations that other editions of Windows Server 2008 do.

Windows Web Server 2008 has the following properties:

The 32-bit version (x86) supports a maximum of 4 GB of RAM and 4 processors in SMP configuration.

The 64-bit version (x64) supports a maximum of 32 GB of RAM and 4 processors in SMP configuration.

Supports Network Load Balancing clusters.

You should plan to deploy Windows Web Server 2008 in the Server Core configuration, which minimizes its attack surface, something that is very important on a server that interacts with hosts external to your network environment. You

should only plan to deploy the full version of Windows Web Server 2008 if your organization\\'s Web applications rely on features such as ASP.NET, because the .NET Framework is not included in a Server Core installation.

Configuring Windows Network Load Balancing

While DNS Round Robin is a simple way of distributing requests, Windows Server 2008 NLB is a much more robust form of providing high availability to applications. Using NLB, an administrator can configure multiple servers to operate as a

single cluster and control the usage of the cluster in near real-time.

NLB operates differently than DNS Round Robin in that NLB uses a virtual network adapter on each host. This virtual network adapter gets a single IP and media access control (MAC) address, which is shared among the hosts participating

in the load-balancing cluster. Clients requesting services from an NLB cluster have their requests sent to the IP address

of the virtual adapter, at which point it can be handled by any of the servers in the cluster.

NLB automatically reconfigures as nodes are added and removed from the cluster. An administrator can add and remove nodes through the NLB Manager interface or the command

line. For example, an administrator might remove each node in turn to perform maintenance on the nodes individually and cause no disruption in service to the end user.

Servers within NLB clusters are in constant communication with each other, determining which servers are available with a process known as heartbeats and convergence. The heartbeat consists of a server participating in an NLB cluster that

sends out a message each second to its NLB-participating counterparts.

When five (by default) consecutive heartbeats are missed, convergence begins. Convergence is the process by which the remaining hosts determine the state of the cluster.

During convergence, the remaining hosts listen for heartbeats from the other servers to determine the host with the highest priority, which is then selected as the default host for the NLB cluster.

Generally, two scenarios can trigger convergence. The first is the missed heartbeat scenario mentioned earlier; the second is removal or addition of a server to the cluster by an administrator.

The heartbeat is reduced by one half during convergence. A less common reason for convergence is a change in the host configuration, such as a host priority.

QUESTION 4

You need to recommend a solution for the Web server content that meets the company\\'s technical requirements.

What should you include in the recommendation?

A. Distributed File System (DFS) Replication

B. folder redirection

C. HTTP redirection

D. IIS Shared Configuration

Correct Answer: D

AD is a prerequisite for DFS and we have workgroup in the perimeter network By using Shared Configuration, you can share your IIS configuration across multiple servers.

Please note that this article is focused on the back end configuration of the web servers and not the front end task of load balancing the servers.

Shared Configuration allows you to set up Internet Information Services (IIS) quickly and easily on multiple servers so that the sites, application pools and IIS server settings are consistent across two or more servers.

You only have to configure a server one time and then you can replicate the IIS settings. Shared Configuration is not for individual sites on a server but for the entire IIS configuration on a server.

QUESTION 5

Your network contains a standalone root certification authority (CA). You have a server named Server1 that runs Windows Server 2008 R2. You issue a server certificate to Server1.

You deploy Secure Socket Tunneling Protocol (SSTP) on Server1.

You need to recommend a solution that allows external partner computers to access internal network resources by using SSTP.

What should you recommend?

A. Enable Network Access Protection (NAP) on the network.

B. Deploy the Root CA certificate to the external computers.

C. Implement the Remote Desktop Connection Broker role service.

D. Configure the firewall to allow inbound traffic on TCP Port 1723.

Correct Answer: B

Lesson 1: Configuring Active Directory Certificate Services

Certificate Authorities are becoming as integral to an organization\\'s network infrastructure as domain controllers, DNS, and DHCP servers. You should spend at least as much time planning the deployment of Certificate Services in your

organization\\'s Active Directory environment as you spend planning the deployment of these other infrastructure servers. In this lesson, you will learn how certificate templates impact the issuance of digital certificates, how to configure

certificates to be automatically assigned to users, and how to configure supporting technologies such as Online Responders and credential roaming. Learning how to use these technologies will smooth the integration of certificates into your

organization\\'s Windows Server 2008 environment.

After this lesson, you will be able to:

Install and manage Active Directory Certificate Services.

Configure autoenrollment for certificates.

Configure credential roaming.

Configure an Online Responder for Certificate Services.

Estimated lesson time: 40 minutes

Types of Certificate Authority

When planning the deployment of Certificate Services in your network environment, you must decide which type of Certificate Authority best meets your organizational requirements. There are four types of Certificate Authority (CA):

Enterprise Root Enterprise Subordinate Standalone Root Standalone Subordinate The type of CA you deploy depends on how certificates will be used in your environment and the state of the existing environment. You have to choose between an Enterprise or a Standalone CA during the installation of the Certificate

Services role, as shown in Figure 10-1. You cannot switch between any of the CA types after the CA has been deployed.

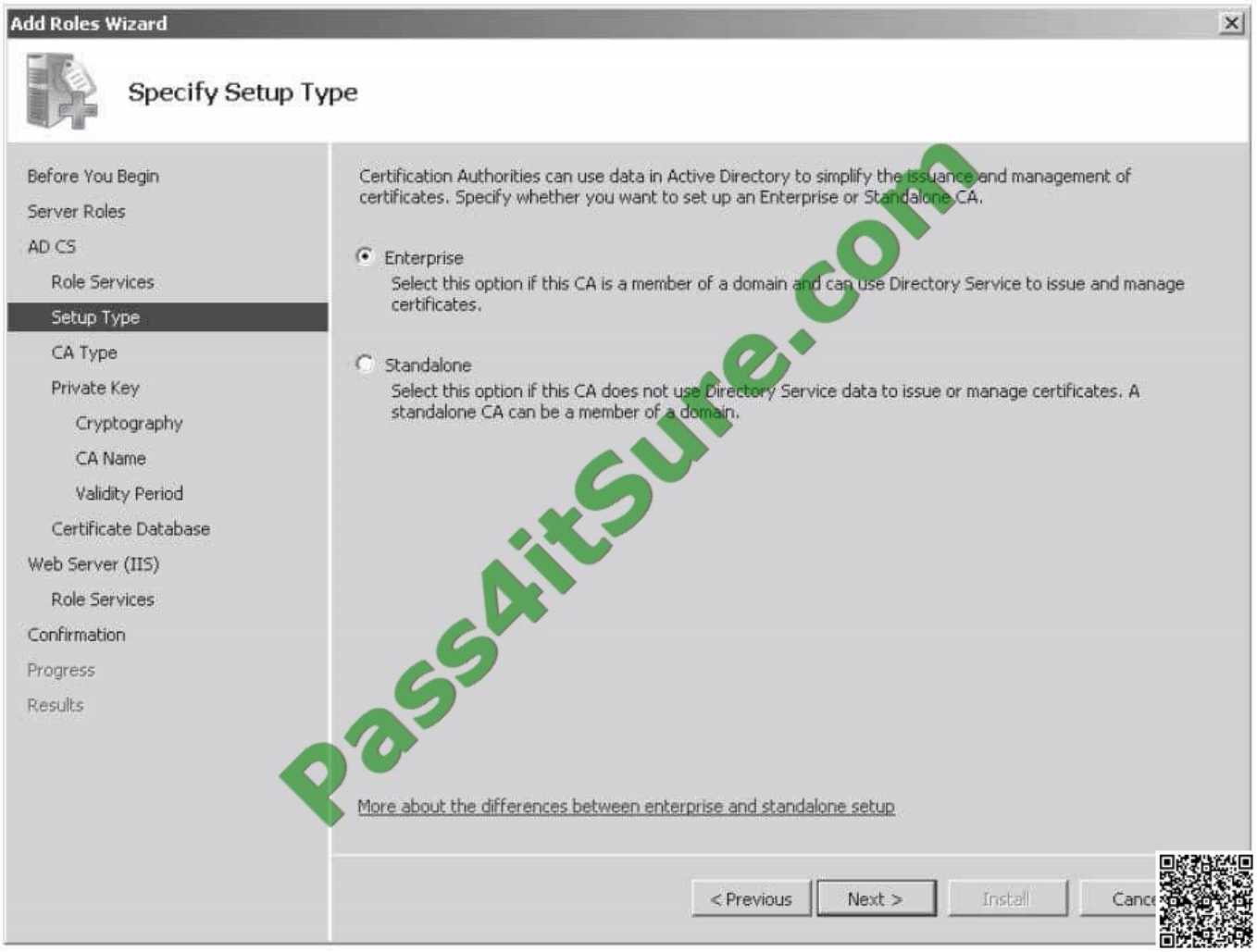


Figure 10-1Selecting an Enterprise or Standalone CA

Enterprise CAs require access to Active Directory. This type of CA uses Group Policy to propagate the certificate trust lists to users and computers throughout the domain and publish certificate revocation lists to Active Directory. Enterprise CAs issue certificates from certificate templates, which allow the following functionality: Enterprise CAs enforce credential checks on users during the certificate enrollment process. Each certificate template has a set of security permissions that determine whether a particular user is authorized to receive certificates generated

from that template.

Certificate names are automatically generated from information stored within Active Directory.

The method by which this is done is determined by certificate template configuration.

Autoenrollment can be used to issue certificates from Enterprise CAs, vastly simplifying the certificate distribution process. Autoenrollment is configured through applying certificate template permissions.

In essence, Enterprise CAs are fully integrated into a Windows Server 2008 environment. This type of CA makes the issuing and management of certificates for Active Directory clients as simple as possible.

Standalone CAs do not require Active Directory. When certificate requests are submitted to Standalone CAs, the requestor must provide all relevant identifying information and manually specify the type of certificate needed. This process

occurs automatically with an Enterprise CA. By default, Standalone CA requests require administrator approval.

Administrator intervention is necessary because there is no automated method of verifying a requestor\\'s credentials. Standalone CAs do not use certificate templates, limiting the ability for administrators to customize certificates for specific organizational needs. You can deploy Standalone CAs on computers that are members of the domain. When installed by a user that is a member of the Domain Admins group, or one who has been delegated similar rights, the Standalone CA\\'s information will be

added to the Trusted Root Certificate Authorities certificate store for all users and computers in the domain. The CA will also be able to publish its certificate revocation list to Active Directory.

Whether you install a Root or Subordinate CA depends on whether there is an existing certificate infrastructure.

Root CAs are the most trusted type of CA in an organization\\'s public key infrastructure (PKI) hierarchy. Root CAs sit at the top of the hierarchy as the ultimate point of trust and hence must be as secure as possible. In many environments, a

Root CA is only used to issue signing certificates to Subordinate CAs. When not used for this purpose, Root CAs are kept offline in secure environments as a method of reducing the chance that they might be compromised. If a Root CA is compromised, all certificates within an organization\\'s PKI infrastructure should be considered compromised. Digital certificates are ultimately statements of trust. If you cannot trust the ultimate authority from which that trust is derived, it follows that you should not trust any of the certificates downstream from that ultimate authority.

Subordinate CAs are the network infrastructure servers that you should deploy to issue the everyday certificates needed by computers, users, and services. An organization can have many Subordinate CAs, each of which is issued a signing certificate by the Root CA. In the event that one Subordinate CA is compromised, trust of that CA can be revoked from the Root CA. Only the certificates that were issued by that CA will be considered untrustworthy. You can replace the compromised Subordinate CA without having to replace the entire organization\\'s certificate infrastructure. Subordinate CAs can be replaced, but a compromised Enterprise Root CA usually means you have to redeploy the Active Directory forest from scratch. If a Standalone Root CA is compromised, it also necessitates the replacement of an organization\\'s PKI infrastructure.