70-649 Q&As

TS: Upgrading Your MCSE on Windows Server 2003 to Windows Server 2008, Technology Specialist

Pass Microsoft 70-649 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.pass4lead.com/70-649.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

QUESTION 1

Your network contains a Web server that runs Windows Server 2008 R2.

Remote management is configured for Internet Information Services (IIS).

From IIS Manager Permissions, you add a user to a Web site.

You need to prevent the user from using Internet Information Services (IIS) Manager to modify the authorization rules of the Web site.

Which settings should you configure?

A. Authorization Rules

B. Feature Delegation

C. IIS Manager Permissions

D. IIS Manager Users

Correct Answer: B

QUESTION 2

Your network contains a server named Server1 that runs Windows Server 2008 R2.

You have a user named User1.

You need to ensure that User1 can view the events in the Security event log. The solution must minimize the number of rights assigned to User1.

What should you do?

A. In the Local Security Policy console, modify the Security Options.

B. In Event viewer, configure the properties of the Security log.

C. In Event viewer, filter the Security log.

D. In the Registry Editor, add a Security Descriptor Definition Language (SDDL) value.

Correct Answer: D

Microsoft Windows uses SDDL to develop and administer object security. SDDL defines security descriptors, which are text strings or binary data structures containing security information for one or more objects, e.g., file, folder, service or

unnamed process. Security descriptors use access control lists (ACLs) to manage access and control entries and audits. Each security descriptor contains a discretionary access control list (DACL) and system access control list (SACL).

The DACL controls access to an object, and the SACL controls logging of access attempts. In addition to the object owner name, most SDDL security descriptor strings are comprised of five parts.

These include DACL, SACL, group and header, which specifies inheritance level and permission.

QUESTION 3

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1. The Active Directory Federation Services (AD FS) role is installed on Server1. Contoso.com is defined as an account

store.

A partner company has a Web-based application that uses AD FS authentication. The partner company plans to provide users from contoso.com access to the Web application.

You need to configure AD FS on contoso.com to allow contoso.com users to be authenticated by the partner company.

What should you create on Server1?

A. a new application

B. a resource partner

C. an account partner

D. an organization claim

Correct Answer: D

The old answer was: a resource partner

Since the account store has already been configured, what needs to be done is to use the account store to map an AD DS global security group to an organization claim (called group claim extraction). So that\\'s what we need to create for

authentication: an organization claim.

Creating a resource/account partner is part of setting up the Federation Trust.

Reference 1:

http://technet.microsoft.com/en-us/library/dd378957.aspx Configuring the Federation Servers

[All the steps for setting up an AD FS environment are listed in an extensive step-by-step guide, too long to post here.]

Reference 2:

http://technet.microsoft.com/en-us/library/cc732147.aspx

Add an AD DS Account Store

If user and computer accounts that require access to a resource that is protected by Active Directory Federation Services (AD FS) are stored in Active Directory Domain Services (AD DS), you must add AD DS as an account store on a

federation server in the Federation Service that authenticates the accounts.

Reference 3:

http://technet.microsoft.com/en-us/library/cc731719.aspx Map an Organization Group Claim to an AD DS Group (Group Claim Extraction) When you use Active Directory Domain Services (AD DS) as the Active Directory Federation Services

(AD FS) account store for an account Federation Service, you map an organization group claim to a security group in AD DS. This mapping is called a group claim extraction.

QUESTION 4

Your network contains a Network Load Balancing (NLB) cluster named NLB01. NLB01 contains two servers named Node1 and Node2 that run Windows Server 2008 R2. Node1 and Node2 are configured as shown in the following table.

Server setting	Server configuration
Initial host state	Started
Retain suspended state after computer starts	Enabled

You need to install Windows updates on Node1 to meet the following requirements:

Prevent new connections to Node1 while the updates are installed. Provide connected users with the ability to complete their session on Node1 before the updates are installed.

What should you do first?

A. From Network Load Balancing Manager, right-click Model and click Drainstop.

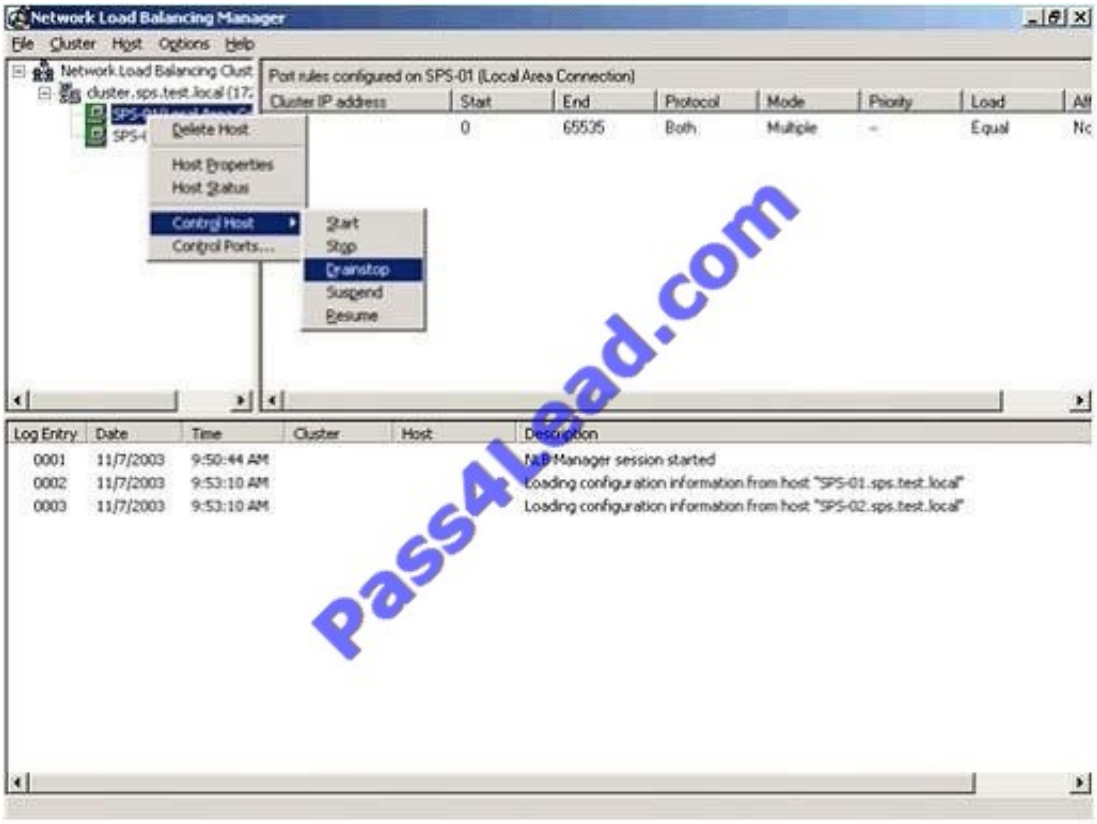
B. From Network Load Balancing Manager, right-click Node1 and click Suspend.

C. From the Services console, right-click Workstation and click Pause.

D. From the Services console, right-click Server and click Pause.

Correct Answer: A

Drainstopping is used to tell the server to continue processing existing requests but not accept any new requests, thus gracefully taking the server down.



http://office.microsoft.com/download/afile.aspx?AssetID=AM102437081033

QUESTION 5

Your company has an Active Directory domain. The company runs Remote Desktop services.

Standard Users who connect to the Remote Desktop Sessions Host Server are in an organizational unit (OU) named OU1. Administrative users are in OU1. No other users connect to the Remote Desktop Session Host Server.

You need to ensure that only members of OU1 can run Remote Desktop Protocol files.

What should you do?

A. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and user\\'s default .rdp settings policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to OU1.

B. Create a Group Policy object (GPO) that configures the Specify SHA1 thumbprints of certificates represting trusted .rdppublishers policy setting in the Remote Desktop Client Connection template to Enabled. Apply the GPO to OU1.

C. Create a Group Policy object (GPO) that configures the Allow .rdp files from unknown publishers policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to OU1.

D. Create a Group Policy object (GPO) that configures the Allow .rdp files from valid publishers and user\\'s default .rdp settings policy setting in the Remote Desktop Client Connection template to Disabled. Apply the GPO to OU1.

Correct Answer: B

To ensure that only members of the TermSerAdmin OU can run the Remote Desktop Protocol files, you need to enable

the Allow .rdp files from valid publishers and users default .rdp settings policy setting in the Remote Desktop Client Connection template. This policy setting allows you to specify whether users can run Remote Desktop Protocol (.rdp) files from a publisher that signed the file with a valid certificate. A valid certificate is one issued by an authority recognized by the client, such as the issuers in the client\\'s Third-Party Root Certification Authorities certificate store. This policy setting also controls whether the user can start an RDP session by using default .rdp settings (for example, when a user directly opens the Remote Desktop Connection [RDC] client without specifying an .rdp file). If you enable this policy setting, users can run .rdp files that are signed with a valid certificate. Users can also start an RDP session with default .rdp settings by directly opening the RDC client. When a user starts an RDP session, the user is asked to confirm whether they want to connect. If you disable this policy setting, users cannot run .rdp files that are signed with a valid certificate. Additionally, users cannot start an RDP session by directly opening the RDC client and specifying the remote computer name. When a user tries to start an RDP session, the user receives a message that the publisher has been blocked

Reference: Remote Desktop Connection Client

http://technet2.microsoft.com/windowsserver2008/en/library/76fb7e12-b823-429b-9887-05dc70d28d0c1033.mspx?mfr=true

Other ref:

Using Group Policy settings to control client behavior when opening a digitally signed .rdp file

You can use Group Policy settings to configure clients to always trust RemoteApp programs from a particular publisher. You can also configure whether clients will block RemoteApp programs and remote desktop connections from external or

unknown sources. By using these policy settings, you can reduce the number and complexity of security decisions that users face. This reduces the chances of inadvertent user actions that may lead to security vulnerabilities.

The relevant Group Policy settings are located in the Local Group Policy Editor at the following location, in the Computer Configuration node and in the User Configuration node:

Administrative Templates\Windows Components\Terminal Services\Remote Desktop Connection Client

The available policy settings include the following:

Specify SHA1 thumbprints of certificates representing trusted .rdp publishers

This policy setting allows you to specify a list of Secure Hash Algorithm 1 (SHA1) certificate thumbprints that represent trusted .rdp file publishers. If you enable this policy setting, any certificate with a SHA1 thumbprint that matches a

thumbprint on the list is trusted.

Allow .rdp files from valid publishers and user\\'s default .rdp settings

This policy setting allows you to specify whether users can run .rdp files from a publisher that signed the file with a valid certificate. This policy setting also controls whether the user can start an RDP session by using default .rdp settings, such

as when a user directly opens the RDC client without specifying an .rdp file.

Allow .rdp files from unknown publishers

This policy setting allows you to specify whether users can run unsigned .rdp files and .rdp files from unknown publishers on the client computer.

Latest 70-649 Dumps 70-649 Practice Test 70-649 Study Guide

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: