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.geekcert.com/70-649.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

Your network contains two standalone servers named Server1and Server2 that have Active Directory Lightweight Directory Services (AD LDS) installed.

Server1 has an AD LDS instance.

You need to ensure that you can replicate the instance from Server1 to Server2.

What should you do on both servers?

A. Obtain a server certificate.

B. Import the MS-User.ldf file.

C. Create a service user account for AD LDS.

D. Register the service location (SRV) resource records.

Correct Answer: C

Explanation: http://technet.microsoft.com/en-us/library/dd548356(v=WS.10).aspx Or/And Considerations when using a domain-based service account with AD LDS By Tony Murray on Monday, April 13, 2009 9:39 PM When creating an AD LDS instance you are prompted to specify an account to use as the service account. At this point you can specify either the Network Service account or another account. Unless you have a particular need, you should choose the built-in Network Service account. If you opt for a domain-based service account you have to jump through a whole lot of hoops to get things working. Also, you typically end up giving your domain-based service account more permissions than are strictly necessary (as described later in this article). The Network Service account on the other hand provides an easy set up option and is a good choice from a security perspective given that the account has limited access to the local computer.

So why bother to use a domain-based service account at all? Well, if you have a number of services on your server all running under the context of the Network Service account there is potential for security compromise. In this scenario you may want to consider isolating the services from each other using dedicated service accounts.

What follows is a discussion of the steps required to configure AD LDS to use a domainbased service account.

1.

Create a user account in AD.

The account doesn\\'t require any specific group memberships. As a service account, you may want to give some thought to the "Password Never Expires" setting, as well as password complexity.

2.

Permission to create serviceConnectionPoint objects. The account you have created requires the ability to create Service Connection Point objects in AD. These objects are typically created automatically as child objects of the AD LDS

computer object when the service is started.

The simplest method is to set the permission using DSACLS. You could alternatively use the security editor from within dsa.msc or adsiedit.msc, but you would first need to edit the %

systemroot%\system32\dssec.dat file to expose the serviceConnectionPoint object. Here\\'s the syntax using DSACLS:

C:\>dsacls /G :CC;"serviceConnectionPoint" e.g.

C:\>dsacls "CN=ADLDS1,OU=Servers,DC=Widget,DC=com" /G MyDom\ADLDS_SVC:

CC;"serviceConnectionPoint"

The setting should appear similar to that shown in the screenshot below.

3.

Permission to create servicePrincipalName objects. Your service account also needs permissions to create Service Principal Name (SPN). The SPNs are generated automatically as attributes of the service account itself in AD when the

service is first started. Note that this is different from the behaviour when running the service under the Network Service account. When using Network Service, the SPNs are created as attributes of the AD LDS server\\'s computer object. To

set the permissions, assign the SELF account Read/Write servicePrincipalName. The permissions are applied onto This object only on the service account object. Here\\'s an example using DSACLS.

C:\>dsacls /G SELF:RPWP;"servicePrincipalName" e.g.

C:\>dsacls "CN=ADLDS_SVC,OU=Service Account,DC=Widget,DC=com" /G SELF:

4.

Grant "Log on as a service" user rights

The service account requires Log on as service user rights on the server running the AD LDS instance. You don\\'t normally have to assign this right in advance because you will be prompted when creating the instance using the setup wizard.

If you have to set this right manually, use the Group Policy Editor to edit the local policy, or alternatively use the GPMC to edit an appropriate domain policy. The location of the setting

is:

Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> User Rights Assignment.

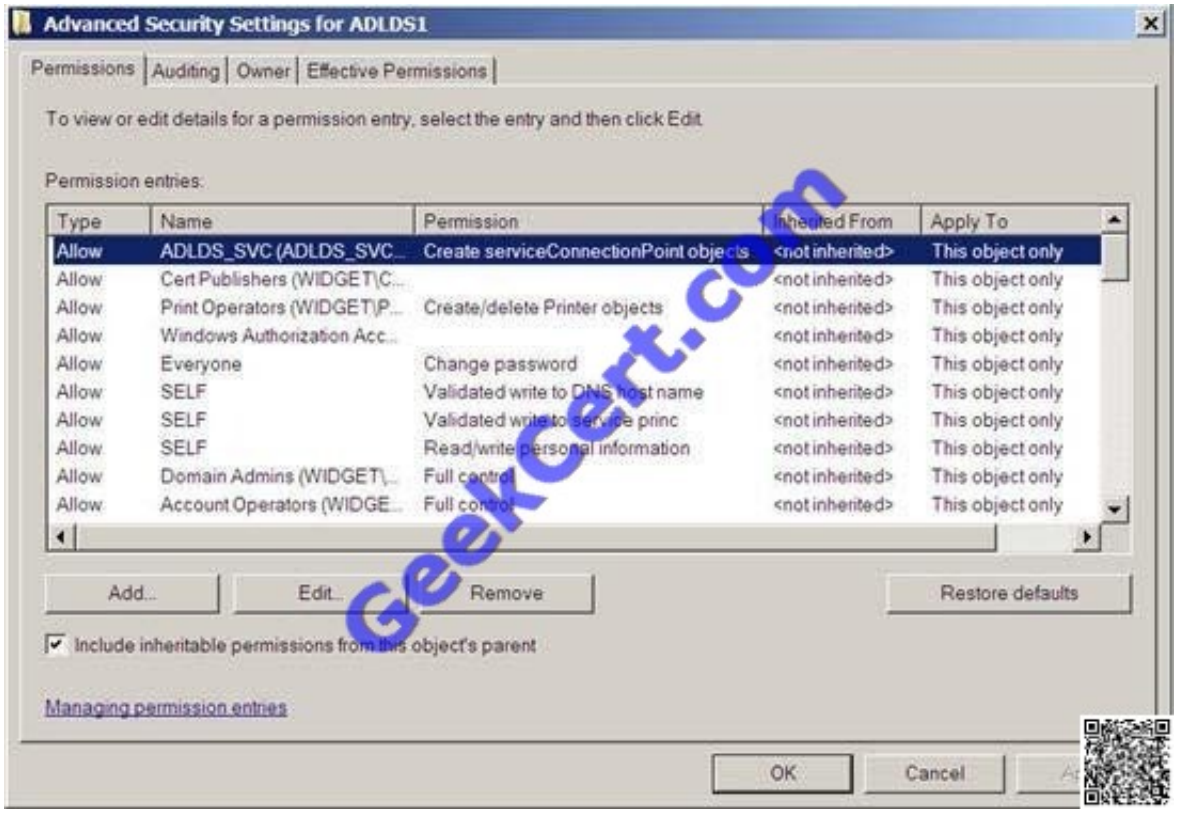
The screenshot below shows the setting.

5.

Membership of the local Administrators group.

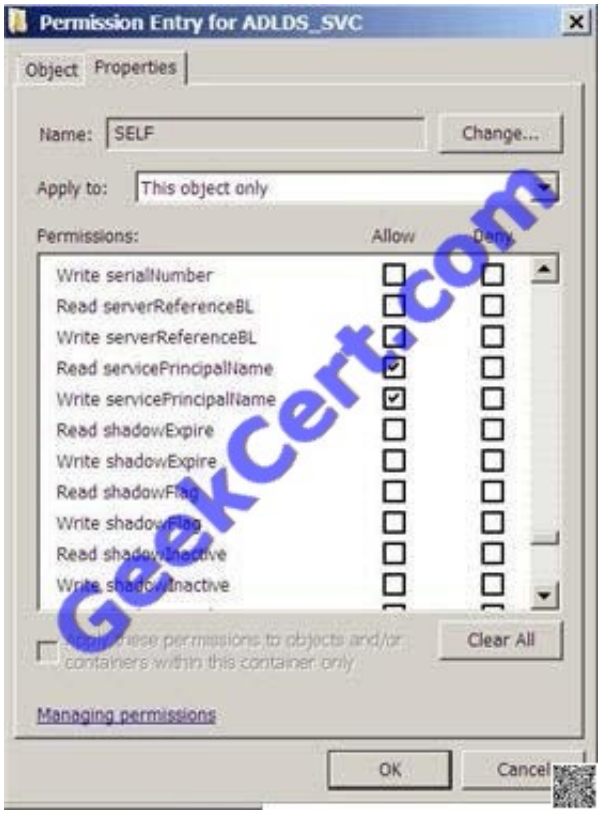
At the time of writing, the AD LDS product documentation indicates that the service account is not required to be a member of the local Administrators group on server running the AD LDS instance. However, my experience is that without this,

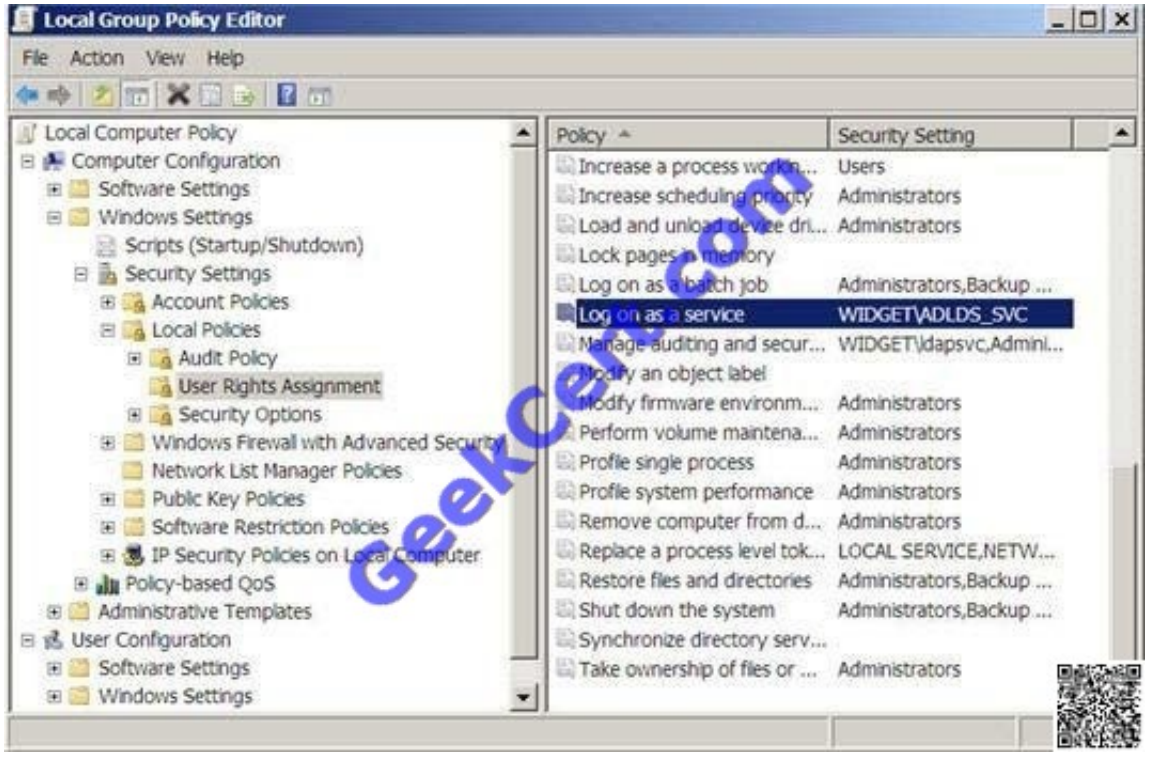
the following error is generated in the event log corresponding to the instance each time the service is re-started.



RPWP;"servicePrincipalName"

The screenshot below shows how the permissions should appear.





Log Name: ADAM (instance1)

Source: ADAM [instance1] General

Date: 6/04/2009 11:22:08 a.m.

Event ID: 1168

Task Category: Internal Processing

Level: Error

Keywords: Classic

User: ANONYMOUS LOGON

Computer: ADLDS1.widget.com

Description:

Internal error: An Active Directory Lightweight Directory Services error has occurred.

Additional Data

Error value (decimal):

-1073741790

Error value (hex):

c0000022

Internal ID:

3000715

The fact that the service account requires membership of the local Administrators group makes the choice to use Network Service even more compelling. The Network Service account has a lower level of privilege on the local machine than

that of members of the Administrators group. This implies the potential for compromise is lower when using Network Service.

Conclusion

As you can see, using domain-based service accounts for your AD LDS instances requires a fair amount of extra work during setup. I recommend that you use Network Service unless your circumstances require you to use a domain account.

QUESTION 2

Your network contains a Key Management Service (KMS) host named Server1.

On a client computer named Computer1 that runs Windows 7, you discover the following error message in the Event log: "0xC004F00F. The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance."

You need to prevent the error message from appearing on Computer1.

What should you do from Computer1?

A. Run slmgr.vbs /xpr.

B. Run slmgr.vbs /ato.

C. Restart the Windows Process Activation Service.

D. Restart the Windows Update service.

Correct Answer: B

Explanation: Error message: The Software Licensing Server reported that the hardware ID binding is beyond level of tolerance.

Cause: The hardware has changed, or the drivers were updated on the system.

Troubleshooting steps: For the

MAK, reactivate the system during the "Out of Tolerance" grace period by using online or telephone activation. For

KMS, run the slmgr.vbs -ato command.

http://technet.microsoft.com/en-us/library/ff793399.aspx

QUESTION 3

Your network contains a server named Server1 that runs a Server Core installation of Windows Server 2008 R2 Service Pack 1 (SP1) Standard.

You have a performance counter log on Server1.

You need to convert the performance counter log to a comma separated value (CSV) file.

Which tool should you use?

A. Perfmon

B. Typeper

C. Relog

D. Logman

Correct Answer: C

QUESTION 4

Your network contains a server named Server1 that runs Windows Server 2008 R2. Server1 has the Network Policy Server (NPS) role service installed.

You need to ensure that the NPS log files on Server1 contain information about the duration of client connections.

What should you do?

A. Enable the Accounting requests setting.

B. Configure the IAS (Legacy) log file format.

C. Configure the DTS Compliant log file format.

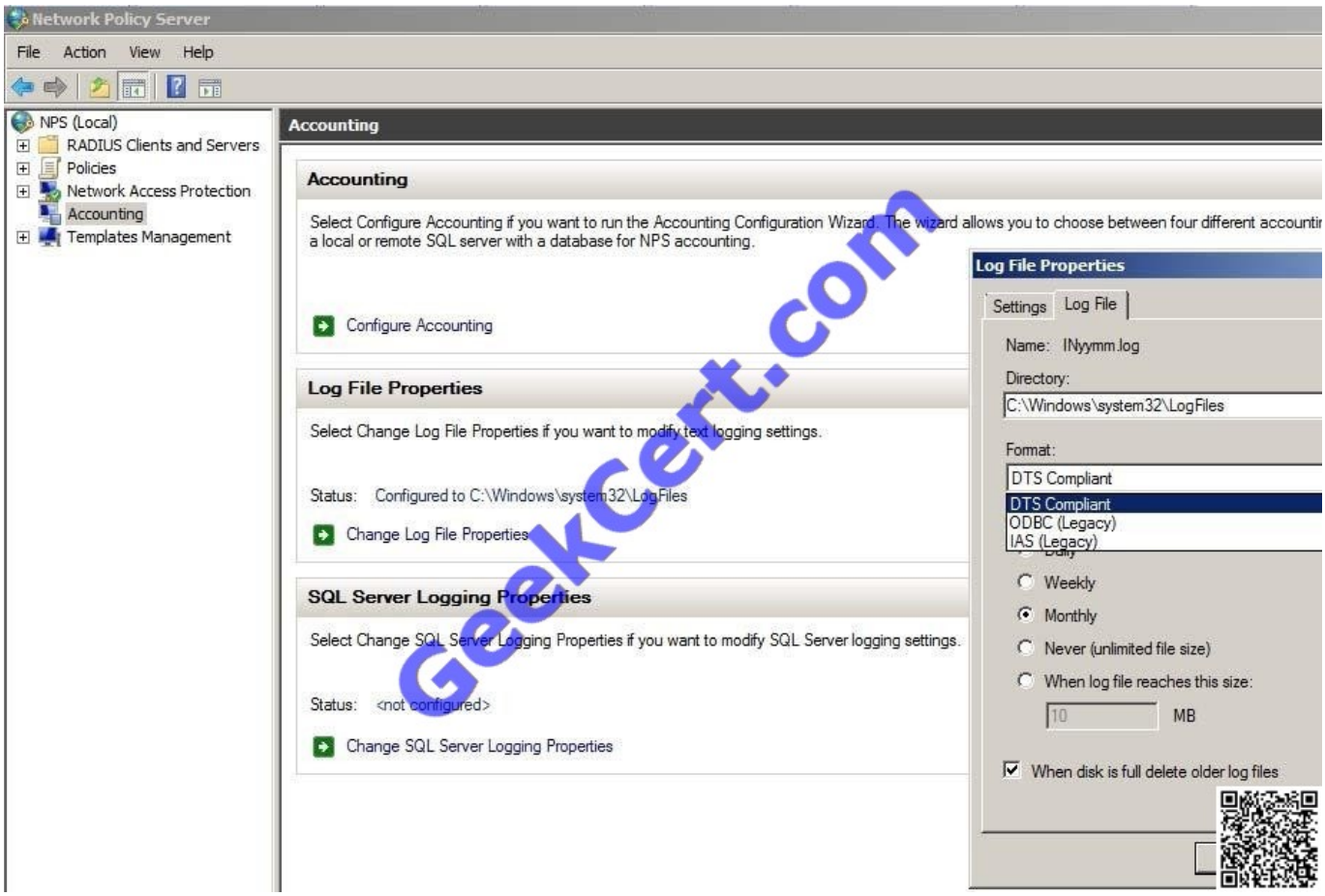
D. Enable the Authentication requests setting.

Correct Answer: C

The old answer was: Enable the Accounting requests setting. The DTS Compliant log format is the newest one and only its XML have attributes for session duration such as Acct-Session-Time = "The length of time (in seconds) for which the

session has been active.

http://technet.microsoft.com/en-us/library/cc771748(v=ws.10).aspx From NPS Console select Accounting Section.



QUESTION 5

Your company has an Active Directory domain. The company runs Remote Desktop Services. You configure the main office printer as the default printer on the Remote Desktop Session Host Server.

The company policy states that all remote client computers must meet the following requirements:

?The main office printer must be the default printer of the client computers.

?Users must be able to access their local printers during a remote desktop session.

You need to create a Group Policy object (GPO) by using the Remote Desktop Session Host Printer Redirection template to meet the company policy.

What should you do?

A. Set the Use Remote Desktop Easy Print printer driver first option to Disabled. Apply the GPO to all the client computers.

B. Set the Use Remote Desktop Easy Print printer driver first option to Disabled. Apply the GPO to the Remote Desktop Session Host Server.

C. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to all the client computers.

D. Set the Do not set default client printer to be default printer in a session option to Enabled. Apply the GPO to the Remote Desktop Session Host Server.

Correct Answer: D

Do not set default client printer to be default printer in a session This policy setting allows you to specify whether the client default printer is automatically set as the default printer in a Terminal Services session. By default, Terminal Services automatically designates the client default printer as the default printer in a Terminal Services session. You can use this policy setting to override this behavior. If you enable this policy setting, the default printer is the printer specified on the remote computer. If you disable this policy setting, the terminal server automatically maps the client default printer and sets it as the default printer upon connection. If you do not configure this policy setting, the default printer is not specified at the Group Policy level. However, an administrator can configure the default printer for client sessions by using the Terminal Services Configuration tool. Source: http://technet.microsoft.com/en-us/library/cc731963(WS.10).aspx