PassTest

Bessere Qualität , bessere Dienstleistungen!

Q&A

http://www.passtest.de

Einjährige kostenlose Aktualisierung

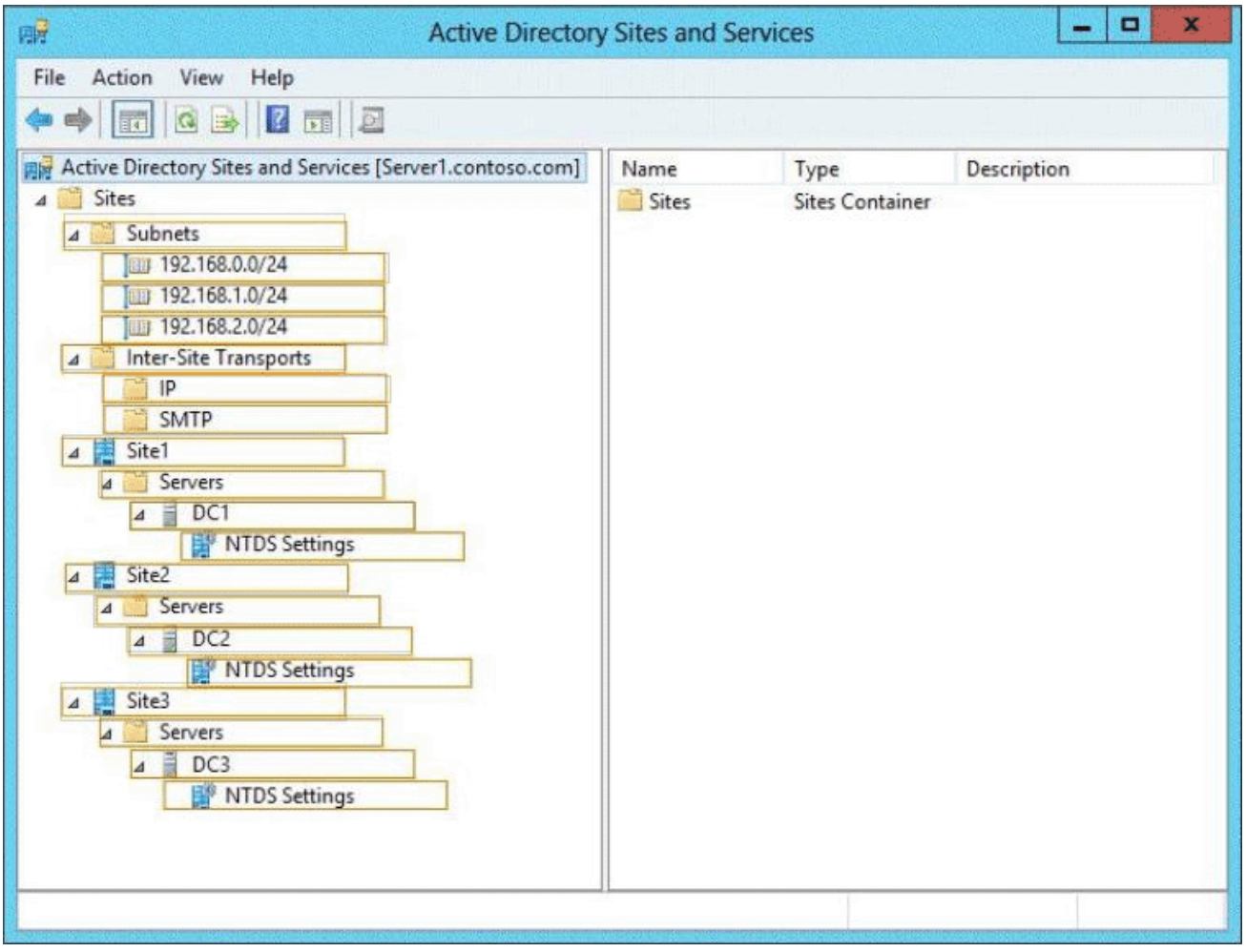
Exam : **070-412**

Title : Configuring Advanced Windows Server 2012 Services

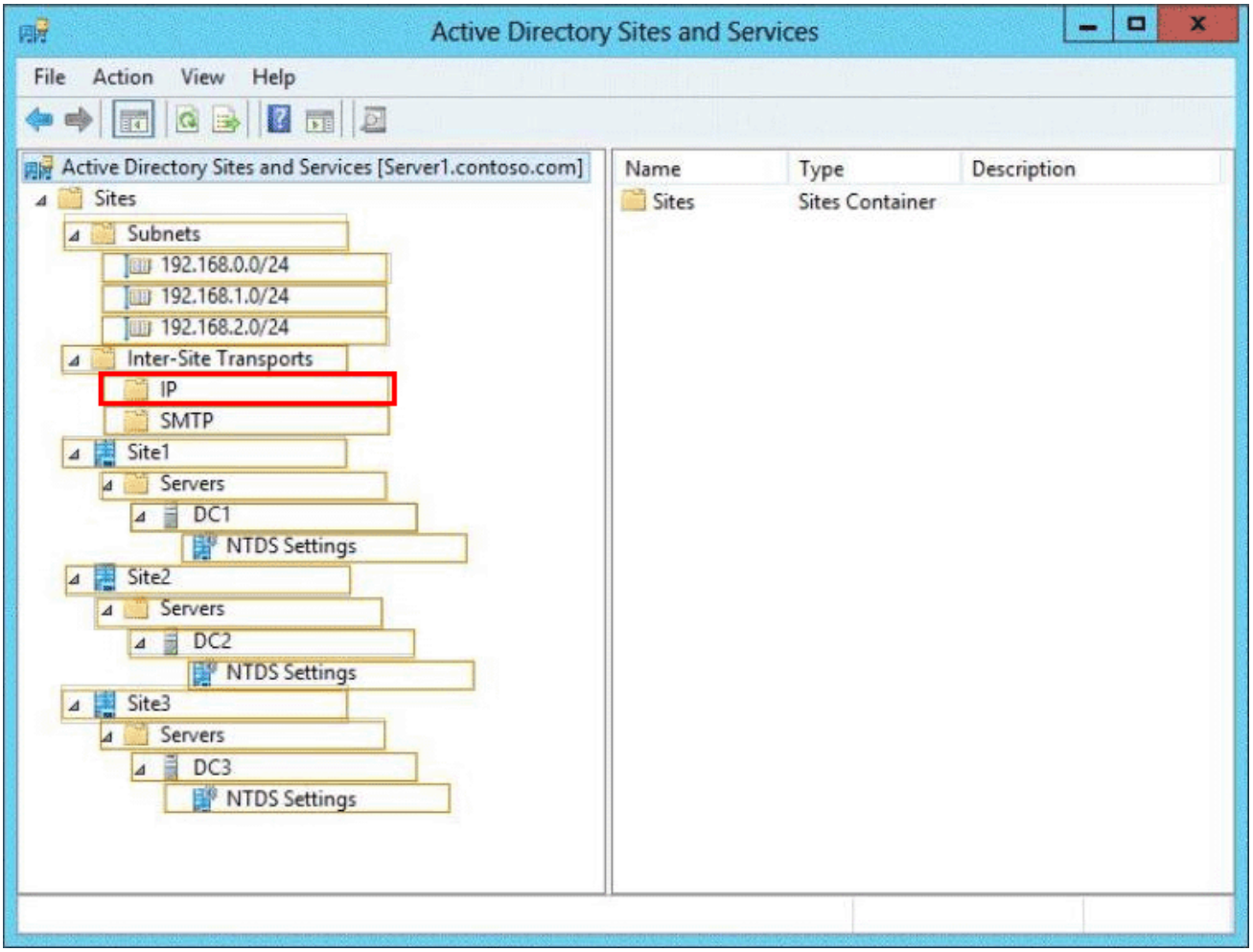
Version : DEMO

1.Your company recently deployed a new Active Directory forest named contoso.com. The first domain controller in the forest runs Windows Server 2012 R2. You need to identify the time-to-live (TTL) value for domain referrals to the NETLOGON and SYSVOL shared folders.
Which tool should you use?
A. Ultrasound
B. Replmon
C. Dfsdiag
D. Frsutil
Answer: C

2.HOTSPOT
Your network contains an Active Directory forest named contoso.com that contains a single domain. The forest contains three sites named Site1, Site2, and Site3. Domain controllers run either Windows Server 2008 R2 or Windows Server 2012 R2. Each site contains two domain controllers. Site1 and Site2 contain a global catalog server. You need to create a new site link between Site1 and Site2. The solution must ensure that the site link supports the replication of all the naming contexts.
From which node should you create the site link? To answer, select the appropriate node in the answer area.

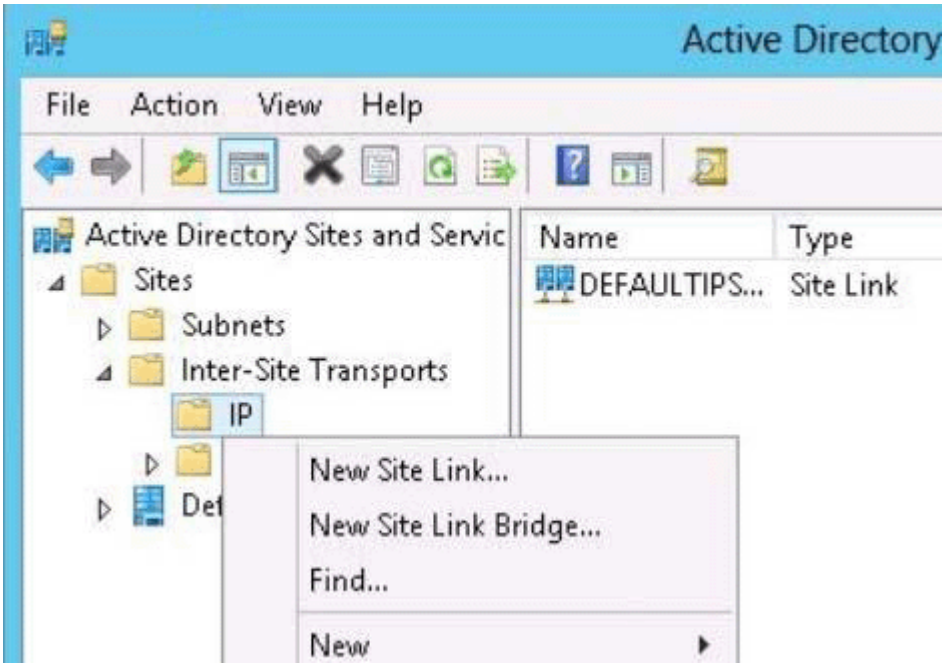


Answer:



Explanation:

http://technet.microsoft.com/en-us/library/cc731294.aspx



Create a site link

4 out of 4 rated this helpful - Rate this topic

Updated: May 1, 2010

Applies To: Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2

To create a site link

1. Open Active Directory Sites and Services.
2. In the console tree, right-click the intersite transport protocol you want the site link to use, and then click **New Site Link**.

   Where?

   - Active Directory Sites and Services/Sites/Inter-Site Transports/*inter-site transport protocol you want the site link to use*
3. In **Name**, type the name to be given to the link.
4. Click two or more sites to connect, and then click **Add**.
5. Configure the site link's cost, schedule, and replication frequency. See Related Topics for information.

3.Your network contains two Active Directory forests named contoso.com and adatum.com. Contoso.com contains one domain. Adatum.com contains a child domain named child.adatum.com. Contoso.com has a one-way forest trust to adatum.com. Selective authentication is enabled on the forest trust. Several user accounts are migrated from child.adatum.com to adatum.com. Users report that after the migration, they fail to access resources in contoso.com. The users successfully accessed the resources in contoso.com before the accounts were migrated. You need to ensure that the migrated users can access the resources in contoso.com.
What should you do?
A. Replace the existing forest trust with an external trust.
B. Run netdom and specify the /quarantine attribute.
C. Disable SID filtering on the existing forest trust.
D. Disable selective authentication on the existing forest trust.
Answer: C
Explanation:
A.
B. Enables administrators to manage Active Directory domains and trust relationships from the command prompt, /quarantine Sets or clears the domain quarantine
C. Need to gain access to the resources in contoso.com
D. Selective authentication over a forest trust restricts access to only those users in a trusted forest who have been explicitly given authentication permissions to computer objects (resource computers) that reside in the trusting forest
http://technet.microsoft.com/en-us/library/cc755321(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/cc758152(v=ws.10).aspx

Disabling SID Filter Quarantining on External Trusts

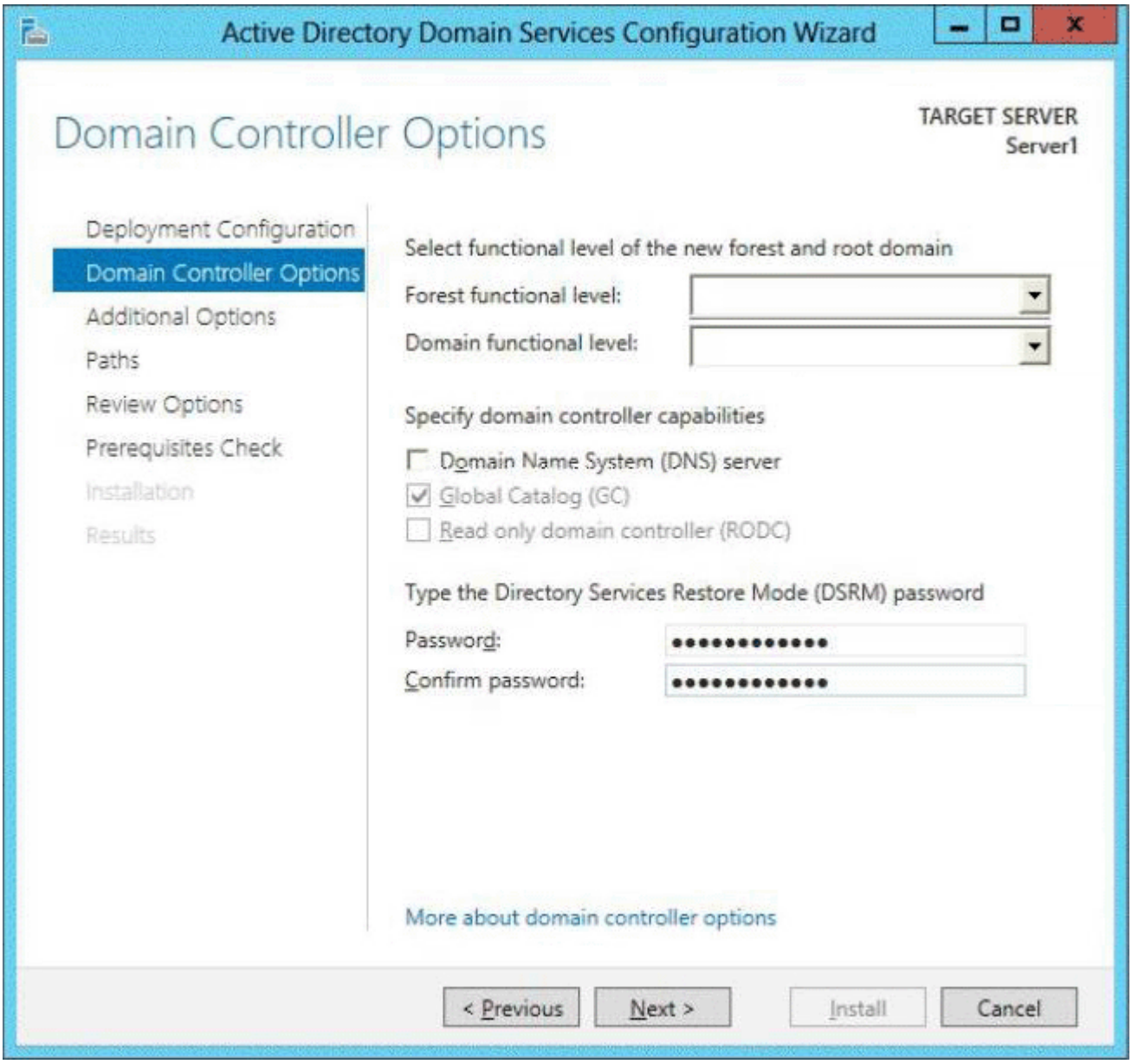
Although it reduces the security of your forest (and is therefore not recommended), you can disable SID filter quarantining for an external trust by using the Netdom.exe tool. You should consider disabling SID filter quarantining only in the following situations:

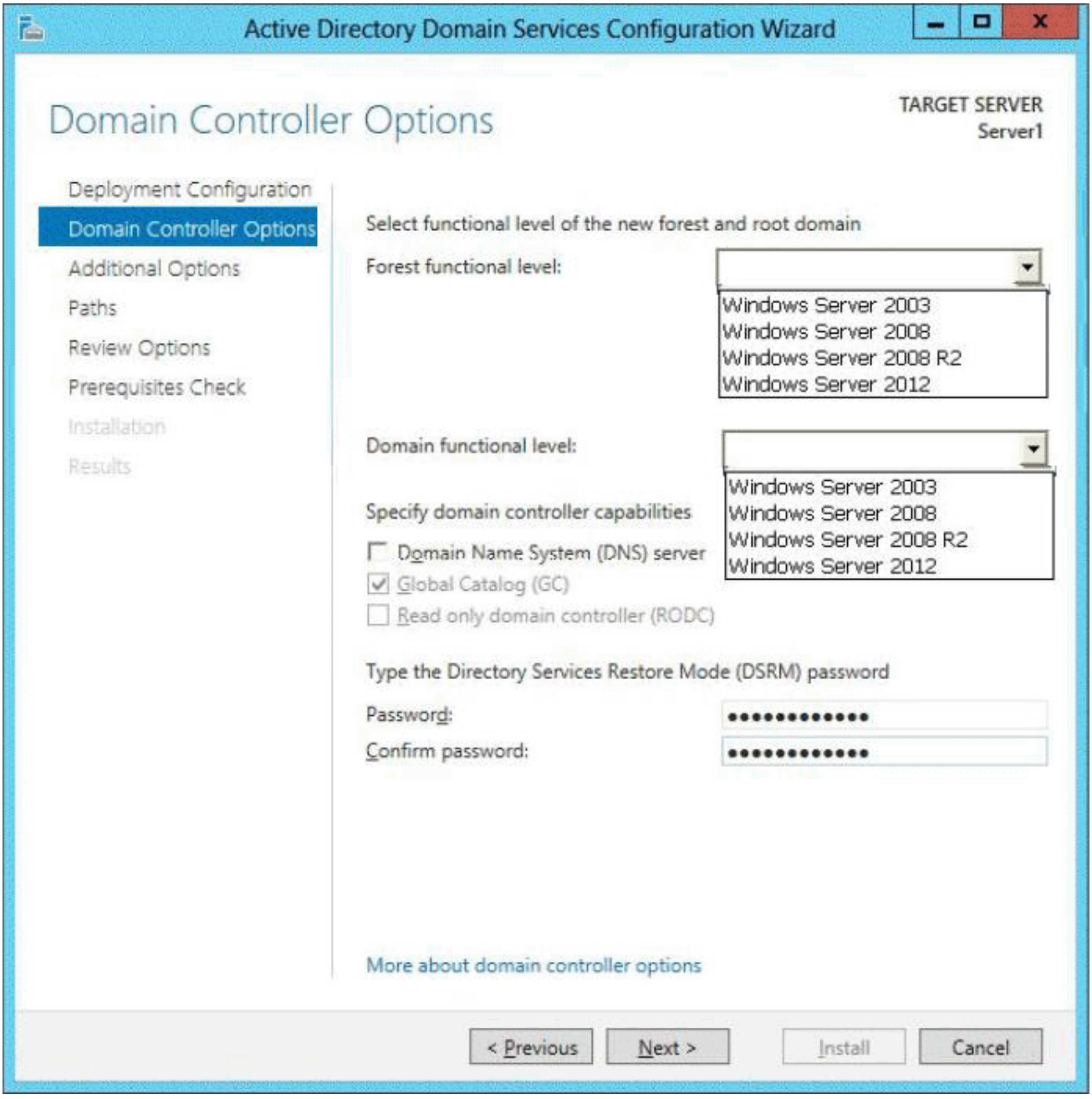
- You have an equally high level of confidence in the administrators who have physical access to domain controllers in the trusted domain and the administrators with such access in the trusting domain.
- You have a strict requirement to assign universal groups to resources in the trusting domain, even when those groups were not created in the trusted domain.
- Users have been migrated to the trusted domain with their SID histories preserved, and you want to grant them access to resources in the trusting domain based on the SID history attribute.

Only domain administrators or enterprise administrators can modify SID filtering settings. To disable SID filter quarantining for the trusting domain, type a command using the following syntax at a command-prompt:

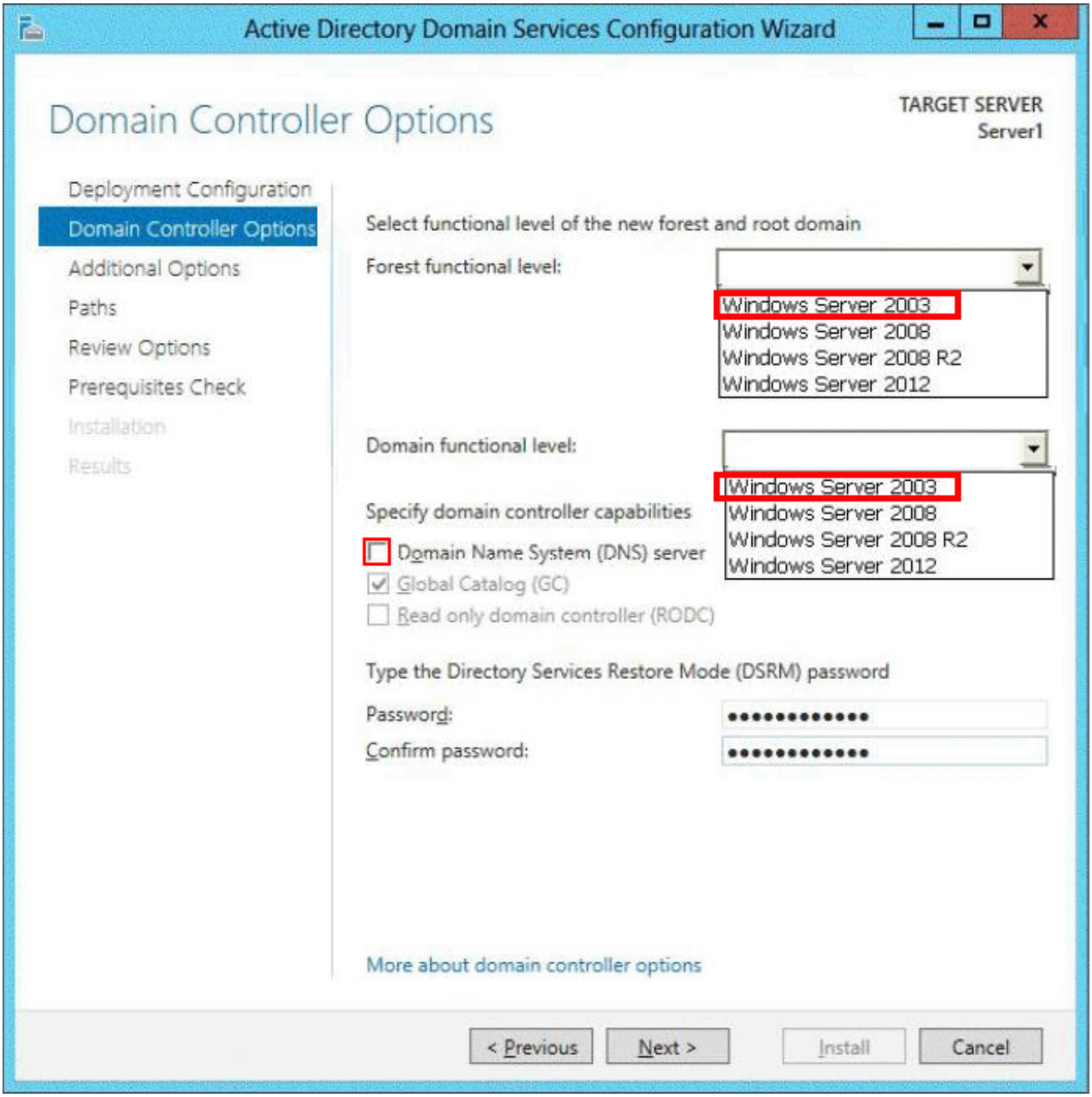
Netdom trust *TrustingDomainName* **/domain:** *TrustedDomainName* **/quarantine:No /usero:** *domainadministratorAcct* **/ passwordo:** *domainadminpwd*
To re-enable SID filtering, set the **/quarantine:** command-line option to **Yes**. For more information about Netdom, see "Domain and Forest Trust Tools and Settings."

4.HOTSPOT
Your network contains an Active Directory domain named contoso.com. The domain contains domain controllers that run either Windows Server 2003, Windows Server 2008 R2, or Windows Server 2012 R2.
You plan to implement a new Active Directory forest. The new forest will be used for testing and will be isolated from the production network. In the test network, you deploy a server named Server1 that runs Windows Server 2012 R2. You need to configure Server1 as a new domain controller in a new forest named contoso.test.
The solution must meet the following requirements:
- The functional level of the forest and of the domain must be the same as that of contoso.com.
- Server1 must provide name resolution services for contoso.test.
What should you do? To answer, configure the appropriate options in the answer area.


Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
Server1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Domain functional level:
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel


Active Directory Domain Services Configuration Wizard
Domain Controller Options
TARGET SERVER
Server1
Deployment Configuration
Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results
Select functional level of the new forest and root domain
Forest functional level:
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Domain functional level:
Windows Server 2003
Windows Server 2008
Windows Server 2008 R2
Windows Server 2012
Specify domain controller capabilities
Domain Name System (DNS) server
Global Catalog (GC)
Read only domain controller (RODC)
Type the Directory Services Restore Mode (DSRM) password
Password:
Confirm password:
More about domain controller options
< Previous
Next >
Install
Cancel

Answer:



5.Your network contains an Active Directory forest named adatum.com. The forest contains a single domain. The domain contains four servers.
The servers are configured as shown in the following table.

Server name	Configuration	Operating system
DC1	• Global catalog server • Domain controller • Schema master • DNS server	Windows Server 2003 R2
DC2	• Domain controller • PDC emulator • DHCP server • DNS server	Windows Server 2003 R2
DC3	• Infrastructure master • Global catalog server • Domain controller • WINS server	Windows Server 2008 R2
Server1	• Member server • WINS server • DNS server	Windows Server 2003 R2

You need to update the schema to support a domain controller that will run Windows Server 2012 R2.
On which server should you run adprep.exe?

A. Server1

B. DC3

C. DC2

D. DC1

Answer: B

Explanation:

You can use adprep.exe on domain controllers that run 64-bit versions of Windows Server 2008 or Windows Server 2008 R2 to upgrade to Windows Server 2012. You cannot upgrade domain controllers that run Windows Server 2003 or 32-bit versions of Windows Server 2008. To replace them, install domain controllers that run a later version of Windows Server in the domain, and then remove the domain controllers that Windows Server 2003.

Ref: http://technet.microsoft.com/en-us/library/hh994618.aspx#BKMK_UpgradePaths

http://technet.microsoft.com/en-us/library/dd464018(v=ws.10).aspx

◢ Considerations for using Adprep.exe in Windows Server 2012

In Windows Server 2012, Adprep.exe is integrated into the AD DS installation process and runs automatically as needed. For example, when you install the irst domain controller that runs Windows Server 2012 into an existing domain and forest, then adprep /forestprep and adprep /domainprep automatically run and report the results of the operations.

Some organizations may prefer to run Adprep.exe separately in advance of an AD DS installation. For this reason, Adprep.exe is also included in the \Support\Adprep folder of the operating system disk.

In Windows Server 2012, there is only one 64-bit version of Adprep.exe. It can be run remotely from any server that runs a 64-bit version of Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012.
The computer where you run it can be either domain-joined or in a workgroup.

The version of Adprep.exe in Windows Server 2012 includes new syntax and parameter options in order to run it remotely. For more information, see Adprep.