Guarantee All Exams 100% Pass One Time!

2016 70-412 NEW Dumps & 70-412 NEW Questions 392q RELEASED Today!

【Exam Code】 70-412
【Exam Name】 Configuring Advanced Windows Server 2012 Services
【Certification Provider】 Microsoft
【Corresponding Certifications】 MCSA: Windows Server 2012, MCSE: Desktop Infrastructure, MCSE: Private Cloud, MCSE: Server Infrastructure

2016 NEW 70-412 Study Guides:

Deploy, manage, and maintain servers
Configure File and Print Services
Configure network services and access
Configure a Network Policy Server (NPS) infrastructure
Configure and manage Active Directory
Configure and manage Group Policy

Braindump2go 2016 NEW 70-412 Dumps PDF & 70-412 NEW Exam Questions 392Q Free Share: 41-60

QUESTION 41
You have a server named Server1 that runs Windows Server 2012 R2.
You have a subscription to Windows Azure.
You need to register the Microsoft Azure Backup Agent on Server1.
What should you do first?

A. Install the Microsoft System Center 2012 Data Protection Manager (DPM) agent.
B. Create a backup vault.
C. Create Site Recovery vault.
D. Configure a passphrase for the Azure Backup Agent.

Answer: B
Explanation:
To back up files and data from your Windows Server to Azure, you must create a backup vault in the geographic region where you want to store the data. The main steps include:
* the creation of the vault you will use to store backups
* downloading a vault credential
* the installation of a backup agent
https://azure.microsoft.com/sv-se/documentation/articles/backup-configure-vault/

QUESTION 42
Your network contains an Active Directory domain named adatum.com. The domain contains a server named CA1 that runs Windows Server 2012 R2. CA1 has the Active Directory Certificate Services server role installed and is configured to support key archival and recovery.
You need to ensure that a user named User1 can decrypt private keys archived in the Active Directory Certificate Services (AD CS) database.
The solution must prevent User1 from retrieving the private keys from the AD CS database.
What should you do?

A. Assign User1 the Issue and Manage Certificates permission to Server1.
B. Assign User1 the Read permission and the Write permission to all certificate templates.
C. Provide User1 with access to a Key Recovery Agent certificate and a private key.
D. Assign User1 the Manage CA permission to Server1.

Answer: C
Explanation:
http://social.technet.microsoft.com/wiki/contents/articles/7573.active-directory-certificate-services-pki-keyarchival-and-management.aspx#Protecting_Key_Recovery_Agent_Keys

Understanding the Key Recovery Agent Role
KRAs are information technology (IT) administrators who can decrypt users' archived private keys. An organization can assign KRAs by issuing KRA certificates to designated administrators and configure them on the CA. The KRA role is not one of the default roles defined by the Common Criteria specifications but a virtual role that can provide separation between Certificate Managers and the KRAs. This allows the separation between the Certificate Manager, who can retrieve the encrypted key from the CA database but not decrypt it, and the KRA, who can decrypt private keys but not retrieve them from the CA database. For more information about how to implement KRAs, see Implementing Key Archival Walkthrough.

QUESTION 43
Your network contains an Active Directory domain named contoso.com.
The domain contains two sites named Site1 and Site2 and two domain controllers named DC1 and DC2. Both domain controllers are located in Site1.
You install an additional domain controller named DC3 in Site1 and you ship DC3 to Site2.
A technician connects DC3 to Site2.
You discover that users in Site2 are authenticated by all three domain controllers.
You need to ensure that the users in Site2 are authenticated by DC1 or DC2 only if DC3 is unavailable.
What should you do?

A. From Network Connections, modify the IP address of DC3.
B. In Active Directory Sites and Services, modify the Query Policy of DC3.
C. From Active Directory Sites and Services, move DC3.
D. In Active Directory Users and Computers, configure the insDS-PrimaryComputer attribute for the users in Site2.

Answer: C
Explanation:

http://social.technet.microsoft.com/wiki/contents/articles/7573.active-directory-certificateservices-pki-keyarchival-and-anagement.aspx#Protecting_Key_Recovery_Agent_Keys

Understanding the Key Recovery Agent Role

KRAs are information technology (IT) administrators who can decrypt users' archived private keys. An organization can assign KRAs by issuing KRA certificates to designated administrators and configure them on the CA. The KRA role is not one of the default roles defined by the Common Criteria specifications but a virtual role that can provide separation between Certificate Managers and the KRAs. This allows the separation between the Certificate Manager, who can retrieve the encrypted key from the CA database but not decrypt it, and the KRA, who can decrypt private keys but not retrieve them from the CA database. For more information about how to implement KRAs, see Implementing Key Archival Walkthrough.

QUESTION 44
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: D
Explanation:
http://technet.microsoft.com/nl-nl/library/cc755321%28v=ws.10%29.aspx
Impact of Selective Authentication
Because all verification of incoming interforest authentication requests is done locally on the receiving domain controller in the trusting forest, access to resources in the trusting forest is likely to be extremely limited for a broad set of users on the network (which is the purpose of this security setting). Consequently, implementing selective authentication might require user education, particularly due to the following reasons:
Users browsing network resources through My Network Places to resources located in a trusting forest might get access denied messages when attempting to access those resources.
Resources in the trusting forest that were once available to users in a trusted forest might no longer be available.

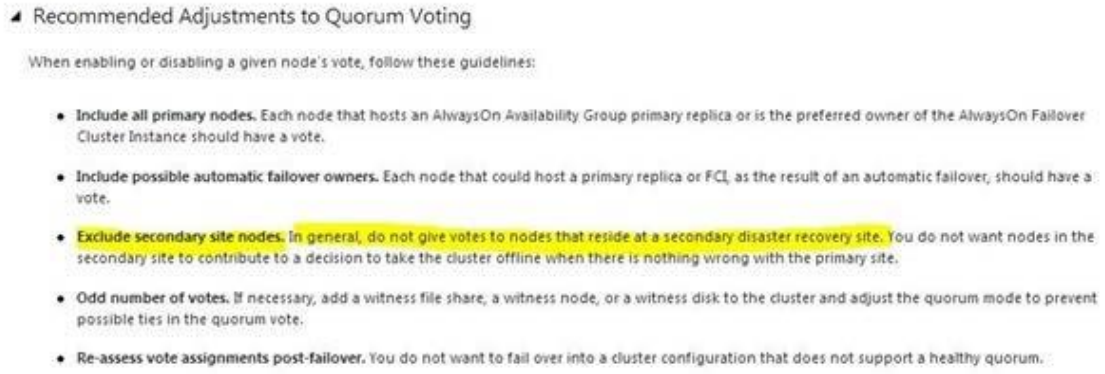
QUESTION 45
You have four servers that run Windows Server 2012 R2.
The servers have the Failover Clustering feature installed.
You deploy a new cluster named Cluster1.
Cluster1 is configured as shown in the following table.

Site name	Server name
Site1	Server1 Server2 Server3
Site2	Server4 Server5

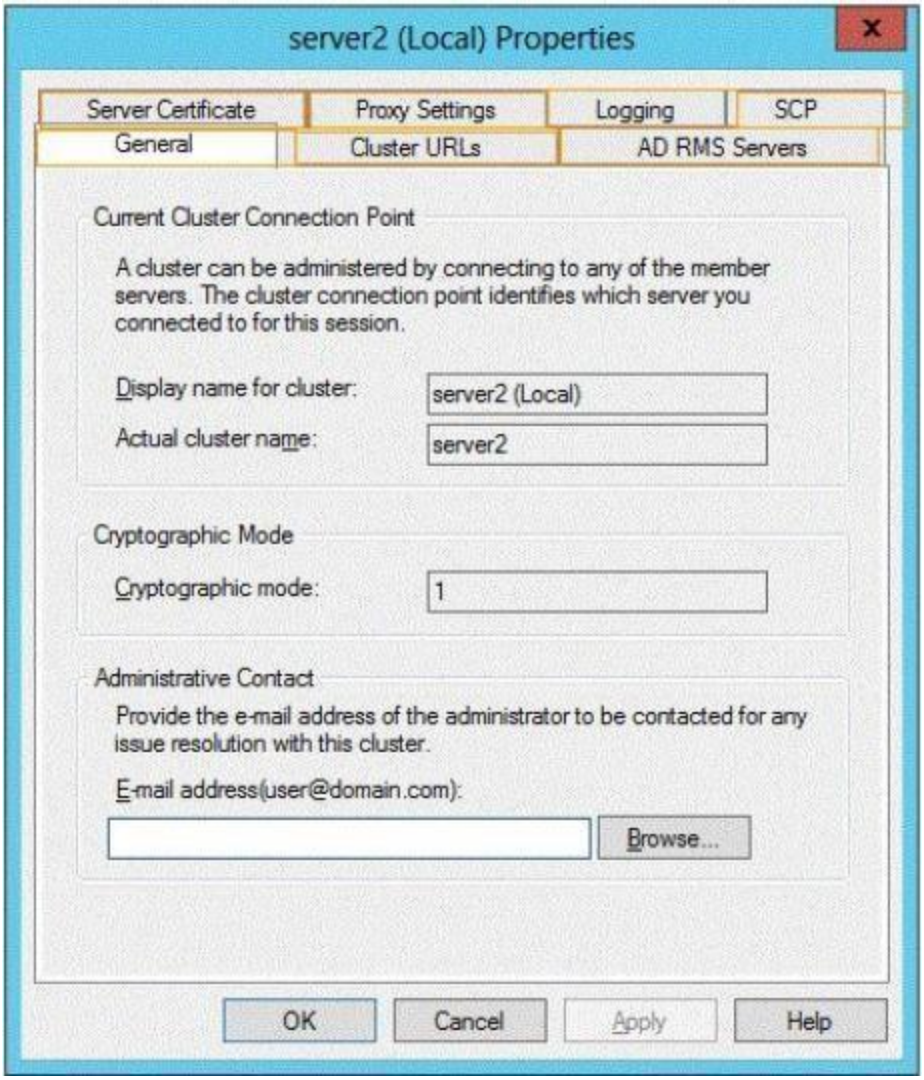
Site2 is a disaster recovery site. Server1, Server2, and Server3 are configured as the preferred owners of the cluster roles. Dynamic quorum management is disabled.
You plan to perform hardware maintenance on Server3.
You need to ensure that if the WAN link between Site1 and Site2 fails while you are performing maintenance on Server3, the cluster resource will remain available in Site1.
What should you do?

A. Enable dynamic quorum management.
B. Remove the node vote for Server3.
C. Add a file share witness in Site1.
D. Remove the node vote for [C1] Server4 and Server5.

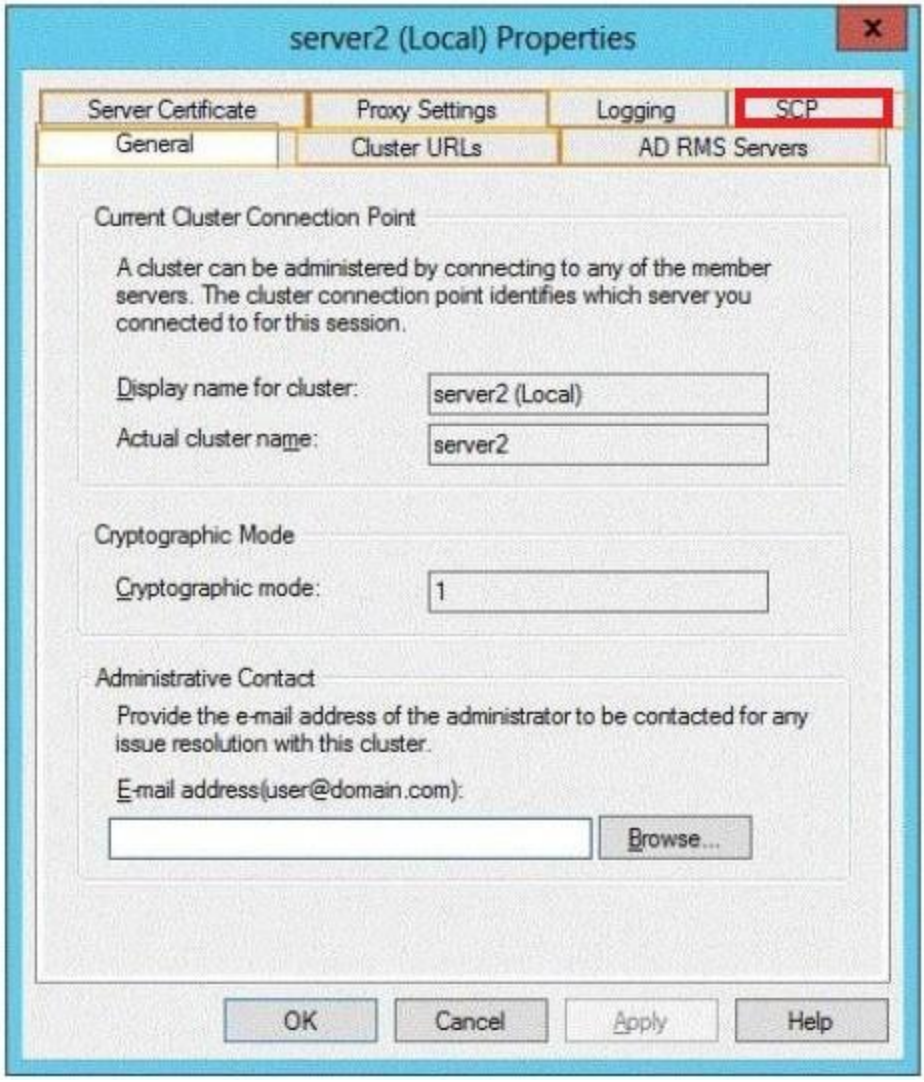
Answer: D
Explanation:
http://msdn.microsoft.com/en-us/library/hh270280.aspx#VotingandNonVotingNodes



QUESTION 46
Your network contains an Active Directory domain named contoso.com.
The domain contains a server named Server2 that runs Windows Server 2012 R2.
You are a member of the local Administrators group on Server2.
You install an Active Directory Rights Management Services (AD RMS) root cluster on Server2.
You need to ensure that the AD RMS cluster is discoverable automatically by the AD RMS client computers and the users in contoso.com.
Which additional configuration settings should you configure? To answer, select the appropriate tab in the answer area.


server2 (Local) Properties
Server Certificate
Proxy Settings
Logging
SCP
General
Cluster URLs
AD RMS Servers
Current Cluster Connection Point
A cluster can be administered by connecting to any of the member servers. The cluster connection point identifies which server you connected to for this session.
Display name for cluster:
server2 (Local)
Actual cluster name:
server2
Cryptographic Mode
Cryptographic mode:
1
Administrative Contact
Provide the e-mail address of the administrator to be contacted for any issue resolution with this cluster.
E-mail address(user@domain.com):
Browse...
OK
Cancel
Apply
Help

Answer:



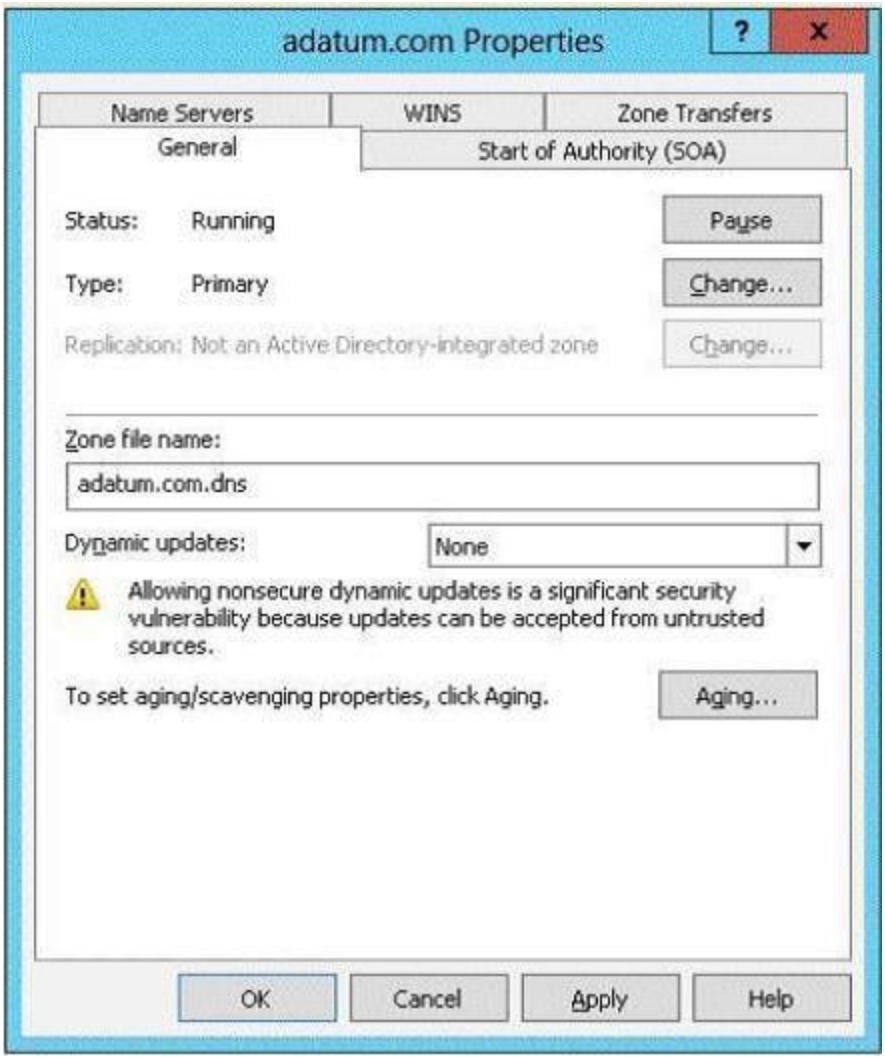
QUESTION 47

Your network contains an Active Directory domain named contoso.com.

The domain contains a domain controller named DC1 that runs Windows Server 2012 R2. DC1 has the DNS Server server role installed.

The network contains client computers that run either Linux, Windows 7, or Windows 8.

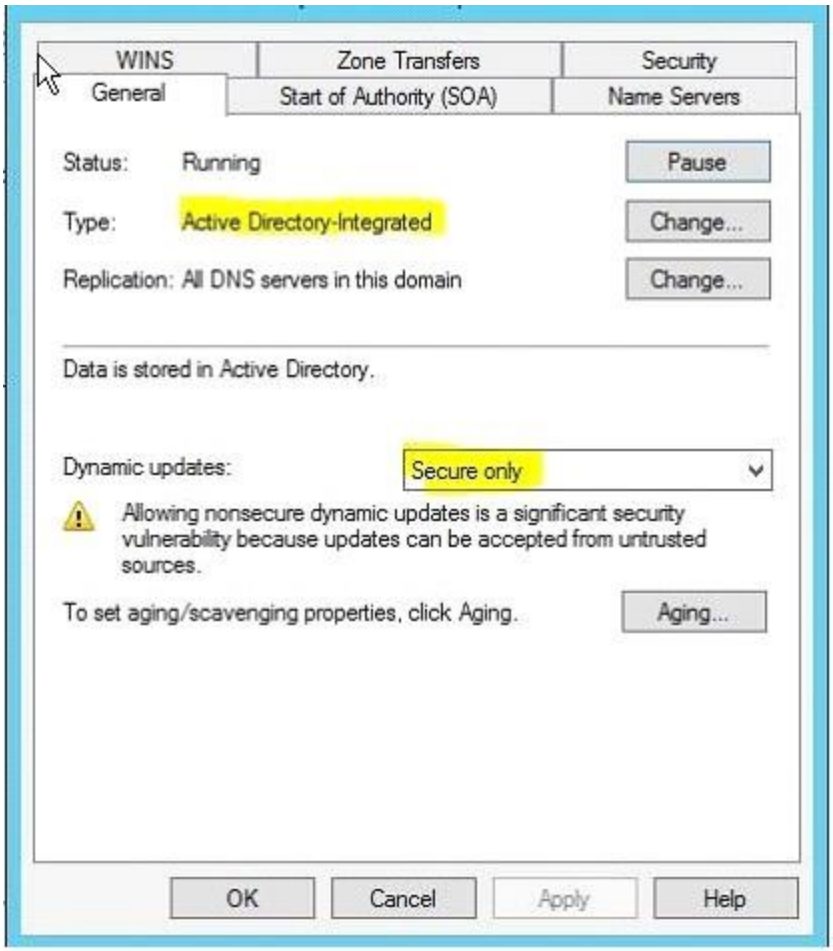
You have a zone named adatum.com as shown in the exhibit. (Click the Exhibit button.)



You plan to configure Name Protection on all of the DHCP servers.
You need to configure the adatum.com zone to support Name Protection.
Which two configurations should you perform from DNS Manager? (Each correct answer presents part of the solution. Choose two.)

A. Sign the zone.
B. Store the zone in Active Directory.
C. Modify the Security settings of the zone.
D. Configure Dynamic updates.
E. Add a DNS key record

Answer: BD
Explanation:
Name protection requires secure update to work.
Without name protection DNS names may be hijacked.
You can use the following procedures to allow only secure dynamic updates for a zone. Secure dynamic update is supported only for Active Directory-integrated zones. If the zone type is configured differently, you must change the zone type and directory-integrate the zone before securing it for Domain Name System (DNS) dynamic updates.
1. (B) Convert primary DNS server to Active Directory integrated primary
2. (D) Enable secure dynamic updates



http://technet.microsoft.com/en-us/library/ee941152(v=ws.10).aspx

QUESTION 48

You have a test server named Server1 that is configured to dual-boot between Windows Server 2008 R2 and Windows Server 2012 R2.

You start Server1 and you discover that the boot entry for Windows Server 2008 R2 no longer appears on the boot menu.

You start Windows Server 2012 R2 on Server1 and you discover the disk configurations shown in the following table.

Disk name	Volume letter	Operating system
Disk1	C	Windows Server 2012 system files
Disk2	D	Windows Server 2008 R2 system files

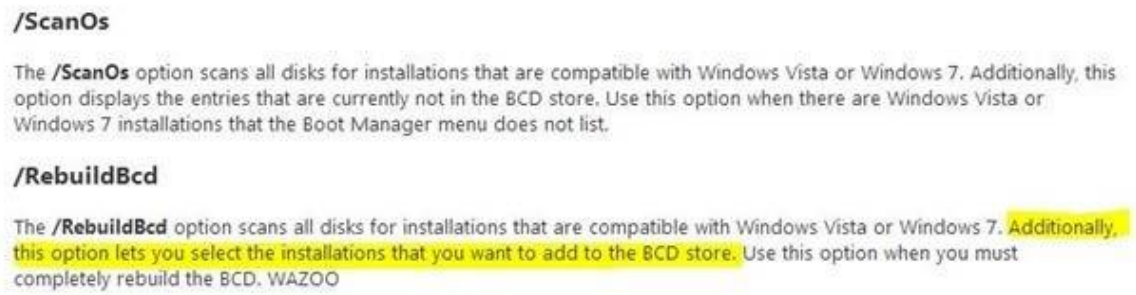
You need to restore the Windows Server 2008 R2 boot entry on Server1.

What should you do?

A. Run bcdedit.exe and specify the /createstore parameter.
B. Run bootrec.exe and specify the /scanos parameter.
C. Run bcdboot.exe d:\windows.
D. Run bootrec.exe and specify the /rebuildbcd parameter.

Answer: D

Explanation:
A. BCDEdit is a command-line tool for managing BCD stores. It can be used for a variety of purposes, including creating new stores, modifying existing stores, adding boot menu options, /Createstore Creates a new empty boot configuration data store.
The created store is not a system store.
B. Bootrec.exe tool to troubleshoot "Bootmgr Is Missing" issue. The /ScanOs option scans all disks for installations that are c mpatible with Windows Vista or Windows 7.
Additionally, this option displays the entries that are currently not in the BCD store.
Use this option when there are Windows Vista or Windows 7 installations that the Boot Manager menu does not list.
D. Bootrec.exe tool to troubleshoot "Bootmgr Is Missing" issue. The /ScanOs option scans all disks for installations that are compatible with Windows Vista or Windows 7.
Additionally, this option displays the entries that are currently not in the BCD store.
Use this option when there are Windows Vista or Windows 7 installations that the Boot Manager menu does not list.
http://technet.microsoft.com/en-us/library/cc709667(v=ws.10).aspx
http://support.microsoft.com/kb/927392/en-us



QUESTION 49
You have a DHCP server named Server1. Server1 has one network adapter. Server1 is located on a subnet named Subnet1. Server1 has scope named Scope1. Scope1 contains IP addresses for the 192.168.1.0/24 network. Your company is migrating the IP addresses on Subnet1 to use a network ID of 10.10.0.0/16. On Server11 you create a scope named Scope2.
Scope2 contains IP addresses for the 10.10.0.0/16 network.
You need to ensure that clients on Subnet1 can receive IP addresses from either scope.
What should you create on Server1?

A. A multicast scope
B. A scope
C. A superscope
D. A split-scope

Answer: C
Explanation:
A. Multicasting is the sending of network traffic to a group of endpointsdestination hosts. Only those members in the group of endpoints hosts that are listening for the multicast traffic (the multicast group) process the multicast traffic
B. A scope is an administrative grouping of IP addresses for computers on a subnet that use the Dynamic Host Configuration Protocol (DHCP) service. The administrator first creates a scope for each physical subnet and then uses the scope to define the parameters used by clients.
C. A superscope is an administrative feature of Dynamic Host Configuration Protocol (DHCP) servers running Windows Server 2008 that you can create and manage by using the DHCP Microsoft Management Console (MMC) snap-in.
By using a superscope, you can group multiple scopes as a single administrative entity.
http://technet.microsoft.com/en-us/library/dd759152.aspx

http://technet.microsoft.com/en-us/library/dd759218.aspx
http://technet.microsoft.com/en-us/library/dd759168.aspx

Configuring a DHCP Superscope

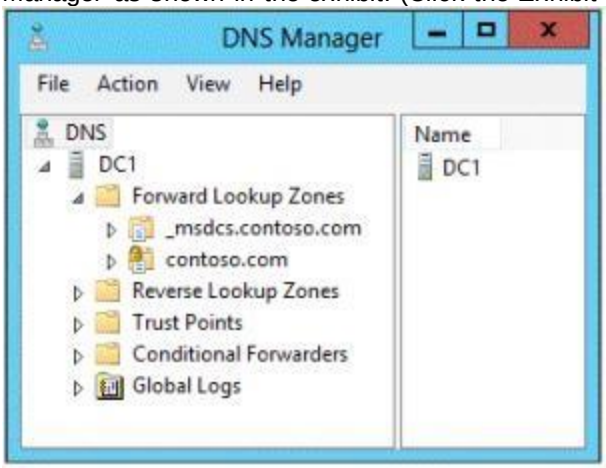
13 out of 17 rated this helpful - Rate this topic

Applies To: Windows Server 2008 R2

A *superscope* is an administrative feature of Dynamic Host Configuration Protocol (DHCP) servers running Windows Server 2008 that you can create and manage by using the DHCP Microsoft Management Console (MMC) snap-in. By using a superscope, you can group multiple scopes as a single administrative entity. With this feature, a DHCP server can:

- Support DHCP clients on a single physical network segment (such as a single Ethernet LAN segment) where multiple logical IP networks are used. When more than one logical IP network is used on each physical subnet or network, such configurations are often called *multinets*.
- Support remote DHCP clients located on the far side of DHCP and BOOTP relay agents (where the network on the far side of the relay agent uses multinets).

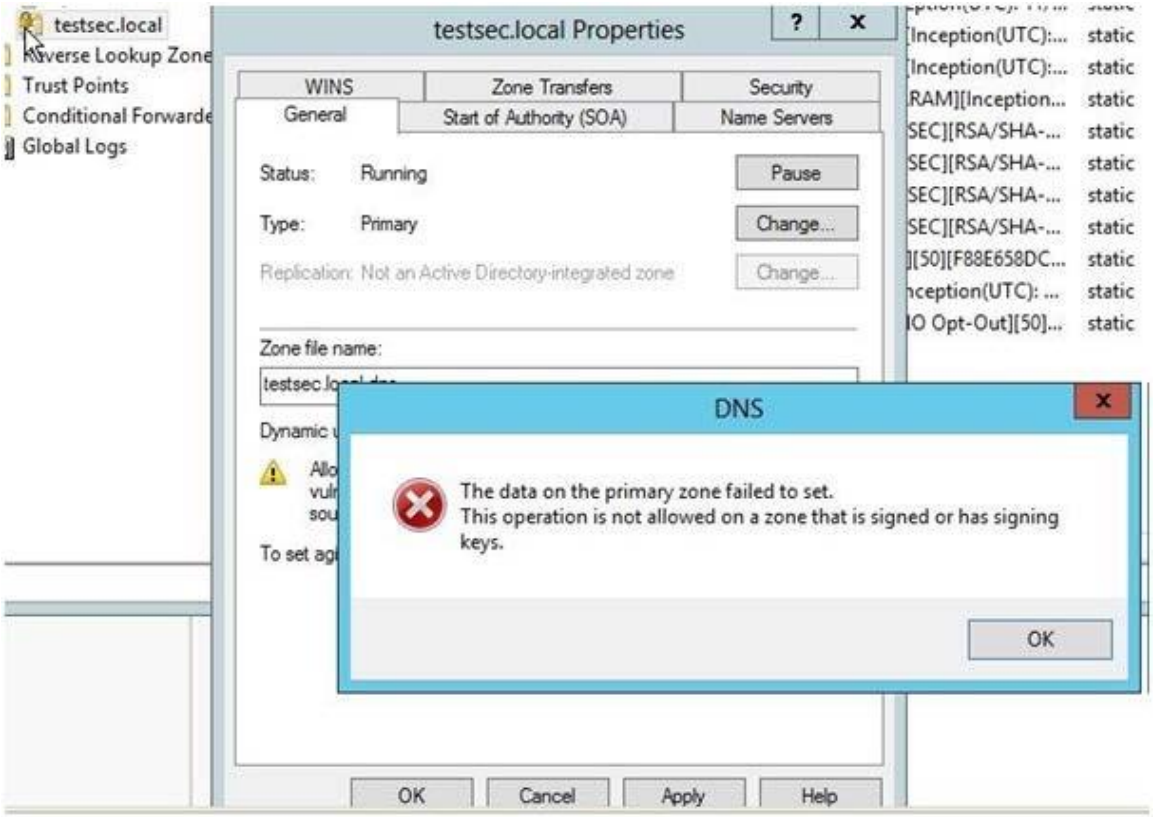
QUESTION 50
Your network contains an Active Directory domain named adatum.com. The domain contains a domain controller named DC1 that runs Windows Server 2012 R2. On Dc1, you open DNS Manager as shown in the exhibit. (Click the Exhibit button.)



You need to change the zone type of the contoso.com zone from an Active Directory-integrated zone to a standard primary zone.
What should you do before you change the zone type?

A. Unsign the zone.
B. Modify the Zone Signing Key (ZSK).
C. Modify the Key Signing Key (KSK).
D. Change the Key Master.

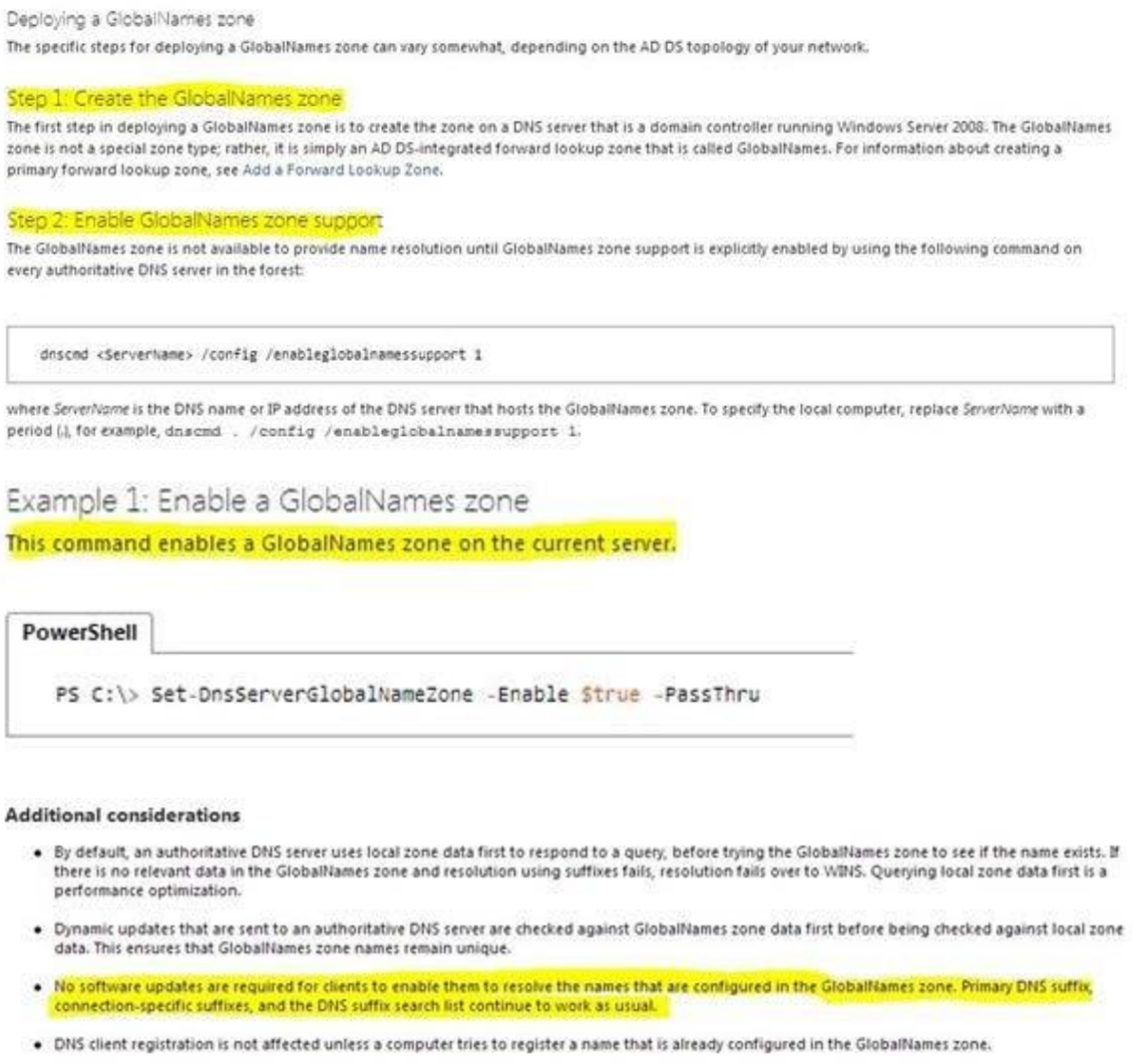
Answer: A
Explanation:
A. Lock icon indicating that it is currently signed with DNSSEC, zone must be unsignes
B. An authentication key that corresponds to a private key used to sign a zone.
C. The KSK is an authentication key that corresponds to a private key used to sign one or more other signing keys for a given zone.
Typically, the private key corresponding to a KSK will sign a ZSK, which in turn has a corresponding private key that will sign other zone data.
http://technet.microsoft.com/en-us/library/hh831411.aspx
http://technet.microsoft.com/en-us/library/ee649132(v=ws.10).aspx



QUESTION 51
You have a server named Server1 that runs Windows Server 2012 R2.
Server1 has the DNS Server server role installed.
You need to configure Server1 to resolve queries for single-label DNS names.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Run the Set-DNSServerGlobalNameZone cmdlet.
B. Modify the DNS suffix search list setting.
C. Modify the Primary DNS Suffix Devolution setting.
D. Create a zone named ".".
E. Create a zone named GlobalNames.
F. Run the Set-DNSServerRootHint cmdlet.

Answer: AE
Explanation:
http://technet.microsoft.com/en-us/library/cc731744.aspx
http://technet.microsoft.com/en-us/library/jj649907(v=wps.620).aspx



Deploying a GlobalNames zone

The specific steps for deploying a GlobalNames zone can vary somewhat, depending on the AD DS topology of your network.

Step 1: Create the GlobalNames zone

The first step in deploying a GlobalNames zone is to create the zone on a DNS server that is a domain controller running Windows Server 2008. The GlobalNames zone is not a special zone type; rather, it is simply an AD DS-integrated forward lookup zone that is called GlobalNames. For information about creating a primary forward lookup zone, see Add a Forward Lookup Zone.

Step 2: Enable GlobalNames zone support

The GlobalNames zone is not available to provide name resolution until GlobalNames zone support is explicitly enabled by using the following command on every authoritative DNS server in the forest:

```
dnscmd <ServerName> /config /enableglobalnamessupport 1
```

where *ServerName* is the DNS name or IP address of the DNS server that hosts the GlobalNames zone. To specify the local computer, replace *ServerName* with a period (.), for example, `dnscmd . /config /enableglobalnamessupport 1`.

Example 1: Enable a GlobalNames zone

This command enables a GlobalNames zone on the current server.

PowerShell

```
PS C:\> Set-DnsServerGlobalNameZone -Enable $true -PassThru
```

Additional considerations

- By default, an authoritative DNS server uses local zone data first to respond to a query, before trying the GlobalNames zone to see if the name exists. If there is no relevant data in the GlobalNames zone and resolution using suffixes fails, resolution fails over to WINS. Querying local zone data first is a performance optimization.
- Dynamic updates that are sent to an authoritative DNS server are checked against GlobalNames zone data first before being checked against local zone data. This ensures that GlobalNames zone names remain unique.
- No software updates are required for clients to enable them to resolve the names that are configured in the GlobalNames zone. Primary DNS suffix, connection-specific suffixes, and the DNS suffix search list continue to work as usual.
- DNS client registration is not affected unless a computer tries to register a name that is already configured in the GlobalNames zone.

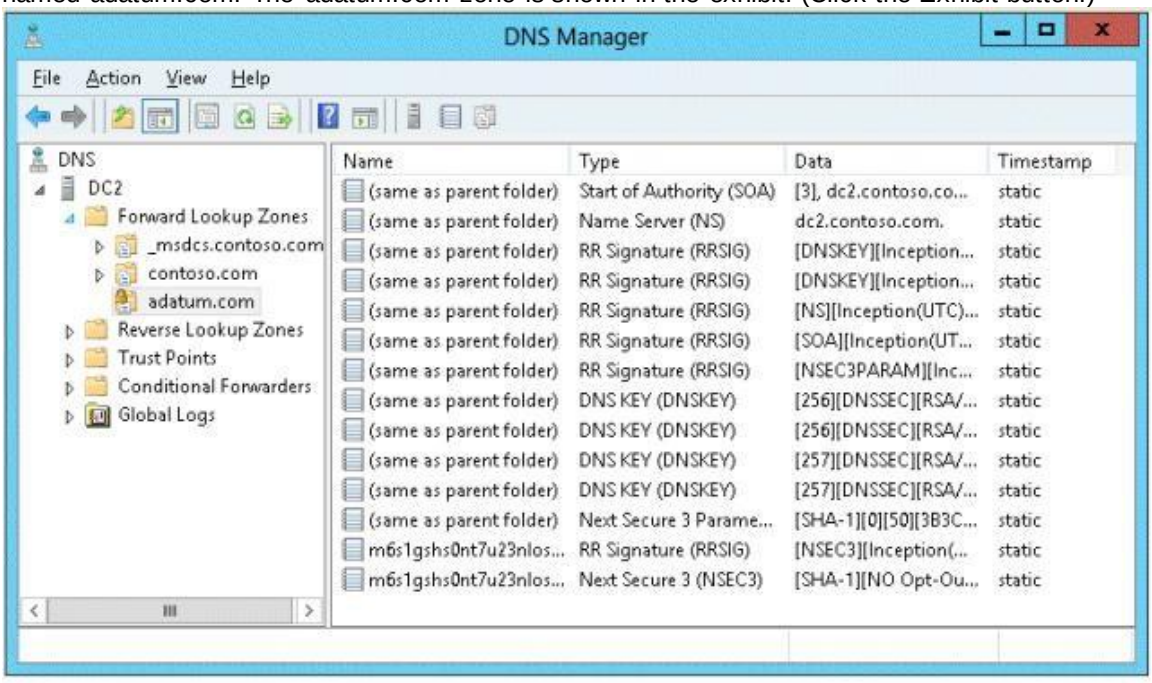
QUESTION 52
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 has the IP Address Management (IPAM) Server feature installed. Server2 has the DHCP Server server role installed. A user named User1 is a member of the IPAM Users group on Server1.
You need to ensure that User1 can use IPAM to modify the DHCP scopes on Server2.
The solution must minimize the number of permissions assigned to User1.
To which group should you add User1?

A. DHCP Administrators on Server2
B. IPAM ASM Administrators on Server1
C. IPAMUG in Active Directory
D. IPAM MSM Administrators on Server1

Answer: D
Explanation:
IPAM MSM administrators - Completely manages DHCP and DNS servers. IPAM MSM Administrators is a local security group on an IPAM server that is created when you install the IPAM feature. Members of this group have all the privileges of the IPAM Users security

group, and can perform server monitoring and management tasks
in addition to IPAM common management tasks.IPAM multi-server management (MSM) administrators can manage DNS and DHCP servers.
IPAM ASM Administrators on Server1 - Completely manages IP addresses.IPAM address space management (ASM) administrators can manage IP address blocks, ranges, and addresses.
IPAM Users Group (IPAMUG) - To access configuration data and server event logs, the IPAM server must be a member of the domain IPAM Users Group (IPAMUG).
DHCP Administrators - Members of the DHCP Administrators group can view and modify any settings on the DHCP server. DHCP Administrators can create and delete
scopes, add reservations, change option values, create superscopes, or perform any other task required to administer the DHCP server, including export or
import of the DHCP server configuration and database.
IPAM Users group - IPAM Users is a local security group on an IPAM server that is created when you install the IPAM feature. Members of this group can view all
information in server inventory, IP address space, and the monitor and manage IPAM console nodes. IPAM Users can view IPAM and DHCP operational events under in
the Event Catalog node, but cannot view IP address tracking data.
More info : https://technet.microsoft.com/en-us/library/dn268500.aspx
https://technet.microsoft.com/en-us/library/jj878311.aspx
https://technet.microsoft.com/en-us/library/dd759157.aspx
https://technet.microsoft.com/en-us/library/jj878342.aspx
https://technet.microsoft.com/en-us/library/jj878348.aspx

QUESTION 53
You have a server named DC2 that runs Windows Server 2012 R2. DC2 contains a DNS zone named adatum.com. The adatum.com zone is shown in the exhibit. (Click the Exhibit button.)

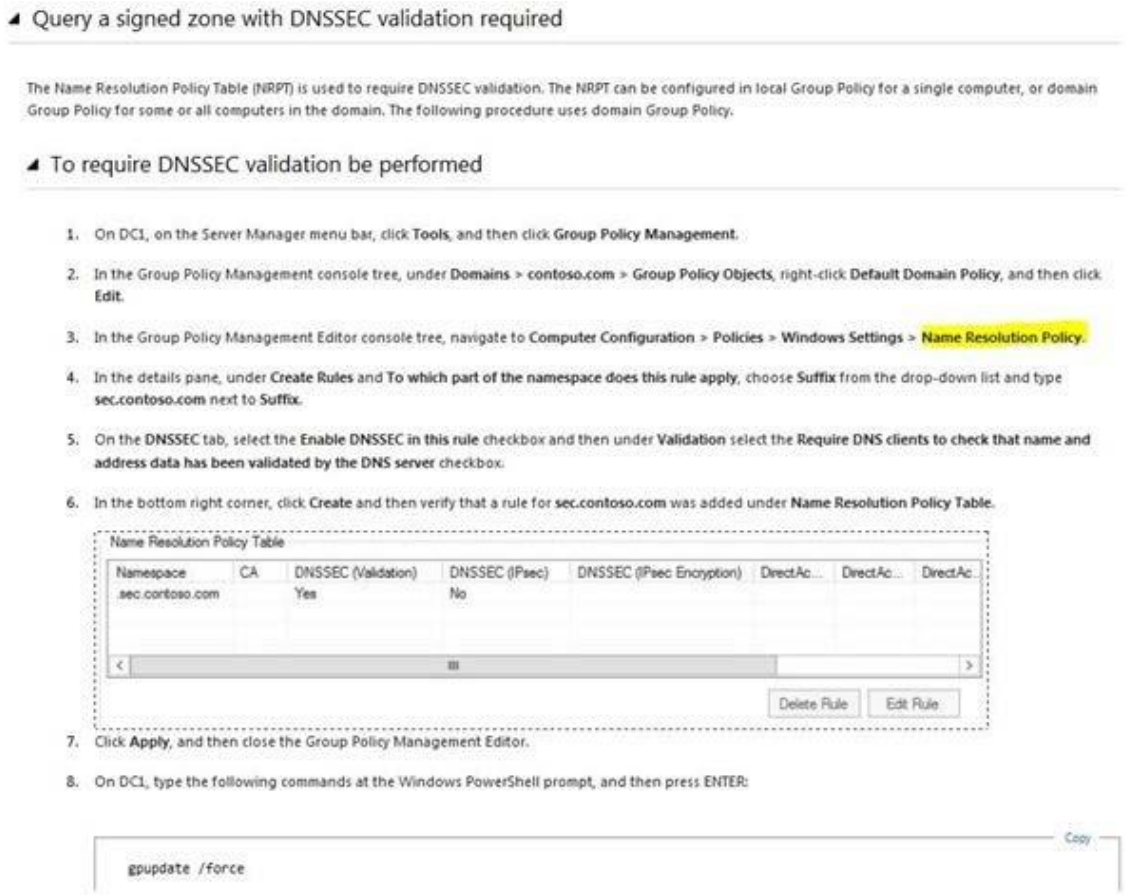


You need to configure DNS clients to perform DNSSEC validation for the adatum.com DNS domain.
What should you configure?

A. The Network Location settings
B. A Name Resolution Policy

C. The DNS Client settings
D. The Network Connection settings

Answer: B
Explanation:
B. The Name Resolution Policy Table (NRPT) is a table that contains rules you can configure to specify DNS settings or special behavior for names or namespaces. The NRPT can be configured using Group Policy or by using the Windows Registry.
C. client component that resolves and caches Domain Name System (DNS) domain names. When the DNS Client service receives a request to resolve a DNS name that it does not contain in its cache, it queries an assigned DNS server for an IP address for the name
D. Network connections make it possible for computers to access resources on the network and the internet
http://technet.microsoft.com/en-us/library/hh831411.aspx#config_client1



QUESTION 54
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 has the DHCP Server server role installed. Server2 has the Hyper-V server role installed. Server2 has an IP address of 192.168.10.50. Server1 has a scope named Scope1 for the 192.168.10.0/24 network. You plan to deploy 20 virtual machines on Server2 that will be connected to the external network. The MAC addresses for the virtual machines will begin with 00-15-SD-83-03.
You need to configure Server1 to offer the virtual machines IP addresses from 192.168.10.200 to 192.168.10.219. Physical computers on the network must be offered IP addresses outside this range.
You want to achieve this goal by using the minimum amount of administrative effort.

What should you do from the DHCP console?

A. Create reservations.
B. Create a policy.
C. Delete Scope1 and create two new scopes.
D. Configure Allow filters and Deny filters.

Answer: B
Explanation:
A. With client reservations, it is possible to reserve a specific IP address for permanent use by a DHCP client. A new feature in Windows Server 2012 R2 called policy based assignment allows for even greater flexibility.
B. Policy based assignment allows the policy to be scoped to a MAC address and IP range
C.
D. A DHCP server offers its services to the DHCP clients based on the availability of MAC address filtering.
Once the Allow filter is set, all DHCP operations are based on the access controls (allow/deny).
http://blogs.technet.com/b/teamdhcp/archive/2012/08/22/granular-dhcp-serveradministration-using-dhcppolicies-in-windows-server-2012.aspx
http://technet.microsoft.com/en-us/library/hh831538.aspx
http://technet.microsoft.com/en-us/library/ee405265(v=ws.10).aspx

QUESTION 55
Your network contains an Active Directory domain named contoso.com.
The domain contains a member server named Server1. Server1 has the IP Address Management (IPAM) Server feature installed.
A technician performs maintenance on Server1.
After the maintenance is complete, you discover that you cannot connect to the IPAM server on Server1.
You open the Services console as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that you can connect to the IPAM server.
Which service should you start?

A. Windows Process Activation Service
B. windows Event Collector
C. Windows Internal Database
D. Windows Store Service (WSService)

Answer: C
Explanation:
IPAM only supports Windows Internal Database (not SQL Server, MySQL, or any other third-party solution). Because of this I believe the answer is C. As long as the Windows Process Activation Service is not disabled and is properly set as a dependency for Windows Internal Database, it will start automatically when you start the Windows Internal Database service.

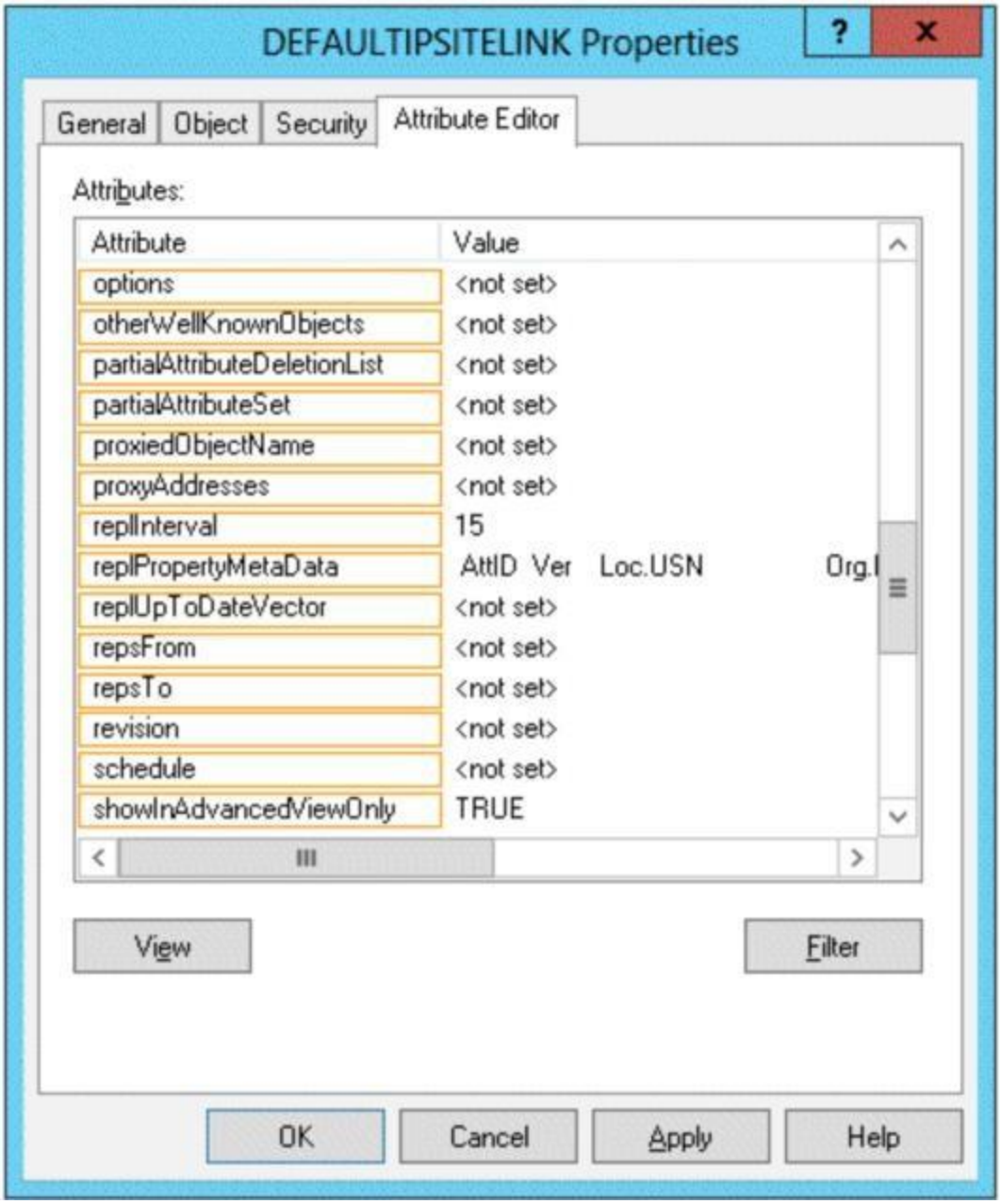
QUESTION 56
Your network contains two Active Directory forests named contoso.com and adatum.com.
All of the domain controllers in both of the forests run Windows Server 2012 R2.
The adatum.com domain contains a file server named Servers. Adatum.com has a one-way forest trust to contoso.com. A contoso.com user name User10 attempts to access a shared folder on Servers and receives the error message shown in the exhibit. (Click the Exhibit button.)

You verify that the Authenticated Users group has Read permissions to the Data folder.
You need to ensure that User10 can read the contents of the Data folder on Server5 in the adatum.com domain.
What should you do?

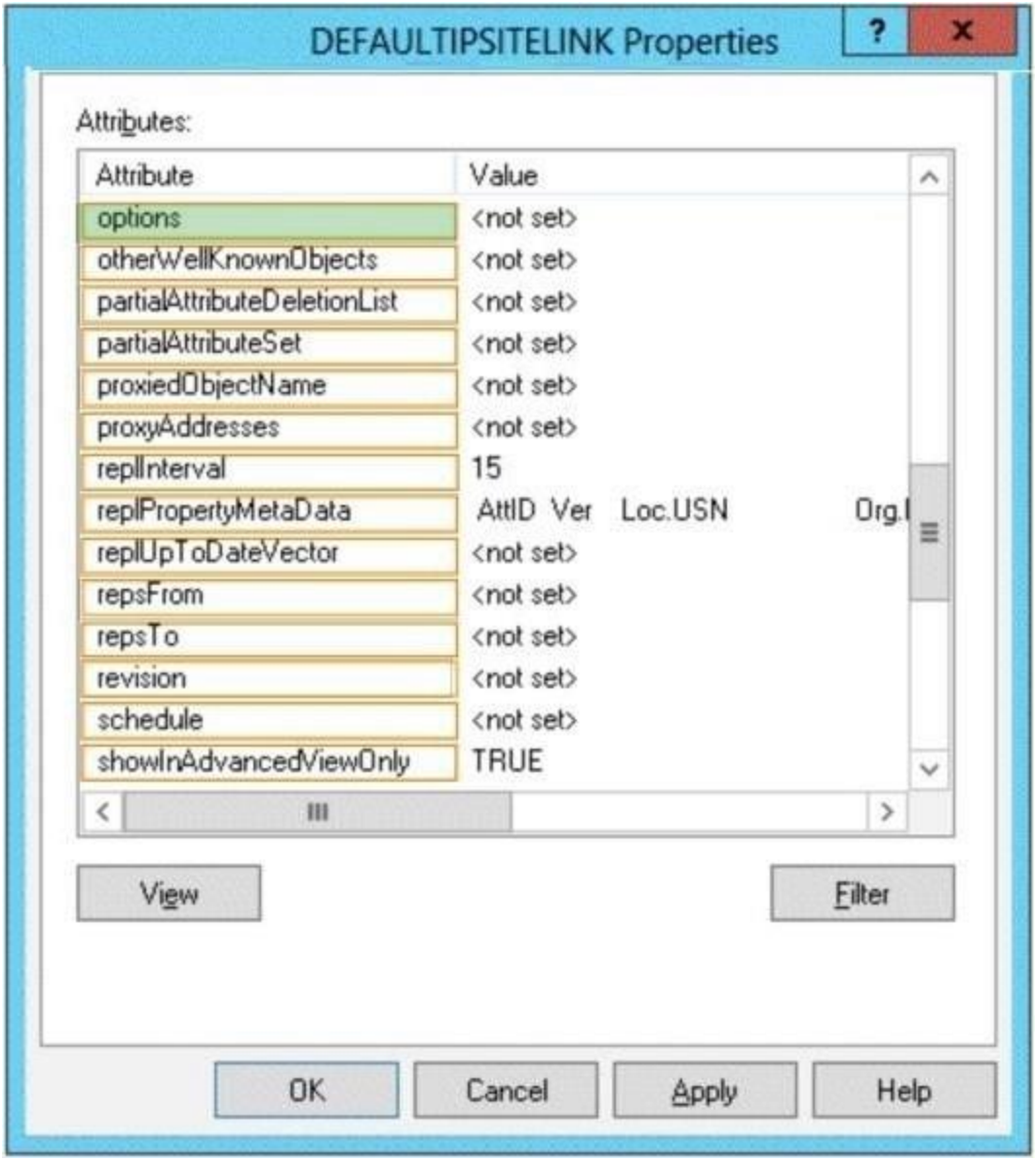
A. Grant the Other Organization group Read permissions to the Data folder.
B. Modify the list of logon workstations of the contoso\User10 user account.
C. Enable the Netlogon Service (NP-In) firewall rule on Server5.
D. Modify the permissions on the Server5 computer object in Active Directory.

Answer: D
Explanation:
To resolve the issue, I had to open up AD Users and Computers --> enable Advanced Features --> Select the Computer Object --> Properties --> Security --> Add the Group I want to allow access to the computer (in this case, DomainA\Domain users) and allow "Allowed to Authenticate". Once I did that, everything worked.

QUESTION 57
Your network contains an Active Directory domain named contoso.com.
The domain contains two Active Directory sites named Site1 and Site2.
You discover that when the account of a user in Site1 is locked out, the user can still log on to the servers in Site2 for up to 15 minutes by using Remote Desktop Services (RDS).
You need to reduce the amount of time it takes to synchronize account lockout information across the domain.
Which attribute should you modify? To answer, select the appropriate attribute in the answer area.


DEFAULTIPSITELINK Properties
General
Object
Security
Attribute Editor
Attributes:
Attribute
Value
options
<not set>
otherWellKnownObjects
<not set>
partialAttributeDeletionList
<not set>
partialAttributeSet
<not set>
proxiedObjectName
<not set>
proxyAddresses
<not set>
replInterval
15
replPropertyMetaData
AttID Ver Loc.USN Org.I
replUpToDateVector
<not set>
repsFrom
<not set>
repsTo
<not set>
revision
<not set>
schedule
<not set>
showInAdvancedViewOnly
TRUE
View
Filter
OK
Cancel
Apply
Help

Answer:



Explanation:
Replinterval must be a multiple of 15 minutes, a minimum of 15 minutes, and a maximum of 10,080 minutes (one week).
Therefore cannot be the 'replinterval' option
http://msdn.microsoft.com/en-us/library/ms679447(v=vs.85).aspx
Answer is 'Options'.
Within the same site, AD replication usees 'Change Notification'. When there is change, source sends 'Change Notification' to replication partners, then, the parters send 'Update Request', then source sends updated AD data.
Between sites, AD replication occurs on scheduled time. Default interval is 180 mins (3 hours). You can set to minimum of 15 mins with 15 mins increment.
Urgent replication:
At some situations, you want to force replicaton between sites like Account Lockout. Two or more ways to do this;
1. Use dssite.msc. right-click on the inbound replication partner which has change, then choose replicate.
2. You can also set automatic replication with Change Notification.

Change Notification is only used intra-site replication.
But by changing an AD attribute 'Options' of the site link, you can force the replication between sites jsut like intra-site repliction using Change Notficiation.
Set Options to 1 (USE_NOTIFY) in adsiedit.msc/ Configuration/ Sites/IP Transports/IP/site link.

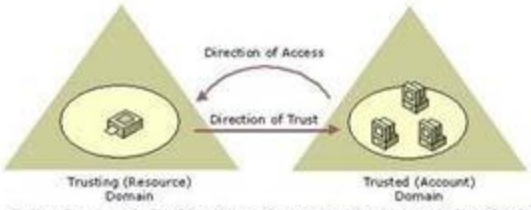
QUESTION 58
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. The functional level of the forest is Windows Server 2003.
You have a domain outside the forest named adatum.com.
You need to configure an access solution to meet the following requirements:
- Users in adatum.com must be able to access resources in contoso.com.
- Users in adatum.com must be prevented from accessing resources in fabrikam.com.
- Users in both contoso.com and fabrikam.com must be prevented from accessing resources in adatum.com.
What should you create?

A. a one-way external trust from adatum.com to fabrikam.com
B. a one-way realm trust from fabrikam.com to adatum.com
C. a one-way realm trust from adatum.com to fabrikam.com
D. a one-way external trust from fabrikam.com to adatum.com

Answer: A
Explanation:
A. A one-way trust is a unidirectional authentication path that is created between two domains. This means that in a one-way trust between Domain A and Domain B, users in Domain A can access resources in Domain B. However, users in Domain B cannot access resources in Domain A. This would allow adatum.com users access to contoso which is desired.
B. This would allow contoso.com users access to adatum which must be prevented and used for non windows realm to AD.
C. This would allow adatum.com users access to contoso which is desired but realm trust types are used for non windows realm to AD.
D. This would allow adatum users access to contoso which must be prevented and You need to make trust relationship where domain contoso.com trusts adatum.com.
NOTE: On exam the domain names were changed, so understand the question well
http://technet.microsoft.com/en-us/library/cc728024(v=ws.10).aspx

Trust direction

The trust type and its assigned direction will impact the trust path used for authentication. A trust path is a series of trust relationships that authentication requests must follow between domains. Before a user can access a resource in another domain, the security system on domain controllers running Windows Server 2003 must determine whether the trusting domain (the domain containing the resource the user is trying to access) has a trust relationship with the trusted domain (the user's logon domain). To determine this, the security system computes the trust path between a domain controller in the trusting domain and a domain controller in the trusted domain. In the following figure, trust paths are indicated by arrows showing the direction of the trust (this is a one-way trust):



All domain trust relationships have only two domains in the relationship: the trusting domain and the trusted domain.

QUESTION 59
Your network contains an Active Directory domain named contoso.com. The domain contains a main office and a branch office. An Active Directory site exists for each office.
All domain controllers run Windows Server 2012 R2. The domain contains two domain controllers. The domain controllers are configured as shown in the following table.

Site	Domain controller name	Configuration
Main	DC1	Writable domain controller Global catalog server DNS server
Branch	DC2	Read-only domain controller (RODC) Global catalog server

DC1 hosts an Active Directory-integrated zone for contoso.com.
You add the DNS Server server role to DC2.
You discover that the contoso.com DNS zone fails to replicate to DC2.
You verify that the domain, schema, and configuration naming contexts replicate from DC1 to DC2.
You need to ensure that DC2 replicates the contoso.com zone by using Active Directory replication.
Which tool should you use?

A. Active Directory Sites and Services
B. Ntdsutil
C. DNS Manager
D. Active Directory Domains and Trusts

Answer: A
Explanation:
A. To control replication between two sites, you can use the Active Directory Sites and Services snap- in to configure settings on the site link object to which the sites are added. By configuring settings on a site link, you can control when replication occurs between two or more sites, and how often
B. Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory Domain Services (AD DS) and Active Directory Lightweight Directory Services (AD LDS).
You can use the ntdsutil commands to perform database maintenance of AD DS, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled.
C. DNS Manager is the tool you'll use to manage local and remote DNS Servers
D. Active Directory Domains and Trusts is the Microsoft Management Console (MMC) snap-in that you can use to administer domain trusts, domain and forest functional levels, and user principal name (UPN) suffixes.
http://technet.microsoft.com/en-us/library/cc731862.aspx
http://technet.microsoft.com/en-us/library/cc753343(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/cc722541.aspx
http://technet.microsoft.com/en-us/library/cc770299.aspx
Note: If you see question about AD Replication, First preference is AD sites and services, then Repadmin and then DNSLINT.

QUESTION 60
Your network contains an Active Directory forest. The forest contains two domains named contoso.com and fabrikam.com. The functional level of the forest is Windows Server 2003. The contoso.com domain contains domain controllers that run either Windows Server 2008 or Windows Server 2008 R2. The functional level of the domain is Windows Server 2008. The fabrikam.com domain contains domain controllers that run either Windows Server 2003 or Windows Server 2008. The functional level of the domain is Windows Server 2003. The contoso.com domain contains a member server named Server1 that runs Windows Server 2012 R2. You install the Active Directory Domain Services server role on Server1.
You need to add Server1 as a new domain controller in the contoso.com domain.

What should you do?

A. Run the Active Directory Domain Services Configuration Wizard.
B. Run adprep.exe /domainprep, and then run dcpromo.exe.
C. Raise the functional level of the forest, and then run dcprorno.exe.
D. Modify the Computer Name/Domain Changes properties.

Answer: A
Explanation:
Windows Server 2012 R2 requires a Windows Server 2003 forest functional level. That is, before you can add a domain controller that runs Windows Server 2012 R2 to an existing Active Directory forest, the forest functional level must be Windows Server 2003 or higher.
http://blogs.technet.com/b/askpfeplat/archive/2012/09/03/introducing-the-first-windowsserver-2012-domaincontroller.aspx
http://technet.microsoft.com/en-us/library/dd464018(v=ws.10).aspx
http://technet.microsoft.com/en-us/library/jj574134.aspx

Domain functional levels

Domain functionality enables features that affect the entire domain and that domain only. The following table lists the domain functional levels and their corresponding supported domain controllers:

Domain functional level	Domain controller operating systems supported
Windows Server 2003	Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	Windows Server 2012 Windows Server 2008 R2 Windows Server 2008
Windows Server 2008 R2	Windows Server 2012 Windows Server 2008 R2
Windows Server 2012	Windows Server 2012

Forest functional levels

Forest functional levels enable features across all the domains in your forest. The following table lists the forest functional levels and their corresponding supported domain controllers.

Forest functional level	Domain controller operating systems supported
Windows Server 2003	Windows Server 2012 Windows Server 2008 R2 Windows Server 2008 Windows Server 2003
Windows Server 2008	Windows Server 2012 Windows Server 2008 R2 Windows Server 2008
Windows Server 2008 R2 (default)	Windows Server 2012 Windows Server 2008 R2
Windows Server 2012	Windows Server 2012

Here we are extending the schema. So this is the equivalent of adprep /forestprep.

Now we are running adprep /domainprep.