NEW QUESTION 1
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains client computers that run either Windows XP or Windows 8. Network Policy Server (NPS) is deployed to the domain. You plan to create a system health validator (SHV). You need to identify which policy settings can be applied to all of the computers. Which three policy settings should you identify? (Each correct answer presents part of the solution. Choose three.)

A. Antispyware is up to date.
B. Automatic updating is enabled.
C. Antivirus is up to date.
D. A firewall is enabled for all network connections.
E. An antispyware application is on.

Answer: BCD
Explanation:
The WSHA on NAP client computers running Windows XP SP3 does not monitor the status of antispyware applications.

NEW QUESTION 2
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1. You run ntdsutil as shown in the exhibit. (Click the Exhibit button.)

You need to ensure that you can access the contents of the mounted snapshot. What should you do?

A. From the snapshot context of ntdsutil, run activate instance "NTDS".
B. From a command prompt, run dsamain.exe -dbpath c:\$snap_201204131056_volumec\windows\ntds\ntd
C. dit -Idapport 389.
D. From the snapshot context of ntdsutil, run mount (79f9f82-5926-4f44-8a0-2f56d827a57d).
E. From a command prompt, run dsamain.exe -dbpath c:\$snap_201204131056_volumec\windows\ntds\ntd
F. dit -Idapport 33389.
Answer: D

Explanation:
By default, only members of the Domain Admins group and the Enterprise Admins group are allowed to view the snapshots because they contain sensitive AD DS data. If you want to access snapshot data from an old domain or forest that has been deleted, you can allow nonadministrators to access the data when you run Dsamain.exe.

If you plan to view the snapshot data on a domain controller, specify ports that are different from the ports that the domain controller will use. A client starts an LDAP session by connecting to an LDAP server, called a Directory System Agent (DSA), by default on TCP port and UDP [7] port 389. The client then sends an operation request to the server, and the server sends responses in return. With some exceptions, the client does not need to wait for a response before sending the next request, and the server may send the responses in any order. All information is transmitted using Basic Encoding Rules (BER).

References:

NEW QUESTION 3
- (Topic 1)

You log on to Server1 by using a user account named User2.

From the Remote Access Management Console, you run the Getting Started Wizard and you receive a warning message as shown in the exhibit. (Click the Exhibit button.)
You need to ensure that you can configure DirectAccess successfully. The solution must minimize the number of permissions assigned to User2.

To which group should you add User2?

A. Enterprise Admins
B. Administrators
C. Account Operators
D. Server Operators

Answer: B

Explanation:
You must have privileges to create WMI filters in the domain in which you want to create the filter. Permissions can be changed by adding a user to the Administrators group.

Administrators (A built-in group)
After the initial installation of the operating system, the only member of the group is the Administrator account. When a computer joins a domain, the Domain Admins group is added to the Administrators group. When a server becomes a domain controller, the Enterprise Admins group also is added to the Administrators group. The Administrators group has built-in capabilities that give its members full control over the system. The group is the default owner of any object that is created by a member of the group.

This example logs in as a test user who is not a domain user or an administrator on the server. This results in the error specifying that DA can only be configured by a user with local administrator permissions.

References:

NEW QUESTION 4
- (Topic 1)
You have a server named Server 1.
You enable BitLocker Drive Encryption (BitLocker) on Server 1.
You need to change the password for the Trusted Platform Module (TPM) chip. What should you run on Server1?

A. Manage-bde.exe
B. Set-TpmOwnerAuth
C. bdehdcfg.exe
D. tpmvscmgr.exe

Answer: B

Explanation:
The Set-TpmOwnerAuth cmdlet changes the current owner authorization value of the Trusted Platform Module (TPM) to a new value. You can specify the current owner authorization value or specify a file that contains the current owner authorization value. If you do not specify an owner authorization value, the cmdlet attempts to read the value from the registry.
Use the ConvertTo-TpmOwnerAuth cmdlet to create an owner authorization value. You can specify a new owner authorization value or specify a file that contains the new value.

NEW QUESTION 5
- (Topic 1)
Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2012 R2. Client computers run either Windows 7 or Windows 8. All of the client computers have an application named App1 installed. The domain contains a Group Policy object (GPO) named GPO1 that is applied to all of the client computers.

You need to add a system variable named App1Data to all of the client computers. Which Group Policy preference should you configure?

A. Environment
B. Ini Files
C. Data Sources
D. Services

Answer: A

Explanation:
Environment Variable preference items allow you to create, update, replace, and delete user and system environment variables or semicolon-delimited segments of the PATH variable. Before you create an Environment Variable preference item, you should review the behavior of each type of action possible with this extension.

NEW QUESTION 6
HOTSPOT - (Topic 1)
Your network contains an Active Directory domain named contoso.com.

You have several Windows PowerShell scripts that execute when users log on to their client computer.

You need to ensure that all of the scripts execute completely before the users can access their desktop.

Which setting should you configure? To answer, select the appropriate setting in the answer area.

A. Mastered
B. Not Mastered

Answer: A

Explanation:

Directs the system to wait for logon scripts to finish running before it starts the Windows Explorer interface program and creates the desktop.

If you enable this policy, Windows Explorer does not start until the logon scripts have finished running. This setting assures that logon script processing is complete before the user starts working, but it can delay the appearance of the desktop.

If you disable this policy or do not configure it, the logon scripts and Windows Explorer are not synchronized and can run simultaneously.

NEW QUESTION 7
DRAG DROP - (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains a domain controller named DC1.

You need to create an Active Directory snapshot on DC1. Which four commands should you run?

To answer, move the four appropriate commands from the list of commands to the answer area and arrange them in the correct order.
A. Mastered
B. Not Mastered

Answer: A

Explanation:
Box 1: ntdsutil
Box 2: snapshot
Box 3: activate instance ntds
Box 4: create

Note:
Create a snapshot of AD DS in Windows Server 2012 R2 by using NTDSUTIL
1 – On the domain server, open command prompt and type ntdsutil and press Enter.
2 – Next, type snapshot and press Enter.
3 – Next, type activate instance ntds and press Enter.
4 – Next, type create (this create command is to generate a snapshot of my AD) and press Enter.

NEW QUESTION 8
HOTSPOT - (Topic 2)
Your company has four offices. The offices are located in Montreal, Seattle, Sydney, and New York.
The network contains an Active Directory domain named contoso.com. The domain contains a server named Server2 that runs Windows Server 2012 R2. Server2 has the DHCP Server server role installed.
All client computers obtain their IPv4 and IPv6 addresses from DHCP.
You need to ensure that Network Access Protection (NAP) enforcement for DHCP applies to all of the client computers except for the client computers in the New York office.
Which two nodes should you configure? To answer, select the appropriate two nodes in the answer area.
NEW QUESTION 9

- (Topic 2)

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2012 R2. An organizational unit (OU) named OU1 contains 200 client computers that run Windows 8 Enterprise. A Group Policy object (GPO) named GPO1 is linked to OU1. You make a change to GPO1. You need to force all of the computers in OU1 to refresh their Group Policy settings immediately. The solution must minimize administrative effort.

Which tool should you use?

A. The Secedit command
B. Group Policy Management Console (GPMC)
C. Server Manager
D. The Gpupdate command

Answer: B
Explanation:
In the previous versions of Windows, this was accomplished by having the user run GPUpdate.exe on their computer. Starting with Windows Server® 2012 and Windows® 8, you can now remotely refresh Group Policy settings for all computers in an OU from one central location through the Group Policy Management Console (GPMC). Or you can use the Invoke-GPUpdate cmdlet to refresh Group Policy for a set of computers, not limited to the OU structure, for example, if the computers are located in the default computers container.

[Image of Group Policy Management Console]

Your network contains a DNS server named Server1 that runs Windows Server 2012 R2. Server1 has a zone named contoso.com. The network contains a server named Server2 that runs Windows Server 2008 R2. Server1 and Server2 are members of an Active Directory domain named contoso.com.

You change the IP address of Server2.

Several hours later, some users report that they cannot connect to Server2.

On the affected users’ client computers, you flush the DNS client resolver cache, and the users successfully connect to Server2.

You need to reduce the amount of time that the client computers cache DNS records from contoso.com.

Which value should you modify in the Start of Authority (SOA) record? To answer, select the appropriate setting in the answer area.

A. Mastered
B. Not Mastered

**Answer:** A

**Explanation:**
The Default TTL is just that a default for newly created records. Once the records are created their TTL is independent of the Default TTL on the SOA. Microsoft DNS implementation copies the Default TTL setting to all newly created records their by giving them all independent TTL settings.

SOA Minimum Field: The SOA minimum field has been overloaded in the past to have three different meanings, the minimum TTL value of all RRs in a zone, the default TTL of RRs which did not contain a TTL value and the TTL of negative responses.

Despite being the original defined meaning, the first of these, the minimum TTL value of all RRs in a zone, has never in practice been used and is hereby deprecated. The second, the default TTL of RRs which contain no explicit TTL in the master zone file, is relevant only at the primary server. After a zone transfer all RRs have explicit TTLs and it is impossible to determine whether the TTL for a record was explicitly set or derived from the default after a zone transfer. Where a server does not require RRs to include the TTL value explicitly, it should provide a mechanism, not being the value of the MINIMUM field of the SOA record, from which the missing TTL values are obtained. How this is done is implementation dependent.

TTLs also occur in the Domain Name System (DNS), where they are set by an authoritative name server for a particular resource record. When a caching (recursive) nameserver queries the authoritative nameserver for a resource record, it will cache that record for the time (in seconds) specified by the TTL. If a stub resolver queries the caching nameserver for the same record before the TTL has expired, the caching server will simply reply with the already cached resource record rather than retrieve it from the authoritative nameserver again.

Shorter TTLs can cause heavier loads on an authoritative nameserver, but can be useful when changing the address of critical services like Web servers or MX records, and therefore are often lowered by the DNS administrator prior to a service being moved, in order to minimize disruptions.
NEW QUESTION 11
- (Topic 2)
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2. Both servers run Windows Server 2012 R2. Both servers have the File and Storage Services server role, the DFS Namespace role service, and the DFS Replication role service installed. Server1 and Server2 are part of a Distributed File System (DFS) Replication group named Group1. Server1 and Server2 are connected by using a high-speed LAN connection.

You need to minimize the amount of processor resources consumed by DFS Replication. What should you do?

A. Modify the replication schedule.
B. Modify the staging quota.
C. Disable Remote Differential Compression (RDC).
D. Reduce the bandwidth usage.

Answer: C

Explanation:
Because disabling RDC can help conserve disk input/output (I/O) and CPU resources, you might want to disable RDC on a connection if the sending and receiving members are in a local area network (LAN), and bandwidth use is not a concern. However, in a LAN environment where bandwidth is contended, RDC can be beneficial when transferring large files.

Question tells it uses a high-speed LAN connection.

References:

NEW QUESTION 12
You have a server named Server1 that runs Windows Server 2012 R2. You create a custom Data Collector Set (DCS) named DCS1. You need to configure Server1 to start DCS1 automatically when the network usage exceeds 70 percent. Which type of data collector should you create?

A. A performance counter alert
B. A configuration data collector
C. A performance counter data collector
D. An event trace data collector

Answer: A

Explanation:
Performance alerts notify you when a specified performance counter exceeds your configured threshold by logging an event to the event log. But rather than notifying you immediately when the counter exceeds the threshold, you can configure a time period over which the counter needs to exceed the threshold, to avoid unnecessary alerts.

---

Your network contains an Active Directory domain named contoso.com. The domain contains a server named Server1 that has the Remote Access server role installed. DirectAccess is implemented on Server1 by using the default configuration. You discover that DirectAccess clients do not use DirectAccess when accessing websites on the Internet. You need to ensure that DirectAccess clients access all Internet websites by using their DirectAccess connection. What should you do?

A. Configure a DNS suffix search list on the DirectAccess clients.
B. Configure DirectAccess to enable force tunneling.
C. Disable the DirectAccess Passive Mode policy setting in the DirectAccess Client Settings Group Policy object (GPO).
D. Enable the Route all traffic through the internal network policy setting in the DirectAccess Server Settings Group Policy object (GPO).

Answer: B

Explanation:
With IPv6 and the Name Resolution Policy Table (NRPT), by default, DirectAccess clients separate their intranet and Internet traffic as follows:
- DNS name queries for intranet fully qualified domain names (FQDNs) and all intranet traffic is exchanged over the tunnels that are created with the DirectAccess server or directly with intranet servers. Intranet traffic from DirectAccess clients is IPv6 traffic.
- DNS name queries for FQDNs that correspond to exemption rules or do not match the intranet namespace, and all traffic to Internet servers, is exchanged over the physical interface that is connected to the Internet. Internet traffic from DirectAccess clients is typically IPv4 traffic.

In contrast, by default, some remote access virtual private network (VPN) implementations, including the VPN client, send all intranet and Internet traffic over the remote access VPN connection. Internet-bound traffic is routed by the VPN server to intranet IPv4 web proxy servers for access to IPv4 Internet resources. It is possible to separate the intranet and Internet traffic for remote access VPN clients by using split tunneling. This involves configuring the Internet Protocol (IP) routing table on VPN clients so that traffic to intranet locations is sent over the VPN connection, and traffic to all other locations is sent by using the physical interface that is connected to the Internet.

You can configure DirectAccess clients to send all of their traffic through the tunnels to the DirectAccess server with force tunneling. When force tunneling is configured, DirectAccess clients detect that they are on the Internet, and they remove their IPv4 default route. With the exception of local subnet traffic, all traffic sent by the DirectAccess client is IPv6 traffic that goes through tunnels to the DirectAccess server.
NEW QUESTION 14
- (Topic 2)
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the Windows Deployment Services server role installed. Server1 contains two boot images and four install images.
You need to ensure that when a computer starts from PXE, the available operating system images appear in a specific order.
What should you do?
A. Modify the properties of the boot images.
B. Create a new image group.
C. Modify the properties of the install images.
D. Modify the PXE Response Policy.

Answer: C

NEW QUESTION 15
- (Topic 2)
You have a cluster named Cluster1 that contains two nodes. Both nodes run Windows Server 2012 R2. Cluster1 hosts a virtual machine named VM1 that runs Windows Server 2012 R2.
You configure a custom service on VM1 named Service1.
You need to ensure that VM1 will be moved to a different node if Service1 fails. Which cmdlet should you run on Cluster1?
A. Add-ClusterVmMonitoredItem
B. Add-ClusterGenericServiceRole
C. Set-ClusterResourceDependency
D. Enable VmResourceMetering

Answer: A

Explanation:
The Add-ClusterVmMonitoredItem cmdlet configures monitoring for a service or an Event Tracing for Windows (ETW) event so that it is monitored on a virtual machine. If the service fails or the event occurs, then the system responds by taking an action based on the failover configuration for the virtual machine resource. For example, the configuration might specify that the virtual machine be restarted.

NEW QUESTION 16
- (Topic 3)
You deploy a Windows Server Update Services (WSUS) server named Server01.
You need to ensure that you can view update reports and computer reports on Server01.
Which two components should you install? Each correct answer presents part of the solution.
A. Microsoft XPS Viewer
B. Microsoft Report Viewer 2008 Redistributable Package
C. Microsoft SQL Server 2008 R2 Report Builder 3.0
D. Microsoft.NET Framework 2.0
E. Microsoft SQL server 2012 Reporting Services (SSRS)

Answer: BD

NEW QUESTION 17
- (Topic 3)
Your network contains an Active Directory domain named contoso.com.
All user accounts reside in an organizational unit (OU) named OU1. All of the users in the marketing department are members of a group named Marketing. All of the users in the human resources department are members of a group named HR.
You create a Group Policy object (GPO) named GPO1. You link GPO1 to OU1. You configure the Group Policy preferences of GPO1 to add two shortcuts named Link1 and Link2 to the desktop of each user.
You need to ensure that Link1 only appears on the desktop of the users in Marketing and that Link2 only appears on the desktop of the users in HR. What should you configure?
A. Security Filtering
B. WMI Filtering
C. Group Policy Inheritance
D. Item-level targeting

Answer: D

Explanation:
You can use item-level targeting to change the scope of individual preference items, so they apply only to selected users or computers. Within a single Group Policy object (GPO), you can include multiple preference items, each customized for selected users or computers and each targeted to apply settings only to the relevant users or computers.

NEW QUESTION 18
- (Topic 3)
The domain contains 10 domain controllers and a read-only domain controller (RODC) named RODC01. All domain controllers and RODCs are hosted on a Hyper-V host that runs Windows Server 2012 R2.
You need to identify which user accounts were authenticated by RODC1. Which cmdlet should you use?
A. Get-ADGroupMember
B. Get-ADDomainControllerPasswordReplicationPolicy
C. Get-ADDomainControllerPasswordReplicationPolicyUsage
D. Get-ADDomain
E. Get-ADOptionalFeature
F. Get-ADAccountAuthorizationGroup

Answer: B

Explanation:
Gets the Active Directory accounts that are authenticated by a read-only domain controller or that are in the revealed list of the domain controller.

NEW QUESTION 19
- (Topic 3)
Your network contains an Active Directory domain named contoso.com. Network Policy Server (NPS) is deployed to the domain.
You plan to deploy Network Access Protection (NAP).
You need to configure the requirements that are validated on the NPS client computers. What should you do?

A. From the Network Policy Server console, configure a network policy.
B. From the Network Policy Server console, configure a health policy.
C. From the Network Policy Server console, configure a Windows Security Health Validator (WSHV) policy.
D. From a Group Policy object (GPO), configure the NAP Client Configuration security setting.
E. From a Group Policy object (GPO), configure the Network Access Protection Administrative Templates setting.

Answer: C

NEW QUESTION 20
- (Topic 3)
You have a server named Server1 that runs Windows Server 2012 R2. Server1 has the File Server Resource Manager role service installed.
Each time a user receives an access-denied message after attempting to access a folder on Server1, an email notification is sent to a distribution list named DLL.
You create a folder named Folder1 on Server1, and then you configure custom NTFS permissions for Folder1.
You need to ensure that when a user receives an access-denied message while attempting to access Folder1, an email notification is sent to a distribution list named DL2. The solution must not prevent DL1 from receiving notifications about other access-denied messages.
What should you do?

A. From the File Server Resource Manager console, create a local classification property.
B. From Server Manager, run the New Share Wizard to create a share for Folder1 by selecting the SMB Share - Applications option.
C. From the File Server Resource Manager console, modify the Access-Denied Assistance settings.
D. From the File Server Resource Manager console, set a folder management property.

Answer: D

NEW QUESTION 21
......
Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions
2nd - Questions and Answers in PDF Format

70-411 Practice Exam Features:

* 70-411 Questions and Answers Updated Frequently
* 70-411 Practice Questions Verified by Expert Senior Certified Staff
* 70-411 Most Realistic Questions that Guarantee you a Pass on Your First Try
* 70-411 Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The 70-411 Practice Test Here