DUMPSARENA

Identity with Windows Server 2016

Microsoft 70-742

Version Demo

Total Demo Questions: 15

Total Premium Questions: 267

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Install and Configure Active Directory Domain Services (AD DS)	77
Topic 2, Manage and Maintain AD DS	49
Topic 3, Create and Manage Group Policy	71
Topic 4, Implement Active Directory Certificate Services	27
Topic 5, Implement Identity Federation and Access Solutions	43
Total	267

QUESTION NO: 1

You have an internal web server that hosts websites. The websites use HTTP and HTTPS.

You deploy a Web Application Proxy to your perimeter network.

You need to ensure that users from the Internet can access the websites by using HTTPS only. Internet access to the websites must use the Web Application Proxy.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. From the web server, enable HTTP Redirect on the Web Application Proxy server.

B. Configure the Web Application Proxy to perform preauthentication by using Oauth2.

C. From the Remote Access Management Console, publish the websites. Configure pass-through authentication and select Enable HTTP to HTTPS redirection.

D. On external DNS name servers, create DNS entries that point to the private IP address of the web server.

E. On external DNS name servers, create DNS entries that point to the public IP address of the Web Application Proxy.

ANSWER: C E

QUESTION NO: 2

Your network contains an Active Directory domain named contoso.com. The domain contains servers that run Windows Server 2016. The servers are configured as shown in the following table:

Name	Configuration
DC1	Domain controller, DNS server
DC2	Domain controller, DNS server
CA1	Enterprise certification authority (CA)
CA2	*None*

You have a research department. The computers in the research department are not domain-joined.

You need to ensure that the research department computers can use automatic certificate enrollment to receive and renew certificates from the CA.

Which two role services should you install and configure on CA1? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Certificate Enrollment Policy Web Service

B. Certificate Authority Web Enrollment

C. Online Responder

D. Certificate Enrollment Web Service

E. Network Device Enrollment Service

ANSWER: A B

Explanation:

References:

https://www.ejbca.org/docs/Part_2__Microsoft_Certification_Authority_and_Group_Policies.html

QUESTION NO: 3 - (HOTSPOT)

HOTSPOT

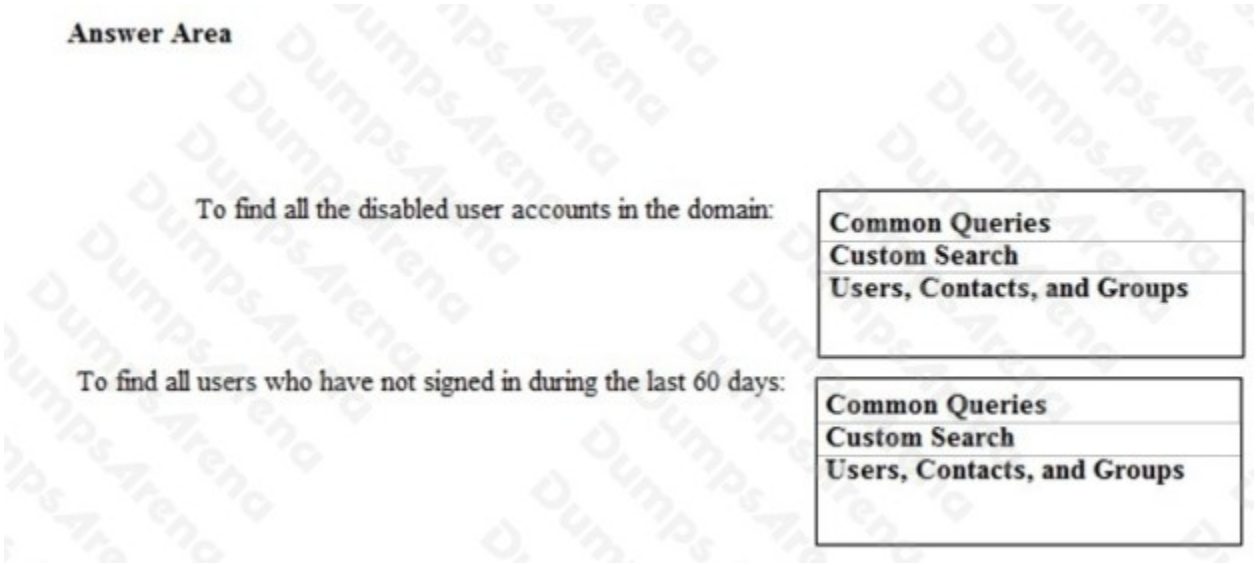
Your network contains an Active Directory domain named contoso.com. You plan to automate user account management.

You need to find user accounts that meet specific criteria by using the find command in Active Directory Users and Computers. The solution must minimize administrative effort.

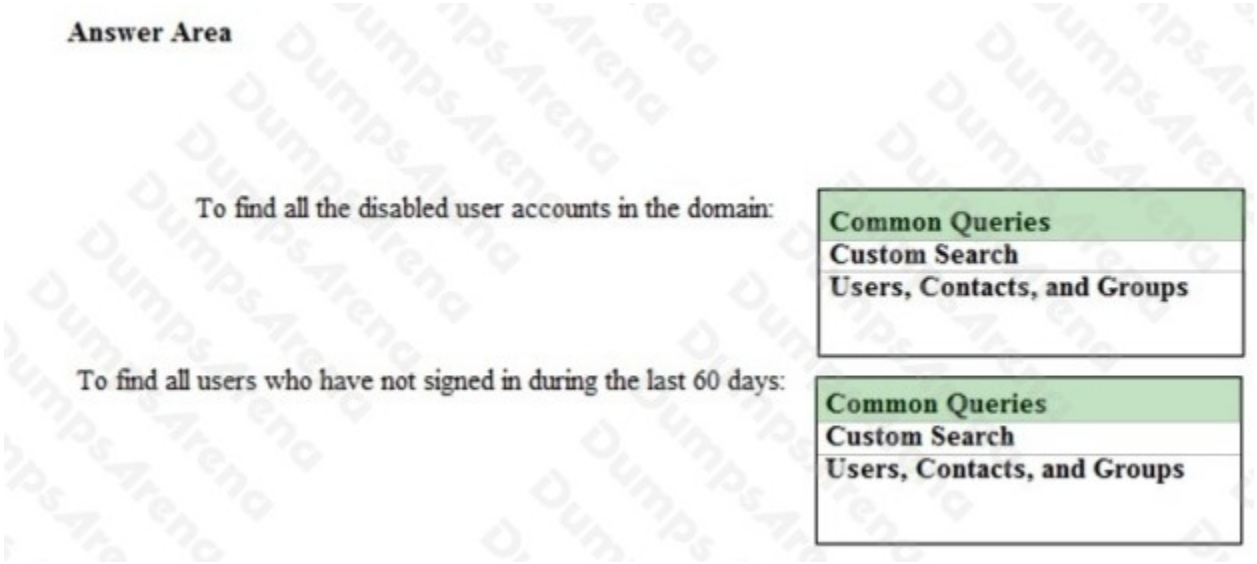
Which Find option should you use for each section? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



Explanation:

References: https://activedirectorypro.com/find-disabled-active-directory-user-accounts/
https://www.oreilly.com/library/view/active-directory-cookbook/0596004648/ch06s29.html

QUESTION NO: 4

You are configuring AD FS. Which server should you deploy on your organization's perimeter network?

A. Web application proxy

B. Relying-party server

C. Federation server

D. Claims-provider server

ANSWER: A

QUESTION NO: 5

Your network contains an Active Directory domain. The domain contains a server named Server1 that runs Windows Server 2016. Server1 runs a service named Service1 in the security context of the Network Service account.

The domain contains an enterprise certification authority (CA).

You plan to create template that will be used to issue certificates for Service1. Server1 will enroll for the certificates on behalf of Service1.

Which template settings must you configure to allow Service1 to access the private keys of the certificates installed on Server1?

A. Issuance requirements

B. Request Handling

C. Extensions

D. Security

ANSWER: D

Explanation:

References:

https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/configure-server-certificate-autoenrollment

QUESTION NO: 6

Your company uses Active Directory Rights Management Services (AD RMS).

You need to ensure that only users who use AD RMS client version 2.1 or newer can obtain a rights account certificate from the AD RMS cluster.

What should you enable first?

A. decommissioning

B. user exclusion

C. lockbox exclusion

D. Application Exclusion

ANSWER: C

Explanation:

References: https://forsenergy.com/en-us/rms_help/html/9a944ab7-f0d9-4224-97c6-b2543f537827.htm

QUESTION NO: 7

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

Your network contains an Active Directory forest. The forest contains a domain named contoso.com. The domain contains three domain controllers.

A domain controller named lon-dc1 fails. You are unable to repair lon-dc1.

You need to prevent the other domain controllers from attempting to replicate to lon-dc1.

Solution: From Active Directory Sites and Trusts, you transfer the operations master roles from lon-dc1.

Does this meet the goal?

A. Yes

B. No

ANSWER: B

QUESTION NO: 8 - (DRAG DROP)

DRAG DROP

Your network contains an Active Directory domain named contoso.com. All servers run Windows Server 2016.

You have a Microsoft Azure Active Directory (Azure AD) tenant named contoso.com.

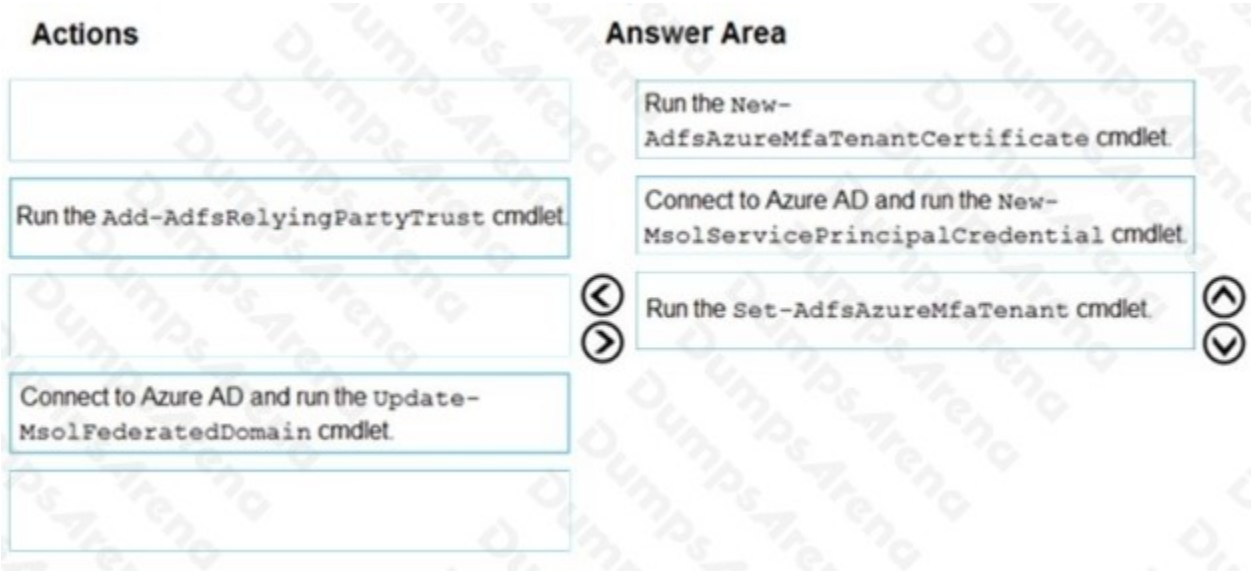
You deploy Active Directory Federation Services (AD FS) and a Web Application Proxy to the Active Directory domain.

You need to configure the AD FS deployment to support Azure Multi-Factor Authentication (MFA) as the primary authentication method.

Which three actions should you perform in sequence on the AD FS server? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Select and Place:

ANSWER:



Explanation:

Box 1: New-AdfsAzureMfaTenantCertificate

First step of the configuration is to generate a certificate for Azure MFA using the New-AdfsAzureMfaTenantCertificate –TenantId cmdlet.

Box 2: New-MsolServicePrincipalCredential

Connect to the Azure AD and use New-MsolServicePrincipalCredential to configure Azure MFA Clients to use it as a credential to connect with AD FS

Box 3 Set-AdfsAzureMfaTenant

Configure ADFS to use Azure AD by using the Set-AdfsAzureMfaTenant –TenantId cmdlet.

Reference: http://www.rebeladmin.com/2017/09/step-step-guide-configure-azure-mfa-adfs-2016/

QUESTION NO: 9

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

The domain contains an enterprise root certification authority (CA) on a server that runs Windows Server 2016.

You need to configure the CA to support Online Certificate Status Protocol (OCSP) responders.

Which two actions should you perform? Each correct selection presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Add a new certificate template to issue.

B. Modify the Authority Information Access (AIA) of the CA.

C. Configure an enrollment agent.

D. Install a standalone subordinate CA.

E. Modify the CRL distribution point (CDP) of the CA.

ANSWER: A B

Explanation:

Once the OCSP service is configured, we need to configure the OCSP Response Signing template. This process includes adding an Authority Information Access (AIA) extension and then issuing a new certificate template.

References: https://www.poweradmin.com/blog/deploying-active-directory-certificate-services-and-online-responder/

QUESTION NO: 10

You deploy a new certification authority (CA) to a server that runs Windows Server 2016.

You need to configure the CA to support recovery of certificates.

What should you do first?

A. Assign the Request Certificates permission to the user account that will be responsible for recovering certificates.

B. Configure the Key Recovery Agent template as a certificate template to issue.

C. Modify the Recovery Agents settings from the properties of the CA.

D. Modify the extension of the OCSP Response Signing template.

ANSWER: B

Explanation:

References: http://markgossa.blogspot.co.uk/2017/03/enable-key-archival-in-server-2012-r2.html

QUESTION NO: 11

Your network contains an Active Directory domain named contoso.com. The domain functional level is Windows Server 2016. The domain contains the servers shown in the following table.

Name	Configuration
DC1	Domain controller
Server1	Member server

The domain has several Managed Service Accounts.

Server1 hosts a service named Service1 that runs in the security context of the LocalSystem account.

You need to implement a group Managed Service Account to run Service1.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. On Server1, modify the properties of Service1.

B. On DC1, run Add-ADComputerServiceAccount.

C. On DC1, run New-ADServiceAccount.

D. On DC1, run Add-KDSRootKey.

ANSWER: A C

QUESTION NO: 12 - (HOTSPOT)

HOTSPOT

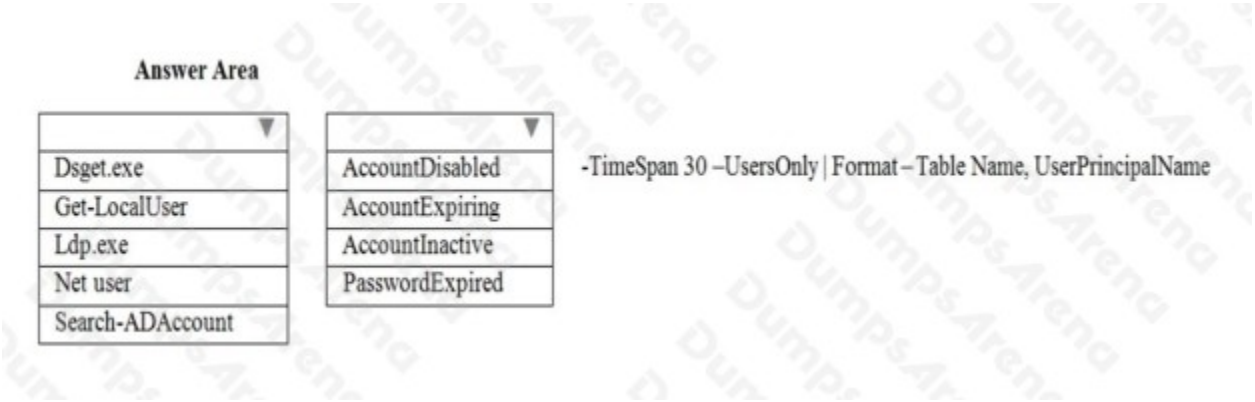
Your network contains an Active Directory domain named contoso.com.

You need to view a list of all the domain user accounts that are enabled, but whose users have not signed in during the last 30 days.

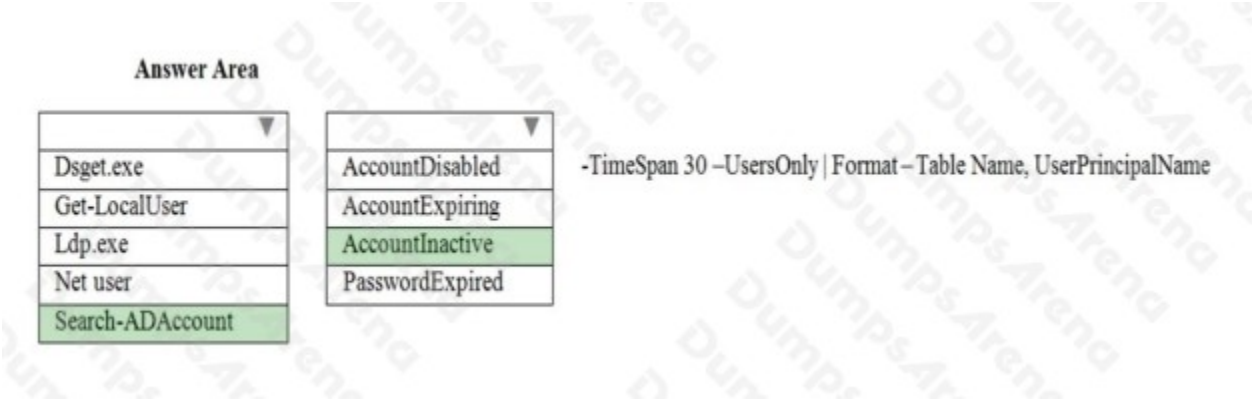
Which command should you run? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



ANSWER:



QUESTION NO: 13

Your network contains a single-domain Active Directory forest named contoso. com. The forest functional level is Windows Server 2016. The forest has Dynamic Access Control enabled. The domain contains two domain controllers named DC1 and DC2. Privileged user accounts used to manage Active Directory reside in a group named Contoso\AD_Admins.

You create an authentication policy named Policy1 and an authentication policy silo named Silo1.

You need to ensure that the accounts in the Contoso\AD_Admins group can sign in to the domain controllers only.

Which three configurations should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Create an access control condition in Policy1.

B. Create a managed service account and add the account to Permitted Accounts in Silo1.

C. Add the domain controllers to the Contoso\AD_Admins group.

D. Add the privileged user accounts and the domain controllers to Permitted Accounts in Silo1.

E. Assign Silo1 to the privileged user accounts and the domain controllers.

ANSWER: A D E

QUESTION NO: 14 - (DRAG DROP)

DRAG DROP

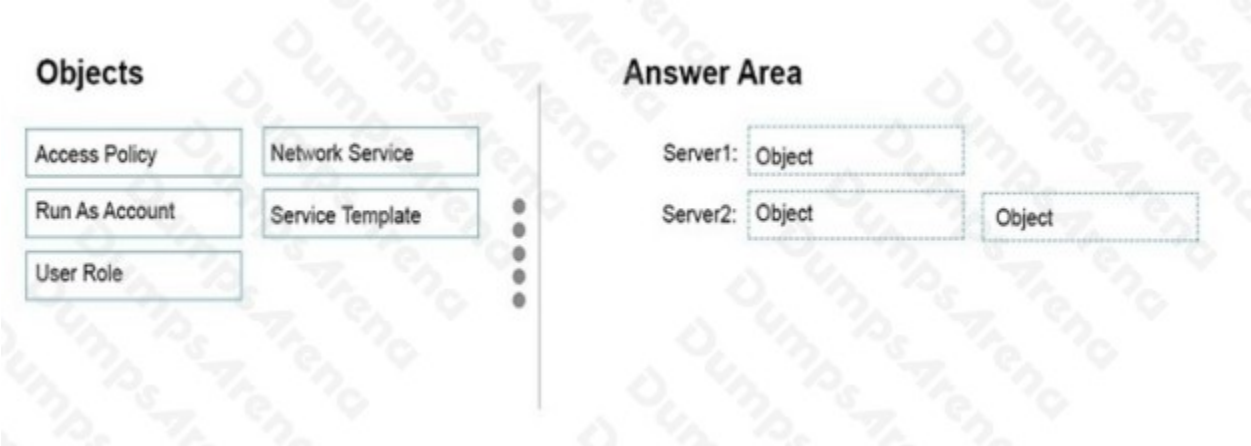
Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2016.

Server1 has IP Address Management (IPAM) installed. Server2 has Microsoft System Center 2016 Virtual Machine Manager (VMM) installed.

You need to integrate IPAM and VMM.

Which types of objects should you create on each server? To answer, drag the appropriate object types to the correct servers. Each object type may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Select and Place:



ANSWER:

Explanation:

Server 1 (IPAM): Access Policy

VMM must be granted permission to view and modify IP address space in IPAM, and to perform remote management of the IPAM server. VMM uses a "Run As" account to provide these permissions to the IPAM network service plugin. The "Run As" account must be configured with appropriate permission on the IPAM server.

To assign permissions to the VMM user account

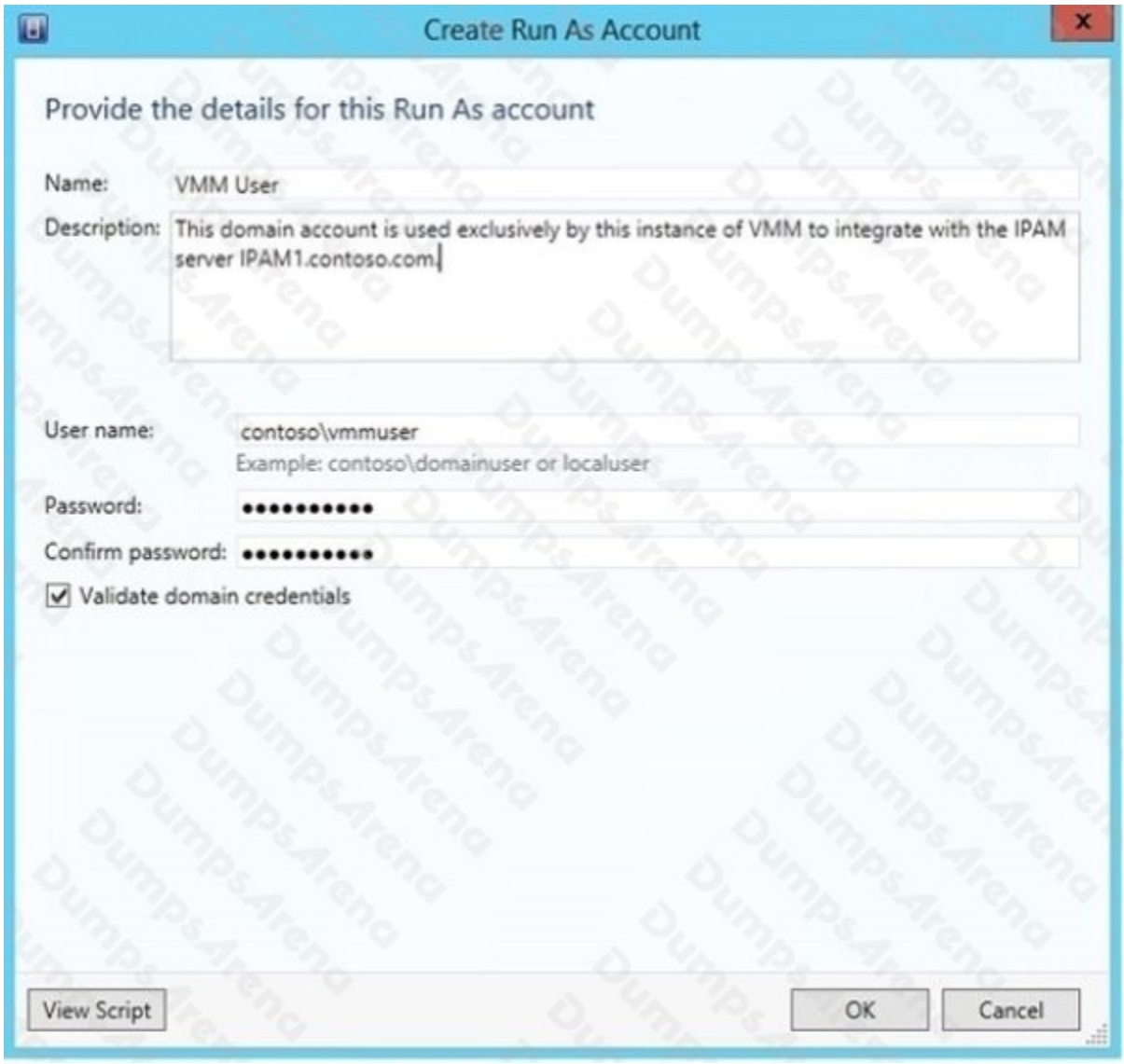
In the IPAM server console, in the upper navigation pane, click ACCESS CONTROL, right- click Access Policies in the lower navigation pane, and then click Add AccessPolicy. Etc.

Server 2 (VMM) #1: Network Service

Server 2 (VMM) #2: Run As Account

Perform the following procedure using the System Center VMM console.

To configure VMM (see step 1-3, step 6-7)



References: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/dn783349(v=ws.11)

QUESTION NO: 15

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

A partner company has a forest named fabrikam.com. Each forest contains one domain.

You need to provide access for a group named Research in fabrikam.com to resources in contoso.com. The solution must use the principle of least privilege.

What should you do?

A. Create an external trust from fabrikam.com to contoso.com. Enable Active Directory split permissions in fabrikam.com.

B. Create an external trust from contoso.com to fabrikam.com. Enable Active Directory split permissions in contoso.com.

C. Create a one-way forest trust from contoso.com to fabrikam.com that uses selective authentication.

D. Create a one-way forest trust from fabrikam.com to contoso.com that uses selective authentication.

ANSWER: C