Custom View Settings

Question #30 *Topic 2*

Your network contains an on-premises Active Directory forest named contoso.com. The forest is synced to an Azure Active Directory (Azure AD) tenant named contoso.com and an Azure AD Domain Services (Azure AD DS) domain named contoso-aad.com.
You have an Azure Storage account named Storage1 that contains a file share named Share1.
You configure NTFS permissions on Share1. You plan to deploy a virtual machine that will be used by several users to access Share1.
You need to ensure that the users can access Share1.
Which type virtual machine should you deploy?

A. a virtual machine that runs Windows Server 2016 and is joined to the contoso.com domain

B. a virtual machine that runs Windows 10 and is joined to the contoso-add.com domain

C. a virtual machine that runs Windows 10 and is hybrid Azure AD joined to the contoso.com domain

D. an Azure virtual machine that runs Windows Server 2016 and is joined to the contoso-add.com domain

**Correct Answer:** *D*
You join the Windows Server virtual machine to the Azure AD DS-managed domain, here named contoso-aad.com.
Note: Azure Files supports identity-based authentication over SMB (Server Message Block) (preview) through Azure Active Directory (Azure AD) Domain
Services. Your domain-joined Windows virtual machines (VMs) can access Azure file shares using Azure AD credentials.
Incorrect Answers:
B, C: Azure AD authentication over SMB is not supported for Linux VMs for the preview release. Only Windows Server VMs are supported.
References:
https://docs.microsoft.com/en-us/azure/storage/files/storage-files-active-directory-enable#mount-a-file-share-from-a-domain-joined-vm

Question #31 *Topic 2*

Note: This question is part of 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 company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).
Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.
The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016.
Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.
You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).
Solution: Deploy one Azure Key Vault to each region. Create two Azure AD service principals. Configure the virtual machines to use Azure Disk Encryption and specify a different service principal for the virtual machines in each region.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
You would also have to import Import the security keys from the HSM into each Azure key vault.

References:
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

Question #32 *Topic 2*

Note: This question is part of 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 company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).
Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.
The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016.
Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.
You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).
Solution: Export a security key from the on-premises HSM. Create one Azure AD service principal. Configure the virtual machines to use Azure Storage Service
Encryption.
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.
The Key Vault has to be in the same region as the VM that will be encrypted.
References:
https://www.ciraltos.com/azure-disk-encryption-v2/

Question #33 *Topic 2*

Note: This question is part of 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 company has an on-premises data center and an Azure subscription. The on-premises data center contains a Hardware Security Module (HSM).
Your network contains an Active Directory domain that is synchronized to an Azure Active Directory (Azure AD) tenant.
The company is developing an application named Application1. Application1 will be hosted in Azure by using 10 virtual machines that run Windows Server 2016.
Five virtual machines will be in the West Europe Azure region and five virtual machines will be in the East US Azure region. The virtual machines will store sensitive company information. All the virtual machines will use managed disks.
You need to recommend a solution to encrypt the virtual machine disks by using BitLocker Drive Encryption (BitLocker).
Solution:
☞ Deploy one Azure key vault to each region
☞ Export two security keys from the on-premises HSM
☞ Import the security keys from the HSM into each Azure key vault
Create two Azure AD service principals
▪
☞ Configure the virtual machines to use Azure Disk Encryption
☞ Specify a different service principal for the virtual machines in each region
Does this meet the goal?

A. Yes

B. No

**Correct Answer:** *A*
We use the Azure Premium Key Vault with Hardware Security Modules (HSM) backed keys.
The Key Vault has to be in the same region as the VM that will be encrypted.
Note: If you want to use a key encryption key (KEK) for an additional layer of security for encryption keys, add a KEK to your key vault. Use the Add-
AzKeyVaultKey cmdlet to create a key encryption key in the key vault. You can also import a KEK from your on-premises key management HSM.
References:
https://www.ciraltos.com/azure-disk-encryption-v2/
https://docs.microsoft.com/en-us/azure/security/azure-security-disk-encryption-prerequisites-aad

Question #34 *Topic 2*

Note: This question is part of 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 company has deployed several virtual machines (VMs) on-premises and to Azure. Azure ExpressRoute has been deployed and configured for on-premises to Azure connectivity.
Several VMs are exhibiting network connectivity issues.
You need to analyze the network traffic to determine whether packets are being allowed or denied to the VMs.
Solution: Use Azure Advisor to analyze the network traffic.
Does the solution meet the goal?

A. Yes

B. No

**Correct Answer:** *B*
Instead use Azure Network Watcher to run IP flow verify to analyze the network traffic.
Note: Advisor is a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.
With Advisor, you can:
Get proactive, actionable, and personalized best practices recommendations.
Improve the performance, security, and high availability of your resources, as you identify opportunities to reduce your overall Azure spend.
Get recommendations with proposed actions inline.
References:
https://docs.microsoft.com/en-us/azure/advisor/advisor-overview

Previous Questions Next Questions