

➤ **Vendor: Microsoft**

➤ **Exam Code: AZ-304**

➤ **Exam Name: Microsoft Azure Architect Design**

➤ **New Updated Questions from [Braindump2go](#) (Updated in [August/2020](#))**

[Visit Braindump2go and Download Full Version AZ-304 Exam Dumps](#)

QUESTION 12
HOTSPOT

You need to design a resource governance solution for an Azure subscription. The solution must meet the following requirements: Ensure

- that all ExpressRoute resources are created in a resource group named RG1.
- Delegate the creation of the ExpressRoute resources to an Azure Active Directory (Azure AD) group named Networking. Use
- the principle of least privilege.

What should you include in the solution? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Ensure that all ExpressRoute resources are created in RG1:	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value=""/> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>A custom RBAC role assignment at the level of RG1</td></tr> <tr><td>A custom RBAC role assignment at the subscription level</td></tr> <tr><td>An Azure Blueprints assignment that sets locking mode for the level of RG1</td></tr> <tr><td>An Azure Policy assignment at the subscription level that has an exclusion</td></tr> <tr><td>Multiple Azure Policy assignments at the resource group level except for RG1</td></tr> </table>	A custom RBAC role assignment at the level of RG1	A custom RBAC role assignment at the subscription level	An Azure Blueprints assignment that sets locking mode for the level of RG1	An Azure Policy assignment at the subscription level that has an exclusion	Multiple Azure Policy assignments at the resource group level except for RG1
A custom RBAC role assignment at the level of RG1						
A custom RBAC role assignment at the subscription level						
An Azure Blueprints assignment that sets locking mode for the level of RG1						
An Azure Policy assignment at the subscription level that has an exclusion						
Multiple Azure Policy assignments at the resource group level except for RG1						
Delegate the creation of the ExpressRoute resources to Networking:	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value=""/> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>A custom RBAC role assignment at the level of RG1</td></tr> <tr><td>A custom RBAC role assignment at the subscription level</td></tr> <tr><td>An Azure Blueprints assignment that sets locking mode for the level of RG1</td></tr> <tr><td>An Azure Policy assignment at the subscription level that has an exclusion</td></tr> <tr><td>Multiple Azure Policy assignments at the resource group level except for RG1</td></tr> </table>	A custom RBAC role assignment at the level of RG1	A custom RBAC role assignment at the subscription level	An Azure Blueprints assignment that sets locking mode for the level of RG1	An Azure Policy assignment at the subscription level that has an exclusion	Multiple Azure Policy assignments at the resource group level except for RG1
A custom RBAC role assignment at the level of RG1						
A custom RBAC role assignment at the subscription level						
An Azure Blueprints assignment that sets locking mode for the level of RG1						
An Azure Policy assignment at the subscription level that has an exclusion						
Multiple Azure Policy assignments at the resource group level except for RG1						

Correct Answer:

Answer Area

Ensure that all ExpressRoute resources are created in RG1:	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value=""/> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr><td>A custom RBAC role assignment at the level of RG1</td></tr> <tr><td>A custom RBAC role assignment at the subscription level</td></tr> <tr><td>An Azure Blueprints assignment that sets locking mode for the level of RG1</td></tr> <tr style="background-color: #e0ffe0;"><td>An Azure Policy assignment at the subscription level that has an exclusion</td></tr> <tr><td>Multiple Azure Policy assignments at the resource group level except for RG1</td></tr> </table>	A custom RBAC role assignment at the level of RG1	A custom RBAC role assignment at the subscription level	An Azure Blueprints assignment that sets locking mode for the level of RG1	An Azure Policy assignment at the subscription level that has an exclusion	Multiple Azure Policy assignments at the resource group level except for RG1
A custom RBAC role assignment at the level of RG1						
A custom RBAC role assignment at the subscription level						
An Azure Blueprints assignment that sets locking mode for the level of RG1						
An Azure Policy assignment at the subscription level that has an exclusion						
Multiple Azure Policy assignments at the resource group level except for RG1						
Delegate the creation of the ExpressRoute resources to Networking:	<div style="border: 1px solid #ccc; padding: 2px;"> <input type="text" value=""/> </div> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr style="background-color: #e0ffe0;"><td>A custom RBAC role assignment at the level of RG1</td></tr> <tr><td>A custom RBAC role assignment at the subscription level</td></tr> <tr><td>An Azure Blueprints assignment that sets locking mode for the level of RG1</td></tr> <tr><td>An Azure Policy assignment at the subscription level that has an exclusion</td></tr> <tr><td>Multiple Azure Policy assignments at the resource group level except for RG1</td></tr> </table>	A custom RBAC role assignment at the level of RG1	A custom RBAC role assignment at the subscription level	An Azure Blueprints assignment that sets locking mode for the level of RG1	An Azure Policy assignment at the subscription level that has an exclusion	Multiple Azure Policy assignments at the resource group level except for RG1
A custom RBAC role assignment at the level of RG1						
A custom RBAC role assignment at the subscription level						
An Azure Blueprints assignment that sets locking mode for the level of RG1						
An Azure Policy assignment at the subscription level that has an exclusion						
Multiple Azure Policy assignments at the resource group level except for RG1						

Explanation

Explanation/Reference:
Explanation:

Box 1: An Azure policy assignment at the subscription level that has an exclusion

2: A custom RBAC role assignment at the level of RG1

Azure role-based access control (Azure RBAC) is the authorization system you use to manage access to Azure resources. To grant access, you assign roles to users, groups, service principals, or managed identities at a particular scope.

Reference:

<https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

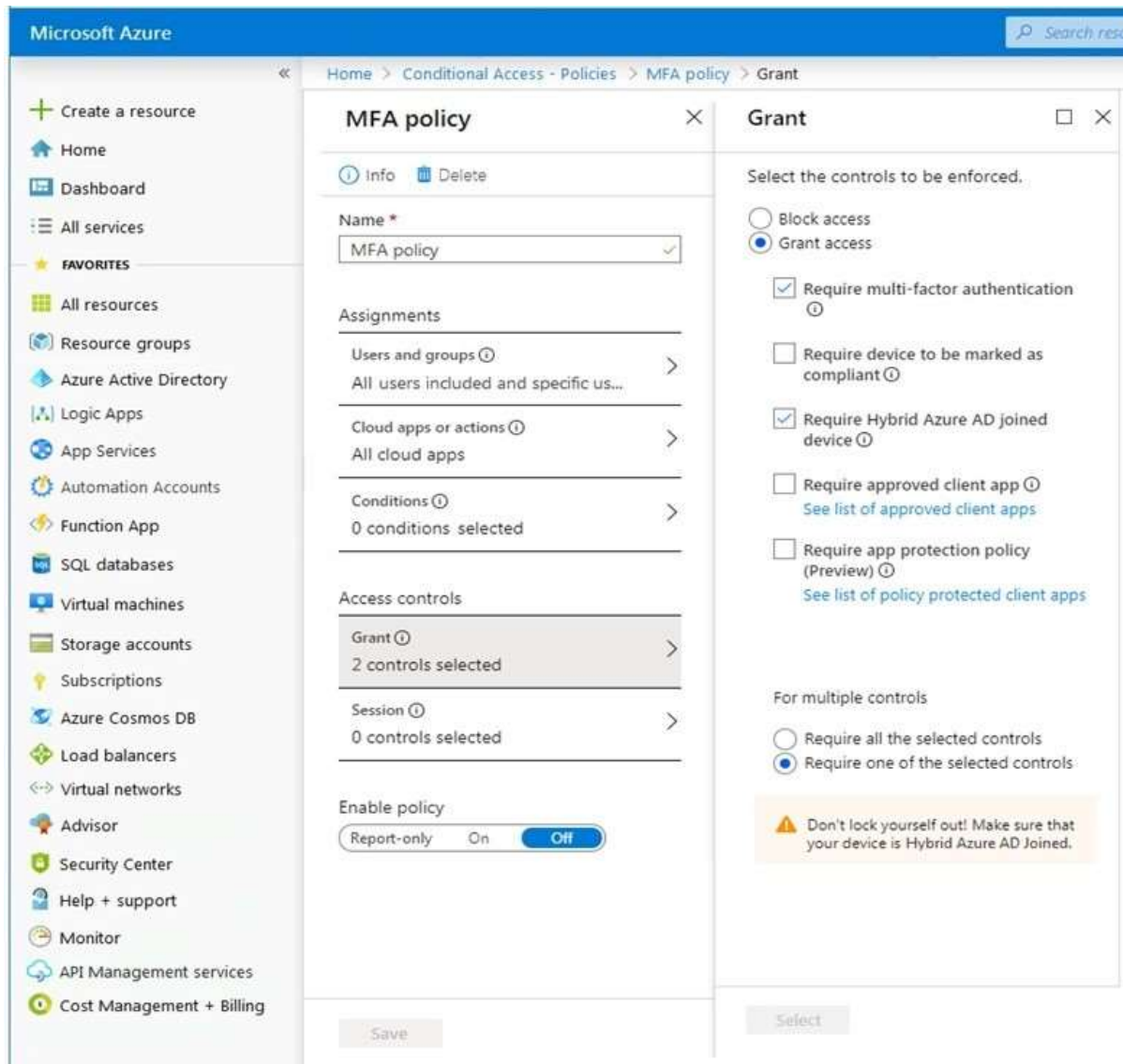
QUESTION 13

You have an Azure Active Directory (Azure AD) tenant and Windows 10 devices.

[AZ-304 Exam Dumps](#) [AZ-304 Exam Questions](#) [AZ-304 PDF Dumps](#) [AZ-304 VCE Dumps](#)

<https://www.braindump2go.com/az-304.html>

You configure a conditional access policy as shown in the exhibit. (Click the **Exhibit** tab.)



The screenshot shows the Azure portal interface for configuring an MFA policy. The 'Grant' tab is active, showing the following settings:

- Name:** MFA policy
- Assignments:**
 - Users and groups: All users included and specific us...
 - Cloud apps or actions: All cloud apps
 - Conditions: 0 conditions selected
- Access controls:**
 - Grant: 2 controls selected
 - Session: 0 controls selected
- Enable policy:** Report-only, On, **Off**

The 'Grant' control configuration panel shows the following options:

- Select the controls to be enforced:**
 - Block access
 - Grant access
 - Require multi-factor authentication
 - Require device to be marked as compliant
 - Require Hybrid Azure AD joined device
 - Require approved client app
 - Require app protection policy (Preview)
- For multiple controls:**
 - Require all the selected controls
 - Require one of the selected controls

A warning message at the bottom states: "Don't lock yourself out! Make sure that your device is Hybrid Azure AD Joined."

What is the result of the policy?

- All users will always be prompted for multi-factor authentication (MFA).
- Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are **NOT** joined to Azure AD.
- All users will be able to sign in without using multi-factor authentication (MFA).
- Users will be prompted for multi-factor authentication (MFA) only when they sign in from devices that are joined to Azure AD.

Correct Answer: B

Explanation

Explanation/Reference:

Explanation:

Either the device should be joined to Azure AD or MFA must be used.

QUESTION 14

You are designing an Azure resource deployment that will use Azure Resource Manager templates. The deployment will use Azure Key Vault to store secrets.

You need to recommend a solution to meet the following requirements:

- Prevent the IT staff that will perform the deployment from retrieving the secrets directly from Key Vault.
- Use the principle of least privilege.

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

NOTE: Each correct selection is worth one point.

- Create a Key Vault access policy that allows all get key permissions, get secret permissions, and get certificate permissions.
- From Access policies in Key Vault, enable access to the Azure Resource Manager for template deployment.
- Create a Key Vault access policy that allows all list key permissions, list secret permissions, and list certificate permissions.
- Assign the IT staff a custom role that includes the Microsoft.KeyVault/Vaults/Deploy/Action permission.
- Assign the Key Vault Contributor role to the IT staff.

Correct Answer: BD

Explanation

Explanation/Reference:

Explanation:

B: To access a key vault during template deployment, set `enabledForTemplateDeployment` on the key vault to true.

D: The user who deploys the template must have the `Microsoft.KeyVault/vaults/deploy/action` permission for the scope of the resource group and key vault.

Incorrect Answers:

E: To grant access to a user to manage key vaults, you assign a predefined key vault Contributor role to the user at a specific scope.

If a user has Contributor permissions to a key vault management plane, the user can grant themselves access to the data plane by setting a Key Vault access policy. You should tightly control who has Contributor role access to your key vaults. Ensure that only authorized persons can access and manage your key vaults, keys, secrets, and certificates.

Reference:

[AZ-304 Exam Dumps](#) [AZ-304 Exam Questions](#) [AZ-304 PDF Dumps](#) [AZ-304 VCE Dumps](#)

<https://www.braindump2go.com/az-304.html>

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/templates/key-vault-parameter>

<https://docs.microsoft.com/en-us/azure/key-vault/general/overview-security>

QUESTION 15

You have an Azure subscription that contains resources in three Azure regions.

You need to implement Azure Key Vault to meet the following requirements:

- In the event of a regional outage, all keys must be readable.
- All the resources in the subscription must be able to access Key Vault.
- The number of Key Vault resources to be deployed and managed must be minimized.

How many instances of Key Vault should you implement?

- A. 1
- B. 2
- C. 3
- D. 6

Correct Answer: A
Explanation

Explanation/Reference:

Explanation:

The contents of your key vault are replicated within the region and to a secondary region at least 150 miles away but within the same geography. This maintains high durability of your keys and secrets. See the Azure paired regions document for details on specific region pairs.

Example: Secrets that must be shared by your application in both Europe West and Europe North. Minimize these as much as you can. Put these in a key vault in either of the two regions. Use the same URI from both regions. Microsoft will fail over the Key Vault service internally.

Reference:

<https://docs.microsoft.com/en-us/azure/key-vault/general/disaster-recovery-guidance>

QUESTION 16

You have an Azure Active Directory (Azure AD) tenant.

You plan to provide users with access to shared files by using Azure Storage. The users will be provided with different levels of access to various Azure file shares based on their user account or their group membership.

You need to recommend which additional Azure services must be used to support the planned deployment.

What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. Azure Information Protection
- C. an Azure AD Domain Services (Azure AD DS) instance
- D. an Azure Front Door instance

Correct Answer: C
Explanation

Explanation/Reference:

Explanation:

Azure Files supports identity-based authentication over Server Message Block (SMB) through two types of Domain Services: on-premises Active Directory Domain Services (AD DS) and Azure Active Directory Domain Services (Azure AD DS).

Reference:

<https://docs.microsoft.com/en-us/azure/storage/files/storage-files-identity-auth-active-directory-domain-service-enable>

QUESTION 17

DRAG DROP

Your company has users who work remotely from laptops.

You plan to move some of the applications accessed by the remote users to Azure virtual machines. The users will access the applications in Azure by using a point-to-site VPN connection. You will use certificates generated from an on-premises-based Certification authority (CA).

You need to recommend which certificates are required for the deployment.

What should you include in the recommendation? To answer, drag the appropriate certificates to the correct targets. Each certificate 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Certificates

A root CA certificate that has the private key

A root CA certificate that has the public key only

A user certificate that has the private key

A user certificate that has the public key only

Answer Area

Trusted Root Certification Authorities certificate store on each laptop: Certificate

The users' Personal store on each laptop: Certificate

The Azure VPN gateway: Certificate

Correct Answer:

Certificates

A root CA certificate that has the private key

A root CA certificate that has the public key only

A user certificate that has the private key

A user certificate that has the public key only

Answer Area

Trusted Root Certification Authorities certificate store on each laptop: A root CA certificate that has the public key only

The users' Personal store on each laptop: A user certificate that has the private key

The Azure VPN gateway: A user certificate that has the public key only

Explanation

Explanation/Reference:

QUESTION 18
HOTSPOT

You are building an application that will run in a virtual machine (VM). The application will use Azure Managed Identity.

The application uses Azure Key Vault, Azure SQL Database, and Azure Cosmos DB.

You need to ensure the application can use secure credentials to access these services.

Which authentication method should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Functionality	Authorization method
Azure Key Vault	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>
Azure SQL	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>
Cosmos DB	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>

Correct Answer:

Answer Area

Functionality	Authorization method
Azure Key Vault	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>
Azure SQL	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>
Cosmos DB	<div style="border: 1px solid gray; padding: 2px;"> <div style="border-bottom: 1px solid gray; padding: 2px;">▼</div> <div style="padding: 2px;"> Hash-based message authentication code (HMAC) Azure Managed Identity Role-Based Access Controls (RBAC) HTTPS encryption </div> </div>

Explanation

Explanation/Reference:

Explanation:

Note: Managed identities for Azure resources is the new name for the service formerly known as Managed Service Identity

(MSI). Reference:

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>

QUESTION 19

You have an Azure subscription that contains a custom application named Application1. Application1 was developed by an external company named Fabrikam, Ltd. Developers at Fabrikam were assigned role-based access control (RBAC) permissions to the Application1 components. All users are licensed for the Microsoft 365 E5 plan.

You need to recommend a solution to verify whether the Fabrikam developers still require permissions to Application1. The solution must meet the following requirements:

- To the manager of the developers, send a monthly email message that lists the access permissions to
- Application1. If the manager does not verify an access permission, automatically revoke that permission.
- Minimize development

effort. What should you

recommend?

- A. Create an Azure Automation runbook that runs the `Get-AzureADUserAppRoleAssignment` cmdlet.
- B. Create an Azure Automation runbook that runs the `Get-AzureRmRoleAssignment` cmdlet.

[AZ-304 Exam Dumps](#) [AZ-304 Exam Questions](#) [AZ-304 PDF Dumps](#) [AZ-304 VCE Dumps](#)

<https://www.braindump2go.com/az-304.html>

- C. In Azure Active Directory (Azure AD), create an access review of Application1.
- D. In Azure Active Directory (AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

Correct Answer: C

Explanation

Explanation/Reference:

QUESTION 20

DRAG DROP

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that uses the Basic license.

You plan to deploy two applications to Azure. The applications have the requirements shown in the following

Application name	Requirement
Customer	Users must authenticate by using a personal Microsoft account and multi-factor authentication
Reporting	Users must authenticate by using either Contoso credentials or a personal Microsoft account. You must be able to manage the accounts from Azure AD.

table.

Which authentication strategy should you recommend for each application? To answer, drag the appropriate authentication strategies to the correct applications. Each authentication strategy 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Authentication Strategies	Answer Area
An Azure AD B2C tenant	Customer: Authentication strategy
An Azure AD v1.0 endpoint	Reporting: Authentication strategy
An Azure AD v2.0 endpoint	

Correct Answer:

Authentication Strategies	Answer Area
An Azure AD B2C tenant	Customer: An Azure AD v2.0 endpoint
An Azure AD v1.0 endpoint	Reporting: An Azure AD B2C tenant
An Azure AD v2.0 endpoint	

Explanation

Explanation/Referen

ce:
Explanation:

Box 1: Azure AD V2.0 endpoint

Microsoft identity platform is an evolution of the Azure Active Directory (Azure AD) developer platform. It allows developers to build applications that sign in all Microsoft identities and get tokens to call Microsoft APIs, such as Microsoft Graph, or APIs that developers have built. The Microsoft identity platform consists of:

- OAuth 2.0 and OpenID Connect standard-compliant authentication service that enables developers to authenticate any Microsoft identity, including: Work or school accounts (provisioned through Azure AD)
- Personal Microsoft accounts (such as Skype, Xbox, and Outlook.com)
- Social or local accounts (via Azure AD B2C)

Box 2: Azure AD B2C tenant

Azure Active Directory B2C provides business-to-customer identity as a service. Your customers use their preferred social, enterprise, or local account identities to get single sign-on access to your applications and APIs.

Azure Active Directory B2C (Azure AD B2C) integrates directly with Azure Multi-Factor Authentication so that you can add a second layer of security to sign-up and sign-in experiences in your applications.

Reference:

[https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-](https://docs.microsoft.com/en-us/azure/active-directory-b2c/active-directory-b2c-reference-mfa)

[mfa https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview](https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-overview)

QUESTION 21

HOTSPOT

You manage a network that includes an on-premises Active Directory domain and an Azure Active Directory (Azure AD).

Employees are required to use different accounts when using on-premises or cloud resources. You must recommend a solution that lets employees sign in to all company resources by using a single account. The solution must implement an identity provider.

You need to provide guidance on the different identity providers.

How should you describe each identity provider? To answer, select the appropriate description from each list in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Identity Provider	Description
synchronized identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.
federated identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.

Correct Answer:

Identity Provider	Description
synchronized identity	<input checked="" type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.
federated identity	<input type="checkbox"/> User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords. <input checked="" type="checkbox"/> User management occurs on-premises. The on-premises domain controller authenticates employee credentials. <input type="checkbox"/> Both user management and authentication occur in Azure AD.

Explanation

Explanation/Referenc

e:

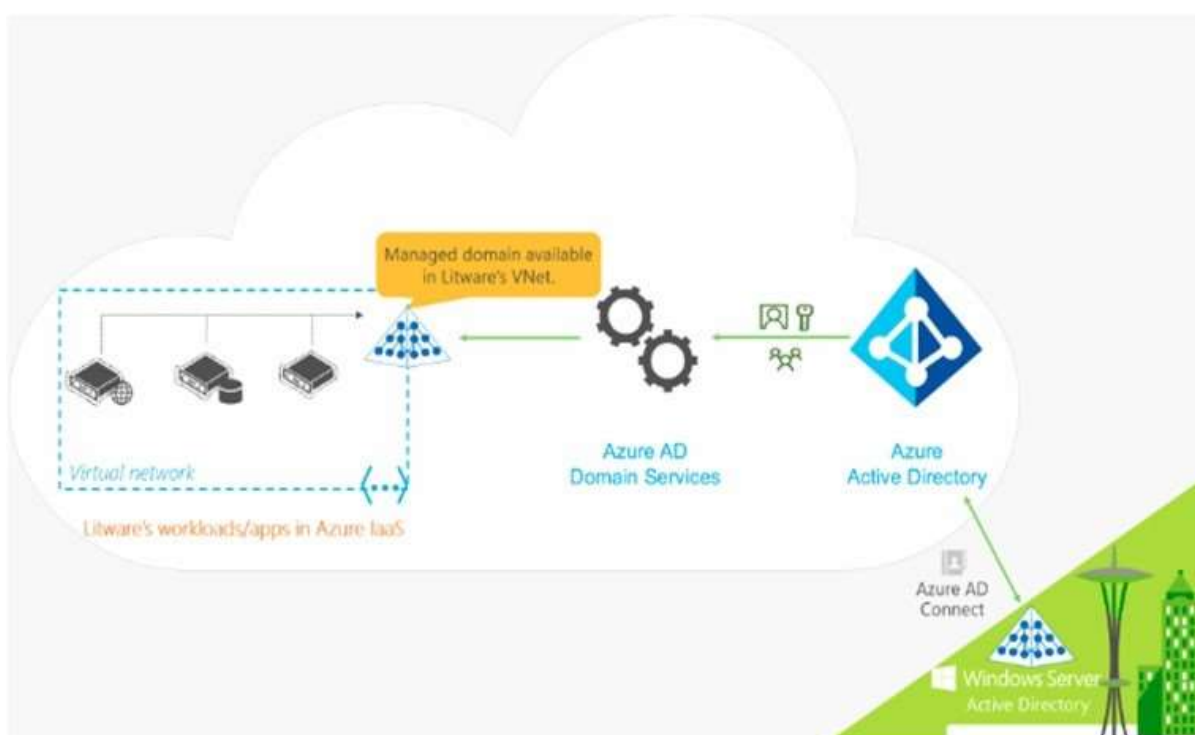
Explanation:

Box1: User management occurs on-premises. Azure AD authenticates employees by using on-premises passwords.

Azure AD Domain Services for hybrid organizations

Organizations with a hybrid IT infrastructure consume a mix of cloud resources and on-premises resources. Such organizations synchronize identity information from their on-premises directory to their Azure AD tenant. As hybrid organizations look to migrate more of their on-premises applications to the cloud, especially legacy directory-aware applications, Azure AD Domain Services can be useful to them.

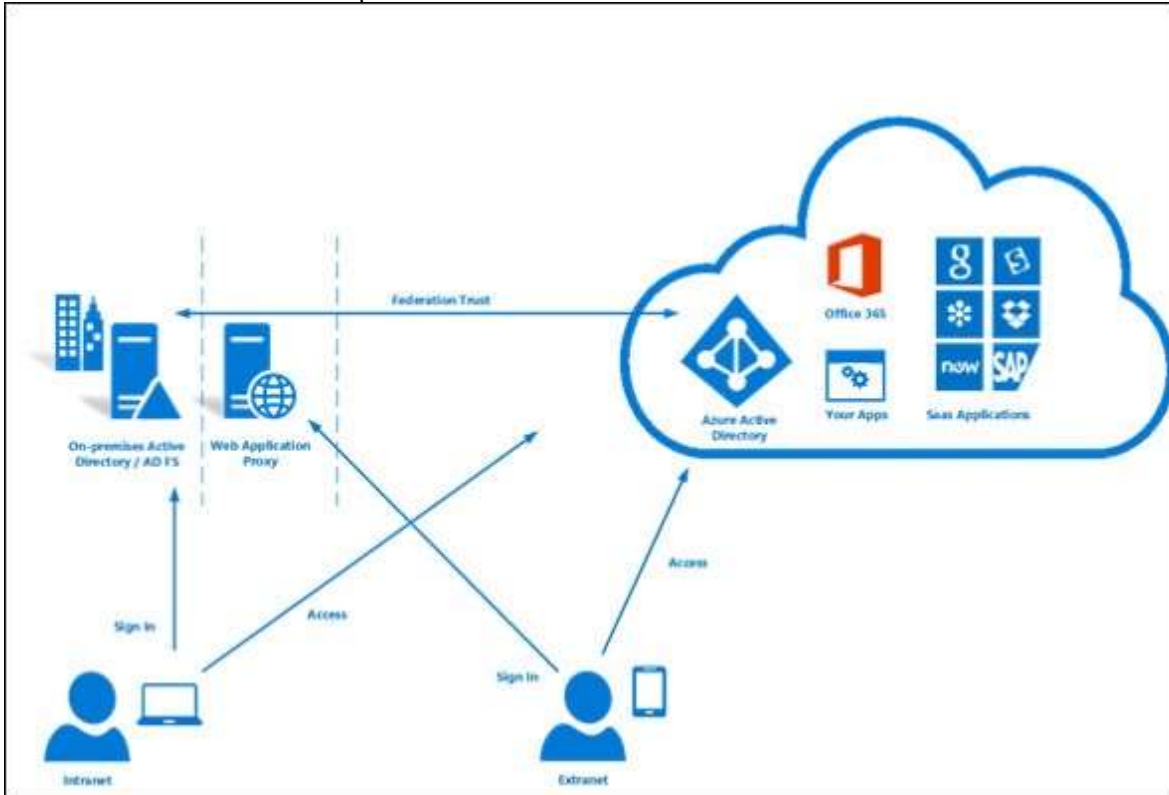
Example: Litware Corporation has deployed Azure AD Connect, to synchronize identity information from their on-premises directory to their Azure AD tenant. The identity information that is synchronized includes user accounts, their credential hashes for authentication (password hash sync) and group memberships.



[Dumps AZ-304 VCE Dumps](https://www.braindump2go.com)

User accounts, group memberships, and credentials from Litware's on-premises directory are synchronized to Azure AD via Azure AD Connect. These user accounts, group memberships, and credentials are automatically available within the managed domain.

Box 2: User management occurs on-premises. The on-premises domain controller authenticates employee credentials. You can federate your on-premises environment with Azure AD and use this federation for authentication and authorization. This sign-in method ensures that all user authentication occurs on-premises.



Reference:

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/active-directory-ds-overview>

<https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-fed>

QUESTION 22
HOTSPOT

You configure the Diagnostics settings for an Azure SQL database as shown in the following exhibit.

Diagnostics settings ✕

Save ✕ Discard 🗑 Delete

Name
Diagnostics

Archive to a storage account

Stream to an event hub

Send to Log Analytics

Subscription
Azure Pass - Sponsorship ▼

Log Analytics Workspace
sk191124 (westeurope) ▼

log

SQLInsights

AutomaticTuning

QueryStoreRuntimeStatistics

QueryStoreWaitStatistics

Errors

DatabaseWaitStatistics

Timeouts

Blocks

Deadlocks

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

[AZ-304 Exam Dumps](#) [AZ-304 Exam Questions](#) [AZ-304 PDF Dumps](#) [AZ-304 VCE Dumps](#)

<https://www.braindump2go.com/az-304.html>

Hot Area:

Answer Area

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

clear Send to Log Analytics
clear SQLInsights
select Archive to a storage account
select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

Azure Analysis Services
Azure Application Insights
Azure SQL Analytics
Microsoft SQL Server Analysis Services (SSAS)
SQL Health Check

Correct Answer:

Answer Area

To perform real-time reporting by using Microsoft Power BI, you must first **[answer choice]**.

clear Send to Log Analytics
clear SQLInsights
select Archive to a storage account
select Stream to an event hub

Diagnostics data can be reviewed in **[answer choice]**.

Azure Analysis Services
Azure Application Insights
Azure SQL Analytics
Microsoft SQL Server Analysis Services (SSAS)
SQL Health Check

Explanation

Explanation/Reference:

