Question #29

Topic 1

HOTSPOT -

You have an Azure subscription that contains a virtual network named VNET1 and 10 virtual machines. The virtual machines are connected to VNET1.

You need to design a solution to manage the virtual machines from the internet. The solution must meet the following requirements:

✑ Incoming connections to the virtual machines must be authenticated by using Azure Multi-Factor Authentication (MFA) before network connectivity is allowed.

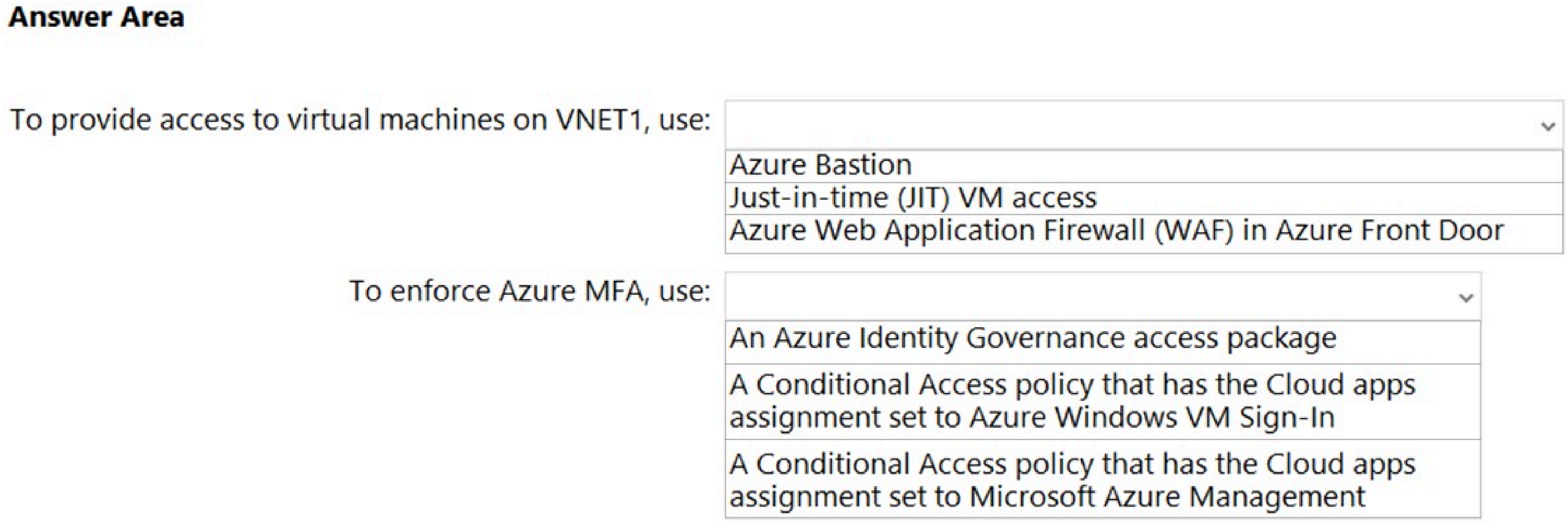
✑ Incoming connections must use TLS and connect to TCP port 443.

✑ The solution must support RDP and SSH.

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

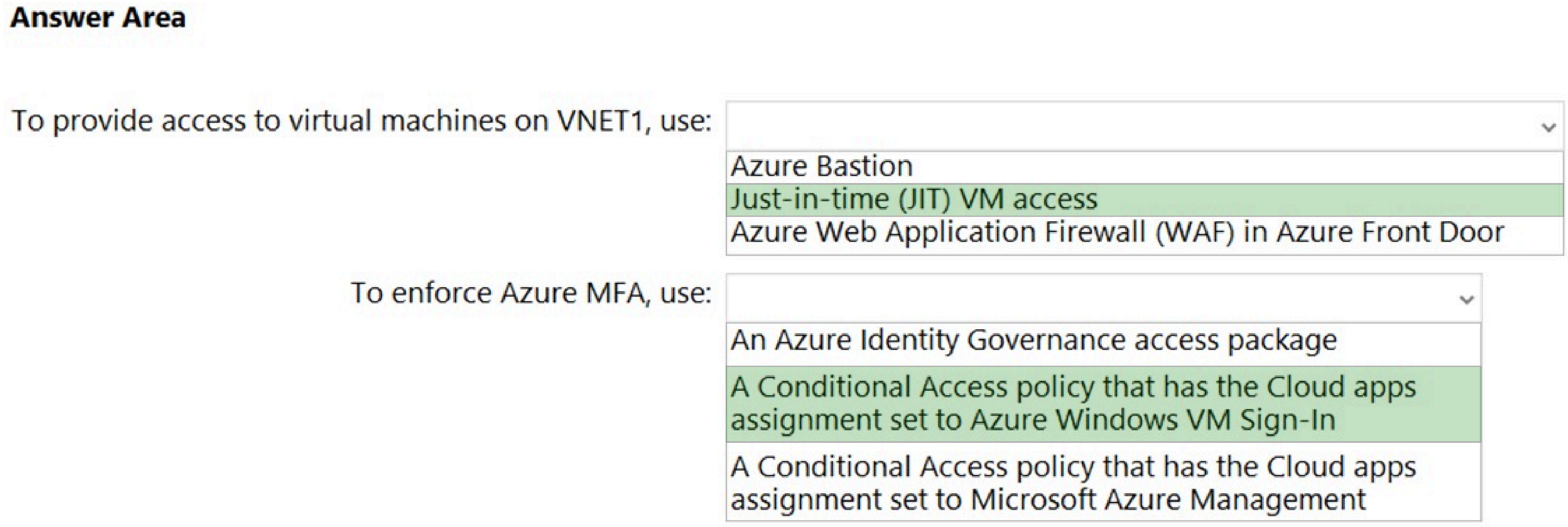
To provide access to virtual machines on VNET1, use:

- Azure Bastion
- Just-in-time (JIT) VM access
- Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

- An Azure Identity Governance access package
- A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In
- A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Correct Answer:



Answer Area

To provide access to virtual machines on VNET1, use:

- Azure Bastion
- [✓ Just-in-time (JIT) VM access]
- Azure Web Application Firewall (WAF) in Azure Front Door

To enforce Azure MFA, use:

- An Azure Identity Governance access package
- [✓ A Conditional Access policy that has the Cloud apps assignment set to Azure Windows VM Sign-In]
- A Conditional Access policy that has the Cloud apps assignment set to Microsoft Azure Management

Box 1: Just-in-time (JIT) VN access

Lock down inbound traffic to your Azure Virtual Machines with Microsoft Defender for Cloud's just-in-time (JIT) virtual machine (VM) access feature. This reduces exposure to attacks while providing easy access when you need to connect to a VM.

Note: Threat actors actively hunt accessible machines with open management ports, like RDP or SSH. Your legitimate users also use these ports, so it's not practical to keep them closed.

When you enable just-in-time VM access, you can select the ports on the VM to which inbound traffic will be blocked.

To solve this dilemma, Microsoft Defender for Cloud offers JIT. With JIT, you can lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Box 2: A conditional Access policy that has Cloud Apps assignment set to Azure Windows VM Sign-In

You can enforce Conditional Access policies such as multi-factor authentication or user sign-in risk check before authorizing access to Windows VMs in Azure that are enabled with Azure AD sign in. To apply Conditional Access policy, you must select the "Azure Windows VM Sign-In" app from the cloud apps or actions assignment option and then use Sign-in risk as a condition and/or require multi-factor authentication as a grant access control.

Reference:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-overview https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-vm-sign-in-azure-ad-windows

Question #30 *Topic 1*

You are designing an Azure governance solution.
All Azure resources must be easily identifiable based on the following operational information: environment, owner, department and cost center.
You need to ensure that you can use the operational information when you generate reports for the Azure resources.
What should you include in the solution?

A. an Azure data catalog that uses the Azure REST API as a data source

B. an Azure management group that uses parent groups to create a hierarchy

C. an Azure policy that enforces tagging rules

D. Azure Active Directory (Azure AD) administrative units

Correct Answer: *C*
You apply tags to your Azure resources, resource groups, and subscriptions to logically organize them into a taxonomy. Each tag consists of a name and a value pair.
You use Azure Policy to enforce tagging rules and conventions. By creating a policy, you avoid the scenario of resources being deployed to your subscription that don't have the expected tags for your organization. Instead of manually applying tags or searching for resources that aren't compliant, you create a policy that automatically applies the needed tags during deployment.
Reference:
https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

Community vote distribution

C (100%)

Question #31 *Topic 1*

A company named Contoso, Ltd. has an Azure Active Directory (Azure AD) tenant that is integrated with Microsoft 365 and an Azure subscription.
Contoso has an on-premises identity infrastructure. The infrastructure includes servers that run Active Directory Domain Services (AD DS) and Azure AD Connect.
Contoso has a partnership with a company named Fabrikam. Inc. Fabrikam has an Active Directory forest and a Microsoft 365 tenant. Fabrikam has the same on- premises identity infrastructure components as Contoso.
A team of 10 developers from Fabrikam will work on an Azure solution that will be hosted in the Azure subscription of Contoso. The developers must be added to the Contributor role for a resource group in the Contoso subscription.
You need to recommend a solution to ensure that Contoso can assign the role to the 10 Fabrikam developers. The solution must ensure that the Fabrikam developers use their existing credentials to access resources
What should you recommend?

A. In the Azure AD tenant of Contoso. create cloud-only user accounts for the Fabrikam developers.

B. Configure a forest trust between the on-premises Active Directory forests of Contoso and Fabrikam.

C. Configure an organization relationship between the Microsoft 365 tenants of Fabrikam and Contoso.

D. In the Azure AD tenant of Contoso, create guest accounts for the Fabnkam developers.

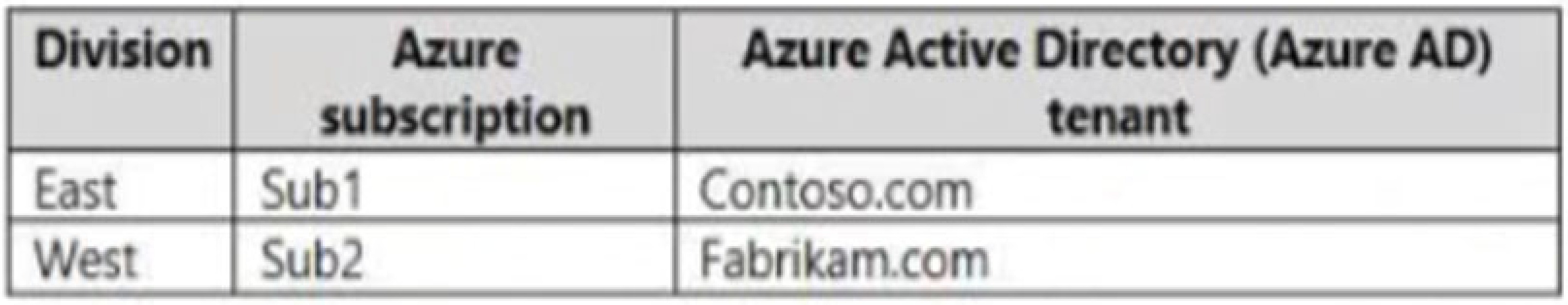
Correct Answer: *D*
You can use the capabilities in Azure Active Directory B2B to collaborate with external guest users and you can use Azure RBAC to grant just the permissions that guest users need in your environment.
Incorrect:
Not B: Forest trust is used for internal security, not external access.
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users

Community vote distribution

D (94%) 4%

Question #32 *Topic 1*

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.
You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.
What should you recommend?

A. Configure the Azure AD provisioning service.

B. Enable Azure AD pass-through authentication and update the sign-in endpoint.

C. Use Azure AD entitlement management to govern external users.

D. Configure Azure AD join.

Correct Answer: *A*
You can enable automatic user provisioning for your multi-tenant application in Azure Active Directory.
Automatic user provisioning is the process of automating the creation, maintenance, and removal of user identities in target systems like your software-as-a- service applications.
Azure AD provides several integration paths to enable automatic user provisioning for your application.
* The Azure AD Provisioning Service manages the provisioning and deprovisioning of users from Azure AD to your application (outbound provisioning) and from your application to Azure AD (inbound provisioning). The service connects to the System for Cross-Domain Identity Management (SCIM) user management API endpoints provided by your application.
* Microsoft Graph
* The Security Assertion Markup Language Just in Time (SAML JIT) user provisioning.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/isv-automatic-provisioning-multi-tenant-apps

Community vote distribution

C (100%)

Question #33 *Topic 1*

HOTSPOT -

Your company has 20 web APIs that were developed in-house.

The company is developing 10 web apps that will use the web APIs. The web apps and the APIs are registered in the company s Azure Active Directory (Azure
AD) tenant. The web APIs are published by using Azure API Management.

You need to recommend a solution to block unauthorized requests originating from the web apps from reaching the web APIs. The solution must meet the following requirements:

➾ Use Azure AD-generated claims.

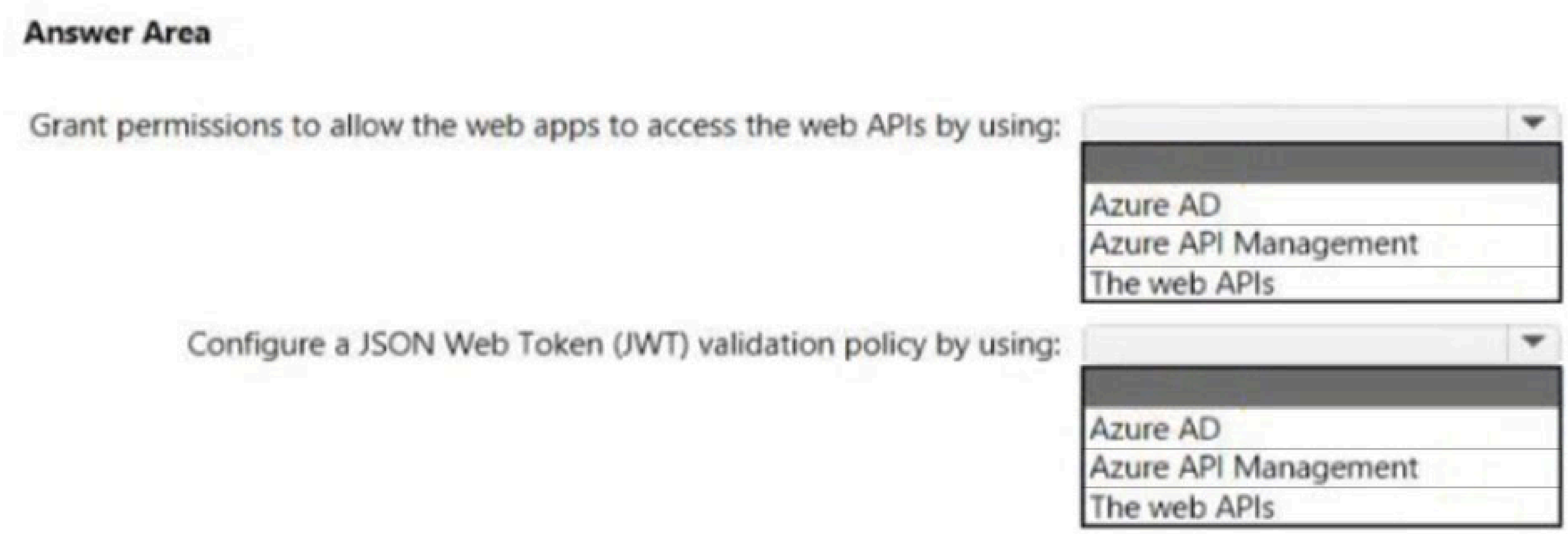
Minimize configuration and management effort.

▪

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

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

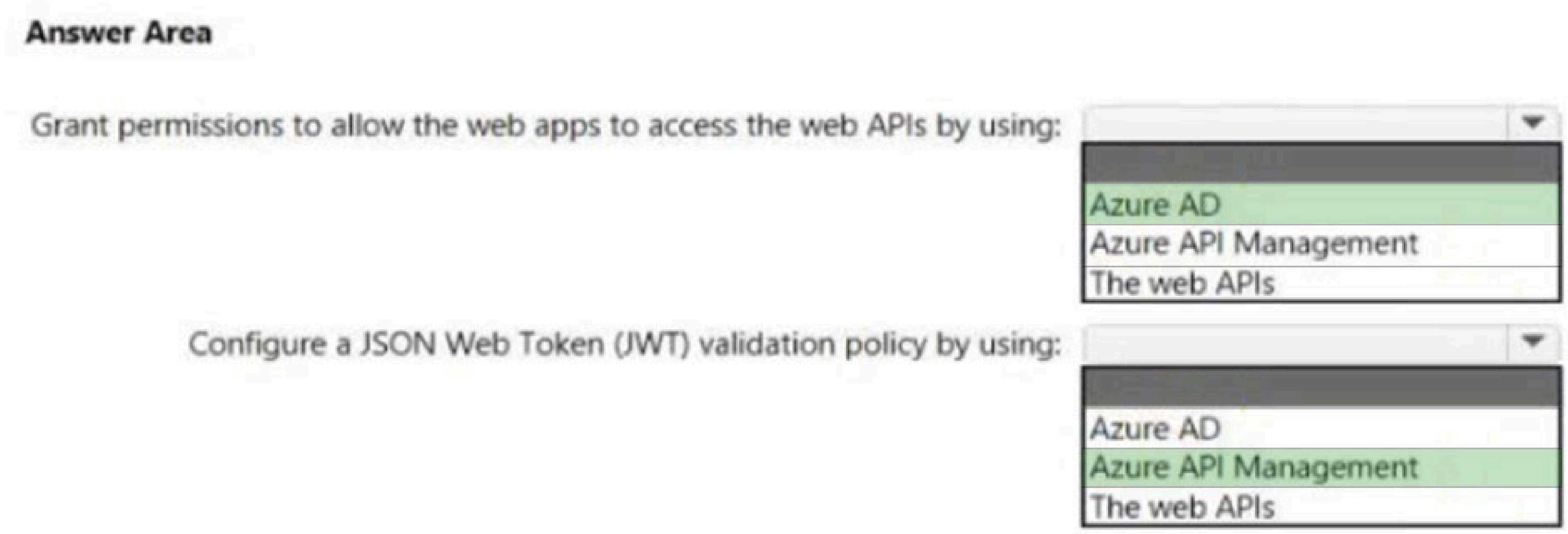
Grant permissions to allow the web apps to access the web APIs by using:

- Azure AD
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- Azure API Management
- The web APIs

Correct Answer:



Answer Area

Grant permissions to allow the web apps to access the web APIs by using:

- [✓ Azure AD]
- Azure API Management
- The web APIs

Configure a JSON Web Token (JWT) validation policy by using:

- Azure AD
- [✓ Azure API Management]
- The web APIs

Box 1: Azure AD -

Grant permissions in Azure AD.

Box 2: Azure API Management -

Configure a JWT validation policy to pre-authorize requests.

Pre-authorize requests in API Management with the Validate JWT policy, by validating the access tokens of each incoming request. If a request does not have a valid token, API Management blocks it.

Reference:

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-protect-backend-with-aad

Question #34 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.
What should you include in the recommendation?

A. Azure Log Analytics

B. Azure Arc

C. Azure Analysis Services

D. Application Insights

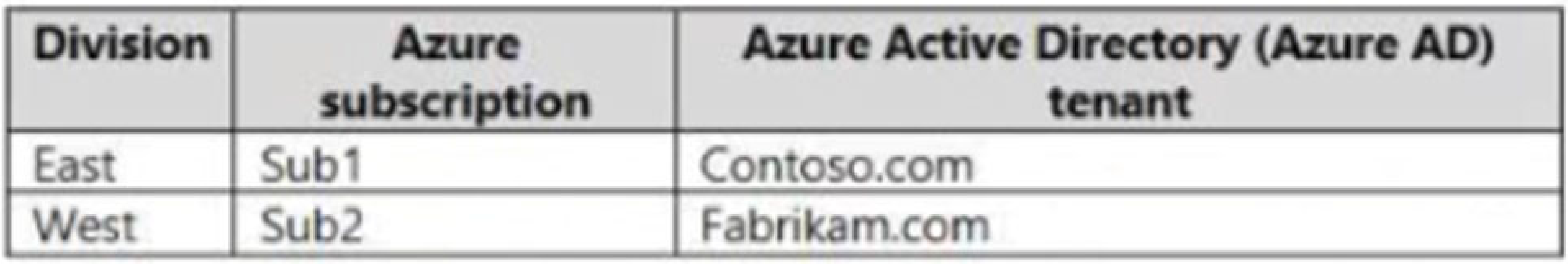
Correct Answer: *A*
The Activity log is a platform log in Azure that provides insight into subscription-level events. Activity log includes such information as when a resource is modified or when a virtual machine is started.
Activity log events are retained in Azure for 90 days and then deleted.
For more functionality, you should create a diagnostic setting to send the Activity log to one or more of these locations for the following reasons: to Azure Monitor Logs for more complex querying and alerting, and longer retention (up to two years) to Azure Event Hubs to forward outside of Azure to Azure Storage for cheaper, long-term archiving
Note: Azure Monitor builds on top of Log Analytics, the platform service that gathers log and metrics data from all your resources. The easiest way to think about it is that Azure Monitor is the marketing name, whereas Log Analytics is the technology that powers it.
Reference:
https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

Community vote distribution

A (100%)

Question #35 *Topic 1*

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure Active Directory (Azure AD) tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.
You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.
What should you recommend?

A. Configure the Azure AD provisioning service.

B. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

C. Use Azure AD entitlement management to govern external users.

D. Configure Azure AD Identity Protection.

Correct Answer: *C*
Entitlement management is an identity governance capability that enables organizations to manage identity and access lifecycle at scale by automating access request workflows, access assignments, reviews, and expiration. Entitlement management allows delegated non-admins to create access packages that external users from other organizations can request access to. One and multi-stage approval workflows can be configured to evaluate requests, and provision users for time-limited access with recurring reviews. Entitlement management enables policy-based provisioning and deprovisioning of external accounts.

Note: Access Packages -
An access package is the foundation of entitlement management. Access packages are groupings of policy-governed resources a user needs to collaborate on a project or do other tasks. For example, an access package might include: access to specific SharePoint sites. enterprise applications including your custom in-house and SaaS apps like Salesforce.
Microsoft Teams.
Microsoft 365 Groups.
Incorrect:
Not A: Automatic provisioning refers to creating user identities and roles in the cloud applications that users need access to. In addition to creating user identities, automatic provisioning includes the maintenance and removal of user identities as status or roles change.
Not B: Privileged Identity Management provides time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources that you care about. Here are some of the key features of Privileged Identity Management:
Provide just-in-time privileged access to Azure AD and Azure resources
Assign time-bound access to resources using start and end dates
Etc.
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/6-secure-access-entitlement-managment
https://docs.microsoft.com/en-us/azure/active-directory/app-provisioning/how-provisioning-works https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure

Community vote distribution

C (100%)

Question #36 *Topic 1*

You are developing an app that will read activity logs for an Azure subscription by using Azure Functions.

You need to recommend an authentication solution for Azure Functions. The solution must minimize administrative effort.

What should you include in the recommendation?

A. an enterprise application in Azure AD

B. system-assigned managed identities

C. shared access signatures (SAS)

D. application registration in Azure AD

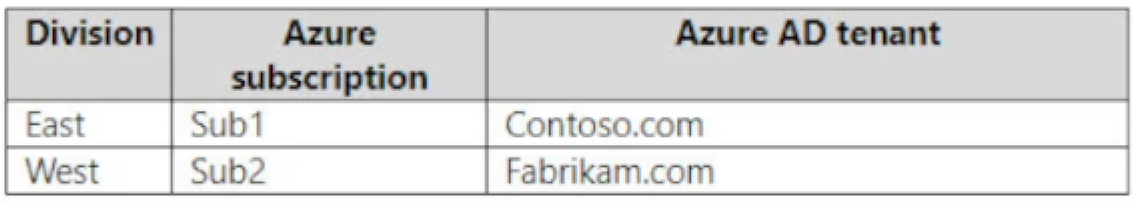
Correct Answer: *B*

Community vote distribution

B (100%)

Question #37 *Topic 1*

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Use Azure AD entitlement management to govern external users.

C. Enable Azure AD pass-through authentication and update the sign-in endpoint.

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

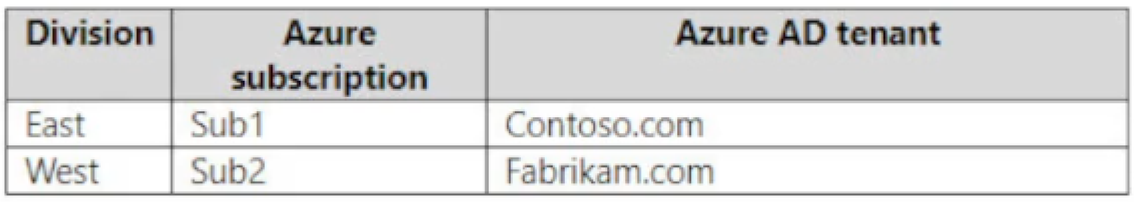
Correct Answer: *B*

Community vote distribution

B (100%)

Question #38 *Topic 1*

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Configure Azure AD Identity Protection.

C. Use Azure AD entitlement management to govern external users.

D. Configure assignments for the fabrikam.com users by using Azure AD Privileged Identity Management (PIM).

Correct Answer: *C*

Community vote distribution

C (100%)

Question #39 *Topic 1*

You need to recommend a solution to generate a monthly report of all the new Azure Resource Manager (ARM) resource deployments in your Azure subscription.

What should you include in the recommendation?

A. Azure Activity Log

B. Azure Arc

C. Azure Analysis Services

D. Azure Monitor metrics

Correct Answer: *A*

Community vote distribution

A (100%)

Question #40

Topic 1

HOTSPOT

-

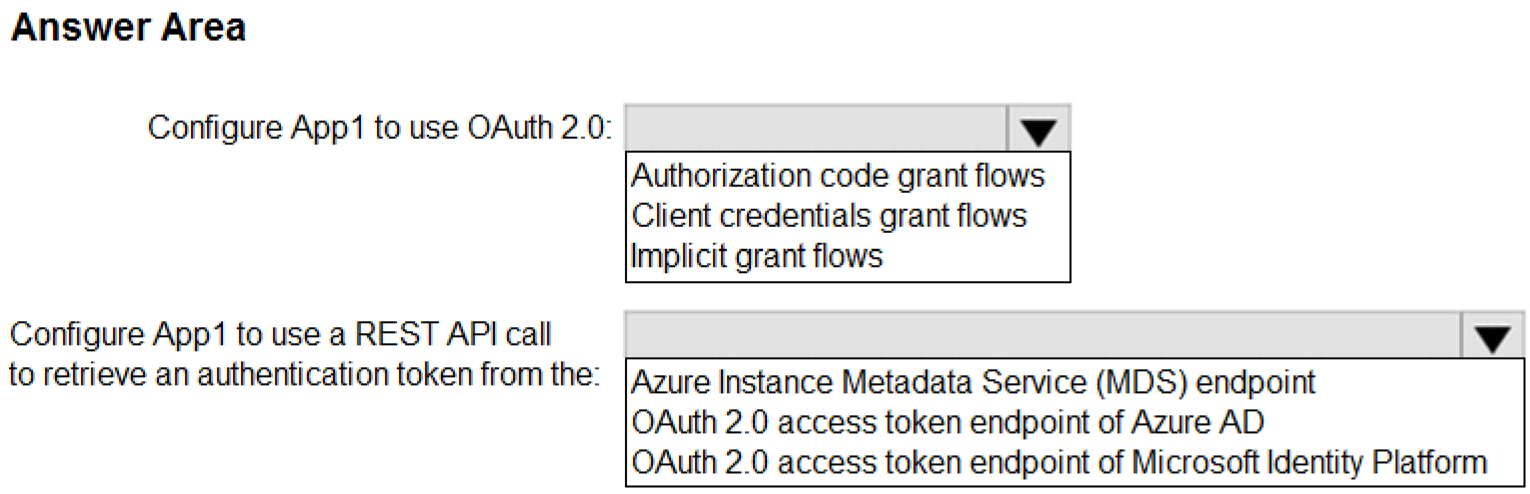
You have an Azure subscription that contains an Azure key vault named KV1 and a virtual machine named VM1. VM1 runs Windows Server 2022: Azure Edition.

You plan to deploy an ASP.Net Core-based application named App1 to VM1.

You need to configure App1 to use a system-assigned managed identity to retrieve secrets from KV1. The solution must minimize development effort.

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

NOTE: Each correct selection is worth one point.



Answer Area

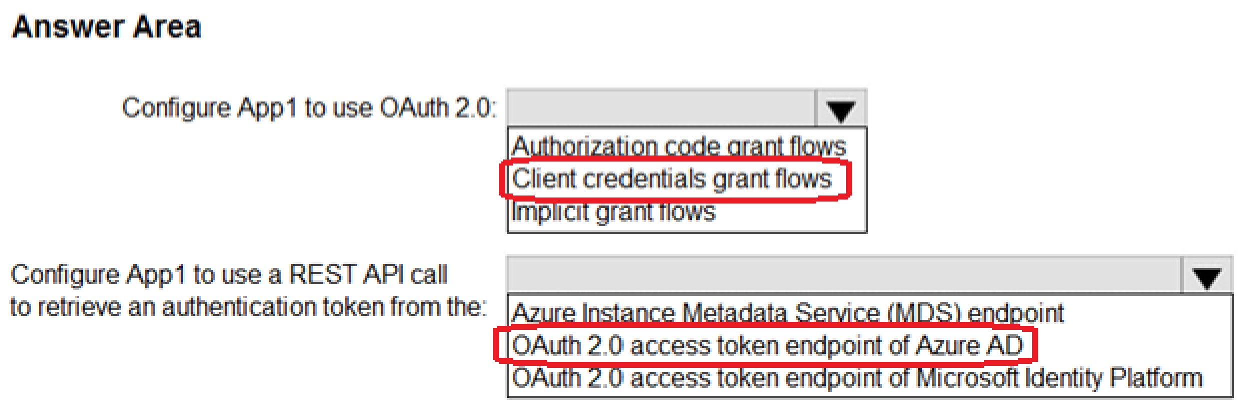
Configure App1 to use OAuth 2.0:

- Authorization code grant flows
- Client credentials grant flows
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

- Azure Instance Metadata Service (MDS) endpoint
- OAuth 2.0 access token endpoint of Azure AD
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Correct Answer:



Answer Area

Configure App1 to use OAuth 2.0:

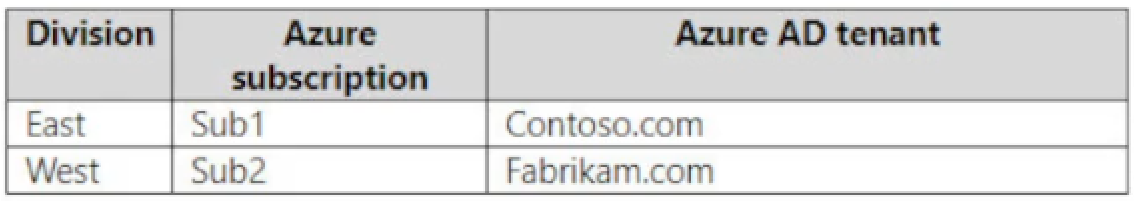
- Authorization code grant flows
- [✓ Client credentials grant flows]
- Implicit grant flows

Configure App1 to use a REST API call to retrieve an authentication token from the:

- Azure Instance Metadata Service (MDS) endpoint
- [✓ OAuth 2.0 access token endpoint of Azure AD]
- OAuth 2.0 access token endpoint of Microsoft Identity Platform

Question #41 *Topic 1*

Your company has the divisions shown in the following table.



Division	Azure subscription	Azure AD tenant
East	Sub1	Contoso.com
West	Sub2	Fabrikam.com

Sub1 contains an Azure App Service web app named App1. App1 uses Azure AD for single-tenant user authentication. Users from contoso.com can authenticate to App1.

You need to recommend a solution to enable users in the fabrikam.com tenant to authenticate to App1.

What should you recommend?

A. Configure Azure AD join.

B. Configure Azure AD Identity Protection.

C. Configure a Conditional Access policy.

D. Configure Supported account types in the application registration and update the sign-in endpoint.

Correct Answer: *D*

Community vote distribution

D (100%)

Question #42 *Topic 1*

You have an Azure AD tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned memberships. Group1 has 50 members, including 20 guest users.

You need to recommend a solution for evaluating the membership of Group1. The solution must meet the following requirements:

- The evaluation must be repeated automatically every three months.
- Every member must be able to report whether they need to be in Group1.
- Users who report that they do not need to be in Group1 must be removed from Group1 automatically.
- Users who do not report whether they need to be in Group1 must be removed from Group1 automatically.

What should you include in the recommendation?

A. Implement Azure AD Identity Protection.

B. Change the Membership type of Group1 to Dynamic User.

C. Create an access review.

D. Implement Azure AD Privileged Identity Management (PIM).

Correct Answer: *D*

Community vote distribution

C (97%)