Advanced Multiple Choice Questions: Part 1 - Results

Back to result overview

Attempt 1

All domains

35 all | 0 correct | 0 incorrect | 35 skipped | 0 marked

Collapse all questions

Question 1 Skipped

You are designing a large Azure environment that will contain many subscriptions.

You plan to use Azure Policy as part of a governance solution.

To which three scopes can you assign Azure Policy definitions? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

compute resources

Correct selection

management groups

Correct selection

resource groups

Azure Active Directory (Azure AD) administrative units

Correct selection

subscriptions

Azure Active Directory (Azure AD) tenants

Overall explanation

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources.

https://docs.microsoft.com/en-us/azure/governance/policy/overview

Question 2 Skipped

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 on the review screen.

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Advisor to analyze the network traffic.

Does this meet the goal?

Correct answer

No

Yes

Overall explanation

Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.

Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Question 3 Skipped

Your company, named Contoso, Ltd., implements several Azure logic apps that have HTTP triggers. The logic apps provide access to an on-premises web service.

Contoso establishes a partnership with another company named Fabrikam, Inc.

Fabrikam does not have an existing Azure Active Directory (Azure AD) tenant and uses third-party OAuth 2.0 identity management to authenticate its users.

Developers at Fabrikam plan to use a subset of the logic apps to build applications that will integrate with the on-premises web service of Contoso.

You need to design a solution to provide the Fabrikam developers with access to the logic apps. The solution must meet the following requirements:

- Requests to the logic apps from the developers must be limited to lower rates than the requests from the users at Contoso.

- The developers must be able to rely on their existing OAuth 2.0 provider to gain access to the logic apps.
- The solution must NOT require changes to the logic apps.
- The solution must NOT use Azure AD guest accounts.

What should you include in the solution?

Correct answer

Azure API Management

Azure AD business-to-business (B2B)

Azure AD Application Proxy

Azure Front Door

Overall explanation

Many APIs support OAuth 2.0 to secure the API and ensure that only valid users have access, and they can only access resources to which they're entitled. To use Azure API Management's interactive developer console with such APIs, the service allows you to configure your service instance to work with your OAuth 2.0-enabled API.

https://docs.microsoft.com/en-us/azure/api-management/api-management-howto-oauth2

Question 4 Skipped

You have an Azure subscription that contains two applications named App1 and App2. App1 is a sales processing application. When a transaction in App1 requires shipping, a message is added to an Azure Storage account queue, and then App2 listens to the queue for relevant transactions.

In the future, additional applications will be added that will process some of the shipping requests based on the specific details of the transactions.

You need to recommend a replacement for the storage account queue to ensure that each additional application will be able to read the relevant transactions.

What should you recommend?

multiple storage account queues

one Azure Data Factory pipeline

Correct answer

one Azure Service Bus topic

one Azure Service Bus queue

Overall explanation

A queue allows the processing of a message by a single consumer. In contrast to queues, topics, and subscriptions provide a one-to-many form of communication in a publish and subscribe pattern. It's useful for scaling to large numbers of recipients. Each published message is made available to each subscription registered with the topic. Publisher sends a message to a topic and one or more subscribers receive a copy of the message, depending on filter rules set on these subscriptions.

https://docs.microsoft.com/en-us/azure/service-bus-messaging/service-bus-queues-topics-subscriptions

Question 5 Skipped

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?

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

Azure Active Directory (Azure AD) administrative units

Correct answer

an Azure policy that enforces tagging rules

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

Overall explanation

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.

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/tag-policies

Question 6 Skipped

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

You plan to deploy Azure Cosmos DB databases that will use the SQL API.

You need to recommend a solution to provide specific Azure AD user accounts with read access to the Cosmos DB databases.

What should you include in the recommendation?

Master keys and Azure Information Protection policies

Certificates and Azure Key Vault

Correct answer

a resource token and an Access control (IAM) role assignment

Shared Access Signatures (SAS) and Conditional Access policies

Overall explanation

The Access control (IAM) pane in the Azure portal is used to configure role-based access control on Azure Cosmos resources. The roles are applied to users, groups, service principals, and managed identities in Active Directory. You can use built-in roles or custom roles for individuals and groups.

Note: To use the Azure Cosmos DB RBAC in your application, you have to update the way you initialize the Azure Cosmos DB SDK. Instead of passing your account's primary key,

you have to pass an instance of a TokenCredential class. This instance provides the Azure Cosmos DB SDK with the context required to fetch an Azure AD (AAD) token on behalf of the identity you wish to use.

https://docs.microsoft.com/en-us/azure/cosmos-db/role-based-access-control

https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-setup-rbac

Question 7 Skipped

You plan to deploy an Azure SQL database that will store Personally Identifiable Information (PII).

You need to ensure that only privileged users can view the PII.

What should you include in the solution?

Correct answer

Dynamic Data Masking

Transparent Data Encryption (TDE)

Role-Based Access Control (RBAC)

Data Discovery & Classification

Overall explanation

Dynamic data masking limits sensitive data exposure by masking it to non-privileged users.

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on

the application layer. It's a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

https://docs.microsoft.com/en-us/azure/azure-sql/database/dynamic-data-masking-overview

Question 8 Skipped

You have an Azure subscription that contains 1,000 resources.

You need to generate compliance reports for the subscription. The solution must ensure that the resources can be grouped by department.

What should you use to organize the resources?

resource groups and role assignments

administrative units and Azure Lighthouse

Correct answer

Azure Policy and tags

application groups and quotas

Overall explanation

Azure Policy and tags provide a powerful combination to organize and manage resources in Azure. You can create and apply Azure Policy definitions to enforce compliance requirements across your subscription. Azure Policy enables you to define and enforce rules and guidelines for resource configurations, access controls, and other governance

aspects. By applying policies, you can ensure that resources adhere to specific compliance standards.

In addition to Azure Policy, you can use tags to categorize resources based on different criteria, such as department, environment, project, or cost center. By applying tags to resources, you can easily group and classify them for organizational purposes. By leveraging Azure Policy and tags together, you can enforce compliance rules and also organize resources based on the department. This allows you to generate compliance reports specific to each department, providing clear visibility and control over the compliance status of resources.

Question 9 Skipped

You plan to deploy an application named App1 that will run on five Azure virtual machines. Additional virtual machines will be deployed later to run App1.

You need to recommend a solution to meet the following requirements for the virtual machines that will run App1:

- Ensure that the virtual machines can authenticate to Azure Active Directory (Azure AD) to gain access to an Azure key vault, Azure Logic Apps instances, and an Azure SQL database.
- Avoid assigning new roles and permissions for Azure services when you deploy additional virtual machines.
- Avoid storing secrets and certificates on virtual machines.
- Minimize administrative effort for managing identities.

Which type of identity should you include in the recommendation?

a service principal that is configured to use a certificate

a system-assigned managed identity

Correct answer

a user-assigned managed identity

a service principal that is configured to use a client secret

Overall explanation

Managed identities provide an identity for applications to use when connecting to resources that support Azure Active Directory (Azure AD) authentication.

A user-assigned managed identity:

- Can be shared.
- The same user-assigned managed identity can be associated with more than one Azure resource.

Common usage:

- Workloads that run on multiple resources and can share a single identity.
- For example, a workload where multiple virtual machines need to access the same resource.

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

Question 10 Skipped

You are developing an app that will use Azure Functions to process Azure Event Hubs events. Request processing is estimated to take between five and 20 minutes.

You need to recommend a hosting solution that meets the following requirements:

- Supports estimates of request processing runtimes
- Supports event-driven autoscaling for the app

Which hosting plan should you recommend?

Correct answer

Premium

Dedicated

Consumption

App Service

Overall explanation

The Premium plan is the best fit for this scenario. It supports both longer execution times and event-driven scaling, which are the requirements specified in the question. Azure Functions on a Premium plan can run for a longer period, up to 60 minutes (or indefinitely if the host.json "functionTimeout" setting is null), making it suitable for the estimated request processing times of five to 20 minutes. The Premium plan also supports event-driven autoscaling. The Consumption plan supports event-driven autoscaling but only allows functions to run for up to 10 minutes, so it wouldn't support the estimated request processing times of five to 20 minutes. The Dedicated and App Service plans can run for a longer period, but they do not support event-driven autoscaling. The Dedicated plan is also the most costly option and should be used when you need the most control over the function app environment.

https://learn.microsoft.com/en-us/azure/event-hubs/compare-tiers

Question 11 Skipped

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?

Correct answer

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

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

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

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

Overall explanation

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.

https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-external-users

Question 12 Skipped

You have 100 servers that run Windows Server 2012 R2 and host Microsoft SQL Server 2014 instances. The instances host databases that have the following characteristics:

- Stored procedures are implemented by using CLR.
- The largest database is currently 3 TB. None of the databases will ever exceed 4 TB.

You plan to move all the data from SQL Server to Azure.

You need to recommend a service to host the databases. The solution must meet the following requirements:

- Whenever possible, minimize management overhead for the migrated databases.
- Ensure that users can authenticate by using Azure Active Directory (Azure AD) credentials.
- Minimize the number of database changes required to facilitate the migration.

What should you include in the recommendation?

SQL Server 2016 on Azure virtual machines

Correct answer

Azure SQL Managed Instance

Azure SQL Database elastic pools

Azure SQL Database single databases

Overall explanation

SQL Managed Instance allows existing SQL Server customers to lift and shift their on-premises applications to the cloud with minimal application and database changes. At the same time, SQL Managed Instance preserves all PaaS capabilities (automatic patching and version updates, automated backups, high availability) that drastically reduce management overhead and TCO.

https://docs.microsoft.com/en-us/azure/sql-database/sql-database-managed-instance

Question 13 Skipped

You have an Azure subscription that contains 10 web apps. The apps are integrated with Azure AD and are accessed by users on different project teams.

The users frequently move between projects.

You need to recommend an access management solution for the web apps. The solution must meet the following requirements:

- The users must only have access to the app of the project to which they are assigned currently.
- Project managers must verify which users have access to their project's app and remove users that are no longer assigned to their project.
- Once every 30 days, the project managers must be prompted automatically to verify which users are assigned to their projects.

What should you include in the recommendation?

Microsoft Defender for Identity

Azure AD Identity Protection

Correct answer

Azure AD Identity Governance

Microsoft Entra Permissions Management

Overall explanation

Azure AD Identity Governance provides a comprehensive solution for managing identity and access lifecycle, ensuring that access is granted in line with the principle of least privilege and is revoked when no longer needed1. It allows project managers to verify which users have access to their project's app and remove users that are no longer assigned to their project.

Question 14 Skipped

You have an Azure Active Directory (Azure AD) tenant named contoso.com that has a security group named Group1. Group1 is configured for assigned membership. 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?

Implement Azure AD Privileged Identity Management (PIM).

Change the Membership type of Group1 to Dynamic User.

Correct answer

Create an access review.

Implement Azure AD Identity Protection.

Overall explanation

Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User's access can be reviewed on a regular basis to make sure only the right people have continued access.

https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question 15 Skipped

You plan to deploy an app that will use an Azure Storage account.

You need to deploy the storage account. The storage account must meet the following requirements:

- Store the data for multiple users.
- Encrypt each user's data by using a separate key.
- Encrypt all the data in the storage account by using customer-managed keys.

What should you deploy?

files in a general purpose v2 storage account

files in a premium file share storage account

Correct answer

blobs in a general purpose v2 storage account

blobs in an Azure Data Lake Storage Gen2 account

Overall explanation

You can specify a customer-provided key on Blob storage operations. A client making a read or write request against Blob storage can include an encryption key on the request for granular control over how blob data is encrypted and decrypted.

https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption

Question 16 Skipped

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?

Application Insights

Correct answer

Azure Log Analytics

Azure Arc

Azure Analysis Services

Overall explanation

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.

https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log

Question 17 Skipped

You have an Azure Active Directory (Azure AD) tenant that syncs with an on-premises Active Directory domain.

You have an internal web app named WebApp1 that is hosted on-premises. WebApp1 uses Integrated Windows authentication.

Some users work remotely and do NOT have VPN access to the on-premises network.

You need to provide the remote users with single sign-on (SSO) access to WebApp1.

Which two features should you include in the solution? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

Correct selection

Azure AD Enterprise Applications

Conditional Access Policies

Azure Application Gateway

Azure AD Privileged Identity Management (PIM)

Correct selection

Azure AD Application Proxy

Azure Arc

Overall explanation

- **Application Proxy** is a feature of Azure AD that enables users to access on-premises web applications from a remote client. Application Proxy includes both the Application Proxy service which runs in the cloud and the Application Proxy connector which runs on an on-premises server. You can configure a single sign-on to an Application Proxy application.
- **Add an on-premises app to Azure AD:** Now that you've prepared your environment and installed a connector, you're ready to add on-premises applications to Azure AD.

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-add-on-premises-application

Question 18 Skipped

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?

Azure Monitor action groups

Azure Analysis Services

Azure Advisor

Correct answer

Azure Activity Log

Overall explanation

Activity logs are kept for 90 days. You can query for any range of dates, as long as the starting date isn't more than 90 days in the past.

Through activity logs, you can determine:

- what operations were taken on the resources in your subscription
- who started the operation
- when the operation occurred
- the status of the operation
- the values of other properties that might help you research the operation

https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/view-activity-logs

Question 19 Skipped

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 for 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?

In Azure Active Directory (Azure AD) Privileged Identity Management, create a custom role assignment for the Application1 resources.

Correct answer

In Azure Active Directory (Azure AD), create an access review of Application1.

Create an Azure Automation runbook that runs the Get-AzureADUserAppRoleAssignment cmdlet.

Create an Azure Automation runbook that runs the Get-AzRoleAssignment cmdlet.

Overall explanation

An access review is a feature in Azure AD that enables an administrator to review the membership of a group or application role to ensure that only the right people have

continued access. This aligns with the requirement to verify access permissions to Application1. Access reviews can be scheduled to run on a regular basis and can be configured to send email notifications to reviewers. This satisfies the requirement to send a monthly email message to the manager of the developers listing the access permissions to Application1. Access reviews also provide the option to automatically revoke access if the reviewer does not verify access permission, which fulfills the requirement to automatically revoke permissions if the manager does not verify them. Implementing an access review in Azure AD requires minimal development effort and can be set up through the Azure portal with a few simple clicks.

https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-user-access-with-access-reviews

Question 20 Skipped

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?

Configure Azure AD join.

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

Correct answer

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

Configure the Azure AD provisioning service.

Overall explanation

In order to allow users from the fabrikam.com tenant to authenticate to App1, you need to configure the application registration for App1 to support multiple account types, including users from different Azure AD tenants.

By configuring the Supported account types in the application registration, you can specify that both "Accounts in any organizational directory (Any Azure AD directory - Multitenant)" and "Accounts in any organizational directory (Any Azure AD directory - Single tenant)" are supported. This allows users from both contoso.com and fabrikam.com tenants to authenticate to App1.

Additionally, you need to update the sign-in endpoint of App1 to reflect the changes. The sign-in endpoint should be updated to redirect users to the appropriate Azure AD tenant for authentication.

By implementing these recommendations, users from the fabrikam.com tenant will be able to successfully authenticate to App1 and access its functionality.

https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types

Question 21 Skipped

You are designing an application that will be hosted in Azure.

The application will host video files that range from 50 MB to 12 GB. The application will use certificate-based authentication and will be available to users on the Internet.

You need to recommend a storage option for the video files. The solution must provide the fastest read performance and must minimize storage costs.

What should you recommend?

Azure Files

Azure SQL Database

Correct answer

Azure Blob Storage

Azure Data Lake Storage Gen2

Overall explanation

Blob Storage: Stores large amounts of unstructured data, such as text or binary data, that can be accessed from anywhere in the world via HTTP or HTTPS. You can use Blob storage to expose data publicly to the world or to store application data privately. Max file in Blob Storage. 4.77 TB.

https://docs.microsoft.com/en-us/azure/architecture/solution-ideas/articles/digital-media-video

Question 22 Skipped

You are developing a sales application that will contain several Azure cloud services and handle different components of a transaction. Different cloud services will process customer orders, billing, payment, inventory, and shipping.

You need to recommend a solution to enable the cloud services to asynchronously communicate transaction information by using XML messages.

What should you include in the recommendation?

Azure Notification Hubs

Azure Data Lake

Azure Service Fabric

Correct answer

Azure Queue Storage

Overall explanation

Queue Storage delivers asynchronous messaging between application components, whether they are running in the cloud, on the desktop, on an on-premises server, or on a mobile device. The maximum message size supported by Azure Storage Queues is 64KB while Azure Service Bus Queues support messages up to 256 KB. This becomes an important factor especially when the message format is padded (such as XML).

https://docs.microsoft.com/en-us/azure/storage/queues/storage-dotnet-how-to-use-queues

https://blog.kloud.com.au/2016/03/01/cloud-cushioning-using-azure-queues/

Question 23 Skipped

You have a multi-tier app named App1 and an Azure SQL database named SQL1. The backend service of App1 writes data to SQL1. Users use the App1 client to read the data from SQL1.

During periods of high utilization, the users experience delays in retrieving the data.

You need to minimize how long it takes for data requests.

What should you include in the solution?

Azure Data Factory

Correct answer

Azure Cache for Redis

Azure Content Delivery Network (CDN)

Azure Synapse Analytics

Overall explanation

Azure Cache for Redis provides an in-memory data store based on the open-source software Redis. It can be used to cache the most frequently accessed data, thus significantly reducing latency and increasing throughput for the application data requests. By storing data that are accessed often in a cache, you can improve app performance by reducing the load on your main database and making the app more responsive even during high traffic. Azure Content Delivery Network (CDN) is more for delivering static content to users and is not designed for database queries.

https://learn.microsoft.com/en-us/azure/azure-cache-for-redis/cache-overview

Question 24 Skipped

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?

Configure a Conditional Access policy.

Configure Azure AD Identity Protection.

Correct answer

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

Configure Azure AD join.

Overall explanation

To enable users in the fabrikam.com tenant to authenticate to App1, you need to configure the application registration for App1 in Azure AD to support users from both contoso.com and fabrikam.com. This can be done by updating the "Supported account types" in the application registration to allow users from any organizational directory (Any Azure AD directory - Multitenant). Once this is done, you need to update the sign-in endpoint for the application to include the fabrikam.com tenant. This will allow users from the fabrikam.com tenant to authenticate to App1 using their Azure AD credentials.

https://learn.microsoft.com/en-us/security/zero-trust/develop/identity-supported-account-types

Question 25 Skipped

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 on the review screen.

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Network Watcher to run IP flow verify to analyze the network traffic.

Does this meet the goal?

No

Correct answer

Yes

Overall explanation

Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps

administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Question 26 Skipped

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?

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

Configure Azure AD join.

Configure the Azure AD provisioning service.

Correct answer

Use Azure AD entitlement management to govern external users.

Overall explanation

The app is single tenant authentication so users must be present in the Contoso directory.

https://docs.microsoft.com/en-us/azure/active-directory/develop/single-and-multi-tenant-apps

With Azure AD B2B, external users authenticate to their home directory but have a representation in your directory.

https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-external-users

Question 27 Skipped

You have an Azure subscription. The subscription has a blob container that contains multiple blobs.

Ten users in the finance department of your company plan to access the blobs during the month of April.

You need to recommend a solution to enable access to the blobs during the month of April only.

Which security solution should you include in the recommendation?

Conditional Access Policies

Certificates

Access Keys

Correct answer

Shared Access Signatures (SAS)

Overall explanation

Shared Access Signatures (SAS) allow for limited-time fine-grained access control to resources. So you can generate a URL, specify the duration (for the month of April) and disseminate the URL to 10 team members. On May 1, the SAS token is automatically invalidated, denying team members continued access.

https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

Question 28 Skipped

You have an Azure subscription that contains an Azure Blob Storage account named store1.

You have an on-premises file server named Server1 that runs Windows Server 2016. Server1 stores 500 GB of company files.

You need to store a copy of the company files from Server1 in store1.

Which two possible Azure services achieve this goal? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

an Azure Batch account

Correct selection

an Azure Import/Export job

Correct selection

Azure Data Factory

an Azure Analysis services On-premises data gateway

an Azure Logic Apps integration account

Overall explanation

- You can use the Azure Import/Export service to securely export large amounts of data from Azure Blob storage. The service requires you to ship empty drives to the Azure data center. The service exports data from your storage account to the drives and then ships the drives back.
- Big data requires a service that can orchestrate and operationalize processes to refine these enormous stores of raw data into actionable business insights. Azure Data Factory is a managed cloud service that's built for these complex hybrid extract-transform-load (ETL), extract-load-transform (ELT), and data integration projects.

https://docs.microsoft.com/en-us/azure/storage/common/storage-import-export-data-from-blobs

https://docs.microsoft.com/en-us/azure/data-factory/introduction

Question 29 Skipped

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 on the review screen.

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Install and configure the Azure Monitoring agent and the Dependency Agent on all the virtual machines. Use VM insights in Azure Monitor to analyze the network traffic.

Does this meet the goal?

Yes

Correct answer

No

Overall explanation

Use the Azure Monitor agent if you need to:

- Collect guest logs and metrics from any machine in Azure, in other clouds, or on-premises.

Use the Dependency agent if you need to:

- Use the Map feature VM insights or the Service Map solution.

Note: Instead use Azure Network Watcher IP Flow Verify allows you to detect traffic filtering issues at a VM level.

IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen,

IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview

Question 30 Skipped

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?

Change the Membership type of Group1 to Dynamic User.

Correct answer

Create an access review.

Implement Azure AD Identity Protection.

Implement Azure AD Privileged Identity Management (PIM).

Overall explanation

Azure AD access reviews provide an efficient way to evaluate the membership of a group and automatically manage user access based on their responses. By creating an access review for Group1, you can set it to repeat every three months, allowing members to report whether they need to be in the group. Users who report that they don't need to be

in Group1 or don't respond at all will be removed from the group automatically, meeting all the stated requirements.

https://learn.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview

Question 31 Skipped

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?

Application Registration in Azure AD

Shared Access Signatures (SAS)

an Enterprise Application in Azure AD

Correct answer

System-Assigned Managed Identities

Overall explanation

System-assigned managed identities provide a way for Azure Functions to authenticate to other Azure services, such as Activity Logs, without the need for storing or managing secrets. This approach minimizes administrative effort because the identity is tied directly to the Azure Functions service and is automatically managed by Azure. When the Azure

Functions instance is deleted, the associated managed identity will also be removed. This simplifies the authentication process and helps improve the security posture of your app.

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

Question 32 Skipped

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 on the review screen.

Your company deploys several virtual machines on-premises and to Azure. ExpressRoute is deployed and configured for on-premises to Azure connectivity.

Several virtual machines exhibit network connectivity issues.

You need to analyze the network traffic to identify whether packets are being allowed or denied to the virtual machines.

Solution: Use Azure Traffic Analytics in Azure Network Watcher to analyze the network traffic.

Does this meet the goal?

Yes

Correct answer

No

Overall explanation

Instead use Azure Network Watcher IP Flow Verify, which allows you to detect traffic filtering issues at a VM level.

Note: IP flow verify checks if a packet is allowed or denied to or from a virtual machine. The information consists of direction, protocol, local IP, remote IP, local port, and remote

port. If the packet is denied by a security group, the name of the rule that denied the packet is returned. While any source or destination IP can be chosen, IP flow verify helps administrators quickly diagnose connectivity issues from or to the internet and from or to the on-premises environment.

https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-ip-flow-verify-overview

Question 33 Skipped

You are designing a SQL database solution. The solution will include 20 databases that will be 20 GB each and have varying usage patterns.

You need to recommend a database platform to host the databases. The solution must meet the following requirements:

- The solution must meet a Service Level Agreement (SLA) of 99.99% uptime.
- The compute resources allocated to the databases must scale dynamically.
- The solution must have reserved capacity.
- Compute charges must be minimized.

What should you include in the recommendation?

Correct answer

an elastic pool that contains 20 Azure SQL databases

20 databases on a Microsoft SQL server that runs on an Azure virtual machine

20 databases on a Microsoft SQL server that runs on an Azure virtual machine in an availability set

20 instances of Azure SQL Database serverless

Overall explanation

The compute and storage redundancy is built in for business-critical databases and elastic pools, with an SLA of 99.99%. Reserved capacity provides you with the flexibility to temporarily move your hot databases in and out of elastic pools (within the same region and performance tier) as part of your normal operations without losing the reserved capacity benefit.

https://azure.microsoft.com/en-us/blog/understanding-and-leveraging-azure-sql-database-sla/

Question 34 Skipped

You have an application that is used by 6,000 users to validate their vacation requests. The application manages its own credential store.

Users must enter a username and password to access the application. The application does NOT support identity providers.

You plan to upgrade the application to use single sign-on (SSO) authentication by using an Azure Active Directory (Azure AD) application registration.

Which SSO method should you use?

OpenID Connect

SAML

header-based

Correct answer

password-based

Overall explanation

Password - On-premises applications can use a password-based method for SSO. This choice works when applications are configured for Application Proxy.

With password-based SSO, users sign in to the application with a username and password the first time they access it. After the first sign-on, Azure AD provides the username and password to the application. Password-based SSO enables secure application password storage and replay using a web browser extension or mobile app. This option uses the existing sign-in process provided by the application, enables an administrator to manage the passwords, and doesn't require the user to know the password.

https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-single-sign-on

Question 35 Skipped

You have the resources shown in the following table:

Name	Type
AS1	Azure Synapse Analytics instance
CDB1	Azure Cosmos DB SQL API account

CDB1 hosts a container that stores continuously updated operational data.

You are designing a solution that will use AS1 to analyze the operational data daily.

You need to recommend a solution to analyze the data without affecting the performance of the operational data store.

What should you include in the recommendation?

Azure Cosmos DB change feed

Azure Synapse Analytics with PolyBase data loading

Azure Data Factory with Azure Cosmos DB and Azure Synapse Analytics connectors

Correct answer

Azure Synapse Link for Azure Cosmos DB

Overall explanation

Azure Synapse Link for Azure Cosmos DB creates a tight integration between Azure Cosmos DB and Azure Synapse Analytics. It enables customers to run near real-time analytics over their operational data with full performance isolation from their transactional workloads and without an ETL pipeline.

https://docs.microsoft.com/en-us/azure/cosmos-db/synapse-link-frequently-asked-questions

Back to result overview

Scroll back to top