MS-600 Correct Answers

Wednesday, August 5, 2020   3:43 PM

1. Which of the following is NOT a main component of an Actionable Messages in Outlook solution?

- ○ A web API that is called when the user activates actions
- ◉ An application installed on the recipient's device
- ○ An application or service that sends HTML-formatted email with Adaptive Card markup

2. Which of the following action types can be auto-invoked when the user opens the message, allowing the card to update with fresh data?

- ◉ Action.Http
- ○ Action.InvokeAddInCommand
- ○ Action.OpenUrl

3. What method does a web API use to ensure that a request is valid?

- ○ Verifying the calling server's IP address with a list of accepted IP addresses
- ◉ Validating the bearer token
- ○ Including a secret value in the body of the HTTP POST

1. Suppose you have a system that contains sales contacts, and your sales team regularly needs to search for contacts, share them with the team, and have a conversation about them. What Microsoft Teams extensibility point would be most suited to facilitate this process?

- ○ A conversational bot in a channel.
- ◉ A messaging extension with a search command.
- ○ A personal app with a tab.

2. Which of the following is NOT part of your Microsoft Teams app package?

- ○ Your app icons.
- ◉ HTML formatted app description.
- ○ Your app manifest file.

3. If your app is for a particular company, which distribution model should you choose?

- ○ Publish your app to the public app store.
- ○ Distribute your app package for users to install directly.
- ◉ Publish to the organizational app catalog.

1. The SharePoint Framework is available in which of the following SharePoint environments?

- ○ SharePoint Server 2016
- ○ SharePoint Server 2019
- ○ SharePoint Online
- ◉ All of these environments

2. Which of the following statements isn't correct about the SharePoint Framework?

- ○ SharePoint Framework packages can be deployed to the tenant or site collection scoped app catalog to control where apps can be installed and used.
- ◉ Because SharePoint Framework components are entirely client-side components, it's impossible to limit the permissions granted to any particular component.
- ○ Users can add multiple web parts to pages, or they can be configured by the developer to be the only component on a page using the site part app page capability.

3. SharePoint Framework includes APIs that can be used to call all of the following resources, except which one?

- ○ Anonymous/unsecured HTTP REST endpoints
- ○ Microsoft Graph
- ○ Microsoft hosted endpoints secured with Azure AD
- ○ Any endpoint secured with Azure AD
- ◉ All of these are supported endpoints that developers can call from the included SharePoint Framework API.

1. Which of the following statements is true about Office add-ins?

    ○ Add-ins can run only in Office on Windows, Mac, and iPad/iOS.

    ◉ Office 365 administrators can use centralized deployment to deploy add-ins across their organization.

    ○ A developer publishes their add-in to AppSource to hide it from the general public.

2. The user needs to sign in to access add-in functionality within an Office application. Which Office add-in platform feature should the developer display to facilitate the sign-in process?

    ○ add-in command

    ○ custom function

    ◉ dialog

3. What file defines the settings and capabilities of an Office add-in?

    ○ dialog file

    ◉ manifest file

    ○ web.config file

1. Which of the following statements is true about Office JavaScript APIs?

- ○ Requirement sets can only be specific to Office hosts.

- ○ `https://appsforoffice.microsoft.com/lib/beta/hosted/office.js` is the link to the production APIs on the Office JavaScript CDN.

- ⦿ The properties of a proxy object must first be loaded with data from the Office file.

2. A developer wants to use an add-in to visualize data in Excel. What would be a good object to use?

- ⦿ Chart

- ○ Range

- ○ Value

3. An Outlook add-in is configured to appear in the Outlook navigation bar, that is, alongside mail and calendar. What kind of add-in is it?

- ○ Content

- ⦿ Module

- ○ Task pane

4. What is a good tool for trying out the Word APIs without creating an add-in?

- ⦿ Script Lab

- ○ Visual Studio

- ○ Yeoman generator

5. A developer is setting up an add-in with a custom function and a task pane. How should data be shared between them?

- ○ Dialog API

- ○ Document Object Model (DOM)

- ⦿ Storage API

1. An Outlook add-in needs to store data. What's an Office JavaScript object the add-in developer might use?

- ⦿ CustomProperties
- ○ CustomXmlParts
- ○ Settings

2. Joe has decided to use Office UI Fabric in an add-in. What is an advantage of doing so?

- ○ Fabric has three (3) main areas.
- ○ Fabric Core is built on Fabric React.
- ⦿ Fabric reflects Office branding.

3. Joe's connecting to Microsoft Graph in an add-in. Where should the add-in display the Azure Active Directory (AAD) sign-in form for a user in Office on the web?

- ○ Custom function
- ⦿ Dialog
- ○ Task pane

1. A developer is about to test and debug their new add-in. What's the best deployment option?

- ○ AppSource
- ○ Exchange server
- ⦿ Sideloading

2. To debug a custom function, a developer should use which tool?

- ○ Visual Studio
- ⦿ Visual Studio Code
- ○ Yeoman generator for Office add-ins

3. A developer would like to publish their add-in on AppSource. What are the three (3) key areas they should validate?

- ⦿ Browsers, Office applications, Operating systems
- ○ Browsers, Office applications, Organizations
- ○ Monitor resolutions, Office applications, Operating systems

1. Which query parameter is used to limit the results returned to a specified number?

- ◯ $limit
- ◉ $top
- ◯ $select

2. Which of the following query parameter combinations would return only the email address of users with the last name 'Smith'?

- ◯ ?$filter=equals(surname,'Smith')&$only=Mail
- ◉ ?$filter=surname eq 'Smith'&$select=Mail
- ◯ ?$filter=(surname = 'Smith')&$select=Mail

1. Which of the following query parameters is used to include related content?

- ◯ ?$include
- ◯ ?$join
- ◉ ?$expand

2. Which of the following query parameter combinations would search for all users that have the string 'wilk' in their name?

- ◯ ?$find("wilk*")
- ◯ ?$find="wilk*"
- ◯ ?$search("wilk*")
- ◉ ?$search="wilk*"

1. Which of the following statements is true about the batch request support in Microsoft Graph?

- ● Batching reduces the number of round trips an application makes to Microsoft Graph by submitting multiple requests in one HTTP round trip.
- ○ Batching enables applications to implement transactions so if one request fails, all others will fail and be rolled back.
- ○ Microsoft Graph prioritizes requests submitted as a batch to reward applications that submit fewer HTTP requests.

2. How can multiple requests be executed in order within a batch request?

- ○ The order requests are specified in the batch object is the order Microsoft Graph will execute them.
- ○ Requests can be nested in the batch object submitted to Microsoft Graph to define a dependency hierarchy.
- ● Each request must include an ID property. Other requests use a DependsOn array to define the requests it depends on.

1. What does it mean when a request is throttled by Microsoft Graph?

- ○ An application has issued more than the allowed request quota for the tenant and needs to wait for the quota to reset.
- ○ Microsoft Graph is in an unhealthy state and the requester should try their request again later.
- ● Microsoft Graph has determined the number of requests submitted by an app is excessive and could impact the service's overall health. Throttling is how Microsoft Graph tells the requester to reduce the number of requests to an acceptable level over a period of time.

2. Which of the following statements about the HTTP header Retry-After is not true?

- ● The Retry-After header value instructs the requestor the date and time when to resubmit their request.
- ○ The Retry-After HTTP header instructs the requester to not resubmit the request before the specified number of seconds has elapsed.
- ○ The Retry-After header my or may not be included in every throttling response from Microsoft Graph.

3. What will happen if an application resubmits a request prior to the specified Reply-After HTTP header value?

- ● Microsoft Graph will continue to throttle the request and provide a new Request-After header value.
- ○ Microsoft Graph will disable the requesting application and an administrator will need to manually reactivate it.
- ○ Microsoft Graph will process the request and respond with the results because the Retry-After HTTP header value is only a suggestion.

1. How does the Microsoft Graph SDK address throttled responses?

- ○ Applications that use the Microsoft Graph SDK are not subjected to throttling, only applications that use the Microsoft Graph API.

- ◉ The Microsoft Graph SDK internally handles the delay and resubmission of a request when it receives a throttling response.

- ○ The Microsoft Graph SDK does not do anything to address throttled responses. Applications that use the Microsoft Graph SDK must handle throttled responses the same way when using the Microsoft Graph API.

2. Applications can avoid from being throttled in various ways except for which of the following?

- ○ An application can minimize the number of complex requests over a short period of time to Microsoft Graph.

- ○ An application can minimize the number of requests to Microsoft Graph using batching, delta query and change notifications.

- ◉ An application author can purchase an enterprise agreement from Microsoft Graph to avoid being throttled.

3. Applications can request only new and updated resources from Microsoft Graph which of the following ways?

- ◉ Submit an initial request and include the delta function. Use the returned `deltaLink` property when submitting the next request to Microsoft Graph to receive only the entities that have been created or changed since the initial request.

- ○ When submitting a request to Microsoft Graph, include the desired date and time to the delta function to receive all entities that have been added or changed since that time.

- ○ When submitting a request to Microsoft Graph, include the desired date and time to the `changedSince` function to receive all entities that have been added or changed since that time.

1. Which of the following Microsoft Graph endpoints won't return the currently signed-in user?

- ○ Issue an HTTP GET request to https://graph.microsoft.com/v1.0/me

- ○ Issue an HTTP GET request to https://graph.microsoft.com/v1.0/users/{user-id}

- ◉ Issue an HTTP GET request to https://graph.microsoft.com/v1.0/users/me

- ○ Issue an HTTP GET request to https://graph.microsoft.com/v1.0/users/{user-upn}

2. Which of the following permissions can be granted by a user and don't require an administrator?

- ○ Directory.Read.All

- ○ User.ReadWrite.All

- ◉ User.ReadWrite

1. When requested using Microsoft Graph, profile photos are returned in what data format?

- ○ Link to file attachment
- ⦿ Binary
- ○ Base-64

2. Microsoft Graph can retrieve and set the profile photo on which of the following resources?

- ⦿ Users, groups, and contacts (in Office 365)
- ○ Users
- ○ Users and groups

1. When creating a new user with Microsoft Graph, which of the following properties are required?

- ⦿ accountEnabled, mailNickname, displayName, and passwordProfile, userPrincipalName
- ○ accountEnabled, mailNickname, givenName, surname, and passwordProfile
- ○ givenName, surname, passwordProfile, userPrincipalName

2. How do you specify which user to update or delete with Microsoft Graph?

- ○ Specify the userPrincipalName in the JSON string included in the body of the request and submit it to the /users endpoint.
- ○ Specify the user ID in the JSON string included in the body of the request and submit it to the /users endpoint.
- ⦿ Specify the user in the target endpoint, using the user's ID or userPrincipalName.

1. Which of the following groups can you create and manage using Microsoft Graph?

- ⦿ Office 365 groups and security groups
- ○ Office 365 groups and mail-enabled security groups
- ○ Distribution groups and security groups

2. Which of the following statements isn't true as it relates to Microsoft Graph, groups and permissions?

- ○ Both administrators and users can consent to group-related operations.
- ○ Both administrators and users can consent to group-related operations, but only administrators can consent to writeable operations.
- ⦿ All group-related operations in Microsoft graph require administrator consent.

1. What type of resources are returned from a request to the Microsoft Graph `/groups` endpoint?

- ○ Office 365 groups
- ○ Security groups
- ◉ Directory objects and objects based on it, including Office 365 groups and security groups

2. What is the difference between direct and transient group membership?

- ◉ Direct membership means a user has been added to the group while transient membership means a user is a member though dynamic membership or as a member of another security group that has been added to the group.
- ○ Direct membership means a user has been permanently granted access to the group while transient membership means a user has only temporary membership.
- ○ Users can have either direct or transient membership to both Office 365 groups and security groups.

1. When creating a new group with Microsoft Graph, which of the following properties are required?

- ◉ displayName, mailEnabled, mailNickname, securityEnabled
- ○ displayName, mailEnabled, mailNickname, groupTypes
- ○ displayName, owners, members, securityEnabled

2. How do you specify which group to update or delete with Microsoft Graph?

- ○ Specify the group's ID in the JSON string included in the body of the request and submit it to the /groups endpoint.
- ○ Get a reference to the group, update it's properties, and submit it as an HTTP POST to the `/groups` endpoint.
- ◉ Specify the group in the target endpoint, using the group's ID.

1. Developers can access files with Microsoft Graph from which of the following entity types?

- ○ Only files stored in an Office 365 group
- ○ Only an individual user's files in OneDrive for Business.
- ○ Only files from a SharePoint Online site.
- ⊙ Files from all of these entity types (users, groups, and SharePoint sites) are accessible with Microsoft Graph.

2. What is returned when submitting a request to the Microsoft Graph endpoint `/me/drive/root` ?

- ⊙ Information about currently signed-in user's root OneDrive folder, such as the location of the folder and quota information.
- ○ All the files of the currently signed-in user's root OneDrive folder, but not the subfolders.
- ○ All the files and folders of the currently signed-in user's root OneDrive folder.

1. Simple file uploads differ from large file uploads differ in all except which of the following ways?

- ○ Large file uploads allow you to upload multiple chunks of a file in a resumable session, while simple file uploads involve a single request.
- ⊙ Developers can upload files of any size using either option, but can get additional progress reporting when using the large file upload option.
- ○ Large file uploads are resumable in the case of an interrupted connection while simple file uploads aren't resumable.

2. Developers can upload files of any size using either the simple upload or large file upload approach.

- ⊙ False - simple file uploads are limited to files smaller than 4 MB.
- ○ True - file size is not a factor in the two options, rather resumable uploads and progress reporting are additional capabilities for large file uploads.

1. The Microsoft Graph insights endpoint includes all except which of the following insights?

- ○ Files the user has accessed or modified.
- ◉ Files the user is likely to be interested in.
- ○ Files that have been shared with the user.
- ○ Files trending around the user.

2. The results returned by Microsoft Graph insights endpoint include which of the following properties?

- ○ The `Id` of the insight response record.
- ○ A `resourceVisualization` object that contains details on the file returned and used in experiences such as Delve.
- ○ A `resourceRefrence` object that contains properties such as the Id and URL of the file returned.
- ◉ All of these properties are returned for all insights endpoints. Some endpoints may also return additional details.

1. Microsoft Graph supports access tokens generated on behalf of users that are signed in using which types of accounts?

- ○ Only Microsoft accounts (consumer logins, LiveID, Outlook.com).
- ○ Only Work and School (Azure AD) accounts.
- ◉ Both Microsoft accounts and work and school (Azure AD) accounts.

2. What benefits does Microsoft Graph have over using individual service endpoints?

- ○ Microsoft Graph's single endpoint simplifies apps as developers don't have to submit requests to individual service endpoints.
- ○ Microsoft Graph has a single well-known endpoint while individual service endpoints may differ from user to user, tenant to tenant, or consumer to business services (such as OneDrive).
- ◉ All of these are benefits to using Microsoft Graph over using individual service endpoints.

1. What elements are required to create, configure and/or collect when registering an Azure AD app for use with the OAuth 2.0 authorization code grant flow?

- ⊙ Tenant ID, application ID, application secret, and the redirect URI
- ○ Application ID, application secret, and the redirect URI.
- ○ Tenant ID, application ID, and the application secret.

2. What is the difference between static and dynamic consent?

- ⊙ Static consent is when the permissions are defined ahead of time in the app registration, while dynamic consent defines the permissions as they are needed by the app.
- ○ Dynamic consent is when the permissions can change over time with an app, while static consent permissions never change.
- ○ Static consent refers to the permissions all users have, while dynamic permissions only apply to some users.

1. Which object in the MSAL SDK best best suited to obtain an access token from Microsoft identity for ASP.NET applications with interactive users?

- ○ The `PublicClientApplication` is preferred object to use for web applications.
- ⊙ The `ConfidentialClientApplication` is the ideal client in this scenario.
- ○ The `WebClientApplication` is preferred object to use for web applications.

2. What object included in the Microsoft Graph SDK is used to submit requests to Microsoft Graph?

- ⊙ The `GraphServiceClient` is the object used to submit requests to Microsoft Graph when using the Microsoft Graph .NET SDK.
- ○ The `MicrosoftGraphClient` is the object used to submit requests to Microsoft Graph when using the Microsoft Graph .NET SDK.
- ○ The `MSGraphClient` is the object used to submit requests to Microsoft Graph when using the Microsoft Graph .NET SDK.

1. What information is included in the payload of Microsoft Graph change notifications?

   ⦿ Just that an entity has been created, updated, or deleted.

   ○ The specific property, including the before and after value, of the change to an entity.

   ○ Only entities that have changed, not new or deleted entities.

2. What types of entities support change notifications in Microsoft Graph?

   ○ Email messages, events, contacts, users, groups, devices enrolled in Intune, conversations, and OneDrive files.

   ⦿ Email messages, events, contacts, users, groups, conversations, and OneDrive files.

   ○ All entities exposed by Microsoft Graph support change notifications.

1. How long are change notification subscriptions valid?

   ⦿ It depends on the entity the subscription is for and not an indefinite period.

   ○ Three days

   ○ Three hours

2. What is the purpose of the `clientSecret` property when creating a new change notification subscription?

   ○ It must be the client secret associated with the registered Azure AD app used by your custom app.

   ⦿ Your app can check the value of this property for all notification requests received from Microsoft Graph to ensure it was triggered by your app's subscription.

   ○ It must be the x509 certificate associated with the registered Azure AD app used by your custom app.

1. Microsoft Graph's track changes (delta query) capability does which of the following things?

   ⦿ Returns only those entities that have been created, updated, or deleted since the previous time the query was executed.

   ○ Returns a list of the properties, with the before and after values, for the entity specified in the query that changed.

   ○ Returns a list of the users and apps who have changed the entity specified in the query.

2. What types of entities support track changes (delta query) in Microsoft Graph?

   ⦿ Email messages, groups, users, and events.

   ○ Email messages, groups, users, and files in OneDrive.

   ○ Email messages, groups, users, and contacts.

1. Which of the following statements about ID tokens is correct?

- ◉ ID tokens contain basic identity information about the currently logged in user.
- ○ ID tokens can be submitted in an authentication request to prove the identity of the user.
- ○ ID tokens include both identity information and the permissions a user has been granted to an application.

2. Which of the following statements about access tokens is incorrect?

- ○ Access tokens can be created by Azure AD either for a user or for an application.
- ○ Azure AD supports multiple OAuth 2.0 flows that developers can use to obtain an access token.
- ◉ Access tokens are submitted by the application to the identity provider to request permissions to a resource on behalf of a user.

1. What is the primary difference between single tenant apps and multi-tenant apps?

- ○ Single tenant apps reserve the name of the app across all Azure AD directories, while the name of multi-tenant apps can be used in multiple Azure AD directories.
- ○ Single tenant apps can only be used in one tenant while multi-tenant apps can be copied into multiple Azure AD directories.
- ◉ Single tenant apps allow only users from the app's directory to sign in, while multi-tenant apps support users multiple tenants to sign in and use the app.

2. What is the key difference between an application and a service principal?

- ◉ Application objects exist in the directory where the application is created, where service principal objects exist in each Azure AD tenant where the application is used.
- ○ Application objects are templates that exist in every directory where an application is used. They're used to create service principals that can be customized in each directory.
- ○ Service principals exist in the directory where the application is created, where application objects exist in each Azure AD tenant where the application is used.

1. Microsoft Identity supports multiple topology options. Which of the following options does not support using Microsoft Accounts for user sign-in?

- ○ Consumer
- ◉ Azure AD Business to Business (B2B)
- ○ Azure AD Business to Customer (B2C)

2. How do Azure AD B2B and B2C differ?

- ○ Azure AD B2B refers to users who are already paid customers while B2C refers to leads, or potential customers who haven't yet purchased a product.
- ○ Azure AD B2B refers to the collaboration of users in two organizations who have entered into formal partnership while B2C is more of a loose partnership between organizations.
- ◉ Azure AD B2B refers to users sharing or collaborating between two organizations, while B2C is more about businesses implementing an application for their customers.

1. Which of the following options isn't a characteristic that makes SPAs stand out from web apps?

- ○ Security characteristics of these apps are different from traditional server-based web applications
- ◉ JavaScript-based client-side solutions don't have the ability to process the authorization code used in other OAuth 2.0 flows
- ○ Full-page browser redirects away from the app become invasive to the user experience
- ○ Many authorization servers and identity providers don't support CORS requests

2. Why is an application secret not required when authenticating with Azure AD in a SPA?

- ○ Instead of using an app secret, the SPA can use a x509 certificate. One of the two options is required.
- ○ They aren't needed because the user's password acts as the Azure AD app's secret.
- ◉ Secrets can't be reliably secured in a SPA because its inherently a client-side application. In no scenario can the secret reach the user's browser and be secured.

1. Which of the following unique characteristics of the authorization code grant flow makes it a preferred option for securing web apps?

- ⦿ The web app never has access to the user's credentials because the user signs in with Azure AD, not with the app.
- ○ All communication between the web app and Azure AD is secured.
- ○ The web app authenticates with Azure AD using a x509 certificate when obtaining an access token.

2. What elements are required to create, configure and/or collect when registering an Azure AD app for use with the OAuth 2.0 authorization code grant flow?

- ⦿ Tenant ID, application ID, application secret, and the redirect URI
- ○ Application ID, application secret, and the redirect URI.
- ○ Tenant ID, application ID, and the application secret.

1. Which of the following ways isn't a valid authentication option for an app using the OAuth 2.0 client credentials flow?

- ○ Include the client ID and certificate assigned to the app within the Azure AD management portal.
- ⦿ Include the client ID as well as a user account's credentials that acts as a service account.
- ○ Include the client ID and client password assigned to the app within the Azure AD management portal.

2. What minimal scope(s) must a daemon or service app include in the access token request to Azure AD?

- ⦿ A single scope of the resource followed by `.default`, such as https://graph.microsoft.com /.default`.
- ○ Every scope added from within the Azure AD admin center for the registered app.
- ○ Nothing - because the permissions were statically specified on the app in the Azure AD admin center, daemon apps don't need to include specific permissions the access token request.

1. Which of the following statements is correct about consent?

   ○ Only users can grant consent for an app to act on their behalf; no one can grant consent for another user.

   ◉ Users can grant permission consent to an app that requests it as long as the user has the permission.

   ○ Users can grant permission consent to an app that requests it regardless if the user has or doesn't have the permission.

2. Which of the following options isn't a good practice to adopt when it comes to permissions.

   ○ Only ask for the permissions required for implemented app functionality.

   ○ When requesting permissions for app functionality, you should request the lease-privileged access.

   ◉ When registering apps with Azure AD, it's a good idea to always use the admin consent option so users aren't bothered with permission consent requests.

   ○ Apps should gracefully handle scenarios where the user doesn't grant consent to the app when permissions are requested.

1. What is the difference between static and dynamic consent?

   ◉ Static consent is when the permissions are defined ahead of time in the app registration, while dynamic consent defines the permissions as they are needed by the app.

   ○ Dynamic consent is when the permissions can change over time with an app, while static consent permissions never change.

   ○ Static consent refers to the permissions all users have, while dynamic permissions only apply to some users.

2. What role does the /.default scope serve?

   ○ The /.default scope represents the basic permissions all apps need.

   ◉ A request for the /.default scope is equivalent to requesting all static permissions defined in the app registration.

1. Application permissions differ from delegated permissions in all except which of the following ways?

- ○ Application permissions are for when there's no user interaction while delegated permissions involve interaction of a signed-in user.

- ◉ Application permissions are granted by a user to the application to act on their behalf while delegated permissions are granted by an application to a user.

- ○ Application permissions are higher-privileged permissions than delegated permissions.

2. To grant application permissions, which of the following statements isn't a valid option?

- ◉ Send a user to the application consent endpoint with the proper parameters on the query string.

- ○ Send a user to the admin consent endpoint with the proper parameters on the query string.

- ○ Select the 'Grant admin consent' button within the Azure AD admin center that will display an admin consent.

1. Developers can use Microsoft identity to secure which types of apps?

- ○ Web applications
- ○ Desktop and mobile applications
- ○ Web APIs
- ◉ All of these applications can be secured with Microsoft identity

2. What types of authentication flows can developers use when securing a web API with Microsoft identity?

- ○ Only the on behalf of flow is supported by Microsoft identity with web APIs.

- ○ Only applications that access the web API as themselves, not as a user.

- ◉ Both applications that access the web API without a user and the on behalf of flow are supported.

1. Which of the following best explains the on-behalf-of flow?

- ◉ Using its credentials and the currently signed in user's access token, an API obtains a new access token to call a secured API.

- ○ Using the credentials of the currently signed in user and the app's credentials, an app obtains a new access token to call a secured API.

- ○ An app uses the currently signed in user's access token to call a secured API.

2. Which is the correct way to reference custom scopes (*such as Product.Read*) when including them in an access token request?

- ◉ `api://[web-api-client-id]/Product.Read`

- ○ `Product.Read`

- ○ `api://Product.Read`

1. Apps that implement the OAuth 2.0 client credentials grant flow submit which of the following things to authenticate and obtain an access token?

- ◉ Client ID and a secret or a certificate.

- ○ Client ID and an access token.

- ○ Client ID, a secret or certificate, and a user-provided access token.

2. How are permissions granted to daemon apps?

- ○ The first time a daemon app runs, it will prompt a user to log in and grant the requested permissions using a code returned by Microsoft identity.

- ○ Permissions are automatically granted to registered apps in the Azure AD admin center when the permissions are selected.

- ◉ An admin user grants permissions using the admin consent framework.

1. How can you restrict your app to only allow specific users to sign in and use it with Microsoft identity?

⦿ Enable the **User assignment required** setting on the app in the Azure AD admin center and assign specific users to the app.

○ Disable the **Allow all users to sign in** setting on the app in the Azure AD admin center and assign specific users to the app.

○ Remove the **Everyone** group from the list of users allowed to sign in to the Azure AD app and assign specific users to the app.

2. What elements are required to create, configure or collect when registering an Azure AD app for use with an ASP.NET Core web app?

⦿ Tenant ID, application ID, application secret, and the redirect URI

○ Application ID, application secret, and the redirect URI.

○ Tenant ID, application ID, and the application secret.

1. How can users be added to security groups?

○ Users can be manually added to a group using the Azure AD admin center by group owners.

○ Users can search and apply to join groups; group owners can review and approve requests to join the group.

○ Users can search and join groups automatically if the groups are configured correctly.

⦿ All of these options are valid ways to add users to groups.

2. To support security groups in a custom ASP.NET app that uses MSAL and the OpenID Connect middleware, you must do which of the following things?

○ Set the OpenID Connect middleware `RoleClaimType` property to `groups`.

○ Set the `RoleClaimType` on the OpenID Connect middleware to `securityGroups`.

⦿ Set the app's manifest property `groupMembershipClaims` to `SecurityGroup` and the OpenID Connect middleware `RoleClaimType` property to `groups`.

1. Which of the following statements best describes RBAC?

- ◉ Role-Based Access Control is when users are assigned to roles instead of being directly assigned access or permissions in an app.

- ○ Request-Based Access Control is when a user requests access to a group and a group owner approves the request.

2. To support application roles in a custom ASP.NET app that uses MSAL and the OpenID Connect middleware, you must do which of the following?

- ○ Enable the default claim mapping on the OpenID Connect middleware and set the `RoleClaimType` to `roles`.

- ○ Disable the default claim mapping on the OpenID Connect middleware and set the `RoleClaimType` to `approles`.

- ◉ Disable the default claim mapping on the OpenID Connect middleware and set the `RoleClaimType` to `roles`.