Okta

Okta Certified Consultant

Okta Certified Consultant (Part I) - 2024

Question: 950

While configuring the SAML settings for an application in Okta, which of the following must be included to ensure that the application can handle SAML logout requests?

A. Logout URL
B. Assertion Consumer Service URL
C. User Role Attribute
D. Audience URI

Answer: A

Explanation: The Logout URL must be configured to ensure that the application can process SAML logout requests properly, allowing users to be logged out effectively.

Question: 951

In the context of Active Directory (AD) integration with Okta, what is the primary role of the Okta Active Directory Agent?

A. To provide a web-based interface for user management.
B. To synchronize user identities and attributes between Okta and Active Directory.
C. To enforce password policies directly within Active Directory.
D. To manage multi-factor authentication settings for AD users.

Answer: B

Explanation: The Okta Active Directory Agent is responsible for synchronizing user identities and attributes between Okta and Active Directory, facilitating seamless identity management across both platforms.

Question: 952

In an Okta API request, which parameter is essential for identifying the specific user whose information is being requested or manipulated, especially when performing user management actions?

A. 'user_id'
B. 'principal'
C. 'id_token'
D. 'sub'
E. 'uid'

Answer: A,D

Explanation: The 'user_id' and 'sub' parameters uniquely identify a user within Okta’s system, enabling precise operations on user data or authentication processes.

Question: 953

In the context of Okta’s entitlement architecture, what role do scopes play in the context of access management for APIs?

A. Scopes are used to define roles within the organization.
B. Scopes specify the level of access requested by the application to various resources.
C. Scopes are irrelevant in the context of API access management.
D. Scopes only apply to user authentication and not API access.

Answer: B

Explanation: Scopes specify the level of access requested by the application to various resources, thus playing a crucial role in API access management.

Question: 954

To expose application groups in the LDAP interface directory information tree, which approach must be taken to ensure that these groups are visible and usable by applications relying on LDAP?

A. Manually creating an LDAP group for each application in the directory.
B. Configuring group mappings in the Okta Admin Dashboard to reflect application roles.
C. Automatically synchronizing all application groups to LDAP.
D. Limiting the visibility of groups to only those assigned to administrators.

Answer: B

Explanation: Configuring group mappings in the Okta Admin Dashboard allows application groups to be reflected in the directory information tree, making them visible and usable.

Question: 955

In the event of a failure during inbound federation, which logging feature in Okta can assist in diagnosing the problem?

A. Event Hooks
B. System Log
C. API Access Management
D. User Audit Logs

Answer: B

Explanation: The System Log in Okta provides detailed information about authentication events and errors, helping diagnose issues with inbound federation.

Question: 956

In the Access Gateway configuration, what is the primary purpose of the "Logout Redirect URL"?

A. To specify where users are taken after logging out of Okta
B. To enforce session termination on all connected applications
C. To redirect users to a custom application page upon logout
D. To manage the logging of logout events

Answer: C

Explanation: The "Logout Redirect URL" allows administrators to redirect users to a custom application page upon logout, enhancing user experience and branding.

Question: 957

When configuring an Okta application, which of the following is a requirement for implementing the OAuth 2.0 authorization code flow securely?

A. The application must use HTTP instead of HTTPS for communication
B. The application must validate the redirect_uri against the registered URI
C. The application must store access tokens in local storage
D. The application must always request the 'offline_access' scope

Answer: B

Explanation: It is essential for the application to validate the 'redirect_uri' against the registered URI to prevent open redirect vulnerabilities and ensure that the authorization response is sent to a trusted endpoint.

Question: 958

Which of the following is a key consideration when implementing agentless Desktop Single Sign-On in a multi-domain Active Directory environment?

A. Users must be in the same domain as the applications they access.
B. The Okta service must have visibility into all domains to authenticate users.
C. Each domain must be configured with its own Okta instance.
D. Multi-factor authentication must be disabled for all users.

Answer: B

Explanation: In a multi-domain Active Directory environment, the Okta service must have visibility into all domains to successfully authenticate users, ensuring a unified SSO experience.

Question: 959

When evaluating the pros and cons of the "Cloud" deployment model for Okta, which of the following is a notable advantage?

A. It requires extensive hardware management by the organization.
B. It offers immediate scalability and reduced time to deployment.
C. It limits integration capabilities with on-premises applications.
D. It necessitates a higher level of security expertise from internal IT teams.

Answer: B

Explanation: The Cloud deployment model offers immediate scalability and reduced time to deployment, allowing organizations to quickly adapt to changing needs without the burden of hardware management.

Question: 960

Which of the following potential pitfalls should be avoided when setting up the LDAP interface to ensure effective user authentication and authorization?

A. Overcomplicating the LDAP schema with too many custom attributes.
B. Regularly updating the Okta AD Agent to the latest version.
C. Testing the configuration in a staging environment before going live.
D. Documenting the LDAP configuration settings and group mappings.

Answer: A

Explanation: Overcomplicating the LDAP schema can lead to maintenance challenges and potential issues in user authentication and authorization processes.

Question: 961

In an OAuth 2.0 implementation, which statement accurately characterizes the authorization code grant type and its typical use case?

A. It is suitable for server-side applications where the client secret can be kept confidential.
B. It is primarily used for native mobile applications that cannot maintain a client secret.
C. It allows for the direct exchange of user credentials for access tokens.
D. It is designed for public clients that operate entirely in a user's browser.

Answer: A

Explanation: The authorization code grant type is ideal for server-side applications, as it allows for a secure exchange of an authorization code for an access token, keeping the client secret confidential.

Question: 962

When implementing an Org2Org SAML integration, how can one ensure that users maintain their roles across both organizations effectively?

A. Use the same user ID in both organizations.
B. Implement role mapping based on SAML assertions.
C. Manually assign roles after user login.
D. Ensure that both organizations use the same authentication method.

Answer: B

Explanation: Implementing role mapping based on SAML assertions allows users to maintain their roles across both organizations effectively, streamlining access management.

Question: 963

In the context of Okta's Global Session Policies, which of the following actions is generally considered best practice when configuring behavioral detection?

A. Setting a universal threshold for all users based on average behavior.
B. Customizing detection parameters for different user roles based on their typical access patterns.
C. Disabling behavioral detection for all users to simplify access management.
D. Implementing behavioral detection without any user communication to avoid confusion.

Answer: B

Explanation: Customizing detection parameters for different user roles based on their typical access patterns allows for more effective security measures tailored to specific user behaviors.

Question: 964

In the context of Active Directory integration with Okta, which specific configuration must be performed to ensure that user accounts are created in Okta according to the settings defined in the Active Directory import process?

A. Enabling the "Automatically create users" setting
B. Setting up a scheduled task for manual imports
C. Configuring LDAP filters to limit user imports
D. Defining custom user roles in Okta

Answer: A

Explanation: Enabling the "Automatically create users" setting ensures that new accounts in Active Directory are automatically created in Okta, simplifying user management.

Question: 965

During the IdP-initiated SSO process, which piece of information is essential for the SP to validate the SAML response?

A. The user's email address
B. The SAML assertion's signature
C. The session ID from the IdP
D. The user's group membership

Answer: B

Explanation: The SAML assertion's signature is critical for the SP to validate the authenticity and integrity of the SAML response received from the IdP.

Question: 966

When creating an authentication policy in Okta, which factor can be configured to allow or block access based on the risk profile of the user’s login attempt?

A. User group membership
B. Network zone definition
C. Device type and operating system
D. All of the above

Answer: D

Explanation: Authentication policies in Okta can utilize user group membership, network zones, and device information to evaluate the risk profile and determine access.

Question: 967

When developing scripts to interact with Okta APIs, which of the following scripted API calls would effectively deactivate or delete all users within a specified group, while ensuring that the process is efficient and manageable?

A. Loop through each user in the group and call the deactivate API individually.
B. Send a bulk deactivate request through a single API call specifying the group ID.
C. Use the user listing API to retrieve all users, then deactivate them one by one.
D. Directly delete the group to remove all associated users.

Answer: B

Explanation: Sending a bulk deactivate request through a single API call is the most efficient method for managing user status in a group, minimizing API call overhead.

Question: 968

What happens if a client attempts to request an access token with a scope that has not been defined in the authorization server?

A. The request will succeed with default permissions.
B. The request will be rejected with an error indicating invalid scope.
C. The token will be issued with reduced privileges.
D. The application will receive an ID token instead of an access token.

Answer: B

Explanation: If a requested scope has not been defined in the authorization server, the request will be rejected with an error indicating that the scope is invalid.

Question: 969

When configuring an SSO solution for a web application that utilizes the authorization code flow, what is the primary purpose of the redirect URI?

A. To specify the endpoint that will receive the access token from the resource server.
B. To direct the authorization server where to send the authorization code after user authentication.
C. To provide a fallback mechanism for handling failed login attempts.
D. To ensure that the user's credentials are securely transmitted.

Answer: B

Explanation: The redirect URI is crucial as it defines where the authorization server will send the user back after authentication, carrying the authorization code for further token exchange.

Question: 970

When configuring an Okta application to utilize the OAuth 2.0 implicit flow, which of the following security considerations should be taken into account?

A. The access token is passed directly to the application via the URL fragment, exposing it to potential interception
B. The application must include a client secret in the authorization request
C. The access token has a longer expiration time than when using the authorization code flow
D. The implicit flow is ideal for confidential clients that can securely store secrets

Answer: A

Explanation: In the implicit flow, the access token is returned directly in the URL fragment, which poses a risk of interception by malicious actors. This flow is best suited for public clients that cannot securely store credentials.

Question: 971

What is the purpose of the "Source Filter" option in Okta's attribute sourcing configuration?

A. To limit the number of attributes fetched from each source
B. To specify which attributes from a source should be included or excluded
C. To enhance the performance of data synchronization
D. To automatically validate the data fetched from sources

Answer: B

Explanation: The "Source Filter" option allows administrators to include or exclude specific attributes from a source, tailoring the data that is brought into Okta.

Question: 972

In the context of Okta's API, what does it mean to "scope down" your access when requesting tokens?

A. To request more privileges than necessary for the application.
B. To limit the access privileges granted by specifying fewer scopes.
C. To allow users to grant access to multiple applications at once.
D. To increase the refresh token expiration time.

Answer: B

Explanation: "Scoping down" refers to the practice of requesting only the necessary permissions (scopes) required for the application, minimizing excess privileges and enhancing security.

Question: 973

In the context of implementing Okta Policies, what is the most effective way to balance user experience with security requirements?

A. Enforce the strictest security measures without considering user feedback.
B. Regularly engage users to understand their needs while adapting security policies accordingly.
C. Simplify all security measures to enhance user experience, disregarding potential risks.
D. Implement policies that are uniformly applied across all user types, ignoring context.

Answer: B

Explanation: Regularly engaging users to understand their needs allows organizations to adapt security policies in a way that balances user experience with necessary security requirements.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Find Exam
Search your required exam

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.