Okta Consultant Practice Questions:

Question 1

Is this a capability supported by the Okta Org Authorization Server?

Option	Yes/No	Feedback
Integration with an API Gateway	No	This option is incorrect because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets. Access tokens with Okta API scope can only be minted using Org Authorization server.
Addition of custom scopes or claims to tokens.	No	This option is incorrect because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets. Access tokens with Okta API scope can only be minted using Org Authorization server.
Machine-to-machine or microservices architecture	No	This option is incorrect because an Org Authorization Server can be used for SSO with OpenID Connect Apps, Developer SDK, and Okta widgets.

Question 2

Required info for testing Okta RADIUS Server Agent deployment.

Option	Yes/No	Feedback
RADIUS Server (IP address and port number).	Yes	This option is correct because setting up NTRadiusPlay, a RADIUS testing tool for verifying if this configuration of Okta RADIUS Agent is done correctly, requires entering the server IP Address where

		you have your Okta RADIUS Agent installed and the port you set up in your Okta RADIUS Application from the Admin Dashboard.
Okta Super Administrator credentials.	No	This option is incorrect because Okta Super Administrator credentials are not required. The Okta Implementation Consultant needs the credentials from a user assigned to the Okta RADIUS applications but this user does not need to be an Okta Administrator.
RADIUS Application Secret Key	Yes	This option is correct because setting up NTRadPing, a RADIUS testing tool for verifying if the configuration of Okta RADIUS Agent or designated RADIUS Appis done correctly, requires entering the Secret Key from the Okta RADIUS Application from the Admin Dashboard.

Question 3

Behavior of four failed Okta Active Directory Agents.

Option	Yes/No	Feedback
The Active Directory Agent that is next closest geographically will be selected first.	No	This option is incorrect because high availability and failover for the Active Directory Agents would not be based on geographic location of the agent.
The two failed Active Directory Agents will remain in the queue.	No	This option is incorrect because the failed Active Directory Agents would be marked unavailable.

Question 4

True statement regarding Identity Provider (IdP) routing rules.

Option	Yes/No	Feedback
You CANNOT create a rule for Okta as your provider.	No	This option is incorrect because you can create a rule for Okta as your provider.
IdP routing rules are helpful in an on-network vs. off-network scenario.	Yes	This option is correct because you can maintain alternate or legacy authentication for off-network users and use Okta for on-network users.
You can create a rule for each of your providers.	Yes	This option is correct because you can direct authentication based on the Okta user attributes or the application being accessed.
You can redirect authentication based on app user attribute	No	This option is incorrect because you cannot redirect authentication based on app user attributes.

Question 5

Step a Consultant needs to complete when creating a SAML app integration using the App Integration Wizard.

Option	Yes/No	Feedback
Configure the app integration to verify signed SAML assertions for SSO.	Yes	This option is correct because this is a task that is required when using the App Integration Wizard to create a SAML app integration. This step must be completed once the general settings, SAML settings, and feedback have been configured.
Configure the app integration to trust Okta as the Identity Provider (IdP).	Yes	This option is correct because this is a task that is required when using the App Integration Wizard to create a SAML app integration. This step must be completed once the general settings, SAML settings, and feedback have

		been configured.

Question 6

Step a Consultant should take to address an issue where a user's Okta session is not matched to the Okta authentication response from the Org's inbound IdP request.

Option	Yes/No	Feedback
Configure Okta to deactivate users who are deactivated in Okta.	No	This option is incorrect because user deactivation and deactivation are not related to the configuration setting which allows inbound Identity Federation does not match an existing user.
Configure Okta to create a new user using Just-in-Time (JIT) provisioning.	No	This option is incorrect because if the user is found but the incoming identity of the user the two accounts are not configured one to automatically create a new user just using JIT and instead redirect the user to the Okta Sign-in page of the destination Okta org.
Redirect the user to the Okta sign-in page.	Yes	This option is correct because if the existing user is found but the incoming identity of the user the two options are not configured one to automatically create a new user just using JIT and instead redirect the user to the Okta Sign-in page of the destination Okta org.
Configure Okta to create a new user account using Just-in-Time (JIT) provisioning.	Yes	The option is correct because if no match is found for the incoming identity of the user the two options that can be configured are to automatically create a new user just-in-time (JIT) or to redirect the user to the Okta Sign-in page of the destination Okta org.

Question 7

True statement regarding data migration.

Option	Yes/No	Feedback
A hybrid live migration combines aspects of bulk import and Just-in-Time (JIT) migration.	Yes	This option is correct because hybrid live migration is created by first bulk importing identity attributes of the user and then setting their password during their first login (Just-in-Time).
Okta does NOT set the default profile source. The Okta Implementation Consultant needs to set it after the data migration.	No	This option is incorrect because the source of truth for attributes must be set at the stage of the migration process.

Question 8

What a Consultant should tell an app manager to help them achieve security goals.

Option	Yes/No	Feedback
An authentication policy will enforce factor requirements on users when they sign in for an app.	Yes	This option is correct because authentication policies verify that users who try to sign in to the app meet the specifications and enforces factor requirements based on those conditions.

Question 9

True statement regarding Advanced Server Access (ASA) management.

Option	Yes/No	Feedback
It provides Zero Trust identity and access management for cloud and on-premises infrastructures.	Yes	This option is correct because ASA provides Zero Trust identity and access management for both cloud and on-premises

		infrastructures.
Admin users are required to log in using a shared Super Admin account.	No	This option is incorrect because ASA allows teams to control device access using their existing AD accounts, groups, and permissions.
It scopes credential management to an Advanced Server Access tenant.	No	This option is incorrect because all configurations and resources in ASA are scoped to a team. In ASA, a team is a named group of users who can authenticate with Okta.

Question 10

Branding the end-user experience.

Option	Yes/No	Feedback
The custom URL domain feature in Okta.	Yes	This option is correct because this feature allows you to create a custom domain and to configure a custom email address so that you can present a branded experience to your end-users.
The Okta-hosted Sign-in Widget.	No	This option is incorrect because the Okta-hosted Sign-in Widget allows you to add any HTML, CSS, or JavaScript to the sign-in page and also customize the sign-in page per application and sets multiple brands but it does not allow you to customize the Okta URL domain.

Question 11

True statement regarding embedded authentication using Okta SDKs.

Option	Yes/No	Feedback
Embedded authentication	No	This option is incorrect

using SDK redirects the user to Okta for authentication.		because in embedded authentication, the user is kept in the application which reduces redirects to and from Okta.
WebView is a more secure approach for authentication in mobile applications	No	The Option is incorrect because Okta native SDK is more secure than using WebViews for authentication on mobile apps because this practice exposes users to unacceptable security risks.
Embedded authentication is the only deployment model supported by SDKs	No	The option is incorrect because embedded authentication is not the only deployment model supported by SDKs
Okta native SDK provides more secure authentication than using WebView in mobile application	Yes	This option is correct because Okta native SDK is more secure than using WebViews for authentication on mobile apps because this practice exposes users to unacceptable security risks.

Question 12

The Okta implementation Consultant already configured an OAuth 2.0 client in LinkedIn and created an OIDC application in Okta.
Is this the configuration step the consultant needs to complete?

Option	Yes/No	Feedback
Add the LinkedIn Identity Provider (IdP) in Okta with the Account Link Policy set to disabled.	No	This option is incorrect because the Account Link policy is used to specify whether Okta automatically links the user's IdP account with a matching Okta account.
Add the LinkedIn Identity Provider (IdP) in Okta with the Account Link Policy set to enabled.	No	This option is incorrect because the Account Link policy is used to specify whether Okta automatically links the user's IdP account with a matching Okta account.
Add the LinkedIn Identity	No	This option is incorrect

Provider (IdP) in Okta with the Account Link Policy set to 'Auto-link users' set to link the user's IdP account with a matching Okta account.		because setting the 'Auto-link users' to link the user's IdP account with a matching Okta account would not meet the requirement of the scenario that existing Okta accounts who are members of the Okta-LinkedIn group should be auto-linked.
Add the LinkedIn Identity Provider (IdP) in Okta with the Account Link restriction set to the Okta-LinkedIn group.	Yes	

Question 13

True statement regarding on-premises provisioning (SCIM/JIT-P).

Option	Yes/No	Feedback
Only a single connector can be created to provide connectivity to different on-premises applications.	No	This option is incorrect because you can create multiple provisioning connectors to connect different on-premises applications.
Communication between Okta and on-premises applications will only occur through the Okta Provisioning Agent and a native SCIM server.	No	This option is incorrect because Okta and on-premises applications communicate with each other through the Okta Provisioning Agent, a SCIM server, if an on-premises application does NOT support a SCIM server, or an SCIM connector can be built using the Provisioning Agent SDK, a SCIM connector acts as a SCIM server and communicates between Okta and the on-premises application.
The provisioning connector receives SCIM messages from the Okta Provisioning agent, to complete an on-premises application using the API interface used by that application.	Yes	This option is correct because a SCIM connector acts as a SCIM server and completes provisioning to the on-premises application.

Question 14

Setting up inbound federation for users in multiple AD domains (Domain A, Domain B).

Option	Yes/No	Feedback
Place Domain B as priority #1 in Profile Sources.	No	This option is incorrect because with this configuration, users in multiple domains will be authenticated against Domain B.
Place Domain A as priority #1 in Profile Sources.	Yes	This option is correct because it would ensure that users in multiple domains will be authenticated against Domain A.
Ensure the Okta attribute "department" is set to inherit from Okta.	No	This option is incorrect because with this configuration, the value from Domain B will not be placed in the Okta attribute.
Ensure the Okta attribute "department" is set to override profile source and inherit from Domain B.	Yes	This option is correct because it would ensure that users in multiple domains will be authenticated against Domain A and the 'department' value from Domain B is reflected in Okta for all users.

Question 15

Possible source for a Consultant to set up for inbound federation to access multiple applications and domains.

Option	Yes/No	Feedback
A token server.	No	This option is incorrect because a token server cannot be set as an IdP.
A SAML integration.	Yes	This option is correct because a SAML integration can be set as an IdP.
Azure AD using OpenID Connect.	Yes	This option is correct because an Active Directory source can be set as an IdP.

An API request	No	This option is incorrect because an API request cannot be set as an IdP.

Question 16

Expected behavior when configuring an Okta OAuth 2.0 Client to protect APIs in multiple access policies and authorization servers.

Option	Yes/No	Feedback
Multiple tokens will be generated, each with separate authorization policies, token expiration times, and scopes.	Yes	This option is correct because an OAuth 2.0 client can be assigned to any number of authorization servers. Developers configure for a variety of tokens to be generated, each with separate authorization policies, token expiration times, and scopes.
The Resource Owner Password grant type will be used to determine which scopes are generated	No	This option is incorrect because Okta recommends not using the resource owner password grant type in this scenario.
Access tokens can be retrieved from the various authorization servers	Yes	The option is correct because OAuth clients and authorization servers can be assigned on a many-to-many basis. This allows a developer to use a single OAuth client to retrieve access tokens from different authorization servers depending on the use case.

Question 17

Step to unblock an IP blocked by Okta ThreatInsight (currently configured with "Log and enforce security based on threat level").

Option	Yes/No	Feedback
Search the IP in the System Log and add it to the exempted zone directly from the System Log.	Yes	This option is correct because an IP can be added to an IP zone that is exempted by either going to the Network Zone section

		or directly from the System Log.
In the Okta Admin Panel, go to Network Zones and remove the IP from the BlockedIpZone.	No	This option is incorrect because an IP can be only added to an IP zone that is exempted by going to the Network Zone section or directly from the System Log.
Enable the 'Log authentication attempts from malicious IPs' action.	No	This option is incorrect because an IP can be only added to an IP zone that is exempted by going to the Network Zone section or directly from the System Log.

Question 18

Use case for the Users API.

Option	Yes/No	Feedback
The Okta Implementation Consultant needs to address IT requirements to create a user in a way that allows an email to be sent to the user with an activation token that the user can use to complete the activation process.	Yes	This option is correct because this is a use case for the Users API.

Question 19

Benefit of using an Okta-managed certificate with a custom URL domain.

Option	Yes/No	Feedback
It is faster and easier to configure.	Yes	This option is correct because using an Okta-managed certificate when configuring an Okta custom domain is faster and easier than configuring a custom

		domain with your own TLS certificate.
Okta manages certificate renewals.	Yes	This option is correct because when using an Okta-managed certificate, Okta manages your certificate renewals in perpetuity.
It eliminates the risk of a site outage when the certificate expires.	Yes	This option is correct because when using an Okta-managed certificate, Okta manages your certificate renewals in perpetuity.

Question 20

Required component for configuring on-premises provisioning (OPP).

Option	Yes/No	Feedback
On-premise application.	Yes	This option is correct because on-premises provisioning (OPP) combines an on-premise application with a SCIM server or custom connector together with the Okta Provisioning Agent to send user information to and from Okta.
Cloud application.	No	This option is incorrect because on-premises provisioning (OPP) utilizes on-premise application, not cloud applications.
Okta Provisioning Agent.	Yes	This option is correct because on-premises provisioning (OPP) combines an on-premise application with a SCIM server or custom connector together with the Okta Provisioning Agent to send user information to and from Okta.
SCIM server or custom	Yes	This option is correct

connectors.		because on-premises provisioning (OPP) combines an on-premise application with a SCIM server or custom connectors together with the Okta Provisioning Agent to send user information to and from Okta.
Integrated Windows Authorization Agent.	No	This option is incorrect because the Integrated Windows Authorization Agent is not a part of the Okta Provisioning Agent.
Integrated Windows Authentication Agent.	No	This option is incorrect because on-premises provisioning utilizes the Okta Provisioning Agent.

Question 21

Scope needed to configure access to the user's attribute `family_name` in the ID token.

Option	Yes/No	Feedback
Openid	No	This option is incorrect because `openid` is one of the default profile claims.
mail	No	This option is incorrect because `mail` is not one of the default profile claims.
phone	No	This option is incorrect because `phone` is not one of the default profile claims.

Question 22

Valid advantage of using delegated authentication (LDAP Agent).

Option	Yes/No	Feedback
Allows users to reuse their existing LDAP password.	Yes	This option is correct because using delegated authentication when integrating the Okta LDAP Agent allows LDAP to authenticate users when they sign in to Okta.
Enables LDAP to authenticate users when	Yes	This option is correct because using delegated

they sign in to Okta.		authentication when integrating the Okta LDAP Agent allows LDAP to authenticate your users when they sign in to Okta.
Makes LDAP the source of truth of the user.	No	This option is incorrect because using delegated authentication when integrating the Okta LDAP Agent into a customer's existing environment does not make LDAP the source of truth of the user.
Eliminates the need to import users in bulk to Okta	No	This option is incorrect because using delegated authentication when integrating the Okta LDAP Agent with an existing environment does not eliminate the need to import users in bulk in Okta
Enables delegated authentication without the use of the Active Directory domain name suffix	No	This option is incorrect because using delegated authentication when integrating the Okta LDAP Agent in an existing environment does not enable delegated authentication without the use of the Active Directory domain name suffix.

Question 23

Solution for mitigating credential-based attacks (password spraying, brute-force, etc.).

Option	Yes/No	Feedback
Behavior Detection.	No	This option is incorrect because Okta captures patterns of user behavior and uses this information to create profiles that describe typical patterns based on previous activity. After you configure the behavior conditions you're interested in, you can add them to your sign-on policy rules to control when users are

		required to provide multifactor authentication.
Multifactor Authentication.	No	This option is incorrect because the purpose of multifactor authentication is to require users to verify their identity in two or more ways to gain access to their account.

Question 24

Valid sequence of steps to configure a custom authorization server in Okta.

Option	Yes/No	Feedback
1. Create scopes, 2. Create claims, 3. Configure access policies, 4. Create Authorization server.	No	This option is incorrect because the sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients is incorrect.
1. Create Authorization server, 2. Create scopes, 3. Create claims, 4. Configure access policies.	Yes	This option is correct because this is the correct sequence of steps for configuring a custom authorization server in Okta with custom scopes and claims for OAuth 2.0 clients.

Question 25

Role that provides the access token during the Resource Owner Password grant flow.

Option	Yes/No	Feedback
Resource owner.	No	This option is incorrect because it is the resource owner that owns some of the resources hosted by the resource server. This is also known as the user.

Question 26

Protocol supported by the Okta LDAP Interface.

Option	Yes/No	Feedback
RADIUS	No	This option is incorrect because RADIUS is not supported by the Okta LDAP Interface.
StartTLS (LDAP over TLS).	Yes	This option is correct because StartTLS (LDAP over TLS) is supported by the Okta LDAP Interface.
LDAPS (LDAP over SSL).	Yes	This option is correct because LDAPS (LDAP over SSL) is supported by the Okta LDAP Interface.

Question 27

Approach to update the lifetime of an ID token.

Option	Yes/No	Feedback
Identity Provider routing rules.	No	This option is incorrect because Identity Provider routing rules are used to direct users to identity providers based on the user's location, device, email domain, attributes, or the app they are attempting to access.
Token Inline Hook.	Yes	This option is correct because the Token Inline Hook allows you to update how long an access token or an ID token is valid.

Question 28

Functionality supported when using an LDAP directory integration.

Option	Yes/No	Feedback
Self-service password reset.	Yes	This option is correct because self-service password reset is supported when using an

		LDAP directory integration.
Filtering users and groups by selecting an LDAP filter and selecting OUs.	No	This option is incorrect because filtering users and groups by selecting an LDAP filter and selecting OUs is not supported when using an LDAP directory integration.
Active Directory Lightweight Directory Services (AD LDS).	Yes	This option is correct because Active Directory Lightweight Directory Services (AD LDS) is supported when using an LDAP directory integration.
Universal Security Groups.	No	This option is incorrect because universal security groups are not supported when using an LDAP directory integration.

Question 29

Hub-and-Spoke SAML setup. Is this the IdP-initiated URL?

Option	Yes/No	Feedback
Hub Assertion Consumer Service URL.	No	This option is incorrect because the IdP (source) in the Hub and Spoke model, hence, the IdP-initiated URL will be an application-embedded link of the Org2Org application in Spoke.

Question 30

Method for integrating Azure AD as an external IdP for a supply chain partner.

Option	Yes/No	Feedback
Smart Card	No	This option is incorrect because Smart Card is not an option for integrating Azure AD as the external service for this scenario.
SAML 2.0	Yes	This option is correct because SAML 2.0 can be

		used to integrate Azure AD as the external service for this scenario
WS-Fed	No	This option is incorrect because WS-Fed is not an option for integrating Azure AD as the external service for this scenario.
OpenID Connect	Yes	This option is correct because OIDC is an option for integrating Azure AD as the external service for this scenario.
SWA	No	This option is incorrect because SWA is not an option for integrating Azure AD as the external service for this scenario.

Question 31

Expected behavior when an end-user attempts to log in from a high-risk network zone with a deny sign-on policy.

Option	Yes/No	Feedback
The end user receives a message that indicates that only two more login attempts are allowed before the user will be locked out.	No	This option is incorrect because the user will not receive a message regarding their login attempt.
The end user receives a message that indicates that logging in from a restricted zone is prohibited.	No	This option is incorrect because the user will not receive a message regarding their login attempt.

Question 32

Correct flow for Okta Implementation Consultant to select when implementing OIDC for a native application.

Option	Yes/No	Feedback
Client credentials flow.	No	This option is incorrect because Authorization Code with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications, whether

		server-side (web), native, or mobile.

Question 33

True statement about the Redirect Authentication Model.

Option	Yes/No	Feedback
When the Redirect Authentication Deployment Model is used, the user is automatically redirected to and from Okta.	No	This option is incorrect because when the Redirect Authentication Model is used, the user session is redirected to Okta for credential verification and is then redirected to the authenticated access to the client application and other secured resources.
The Redirect Authentication Deployment Model requires a greater level of effort to integrate and maintain compared to the Embedded Authentication Model.	No	This option is incorrect because the Redirect Authentication Model requires a higher level of effort to integrate and maintain compared to the Okta-hosted Sign-in Widget.
When the Redirect Authentication Deployment Model is used, the deployment mitigates DDOS attacks on the application can result in slower sign-in experience.	No	This option is incorrect because SSO (single-sign-on), including single-page application, do not affect the sign-in experience during the Redirect Authentication Deployment Model.
The Redirect Authentication Deployment Model is fully customizable using HTML, CSS, and JavaScript.	Yes	This option is correct because the Redirect Authentication Model is fully customizable through HTML, CSS, and JavaScript.

Question 34

API call for creating an active user in Okta with a password (for a custom email domain).

Option	Yes/No	Feedback
https://[yourOktaDomain]/api/v1/users?activate=true	Yes	This option is correct because it is

		used to create a new user with password and sets the user to active.

Question 35

Use case for a custom email domain.

Option	Yes/No	Feedback
Okta needs to send emails through a domain that uses SendGrid.	No	This option is incorrect because you cannot configure Okta to send emails through a domain that uses SendGrid.

Question 36

A customer needs to brand the domain experience for end users.
Is this what an Okta Implementation Consultant should use to achieve this goal?.

Option	Yes/No	Feedback
The Okta Brands API	No	This option is incorrect because the Okta Brands API allows you to customize the look and feel of the pages and templates but does not allow you to customize the domain.
The background image of the sign-in page	No	This option is incorrect because it does not allow you to create a custom domain.

CASE STUDY

Sound Healthcare Technology Case Study

Company Description

- Multinational healthcare technology company with three global offices
- 2,500 employees
- 300,000 customers

Existing Technical Setup of Sound Healthcare Technology

1. The company has two Active Directory forests and five domains.
2. Internally developed applications use OpenID Connect (OIDC)/OAuth 2.0.
3. User accounts are available in multiple places such as a Microsoft SQL Server database, a CSV file, and Workday.
4. Each partner has its own identity infrastructure and applications.
5. The company's customers include companies with employees who work with applications that are hosted on-premises at Cloud Vault Financials. Some of those applications are custom-developed tools, scripts, and applications that run on Windows and Linux servers.
6. Each internal business unit (for example, Sales, HR, Finance) maintains its own infrastructure and set of applications.
7. Enterprise and cloud-based applications provide domain-specific access.
8. Multifactor authentication (MFA) is NOT compatible with enterprise on-premise applications; users must authenticate to the corporate network via VPN.
9. MFA is currently used for cloud-based applications.

Customer Solution Goals

1. Add external user accounts into a centralized identity service; allow customers to self-register.
2. Automate the creation of partner, contractor, and employee accounts.
3. Adopt a more centralized approach to Identity and Access Management (IAM).
4. Allow partners, customers, and contractors/employees to access applications for daily tasks more efficiently and effectively.
5. Automate the process of provisioning users to applications seamlessly.
6. Implement IT solutions that enhance user productivity and efficiency by ensuring end users can easily access applications.
7. Deliver a return on investment (ROI) within one year and reduce the total cost of ownership (TCO) over the lifetime of the product.
8. Develop an onboarding process via Workday as a source to minimize processing time for hire requests.
9. Enable Single Sign-On (SSO) for specified applications.
10. Implement a password-less authentication experience.
11. Ensure solution supports flexibility to add external use cases for future business-to-business (B2B) solutions so supply-chain partners can easily use applications.

12. Ensure that only employee-trusted devices gain access to company applications such as Microsoft Office 365.

Technical Requirements for a New Solution with Okta

1. Employees must be able to sign in to applications by using their Okta accounts.
2. When accessing corporate resources remotely, authentication must meet more stringent Authentication Assurance Levels (AALs).
3. Internal IT specifications and other documents should be shared between internal business units and partners by using Box or a similar application.
4. Sales data must be shared across internal business units and partners by using Salesforce.
5. Branding is very important; partners and customers must NOT see Okta domain.
6. Users must NOT see redirects to different domains during authentication for a seamless experience.
7. Adaptive MFA must be used to secure the partners' authentication to the company's apps.
8. Okta's core identity and access controls must be extended to the company's infrastructure and applications.
9. Extend Okta's identity solutions to Linux and Windows servers through Secure Shell (SSH) and Microsoft Remote Data Protocol (RDP).
10. Self-service options must be available to customers (registration, password operations, and so forth).
11. Workday must be implemented as a source of truth for employees.

Question 36

Sound Healthcare Technology wants to require Workforce users to authenticate using Okta and to use a custom Multifactor Authentication (MFA) solution as the second factor. After the Okta Implementation Consultant completed the configuration of the Identity Provider (IdP), routing rules, custom authenticator, and authentication policies, target users are NOT able to use the custom MFA solution as the second factor. Is this a possible reason for the failure?

Option	Yes/No	Feedback
The IdP certificate is NOT managed by Okta.	No	This option is incorrect because the certificate must only be valid; it does not need to be managed by Okta.
The custom authenticator is inactive.	Yes	This option is correct because the custom authenticator must be enabled and appropriately configured to use a custom Multifactor Authentication

		(MFA) solution as the second factor.
The IdP is active.	No	This option is incorrect, the IdP should be active.
The IdP Usage setting is set for SSO only.	Yes	This option is correct because to meet the requirements, the Consultant must select the Factor only option from the IdP Usage dropdown; you can't use the SSO only option with the IdP authenticator.

Question 37

The Okta Implementation Consultant for Sound Healthcare Technology is configuring Multifactor Authentication (MFA) as a service for Active Directory Federation Services (ADFS). The Okta Implementation Consultant completed the following steps:

- Installed and configured Microsoft ADFS in Okta
- Installed the Okta ADFS Plugin on the ADFS server
- Enabled the Okta MFA Provider in ADFS

When the Okta Implementation Consultant attempts to log in to ADFS with a test user account, an error does NOT appear, but the Okta MFA prompt does NOT appear. Is this a possible reason for this result?

Option	Yes/No	Feedback
The Okta Implementation Consultant did NOT add the Access Control Policy to the relying party application.	Yes	This option is correct because adding the Access Control Policy is a Relying Party Application step that is required when configuring MFA in ADFS.
The ADFS setup is not correct.	No	This option is incorrect because the setup looks correct.
The IP Address setting is not correct.	No	This option is incorrect because the ADFS setup is not based on IP address settings.
The UDP port used by Okta is not correct.	No	This option is incorrect because the default UDP port is correct.

Question 38

Sound Healthcare Technology wants to enforce Multifactor Authentication (MFA) for their employees who access network remotely using a VPN. For technical reasons, the organization has multiple VPN solutions deployed on their infrastructure. Sound Healthcare Technology is anxious to get a single Okta RADIUS server agent used with multiple integrations. The company has engaged an Okta Implementation Consultant to set up MFA with the Okta RADIUS server agent to support the integration with multiple RADIUS-enabled applications at the same time. Is this a consideration the Okta Implementation Consultant must keep in mind when configuring MFA?

Option	Yes/No	Feedback
Multiple RADIUS apps must be added in Okta: one for each RADIUS-enabled application, configured with a different UDP port.	Yes	This option is correct because the Okta RADIUS server agent supports multiple ports simultaneously but one RADIUS app must be added in Okta for each RADIUS-enabled application being integrated with Okta.
A minimum of one Okta RADIUS server agent must be deployed for every RADIUS-enabled application.	No	This option is incorrect because one RADIUS app (not one Okta RADIUS server agent) must be added in Okta for each RADIUS-enabled application being integrated with Okta. (Existing Technical Setup, Point 8)

Question 39

An Okta Implementation Consultant configured Okta FastPass for employees and contractors at Sound Healthcare Technology. During testing, the Okta Implementation Consultant signs in to Salesforce on a macOS desktop set up for authentication with Okta FastPass. The Okta Implementation Consultant then logs out and attempts to sign in to Salesforce from a private browser window (Incognito mode). Is this the behavior the Okta Implementation Consultant should expect?

Option	Yes/No	Feedback
The user is automatically logged in.	Yes	This option is correct because on macOS or Windows desktops set up for authentication with Okta

		FastPass, if users access the Okta End-User Dashboard from a private browser window (Incognito mode), they gain access to the page as if they were in a regular browser session. Okta Verify runs on the desktop, verifies the identity of the users, and grants them access to the dashboard. The authentication is not affected by the browser mode (regular or private). (Customer Solution Goals, Point 10)
The user is redirected to the Okta sign-in page.	No	This option is incorrect because for FastPass, the authentication is not affected by the browser mode (regular or private).

Question 40

An Okta Implementation Consultant completed an integration of single sign-on with Sound Healthcare Technology's Salesforce instance. When the Okta Implementation Consultant accesses the Tasks page in the Okta dashboard, the following error is displayed: "Automatic provisioning of user John Doe to app Salesforce.com failed: Matching user not found." Is this a possible cause of this error message?

Option	Yes/No	Feedback
The third-party admin account reached a password expiration date.	No	This option is incorrect because it is associated with a different error: "Automatic provisioning of user John Doe to app Salesforce.com failed: The credentials used to connect to the API were invalid; please check your configuration."
The third-party admin password was changed but NOT updated in Okta.	No	This option is incorrect because it is associated with a different error: "Automatic provisioning of user John Doe to app

		Salesforce.com failed: The credentials used to connect to the API were invalid; please check your configuration."
The provisioning feature is enabled in Okta but the create, update, and deactivate users options are NOT turned on.	Yes	This option is correct because the error message tells you that the Create user option is not on, as the error message states that it was unable to find a user in the Salesforce application that matches this user, and therefore it could not assign the app integration.

Question 41

The Okta Implementation Consultant for Sound Healthcare Technology configured Workday as a profile source for Okta. The Workday Administrator made updates to the emails of User A and User B, but only User A is reflecting the changes in Okta after repeated imports. Is this a potential cause of the issue?

Option	Yes/No	Feedback
User B is NOT linked to the corresponding profile in Workday.	Yes	This option is correct because if User B is not linked to the corresponding profile in Workday, his email information will not be imported to Okta when Workday is configured as the profile source.
Attribute-level sourcing is NOT configured correctly.	Yes	This option is correct because attribute-level sourcing allows you to designate different profile sources for different user attributes. If attribute-level sourcing is configured differently for Users A and B, User A could have been updated but not User B due to the different configurations. (Technical Requirements, Point 11)

Question 42

Sound Healthcare Technology configured Okta to bring in users from Workday HR, Active Directory, and a CSV file. All three identity stores are configured to be a profile source. In some cases, users will exist in two of the identity stores, and in some cases a user may exist in all three identity stores. The business requirements include using Workday data if it is available for a user, and the Workday data should be reflected in Okta. Is this the correct priority setting that the Okta Implementation Consultant must set to achieve the requirements?

Option	Yes/No	Feedback
Set Workday below CSV in profile sources	No	This option is incorrect because the CSV file data would take priority over Workday data if both are available.
Set Workday below Active Directory in profile sources	No	This option is incorrect because the Active Directory data would take priority over Workday data if both are available.
Set Workday as priority 1 in profile sources	Yes	This option is correct because setting Workday as priority 1 achieves the goal of using Workday data as the source, if it is available for a user. (Technical Requirements, Point 11)

Question 43

The Okta Implementation Consultant for Sound Healthcare Technology configured Workday as a source of truth for Okta. During testing, the Workday Administrator is NOT able to edit provisioned user groups in Okta. Is this a potential cause of this issue?

Option	Yes/No	Feedback
The Domain Security Policy in Provisioning Group Administration is disabled	Yes	This option is correct because the Workday Administrator was have the correct privileges to edit provisioned user groups. The Domain Security Policy in Provisioning Group

		Administration must be enabled and the Workday Administrator must belong to a security group with modify permissions in Okta. (Customer Solution Goals, Point 5)

Question 44

A company has a user in Chicago, Illinois. This user logged in to Okta at 3:00 PM CDT and 25 minutes later, the same user attempted to log in from Bucharest, Romania. Is this the component of behavior detection that is responsible for flagging this issue?

Option	Yes/No	Feedback
Location	No	This option is incorrect because this setting checks a city, state, country, or location outside of a specified radius that has not been seen in the user's past successful sign-in attempt. It does not take time between attempts into consideration.
Velocity	Yes	This option is correct because Velocity looks at the time between consecutive sign-in attempts from different locations to determine if a human could have made the journey. Since a human can't travel from Chicago to Bucharest in 25 minutes, this is a velocity issue.
IP	No	This option is incorrect because IP checks if the sign-in attempt is from a bad or malicious IP address.
Device	No	This option is incorrect because Device checks if the sign-in attempt is from a trusted device.

Question 45

An Okta Implementation Consultant is configuring a native application for Sound Healthcare Technology that CANNOT store the secret. Is this the OpenID Connect flow that the Okta Implementation Consultant should choose?

Option	Yes/No	Feedback
Implicit flow	No	This option is incorrect because the Implicit flow is a legacy flow used only for SPAs that cannot support PKCE.
Authorization code + PKCE	Yes	This option is correct because the Authorization Code flow with Proof Key for Code Exchange (PKCE) is the recommended flow for most applications whether server-side (web), native, or mobile. (Existing Technical Setup, Point 2)

Question 46

An Okta Implementation Consultant needs to provide a list of security best practices recommended for an Okta Access Gateway (OAG) deployment to Sound Healthcare Technology's security team. Is this a security best practice to securely deploy OAG?

Option	Yes/No	Feedback
Deploy Access Gateway admin node on the internal network	Yes	This option is correct because Okta recommends deploying the Access Gateway admin node on the internal network separate from worker nodes so that the admin node is unreachable from the public internet.
Deploy Access Gateway worker node on the internal network	No	This option is incorrect because the OAG worker node should be on the DMZ (separate from the admin node) to be accessible from the public internet.

Change passwords for the Access Gateway Management Console and Access Gateway Admin UI.	Yes	The option is correct because Okta recommends resetting the Admin UI and Management console default passwords.
Install OAG on a physical server	No	This option is incorrect. OAG can be installed on a virtual machine and is generally recommended for ease of management and deployment.
Use TLS/SSL certificate signed by a Certificate Authority (CA).	Yes	This option is correct. The OAG should use TLS/SSL certificates signed by a trusted CA to ensure secure communication and verification.

Question 47

Sound Healthcare Technology configured agentless Desktop Single Sign-On (DSSO) and Just-in-Time (JIT) Provisioning. Is this the correct flow when a user that has NOT been imported into Okta tries to log in via agentless DSSO?

Option	Yes/No	Feedback
1. The web browser sends the Kerberos ticket to Okta. 2. The Integrated Web Authentication (IWA) Agent looks up the user's `SAMAccountName`. 3. If the user's `SAMAccountName` is found, Okta validates the Kerberos ticket. 4. Okta creates the user. 5. The user signs in successfully.	No	This option is incorrect because in Step 2, the Okta Active Directory Agent looks up the user's UPN, not the Integrated Web Authentication (IWA) Agent looking up the `SAMAccountName`.
1. The web browser sends the Kerberos ticket to Okta. 2. The Okta Active Directory Agent looks up the user's UPN. 3. If the user's UPN is found, Okta validates the Kerberos ticket. 4. Okta creates the user. 5. The user signs in successfully.	Yes	This option is correct because if a user has not been imported into Okta and logs in via agentless DSSO with JIT enabled, Okta uses the UPN to validate the user. If the Okta username format isn't a UPN and instead uses another format, Okta ignores this setting and uses the UPN

		validation.