Free Questions for IdentityNow-Engineer

Shared by Faulkner on 29-10-2024

For More Free Questions and Preparation Resources

Question 1

Is this an item that an IdentityNow engineer should configure when implementing a source that uses a JDBC connector?

Solution: This item is complete

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, the statement 'This item is complete' is vague and does not represent any actionable configuration when implementing a JDBC connector. An IdentityNow engineer needs to focus on specific technical configurations like setting up schemas, defining SQL queries, mapping attributes, and ensuring the correct service account permissions. Simply stating 'This item is complete' is not a valid step in the

implementation process.

SailPoint IdentityNow JDBC Connector Implementation Checklist.

SailPoint IdentityNow Configuration and Implementation Documentation.

Question 2

Question Type: MultipleChoice

Is this an item that an IdentityNow engineer should configure when implementing a source that uses a JDBC connector?

Solution: Use a query select statement with a clause to match the incoming account to an existing account for the Single Account SQL Query configuration item

Options:

A- Yes

B- No

Answer:

A

Explanation:

Yes, using a query select statement with a clause to match the incoming account to an existing account is a key configuration for the Single Account SQL Query in a JDBC connector. This query is used to fetch specific account details from the database and must be written in such a way that it uniquely identifies each account, ensuring accurate correlation between the data in the source and the identities in IdentityNow. Properly configuring this SQL query ensures the right accounts are matched and managed.

SailPoint IdentityNow JDBC Connector Single Account Query Configuration Guide.

SailPoint IdentityNow SQL Query Best Practices Documentation.

Question 3

Question Type: **MultipleChoice**

Is this an item that an IdentityNow engineer should configure when implementing a source that uses a JDBC connector?

Solution: Define an account schema by using 'Discover Schema'' or by manually configuring the schema attributes.

A- Yes

B- No

Answer:

A

Explanation:

Yes, defining an account schema is an essential step when implementing a JDBC connector. The schema defines the structure of the identity data being pulled from the database, including the attributes that will be mapped to identity profiles in IdentityNow. The schema can be defined either by using the 'Discover Schema' option, which automatically identifies available attributes, or by manually configuring the schema attributes if specific custom mappings are required.

SailPoint IdentityNow JDBC Connector Schema Configuration Guide.

SailPoint IdentityNow Source Schema Discovery Documentation.

Question 4

Question Type: MultipleChoice

Is this an item that an IdentityNow engineer should configure when implementing a source that uses a JDBC connector?

Solution: Select the checkbox to use database admin as service account.

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, selecting a checkbox to use the database admin as the service account is not a recommended or required configuration when implementing a source that uses a JDBC connector. Typically, for security and least privilege, a dedicated service account with only the necessary permissions to read and manage identities within the database is used. Granting database administrator (DBA) privileges to the service account introduces unnecessary security risks and is against best practices.

SailPoint IdentityNow JDBC Connector Configuration Guide.

SailPoint IdentityNow Best Practices for Service Accounts Documentation.

Question 5

The customer has a system that matches the following description. Is this a suitable connector type to use?

The system is a modern, cloud-based, web application that uses a MySQL database backend provided by the cloud platform. The database is only accessible from the web application. The web application exposes a fully compliant SCIM 2.0 interface with OAuth 2.0 client credentials.

Solution: SCIM 2.0 Connector

Options:

A- Yes

B- No

Answer:

A

Explanation:

Yes, the SCIM 2.0 Connector is the most suitable connector for this use case. The system described is a modern, cloud-based web application that exposes a fully compliant SCIM 2.0 interface and uses OAuth 2.0 client credentials for authentication. SCIM (System for Cross-domain Identity Management) is a standardized protocol designed to simplify identity management in cloud applications. The SCIM 2.0 Connector in SailPoint IdentityNow is specifically built to integrate with systems that provide a SCIM interface, making it the ideal connector for this scenario.

SailPoint IdentityNow SCIM 2.0 Connector Guide.

SailPoint IdentityNow Cloud-Based Integration Documentation.

Question 6

Question Type: MultipleChoice

The customer has a system that matches the following description. Is this a suitable connector type to use?

The system is a modern, cloud-based, web application that uses a MySQL database backend provided by the cloud platform. The database is only accessible from the web application. The web application exposes a fully compliant SCIM 2.0 interface with OAuth 2.0 client credentials.

Solution: OpenLDAP Connector

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, the OpenLDAP Connector is not suitable for this use case. OpenLDAP is designed for integrating with LDAP-based directories, and the system described is a cloud-based web application that uses a SCIM 2.0 interface with OAuth 2.0 for authentication. Since the system supports SCIM, the correct connector would be the SCIM 2.0 Connector, which is tailored for cloud-based systems with SCIM interfaces.

SailPoint IdentityNow OpenLDAP Connector Guide.

SailPoint IdentityNow SCIM 2.0 Connector Documentation.

Question 7

The customer has a system that matches the following description. Is this a suitable connector type to use?

The system is a modern, cloud-based, web application that uses a MySQL database backend provided by the cloud platform. The database is only accessible from the web application. The web application exposes a fully compliant SCIM 2.0 interface with OAuth 2.0 client credentials.

Solution: Generic Cloud Connector

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, the Generic Cloud Connector is not the most suitable connector type for this use case. The system described is a modern, cloud-based web application that exposes a SCIM 2.0 interface with OAuth 2.0 client credentials for authentication. The Generic Cloud

Connector is typically used for systems that do not have specialized connectors but can integrate via general APIs or REST endpoints. Since the application supports SCIM 2.0, which is a standardized protocol for managing identities, the SCIM 2.0 Connector would be the more appropriate choice, as it is specifically designed for this type of integration.

SailPoint IdentityNow SCIM 2.0 Connector Guide.

SailPoint IdentityNow Connector Overview Documentation.

Question 8

Question Type: **MultipleChoice**

Can a user with Report-admin level permissions within IdentityNow perform this action?

Solution: View a live display of events in progress

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, a user with Report-admin level permissions cannot view a live display of events in progress. The Report-admin role is primarily concerned with reporting functions, such as viewing and managing reports. Viewing live events, especially operational or real-time system events, would require higher-level permissions, typically associated with System Admin or Operations Admin roles, which have access to system dashboards, monitoring tools, and event logs.

SailPoint IdentityNow Role-Based Access Control (RBAC) Documentation.

SailPoint IdentityNow Monitoring and Event Logging Permissions Guide.

Question 9

Question Type: **MultipleChoice**

Can a user with Report-admin level permissions within IdentityNow perform this action?

Solution: invite new users to IdentityNow.

Options:

A- Yes

B- No

Answer:

B

Explanation:

No, a user with Report-admin level permissions cannot invite new users to IdentityNow. The Report-admin role in IdentityNow is restricted to managing reports---this includes generating, viewing, and managing access to reports but does not extend to user management tasks such as inviting new users. Only users with Admin, Org Admin, or other higher-level roles with explicit user management permissions can invite new users to the platform.

SailPoint IdentityNow Role-Based Access Control Documentation.

SailPoint IdentityNow Permissions Matrix for Admin Roles.