DUMPSARENA

SailPoint Certified IdentityNow Engineer

SailPoint IdentityNow-Engineer

Version Demo

Total Demo Questions: 11

Total Premium Questions: 119

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

QUESTION NO: 1

A customer wants to configure a virtual appliance (VA) to use a static IP address. Does this file on the VA need to be modified to perform the configuration?

Solution: /etc/ systemd/network/ static, network

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. The intended path is `/etc/systemd/network/static.network`, with the spaces and comma in the question understood as formatting errors. This systemd-networkd configuration file is used by the Virtual Appliance to define static network settings. An administrator configures the applicable network interface and supplies the fixed address information, including the IP address and prefix, default gateway, and—where required—DNS settings. The Virtual Appliance can then consistently communicate with Identity Security Cloud and with the systems it connects to, without relying on a DHCP lease that could change over time.

The file uses the standard systemd-networkd configuration approach: a `[Match]` section identifies the relevant interface, and a `[Network]` section contains the desired addressing and routing values. Because the VA is an appliance managed for a specific integration purpose, static addressing should be planned carefully to avoid IP conflicts and to ensure required routes, name resolution, firewall rules, and outbound connectivity remain available after the network configuration is applied. SailPoint's Virtual Appliance documentation provides deployment and networking guidance at SailPoint Virtual Appliance documentation. The systemd-networkd file format and network settings are documented at systemd.network.

QUESTION NO: 2

Is this statement correct about security and/or encryption of data?

Solution: When setting up a virtual appliance cluster. SailPoint creates an asymmetnc key pair based on a user-provided passphrase. and then uses this key pair to communication with the IdentityNow tenant.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. During Virtual Appliance cluster setup, the administrator supplies a passphrase that protects the cryptographic material generated for the cluster. SailPoint uses asymmetric cryptography to establish the Virtual Appliance cluster's trusted identity with the IdentityNow tenant (now SailPoint Identity Security Cloud). The generated key pair supports secure authentication and protected communications between the tenant and the Virtual Appliances, including the delivery of configuration and the execution of connector-related operations through the Virtual Appliance.

The private portion of the key material remains protected within the Virtual Appliance environment; the passphrase is a critical part of safeguarding that material and must be retained securely by the organization. This trust arrangement allows the cloud tenant to recognize the configured cluster while avoiding exposure of the private key. Consequently, protecting the passphrase and applying SailPoint's recommended Virtual Appliance deployment and operational controls are important responsibilities for the customer operating the cluster.

For SailPoint's current Virtual Appliance documentation and deployment guidance, see the SailPoint Documentation portal and SailPoint's Support portal.

QUESTION NO: 3

Is the following true about the web-services connector in IdentityNow?

Solution: The connector supports SAML authentication.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. The IdentityNow Web Services connector is intended to integrate with REST- or SOAP-based services by making API requests to a target system. Its connection configuration supports API-oriented authentication mechanisms, including basic authentication, bearer-token authentication, OAuth 2.0 flows, API keys, and custom request headers, depending on the endpoint's requirements. SAML is a browser-based federation protocol principally used to establish user single sign-on sessions between an identity provider and a service provider. It is not an authentication type supported by the Web Services connector's native connection authentication configuration.

For integrations that need to call an API protected by an identity platform, the connector should instead be configured with the API's supported token or OAuth-based method. This enables the connector to obtain or supply credentials in a format that can be included in its HTTP requests and refreshed when applicable. SailPoint's Web Services connector documentation describes configuring the connection and its available authentication approaches for API integrations. See the SailPoint Web Services connector documentation and the Web Services connector authentication documentation.

QUESTION NO: 4

An IdentityNow engineer has set up an access profile for an application. The access profile allows for users to request access, and for a user's manager to approve or deny access.

After a recent staff meeting, management has expressed that they want to remove any approval requirements for this application.

Is management's request possible in IdentityNow. and. if so. are these the recommended steps the engineer should take to meet their new requirement?

Solution: It is possible. Edit the access profile, and uncheck the box marked 'Required Approval'.

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityNow supports requestable access profiles with no approval step. An engineer can edit the relevant access profile and clear the *Required Approval* setting in its request configuration. This retains the profile's requestable behavior, allowing users to submit access requests, while removing the manager approval decision from the workflow. After the request is submitted, IdentityNow can proceed directly with provisioning the entitlements represented by that access profile, subject to the source and provisioning configuration being able to fulfill the assignment.

This setting is appropriate when the organization has determined that the access represented by the profile is sufficiently low-risk, broadly eligible, or otherwise governed through controls outside an individual manager-approval process. The change should be made on the specific access profile so that its request and approval behavior matches the application's updated business policy. SailPoint documents access-profile configuration, including requestability and approval settings, in its Access Profiles documentation. Additional context on how users request access and how request workflows are handled is available in SailPoint's Access Requests documentation.

QUESTION NO: 5

An IdentityNow engineer needs to find identities with disabled AD accounts by using IdentityNow ' s search features. Is this the correct search syntax to perform this task?

Solution:

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct. IdentityNow Search supports the `@accounts(...)` nested-query syntax to return identities based on properties of their linked account documents. Within that account query, `source.name:"AD"` scopes the match to accounts from the source named AD, while `disabled:true` filters for account records whose normalized `disabled` field is set to true. Together, `@accounts(source.name:"AD" AND disabled:true)` identifies identities that have at least one disabled account on that AD source. This is particularly useful when an identity has accounts on multiple sources and the engineer must distinguish a disabled Active Directory account from an account disabled elsewhere. The query relies on IdentityNow's indexed account data, so the source name must match the configured source name and the source aggregation must have populated the account's disabled status. SailPoint's Search documentation describes using the account annotation to search account attributes associated with identities and combining criteria with Boolean operators. The account data model also includes a Boolean disabled property for an account, making `disabled:true` the appropriate condition for this search. See SailPoint's Search query syntax documentation and Account model reference.

QUESTION NO: 6

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.

A. Yes

B. No

ANSWER: B

Explanation:

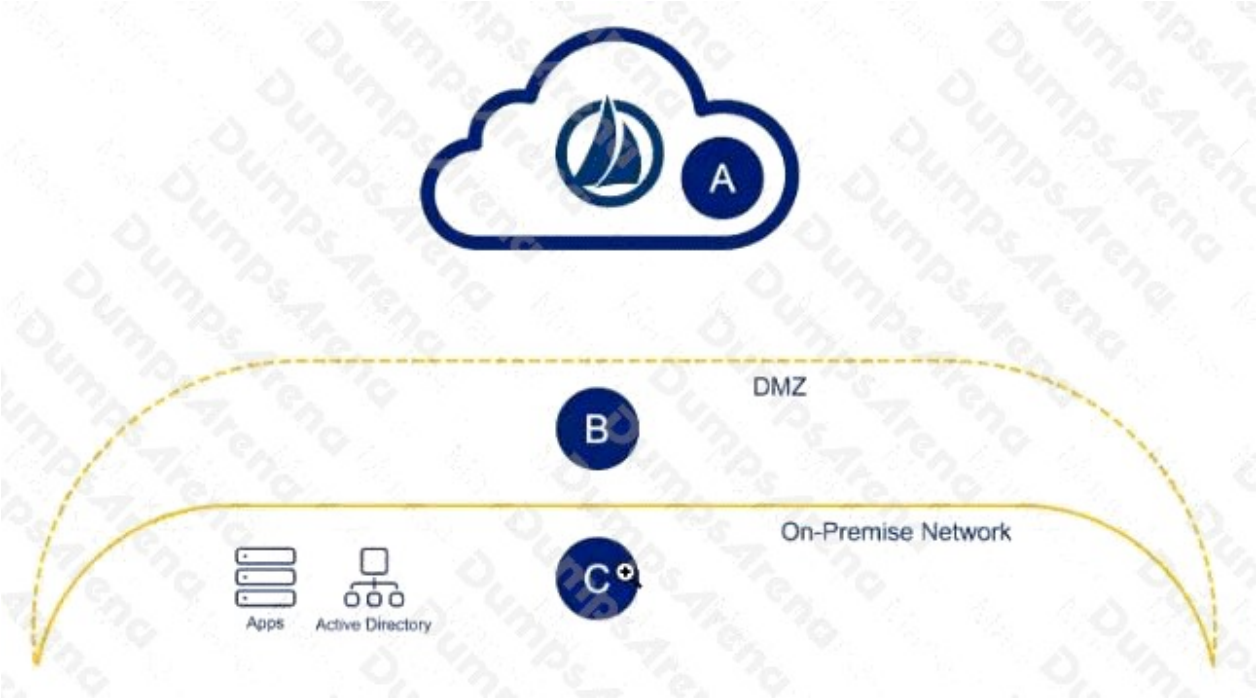
No is correct. When configuring a JDBC source, the connection account should be a dedicated database service account that has only the permissions needed for the connector's required operations. This normally includes the ability to connect to the database and read the tables, views, or stored procedures used for account and entitlement aggregation. If the source is configured for provisioning, the account should receive only the additional, narrowly scoped permissions required to perform the approved create, update, enable, disable, or delete operations.

Using a database administrator account as the connector service account violates the principle of least privilege. DBA-level credentials commonly have broad authority over database objects, users, schemas, configuration, and potentially sensitive data. Compromise or misuse of those credentials would therefore create an unnecessarily large security impact. An IdentityNow engineer should instead work with the database owner to establish a non-personal account, restrict it to the required database and objects, protect and rotate its credentials, and validate that the account can complete the connector operations without elevated administrative access.

See SailPoint's JDBC connector documentation and the SailPoint identity security best-practices guidance.

QUESTION NO: 7

Exhibit.



Solution: An engineer has one small production data center with an Active Directory, a database server, and two cloud applications to which they need to connect Where would the virtual appliances (VAs) reside In this scenario?

Solution: B

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. For this environment, the Virtual Appliance should be deployed on the trusted internal network where it can establish secure outbound connectivity to SailPoint and directly communicate with the on-premises systems it must service. In particular, the VA requires network access to the Active Directory domain controllers and the database server so that the relevant connectors can perform aggregation, authentication, and provisioning operations. Positioning the VA with the internal resources also supports the principle of minimizing firewall exposure: the VA initiates encrypted outbound communications to SailPoint rather than requiring broad inbound access from the internet.

The cloud applications do not require the VA to sit in a perimeter network merely because they are cloud-hosted. Their connectors can use SailPoint's SaaS connectivity where appropriate, while the VA remains the secure bridge for systems that are reachable only from the organization's private network. SailPoint's Virtual Appliance architecture is specifically intended to provide this controlled connection between Identity Security Cloud and private-network applications, directories, and databases. For deployment and network guidance, see SailPoint's Virtual Appliance overview and Virtual Appliance requirements.

QUESTION NO: 8 - (SIMULATION)

What is the required order of steps to implement an identity model for a given authoritative source? Drag the five steps from the left to the answer area on the right, and place them in the coned order. Not all options will be used.

ANSWER: Check the explanation for the answer

Explanation:

The required order is:

1. **Create a source and aggregate the data.**
2. **Create an identity profile and associate it with the source.**
3. **Define the identity mappings, including any required transforms.**
4. **Preview the identity mappings using the aggregated data.**
5. **Finalize the source create profile.**

This sequence ensures that data is available before mappings are configured and previewed, then the source configuration can be finalized.

QUESTION NO: 9

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

A. Yes

B. No

ANSWER: A

Explanation:

Yes is correct because the application exposes a fully compliant SCIM 2.0 service, which is the integration interface SailPoint IdentityNow should use. The SCIM 2.0 Connector is designed for applications that support the System for Cross-domain Identity Management protocol and enables IdentityNow to manage identity data through the application's supported SCIM resources and operations. OAuth 2.0 client-credentials authentication is also an appropriate machine-to-machine authentication method for this connector, allowing IdentityNow to authenticate to the application's SCIM API without relying on an interactive user session.

The MySQL database does not change that conclusion. Its access is restricted to the web application, so it is neither an available nor an appropriate direct integration point. SailPoint should connect through the application's supported public identity-management interface rather than attempt database-level access. Using the SCIM endpoint also respects the application's intended security and data model while supporting account aggregation and provisioning through the standard API. SailPoint's connector documentation describes the SCIM 2.0 Connector as an integration for SCIM 2.0-enabled systems and documents its authentication configuration, including OAuth-based approaches. See the SailPoint SCIM 2.0 Connector documentation and the SCIM Protocol specification.

QUESTION NO: 10

An IdentityNow engineer has the following problem:

IdentityNow shows status failed on a virtual appliance (VA).

Is this one of the steps that should be taken troubleshoot the issue?

Solution: Verify that the VA is configured for automatic updates by setting 'autoupdate=true' in the config.yaml file.

A. Yes

B. No

ANSWER: B

Explanation:

No is correct. A failed Virtual Appliance status requires investigation of the condition currently preventing the VA from communicating with IdentityNow or operating its required services. Appropriate troubleshooting begins by checking VA connectivity and health, confirming that required services are running, and reviewing relevant VA logs for errors such as network, DNS, proxy, certificate, resource, or service-startup failures. These checks help identify the immediate cause of the failed state and provide evidence for remediation.

Automatic-update configuration is a lifecycle and maintenance setting rather than a diagnostic or recovery action for a VA that is already reporting failed. Although maintaining supported VA software levels is important operationally, changing or validating an automatic-update setting does not establish connectivity, restart a failed service, or identify the error that caused the status to fail. Engineers should first follow the Virtual Appliance troubleshooting and log-collection guidance, then apply updates through the supported process when appropriate. SailPoint's Virtual Appliance documentation is available at Virtual Appliance documentation, and the IdentityNow support resources are available through the SailPoint Community.

QUESTION NO: 11

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 is correct. An IdentityNow JDBC source requires an account schema so IdentityNow can interpret the account records returned by the database query. The schema defines the account attributes available to the source, including the attribute used as the account identifier and any additional attributes needed for identity correlation, access profiles, provisioning use cases, or reporting. During source configuration, an engineer can use schema discovery to retrieve attributes from the JDBC account query and build the schema from the query results. This is often the most efficient approach when the query is complete and representative of the account data. The engineer can also configure schema attributes manually when the implementation requires deliberate control over attribute names, types, or definitions. In either case, defining the schema is a core implementation activity because downstream identity-profile mappings and correlation depend on the source exposing usable account attributes. SailPoint's JDBC connector documentation describes configuring account aggregation and source schema details, while the general source documentation explains the role of account schemas in representing account data within IdentityNow. See SailPoint JDBC Connector documentation and SailPoint Sources documentation.