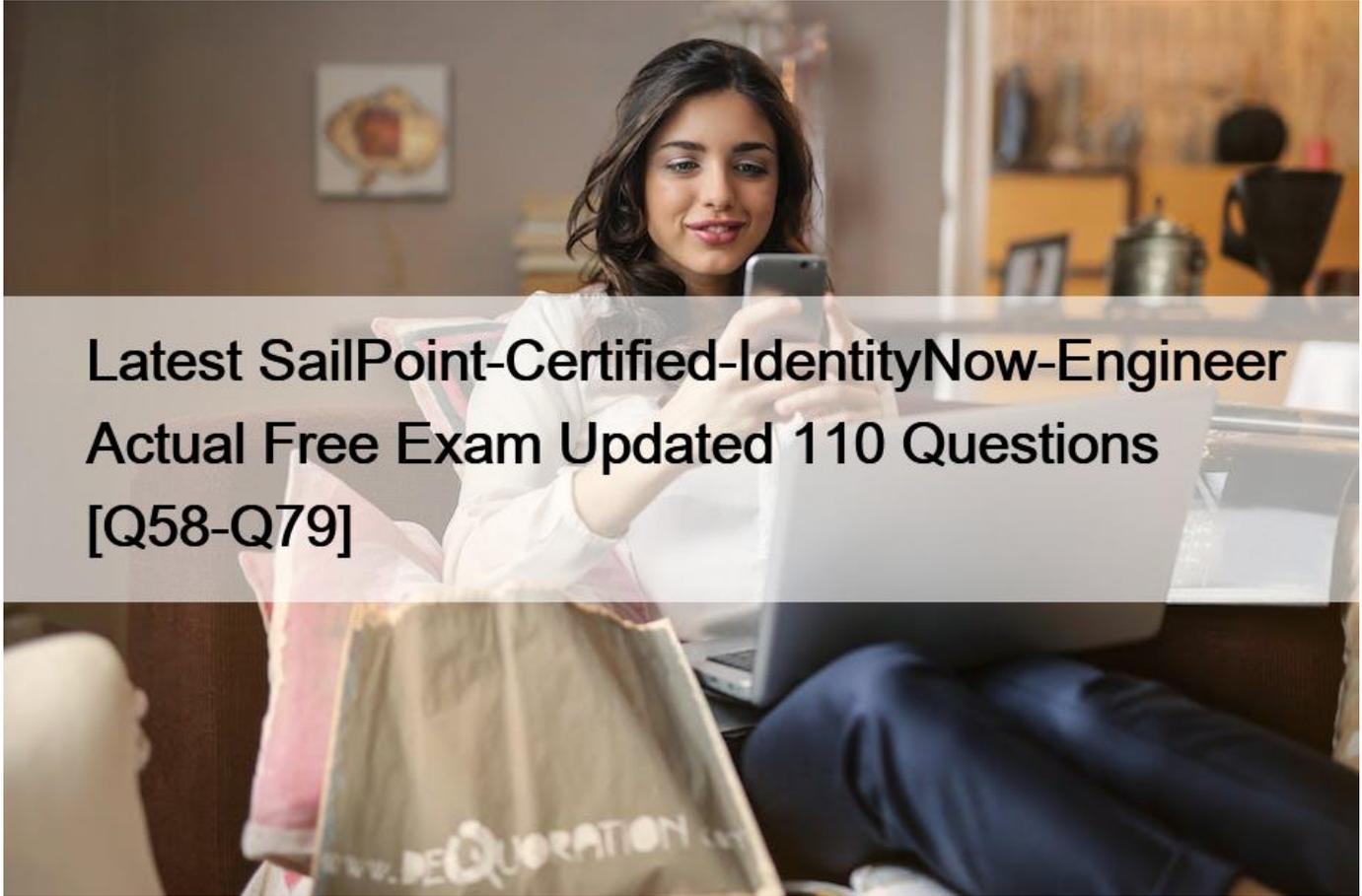


Latest SailPoint-Certified-IdentityNow-Engineer Actual Free Exam Updated 110 Questions [Q58-Q79]



Latest SailPoint-Certified-IdentityNow-Engineer Actual Free Exam Updated 110 Questions [Q58-Q79]

Latest SailPoint-Certified-IdentityNow-Engineer Actual Free Exam Updated 110 Questions
Online Questions - Valid Practice SailPoint-Certified-IdentityNow-Engineer Exam Dumps Test Questions

NO.58 When preparing for a manager certification campaign is this a step that is considered a best practice before the campaign preview is generated?

Solution: validate the email template. Certification Due

- * Yes
- * No

Yes, validating the email template (e.g., Certification Due) is a best practice before the campaign preview is generated. Communication during a certification campaign is key to ensuring that managers are aware of their tasks and deadlines. Validating the email templates helps ensure that the messaging is clear, correct, and aligned with the campaign's objectives. It also ensures that any necessary details, such as deadlines, instructions, and links to the certification tasks, are properly included.

Proper validation of email templates helps avoid communication issues that could delay or negatively impact the campaign's success.

Reference:

SailPoint IdentityNow Certification Campaign Email Templates Guide.

SailPoint IdentityNow Best Practices for Campaign Communication.

NO.59 Is this statement accurate regarding SailPoint's multi-tenant processing environment?

Solution: identityNow admins have the option to choose how often updates to their tenant occur.

* Yes

* No

No, IdentityNow administrators do not have the option to choose how often updates to their tenant occur. As part of SailPoint's multi-tenant SaaS platform, updates are managed and controlled by SailPoint and are pushed out automatically to all tenants. Administrators do not have the ability to schedule or defer updates, as this ensures all customers are running on the latest and most secure version of the software.

Reference:

SailPoint IdentityNow SaaS Release and Update Policy.

SailPoint IdentityNow Multi-Tenant Environment Overview.

NO.60 Does this example accurately describe an IdentityNow data flow?

Solution:

1. The IdentityNow engineer logs into the virtual appliance and creates a new identity profile.
2. The virtual appliance contacts the IdentityNow tenant to synchronize the identity profile.
3. The IdentityNow tenant provisions accounts to source systems.
4. The IdentityNow tenant sends an API call to the virtual appliance with confirmation that accounts were provisioned

* Yes

* No

No, this example does not accurately describe an IdentityNow data flow. The incorrect part of this flow is that identity profiles are not created within the Virtual Appliance (VA). Identity profiles are created and managed directly within the IdentityNow tenant, not the VA. Additionally, the provisioning process is handled by the IdentityNow tenant through provisioning tasks and API calls to the VA for execution, but the VA does not initiate identity profile creation or manage the full synchronization of those profiles.

Reference:

SailPoint IdentityNow Identity Profile Configuration Guide.

SailPoint IdentityNow Virtual Appliance and Tenant Data Flow Documentation.

NO.61 Is this statement true?

Solution: All emails generated from a tenant go to the intended recipient by default.

* Yes

* No

By default, not all emails generated from a SailPoint IdentityNow tenant are sent directly to the intended recipient. SailPoint IdentityNow provides an email testing mode (sandbox mode) where emails generated from the platform, such as access request notifications or password reset messages, can be routed to a specified test recipient instead of the actual intended users. This feature is commonly used during implementation or testing phases to verify email content and delivery without impacting real users.

Once the system is out of the testing phase and the email routing rules are removed, emails will be sent directly to their intended recipients. This ensures that email communications during testing do not reach end users prematurely.

Key Reference from SailPoint Documentation:

Testing Mode for Email Routing in IdentityNow: IdentityNow allows administrators to configure an email routing setting where all emails can be sent to a test inbox to ensure that email communications are functioning properly before going live to end users.

NO.62 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'.

* Yes

* No

Yes, it is possible to remove the approval requirement for an application in IdentityNow by editing the access profile and unchecking the 'Required Approval' box. This configuration change would eliminate the need for a manager or other approver to review access requests, allowing users to be granted access without requiring approval.

Key Reference from SailPoint Documentation:

Access Profile Configuration: Access profiles can be configured to require or not require approval for access requests, and this option can be modified directly in the profile settings.

NO.63 Is the following true about the web-services connector in IdentityNow?

Solution: The connector only supports JSON content-types.

* No

* Yes

The Web Services connector in IdentityNow does not exclusively support JSON content-types; it also supports XML as a content type for communication. JSON (JavaScript Object Notation) is widely used, but the connector is flexible and can be configured to handle XML-based APIs as well, depending on the requirements of the target system. Thus, it does not only support JSON.

Reference:

SailPoint IdentityNow Web Services Connector Documentation.

SailPoint IdentityNow Web Services Connector Content-Type Configuration Guide.

NO.64 Is the following true about custom connectors in IdentityNow?

Solution: Custom connector configurations can have account correlation settings defined.

- * Yes
- * No

Yes, custom connector configurations in SailPoint IdentityNow can have account correlation settings defined. Account correlation is used to link accounts from different sources to the correct identity in IdentityNow. When configuring a custom connector, it is possible to define how accounts from the connected system are correlated to existing identities based on attributes like usernames or other unique identifiers.

Key Reference from SailPoint Documentation:

Custom Connector Configuration: SailPoint allows for the definition of account correlation settings in custom connectors to ensure proper linking of external accounts to internal identities.

NO.65 An IdentityNow engineer has the following problem:

An identity is listed under Identities with Errors.

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

Solution: Check for missing lastname, email, or uid attributes.

- * Yes
- * No

Yes, checking for missing critical attributes like lastname, email, or uid is a valid step when troubleshooting an identity listed under [Identities with Errors](#) in SailPoint IdentityNow. These attributes are often required for proper identity processing, synchronization, and provisioning. If any of these attributes are missing or incorrectly configured, it could result in errors, preventing the identity from being fully processed by the system.

Key Reference from SailPoint Documentation:

Identity Attributes and Error Handling: SailPoint IdentityNow requires certain core identity attributes (such as lastname, email, uid) to be present and correctly populated. Missing or invalid values for these attributes can lead to errors and prevent identity synchronization or provisioning.

NO.66 Is this statement accurate regarding SailPoint's multi-tenant processing environment?

Solution: Updates are rolled out on a continuous basis, which allows for rapid development and deployment of new features, security updates, and bug fixes.

- * Yes
- * No

Yes, SailPoint follows a continuous delivery and rolling update model for IdentityNow, which allows for the rapid development and deployment of new features, security updates, and bug fixes. Updates are rolled out automatically to tenants as part of this process, ensuring that customers always have the latest version of the platform. This continuous approach minimizes downtime and allows SailPoint to address security vulnerabilities and improve functionality in a timely manner.

Reference:

SailPoint IdentityNow Continuous Delivery and Deployment Documentation.

SailPoint IdentityNow Release Management and Update Policy Guide.

NO.67 Is this statement true about deploying and configuring IdentityNow's virtual appliance (VA)?

Solution: When using the AWS deployment option, SailPoint shares an AWS Amazon Machine image (AMI) with the customer's AWS account on a region they select.

- * Yes
- * No

Yes, when using the AWS deployment option, SailPoint shares an Amazon Machine Image (AMI) with the customer's AWS account in the selected region. This AMI contains the pre-configured Virtual Appliance (VA) image that the customer can use to deploy within their own AWS environment, simplifying the deployment process and ensuring compatibility with AWS services.

Key Reference from SailPoint Documentation:

AWS AMI for VA Deployment: SailPoint provides a dedicated AMI that is shared with customers in their chosen AWS region to facilitate the deployment of the Virtual Appliance.

NO.68 Is this an example of a vanity URL?

Solution: <https://identityNowacme.com>

- * Yes
- * No

<https://identityNowacme.com> is not typically considered a vanity URL. While it includes the

identityNow term, it does not appear to follow the format of a vanity URL, which generally includes a company-specific subdomain (like my) and a custom domain (example.com). In this case, the URL is more generic and lacks the branding or simplicity typically associated with vanity URLs.

Key Reference from SailPoint Documentation:

Vanity URL Structure in IdentityNow: Vanity URLs typically feature a customized subdomain that reflects the organization's branding, and identityNowacme.com does not fit this pattern.

NO.69 In an IdentityNow environment, the source last connection is failing with a timeout error.

Is this a step an identityNow engineer should take to troubleshoot the problem?

Solution: Turn off the virtual appliance's (VA) internal firewall.

- * Yes
- * No

Turning off the Virtual Appliance's (VA) internal firewall is not recommended as a standard troubleshooting step in SailPoint IdentityNow. The VA's firewall is crucial for maintaining the security of the environment, and disabling it can expose the system to unnecessary risks. Instead, an IdentityNow engineer should verify the VA's network configuration and ensure that the required ports are open for communication between the VA and the source.

Key Reference from SailPoint Documentation:

VA Configuration and Network Troubleshooting: Troubleshooting connection issues typically involves checking network connectivity and firewall rules, not turning off the internal firewall.

NO.70 Is this statement true about certification campaigns?

Solution: A certification item can be reassigned multiple times.

- * Yes
- * No

Yes, a certification item can be reassigned multiple times during a certification campaign. If a reviewer is unable to certify an item or needs another individual to review the access, they can reassign the certification to a different reviewer. This reassignment functionality allows flexibility in handling access certifications and ensuring the right person evaluates the access. There are no limits on how many times an item can be reassigned, making it a versatile feature within the certification process.

Reference:

[SailPoint IdentityNow Certification Reassignment Feature Documentation.](#)

[SailPoint IdentityNow Certification Workflow Guide.](#)

NO.71 Is this statement true about using the IdentityNow APIs?

Solution: The APIs are authenticated using a client-certificate.

- * Yes
- * No

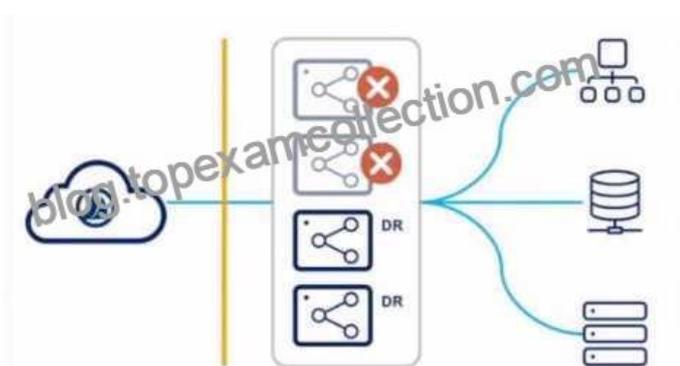
SailPoint IdentityNow APIs are not authenticated using client certificates. Instead, they use OAuth

2.0 for secure authentication and authorization. API consumers are required to obtain an access token, which is used to authenticate requests made to the IdentityNow API. The token is typically obtained by sending client credentials (client ID and client secret) to the IdentityNow authorization server, which grants the token for API access.

Key Reference from SailPoint Documentation:

API Authentication: SailPoint IdentityNow uses OAuth 2.0 for API authentication rather than client certificates. Detailed steps on how to implement OAuth-based authentication are available in [SailPoint's API documentation](#).

NO.72 Refer to the following diagram.



For this strategy, all virtual appliances (VAs) are deployed in a single VA cluster, with all VAs running concurrently. Some of these VAs are in the primary data center, and others (called OR VAs) are deployed in a DR data center.

While using this strategy, is this a disadvantage?

Solution: A reconfiguration will be required within IdentityNow to connect to the disaster recovery VAs. If there are many sources configured, this will cause overhead in performing this failover

- * Yes
- * No

No, reconfiguration within IdentityNow is not required to connect to the disaster recovery (DR) VAs, which makes this scenario not a disadvantage. When properly configured, all VAs (including DR VAs) in a cluster are part of the same logical unit, meaning that failover to the DR VAs should happen seamlessly without manual intervention or significant reconfiguration. IdentityNow handles the failover automatically, directing traffic to the DR VAs when primary VAs become unavailable.

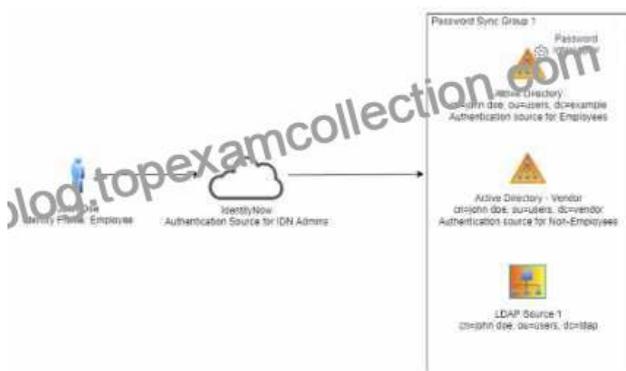
While there might be some overhead in a manual failover scenario for certain configurations, the use of a single VA cluster helps mitigate this by ensuring the system can failover without needing complex reconfigurations for every source.

Reference:

SailPoint IdentityNow Virtual Appliance Failover and Disaster Recovery Configuration.

SailPoint IdentityNow High Availability Architecture Guide.

NO.73 Review the current identity model and scenario below.



Scenario

John Doe requests access to Salesforce for himself. In the approval process, John Doe's manager approves. The access request is still the expected provisioning action sent to the source connectors?

Solution: Expected Provisioning No provisioning is sent out.

- * Yes
- * No

In SailPoint IdentityNow, provisioning is the process of granting or revoking access to systems and applications based on access requests or changes in user identity attributes. The scenario describes John Doe requesting access to the Salesforce profile in Salesforce, which is approved by his manager.

However, simply approving an access request does not automatically trigger provisioning unless specific conditions are met:

Provisioning Policy: For the access to be provisioned, SailPoint IdentityNow requires a provisioning policy that defines the action to be taken after the approval process. This policy is often configured to specify whether access should be granted or denied after

approval. If no provisioning policy is linked to the requested access, no action will be triggered.

Source Configuration: The Salesforce source (connector) in SailPoint IdentityNow must also be properly configured to handle provisioning tasks. Without proper configuration of the Salesforce source, no provisioning action will be sent even if the request is approved.

Manual Provisioning Workflow: In some cases, IdentityNow might be configured to require manual intervention after approval (e.g., triggering a manual provisioning workflow or an additional step) to enforce the provisioning action. If this configuration is missing, the approved request will not lead to automatic provisioning.

Since the scenario does not explicitly state that a provisioning policy or source configuration exists to handle the access request, the correct conclusion is that no provisioning would be sent out.

Key Reference from SailPoint Documentation:

Provisioning Concepts in IdentityNow: Documentation emphasizes that provisioning is triggered by defined workflows and provisioning policies that link the request to the connector source. Without these, the approval does not lead to actual provisioning.

NO.74 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: /home/sailpoint/config.yaml

* Yes

* No

The /home/sailpoint/config.yaml file is not used to configure the Virtual Appliance (VA) to use a static IP address. This file is generally used for other configuration purposes related to the SailPoint IdentityNow application settings, not for network configurations like setting static IP addresses.

Network configurations are handled at the system or network service level within the VA's Linux environment.

Reference:

SailPoint IdentityNow Virtual Appliance Configuration Guide.

SailPoint IdentityNow Networking Configuration Documentation.

NO.75 An IdentityNow engineer needs to review logs to diagnose when the secure tunnel fails to allow communication. Could reviewing this log file help diagnose the issue?

Solution: /home/sailpoint/log/vs_agent.log

* Yes

* No

No, the vs_agent.log file is not typically used to diagnose secure tunnel communication issues. The vs_agent.log file is related to virtual appliance services and tasks but does not provide detailed information about the secure tunnel or communication errors. For troubleshooting the secure tunnel, the relay.log file is more appropriate.

Key Reference from SailPoint Documentation:

Log File Purposes: The vs_agent.log does not capture information about secure tunnel communication issues. Instead, the relay.log is the correct log file for such issues.

NO.76 Is the following description of an access profile correct?

Solution: it can be acknowledged during certifications.

- * Yes
- * No

Yes, an access profile can be acknowledged during certifications. During access certification campaigns, reviewers can review access profiles as part of the items that need to be certified. They can either approve or revoke access to the access profiles, just like they would with individual entitlements. This ensures that users' access to these bundled entitlements is regularly reviewed and compliant with organizational policies.

Reference:

SailPoint IdentityNow Certification Campaigns Guide.

SailPoint IdentityNow Access Profile Certification Documentation.

NO.77 Does the following use case accurately describe provisioning on a source that has provisioning disabled?

Solution: Provisioning is initiated by a process (e.g. Access Request Role Assignments). Provisioning instructions are calculated based on current access, and go through filtering and expansion processes. Provisioning is then assigned to a source for provisioning. A virtual appliance retries the provisioning request and carries out the provisioning via the connector. The results are communicated back to identityNow.

- * Yes
- * No

The provided use case incorrectly describes the provisioning process on a source that has provisioning disabled. If provisioning is disabled for a source, automated provisioning via the Virtual Appliance and connectors is not possible. The Virtual Appliance cannot retry or carry out the provisioning in this case, as the system explicitly prevents automated provisioning operations on sources marked as non-provisionable.

When a source has provisioning disabled, the system only supports manual provisioning, where a task is opened in IdentityNow for a person to manually execute the provisioning steps. The Virtual Appliance does not handle provisioning for disabled sources, so the described scenario where it retries the request and carries out provisioning is inaccurate.

Reference:

SailPoint IdentityNow Provisioning Configuration Guide.

SailPoint IdentityNow Virtual Appliance and Connector Operations Documentation.

NO.78 An engineer needs to troubleshoot the following issue:

Incomplete Identities on authoritative source

Is this a reasonable action for the engineer to take?

Solution: Review the identities without Managers report.

- * Yes
- * No

Reviewing the Identities without Managers report is not directly related to troubleshooting incomplete identities on an authoritative

source. The 'Identities without Managers' report is specifically useful for identifying identities that are missing a manager assignment, which might be relevant for access reviews or other management-related tasks. However, when troubleshooting incomplete identities, the focus is typically on missing attributes or data mappings, not the manager attribute specifically.

Therefore, this report is not the most appropriate action for this particular issue.

Reference:

SailPoint IdentityNow Reporting and Identity Data Review Documentation.

SailPoint IdentityNow Troubleshooting Incomplete Identities.

NO.79 Is this an item that an IdentityNow engineer should configure when implementing a source that uses a JDBC connector?

Solution: This item is complete

* Yes

* No

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.

Reference:

SailPoint IdentityNow JDBC Connector Implementation Checklist.

SailPoint IdentityNow Configuration and Implementation Documentation.

SailPoint-Certified-IdentityNow-Engineer Exam PDF [2025 Tests Free Updated Today with Correct 110 Questions:
<https://www.topexamcollection.com/SailPoint-Certified-IdentityNow-Engineer-vce-collection.html>]