



Saviynt SCAIP Practice Questions

Shared by Waller on 08-10-2026

For More Free Questions and Preparation Resources

Check the Links on Last Page



Question 1

Question Type: MultipleChoice

Which User Update Rule action is used to automatically change service account ownership when the current owner is terminated?

Options:

- A- Transfer Ownership
- B- Run Role Mining
- C- Launch Campaign
- D- Disable SMTP



Answer:

A

Explanation:

The correct answer is A. Transfer Ownership. Saviynt documentation on User Update Rules explains that the purpose of Transfer Ownership is to change ownership, and specifically notes that service accounts can be reassigned to the OwnerOnTerminate user when the current owner is terminated. The documentation further states that when the current service account owner is terminated, a user update rule with the action Transfer Ownership is triggered so that service account ownership is moved appropriately. This directly matches the scenario in the question.

This is also consistent with Saviynt's service account model, where every service account must have at least one designated owner who is authorized to manage it. Because ownership is required, Saviynt provides lifecycle controls to preserve accountable ownership when a human owner leaves the organization. The remaining options are unrelated. Run Role Mining belongs to analytics and role engineering, Launch Campaign belongs to certification processes, and Disable SMTP is an email configuration concept. For Level 200 understanding, the key takeaway is that automatic service account ownership continuity is handled through a User Update Rule using the Transfer Ownership action, often combined with OwnerOnTerminate configuration.

Question 2

Question Type: MultipleChoice

What configuration types are needed to set up an emergency access role request?

Options:

- A- Select emergency access related parameters in the Role-level Configurations
- B- All the above
- C- Select required feature access in SAV Role Configurations
- D- Select a workflow under Global Configurations

Answer:

B

Explanation:

Setting up an Emergency Access Role (EAR) request in Saviynt EIC requires multiple coordinated configurations across different components of the system. Option A is correct because emergency access roles must be configured at the role level, where parameters such as emergency access flag, duration, justification requirement, and elevated privileges are defined.

Option C is also necessary because SAV Role Configurations control which users (such as administrators or requesters) have the ability to request or manage emergency access roles. Without proper SAV role permissions, users cannot initiate or approve EAR requests.

Option D is equally important because workflows defined under Global Configurations govern the approval process, escalation paths, and auditing requirements for emergency access. These workflows ensure that emergency access is properly controlled, reviewed, and revoked after use.

Since all these configurations collectively enable emergency access functionality in Saviynt, the correct answer is All the above. This aligns with Saviynt best practices for implementing secure, auditable, and compliant emergency access management.

Question 3

Question Type: MultipleChoice

What are the different actions available while using the Duplicate Identity Management (DIM) feature?

Options:

- A- Detect duplicates before importing identities or within existing identities
- B- Perform a side-by-side comparison of ambiguous duplicates
- C- Deactivate the duplicate identity after the merge process
- D- The existing user is updated and satisfies a user update rule with action as Re-run provisioning rules

Answer:

D

Explanation:

Saviynt's Duplicate Identity Management (DIM) feature is designed to identify, analyze, and remediate duplicate identities within the Identity Repository, ensuring data integrity and governance. All the listed actions are core capabilities of DIM, making Option D (All of the Above) the correct answer.

Firstly, DIM enables duplicate detection both during identity import (pre-processing stage) and for already existing identities using detective jobs. This ensures that duplicates are identified proactively and retrospectively. Secondly, DIM provides a side-by-side comparison view, allowing administrators or reviewers to analyze ambiguous duplicate records and decide whether they should be merged. This comparison highlights attribute-level differences for informed decision-making.

Finally, after merging duplicate identities, Saviynt allows administrators to deactivate or retire redundant identities, ensuring only a single authoritative identity remains active. This helps maintain clean identity data and prevents access risks.

Together, these features support identity consolidation, reduce redundancy, and improve overall governance, making DIM a critical component of Saviynt's intelligence and analytics capabilities.

Question 4

Question Type: MultipleChoice

The EIC Administrator observed that all accounts were disabled in Saviynt due to incorrect configuration in the target application. What controls can be implemented in Saviynt to avoid such scenarios?

Options:

- A- Use the accEntThresholdValue attribute in the STATUS_THRESHOLD_CONFIG connection parameter
- B- It is not possible to set a limit
- C- Set the limit in the external config file
- D- Use the accountThresholdValue attribute in the STATUS_THRESHOLD_CONFIG connection parameter

Answer:

D

Explanation:

In Saviynt EIC, mass unintended changes---such as all accounts being disabled due to incorrect target application configuration---can be prevented using threshold-based controls. These controls are defined using the STATUS_THRESHOLD_CONFIG connection parameter, which acts as a safeguard during reconciliation and provisioning processes.

The correct attribute in this scenario is accountThresholdValue (Option D). This parameter allows administrators to define a threshold limit for account status changes (such as disablement). If the number or percentage of accounts being disabled exceeds the defined threshold, Saviynt can stop or flag the operation, preventing large-scale unintended impact.

Option A (accEntThresholdValue) is used for entitlement-level thresholds, not account status changes. Option B is incorrect because Saviynt does provide this safeguard mechanism. Option C is also incorrect since such controls are not managed externally but are part of Saviynt's connector configuration.

By using accountThresholdValue within STATUS_THRESHOLD_CONFIG, organizations can implement strong governance and prevent bulk account disablement due to misconfigurations or data issues during account import or reconciliation.

Question 5

Question Type: MultipleChoice

EIC Admin encounters an error "Connection Name Specified in accountJSON is not found" while running the WSRETRY job. Which JSON needs to be corrected?

Options:

- A- Update the correct connection name in CreateAccountJSON
- B- Update the correct connection name in ImportUserJSON

- C- Update the correct connection name in ImportAccountEntJSON
- D- Update the correct connection name in ImportAccountJSON

Answer:

D

Explanation:

The error message 'Connection Name Specified in accountJSON is not found' clearly indicates that the issue is related to the accountJSON configuration, which directly corresponds to ImportAccountJSON in Saviynt REST connector terminology. This JSON is responsible for handling account import (reconciliation) operations, including defining the connection name, API endpoints, and parsing logic for retrieving account data.

The WSRETRY job is typically used to retry failed web service (REST) operations, especially related to account imports or provisioning failures. Since the error explicitly references accountJSON, it means the system is unable to locate the connection name defined within the ImportAccountJSON configuration. This usually happens when the connection name is either misspelled, mismatched with the ConnectionJSON configuration, or incorrectly referenced.

Other options are incorrect because CreateAccountJSON is used for provisioning (account creation), ImportUserJSON is for identity import, and ImportAccountEntJSON is primarily used for entitlement and combined account-entitlement imports.

Therefore, correcting the connection name in ImportAccountJSON resolves this issue.

Question 6

Question Type: MultipleChoice

Which option best statements are correct? (Multi-Select)

Options:

- A- The role mining process discovers relationships between users based on similar access permissions that can logically be grouped to form a role
- B- In the Role mining, if the percentage cut-off = 60%, it would perform mining on only the access which is associated with 100% users
- C- Duplicate Identity Management feature access need to be added to the SAV Role to view the duplicate identity management
- D- Duplicate Identity Management can only merge user attributes but not user access

Answer:

A, C

Explanation:

Statement A is correct because Role Mining in Saviynt analyzes user access patterns and identifies relationships between users who share similar entitlements. These patterns are then used to logically group access into roles, enabling efficient role-based access control (RBAC) implementation and reducing manual effort in role creation.

Statement B is incorrect because a percentage cut-off (e.g., 60%) in role mining means that entitlements common to at least 60% of users are considered for role creation---not 100%. The statement incorrectly interprets how threshold-based mining works.

Statement C is correct since access to Duplicate Identity Management (DIM) features is controlled via SAV Role configurations. Administrators must grant appropriate permissions within SAV roles to allow users to view and manage duplicate identities in the system.

Statement D is incorrect because DIM supports merging not only user attributes but also associated accounts and access depending on configuration. It is not limited to attributes alone.

Thus, the correct answers are A and C.

Question 7

Question Type: MultipleChoice

The EIC administrator has a requirement for integrating EIC with ServiceNow as a ticketing system, where end users should be able to check the status of associated tickets in ServiceNow from EIC. What option can the administrator utilize to fulfill this requirement?

Options:

A- SYNCTICKETSTATUSJSON

B- CREATETICKETJSON

C- TICKETSTATUSJSON

D- It is not possible to check the status of ticket in ServiceNow

Answer:

C

Explanation:

In Saviynt EIC integration with ServiceNow as a ticketing system (ITSM), various JSON configurations are used to define how tickets are created, updated, and tracked. To enable users to check the status of tickets from EIC, the correct configuration is TICKETSTATUSJSON.

TICKETSTATUSJSON is specifically used to define how Saviynt retrieves the current status of a ticket from ServiceNow. It maps the API response fields from ServiceNow (such as state, status, or resolution) to Saviynt fields, allowing the system to display real-time ticket status within the EIC interface.

Option A (SYNCTICKETSTATUSJSON) is typically used for synchronization jobs that update ticket statuses in bulk, not for direct user-level status retrieval. Option B (CREATETICKETJSON) is used only for ticket creation, defining how requests are sent to ServiceNow. Option D is incorrect because Saviynt does support ticket status tracking through proper integration configuration.

Thus, TICKETSTATUSJSON is the correct option to enable visibility of ticket status within Saviynt EIC.

Question 8

Question Type: MultipleChoice

What are the different authentication modes supported for SMTP configurations? (Multi Choose)

Options:

- A- NTLM
- B- OAuth
- C- User can only view all EIC configurations
- D- Basic

Answer:

A, B, D

Explanation:

In Saviynt EIC, SMTP configuration is used to enable email notifications for workflows such as access requests, certifications, alerts, and system communications. To securely connect with mail servers, Saviynt supports multiple authentication mechanisms. The valid authentication

modes are NTLM, OAuth, and Basic, making Options A, B, and D correct.

Basic Authentication (Option D) is the traditional method where a username and password are used to authenticate with the SMTP server. While widely supported, it is less secure compared to modern methods and is being phased out in many environments.

NTLM (Option A) is commonly used in Microsoft-based environments (e.g., Exchange servers) and provides integrated authentication using Windows credentials, offering better security than basic authentication.

OAuth (Option B) is a modern and more secure authentication mechanism that uses token-based authorization instead of storing credentials. It is commonly used with cloud-based email services such as Microsoft 365 or Google Workspace.

Option C is incorrect because Saviynt explicitly supports multiple authentication modes.

Thus, NTLM, OAuth, and Basic are the supported SMTP authentication modes in Saviynt.

Question 9

Question Type: MultipleChoice

An EIC Administrator has created a workflow containing hidden dynamic attributes; however, the administrator is unable to fetch the value of the hidden Dynamic Attributes in the request. How can this issue be resolved?

Options:

- A- Enable the 'Expose hidden dynamic attributes in workflow' setting in Global Config
- B- Enable the 'Expose hidden dynamic attributes in workflow' setting in Endpoint
- C- Enable the 'Save Hidden Dynamic Attribute Default Value' setting in Global Config
- D- Enable the 'Enable use for default attributes in workflow' setting in Global Config

Answer:

A

Explanation:

In Saviynt EIC, Dynamic Attributes are often used in request forms to capture additional information, and some of these attributes may be configured as hidden fields for backend processing. By default, hidden dynamic attributes are not exposed in workflows, which can prevent administrators from accessing their values during request processing.

To resolve this issue, Saviynt provides a specific configuration in Global Configurations called "Expose hidden dynamic attributes in workflow". Enabling this setting (Option A) ensures that even if the dynamic attributes are hidden in the UI, their values are still accessible within workflows for processing, approvals, and provisioning logic.

Option B is incorrect because this setting is not configured at the endpoint level. Option C relates to saving default values but does not ensure visibility in workflows. Option D is unrelated to hidden attribute exposure.

Thus, enabling the Global Config setting to expose hidden dynamic attributes is the correct solution to ensure their values are available within workflow execution.

Question 10

Question Type: MultipleChoice

An EIC Administration has a requirement to configure a separate password policy for service accounts along with the password policy for regular accounts. How can this be achieved in EIC?

Options:

- A- Define a separate Password Policy for Service Account and select it in Policy Rule Service Account field under Security System
- B- Only one Password Policy can be defined in the Security System which applies to both regular and service accounts
- C- Define a separate Password Policy for Service Account and select the checkbox Password Policy Service Account field under Password Policy configurations
- D- Define a separate Password Policy for Service Account and select it in Policy Rule Service Account field under Global Configurations

Answer:

A

Explanation:

In Saviynt EIC, password management is highly configurable, allowing organizations to define separate password policies for different account types, including service accounts and regular user accounts. This requirement is achieved by creating a dedicated password policy specifically for service accounts and associating it appropriately within the system.

Option A is correct because Saviynt allows administrators to define a separate Password Policy for Service Accounts and map it using the Policy Rule Service Account field under the Security

System configuration. This ensures that when service account operations such as password resets or provisioning occur, the system enforces the correct policy distinct from regular user accounts.

Option B is incorrect since Saviynt supports multiple password policies and does not restrict to a single policy. Option C is incorrect because simply selecting a checkbox in password policy configuration does not link it to service account usage. Option D is incorrect as Global Configurations do not directly assign password policies for service accounts at the execution level.

Thus, configuring and mapping the policy at the Security System level ensures correct enforcement for service accounts.



Question 11

Question Type: MultipleChoice

Scenario:

John, an EIC System Administrator, encounters a situation where a user account has been compromised, and he needs to take immediate action to prevent further unauthorized access.

Given the scenario, which action should John take on EIC to prevent compromised user account access on the impacted application?

Options:

- A- Lock
- B- Suspend
- C- Expire
- D- Delete



Answer:

A

Explanation:

In Saviynt EIC, when an account is compromised and requires immediate containment, the most appropriate action is to lock the account (Option A). Locking an account ensures that the user is instantly prevented from logging into the target system without removing the account or affecting its underlying configuration. This action is reversible and allows administrators to quickly secure the account while further investigation or remediation steps (such as password

reset or access review) are performed.

Option B (Suspend) is typically used for longer-term access revocation scenarios, such as employee leave or inactivity, and may depend on application-specific configurations. Option C (Expire) relates to setting an end date for account validity, which is not suitable for immediate threat mitigation. Option D (Delete) is a permanent and destructive action, generally avoided in incident response because it removes audit trails and complicates recovery.

Therefore, locking the account aligns with Saviynt best practices for incident response and rapid risk mitigation, ensuring security without losing account traceability.



To Get Premium Files for SCAIP Visit

<https://www.p2pexams.com/products/scaip>

For More Free Questions Visit

<https://www.p2pexams.com/saviynt/pdf/scaip>

20%
DISCOUNT

P2P
exams