New Saviynt SCAIP Exam Papers, Authorized SCAIP Certification

What's more, part of that Exams4Collection SCAIP dumps now are free: https://drive.google.com/open?id=1EuwP4jKI3bXtfrSqcGe4IJG1hVGEFa_T

Success in the Saviynt Certified Advanced IGA Professional (Level 200) (SCAIP) certification exam helps people update their skills. Many aspirants don't find updated Saviynt SCAIP practice test questions and fail the final test. This failure in the Saviynt SCAIP Exam leads to a loss of money and time. If you are also planning to attempt the Saviynt Certified Advanced IGA Professional (Level 200) (SCAIP) exam and are confused about where to prepare yourself for it then you are at the right place.

Saviynt SCAIP Exam Syllabus Topics:

Topic	Details

Topic 1	• Access Reviews: This section covers the configuration and execution of access review campaigns across different reviewer types, along with campaign tracking and post-certification processes.
Topic 2	• Building Identity Warehouse: This section covers setting up the foundation of Saviynt by importing users, onboarding applications, and managing roles and access within the identity warehouse.
Topic 3	• Analytics: This section focuses on building, configuring, and delivering reports, analytic controls, and dashboards to support data-driven identity governance decisions.

Authorized SCAIP Certification, SCAIP Certification Exam Cost

It is widely accepted that where there is a will, there is a way; so to speak, a man who has a settled purpose will surely succeed. To obtain the SCAIP certificate is a wonderful and rapid way to advance your position in your career. In order to reach this goal of passing the SCAIP Exam, you need more external assistance to help yourself. With our SCAIP exam questions, you will not only get aid to gain your dreaming certification, but also you can enjoy the first-class service online.

Saviynt Certified Advanced IGA Professional (Level 200) Sample Questions (Q56-Q61):

NEW QUESTION # 56
What are the different features available under Role Intelligence? (Multi-Select)

- A. Role-Access Mismatches
- B. Role Mining
- C. Role Governance
- D. Entitlement Discovery

Answer: B,C,D

Explanation:
In Saviynt EIC,Role Intelligenceis a key component of Identity Governance that focuses on analyzing, optimizing, and managing roles effectively. It provides multiple features that help organizations improve role design and maintain compliance.
Role Governance (A)is a core feature that ensures roles are properly defined, reviewed, and certified. It helps maintain accountability and ensures that roles align with business policies.
Entitlement Discovery (B)enables identification and analysis of entitlements across applications, helping administrators understand what access exists and how it can be grouped into meaningful roles. This is essential for building accurate and efficient role models.
Role Mining (C)is one of the most important capabilities, allowing organizations to analyze user access patterns and automatically suggest roles based on common entitlement combinations. This improves role engineering and reduces manual effort.
Option D (Role-Access Mismatches) is not considered a standard feature under Role Intelligence; it is more aligned with analytics or audit findings rather than a core Role Intelligence function.
Therefore, the correct answers areA, B, and C, which represent the foundational features of Role Intelligence in Saviynt.

NEW QUESTION # 57
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?

- A. Use the accountThresholdValue 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 accEntThresholdValue attribute in the STATUS_THRESHOLD_CONFIG connection parameter

Answer: A

Explanation:

In Saviynt EIC, mass unintended changes-such as all accounts being disabled due to incorrect target application configuration-can be prevented usingthreshold-based controls. These controls are defined using theSTATUS_THRESHOLD_CONFIGconnection parameter, which acts as a safeguard during reconciliation and provisioning processes.
The correct attribute in this scenario isaccountThresholdValue (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.
OptionA (accEntThresholdValue)is used for entitlement-level thresholds, not account status changes.
OptionBis incorrect because Saviynt does provide this safeguard mechanism. OptionCis also incorrect since such controls are not managed externally but are part of Saviynt's connector configuration.
By usingaccountThresholdValuewithin STATUS_THRESHOLD_CONFIG, organizations can implement strong governance and prevent bulk account disablement due to misconfigurations or data issues during account import or reconciliation.

NEW QUESTION # 58
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?

- A. CREATETICKETJSON
- B. SYNCTICKETSTATUSJSON
- C. It is not possible to check the status of ticket in ServiceNow
- D. TICKETSTATUSJSON

Answer: D

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 tocheck the status of tickets from EIC, the correct configuration isTICKETSTATUSJSON.
TICKETSTATUSJSONis 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,TICKETSTATUSJSONis the correct option to enable visibility of ticket status within Saviynt EIC.

NEW QUESTION # 59
Which of the following options are True with respect to Password Policy in EIC? (Multi-Select)

- A. When a password policy is configured at both the security system and connector, the password policy assigned to the connector takes precedence and is applied
- B. When a password policy is configured at both the security system and connector, the password policy assigned to the security system takes precedence and is applied
- C. If you want to restrict the password change for users for a particular endpoint, you can configure "Change Password Access Query" in the endpoint
- D. If a password policy is defined only at the connector, the password policy configured at the connector will be applied

Answer: B,C,D

Explanation:
In Saviynt EIC,Password Policy precedence and enforcementdepend on where the policy is configured within the hierarchy of Security System and Connector.
Option A is correct because when password policies are defined at both levels, theSecurity System-level policy takes precedence. This ensures centralized governance and consistency across all endpoints under that security system.
Option B is also correct since Saviynt allows administrators to control password change permissions at a granular level using the"Change Password Access Query"at the endpoint. This enables restriction of password changes based on user attributes or conditions.
Option C is incorrect because connector-level policies do not override security system-level configurations when both are present.
Option D is correct because if no policy is defined at the security system level, theconnector-level password policy will be applied by default, ensuring that password rules are still enforced.

Thus, the correct answers areA, B, and D, reflecting Saviynt's hierarchical and flexible password policy framework.

NEW QUESTION # 60
What are the different features available under Role Intelligence? (Multi-Select)

- A. Role-Access Mismatches
- B. Role Mining
- C. Role Governance
- D. Entitlement Discovery

Answer: B,C,D

NEW QUESTION # 61
.....

Do you want to find a job that really fulfills your ambitions? That's because you haven't found an opportunity to improve your ability to lay a solid foundation for a good career. Our SCAIP learning materials are carefully compiled by industry experts based on the examination questions and industry trends in the past few years. The knowledge points are comprehensive and focused. You don't have to worry about our learning from SCAIP Exam Question. We assure you that our SCAIP learning materials are easy to understand and use the fewest questions to convey the most important information.