KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **SCAIP**

Title : Saviynt Certified Advanced IGA Professional (Level 200)

Version : DEMO

1.An EIC Administrator has a requirement to filter the list of roles based on user location, for example: A user from country A should be able to request only roles for country A.
What configuration administrator can use here?
A. SAV Role
B. Global Configuration -> Role Request Query
C. Role Configuration -> User Query
D. Role cannot be filtered based on user attribute
Answer: B
Explanation:
In Saviynt EIC, the correct configuration for controlling which roles appear in the Access Request screen is the Request Roles Query / Role Request Query under Global Configuration. Saviynt's official documentation for Configuring Role Requests states that this setting is used to specify a query to control the display of roles in Access Request, meaning only roles returned by that query are shown to the requester. That is exactly the use case in this question: filtering the visible role list by a user attribute such as country or location. A query can be written so that users from Country A see only the roles mapped for Country A.
The other options are not correct in this context. SAV Role controls administrative UI permissions in Saviynt, not end-user role catalog filtering. Role Configuration -> User Query is not the standard setting used to drive request-time role visibility for this scenario.
Option D is incorrect because Saviynt explicitly supports this use case through the Request Roles Query capability.

2.Problem Statement:
Access request approval is not being assigned to the correct approver for a given endpoint.
In this scenario, what configurations will you check? (Multi-Select)
A. Verify the workflow attached to the corresponding Endpoint to ensure it is correctly configured
B. Verify if Delegate is configured for the intended approver
C. Verify the workflow attached to the corresponding Security System to ensure it is correctly configured
D. Verify the requestor selected the correct approver while submitting the request
Answer: A,B,C
Explanation:
In Saviynt EIC, approval assignment for access requests is primarily controlled through workflow configurations, which are associated either at the endpoint level or security system level. Therefore, the first step in troubleshooting incorrect approver assignment is to validate whether the correct workflow is attached and properly configured at both levels (Options A and C). Workflows define approval logic such as manager, owner, or custom approvers, and misconfiguration here often leads to incorrect routing.
Option B is also correct because delegation settings can override the intended approver. If a delegate is configured for an approver, the request may be routed to the delegate instead of the original approver, causing confusion if not validated.
Option D is incorrect because in Saviynt, approvers are typically system-driven based on workflow rules, not manually selected by the requester in most standard configurations. The requester does not usually control approver assignment unless explicitly customized, making this option irrelevant for standard troubleshooting.

3.Which statement correctly describes the two major ServiceNow integration modes supported by Saviynt?
A. ServiceNow as a Managed Application supports import, provisioning, and deprovisioning; ServiceNow as a Ticketing System supports ticket-based ITSM integration.
B. ServiceNow as a Managed Application is only for branding and labels; ServiceNow as a Ticketing System is only for analytics.
C. ServiceNow as a Managed Application is used only for SAV roles; ServiceNow as a Ticketing System is used only for password sync.
D. Both modes are the same and serve identical purposes.
Answer: A
Explanation:
The correct answer is A. Saviynt documentation describes two major ServiceNow integration models: ServiceNow as a Managed Application and ServiceNow as a Ticketing System. The managed application model is used for application-style integration, including reconciliation or import and provisioning or deprovisioning activities. The ticketing system model is used when ServiceNow functions as the ITSM workflow and ticket platform connected to Saviynt request processing. This distinction is repeatedly emphasized in the ServiceNow integration overview documentation.
Saviynt further notes that integration with ServiceNow is required to perform reconciliation, provisioning, and deprovisioning tasks, and separately documents ServiceNow as a ticketing system for request-related use cases. That means the two modes are complementary but not identical.
Option D is therefore wrong because the modes serve different architectural purposes.
Options B and C are incorrect because branding, analytics-only usage, SAV-role-only usage, and password-sync-only behavior do not describe the documented ServiceNow integration patterns. For Level 200 exam preparation, this is a high-value distinction: choose Managed Application when ServiceNow is the governed target system, and Ticketing System when ServiceNow is the ITSM workflow engine around Saviynt processes

4.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?
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.

5.What configuration types are needed to set up an emergency access role request?
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 isAll the above. This aligns with Saviynt best practices for implementing secure, auditable, and compliant emergency access management.