

Pass Guaranteed Quiz SAVIGA-C01 - Accurate Valid Dumps Saviynt IGA Certified Professional Exam (L100) Questions



Saviynt SAVIGA-C01

Saviynt Certified IGA Professional Exam (L100) Exam

For More Information – Visit link below:

<https://www.examsempire.com/>

Product Version

1. Up to Date products, reliable and verified.
2. Questions and Answers in PDF Format.



<https://examsempire.com/>

Visit us at: <https://www.examsempire.com/saviga-c01>

What's more, part of that Actual4Labs SAVIGA-C01 dumps now are free: https://drive.google.com/open?id=1_3th6lxmoptvqr9B8ozULfhUFXzCPJPK

In the present society, the workplace is extremely cruel. There is no skill, no certificate, and even if you say it admirably, it is useless. If you want to work, you must get a SAVIGA-C01 certificate. The certificate is like a stepping stone. It is the key to the unimpeded workplace and the cornerstone of value. And our SAVIGA-C01 study braindumps will help you pass the exam and get the certification with the least time and efforts. Just buy our SAVIGA-C01 learning question if you want to be successful!

Saviynt SAVIGA-C01 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• Implement IGA Solutions: This section focuses on the practical implementation of IGA solutions using Saviynt. It covers project planning, requirements gathering, and solution design. Saviynt IGA Administrators should be able to translate business needs into technical solutions.
Topic 2	<ul style="list-style-type: none">• Analytics: Saviynt IGA Administrators are expected to demonstrate knowledge of analytics capabilities in the Saviynt IGA platform. This section covers reporting, dashboards, and data analysis techniques.

Topic 3	<ul style="list-style-type: none"> • Saviynt IGA Implementation: This section focuses on the implementation aspects of Saviynt IGA solutions. It covers deployment strategies, integration with existing systems, and customization techniques.
Topic 4	<ul style="list-style-type: none"> • Saviynt IGA Administration: Saviynt IGA Administrators are expected to demonstrate proficiency in administering the Saviynt IGA platform. This section covers user management, role management, and system configuration.
Topic 5	<ul style="list-style-type: none"> • SoDs: Saviynt IGA Administrators are expected to demonstrate proficiency in Segregation of Duties (SoD) management. This section covers SoD rule creation, conflict detection, and mitigation strategies.
Topic 6	<ul style="list-style-type: none"> • Identity Warehouse: Saviynt IGA Professionals are expected to showcase their understanding of the Identity Warehouse concept in this section. It covers data modeling, identity reconciliation, and data synchronization.

>> Valid Dumps SAVIGA-C01 Questions <<

Latest SAVIGA-C01 Exam Topics & Sample SAVIGA-C01 Test Online

In order to cater to meet different needs of our customers, three versions of SAVIGA-C01 exam bootcamp are available. Each version has its own advantages, and you can choose the most suitable one in accordance with your needs. Furthermore, SAVIGA-C01 exam bootcamp is compiled by outstanding experts, therefore the quality and the accuracy can be guaranteed. Besides, we have the professional technicians to examine the website on a regular basis, hence a clean and safe shopping environment will be provided to you. You just need to buy the SAVIGA-C01 Exam Dumps with ease.

Saviynt IGA Certified Professional Exam (L100) Sample Questions (Q32-Q37):

NEW QUESTION # 32

If you want an application to be available for requesting access (self or other), which of the following should be configured?

- A. Proposed Accounts Workflow
- B. Emergency Access ID Request Workflow
- C. Access Remove Workflow
- **D. Access Add Workflow**

Answer: D

Explanation:

To make an application available for access requests (either self-service or requests for others), the Access Add Workflow needs to be configured within Saviynt. This workflow defines the process that governs how access to the application is granted. Here's a breakdown with Saviynt IGA references:

* Saviynt's Access Request System (ARS): This is the module within Saviynt that handles access requests. The ARS relies on defined workflows to manage the approval and provisioning process.

* Access Add Workflow: This specific type of workflow within Saviynt's ARS is triggered when a user requests access to an application or entitlement. It dictates the steps involved, such as:

* Requester Details: Capturing information about who is requesting access.

* Application/Entitlement Selection: The user selects the application (and potentially specific roles or entitlements within that application) for which they are requesting access.

* Approval Routing: Defining the approval chain (e.g., manager approval, application owner approval, etc.). This is configured within the workflow using various approval activities.

* Provisioning: Upon approval, the workflow can trigger automated provisioning of access to the target system (if connected integration is set up).

* Saviynt's Application Onboarding: For an application to be available in the ARS, it needs to be onboarded into Saviynt. During this process, you would typically define the relevant entitlements (access rights) associated with the application.

* Workflow Configuration in Saviynt: Saviynt's admin interface allows administrators to create and customize workflows using a visual designer. This includes setting up conditions, defining approval steps, and configuring actions to be taken at each stage of the workflow.

- * Other options:
- * Proposed Accounts Workflow: This is less common, often used to suggest potential accounts during the request or account creation process. It's not the primary mechanism for making an application available for access requests.
- * Access Remove Workflow: This workflow is used when access needs to be revoked, not granted.
- * Emergency Access ID Request Workflow: This workflow is specific to requesting temporary, elevated access in emergency situations. It's not the workflow for general access requests to applications.

NEW QUESTION # 33

Which of the following options is part of the Saviynt Identity Repository?

- A. Users, Identity Rules, Workflows, Roles
- **B. Users, Accounts, Entitlements, Roles**
- C. Users, Accounts, Entitlements, Workflows
- D. Users, User Groups, Workflows, SAV Roles

Answer: B

Explanation:

Saviynt's Identity Repository is the central hub for storing and managing all identity-related information. It includes:

- * Users: Representing individuals and their attributes.
- * Accounts: Representing user access to specific systems or applications.
- * Entitlements: Representing permissions and access rights within those systems.
- * Roles: Representing collections of entitlements that define job functions or responsibilities.

Why other options are incorrect:

* A, B, and D: These options include elements like Identity Rules, Workflows, and SAV Roles, which are important components of Saviynt but are not core parts of the Identity Repository itself.

Saviynt IGA References:

- * Saviynt Documentation: The section on the Identity Repository describes its function and the types of data it stores.
- * Saviynt User Interface: The Identity Repository is a key section within the Saviynt interface, where you can view and manage users, accounts, entitlements, and roles.

NEW QUESTION # 34

Which of the following objects is available in the User Update Rule to configure Rule conditions?

- A. Accounts
- B. Roles
- C. Entitlements
- **D. Users**

Answer: D

Explanation:

The object that is available in the User Update Rule to configure Rule conditions in Saviynt is A. Users.

Here's an explanation:

- * User Update Rule Purpose: As mentioned before, User Update Rules are used to automatically update user attributes based on certain conditions.
- * Condition Based on User Attributes: The conditions for triggering a User Update Rule are primarily based on attributes of the User object itself.
- * Examples of User Attributes: These attributes can include:
 - * User Status: (e.g., Active, Inactive, Disabled)
 - * Department:
 - * Location:
 - * Job Title:
 - * Manager:
 - * Custom Attributes: Any custom attributes defined for users in your Saviynt environment.
- * Triggering the Rule: When a user's attributes change, and those changes match the conditions defined in a User Update Rule, the rule is triggered.
- * Other Options:
- * B. Accounts: While account attributes can be updated as an action of a User Update Rule, the conditions for triggering the rule are

typically based on user attributes, not account attributes.

* C. Roles: Similar to accounts, roles can be assigned or removed as an action of a User Update Rule, but the triggering conditions are usually based on user attributes.

* D. Entitlements: Entitlements are also typically managed as an action of a User Update Rule, not as part of the triggering condition.

In conclusion: The User object and its attributes are the primary focus for defining conditions within a Saviynt User Update Rule.

Changes to user attributes trigger the rule, which can then perform actions such as updating other user attributes, accounts, roles, or entitlements.

NEW QUESTION # 35

In the process of setting up Single Sign-On using SAML 2.0, the "SP Entity ID" acts as a unique identifier for the Saviynt SP. If "SP Entity ID" is set to the value of SaviyntSP, which of the following will be the correct Single Sign-On URL to log in to EIC?

- A. <https://myorg.saviyntcloud.com/ECM/saml/SSO/SaviyntSP>
- B. <https://myorg.saviyntcloud.com/SaviyntSP>
- C. <https://myorg.saviyntcloud.com/ECM/saml/SSO/alias/SaviyntSP>

Answer: C

Explanation:

In Saviynt's SAML 2.0 based Single Sign-On (SSO) configuration, the "SP Entity ID" uniquely identifies Saviynt as the Service Provider (SP) to the Identity Provider (IdP). The correct SSO URL structure incorporates this "SP Entity ID" within a specific path.

* Saviynt's URL Structure: Saviynt's SSO URLs follow a pattern to ensure proper routing and authentication. The /ECM/saml/SSO/alias/ portion is crucial for directing SAML-based login attempts.

Why the other options are incorrect:

* A. <https://myorg.saviyntcloud.com/ECM/saml/SSO/SaviyntSP>: This URL is missing the crucial "alias" segment in the path, making it invalid for SAML SSO.

* B. <https://myorg.saviyntcloud.com/SaviyntSP>: This URL doesn't include the necessary components for SAML-based authentication within Saviynt.

Saviynt IGA References:

* Saviynt Documentation: Saviynt's official documentation on configuring SAML SSO provides details on the correct URL structure and the significance of the "SP Entity ID."

* Saviynt Support: Saviynt's support resources and knowledge base articles often address issues related to SSO configuration, reinforcing the correct URL format

NEW QUESTION # 36

The Sales department of a company requires an approval workflow to be created for an application where the Manager's approval should be followed by the Application Owner's approval. Which of the following sequences form the correct order of the workflow events?

- A. Start > Manager's Approval > Custom Assignment > Approve/Reject > End
- B. Start > Manager's Approval > Access Approval > Approve/Reject > End
- C. Start > Manager's Approval > Resource Owner's Approval > Approve/Reject > End
- D. Start > Resource Owner's Approval > Manager's Approval > Approve/Reject > End

Answer: C

Explanation:

The correct sequence of workflow events for an application where the Manager's approval should be followed by the Application Owner's approval is D. Start > Manager's Approval > Resource Owner's Approval > Approve/Reject > End. Here's a breakdown:

* Saviynt's Workflow Structure: Saviynt workflows follow a sequential structure, starting with a "Start" event and ending with an "End" event.

* Workflow Activities: Each step in the workflow is represented by an activity, such as an approval task.

* Manager's Approval: In this scenario, the first required approval is from the Manager. This would be represented by a "TASK Access Approve" activity (or similar, depending on the specific configuration) assigned to the user's manager.

* Application Owner's Approval: After the Manager's approval, the workflow needs to proceed to the Application Owner for their approval. This would be another "TASK Access Approve" activity assigned to the Application Owner. In Saviynt terms, Application Owner is a type of Resource Owner.

* Approve/Reject: This activity represents the decision point where the final approver (in this case, the Application Owner) either approves or rejects the request.

P.S. Free 2025 Savynt SAVIGA-C01 dumps are available on Google Drive shared by Actual4Labs:

https://drive.google.com/open?id=1_3th6kmoptvqr9B8ozULfhUFXzCPJPK