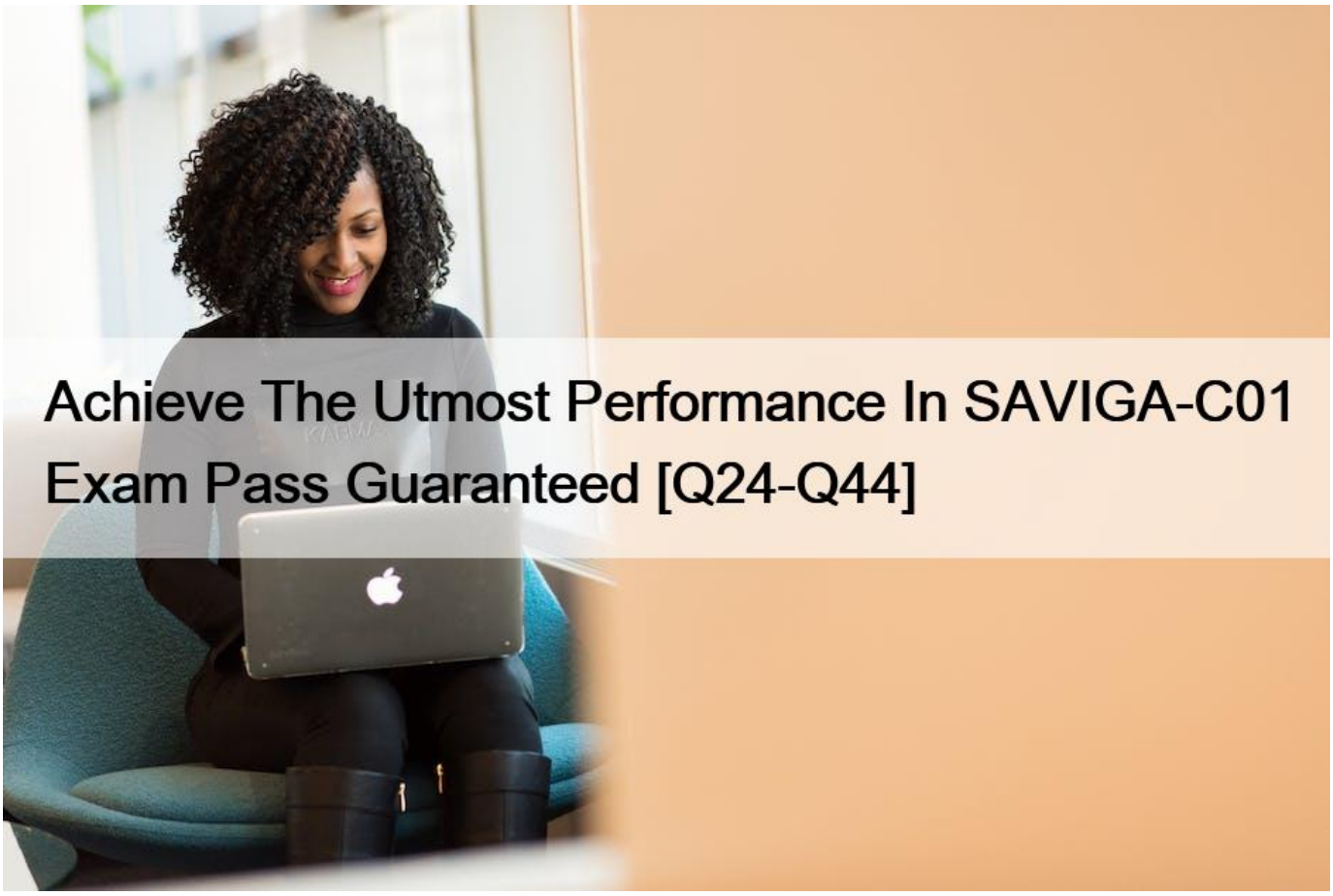
Achieve The Utmost Performance In SAVIGA-C01 Exam Pass Guaranteed [Q24-Q44



Achieve The Utmost Performance In SAVIGA-C01 Exam Pass Guaranteed Achive your Success with Latest Saviynt SAVIGA-C01 Exam QUESTION 24

Which of the following objects is available in the User Update Rule to configure Rule conditions?
* Users
* Accounts
* Roles
* Entitlements
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.

QUESTION 25

Which of the following should be enabled in the User Update Rule when the Rule has to be applied for an existing user?
* Trigger when user is created from import
* Retrofit rule actions for users
* Trigger when user is updated from import
* Action > Rerun All Provisioning Rules

To apply a User Update Rule to existing users in Saviynt, you should enable the option B. Retrofit rule actions for users. Here’s an explanation:

* Saviynt’s User Update Rules – Initial Application: When a User Update Rule is created, it typically applies to users who are newly created or updated after the rule is put in place.

* Retrofit Functionality: The “Retrofit rule actions for users” option allows you to apply the rule retroactively to users who already exist in the system and meet the rule’s conditions.

* How it Works: When enabled, Saviynt will evaluate the rule against all existing users. If a user matches the rule’s

conditions, the defined actions (e.g., assigning roles, updating attributes) will be applied to that user, even if they were created before the rule.

* Use Cases: This is useful when you create a new rule that should have been in place all along, or when you need to make a broad change to existing user configurations based on a new policy.

* Other Options:

* A. Trigger when user is created from import: This applies the rule to new users imported into Saviynt, not existing users.

* C. Trigger when user is updated from import: This applies the rule when existing users are updated via import, but it won’t necessarily apply to all existing users who meet the conditions.

* D. Action > Rerun All Provisioning Rules: This action is more general and might not be the most efficient way to apply a specific User Update Rule retroactively.

In summary: The “Retrofit rule actions for users” setting within a Saviynt User Update Rule is crucial for applying the rule’s logic and actions to existing users, ensuring consistent configuration across the user base.

QUESTION 26

Which of the following configurations on Entitlement Type is used to make an Entitlement request time- bound?
* Ask for Start Date while revoking
* Allow update of Access End Date
* Config JSON for Request Dates
* Start Date/End Date while raising a Request
To make an Entitlement request time-bound in Saviynt, the configuration used on the Entitlement Type is D.

Start Date/End Date while raising a Request. Here’s a breakdown:

* Saviynt’s Entitlement Management: Entitlements represent specific access rights within an application. Saviynt allows fine-grained control over how these entitlements are requested and granted.

* Entitlement Type Configuration: Within Saviynt, each Entitlement Type can be configured with various settings that govern its behavior during access requests.

* Time-Bound Access: To enforce time-limited access, Saviynt provides the option to require a Start Date and End Date during the request process.

* “Start Date/End Date while raising a Request”: This configuration setting, when enabled on an Entitlement Type, forces the requester to specify a desired start and end date for the access. This ensures that the granted access will only be valid for a specific period.

* Saviynt’s Workflow Engine and Provisioning: When a request with a start and end date is approved, Saviynt’s workflow engine will typically handle the provisioning and de-provisioning based on these dates. If connected integration is set up, it may schedule the activation and deactivation of the access in the target system accordingly.

* Other Options:

* A. Ask for Start Date while revoking: This setting is related to revoking access, not granting time-bound access.

* B. Allow update of Access End Date: This allows modification of the end date after the access has been granted, but it doesn’t enforce a time-bound request from the outset.

* C. Config JSON for Request Dates: While JSON might be used internally for configuration, this is not the specific setting that directly enables time-bound access requests.

In summary: The “Start Date/End Date while raising a Request” configuration on an Entitlement Type in Saviynt is the key to enforcing time-bound access, ensuring that access is granted only for a specific, pre- defined period.

QUESTION 27

What triggers a Request Rule?
* When a user is imported
* When Access Request is created and matches the conditions
* When the Run Detective Rule job is run
* When changes are detected in the import
A Request Rule in Saviynt is triggered B. When an Access Request is created and matches the conditions.

Here’s a detailed explanation:

* Saviynt’s Request Rules: Request Rules are a type of rule specifically designed to govern the access request process.

* Triggering Event: The primary trigger for a Request Rule is the creation of a new access request within Saviynt’s Access Request System (ARS).

* Condition Evaluation: When a new request is submitted, Saviynt evaluates the conditions defined in any applicable Request Rules. These conditions can be based on:

* Requester Attributes: (e.g., department, location, job title)

* Beneficiary Attributes: (if the request is for another user)

* Requested Resource: (e.g., application, role, entitlement)

* Request Details: (e.g., requested start/end dates)

* Rule Actions: If the conditions of a Request Rule are met, the rule’s defined actions are executed.

These actions can include:

* Modifying the request: (e.g., adding approvers, changing the approval workflow)

* Auto-approving or auto-rejecting the request:

* Generating notifications:

* Triggering other workflows:

* Other Options:

* A. When a user is imported: This might trigger User Update Rules or birthright rules, but not Request Rules.

* C. When the Run Detective Rule job is run: This job evaluates detective rules, not Request Rules.

* D. When changes are detected in the import: This could trigger various rules, but not specifically Request Rules.

QUESTION 28

Which of the following formats is suitable for downloading an Analytics report? (Select all that apply)
* CSV file and Excel Sheet
* Text file
* CSV file only
The formats suitable for downloading an Analytics report in Saviynt typically include A. CSV file and Excel Sheet. Here’s an explanation:

* Saviynt’s Reporting Capabilities: Saviynt provides options for exporting and downloading analytics reports in various formats to facilitate data sharing and further analysis.

* Common Export Formats:

* CSV (Comma Separated Values): A widely used format for storing tabular data in plain text.

It’s easily imported into various data analysis tools and spreadsheet programs.

* Excel Sheet (e.g., .xlsx): A popular spreadsheet format that allows for data organization, formatting, and calculations.

* Why These Formats Are Suitable:

* Data Analysis: Both CSV and Excel formats are well-suited for further data analysis and manipulation.

* Reporting: They are commonly used for creating reports and sharing data with stakeholders.

* Compatibility: Most data analysis and reporting tools support these formats.

* Other Less Common Options: While less frequent, Saviynt might offer other export formats like PDF, depending on the specific version and configuration.

* B. Text file: Although technically a text file, a raw .txt export might not be as useful for structured data like analytics reports. CSV would be preferred.

In conclusion: CSV and Excel are the most common and practical formats for downloading analytics reports from Saviynt, offering flexibility for data analysis, reporting, and sharing.

QUESTION 29

There is a requirement to have multiple users as Campaign Owners for a User Manager Campaign.

Which of the following configurations would be appropriate to achieve this?
* Create a user Query and add users

* Create a user group and choose the user group as the Campaign Owner
* Create a Roles Query and add Roles of various users
* Create an Organization Query and add users

To have multiple users as Campaign Owners for a User Manager Campaign in Saviynt, the appropriate configuration is to B. Create a user group and choose the user group as the Campaign Owner. Here’s the explanation:

* Saviynt’s User Groups: User groups are collections of users that can be used for various purposes, including assigning roles, permissions, and ownership.

* Campaign Owner as a User Group: Saviynt allows you to specify a user group as the owner of a campaign. This means that all members of the group will have the same campaign ownership permissions.

* Benefits of Using a User Group:

* Simplified Management: It’s easier to manage a group of users than to assign individual users as campaign owners.

* Flexibility: You can easily add or remove users from the group to adjust campaign ownership as needed.

* Shared Responsibility: All members of the group share responsibility for managing the campaign.

* Why Other Options Are Less Suitable:

* A. Create a user Query and add users: While you can use queries to select users, directly using a user group is a more standard and manageable approach for assigning multiple campaign owners.

* C. Create a Roles Query and add Roles of various users: Roles are typically used for granting access rights, not for defining campaign ownership.

* D. Create an Organization Query and add users: Organization queries are related to the organizational structure and are not the best way to define a group of campaign owners.

In conclusion: Using a user group as the Campaign Owner in Saviynt provides a flexible and manageable way to assign multiple users as owners, simplifying administration and promoting shared responsibility for campaign management.

QUESTION 30

John, who recently joined an organization as a full-time employee, is required to work from the Sydney office. He was assigned birthright entitlements as part of the new joiner provisioning. Which of the following Enterprise Roles will be assigned to John from the Birthright Rule?

* Birthright – Sydney
* Birthright – Permanent – Full-time
* Birthright – All
* Birthright – Employee

In this scenario, where John is a new full-time employee required to work from the Sydney office, the most specific and appropriate Enterprise Role assigned from the Birthright Rule would likely be A. Birthright – Sydney. Here’s the reasoning:

* Saviynt’s Birthright Roles and Rules: Birthright roles are designed to automatically provision access based on specific criteria like location, job role, or employment type. Birthright rules define the conditions for assigning these roles.

* Specificity of Role Assignment: The goal is to assign the most relevant and granular role based on the available information. In

this case, John’s location (Sydney) is the most specific criterion mentioned.

* Why Other Options Are Less Likely:

* B. Birthright – Permanent – Full-time: While John is a full-time employee, this role might be too broad if there are other location-specific roles.

* C. Birthright – All: This role is likely too generic and would grant excessive access. It’s generally not good practice to have an “all-encompassing” birthright role.

* D. Birthright – Employee: Similar to the “Full-time” role, this might be too broad if location- specific roles are available.

* Best Practices: It’s a best practice in identity governance to use the most specific criteria possible when assigning birthright access. This helps enforce the principle of least privilege.

In summary: The “Birthright – Sydney” role is the most appropriate choice because it aligns with John’s specific work location, ensuring he receives the necessary access for his role while adhering to the principle of least privilege.

QUESTION 31

An Application Owner Campaign can have multiple primary Certifiers and a single secondary Certifier.
* True
* False
The statement “An Application Owner Campaign can have multiple primary Certifiers and a single secondary Certifier” is generally False in Saviynt. Here’s why:

* Saviynt’s Application Owner Campaign: This campaign type is designed for Application Owners to review and certify access to their applications.

* Primary Certifier: There is usually a single designated Application Owner for each application. This is because application ownership is typically a single point of accountability. While it is technically possible to assign multiple owners, it is not considered a best practice.

* Secondary Certifiers (Backup/Delegates): Application Owner Campaigns can have multiple secondary certifiers. These are often used as:

* Backup: To ensure the campaign can proceed if the primary certifier is unavailable.

* Delegates: To allow the primary certifier to delegate some of the certification tasks.

* Consultants: Other stakeholders, such as security or compliance teams, who can be consulted during the decision-making process.

* Why the Statement Is Generally False: The core principle of application ownership implies a single point of accountability. While multiple secondary certifiers can assist, having multiple primary certifiers can lead to confusion and conflicting decisions.

* Possible Exceptions (Less Common):

* Highly Customized Configurations: In some very specific scenarios, organizations might customize Saviynt to allow multiple

primary certifiers for an application, but this is not a standard or recommended practice.

QUESTION 32

Which of the following Account statuses is not considered in a User Manager Campaign certification?
* Manually Suspended
* Inactive
* Suspended from Import Service
* Manually Provisioned
The Account status that is not typically considered in a User Manager Campaign certification in Saviynt is D.

Manually Provisioned. Here’s why:

* Saviynt’s User Manager Campaign Focus: User Manager Campaigns primarily focus on reviewing and certifying access that is actively managed and tracked within Saviynt.

* Account Statuses and Their Relevance:

* A. Manually Suspended: Indicates an account that has been intentionally disabled within Saviynt. These accounts are often included in reviews to ensure the suspension is still valid.

* B. Inactive: Indicates an account that has not been used for a certain period. These accounts are often included in reviews to determine if they should be disabled or removed.

* C. Suspended from Import Service: Indicates an account that has been suspended due to issues during an import process. These accounts are typically reviewed to resolve the import problem and determine the appropriate account status.

* Manually Provisioned Accounts: These accounts are created directly in the target system, bypassing Saviynt’s provisioning processes. As such, they might not be fully tracked or managed within Saviynt.

* Out-of-Band Access: Manually provisioned accounts represent a form of out-of-band access, which is often excluded from standard User Manager Campaigns.

* Separate Review Process: Organizations might have separate processes for reviewing manually provisioned accounts, such as using the RevokeOutOfBandAccessJob or a different type of campaign.

In conclusion: While other account statuses like Manually Suspended, Inactive, and Suspended from Import Service are relevant to access management within Saviynt and are often included in User Manager Campaigns, Manually Provisioned accounts might be excluded because they represent access granted outside of Saviynt’s control and might require a different review process.

QUESTION 33

Multiple indices can be selected while creating Analytics using the Elasticsearch Query.
* True
* False
It is True that multiple indices can be selected while creating Analytics using the Elasticsearch Query in Saviynt. Here’s why:

* Saviynt’s Analytics and Elasticsearch: Saviynt’s analytics capabilities are often built on top of Elasticsearch, a powerful search and analytics engine.

* Indices in Elasticsearch: In Elasticsearch, an index is like a database table. It’s a collection of documents with similar characteristics. Saviynt uses indices to store various types of data, such as user data, account data, entitlement data, and event logs.

* Multi-Index Queries: Elasticsearch allows you to query across multiple indices simultaneously. This is a fundamental feature of the search engine.

* Saviynt’s Interface: When creating analytics in Saviynt using Elasticsearch queries, the interface typically allows you to select multiple indices as the data source for your analysis.

* Use Cases: This capability is essential for creating comprehensive analytics that span different data domains. For example, you might want to analyze user access patterns (from one index) in conjunction with application usage data (from another index).

In conclusion: The ability to select multiple indices is a core feature of Elasticsearch and is supported within Saviynt’s analytics interface,

QUESTION 34

Which of the following Rules should always be used in conjunction with the Organization object?
* Technical Rule
* User Update Rule
* Scan Rule
* Request Rule
The type of Rule that should always be used in conjunction with the Organization object in Saviynt is the B.

User Update Rule. Here’s the explanation:

* Saviynt’s Organization Object: The Organization object in Saviynt represents the organizational structure or hierarchy (e.g., departments, locations, cost centers). It’s often used to define relationships between users and organizational units.

* User Update Rule: This type of rule is designed to automatically update user attributes based on changes in other user attributes or related objects.

* Using Organization with User Update Rule: The User Update Rule is frequently used with the Organization object to automate user management based on organizational changes.

* Example: You can create a User Update Rule that automatically assigns users to specific roles or groups based on their department (defined in the Organization object). If a user is moved to a different department, the rule will trigger and update their roles or group memberships accordingly.

* Dynamic User Management: This combination enables dynamic user management, ensuring that user attributes and access rights are automatically adjusted as users move within the organization.

* Other Options:

* A. Technical Rule: Technical Rules are more general-purpose and can be used for various tasks, but they are not specifically tied to the Organization object.

* C. Scan Rule: Scan Rules are used for data analysis and identifying potential issues, not for updating user attributes based on organizational structure.

* D. Request Rule: Request Rules are related to access request workflows, not to automatic user updates.

In essence: The User Update Rule, when used in conjunction with the Organization object, provides a powerful way to automate user management in Saviynt, ensuring that user attributes and access rights are dynamically updated based on changes in the organizational structure.

QUESTION 35

Which of the following aspects in EIC is regarded as a unique identity of a person?
* Endpoint
* Employee
* Account
* User
In Saviynt, a User represents the unique identity of a person. It’s the central object that ties together all the information about an individual, including their accounts, entitlements, roles, and attributes.

Why other options are incorrect:

* Endpoint: Represents a system or application, not a person.

* Employee: While many users might be employees, the term “user” is more general and can include contractors, partners, etc.

* Account: Represents a user’s access to a specific system, not their overall identity.

Saviynt IGA References:

* Saviynt Documentation: Throughout the documentation, “User” consistently refers to the individual’s identity within the system.

* Saviynt User Interface: The User Management section in Saviynt focuses on managing the lifecycle and access of individual users.

QUESTION 36

Access privileges for any specific Analytical Control can be assigned using SAV Roles. Which of the following tasks can be performed, by default, by users belonging to an SAV Role?
* Only view the configurations of the Control
* View Control, Run Control, and View Analytic History of the Control
* Only view the Analytic History of the Control
* View Control and Run Control
When access privileges for a specific Analytical Control are assigned using SAV Roles in Saviynt, users belonging to that role can, by default, perform the following tasks: B. View Control, Run Control, and View Analytic History of the Control. Here’s a breakdown:

* Saviynt’s Role-Based Access Control (RBAC): Saviynt uses RBAC to manage access to various features and functionalities, including Analytical Controls.

* Analytical Controls: These are pre-defined or custom-built analytics reports or dashboards.

* Default Permissions: When a user is granted access to an Analytical Control via an SAV Role, they typically receive a set of default permissions:

* View Control: Allows the user to view the configuration and definition of the Analytical Control (e.g., the query, parameters, visualization).

* Run Control: Allows the user to execute the Analytical Control and generate results.

* View Analytic History: Allows the user to see the history of previous executions of the Analytical Control, including the results and timestamps.

* Why These Permissions Are Important:

* Transparency: Users can understand how the analytics are defined and generated.

* Usability: Users can run the analytics and obtain insights.

* Auditing: Users can review past results for trend analysis or investigation.

* Other Options:

* A. Only view the configurations of the Control: This is too restrictive; users need to be able to run the control to get value from it.

* C. Only view the Analytic History of the Control: This is also too limited; users should be able to run the control and view its configuration as well.

* D. View Control and Run Control: While closer, it’s missing the “View Analytic History” permission, which is important for auditing and analysis.

MISCELLANEOUS

QUESTION 37

Which of the following Access Request configurations can be set up as either optional or mandatory, based on business requirements?
* Approval comments
* Add Attachment
* Business justification at Request level
* None of the above
In Saviynt’s Access Request configurations, the following can be set up as either optional or mandatory based on business requirements:

* A. Approval comments: When an approver approves or rejects a request, they can be required to provide comments, or it can be made optional.

* B. Add Attachment: Requesters can be allowed or required to attach supporting documentation to their access requests.

* C. Business justification at Request level: Requesters can be obligated to provide a business justification for their access request, or it can be made optional.

Here’s a breakdown with Saviynt IGA references:

* Saviynt’s Access Request System (ARS) Configuration: Saviynt provides granular control over the ARS’s behavior, allowing administrators to customize various aspects of the request process, including data validation and required fields.

* Mandatory vs. Optional Fields: Many fields and actions within the ARS can be configured as either mandatory or optional. This allows organizations to tailor the request process to their specific needs and compliance requirements.

* Configuration Locations: These settings are typically found within the ARS configuration section of Saviynt’s administrative interface.

* Approval Comments: Often configurable within the workflow definition, at the approval step level. You can define whether comments are required for approval, rejection, or both.

* Add Attachment: Generally found under general ARS settings, allowing you to enable or disable attachments and potentially set them as mandatory.

* Business Justification: Also found within the ARS settings, allowing you to toggle the requirement for a business justification at the request level or even at the individual entitlement level.

* Business Rationale: The flexibility to make these elements optional or mandatory allows organizations to balance the need for information with the desire for a streamlined user experience. For example, high- risk access requests might require detailed justification and attachments, while low-risk requests might not.

* Saviynt’s Audit Trail: Regardless of whether these fields are mandatory or optional, Saviynt’s audit trail will capture the information provided, ensuring a complete record of the request and approval process.

In summary: Saviynt’s ARS allows administrators to configure approval comments, attachments, and business justifications as either optional or mandatory, providing the flexibility to adapt the access request process to meet diverse organizational needs and compliance requirements.

QUESTION 38

Where can an Admin get the details of a successfully executed Rule?
* Archived Rule Trail
* Archived Application Logs
* Current Rule Trail
* Action Trail

To get the details of a successfully executed Rule in Saviynt, an Admin should look in the C. Current Rule Trail. Here’s why:

* Saviynt’s Rule Engine and Logging: Saviynt’s rule engine executes various types of rules (e.g., birthright rules, user update rules, technical rules). It maintains logs to track rule execution and outcomes.

* Current Rule Trail: This log specifically captures the details of recently executed rules, including:

* Rule Name: The name of the rule that was executed.

* Execution Time: The timestamp of when the rule was executed.

* Status: Whether the rule execution was successful or not.

* Details: Specific information about the rule’s execution, such as the conditions that were evaluated and the actions that were taken.

* Troubleshooting and Auditing: The Current Rule Trail is invaluable for troubleshooting rule behavior and for auditing purposes, providing a clear record of what rules were executed and their results.

* Other Options:

* A. Archived Rule Trail: This log stores details of older rule executions that have been archived.

It’s useful for historical analysis but not for recent executions.

* B. Archived Application Logs: These logs are related to application activity, not rule execution.

* D. Action Trail: The Action Trail captures general user and administrative actions within Saviynt, but it might not provide the detailed information about rule execution that the Current Rule Trail does.

QUESTION 39

_____ filters the requestable applications under “Request New Access.”
* Access Add Workflow
* Access Query
* Provisioning Connection
* Whom to Request
The component that filters the requestable applications under “Request New Access” in Saviynt is the Access Query. Here’s a detailed explanation:

* Saviynt’s Access Request System (ARS): As the front end for requesting access, the ARS needs a mechanism to determine which applications (and entitlements) should be displayed to a user as requestable.

* Access Query: This is a powerful feature within Saviynt that allows administrators to define specific criteria to control the visibility of applications and entitlements in the ARS. Think of it as a filter that determines what a user can see and request.

* How Access Queries Work:

* Defined on Applications/Entitlements: Access Queries are configured on individual applications or entitlements within Saviynt.

* Based on User Attributes: They use user attributes (e.g., department, location, job title, group memberships) and other criteria (e.g., risk level) to determine if a user should see a particular application or entitlement.

* Dynamic Filtering: When a user accesses the “Request New Access” section, Saviynt evaluates the Access Queries associated with each application and entitlement in real-time. Based on the user’s attributes, the system dynamically filters the list, showing only the applications and entitlements that match the query conditions.

* Saviynt’s Security Model: Access Queries are a fundamental part of Saviynt’s security model. They ensure that users are only presented with access options that are relevant and appropriate for their role and context, preventing accidental over-provisioning and reducing the attack surface.

* Other Options:

* Access Add Workflow: While essential for processing access requests, the workflow itself doesn’t filter which applications are initially displayed.

* Provisioning Connection: This relates to how Saviynt connects to target systems for automated provisioning. It doesn’t control the initial visibility of applications in the ARS.

* Whom to Request: This setting might determine the available approvers, but it doesn’t filter the list of requestable applications.

In essence: Access Queries act as a dynamic filter, leveraging user attributes and defined criteria to determine which applications and entitlements are presented to a user within Saviynt’s “Request New Access” interface, ensuring a personalized and secure access request experience.

QUESTION 40

What does the following image signify?

Assigning of Enterprise Role based on a dynamic variable city.
* Assigning of Enterprise Role based on users’ department
* Assigning of Enterprise Role based on users’ location
* Assigning of Enterprise Role based on concatenation of dynamic variable city and Finance

The image signifies B. Assigning of Enterprise Role based on users’ location. Here’s a breakdown, assuming the image depicts a portion of a Saviynt User Update Rule configuration:

* Dynamic Variable “City”: The image highlights the use of a dynamic variable called “city.” This strongly suggests that the rule is using the user’s location (city) as a key factor in determining role assignment.

* Saviynt’s User Update Rules and Dynamic Variables: User Update Rules in Saviynt allow for the use of dynamic variables, which represent user attributes. These variables can be used in conditions and actions within the rule.

* Enterprise Role Assignment: The context of the question implies that the rule is assigning an Enterprise Role based on the value of this “city” variable.

* Example: The rule might be configured to assign an Enterprise Role like “Sydney-Users” to users whose “city” attribute is “Sydney.”

* Why Other Options Are Less Likely:

* A. Assigning of Enterprise Role based on users’ department: There’s no mention of

“department” in the provided information.

* C. Assigning of Enterprise Role based on concatenation of dynamic variable city and Finance: While concatenation is possible in Saviynt, there’s no indication that “Finance” is involved here. The focus seems to be solely on the “city” variable.

In conclusion: Based on the information given, the image most likely represents a Saviynt User Update Rule that assigns an Enterprise Role based on the user’s location, as indicated by the dynamic variable “city.

QUESTION 41

Which of the following connection types is best suited to expose Workday reports as a data service?
* Workday-RAAS
* Workday-REST
* Workday-OAuth
* Workday-SOAP
The connection type best suited to expose Workday reports as a data service in Saviynt is A. Workday- RAAS (Report as a Service). Here’s why:

* Workday-RAAS: This connection type is specifically designed to integrate with Workday’s RaaS functionality. Workday RaaS allows you to expose custom reports created within Workday as web services that can be consumed by external applications like Saviynt.

* Data Service for Reports: RaaS essentially turns a Workday report into a data service, making it easy to retrieve the report’s data in a structured format (typically XML or JSON).

* Saviynt’s Integration: Saviynt’s Workday-RAAS connection type is built to leverage this capability, allowing you to:

* Select Workday Reports: Choose the specific Workday reports you want to integrate with.

* Import Data: Import the data from those reports into Saviynt for various purposes (e.g., identity governance, access certification, analytics).

* Schedule Imports: Schedule regular data imports to keep Saviynt’s data synchronized with Workday.

* Why Other Options Are Less Suitable:

* B. Workday-REST: While Workday has a REST API, it’s more general-purpose and not specifically tailored for exposing reports as data services in the same way as RaaS.

* C. Workday-OAuth: OAuth is an authorization protocol, not a connection type for retrieving report data.

* D. Workday-SOAP: Workday’s SOAP API is being gradually replaced by the REST API and is less focused on report data retrieval than RaaS.

QUESTION 42

_____ refers to any type of access that is associated with a managed system or application, such as groups, roles, permissions, or responsibilities.
* Entitlements
* Endpoints
* Workflows
* Accounts
In Saviynt, “Entitlements” refers to any type of access granted to users within a managed system or application. This broad term encompasses various forms of access controls, including:

* Groups: Collections of users with shared access permissions.

* Roles: Sets of permissions that define a user’s job function or responsibilities.

* Permissions: Specific access rights to resources or functionalities.

* Responsibilities: Duties or tasks associated with a particular role.

Why other options are incorrect:

* Endpoints: Refer to network devices or systems, not access rights.

* Workflows: Are automated processes for tasks like approvals, not access itself.

* Accounts: Represent user identities, not the specific access they have.

Saviynt IGA References:

* Saviynt Documentation: Saviynt’s documentation consistently uses the term “Entitlements” to describe the various types of access it manages.

* Saviynt User Interface: The Saviynt interface uses “Entitlements” throughout its menus and features related to access management.

QUESTION 43

Which of the following Role types should be selected for a Role containing Entitlements that span across multiple applications?
* Application Role
* Transactional Role
* Enabler Role
* Enterprise Role
In Saviynt, Enterprise Roles are specifically designed to encompass entitlements that span multiple applications. This is in contrast to Application Roles, which are limited to entitlements within a single application.

* Enterprise Roles: Provide a way to group entitlements across different applications, reflecting a user’s overall job function or responsibilities within the organization. This is essential for managing access for users who need permissions in various systems to perform their duties.

* Other Role Types:

* Application Role: Grants permissions specific to a single application.

* Transactional Role: Focuses on granting permissions for specific tasks or transactions within an application.

* Enabler Role: Provides supplementary permissions that enhance or support other roles.

Saviynt IGA References:

* Saviynt Documentation: The section on Role Management within Saviynt’s documentation clearly defines the different role types and their purposes.

* Saviynt Training Materials: Saviynt’s training courses emphasize the importance of Enterprise Roles in managing cross-application access.

QUESTION 44

Which of the following features best describe the Authorization mechanism for the EIC application?
* Security System
* SSO
* WSRETRY Job
The feature that best describes the Authorization mechanism for the EIC (Enterprise Identity Cloud) application in Saviynt is A. Security System. Here’s an explanation:

* Saviynt’s Security System: This is the core component within Saviynt that handles authentication and authorization for various applications and resources, including EIC.

* Authorization in EIC: The Security System determines what actions users are allowed to perform within EIC, such as:

* Creating, updating, or deleting users.

* Managing roles and entitlements.

* Running reports.

* Configuring connections.

* Role-Based Access Control (RBAC): The Security System typically uses RBAC to manage these permissions. Users are assigned to roles, and roles are granted specific permissions within EIC.

* Why Other Options Are Less Relevant:

* B. SSO (Single Sign-On): SSO is an authentication mechanism that allows users to log in once and access multiple applications. While Saviynt supports SSO, it’s not the primary authorization mechanism for EIC.

* C. WSRETRY Job: This is a job related to retrying web service calls, not authorization.