Saviynt Level 100 (L100) Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Questions

1. Where do we add the delegation notification template?

A. SAV Role

B. User Update Rules

C. Technical Rules

D. Global Configurations

2. What is the maximum number of files that can be attached in a request?

A. 2

B. 3

C. 4

D. 5

3. What is the supported file type extension to send analytical result set through email attachment?

A. .csv

B. .xls

C. .pdf

D. .txt

4. Which of the following would typically not be used in analytics controls?

A. User Privileges

B. Database Access

C. Real-time User Interaction

D. Historical Data Queries

5. User Manager Certification can be triggered from which of the following?

A. Technical Rule

B. User Update Rule

C. Analytics

D. Global Configurations

6. Which keyword can be used as a column name when constructing an SQL query for V2 controls?

- **A. status**
- **B. analyticshistorykey**
- **C. hashcode**
- **D. employeeType**

7. What is a connector group in Saviynt?

- **A. A collection of data connectors that facilitate access to multiple applications**
- **B. A team responsible for managing access controls**
- **C. A set of compliance policies for user access**
- **D. A module for user data analytics**

8. How are 'Audit Reports' beneficial in Saviynt?

- **A. They offer insights into user satisfaction**
- **B. They provide a comprehensive view of access events for compliance and investigations**
- **C. They track user engagement metrics**
- **D. They detail system performance statistics**

9. What type of backup process does Saviynt implement?

- **A. Full backup weekly**
- **B. Incremental backup daily**
- **C. Daily full backup**
- **D. Cloud backup monthly**

10. What job type is used for SOD Evaluation?

- **A. RiskSODEvaluationJob**
- **B. RiskSODJob**
- **C. SODEvaluationJob**
- **D. RiskEvaluationJob**

Answers

1. A
2. D
3. A
4. C
5. B
6. D
7. A
8. B
9. C
10. A

Explanations

1. Where do we add the delegation notification template?

A. SAV Role

B. User Update Rules

C. Technical Rules

D. Global Configurations

The delegation notification template is added in the SAV Role. This is because the SAV Role contains the specific configurations and attributes necessary for defining the behaviors associated with delegation notifications. Delegation relates to granting permissions or access rights to other users within the Saviynt platform, and these roles are essential in managing who can perform actions on behalf of others. When configuring delegation notifications, it is crucial to designate the context and audience for these messages, which is why the appropriate setting falls within the SAV Role framework. Roles in Saviynt often dictate not only access control but also the notifications and alerts that are triggered based on certain actions or events, such as delegating authority. This focus on roles aligns with general practices in identity governance and administration systems, where user permissions and notifications are closely tied to specific roles defined within the system. In other areas like User Update Rules, Technical Rules, or Global Configurations, the management of templates would not be appropriate or as effective, as these aspects serve different functions within the overall identity management strategy.

2. What is the maximum number of files that can be attached in a request?

A. 2

B. 3

C. 4

D. 5

The maximum number of files that can be attached in a request is five. This limit is established to balance user needs for providing additional documentation or information in their requests while maintaining system performance and usability. By allowing multiple attachments, users can ensure they submit comprehensive details needed for processing their requests without overwhelming the system with excessive data. The capability to attach multiple files is important in workflows where supporting documentation is necessary for decision-making or compliance purposes. This flexibility accommodates various scenarios, such as submitting multiple forms, reports, images, or other relevant documents, thus enhancing the overall efficiency of request handling in the system.

3. What is the supported file type extension to send analytical result set through email attachment?

A. .csv

B. .xls

C. .pdf

D. .txt

The supported file type extension for sending analytical result sets through email as an attachment is .csv. This format is widely used for data analysis and represents data in a structured manner, where each piece of data is separated by a comma. This makes it easy for various software applications, including spreadsheet programs, database systems, and data analysis tools to read, interpret, and manipulate the data efficiently. The .csv format is particularly beneficial when sharing large datasets because it is relatively lightweight compared to other file types, ensuring quick transfers over email. Its simplicity and compatibility with a variety of data handling applications add to its utility in analytical contexts. While other formats such as .xls (Excel spreadsheet), .pdf (portable document format), and .txt (text file) can also be used for data, they do not offer the same advantages as .csv in terms of structured data interchange, ease of analysis, and compatibility with data processing tools commonly used in analytics.

4. Which of the following would typically not be used in analytics controls?

A. User Privileges

B. Database Access

C. Real-time User Interaction

D. Historical Data Queries

Real-time user interaction is not typically utilized in analytics controls because analytics controls primarily focus on examining and interpreting historical data to inform decision-making. This involves analyzing past trends, patterns, and performance metrics, which can all be derived from historical data queries. User privileges and database access are crucial components in analytics controls as they pertain to the security and management of data access. Understanding who has the rights to access certain data is essential for maintaining data integrity and compliance. Historical data queries are fundamental to analytics controls since they provide the necessary information for trend analysis and reporting, allowing organizations to make data-driven decisions based on observed past behaviors and outcomes. In contrast, real-time user interaction implies an immediate engagement that does not inherently contribute to the structured analysis that analytics controls require; therefore, it does not fit into the typical framework used in this context.

5. User Manager Certification can be triggered from which of the following?

A. Technical Rule

B. User Update Rule

C. Analytics

D. Global Configurations

User Manager Certification can be triggered from a User Update Rule due to its specific function in identity governance and administration processes. When a User Update Rule is applied, it means that changes were made to user attributes or permissions that may warrant a review of the user's access. This aligns directly with the purpose of a certification, which is to verify that users have the appropriate access rights in accordance with their roles and responsibilities within the organization. By using a User Update Rule to trigger certification, organizations can ensure that any modifications—whether due to role changes, new responsibilities, or other alterations—are thoroughly audited and confirmed by the appropriate stakeholders. This process helps maintain compliance, provides oversight, and mitigates potential security risks from outdated or unnecessary access privileges. While other options might relate to different aspects of identity management, they do not directly initiate user certifications in the way a User Update Rule does. Technical Rules may define access control policies, Analytics may assist in reporting and insights but not trigger certifications, and Global Configurations refer to overall settings for the environment but do not specifically manage user access certifications. Thus, the User Update Rule serves a crucial role in engaging the certification process following changes in user data.

6. Which keyword can be used as a column name when constructing an SQL query for V2 controls?

A. status

B. analyticshistorykey

C. hashcode

D. employeeType

When constructing an SQL query for V2 controls, the keyword that can be used as a column name is employeeType. This column name does not conflict with any reserved SQL keywords, making it a valid choice for use in queries without the risk of confusion or syntax errors that might occur if you used a keyword that has a predefined meaning in SQL. On the other hand, names like status, analyticshistorykey, and hashcode may represent either reserved words in SQL or have special significance that could cause issues when they are used as column names. In SQL, it is crucial to choose names that avoid these conflicts to ensure that the queries run smoothly and can be understood by the SQL parser without any ambiguities. Selecting a name like employeeType, which does not have any such issues, is the best option for constructing effective and functional queries in this context.

7. What is a connector group in Saviynt?

A. A collection of data connectors that facilitate access to multiple applications

B. A team responsible for managing access controls

C. A set of compliance policies for user access

D. A module for user data analytics

A connector group in Saviynt serves as a collection of data connectors that facilitate access to multiple applications. This concept is crucial because it allows organizations to streamline how they manage integrations with various systems and applications. By grouping connectors that can connect to different resources, administrators can easily apply policies and configurations across those resources, ensuring consistent access and governance. The use of connector groups helps in simplifying the management of identity and access rights within an organization's IT landscape. Such groups can be particularly useful when implementing common access controls or provisioning workflows that span multiple applications, thereby enhancing efficiency and reducing the risk of errors. This understanding highlights the central role connector groups play in integrating and managing diverse applications within Saviynt, ensuring that users have the appropriate access while aligning with organizational policies.

8. How are 'Audit Reports' beneficial in Saviynt?

A. They offer insights into user satisfaction

B. They provide a comprehensive view of access events for compliance and investigations

C. They track user engagement metrics

D. They detail system performance statistics

Audit Reports in Saviynt are primarily beneficial because they provide a comprehensive view of access events, which is crucial for compliance and investigations. These reports allow organizations to monitor who accessed what information, when, and how, thereby facilitating accountability and transparency. By capturing a detailed trail of access events, these reports help organizations comply with regulatory requirements and internal policies, assisting in audits and investigations when necessary. The data obtained from audit reports can highlight anomalies or unauthorized access attempts, enabling organizations to swiftly address any security concerns. This insight is essential not only for fulfilling compliance obligations but also for strengthening the overall security posture of the organization. Hence, the comprehensive nature of access event reporting is key to understanding and managing user access effectively.

9. What type of backup process does Saviynt implement?

A. Full backup weekly

B. Incremental backup daily

C. Daily full backup

D. Cloud backup monthly

Saviynt implements a daily full backup process, which is crucial for maintaining data integrity and accessibility. This approach ensures that a complete snapshot of all configurations, user data, and relevant system information is saved every day. The advantage of a daily full backup is that it minimizes the risk of data loss since even the most recent updates are included in the backup. Should a recovery be necessary, this strategy allows for a straightforward restoration process, enabling users to revert systems back to a specific point in time. Moreover, having daily backups can be essential for environments where changes to data occur frequently, ensuring that there is always up-to-date information available. This comprehensive approach also helps in reducing the complexity associated with managing incremental backups, where only changes since the last backup would be saved and potentially complicate restoration processes. This contrasts with other backup types, such as incremental backups, which may not capture all data on a daily basis, and full backups less frequent than daily, which might risk data loss between backup points. The monthly cloud backup reflects a more sporadic approach which, while useful in certain scenarios, does not provide the same level of immediate recoverability as daily full backups.

10. What job type is used for SOD Evaluation?

A. RiskSODEvaluationJob

B. RiskSODJob

C. SODEvaluationJob

D. RiskEvaluationJob

The job type used for SOD (Segregation of Duties) Evaluation is identified as RiskSODEvaluationJob. This job is specifically designed to assess and evaluate any potential conflicts between roles and responsibilities within an organization, which is critical for maintaining compliance and security. Segregation of Duties is a key principle in internal controls that helps prevent fraud and errors by ensuring that no single individual has control over all aspects of any financial transaction. The RiskSODEvaluationJob operates within this context, examining user access and permissions to identify risks where conflicting duties may reside. Understanding the distinction between this option and others is important; while they may suggest various evaluations or risks, only RiskSODEvaluationJob is explicitly tailored for the unique requirements of SOD analysis, focusing on the risk assessments that pertain to the separation of roles in business processes.