# SailPoint IdentityIQ (IIQ) Certification Practice Test (Sample)

## Study Guide

BY EXAMZIFY

**Everything you need from our exam experts!**

Sample study guide. Visit https://sailpointidentityiq-iiq.examzify.com

**Notice: Examzify makes every reasonable effort to obtain from reliable sources accurate, complete, and timely information about this product.**

# Questions

1. **What is the purpose of the Certified Entity Completion rule?**

   **A. To finalize roles after approval**

   **B. To trigger identity updates**

   **C. To manage certification reporting**

   **D. To execute data backups**

2. **What is the average round trip commit time for an 8k block of data?**

   **A. 18ms or less**

   **B. 20ms or less**

   **C. 22ms or less**

   **D. 25ms or less**

3. **What is a key advantage of using IIQ for identity management?**

   **A. Centralized management of user identities**

   **B. High user access variability**

   **C. Lower initial setup costs**

   **D. Independence from network security protocols**

4. **What is the recommended architecture for SailPoint IdentityIQ?**

   **A. Two-Tier Architecture**

   **B. Standard 2 Tier**

   **C. Three-Tier Architecture**

   **D. Standard Single Tier**

5. **What is typically a feature of Identity Governance?**

   **A. User satisfaction surveys**

   **B. Automated access provisioning**

   **C. Role-based access controls**

   **D. Frequent password changes**

**6. What should future updates in an IIQ project be captured in?**

**A. The build directory**

**B. The source directory**

**C. The downloaded folder**

**D. The logs folder**

**7. How does SailPoint IdentityIQ define its authorization model?**

**A. Using user roles only**

**B. Through capabilities and SPrights**

**C. By limiting access based on IP addresses**

**D. Through manual approval processes**

**8. What does IdentityIQ aim to achieve through the management of policy exceptions?**

**A. To enforce outdated policies**

**B. To ensure flexibility and compliance**

**C. To eliminate all exceptions**

**D. To complicate user access**

**9. Which application servers are supported by SailPoint IdentityIQ?**

**A. Apache Tomcat, JBoss Enterprise Application Platform**

**B. Oracle WebLogic, Microsoft IIS**

**C. IBM WebSphere, Nginx**

**D. Apache HTTP, IBM WebSphere Liberty**

**10. What characterizes conditionally managed artifacts in SailPoint IdentityIQ?**

**A. They are always migrated across environments**

**B. They may or may not be migrated across environments**

**C. They are never managed**

**D. They are implemented with strict policies**

# Answers

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

# Explanations

## 1. What is the purpose of the Certified Entity Completion rule?

A. To finalize roles after approval

B. To trigger identity updates

C. To manage certification reporting

D. To execute data backups

**The purpose of the Certified Entity Completion rule is to finalize roles after they have undergone the certification process. When certifications are conducted within SailPoint IdentityIQ, this rule plays a critical role in ensuring that entities (such as user accounts or roles) that have been reviewed by certifiers are marked as complete and reflect the final approved status. This process ensures that authorized access is maintained and that any necessary changes based on the certification review are properly enforced. In this context, the other options do not accurately represent the function of the Certified Entity Completion rule. While triggering identity updates, managing certification reporting, and executing data backups are all important aspects of identity governance and management, they fall within different functionalities within IdentityIQ and are not the primary focus of the Certified Entity Completion rule. This distinction is crucial for understanding how the certification process is managed and completed within the platform.**

## 2. What is the average round trip commit time for an 8k block of data?

A. 18ms or less

B. 20ms or less

C. 22ms or less

D. 25ms or less

**The average round trip commit time for an 8k block of data is generally understood to be around 20ms or less. This measurement is crucial for performance benchmarks in data handling, particularly in systems that rely on efficient data transfer and transaction processing. A round trip commit time refers to the duration it takes for a data request to travel from the origin to the destination and back again, ensuring that the data has been successfully processed and acknowledged. In many modern applications, especially those leveraging high-performance databases and storage systems, optimizing for speed is essential. Therefore, achieving a commit time of 20ms or less indicates that the system is handling operations effectively within an acceptable performance range. While other answers suggest slightly longer times, the choice of 20ms reflects a balance that many systems strive for to maintain optimal performance for transactions. Systems that exceed this average may begin experiencing latency issues, negatively impacting user experience and system efficiency.**

## 3. What is a key advantage of using IIQ for identity management?

**A. Centralized management of user identities**

**B. High user access variability**

**C. Lower initial setup costs**

**D. Independence from network security protocols**

**A key advantage of using SailPoint IdentityIQ for identity management is the centralized management of user identities. This centralized approach allows organizations to streamline processes related to user provisioning, de-provisioning, access requests, and compliance reporting, creating a more efficient and standardized way to manage identities across different systems and applications. With a single point of control, administrators can easily manage access rights, enabling better governance and security while also reducing the risks of errors or mismanagement associated with decentralized identity management practices.  Centralized identity management also enhances visibility into user access across the enterprise, making it easier to enforce policies and perform audits. This can lead to improved compliance with regulations and internal policies, as all identity data is aggregated in one place.  The other options, while potentially relevant in certain contexts, do not capture the fundamental strength of SailPoint IIQ as well as the centralized management does. For instance, high user access variability does not suggest an effective management strategy, and lower initial setup costs may not reflect the total cost of ownership. Independence from network security protocols does not inherently contribute to the effectiveness of identity management itself, as secure network protocols are still vital in protecting identity data.**

## 4. What is the recommended architecture for SailPoint IdentityIQ?

**A. Two-Tier Architecture**

**B. Standard 2 Tier**

**C. Three-Tier Architecture**

**D. Standard Single Tier**

**The recommended architecture for SailPoint IdentityIQ is the Standard 2 Tier. This architecture is considered effective because it separates the application server from the database server, allowing for improved performance, scalability, and manageability. In this setup, the application server handles the business logic, user interface, and integrates with other systems, while the database server is dedicated to data storage and retrieval.  By employing a two-tier architecture, organizations can benefit from reduced latency due to direct communication between the application server and the database, which enhances overall responsiveness. Additionally, this model allows for easier upgrades and maintenance since the application and database can be managed separately.  In contrast, options like Three-Tier Architecture, while often beneficial in different contexts, introduce additional complexity with an intermediary layer for application services, which may not be necessary for most implementations of IdentityIQ. Single Tier architecture lacks the separation of concerns, which can lead to performance drawbacks as the application grows. A Standard 2 Tier model strikes a balance between functionality and performance, making it the recommended approach for deploying SailPoint IdentityIQ.**

## 5. What is typically a feature of Identity Governance?

- A. User satisfaction surveys
- B. Automated access provisioning
- C. Role-based access controls
- D. Frequent password changes

**Role-based access controls (RBAC) are a fundamental feature of Identity Governance, as they enable organizations to manage user access rights based on their role within the organization. By assigning permissions to roles rather than individual users, organizations can streamline access management, ensuring that users have the appropriate level of access necessary for their job functions. This also enhances security and compliance, as it simplifies the enforcement of policies and audits of user permissions. In the context of Identity Governance, RBAC helps to minimize the risk of privilege creep, where users accumulate excessive permissions over time. This is critical in maintaining an organized and secure access environment, ensuring that users cannot access information or systems that are not relevant to their role. Other options, while relevant to certain aspects of identity and access management, do not directly align with the core principles of Identity Governance in the same way that RBAC does. For instance, automated access provisioning is important for operational efficiency, but it operates under the frameworks established by Identity Governance like RBAC. User satisfaction surveys can be useful for understanding the user experience but do not pertain to the governance of identity and access management itself. Frequent password changes can enhance security but are more aligned with password policies rather than the broader scope of Identity Governance.**

## 6. What should future updates in an IIQ project be captured in?

- A. The build directory
- B. The source directory
- C. The downloaded folder
- D. The logs folder

**Future updates in an IdentityIQ project should be captured in the build directory. This is because the build directory is where the compiled code, resources, and any necessary dependencies for the project are organized and stored. It serves as the staging area for the software that will be put into production or further testing. Capturing updates here ensures that any new features or changes made to the project are effectively versioned and integrated into the compiled outputs. This practice allows for better tracking of modifications and facilitates easier deployment processes. The other options, such as the source directory, downloaded folder, and logs folder, serve different purposes. The source directory is meant for the raw code and configuration files, while the downloaded folder is typically used for external libraries or tools that have been imported into the project. The logs folder is designated for runtime logs generated by the application, making it essential for monitoring and troubleshooting, but not for capturing updates or changes to the project itself.**

## 7. How does SailPoint IdentityIQ define its authorization model?

A. Using user roles only

B. Through capabilities and SPrights

C. By limiting access based on IP addresses

D. Through manual approval processes

SailPoint IdentityIQ defines its authorization model primarily through capabilities and SPrights, which represent a more granular approach to managing access permissions. Capabilities in IdentityIQ allow organizations to define what actions a user can perform within the system based on their roles and responsibilities, while SPrights govern the specific permissions associated with those capabilities. This model enables fine-tuning of access control, ensuring that users have the right level of access to resources based on their operational needs, thereby enhancing security and compliance. This approach stands in contrast to relying solely on user roles, which can be overly simplistic and may not provide the necessary level of detail for managing complex permissions scenarios. Limiting access based on IP addresses is a network security measure and does not directly relate to the authorization model within IdentityIQ. Similarly, manual approval processes can be part of overall governance but are not the foundation of the authorization model itself. The focus on capabilities and SPrights makes the authorization structure flexible and aligned with the dynamic requirements of enterprise environments.

## 8. What does IdentityIQ aim to achieve through the management of policy exceptions?

A. To enforce outdated policies

B. To ensure flexibility and compliance

C. To eliminate all exceptions

D. To complicate user access

The aim of IdentityIQ in managing policy exceptions is to ensure flexibility and compliance. Effective identity governance requires a balance between adhering to security policies and allowing necessary exceptions that accommodate varying business needs. By managing policy exceptions, IdentityIQ provides organizations the ability to streamline their compliance efforts while also being adaptable; this means users can operate efficiently without being hindered by rigid policies that may not apply in all situations. This approach allows organizations to assess and document exceptions in a manner that aligns with regulatory requirements, ensuring that they still meet compliance standards despite having these exceptions in place. Such flexibility is essential for promoting user productivity while maintaining the overall integrity and security of the identity governance framework. The other options do not align with the goals of IdentityIQ. Enforcing outdated policies would not support a modern, adaptable security posture. The notion of eliminating all exceptions is impractical, as it would inhibit business operations and restrict necessary access. Complicating user access goes against the purpose of providing a streamlined identity governance experience, promoting security without layering unnecessary difficulties for users.

## 9. Which application servers are supported by SailPoint IdentityIQ?

A. Apache Tomcat, JBoss Enterprise Application Platform

B. Oracle WebLogic, Microsoft IIS

C. IBM WebSphere, Nginx

D. Apache HTTP, IBM WebSphere Liberty

**SailPoint IdentityIQ supports specific application servers that are compatible with its architecture and functionality. The choice that includes Apache Tomcat and JBoss Enterprise Application Platform is correct because these servers are well-suited for hosting Java-based applications, which IdentityIQ is built upon. Apache Tomcat is a widely used open-source servlet container that allows for running Java Servlets and rendering web pages that use Java Server Pages (JSP). Its lightweight nature makes it a popular choice for many organizations implementing IdentityIQ. JBoss Enterprise Application Platform, on the other hand, is a robust application server that provides additional services such as clustering, messaging, and transaction management, which can significantly enhance the capabilities of IdentityIQ for enterprise environments. In contrast, other options contain application servers that either do not align with the primary technology stack of IdentityIQ or are primarily designed for different types of applications or workloads. This mismatch makes the other options less suitable for deploying SailPoint IdentityIQ effectively.**

## 10. What characterizes conditionally managed artifacts in SailPoint IdentityIQ?

A. They are always migrated across environments

B. They may or may not be migrated across environments

C. They are never managed

D. They are implemented with strict policies

**Conditionally managed artifacts in SailPoint IdentityIQ are characterized by the possibility of migration across environments depending on specific conditions or criteria. This means that not all such artifacts will necessarily be carried over to different environments, such as from development to production; rather, their migration can be influenced by factors like the current state of the artifact, the policies associated with it, or specific deployment requirements. The nature of conditional management allows for flexibility, ensuring that only relevant artifacts are transferred, aiding in maintaining the integrity and context of the identity management processes across different settings. This approach considers various operational parameters, allowing administrators to optimize what gets migrated based on the needs of the organization and the intended environment. In contrast, other characteristics or options mentioned do not accurately capture the essence of conditional management for artifacts within SailPoint IdentityIQ. For instance, stating that they are always or never managed suggests a rigid approach that does not exist for conditionally managed artifacts. Additionally, while strict policies may indeed play a role in managing artifacts, they are not the defining characteristic of conditional management, which is primarily about the selective and situational nature of migration.**