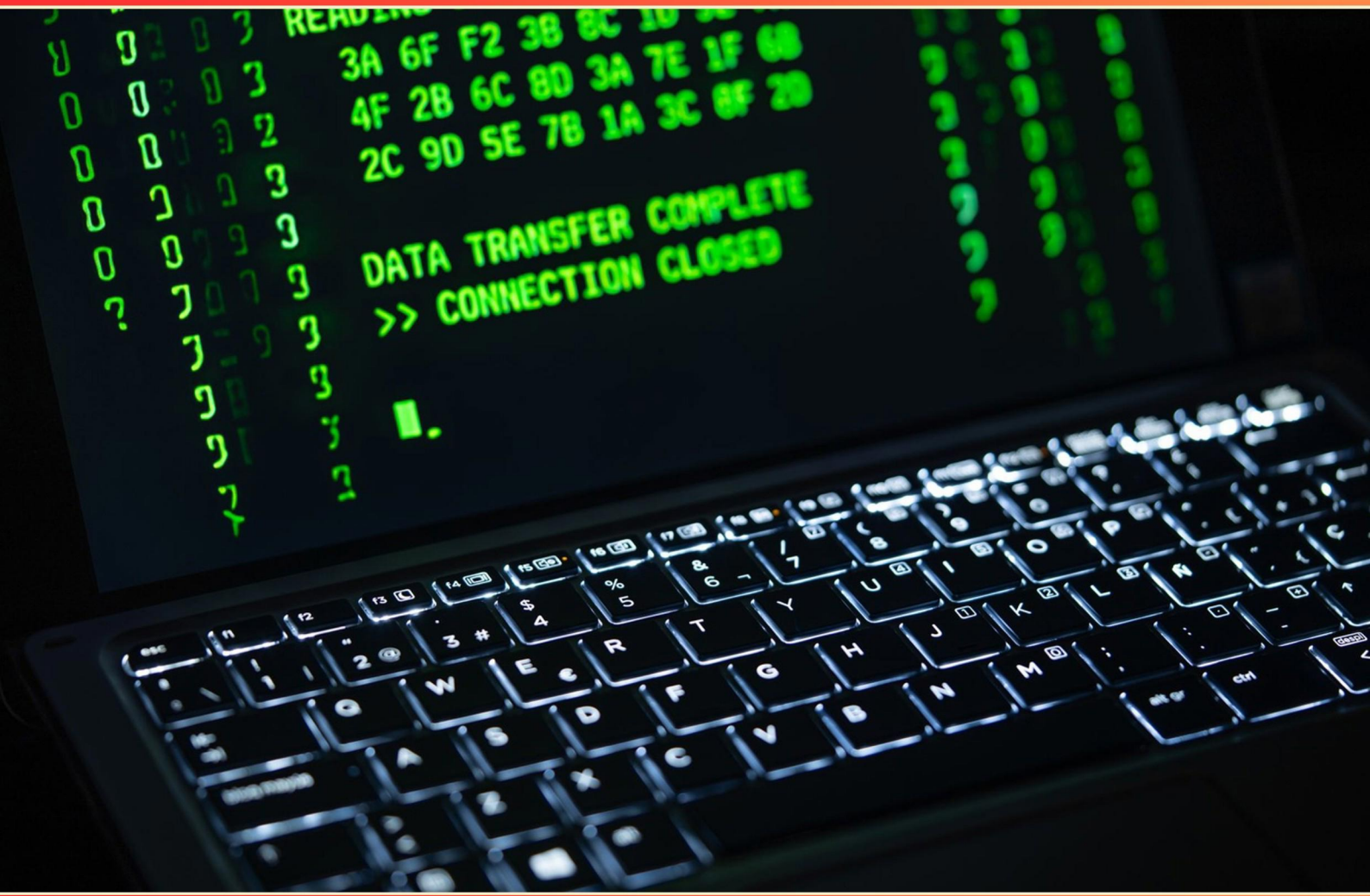
SAILPOINT IDENTITYIQ (IIQ) CERTIFICATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://sailpointidentityiq-iiq.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

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

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 16

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. What are "certification campaigns" in IdentityIQ designed to achieve?

A. To create new user accounts

B. To review access rights and ensure appropriateness

C. To automate identity provisioning

D. To manage cloud application integration

2. What are customizable configuration artifacts in SailPoint IdentityIQ?

A. Elements that cannot be modified for customer implementations

B. Core components that can be customized for each customer implementation

C. Add-ons that require separate licenses for use

D. External modules that enhance functionality

3. How does IdentityIQ facilitate the user onboarding process?

A. By automating the scheduling of training sessions

B. By streamlining account creation and access rights grant

C. By conducting interviews with new users

D. By providing a user-friendly interface

4. What does IdentityIQ provide to track compliance and policy violations?

A. Reporting capabilities

B. System performance metrics

C. Customer feedback tools

D. Employee productivity assessments

5. What is the recommended maximum heap size for JVM as per SailPoint guidelines?

A. 512m

B. 1024m

C. 2048m

D. 256m

SAMPLE

6. Which of the following is a recommended configuration for a small IdentityIQ implementation?

A. Single application server

B. Separate database and host servers

C. Shared database services

D. Dual firewalls

7. What types of authentication does SailPoint IdentityIQ support?

A. LDAP and RADIUS

B. SAML, SSO, and OTP

C. Kerberos and NTLM

D. OAuth and OpenID

8. Among the steps for patching IIQ, which involves the execution of scripts?

A. Backup existing files and database

B. Unpack upgrade files

C. Run relevant database upgrade scripts

D. Regression test

9. How can entitlements affect compliance requirements?

A. They can simplify financial audits

B. They represent access rights that must be monitored for compliance

C. They can eliminate the need for user training

D. They ensure all applications are secure

10. Can IIQ Console connect using JNDI?

A. Yes, it connects through the app server

B. No, it does not connect through the app server

C. Only in specific configurations

D. Yes, but requires additional setup

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What are "certification campaigns" in IdentityIQ designed to achieve?

A. To create new user accounts

B. To review access rights and ensure appropriateness

C. To automate identity provisioning

D. To manage cloud application integration

Certification campaigns in IdentityIQ are specifically designed to review user access rights and assess their appropriateness. The primary goal of these campaigns is to ensure that users have the correct access levels according to their roles and responsibilities within the organization. By conducting certification campaigns, organizations can identify any discrepancies or excessive access that may pose security risks, allowing for timely remediation to maintain compliance and protect sensitive data. Utilizing certification campaigns helps organizations uphold governance standards, mitigate the risk of unauthorized access, and ensure that access rights are constantly aligned with business needs. This process fosters accountability through regular reviews, enabling organizations to make informed decisions about user access and maintain a tight rein on security policies. The other options relate to distinct functionalities of IdentityIQ that are not the primary focus of certification campaigns. For instance, creating new user accounts, automating identity provisioning, and managing cloud application integration serve different purposes within the Identity and Access Management (IAM) framework but do not pertain directly to the certification process aimed at validating and affirming user access rights.

2. What are customizable configuration artifacts in SailPoint IdentityIQ?

A. Elements that cannot be modified for customer implementations

B. Core components that can be customized for each customer implementation

C. Add-ons that require separate licenses for use

D. External modules that enhance functionality

Customizable configuration artifacts in SailPoint IdentityIQ refer to core components that can be tailored to meet the specific needs of each customer implementation. This flexibility is crucial for organizations as it allows them to adapt IdentityIQ to better align with their unique business processes, compliance requirements, and identity governance needs. These artifacts typically include various elements such as workflows, connectors, rules, and policies, which can be adjusted or configured to fit the particular environment or operational requirements of a customer. This capability enables organizations to effectively manage identity and access governance in a way that is optimal for their structure and needs. The other options do not accurately reflect the nature of customizable configuration artifacts. For example, elements that cannot be modified or those that require separate licenses do not align with the concept of configuration artifacts that are intended to be adjustable for organizational requirements. Additionally, while external modules may enhance functionality, they are not the primary focus of customizable artifacts, which are integral to the IdentityIQ framework itself.

SAMPLE

3. How does IdentityIQ facilitate the user onboarding process?

A. By automating the scheduling of training sessions

B. By streamlining account creation and access rights grant

C. By conducting interviews with new users

D. By providing a user-friendly interface

IdentityIQ significantly enhances the user onboarding process primarily through the streamlining of account creation and access rights grants. This automation reduces the time and effort involved in setting up new users within the system. When an organization hires a new employee, it is crucial to ensure they have the appropriate access to necessary resources and systems from the outset. IdentityIQ achieves this by automating the assignment of roles and access rights based on predefined policies, ensuring that users receive the correct permissions aligned with their job functions without manual intervention. This not only improves efficiency and accelerates the onboarding timeline but also minimizes the possibility of human error, enhancing security and compliance by ensuring that access permissions align with organizational policies. Other options, such as automating training sessions or conducting interviews, do not specifically address access management or account setup, which are core elements of the onboarding experience that IdentityIQ focuses on streamlining.

4. What does IdentityIQ provide to track compliance and policy violations?

A. Reporting capabilities

B. System performance metrics

C. Customer feedback tools

D. Employee productivity assessments

IdentityIQ provides robust reporting capabilities that are essential for tracking compliance and identifying policy violations. These reporting tools allow organizations to generate detailed analyses of user access, roles, and entitlements, which help ensure adherence to regulatory requirements and internal policies. By utilizing these capabilities, organizations can easily assess whether access controls are being maintained as intended and identify any deviations that may pose compliance risks. This functionality is critical in auditing processes, where documentation of compliance is necessary. Through various pre-built and customizable reports, administrators can monitor access patterns and quickly highlight any anomalies or violations, facilitating timely remediation actions. As a result, organizations can better protect sensitive information while ensuring that they meet the necessary compliance standards. The other options do not directly address compliance tracking. System performance metrics focus on operational efficiency rather than policy adherence. Customer feedback tools are aimed at enhancing client satisfaction and do not relate to compliance issues. Employee productivity assessments measure work output and efficiency, which is unrelated to the tracking of compliance and policy violations.

SAMPLE

5. What is the recommended maximum heap size for JVM as per SailPoint guidelines?

A. 512m

B. 1024m

C. 2048m

D. 256m

The recommended maximum heap size for the Java Virtual Machine (JVM) in SailPoint IdentityIQ is 1024m (or 1GB). This value is considered optimal for balancing performance and resource usage in the environment where IdentityIQ operates. Setting the heap size at this level allows the application to manage memory effectively, supporting the various operations, such as policy enforcement, provisioning, and reporting, without triggering memory-related performance issues. While larger heap sizes can accommodate more data, they can also lead to longer garbage collection pauses, which may negatively impact application performance. Choosing a smaller heap size, like 512m or 256m, might lead to insufficient memory for application demands, resulting in potential out-of-memory errors during peak usage periods. On the other hand, opting for 2048m would generally be considered excessive for most standard deployments of IdentityIQ, given that it can introduce complexity in memory management and may not provide additional benefits compared to a 1024m setting. By following the recommended maximum heap size of 1024m, organizations implementing SailPoint IdentityIQ can ensure efficient operation while minimizing potential performance issues associated with improper memory configuration.

6. Which of the following is a recommended configuration for a small IdentityIQ implementation?

A. Single application server

B. Separate database and host servers

C. Shared database services

D. Dual firewalls

In a small IdentityIQ implementation, recommending the use of separate database and host servers is advantageous for a few reasons. This configuration helps ensure that the application server, responsible for running IdentityIQ and handling user requests, is decoupled from the database server, which stores all the critical data. By separating these components, you improve security by limiting the attack surface; if the application server is compromised, the database remains isolated and protected. Additionally, having separate servers can lead to better performance since you can allocate specific resources to each server based on their distinct functions. The application server can be optimally configured to handle user transactions, while the database server can be optimized for data storage and retrieval without competing for resources. This setup enhances overall system reliability and scalability, allowing easier upgrades and maintenance for either component without affecting the other. Configurations such as single application servers or shared database services present risks that may not align with best practices for data security and performance, especially as the number of users grows or when regulatory compliance becomes a concern. While dual firewalls add layers of security, they may not be strictly necessary for smaller setups compared to the benefits provided by using separate servers.

SAMPLE

7. What types of authentication does SailPoint IdentityIQ support?

A. LDAP and RADIUS

B. SAML, SSO, and OTP

C. Kerberos and NTLM

D. OAuth and OpenID

SailPoint IdentityIQ supports several types of authentication mechanisms that facilitate secure user access and session management. The selected answer highlights SAML (Security Assertion Markup Language), SSO (Single Sign-On), and OTP (One-Time Password), which are crucial for modern identity and access management. SAML is an open standard that allows for identity federation, enabling users to log in once and gain access to multiple services without having to re-enter credentials, promoting both security and user convenience. SSO enhances this experience by streamlining the login process across various applications. OTP is a robust authentication method that requires users to enter a unique, time-sensitive code for access, thus adding an extra layer of security beyond the traditional username and password. While other options include various authentication protocols, they may not cover the full capability of IdentityIQ or might be less relevant to the functionality provided by the platform in terms of identity management and user experience. SAML, SSO, and OTP effectively reflect the comprehensive approach to authentication in IdentityIQ, catering to both user-friendly access and security requirements.

8. Among the steps for patching IIQ, which involves the execution of scripts?

A. Backup existing files and database

B. Unpack upgrade files

C. Run relevant database upgrade scripts

D. Regression test

The execution of scripts is a crucial step in the patching process of SailPoint IdentityIQ, particularly when it comes to updating the database schema or applying necessary changes that come with a patch. Running relevant database upgrade scripts ensures that the database is aligned with the latest application code, allowing for new features and fixes to function correctly. This step typically involves executing SQL scripts that modify the database structure, update existing data, or add new data, tailored to the new version of the software. While backing up existing files and the database is critical for safety and rollback purposes, it does not involve script execution. Unpacking upgrade files prepares the installation, but it is still not an execution of scripts. Regression testing ensures that existing functions perform as expected after the upgrade, but again, it doesn't pertain directly to executing any scripts intended for updating the database. Thus, the focus on running relevant database upgrade scripts is essential for ensuring that the application's backend can support the new features and adheres to any changes dictated by the latest patch.

SAMPLE

9. How can entitlements affect compliance requirements?

A. They can simplify financial audits

B. They represent access rights that must be monitored for compliance

C. They can eliminate the need for user training

D. They ensure all applications are secure

Entitlements play a critical role in determining access rights for users within an organization. They define what resources users can access and what actions they can perform on those resources. Because of this foundational role in access management, entitlements must be closely monitored to ensure compliance with various regulations and internal policies. This monitoring process helps organizations validate that users have appropriate access levels, which aligns with compliance requirements such as those mandated by regulations like Sarbanes-Oxley (SOX) or GDPR. Compliance frameworks often require organizations to ensure that access rights are properly assigned and managed to mitigate risks associated with unauthorized access or data breaches. Therefore, understanding and monitoring entitlements is essential for demonstrating compliance and for accountability in governance. The other choices provided do not capture the essence of how entitlements specifically relate to compliance. While they may reference other aspects of user access or training, they do not address the fundamental link between entitlements and the ongoing need for compliance oversight. Hence, monitoring entitlements is integral in ensuring compliance is upheld, making the correct choice clear in the context of compliance and identity governance.

10. Can IIQ Console connect using JNDI?

A. Yes, it connects through the app server

B. No, it does not connect through the app server

C. Only in specific configurations

D. Yes, but requires additional setup

The ability of the IIQ Console to connect using JNDI primarily depends on the architecture and deployment of the application server. The correct response establishes that the IIQ Console does not connect through the app server with JNDI. In typical configurations for SailPoint IdentityIQ, the interactions programmed in the console are designed for local processes rather than establishing a JNDI-based connection. Choosing this option indicates an understanding of the underlying mechanics of how the IIQ Console operates without needing a JNDI connection, aligning with best practices in managing system interactions effectively. The traditional approach of IdentityIQ does not necessitate JNDI for its console operations, as the console can work directly with the IdentityIQ environment configured already. The other choices imply different levels of connectivity or dependency on configurations that are usually not applicable to the general operation of the IIQ Console. This aligns with standard practices within SailPoint's architecture regarding data access and system management.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://sailpointidentityiq-iiq.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE