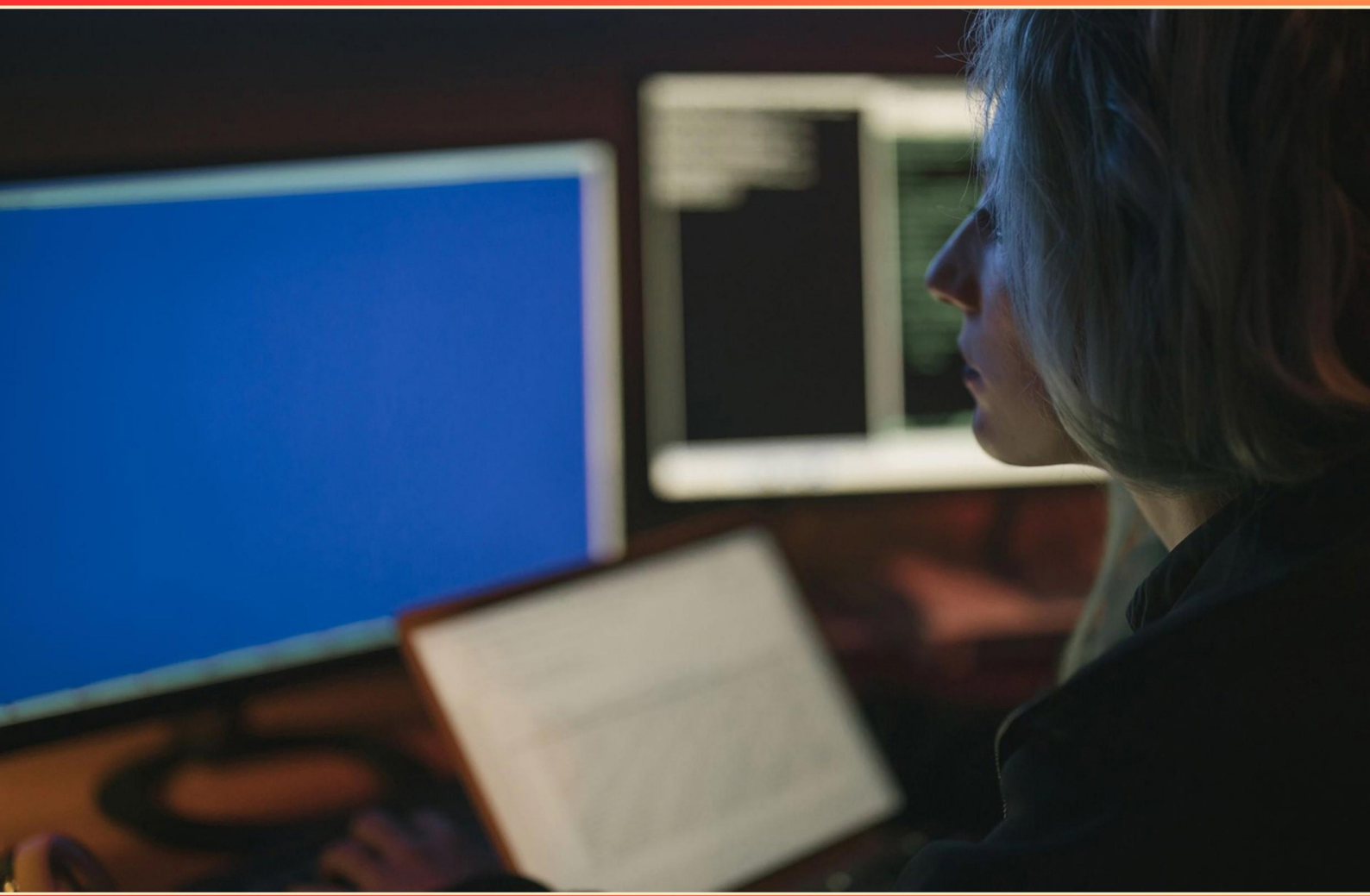
SAVIYNT LEVEL 100 (L100) PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://saviyntl100.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 is the maximum number of records that can be returned when executing an analytics control?

A. 40000

B. 400000

C. 4000000

D. 50000

2. What are the options available in "employment status" within User Manager Certification?

A. Terminated

B. Works for me

C. Extend end date

D. All of the above

3. Which analytical type is considered valid in the system?

A. V0

B. V1

C. V2

D. V3

4. What role does the Saviynt Dashboard play in identity governance?

A. It logs security incidents for future reference

B. It displays graphical analyses of user access and activities

C. It facilitates direct access to all backend features

D. It automates system updates and migrations

5. Which SOD analysis process is designed in Saviynt to identify conflicts or violations after they have occurred according to the pre-defined rulesets?

A. Preventive

B. Detective

C. Simulation

D. Mitigating

SAMPLE

6. Which service does EIC use for user authentication?

A. Only internal database

B. Only external services

C. Both internal and external services

D. None of the above

7. What does 'Audit Trail' signify in Saviynt?

A. A record of user training sessions

B. A log of system errors

C. A log of all access and permission changes

D. A summary of application usage

8. What is the key functionality of SCAN rules?

A. To enforce role-based access controls

B. To handle attribute mapping during user import

C. To assess compliance based on user activity

D. To execute rules based on events

9. What type of security model does Saviynt implement for managing identities?

A. Zero Trust security model

B. Traditional perimeter security model

C. Access Control List (ACL) model

D. Risk-based security model

10. What kind of ruleset would you use for managing non-SAP systems in Saviynt?

A. SAP Ruleset

B. Logical Ruleset

C. Non-SAP Ruleset

D. Mitigation Ruleset

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What is the maximum number of records that can be returned when executing an analytics control?

A. 40000

B. 400000

C. 4000000

D. 50000

The maximum number of records that can be returned when executing an analytics control is 4,000,000. This limit is set to ensure efficient handling of data and to maintain performance standards within the Saviynt platform. Allowing such a large number of records facilitates comprehensive data analysis while still adhering to resource management practices. This capability is particularly important for organizations that need to analyze large datasets for compliance, access management, and governance purposes. It allows users to execute extensive queries without being restricted by lower limits, which could hinder the insights gained from analytics. The other figures provided do not align with the platform's capabilities for handling analytics control returns. Lower limits could potentially limit the functionality for users who need to analyze vast datasets or aggregate information across multiple records, leading to incomplete analyses.

2. What are the options available in "employment status" within User Manager Certification?

A. Terminated

B. Works for me

C. Extend end date

D. All of the above

The correct choice indicates that all listed options are available concerning "employment status" in User Manager Certification. Understanding this involves recognizing the context and roles associated with user management in identity governance. "Terminated" is a status that reflects the current employment state of an individual who is no longer with the organization, which is critical for ensuring that access is effectively managed and that compliance standards are upheld. The option "Works for me" likely represents active employment status, indicating that the user is still engaged with the company and should be granted the appropriate access rights. The choice "Extend end date" suggests that there may be scenarios where an employee's end date (the date their employment is expected to terminate) needs to be modified. This action can be important when considering contract extensions or leaves of absence, contributing to accurate user access management based on employment duration. By encompassing all these statuses, the practice test highlights the necessity for organizations to manage various aspects of user employment comprehensively, ensuring that access and permissions align with current roles within the organization.

SAMPLE

3. Which analytical type is considered valid in the system?

A. V0

B. V1

C. V2

D. V3

In the context of Saviynt and its analytical types, V2 is recognized as a valid analytical type within the system. This designation typically relates to the versioning of analytical data or reporting capabilities that Saviynt supports. Each analytical type corresponds to different functionalities and data structures that can be leveraged for insights and reporting. V2 indicates a level of sophistication or a specific characteristic set that aligns with the requirements of the Saviynt platform, allowing users to engage with the system effectively. This may include improved data handling, integration capabilities, or analytical features that enhance the overall functionality compared to other analytical types. The other options do not represent valid analytical types within the system framework, either due to being outdated or not meeting the operational criteria necessary for effective performance in Saviynt. Understanding these distinctions is crucial for users to optimize their use of the system and ensure they are working with the most compatible and powerful analytical tools available.

4. What role does the Saviynt Dashboard play in identity governance?

A. It logs security incidents for future reference

B. It displays graphical analyses of user access and activities

C. It facilitates direct access to all backend features

D. It automates system updates and migrations

The Saviynt Dashboard serves a pivotal role in identity governance by providing graphical analyses of user access and activities. This capability is essential for organizations seeking to maintain visibility and control over who has access to sensitive resources, thereby aiding in compliance and risk management. By analyzing user access patterns and activities visually, stakeholders can easily identify trends, potential security risks, and anomalies in user behavior. Such insights are crucial for making informed decisions about access privileges, implementing appropriate policies, and responding swiftly to any identified issues. In contrast, logging security incidents is not a function of the dashboard but rather part of incident management processes. Direct access to backend features typically requires administrative privileges and is managed through separate interfaces rather than being a primary function of the dashboard. Lastly, while system updates and migrations are important aspects of maintaining an identity governance system, they do not fall within the dashboard's scope, which is focused on user access analysis rather than system maintenance.

SAMPLE

5. Which SOD analysis process is designed in Saviynt to identify conflicts or violations after they have occurred according to the pre-defined rulesets?

A. Preventive

B. Detective

C. Simulation

D. Mitigating

The detective analysis process in Saviynt is specifically designed to identify conflicts or violations that have already occurred, based on established rulesets. This process plays a crucial role in risk management and compliance, allowing organizations to monitor and review access rights and configurations after they are implemented. By doing so, it ensures that any discrepancies or policy violations can be detected and addressed subsequently. Detective controls are essential in governance as they help organizations understand their security posture and compliance status, often leading to investigations and corrective actions to remedy any identified issues. This is distinct from preventive controls, which aim to stop violations before they happen, and from simulation, which involves testing the system under hypothetical scenarios without affecting live data. Mitigating, on the other hand, refers to strategies put in place to reduce the impact of violations, rather than identifying them post-factum.

6. Which service does EIC use for user authentication?

A. Only internal database

B. Only external services

C. Both internal and external services

D. None of the above

EIC, or Enterprise Identity Cloud, utilizes both internal and external services for user authentication to provide a flexible and comprehensive identity management solution. By incorporating both types of services, EIC can cater to various user authentication needs, integrating seamlessly with existing internal systems while also leveraging external identity providers and services for enhanced security and scalability. The combination allows organizations to authenticate users based on their existing infrastructure, such as directories or databases, while also utilizing third-party solutions for advanced features or when dealing with external partners. This hybrid approach ensures that a wide range of authentication methods can be employed, accommodating various organizational requirements and user scenarios efficiently.

7. What does 'Audit Trail' signify in Saviynt?

A. A record of user training sessions

B. A log of system errors

C. A log of all access and permission changes

D. A summary of application usage

The concept of 'Audit Trail' in Saviynt specifically refers to a comprehensive log of all access and permission changes within the system. This feature plays a crucial role in maintaining security and accountability as it provides a detailed record of who accessed what information, when changes were made to permissions, and the nature of those changes. This logging mechanism is vital for auditing purposes, allowing organizations to track modifications, investigate incidents, and ensure compliance with regulatory standards. The significance of having an Audit Trail extends to safeguarding sensitive data by making it easier to identify unauthorized access or misconfigurations. By having this thorough visibility into access and changes, organizations can better manage risk and protect their information assets.

SAMPLE

8. What is the key functionality of SCAN rules?

A. To enforce role-based access controls

B. To handle attribute mapping during user import

C. To assess compliance based on user activity

D. To execute rules based on events

The key functionality of SCAN rules is to assess compliance based on user activity. SCAN rules are fundamentally designed to monitor and analyze user actions within an organization to ensure they align with compliance requirements, internal policies, and regulatory standards. By evaluating user behavior, these rules can identify any anomalies or potential violations that need to be addressed, thereby supporting the security and governance frameworks of the organization. Understanding user activity in terms of compliance is crucial for maintaining security standards and compliance with industry regulations. SCAN rules help organizations proactively manage risk and enforce accountability by providing insights into how users interact with systems and data. This capability is vital for organizations striving to maintain a secure and compliant operational environment.

9. What type of security model does Saviynt implement for managing identities?

A. Zero Trust security model

B. Traditional perimeter security model

C. Access Control List (ACL) model

D. Risk-based security model

Saviynt implements a Zero Trust security model for managing identities, which is foundational to its approach in identity governance. The Zero Trust framework is based on the principle of "never trust, always verify." In this model, no user, device, or network is automatically trusted; instead, all interactions must be verified and authenticated before access to resources is granted. This is particularly important in today's diverse IT environments, where users access company resources from various locations and devices. By utilizing a Zero Trust model, Saviynt enhances security through continuous monitoring and validation of user identities and access rights. This model focuses on minimizing the attack surface and mitigating risks by enforcing least privilege access, dynamic access controls, and contextual policies. It aligns with modern security needs, as threats are often internal or stem from trusted devices that have been compromised. While traditional perimeter security models rely on fortified boundaries to protect the network, they can fall short in a world where cloud services and remote work are prevalent. Similarly, Access Control Lists (ACL) provide a simplistic way to manage permissions but do not encompass the adaptive and contextual analysis required in today's security landscape. The Risk-based security model evaluates risks associated with specific behaviors or contexts, but it lacks the comprehensive approach that Zero Trust embodies, focusing

SAMPLE

10. What kind of ruleset would you use for managing non-SAP systems in Saviynt?

A. SAP Ruleset

B. Logical Ruleset

C. Non-SAP Ruleset

D. Mitigation Ruleset

The appropriate choice for managing non-SAP systems in Saviynt is a Non-SAP Ruleset. This type of ruleset is specifically designed to cater to the governance, risk, and compliance (GRC) needs of systems that are not part of the SAP ecosystem. It provides the necessary framework for managing user access and entitlements in various types of non-SAP applications, ensuring that organizations can effectively apply their security policies and compliance requirements across a diverse range of systems. By using a Non-SAP Ruleset, organizations can implement tailored controls and rules that are specifically relevant to their non-SAP applications, which might have different functionalities, permission sets, and compliance requirements compared to SAP systems. This approach ensures a more effective management of identity governance, access controls, and overall risk management for non-SAP environments. The other types of rulesets mentioned do not serve the same purpose as the Non-SAP Ruleset. For instance, a SAP Ruleset is specifically tailored for SAP systems and would not be suitable for non-SAP applications. Logical Rulesets might focus on logical attributes or conditions within applications but do not specifically address the unique needs of non-SAP systems. Mitigation Rulesets typically deal with the processes and protocols to mitigate risks associated

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://saviyntl100.examzify.com

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

SAMPLE