CYBERARK PRIVILEGED ACCESS SECURITY (PAS) ADMINISTRATION PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberarkpasadmin.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. Which report would show the accounts and safes a user can access?

A. Privileged Account Inventory Report

B. Entitlement Report

C. Applications Inventory Report

D. Activity Log Report

2. Which of the following best describes the relationship between the Server Key and the Safe Key?

A. The Server Key encrypts the Safe Key

B. The Safe Key encrypts the Server Key

C. The Server Key is used to decrypt the Safe Key

D. The Safe Key is used to manage the Server Key

3. What is the goal of the password verification process in CyberArk?

A. Update passwords periodically

B. Confirm passwords stored in the Vault match the target system

C. Eliminate duplicate passwords

D. Secure user credentials

4. What is the function of Password Vault Web Access (PVWA)?

A. Configures hardware security

B. Provides access to privileged account information

C. Changes server configurations

D. Manages user roles and permissions

5. Which role is specifically designated to checks and audits within the PSM recording safe?

A. System Administrator

B. Auditor

C. Vault Manager

D. Data Reviewer

SAMPLE

6. What are the three safes created during the installation of Vault?

A. Notification Engine, System, VaultInternal

B. Database, User, System

C. Report, Configuration, Private User Preferences

D. Admin, Backup, Security

7. Which of the following is NOT one of the steps in PAM Protection?

A. Proactive protection

B. Systematic assessment

C. Targeted detection

D. Real-time response

8. What is the purpose of fetching the privileged account password from the Vault in the PSMP flow?

A. To authenticate the session

B. To encrypt data

C. To log user actions

D. To store session history

9. What occurs during the communication process after SSH session establishment?

A. All data is transmitted in plaintext

B. Both client and server use passwords for communication

C. All communication is encrypted with the agreed session key

D. Commands are logged by the server for auditing

10. Which report would you use to see a list of all user authorizations?

A. License Capability Report

B. Users List

C. Active/Non-Active Users

D. Safes List

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which report would show the accounts and safes a user can access?

A. Privileged Account Inventory Report

B. Entitlement Report

C. Applications Inventory Report

D. Activity Log Report

The Entitlement Report is the correct choice for displaying the accounts and safes that a user can access within CyberArk's Privileged Access Security framework. This report is specifically designed to showcase the privileges assigned to each user, detailing what accounts, safes, and the associated permissions are granted to them. In the context of privileged access management, understanding user entitlements is crucial for maintaining security and compliance. It enables administrators to ensure that users have appropriate access levels, thereby minimizing the risk of unauthorized access to sensitive data. Other reports do not provide the same level of detail regarding user access permissions. For example, the Privileged Account Inventory Report focuses on listing the privileged accounts available in the system but does not give insights into which specific users have access to those accounts. The Applications Inventory Report typically catalogs applications and their configurations rather than user entitlements. Finally, the Activity Log Report is intended to track user activities and actions but does not indicate what accounts or safes a user can access. This context underscores why the Entitlement Report is the most relevant option for identifying user access within the CyberArk PAS environment.

2. Which of the following best describes the relationship between the Server Key and the Safe Key?

A. The Server Key encrypts the Safe Key

B. The Safe Key encrypts the Server Key

C. The Server Key is used to decrypt the Safe Key

D. The Safe Key is used to manage the Server Key

The relationship between the Server Key and the Safe Key is fundamentally about encryption and security management within CyberArk's architecture. The Server Key acts as a protective mechanism that secures sensitive keys, including the Safe Key, which is responsible for controlling access to secrets stored in CyberArk. When considering the correct answer, the role of the Server Key in the decryption process is essential; it is used to decrypt the Safe Key. This means that the Safe Key cannot be accessed or utilized unless it is first decrypted by the Server Key. This relationship emphasizes the hierarchical nature of key management in CyberArk, where the Server Key provides the underlying security framework that protects other keys. In this operational model, understanding the hierarchy and the functions of these keys is critical for effective privileged access management. Properly managing these keys ensures that sensitive data remains secure while still being accessible to authorized processes within the CyberArk infrastructure.

SAMPLE

3. What is the goal of the password verification process in CyberArk?

A. Update passwords periodically

B. Confirm passwords stored in the Vault match the target system

C. Eliminate duplicate passwords

D. Secure user credentials

The goal of the password verification process in CyberArk is to confirm that the passwords stored in the Vault match those on the target system. This verification is crucial in maintaining the integrity and accuracy of the passwords that CyberArk manages for privileged accounts. When the passwords in the Vault align with those on the actual target systems, it ensures that users can effectively authenticate and access the necessary resources without compromising security. This process not only helps in ensuring that users have the correct credentials to access privileged accounts but also serves as a security measure to detect any discrepancies that might indicate a compromised account or potential security breach. By regularly verifying these passwords, CyberArk helps organizations maintain strong security postures over their privileged access.

4. What is the function of Password Vault Web Access (PVWA)?

A. Configures hardware security

B. Provides access to privileged account information

C. Changes server configurations

D. Manages user roles and permissions

The function of Password Vault Web Access (PVWA) is primarily focused on providing access to privileged account information. PVWA serves as the web interface for CyberArk's Privileged Access Security solution, enabling users to securely access and manage privileged accounts such as administrator credentials. Through PVWA, authorized users can view, retrieve, and request access to credentials stored in the CyberArk vault, ensuring that sensitive information is carefully controlled and monitored. This role is critical in maintaining security and compliance, as it facilitates the proper handling of privileged accounts while allowing for efficient workflows. Other options pertain to functionalities that are not specific to PVWA. While managing user roles and permissions is a function within the CyberArk ecosystem, it typically takes place in the CyberArk administration tools rather than directly through PVWA. Conversely, configuring hardware security and changing server configurations fall outside the scope of what PVWA handles, as those tasks are generally managed through other components of the CyberArk system or external systems altogether.

5. Which role is specifically designated to checks and audits within the PSM recording safe?

A. System Administrator

B. Auditor

C. Vault Manager

D. Data Reviewer

The role designated specifically for checks and audits within the Privileged Session Manager (PSM) recording safe is the Auditor role. This role is crucial for ensuring compliance and security within the organization. Auditors have access rights that may include the capability to review and analyze recorded sessions, which typically consist of privileged actions taken during those sessions. Their responsibilities often involve maintaining oversight, conducting investigations, and ensuring that all activities align with organizational policies and regulatory requirements. The Auditor's functions are pivotal in facilitating transparency and accountability in the management of privileged access, making this role essential for any security framework. By regularly reviewing PSM recordings, auditors can identify potential security breaches or policy violations, thus playing a vital role in enhancing the overall security posture of the organization.

SAMPLE

6. What are the three safes created during the installation of Vault?

A. Notification Engine, System, VaultInternal

B. Database, User, System

C. Report, Configuration, Private User Preferences

D. Admin, Backup, Security

The three safes created during the installation of Vault — Notification Engine, System, and VaultInternal — serve essential functions in the CyberArk environment. The Notification Engine safe stores credentials that allow the Vault to communicate with the Notification Engine service, enabling alerts and notifications based on predefined conditions. This is crucial for maintaining awareness of system status and alerts regarding any activities that require administrator attention. The System safe is a central repository for CyberArk's internal processes and configurations. It typically contains critical information necessary for the overall operation of the CyberArk platform, including configurations related to other components, making it pivotal for the system's functionality and integrity. The VaultInternal safe is specifically designed to store data required for internal Vault operations, including the storage of administrative credentials and other components vital for the secure and effective management of privileged accounts and access. Together, these safes ensure the secure operation and communication of various aspects of the CyberArk PAS, which is integral for managing privileged access securely and effectively within an organization.

7. Which of the following is NOT one of the steps in PAM Protection?

A. Proactive protection

B. Systematic assessment

C. Targeted detection

D. Real-time response

In the context of PAM (Privileged Access Management) Protection, each step is crucial in securing privileged credentials and preventing unauthorized access. Proactive protection, targeted detection, and real-time response all emphasize an active approach to safeguarding privileged accounts. Proactive protection involves putting measures in place to prevent potential breaches before they occur. Targeted detection focuses on identifying any suspicious activities or anomalies related to privileged accounts. Real-time response ensures that organizations can act swiftly in reaction to any detected threats, minimizing the risk of damage. "Systematic assessment" does not typically align with the primary steps in PAM protection as outlined in standard frameworks. While assessment might play a role in the overall security posture, it isn't part of the core PAM Protection process, which is more focused on active measures rather than evaluative assessments. Thus, it is seen as an outlier compared to the other steps, leading to its classification as not a step in the PAM Protection framework.

SAMPLE

8. What is the purpose of fetching the privileged account password from the Vault in the PSMP flow?

A. To authenticate the session

B. To encrypt data

C. To log user actions

D. To store session history

Fetching the privileged account password from the Vault during the Privileged Session Manager for PaaS (PSMP) flow serves a critical function in establishing a secure authentication process for user sessions. When a user initiates a session to access a privileged account, the PSMP utilizes the stored password from the Vault to authenticate that session. This ensures that only authorized users can gain access to sensitive systems and resources, thus maintaining the integrity and security of the environment. The act of retrieving the password securely from the Vault allows for a controlled access mechanism, where the password is never directly exposed to the user or the application facilitating the session. By authenticating the session in this manner, CyberArk enhances security while enabling compliance with best practices in privileged access management. Other options focus on aspects that are not directly related to the core functionality of fetching the password for initiating and securing a session. For instance, while encryption of data and logging user actions are important aspects of overall security processes, they do not represent the primary reason for obtaining the privileged account password specifically from the Vault. Similarly, storing session history is an essential part of compliance and auditing but does not explain the immediate function of password retrieval in the context of authenticating a session. Thus, the primary purpose is centered on

9. What occurs during the communication process after SSH session establishment?

A. All data is transmitted in plaintext

B. Both client and server use passwords for communication

C. All communication is encrypted with the agreed session key

D. Commands are logged by the server for auditing

After an SSH (Secure Shell) session is established, the critical aspect of the communication process is that all communication between the client and server is encrypted using the session key agreed upon during the initial handshake process. This encryption ensures that sensitive data, including commands and responses, is protected from eavesdropping, man-in-the-middle attacks, and other potential vulnerabilities. During the SSH session establishment, the client and server agree on encryption algorithms and generate a session key. This key is used to encrypt all data transmitted during the session. As a result, any information exchanged remains confidential and secure, preventing unauthorized access and maintaining the integrity of the communication. The encryption provided by SSH is a fundamental feature that distinguishes it from other protocols, allowing secure remote administration and file transfers over insecure networks. This capability is particularly crucial in environments where data sensitivity and security are paramount. Other options do not reflect the core functionality of SSH. For example, transmitting data in plaintext contradicts the purpose of SSH. Using passwords for communication is not accurate as SSH primarily relies on public/private key pairs for secure authentication, although passwords can be an option. While logging commands for auditing is a best practice in maintaining access records, it is not a fundamental characteristic of the SSH protocol itself.

SAMPLE

10. Which report would you use to see a list of all user authorizations?

A. License Capability Report

B. Users List

C. Active/Non-Active Users

D. Safes List

The Users List report is specifically designed to provide comprehensive details regarding user accounts within CyberArk, including their authorizations and the associated privileges. This report allows administrators to review each user's access levels and permissions to various safes or resources managed by CyberArk. By analyzing the Users List, one can effectively assess and manage user privileges, ensuring that access is granted appropriately and securely. In contrast, the other reports have different focuses. The License Capability Report primarily provides information on the licenses allocated and the capabilities associated with them, but it does not detail user access rights. The Active/Non-Active Users report categorizes users based on their activity status but does not reflect their authorizations. The Safes List report gives an overview of safes in the system and their configurations, but it does not provide insights into individual user permissions. Hence, for a clear view of all user authorizations, the Users List is the most relevant report.

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://cyberarkpasadmin.examzify.com

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

SAMPLE