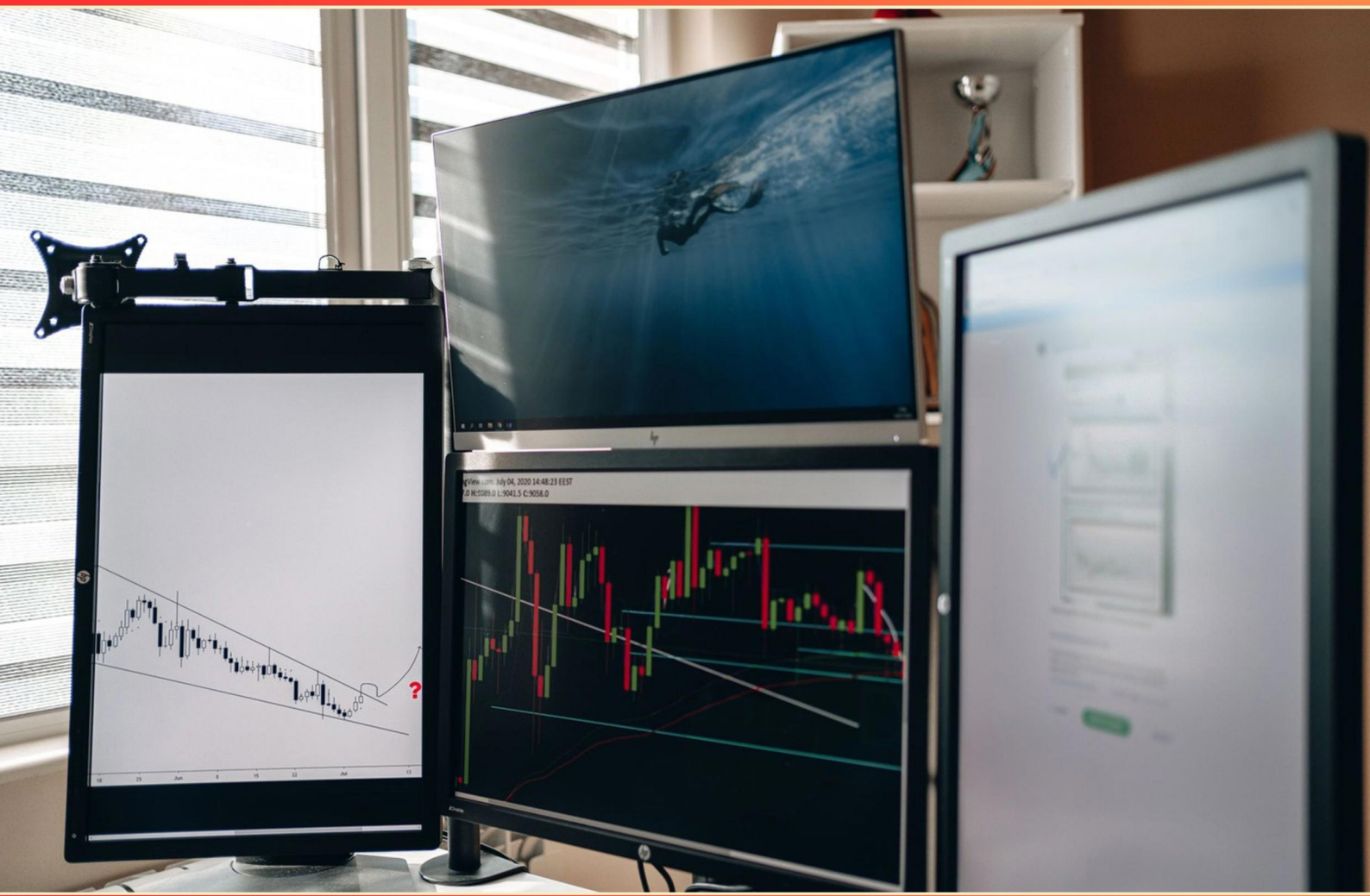
CYBERARK CERTIFIED DELIVERY ENGINEER (CDE) TRAINING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberarkcdetraining.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. **The Safes List report is essential for managing what aspect of CyberArk?**
   - A. User login credentials
   - B. Safe-related access controls
   - C. Password complexities
   - D. Audit compliance

2. **What is the primary authentication method for Windows in CyberArk?**
   - A. SAML
   - B. OracleSSO
   - C. Windows
   - D. RADIUS

3. **What does the Users List Report include about disabled users?**
   - A. Only shows their last active date
   - B. Excludes them from the report entirely
   - C. Lists all users including disabled according to location
   - D. Shows only the user IDs

4. **What type of load balancing does CyberArk recommend?**
   - A. Round-robin based
   - B. Application-aware deployed as reverse proxy
   - C. IP-based load balancing
   - D. Content-based routing

5. **Why might an organization run the Users List Report?**
   - A. To determine potential security risks
   - B. To assess user permissions
   - C. To identify only active users
   - D. To verify audit trails

6. **What type of authenticators does CyberArk require for 2-factor authentication?**
   - A. Only primary authenticators
   - B. Only secondary authenticators
   - C. Two different types of authenticators
   - D. Exclusive use of biometric authentication

SAMPLE

7. What strategy is recommended for creating a CyberArk Recovery Plan?

A. Test it once a year

B. Implement regular updates without testing

C. Create and periodically test the recovery plan

D. Depend on user backup plans

8. What integration allows the Vault Administrator to forward audit records from the Vault to SIEM?

A. SNMP

B. SYSLOG

C. HTTP

D. SMTP

9. What can users do with the Safe permission Update Account Properties?

A. Manage logon and reconcile accounts

B. Copy account configurations

C. Lock accounts for security

D. Sell account access rights

10. What action can users take with the Safe permission "Backup Safe"?

A. Restore previous versions of accounts

B. Backup the Safe

C. View audit logs

D. Manage permissions for safe members

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. The Safes List report is essential for managing what aspect of CyberArk?

A. User login credentials

B. Safe-related access controls

C. Password complexities

D. Audit compliance

The Safes List report plays a critical role in managing safe-related access controls within CyberArk. This report provides a comprehensive view of all the safes configured in the CyberArk environment, detailing which users or groups have access to each safe, along with the specific privileges assigned. By using this report, administrators can effectively review and manage permission settings, ensuring that access is granted appropriately based on user roles and security policies. Proper management of access controls is vital for maintaining the principle of least privilege, minimizing the risk of unauthorized access to sensitive credentials and information stored within safes. Additionally, it aids in regular review processes and expedites audits, as administrators can quickly identify who has access to what, and adjust permissions if necessary. While user login credentials, password complexities, and audit compliance are important aspects of CyberArk, they are not the primary focus of the Safes List report. Instead, this report directly addresses the management and oversight of access controls associated with the safes, emphasizing its essential function in maintaining security and organization within CyberArk's privileged access management framework.

2. What is the primary authentication method for Windows in CyberArk?

A. SAML

B. OracleSSO

C. Windows

D. RADIUS

The primary authentication method for Windows in CyberArk is Windows authentication. This method leverages the built-in authentication mechanisms of the Windows operating system, allowing users to authenticate using their existing Windows credentials. This approach integrates seamlessly with Active Directory, enabling organizations to manage access securely and efficiently without requiring additional credentials or systems. Using Windows authentication simplifies user login processes and enhances security by utilizing the robust security policies inherent within the Windows environment. It is the most straightforward method for users who are already part of a Windows domain, as it allows for single sign-on capabilities and minimizes the risk of password fatigue. Other options, while relevant in specific contexts, serve different purposes or apply to different systems. SAML is typically used for web-based single sign-on and federated identity management. OracleSSO is designed for Oracle systems and is not commonly associated with CyberArk's primary authentication needs. RADIUS, while a widely-used protocol for network authentication, does not specifically represent the primary method used for Windows authentication in CyberArk's environment. Therefore, Windows authentication stands out as the standard and prominent method in this context.

SAMPLE

3. What does the Users List Report include about disabled users?

A. Only shows their last active date

B. Excludes them from the report entirely

C. Lists all users including disabled according to location

D. Shows only the user IDs

The Users List Report is designed to provide a comprehensive view of all users within the environment, including those who are disabled. By listing all users, the report enables administrators to have a complete understanding of the user landscape, facilitating better management and compliance. Including disabled users in the report is important for several reasons. It allows organizations to track user accounts that may need to be reviewed for security purposes or potential reactivation. Additionally, it assists in monitoring compliance with internal policies regarding user access and can help in audits where visibility into all accounts, including those that are inactive, is necessary. This feature is particularly useful for organizations that adhere to strict regulatory standards or those that require detailed record-keeping for security audits. The report may also provide filtering options based on location, making it easier to manage users across different geographies. This comprehensive approach ensures that no aspect of user management is overlooked, especially concerning disabled accounts.

4. What type of load balancing does CyberArk recommend?

A. Round-robin based

B. Application-aware deployed as reverse proxy

C. IP-based load balancing

D. Content-based routing

CyberArk recommends application-aware load balancing deployed as a reverse proxy because this approach ensures that the load balancer can intelligently route traffic based on the specific application layer protocols and user requests. Application-aware load balancing can perform health checks on backend services and make routing decisions based on the state of the application or the content of requests. This means it can ensure that traffic is directed to the most appropriate endpoint, which can improve performance and reliability significantly. In contrast, round-robin based load balancing, while simple, does not consider the health or performance of the back-end servers or services. It treats each server equally regardless of its current load or ability to handle requests effectively. IP-based load balancing also lacks the fine-tuned control of application-state and specific request handling that application-aware systems provide, leading to potential inefficiencies. Content-based routing, while useful in some contexts, can introduce additional complexity and may not always be necessary for typical CyberArk deployments. Thus, application-aware load balancing deployed as a reverse proxy is favored for its ability to dynamically adapt to the needs of the application and ensure optimal performance and security.

SAMPLE

5. Why might an organization run the Users List Report?

A. To determine potential security risks

B. To assess user permissions

C. To identify only active users

D. To verify audit trails

Running the Users List Report provides valuable insights into the user accounts within an organization's system. This report specifically aids in determining potential security risks by highlighting various aspects such as account status, roles, and permissions. By examining the users listed and their associated privileges, organizations can identify any accounts that may have excessive permissions or those that are no longer needed. Such accounts may pose security risks, especially if they belong to former employees or if roles have changed without corresponding updates to access rights. This context helps organizations maintain tighter security and better governance over their user base. While other reports might focus on permissions or user activity, the primary utility of the Users List Report is its ability to give a broad view of user accounts, enabling organizations to proactively address potential vulnerabilities stemming from improper access levels or inactive accounts.

6. What type of authenticators does CyberArk require for 2-factor authentication?

A. Only primary authenticators

B. Only secondary authenticators

C. Two different types of authenticators

D. Exclusive use of biometric authentication

In the context of CyberArk's approach to securing access, two-factor authentication (2FA) is designed to enhance security by requiring users to present two different types of authenticators before granting access. This adds an additional layer of protection because it combines something the user knows (like a password) with something the user has (like a token or a smartphone app) or even something the user inherently is (biometric data). The requirement for two different types of authenticators allows for a more robust security posture, making it significantly more difficult for unauthorized users to gain access. For instance, if a password is compromised, the second factor (a physical token or biometric verification) is still needed to complete the authentication process, thus safeguarding sensitive information housed within the CyberArk vault. Other options might suggest limitations to primary or secondary authenticators only or focus on singular methods like biometrics. However, CyberArk's design philosophy prioritizes flexibility and security by incorporating a range of authentication methods to cover various scenarios and user environments. This ensures that organizations can adapt their authentication methods to meet their specific security requirements.

SAMPLE

7. What strategy is recommended for creating a CyberArk Recovery Plan?

A. Test it once a year

B. Implement regular updates without testing

C. Create and periodically test the recovery plan

D. Depend on user backup plans

Creating and periodically testing a recovery plan is essential in ensuring that an organization can swiftly restore its CyberArk environment in the event of a failure or disaster. This strategy emphasizes not just the creation of a recovery plan but also the importance of regular testing to validate its effectiveness. Periodic testing allows teams to familiarize themselves with the recovery processes and identify any potential gaps or issues in the plan, making necessary adjustments. By actively engaging in this cycle of review and improvement, organizations can ensure that their recovery strategies remain relevant to evolving technology and compliance requirements. Regular updates, when paired with testing, help to reinforce confidence that the procedures will work as intended when actually needed, thus safeguarding the organization's assets and reducing downtime. Other strategies, such as relying on user backup plans or implementing updates without testing, are less effective because they may not ensure a thorough and systematic approach to recovery. Testing once a year may seem sufficient, but regular and more frequent testing promotes continuous improvement and readiness. Therefore, the best approach combines the creation of the recovery plan with ongoing testing to ensure resilience and preparedness.

8. What integration allows the Vault Administrator to forward audit records from the Vault to SIEM?

A. SNMP

B. SYSLOG

C. HTTP

D. SMTP

The correct choice is SYSLOG, which is a standard protocol used for sending and receiving log messages in an IP network. In the context of CyberArk, SYSLOG integration enables the Vault Administrator to forward audit records generated by the Vault to a Security Information and Event Management (SIEM) system. This integration is crucial for monitoring, analyzing, and correlating security events in real-time. Using SYSLOG provides the advantage of streamlined log management where audit records from various sources can be consolidated into a central SIEM system. This enhances the organization's ability to detect and respond to security incidents effectively. The SYSLOG format is widely accepted, making it compatible with many SIEM products, allowing for easier integration and management of security logs. The other options, while they may have their specific uses, do not facilitate the forwarding of audit records in the same standardized manner as SYSLOG. For instance, SNMP is typically used for network management protocols and monitoring, while HTTP and SMTP are protocols primarily used for web communication and email transfer, respectively. These do not align with the primary function of handling and transmitting log data securely to a SIEM system.

SAMPLE

9. What can users do with the Safe permission Update Account Properties?

A. Manage logon and reconcile accounts

B. Copy account configurations

C. Lock accounts for security

D. Sell account access rights

The Safe permission "Update Account Properties" allows users to manage logon and reconcile accounts effectively. This permission is essential for maintaining and configuring sensitive account settings within CyberArk's privileged access management system. Users with this permission can modify necessary parameters such as the username, password, and other account properties, which are crucial for ensuring that services have access to the right credentials and that those credentials are regularly updated and reconciled to adhere to security policies. The ability to manage logon ensures that the accounts can access the necessary resources, while reconciliation automates the process of verifying that passwords are current and accurately stored in the vault. This helps maintain the integrity and security of sensitive account information, which is paramount in managing privileged access and minimizing potential risks associated with account misuse. The other options do not accurately describe the purpose of the "Update Account Properties" permission. For instance, copying account configurations and locking accounts may relate to different permissions that facilitate administrative tasks but are not covered under the scope of updating account properties. Selling account access rights is not a function of any permission within the CyberArk system and contradicts security best practices regarding privileged access.

10. What action can users take with the Safe permission "Backup Safe"?

A. Restore previous versions of accounts

B. Backup the Safe

C. View audit logs

D. Manage permissions for safe members

The "Backup Safe" permission in CyberArk is specifically designed to allow users the capability to create a backup of a Safe. This action is critical for ensuring that the data stored within the Safe can be preserved and restored in case of data loss or corruption. When a user has the "Backup Safe" permission, they can securely export the contents of the Safe, which includes sensitive information such as passwords and other secrets, to a backup file. This functionality is essential for organizations to maintain a robust disaster recovery strategy and to comply with security and regulatory requirements. By enabling backups, organizations ensure that they have a reliable measure in place to retrieve vital information when needed and safeguard against potential data compromises. In contrast, the other options do not accurately align with the capabilities granted by the "Backup Safe" permission. For instance, restoring previous versions of accounts involves functionalities not specifically linked to the backup process, viewing audit logs pertains to monitoring activity, and managing permissions for Safe members deals with access control rather than data backup. Each of these aspects serves distinct purposes within the CyberArk ecosystem.

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://cyberarkcdetraining.examzify.com

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

SAMPLE