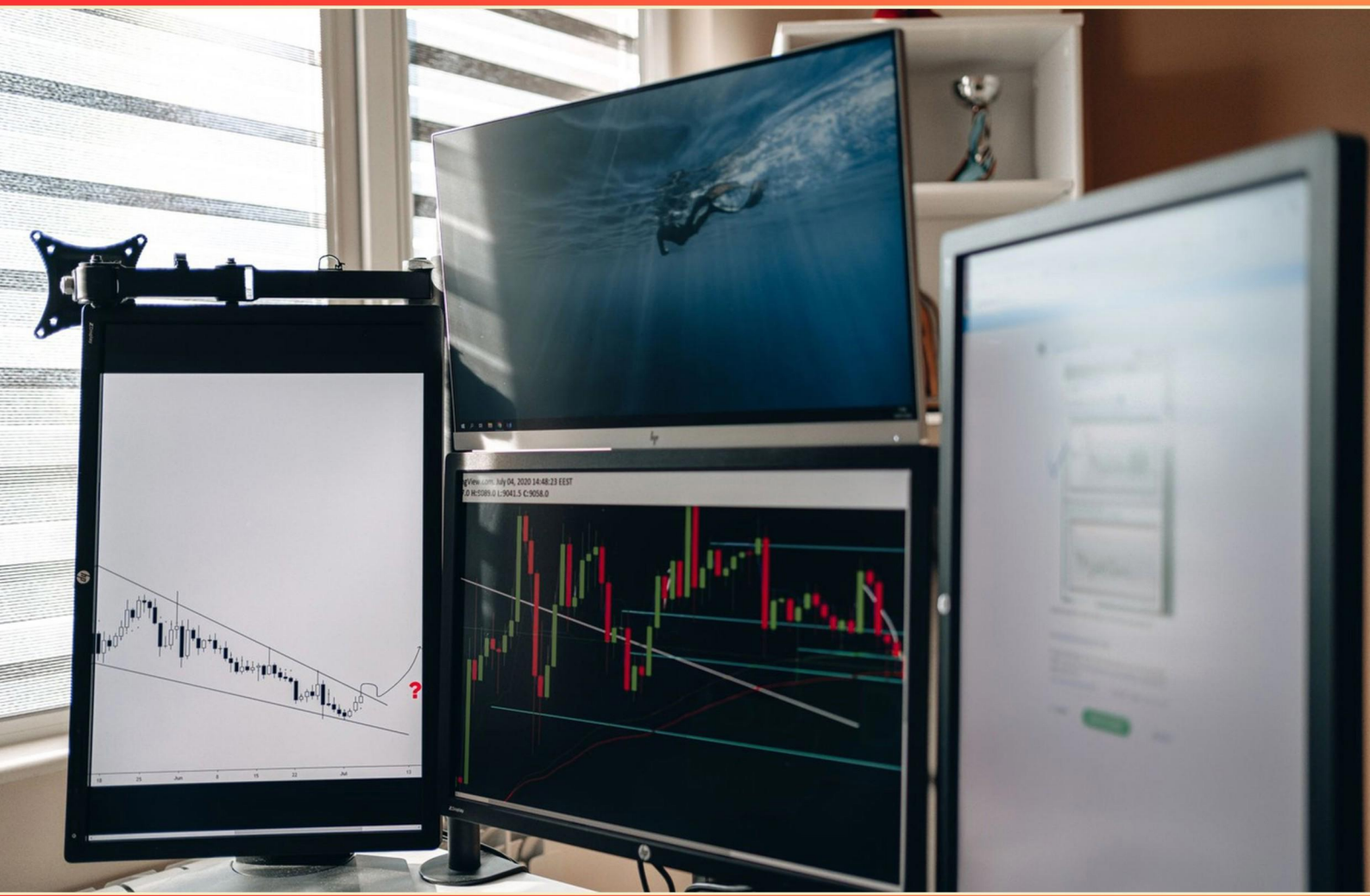
CYBERARK CERTIFIED DELIVERY ENGINEER (CDE) TRAINING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cyberarkcdetraining.examzify.com

Table of Contents

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.

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!

Questions

1. How many permissions can be assigned to a user in the Vault?

A. 5

B. 10

C. 15

D. 20

2. How does a Vault Administrator configure the CyberArk Disaster Recovery (DR) solution to perform automatic failover in case of a failure in the Primary Vault?

A. Setting EnableFailover=yes in vault.ini

B. Setting EnableFailover=yes in padr.ini

C. Modifying the dbparm.ini file

D. Updating the cpm.ini file

3. What is the primary action associated with the permission "Backup Safe"?

A. Restore previous data

B. Generate reports about account usage

C. Create a backup of the Safe

D. Change passwords for all accounts

4. Which port is used by NTP for network time synchronization?

A. UDP port 123

B. TCP port 22

C. TCP port 3389

D. TCP port 445

5. What does the Safe permission Create Folders allow users to do?

A. Rename existing folders in a safe

B. Delete folders within a safe

C. Create new folders in a safe

D. Move existing accounts to different folders

6. What information is provided by the PrivateArk report Users List Report?

A. Lists all users according to their roles

B. Lists all users (including disabled) according to location

C. Displays active users only during business hours

D. Shows user permissions for each safe

7. What does the Safe permission Add Accounts allow users to do?

A. Add accounts in the safe

B. View account details

C. Edit existing accounts

D. Run accounts backup

8. What file is utilized for configuring new firewall rules on the vault?

A. firewall.cfg

B. dbparm.ini

C. config.xml

D. rules.txt

9. What does the Export Data Vault (EVD) utility do?

A. Imports data into the vault

B. Exports vault data to txt or csv files

C. Creates backups of the vault data

D. Monitors user activity within the Vault

10. Which authentication method is NOT typically categorized as primary?

A. IIS (SFE, PVWA)

B. CyberArk

C. OracleSSO

D. Windows

Answers

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

Explanations

1. How many permissions can be assigned to a user in the Vault?

A. 5

B. 10

C. 15

D. 20

The correct answer is 10 because in CyberArk's Vault, users can be assigned a maximum of ten distinct permissions that dictate their access levels and operations they can perform on the Vault. These permissions cover a range of functionalities that are crucial for maintaining security and operational integrity within an enterprise's privileged access management framework. Understanding the limit of 10 permissions helps users configure access controls appropriately, ensuring that individuals have access only to the necessary resources for their roles, enhancing security by minimizing unnecessary access rights. While the specific figures for the other choices do not reflect the established guidelines within the CyberArk documentation, focusing on the correct maximum limit allows for effective training and implementation of security protocols in real-world situations.

2. How does a Vault Administrator configure the CyberArk Disaster Recovery (DR) solution to perform automatic failover in case of a failure in the Primary Vault?

A. Setting EnableFailover=yes in vault.ini

B. Setting EnableFailover=yes in padr.ini

C. Modifying the dbparm.ini file

D. Updating the cpm.ini file

The configuration of the CyberArk Disaster Recovery (DR) solution to enable automatic failover involves editing specific settings to ensure the system behaves as intended during a failure scenario. In this case, setting "EnableFailover=yes" in the padr.ini file is the necessary step. The padr.ini file is crucial in the context of the Primary and DR Vaults. This configuration file focuses on parameters relevant to the productivity and connectivity of the vaults, and specifically, it manages the failover capabilities among the Vaults. By making this change, the Vault Administrator instructs the system to automatically switch to the secondary (or DR) Vault if the primary Vault becomes unavailable, thereby ensuring continuity of service and data protection. Other configuration files mentioned serve different purposes within CyberArk's architecture and do not pertain directly to the automatic failover process. While they are essential for overall system performance and operation, they do not facilitate DR failover conditions directly in the same manner as the padr.ini file.

3. What is the primary action associated with the permission "Backup Safe"?

A. Restore previous data

B. Generate reports about account usage

C. Create a backup of the Safe

D. Change passwords for all accounts

The primary action associated with the permission "Backup Safe" is the ability to create a backup of the Safe. This permission enables users to securely copy all the contents and configurations of a Safe, ensuring that critical information remains protected and can be recovered in the event of data loss or corruption. This functionality is essential for maintaining data integrity and provides a safety net for organizations relying on CyberArk for credential management. Creating backups is a fundamental part of data management practices, allowing organizations to safeguard their sensitive information and comply with regulatory requirements. The capability to back up a Safe is crucial for disaster recovery scenarios, ensuring that previously stored data can be restored when needed. In contrast, restoring previous data focuses on retrieving that which has already been backed up, generating reports pertains to assessing the usage of accounts without affecting their backup status, and changing passwords for all accounts addresses the security aspect of account management but does not involve data backup processes.

4. Which port is used by NTP for network time synchronization?

A. UDP port 123

B. TCP port 22

C. TCP port 3389

D. TCP port 445

Network Time Protocol (NTP) is essential for synchronizing clocks of computer systems over packet-switched data networks. The specific port that NTP uses for this purpose is UDP port 123. This protocol operates over the User Datagram Protocol (UDP) rather than the Transmission Control Protocol (TCP), which is often used for other types of data transmission where reliability is crucial. Using UDP allows NTP to efficiently transmit small packets of time synchronization data without the overhead associated with TCP connections, which is important for maintaining accurate time across devices in a network. This efficiency is critical when multiple devices must synchronize their clocks, as it minimizes latency and provides faster synchronization. The other ports listed correspond to different protocols and services, which do not relate to NTP. For instance, TCP port 22 is commonly used for SSH (Secure Shell), while port 3389 is associated with Remote Desktop Protocol (RDP), and port 445 is used primarily for SMB (Server Message Block) services. None of these ports are involved in time synchronization tasks. Thus, the use of UDP port 123 by NTP is both specific and intentional to accommodate the requirements of precise timekeeping over networks.

5. What does the Safe permission Create Folders allow users to do?

A. Rename existing folders in a safe

B. Delete folders within a safe

C. Create new folders in a safe

D. Move existing accounts to different folders

The permission to Create Folders within a safe grants users the ability to add new folders inside that safe. This capability is essential for organizing accounts and data effectively within the CyberArk Vault. By creating new folders, users can categorize information, making it easier to manage and locate sensitive assets. This permission is particularly valuable in environments where there is a need for structured data management, allowing for a hierarchical organization of accounts that can reflect varying access levels, business functions, or project needs. Users who have this permission will be able to enhance the organization of their vault, thereby contributing to better security practices and improved operational efficiencies. Other permissions, though important in their own rights, pertain to different functionalities. For instance, renaming, deleting, or moving folders all deal with modifying existing structures rather than creating new organizational elements, which is the specific focus of the Create Folders permission.

6. What information is provided by the PrivateArk report Users List Report?

A. Lists all users according to their roles

B. Lists all users (including disabled) according to location

C. Displays active users only during business hours

D. Shows user permissions for each safe

The PrivateArk report known as the Users List Report specifically provides a comprehensive overview of all users within the CyberArk environment, including those that may be disabled. This report categorizes users based on their physical or organizational locations, presenting a holistic view that can be critical for administrative and security purposes. Understanding user location in context allows organizations to effectively manage access controls and ensure compliance with corporate policies and regulatory requirements. This capability of listing users by location, including those who are not currently active, enables administrators to have an informed perspective on all user accounts within the system. Therefore, the correct choice highlights the function of the report in offering insights into user management based on geographical distribution or organizational assignments, which can aid in auditing and monitoring user access and roles systematically.

7. What does the Safe permission Add Accounts allow users to do?

A. Add accounts in the safe

B. View account details

C. Edit existing accounts

D. Run accounts backup

The permission "Add Accounts" within a Safe in CyberArk allows users to create and store new accounts within that specific Safe. This capability is crucial for maintaining organized management of privileged accounts, as it enables authorized users to securely add necessary accounts as needed for various applications, systems, or services. When users have this permission, they can effectively contribute to the inventory of accounts under the Safe, thereby facilitating better security practices by ensuring that all required accounts are appropriately recorded and maintained. It is a foundational action that supports account management processes, ensuring new accounts can be added in alignment with organizational policies and security protocols. In contrast, the other options highlight actions that are not encompassed by the "Add Accounts" permission. For instance, viewing account details pertains to a different permission focused on access rights rather than account creation. Editing existing accounts and running backup operations involve distinct permissions that allow for modifications and data protection tasks, respectively, which are separate functions from adding new accounts.

8. What file is utilized for configuring new firewall rules on the vault?

A. firewall.cfg

B. dbparm.ini

C. config.xml

D. rules.txt

The file used for configuring new firewall rules on the vault is dbparm.ini. This file is crucial as it contains various parameters that control the behavior of the CyberArk Vault, including security settings. It allows administrators to define the necessary configurations for firewall rules that help manage and protect sensitive data. The importance of this file lies in its role in centralizing critical configuration options relevant to the operation of CyberArk components, ensuring that the firewall rules effectively enhance security. In contrast, the other options serve different purposes or don't specifically pertain to firewall rules. For example, firewall.cfg may seem like a logical choice but is not a recognized file within CyberArk for this purpose. Config.xml typically manages application configuration settings but doesn't directly handle firewall rules. Lastly, rules.txt might imply a document containing rules; however, it's not the standard file used by CyberArk for defining such configurations. Thus, dbparm.ini stands out as the correct file for configuring new firewall rules within the CyberArk Vault.

9. What does the Export Data Vault (EVD) utility do?

A. Imports data into the vault

B. Exports vault data to txt or csv files

C. Creates backups of the vault data

D. Monitors user activity within the Vault

The Export Data Vault (EVD) utility serves a crucial function in managing vault data by allowing users to export information stored within the vault into accessible formats, such as text (txt) or comma-separated values (csv) files. This capability is essential for several reasons, including data analysis, reporting, or compliance purposes, where stakeholders may need to review or manipulate the data outside the vault environment. By exporting data to these formats, organizations can easily share information with other systems or departments, aiding in integration and enhancing overall operational efficiency. The selected answer highlights the primary functionality of the EVD utility, which is pivotal in maintaining effective data management practices within CyberArk's secure environments.

10. Which authentication method is NOT typically categorized as primary?

A. IIS (SFE, PVWA)

B. CyberArk

C. OracleSSO

D. Windows

In the context of authentication methods, the classification of primary authentication typically refers to the mechanisms that are utilized to verify the identity of users in a straightforward and direct manner. These methods usually include standard operating system-based authentication processes or those that are commonly employed in network environments. The selection of CyberArk as the answer indicates an understanding that CyberArk functions primarily as a privileged access management solution rather than a direct authentication protocol. While CyberArk can integrate with various authentication methods and manage credentials, it itself is not an authentication method but rather a platform that secures and manages access to sensitive accounts and systems. Primary authentication methods, such as Windows or Oracle SSO, provide direct user verification services, making them fundamentally different from CyberArk's role. In contrast, the other options—IIS (Internet Information Services), OracleSSO (Single Sign-On), and Windows—are well-established forms of primary authentication used to authenticate users as they access systems and services. Each of them plays a direct role in establishing user identity, whereas CyberArk's focus is on the management of access and providing secure pathways to systems rather than authenticating users directly.

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!