# CyberArk Certified Delivery Engineer (CDE) Training Practice Test (Sample)

**Study Guide**

BY EXAMZIFY

**Everything you need from our exam experts!**

# 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. **What is the purpose of the Safe permission Delete Folders?**

    A. To restrict access to high-privilege accounts

    B. To enable users to create new safes

    C. To allow users to permanently remove folders from a safe

    D. To modify permissions assigned to users

2. **Which services should be running on the DR vault of a CyberArk Disaster Recovery (DR) solution?**

    A. CyberArk Vault Disaster Recovery (DR), PrivateArk Database

    B. Cluster Vault Manager, Disaster Recovery Agent

    C. High Availability Manager, Backup Database

    D. Vault Manager, PrivateArk Server

3. **What does the Update Account Properties permission primarily relate to?**

    A. Managing attributes of existing accounts

    B. Creating new user accounts

    C. Deleting expired accounts

    D. Running secure backups

4. **What is the intent of the ImmediateInterval parameter in a CPM configuration?**

    A. Control scheduling of user access

    B. Manage immediate password changes

    C. Set policies for user activity

    D. Determine password length policies

5. **What is one purpose of the dbparm.ini file in CyberArk?**

    A. To configure backup settings

    B. To set parameters for the RADIUS integration

    C. To manage user permissions

    D. To store logs for auditing

6. **Does the Vault support dual-factor authentication?**

    A. Yes

    B. No

    C. Only for admin users

    D. Only if configured

7. **How does the allowed Safes parameter enhance security in a CPM policy?**

    A. By allowing access to all users

    B. By specifying which Safes the policy can affect

    C. By eliminating outdated Safes from consideration

    D. By tracking attempts to access prohibited Safes

8. **What is the purpose of the interval setting in a CPM policy?**

    A. To determine how often logs are archived

    B. To control how often the CPM looks for system-initiated CPM work

    C. To set the duration for password validity

    D. To manage the number of simultaneous password changes

9. **What type of logs provide component level entries such as service up or down?**

    A. Debug Logs

    B. Error Logs

    C. Console Logs

    D. Trace Logs

10. **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

# **Answers**

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

# Explanations

## 1. What is the purpose of the Safe permission Delete Folders?

A. To restrict access to high-privilege accounts

B. To enable users to create new safes

C. To allow users to permanently remove folders from a safe

D. To modify permissions assigned to users

The purpose of the Safe permission "Delete Folders" is to allow users to permanently remove folders from a safe. This capability is essential in the context of managing data and resources within a safe, particularly when certain folders are no longer needed or relevant. By providing this permission, an organization ensures that only authorized users can perform such deletions, helping to maintain the integrity and organization of stored data. The ability to delete folders involves a level of trust granted to specific users, as this action can significantly alter the structure and contents of the safe. This function is particularly important for effective data management, enabling the organization to efficiently handle its resources and maintain an orderly safe environment. While restricting access to high-privilege accounts, enabling users to create new safes, and modifying permissions are also crucial aspects of safe management, they serve different purposes. These aspects focus more on security, creation, and administrative tasks rather than directly addressing the removal of data.

## 2. Which services should be running on the DR vault of a CyberArk Disaster Recovery (DR) solution?

A. CyberArk Vault Disaster Recovery (DR), PrivateArk Database

B. Cluster Vault Manager, Disaster Recovery Agent

C. High Availability Manager, Backup Database

D. Vault Manager, PrivateArk Server

In a CyberArk Disaster Recovery solution, the services that should be running on the DR vault are specifically tailored to ensure that the vault can function effectively in a recovery scenario. The first option, which includes the CyberArk Vault Disaster Recovery (DR) service and the PrivateArk Database, is essential because it allows for the replicated storage and management of sensitive information. The CyberArk Vault Disaster Recovery (DR) service is responsible for handling the disaster recovery operations, ensuring that the primary vault's data is available and consistent in the event of a failure. Meanwhile, the PrivateArk Database is critical since it stores the vault's core data, including credentials and permissions. Without these services running, the DR vault would not be able to perform its primary function of securing and managing privileged accounts during a disaster. The other options focus on various components that might be pertinent in other contexts, such as high availability or general vault management, but do not encompass the specific requirements and roles necessary for the effective operation of a DR vault. Thus, the first option accurately reflects the necessary services for a successful CyberArk Disaster Recovery implementation.

## 3. What does the Update Account Properties permission primarily relate to?

**A. Managing attributes of existing accounts**

**B. Creating new user accounts**

**C. Deleting expired accounts**

**D. Running secure backups**

The Update Account Properties permission is primarily associated with managing attributes of existing accounts. This permission allows users to modify various settings and details for accounts already stored in the system. For example, it includes changing passwords, updating account statuses, and altering any associated metadata that might affect how the accounts are utilized within the CyberArk environment. Being able to update these attributes is essential for maintaining security and operational efficiency. It ensures that account information remains current, which can help to prevent unauthorized access or misuse of accounts. This responsibility is key in environments where account management is critical and contributes to the overall security governance of privileged access management. In contrast, other options such as creating new user accounts, deleting expired accounts, or running secure backups involve different permissions and responsibilities that are distinct from simply updating the properties of existing accounts. These actions are part of broader account management or system administration tasks, rather than the specific task of modifying account properties.

## 4. What is the intent of the ImmediateInterval parameter in a CPM configuration?

**A. Control scheduling of user access**

**B. Manage immediate password changes**

**C. Set policies for user activity**

**D. Determine password length policies**

The ImmediateInterval parameter in a CyberArk Privileged Account Manager (CPM) configuration is specifically designed for managing immediate password changes. This parameter allows administrators to define an interval during which the CPM can perform immediate or on-demand password changes for accounts. This is particularly important in scenarios where sensitive accounts need to have their passwords rotated quickly in response to security incidents or for compliance requirements. By utilizing the ImmediateInterval parameter, organizations can enhance their security posture by ensuring that passwords are updated promptly and ensuring that any potential compromise is mitigated swiftly. This immediate response capability is crucial for maintaining the integrity and confidentiality of privileged accounts. In contrast, the other choices pertain to different aspects of CyberArk's functionality. Scheduling user access relates to the timing and management of user permissions rather than password management. Policies for user activity focus on monitoring or restricting what users can do within the system, and determining password length policies addresses the criteria for password composition rather than the timing of password changes. None of these options align with the specific function of the ImmediateInterval parameter, which is solely about managing the promptness of password updates.

## 5. What is one purpose of the dbparm.ini file in CyberArk?

A. To configure backup settings

**B. To set parameters for the RADIUS integration**

C. To manage user permissions

D. To store logs for auditing

The dbparm.ini file in CyberArk serves as a configuration file that specifically sets parameters for database connections, which includes RADIUS integration settings. This file helps define how CyberArk interacts with its databases, including attributes specific to security protocols like RADIUS, which is used for authentication and authorization processes.   The configuration of RADIUS integration within dbparm.ini allows CyberArk to communicate with RADIUS servers, ensuring that user authentication processes are handled securely and efficiently. This integration is essential for organizations that need to centralize their authentication methods across various platforms, enhancing security and compliance.  The other options do not align with the primary purpose of the dbparm.ini file. Backup settings are typically managed elsewhere, user permissions are usually handled through other configuration files or the CyberArk Policy Manager, and logging for auditing is generally conducted through dedicated logging systems and files designed for that explicit purpose.

## 6. Does the Vault support dual-factor authentication?

**A. Yes**

B. No

C. Only for admin users

D. Only if configured

The Vault does support dual-factor authentication as a security measure to enhance user access control. This feature is integral to CyberArk's commitment to ensuring that only authorized personnel have access to potentially sensitive information stored in the Vault. Dual-factor authentication adds an extra layer of security beyond just the username and password by requiring a second form of identification, which can include something the user has (like a mobile device or hardware token) or something the user is (like a fingerprint). This is particularly important in protecting sensitive data and credentials from unauthorized access.  Implementing dual-factor authentication in the Vault helps mitigate the risks associated with stolen credentials and enhances overall security posture, making it a crucial component for organizations that require stringent access controls. Options indicating the Vault does not support this feature or is limited to certain user types miss the broader applicability and importance of dual-factor authentication across the entire system for both regular and administrative users.

## 7. How does the allowed Safes parameter enhance security in a CPM policy?

A. By allowing access to all users

**B. By specifying which Safes the policy can affect**

C. By eliminating outdated Safes from consideration

D. By tracking attempts to access prohibited Safes

The allowed Safes parameter enhances security in a Central Credential Provider (CPM) policy by specifically defining the Safes that the policy can influence. This targeted approach ensures that only the designated Safes are included in the policy's operations, which tightens control over access and management of sensitive credentials stored within those Safes. By limiting the scope of the policy, the organization can enforce stricter security measures, reduce potential attack vectors, and ensure that only authorized credentials are handled according to the defined policy. This specificity allows security teams to streamline their management processes, ensuring that each Safe is only accessed according to its designated policy, thereby minimizing risks associated with broader access that might lead to unintentional exposure or misuse of sensitive information.

## 8. What is the purpose of the interval setting in a CPM policy?

A. To determine how often logs are archived

**B. To control how often the CPM looks for system-initiated CPM work**

C. To set the duration for password validity

D. To manage the number of simultaneous password changes

The interval setting in a CyberArk Central Password Manager (CPM) policy plays a critical role in specifying how frequently the CPM checks for system-initiated tasks or work. This includes actions such as password rotations and other maintenance activities that the CPM must undertake to ensure that privileged account credentials remain secure and up to date. By controlling this interval, administrators can optimize the performance of the CPM by adjusting how often it initiates these tasks, thereby balancing system resource usage with the need for timely password updates. The other choices do not accurately reflect the role of this particular setting. For example, logging and password validity are important, but they are governed by different aspects of CyberArk's management policies, not the interval setting for system work.

## 9. What type of logs provide component level entries such as service up or down?

A. Debug Logs

B. Error Logs

**C. Console Logs**

D. Trace Logs

Console logs are designed to provide real-time feedback on the status of various components within a system, including entries that indicate whether a service is up or down. These logs help administrators monitor the functioning of applications and detect any changes in the operational state of components. They are particularly useful for tracking the overall performance and health of services, which makes them suitable for reporting component-level information.  Other log types have different focuses; for instance, debug logs typically capture detailed information used for troubleshooting, but they may not always reflect the operational status of services. Error logs concentrate on capturing issues or failures within applications, while trace logs usually provide a more granular level of detail regarding the execution flow of applications, often intended for debugging complex issues rather than monitoring service availability. Therefore, console logs are the most appropriate choice for observing component-level entries such as service status changes.

## 10. 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.

# 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!