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

Study Guide

Everything you need from our exam experts!

Copyright © 2025 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 from reliable sources accurate, complete, and timely information about this product.

SAMPLE

Questions

SAMPLE

1. How many CPM and DR vaults should be created for effective management?

A. One per data center

B. Two per data center

C. Three per data center

D. One per user account

2. How many permissions can be applied on a safe to a user?

A. 16 or 22

B. 10 or 15

C. 20 or 30

D. 5 or 7

3. What does the permission "Validate Safe Content" require to retrieve an object?

A. The status must be valid

B. Permission from a Safe member

C. Backup the Safe first

D. A password reset

4. What port is associated with SMB for file sharing services?

A. UDP port 123

B. TCP port 22

C. TCP port 445

D. TCP port 636

5. What is the main purpose of load balancing in a privileged access management environment?

A. To enhance security by isolating systems

B. To distribute workloads across multiple resources

C. To prevent unauthorized access

D. To simplify system recovery

SAMPLE

6. What type of logs provide only error entries and only exist for some components?

A. Debug Logs

B. Trace Logs

C. Console Logs

D. Error Logs

7. What port does SAML use for security assertions?

A. TCP port 88

B. UDP port 123

C. TCP port 636

D. TCP port 443

8. What controls the behavior of the CPM in relation to recently completed Dual Control requests?

A. The CPM does change passwords under this circumstance

B. The CPM does not change passwords under this circumstance

C. The CPM automatically resets passwords for Dual Control requests

D. The CPM sends alerts for Dual Control requests

9. How does the Vault administrator configure the FQDN of the DC during LDAP/S integration?

A. PVWA -> Administration -> LDAP Settings

B. PVWA -> Administration -> LDAP Integration

C. PVWA -> Security -> Active Directory Settings

D. PVWA -> Configuration -> LDAP Integration

10. 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

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How many CPM and DR vaults should be created for effective management?

A. One per data center

B. Two per data center

C. Three per data center

D. One per user account

For effective management of privileged accounts, the best practice is to create one Central Password Manager (CPM) vault and one Disaster Recovery (DR) vault for each data center. This setup simplifies the management and ensures that there is a dedicated vault for secure password storage and an additional vault as a backup in case of a disaster. Having one vault per data center centralizes the management, helping in compliance and making it easier to enforce policies related to privileged account access. Creating more than one vault for CPM and DR in a single data center can complicate management and lead to issues with consistency in password policies and access controls. This could also increase administrative overhead and complicate disaster recovery processes, as more than one vault would need to be synchronized and managed.

2. How many permissions can be applied on a safe to a user?

A. 16 or 22

B. 10 or 15

C. 20 or 30

D. 5 or 7

The correct answer reflects the known limitations of permissions that can be assigned to a user for a safe within CyberArk. Specifically, a user can have a combination of permissions that adds up to either 16 or 22 distinct permissions on a safe. This flexibility allows organizations to tailor access levels according to different roles or requirements, ensuring that users have the appropriate capabilities while maintaining security. The options that suggest different numbers of permissions, such as 10 or 15, 20 or 30, or 5 or 7, do not align with the established configurations within CyberArk's permissions model. The list of applicable permissions includes various actions that can be granted, which is where the higher numbers in the correct choice come into play. Understanding these details is crucial for effectively managing user access and maintaining the integrity of secrets management within CyberArk environments.

SAMPLE

3. What does the permission "Validate Safe Content" require to retrieve an object?

A. The status must be valid

B. Permission from a Safe member

C. Backup the Safe first

D. A password reset

The permission "Validate Safe Content" is linked to the requirement that the status must be valid in order to retrieve an object. This means that before any action can be taken regarding an object stored in the Safe, the system checks to ensure that the object is in a valid state. A valid status typically indicates that the object, such as a credential or a document, is current, properly formatted, not expired, and meets any predefined criteria set by the organization's security protocols. This ensures the integrity and reliability of the data being accessed, minimizing risks associated with retrieving outdated or invalid information. In contrast, the other options focus on different aspects of permission or actions that do not specifically relate to the status of the object. For example, permission from a Safe member refers to user privileges rather than the status of the object itself. Backing up the Safe and a password reset involve different procedures and are not directly linked to validating the status of an object for retrieval purposes.

4. What port is associated with SMB for file sharing services?

A. UDP port 123

B. TCP port 22

C. TCP port 445

D. TCP port 636

The correct association of port 445 with SMB (Server Message Block) is critical for file sharing services in various operating systems, particularly Windows. Port 445 is used for direct SMB over TCP, which enables clients to access shared files and printers over the network without the need for NetBIOS, a legacy protocol that operates over ports 137, 138, and 139. SMB is a network file sharing protocol that allows applications to read and write to files and request services from server programs. By using TCP over port 445, it ensures a reliable and efficient transport mechanism for file sharing, making it crucial to many network implementations today. The usage of port 445 significantly contributes to improved performance and is fundamental for modern networking operations. In this context, the other options do not apply to SMB file sharing. UDP port 123 is used for the Network Time Protocol (NTP) to synchronize clocks over a network. TCP port 22 is primarily used for SSH (Secure Shell), which is used for secure remote administration and file transfers. TCP port 636 is associated with LDAPS (LDAP over SSL), which is used for secure directory services. Thus, these ports serve entirely different purposes compared to port 445, which is specifically designated

SAMPLE

5. What is the main purpose of load balancing in a privileged access management environment?

A. To enhance security by isolating systems

B. To distribute workloads across multiple resources

C. To prevent unauthorized access

D. To simplify system recovery

The main purpose of load balancing in a privileged access management environment is to distribute workloads across multiple resources. This ensures that no single resource is overwhelmed by requests, which can lead to performance degradation or system failures. By effectively managing the distribution of workloads, load balancing enhances the availability and reliability of the privileged access management solution. In environments where numerous users or systems require access, load balancing optimally allocates requests across various servers or instances, ensuring that each server operates within its capacity. This approach not only improves performance but also contributes to effective resource utilization, enabling systems to handle high traffic without diminishing operational efficiency. While enhancing security by isolating systems, preventing unauthorized access, and simplifying system recovery are certainly important aspects of a privileged access management strategy, they do not directly pertain to the specific functionality of load balancing. Load balancing primarily focuses on performance and resource management rather than security measures or recovery procedures.

6. What type of logs provide only error entries and only exist for some components?

A. Debug Logs

B. Trace Logs

C. Console Logs

D. Error Logs

Error logs are specifically designed to capture and record entries related to error events that occur within a system or application. These logs focus solely on incidents that result in failures or issues, making them an essential tool for troubleshooting and diagnosing problems. By containing only error entries, they allow engineers and system administrators to quickly identify and address critical issues without sifting through unrelated information. In the context of various types of logs, error logs are distinct from others like debug or trace logs that track more detailed operation information or provide comprehensive visibility into the system's functioning. Console logs can also contain a broad range of information, including warnings and status messages, rather than being strictly limited to error entries. This specificity of content makes error logs invaluable for maintaining system integrity and ensuring timely responses to potential failures.

SAMPLE

7. What port does SAML use for security assertions?

A. TCP port 88

B. UDP port 123

C. TCP port 636

D. TCP port 443

SAML (Security Assertion Markup Language) uses TCP port 443 for security assertions. This is primarily due to the fact that SAML assertions are often sent over HTTP or HTTPS. TCP port 443 is the standard port for HTTPS, which provides a secure communication channel using SSL/TLS encryption. The use of this port ensures that SAML assertions, which contain sensitive authentication and authorization information, are transmitted securely over the internet. The other ports mentioned in the options are associated with different protocols. For example, TCP port 88 is typically used for Kerberos authentication, which is not directly related to SAML. UDP port 123 is used by the Network Time Protocol (NTP), and TCP port 636 is used for LDAP over SSL (LDAPS). While these are important in their own contexts, they do not pertain to the transmission of SAML security assertions. Thus, the choice of TCP port 443 is directly relevant to the security and proper functioning of SAML.

8. What controls the behavior of the CPM in relation to recently completed Dual Control requests?

A. The CPM does change passwords under this circumstance

B. The CPM does not change passwords under this circumstance

C. The CPM automatically resets passwords for Dual Control requests

D. The CPM sends alerts for Dual Control requests

The behavior of the Central Password Manager (CPM) in relation to recently completed Dual Control requests is governed by specific security guidelines designed to ensure a high level of security and control over privileged accounts. When a Dual Control request is made, the process requires two separate approvals from different users to execute privileged actions, such as password changes. In this context, the CPM does not change passwords related to Dual Control requests immediately after they are completed. This approach is in line with best practices for maintaining accountability and verification, ensuring that any password changes made under a Dual Control request are carefully modified only after the appropriate checks are performed. This behavior helps to mitigate risks associated with privileged account management, as it does not allow for immediate password alteration which could potentially bypass established approval workflows. Other options imply that the CPM would either automatically change passwords or issue alerts, which doesn't accurately reflect its function in handling Dual Control requests. Understanding how the CPM interacts with Dual Control requests is crucial for ensuring a secure environment where privileged access is tightly regulated. Thus, knowing that it does not change passwords under these circumstances is vital for maintaining effective governance and compliance within an organization's security policy.

SAMPLE

9. How does the Vault administrator configure the FQDN of the DC during LDAP/S integration?

A. PVWA -> Administration -> LDAP Settings

B. PVWA -> Administration -> LDAP Integration

C. PVWA -> Security -> Active Directory Settings

D. PVWA -> Configuration -> LDAP Integration

The configuration of the Fully Qualified Domain Name (FQDN) of the Domain Controller (DC) during LDAP/S integration is specifically handled through the LDAP Integration settings in the Private Vault Web Application (PVWA). This option allows Vault administrators to set up and manage the integration with LDAP, including defining the DC's FQDN, which is crucial for ensuring proper communication and authentication between the Vault and the Active Directory. By selecting the LDAP Integration path, administrators can enter necessary details such as the DC's FQDN, connection settings, and other relevant configurations needed for the integration to succeed. This integration is essential as it enables the Vault to authenticate users and manage their credentials securely within a corporate Active Directory environment. The other options, while related to administration and configuration, do not directly lead to the specific settings required for LDAP/S integration, making them unsuitable for setting the FQDN of the DC.

10. 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.

SAMPLE