Perform User Account Management Phase 1 Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

Sample study guide. For the full version with hundreds of questions, visit: https://performuseracctmgmt.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

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 benefit does access packaging provide during onboarding?**

   A. Access packaging reduces friction by provisioning a predefined set of entitlements in one request.

   B. Access packaging increases the workload by requiring per-app approvals.

   C. Access packaging has no impact on onboarding.

   D. Access packaging refers to packaging hardware for onboarding.

2. **What is the name of a DD Form 2875?**

   A. System Access Request Form (SAR)

   B. DoD Access Verification Form

   C. Information System Access Log (ISAL)

   D. System Authorization Access Request (SAAR)

3. **Which metric is commonly used to measure how quickly new user accounts are provisioned?**

   A. Time-to-deprovision.

   B. Number of licenses purchased.

   C. Time-to-provision.

   D. Mouse clicks required to login.

4. **In federated identity management, which practice helps maintain trust between identity providers?**

   A. Exchange metadata, configure certificates, set up signing and encryption, manage trust stores, and rotate keys periodically; monitor trust relationships.

   B. Rely on a single shared password for all providers.

   C. Disable trust monitoring to reduce overhead.

   D. Use a different authentication protocol that skips federation.

5. **Active Directory saves information about network objects and makes it easier to use. This statement describes:**

   A. ATCTS

   B. Active Directory

   C. DoD VTE

   D. DWCA

SAMPLE

6. How should data associated with deprovisioned accounts be handled for compliance?

- **A. Archive or delete according to policy; ensure no active credentials remain; secure retained data for audits while respecting retention requirements.**
- **B. Leave all data in place indefinitely.**
- **C. Delete the data immediately and purge any logs.**
- **D. Archive all data regardless of retention requirements.**

7. In Active Directory, a domain is best described as:

- **A. A Basic administrative unit in Active Directory**
- **B. A collection of network resources that share a common directory database and security policies**
- **C. An organizational unit**
- **D. The entire forest**

8. What are impossible travel risk signals?

- **A. Risk signals from login location anomalies; trigger MFA or challenge.**
- **B. Travel schedule conflicts that delay login.**
- **C. GPS location matching that is always correct.**
- **D. Device type mismatch with user role.**

9. Explain the concept of "separation of duties" in account management.

- **A. Ensure no single user has conflicting privileges that enable critical actions; split responsibilities to reduce fraud.**
- **B. Having one administrator manage all tasks.**
- **C. Daily rotating passwords for each user.**
- **D. Using only one factor authentication.**

10. What is the purpose of a service catalog in account management?

- **A. Lists all software installed on every device.**
- **B. Replaces identity provider in auth.**
- **C. Standardizes access requests, approvals, and provisioning steps for services and roles.**
- **D. Stores user passwords for services.**

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which benefit does access packaging provide during onboarding?

A. Access packaging reduces friction by provisioning a predefined set of entitlements in one request.

B. Access packaging increases the workload by requiring per-app approvals.

C. Access packaging has no impact on onboarding.

D. Access packaging refers to packaging hardware for onboarding.

Access packaging speeds onboarding by bundling a predefined set of entitlements into a single package that can be provisioned in one request. This means new users get the required apps and permissions upfront, reducing manual steps and the number of separate approvals, which leads to faster and more consistent provisioning. The idea is to streamline and standardize access so onboarding isn't slowed by piecemeal grants. The other options don't fit because increasing per-app approvals would slow things down, claiming no impact ignores the efficiency gains, and packaging hardware is unrelated to software access provisioning.

2. What is the name of a DD Form 2875?

A. System Access Request Form (SAR)

B. DoD Access Verification Form

C. Information System Access Log (ISAL)

D. System Authorization Access Request (SAAR)

System Authorization Access Request (SAAR) is the official name of the form used to request access to DoD information systems. This form, DD Form 2875, collects who you are, what system you need to access, the level of access required, and the justification for that access. Security officials use the SAAR to authorize and provision accounts, ensuring access aligns with your role and security policies. The other names are not the formal DoD terminology for this form, as they describe related concepts but not the official access-authorization document.

SAMPLE

3. Which metric is commonly used to measure how quickly new user accounts are provisioned?

A. Time-to-deprovision.

B. Number of licenses purchased.

C. Time-to-provision.

D. Mouse clicks required to login.

Measuring how quickly a new user account can be created and made usable hinges on provisioning speed. Time-to-provision captures the total elapsed time from when an account request is made (or when the provisioning process starts) to when the account is fully provisioned and the user can access resources. This directly reflects the efficiency of onboarding workflows and any automation in the identity system. Other metrics look at different things: time-to-deprovision tracks how long it takes to remove access when someone leaves; the number of licenses purchased reflects capacity or cost, not speed; and mouse clicks required to login gauges user effort to log in, not how fast an account is created. In practice, focusing on time-to-provision helps identify bottlenecks in the provisioning process and drives improvements to onboard users more quickly.

4. In federated identity management, which practice helps maintain trust between identity providers?

A. Exchange metadata, configure certificates, set up signing and encryption, manage trust stores, and rotate keys periodically; monitor trust relationships.

B. Rely on a single shared password for all providers.

C. Disable trust monitoring to reduce overhead.

D. Use a different authentication protocol that skips federation.

Maintaining trust in federated identity management rests on a secure, verified relationship between identity providers and service providers. Exchanging metadata lets each party automatically learn the other's endpoints, supported protocols, and certificate requirements, so trust is configured consistently and correctly. Configuring certificates and enabling signing and encryption ensures that assertions and responses are genuinely from trusted sources and stay protected in transit. Managing trust stores keeps a reliable list of trusted authorities, while rotating keys periodically reduces risk if a credential is compromised. Monitoring trust relationships provides ongoing visibility to detect issues like expired certificates or misconfigurations and respond quickly. The other options undermine trust: a single shared password creates a single point of failure; disabling trust monitoring removes essential oversight; and using a different protocol that skips federation defeats the purpose of federated identity and its trust framework.

SAMPLE

5. Active Directory saves information about network objects and makes it easier to use. This statement describes:

A. ATCTS

B. Active Directory

C. DoD VTE

D. DWCA

This describes a directory service—the centralized system that stores information about network resources and makes them easier to use by organizing and managing them from one place. A directory service keeps data about users, computers, printers, groups, and policies, and it handles authentication and authorization so you can access resources efficiently. Active Directory is Microsoft's implementation of this concept for Windows networks, organizing data in a structured hierarchy (domains, organizational units, and a schema) and providing access through standard protocols like LDAP and Kerberos, with DNS integration for locating services. This combination of storing object information and enabling centralized management and access is exactly what the statement is conveying. The other options aren't directory services and don't describe how Windows networks organize and manage objects, so they don't fit.

6. How should data associated with deprovisioned accounts be handled for compliance?

A. Archive or delete according to policy; ensure no active credentials remain; secure retained data for audits while respecting retention requirements.

B. Leave all data in place indefinitely.

C. Delete the data immediately and purge any logs.

D. Archive all data regardless of retention requirements.

When handling data for deprovisioned accounts, the guiding idea is to manage information in line with policy, balancing security, privacy, and regulatory or legal retention needs. First, revoke access so no active credentials or permissions remain for the former user, and remove them from systems, groups, and integrations. Then handle the associated data by archiving or deleting according to the organization's retention policy and any applicable laws, while preserving only what is required for audits, investigations, or business needs. Secure any retained data so it's protected against tampering and access is tightly controlled, and ensure the retention period is enforced. If there are legal holds or ongoing investigations, preserve the data accordingly. This is why the best approach is to archive or delete according to policy, ensure no active credentials remain, and secure retained data for audits while respecting retention requirements. The other options fail to balance access management, retention obligations, and auditability: leaving data indefinitely ignores retention rules; deleting data immediately and purging logs can hinder audits and regulatory obligations; archiving everything regardless of retention needs can waste resources and violate privacy or retention policies.

SAMPLE

7. In Active Directory, a domain is best described as:

A. A Basic administrative unit in Active Directory

B. A collection of network resources that share a common directory database and security policies

C. An organizational unit

D. The entire forest

A domain in Active Directory is the security and administration boundary that groups together network resources—such as users, computers, printers, and groups—under one shared directory database and a common set of security policies. All objects in the domain reside in the AD DS database on domain controllers and are governed by the domain's policies, including Group Policy. This setup provides centralized authentication and authorization within the domain. An Organizational Unit is a container inside the domain used for delegation and policy application, not the domain itself. The forest is the top-level collection of one or more domains that share a schema and global catalog, so a domain is not the entire forest. Therefore, the best description is a collection of network resources that share a common directory database and security policies.

8. What are impossible travel risk signals?

A. Risk signals from login location anomalies; trigger MFA or challenge.

B. Travel schedule conflicts that delay login.

C. GPS location matching that is always correct.

D. Device type mismatch with user role.

Impossible travel risk signals show up when a login occurs from a location that would require impossible travel time from where the user logged in before. In other words, the system detects a suspicious jump in location between sessions, suggesting the account may be used by someone else. That's precisely what a risk signal from login location anomalies captures, and the typical response is to require stronger verification like MFA or an additional challenge. Other options don't fit because travel schedule conflicts aren't an authentication risk signal, GPS being always correct would eliminate anomalies rather than flag them, and a device-type mismatch with user role is about what device is used rather than where the login occurred.

SAMPLE

9. Explain the concept of "separation of duties" in account management.

A. Ensure no single user has conflicting privileges that enable critical actions; split responsibilities to reduce fraud.

B. Having one administrator manage all tasks.

C. Daily rotating passwords for each user.

D. Using only one factor authentication.

Separation of duties is a control that splits critical tasks among multiple people so no single individual can perform all steps of a sensitive action. In account management, this means distributing responsibilities and privileges so different people handle different parts of a process, such as requesting access, approving that access, and provisioning or deprovisioning accounts. This creates checks and balances, making fraud or mistakes harder because the action requires independent review and authorization from others. It also improves accountability, since different roles are involved, and activities can be traced to the appropriate person or role. The other options miss the point: having one administrator manage everything places too much power in one person and removes the necessary checks; rotating passwords or using a single authentication factor addresses authentication or credential management, not the need to divide responsibilities to prevent misuse of privileges.

10. What is the purpose of a service catalog in account management?

A. Lists all software installed on every device.

B. Replaces identity provider in auth.

C. Standardizes access requests, approvals, and provisioning steps for services and roles.

D. Stores user passwords for services.

Standardizing how access to services is requested, approved, and provisioned is what a service catalog is for in account management. It serves as a central list of available IT services and the entitlements tied to each service or role. When a user requests access, the catalog defines the exact request workflow, who must approve, and the provisioning steps that grant or revoke access, often enabling automation and consistent governance. This approach supports least privilege, speeds up onboarding and changes, and provides an auditable trail for compliance. It isn't about listing software installed on devices (that's asset inventory), replacing an identity provider (that's authentication infrastructure), or storing user passwords (that's credential management).

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://performuseracctmgmt.examzify.com

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

SAMPLE