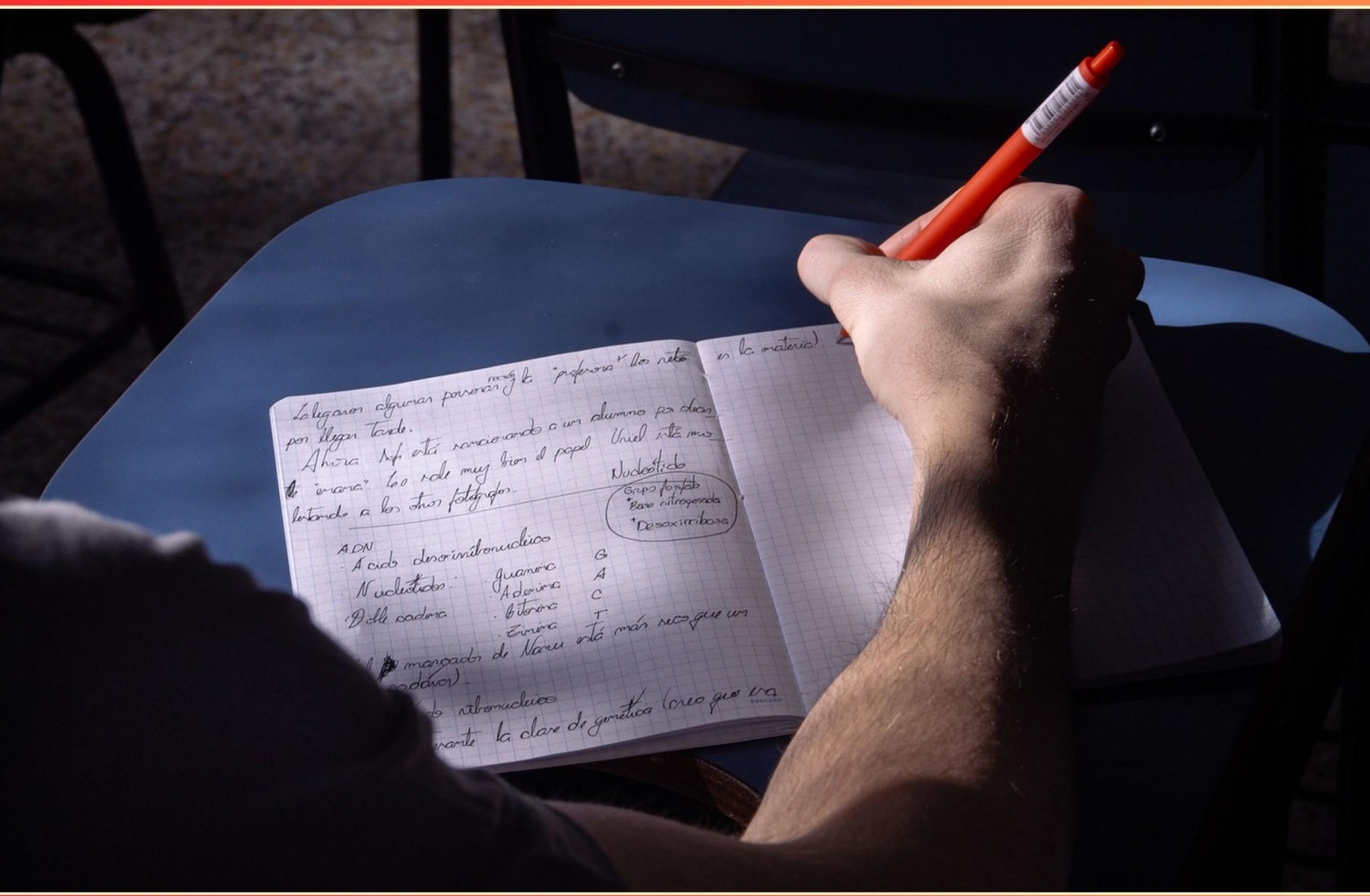
DSAC-11 ANNEX B PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dsac11annexb.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. What is the primary purpose of Transport Layer Security (TLS)?

A. Improve network routing efficiency

B. Provide secure communication over a network

C. Store user credentials locally

D. Compress data to reduce bandwidth

2. How does the DNS Client service assist in the authentication process for Active Directory domains?

A. By querying the DNS server to locate domain controllers

B. By authenticating with the domain using cached credentials

C. By bypassing DNS during authentication

D. By caching logon tokens locally

3. A _____ is an optional set of folders that contain custom scripts, images, branding, applications, drivers, and other files.

A. Distribution Share

B. User Profile

C. Shared Folder

D. System Image

4. Which of the following describes a GPO's password policy capability?

A. They only enforce password length

B. They determine password length, reuse rules, and other criteria

C. They never enforce reuse rules

D. They are decided by users

5. In an incident response plan, which phase focuses on restoring services and operations to normal after containment and eradication?

A. Preparation

B. Containment

C. Recovery

D. Lessons Learned

6. In an incident response plan, which phase focuses on analyzing the incident after recovery to improve future responses?

A. Preparation

B. Containment

C. Recovery

D. Lessons Learned

7. What is the effect of applying a Local GPO to a computer and the users who log on to it?

A. Changes apply only to that computer and to users logging on to it

B. Changes apply domain-wide

C. Changes apply to all computers in the forest

D. No effect until reboot

8. How do you perform risk treatment and choose mitigations in Annex B?

A. Evaluate risk level, select controls or actions to reduce/transfer/avoid/accept risk, and document rationale.

B. Ignore risks and hope they go away.

C. Transfer risk by common sense.

D. Accept risk without documenting.

9. Which statement best describes the primary role of an operating system?

A. Manages hardware and software resources and provides common services for programs

B. Manages only memory

C. Runs applications directly without OS

D. Is optional for most computers

10. What is the principle of least privilege and how is it applied in DSAC-11 Annex B?

A. Users and processes receive only necessary privileges; applied via role-based access, constrained permissions, and need-to-know.

B. Privileges should be granted liberally to improve efficiency.

C. Privileges are determined randomly.

D. Privileges are only relevant for administrators.

Answers

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

Explanations

1. What is the primary purpose of Transport Layer Security (TLS)?

A. Improve network routing efficiency

B. Provide secure communication over a network

C. Store user credentials locally

D. Compress data to reduce bandwidth

The main point of TLS is to enable secure communication over a network. It does this by creating an encrypted and authenticated channel between two endpoints. Through a handshake, the parties verify each other's identities with certificates, agree on cryptographic keys, and establish protections that keep data private in transit, detect any tampering, and confirm who you're talking to. This combination of confidentiality, integrity, and authenticity is what makes TLS essential for securing protocols like HTTPS. It isn't about routing efficiency, storing credentials locally, or compressing data, which are separate concerns.

2. How does the DNS Client service assist in the authentication process for Active Directory domains?

A. By querying the DNS server to locate domain controllers

B. By authenticating with the domain using cached credentials

C. By bypassing DNS during authentication

D. By caching logon tokens locally

In Active Directory authentication, finding a domain controller is the first crucial step, and the DNS Client service makes that possible. It uses DNS to locate which servers are domain controllers by querying the domain's service records. These SRV records, such as those for LDAP and Kerberos services, tell the client where to connect to perform authentication. Once the client discovers a DC through DNS, it can contact that DC to complete the logon process. The DNS Client service may cache these results to speed up future logons, but it does not perform the actual authentication itself, nor does it bypass DNS or cache logon tokens locally.

3. A _____ is an optional set of folders that contain custom scripts, images, branding, applications, drivers, and other files.

A. Distribution Share

B. User Profile

C. Shared Folder

D. System Image

Distribution share refers to the central repository used in deployment tools like MDT/WDS to store all files needed for an OS deployment. It is an optional set of folders that contain custom scripts, images, branding, applications, drivers, and other files that the deployment process uses to customize and install systems. This makes it the best fit because it's specifically designed to house the organized collection of deployment assets in one shared location the deployment framework references during automation. A user profile is personal user data and settings, not a repository for deployment assets. A shared folder is a generic file share without the deployment-specific organization. A system image is a complete snapshot of an operating system, not a collection of foldered resources like scripts, drivers, and applications.

4. Which of the following describes a GPO's password policy capability?

A. They only enforce password length

B. They determine password length, reuse rules, and other criteria

C. They never enforce reuse rules

D. They are decided by users

Group Policy Objects give admins a centralized way to enforce password requirements across a Windows domain. Through a GPO, you can set the minimum password length, enforce complexity, specify how many previous passwords cannot be reused, and impose rules about password aging and lockout. This means the policy covers length, reuse rules, and other criteria, which is why this option best describes a GPO's password policy capability. GPOs manage more than just length, they enforce reuse rules via password history, and these settings are configured by administrators rather than chosen by users.

5. In an incident response plan, which phase focuses on restoring services and operations to normal after containment and eradication?

A. Preparation

B. Containment

C. Recovery

D. Lessons Learned

The recovery phase is about bringing services and operations back to normal after the threat has been contained and eradicated. Once the immediate danger is removed, the focus shifts to restoring IT services, bringing affected systems back online, and replenishing data from verified-clean backups. This includes validating that systems are functioning correctly, performing tests to confirm that normal operations can resume without issues, and coordinating with business units to reinstate workflows and user access. It also involves monitoring for any signs of residual problems and applying necessary hardening or patches to prevent recurrence. Other phases set up and prevent or remove the threat, but they don't focus on the long, steady process of returning everything to its normal state. Preparation is about readiness before anything happens, containment limits the spread during an incident, eradication removes the threat, and lessons learned looks at what happened to improve future responses.

6. In an incident response plan, which phase focuses on analyzing the incident after recovery to improve future responses?

A. Preparation

B. Containment

C. Recovery

D. Lessons Learned

The main idea tested is how we learn from an incident after things have been brought back to normal. This phase is about looking back at what happened, analyzing what went well and what didn't, and turning those insights into concrete improvements for the future. By conducting a post-incident review, you identify root causes, gaps in detection, delays in response, and communication or coordination issues. Then you update the incident response plans, runbooks, training, and controls so future incidents can be detected sooner, contained faster, and recovered more smoothly. Other phases focus on getting ready beforehand, stopping the incident from spreading, or restoring services, but the reflective work that feeds back into better preparedness and response is the lessons-learned phase.

7. What is the effect of applying a Local GPO to a computer and the users who log on to it?

A. Changes apply only to that computer and to users logging on to it

B. Changes apply domain-wide

C. Changes apply to all computers in the forest

D. No effect until reboot

Local Group Policy is stored on the computer itself and controls both computer configuration and user settings for anyone who signs in to that machine. Because it's local, it doesn't propagate to other computers or across the domain or forest. When the computer starts, the Local GPO's computer settings are applied; when a user logs on, the Local GPO's user settings apply for that user on that machine. The policy framework refreshes periodically, so many changes take effect on logon or during a background refresh, and reboot isn't required for all changes (though some settings do need a restart). In short, applying a Local GPO affects only that specific computer and the users who log on to it.

8. How do you perform risk treatment and choose mitigations in Annex B?

A. Evaluate risk level, select controls or actions to reduce/transfer/avoid/accept risk, and document rationale.

B. Ignore risks and hope they go away.

C. Transfer risk by common sense.

D. Accept risk without documenting.

The idea being tested is how to approach risk treatment in a structured way and pick mitigations. Start by assessing the risk level, usually by considering how likely the event is and how severe its impact would be. With that understanding, you choose a treatment approach that fits the situation: reduce the risk by adding controls or actions that lower either the probability of the event or the severity of its consequences; transfer the risk to someone else (for example, through contracts or insurance); avoid the risk entirely by changing plans so the risk no longer applies; or accept the risk if the remaining level is within acceptable tolerance. Importantly, you document the rationale for why a particular mitigation was chosen, so decisions are transparent and auditable, and you assign responsibility and resources with timelines. After implementing the mitigation, you re-check the residual risk to ensure it aligns with the organization's risk appetite. The emphasis on a clear assessment, deliberate selection of mitigation strategies, and documented justification distinguishes this approach from ad hoc or undocumented practices.

9. Which statement best describes the primary role of an operating system?

A. Manages hardware and software resources and provides common services for programs

B. Manages only memory

C. Runs applications directly without OS

D. Is optional for most computers

An operating system coordinates hardware and software resources and provides common services that programs rely on. It acts as a manager and mediator between applications and the computer's components, allocating CPU time, memory, and I/O devices, while keeping programs isolated from each other and from the hardware. It also offers essential services such as file management, device drivers, networking, and security, presenting a consistent interface so software can run without needing to know hardware specifics. This combination enables multitasking, efficient resource use, and safe, stable operation of all programs. The other statements are narrower or incorrect: focusing only on memory misses the broader role of scheduling, I/O handling, and service provision; running applications directly without an OS isn't how modern computers operate; and the OS is not optional for typical computers since some management layer is needed to coordinate resources and services.

10. What is the principle of least privilege and how is it applied in DSAC-11 Annex B?

A. Users and processes receive only necessary privileges; applied via role-based access, constrained permissions, and need-to-know.

B. Privileges should be granted liberally to improve efficiency.

C. Privileges are determined randomly.

D. Privileges are only relevant for administrators.

The principle of least privilege means giving each user or process only the access needed to perform their tasks, no more. In DSAC-11 Annex B, this is put into practice by tying permissions to roles (role-based access control), constraining what those permissions allow, and restricting access based on need-to-know. This combination reduces the potential impact of a compromised account, makes it easier to revoke or adjust access, and helps keep sensitive information protected by ensuring only those with a legitimate reason can see it. This exact approach is the best fit because it describes not just the idea of minimal access, but also how it's achieved in real systems—through RBAC, restricted permissions, and need-to-know controls. Other options don't align with the goal: granting privileges broadly increases risk, random assignment has no security basis, and limiting privileges only to administrators ignores the needs of regular users and services that require access to perform tasks.

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://dsac11annexb.examzify.com

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