Citrix Deploy and Manager Citrix ADC13 with Citrix Gateway 1Y0-231 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

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. **Which action would administrators take to enhance TLS security by enabling a modern protocol?**
   - **A. Enable RC4 cipher suite**
   - **B. Create SHA1 key**
   - **C. Enable TLSv1.2**
   - **D. Disable SSLv3**

2. **Which NetScaler tool would you use to troubleshoot resets on an intranet server load-balanced by NetScaler?**
   - **A. Look in the Event Viewer**
   - **B. nslog via CLI**
   - **C. Take a packet trace with nstrace and analyze with WireShark**
   - **D. nslog**

3. **Which policy type defines criteria for granting access to internal resources after user authentication?**
   - **A. Client policy**
   - **B. Access policy**
   - **C. Authorization policy**
   - **D. VPN policy**

4. **Which step is essential to integrate an existing CERT-based authentication policy on Citrix Gateway?**
   - **A. Change the client certificate to Mandatory on the SSL parameters of the virtual server**
   - **B. Enable the two-factor option on the existing CERT authentication profile**
   - **C. Bind the existing CERT authentication policy to the Citrix Gateway virtual server**
   - **D. Create a CERT authentication policy and bind it to the Citrix Gateway virtual server**

5. How can the administrator use Citrix Application Delivery Management to alert when the number of connections to virtual servers exceeds a threshold?

A. Configure Network Reporting on the Citrix Application Delivery Management by setting the threshold and email address

B. Configure TCP Insight on the Citrix Application Delivery Management

C. Configure specific alerts for virtual servers using Citrix Application Delivery Management

D. Configure SMTP Reporting on the Citrix Application Delivery Management by adding the threshold and email address

6. If a team member has full admin partition permissions but cannot use aaad.debug in the CLI, what is the most likely reason?

A. The team member does NOT have permission to use the CLI.

B. The team member does NOT have Shell access by design.

C. The team member needs to troubleshoot the issue from the GUI.

D. The team member is NOT using the CLI correctly.

7. Which symptom would most strongly suggest SSL encryption is not configured on a server?

A. Packets captured show plaintext data

B. The connection completes TLS handshake with a strong cipher

C. The server returns 500 Internal Server Error

D. The data transfer is always encrypted

8. What is the purpose of the nslog log type on Citrix ADC?

A. It stores server access logs

B. It stores detailed statistics, metrics and debugging data in a proprietary binary format

C. It stores configuration changes

D. It stores user authentication events

9. What is the effect of enabling caseSensitive ON on a vserver in terms of host header matching?

A. It disables host header matching.

B. It makes host header matching case-insensitive.

C. It triggers SSL offload.

D. It makes host header matching case-sensitive.

10. Which setting reduces server load and increases SSL transactions per second on a SSL virtual server created with default settings?

A. SSLv3

B. Session Reuse

C. Session Timeout

D. SSLv2 Redirect

Answers

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

Explanations

1. Which action would administrators take to enhance TLS security by enabling a modern protocol?

A. Enable RC4 cipher suite

B. Create SHA1 key

C. Enable TLSv1.2

D. Disable SSLv3

Using a modern TLS protocol version improves security by defining how keys are exchanged, which ciphers are allowed, and how data integrity is ensured. Enabling TLSv1.2 puts you on a current, well-supported protocol that offers strong ciphers (like AES-GCM) and robust hash algorithms (such as SHA-256/384), along with features like forward secrecy. This combination makes the connection much harder to compromise compared to older protocols. Enabling the RC4 cipher suite would actually weaken security because RC4 has known biases and vulnerabilities that attackers can exploit. Creating a SHA-1 key doesn't upgrade the protocol or its security level—SHA-1 is considered weak for modern TLS signatures. SSLv3 is outdated and vulnerable to several attacks, so retiring or disabling it improves security, but the action described as adopting a modern protocol is specifically enabling TLSv1.2.

2. Which NetScaler tool would you use to troubleshoot resets on an intranet server load-balanced by NetScaler?

A. Look in the Event Viewer

B. nslog via CLI

C. Take a packet trace with nstrace and analyze with WireShark

D. nslog

To diagnose TCP resets, you need visibility at the packet level to see exactly who is sending the reset and why. Taking a packet trace with nstrace on the NetScaler captures the traffic between the client, the appliance, and the backend servers, including the RST packets and the surrounding TCP state. Analyzing that trace in WireShark lets you inspect TCP flags, sequence numbers, and the handshake state, so you can determine whether the reset comes from the client, NetScaler, or a backend server, and reveal the cause (timeout, invalid state, server closing, MTU issues, etc.). Other options don't provide that direct packet-level insight: Event Viewer shows Windows events, not the actual TCP reset flow; NetScaler logs (nslog) record events but not the full packet detail needed to pinpoint the reset cause. Thus, combining nstrace with WireShark analysis is the most effective way to troubleshoot resets.

3. Which policy type defines criteria for granting access to internal resources after user authentication?

A. Client policy

B. Access policy

C. Authorization policy

D. VPN policy

After a user has been authenticated, the system must decide what they are allowed to do. This is governed by an authorization policy, which defines the rules and permissions that control access to internal resources. It uses identity, roles, group membership, and other attributes to determine concrete rights—such as which applications can be launched, which files can be opened, or which actions are permitted. It can also include conditions like time of day, device type, or location. VPN policy governs how a user connects to the network, not what they can access once connected. Client policy typically refers to settings on the user’s device. While sometimes you’ll see broader terms like access policy, the specific mechanism that determines access after authentication is the authorization policy.

4. Which step is essential to integrate an existing CERT-based authentication policy on Citrix Gateway?

A. Change the client certificate to Mandatory on the SSL parameters of the virtual server

B. Enable the two-factor option on the existing CERT authentication profile

C. Bind the existing CERT authentication policy to the Citrix Gateway virtual server

D. Create a CERT authentication policy and bind it to the Citrix Gateway virtual server

Binding the existing certificate-based authentication policy to the Citrix Gateway virtual server is the essential step because policies only take effect when they are attached to the traffic they should protect. The certificate-based policy defines how client certificates are evaluated and what authentication result to return, and binding ties that evaluation to the gateway’s virtual server so user requests are actually checked during authentication. Without this binding, the policy exists but is not applied to any traffic, so it won’t influence access.   Changing the SSL parameter to require client certificates, or enabling two-factor on the policy, would adjust security behavior in different ways but aren’t what makes the existing policy active for the gateway. Creating a new CERT authentication policy isn’t necessary since an appropriate existing policy already exists; binding it is the proper step to apply it to the Citrix Gateway virtual server.

5. **How can the administrator use Citrix Application Delivery Management to alert when the number of connections to virtual servers exceeds a threshold?**

   A. **Configure Network Reporting on the Citrix Application Delivery Management by setting the threshold and email address**

   B. **Configure TCP Insight on the Citrix Application Delivery Management**

   C. **Configure specific alerts for virtual servers using Citrix Application Delivery Management**

   D. **Configure SMTP Reporting on the Citrix Application Delivery Management by adding the threshold and email address**

Monitoring and alerting for high connection counts to virtual servers is handled by Network Reporting in Citrix ADM. By enabling Network Reporting, you can set a threshold for the number of connections and specify an email address to receive alerts when that threshold is exceeded. This gives real-time notification when load crosses the limit, so you can respond quickly. Other options don't fit as well because TCP Insight is focused on TCP performance diagnostics rather than triggering threshold-based alerts, and SMTP Reporting is about sending scheduled reports rather than live alerts. While configuring alerts for virtual servers might seem related, the established path for this specific scenario is to use Network Reporting with a threshold and an email target.

6. **If a team member has full admin partition permissions but cannot use aaad.debug in the CLI, what is the most likely reason?**

   A. **The team member does NOT have permission to use the CLI.**

   B. **The team member does NOT have Shell access by design.**

   C. **The team member needs to troubleshoot the issue from the GUI.**

   D. **The team member is NOT using the CLI correctly.**

Shell access and partition-level admin rights operate at different layers. The aaad.debug command is a debugging tool that runs in the underlying operating system shell, not in the NetScaler management CLI. Even with full admin partition permissions, you don't automatically gain access to the OS shell. If shell access is disabled by design for that user, the command won't be available in the CLI. To troubleshoot, you'd need to enable shell access for that account (if allowed) or use diagnostics available within the NetScaler CLI or GUI that don't require OS-shell access.

7. Which symptom would most strongly suggest SSL encryption is not configured on a server?

A. Packets captured show plaintext data

B. The connection completes TLS handshake with a strong cipher

C. The server returns 500 Internal Server Error

D. The data transfer is always encrypted

When SSL/TLS is in use, the data payload is encrypted after the handshake, so what you see on the network is unreadable application data even though the connection is secure. If you capture packets and the contents are readable in cleartext, that means the traffic isn’t being encrypted by SSL/TLS for that server, so SSL encryption is not configured there. This is the most definitive signal that encryption isn’t applied to the connection. Seeing a TLS handshake with a strong cipher would indicate encryption is configured, because the handshake and certificate exchange establish the secure channel. A 500 Internal Server Error is just an HTTP error and doesn’t reveal anything about whether SSL is enabled. If the data transfer is always encrypted, that points to encryption being in place (though it could be due to other factors like an upstream terminator), not to a lack of SSL configuration on the server.

8. What is the purpose of the nslog log type on Citrix ADC?

A. It stores server access logs

B. It stores detailed statistics, metrics and debugging data in a proprietary binary format

C. It stores configuration changes

D. It stores user authentication events

The nslog log type is meant for deep diagnostic telemetry from Citrix ADC. It captures detailed statistics, metrics, and debugging data about the appliance’s internal state and events, packaged in a compact binary format for efficient storage and processing. This kind of log is designed for troubleshooting and performance analysis, not for everyday user activity or operational events. Because the data is in a proprietary binary format, it isn’t meant to be read like plain text logs; you typically use Citrix tooling or a specialized parser to interpret it. This makes nslog distinct from logs that record server access, configuration changes, or user authentication events, which are more routine and human-readable.

9. What is the effect of enabling caseSensitive ON on a vserver in terms of host header matching?

A. It disables host header matching.

B. It makes host header matching case-insensitive.

C. It triggers SSL offload.

D. It makes host header matching case-sensitive.

Enabling caseSensitive on a vserver makes Host header matching exact and case-sensitive. The Host header is used to route requests to the correct backend when you rely on host-based routing. With this setting on, the Host header value must match the configured host exactly, including the case of letters. For instance, a Host header of example.com will match only a configured host of example.com, not EXAMPLE.COM or Example.COM. If you don't enable this, Host header comparisons are effectively case-insensitive, so different casings would still route to the same vserver. This behavior is specific to Host header matching and doesn't impact SSL offload or other unrelated functions.

10. Which setting reduces server load and increases SSL transactions per second on a SSL virtual server created with default settings?

A. SSLv3

B. Session Reuse

C. Session Timeout

D. SSLv2 Redirect

Reusing SSL/TLS sessions reduces the work the server must do for each new connection. When a client first connects, the SSL/TLS handshake performs expensive public-key operations and certificate checks. If session reuse is enabled, subsequent connections from the same client can resume that prior session instead of doing a full handshake, skipping those heavy steps. This cuts CPU load and frees up capacity, increasing SSL transactions per second on the virtual server with default settings. In Citrix ADC, this TLS session resumption is typically realized via a session ID or session ticket, allowing the server to rapidly establish new connections without the full handshake each time. The other options don't provide this capability: legacy protocols (SSLv3, SSLv2) are not about performance gains in this context, and adjusting session timeout changes how long a session remains valid rather than enabling efficient reuse across connections.

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://citrix1y0231.examzify.com

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