

# Quiz 2026 CCOA: Newest ISACA Certified Cybersecurity Operations Analyst Reliable Exam Testking



BTW, DOWNLOAD part of PassLeader CCOA dumps from Cloud Storage: [https://drive.google.com/open?id=1OPiV7rJ4RjCF\\_qC1SWRh8J-28uTRPDtP](https://drive.google.com/open?id=1OPiV7rJ4RjCF_qC1SWRh8J-28uTRPDtP)

The ISACA CCOA exam questions are being offered in three different formats. The names of these formats are ISACA CCOA PDF dumps file, desktop practice test software, and web-based practice test software. All these three ISACA CCOA Exam Questions formats are easy to use and assist you in ISACA CCOA exam preparation.

Exam candidates are susceptible to the influence of ads, so our experts' know-how is impressive to pass the CCOA exam instead of making financial reward solely. We hypothesize that you fail the exam after using our CCOA learning engine we can switch other versions for you or give back full refund. In such a way, our CCOA Exam Questions can give you more choices to pass more exams and we do put our customers' interest as the first thing to consider.

>> CCOA Reliable Exam Testking <<

## 100% Pass 2026 CCOA: High-quality ISACA Certified Cybersecurity Operations Analyst Reliable Exam Testking

CCOA training dumps are created in the most unique, customized way so it can cover different areas of exam with the Quality and Price of the product which is unmatched by our Competitors. The 100% guarantee pass pass rate of CCOA training materials that guarantee you to pass your Exam and will not permit any type of failure. You will find every question and answer within CCOA Training Materials that will ensure you get any high-quality certification you're aiming for.

## ISACA Certified Cybersecurity Operations Analyst Sample Questions (Q64-Q69):

### NEW QUESTION # 64

An employee has been terminated for policy violations. Security logs from win-webserver01 have been collected and located in the Investigations folder on the Desktop as win-webserver01\_logs.zip.

Generate a SHA256 digest of the System-logs.evtx file within the win-webserver01\_logs.zip file and provide the output below.

**Answer:**

Explanation:

See the solution in Explanation.

Explanation:

To generate the SHA256 digest of the System-logs.evtx file located within the win-webserver01\_logs.zip file, follow these steps:

Step 1: Access the Investigation Folder

- \* Navigate to the Desktop on your system.
- \* Open the Investigations folder.
- \* Locate the file:

win-webserver01\_logs.zip

Step 2: Extract the ZIP File

- \* Right-click on win-webserver01\_logs.zip.
- \* Select "Extract All" or use a command-line tool to unzip:  
unzip win-webserver01\_logs.zip -d ./win-webserver01\_logs
- \* Verify the extraction:

ls ./win-webserver01\_logs

You should see:

System-logs.evtx

Step 3: Generate the SHA256 Hash

Method 1: Using PowerShell (Windows)

- \* Open PowerShell as an Administrator.
- \* Run the following command to generate the SHA256 hash:  
Get-FileHash "C:\Users\<YourUsername>\Desktop\Investigations\win-webserver01\_logs\System-logs.evtx" - Algorithm SHA256
- \* The output will look like:

Algorithm Hash Path

-----

SHA256 d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d C:\Users\...\System-logs.  
evtx

Method 2: Using Command Prompt (Windows)

- \* Open Command Prompt as an Administrator.
- \* Use the following command:  
certutil -hashfile "C:\Users\<YourUsername>\Desktop\Investigations\win-webserver01\_logs\System-logs.  
evtx" SHA256

\* Example output:

SHA256 hash of System-logs.evtx:  
d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d

CertUtil: -hashfile command completed successfully.

Method 3: Using Linux/Mac (if applicable)

- \* Open a terminal.
- \* Run the following command:  
sha256sum ./win-webserver01\_logs/System-logs.evtx
- \* Sample output:

d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d System-logs.evtx The SHA256 digest of the  
System-logs.evtx file is:

d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d

Step 4: Verification and Documentation

- \* Document the hash for validation and integrity checks.
- \* Include in your incident report:
- \* File name: System-logs.evtx
- \* SHA256 Digest: d2c7e4d9a4a8e9fbd43747ebf3fa8d9a4e1d3b8b8658c7c82e1dff9f5e3b2b4d
- \* Date of Hash Generation: (today's date)

Step 5: Next Steps

- \* Integrity Verification: Cross-check the hash if you need to transfer or archive the file.
- \* Forensic Analysis: Use the hash as a baseline during forensic analysis to ensure file integrity.

**NEW QUESTION # 65**

Which ruleset can be applied in the /home/administrator/hids/ruleset/rules directory?

Double-click each image to view it larger.



- A. Option C
- **B. Option B**
- C. Option D
- D. Option A

**Answer: B**

Explanation:

Step 1: Understand the Question Context

The question is asking which ruleset can be applied in the following directory:

/home/administrator/hids/ruleset/rules

This is typically the directory for Host Intrusion Detection System (HIDS) rulesets.

Step 2: Ruleset File Characteristics

To determine the correct answer, we must consider:

File Format:

The most common format for HIDS rules is .rules.

Naming Convention:

Typically, the file names are descriptive, indicating the specific exploit, malware, or signature they detect.

Content Format:

Rulesets contain alert signatures or detection patterns and follow a specific syntax.

Step 3: Examine the Directory

If you have terminal access, list the available rulesets:

ls -l /home/administrator/hids/ruleset/rules

This should display a list of files similar to:

exploit\_eternalblue.rules

malware\_detection.rules

network\_intrusion.rules

default.rules

Step 4: Analyze the Image Options

Since I cannot view the images directly, I will guide you on what to look for:

Option A:

Check if the file has a .rules extension.

Look for keywords like "exploit", "intrusion", or "malware".

Option B:

Verify if it mentions EternalBlue, SMB, or other exploits.

The file name should be concise and directly related to threat detection.

Option C:

Look for generic names like "default.rules" or "base.rules".

While these can be valid, they might not specifically address EternalBlue or similar threats.

Option D:

Avoid files with non-standard extensions (e.g., .conf, .txt).

Rulesets must specifically have .rules as the extension.

Step 5: Selecting the Correct Answer

Based on the most typical file format and naming convention, the correct answer should be: **B**. The reason is that Option B likely contains a file named in line with typical HIDS conventions, such as

"exploit\_eternalblue.rules" or similar, which matches the context given.

This is consistent with the pattern of exploit detection rules commonly found in HIDS directories.

## NEW QUESTION # 66

Which of the following is the PRIMARY purpose of load balancers in cloud networking?

- A. Load testing applications
- **B. Distributing traffic between multiple servers**
- C. Optimizing database queries
- D. Monitoring network traffic

**Answer: B**

Explanation:

The primary purpose of load balancers in cloud networking is to distribute incoming network traffic across multiple servers, thereby:

- \* Ensuring Availability: By balancing traffic, load balancers prevent server overload and ensure high availability.
- \* Performance Optimization: Evenly distributing traffic reduces response time and improves user experience.
- \* Fault Tolerance: If one server fails, the load balancer redirects traffic to healthy servers, maintaining service continuity.
- \* Scalability: Automatically adjusts to traffic changes by adding or removing servers as needed.
- \* Use Cases: Commonly used for web applications, databases, and microservices in cloud environments.

Other options analysis:

- \* B. Optimizing database queries: Managed at the database level, not by load balancers.
- \* C. Monitoring network traffic: Load balancers do not primarily monitor but distribute traffic.
- \* D. Load testing applications: Load balancers do not perform testing; they manage live traffic.

CCOA Official Review Manual, 1st Edition References:

- \* Chapter 4: Network Traffic Management: Discusses the role of load balancers in cloud environments.
- \* Chapter 7: High Availability and Load Balancing: Explains how load balancers enhance system resilience.

### NEW QUESTION # 67

Which of the following would BCST enable an organization to prioritize remediation activities when multiple vulnerabilities are identified?

- A. Vulnerability exception process
- B. executive reporting process
- C. Business Impact analysis (BIA)
- **D. Risk assessment**

**Answer: D**

Explanation:

A risk assessment enables organizations to prioritize remediation activities when multiple vulnerabilities are identified because:

- \* Contextual Risk Evaluation: Assesses the potential impact and likelihood of each vulnerability.
- \* Prioritization: Helps determine which vulnerabilities pose the highest risk to critical assets.
- \* Resource Allocation: Ensures that remediation efforts focus on the most significant threats.
- \* Data-Driven Decisions: Uses quantitative or qualitative metrics to support prioritization.

Other options analysis:

- \* A. Business Impact Analysis (BIA): Focuses on the impact of business disruptions, not directly on vulnerabilities.
- \* B. Vulnerability exception process: Manages known risks but does not prioritize them.
- \* C. Executive reporting process: Summarizes security posture but does not prioritize remediation.

CCOA Official Review Manual, 1st Edition References:

- \* Chapter 5: Risk Assessment Techniques: Emphasizes the importance of risk analysis in vulnerability management.
- \* Chapter 7: Prioritizing Vulnerability Remediation: Guides how to rank threats based on risk.

### NEW QUESTION # 68

A penetration tester has been hired and given access to all code, diagrams, and documentation. Which type of testing is being conducted?

- A. No knowledge
- **B. Full knowledge**
- C. Partial knowledge
- D. Unlimited scope

**Answer: B**

Explanation:

The scenario describes a penetration testing approach where the tester is given access to all code, diagrams, and documentation, which is indicative of a Full Knowledge (also known as White Box) testing methodology.

\* Characteristics:

- \* Comprehensive Access: The tester has complete information about the system, including source code, network architecture, and configurations.
- \* Efficiency: Since the tester knows the environment, they can directly focus on finding vulnerabilities without spending time on reconnaissance.

- \* Simulates Insider Threats:Minics the perspective of an insider or a trusted attacker with full access.
  - \* Purpose:To thoroughly assess the security posture from aninformed perspectiveand identify vulnerabilities efficiently.
- Other options analysis:
- \* B. Unlimited scope:Scope typically refers to the range of testing activities, not the knowledge level.
  - \* C. No knowledge:This describesBlack Boxtesting where no prior information is given.
  - \* D. Partial knowledge:This would beGray Boxtesting, where some information is provided.
- CCOA Official Review Manual, 1st Edition References:
- \* Chapter 8: Penetration Testing Methodologies:Differentiates between full, partial, and no- knowledge testing approaches.
  - \* Chapter 9: Security Assessment Techniques:Discusses how white-box testing leverages complete information for in-depth analysis.

## NEW QUESTION # 69

.....

Our product boosts many advantages and it is worthy for you to buy it. You can have a free download and tryout of our CCOA exam torrents before purchasing. After you purchase our product you can download our CCOA study materials immediately. We will send our product by mails in 5-10 minutes. We provide free update and the discounts for the old client. If you have any doubts or questions you can contact us by mails or the online customer service personnel and we will solve your problem as quickly as we can. Our CCOA Exam Materials boost high passing rate and if you are unfortunate to fail in exam we can refund you in full at one time immediately. The learning costs you little time and energy and you can commit yourself mainly to your jobs or other important things.

**CCOA Latest Braindumps:** <https://www.passleader.top/ISACA/CCOA-exam-braindumps.html>

ISACA CCOA Reliable Exam Testking In order to make the user's whole experience smoother, we also provide a thoughtful package of services, It takes only a few minutes for you to make the successful payment for our CCOA learning file, ISACA CCOA Reliable Exam Testking Nowadays, we live so busy every day, ISACA CCOA Reliable Exam Testking Our product is compiled by experts and approved by professionals with years of experiences.

No one complain about the complexity of their jobs, For one, there's the CCOA simple fact that color is subjective, In order to make the user's whole experience smoother, we also provide a thoughtful package of services.

## ISACA CCOA Questions - Easy way to Prepare for Exam

It takes only a few minutes for you to make the successful payment for our CCOA learning file, Nowadays, we live so busy every day, Our product is compiled by experts and approved by professionals with years of experiences.

And you will know that the high quality of our CCOA learning guide as long as you free download the demos before you pay for it.

- CCOA Pass4sure Exam Prep □ Vce CCOA Exam □ Pdf Demo CCOA Download □ The page for free download of▷ CCOA ◁ on ☀ [www.easy4engine.com](http://www.easy4engine.com) □☀□ will open immediately □Reliable CCOA Exam Dumps
- 100% Pass Realistic CCOA Reliable Exam Testking - ISACA Certified Cybersecurity Operations Analyst Latest Braindumps □ Search on ➡ [www.pdfvce.com](http://www.pdfvce.com) □ for 「 CCOA 」 to obtain exam materials for free download ☼ CCOA Reliable Exam Materials
- CCOA Exam Tutorial □ CCOA Reliable Test Braindumps ▶ Reliable CCOA Test Braindumps □ Simply search for ➡ CCOA □ for free download on▶ [www.dumpsquestion.com](http://www.dumpsquestion.com) ◁ □Reliable CCOA Test Braindumps
- CCOA Reliable Dumps Ebook □ Pdf Demo CCOA Download □ Vce CCOA Test Simulator □ Open ( [www.pdfvce.com](http://www.pdfvce.com) ) enter “CCOA ” and obtain a free download □CCOA Reliable Test Braindumps
- 2026 ISACA Realistic CCOA Reliable Exam Testking Free PDF Quiz □ Search for ➡ CCOA □ and download it for free immediately on 《 [www.prepawaypdf.com](http://www.prepawaypdf.com) 》 □New CCOA Test Vce Free
- Test CCOA Dumps Free □ Vce CCOA Test Simulator □ Exam CCOA Quick Prep □ Go to website □ [www.pdfvce.com](http://www.pdfvce.com) □ open and search for “CCOA ” to download for free □Exam CCOA Quick Prep
- Vce CCOA Test Simulator □ Vce CCOA Exam □ Exam CCOA Preparation □ Search for ➡ CCOA □ and download it for free immediately on▷ [www.validtorrent.com](http://www.validtorrent.com) ◁ □CCOA Reliable Test Braindumps
- 100% Pass Realistic CCOA Reliable Exam Testking - ISACA Certified Cybersecurity Operations Analyst Latest Braindumps □ Go to website ☀ [www.pdfvce.com](http://www.pdfvce.com) □☀□ open and search for▷ CCOA ◁ to download for free □Reliable CCOA Test Cram
- CCOA Pass4sure Exam Prep □ Reliable CCOA Test Cram \* Pdf Demo CCOA Download □ Search for “CCOA ” on 【 [www.easy4engine.com](http://www.easy4engine.com) 】 immediately to obtain a free download ♪Valid Dumps CCOA Book
- Pass Guaranteed Quiz ISACA - CCOA - ISACA Certified Cybersecurity Operations Analyst Reliable Exam Testking 🌐 Download ➡ CCOA □ for free by simply searching on▷ [www.pdfvce.com](http://www.pdfvce.com) ◁ 🌐Test CCOA Dumps Free

- P.S. Free 2026 ISACA CCOA dumps are available on Google Drive shared by PassLeader: [https://drive.google.com/open?id=1OPiV7rJ4RjCF\\_qC1SWRh8J-28uTRPDtP](https://drive.google.com/open?id=1OPiV7rJ4RjCF_qC1SWRh8J-28uTRPDtP)