ITCertMagic GH-500 Mock Exam/Download Instantly


ITCertMagic

Itcertmagic Guarantee All Exams 100% Pass One Time!

NEW QUESTION 41
You want to implement a 28-day backup cycle. Which scenario uses the least storage?
A. Full backup, incremental backup, log backup
B. Full backup, log backup
C. Incremental backup, log backup
D. Full backup, differential backup, log backup
Answer: B

NEW QUESTION 42
You are running an SAP HANA database in log mode "normal"
Under what circumstances does the database automatically execute a regular log backup?
Note: There are 2 correct answers to this question.
A. When a commit occurs
B. When the log segment is full
C. When the time threshold is exceeded
D. When the log buffer is full
Answer: B,C

NEW QUESTION 43
Which database objects can manipulate if you have the Object privilege activity ALL PRIVILEGES? Note: There are 2 correct answers to this question.
A. Views
B. Functions
C. Procedures
D. Schemas
Answer: A,D

NEW QUESTION 44
What action(s) can you perform in the SAP HANA cockpit to back up the complete database system?
A. Back up the system using a fallback snapshot for every database
B. Back up the system database and all tenant databases individually
C. Back up the system database and all tenant databases in one step
D. Back up the system using a database snapshot and a data snapshot.

https://itcertmagic.com/SAP/real-C_HANATEC_18-exam-prep-dumps.html

The ITCertMagic Microsoft GH-500 exam dumps are ready for quick download. Just choose the right ITCertMagic Microsoft GH-500 exam questions format and download it after paying an affordable ITCertMagic GitHub Advanced Security (GH-500) practice questions charge and start this journey. Best of luck in Microsoft GH-500 exam and career!!!

Microsoft GH-500 Exam Syllabus Topics:

Topic	Details
Topic 1	• Configure and use Dependabot and Dependency Review: Focused on Software Engineers and Vulnerability Management Specialists, this section describes tools for managing vulnerabilities in dependencies. Candidates learn about the dependency graph and how it is generated, the concept and format of the Software Bill of Materials (SBOM), definitions of dependency vulnerabilities, Dependabot alerts and security updates, and Dependency Review functionality. It covers how alerts are generated based on the dependency graph and GitHub Advisory Database, differences between Dependabot and Dependency Review, enabling and configuring these tools in private repositories and organizations, default alert settings, required permissions, creating Dependabot configuration files and rules to auto-dismiss alerts, setting up Dependency Review workflows including license checks and severity thresholds, configuring notifications, identifying vulnerabilities from alerts and pull requests, enabling security updates, and taking remediation actions including testing and merging pull requests.
Topic 2	• Describe the GHAS security features and functionality: This section of the exam measures skills of Security Engineers and Software Developers and covers understanding the role of GitHub Advanced Security (GHAS) features within the overall security ecosystem. Candidates learn to differentiate security features available automatically for open source projects versus those unlocked when GHAS is paired with GitHub Enterprise Cloud (GHEC) or GitHub Enterprise Server (GHES). The domain includes knowledge of Security Overview dashboards, the distinctions between secret scanning and code scanning, and how secret scanning, code scanning, and Dependabot work together to secure the software development lifecycle. It also covers scenarios contrasting isolated security reviews with integrated security throughout the development lifecycle, how vulnerable dependencies are detected using manifests and vulnerability databases, appropriate responses to alerts, the risks of ignoring alerts, developer responsibilities for alerts, access management for viewing alerts, and the placement of Dependabot alerts in the development process.
Topic 3	• Configure and use secret scanning: This domain targets DevOps Engineers and Security Analysts with the skills to configure and manage secret scanning. It includes understanding what secret scanning is and its push protection capability to prevent secret leaks. Candidates differentiate secret scanning availability in public versus private repositories, enable scanning in private repos, and learn how to respond appropriately to alerts. The domain covers alert generation criteria for secrets, user role-based alert visibility and notification, customizing default scanning behavior, assigning alert recipients beyond admins, excluding files from scans, and enabling custom secret scanning within repositories.

Topic 4	• Configure and use Code Scanning with CodeQL: This domain measures skills of Application Security Analysts and DevSecOps Engineers in code scanning using both CodeQL and third-party tools. It covers enabling code scanning, the role of code scanning in the development lifecycle, differences between enabling CodeQL versus third-party analysis, implementing CodeQL in GitHub Actions workflows versus other CI tools, uploading SARIF results, configuring workflow frequency and triggering events, editing workflow templates for active repositories, viewing CodeQL scan results, troubleshooting workflow failures and customizing configurations, analyzing data flows through code, interpreting code scanning alerts with linked documentation, deciding when to dismiss alerts, understanding CodeQL limitations related to compilation and language support, and defining SARIF categories.
Topic 5	• Describe GitHub Advanced Security best practices, results, and how to take corrective measures: This section evaluates skills of Security Managers and Development Team Leads in effectively handling GHAS results and applying best practices. It includes using Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) identifiers to describe alerts and suggest remediation, decision-making processes for closing or dismissing alerts including documentation and data-based decisions, understanding default CodeQL query suites, how CodeQL analyzes compiled versus interpreted languages, the roles and responsibilities of development and security teams in workflows, adjusting severity thresholds for code scanning pull request status checks, prioritizing secret scanning remediation with filters, enforcing CodeQL and Dependency Review workflows via repository rulesets, and configuring code scanning, secret scanning, and dependency analysis to detect and remediate vulnerabilities earlier in the development lifecycle, such as during pull requests or by enabling push protection.

Microsoft GH-500 Exam Prep Solutions

The Microsoft GH-500 practice material of ITCertMagic came into existence after consultation with many professionals and getting their positive reviews. The majority of aspirants are office professionals, and we recognize that you don't have enough time to prepare for the Microsoft GH-500 Certification Exam. As a result, several versions of the GitHub Advanced Security (GH-500) exam questions will be beneficial to you.

Microsoft GitHub Advanced Security Sample Questions (Q50-Q55):

NEW QUESTION # 50
In the pull request, how can developers avoid adding new dependencies with known vulnerabilities?

- A. Enable Dependabot alerts.
- B. Add a workflow with the dependency review action.
- C. Add Dependabot rules.
- D. Enable Dependabot security updates.

Answer: B

Explanation:
To detect and block vulnerable dependencies before merge, developers should use the Dependency Review GitHub Action in their pull request workflows. It scans all proposed dependency changes and flags any packages with known vulnerabilities.
This is a preventative measure during development, unlike Dependabot, which reacts after the fact.

NEW QUESTION # 51
What are Dependabot security updates?

- A. Automated pull requests to update the manifest to the latest version of the dependency
- B. Automated pull requests that help you update dependencies that have known vulnerabilities
- C. Automated pull requests that keep your dependencies updated, even when they don't have any vulnerabilities
- D. Compatibility scores to let you know whether updating a dependency could cause breaking changes to your project

Answer: B

Explanation:
Dependabot security updates are automated pull requests triggered when GitHub detects a vulnerability in a dependency listed in your manifest or lockfile. These PRs upgrade the dependency to the minimum safe version that fixes the vulnerability.
This is separate from regular updates (which keep versions current even if not vulnerable).

NEW QUESTION # 52
Which of the following is the most complete method for Dependabot to find vulnerabilities in third-party dependencies?

- A. The build tool finds the vulnerable dependencies and calls the Dependabot API
- B. CodeQL analyzes the code and raises vulnerabilities in third-party dependencies
- C. Dependabot reviews manifest files in the repository
- D. A dependency graph is created, and Dependabot compares the graph to the GitHub Advisory database

Answer: D

Explanation:
Dependabot builds a dependency graph by analyzing package manifests and lockfiles in your repository. This graph includes both direct and transitive dependencies. It then compares this graph against the GitHub Advisory Database, which includes curated, security-reviewed advisories.
This method provides a comprehensive and automated way to discover all known vulnerabilities across your dependency tree.

NEW QUESTION # 53
Secret scanning will scan:

- A. The GitHub repository.
- B. External services.
- C. A continuous integration system.
- D. Any Git repository.

Answer: A

Explanation:
Secret scanning is a feature provided by GitHub that scans the contents of your GitHub repositories for known types of secrets, such as API keys and tokens. It operates within the GitHub environment and does not scan external systems, services, or repositories outside of GitHub. Its primary function is to prevent the accidental exposure of sensitive information within your GitHub-hosted code.

NEW QUESTION # 54
How would you build your code within the CodeQL analysis workflow? (Each answer presents a complete solution. Choose two.)

- A. Use jobs.analyze.runs-on.
- B. Implement custom build steps.
- C. Ignore paths.
- D. Use CodeQL's init action.
- E. Upload compiled binaries.
- F. Use CodeQL's autobuild action.

Answer: B,F

Explanation:
Comprehensive and Detailed Explanation:
When setting up CodeQL analysis for compiled languages, there are two primary methods to build your code:
GitHub Docs
Autobuild: CodeQL attempts to automatically build your codebase using the most likely build method. This is suitable for standard build processes.
GitHub Docs

Custom Build Steps: For complex or non-standard build processes, you can implement custom build steps by specifying explicit build commands in your workflow. This provides greater control over the build process.
GitHub Docs
The init action initializes the CodeQL analysis but does not build the code. The jobs.analyze.runs-on specifies the operating system for the runner but is not directly related to building the code. Uploading compiled binaries is not a method supported by CodeQL for analysis.

NEW QUESTION # 55
......

Due to the shortage of useful practice materials or being scanty for them, many candidates may choose the bad quality exam materials, but more and more candidates can choose our GH-500 study materials. Actually, some practice materials are shooting the breeze about their effectiveness, but our GH-500 training quiz are real high quality practice materials with passing rate up to 98 to 100 percent. And you will be amazed to find that our GH-500 exam questions are exactly the same ones in the real exam.

GH-500 Test Answers: https://www.itcertmagic.com/Microsoft/real-GH-500-exam-prep-dumps.html

- Pass-Sure GH-500 Mock Exam, Ensure to pass the GH-500 Exam □ Copy URL ➽ www.free4dump.com □ open and search for [GH-500] to download for free □Exam GH-500 Revision Plan
- First-hand Microsoft GH-500 Mock Exam - GitHub Advanced Security Test Answers □ Search for 《 GH-500 》 on ➠ www.pdfvce.com □ immediately to obtain a free download □Valid GH-500 Exam Review
- First-hand Microsoft GH-500 Mock Exam - GitHub Advanced Security Test Answers □ Open website ➽ www.dumpsquestion.com □ and search for ⇛ GH-500 ⇚ for free download □Valid Test GH-500 Test
- Valid GH-500 Exam Review □ Premium GH-500 Files 🈵 GH-500 Upgrade Dumps □ Search for ✔ GH-500 □✔□ and obtain a free download on ▹ www.pdfvce.com ◃ □GH-500 Certification Exam Cost
- GH-500 Latest Test Fee □ Valid GH-500 Exam Review □ GH-500 Test Collection Pdf □ Search for ➤ GH-500 □ and easily obtain a free download on [www.vceengine.com] □Valid Test GH-500 Test
- Reliable GH-500 Exam Pdf □ Valid GH-500 Exam Review □ GH-500 Latest Test Fee □ Open （ www.pdfvce.com ） enter □ GH-500 □ and obtain a free download □Associate GH-500 Level Exam
- How Microsoft GH-500 Exam Questions Can Help You in Preparation? □ 「 www.testsimulate.com 」 is best website to obtain ➥ GH-500 □ for free download □Exam GH-500 Revision Plan
- Microsoft GitHub Advanced Security Exam Questions in 3 User-Friendly Formats □ Search for ➽ GH-500 □ and easily obtain a free download on ➽ www.pdfvce.com □ □Valid Test GH-500 Test
- Reliable GH-500 Exam Pdf □ Exam GH-500 Training □ Exam GH-500 Training □ Easily obtain [GH-500] for free download through ➡ www.real4dumps.com □□□ □Braindumps GH-500 Downloads
- First-hand Microsoft GH-500 Mock Exam - GitHub Advanced Security Test Answers □ Easily obtain ☀ GH-500 □☀□ for free download through [www.pdfvce.com] □Latest GH-500 Cram Materials
- Valid GH-500 Exam Testking □ GH-500 Upgrade Dumps □ GH-500 Latest Exam Cost □ The page for free download of " GH-500 " on □ www.dumps4pdf.com □ will open immediately □Exam GH-500 Training
- myportal.utt.edu.tt, motionentrance.edu.np, kareyed271.ka-blogs.com, dakusfranlearning.com, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, training.autodetailing.app, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes