Microsoft

Exam Questions GH-100

GitHub Administration Exam

NEW QUESTION 1
Why is a GitHub App preferred over a PAT for machine authentication?

A. GitHub Apps are required to pass SAML assertions
B. GitHub Apps have time-limited installation tokens with scoped access
C. PATs cannot be used in GitHub Actions
D. PATs support fewer GitHub APIs than Apps

Answer: B

Explanation:
GitHub Apps issue short#lived installation tokens that you scope to only the permissions and repositories your automation needs, reducing blast radius and automatically rotating credentials.

NEW QUESTION 2
Which of the following is a key benefit of using GitHub Marketplace Apps in an enterprise?

A. They guarantee no downtime during enterprise GitHub maintenance windows
B. They often include integrations with external services, reducing the need for custom code
C. Apps eliminate the need for GitHub Actions entirely
D. All apps come pre-approved by GitHub's internal security team

Answer: B

Explanation:
GitHub Marketplace Apps come with built?in integrations to external services - so you can plug in things like CI servers, code-quality scanners, or deployment tools without writing and maintaining custom connectors.

NEW QUESTION 3
How is CodeQL different from other static analysis tools?

A. It removes insecure code automatically
B. It allows querying of code semantics using a database-like language.
C. It only works for open-source projects.
D. It runs analysis only after a security breach.

Answer: B

Explanation:
CodeQL differs from traditional static analysis tools by ingesting your code into a queryable database and letting you write QL queries - its own database?style language - to express semantic checks and find patterns across the codebase.

NEW QUESTION 4
When a token is used to perform actions across different GitHub resources, how is this reflected in audit logs?

A. Each API action made with the token generates a separate audit log entry
B. Only the first repository accessed is recorded
C. GitHub creates a ZIP archive of all token activity
D. The audit log stores only the token name and not its actions

Answer: A

Explanation:
Each API call authenticated with a token generates its own audit-log event, so you'll see a distinct entry for every action performed across different resources, each annotated with the token's hashed ID, actor, and source IP.

NEW QUESTION 5
What will happen if Dependabot discovers a vulnerable transitive dependency in a repository?

A. It creates a pull request to update the direct dependency to a version that resolves the vulnerability.
B. It opens a pull request to update the affected package directly, regardless of version compatibility.
C. It automatically removes the package from the repository.
D. It sends an email to the repository owner but does not alter code.

Answer: A

Explanation:
Dependabot will automatically open a pull request that updates the direct dependency to a version which, in turn, resolves (or removes) the vulnerable transitive dependency—ensuring the fix is applied via your declared dependencies.

NEW QUESTION 6
Which of the following correctly describes the difference between controlling actions at the enterprise level versus the organization level in GitHub?

A. Enterprise policies and organization policies are independent, with organization policies taking precedence for repositories within the organization.
B. Enterprise policies configure mandatory settings for organizations.

C. Enterprise policies apply only to public repositories, while organization policies apply to public, internal, and private repositories.
D. Enterprise policies can block specific actions, while organization policies can only enable or disable actions entirely.

Answer: B

Explanation:
Enterprise policies let you define and enforce mandatory settings across all member organizations - organization#level policies then operate within the options that the enterprise policy exposes.

NEW QUESTION 7
What distinguishes Enterprise Managed Users (EMUs) from standard GitHub accounts?

A. EMUs are fully controlled by an IdP and cannot log in with personal credentials
B. EMUs can only be created using email invites
C. EMUs are managed in GitHub and use GitHub authentication
D. EMUs are only available for GitHub Enterprise Server

Answer: A

Explanation:
EMU accounts are provisioned and authenticated exclusively through your identity provider - users sign in via the IdP and cannot use or manage GitHub-native credentials.

NEW QUESTION 8
In a GitHub repository using Dependabot, which of the following best describes the purpose of the .github/dependabot.yml file?

A. It configures scheduling, package ecosystems, and target directories for update checks.
B. It lists commit SHAs to exclude from automatic pull requests.
C. It enables GitHub to scan for secrets in dependency files.
D. It encrypts dependency versions before storing them in the repo.

Answer: A

Explanation:
The .github/dependabot.yml file defines Dependabot's package-ecosystem, the directories to inspect, and the update schedule (daily/weekly/monthly), controlling when and where Dependabot checks for new versions.

NEW QUESTION 9
When a user becomes a member of multiple GitHub organizations, which THREE of the following are important considerations for administrators? (Choose three.)

A. The user will automatically have the same role across all organizations.
B. The user's repository access and/or team membership needs to be managed separately for each organization.
C. The user will need to authorize credentials separately for each SAML-enabled organization.
D. The user will have different permission levels in each organization.
E. The user's profile information becomes private to non-organization members.
F. The user's personal repositories will become accessible to all organizations.

Answer: BCD

Explanation:
A user's repository access and team memberships are scoped to each organization, so admins must configure permissions separately per org.
When an organization enforces SAML SSO, each member must authorize their personal access tokens or SSH keys for that org, requiring separate approval for each SAML?enabled organization
Roles and permission levels (owner, member, billing manager, repository roles, etc.) are assigned on a per?organization basis, so a user often has different permissions in different organizations.

NEW QUESTION 10
What benefit does GitHub Advanced Security provide?

A. helps organization administrators analyze and configure permissions to the least privilege required
B. helps developers improve and maintain the security and quality of code
C. helps enterprise administrators improve and maintain network security for their GitHub Enterprise Server instances
D. helps organization administrators manage security tokens

Answer: B

Explanation:
GitHub Advanced Security equips developers with built?in code scanning (CodeQL), secret scanning, dependency review, and other AppSec tools - helping them find, fix, and prevent security vulnerabilities while maintaining code quality.

NEW QUESTION 10
A team member is unable to push to a repository due to a 403-error related to branch protection. What should the GitHub Enterprise administrator do first?

A. Remove the user from the team and re-add them
B. Check the user's permissions and rulesets applied to the branch
C. Raise a GitHub Support request for permissions issues
D. Revert the branch to an earlier state

Answer: B

Explanation:
The administrator should first review the user's repository role and the branch protection rules applied to that branch. A 403 error on push almost always indicates that the user either lacks the necessary write permissions or is not listed among the actors authorized by the branch protection settings.

NEW QUESTION 13
What needs to be done to ensure that only specific repositories can access the runners in an organization runner group?

A. Use GitHub's meta API to configure access.
B. Add a label to the runner group.
C. Configure repository access in the runner group settings.
D. Configure the Actions Policies to "Only selected repositories".

Answer: C

Explanation:
In the organization's runner group settings, switch the access from "All repositories" to "Selected repositories" and then explicitly choose which repos may use those runners.

NEW QUESTION 14
Which practice helps avoid service disruption when consuming GitHub APIs at scale?

A. Designingyour application to work within GitHub's rate limits
B. Using multiple tokens to bypass limits
C. Caching all API responses permanently
D. Ignoring secondary rate limits

Answer: A

Explanation:
Designing your integration to stay within GitHub's documented rate limits—by batching requests, using conditional requests, handling 429 responses with back?off, and monitoring the X?RateLimit-* headers - ensures you won't be temporarily throttled or cut off when you hit secondary limits.

NEW QUESTION 17
Which of the following is the responsibility of a Team Maintainer in a GitHub organization? (Choose two.)

A. Modifying organization-wide settings.
B. Managing nested sub-teams.
C. Adding or removing team members.
D. Deleting repositories assigned to the team.

Answer: BC

Explanation:
Team maintainers can manage nested sub?teams - requesting to add or change parent/child teams within the organization's hierarchy.
Team maintainers have permission to add and remove members from their team, controlling day?to?day team membership.

NEW QUESTION 19
When comparing a partner identity provider integration with a non-partner identity management solution for GitHub Enterprise Managed Users, which statement is Correct?

A. The non-partner identity provider integrations can utilize OIDC for authentication.
B. The non-partner identity provider integrations require manual configuration of SAML 2.0 details.
C. The partner identity provider integrations support fewer GitHub-supported authentication methods.
D. The partner identity provider integrations rely on the partner to support the application on the partner IdP.

Answer: B

Explanation:
Non?partner identity provider integrations require you to enter SAML?2.0 configuration details by hand - such as the Sign?on URL, Issuer, and X.509 certificate - whereas partner IdPs supply a pre?configured application integration.

NEW QUESTION 23
Which product's usage is not included in GitHub Enterprise Cloud's monthly metered billing report?

A. Git LFS bandwidth
B. GitHub Actions minutes
C. GitHub Discussions engagement
D. GitHub Packages storage

Answer: C

Explanation:
GitHub?Discussions engagement isn't a metered product and doesn't appear in the "Product billing" list, so its usage isn't included in the monthly metered billing report.

NEW QUESTION 27

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

GH-100 Practice Exam Features:

* GH-100 Questions and Answers Updated Frequently

* GH-100 Practice Questions Verified by Expert Senior Certified Staff

* GH-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* GH-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
Order The GH-100 Practice Test Here