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
When comparing fine-grained Personal Access Tokens (PATs) with classic PATs, which of the following statements is accurate?

A. Fine-grained PATs automatically renew while classic PATs require manual renewal.
B. Fine-grained PATs permissions can be scoped to specific repositories.
C. Classic PATs offer more permission controls than fine-grained PATs.
D. Classic PATs can be restricted to specific organizations, but fine-grained PATs cannot.

Answer: B

Explanation:
Fine?grained personal access tokens let you scope permissions down to individual repositories, whereas classic PATs grant access across every repo the user can reach.

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
What is the effect of enforcing a policy that restricts GitHub Actions to only those created by the enterprise?

A. Marketplace actions are allowed only with SSO enabled
B. Actions can only be triggered by organization members
C. Only actions created within the enterprise are allowed
D. All public actions are allowed

Answer: C

Explanation:
When you enforce the "Allow enterprise actions and reusable workflows" policy, GitHub will block all workflows from using actions or reusable workflows that aren't defined in a repository within your enterprise - so only actions created inside your enterprise are allowed.

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
A financial services company is evaluating GitHub account types. Which of the following is a key distinction between GitHub Enterprise Managed Users and Personal Accounts?

A. Enterprise Managed Users can collaborate across both personal and enterprise repositories.

B. Personal Accounts are owned by users and can be used for both personal and professional work.
C. Personal Accounts provide stricter control over repositories and user activity.
D. Enterprise Managed Users require the organization to manage their own authentication server.

Answer: B

Explanation:
Personal Accounts are owned and controlled by individual users and can serve both their personal projects and professional work, whereas Enterprise Managed Users exist solely within the enterprise context and cannot be used for personal repositories.

NEW QUESTION 7
You discover that a secret (e.g., a token or password) was accidentally committed to a GitHub repository. What is the first step you should take to mitigate the risk?

A. Contact GitHub Support to remove the secret from all forks and clones of the repository.
B. Revoke and/or rotate the secret to render it unusable, then assess whether history rewriting is necessary.
C. Rewrite the repository history using git filter-repo or BFG Repo-Cleaner to remove the secret from all commits.
D. Delete the repository and create a new one to ensure the secret is no longer accessible.

Answer: B

Explanation:
The immediate priority is to revoke or rotate the exposed credential so it can no longer be used; once it??s invalidated, you can safely proceed with history?rewriting or other cleanup steps.

NEW QUESTION 8
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 9
You are managing a repository in your organization's GitHub account. A team member asks you to confirm who has access to the repository and their permission levels. Which tool should you use to review and manage repository access?

A. GitHub Pages Settings.
B. GitHub Actions Logs.
C. Repository Settings > Manage Access.
D. Branch Protection Rules.

Answer: C

Explanation:
Use the?Repository?Settings???Manage?Access page to view all users and teams with access and their assigned permission levels.

NEW QUESTION 10
Your organization is implementing team synchronization. Which of the following should you prioritize during the setup process?

A. Disabling the audit log stream
B. Setting an infrequent sync schedule to reduce performance impact
C. Allowing manual updates to team memberships
D. Clearly define how identity provider groups will align with GitHub teams and roles

Answer: D

Explanation:
Before you enable team synchronization, you should clearly define how groups in your identity provider will map to GitHub teams and roles - ensuring that when the sync runs, users land in the correct teams with the right permissions.

NEW QUESTION 10
Which events from the audit log are exposed by the GraphQL API? Each answer presents a complete solution. (Choose three.)

A. changes in permissions
B. promoting users to administrators
C. pushes to repositories

D. changes to permissions of a GitHub App
E. cloning of repositories

Answer: ABD

Explanation:
The GraphQL Audit Log API surfaces entries whenever repository or organization permissions are changed ("Changes permissions").
It records when users are elevated to administrative roles ("Promotes users to admin").
It logs alterations to a GitHub App's granted permissions ("Changes permissions of a GitHub App").

NEW QUESTION 13
Which factor affects GitHub Actions pricing for GitHub-hosted runners on GitHub Enterprise Cloud?

A. Number of workflows defined in .github/workflows/
B. Number of contributors to the repository Explanation:Incorrec
C. Contributor count does not impact billing for Actions
D. Total number of repositories using Actions
E. Operating system used in the runner environment

Answer: D

Explanation:
GitHub Actions billing for GitHub?hosted runners is based on the number of minutes consumed and the operating system of the runner - Linux, Windows, and macOS each have different per?minute rates.

NEW QUESTION 16
A token was used to access an organization's resource via API. What fields in the audit log help determine who used it?

A. The token's permissions and the geographic region of access
B. The token expiration date
C. The GitHub Actions runner name
D. The token ID, requesting IP address, and associated user

Answer: D

Explanation:
The audit log records the token's identifier (the hashed_token value), the source IP address of the request, and the actor (the user or app) associated with that token, allowing you to trace exactly who used it.

NEW QUESTION 18
What is the new capability of GitHub's billing dashboard?

A. Automatically removes unused users from billing
B. Enables tracking of GitHub Copilot usage byuser
C. Allows self-service plan upgrades
D. Offers real-time Slack alerts for billing

Answer: B

Explanation:
The revamped Billing?&?Licensing dashboard now includes a dedicated?"Copilot" tab that shows per?user seat assignments, usage counts, and estimated costs for your organization's GitHub Copilot licenses, enabling you to track Copilot consumption by individual users.

NEW QUESTION 19
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 23
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 28
Which of the following actions can a user with Write permissions perform in a GitHub repository?

A. Manage repository settings, such as labels and GitHub Pages.
B. Push code to non-protected branches.
C. Configure branch protection rules.
D. Delete the repository.

Answer: B

Explanation:
Users granted Write permission can push commits to non?protected branches, allowing them to update code without needing administrative rights.

NEW QUESTION 33
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 38
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 42
You are an administrator and need to enforce a policy on forking private and internal repositories. Which options are available for configuring the policy at the enterprise level? (Each answer presents a complete solution. Choose three.)

A. Allow organization owners to administer the setting at the organization level.
B. Allow people who have access to private and internal repositories to fork these repositories.
C. Allow specific people or teams to fork private and internal repositories.
D. Disallow repository owners from administering the setting at the repository level.
E. Disallow forking of private and internal repositories.

Answer: ABE

Explanation:
You can configure the enterprise policy to?allow organization owners to administer the forking setting at the organization level, giving them control over how repos fork within their orgs.
You can choose to?allow any user who already has access to a private or internal repo to fork it.
You can also set the policy to?never allow forking?of private or internal repositories across all organizations.

NEW QUESTION 43
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 48
What is the key benefit of using a GitHub security advisory within a repository?

A. It automatically reverts commits that introduced the vulnerability.
B. It allows maintainers to privately disclose, discuss, and publish vulnerabilities.
C. It flags all forks of the repository as vulnerable.
D. It prevents users from cloning the repository until issues are resolved.

Answer: B

Explanation:
GitHub security advisories let maintainers privately disclose, discuss fixes, and then publish vulnerabilities in a controlled manner within the repository.

NEW QUESTION 52
.....

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