Microsoft

Exam Questions GH-100

GitHub Administration Exam

NEW QUESTION 1
Which feature is unique to self-hosted runners?

A. Execute scripts before and after a job
B. Dynamic scaling
C. Automatic updates to the operating system
D. GPU support

Answer: A

Explanation:
Self#hosted runners support custom pre#and post#job scripts via runner hooks, letting you run arbitrary scripts before a job starts and after it finishes - capabilities not available on GitHub#hosted runners.

NEW QUESTION 2
You need GitHub to automatically notify a third-party service any time a new repository is created. You want to avoid writing custom code. The vendor has told you that they have a tool in the GitHub Marketplace. Which type of tool do you need?

A. GitHub App
B. GitHub Copilot Extension
C. GitHub Models
D. GitHub Action

Answer: A

Explanation:
You need a GitHub App. Marketplace integrations that listen for events like repository.created and send notifications are delivered as GitHub Apps, since they can subscribe to organization#level webhooks without you writing custom code.

NEW QUESTION 3
How does metered billing work in GitHub Enterprise Cloud with Enterprise Managed Users (EMU)?

A. Billing is based on number of total users in the enterprise
B. Billing is based on owners and members of GitHub organizations
C. Billing is based on total users in the enterprise that are not dormant
D. Billing is based on the number of users created in Azure AD

Answer: A

Explanation:
Billing for GitHub Enterprise Cloud under metered (usage#based) billing is calculated by the total number of Enterprise Managed Users (and other license#consuming accounts) in your enterprise - each EMU consumes a seat and contributes to the monthly bill.

NEW QUESTION 4
A GitHub Enterprise administrator is planning to implement SAML SSO across their company. Which of the following correctly distinguishes enterprise-wide SAML SSO from organization-level SAML SSO?

A. Enterprise-wide SAML SSO requires less initial administrative overhead than organization-level implementation.
B. Enterprise-wide SAML SSO allows different organizations to use different authentication methods.
C. Enterprise-wide SAML SSO immediately removes users who fail to authenticate via the IdP.
D. Enterprise-wide SAML SSO ensures users authenticate through the same IdP across all organizations.

Answer: D

Explanation:
Enterprise#wide SAML SSO enforces a single IdP across all member organizations—its configuration overrides any per#organization SAML settings, so everyone must authenticate through the same provider.

NEW QUESTION 5
Our organization is updating its enterprise policies. Which of the following steps should you take to ensure alignment with security requirements?

A. Maintain clear documentation of existing policies and policy changes.
B. Implement the new enterprise policies across the organization first and then consult with the security team to identify- any necessary adjustments or retrofits
C. Implement changes without consulting stakeholders.
D. Regularly assess and adjust policies based on evolving risks.

Answer: AB

NEW QUESTION 6
What is the first step when sensitive data is accidentally pushed to a public GitHub repository?

A. Revoke any exposed credentials immediately
B. Force push a commit removing the data
C. Open an issue to inform users
D. Delete the repository

Answer: A

Explanation:
Revoke and/or rotate the exposed credentials immediately so they can no longer be used - this is the critical first step before you undertake any history?rewriting or cleanup.

NEW QUESTION 7
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 8
Which Git operation is not included in the Git activity audit log?

A. Delete branch
B. Fetch
C. Push
D. Clone

Answer: A

Explanation:
Delete branch operations aren't tracked as Git-activity events; the Git activity audit log only records Git events such as clone, fetch (pull), and push.

NEW QUESTION 9
What is the potential consequence of enabling multiple rulesets that apply to the same branch in a repository?

A. Only organization-level rulesets are enforced over repository-level ones
B. All applicable rulesets will be evaluated, and their combined rules enforced
C. Only the most recently created ruleset will be enforced
D. Rulesets will override each other, leading to unpredictable behavior

Answer: B

Explanation:
If you enable multiple rulesets that target the same branch, GitHub will evaluate every matching ruleset and enforce the aggregate of their rules - so all constraints from all applicable rulesets apply.

NEW QUESTION 10
You want to ensure a secret is automatically available to only workflows in internal and private repositories in the organization. Where do you configure the required access policy?

A. Actions policies
B. Runner groups
C. Rulesets
D. Organization secret

Answer: D

Explanation:
You set the access policy on the Organization Secret itself - configuring its visibility so it??s scoped automatically to only internal and private repositories.

NEW QUESTION 10
Your enterprise has multiple organizations, and you want to ensure consistent security policies across all teams. Which feature should you use?

A. Outside collaborators for all repositories.
B. Organization-specific teams with custom policies.
C. Enterprise-level teams with inherited enterprise policies.
D. Assigning admin permissions to all team members.

Answer: C

Explanation:
By using enterprise#level teams with inherited enterprise policies, you can group members across all your organizations and enforce the same security settings globally - ensuring every team abides by the enterprise??s mandatory policies.

NEW QUESTION 14

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 17
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 19
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 24
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 29
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 32
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 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 34
How does GitHub support compliance requirements for enterprises?

A. GitHub provides configurable controls such as an audit log, SAML authentication, and enterprise rulesets.
B. GitHub disables all external collaboration features.
C. GitHub only allows those with repository owner (admin) permissions to write changes to repositories.
D. GitHub automatically encrypts user passwords in plaintext for quick access.

Answer: A

Explanation:
GitHub Enterprise gives you a suite of configurable controls - like a comprehensive audit log, enforced SAML single sign?on, and enterprise?level rulesets - that you can tailor and enforce to meet your organization's compliance mandates.

NEW QUESTION 38
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 42
When comparing Group SCIM to Team Sync for identity management in GitHub Enterprise, which statement is Correct?

A. Group SCIM requires less initial configuration than Team Sync.
B. Team Sync supports more identity providers than Group SCIM.
C. Team Syncprovides more automated user deprovisioningthan Group SCIM.
D. Group SCIM enablescentralized user and group management through the IdP.

Answer: D

Explanation:
Group?SCIM lets you manage both user accounts and group memberships centrally in your identity provider - automatically provisioning, updating, and deprovisioning users and groups in GitHub - whereas Team?Sync only mirrors IdP group membership into existing GitHub teams.

NEW QUESTION 47
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 49

.....

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