Microsoft

Exam Questions GH-100

GitHub Administration Exam

NEW QUESTION 1
Which of the following is a key benefit of setting default read permissions across organizations?

A. Suits environments where all users need write access.
B. Improves collaboration by allowing users to modify content directly.
C. Increases efficiency in content creation and updates.
D. Enhances security by minimizing unintended modifications.

Answer: D

Explanation:
Enforcing a default of Read for organization members ensures they can view content without the ability to push changes, reducing the risk of accidental or unauthorized modifications.

NEW QUESTION 2
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 3
Which GitHub feature is responsible for tracking dependencies and known vulnerabilities in those dependencies from an advisory database?

A. Repository Insights
B. Dependency Graph
C. Security Policy
D. CodeQL

Answer: B

Explanation:
The Dependency Graph continuously analyzes your repository??s manifest and lock files to build an inventory of direct and transitive dependencies and flags any that match entries in the GitHub Advisory Database, surfacing known vulnerabilities.

NEW QUESTION 4
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 5
You are planning GitHub account management for a healthcare organization with strict compliance requirements. Which THREE of the following statements accurately describe GitHub Enterprise Managed Users (EMU) accounts? (Choose three.)

A. EMU accounts can be used for both personal and enterprise repositories.
B. EMU accounts are managed through an identity provider such as Azure AD.
C. EMU accountsallow users to create and manage their own credentials.
D. EMU accounts restrict users to enterprise-related activities only
E. EMU accounts are created and managed by individual users.
F. EMU accounts are owned by the organization and cannot be unlinked.

Answer: BDF

Explanation:
Enterprise Managed User accounts are provisioned and authenticated exclusively through your identity provider (for example, Azure?AD), so the IdP handles their creation, attribute updates, and deprovisioning.
Managed user accounts cannot create public content or interact with repositories outside your enterprise; they're confined to private and internal repos within the enterprise.
EMU accounts are owned and controlled by the enterprise (via the IdP) and cannot be converted into or unlinked as personal accounts outside that enterprise.

NEW QUESTION 6
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 7
Which of the following accurately contrasts a GitHub App and a GitHub Action?

A. GitHub Apps can only be used inside .github/workflows
B. GitHub Actions are limited to reading repository content only
C. GitHub Apps run only on GitHub-provided virtual machines, while GitHub Actions run only on customer-hosted machines
D. GitHub Actions can only be used to respond to events within a single repository while GitHub Apps can respond to events from multiple repositories

Answer: D

Explanation:
GitHub Actions workflows are defined and triggered within a single repository??s context, whereas GitHub Apps are installed at the organization or user level and can subscribe to events across multiple repositories.

NEW QUESTION 8
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 9
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 10
You are using GitHub-hosted runners and need to securely deploy to an internal system. The security team requires that these runners use IP address ranges that would not be shared with other companies. Which of the following approaches would meet their requirements?

A. GitHub-hosted larger runners with Azure private networking
B. GitHub-hosted standard runners, using the IP addresses provided in "actions" from https://api.githu
C. com/meta
D. GitHub-hosted standard runners, using the IP addresses provided in "api" from https://api.github.com/meta
E. GitHub-hosted larger runners with static IP addresses

Answer: D

Explanation:
GitHub??s larger runners let you reserve dedicated static IP addresses for your workflows - so you can allow#list those IPs in your firewall and be sure they aren??t shared with any other tenant.

NEW QUESTION 10
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 11
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 13
Which THREE of the following accurately describe how the SCIM protocol enhances user management in GitHub Enterprise Cloud? (Choose three.)

A. SCIM synchronizes changes to user attributes from the identity provider to GitHub.
B. SCIM deactivates GitHub accounts when users are deleted from the identity provider.
C. SCIM automatically deletes organization repositories when administrators are removed.
D. SCIM automates user provisioning when new users are added to the identity provider.
E. SCIM generates authentication tokens for accessing GitHub's REST API.
F. SCIM configures repository permissions based on user roles within the organization.

Answer: AB

Explanation:
SCIM automatically updates a user's account on GitHub whenever their profile attributes change in the identity provider.
When a user is removed or deactivated in the IdP, SCIM deactivates (soft?deprovisions) their GitHub account and disables access.
SCIM provisions new GitHub Enterprise Cloud accounts automatically when users are added in the identity provider.

NEW QUESTION 16
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 18
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 20
Why would someone choose to configure a security policy?

A. To communicate corporate security and compliance policies for end users on a private repository.
B. To provide information on an open source repository for open source collaborators and researchers that may need to report and disclose sensitive security findings to maintainers securely.

C. To prevent anyone from pushing to the repository without approval.
D. To define which open source packages are permitted for use as part of that repository.

Answer: B

Explanation:
A security policy (the SECURITY.md file) lets maintainers of an open source repository provide clear, private instructions for collaborators and external researchers on how to report and disclose security vulnerabilities responsibly.

NEW QUESTION 23
What is a key characteristic of GitHub Enterprise Server (GHES) compared to GitHub Enterprise Cloud (GHEC)?

A. GHES is hosted by GitHub and offers automatic scaling, while GHEC requires self-hosting.
B. GHEC offers data residency options in regions that GHES does not support.
C. GHES allows enterprises to have complete control over their hosting environment, including data storage and network security policies.
D. GHES users cannot integrate with external identity providers for authentication.

Answer: C

Explanation:
GitHub Enterprise Server is a self?hosted product you install and manage on your own infrastructure - giving you full control over data storage, network security policies, and the underlying environment.

NEW QUESTION 25
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 29
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 31
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 33
Which of the following is true about outside collaborators in a GitHub organization?

A. They are granted explicit access to specific repositories.
B. They inherit organization-wide policies, such as SSO requirements.
C. They have access to all private repositories by default.
D. They appear in the organization's internal member list.

Answer: A

Explanation:

Outside collaborators aren't organization members; instead, they're granted explicit access - at read, write, or admin level - to only the repositories you choose.

NEW QUESTION 35
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 39
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 41
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 44
.....

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