

Exam Questions GH-100

GitHub Administration Exam

<https://www.2passeasy.com/dumps/GH-100/>



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

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 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

Why would a GitHub App be favored over a machine account for automation tasks?

- A. Machine accounts are required for webhook delivery.
- B. GitHub Apps provide a higher rate limit ceiling than using a personal access token on a machine account, when they use an install token and are owned by a GitHub Enterprise Cloud licensed enterprise.
- C. GitHub Apps are limited to a single repository.
- D. Machine accounts are easier to audit than GitHub Apps.

Answer: B

Explanation:

GitHub Apps authenticate with short-lived installation tokens scoped to fine-grained permissions and, when owned by a GitHub Enterprise Cloud organization, enjoy a higher rate limit (15,000 requests/hour) compared to a machine account's personal access token.

NEW QUESTION 5

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 6

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 7

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 accounts allow 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 8

What do you need to successfully generate a support bundle on a GitHub Enterprise Server?

- A. Approval from GitHub Support
- B. A custom GitHub Action in the root repo
- C. Administrator SSH access to the appliance
- D. A GitHub App with read:org permissions

Answer: C

Explanation:

You must have administrator-level SSH access to the GitHub Enterprise Server appliance so you can run the ghe-support-bundle command over SSH and capture the bundle locally.

NEW QUESTION 9

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 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 10

You need to create a support bundle for your GitHub Enterprise Server instance with the hostname ghe. avocado.corp. What command should you use to create a support bundle?

- A. `ssh -p 122 admin@ghe.avocado.corp -- 'ghe-support-bundle -o' > support-bundle.tgz`
- B. `ssh -p 122 admin@ghe.avocado.corp -- 'ghe-diagnostics' > support-bundle.tgz`
- C. `curl -u admin https://ghe.avocado.corp/diagnostics/support-bundle.tgz -o`
- D. `ssh -p 122 admin@ghe.avocado.corp -- 'ghe-config generate-support-bundle' > support-bundle.tgz`

Answer: A

Explanation:

Run the `ghe-support-bundle` command over SSH on your appliance and redirect its output to a file. For example:

```
ssh -p 122 admin@ghe.avocado.corp -- 'ghe-support-bundle -o' > support-bundle.tgz
```

This invokes the built-in `support#bundle` utility on your GitHub Enterprise Server instance and captures the resulting archive locally.

NEW QUESTION 14

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 16

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.github.com/actions>
- 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 allowlist those IPs in your firewall and be sure they aren't shared with any other tenant.

NEW QUESTION 19

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 21

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 25

Your organization wants to reduce costs. Which of the following actions should you take?

- A. Grant all users admin permissions
- B. Remove all outside collaborators
- C. Regularly audit for inactive users
- D. Disable SAML SSO for members

Answer: C

Explanation:

Regularly auditing for inactive (dormant) users lets you suspend or remove accounts that aren't consuming seats - freeing up licenses and directly lowering your per-user subscription costs.

NEW QUESTION 29

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 31

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:Incorrect
- 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 34

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 36

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 41

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 43

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 44

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 47

You need to contact GitHub Premium Support. What are valid reasons for submitting a support ticket? (Each answer presents a complete solution. Choose two.)

- A. A.license renewal
- B. B.hardware setup issues or errors
- C. C.business impact from security issues within your organization
- D. D.outages on GitHub.com affecting core Git functionality

Answer: CD

NEW QUESTION 48

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 51

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 53

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual GH-100 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the GH-100 Product From:

<https://www.2passeasy.com/dumps/GH-100/>

Money Back Guarantee

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