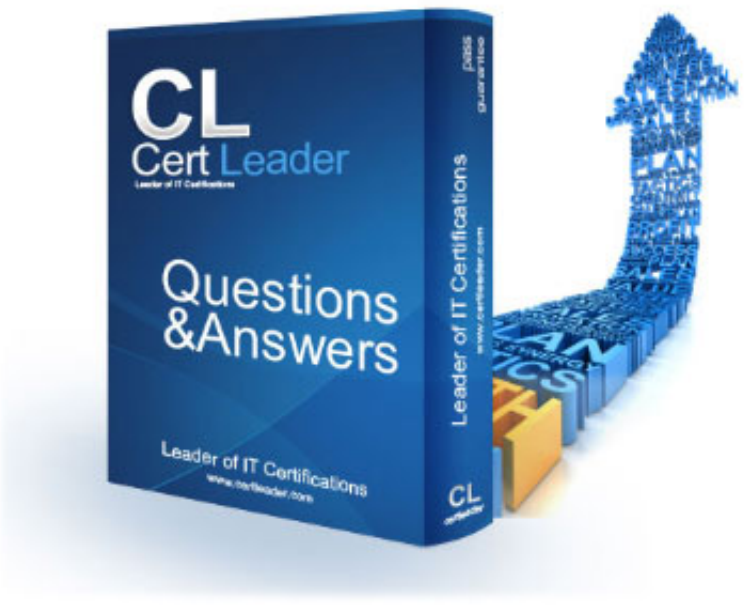
GH-100 Dumps

GitHub Administration Exam

https://www.certleader.com/GH-100-dumps.html



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
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
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 4
An organization wants to share a single API key required for their Actions workflows. They need to restrict its use to only a subset of repositories. Where should they configure the secrets to minimize maintenance?

A. Repository secrets
B. Environment secrets
C. Organization secrets
D. Development environment secrets

Answer: C

Explanation:
By defining the API key as an organization secret, you centralize management and can grant access only to the subset of repositories you choose - eliminating per?repo duplication while enforcing the desired scope.

NEW QUESTION 5
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 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 is a benefit of creating a new GitHub organization?

A. Automatic inheritance of policies from other organizations.
B. Reduced administrative overhead.
C. Clear separation of reggs, projects, teams, billing, and organization-specific policies.
D. Simplified collaboration across all organizations.

Answer: C

Explanation:
Creating a new organization gives you a dedicated container for your shared work, letting you isolate repositories, projects, teams, billing settings, and policy configurations on an organization#by#organization basis.

NEW QUESTION 8
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 9
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
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 10
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 11
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 15
How does GitHub handle secrets found via secret scanning in a public repository?

A. It alerts the service provider (e.g., AWS, Stripe).
B. It immediately blocks the commit to protect the secret.
C. It deletes the secret from the repository automatically.
D. It notifies the admin via webhook.

Answer: A

Explanation:
When secret scanning detects a supported credential in a public repository, GitHub notifies the issuing service provider so they can revoke or rotate the exposed secret.

NEW QUESTION 17
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 18
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 19
.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your GH-100 Exam with Our Prep Materials Via below:

https://www.certleader.com/GH-100-dumps.html