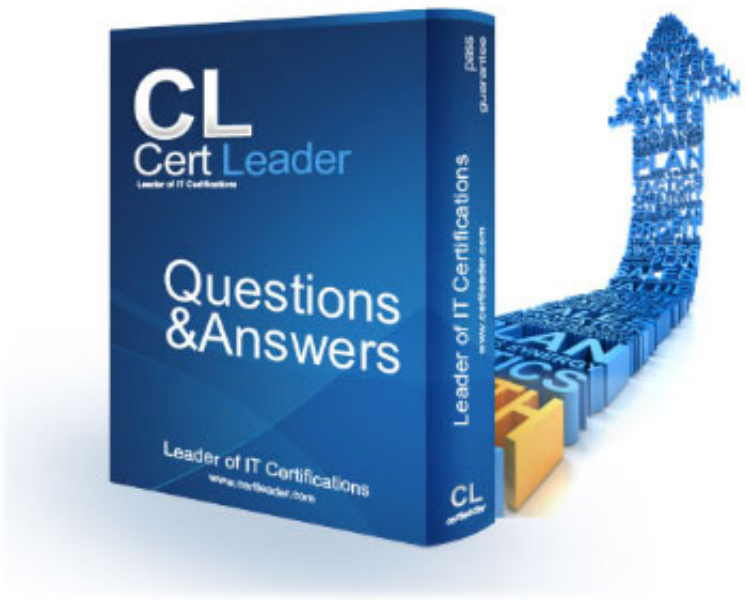
GH-100 Dumps

GitHub Administration Exam

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



NEW QUESTION 1
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 2
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 3
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 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
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 6
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 7
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 adming@ghe.avocado.corp -- 'ghe-support-bundle -o' > support-bundle.tgz
B. ssh -p 122 adming@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 adming@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 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
In a GitHub repository using Dependabot, which of the following best describes the purpose of the .github/dependabot.yml file?

A. It configures scheduling, package ecosystems, and target directories for update checks.
B. It lists commit SHAs to exclude from automatic pull requests.
C. It enables GitHub to scan for secrets in dependency files.
D. It encrypts dependency versions before storing them in the repo.

Answer: A

Explanation:
The .github/dependabot.yml file defines Dependabot's package-ecosystem, the directories to inspect, and the update schedule (daily/weekly/monthly), controlling when and where Dependabot checks for new versions.

NEW QUESTION 10
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 10
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 11
What makes GitHub Apps a more secure choice for automation over OAuth Apps?

A. GitHub Apps always require two-factor authentication.
B. GitHub Apps can only be installed by organization owners.
C. GitHub Apps are limited to read-only access and cannot write to repositories.
D. GitHub Apps authenticate as an appwithfine-grained permissions, not as a user.

Answer: D

Explanation:
GitHub Apps authenticate as themselves with fine?grained, installation?scoped permissions and short?lived tokens - rather than inheriting a user's broad OAuth scopes - minimizing blast radius and aligning with least?privilege principles.

NEW QUESTION 16
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 20
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
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 renewalB.hardware setup issues or errorsC.business impact from security issues within your organizationD.outages on GitHub.com affecting core Git functionality

Answer: CD

NEW QUESTION 27
.....

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