Microsoft

Exam Questions GH-100

GitHub Administration Exam

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
How does Dependabot determine which security update PRs to open?

A. It waits for manual triage of all CVEs.
B. It uses the dependency graph and Dependabot alerts to open PRs for patched versions.
C. It reads the GitHub Issues and automatically suggests fixes.
D. It compares your codebase to the GitHub Trending list.

Answer: B

Explanation:
Dependabot relies on your repository??s enabled Dependency Graph and Dependabot Alerts to identify vulnerable dependencies; it then automatically opens pull requests to update to the patched versions that resolve those alerts.

NEW QUESTION 3
Which of the following are valid ways to pass data to a reusable workflow in a separate repository?

A. Use environment variables to pass data directly to the reusable workflow.
B. Define inputs in the reusable workflow and pass values from the calling workflow.
C. Define the secrets in the caller repository and call the reusable workflow using the ??secrets?? keyword.
D. Define the secrets in the reusable workflow's repository and reference the secret using the ??secrets?? context.

Answer: BC

Explanation:
You declare named inputs in the reusable workflow??s on.workflow_call block and then pass values from the caller using the with keyword, allowing the called workflow to consume those parameters.
You define required secrets in the caller repository and supply them to the reusable workflow via the secrets keyword in the workflow-call step, ensuring sensitive values are securely passed.

NEW QUESTION 4
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 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
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 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 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 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
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
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 15
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 19
You are managing a repository in your organization's GitHub account. A team member asks you to confirm who has access to the repository and their permission levels. Which tool should you use to review and manage repository access?

A. GitHub Pages Settings.
B. GitHub Actions Logs.
C. Repository Settings > Manage Access.
D. Branch Protection Rules.

Answer: C

Explanation:
Use the?Repository?Settings???Manage?Access page to view all users and teams with access and their assigned permission levels.

NEW QUESTION 23
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 26
A team member is unable to push to a repository due to a 403-error related to branch protection. What should the GitHub Enterprise administrator do first?

A. Remove the user from the team and re-add them
B. Check the user's permissions and rulesets applied to the branch
C. Raise a GitHub Support request for permissions issues
D. Revert the branch to an earlier state

Answer: B

Explanation:
The administrator should first review the user's repository role and the branch protection rules applied to that branch. A 403 error on push almost always indicates that the user either lacks the necessary write permissions or is not listed among the actors authorized by the branch protection settings.

NEW QUESTION 28
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 31
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 35
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 36
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 41
What additional capability does secret scanning offer for private repositories on GitHub Enterprise Cloud?

A. Allows custom pattern definitions for internal secret formats.
B. Disables any code that contains a secret.
C. Rewrites history to remove secrets.
D. Revokes GitHub access tokens automatically.

Answer: A

Explanation:
Secret scanning in private repositories on GitHub Enterprise Cloud lets you define and use custom regular?expression patterns - so you can detect internal or proprietary secret formats beyond the default partner?provided types.

NEW QUESTION 45
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 48
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 49
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
.....

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