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
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 3
Our organization is updating its enterprise policies. Which of the following steps should you take to ensure alignment with security requirements?

A. Maintain clear documentation of existing policies and policy changes.
B. Implement the new enterprise policies across the organization first and then consult with the security team to identify- any necessary adjustments or retrofits
C. Implement changes without consulting stakeholders.
D. Regularly assess and adjust policies based on evolving risks.

Answer: AB

NEW QUESTION 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 14
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 17
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 22
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 25
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 29
.....

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