Microsoft

Exam Questions GH-100

GitHub Administration Exam

NEW QUESTION 1
Which of the following is the responsibility of an Organization Owner in GitHub? (Choose three.)

A. View and manage organization billing information.
B. Create repositories without approval from other members.
C. Manage organization settings, such as configuration and default permissions.
D. Access repositories only if explicitly granted by a team maintainer.

Answer: ABC

Explanation:
Organization owners can view and edit billing information for the organization.
Organization owners may create new repositories in the organization without needing approval from other members.
Organization owners have full administrative control over organization settings, including configuring default repository permissions.

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
How does metered billing work in GitHub Enterprise Cloud with Enterprise Managed Users (EMU)?

A. Billing is based on number of total users in the enterprise
B. Billing is based on owners and members of GitHub organizations
C. Billing is based on total users in the enterprise that are not dormant
D. Billing is based on the number of users created in Azure AD

Answer: A

Explanation:
Billing for GitHub Enterprise Cloud under metered (usage#based) billing is calculated by the total number of Enterprise Managed Users (and other license#consuming accounts) in your enterprise - each EMU consumes a seat and contributes to the monthly bill.

NEW QUESTION 4
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 5
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 6
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 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
When a token is used to perform actions across different GitHub resources, how is this reflected in audit logs?

A. Each API action made with the token generates a separate audit log entry
B. Only the first repository accessed is recorded
C. GitHub creates a ZIP archive of all token activity
D. The audit log stores only the token name and not its actions

Answer: A

Explanation:
Each API call authenticated with a token generates its own audit-log event, so you'll see a distinct entry for every action performed across different resources, each annotated with the token's hashed ID, actor, and source IP.

NEW QUESTION 9
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 10
What is the potential consequence of enabling multiple rulesets that apply to the same branch in a repository?

A. Only organization-level rulesets are enforced over repository-level ones
B. All applicable rulesets will be evaluated, and their combined rules enforced
C. Only the most recently created ruleset will be enforced
D. Rulesets will override each other, leading to unpredictable behavior

Answer: B

Explanation:
If you enable multiple rulesets that target the same branch, GitHub will evaluate every matching ruleset and enforce the aggregate of their rules - so all constraints from all applicable rulesets apply.

NEW QUESTION 10
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 12
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 14
Which of the following correctly describes the difference between controlling actions at the enterprise level versus the organization level in GitHub?

A. Enterprise policies and organization policies are independent, with organization policies taking precedence for repositories within the organization.
B. Enterprise policies configure mandatory settings for organizations.
C. Enterprise policies apply only to public repositories, while organization policies apply to public, internal, and private repositories.
D. Enterprise policies can block specific actions, while organization policies can only enable or disable actions entirely.

Answer: B

Explanation:
Enterprise policies let you define and enforce mandatory settings across all member organizations - organization#level policies then operate within the options that the enterprise policy exposes.

NEW QUESTION 17
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 19
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 20
You have subscribed to GitHub Premium Support, and you need to submit a support ticket. GitHub Premium Support can help you with:

A. writing scripts.
B. installing GitHub Enterprise Server.
C. setting up hardware.
D. integrating with third-party applications.

Answer: B

Explanation:
GitHub Premium Support includes assistance with installing and using GitHub Enterprise Server, ensuring your deployment is configured correctly and any installation issues are resolved.

NEW QUESTION 22
You discover that a secret (e.g., a token or password) was accidentally committed to a GitHub repository. What is the first step you should take to mitigate the risk?

A. Contact GitHub Support to remove the secret from all forks and clones of the repository.
B. Revoke and/or rotate the secret to render it unusable, then assess whether history rewriting is necessary.
C. Rewrite the repository history using git filter-repo or BFG Repo-Cleaner to remove the secret from all commits.
D. Delete the repository and create a new one to ensure the secret is no longer accessible.

Answer: B

Explanation:
The immediate priority is to revoke or rotate the exposed credential so it can no longer be used; once it??s invalidated, you can safely proceed with history?rewriting or other cleanup steps.

NEW QUESTION 25
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 28
Which THREE of the following accurately describe how the SCIM protocol enhances user management in GitHub Enterprise Cloud? (Choose three.)

A. SCIM synchronizes changes to user attributes from the identity provider to GitHub.
B. SCIM deactivates GitHub accounts when users are deleted from the identity provider.
C. SCIM automatically deletes organization repositories when administrators are removed.
D. SCIM automates user provisioning when new users are added to the identity provider.
E. SCIM generates authentication tokens for accessing GitHub's REST API.
F. SCIM configures repository permissions based on user roles within the organization.

Answer: AB

Explanation:
SCIM automatically updates a user's account on GitHub whenever their profile attributes change in the identity provider.
When a user is removed or deactivated in the IdP, SCIM deactivates (soft?deprovisions) their GitHub account and disables access.
SCIM provisions new GitHub Enterprise Cloud accounts automatically when users are added in the identity provider.

NEW QUESTION 32
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 33
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 37
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 41
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:Incorrec
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 46
What is the new capability of GitHub's billing dashboard?

A. Automatically removes unused users from billing
B. Enables tracking of GitHub Copilot usage byuser
C. Allows self-service plan upgrades
D. Offers real-time Slack alerts for billing

Answer: B

Explanation:
The revamped Billing?&?Licensing dashboard now includes a dedicated?"Copilot" tab that shows per?user seat assignments, usage counts, and estimated costs for your organization's GitHub Copilot licenses, enabling you to track Copilot consumption by individual users.

NEW QUESTION 48
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 53
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 56
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 60
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 63
When comparing Group SCIM to Team Sync for identity management in GitHub Enterprise, which statement is Correct?

A. Group SCIM requires less initial configuration than Team Sync.
B. Team Sync supports more identity providers than Group SCIM.
C. Team Syncprovides more automated user deprovisioningthan Group SCIM.
D. Group SCIM enablescentralized user and group management through the IdP.

Answer: D

Explanation:
Group?SCIM lets you manage both user accounts and group memberships centrally in your identity provider - automatically provisioning, updating, and deprovisioning users and groups in GitHub - whereas Team?Sync only mirrors IdP group membership into existing GitHub teams.

NEW QUESTION 65
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 66
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 70
.....

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