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 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 3
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 4
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 5
Why would a GitHub App be favored over a machine account for automation tasks?

A. Machine accounts are required for webhook delivery.
B. GitHub Apps provide a higher rate limit ceiling than using a personal access token on a machine account, when they use an install token and are owned by a GitHub Enterprise Cloud licensed enterprise.
C. GitHub Apps are limited to a single repository.
D. Machine accounts are easier to audit than GitHub Apps.

Answer: B

Explanation:
GitHub Apps authenticate with short?lived installation tokens scoped to fine?grained permissions and, when owned by a GitHub Enterprise Cloud organization, enjoy a higher rate limit (15,000 requests/hour) compared to a machine account's personal access token.

NEW QUESTION 6
When comparing fine-grained Personal Access Tokens (PATs) with classic PATs, which of the following statements is accurate?

A. Fine-grained PATs automatically renew while classic PATs require manual renewal.
B. Fine-grained PATs permissions can be scoped to specific repositories.
C. Classic PATs offer more permission controls than fine-grained PATs.
D. Classic PATs can be restricted to specific organizations, but fine-grained PATs cannot.

Answer: B

Explanation:
Fine?grained personal access tokens let you scope permissions down to individual repositories, whereas classic PATs grant access across every repo the user can reach.

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 14
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 15
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 20
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 24
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 26
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 27
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 31
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 33
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 34
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 38
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 40

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 45
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
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 49
How does GitHub support compliance requirements for enterprises?

A. GitHub provides configurable controls such as an audit log, SAML authentication, and enterprise rulesets.
B. GitHub disables all external collaboration features.
C. GitHub only allows those with repository owner (admin) permissions to write changes to repositories.
D. GitHub automatically encrypts user passwords in plaintext for quick access.

Answer: A

Explanation:
GitHub Enterprise gives you a suite of configurable controls - like a comprehensive audit log, enforced SAML single sign?on, and enterprise?level rulesets - that you can tailor and enforce to meet your organization's compliance mandates.

NEW QUESTION 50
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 54
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 56
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 60
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 64
.....

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