[2025-August-NewBraindump2go GH-100 Dumps PDF Free[Q1-Q28

2025/August Latest Braindump2go GH-100 Exam Dumps with PDF and VCE Free Updated Today! Following are some new Braindum2go GH-100 Exam Questions!Question: 1You 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.Question: 2You need to contact GitHub Premium Support. What are valid reasons for submitting a support ticket? (Each answer presents a complete solution. Choose two.)A. license renewalB. hardware setup issues or errorsC. business impact from security issues within your organizationD. outages on GitHub.com affecting core Git functionalityAnswer: C, D Explanation: Business-impact security issues (for example, a critical vulnerability affecting your organization) are classified as High-priority tickets and are covered under your Premium Support SLA.Outages on GitHub.com that disrupt core Git or web application functionality trigger Urgent-priority responses under Premium Support's SLA.Question: 3Which of the following is a key benefit of using GitHub Marketplace Apps in an enterprise? A. They guarantee no downtime during enterprise GitHub maintenance windowsB. They often include integrations with external services, reducing the need for custom codeC. Apps eliminate the need for GitHub Actions entirelyD. All apps come pre-approved by GitHub's internal security teamAnswer: 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.Question: 4You 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.tgzB. ssh -p 122 adming@ghe.avocado.corp ? 'ghe-diagnostics' > support-bundle.tgzC. curl -u admin https://ghe.avocado.corp/diagnostics/support-bundle.tgz -oD. ssh -p 122 adming@ghe.avocado.corp -- 'ghe-config generate-support-bundle' > support- bundle.tgzAnswer: 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.tgzThis invokes the built-in support-bundle utility on your GitHub Enterprise Server instance and captures the resulting archive locally.Question: 5What do you need to successfully generate a support bundle on a GitHub Enterprise Server?A. Approval from GitHub SupportB. A custom GitHub Action in the root repoC. Administrator SSH access to the applianceD. A GitHub App with read:org permissionsAnswer: 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. Question: 6A 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.Question: 7Which 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: A, B 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.Question: 8When comparing a partner identity provider integration with a non-partner identity management solution for GitHub Enterprise Managed Users, which statement is Correct?A. The non-partner identity provider integrations can utilize OIDC for authentication.B. The non-partner identity provider integrations require manual configuration of SAML 2.0 details.C. The partner identity provider integrations support fewer GitHub-supported authentication methods.D. The partner identity provider integrations rely on the partner to support the application on the partner IdP.Answer: B Explanation:Non-partner identity provider integrations require you to enter SAML?2.0 configuration details by hand - such as the Sign-on URL, Issuer, and X.509 certificate -

whereas partner IdPs supply a pre- configured application integration.Question: 9When 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 Sync provides more automated user deprovisioning than Group SCIM.D. Group SCIM enables centralized 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.Question: 10Why is a GitHub App preferred over a PAT for machine authentication?A. GitHub Apps are required to pass SAML assertionsB. GitHub Apps have time-limited installation tokens with scoped accessC. PATs cannot be used in GitHub ActionsD. PATs support fewer GitHub APIs than AppsAnswer: B Explanation:GitHub Apps issue short-lived installation tokens that you scope to only the permissions and repositories your automation needs, reducing blast radius and automatically rotating credentials.Question: 11You 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 accounts allow users to create and manage their own credentials.D. EMU accounts restrict users to enterprise-related activities onlyE. EMU accounts are created and managed by individual users.F. EMU accounts are owned by the organization and cannot be unlinked.Answer: B, D, F 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.Question: 12A GitHub Enterprise administrator is planning to implement SAML SSO across their company. Which of the following correctly distinguishes enterprise-wide SAML SSO from organization-level SAML SSO?A. Enterprise-wide SAML SSO requires less initial administrative overhead than organization-level implementation.B. Enterprise-wide SAML SSO allows different organizations to use different authentication methods.C. Enterprise-wide SAML SSO immediately removes users who fail to authenticate via the IdP.D. Enterprise-wide SAML SSO ensures users authenticate through the same IdP across all organizations.Answer: D Explanation:Enterprise-wide SAML SSO enforces a single IdP across all member organizations?its configuration overrides any per-organization SAML settings, so everyone must authenticate through the same provider.Question: 13What distinguishes Enterprise Managed Users (EMUs) from standard GitHub accounts? A. EMUs are fully controlled by an IdP and cannot log in with personal credentialsB. EMUs can only be created using email invitesC. EMUs are managed in GitHub and use GitHub authenticationD. EMUs are only available for GitHub Enterprise ServerAnswer: 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.Question: 14Your organization is implementing team synchronization. Which of the following should you prioritize during the setup process?A. Disabling the audit log streamB. Setting an infrequent sync schedule to reduce performance impactC. Allowing manual updates to team membershipsD. Clearly define how identity provider groups will align with GitHub teams and rolesAnswer: 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.Question: 15What 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 app with fine-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.Question: 16Why 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.Question: 17When 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.Question: 18What is the new capability of GitHub's billing dashboard?A. Automatically removes unused users from billingB. Enables tracking of GitHub Copilot usage by userC. Allows self-service plan upgradesD. Offers real-time Slack alerts for billingAnswer: 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. Question: 19What 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.Question: 20Your organization wants to reduce costs. Which of the following actions should you take?A. Grant all users admin permissionsB. Remove all outside collaboratorsC. Regularly audit for inactive usersD. Disable SAML SSO for membersAnswer: 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.Question: 21How does metered billing work in GitHub Enterprise Cloud with Enterprise Managed Users (EMU)?A. Billing is based on number of total users in the enterpriseB. Billing is based on owners and members of GitHub organizationsC. Billing is based on total users in the enterprise that are not dormantD. Billing is based on the number of users created in Azure ADAnswer: 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.Question: 22A 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 themB. Check the user's permissions and rulesets applied to the branchC. Raise a GitHub Support request for permissions issuesD. Revert the branch to an earlier stateAnswer: 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.Question: 23Which 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.Question: 24Which 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: CExplanation: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.Question: 25Which 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: A, B, C 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.Question: 26Which 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.Question: 27Which of the following is a key benefit of setting default read permissions across organizations?A. Suits environments where all users need write access.B. Improves collaboration by allowing users to modify content directly.C. Increases efficiency in content creation and updates.D. Enhances security by minimizing unintended modifications. Answer: D Explanation:Enforcing a default of Read for organization members ensures they can view content without the ability to push changes, reducing the risk of accidental or unauthorized modifications.Question: 28Which 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: B, C 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.Resources From:1.2025 Latest Braindump2go GH-100 Exam Dumps (PDF & VCE) Free Share: https://www.braindump2go.com/gh-100.html2.2025 Latest Braindump2go GH-100 PDF and GH-100 VCE Dumps Free Share: https://drive.google.com/drive/folders/1-z_1l-dxGxUjj-HMR-fiQ4lPNA67NpY5?usp=sharing**3.2025 Free Braindump2go GH-100 Exam Questions Download:**https://www.braindump2go.com/free-online-pdf/GH-100-VCE-Dumps(1-28)pdf.pdf**Free Resources from Braindump2go,We Devoted to Helping You 100% Pass All Exams!**