Question #1 *Topic 1*

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.

Suggested Answer: *B*

Community vote distribution

A (100%)

None

Question #2 *Topic 1*

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. license renewal

B. hardware setup issues or errors

C. business impact from security issues within your organization

D. outages on GitHub.com affecting core Git functionality

Suggested Answer: *CD*

None

Question #3 *Topic 1*

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

Suggested Answer: *B*

None

Question #4 *Topic 1*

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

Suggested Answer: *A*

None

Question #5 *Topic 1*

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

Suggested Answer: *C*

None

Question #1 *Topic 2*

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.

Suggested Answer: *B*

None

Question #2 *Topic 2*

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.

Suggested Answer: *ABD*

None

Question #3 *Topic 2*

When 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.

Suggested Answer: *B*

None

Question #4 *Topic 2*

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 Sync provides more automated user deprovisioning than Group SCIM.

D. Group SCIM enables centralized user and group management through the IdP.

Suggested Answer: *D*

None

Question #5 *Topic 2*

Why is a GitHub App preferred over a PAT for machine authentication?

A. GitHub Apps are required to pass SAML assertions

B. GitHub Apps have time-limited installation tokens with scoped access

C. PATs cannot be used in GitHub Actions

D. PATs support fewer GitHub APIs than Apps

Suggested Answer: *B*

None

Question #6 *Topic 2*

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 accounts allow 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.

Suggested Answer: *BDF*

None

Question #7 *Topic 2*

A 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.

Suggested Answer: *D*

None

Question #8 *Topic 2*

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

Suggested Answer: *A*

None

Question #9 *Topic 2*

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

Suggested Answer: *D*

None

Question #10 *Topic 2*

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 app with fine-grained permissions, not as a user.

Suggested Answer: *D*

None

Question #11 *Topic 2*

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.

Suggested Answer: *B*

None

Question #12 *Topic 2*

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.

Suggested Answer: *B*

None

Question #1 *Topic 3*

What is the new capability of GitHub's billing dashboard?

A. Automatically removes unused users from billing

B. Enables tracking of GitHub Copilot usage by user

C. Allows self-service plan upgrades

D. Offers real-time Slack alerts for billing overages

Suggested Answer: *B*

None

Question #2 *Topic 3*

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.

Suggested Answer: *C*

None

Question #3 *Topic 3*

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

Suggested Answer: *C*

None

Question #4 *Topic 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

Suggested Answer: *A*

None

Question #1 *Topic 4*

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

Suggested Answer: *B*

None

Question #2 *Topic 4*

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.

Suggested Answer: *A*

None

Question #3 *Topic 4*

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 repos, projects, teams, billing, and organization-specific policies.

D. Simplified collaboration across all organizations.

Suggested Answer: *C*

None

Question #4 *Topic 4*

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.

Suggested Answer: *ABC*

None

Question #5 *Topic 4*

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.

Suggested Answer: *B*

None

Question #6 *Topic 4*

Which 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.

Suggested Answer: *D*

None

Question #7 *Topic 4*

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.

Suggested Answer: *BC*

None

Question #8 *Topic 4*

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.

Suggested Answer: *C*

None

Question #9 *Topic 4*

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.

Suggested Answer: *BCD*

None

Question #1 *Topic 5*

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

Suggested Answer: *D*

None

Question #2 *Topic 5*

What will happen if Dependabot discovers a vulnerable transitive dependency in a repository?

A. It creates a pull request to update the direct dependency to a version that resolves the vulnerability.

B. It opens a pull request to update the affected package directly, regardless of version compatibility.

C. It automatically removes the package from the repository.

D. It sends an email to the repository owner but does not alter code.

Suggested Answer: *A*

None