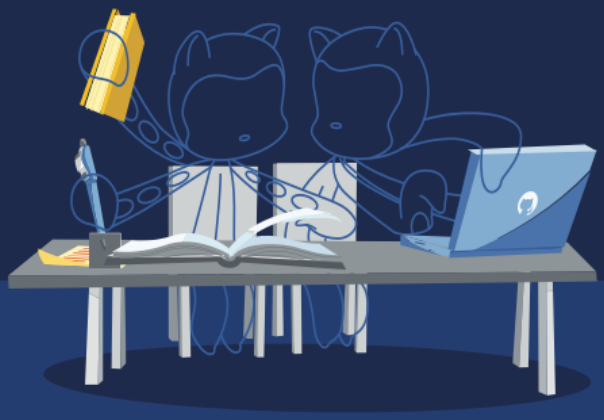
GitHub

Guia de estudo
GitHub Administration



Prepare-se para o exame da certificação do GitHub Administration com nosso abrangente guia de estudo. Nós consolidamos as atividades de aprendizado e os recursos essenciais para melhor preparar você para o exame do GitHub Administration e impulsionar suas chances de sucesso.

Perfil do público

Este exame foi concebido para administradores de sistemas, desenvolvedores de software, administradores de aplicações e profissionais de TI com uma experiência de nível intermediário no GitHub Enterprise Administration.

Domínios de objetivos

Um domínio de objetivo para um exame de certificação, geralmente denominado como “domínio” ou “domínio do exame”, é uma estrutura ou um resumo estruturado que define tópicos, habilidades e conhecimentos específicos que o exame da certificação vai abranger. Ele fornece um roteiro claro para que os candidatos saibam o que poderão encontrar no exame e o que precisam estudar para se preparar.

Os domínios fornecidos neste guia de estudo têm como objetivo fornecer insights sobre as categorias dos tópicos abordados no exame do GitHub Administration, junto com o objetivo de aprendizado em cada domínio.

Discriminação dos domínios	Porcentagem do exame
Domínio 1: Suporte do GitHub Enterprise para usuários e os principais stakeholders	15%
Domínio 2: Gerenciar identidades de usuários e autenticação do GitHub	20%
Domínio 3: Descrever como o GitHub é implantado, distribuído e licenciado	5%
Domínio 4: Gerenciar o acesso e as permissões com base na inscrição	20%
Domínio 5: Habilitar o desenvolvimento de software seguro e garantir a conformidade	15%
Domínio 6: Gerenciar o GitHub Actions	20%
Domínio 7: Gerenciar o GitHub Packages	5%

Recomendações e as melhores práticas para o sucesso

Para aumentar as chances de obter sucesso no exame do GitHub Administration, é essencial começar com uma base sólida de exposição, proficiência e experiência básica do GitHub Administration. Os caminhos de aprendizado recomendados para este exame proporcionam um estudo aprofundado do conteúdo de aprendizado, seguido de exercícios práticos e perguntas preparatórias para a avaliação que foram criados para possibilitar uma preparação e um conhecimento aperfeiçoado para o exame da certificação.

Recursos de conteúdo

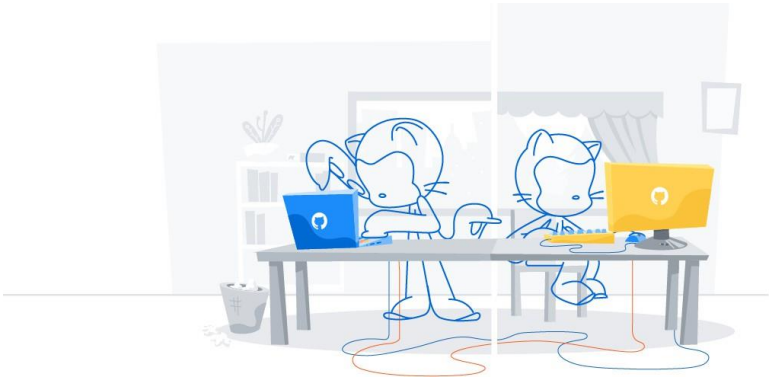
Os recursos a seguir foram criados em colaboração com o GitHub como um conteúdo recomendado que abrange os objetivos de aprendizado em cada domínio para o exame do GitHub Administration. Tanto o Microsoft Learn como o LinkedIn Learning fornecem um caminho de aprendizado completo para o exame, mas oferecem uma experiência de aprendizado diferente.

Microsoft Learn

O caminho de aprendizado do GitHub Administration no MS Learn fornece uma coleção robusta de módulos de aprendizado elaborados para preparar você para o exame do GitHub Administration. Como administrador do GitHub, você precisa manter um ambiente íntegro, robusto e seguro do GitHub que dê suporte às necessidades dos requisitos da organização e dos fluxos de trabalho do desenvolvedor. Os módulos a seguir fornecerão uma visão geral das várias opções e personalizações disponíveis para você como administrador na plataforma do GitHub. Obtenha mais insights no gerenciamento de autenticação e identidades de usuários, nas opções de implantação, acesso e permissões, no desenvolvimento de software seguro e na garantia da conformidade.

LinkedIn Learning

Dedique-se ao caminho de aprendizado Preparar-se para a certificação do GitHub Administration no LinkedIn Learning, que apresenta uma série de cursos de vídeos elaborados especificamente para o exame do GitHub Administration. Como administrador do GitHub, seu papel é crucial em manter um ambiente do GitHub robusto, seguro e altamente eficiente que se alinhe perfeitamente com as necessidades exclusivas da sua organização e de seus fluxos de trabalho do desenvolvedor. Explore nossos módulos consolidados, orientados por especialistas do setor, para se aprofundar na infinidade de opções e personalizações disponíveis para você como administrador do GitHub. Obtenha insights valiosos sobre o gerenciamento de identidades de usuários, autenticação, estratégias de implantação, controle de acesso e medidas de segurança cruciais para o desenvolvimento e a conformidade de software.



Domínio 1: Suporte do GitHub Enterprise para usuários e os principais stakeholders

Suporte do GitHub Enterprise para usuários e os principais stakeholders
Diferenciar os problemas que podem ser resolvidos por um administrador daqueles que precisam do suporte do GitHub
Descrever como gerar pacotes e diagnósticos de suporte
Descrever como os produtos e serviços do GitHub são usados na empresa para identificar os recursos subutilizados, as integrações em uso, as equipes mais ativas e os repositórios.
Padrões de recomendações para fluxos de trabalho do desenvolvedor, incluindo colaboração de código (fork e pull versus branching), branch, regras de proteção de branch, proprietários do código, o processo de revisão de código, automação e estratégia de lançamento.
Explicar o ecossistema de ferramentas na empresa
Explicar a estratégia de CI/CD da empresa
Discutir como recomendar ferramentas e fluxos de trabalho para as equipes de uma empresa
Explicar como as APIs do GitHub podem ser usadas para estender as capacidades do administrador da interface de usuário, como consultar ou armazenar o log de auditoria
Localizar um ativo do GitHub Marketplace para uma necessidade específica (por exemplo, encontre o Azure Pipelines GitHub App no Marketplace, instale-o e configure-o para implantar o código)
Comparar o GitHub App e Action (por exemplo, suas permissões, como são desenvolvidos e como são consumidos)
Listar os benefícios e riscos de usar as aplicações e ações do GitHub Marketplace

Domínio 2: Gerenciar identidades de usuários e autenticação do GitHub

Gerenciar identidades de usuários e autenticação do GitHub
Listar as implicações de habilitar o single sign-on (SSO) de SAML para uma organização individual versus todas as organizações em uma conta Enterprise
Listar as etapas para habilitar e impor o SSO de SAML para uma única organização e várias organizações usando contas Enterprise.
Explicar como exigir autenticação de dois fatores (2FA) para uma organização.
Explicar como escolher provedores de identidade compatíveis.
Descrever como identificar trabalhos de gerenciamento e autorização no GitHub
Listar as consequências de uma inscrição de usuário na instância, em uma organização ou em várias organizações
Descrever o modelo de autenticação e autorização (especificamente como os usuários acessam o sistema e como eles têm o acesso concedido para coisas específicas no GihHub)
Listar os provedores SCIM compatíveis (Azure, Okta, autodesenvolvido)
Descrever como o protocolo de SCIM funciona e como é compatível com o GH
Descrever como a sincronização de equipes funciona
Comparar o SCI e a sincronização de equipes

Domínio 3: Descrever como o GitHub é implantado, distribuído e licenciado

Comparar as capacidades do GHES, GHEC e GHAE
Descrever o GitHub Enterprise Cloud (GHEC)
Descrever o GitHub Enterprise Server (GHES)
Descrever o GitHub AE

Diferenciar como os produtos são faturados, incluindo as licenças de estação, o GitHub Actions e o GitHub Packages
Descrever os preços do GitHub Actions
Descrever as opções de suporte e preço para as organizações
Descrever como encontrar as estatísticas de uso de licença para uma organização específica
Descrever como encontrar as estatísticas de uso de licença para contas de máquina e serviços periféricos
Explicar o consumo de produtos limitados de um determinado relatório (por exemplo, minutos ou armazenamento do GitHub Actions para o GitHub Packages)

Domínio 4: Gerenciar o acesso e as permissões com base na inscrição

Descrever as permissões e políticas da empresa
Explicar os benefícios e custos de implantar uma única organização versus várias organizações
Descrever como definir permissões de leitura padrão versus permissões de gravação entre organizações
Descrever a sincronização de equipes por meio do AD
Explicar a capacidade de manutenção; gravação de scripts versus várias organizações e vários direitos de acesso
Descrever como ajustar as políticas da empresa e as permissões da organização em alinhamento com a posição de controle e a confiança da empresa

Descrever as permissões e políticas da empresa
Definir uma organização do GitHub
Listar as possíveis funções de um membro da organização
Comparar as permissões para gerentes de cobrança, proprietários e membros da organização
Descrever a diferença entre ser um colaborador externo ou um membro da organização
Listar as consequências de uma inscrição de usuário em uma instância ou organização
Explicar como dar a um usuário as permissões mínimas exigidas para acesso à equipe, à organização e ao repositório.
Listar os benefícios e as desvantagens de criar uma nova organização

Descrever as permissões de equipes
Definir as equipes em uma organização do GitHub
Listar as possíveis funções de um membro da equipe
Descrever os diferentes modelos de permissão

Permissões de repositório
Explicar as ações de um usuário considerando a lista de suas permissões, como função de repositório, inscrição de equipe ou inscrição da organização (https://github.com/organizations/<ORG_NAME>/settings/member_privileges)
Listar as opções de inscrição de repositório
Explicar o acesso de auditoria a um repositório

Domínio 5: Habilitar o desenvolvimento de software seguro e garantir a conformidade

Possibilitar o desenvolvimento de software seguro e garantir a conformidade
Explicar como o GitHub é compatível com a postura de segurança da empresa
Descrever a anulação de dados confidenciais de um repositório Git (filter-branch/BFG)
Descrever a anulação de dados confidenciais do GitHub (entrando em contato com o suporte)
Explicar como escolher uma política baseada no nível de controle necessário
Explicar os impactos de escolher um conjunto de políticas específico
Definir as políticas da organização
Definir as políticas da empresa

Descrever como usar as APIs de log de auditoria (Rest e GraphQL) para explicar um ativo ausente
Definir o caso de uso para logs de auditoria
Descrever os conceitos de conformidade e segurança com o GitHub
Explicar como fornecer relatórios para auditoria

Definir e explicar a importância dos recursos de segurança de um repositório do GitHub
Explicar a importância de uma política de segurança
Definir uma vulnerabilidade
Descrever uma dependência vulnerável
Explicar a importância da verificação de segredo
Explicar a importância da varredura de código
Descrever a varredura de código automatizada (CodeQL)
Explicar o gráfico de dependência
Explicar a importância de um aviso de segurança
Descrever o Dependabot
Detectar e corrigir dependências desatualizadas com as vulnerabilidades de segurança
Descrever os alertas de vulnerabilidade de segurança
Criar e implementar um plano de resposta de segurança que trate dos dados confidenciais em um repositório do GitHub
Descrever como usar as chaves SSH e implantá-las para acessar os dados do repositório

Integrações e acesso à API
Listar tokens de acesso compatíveis (p. ex., token pessoal de acesso, tokens de instalação, tokens OAuth e aplicações OAuth e GitHub, tokens de dispositivo e tokens de atualização)
Explicar como encontrar os limites de taxas de tokens
Descrever o GitHub Apps, as permissões de repositório, as permissões de usuário e as assinaturas de eventos
Descrever aplicações Oauth, as permissões e as assinaturas de eventos
Comparar o uso de um token pessoal de acesso (PAT) ou um GitHub App para autenticação na conta de máquina
Descrever o uso de contas de máquina versus GitHub Apps
Explicar como aprovar ou recusar o GitHub Apps e aplicações OAuth criados pelo usuário com base na política de segurança
Definir um Enterprise Managed User (EMU)

Domínio 6: Gerenciar o GitHub Actions

Distribuir ações e fluxos de trabalho para a empresa
Identificar modelos de reutilização para ações e fluxos de trabalho
Definir uma abordagem para gerenciar e aproveitar componentes reutilizáveis (por exemplo, repositórios para armazenamento, convenções de nomenclatura para arquivos/pastas, planos para manutenção contínua)
Definir como distribuir ações para uma empresa
Explicar como controlar o acesso às ações na empresa
Configurar as políticas organizacionais de uso do GitHub Actions

Gerenciar os executores da empresa
Descrever os efeitos de configurar listas de permissão de IPs em executores auto-hospedados e hospedados no GitHub
Configurar listas de permissão de IPs em sistemas e aplicações internos para permitir a interação com executores hospedados no GitHub
Listar os efeitos e os possíveis vetores de abuso ao habilitar repositórios públicos e executores auto-hospedados
Selecionar executores apropriados para serem compatíveis com cargas de trabalho (por exemplo, usar um executor auto-hospedado versus um hospedado no GitHub, escolher sistemas operacionais compatíveis)
Comparar executores auto-hospedados e hospedados no GitHub
Configurar executores auto-hospedados para uso da empresa (por exemplo, incluir proxies, etiquetas, sistema de rede)
Gerenciar executores auto-hospedados usando grupos (por exemplo, gerenciar acesso, mover executores nos grupos e entre eles)
Monitorar, solucionar problemas e atualizar executores auto-hospedados

Gerenciar segredos criptografados na empresa
Identificar o escopo de segredos criptografados
Explicar como acessar segredos criptografados em ações e fluxos de trabalho
Explicar como gerenciar segredos criptografados no nível da organização
Descrever como gerenciar segredos criptografados no nível de repositório
Descrever como usar cofres de terceiros

Domínio 7: Gerenciar o GitHub Packages

Gerenciar segredos criptografados na empresa
Descrever quais GH Packages são compatíveis
Descrever como acessar, gravar e compartilhar GH Packages
Descrever como usar GH Packages em fluxos de trabalho (por exemplo, GH Actions ou outras ferramentas de CI/CD)
Explicar as diferenças e os casos de uso entre GH Packages e as versões