About private networking with GitHub-hosted runners

In this article

You can connect GitHub-hosted runners to resources on a private network, including package registries, secret managers, and other on-premises services.

Note: GitHub-hosted runners are not currently supported on GitHub Enterprise Server. You can see more information about planned future support on the GitHub public roadmap.

About GitHub-hosted runners networking

By default, GitHub-hosted runners have access to the public internet. However, you may also want these runners to access resources on your private network, such as a package registry, a secret manager, or other on-premise services.

GitHub-hosted runners are shared across all GitHub customers, so you will need a way of connecting your private network to just your runners while they are running your workflows. There are a few different approaches you could take to configure this access, each with different advantages and disadvantages.

Using an API Gateway with OIDC

With GitHub Actions, you can use OpenID Connect (OIDC) tokens to authenticate your workflow outside of GitHub Actions. For more information, see "Using an API gateway with OIDC."

Using WireGuard to create a network overlay

If you don't want to maintain separate infrastructure for an API Gateway, you can create an overlay network between your runner and a service in your private network, by running WireGuard in both places. For more information, see "Using WireGuard to create a network overlay."