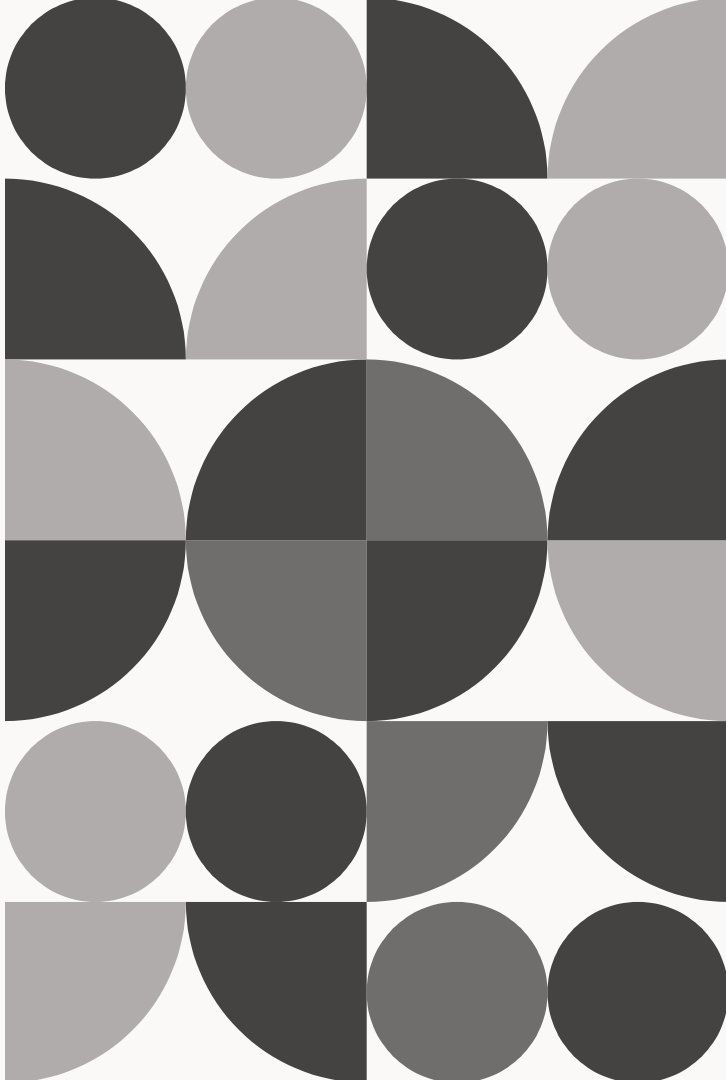
Unlocking new workflows with Tailscale & GitHub Actions

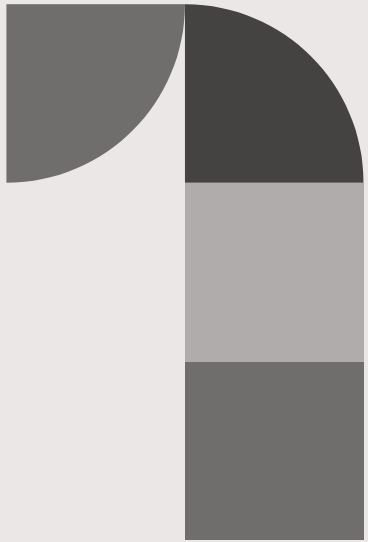


tailscale

Agenda

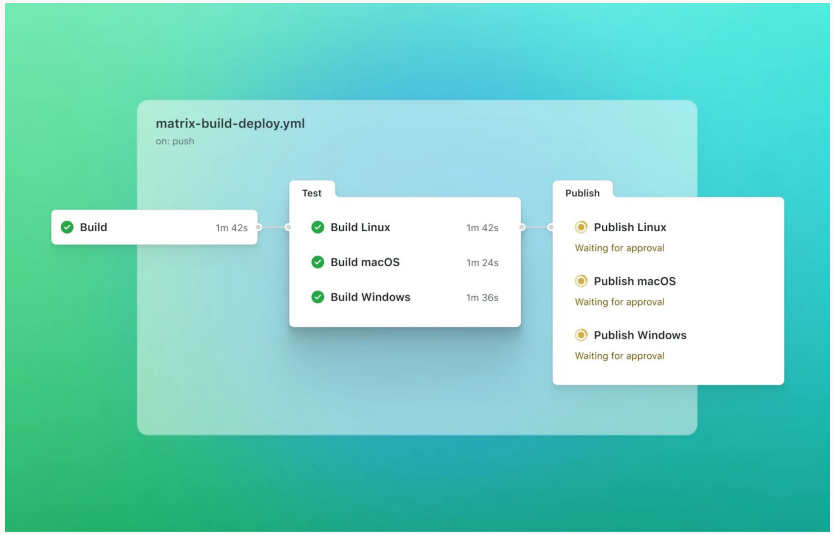
1. **GitHub Actions**
   Your automation super power
2. **The Tailscale GitHub Action**
   A simple way to connect pipelines to your infrastructure
3. **Exciting Changes!**
   Some new announcements
4. **A Demo**
   Let’s see it in action
5. **Wrap up**
   Thank you!

GitHub Actions



tailscale

GitHub Actions



Composable workflows to solve any automation problem

GitHub Actions is a powerful, flexible CI/CD and automation platform that can operate like a full workflow engine.

Workflows are composed of **reusable steps** that can be pulled from the community or defined in your own repositories — making them **extremely composable, customizable, and powerful.**

Runners

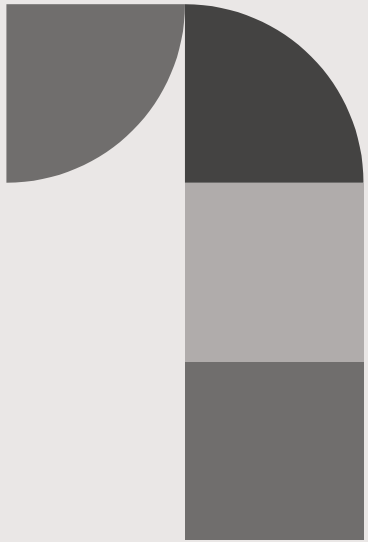
Self Hosted Runners

- You manage compute, scaling, and patching
- Persistent VMs with **long-lived credentials**
- Network exposure risks (open ports, IP allowlists)
- Maintenance overhead (security, updates, capacity)
- Difficult to integrate with ephemeral workflows

Managed Runners

- Ephemeral and automatically managed
- Secure, isolated environment
- No infrastructure to maintain
- But **outside your security boundary**

Tailscale & The GitHub Action

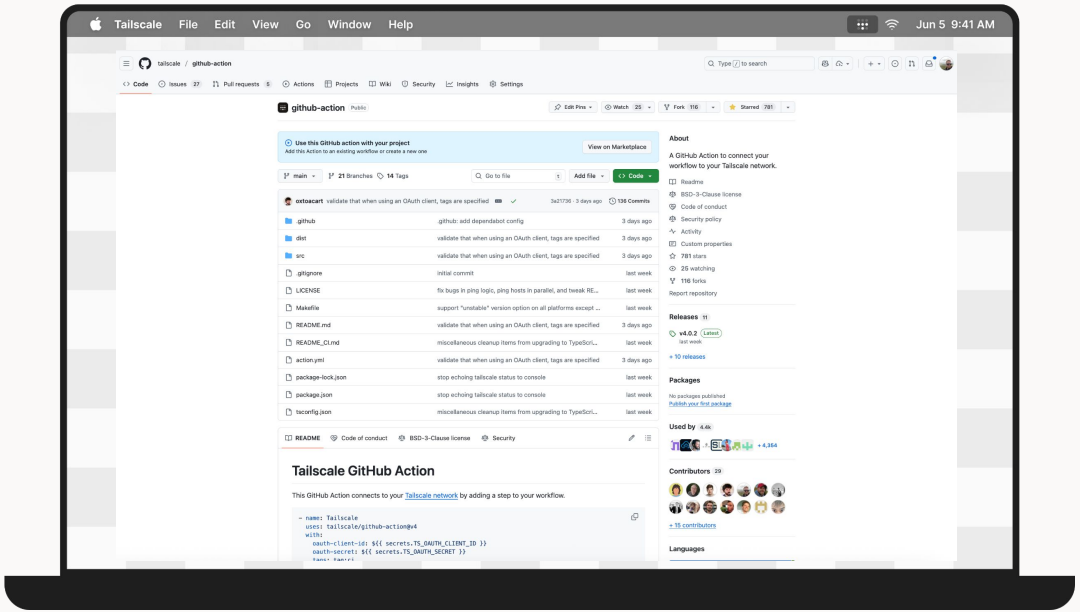


tailscale

Tailscale Github Action

Reliable Connectivity

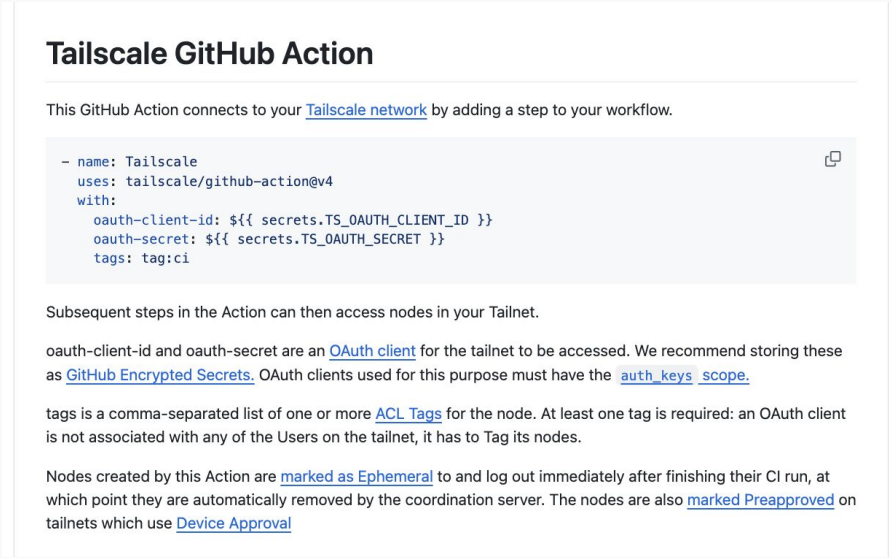
- Published in April 2021
- Used by 4k+ public repos
- Created hundreds of thousands of Tailscale devices



One workflow step

Zero trust connectivity

- Apply granular **tags** to control access
- **Ephemeral** runners — short-lived and automatically removed
- Securely connect CI workflows to **internal infrastructure** without opening the network



Tailscale GitHub Action

This GitHub Action connects to your Tailscale network by adding a step to your workflow.

```
- name: Tailscale
  uses: tailscale/github-action@v4
  with:
    oauth-client-id: ${{ secrets.TS_OAUTH_CLIENT_ID }}
    oauth-secret: ${{ secrets.TS_OAUTH_SECRET }}
    tags: tag:ci
```

Subsequent steps in the Action can then access nodes in your Tailnet.

oauth-client-id and oauth-secret are an OAuth client for the tailnet to be accessed. We recommend storing these as GitHub Encrypted Secrets. OAuth clients used for this purpose must have the `auth_keys` scope.

tags is a comma-separated list of one or more ACL Tags for the node. At least one tag is required: an OAuth client is not associated with any of the Users on the tailnet, it has to Tag its nodes.

Nodes created by this Action are marked as Ephemeral to and log out immediately after finishing their CI run, at which point they are automatically removed by the coordination server. The nodes are also marked Preapproved on tailnets which use Device Approval

Use Cases

Retrieve secrets

Access credentials from internal secrets managers during workflow runs

Database Migrations

Safely and automatically run schema migrations against private/internal databases

IaC

Declaratively manage internal infrastructure using Terraform or Pulumi

Integration Tests

Run tests against internal APIs and staging environments

ETL

Trigger or run internal data workflows that live behind firewalls

Private Artifacts

Pull and push packages or containers from internal registries

Get rid of..

SSH Bastions

- Complex setup and maintenance
- • Shared credentials and audit gaps
- • Difficult to scale across teams

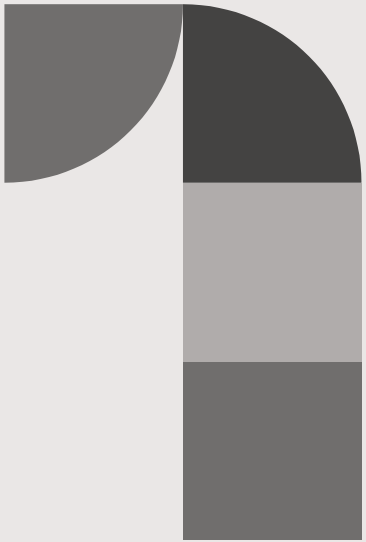
Public-Facing Sensitive Data

- Opening internal APIs or databases to the internet
- • Static IP allowlists that break constantly
- • Increased risk of data leaks or lateral movement

Static Network Workarounds

- VPN tunnels, port forwarding, and NAT hacks
- Hardcoded network configs in CI/CD pipelines
- Slows down development and onboarding

Exciting Changes!



tailscale

Rewritten in Typescript

Using the Actions SDK

- Faster
  - Up to 2x faster, more with caching
- More reliable
  - Waits for setup, allows ping testing before proceeding
- New features!
  - Logout on completion
- Better error validation

OIDC Federation

Authenticate devices with no static credentials!

Configure OIDC federation to trust repos within your GitHub Org, and authenticate Tailscale devices without any static credentials that can be stolen!