GitHub Actions Permissions and Configuration Guide

Repository Settings Required

1. GitHub Actions Permissions

Navigate to: `Settings > Actions > General`

Workflow permissions:
- Read and write permissions
- Allow GitHub Actions to create and approve pull requests

Fork pull request workflows:
- Run workflows from fork pull requests

2. GitHub Pages Configuration

Navigate to: `Settings > Pages`

Source:
- Deploy from a branch
- Branch: `gh-pages` (will be created automatically)
- Folder: `/ (root)`

Custom domain (optional):
- Set to your preferred domain or leave blank for default GitHub Pages URL

3. Environment Configuration

Navigate to: `Settings > Environments`

Create the following environments (optional but recommended):
- `staging` - for develop branch deployments
- `production` - for main branch deployments

4. Required Secrets

Navigate to: `Settings > Secrets and variables > Actions`

Required secrets:
- `GITHUB_TOKEN` - Automatically provided by GitHub (no action needed)

Optional secrets (for enhanced functionality):
- `SNYK_TOKEN` - For Snyk security scanning
- `SEMGREP_APP_TOKEN` - For Semgrep SAST scanning
- `NPM_TOKEN` - For NPM package publishing (if needed)

Workflow Configuration

Current Clean Workflows

1. **CI/CD Pipeline** (`ci-cd-clean.yml`)
   - Triggers: Push to main/develop, PRs to main

- Features: Test, build, deploy to GitHub Pages
    - Permissions: Contents read, Pages write

2. **Security Scanning** (`security-clean.yml`)
    - Triggers: Push to main/develop, PRs to main, weekly schedule
    - Features: CodeQL, dependency scan, SAST
    - Permissions: Security events write

3. **Automated Release** (`release-clean.yml`)
    - Triggers: Push to main, manual dispatch
    - Features: Semantic release, asset creation
    - Permissions: Contents write, Issues write, PRs write

Troubleshooting Common Issues

Startup Failures

If workflows show "startup_failure":

1. **Check repository permissions:**
    ```bash
    # Verify Actions are enabled
    curl -H "Authorization: token YOUR_TOKEN" \
         https://api.github.com/repos/OWNER/REPO/actions/permissions
    ```

2. **Verify branch protection rules:**
    - Ensure workflows can run on target branches
    - Check if required status checks are blocking

3. **Environment setup:**
    - Ensure environments exist if referenced in workflows
    - Check environment protection rules

Permission Errors

If you see permission-related errors:

1. **Update workflow permissions:**
    ```yaml
    permissions:
      contents: read
      pages: write
      id-token: write
    ```

2. **Check token scopes:**
    - GITHUB_TOKEN has appropriate permissions
    - Custom tokens have required scopes

Deployment Issues

For GitHub Pages deployment problems:

1. **Enable GitHub Pages:**
    - Go to Settings > Pages
    - Select source as "GitHub Actions"

2. **Check build artifacts:**
   - Ensure `dist/` or `build/` directory exists
   - Verify artifact upload/download steps

Manual Configuration Commands

Using GitHub CLI

```
# Enable GitHub Actions (if disabled)
gh api repos/:owner/:repo --method PATCH --field has_actions=true

# Configure Pages
gh api repos/:owner/:repo/pages --method POST \
  --field source.branch=gh-pages \
  --field source.path=/

# Set workflow permissions
gh api repos/:owner/:repo --method PATCH \
  --field default_workflow_permissions=write \
  --field can_approve_pull_request_reviews=true
```

Repository Settings Checklist

- [ ] Actions enabled
- [ ] Workflow permissions set to "Read and write"
- [ ] Pages configured for GitHub Actions deployment
- [ ] Required secrets configured
- [ ] Environment protection rules (if using environments)
- [ ] Branch protection rules allow workflow runs

Monitoring and Alerts

Workflow Health Monitoring

Create a monitoring workflow to track failures:

```yaml
name: Workflow Health Monitor
on:
  schedule:
    - cron: '0 9 * * *'  # Daily at 9 AM UTC
  workflow_dispatch:

jobs:
  monitor:
    runs-on: ubuntu-latest
    steps:
    - name: Check workflow status
      uses: actions/github-script@v7
      with:
        script: |
          const workflows = ['ci-cd-clean.yml', 'security-clean.yml', 'release-
clean.yml'];
          for (const workflow of workflows) {
            const runs = await github.rest.actions.listWorkflowRuns({
              owner: context.repo.owner,
              repo: context.repo.repo,
              workflow_id: workflow,
              per_page: 5
            });

            const failures = runs.data.workflow_runs.filter(run =>
              run.conclusion === 'failure' || run.conclusion === 'startup_failure'
            );

            if (failures.length > 0) {
              console.log(`⚠ ${workflow} has ${failures.length} recent failures`);
            } else {
              console.log(`  ${workflow} is healthy`);
            }
          }
```

Success Metrics

Key Performance Indicators

- **Workflow Success Rate:** >95% successful runs
- **Build Time:** <10 minutes for CI/CD pipeline
- **Security Scan Coverage:** 100% of pushes scanned
- **Deployment Frequency:** Automated on every main branch push
- **Mean Time to Recovery:** <30 minutes for failed deployments

Monitoring Dashboard

Track these metrics in your repository:

- Total workflow runs per week
- Success/failure ratio
- Average build duration
- Security vulnerabilities detected and resolved
- Deployment success rate

Support and Resources

GitHub Documentation

- GitHub Actions Documentation (https://docs.github.com/en/actions)
- GitHub Pages Documentation (https://docs.github.com/en/pages)
- Repository Permissions (https://docs.github.com/en/repositories/managing-your-repositorys-settings-and-features)

Community Resources

- GitHub Actions Marketplace (https://github.com/marketplace?type=actions)
- Awesome GitHub Actions (https://github.com/sdras/awesome-actions)
- GitHub Community Forum (https://github.community/)

Last Updated: June 14, 2025
Version: 1.0
Maintainer: Audityzer Team