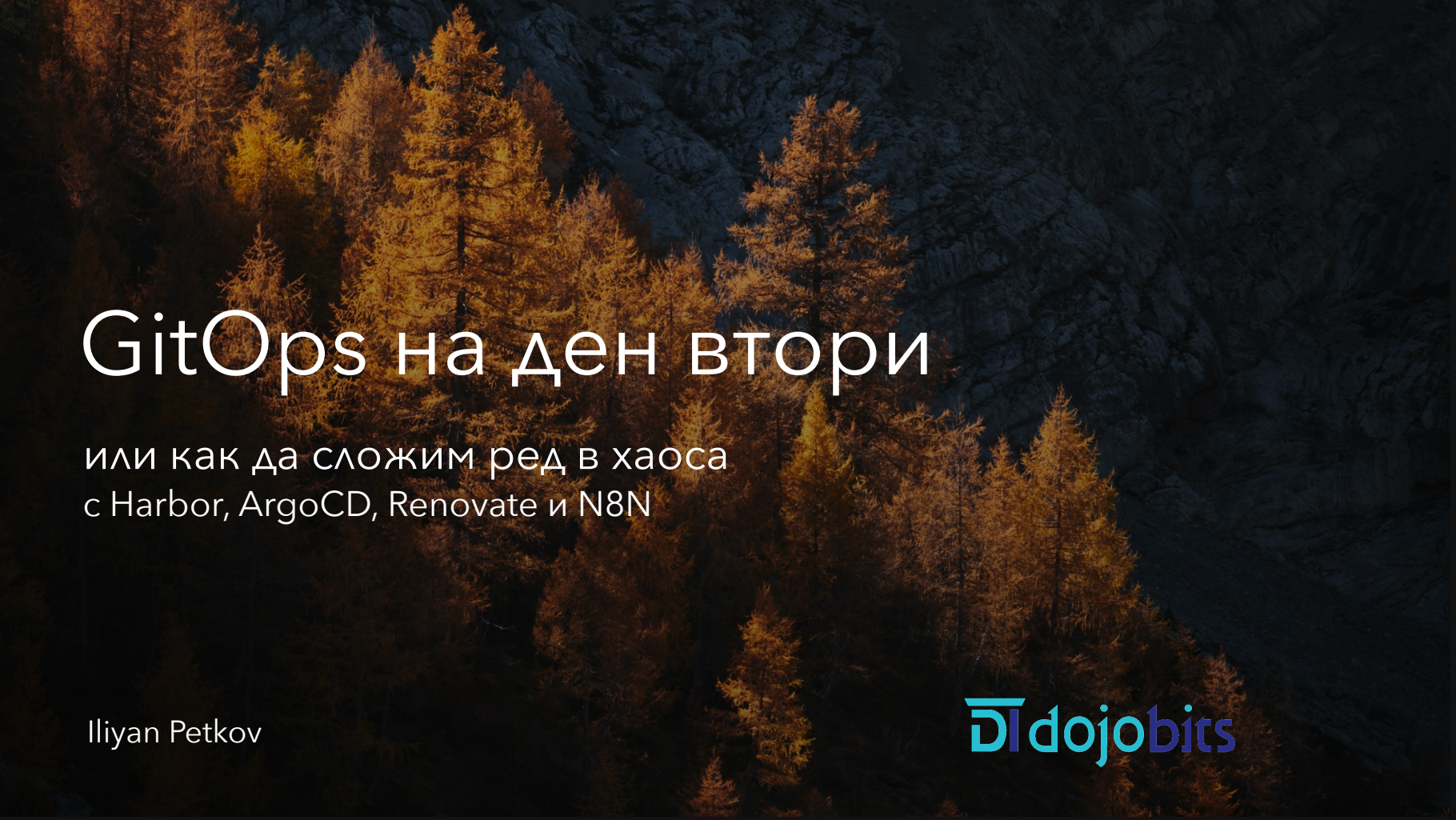


GitOps на ден втори

или как да сложим ред в хаоса
с Harbor, ArgoCD, Renovate и N8N

Iliyan Petkov

dojobits

#whoweare

dojobits

Iliyan Petkov

Valentin Hristev

iliyan-s-petkov
@Iliyan-s-petkov

valentin-hristev
@vhristev

https://dojobits.io/

Why choose us

20 + years
Industry Experience

21 +
Certifications

30 +
Cutting-Edge Technologies

6 +
Countries Served

3 200 +
Training Hours Delivered

Agenda

- Our Focus on Day 2
- GitOps to the Rescue
- Renovate: What It Is And Why You'll Love It
- Supply chain security with Harbor
- Automated Pull Requst review with n8n
- Automated deployment with ArgoCD

Day 2 Operations Focus

Security

- Scan images
- identify CVEs
- generate SBOMs
- enforce policies

Stability

- Automated updates with intelligent review
- control deployment windows

Compliance

- Audit trail in Git
- approval workflows
- maintenance windows

Automating the daily tasks so you can focus on delivering value

GitOps to the Rescue!

Problems

- Infrastructure sprawl
- Manual security reviews
- Inconsistent updates
- High operational overhead
- Risk of vulnerabilities
- Lost audit trails

GitOps Benefits

✅ Declarative infrastructure

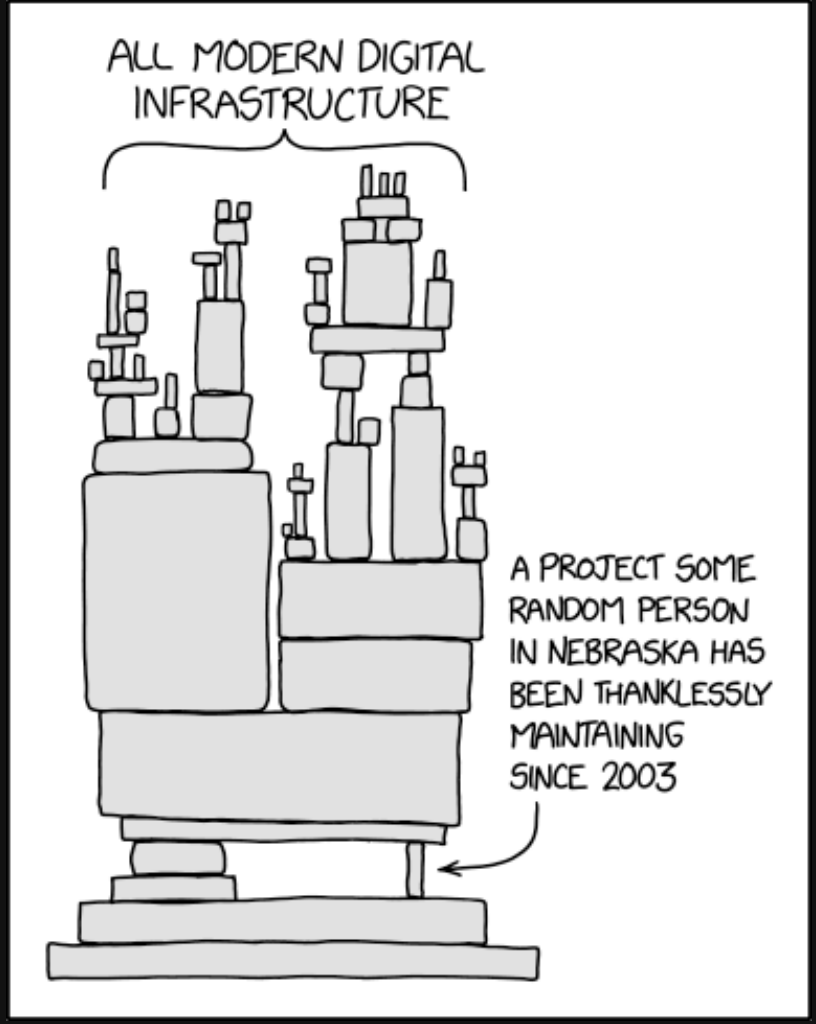
✅ Automated deployments

✅ Complete auditability

✅ Easy rollbacks

✅ Single source of truth

✅ Reproducible state


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

Renovate: Dependency Management at Scale

What is Renovate?

Automated dependency management tool that:

- Monitors all dependency sources
- Creates pull requests for updates
- Includes release notes & changelogs
- Supports 50+ package ecosystems

Key Capabilities

🔄 Multi-ecosystem support

📊 Intelligent grouping

🤖 Auto-merge capabilities

📈 Dashboard insights

🔐 Security-first approach

The Dependency Update Challenge

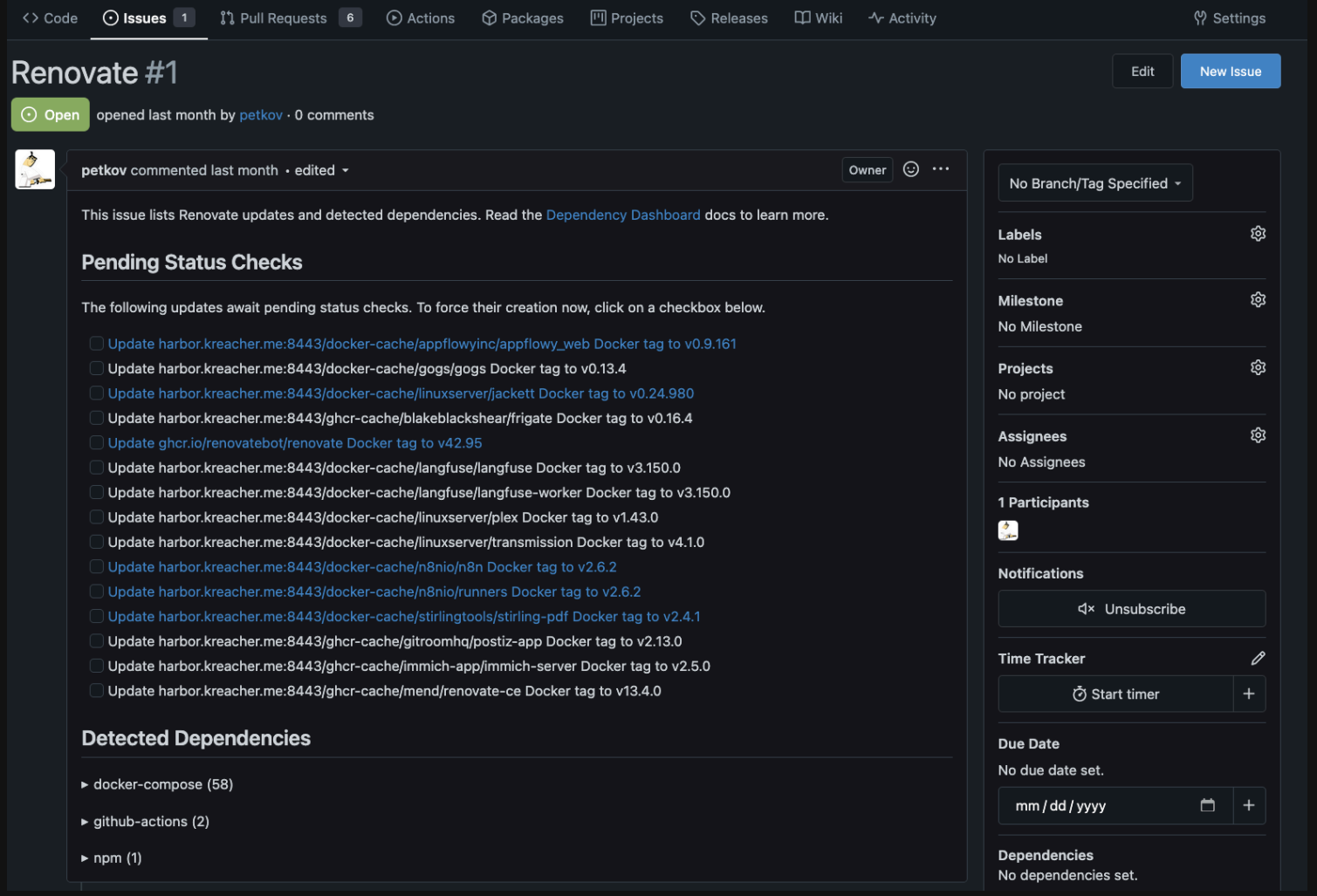
Without Renovate

- ❌ Manual checking for updates
- ❌ Security patches delayed
- ❌ Inconsistent processes
- ❌ High operational cost
- ❌ Risk of supply chain attacks

With Renovate

- ✅ Continuous monitoring
- ✅ Automatic PRs on new versions
- ✅ Security context included
- ✅ Configurable auto-merge rules
- ✅ Proactive vulnerability management

Think of Renovate as your personal assistant that never sleeps, continuously checking for updates and reducing your team's manual overhead.


Code
Issues 1
Pull Requests 6
Actions
Packages
Projects
Releases
Wiki
Activity
Settings
Renovate #1
Edit
New Issue
Open
opened last month by petkov · 0 comments
petkov commented last month • edited
Owner
This issue lists Renovate updates and detected dependencies. Read the Dependency Dashboard docs to learn more.
Pending Status Checks
The following updates await pending status checks. To force their creation now, click on a checkbox below.
Update harbor.kreacher.me:8443/docker-cache/appflowyinc/appflowy_web Docker tag to v0.9.161
Update harbor.kreacher.me:8443/docker-cache/gogs/gogs Docker tag to v0.13.4
Update harbor.kreacher.me:8443/docker-cache/linuxserver/jackett Docker tag to v0.24.980
Update harbor.kreacher.me:8443/ghcr-cache/blakeblackshear/frigate Docker tag to v0.16.4
Update ghcr.io/renovatebot/renovate Docker tag to v42.95
Update harbor.kreacher.me:8443/docker-cache/langfuse/langfuse Docker tag to v3.150.0
Update harbor.kreacher.me:8443/docker-cache/langfuse/langfuse-worker Docker tag to v3.150.0
Update harbor.kreacher.me:8443/docker-cache/linuxserver/plex Docker tag to v1.43.0
Update harbor.kreacher.me:8443/docker-cache/linuxserver/transmission Docker tag to v4.1.0
Update harbor.kreacher.me:8443/docker-cache/n8nio/n8n Docker tag to v2.6.2
Update harbor.kreacher.me:8443/docker-cache/n8nio/runners Docker tag to v2.6.2
Update harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf Docker tag to v2.4.1
Update harbor.kreacher.me:8443/ghcr-cache/gitroomhq/postiz-app Docker tag to v2.13.0
Update harbor.kreacher.me:8443/ghcr-cache/immich-app/immich-server Docker tag to v2.5.0
Update harbor.kreacher.me:8443/ghcr-cache/mend/renovate-ce Docker tag to v13.4.0
Detected Dependencies
▸ docker-compose (58)
▸ github-actions (2)
▸ npm (1)
No Branch/Tag Specified
Labels
No Label
Milestone
No Milestone
Projects
No project
Assignees
No Assignees
1 Participants
Notifications
Unsubscribe
Time Tracker
Start timer
Due Date
No due date set.
mm / dd / yyyy
Dependencies
No dependencies set.

Code | Issues 1 | Pull Requests 7 | Actions | Packages | Projects | Releases | Wiki | Activity | Settings

Update harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf Docker tag to v2.4.0 #205

Edit

Open petkov wants to merge 1 commits from `renovate/harbor.kreacher.me-8443-docker-cache-stirlingtools-stirling-pdf-2.x` into `master`

Conversation 0 | Commits 1 | Files Changed 1 | +1 -1

petkov commented 3 days ago — Owner

This PR contains the following updates:

Package	Update	Change
harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf	minor	`2.3.1` → `2.4.0`

Release Notes

▸ Stirling-Tools/Stirling-PDF (harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf)

Configuration

📅 **Schedule**: Branch creation - At any time (no schedule defined), Automerge - At any time (no schedule defined).

🚦 **Automerge**: Disabled by config. Please merge this manually once you are satisfied.

♻ **Rebasing**: Whenever PR becomes conflicted, or you tick the rebase/retry checkbox.

🔕 **Ignore**: Close this PR and you won't be reminded about this update again.

- [ ] If you want to rebase/retry this PR, check this box

This PR has been generated by Renovate Bot.

Reviewers
No Reviewers
Still in progress? Add **WIP:** prefix

Labels
No Label

Milestone
No Milestone

Projects
No project

Assignees
petkov

1 Participants

Notifications
Unsubscribe

Time Tracker
Start timer +

Update harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf Docker tag to v2.4.0 #205

Edit

Open petkov wants to merge 1 commits from renovate/harbor.kreacher.me-8443-docker-cache-stirlingtools-stirling-pdf-2.x into master

Conversation 0 · Commits 1 · Files Changed 1 · +1 -1

petkov commented 3 days ago — Owner

This PR contains the following updates:

Package	Update	Change
harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf	minor	`2.3.1` → `2.4.0`

Release Notes

▾ Stirling-Tools/Stirling-PDF (harbor.kreacher.me:8443/docker-cache/stirlingtools/stirling-pdf)

`v2.4.0`: 2.4.0 2FA support, Database management, PDF/X and more

Compare Source

Lots of new features in this release

- database backup management (Only for internal H2 database users)
- Full 2FA support with One-time-password auth code app support!
- Get info supporting better compliance verification
- PDF/X conversions
- automation tool now export into folder scan JSONs for folder automation

Bug fixes for

- Sign tool
- SSO user creation
- addStamp not handling timestamps

Thanks as always for all the fixes and work everyone has been doing! such as @balazs-szucs or the new bug fix from @Joey4 !
Special thanks to @Ludy87 for introducing the awesome 2FA feature!

What's Changed

Enhancements

- feat(admin): add H2 database backup & restore management to admin UI by @Ludy87 in #5528
- feat(frontend): enhance icon detection and update config navigation icon by @Ludy87 in #5524
- feat(security): add TOTP-based multi-factor authentication with backend and UI support by @Ludy87 in #5417
- feat(compliance): implement compliance verfication for get info on PDF by @balazs-szucs in #5435

Reviewers
No Reviewers
Still in progress? Add WIP: prefix

Labels
No Label

Milestone
No Milestone

Projects
No project

Assignees
petkov

1 Participants

Notifications
Unsubscribe

Time Tracker
Start timer

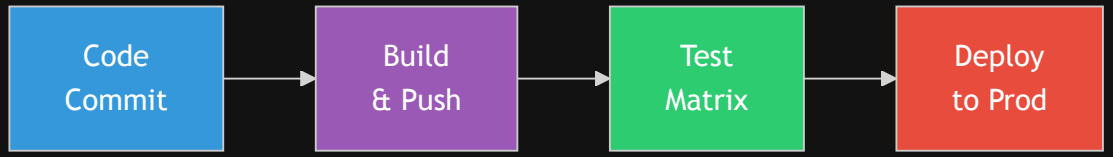
Due Date
No due date set.
mm / dd / yyyy

Dependencies
No dependencies set.
Add dependency...

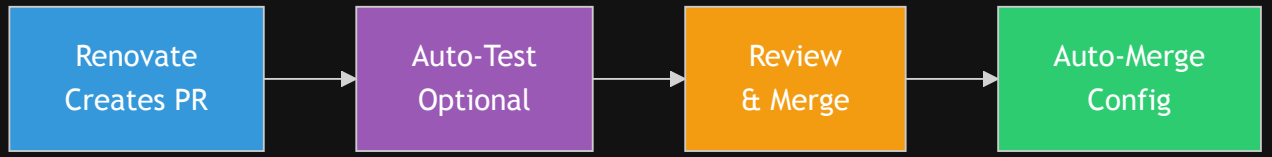
Reference: home/iaas#205

Renovate in the DevOps Pipeline

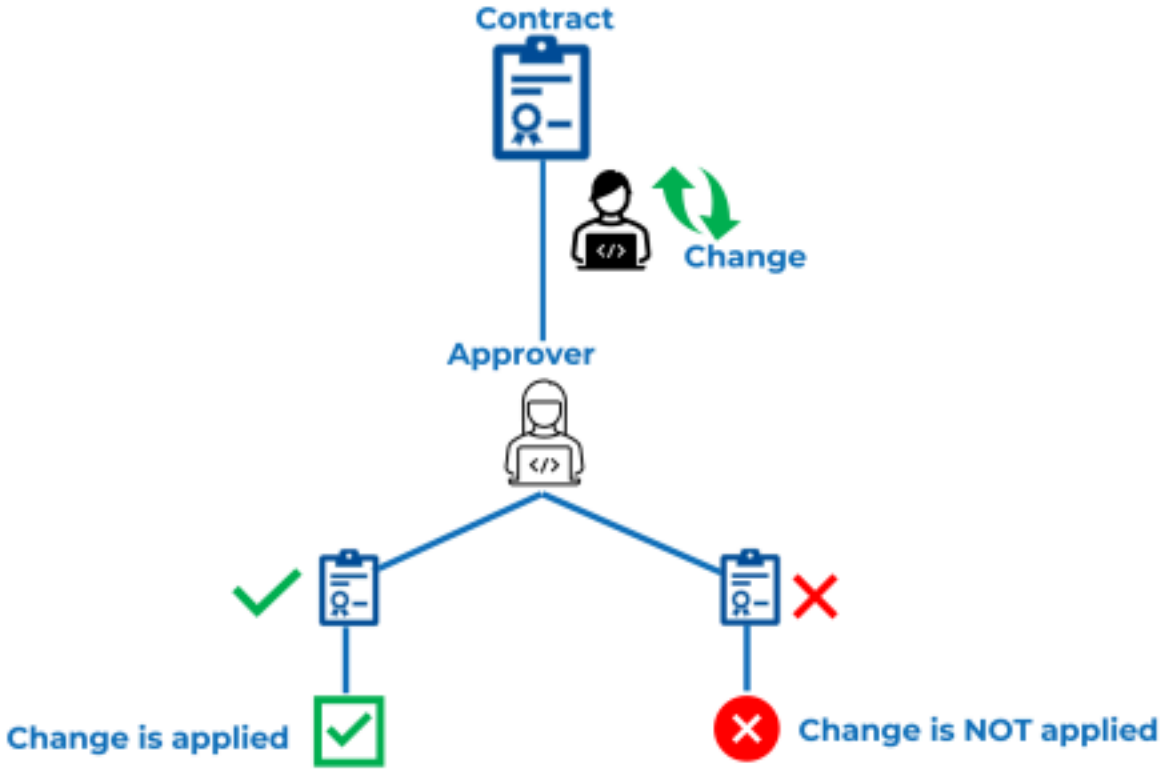
Traditional DevOps Pipeline:



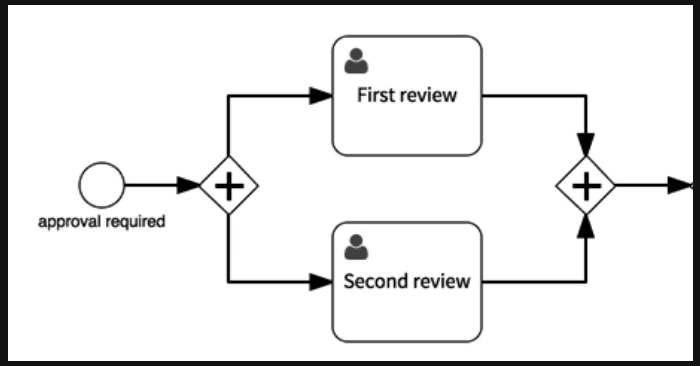
With Renovate Integrated:

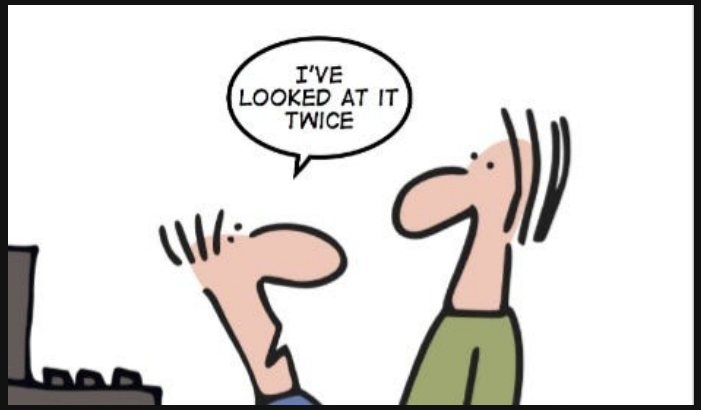


Renovate acts as the **first guardian** of your dependency chain, ensuring updates are available and tested before reaching your team.


Contract
Change
Approver
Change is applied
Change is NOT applied

4 Eyes Principle





Renovate Global Config

```
module.exports = {
  onboarding: false,
  platform: "gitea",
  endpoint: "https://git.kreacher.me/api/v1/",
  autodiscover: false,
  repositories: ["home/iaas"],
  minimumReleaseAge: "2",
  internalChecksFilter: "strict",
  persistRepoData: true,
  prCreation: "not-pending",
  minimumReleaseAgeBehaviour: "timestamp-required",
  pruneStaleBranches: true,
  configMigration: true,
  commitBodyTable: true,
  dependencyDashboard: true,
  username: "petkov",
  gitAuthor: "Petkov <iliyan.petkov@kreacher.me>",
  fetchChangeLogs: "pr",
  optimizeForDisabled: true,
  osvVulnerabilityAlerts: true,
  hostRules: [
    { hostType: 'docker', matchHost: 'docker.io', concurrentRequestLimit: 2 },
    { hostType: 'docker', matchHost: 'lscr.io', concurrentRequestLimit: 2 },
    { hostType: 'docker', matchHost: 'ghcr.io', concurrentRequestLimit: 2 },
    { hostType: 'docker', matchHost: 'harbor.kreacher.me', timeout: 120000 }
```

Renovate Repo Specific Config

```
{
  "$schema": "https://docs.renovatebot.com/renovate-schema.json",
  "extends": ["config:recommended"],
  "dependencyDashboard": true,
  "dependencyDashboardTitle": "Renovate",
  "assignees": ["petkov"],
  "labels": ["renovate"],
  "configMigration": true,
  "prHourlyLimit": 0,
  "prConcurrentLimit": 0,
  "branchConcurrentLimit": 0,
  "docker-compose": {
    "hostRules": [
      {
        "hostType": "docker",
        "matchHost": "harbor.kreacher.me",
        "timeout": 120000
      },
      {
        "matchHost": "docker.io",
        "concurrentRequestLimit": 2
      },
      ...
    ]
```


HARBOR

Harbor: Secure Container Registry

Harbor's Role

- Central image repository
- Pull-through cache for upstream registries
- Vulnerability scanning
- SBOM generation
- Policy enforcement
- Multi-tenant support

Security Pipeline

1. Image pushed to Harbor
2. Automatic vulnerability scan
3. Generate SBOM (all dependencies)
4. Policy evaluation
5. Allow/block based on policies
6. Audit log entry

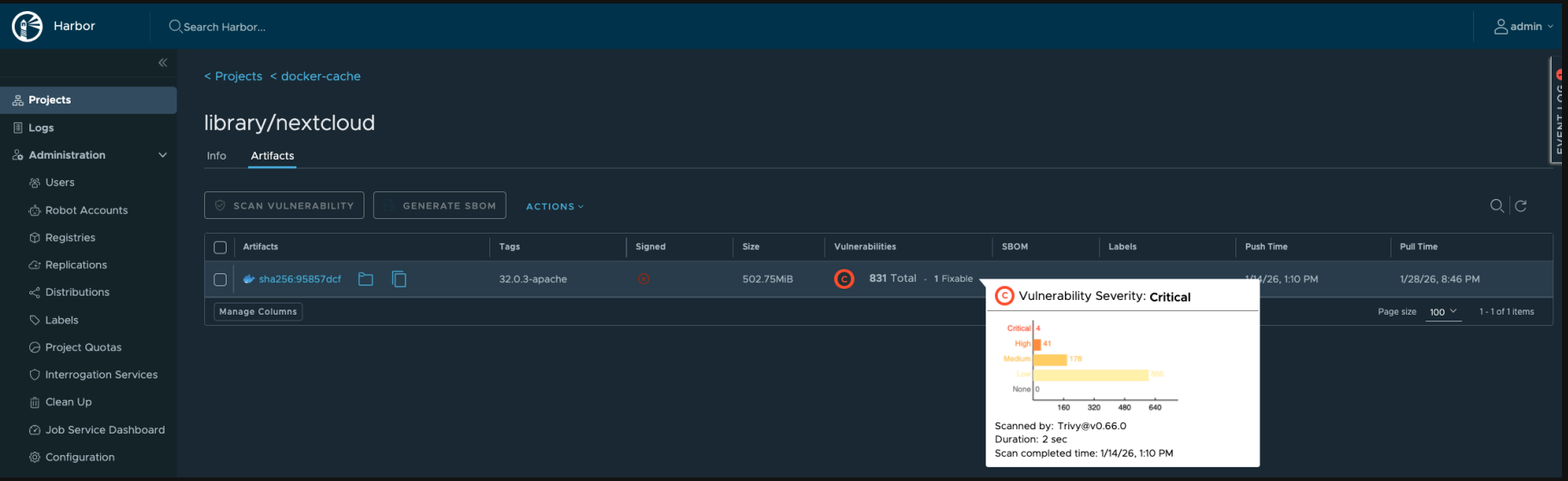
Harbor: Supply Chain Security

Vulnerability Scanning

- Identifies CVEs in image layers and dependencies
- Compares against known vulnerability databases
- Generates detailed reports with severity levels
- Blocks deployment if critical CVEs found

⚡ **Real-time Protection:** Images are scanned automatically on push.

- No manual steps
- No delays
- Security is built into the pipeline


Harbor
Search Harbor...
admin
Projects
Logs
Administration
Users
Robot Accounts
Registries
Replications
Distributions
Labels
Project Quotas
Interrogation Services
Clean Up
Job Service Dashboard
Configuration
< Projects < docker-cache
library/nextcloud
Info
Artifacts
SCAN VULNERABILITY
GENERATE SBOM
ACTIONS
Artifacts
Tags
Signed
Size
Vulnerabilities
SBOM
Labels
Push Time
Pull Time
sha256:95857dcf
32.0.3-apache
502.75MiB
831 Total · 1 Fixable
1/28/26, 8:46 PM
Manage Columns
Page size 100
1 - 1 of 1 items
Vulnerability Severity: Critical
Critical 4
High 41
Medium 178
Low 605
None 0
160
320
480
640
Scanned by: Trivy@v0.66.0
Duration: 2 sec
Scan completed time: 1/14/26, 1:10 PM

< Projects < docker-cache < library/nextcloud

sha256:95857dcf

Tags

REMOVE TAG

Name	Pull Time	Push Time
32.0.3-apache	1/28/26, 6:46 PM	1/14/26, 1:10 PM

Page size 100 1 - 1 of 1 items

Additions

Vulnerabilities SBOM

SCAN VULNERABILITY

Vulnerability	Severity	CVSS3	Status	Package	Current version	Fixed in version	Listed In CVE Allowlist
CVE-2025-13836	Critical	redhat: 6.8	affected	python3.13-minimal	3.13.5-2		No
Description: When reading an HTTP response from a server, if no read amount is specified, the default behavior will be to use Content-Length. This allows a malicious server to cause the client to read large amounts of data into memory, potentially causing OOM or other DoS.							
CVE-2025-13836	Critical	redhat: 6.8	affected	libpython3.13-minimal	3.13.5-2		No
CVE-2025-13836	Critical	redhat: 6.8	affected	libpython3.13-stdlib	3.13.5-2		No
CVE-2025-13836	Critical	redhat: 6.8	affected	python3.13	3.13.5-2		No
CVE-2025-8194	High	bitnami: 7.5 redhat: 7.5	affected	libpython3.13-minimal	3.13.5-2		No

Harbor: Supply Chain Security

Software Bill of Materials (SBOM):

- Complete inventory of all components in image
- Tracks version information and licenses
- Essential for compliance (CycloneDX, SPDX formats)
- Enables rapid response to disclosure of vulnerabilities


n8n

n8n: Intelligent Automation

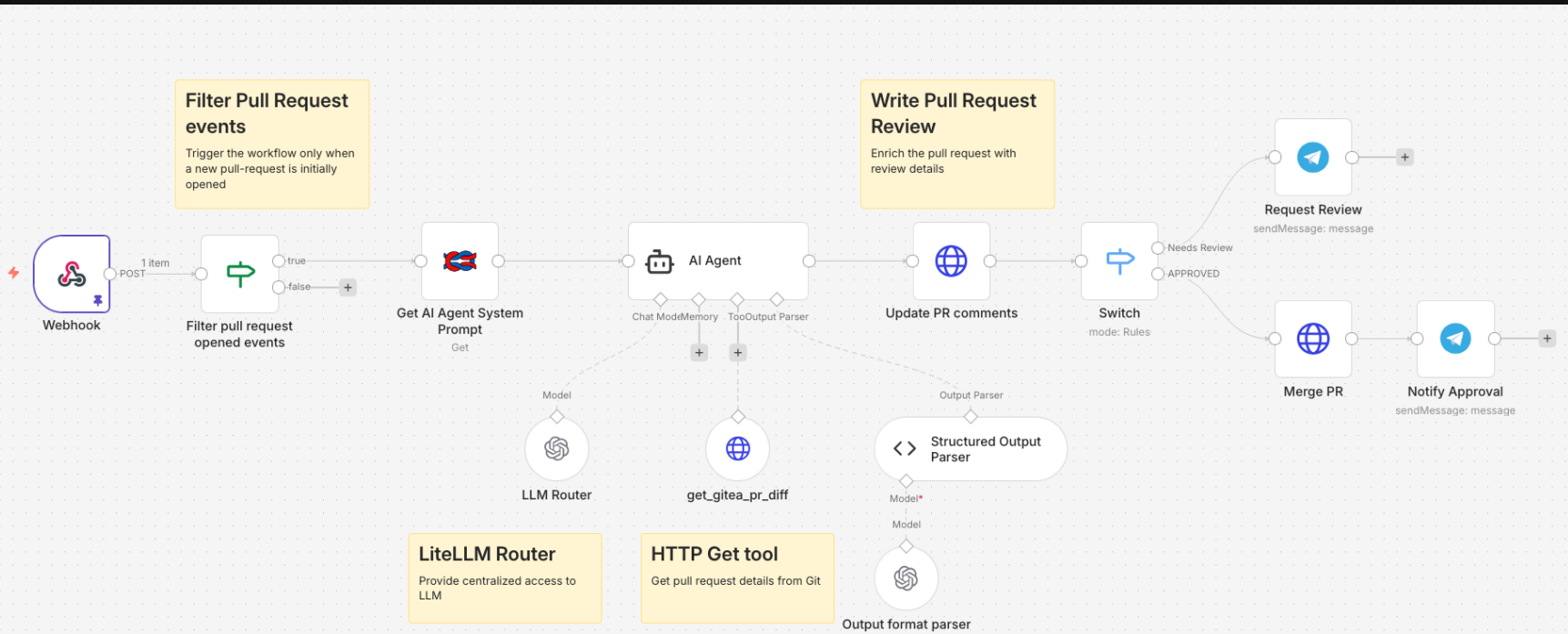
What is n8n?

- Open-source workflow automation platform
- 400+ integrations out of the box
- Visual workflow builder
- Self-hostable (optional)
- LLM integration capabilities

In GitOps Context

Bridges the gap between:

- Automated updates (Renovate)
- Manual review requirements
- Container security (Harbor)
- Deployment decisions (ArgoCD)


Filter Pull Request events
Trigger the workflow only when a new pull-request is initially opened
Write Pull Request Review
Enrich the pull request with review details
Webhook
1 item
POST
Filter pull request opened events
true
false
Get AI Agent System Prompt
Get
AI Agent
Chat Mode
Memory
Too
Output Parser
Update PR comments
Switch
mode: Rules
Needs Review
APPROVED
Request Review
sendMessage: message
Merge PR
Notify Approval
sendMessage: message
Model
LLM Router
get_gitea_pr_diff
Output Parser
Structured Output Parser
Model*
Model
Output format parser
LiteLLM Router
Provide centralized access to LLM
HTTP Get tool
Get pull request details from Git

4-Eyes PR Review with n8n

Renovate opens a PR → a webhook triggers n8n workflow

Intelligent Analysis:

1. Extract PR details: dependencies, versions, changes
2. Query LLM (cloud or self-hosted) with context
3. LLM performs intelligent review:
   - Analyzes release notes
   - Assesses breaking changes
   - Evaluates security implications

Action Taking:

✅ Auto-merge if low-risk (e.g., patch updates)

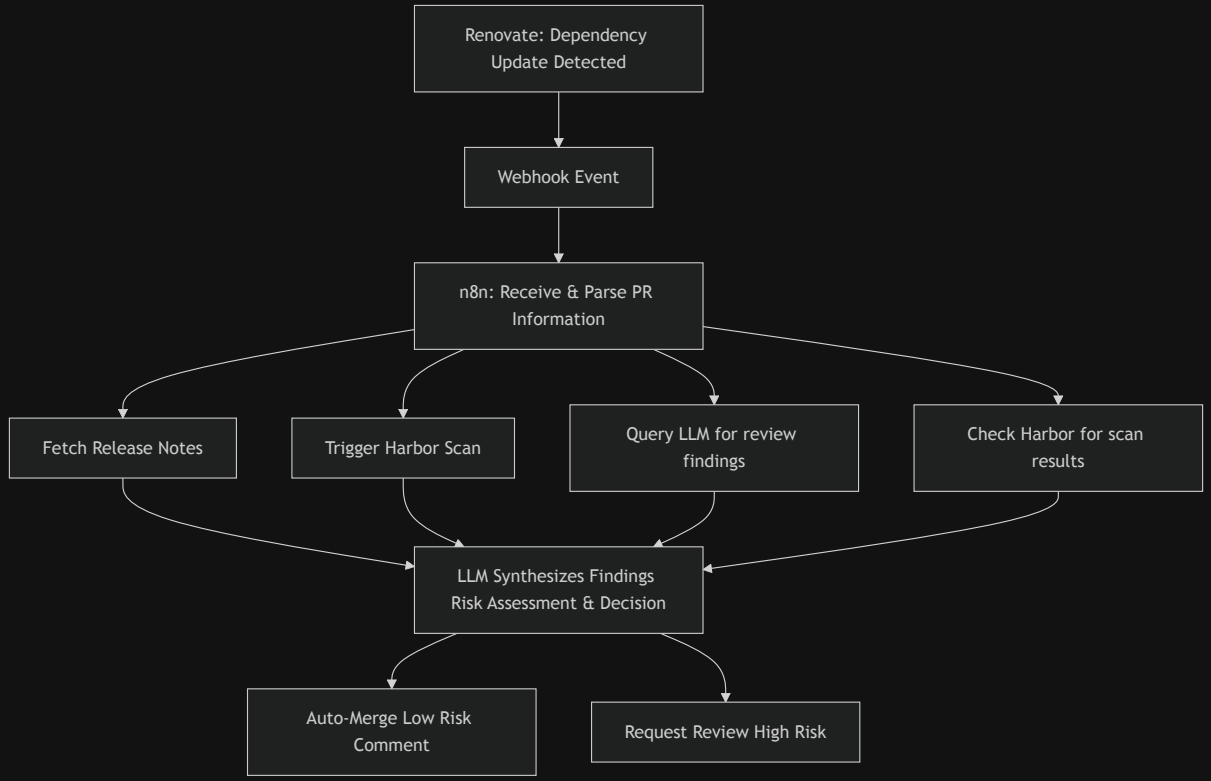
🔍 Request human review if risky

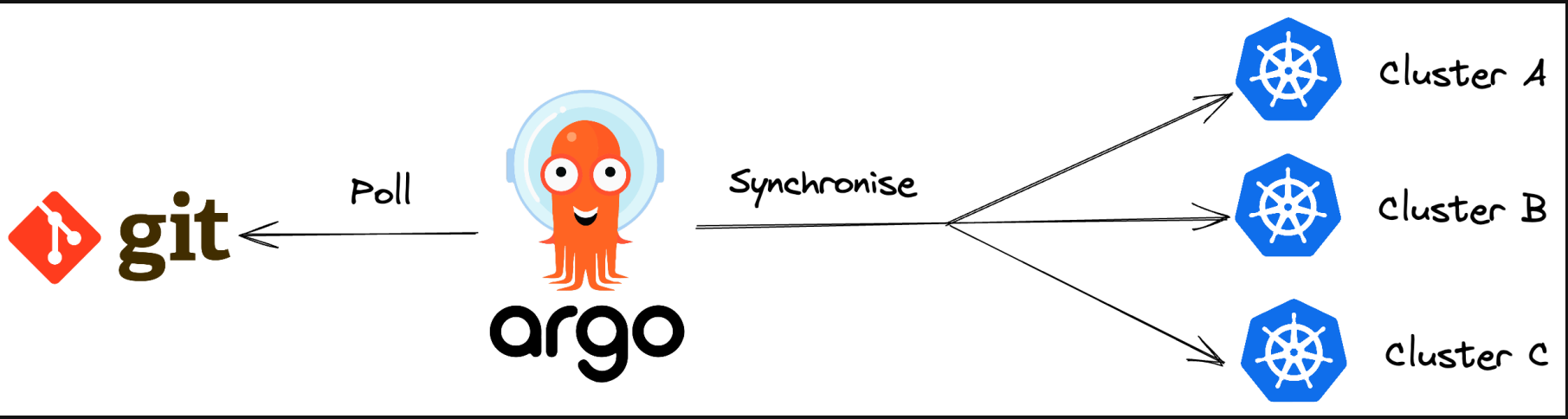
📝 Enrich PR with findings and recommendations

n8n: Extended Review Capabilities

1. **Fetch Release Notes**
   - Use upstream GitHub/GitLab API
   - Extract the release documentation
   - Parse changelog for breaking changes
2. **Trigger Harbor Scanning**
   - Initiate image pull and scan in Harbor
   - Retrieve vulnerability scan results
   - Check for CVEs in the new version
3. **Intelligent Decision**
   - LLM summarize all findings
   - Compares against organizational policies
   - Provides recommendations
4. **Reduce Review Overhead**
   - Developers get rich context, not raw updates
   - Human reviewers focus on exceptions
   - 4-eyes principle with automation assistance

n8n Workflow




git
Poll
argo
Synchronise
Cluster A
Cluster B
Cluster C

ArgoCD: GitOps Deployment

What is ArgoCD?

- Continuous deployment for Kubernetes
- Declarative, Git-based deployments
- Continuous monitoring & reconciliation
- Rollback capabilities
- Multi-cluster support

Core Principles

🎯 Git as source of truth

🔄 Automatic sync with Git state

🔍 Continuous health monitoring

⏮️ Easy rollbacks via Git

🔐 Role-based access control

ArgoCD Sync Windows: Controlled Deployments

Sync Windows allow you to specify when ArgoCD can automatically sync applications:

```yaml
project: production
syncWindows:
  - kind: allow
    schedule: '0 2 ? * SUN'  # Every Sunday 2 AM UTC
    duration: 4h             # 4-hour window
    applications:
      - 'production/*'
```

Benefits:

- ✅ Deploy only during maintenance windows
- ✅ Prevent surprise deployments during business hours
- ✅ Reduce risk of impacting users
- ✅ Align with change management policies
- ✅ Still fully automated and auditable

The Complete GitOps Flow

1. **Renovate** detects a new dependency version
   - Creates a PR in Git with all context
2. **n8n** webhook triggers on PR creation
   - Pulls release notes and security context
   - Queries LLM for intelligent analysis
   - Triggers Harbor scan for vulnerabilities
   - Comments findings on PR
3. **Review Phase** (Human or Auto)
   - Low-risk updates: auto-merge
   - High-risk: await human review
   - All decisions recorded in Git commit history
4. **ArgoCD** monitors the Git repo
   - Detects merged changes
   - Respects maintenance windows
   - Deploys during scheduled window
5. **Harbor** validates image before deployment
   - Policy checks
   - CVE scanning
   - SBOM generation for compliance

Benefits: Security

✅ **Continuous Monitoring**

- No dependencies are "set and forget"
- Vulnerabilities addressed proactively

✅ **Automated Scanning**

- Every image scanned automatically
- Complete SBOM for every artifact

✅ **Intelligent Review**

- LLM understands security context
- Reduces false positives

✅ **Audit Trail**

- Every change tracked in Git
- Who approved, when, and why

✅ **Controlled Updates**

- Updates happen in maintenance windows
- No surprise deployments

✅ **Intelligent Testing**

- LLM reviews breaking changes
- Release notes analyzed automatically

✅ **Rollback Capability**

- Git provides complete version history
- One command rollback if issues occur

✅ **Continuous Reconciliation**

- ArgoCD ensures actual state matches desired
- Detects and corrects drift

Benefits: Stability

✅ **Controlled Updates**

- Updates happen in maintenance windows
- No surprise deployments

✅ **Intelligent Testing**

- LLM reviews breaking changes
- Release notes analyzed automatically

✅ **Rollback Capability**

- Git provides complete version history
- One command rollback if issues occur

✅ **Continuous Reconciliation**

- ArgoCD ensures actual state matches desired
- Detects and corrects drift

Benefits: Operational Efficiency

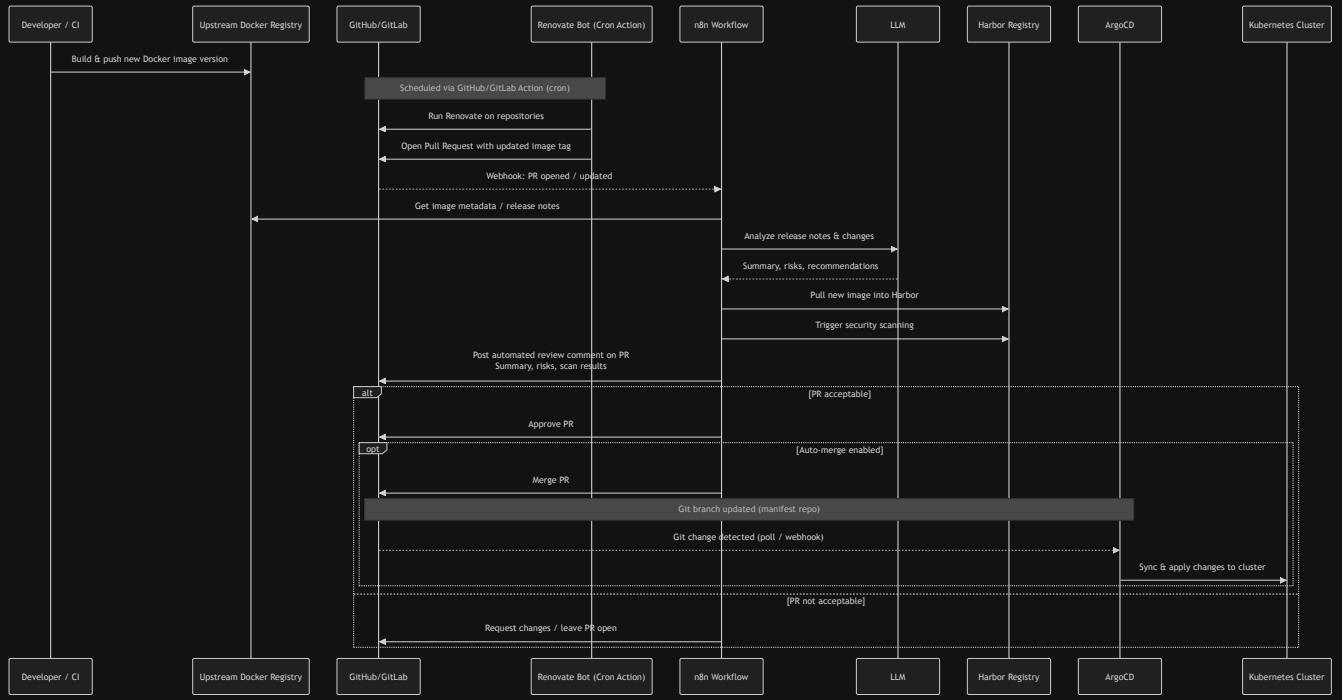
Before

- ❌ Manual dependency checks
- ❌ Manual PR review & merging
- ❌ Manual deployment coordination
- ❌ Manual security scanning
- ❌ Hours per week on maintenance

After

- ✅ Automatic detection & PR creation
- ✅ Intelligent review & auto-merge
- ✅ Scheduled, automatic deployment
- ✅ Automatic vulnerability scanning
- ✅ Minutes per week on oversight

Implementation Architecture



Key Takeaways

🔄 Automation

Renovate + n8n + Harbor + ArgoCD = fully automated, intelligent update pipeline

🔒 Security

Scanning, SBOMs, and intelligent review reduce supply chain risk

📊 Reliability

Git-based deployments with maintenance windows ensure stability

Day 2 Operations is not chaos—it's a solved problem with the right tools, orchestrated together.


Thank You!
Questions?
dojobits