



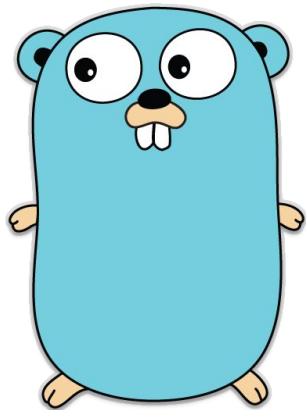
Beveiliging

Leveranciersdag, 29 januari 2020

Inhoud

- Ontwerp van NLX
- Het ontwikkelproces
- NLX in productie
- Roadmap

Ontwerp van NLX



- Ontwikkeld in Go
- Open source programmeertaal, ontwikkeld door Google

Ontwerp van NLX - Go

Enkele populaire projecten die geschreven zijn in Go



kubernetes



docker



Prometheus



LINKERD



Ontwerp van NLX - Go

- Go software compileert naar **één binary** voor alle grote besturingssystemen (o.a. Linux, Windows, FreeBSD en macOS)
- Biedt **memory safety**
- Zeer geschikt voor **netwerk toepassingen** en **multiprocessing** vanwege concurrency features in de taal
- Standaard **TLS1.3** en **HTTP/2** ondersteuning
- Bevat een **hoogwaardige** cryptografische bibliotheek

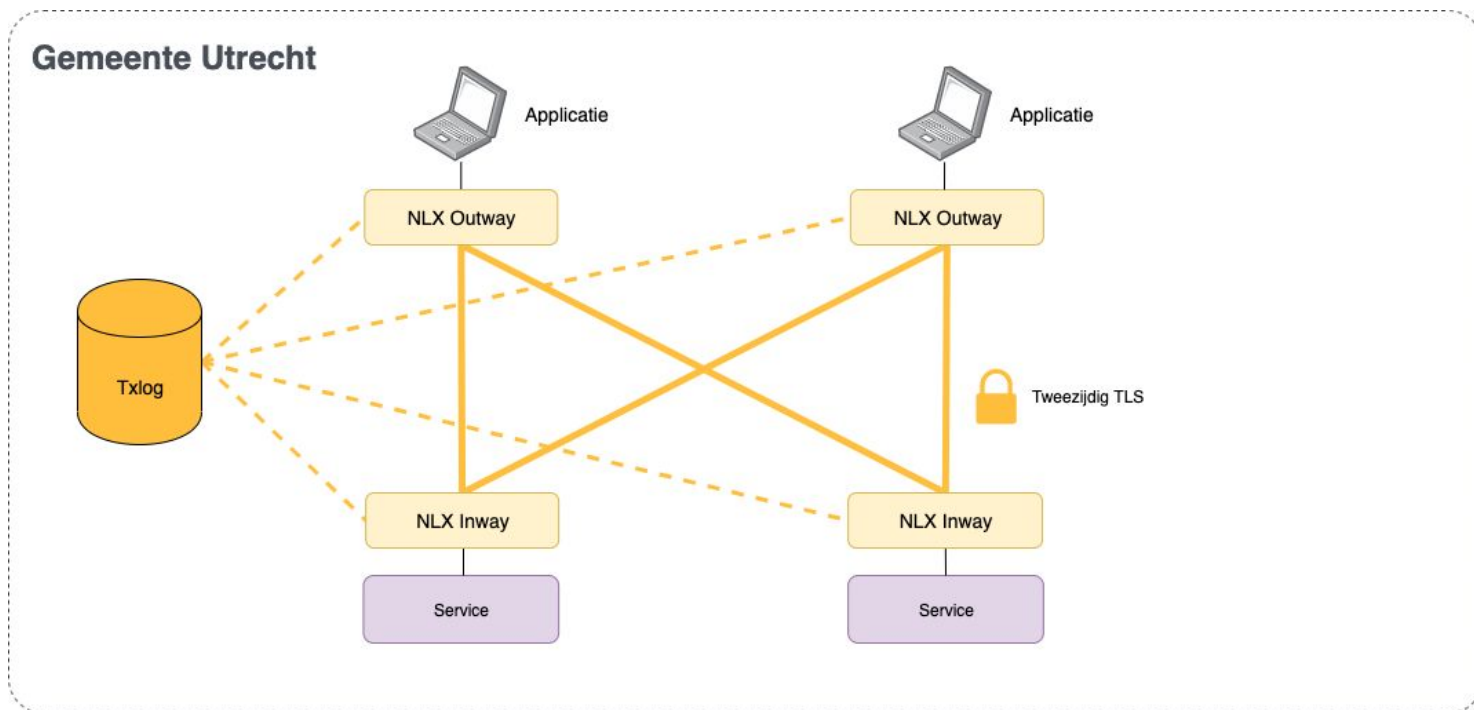
Ontwerp van NLX - omvang code

Vanwege opzet in microservices hebben de afzonderlijke delen een **klein aanvalsvak**:

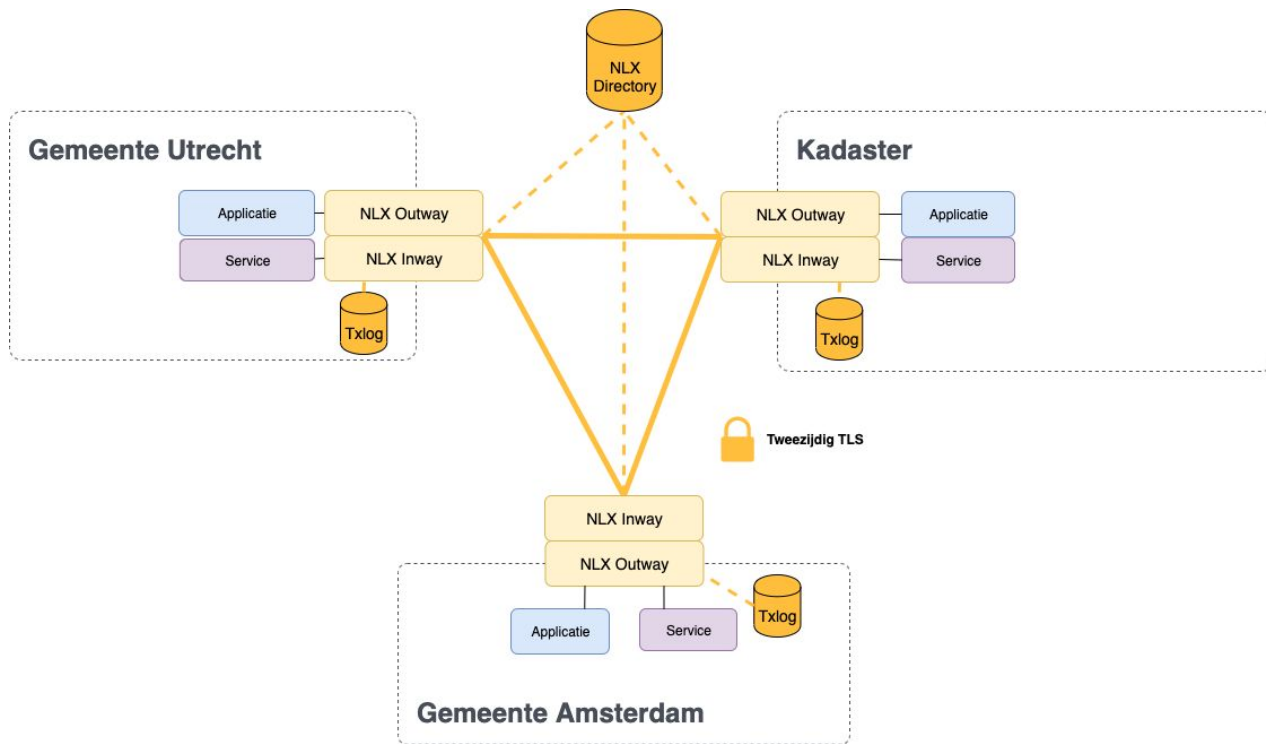
- Inway (~1600 regels code)
- Outway (~1600 regels code)
- Directory (~1000 regels code)

(waarbij een groot deel testen zijn)

Ontwerp van NLX - binnen organisatie



Ontwerp van NLX - tussen organisaties



Ontwerp van NLX - authenticatie

- **Binnen organisaties**

NLX heeft koppelvlakken voor **Identity & Access Management** op de outway. We proberen dus voor gebruikers zoveel mogelijk te integreren met bestaande IAM oplossingen.

- **Tussen organisaties**

Voor authenticatie vertrouwen we op de **PKI-Overheid** certificaatautoriteit (Private services G1)

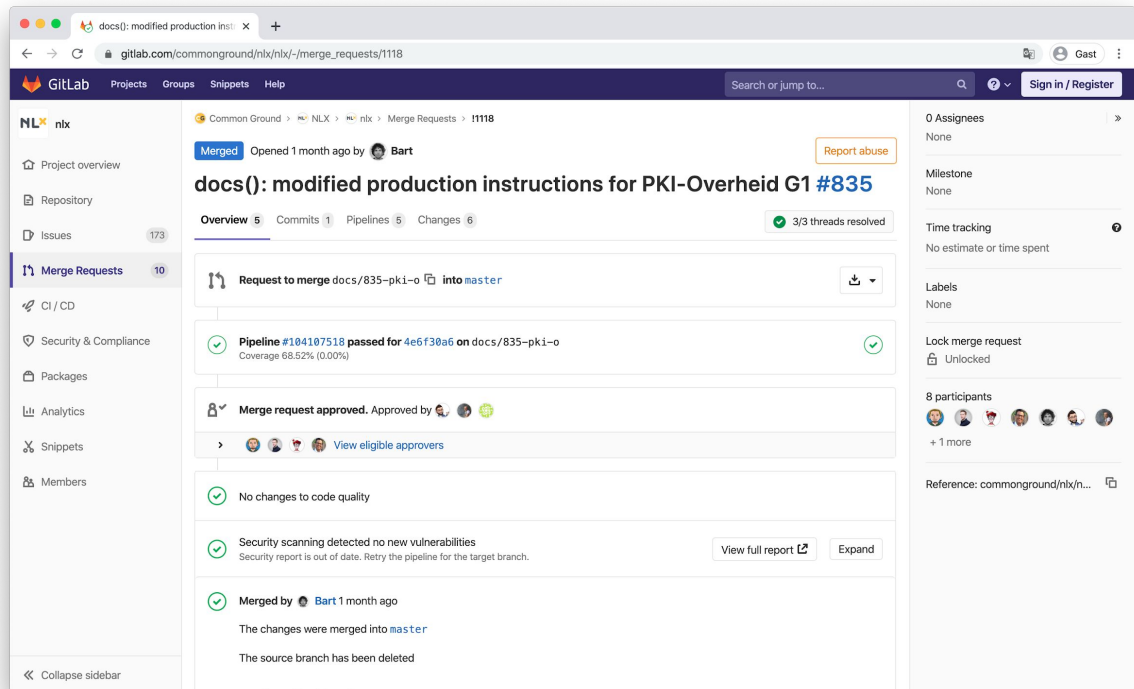
Ontwikkelproces - CI/CD

- Vindt plaats op **GitLab**
- Testen, bouwen en uitrollen volledig geautomatiseerd
- Inzichtelijk voor iedereen
- **Twee-factor** login, binnenkort ook hardware tokens

The screenshot shows the GitLab interface for the 'nlx' project. The left sidebar contains navigation links: Project overview, Repository, Issues (173), Merge Requests (10), CI / CD (selected), Pipelines, Jobs, Schedules, Charts, Security & Compliance, Packages, Analytics, Snippets, and Members. The main area displays a list of pipelines. Each pipeline entry includes a status icon (passed or failed), a pipeline ID, a job icon, and a job name with its commit hash. The jobs are categorized into 'renovate/go...' (dependencies updates) and 'feature/test...' (feature tests). The status of each job is indicated by a green checkmark for 'passed' or a red 'X' for 'failed'.

Pipeline ID	Status	Job Name	Commit Hash
#112258459	passed	renovate/go...	57d71369
#112237102	failed	renovate/go...	da30c120
#112237068	passed	renovate/go...	efb498a1
#112176165	failed	renovate/aL...	742999e0
#111721961	passed	feature/test	77c2606e
#111721662	passed	feature/test	7f71e1cf
#111576373	passed	renovate/go...	c99023e4
#111564627	passed	renovate/go...	958dc4ca
#111549235	passed	renovate/go...	5f60ea86

Ontwikkelproces - goedkeuring

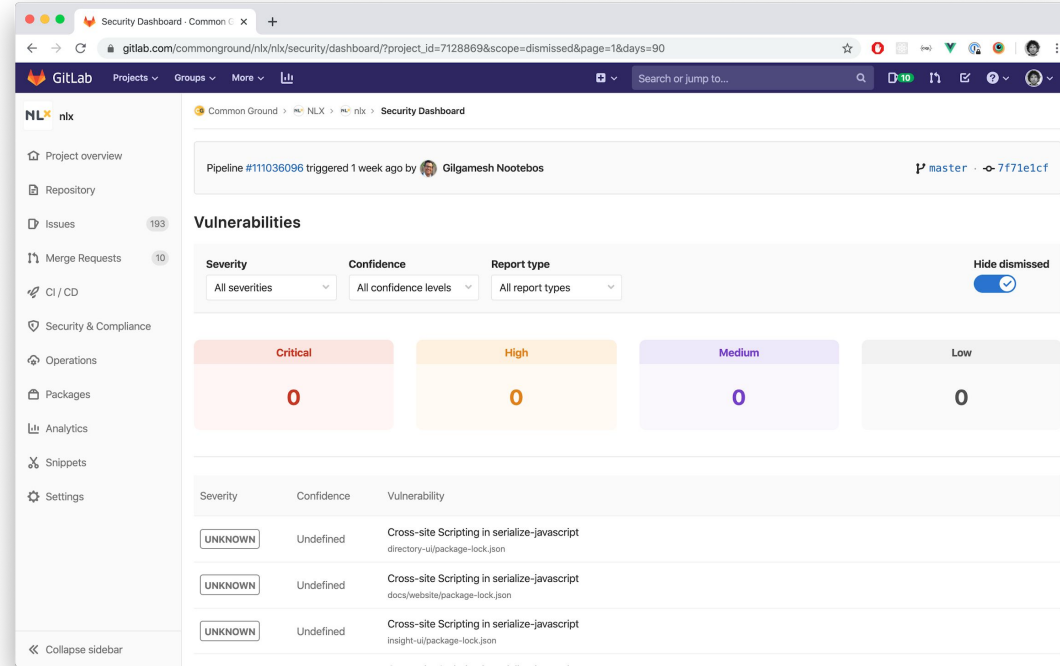


1. Wijziging **start** met een “**issue**”
2. Ontwikkelaar maakt “merge request”
3. **Goedkeuring** vereist voor elke **wijziging** door andere ontwikkelaar & product owner

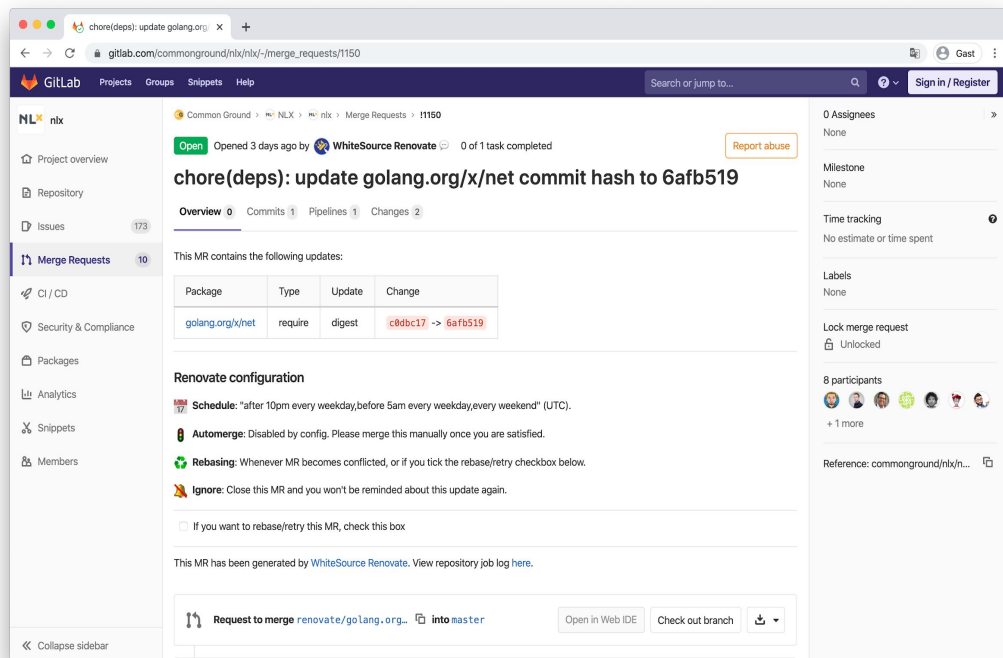
Ontwikkelproces - beveiligingschecks

Nieuwe code en bestaande code wordt automatisch geanalyseerd:

- Statische analyse
- Dynamische analyse
- Container scanning
- Dependency analyse



Ontwikkelproces - dependency monitoring



chore(deps): update golang.org/x/net commit hash to 6afb519

Overview 0 Commits 1 Pipelines 1 Changes 2

This MR contains the following updates:

Package	Type	Update	Change
golang.org/x/net	require	digest	c0dbcb17 -> 6afb519

Renovate configuration

- Schedule:** "after 10pm every weekday,before 5am every weekday,every weekend" (UTC).
- Automerge:** Disabled by config. Please merge this manually once you are satisfied.
- Rebasing:** Whenever MR becomes conflicted, or if you tick the rebase/retry checkbox below.
- Ignore:** Close this MR and you won't be reminded about this update again.

☐ If you want to rebase/retry this MR, check this box

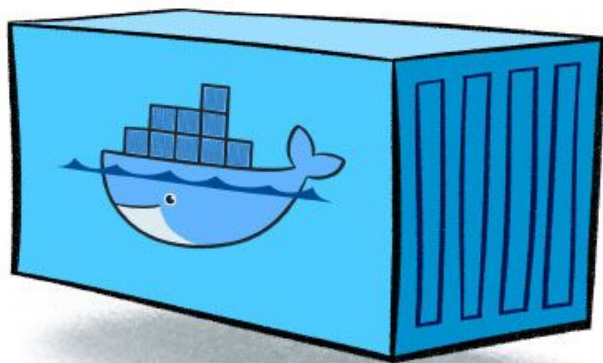
This MR has been generated by [WhiteSource Renovate](#). View repository job log [here](#).

[Request to merge renovate/golang.org...](#) [into master](#) [Open in Web IDE](#) [Check out branch](#) [Download](#)

Renovate bot **monitort dependencies** en maakt merge requests aan voor nieuwe versies



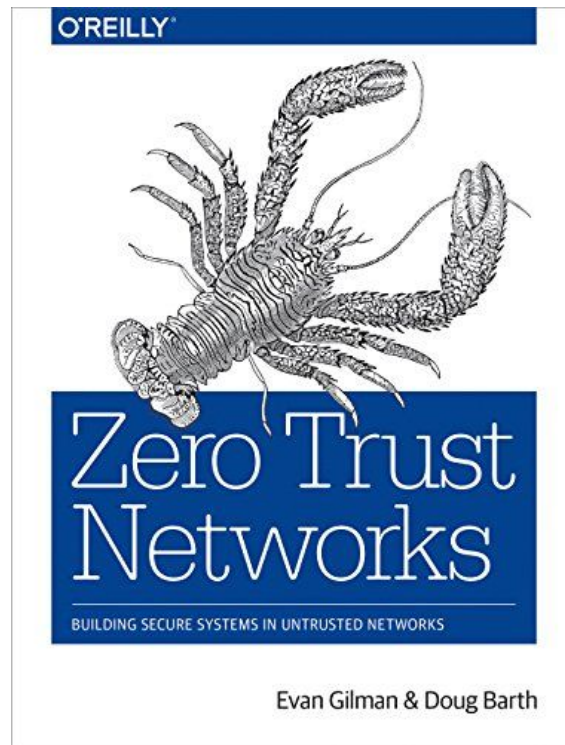
NLX in productie



- NLX gebruik je vanuit door ons aangeleverde **Docker images**
- **Klein aanvalsvak** door minimalistische basis (Alpine Linux)
 - Inway: 12MB
 - Outway: 10MB
- Updaten is **zeer eenvoudig** en **voorspelbaar** (nieuwe versie ongeveer iedere twee weken)

NLX in productie (2)

- Gebruikt één poort, **HTTPS**
- Beveiliging binnen organisatie is gelijk aan beveiliging tussen organisaties: **zero trust networks**



NLX in productie (3)

- Het hele netwerk gebruikt hetzelfde integratie-mechanisme en volgt de **periodieke updates**
- Hierdoor kunnen oude protocollen en onveilige ciphers **snel verwijderd** worden
- Bijv: nu al worden verbindingen op NLX met **TLS <1.2** niet geaccepteerd

Roadmap

Op de planning voor de komende drie maanden:

- **Certificate pinning** (public key)
- Gebruik van **Open Policy Agent** om uitgebreide autorisatieregels te specificeren op outway en inway

In de takenapplicatie voor bouwvergunningen mag alleen een gebruiker met de rol vergunningverlener op werkdagen tussen 09:00 en 17:00 verzoeken doen bij het Kadaster

Roadmap (2)

Functionaliteit die we hierna mogelijk ontwikkelen (op basis van feedback)

- Ondersteuning van Hardware Security Modules (**HSM**) / Key Management Systeem (**KMS**)
- Automatiseren van uitgifte van certificaten binnen organisaties / levensduur van interne certificaten verkorten

Meer informatie en ontwikkeling

Ontwikkeling en discussie vindt open plaats. Je kunt meedenken en discussieren op GitLab.



nlx.io



gitlab.com/commonground/nlx