



QualvoSec

A Security Patch Management Tool
for Linux & BSD.

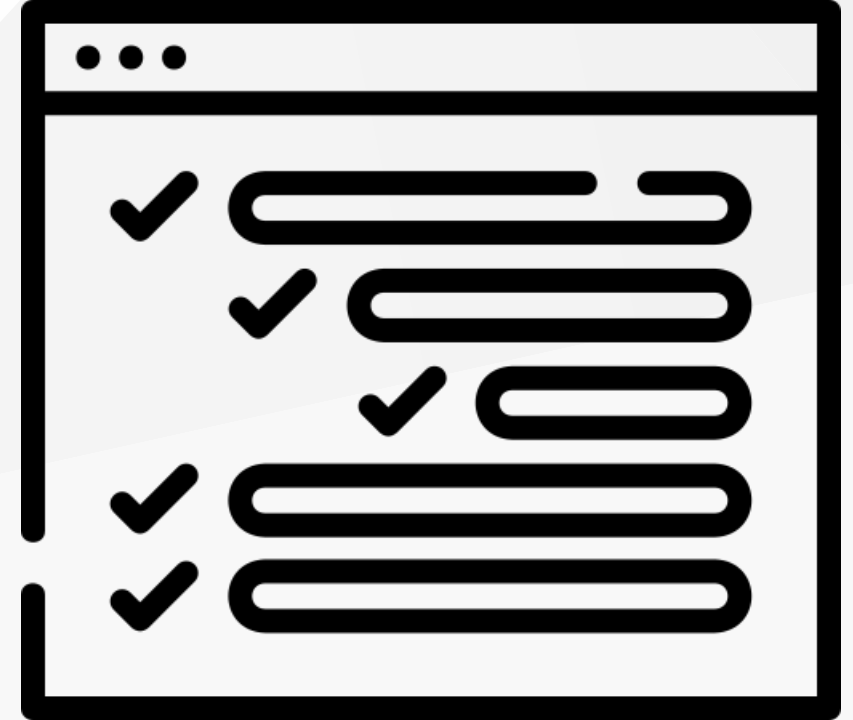


QualvoSec
A minimal security patch framework.



TOC

- Introduction
- Motivation
- Software Overview
 - Server
 - Client
 - Admin
- Communication Overview
- Patch Process Flowchart





Introduction

- Introduced in 2024 by Florian Paul Azim Hoberg @gyptazy
- Daemon not running as root
 - Limited to a specific subset of sudo commands
 - No Agent based code executions
- Pull based
 - Clients pull manifest metadata from server
- Health monitoring endpoint on clients
- Integrated packaging (.deb/.rpm) support by CMake
- Linux and BSD support



Motivation





Software Overview

Software	OS	Lang	Mode
Server	All	Python	Any preconfigured webserver (e.g. nginx) serving the static patch manifest in YAML.
Client	All	Python	Client that pulls metadata and evaluates patch windows.
Admin	All	Python	Administrative tool for creating status overviews, managing systems and patch windows.



Software - Server

YAML based patch manifest file holding all needed information, served on a http/https capable endpoint as a "server".

```
hypervisor01.gyptazy.ch:
  patch: true
  reboot: true
  weekday: 1
  hour: 23
  minute: 30

hypervisor02.gyptazy.ch:      # Defines the remote FQDN of the client system.
  patch: true                 # Defines to patch the system in general.
  reboot: true                # Defines to reboot the system after installing the updates.
  weekday: 2                  # Weekday where the patches should be installed (starting with 0 for Monday).
  hour: 3                     # Hours where the patches should be installed.
  minute: 15                  # Minute where the patches should be installed.
```



Software - Client

- Single daemon (written in Python3)
- Supports different Init-Systems
- Support different log handler

```
[general]
server: https://patching.gyptazy.ch
monitoring: enable
monitoring_port: 8037
monitoring_listener: 127.0.0.1
log_level: CRITICAL
log_handler: SystemdHandler()
```



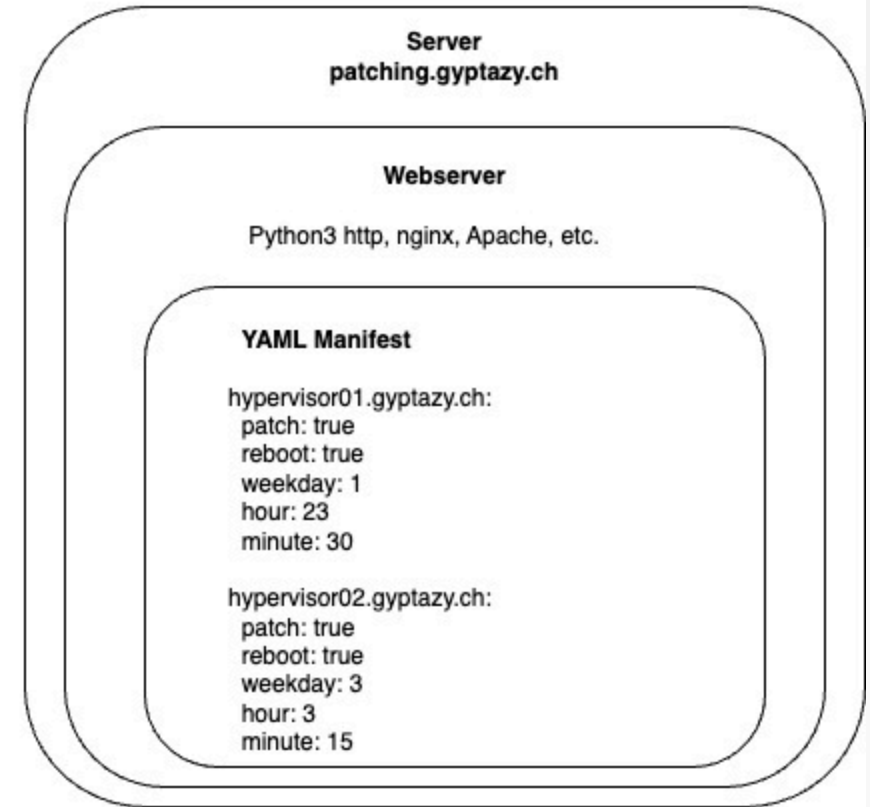
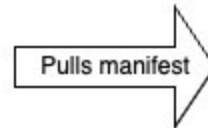
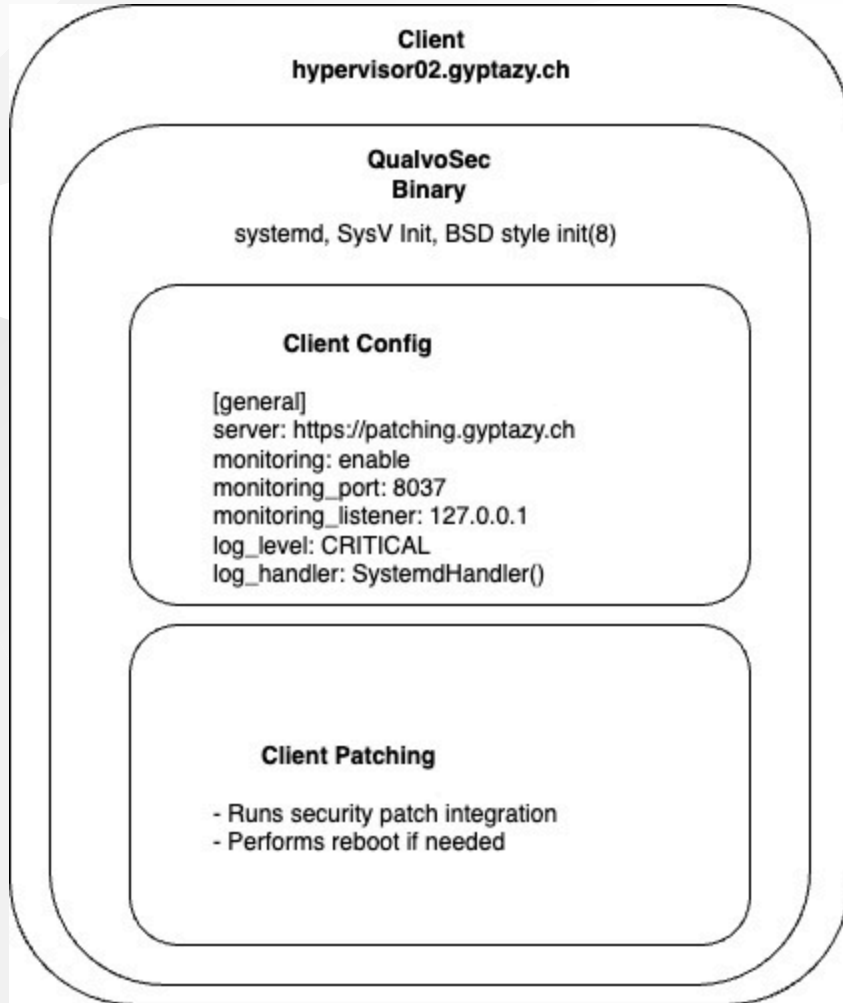
Software - Admin

- Get overview
 - Find orphaned systems
- Add/delete systems for patching

System	Last Seen	Active	Patch Window	Reboot
giro48.gyptazy.ch	2024-02-08	True	Wednesday, 03:15	True
giro49.gyptazy.ch	2024-02-08	True	Friday, 01:15	True
giro50.gyptazy.ch	2024-02-08	True	Sunday, 03:15	True

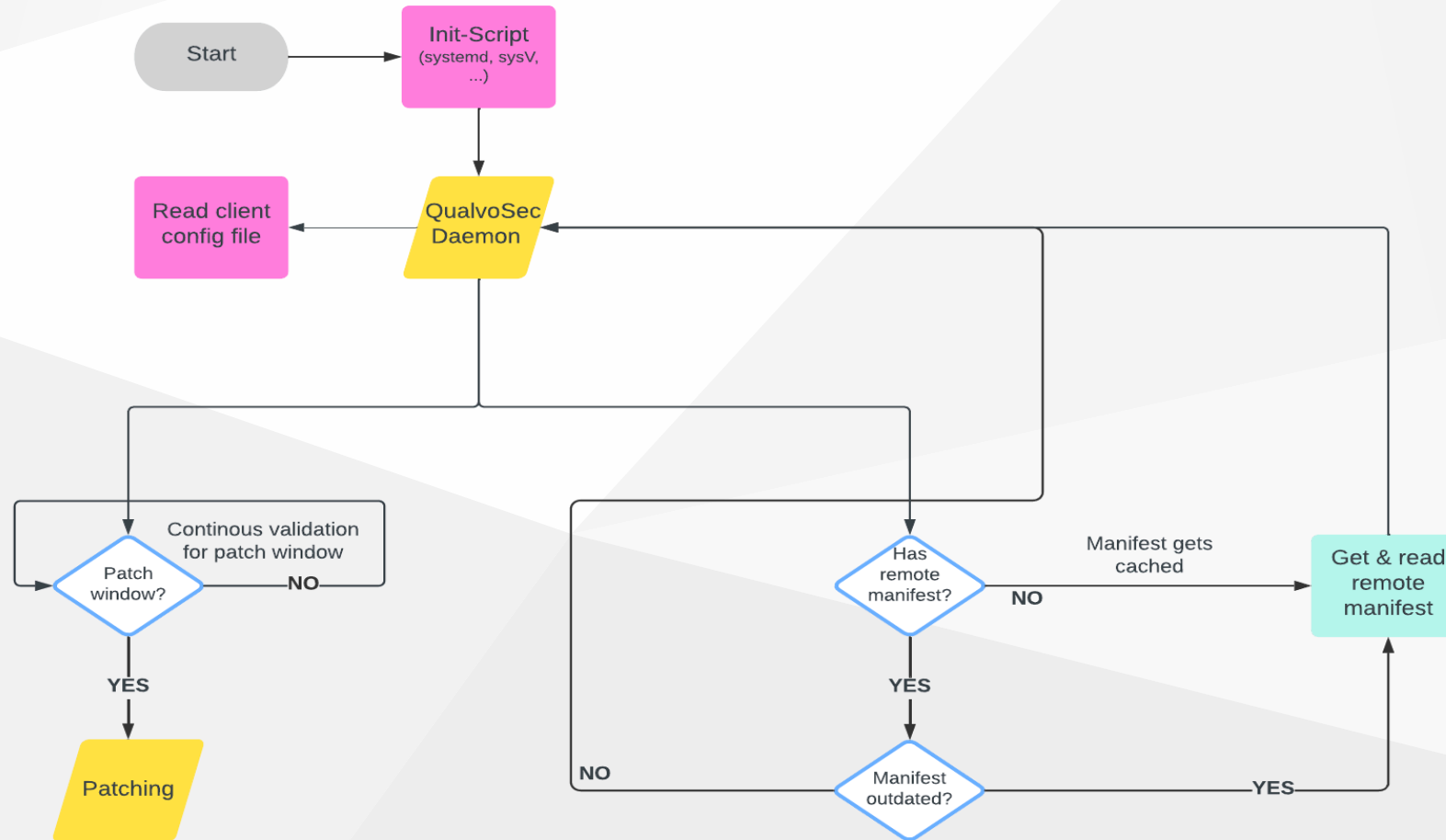


Communication Overview





Patch Process Flowchart





Resources

- Introduction: <https://gyptazy.ch/blog/qualvosec-a-minimalistic-security-patch-management-tools-for-linux-and-bsd/>
- Install HowTo Debian: <https://gyptazy.ch/howtos/howto-install-qualvosec-security-patch-management-on-debian/>
- Sources: <https://github.com/gyptazy/QualvoSec>
- Presentation: <https://gyptazy.ch/talks/>



Thanks!

Blog: <https://gyptazy.ch>
Gemini: gemini://gyptazy.ch
Twitter: @gyptazy
Fediverse: @gyptazy@gyptazy.ch
Matrix: @gyptazy:gyptazy.ch





Credits

- image(annyoing.png): Image from Flaticon.com
- image(more.png): Image from Flaticon.com
- image(gemini_logo.png): Image from Flaticon.com
- image(toc.png): Image from Flaticon.com