MONITORING PROJECT

Handover Document

Grafana - Prometheus - Loki monitoring stack

Delivered and handed over in full to the client.

WHAT THIS DOCUMENT IS

This is the structure of the document delivered at the end of every monitoring project. It records what was built, how to reach it, what each alert means and how to maintain it. The values below are placeholders - your copy is filled in with your own environment.

SCOPE DELIVERED

Servers monitored
[n] Linux hosts

Dashboards built
[n]

Alert rules configured
[n]

Data sources connected
[list]

Log retention
[n] days

Alert channels
[list]

Deployment method
Docker Compose

Admin access
Transferred to client

SECTION 1

Architecture & Access

HOW THE STACK FITS TOGETHER

ACCESS REFERENCE

SERVICE	ADDRESS	PORT	ADMIN HELD BY
Grafana	https://[your-host]	443	Client
Prometheus	internal only	9090	Client
Loki	internal only	3100	Client
Node Exporter	per host, firewalled	9100	Client
Alertmanager	internal only	9093	Client

CREDENTIALS ARE NOT STORED IN THIS DOCUMENT

Passwords, API keys and SSH keys are delivered separately through Upwork messages. Rotate them after handover if you wish - full admin access is yours.

SECTION 2

Dashboards & Alerts

DASHBOARDS DELIVERED

Illustrative panel layout. Your copy contains screenshots of your own dashboards.

ALERT REFERENCE

ALERT	CONDITION	SEVERITY	ACTION
Host down	no scrape 2 min	Critical	Check host and network
CPU high	> 90% for 5 min	Warning	Identify top process
Memory high	> 90% for 5 min	Warning	Check for leaks
Disk filling	> 85% used	Warning	Clear logs, extend volume
Disk critical	> 95% used	Critical	Free space immediately
Service stopped	container not running	Critical	Restart, then check logs
Error rate up	log errors above base	Warning	Search Loki for the trace

EVERY ALERT IS TESTED BEFORE HANDOVER

Each rule is deliberately triggered so you can confirm it fires and reaches your channel.

SECTION 3

Maintenance & Handover

COMMON OPERATIONS

Restart the stack	`docker compose restart`
Check status	`docker compose ps`
View a service log	`docker compose logs -f grafana`
Apply config changes	`docker compose up -d`
Update to newer images	`docker compose pull && docker compose up -d`
Back up dashboards	`export dashboard JSON from the Grafana UI`

EXTENDING THE SETUP

Add a server: install Node Exporter, add the target to the Prometheus scrape config, reload, then add the host to the dashboard variable. Change a threshold: edit the alert rule in Grafana, save, and test it fires. Add a data source: connect it in Grafana, then build panels against it.

NOT INCLUDED - REQUIRES A GRAFANA ENTERPRISE LICENCE

Scheduled PDF reports, SAML single sign-on, fine-grained role-based access control, enterprise data source plugins such as Splunk or ServiceNow, and custom branding. This stack runs the open-source editions, so there are no licence fees.

OPTIONAL ONGOING MANAGEMENT

Most alert tuning happens in the first month, once real traffic shows which thresholds are too sensitive. Ongoing management covers threshold tuning, noise reduction, stack updates and small changes. It is entirely optional - everything here is already yours.