

PSA

SYSTEMÜBERWACHUNG

Mit Prometheus & Grafana.

Agenda

Aufgabe

Anforderungen

Prometheus

Prometheus
Setup
Exporter

Services

Exporter
Unsere Systeme

Grafana

Visualisierung

Alerts

AlertManager
Slack Integration
Unsere Alerts

01

Aufgabe

Systemüberwachung
Anforderungen

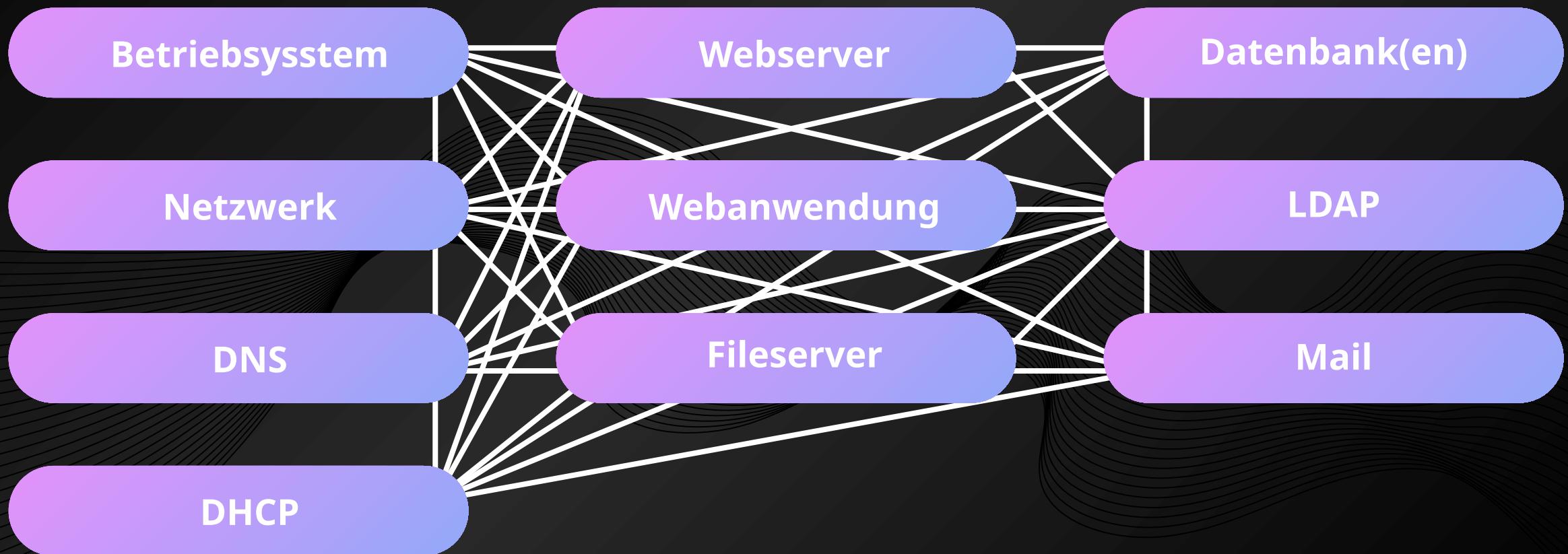


Läuft alles?

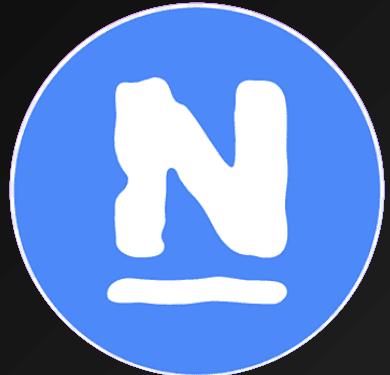
Komplexe System-Strukturen, verteilt auf viele
Maschinen und Services:

Systemüberwachung, nur wie?

Was heißt “alles”?



Große Auswahl.



Nagios

1999

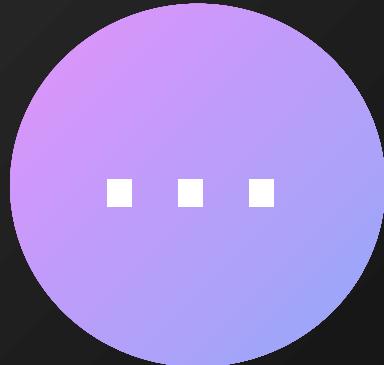
Vom Aufgabenblatt :)
Weit Verbreitet



Prometheus

2012

Industrie-genutzt
Großer Support
Einfache Einrichtung



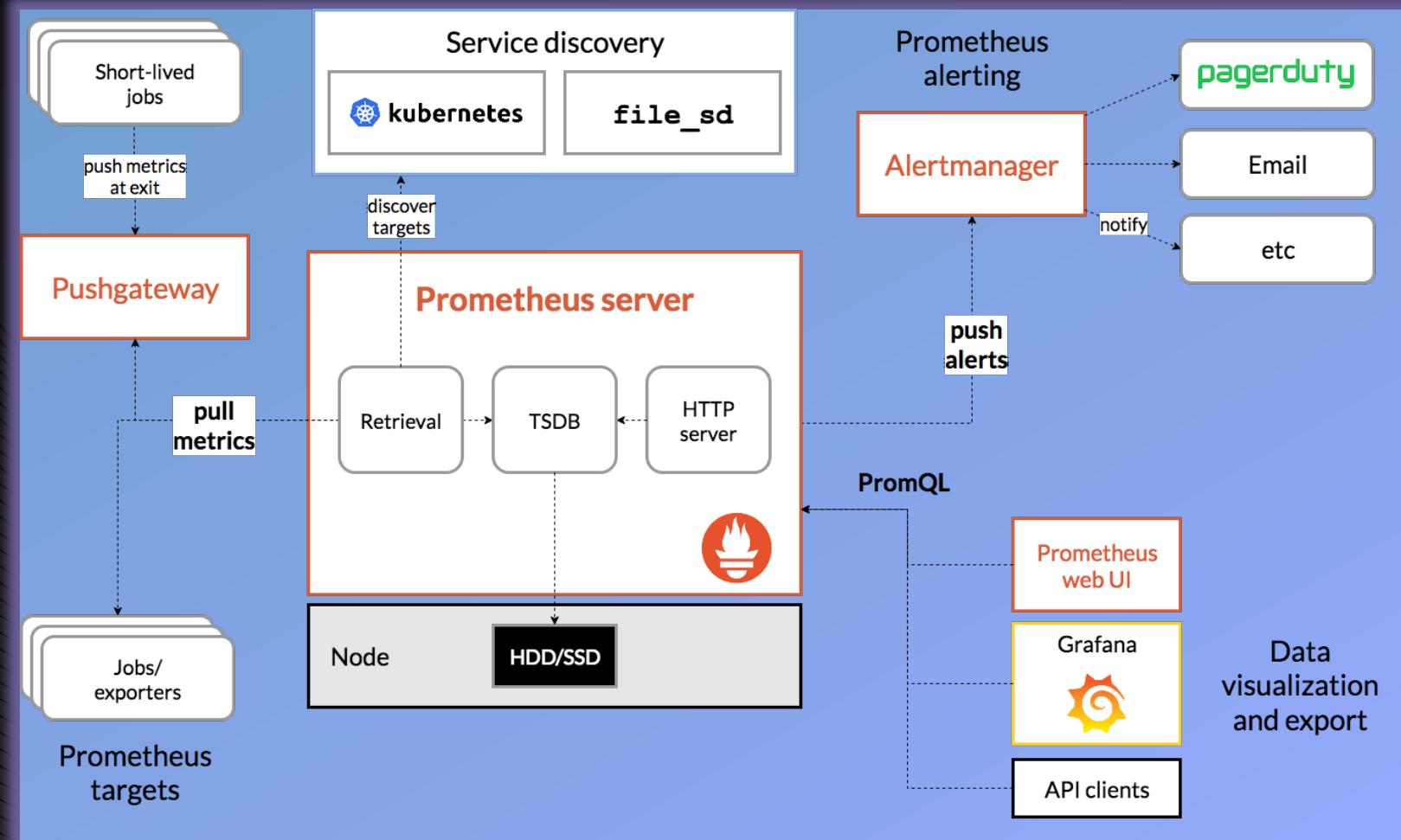
Viele mehr...

02

Prometheus

Architektur
Komponenten
Setup & Installation

Architektur.



Prometheus

Als zentraler Server

Jobs / Exporters

An den Systemen

Grafana

Als visuelles Interface

Alertmanager

Als Alert Manager :P

Prometheus.

The screenshot shows the Prometheus web interface with the following details:

- Header:** Prometheus logo, Query, Alerts, Status > Target health (highlighted), and various UI icons.
- Search and Filter:** Select scrape pool, Filter by target health, and Filter by endpoint or labels.
- Table of Targets:** A list of monitored services with their status and last scrape information.

 - coredns:** 1 / 1 up, Last scrape 14.276s ago, State UP. Endpoint: http://192.168.3.3:9153/metrics. Labels: instance="192.168.3.3:9153", job="coredns".
 - dhcp:** 1 / 1 up, Last scrape 13.296s ago, State UP. Endpoint: http://192.168.3.3:9101/metrics. Labels: instance="192.168.3.3:9101", job="dhcp".
 - fileserver:** 1 / 1 up, Last scrape 25.977s ago, State UP. Endpoint: http://192.168.3.8:9100/metrics. Labels: instance="192.168.3.8:9100", job="fileserver".
 - homeassistant:** 1 / 1 up. (Status is collapsed).
 - mysql-team02:** 1 / 1 up. (Status is collapsed).
 - network:** 20 / 20 up. (Status is collapsed).

Grafana.

Screenshot of a Grafana dashboard titled "06) Database".

The dashboard includes the following sections:

- General Counters, CPU, Memory and File Descriptor Stats:**
 - Version: 17.1.0
 - Start Time: N/A
 - Current fetch data: 19.3 MB
 - Current insert data: 358
 - Current update data: 36
 - Max Connections: 100
- Average CPU Usage:** A line chart showing CPU usage over time. The Y-axis ranges from 2 s to 4 s. The X-axis shows time from 06:00 to 16:00. Data series include CPU Time (Mean: 3.64 s, Last: 4.03 s, Max: 4.03 s, Min: 1.98 s).
- Average Memory Usage:** A line chart showing memory usage over time. The Y-axis ranges from 0 B to 800 kB. The X-axis shows time from 06:00 to 16:00. Data series include Resident Mem (Mean: 483 kB, Last: 588 kB, Max: 798 kB, Min: 225 kB) and Virtual Mem (Mean: 0 B, Last: 0 B, Max: 0 B, Min: 0 kB).
- Open File Descriptors:** A line chart showing open file descriptors over time. The Y-axis ranges from 8 to 9. The X-axis shows time from 06:00 to 16:00. Data series include Open FD (Mean: 8.77, Last: 9, Max: 9, Min: 8).
- Settings:**
 - Shared Buff...: 128 MiB
 - Effective Ca...: 4 GiB
 - Maintenanc...: 64 MiB
 - Work Mem: 4 MiB
 - Max WAL Size: 1.0 GiB
 - Random Pag...: 4
 - Seq ...: 1
 - Max ...: 8
 - Max ...: 8
- Database Stats:** (Partially visible at the bottom)

The left sidebar shows navigation links: Home, Bookmarks, Starred, Dashboards (selected), Playlists, Snapshots, Library panels, Public dashboards, Explore, Alerting, Connections, and Administration.

Alertmanager.

Alertmanager Alerts Silences Status Settings Help

New Silence

Filter Group Receiver: All Silenced Inhibited Muted

Custom matcher, e.g. `env="production"`

+ Silence

+ Expand all groups

- slack Not grouped 2 alerts

2025-01-22T11:31:48.667Z + Info  Source  Silence  Link

alertname="PrometheusTargetMissing" + instance="192.168.3.9:9101" + job="openldap" + severity="critical" +

2025-01-22T11:32:03.667Z + Info  Source  Silence  Link

alertname="PrometheusTargetMissing" + instance="192.168.3.7:9101" + job="postfix" + severity="critical" +

Installation.

Docker

Firewall

Konfiguration

```
# monitoring-config.nix
{ config, lib, pkgs, ... }:
{
  virtualisation.docker.enable = true;
  users.extraGroups.docker.members = [ "root" ];
}
```

NixOS

Docker aktivieren, fertig.

Installation.

Docker

```
# Create the directory structure
mkdir -p /root/docker/alert-manager
mkdir -p /root/docker/grafana
mkdir -p /root/docker/prometheus
mkdir -p /root/docker/blackbox

# Create the config files
touch /root/docker/docker-compose.yaml
touch /root/docker/alert-manager/alertmanager.yml
touch /root/docker/grafana/grafana.ini
touch /root/docker/prometheus/alert-rules.yml
touch /root/docker/prometheus/prometheus.yml
touch /root/docker/blackbox/blackbox.yml
```

Firewall

Konfiguration

Neue Directories

Für jeden Service

Config-Dateien

In den neuen Pfaden

Installation.

Docker

```
# docker-compose.yml
services:
    # Prometheus zur Metriken-Sammlung
    prometheus:
        image: prom/prometheus
        ports:
            - '9090:9090'
        volumes:
            - /root/docker/prometheus:/etc/prometheus
        command:
            - '--config.file=/etc/prometheus/prometheus.yml'
            - '--web.enable-lifecycle'
        restart: unless-stopped

    # Grafana zur Visualisierung
    grafana:
        image: grafana/grafana
        ports:
            - '3000:3000'
        depends_on:
            - prometheus
        restart: unless-stopped
        environment:
            - HTTP_PROXY=http://proxy.cit.tum.de:8080/
            - HTTPS_PROXY=http://proxy.cit.tum.de:8080/
            - NO_PROXY=localhost,127.0.0.1,prometheus
        volumes:
            - grafana-storage:/var/lib/grafana

    # Alertmanager zur Alarmierung bei Fehlern
    alertmanager:
        image: prom/alertmanager
        ports:
            - "9093:9093"
        volumes:
            - /root/docker/alert-manager:/config
        command: --config.file=/config/alertmanager.yml --log.level=debug

    # Blackbox Exporter zur Überwachung von Webseiten
    blackbox:
        image: prom/blackbox-exporter:latest
        ports:
            - 9115:9115
        volumes:
            - /root/docker/blackbox:/etc/blackbox
        command:
            - --config.file=/etc/blackbox/blackbox.yml
        depends_on:
            - prometheus
        restart: unless-stopped
        environment:
            - HTTP_PROXY=http://proxy.cit.tum.de:8080/
            - HTTPS_PROXY=http://proxy.cit.tum.de:8080/
            - NO_PROXY=localhost,127.0.0.1,blackbox

volumes:
    grafana-storage: {}
```

Prometheus

port 9090
config.file

Grafana

port 3000
abhängig von Prometheus
proxy Einstellungen

Alertmanager

port 9093
config.file

Blackbox

port 9115
config.file
abhängig von Prometheus

Installation.

Docker

Firewall

Konfiguration

```
docker compose up -d
```

Docker

Start nach Firewall & Konfiguration.

Installation.

Docker

Firewall

Konfiguration

```
iptables -A INPUT -p tcp --dport 9100 -j ACCEPT  
iptables -A INPUT -p tcp --dport 9090 -j ACCEPT  
iptables -A OUTPUT -p tcp --dport 9100 -j ACCEPT  
iptables -A OUTPUT -p tcp --dport 9090 -j ACCEPT  
...
```

Firewall

Erlauben aller nötigen Verbindungen

Installation.

Docker

Firewall

Konfiguration

```
# prometheus.yml
global:
  scrape_interval: 15s
  evaluation_interval: 15s
scrape_configs:
  # Prometheus selbst als Beispiel
  - job_name: 'prometheus'
    scrape_interval: 5s
    static_configs:
      - targets: ['localhost:9090']
```

Prometheus

Update-Rate, etc.

Jobs

Alle angehängten Jobs, die beobachtet werden sollen.

03

Unsere Services

Exporter
Installation & Setup

Installation.

```
# os-expoerter.nix
{ config, lib, pkgs, ... }:
{
  services.prometheus.exporters.node = {
    enable = true;
    port = 9100;
    enabledCollectors = [
      "logind"
      "systemd"
    ];
    disabledCollectors = [
      "textfile"
    ];
    openFirewall = true;
  };
}
```

NixOS-Config
.nix

Default Exporter
enable
port

weitere Konfigurationen

Installation.

```
# prometheus.yml  
...  
scrape_configs:  
...  
- job_name: 'os-status'  
  static_configs:  
    - targets:  
      - '192.168.3.1:9100' #vm1  
      - '192.168.3.2:9100' #vm2  
      - '192.168.3.3:9100' #router  
      # database, homeassistant up over own exporter  
      - '192.168.3.6:9100' #webserver  
      - '192.168.3.7:9100' #fileserver
```

NixOS-Config

.nix

Job

name
targets

Zum Überwachen.

Betriebssysteme

Webserver

Datenbank(en)

Netzwerk

Webanwendung

LDAP

DNS

Fileserver

Mail

DHCP

Zum Überwachen.

Betriebssysteme & Fileserver

```
# os-exporter.nix
{ config, lib, pkgs, ... }:
{
  services.prometheus.exporters.node = {
    enable = true;
    port = 9100;
    enabledCollectors = [
      "logind"
      "systemd"
    ];
    disabledCollectors = [
      "textfile"
    ];
    openFirewall = true;
  };
}
```

Zum Überwachen.

Netzwerk

```
# prometheus.yml
...
- job_name: 'network'
  metrics_path: /probe
  params:
    module: [ping] # Look for a HTTP 200 response.
  static_configs:
    - targets:
        - vm1.psa-team03.cit.tum.de
        - vm2.psa-team03.cit.tum.de
        - router.psa-team03.cit.tum.de
        - database.psa-team03.cit.tum.de
        - homeassistant.psa-team03.cit.tum.de
        - vm6.psa-team03.cit.tum.de
        - ldap.psa-team03.cit.tum.de
        - fileserver.psa-team03.cit.tum.de
        - mail.psa-team03.cit.tum.de
        - monitoring.psa-team03.cit.tum.de
  # team routers
    - vm001.psa-team01.cit.tum.de
    - vm1.psa-team02.cit.tum.de
    - vm4.psa-team02.cit.tum.de
    - vm04-02.psa-team04.cit.tum.de
    - vm01.psa-team05.cit.tum.de
    - shika.psa-team06.cit.tum.de
    - vm1.psa-team07.cit.tum.de
    - router.psa-team08.cit.tum.de
    - ns01.psa-team09.cit.tum.de
    - vm02.psa-team10.cit.tum.de
  relabel_configs:
    - source_labels: [__address__]
      target_label: __param_target
    - source_labels: [__param_target]
      target_label: instance
    - target_label: __address__
      replacement: blackbox:9115 # muss blackbox:9115 sein
```

Zum Überwachen.

DNS

```
{ ... }:  
{  
    services.coredns = {  
        enable = true;  
        config = ''  
        (default) {  
            bind enp0s8  
            root /etc/nixos/dns  
            log  
            prometheus :9153  
        }  
    ...  
}
```

Zum Überwachen.

DHCP

&

...

```
...  
  "control-socket": {  
    "socket-type": "unix",  
    "socket-name": "/run/kea/kea-dhcp4.socket"  
  },  
...
```

```
{ config, lib, pkgs, ... }:  
{  
  services.prometheus.exporters.node = {  
    enable = true;  
    port = 9100;  
    enabledCollectors = [  
      "logind"  
      "systemd"  
    ];  
    disabledCollectors = [  
      "textfile"  
    ];  
    openFirewall = true;  
  };  
  services.prometheus.exporters.kea = {  
    enable = true;  
    targets = ["/run/kea/kea-dhcp4.socket"];  
    port = 9101;  
  };  
}
```

Zum Überwachen.

Webanwendung

```
cadvisor:  
  container_name: cadvisor  
  image: gcr.io/cadvisor/cadvisor  
  volumes:  
    - /:/rootfs:ro  
    - /var/run:/var/run:rw  
    - /sys:/sys:ro  
    - /var/lib/docker/:/var/lib/docker:ro  
    - /dev/disk/:/dev/disk:ro  
  ports:  
    - "8080:8080"  
  restart: unless-stopped  
  devices:  
    - /dev/kmsg  
  privileged: true
```

Zum Überwachen.

Webserver

```
# prometheus.yml
...
- job_name: 'webserver'
  metrics_path: /probe
  params:
    module: [http_2xx] # Look for a HTTP 200 response.
  static_configs:
    - targets:
        - http://web1.psa-team03.cit.tum.de
        - https://web1.psa-team03.cit.tum.de
        - https://web2.psa-team03.cit.tum.de
        - https://web3.psa-team03.cit.tum.de
  relabel_configs:
    - source_labels: [__address__]
      target_label: __param_target
    - source_labels: [__param_target]
      target_label: instance
    - target_label: __address__
      replacement: 192.168.3.6:9102 # muss blackbox:9115 sein
```

```
# blackbox.yml
modules:
  http_2xx:
    prober: http
    timeout: 5s
  http:
    valid_http_versions: ["HTTP/1.1", "HTTP/2.0"]
    valid_status_codes: []
    method: GET
    follow_redirects: true
    fail_if_ssl: false
    fail_if_not_ssl: false
    tls_config:
      insecure_skip_verify: true
    preferred_ip_protocol: "ip4" # defaults to "ip6"
    ip_protocolFallback: false # no fallback to "ip6"
ping:
  prober: icmp
  timeout: 5s
  icmp:
    preferred_ip_protocol: "ip4"
```

Zum Überwachen.

Datenbank(en)

&

```
# database.nix & database-backup.nix
services.prometheus.exporters.postgres = {
    enable = true;
    port = 9100;
    runAsLocalSuperUser = true;
};
```

```
services.prometheus.exporters.script = {
    enable = true;
    port = 9100;
    settings.scripts = [
        { name = "db-check"; script = "nc -zv 192.168.4.5 3306"; }
    ];
};
```

Zum Überwachen.

LDAP

```
git clone https://github.com/jcollie/openldap_exporter.git  
cd openldap_exporter  
virtualenv --python=/usr/bin/python2 /opt/openldap_exporter  
/opt/openldap_exporter/bin/pip install --requirement requirements.txt  
cp openldap_exporter.py /opt/openldap_exporter  
cp openldap_exporter.yml /opt/openldap_exporter  
vi /opt/openldap_exporter/openldap_exporter.yml  
  
# edit configuration file  
cp openldap_exporter.service /etc/systemd/system  
systemctl daemon-reload  
systemctl enable openldap_exporter  
systemctl start openldap_exporter  
  
docker build . -t openldap_exporter
```

Zum Überwachen.

Mail

```
services.prometheus.exporters.postfix = {  
    enable = true;  
    port = 9154;  
    ...  
};
```

Zeit für eine
Live-Demo!

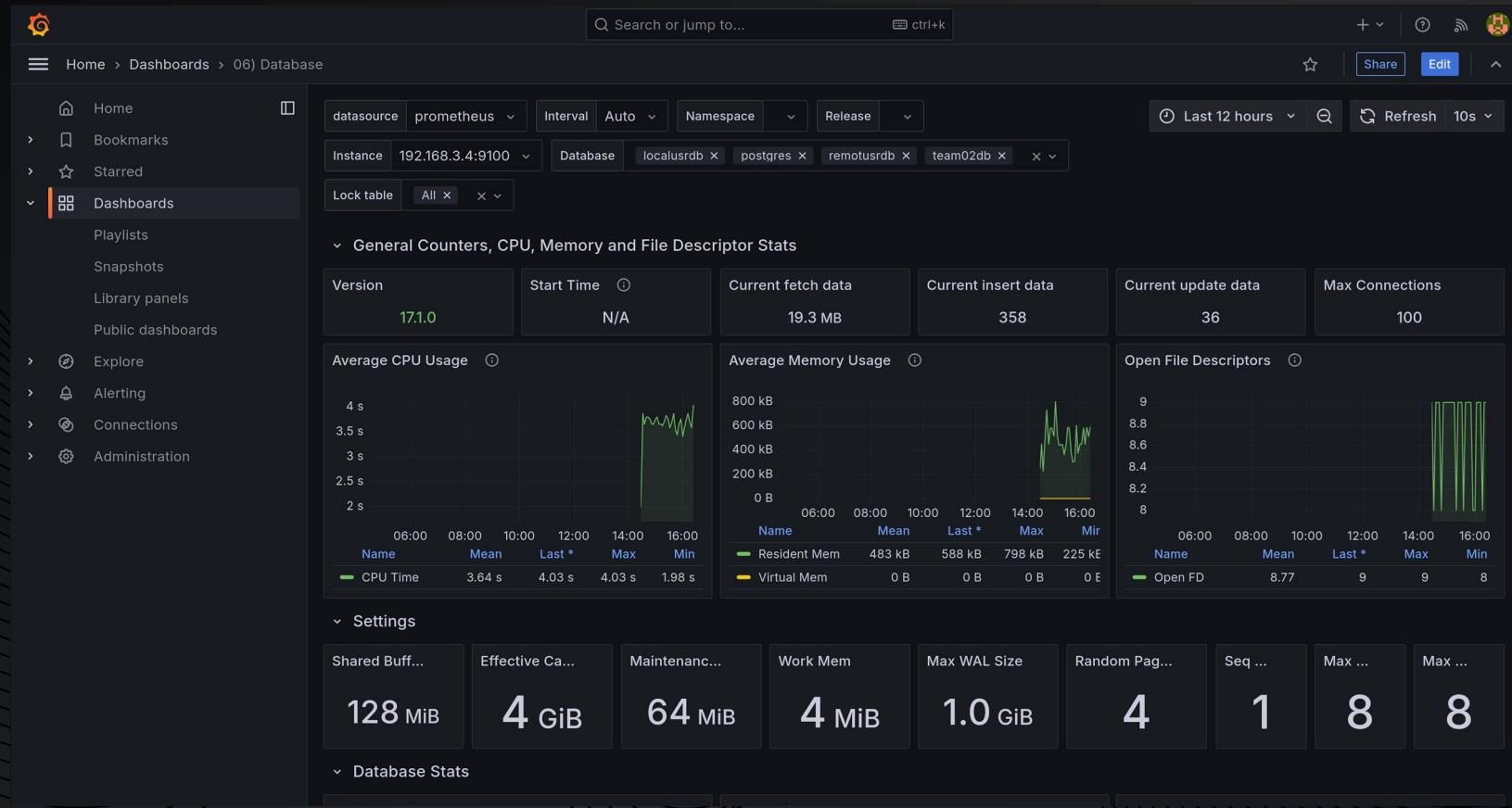
The background features a dark gray gradient with two prominent, thin black wavy lines that curve from the bottom left and right towards the center. A central rectangular area is defined by these lines, containing the main text.

04

Grafana

Visualisierung

Grafana.



Plattformübergreifend

Nicht Prometheus spezifisch.
Bsp. MySQL, Graphite, ...

Grafische Darstellung

Von allerlei Daten.
Unterteilung in Dashboards.
Viele vorkonfigurierte Elemente.

Konfiguration.

Erster Start

Dashboards

Out-of-the-Docker

Web-Interface auf
<http://131.159.74.56:60313/>

Login

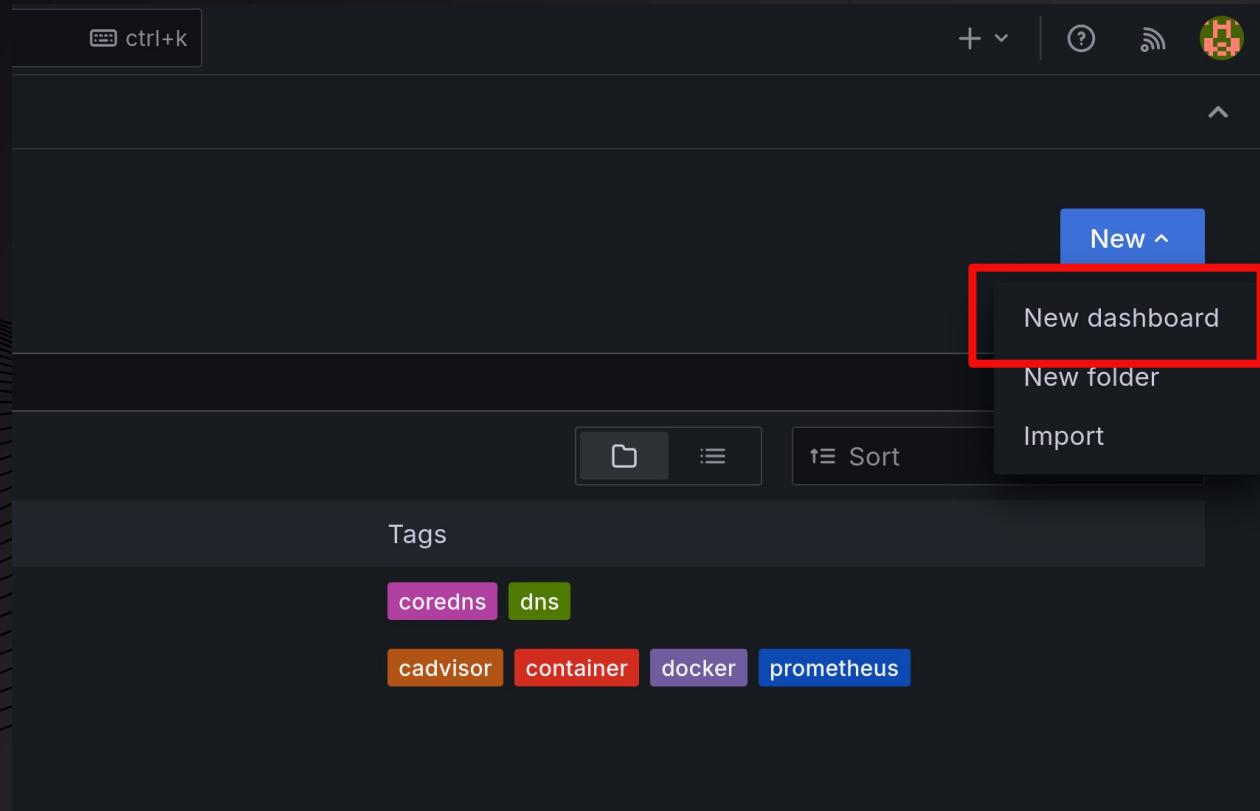
Erster Login:
Username: admin
Passwort: admin

Neues Passwort vergeben, fertig.

Konfiguration.

Erster Start

Dashboards



Neues Dashboard

Hinzufügen

Konfiguration.

Erster Start

Dashboards

Start your new dashboard by adding a visualization

Select a data source and then query and visualize your data with charts, stats and tables or create lists, markdowns and other widgets.

+ Add visualization

Import panel

Add visualizations that are shared with other dashboards.

+ Add library panel

Import a dashboard

Import dashboards from files or [grafana.com](#).

Import dashboard

Neues Dashboard

Hinzufügen

Import / Selbst Bauen

Dashboard Art Angeben
Importieren, oder selbst bauen

Konfiguration.

Erster Start

Dashboards

Import dashboard

Import dashboard from file or Grafana.com

Upload dashboard JSON file
Drag and drop here or click to browse
Accepted file types: .json, .txt

Find and import dashboards for common applications at [grafana.com/dashboards](#)

Grafana.com dashboard URL or ID Load

Import via dashboard JSON model

```
{  
  "title": "Example - Repeating Dictionary variables",  
  "uid": "_0HnEoN4z",  
  "panels": [...]  
}  
...
```

Load Cancel

Neues Dashboard

Hinzufügen

Import / Selbst Bauen

Dashboard Art Angeben
Importieren, oder selbst bauen

Konfiguration.

Erster Start

The screenshot shows the Grafana search interface with the query 'postgresql'. The results are filtered by 'Data Source: All' and 'Collector Types: All'. The results are as follows:

- Prometheus PostgreSQL Database
- Prometheus PostgreSQL Exporter Quickstart and Dashboard
- Prometheus PostgreSQL Exporter
- Prometheus PostgreSQL Overview (Postgres_exporter)
- Prometheus PostgreSQL Statistics
- Prometheus Loki Postgresql

At the bottom, there is a section for sharing dashboards and a link to 'Share your dashboards'.

Dashboards

Neues Dashboard
Hinzufügen

Import / Selbst Bauen
Dashboard Art Angeben
Importieren, oder selbst bauen

Suche Dashboards
<https://grafana.com/grafana/dashboards/>

Zeit für eine
Live-Demo!

The background features a dark gray gradient with two prominent, thin black wavy lines that curve from the bottom left and right towards the center. A central rectangular area is defined by these lines, containing the main text.

05

Alerts

AlertManager
Slack Integration
Unsere Alerts

Konfiguration.

alertmanager.yml

Route

Wer? Welche Art?

Receiver

Receiver Konfiguration

Slack

alert.rules.yml

```
# alertmanager.yml
route:
  receiver: slack
  repeat_interval: 1m
receivers:
  - name: slack
    slack_configs:
      - channel: "#all-praktikum-system-administration-ws2425"
        send_resolved: true
        api_url: "https://hooks.slack.com/services/"
        title: Alert
        text: >-
          {{ range .Alerts -}}
          *Alert:{{ .Annotations.title }}{{ if .Labels.severity }} - `{{ .Labels.severity }}`{{ end }}
          *Description:{{ .Annotations.description }}
          *Details:{{ range .Labels.SortedPairs }} • *{{ .Name }}:{{ .Value }}`{{ end }}`
```

Konfiguration.

alertmanager.yml

Slack App

Neue Slack App

Webhook

Webhook einrichten

Slack

alert.rules.yml

PSA-Alerters Incoming Webhooks

Activate Incoming Webhooks Incoming webhooks are a simple way to post messages from external sources into Slack. They make use of normal HTTP requests with a JSON payload, which includes the message and a few other optional details. You can include message attachments to display richly-formatted messages.

Adding incoming webhooks requires a bot user. If your app doesn't have a bot user, we'll add one for you.

Each time your app is installed, a new Webhook URL will be generated.

If you deactivate incoming webhooks, new Webhook URLs will not be generated when your app is installed to your team. If you'd like to remove access to existing Webhook URLs, you will need to Revoke All OAuth Tokens.

Webhook URLs for Your Workspace To dispatch messages with your webhook URL, send your message in JSON as the body of an application/json POST request.

Add this webhook to your workspace below to activate this curl example.

Sample curl request to post to a channel:

```
curl -X POST -H 'Content-type: application/json' --data '{"text":"Hello, World!"}' https://hooks.slack.com/services/
```

Webhook URL **Channel** **Added By**

https://hooks.slack.com <input type="button" value="Copy"/>	#all-praktikum-system-administration-ws2425	timon.ensel
---	---	-------------

Konfiguration.

alertmanager.yml

Alert Rule Datei

Wo?

Alertmanager

Target angeben.

Slack

alert.rules.yml

```
# prometheus.yml
rule_files:
  - "alert.rules.yml"
alerting:
  alertmanagers:
    - static_configs:
      - targets: ["alertmanager:9093"]
```

Konfiguration.

alertmanager.yml

Gruppe

Name.
Regeln.

Alert

Titel.
Beschreibung.
Level.

Slack

alert.rules.yml

```
# alert.rules.yml
groups:
  - name: <Gruppen-Name>
    rules:
      - alert: <Alert-Titel>
        expr: <Bedingung>
        for: <Dauer>
        labels:
          severity: <Level>
        annotations:
          summary: <Kurz-Beschreibung>
          description: <Beschreibung>
```

Konfiguration.

alertmanager.yml

Slack

alert.rules.yml

Alert

Name.
Expression (Regel).
Dauer.
Level.
Beschreibung.

```
# alert.rules.yml
  - alert: PostgresqlDown
    expr: pg_up == 0
    for: 0m
    labels:
      severity: critical
    annotations:
      summary: Postgresql down (instance {{ $labels.instance }})
      description: "Postgresql instance is down\n  VALUE = {{ $value }}\n  LA
```

Alert! - Prometheus

The screenshot shows the Prometheus Alerting interface. At the top left is the Prometheus logo. To its right is the text "Prometheus" and a file path "/etc/prometheus/alert.rules.yml". On the far right are several icons: sun/moon, user, gear, book, and three horizontal lines. Below this header, there are two alert cards. The first card is for "PrometheusJobMissing" and has a green vertical bar on the left. It shows "FIRING (2)" in a red button and "INACTIVE (16)" in a green button. The second card is for "PrometheusTargetMissing" and has a red vertical bar on the left. It also shows "FIRING (2)" in a red button and "INACTIVE (16)" in a green button. Both cards have a small downward arrow icon at the bottom right.

Prometheus /etc/prometheus/alert.rules.yml

FIRING (2) INACTIVE (16)

PrometheusJobMissing

PrometheusTargetMissing

FIRING (2)

Alert! - Alertmanager

The screenshot shows the Alertmanager web interface. At the top, there is a navigation bar with links for Alertmanager, Alerts, Silences, Status, Settings, and Help. On the far right of the navigation bar is a blue button labeled "New Silence". Below the navigation bar, there are two tabs: "Filter" (selected) and "Group". To the right of these tabs are filter options: "Receiver: All", "Silenced" (unchecked), "Inhibited" (unchecked), and "Muted" (unchecked). A "Custom matcher, e.g. `env="production"`" input field is present, along with a blue "+" button and a "Silence" button with a speaker icon.

Below the filter section, there is a "Expand all groups" link. Under the "slack" receiver, which is currently "Not grouped", there are two alerts listed:

- 2025-01-22T11:31:48.667Z** [+ Info](#) [Source](#) [Silence](#) [Link](#)
alertname="PrometheusTargetMissing" [+](#) instance="192.168.3.9:9101" [+](#) job="openldap" [+](#) severity="critical" [+](#)
- 2025-01-22T11:32:03.667Z** [+ Info](#) [Source](#) [Silence](#) [Link](#)
alertname="PrometheusTargetMissing" [+](#) instance="192.168.3.7:9101" [+](#) job="postfix" [+](#) severity="critical" [+](#)

Alert! - Slack

 AlertManager APP 6:06 PM

[RESOLVED] InstanceDown for (severity="critical")

Alert: Instance localhost:9100 down - **critical**

Description: localhost:9100 of job node_exporter has been down for more than 1 minute.

Details:

- alertname: `InstanceDown`
- instance: `localhost:9100`
- job: `node_exporter`
- severity: `critical`

Alert: Instance localhost:9091 down - **critical**

Description: localhost:9091 of job prom_middleware has been down for more than 1 minute.

Details:

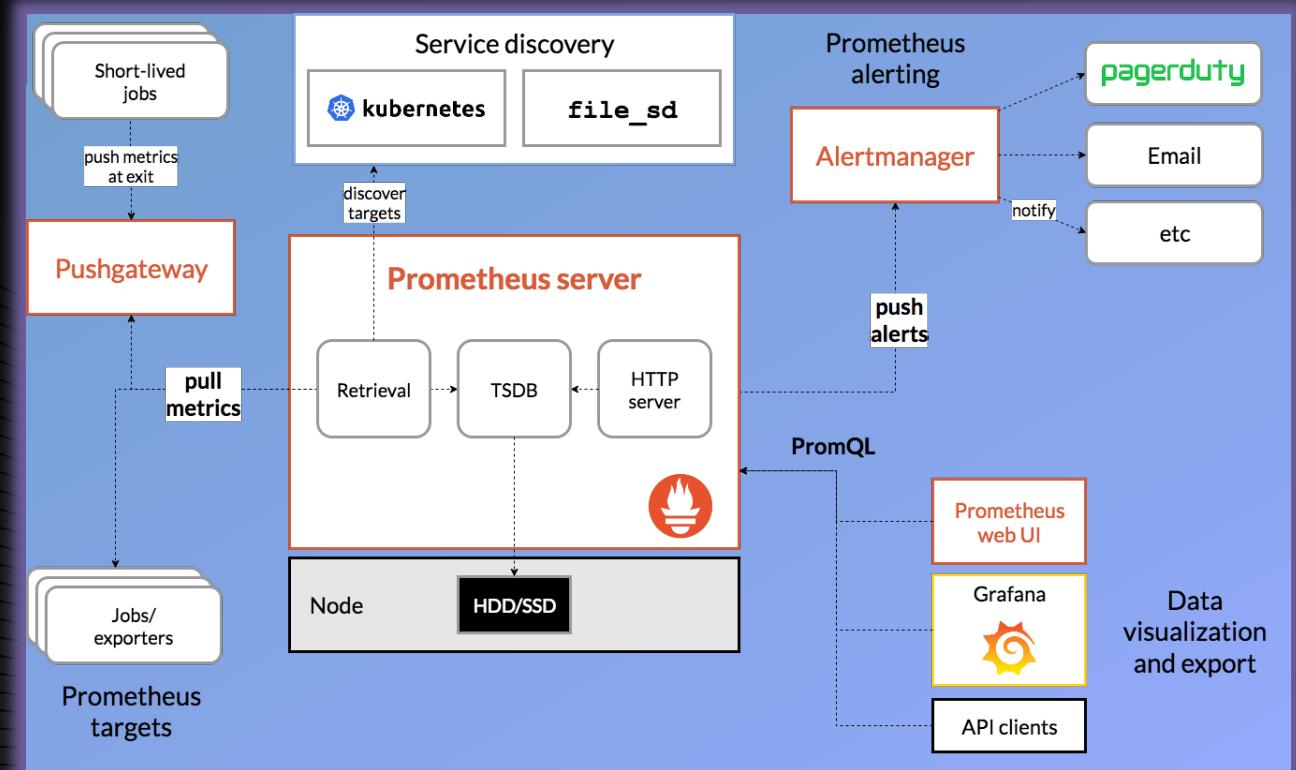
- alertname: `InstanceDown`
- instance: `localhost:9091`
- job: `prom_middleware`
- severity: `critical`

Show less

Danke!

Fragen?

Benjamin Liertz
Timon Ole Ensel



Credits.

Presentation Template: [SlidesMania](#)

Sample Images: [Unsplash](#)

Fonts used in this presentation: DM Sans