



Co-funded by the Horizon 2020
 Framework Programme of the European Union
 Grant Agreement Number 825532

Large-scale EXecution for Industry & Society



  www.lexis-project.eu

MONITORING WITH
 PROMETHEUS AND
 GRAFANA

www.lexis-project.eu

FREDERIC DONNAT

OUTPOST24



100% OPEN SOURCE - Conférences et Workshops



Co-funded by the Horizon 2020
Framework Programme of the European Union
Grant Agreement Number 825532

Large-scale EXecution for Industry & Society



  www.lexis-project.eu

Topic:	HPC and Big Data enabled Large-scale Test-beds and Applications
Topic identifier:	ICT-11-2018-2019
Type of action:	IA Innovation action
Scope:	<p>11a) targeting the development of large-scale HPC-enabled industrial pilot test-beds supporting big data applications and services by combining and/or adapting existing relevant technologies (HPC/BD/cloud) in order to handle and optimize the specific features of processing very large data sets. The industrial pilot test-beds should handle massive amounts of diverse types of big data coming from a multitude of players and sources and clearly demonstrate how they will generate innovation and large value creation. The proposal shall describe the data assets available to the test-beds and, as appropriate, the standards it intends to use to enable interoperability. Pilot test-beds should also aim to provide, via the cloud, simple secure access and secure service provisioning of highly demanding data use cases for companies and especially SMEs.</p>
Project Coordinator:	Jan Martinovič, IT4Innovations, VSB-TU Ostrava
Budget:	14,036,272.5 euro
EC Contribution:	12,218,545.5 euro
Partners:	16
Project duration:	January 2019 – December 2021



Co-funded by the Horizon 2020
 Framework Programme of the European Union
 Grant Agreement Number 825532

Large-scale EXecution for Industry & Society



  www.lexis-project.eu

Topic: HPC and Big Data enabled Large-scale Test-beds and Applications

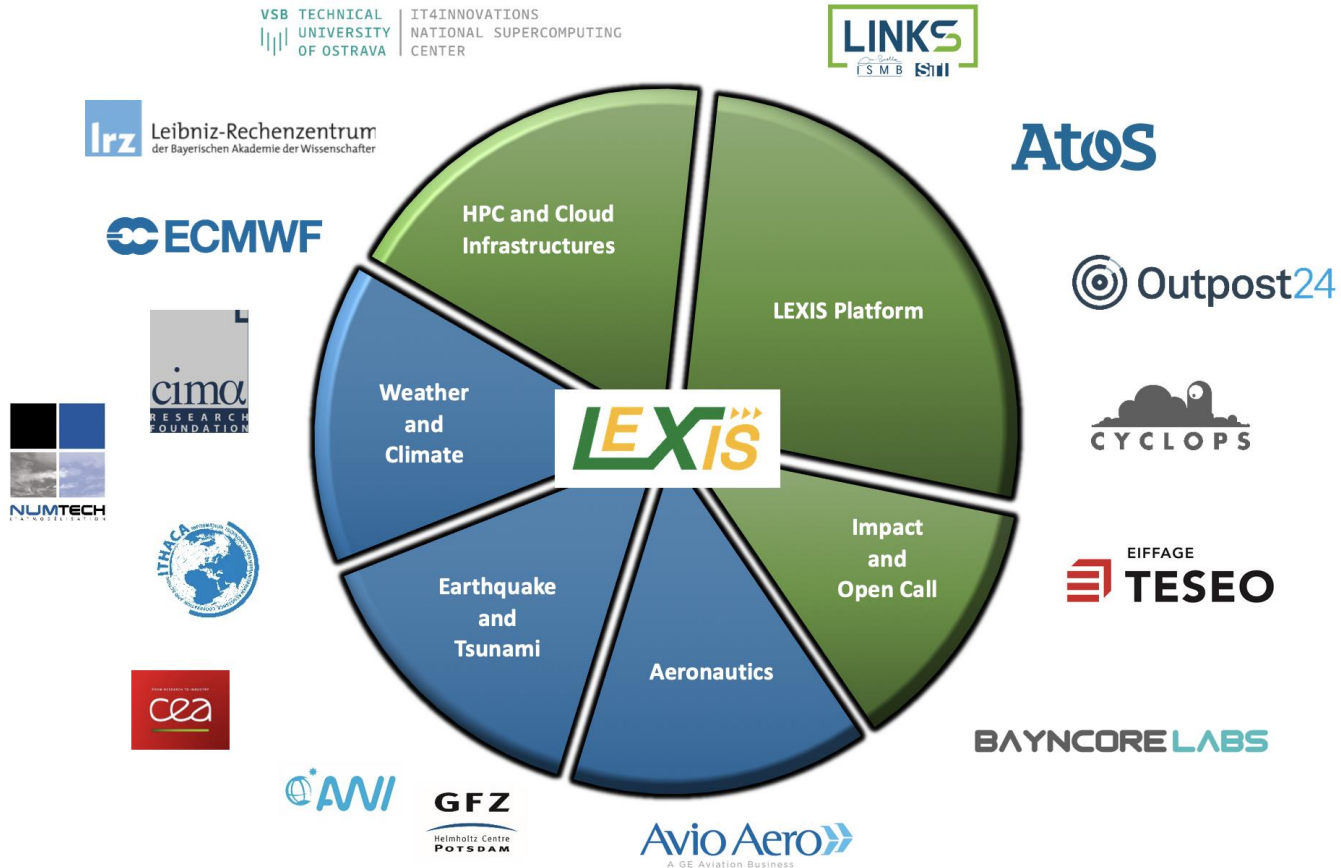
Topic: **LEXIS project builds an advanced engineering platform at the confluence of HPC, Cloud and Big Data which leverages large-scale geographically-distributed resources from existing HPC infrastructure, employ Big Data analytics solutions and augments them with Cloud services.**

Scope: **Driven by the requirements of the pilots, the LEXIS platform builds on best of breed data management solutions (EUDAT) and advanced distributed orchestration solutions (TOSCA), augmenting them with new efficient hardware capabilities in the form of Data Nodes and federation, usage monitoring and accounting/billing supports to realize an innovative solution.**

Project duration: January 2019 - December 2021

ng big
 logies
 e data
 g data
 nerate
 e test-
 t-beds
 ing of

LEXIS CONSORTIUM



COMPANY DESCRIPTION 1/2



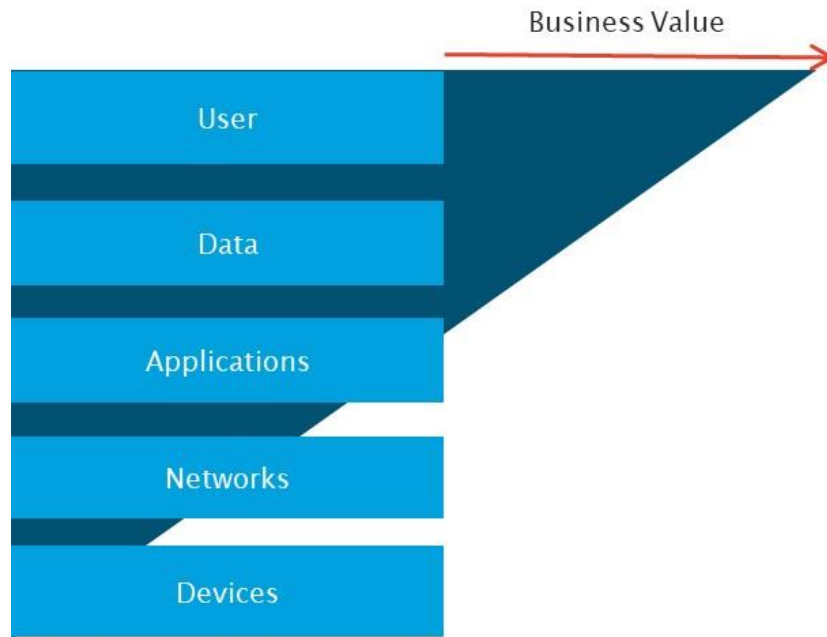
We don't think it's fair that businesses are targets of cybercriminals. As a leading cyber assessment company, we're on a mission to help our customers tighten their cyber exposure before their business can be disrupted. Our ethical hackers and the tools they've created provide a complete view of your security posture with solution-based insights that facilitate and prioritize remediation efforts.

Objective

Secure the assets that improve business resilience

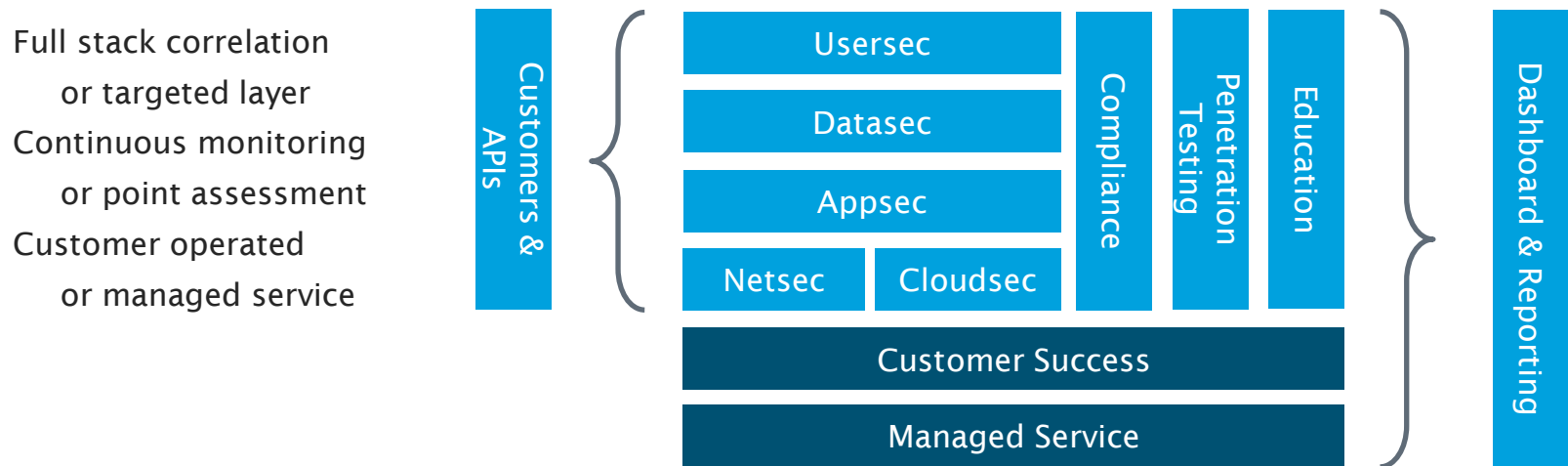
Shifts

- Move beyond owned infrastructure assessment, assess cloud workloads
- Integrate application security testing, and combine with container assessments
- Evaluate data access rights, user access levels then correlate systems, data, and users



MAIN COMPETENCES/SKILLS

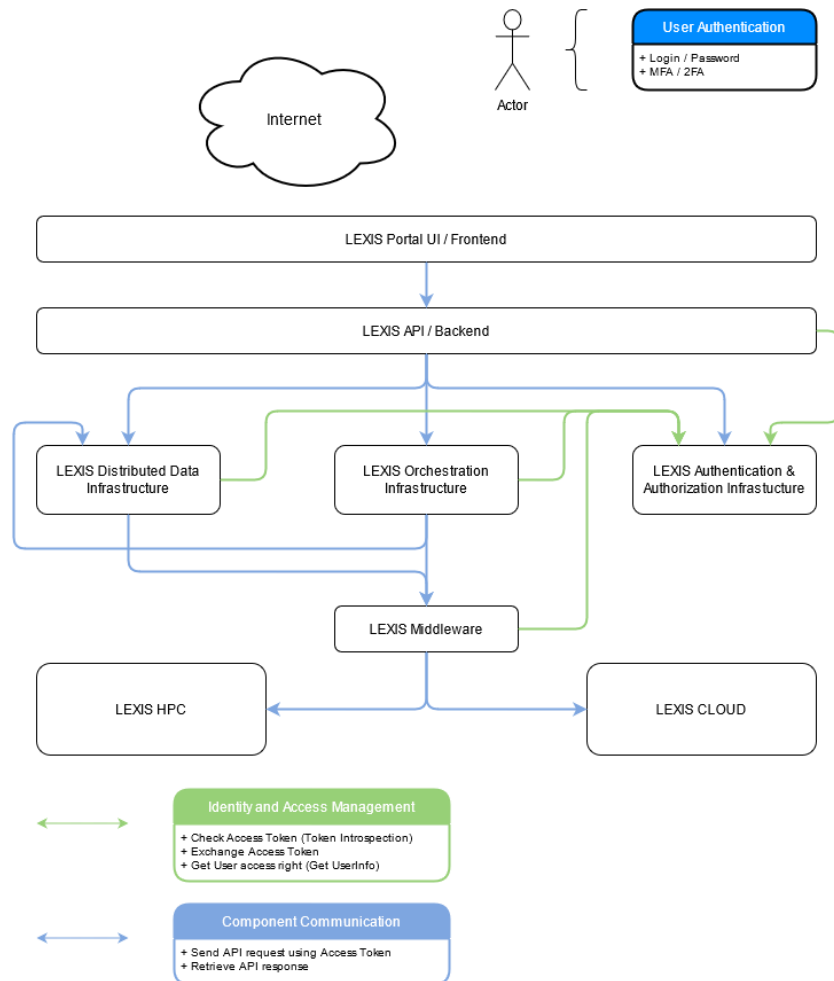
- Full Stack Cyber Exposure Assessment



SECURITY CORNER

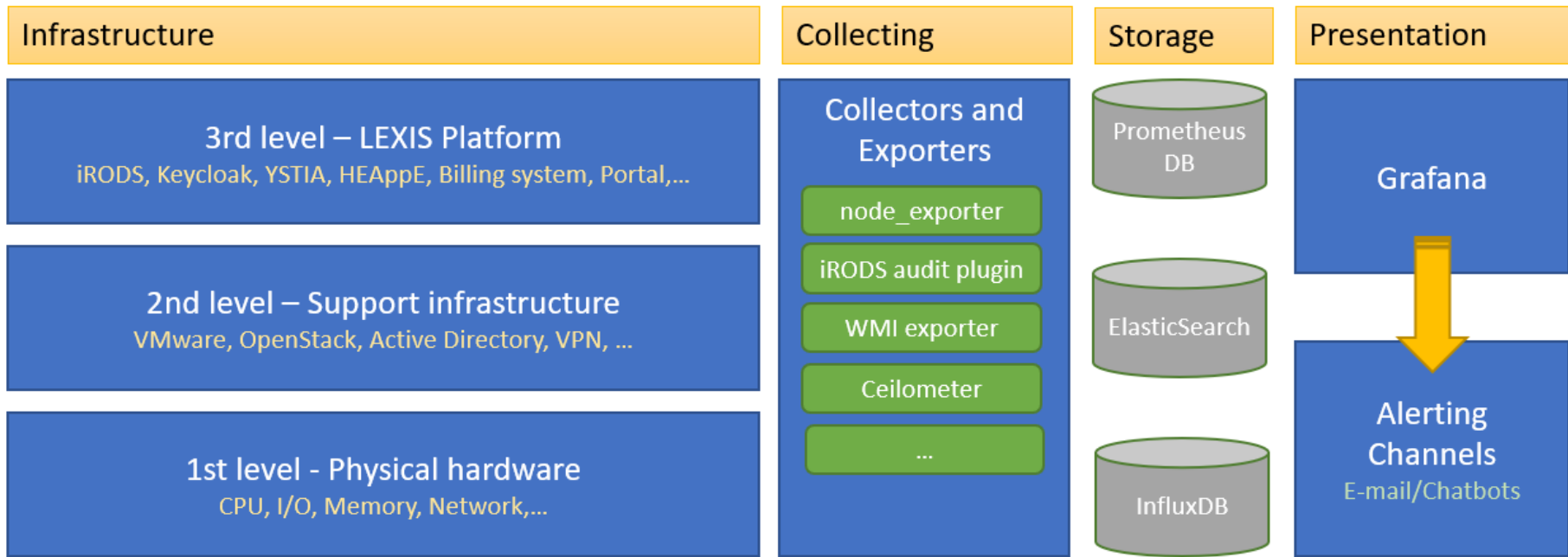
“Zero Trust Architecture”

- Do NOT rely on perimeter-based network security
 - Minimize access to resources
 - Enforce Authentication and Authorization
-
- Do “NOT TRUST” anything inside the perimeter
 - Use secure communication channel
 - Always check Identity and Access



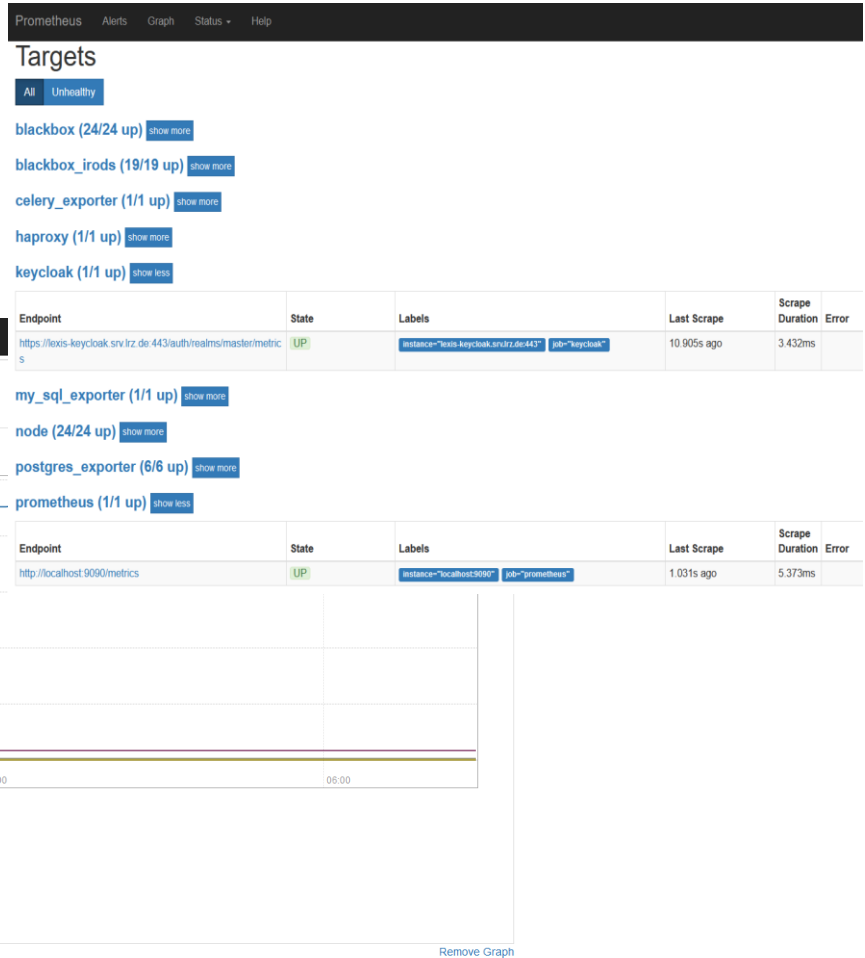
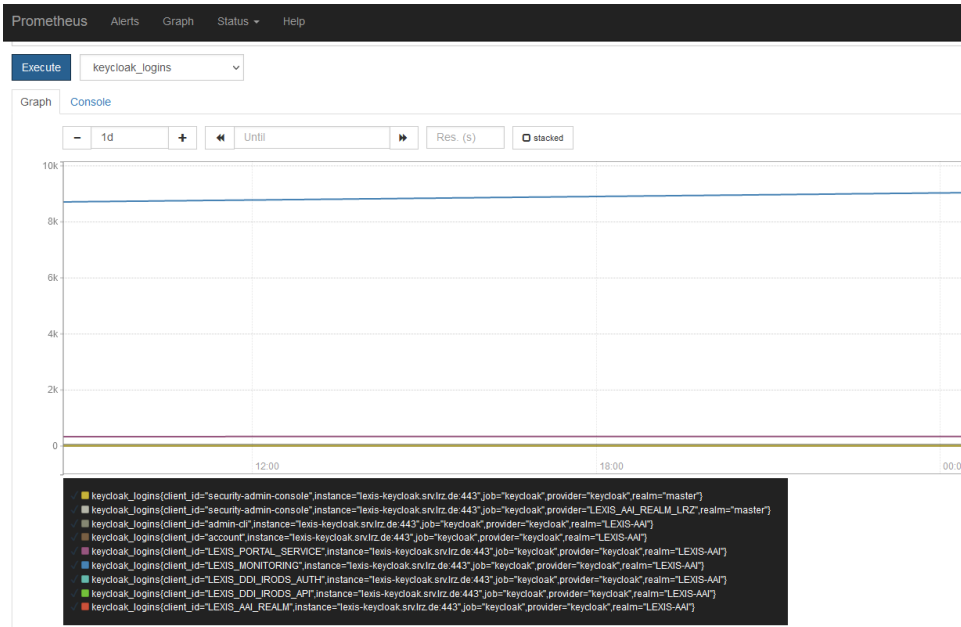
LEXIS MONITORING

- Several Collection Points for all metrics
- Several Storage system
- Only ONE Unified Presentation layer with several alerting capabilities



PROMETHEUS

- Time series database
- Scraping different endpoints to collect “metrics”
- CNCF graduated project



PROMETHEUS EXPORTERS

- Node Exporter: https://github.com/prometheus/node_exporter
- Keycloak Exporter: <https://github.com/aerogear/keycloak-metrics-spi>
- MySQL Exporter: https://github.com/prometheus/mysqld_exporter

```
# HELP keycloak_user_event_UPDATE_PASSWORD Generic Keycloak User event
# TYPE keycloak_user_event_UPDATE_PASSWORD counter
keycloak_user_event_UPDATE_PASSWORD{realm="LEXIS-AAI",} 1.0
# HELP keycloak_user_event_UNREGISTER_NODE Generic Keycloak User event
# TYPE keycloak_user_event_UNREGISTER_NODE counter
# HELP keycloak_user_event_REGISTER_NODE_ERROR Generic Keycloak User event
# TYPE keycloak_user_event_REGISTER_NODE_ERROR counter
# HELP keycloak_user_event_EXECUTE_ACTION_TOKEN_ERROR Generic Keycloak User event
# TYPE keycloak_user_event_EXECUTE_ACTION_TOKEN_ERROR counter
# HELP jvm_memory_pool_allocated_bytes_total Total bytes allocated in a given JVM memory pool.
Only updated after GC, not continuously.
# TYPE jvm_memory_pool_allocated_bytes_total counter
# HELP keycloak_user_event_IDENTITY_PROVIDER_LOGIN_ERROR Generic Keycloak User event
# TYPE keycloak_user_event_IDENTITY_PROVIDER_LOGIN_ERROR counter
keycloak_user_event_IDENTITY_PROVIDER_LOGIN_ERROR{realm="master",} 2.0
# HELP keycloak_user_event_TOKEN_EXCHANGE Generic Keycloak User event
# TYPE keycloak_user_event_TOKEN_EXCHANGE counter
keycloak_user_event_TOKEN_EXCHANGE{realm="LEXIS-AAI",} 2022.0
# HELP keycloak_user_event_LOGIN Generic Keycloak User event
```

```
fdo@sikplrz-lexis-database:~$ wget http://127.0.0.1:9104/metrics
--2021-06-25 09:03:14-- http://127.0.0.1:9104/metrics
Connecting to 127.0.0.1:9104... connected.
HTTP request sent, awaiting response... 200 OK
Length: 237059 (232K) [text/plain]
Saving to: 'metrics'

metrics                               100%[=====] 231.50K  --.-KB/s   in 0.001s

2021-06-25 09:03:14 (418 MB/s) - 'metrics' saved [237059/237059]

fdo@sikplrz-lexis-database:~$ grep -E '(galera|mariadb)' metrics
# HELP mysql_galera_status_info PXC/Galera status information.
# TYPE mysql_galera_status_info gauge
mysql_galera_status_info{wsrep_cluster_state_uuid="1f85838f-76c8-11eb-b0f9-368237fcf42b",wsrep_local_state_uuid="1f85838f-76c8-11eb-b0f9-368237fcf42b",wsrep_provider_version="25.3.33(r15123524)"} 1
# HELP mysql_galera_variables_info PXC/Galera variables information.
# TYPE mysql_galera_variables_info gauge
mysql_galera_variables_info{wsrep_cluster_name="LEXIS-AAI-Database-Cluster"} 1
mysql_version_info{innodb_version="10.3.29",version="10.3.29-MariaDB-1:10.3.29+maria-bionic-log",version_comment="mariadb.org binary distribution"} 1
fdo@sikplrz-lexis-database:~$
```

KEYCLOAK CONFIGURATION FOR GRAFANA

- Create REALM + Client for Monitoring
- Create Role inside Monitoring Client
- Create Mapper for Monitoring Client

Clients > LEXIS_MONITORING

LEXIS_MONITORING 











Settings Credentials **Roles** Client Scopes  Mappers  Scope  Revocation S

Permissions 

Role Name	Composite	Description	Actions	
LEXIS_MONITORING_ADMIN	False	Administrator role for LEXIS Monitoring	Edit	Delete
LEXIS_MONITORING_EDITOR	False	Editor role for LEXIS Monitoring	Edit	Delete

Clients > LEXIS_MONITORING > Mappers > Realm Roles Mapper

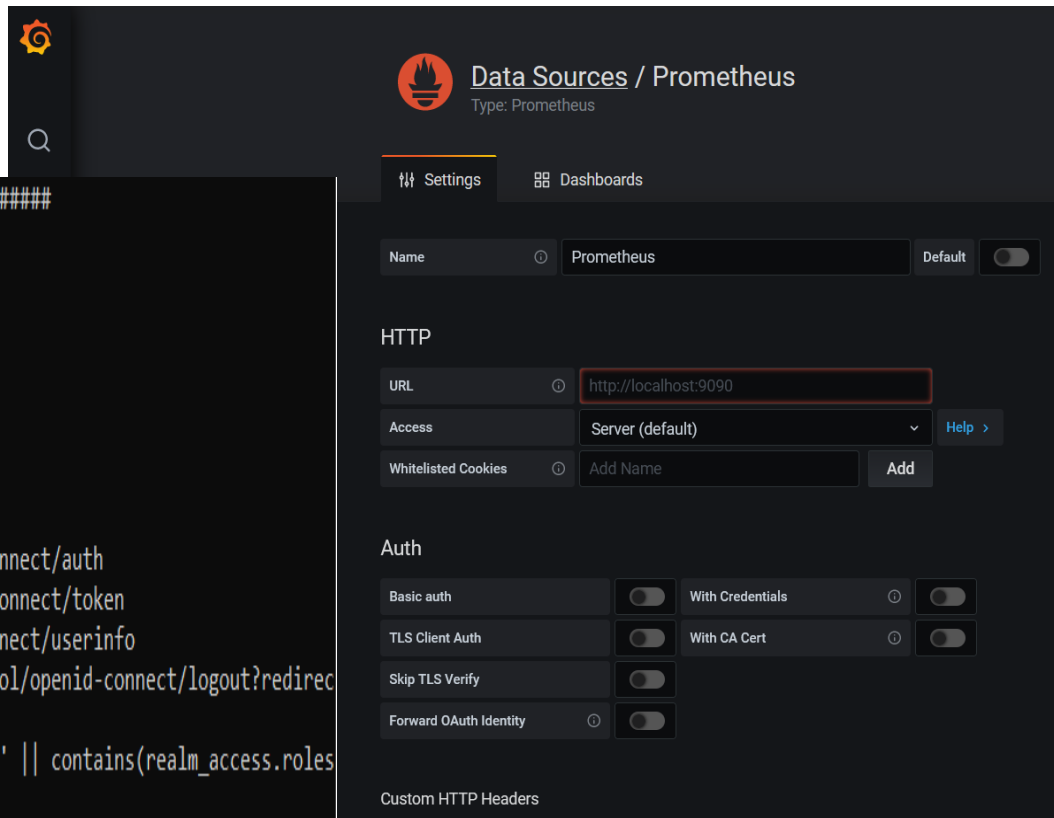
Realm Roles Mapper 

Protocol 	<input type="text" value="openid-connect"/>
ID	<input type="text" value="dc75486a-1a73-492b-8ff2-7c47a78dc724"/>
Name 	<input type="text" value="Realm Roles Mapper"/>
Mapper Type 	<input type="text" value="User Realm Role"/>
Realm Role prefix 	<input type="text"/>
Multivalued 	<input checked="" type="checkbox"/>
Token Claim Name 	<input type="text" value="realm_access.roles"/>
Claim JSON Type 	<input type="text" value="String"/>
Add to ID token 	<input checked="" type="checkbox"/>
Add to access token 	<input checked="" type="checkbox"/>
Add to userinfo 	<input checked="" type="checkbox"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

GRAFANA CONFIGURATION

- Keycloak as OAUTH
- Prometheus as Data Source

```
##### Generic OAuth #####  
[auth.generic_oauth]  
auto_assign_org_id = 1  
enabled = true  
name = OAuth  
allow_sign_up = true  
client_id = <KC_CLIENT_ID>  
client_secret = <KC_CLIENT_SECRET>  
scopes = openid profile email  
auth_url = https://<KC_SERVER>/auth/realms/<KC_REALM>/protocol/openid-connect/auth  
token_url = https://<KC_SERVER>/auth/realms/<KC_REALM>/protocol/openid-connect/token  
api_url = https://<KC_SERVER>/auth/realms/<KC_REALM>/protocol/openid-connect/userinfo  
signout_redirect_url = https://<KC_SERVER>/auth/realms/<KC_REALM>/protocol/openid-connect/logout?redirect_uri=https://<GRAFANA_SERVER>/grafana  
role_attribute_path = contains(realms_access.roles[*], 'ADMIN') && 'Admin' || contains(realms_access.roles[*], 'EDITOR') && 'Editor' || 'Viewer'
```



The screenshot shows the Grafana web interface for configuring a Prometheus data source. The page title is "Data Sources / Prometheus" with the subtitle "Type: Prometheus". There are two tabs: "Settings" (active) and "Dashboards".

Name: Prometheus (Default)

HTTP:

- URL:** http://localhost:9090
- Access:** Server (default) [Help >](#)
- Whitelisted Cookies:** Add Name

Auth:

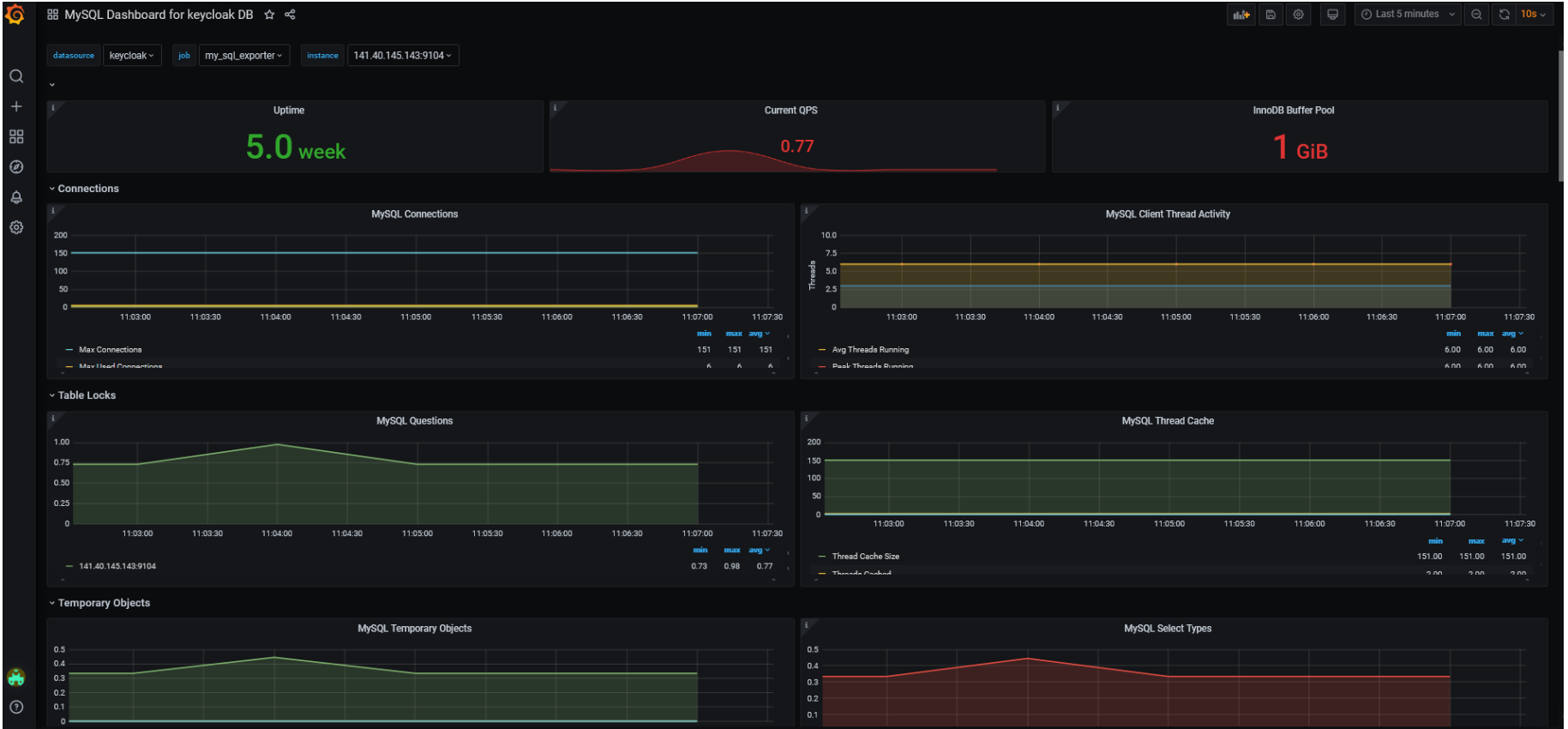
Basic auth	<input type="checkbox"/>	With Credentials	<input type="checkbox"/>
TLS Client Auth	<input type="checkbox"/>	With CA Cert	<input type="checkbox"/>
Skip TLS Verify	<input type="checkbox"/>		
Forward OAuth Identity	<input type="checkbox"/>		

Custom HTTP Headers:

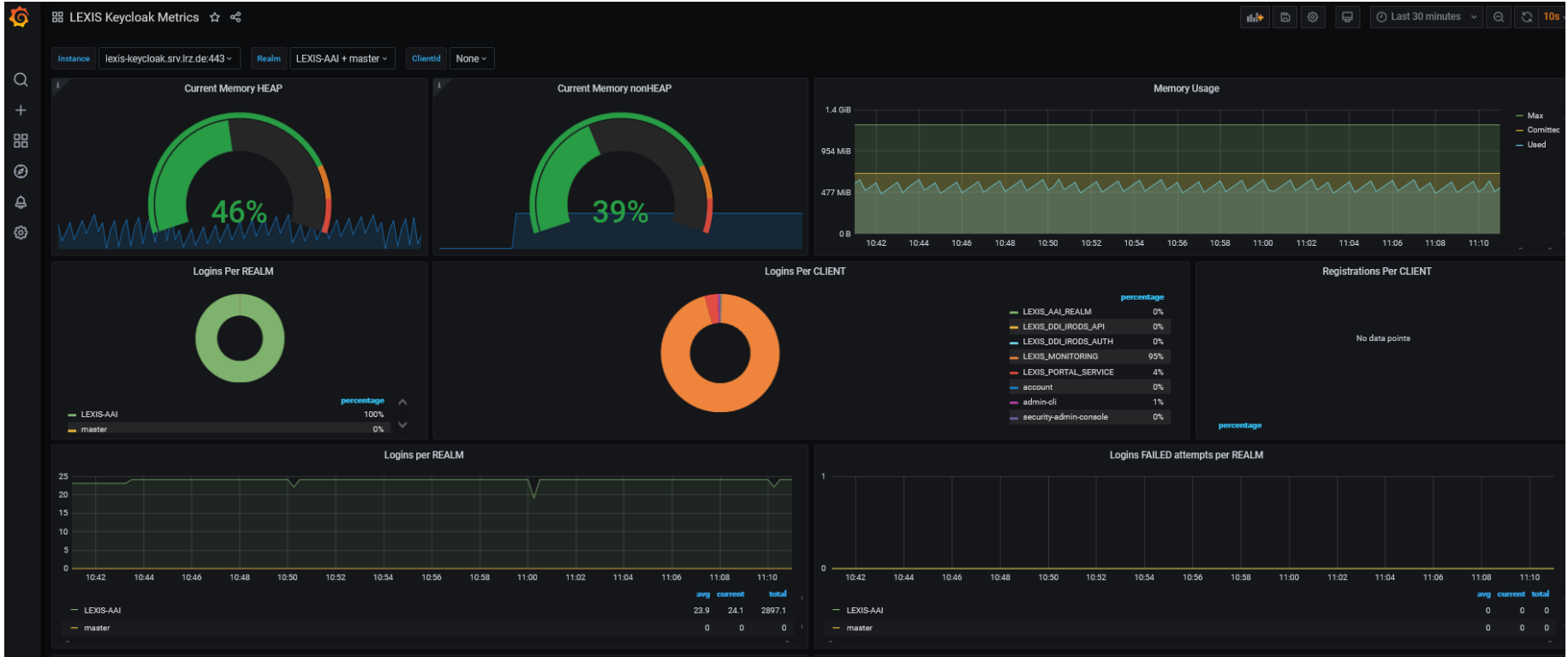
GRAFANA DASHBOARD NODE EXPORTER



GRAFANA DASHBOARD MYSQL EXPORTER

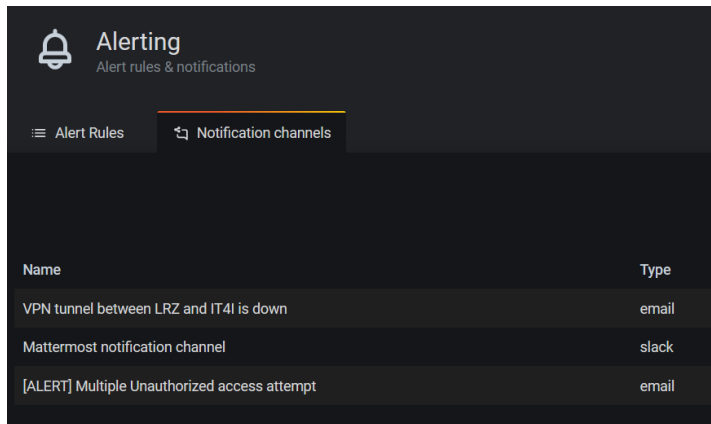


GRAFANA DASHBOARD: KEYCLOAK EXPORTER



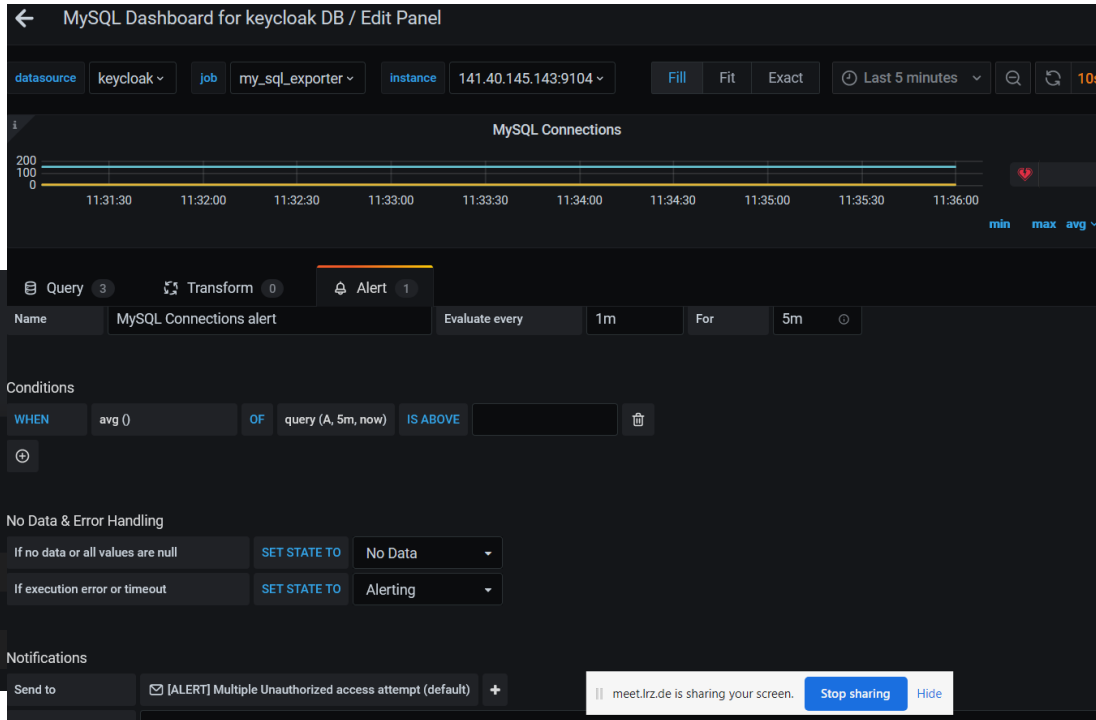
GRAFANA ALERT CONFIGURATION

- Create Notification Channel in Alerting
- Add Alert in Graph/View



The screenshot shows the Grafana Alerting configuration interface. At the top, there is a bell icon and the text "Alerting" with the subtitle "Alert rules & notifications". Below this, there are two tabs: "Alert Rules" and "Notification channels". The "Notification channels" tab is active, showing a table of configured notification channels.

Name	Type
VPN tunnel between LRZ and IT4I is down	email
Mattermost notification channel	slack
[ALERT] Multiple Unauthorized access attempt	email



The screenshot shows the Grafana Alert configuration page for a MySQL dashboard. The dashboard title is "MySQL Dashboard for keycloak DB / Edit Panel". The alert configuration is for "MySQL Connections alert".

Alert Configuration:

- Name:** MySQL Connections alert
- Evaluate every:** 1m
- For:** 5m

Conditions:

- WHEN:** avg ()
- OF:** query (A, 5m, now)
- IS ABOVE:** [Threshold]

No Data & Error Handling:

- If no data or all values are null: SET STATE TO No Data
- If execution error or timeout: SET STATE TO Alerting

Notifications:

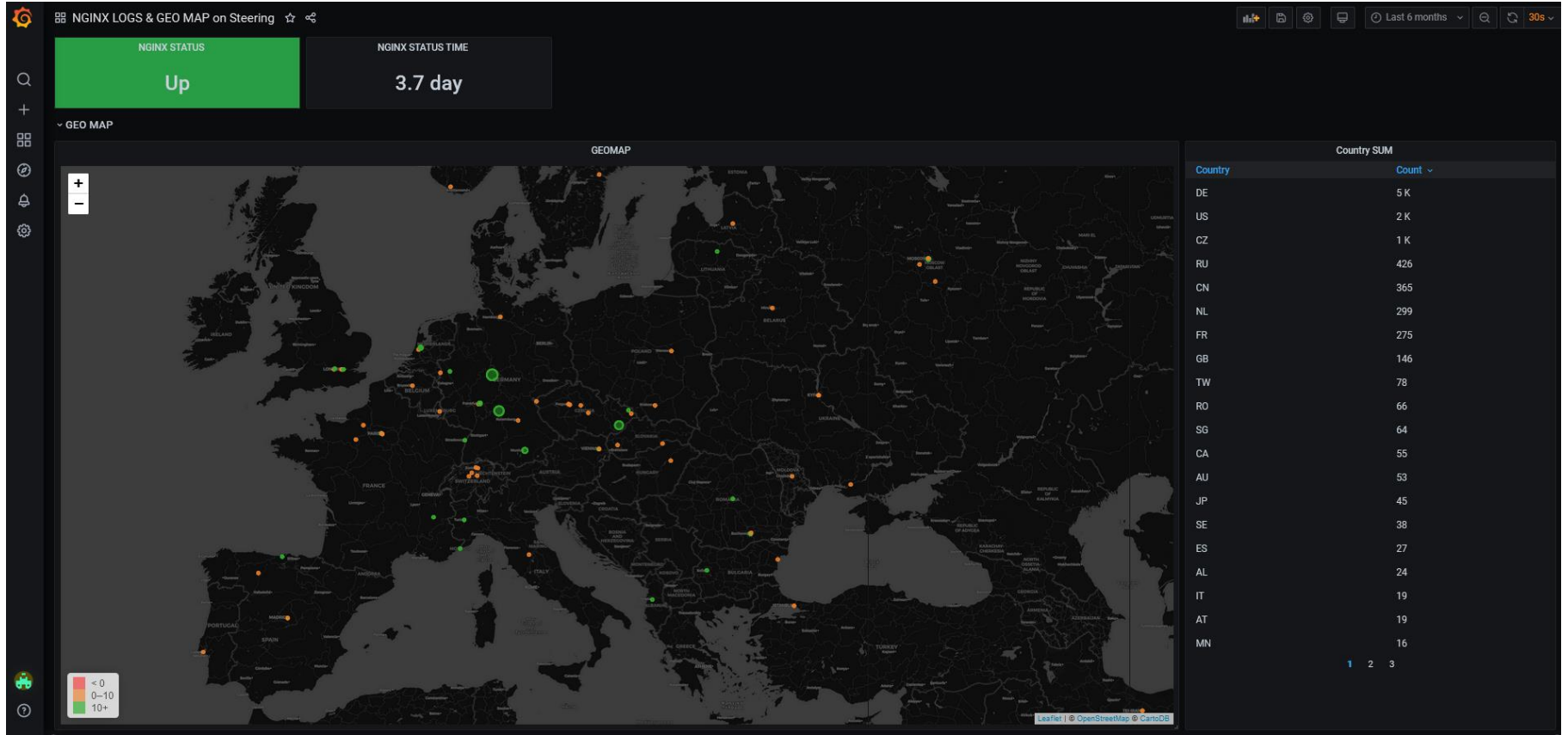
- Send to: [ALERT] Multiple Unauthorized access attempt (default)

GRAFANA ALERT

The screenshot displays the Grafana Alerting dashboard. At the top, there is a bell icon and the title "Alerting" with the subtitle "Alert rules & notifications". Below this, there are two tabs: "Alert Rules" (selected) and "Notification channels". A search bar labeled "Search alerts" is present, along with a "States" dropdown menu set to "All" and a "How to add an alert" button. The main area contains a list of alert rules, each with a green heart icon indicating an "OK" status and a "00" timer. The alert rules listed are:

- CPU Basic alert**: OK for 3 months. Query returned no data.
- ICMP round trip time (IT4) alert**: OK for 11 days. Query returned no data.
- ICMP round trip time lexis-keycloak.srv.lrz.de alert**: OK for 11 days.
- ICMP round trip time lexis-lrzicat1.srv.lrz.de alert**: OK for 11 days.
- ICMP round trip time lexis-lrzicat1.srv.lrz.de alert**: OK for 11 days. Query returned no data.
- ICMP round trip time sikplr-lexis-database.srv.mwn.de alert**: OK for 11 days.
- Memory Basic alert**: OK for 8 months.
- SSH Attack detected**: OK for 11 days.

GRAFANA GEO



DOCUMENTATION & LINKS

- Keycloak
 - <https://www.keycloak.org/>
 - <https://www.keycloak.org/extensions.html>
- Prometheus
 - <https://prometheus.io/>
 - <https://prometheus.io/docs/instrumenting/exporters/>
- Grafana
 - <https://grafana.com/>
 - <https://community.grafana.com/>
 - <https://grafana.com/grafana/dashboards/10441>
- Zero Trust Architecture
 - NIST: <https://csrc.nist.gov/publications/detail/sp/800-207/final>
 - NSA: <https://www.nsa.gov/News-Features/Feature-Stories/Article-View/Article/2515176/nsa-issues-guidance-on-zero-trust-security-model/>

CONTACTS

Frederic Donnat
fdo@outpost24.com

<https://lexis-project.eu>

Large-scale EXecution for Industry & Society

The logo for LEXIS, with 'LEXIS' in green and 'IS' in yellow.

CONSORTIUM

 **VSB TECHNICAL UNIVERSITY OF OSTRAVA** | **IT4INNOVATIONS NATIONAL SUPERCOMPUTING CENTER**

The logo for ANI, featuring a globe icon and the letters 'ANI' in blue.The logo for cea, with the letters 'cea' in white on a red background.The logo for Outpost24, featuring a target icon and the text 'Outpost24'.The logo for Avio Aero, with the text 'Avio Aero' and 'A GE Aviation Business' below it.The logo for Atos, with the text 'Atos' in blue. **lrz** Leibniz-Rechenzentrum der Bayerischen Akademie der WissenschaftlerThe logo for ECMWF, with the letters 'ECMWF' in blue.The logo for LINKS, with the letters 'LINKS' in green and 'SMB IStiI' below it.The logo for Ithaca, featuring a globe icon and the letters 'ITHACA'.The logo for CIMO, with the letters 'CIMO' and 'RESEARCH FOUNDATION' below it.The logo for CYCLOPS, featuring a silhouette of a penguin and the text 'CYCLOPS'.The logo for GFZ, with the letters 'GFZ' and 'Helmholtz Centre POTSDAM' below it.The logo for BAYNCORE LABS, with the text 'BAYNCORE LABS'.The logo for EIFFAGE TESEO, with the letters 'EIFFAGE TESEO' and a red icon.The logo for NUMTECH, with the letters 'NUMTECH' and 'NUMTECH GROUP' below it.