



idh



The open system company

idh Logging Framework ILF

IDH GmbH | www.idh.ch | Wilenstrasse 4 | CH 8832 Wollerau | Tel. +41 52 366 39 01

Motivation



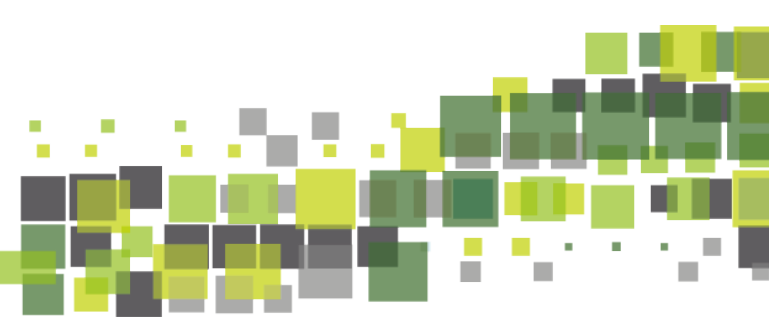
- **Vereinfachtes Troubleshooting**
- **IT Grundschutz**
- **Alarming und Monitoring**

Motivation



- **Machine Learning und Artificial Intelligence**
- **Auswertung**
- **Kosten**

Machine Learning / AI



Machine Learning

Job Management Anomaly Explorer Single Metric Viewer Transforms Analytics Data Visualizer Settings

nginx(5 jobs) demo Edit job selection

Filter by influencer fields... (source.address : 72.570.53)

Top Influencers

source.address

- 72.570.53 99 993
- 19.199.239.172 99 950
- 108.47.35.204 99 1400
- 170.92.28.189 99 2441
- 185.78.31.85 99 9667
- 213.223.20.66 99 1301
- 247.246.17.141 99 3753
- 82.19.123.10 99 191
- 2.111.168.189 99 233
- 204.0.194.114 99 1194

http.response.status_code

- 404 98 8754
- 301 91 4312

Anomaly timeline

Overall

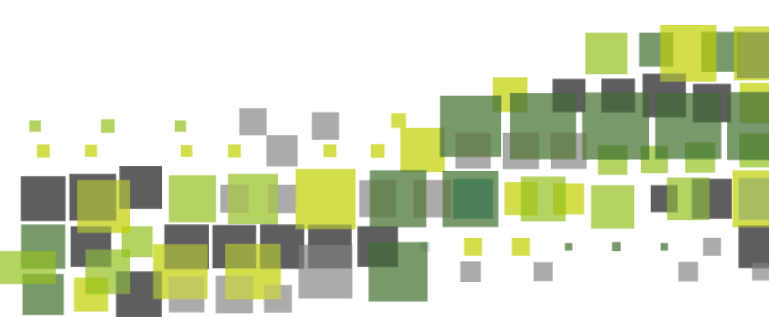
View by: job ID Limit: 10

Anomalies

Severity threshold: warning Interval: Auto

time	severity	detector	found for	influenced by	actual	typical	description	job ID	actions
> February 1st 2017	99	Nginx access source IP high count	19.199.239.172	source.address: 19.199.239.172	5338	2.43	↑ More than 100x higher	demo-source_ip_request_rate_ecs	

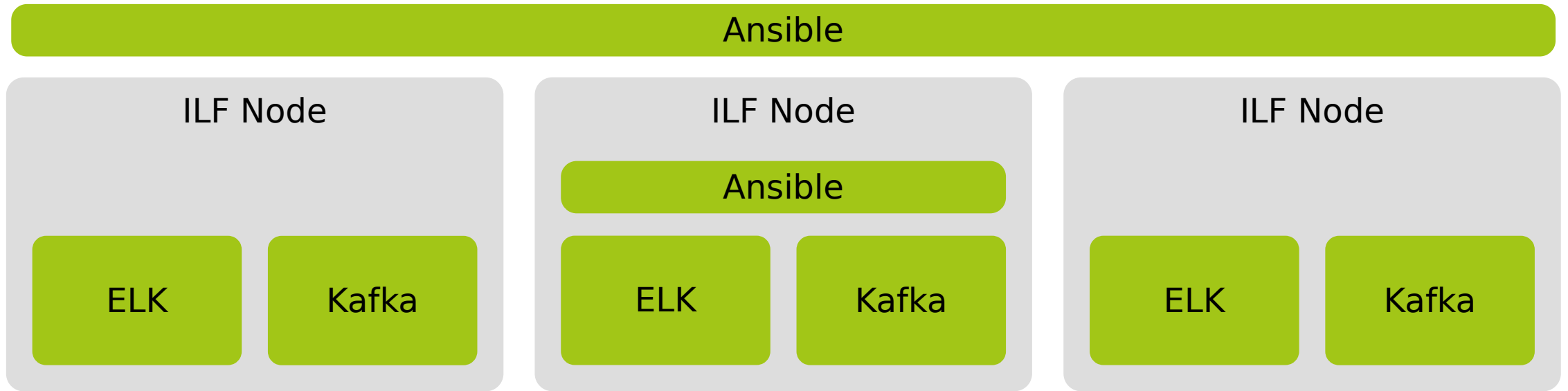
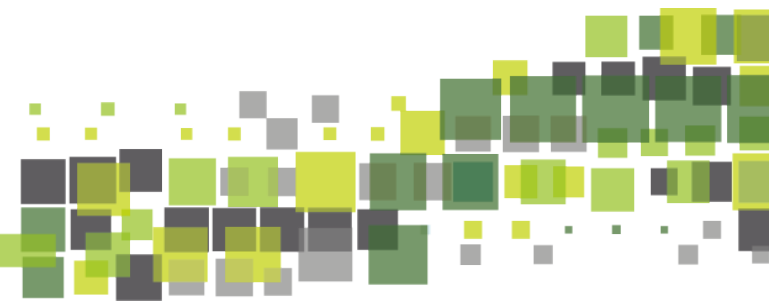
Machine Learning / AI



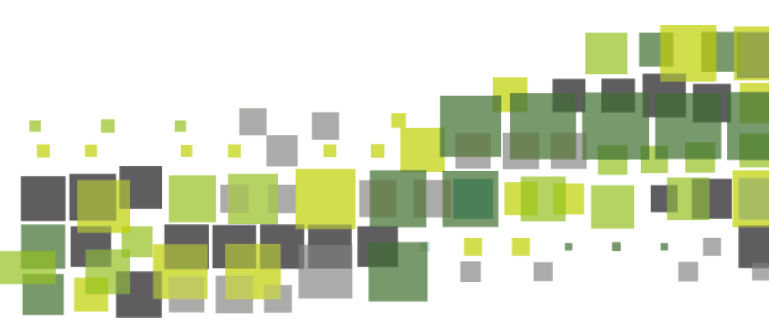
Business Cases

- **Infrastruktur / Netzwerk**
- **Middleware**
- **Technik und Entwicklung**
- **Datenanalyse mittels AI / ML**
- **Performance Analyse / Datendurchsatzkontrolle**

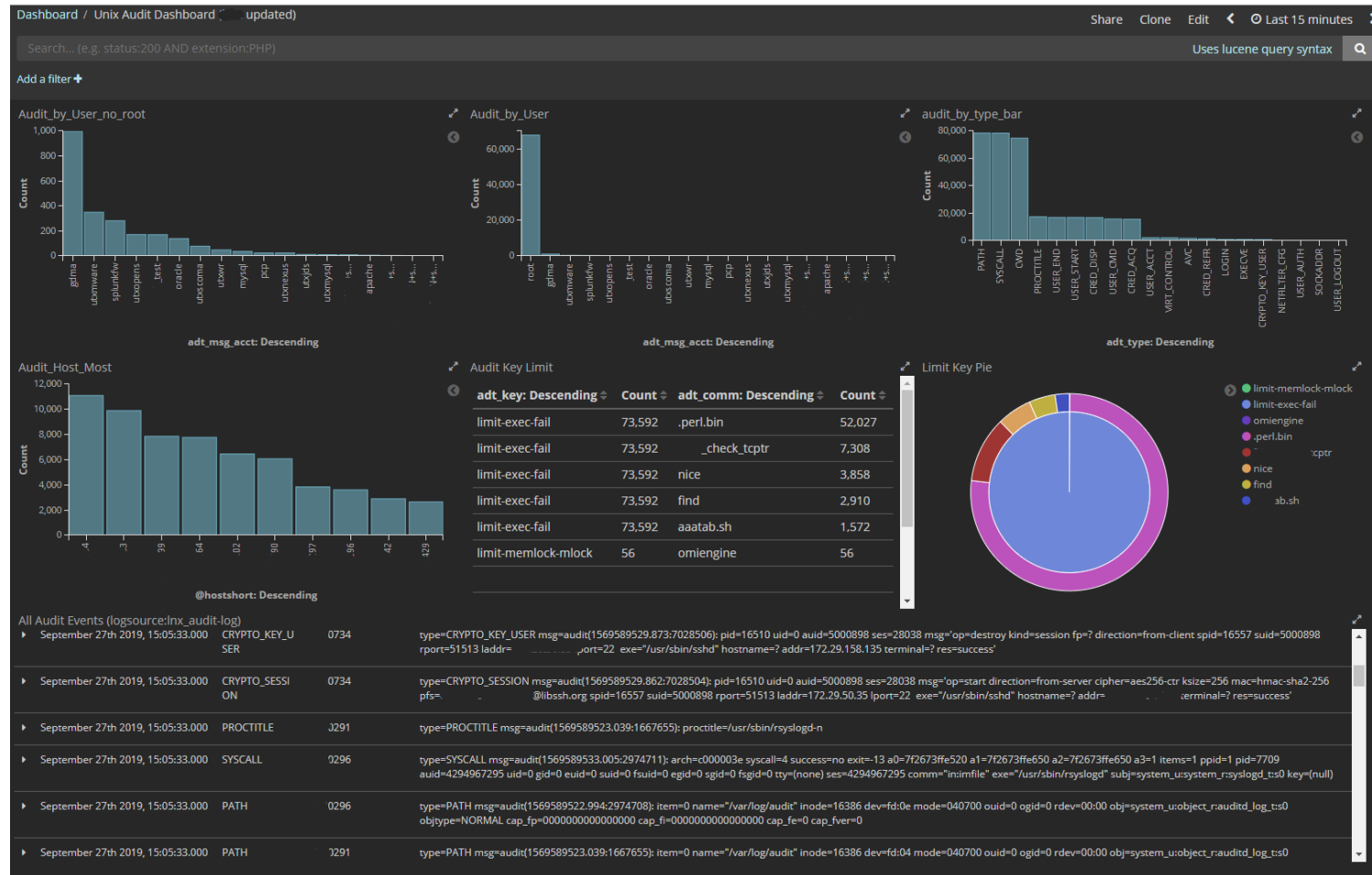
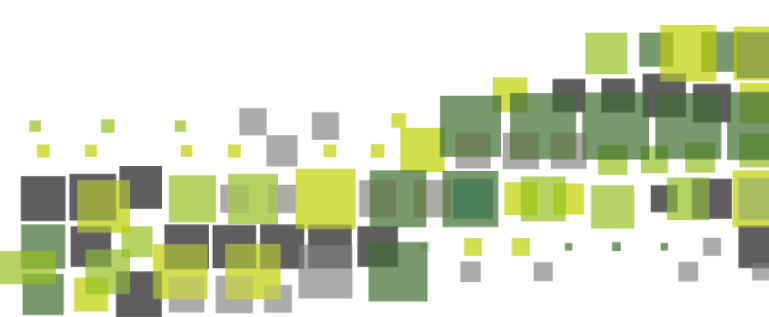
idh Logging Framework (ILF)

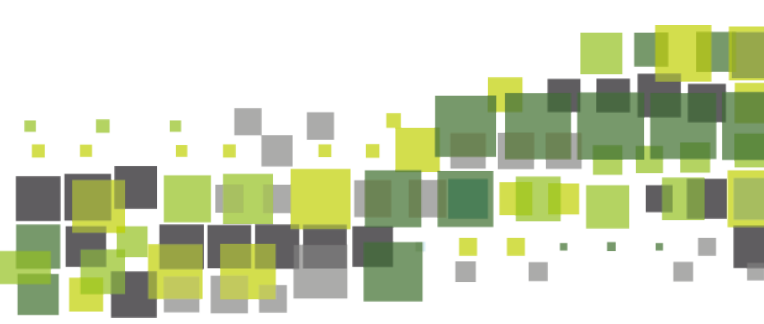


Dashboard

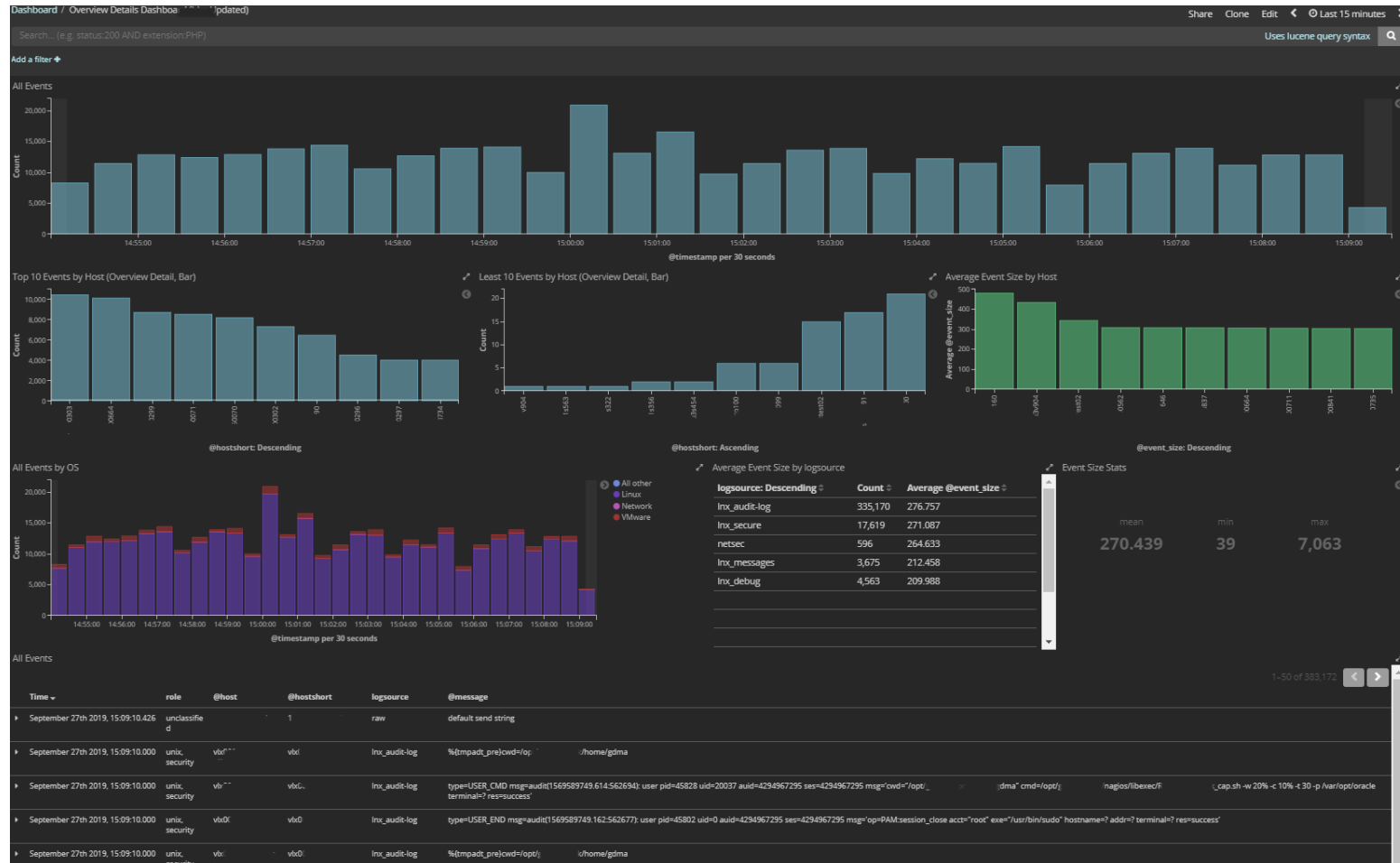


Dashboard

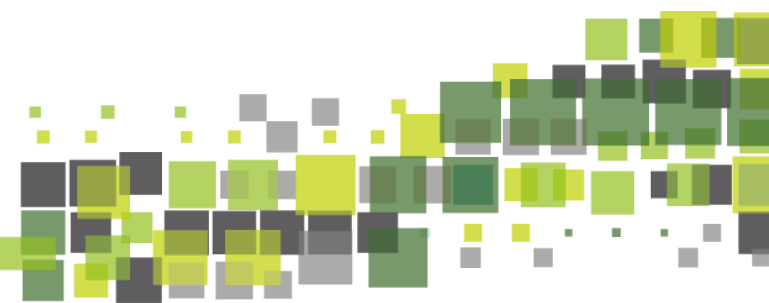




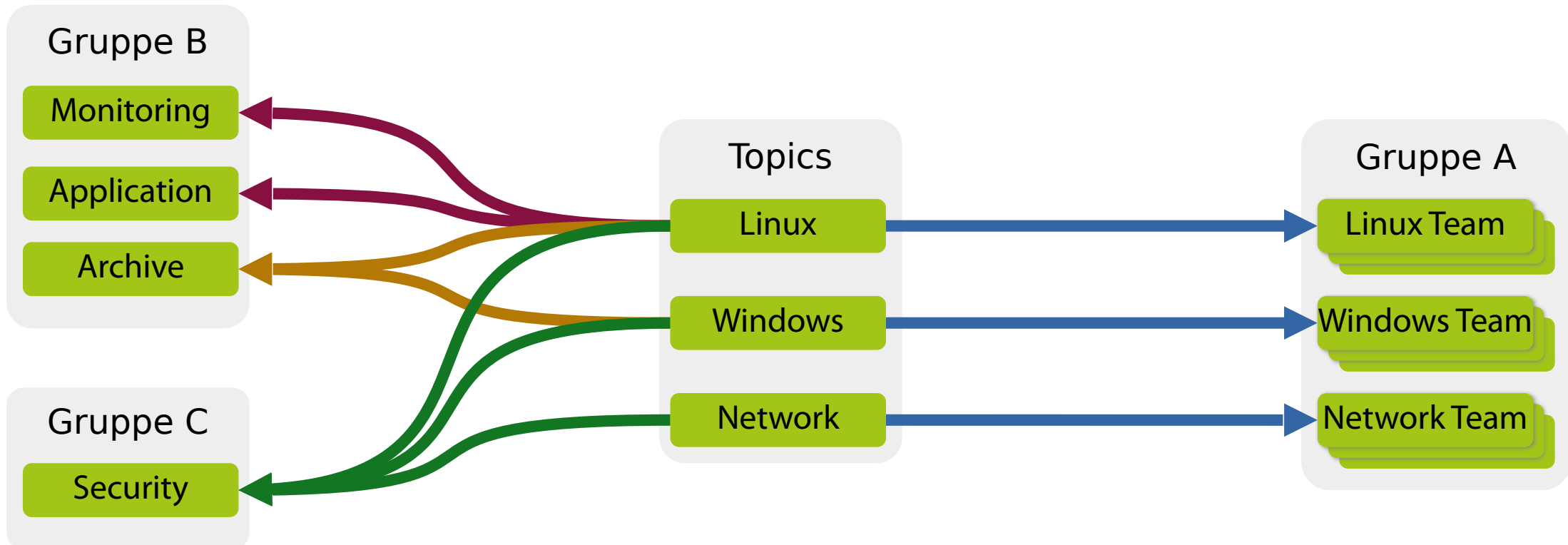
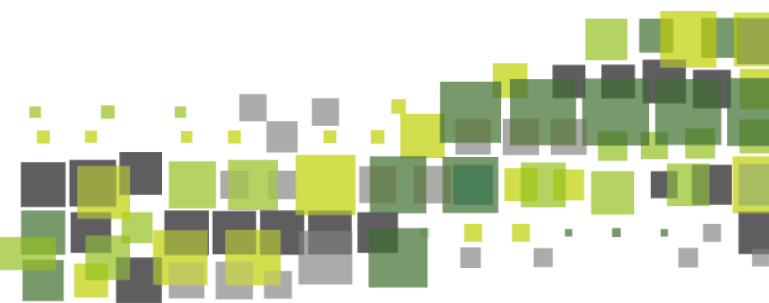
Dashboard



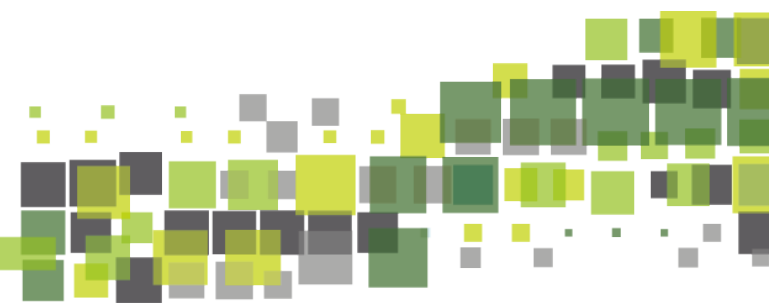
Kafka Konzept



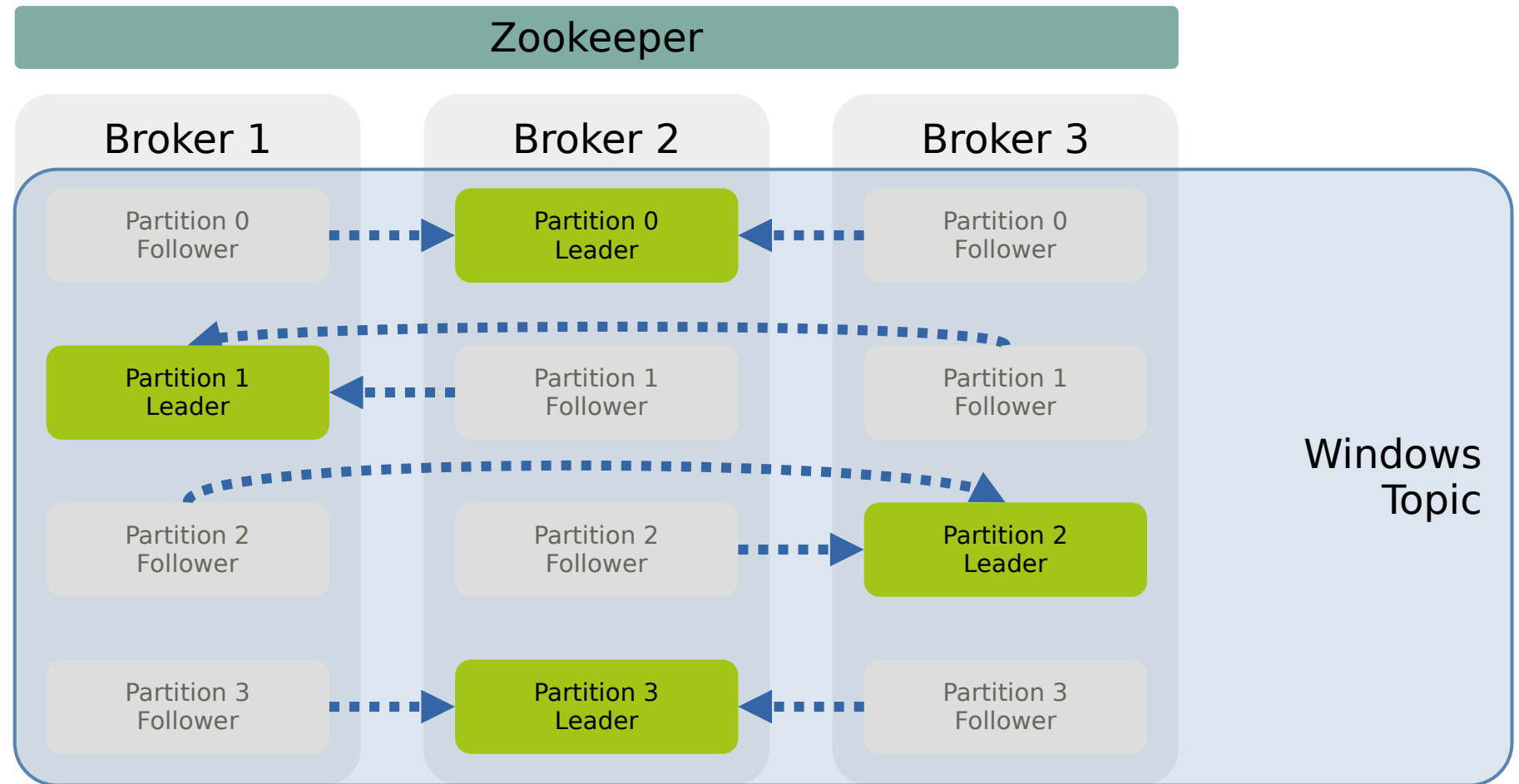
Kafka Topics / Consumer Groups



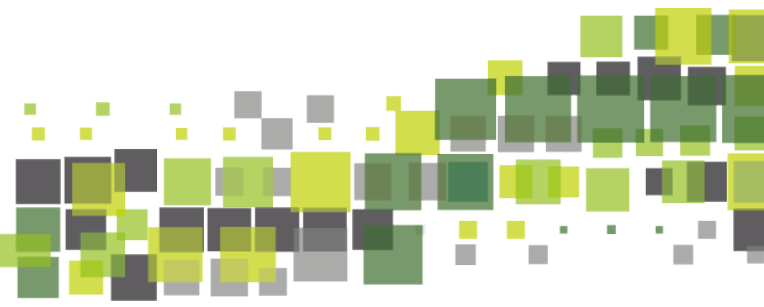
Kafka High Availability (HA)



- Topic with:
- 4 partitions
 - Replication factor = 3

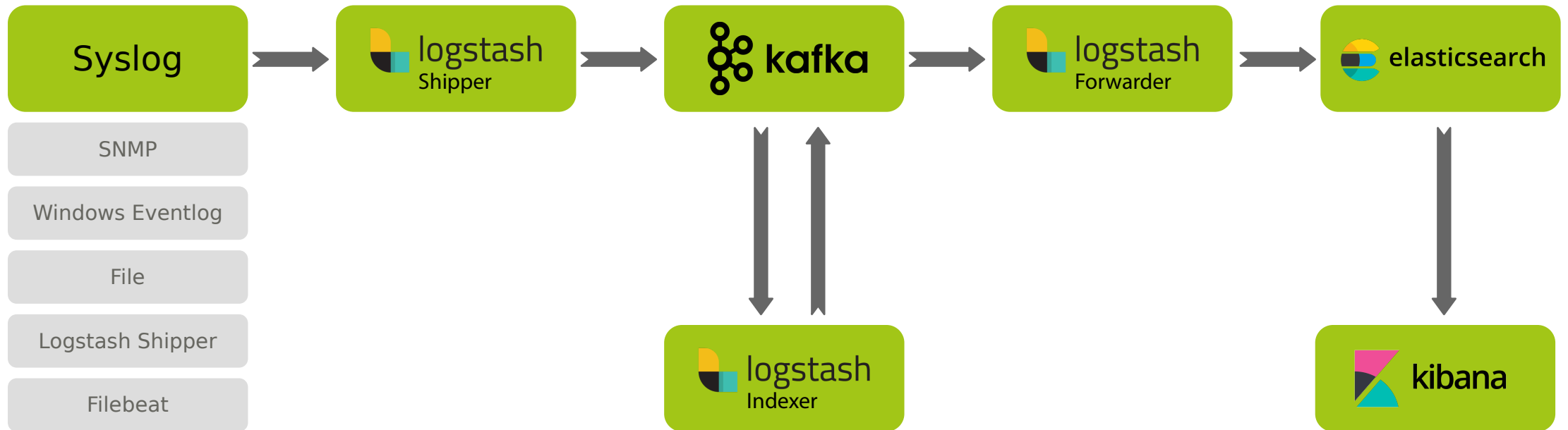
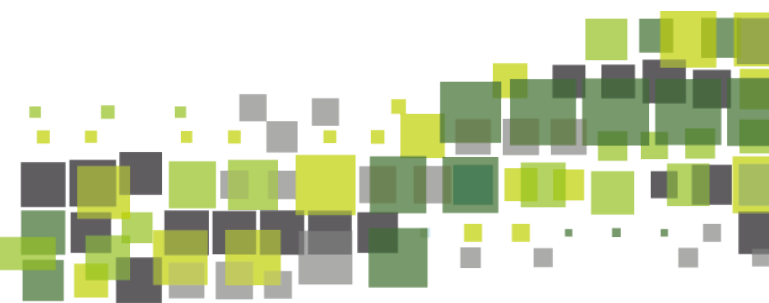


idh Logging Framework (ILF)

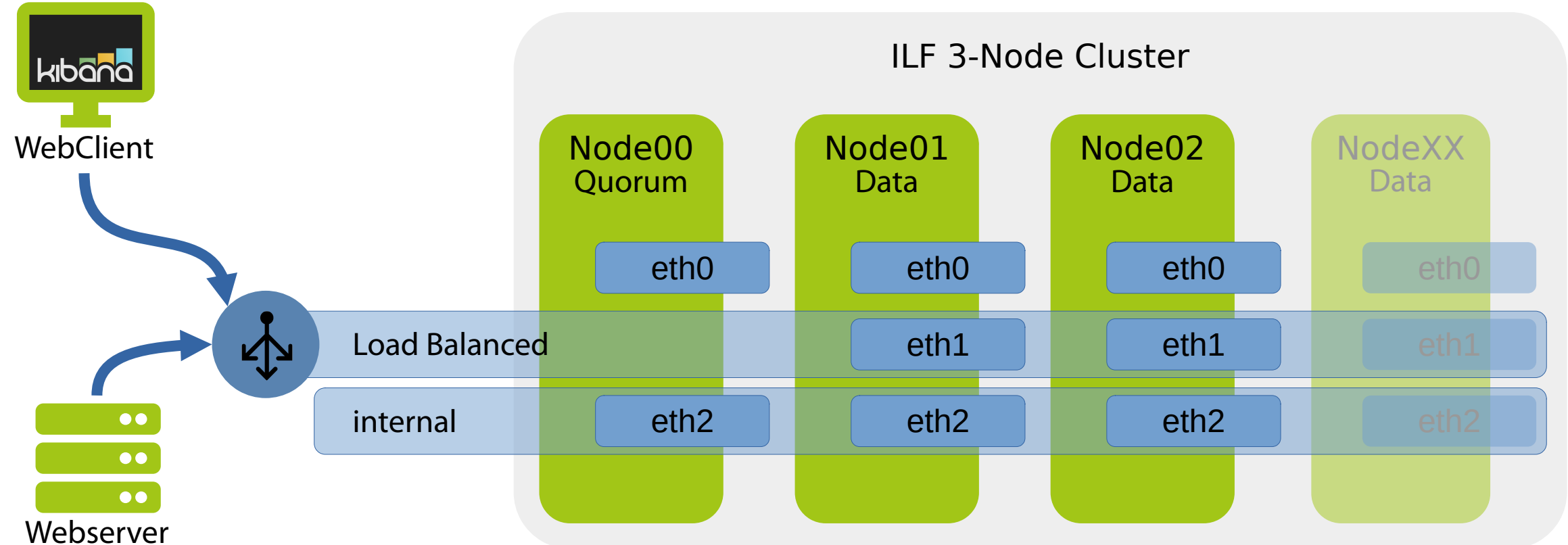
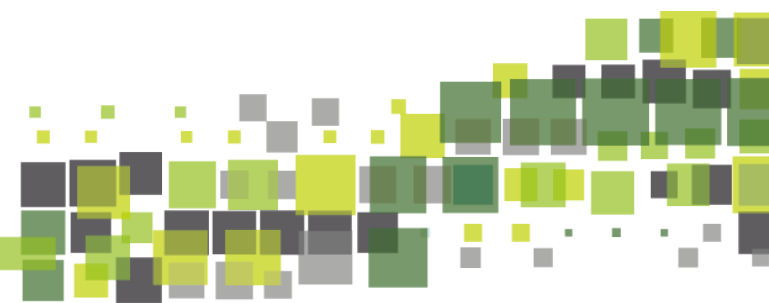


- **Flexible Filezulieferung**
- **Virtual Appliance ansatz**
- **HA fähig**
- **Skalierbar**

idh Logging Framework (ILF)



ILF Cluster



Eigenschaften

- **Höchste Performance**
- **Multi-Threading Architecture**
- **Korreliert Daten von unterschiedlichsten Sourcen**
- **Ad-Hoc Analysen für Business User**

Eigenschaften



- **View auf alle wichtigen Daten**
- **Opensource Komponenten**
- **Keine Limitation / Kosten auf Datendurchsatz**

Eigenschaften

- **Konfigurierbar mit „Configuration Management Tools“**
- **Frontend**
- **Flexibel**

Showcase Setup

