



Network anomaly detection based on logs



Chin : Qin YuKun , Song Yong , Xie Yuchen , Wei QiangShen

Logs are valuable for network maintenance with existing challenges

Huge chunks of data was generated by Network Equipment and these information can be used to detect existing faults to improve the network maintenance.

Log Application

Anomaly Detection

Event Alarm Convergence

Root Cause Analysis

Fault Location

System Evaluation

Fault Warning

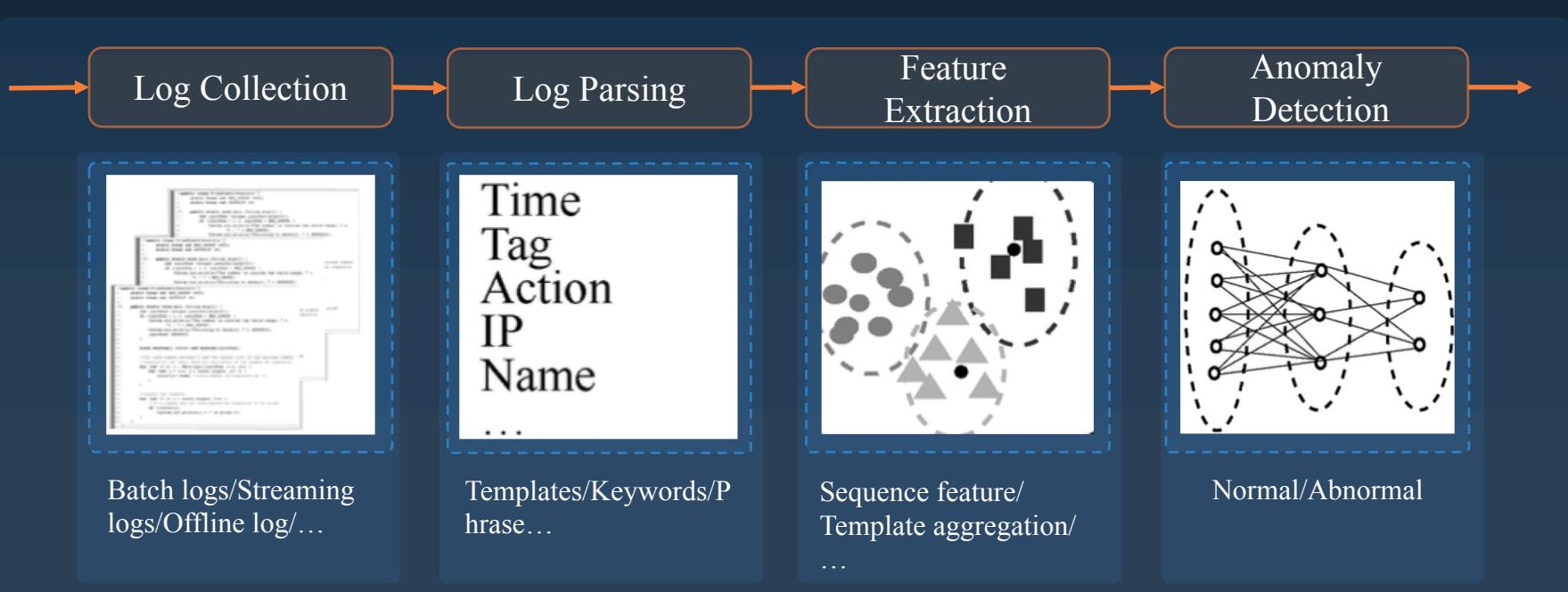
.....

Challenges

- Increasingly vast amount (1GB/H+)
- Various types (Exchanger、 Server、 Router, etc.)
- Unstructured data
- Unsupervised / No-Label
- Tradeoff between effect and efficiency

Ensemble Solution: NLP & Abnormal Detection

Network Abnormal Detection based on Logs was composed by NLP and abnormal detection.



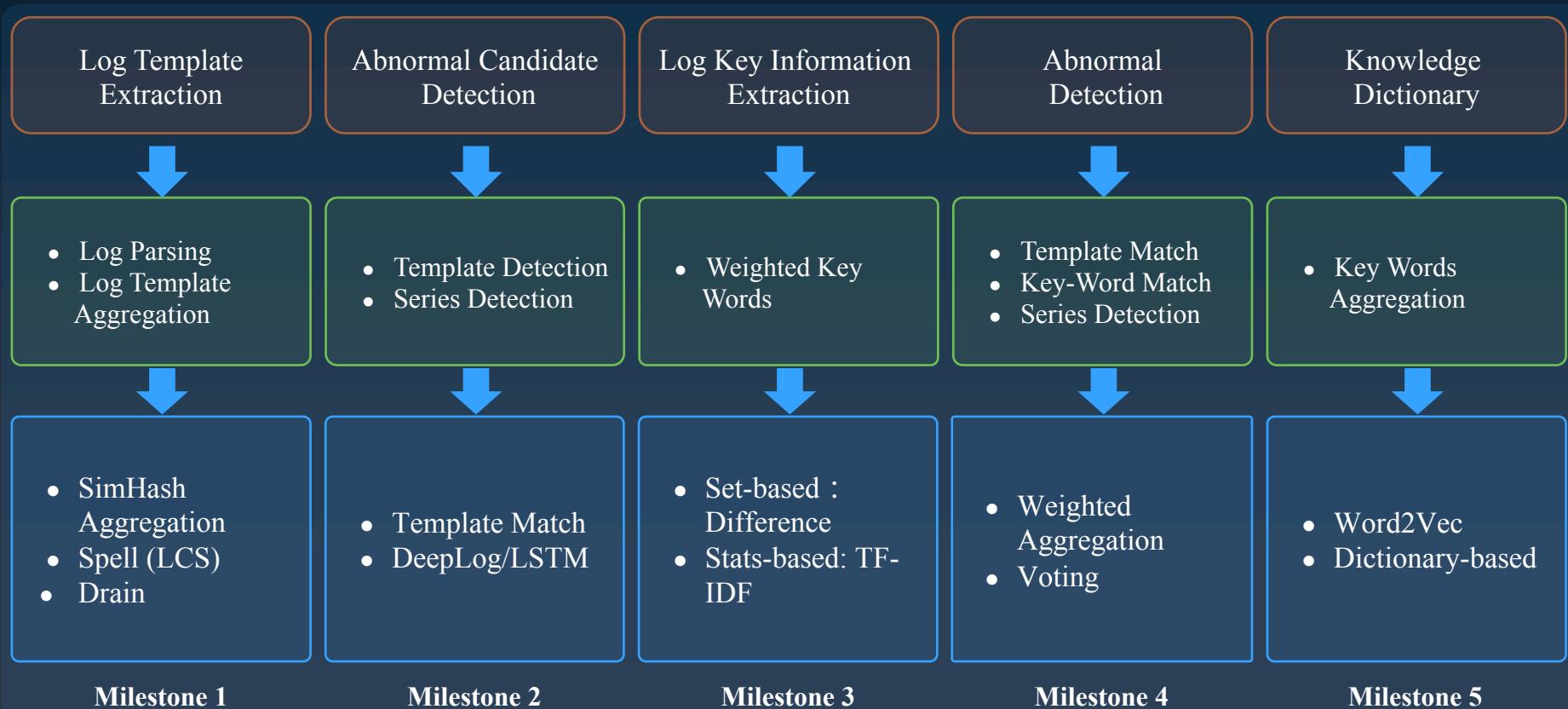
Key-word Dictionary Construction is the most important

Although there are plenty of AI algorithms such as Deep Learning involved in log anomaly detection, all methods without key words performs not good enough.

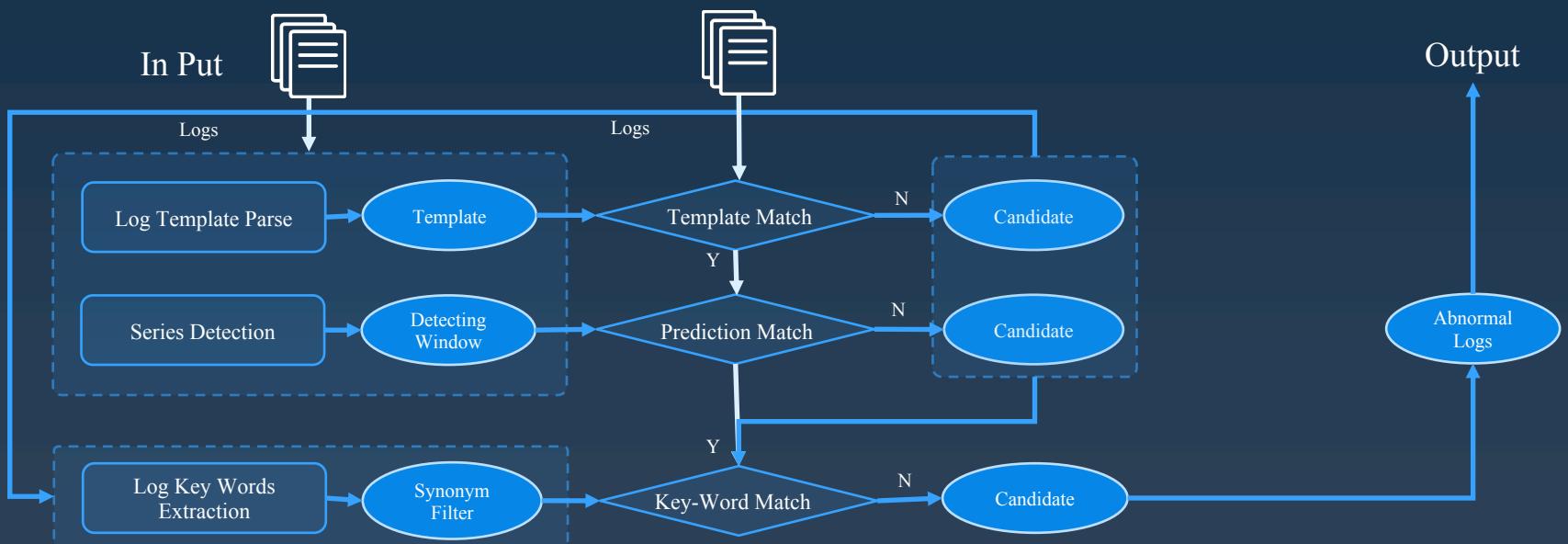
1. RISTO V, PIHELGAS M. LogCluster — a data clustering and pattern mining algorithm for event logs[C]// Conference on Net-work and Service Management (CNSM). 2015: 1-7.
2. HEPJ, ZHUJM, HESL, et al. Towards automated log parsing for large-scale log data analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(6): 931-944.
3. STUDIAWAN H, SOHEL F, PAYNE C. Automatic event log abstraction to support forensic investigation[C]// ACSW 2020. 2020: 1-9.
4. STUDIAWAN H, PAYNE C, SOHEL F. Automatic graph-based clustering for security logs[C]// Advanced Information Networking and Applications(AINA). 2019: 914-926.
5. DAI H, LI H, CHEN C S, et al. Logram: efficient log parsing using n-gram dictionaries[R]. 2020.
6. DU M, LI F F. Spell: online streaming parsing of large unstructured system logs[J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 31(11): 2213-2227.



Industry-level Solution is empowered by iteration

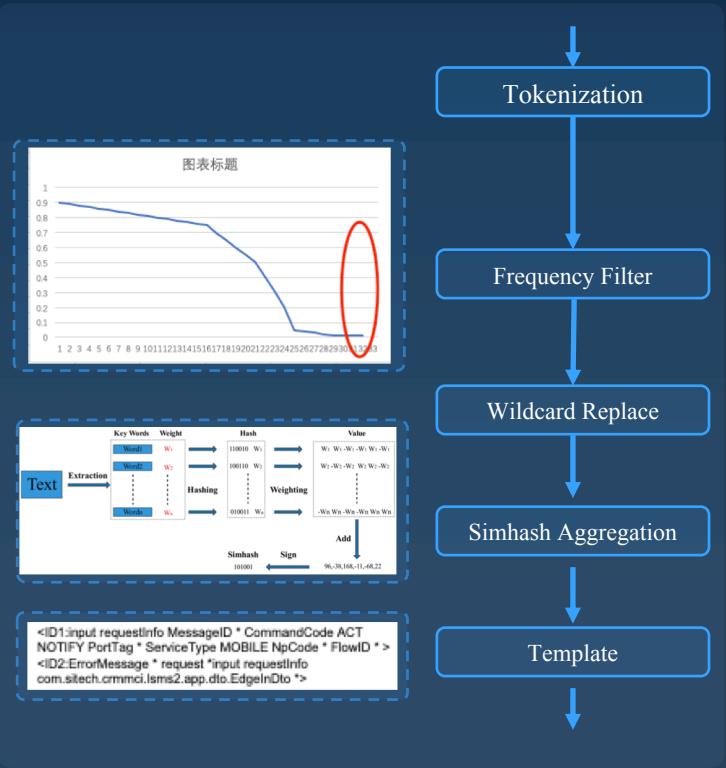


Pre-Detection is used to update key word dictionary for detection fixing

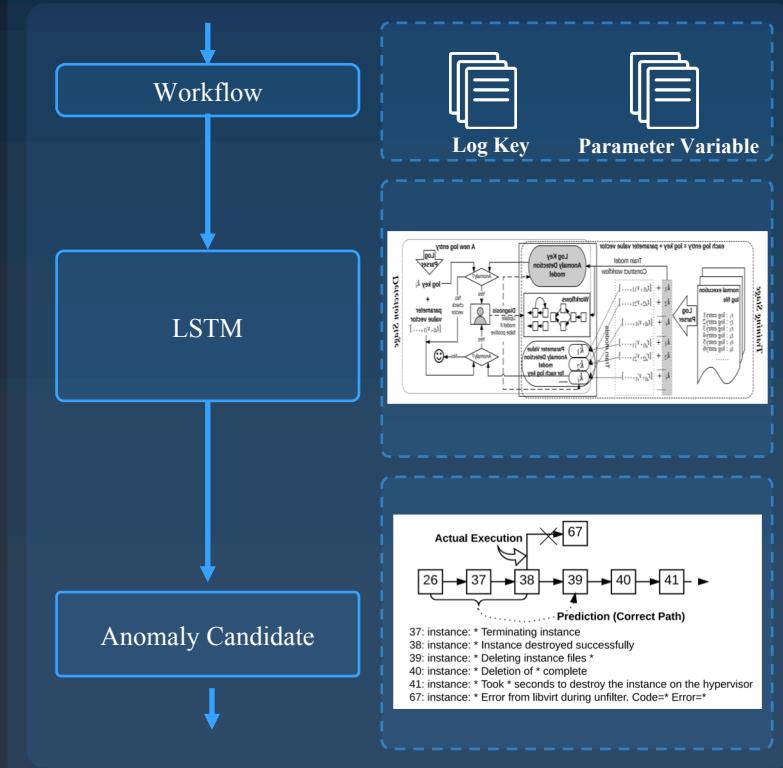


Fast template extraction is utilized to make pre-detection based on LSTM much more efficient

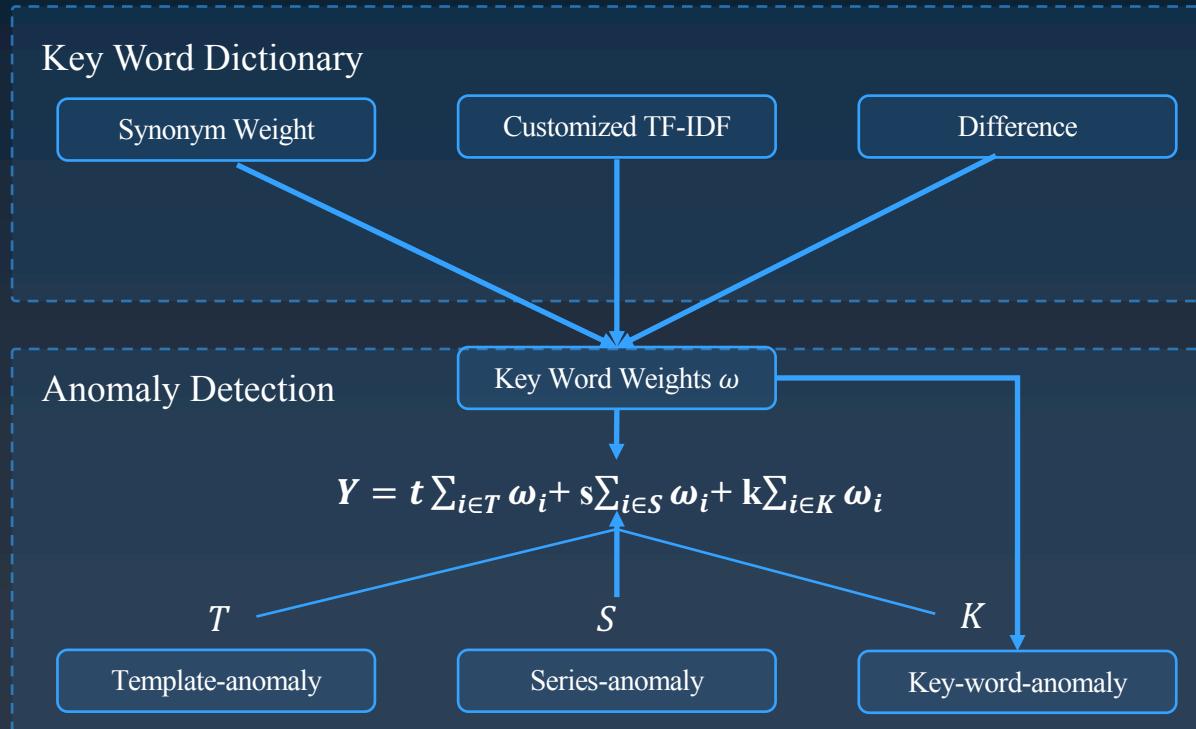
Frequency-based Template Extraction



Series Anomaly Detection by LSTM



Weighted detection with key-words filter generates the final anomaly



The only 100 out of 100 score in competition dataset

P=100% ; R=100% ; F1=1.00 , Top 1 at China Unicom 5G+AI Network Application Special Competition .

- Advantages
 - ① More efficient template extraction ;
 - ② Increasingly accumulated knowledge dictionary and potential knowledge graph construction ;
 - ③ Perfect tradeoff of time consumption and performance ;
 - ④ Optional fast detection with dictionary

• Result



Industrial Application is perfect

Productization in AIOps

Deployed for 20+ system

Daily processed 0.92TB data with 92% precision

The image displays two side-by-side screenshots of a cloud-based AIOps monitoring platform. Both screenshots show the '告警' (Alerts) section of the '日志异常检测' (Log Anomaly Detection) feature.

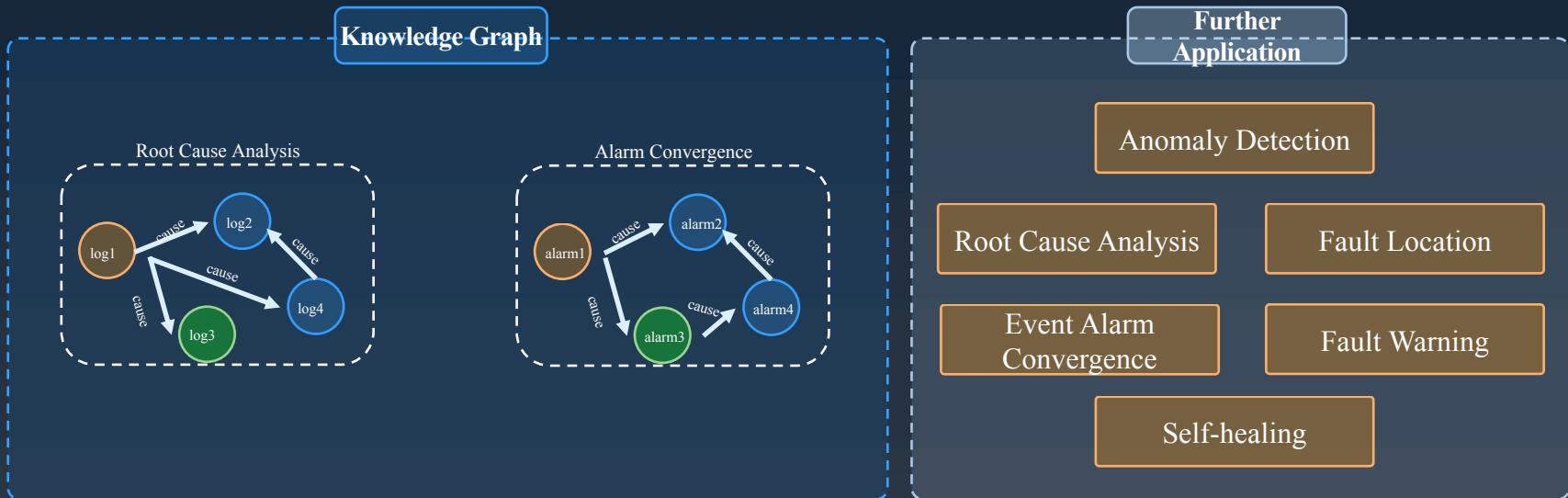
Left Screenshot (LmsSso Service):

- Top Bar:** 日志异常检测 (Log Anomaly Detection), 日志异常检测 (Log Anomaly Detection).
- Filter Options:** 学件名称: 日志异常检测学件-LmsSso, 日志类型: 日志类型, 异常类型: 异常类型, 日志对象: 日志对象, 搜索.
- Time Range:** 异常状态: 请根据, 相对时间: 2021-11-20, 1天, 1周, 30天.
- Chart:** A bar chart showing log anomalies over time. The x-axis represents dates from 2021-11-20 00:00:00 to 2021-11-20 23:00:00. The y-axis ranges from 0 to 20. There are several green bars indicating anomalies, with a notable peak around 2021-11-20 17:00.
- Table:** A detailed table of detected anomalies. It includes columns: 警报排序 (Alert Order), 警报级别 (Alert Level), 学件名称 (Module Name), 日志类型 (Log Type), 日志对象 (Log Object), 异常类型 (Exception Type), 模拟内容 (Simulated Content), 异常描述 (Exception Description), 异常时间 (Exception Time), and 操作 (Operation). The table lists 6 entries, all marked as '正常' (Normal).

Right Screenshot (c.s.c.l.a.s.CallService Service):

- Top Bar:** 日志异常检测 (Log Anomaly Detection), 日志异常检测 (Log Anomaly Detection), 日志异常检测 (Log Anomaly Detection).
- Filter Options:** 学件名称: 日志异常检测学件-LmsSso, 日志类型: LmsSso, 异常类型: 异常类型, 日志对象: c.s.c.l.a.s.CallService, 搜索.
- Time Range:** 2021-11-20, 1天, 1周, 30天.
- Chart:** A bar chart showing log anomalies over time. The x-axis represents dates from 2021-11-20 00:00:00 to 2021-11-20 23:00:00. The y-axis ranges from 0 to 60. A single red bar is visible at approximately 2021-11-20 18:30:00.
- Table:** A detailed table of detected anomalies. It includes columns: 警报排序 (Alert Order), 警报级别 (Alert Level), 学件名称 (Module Name), 日志类型 (Log Type), 日志对象 (Log Object), 异常类型 (Exception Type), 模拟内容 (Simulated Content), 异常描述 (Exception Description), 异常时间 (Exception Time), and 操作 (Operation). The table lists 1 entry, marked as '异常' (Abnormal).
- Bottom Panel:** Includes a '异常时段' (Abnormal Period) section showing the period from 2021-11-20 19:30:00 to 2021-11-20 19:45:00, and a '异常日志摘要' (Summary of Abnormal Log) table with one row: E4C9CCA725FF200C6, 异常日志摘要: '请求头包含必需的 request-CSMS content * Envelope encls * http://schemas.xmlsoap.org/soap/envelope * Header', 异常日志: '请求头包含必需的 request-CSMS content * Envelope encls * http://schemas.xmlsoap.org/soap/envelope * Header.', 日志数: 18, 操作: '查看'.

Knowledge Graph will be constructed by log detection and potential root cause analysis





Thank you