Chronix: Long Term Storage and Retrieval Technology for Anomaly Detection in Operational Data

Florian Lautenschlager,[1] Michael Philippsen,[2] Andreas Kumlehn,[2] and Josef Adersberger[1]

[1]QAware GmbH, Munich, Germany [2]University Erlangen-Nürnberg (FAU), Programming Systems Group, Erlangen

Abstract

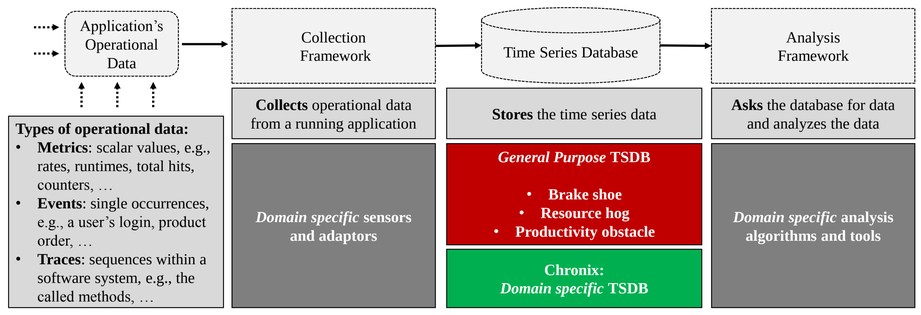
Anomalies in the runtime behavior of software systems, especially in distributed systems, are inevitable, expensive, and hard to locate. To detect and correct such anomalies one has to automatically collect, store, and analyze the operational data of the runtime behavior, often represented as time series. There are efficient means both to collect and analyze the runtime behavior. **But general-purpose time series databases do not focus on the specific needs of anomaly detection. Chronix is a domain specific time series database targeted at anomaly detection in operational data.**

Detecting Anomalies in Running Software matters

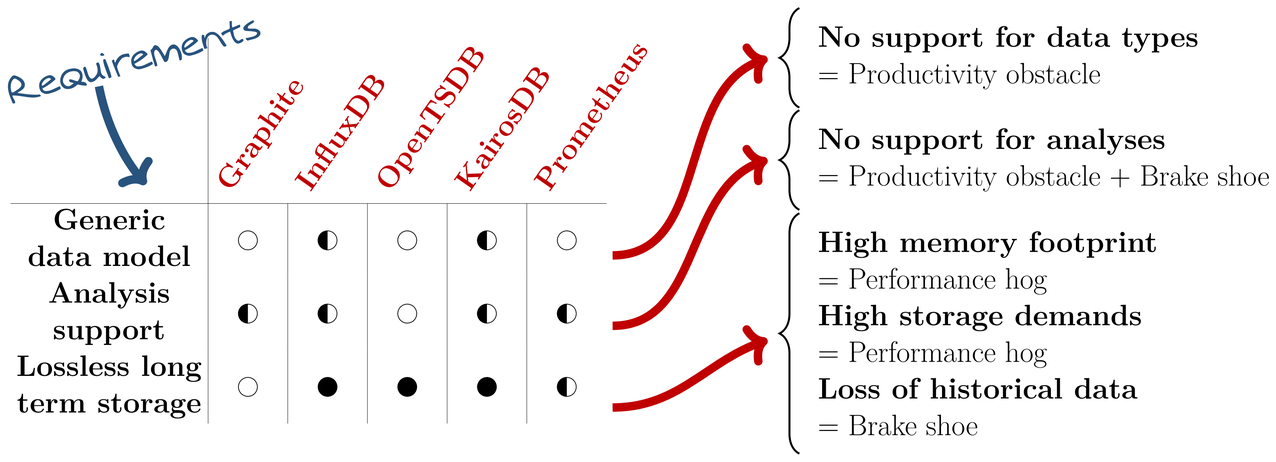
- **Resource consumption:** anomalous memory consumption, high CPU usage, …
- **Sporadic failure:** blocking state, deadlock, dirty read, …
- **Security:** port scanning activity, short frequent login attempts, …

↪ **Economic or reputation loss.**

Anomaly Detection Tool Chain for Operational Data



General-purpose TSDBs in Anomaly Detection

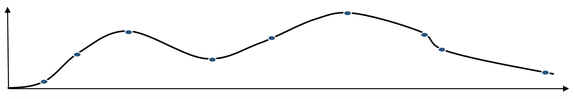


What makes Chronix domain specific?

1. Option to pre-compute an extra representation of the data
2. Optional timestamp compression for almost-periodic time series
3. Records that meet the needs of the domain
4. Compression technique that suits the domain's data
5. Underlying multi-dimensional storage
6. Domain specific query language with server-side evaluation
7. Domain specific commissioning of configuration parameters

How it works!

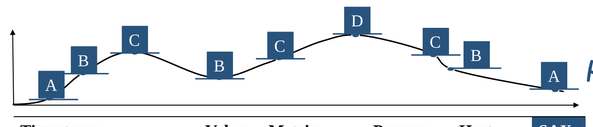
Example: Almost-periodic time series



Timestamp	Value	Metric	Process	Host
25.10.2016 00:00:01.546	218.34	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:06.718	218.37	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:11.891	218.49	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:16.964	218.35	ingester\time	SmartHub	QAMUC
…	…	…	…	…

Select the ideal Compression!

① Optional Pre-compute Extras

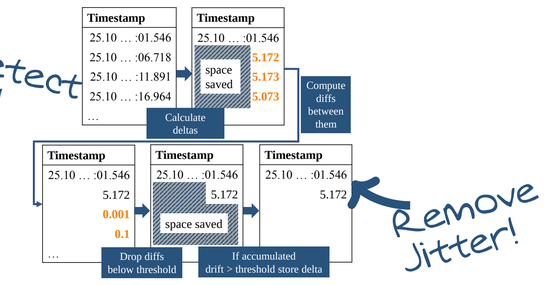


Timestamp	Value	Metric	Process	Host	SAX
25.10.2016 00:00:01.546	218.34	ingester\time	SmartHub	QAMUC	A
25.10.2016 00:00:06.718	218.37	ingester\time	SmartHub	QAMUC	B
25.10.2016 00:00:11.891	218.49	ingester\time	SmartHub	QAMUC	C
25.10.2016 00:00:16.964	218.35	ingester\time	SmartHub	QAMUC	B
…	…	…	…	…	…

Easily detect Pattern!

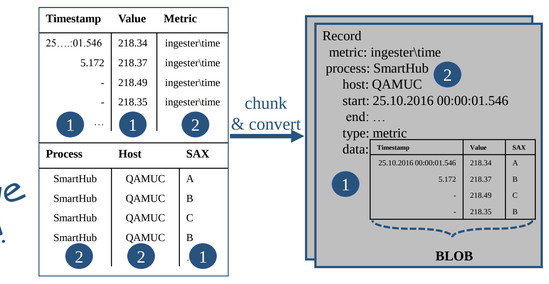
- **Lossless storage** that keeps all details as analyses may need them.
- `Programming interface` to add extra domain specific "columns".
- These "columns" **speed up anomaly detection** queries.

② Optional Timestamp Compaction



- **Date-Delta-Compaction** for almost-periodic time series.
- **Functionally lossless** as all relevant details are kept.
- Degree of inaccuracy is a configuration parameter of ⑦

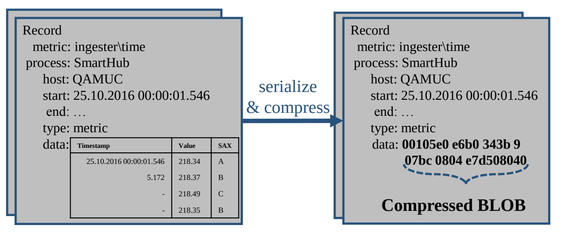
③ Domain Specifc Records



- **Exploit repetitiveness** and bundle 'lines' into data chunks.
- `Programming interface` for a specifc time series record encoding.
- Chunk size is a configuration parameter of ⑦

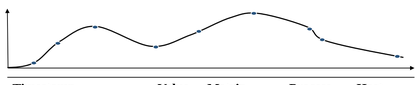
Projects 1–3

④ Domain Specific Compression



- **Lossless compression** techniques minimizes the record size.
- Domain data often has small increments, recurring patterns, etc.
- Choice of compression technqiue is a configuration parameter of ⑦

⑤ Multi-Dimensional Storage

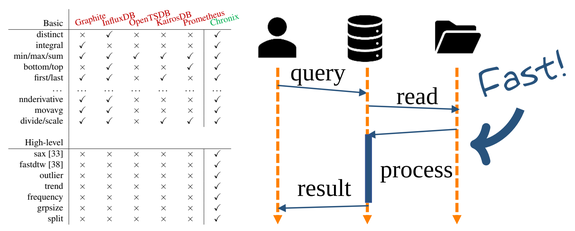


Timestamp	Value	Metric	Process	Host
25.10.2016 00:00:01.546	218.34	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:06.718	218.37	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:11.891	218.49	ingester\time	SmartHub	QAMUC
25.10.2016 00:00:16.964	218.35	ingester\time	SmartHub	QAMUC
…	…	…	…	…

```
q=host:QAMUC AND metric:ingester*
AND type:[metric OR trace] AND end:NOW-7MONTH
```

- **Explorative:** Users can use the attributes to find a record.
- **Correlating:** Queries can use and combine all types.

⑥ Query Language & Server-Side eval.

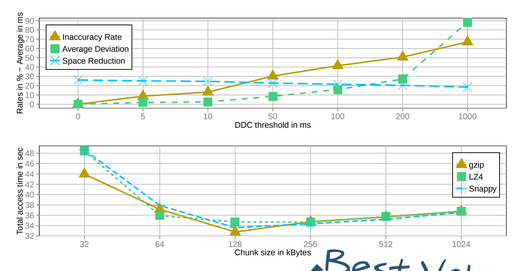



```
q=metric:ingester* & cf=outlier
```

- **Basic functions & high-level** built-in domain specific functions.
- `Plug-in interface` to add functions for server-side evalution.

Projects 1–3

⑦ Domain Specific Commissioning

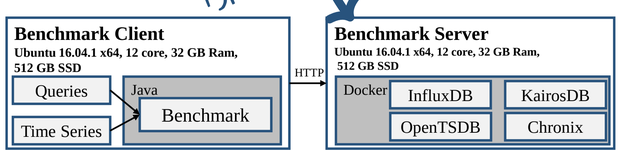


- **DDC-Threshold:** 200 ms.
- **Compression & Chunk Size:** gzip + 128 kByte.

Best Values!

Evaluation

Typical scenario.



Data of 5 Industry Projects.

	Project	1	2	3	4	5	total
	time series	1,080	8,567	4,538	500	24,055	38,740
pairs (mio)	metric	2.4	331.4	162.6	3.9	3,762.3	4,262.6
	lsof	0.0	0.0	0.0	0.4	0.0	0.4
	strace	0.0	0.0	0.0	12.1	0.0	12.1

(a) Pairs and time series per project.

Project	r	0.5	1	7	14	21	28	56	91	180	
1 – 3	q	15	30	30	10	5	3	1	2	0	96
	q	2	11	15	8	12	5	1	2	2	58
4 & 5	b	1	6	5	7	2	4	4	1	2	32
	h	2	6	10	8	6	6	3	2	0	43

(b) Time ranges r (days) and occurrences of queries (q) for raw data retrieval, and of queries with basic (b) and high-level (h) functions.

Evaluation: Projects 4 & 5

Memory footprint (in MBytes)

	InfluxDB	OpenTSDB	KairosDB	Chronix
Initially	33	2,726	8,763	446
Import (max)	10,336	10,111	18,905	7,002
Query (max)	8,269	9,712	11,230	4,792

Chronix has a 34%–69% smaller memory footprint.

Storage demands (in GBytes)

Project	Raw Data	InfluxDB	OpenTSDB	KairosDB	Chronix
4	1.2	0.2	0.2	0.3	0.1
5	107.0	10.7	16.9	26.5	8.6
total	108.2	10.9	17.1	26.8	8.7

Chronix saves 20%–68% of the storage space.

Needed for exploration!

Data retrieval times (in s)

r	q	InfluxDB	OpenTSDB	KairosDB	Chronix
0.5	2	4.3	2.8	4.4	0.9
1	11	5.2	5.6	6.6	5.3
7	15	34.1	17.4	26.8	7.0
14	8	36.2	14.2	25.5	4.0
21	12	76.5	29.8	55.0	6.0
28	5	7.9	3.9	5.6	0.5
56	1	35.4	12.4	24.1	1.2
91	2	47.5	15.5	33.8	1.1
180	2	96.7	36.7	66.6	1.1
total		343.8	138.3	248.4	27.1

Chronix saves 80%–92% on data retrieval time.

Times for b- and h-queries (in s)

	Basic (b)	InfluxDB	OpenTSDB	KairosDB	Chronix
4	Avg.	0.9	6.1	9.8	4.4
5	Max.	1.3	8.4	9.1	6.0
3	Min.	0.7	2.7	5.3	2.8
3	Dev.	6.7	16.7	21.1	2.3
5	Sum	0.7	6.0	12.0	2.0
4	Count	0.8	5.5	10.5	1.0
8	Perc.	10.2	25.8	34.5	8.6
	High-level (h)				
12	Outlier	30.7	29.1	117.6	18.9
14	Trend	162.7	50.4	100.6	30.2
11	Freq.	47.3	23.9	45.7	16.3
3	GroupSize	218.9	2927.8	206.3	29.6
3	Split	123.1	2893.9	47.9	37.2
75	total	604.0	5996.3	620.4	159.3

Important!

Chronix saves 73%–97% on analysis times.

Conclusion

Chronix exploits the characteristics of the domain in many ways and thus achieves better storage and query results. Chronix is open source.

www.chronix.io

Acknowledgements

This research was in part supported by the Bavarian Ministry of Economic Affairs and Media, Energy and Technology as an IuK-grant for the project DfD – Design for Diagnosability.