telelink
business
services

Beyond the Noise:

Automated RCA & Scalable Reporting in Zabbix

A Croatian Telecom Case Study

Aldin Osmanagić,
System Engineer,
Telelink Business Services (TBS)

telelink
business
services

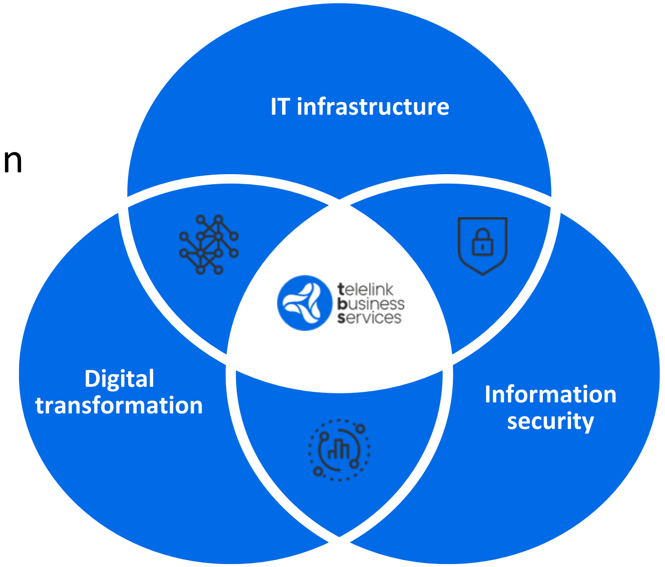
About Us

About Telelink Business Services (TBS)

Who are we?

TBS is a leading ICT solutions provider delivering end-to-end technologies that help businesses run efficiently, protect their data, and enable digital transformation.

Product groups



Software and infrastructure projects

We specialize in custom made solutions for each user, with experience across public and private sectors - from education and healthcare to finance.

Who am I?

Aldin Osmanagić, TBS System Engineer

- Zabbix Certified Expert
- Active in Zabbix Community Since 2011
- Over 20 Years in Open-Source Technologies
- Blog: bestmonitoringtools.com
- Contact: aldin.osmanagic@tbs.tech

Partners

CISCO · F5 · ZABBIX · FORTINET · IBM

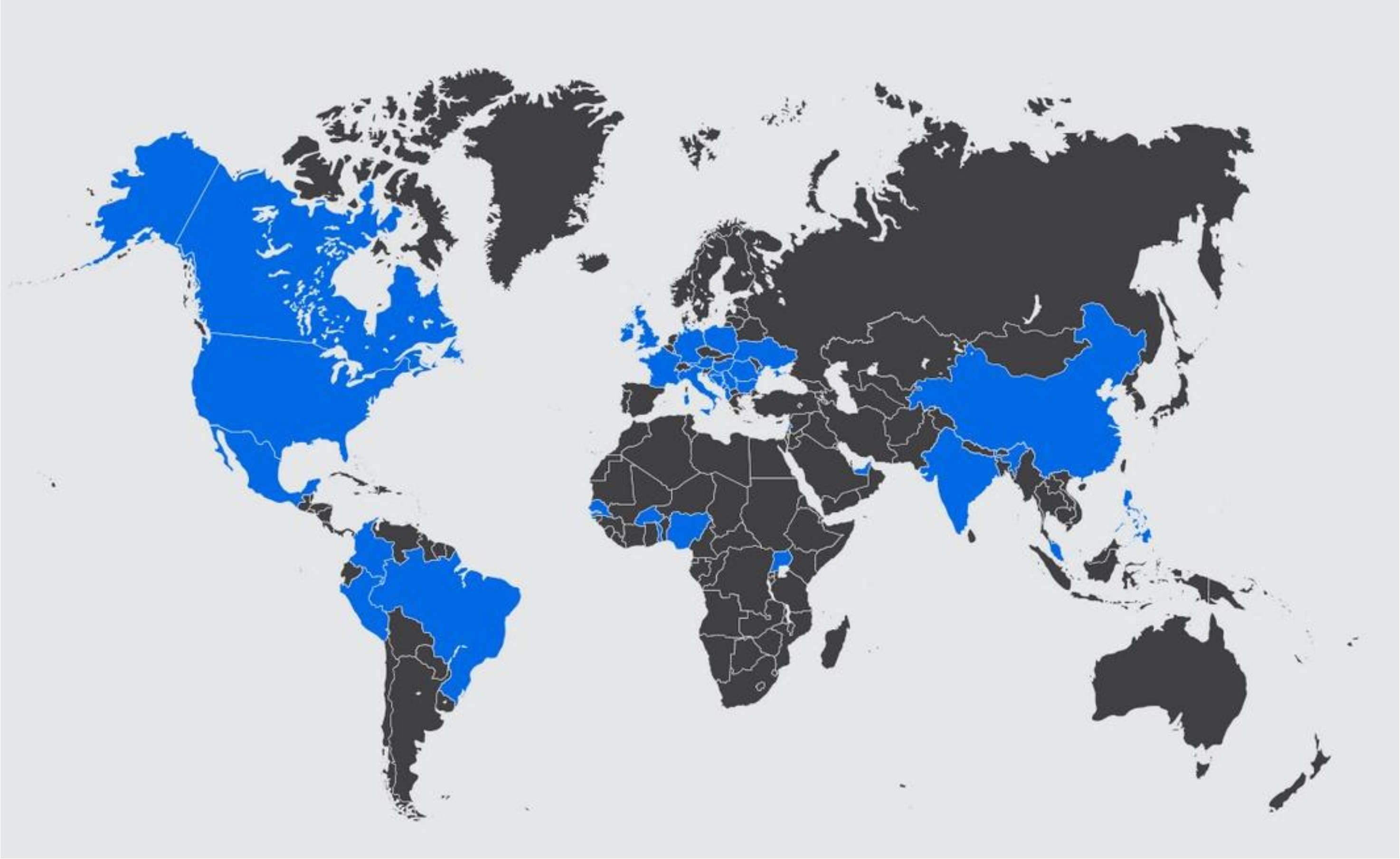
Microsoft · DELL Technologies · THALES · paloalto networks

CYBERARK · aruba a Hewlett Packard Enterprise company · Checkpoint · veeAM

telelink business services

Office Locations and Business Presence

Bulgaria
Bosnia and Herzegovina
Croatia
Germany
Ireland
North Macedonia
Romania
Serbia
Slovenia
UK
USA

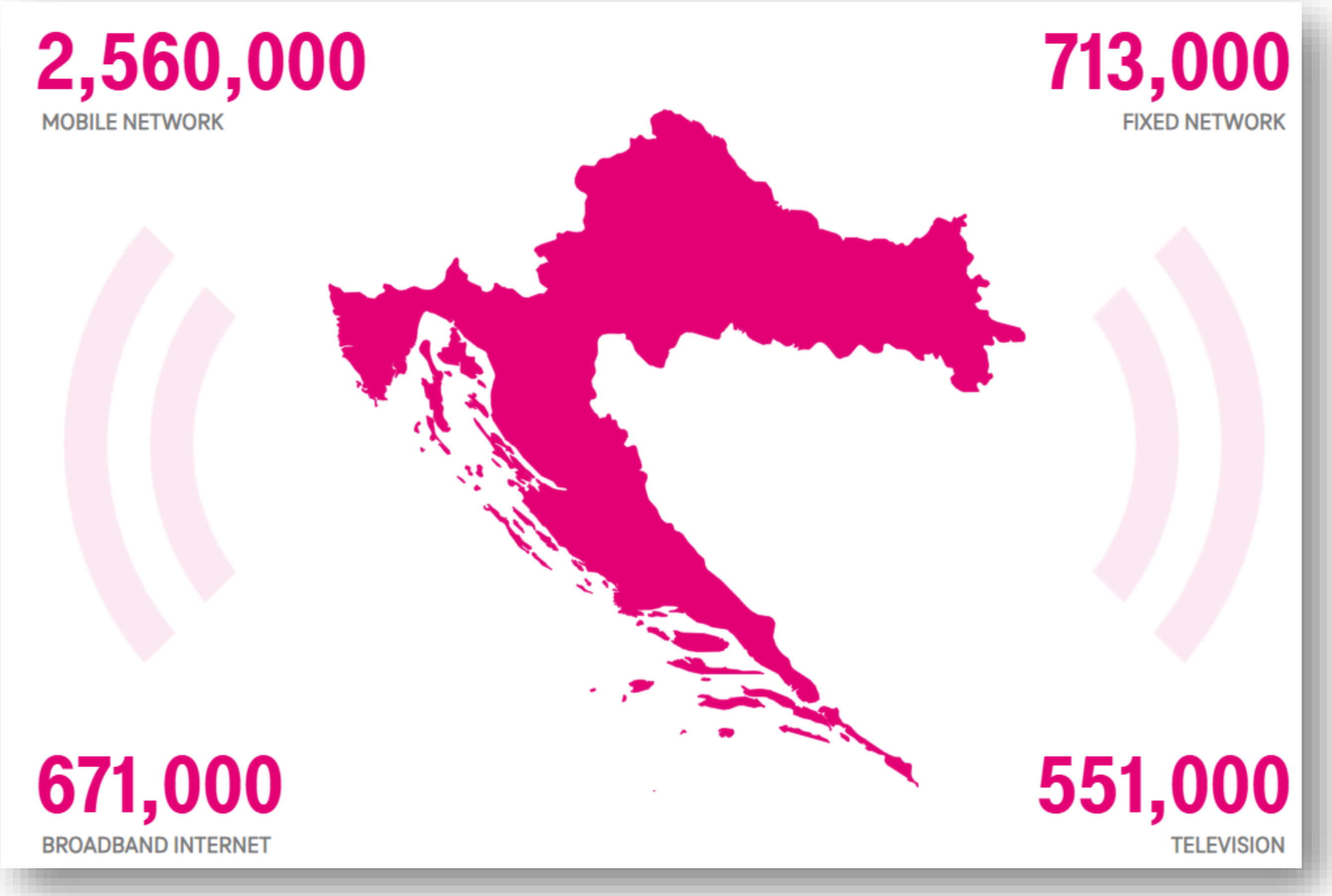


telelink
business
services

Case study: Croatian Telecom

Croatian Telecom Inc.

- Croatian Telecom (locally known as Hrvatski Telekom – part of the Deutsche Telekom Group) is market leader in Croatia providing with full range of telecommunications services, fixed line and mobile telephone services, data transmission, internet and international communications.



Customer Monitoring Requirements

- **Availability & Reliability**: High availability, backup/restore, disaster recovery.
- **Scalability**: Support for large-scale environments, including 20,000+ monitored devices and 1,000,000+ network interfaces.
- **Administration**: Centralized system management, SNMPv3 support, performance and fault integration.
- **Data Collection**: Interfaces with various systems and data sources, with built-in support for data preprocessing, transformation, and manipulation.
- **Advance Alarming:** Reduce false positive alarms, root cause analysis, trend prediction, anomaly detection, and hysteresis support.
- **Reporting & Visualization**: High-level dashboards, scalable reporting, and live views.
- **Security**: User access control, secure protocols, audit logging.
- **Integration**: APIs for external systems, CMDB synchronization, ticketing system integration.
- …etc.

Zabbix Met the Challenge

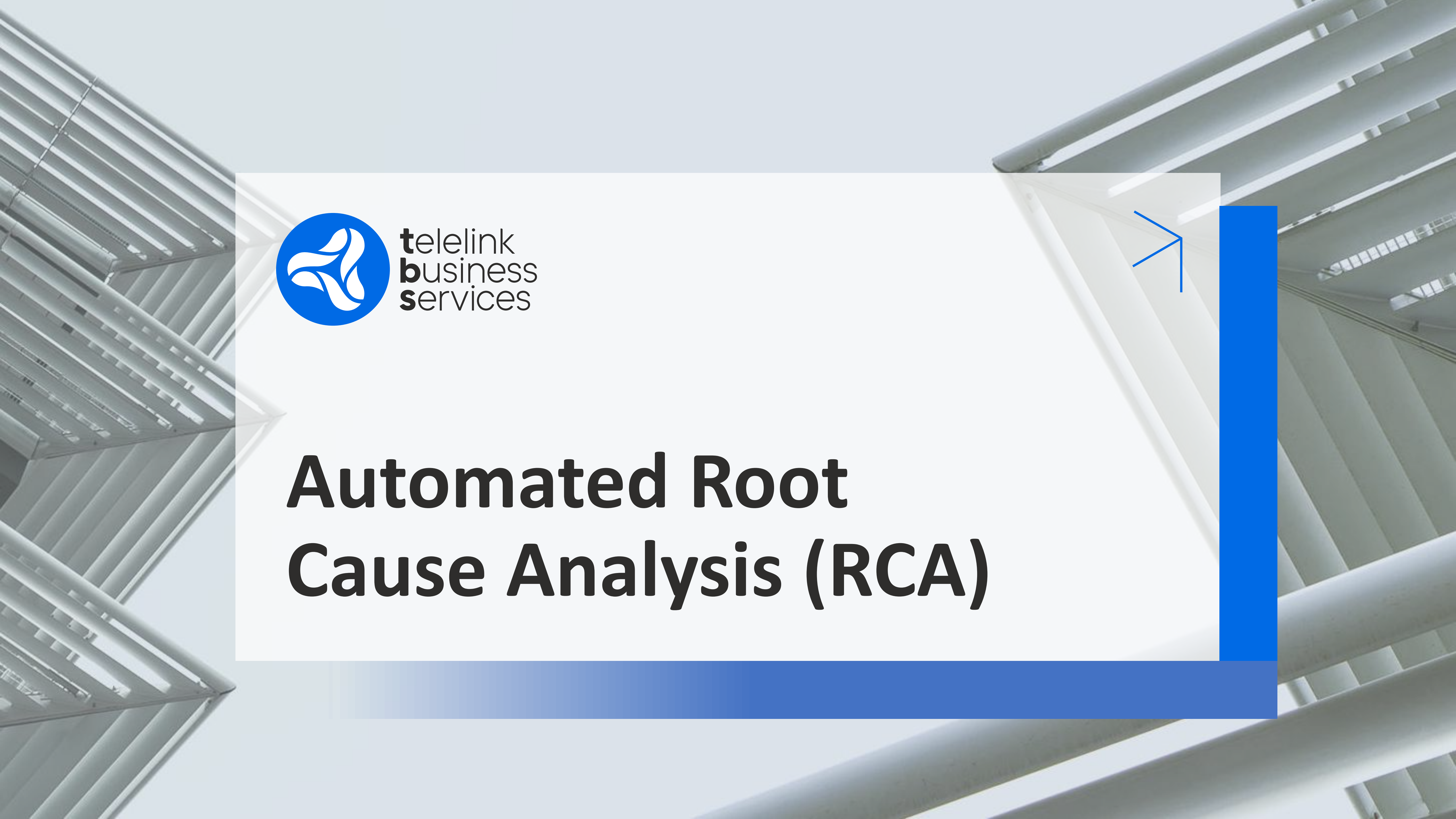
- Zabbix has been successfully implemented at Croatia Telekom, monitoring the entire network:
  - 17k hosts
  - 15 million items
  - 800k triggers
  - 32k new values per second (NVPS)
  - 30 proxy servers
  - 4 TB DB (TimescaleDB, 75% compression)

- **Vendors:** Cisco, Huawei, Juniper, HP, F5, Arbor, Ericsson, Nokia, Palo Alto, 3Com, Mikrotik …
- **Devices:** Routers, Switches, Firewalls, Load Balancers, BRAS, DSLAM, SBC, OLT, ONU/ONT …
- **Services:** Ethernet, QoS, VPN, VoIP, MPLS, BGP, Wi-Fi, xDSL, GPON, ACS, Sensors …

Zabbix Met the Challenge And We Took It Further

- Our team saw an opportunity to enhance Zabbix in these key areas:
  - **Advance Alarming:**
    Reduce false positive alarms, root cause analysis, trend prediction, anomaly detection, and hysteresis support.
  - **Reporting & Visualization**:
    High-level dashboards, scalable reporting, and live views.

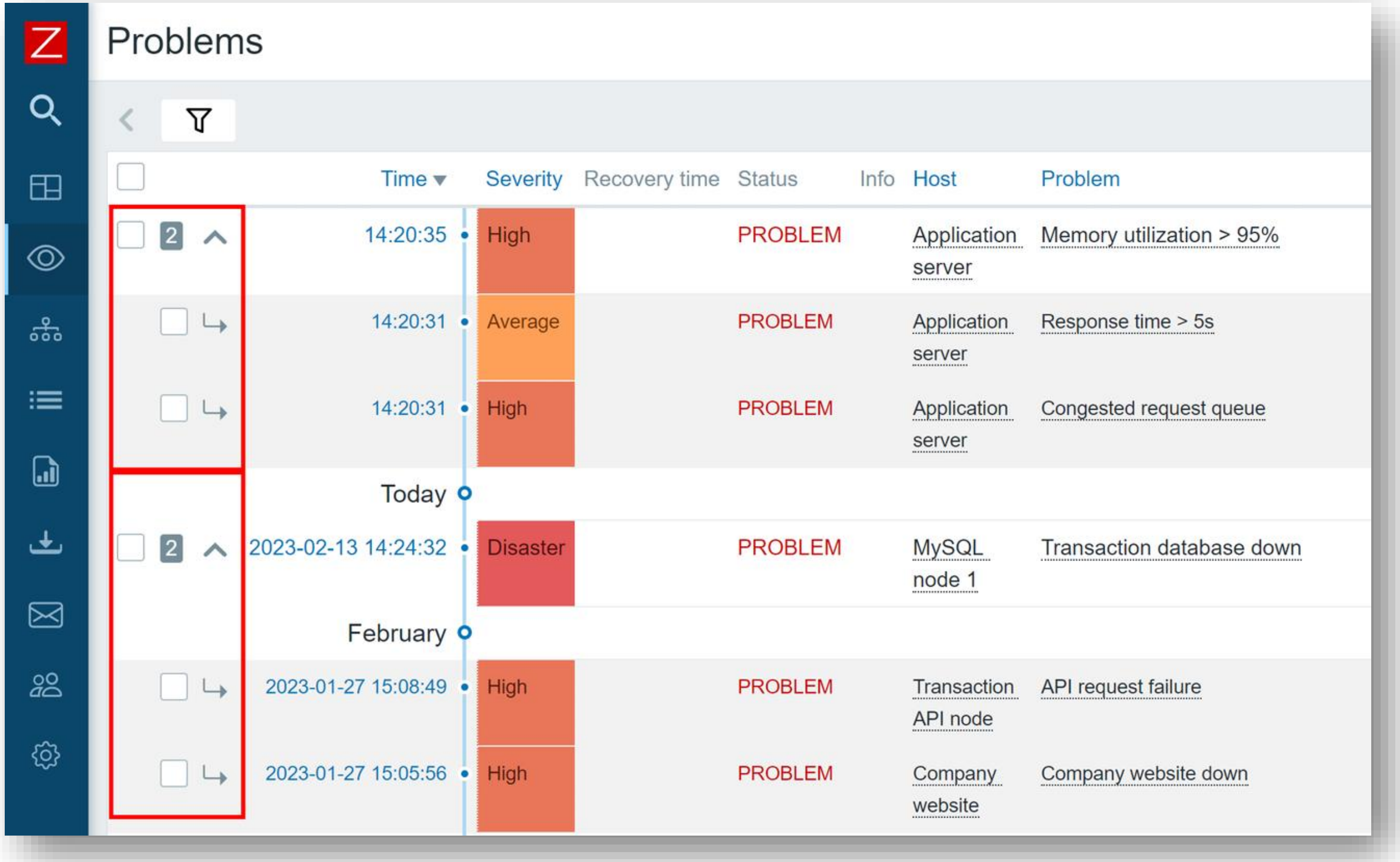
- And we developed custom solutions for Zabbix:
  - Automated Root Cause Analysis (RCA)
  - Advanced Scalable Live Reports



Automated Root Cause Analysis (RCA)

Zabbix Cause and Symptom Feature

- Since Zabbix 6.4 we can use Cause ↔ Symptom problem linking feature
- Zabbix documentation: “By default all new problems are classified as cause problems. It is possible to manually reclassify certain problems as symptom problems of the cause problem.”



Problems

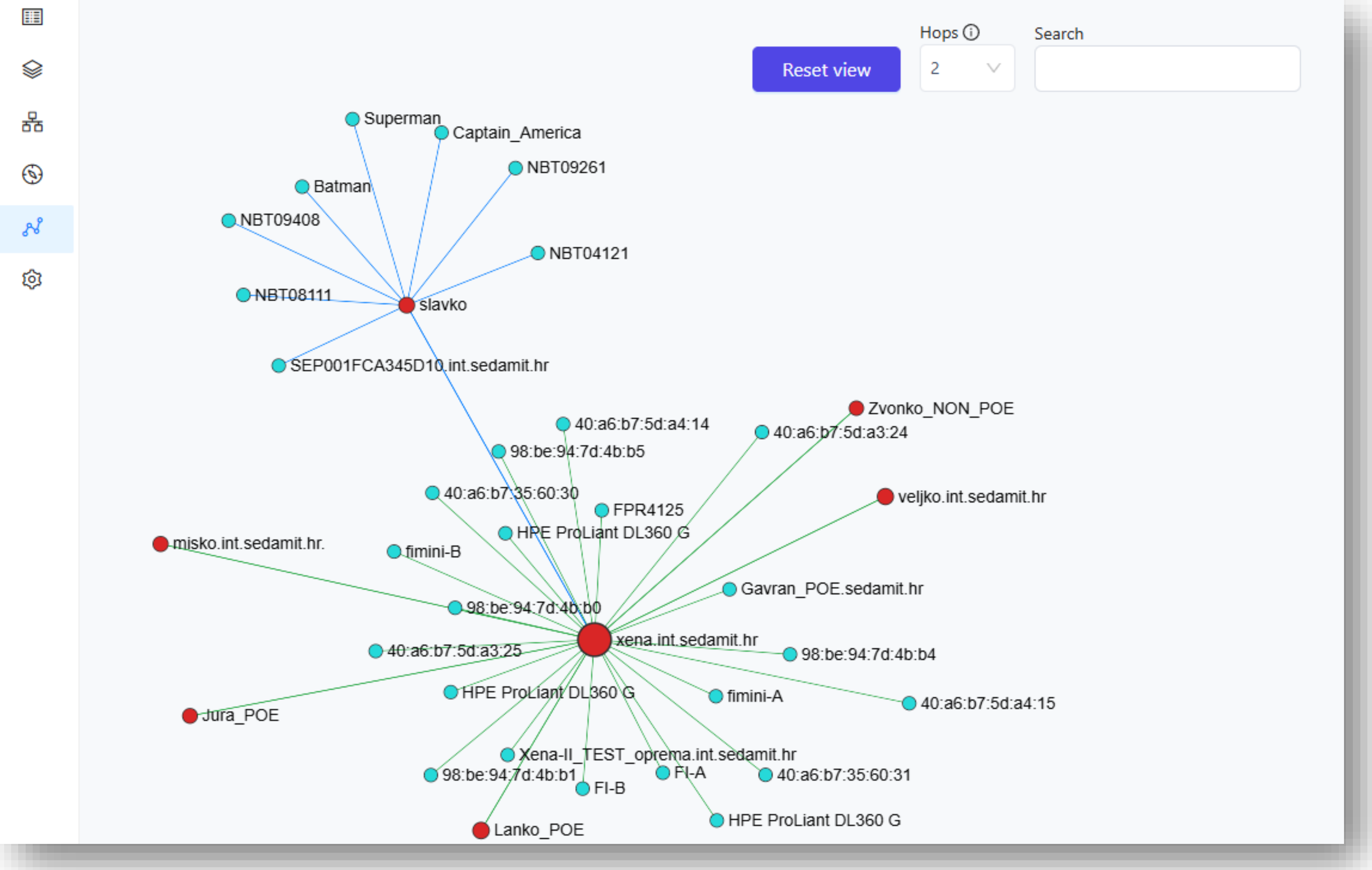
□	Time ▾	Severity	Recovery time	Status	Info	Host	Problem
□ 2 ^	14:20:35	High		PROBLEM		Application server	Memory utilization > 95%
□ ↳	14:20:31	Average		PROBLEM		Application server	Response time > 5s
□ ↳	14:20:31	High		PROBLEM		Application server	Congested request queue
	Today						
□ 2 ^	2023-02-13 14:24:32	Disaster		PROBLEM		MySQL node 1	Transaction database down
	February						
□ ↳	2023-01-27 15:08:49	High		PROBLEM		Transaction API node	API request failure
□ ↳	2023-01-27 15:05:56	High		PROBLEM		Company website	Company website down

From Manual to Automated Network RCA

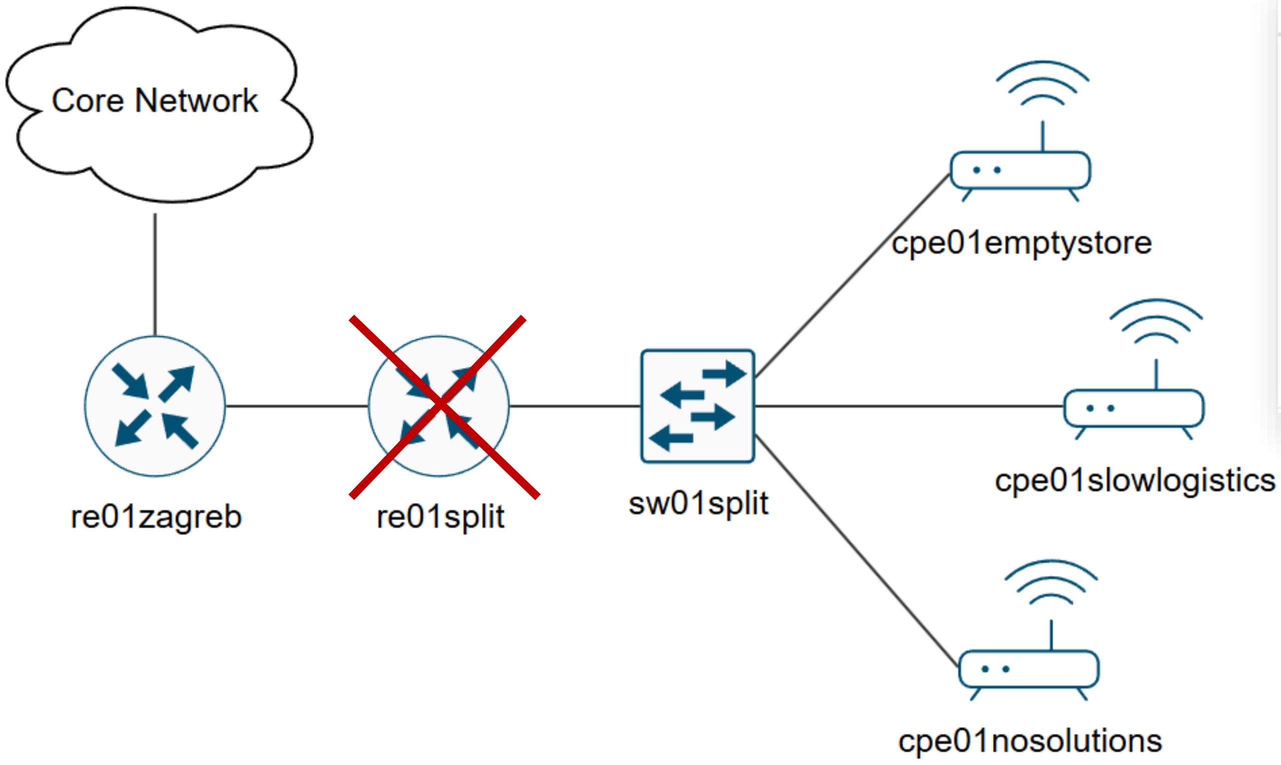
Custom-built agent collects network link data (LLDP) from devices via SNMP protocol.

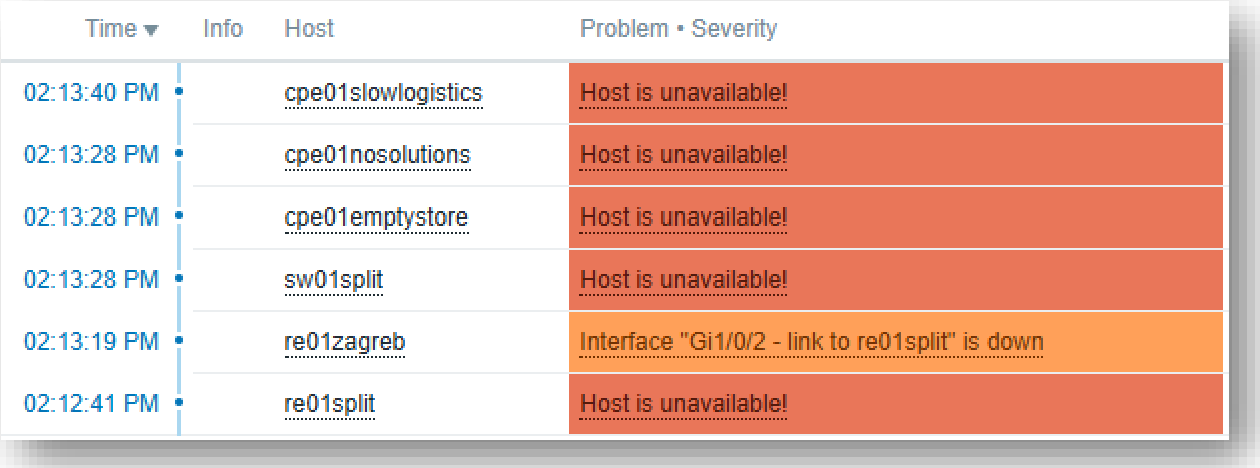
Backend service stores the collected data in a DB and assigns a ranking score to each device

RCA service runs every minute and updates cause-symptom on alarms via Zabbix API.



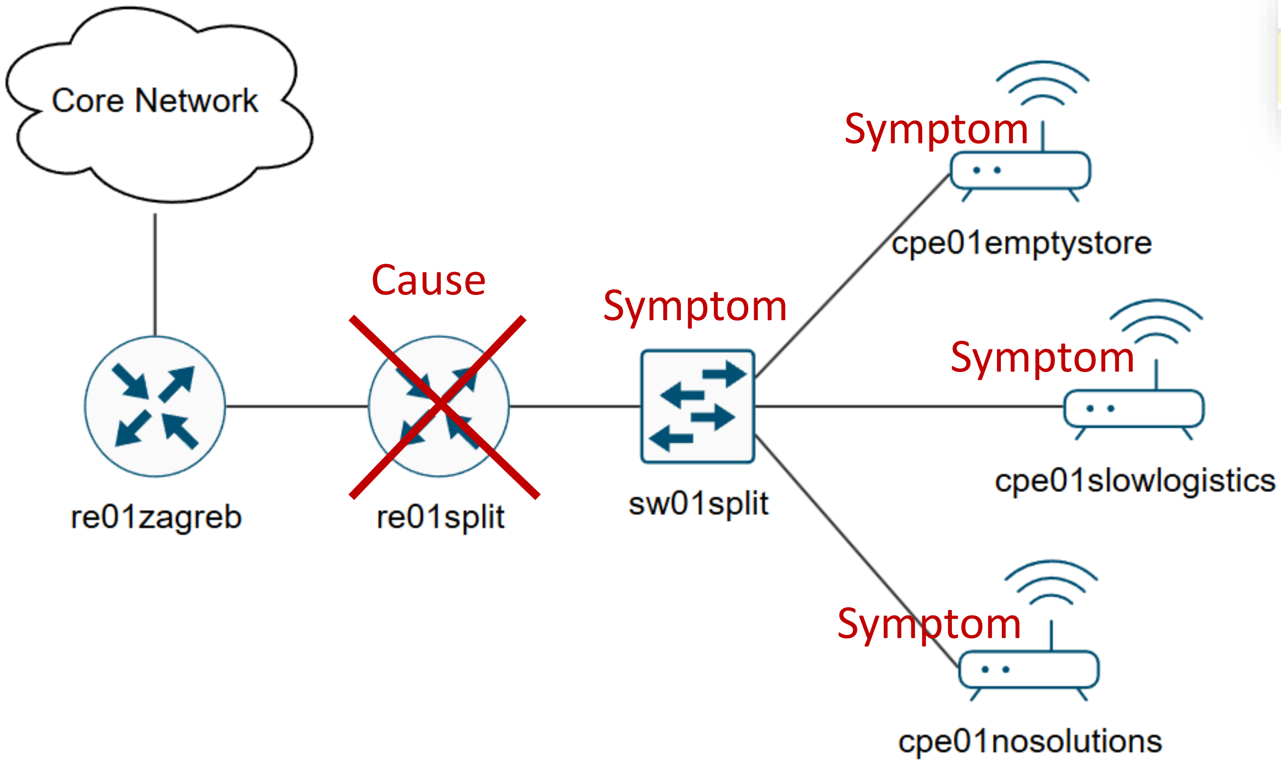
Automated RCA in Practice: Before

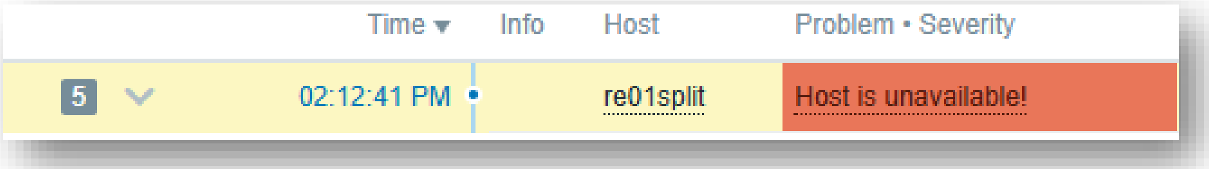




Time ▾	Info	Host	Problem • Severity
02:13:40 PM		cpe01slowlogistics	Host is unavailable!
02:13:28 PM		cpe01nosolutions	Host is unavailable!
02:13:28 PM		cpe01emptystore	Host is unavailable!
02:13:28 PM		sw01split	Host is unavailable!
02:13:19 PM		re01zagreb	Interface "Gi1/0/2 - link to re01split" is down
02:12:41 PM		re01split	Host is unavailable!

Automated RCA in Practice: After



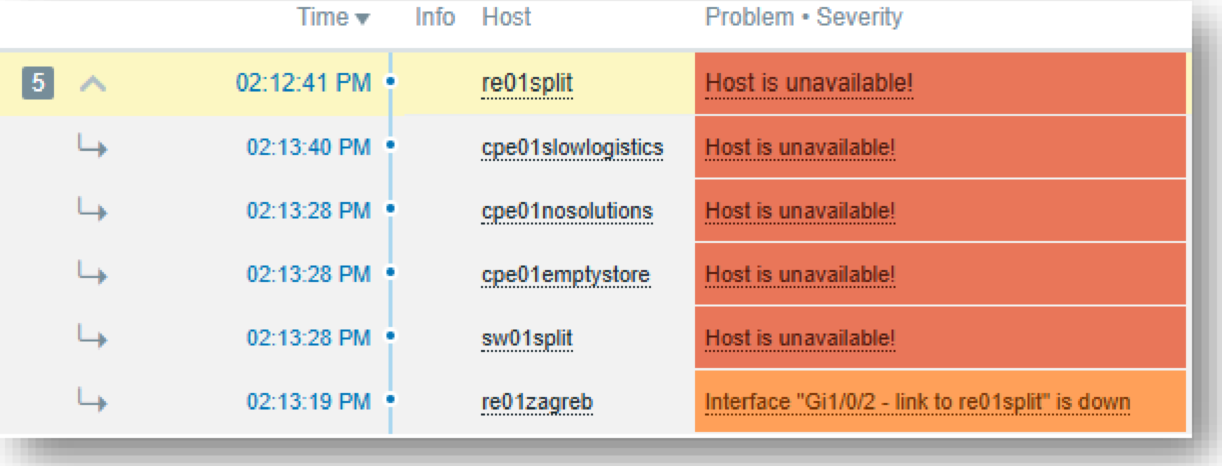


	Time ▾	Info	Host	Problem • Severity
5	02:12:41 PM	•	re01split	Host is unavailable!

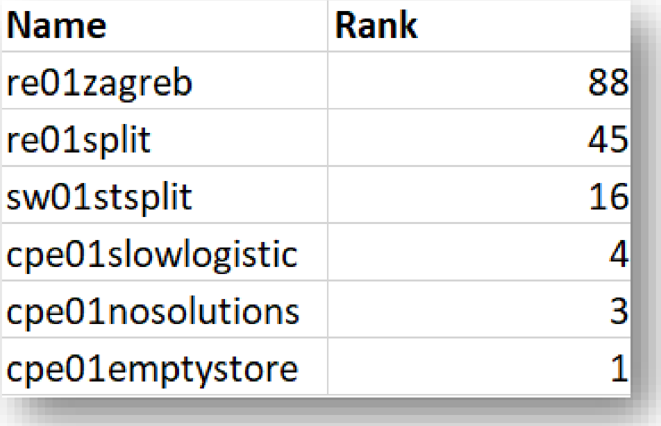
Determining the Root Cause Alarm

- A network link database can sometimes be misleading in determining the cause of an alarm.

- **An additional step is required that:**
  - calculates host importance using metrics such as the number of links, active ports, throughput…
  - and then assigns a ranking score to each device



		Time ▾	Info	Host	Problem • Severity
5	^	02:12:41 PM		re01split	Host is unavailable!
	↳	02:13:40 PM		cpe01slowlogistics	Host is unavailable!
	↳	02:13:28 PM		cpe01nosolutions	Host is unavailable!
	↳	02:13:28 PM		cpe01emptystore	Host is unavailable!
	↳	02:13:28 PM		sw01split	Host is unavailable!
	↳	02:13:19 PM		re01zagreb	Interface "Gi1/0/2 - link to re01split" is down

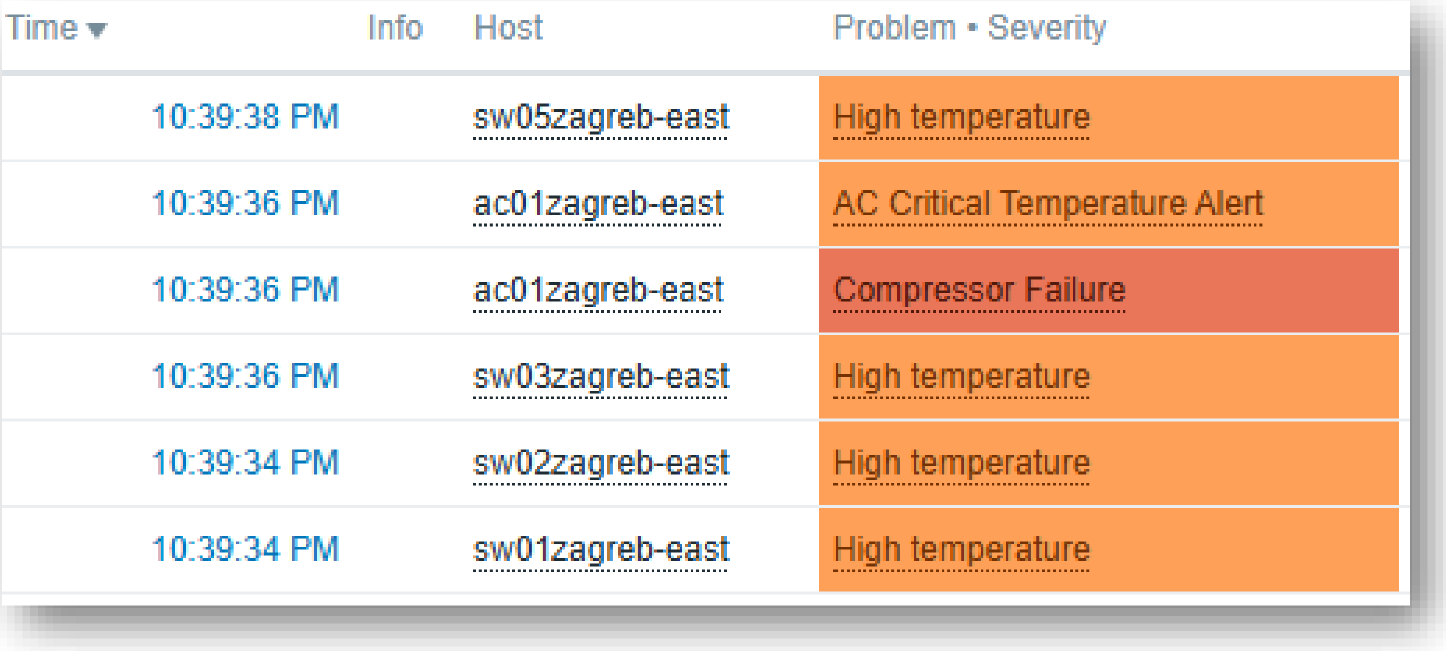


Name	Rank
re01zagreb	88
re01split	45
sw01stsplit	16
cpe01slowlogistic	4
cpe01nosolutions	3
cpe01emptystore	1

telelink business services

Reducing Alarm Noise with User-Defined RCA Rules

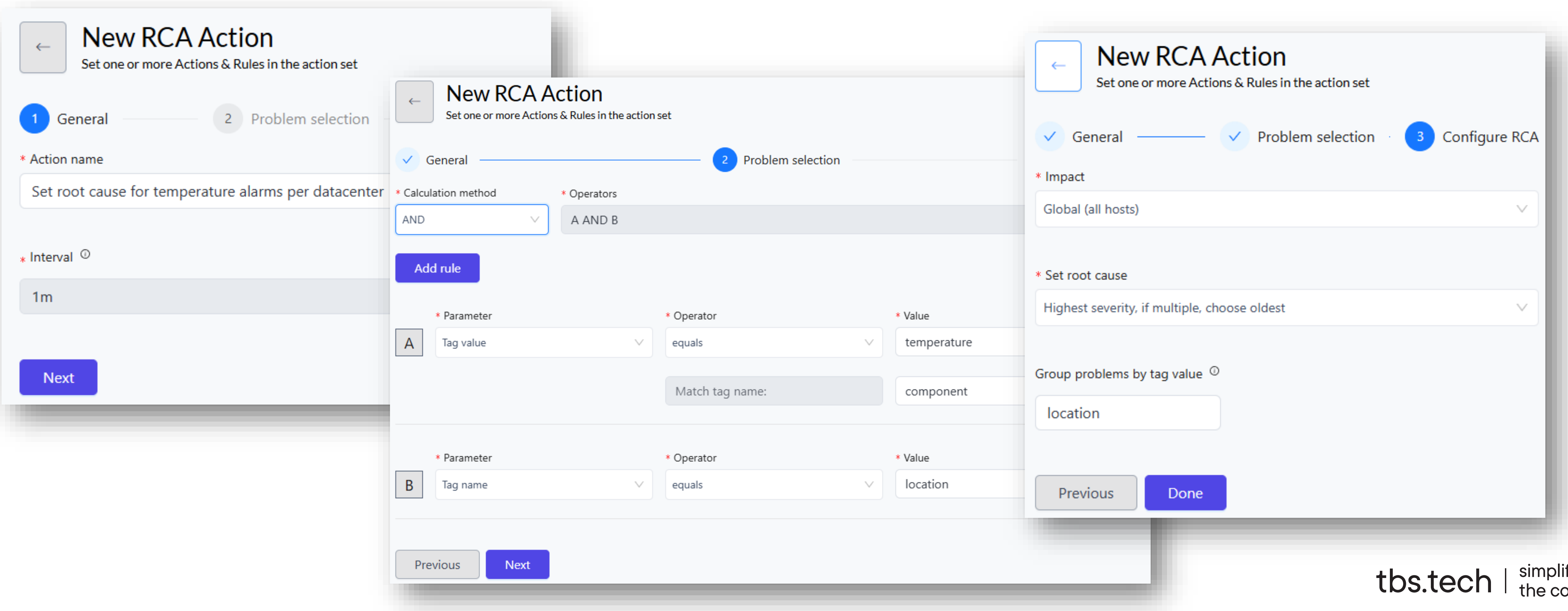
- Example of Zabbix alarms when air conditioning (AC) stops working correctly.



Time ▾	Info	Host	Problem • Severity
10:39:38 PM		sw05zagreb-east	High temperature
10:39:36 PM		ac01zagreb-east	AC Critical Temperature Alert
10:39:36 PM		ac01zagreb-east	Compressor Failure
10:39:36 PM		sw03zagreb-east	High temperature
10:39:34 PM		sw02zagreb-east	High temperature
10:39:34 PM		sw01zagreb-east	High temperature

Reducing Alarm Noise with User-Defined RCA Rules

- Create RCA rules based on Zabbix tags, problem names, host names, host groups, etc.



New RCA Action

Set one or more Actions & Rules in the action set

1 General — 2 Problem selection

* Action name: Set root cause for temperature alarms per datacenter

* Interval: 1m

New RCA Action

Set one or more Actions & Rules in the action set

✓ General — 2 Problem selection

* Calculation method: AND

* Operators: A AND B

A

* Parameter: Tag value

* Operator: equals

* Value: temperature

Match tag name: component

B

* Parameter: Tag name

* Operator: equals

* Value: location

New RCA Action

Set one or more Actions & Rules in the action set

✓ General — ✓ Problem selection — 3 Configure RCA

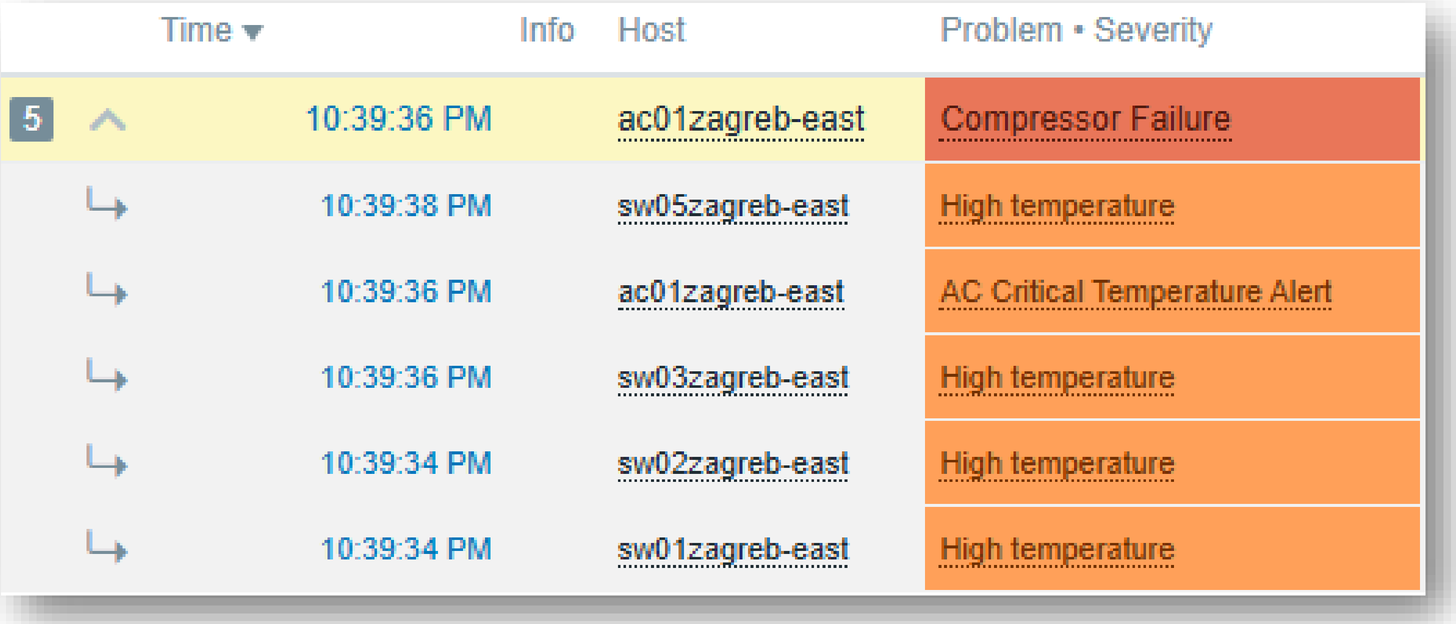
* Impact: Global (all hosts)

* Set root cause: Highest severity, if multiple, choose oldest

Group problems by tag value: location

Reducing Alarm Noise with User-Defined RCA Rules

CAUSE

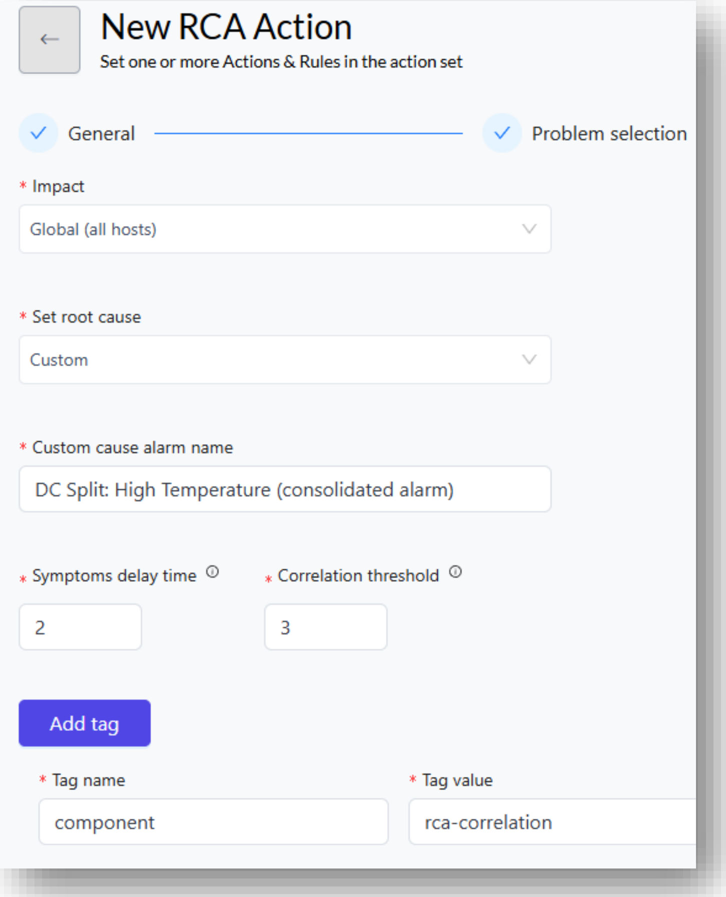


		Time ▼	Info	Host	Problem • Severity
5	^	10:39:36 PM		ac01zagreb-east	Compressor Failure
	↳	10:39:38 PM		sw05zagreb-east	High temperature
	↳	10:39:36 PM		ac01zagreb-east	AC Critical Temperature Alert
	↳	10:39:36 PM		sw03zagreb-east	High temperature
	↳	10:39:34 PM		sw02zagreb-east	High temperature
	↳	10:39:34 PM		sw01zagreb-east	High temperature

telelink business services

Reducing Alarm Noise with User-Defined RCA Rules

- Alternatively, automation can create a custom consolidation alarm



New RCA Action

Set one or more Actions & Rules in the action set

✓ General ✓ Problem selection

* Impact
Global (all hosts)

* Set root cause
Custom

* Custom cause alarm name
DC Split: High Temperature (consolidated alarm)

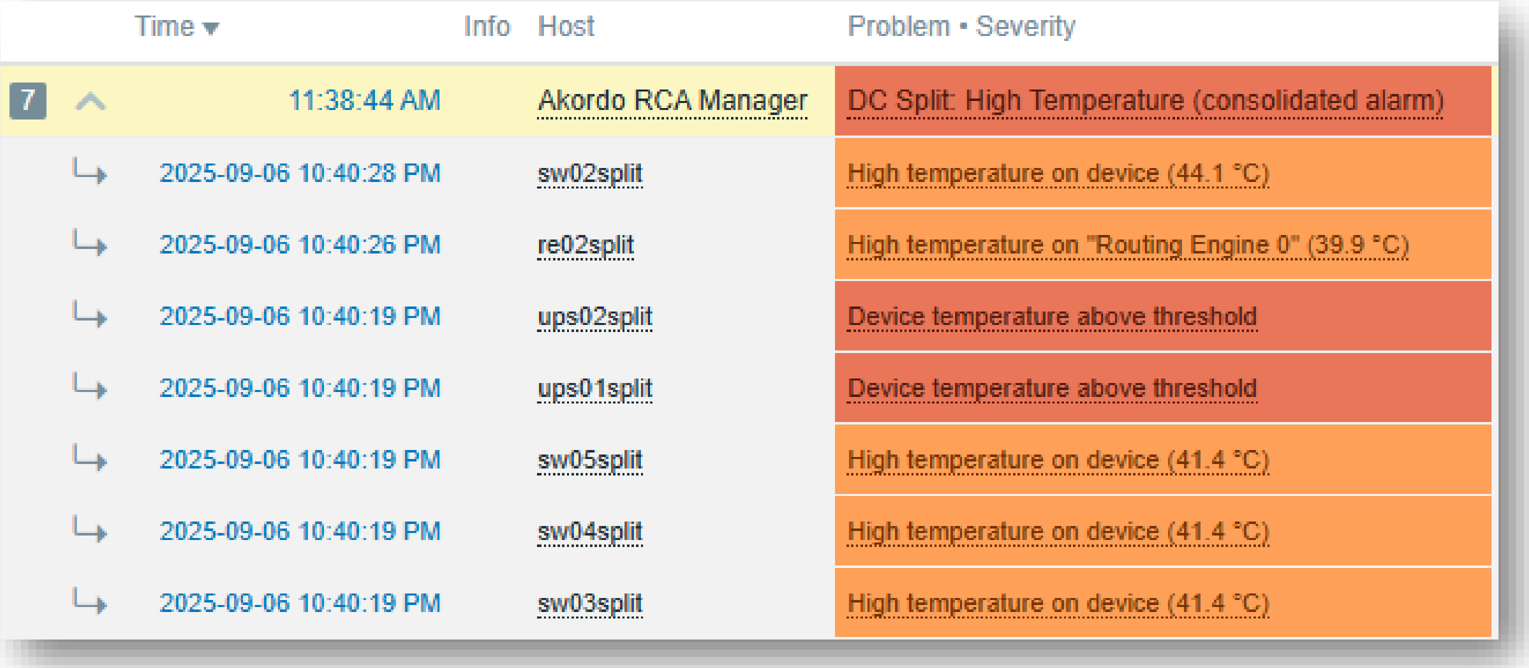
* Symptoms delay time
2

* Correlation threshold
3

Add tag

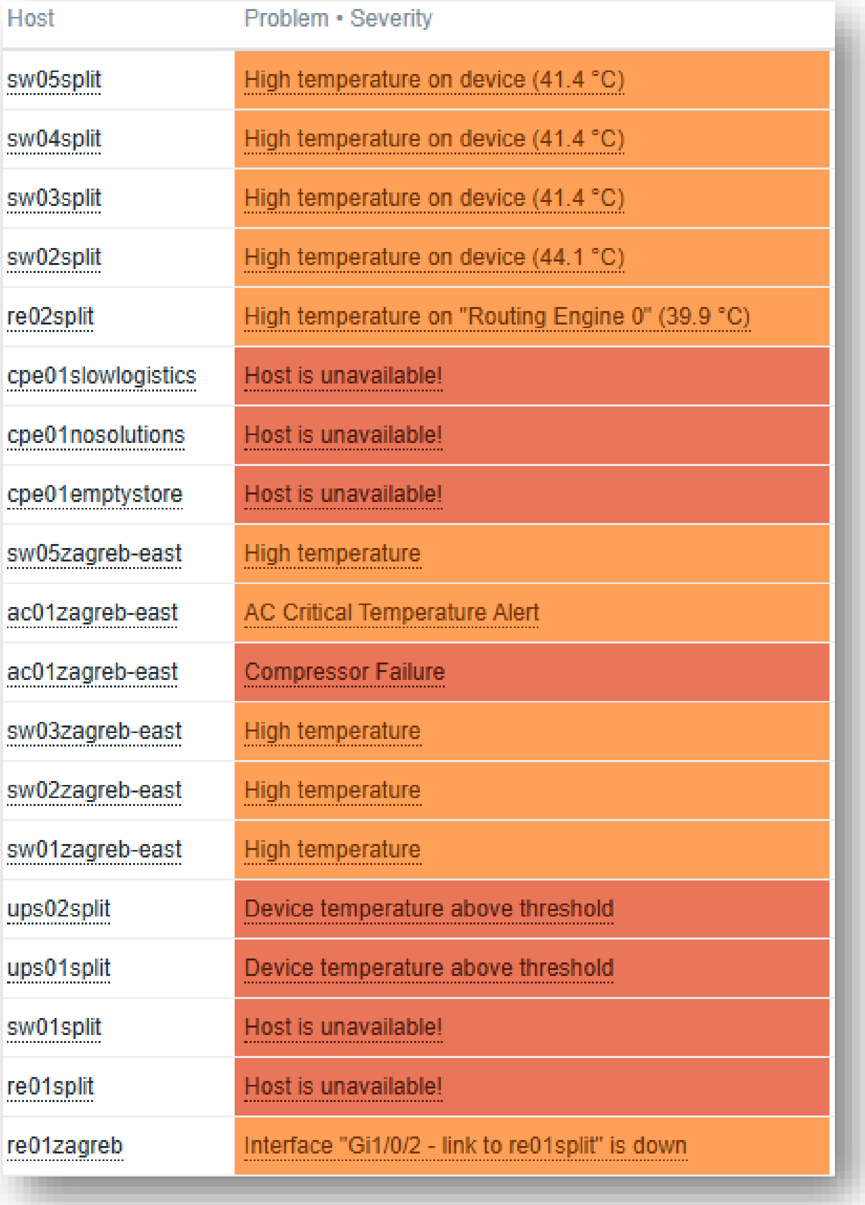
* Tag name
component

* Tag value
rca-correlation

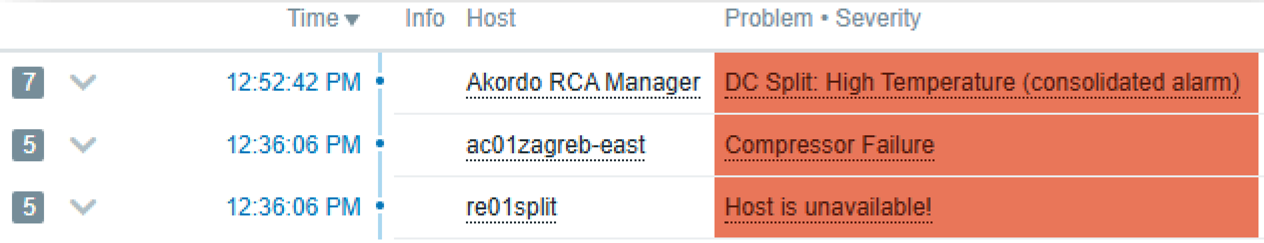


	Time ▾	Info	Host	Problem • Severity
7 ^	11:38:44 AM		Akordo RCA Manager	DC Split: High Temperature (consolidated alarm)
↳	2025-09-06 10:40:28 PM		sw02split	High temperature on device (44.1 °C)
↳	2025-09-06 10:40:26 PM		re02split	High temperature on "Routing Engine 0" (39.9 °C)
↳	2025-09-06 10:40:19 PM		ups02split	Device temperature above threshold
↳	2025-09-06 10:40:19 PM		ups01split	Device temperature above threshold
↳	2025-09-06 10:40:19 PM		sw05split	High temperature on device (41.4 °C)
↳	2025-09-06 10:40:19 PM		sw04split	High temperature on device (41.4 °C)
↳	2025-09-06 10:40:19 PM		sw03split	High temperature on device (41.4 °C)

As Zabbix Scales, RCA Must Be Automated



Host	Problem • Severity
sw05split	High temperature on device (41.4 °C)
sw04split	High temperature on device (41.4 °C)
sw03split	High temperature on device (41.4 °C)
sw02split	High temperature on device (44.1 °C)
re02split	High temperature on "Routing Engine 0" (39.9 °C)
cpe01slowlogistics	Host is unavailable!
cpe01nosolutions	Host is unavailable!
cpe01emptystore	Host is unavailable!
sw05zagreb-east	High temperature
ac01zagreb-east	AC Critical Temperature Alert
ac01zagreb-east	Compressor Failure
sw03zagreb-east	High temperature
sw02zagreb-east	High temperature
sw01zagreb-east	High temperature
ups02split	Device temperature above threshold
ups01split	Device temperature above threshold
sw01split	Host is unavailable!
re01split	Host is unavailable!
re01zagreb	Interface "Gi1/0/2 - link to re01split" is down



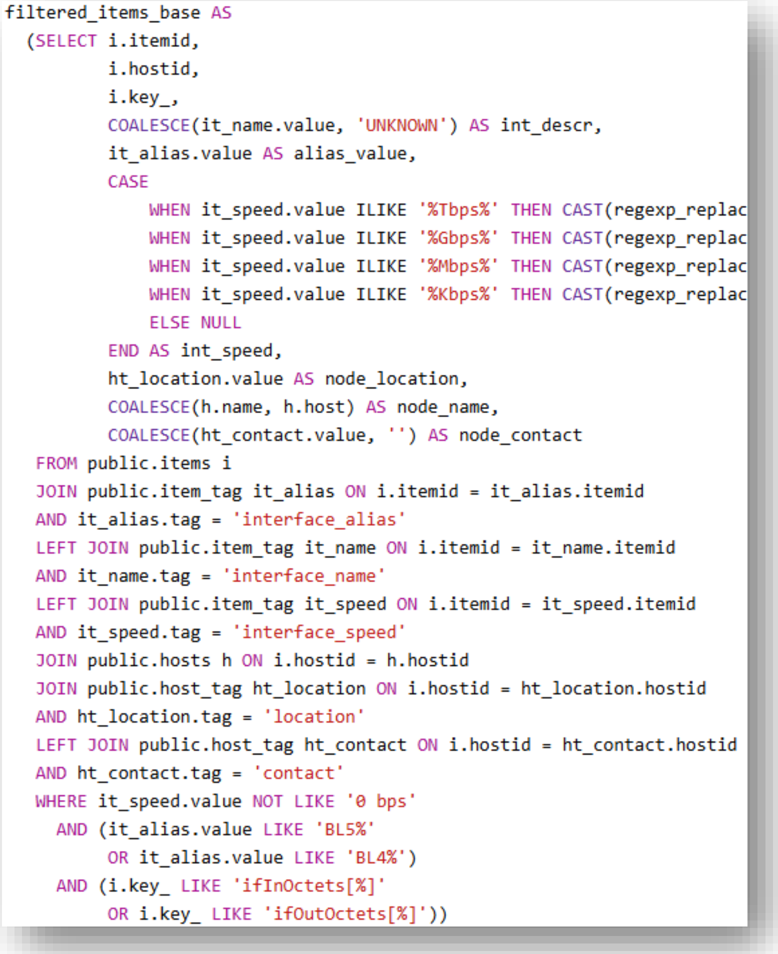
	Time ▾	Info	Host	Problem • Severity
7	12:52:42 PM		Akordo RCA Manager	DC Split: High Temperature (consolidated alarm)
5	12:36:06 PM		ac01zagreb-east	Compressor Failure
5	12:36:06 PM		re01split	Host is unavailable!

telelink
business
services

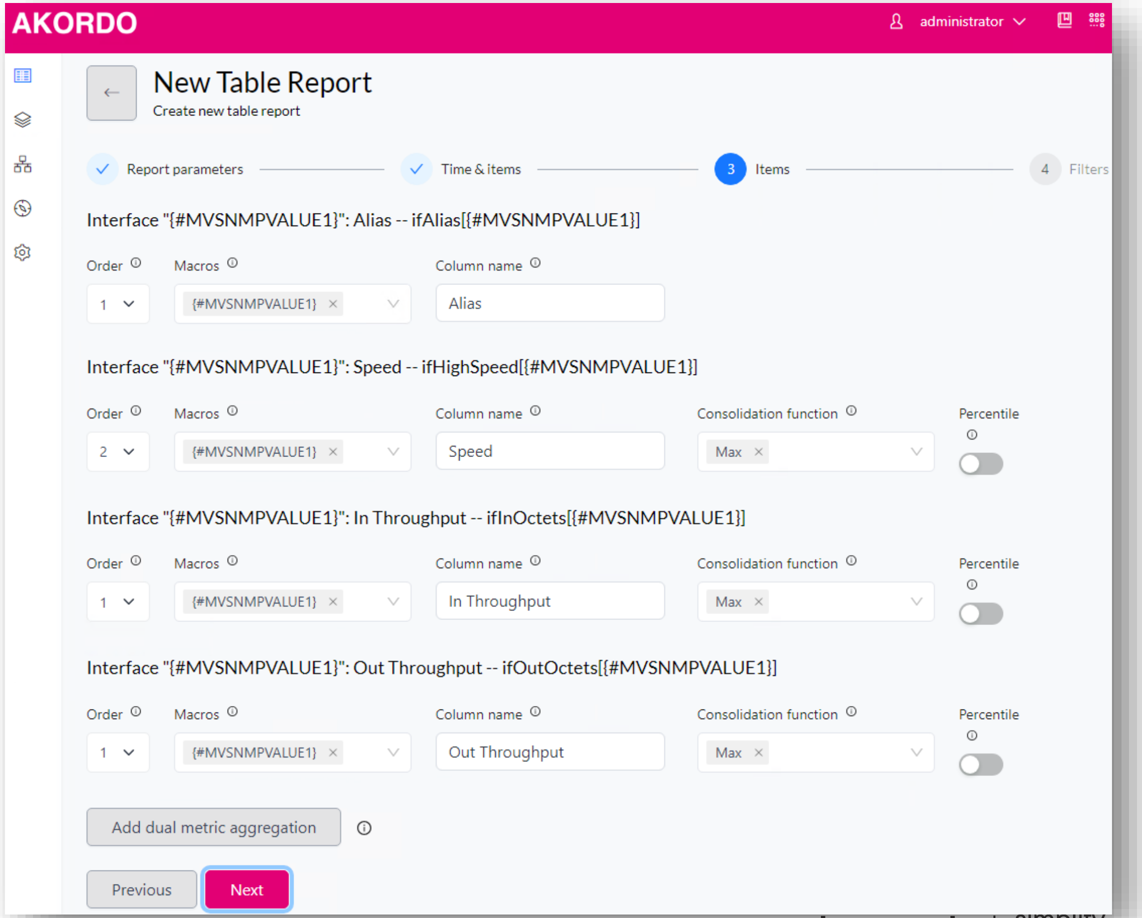
Advanced Scalable Live Reports

Solution for Large Reports:
No More SQL and Excel

- Visualize large reports with **100k+** rows in real time, directly in a web browser.



```
filtered_items_base AS
  (SELECT i.itemid,
          i.hostid,
          i.key_,
          COALESCE(it_name.value, 'UNKNOWN') AS int_descr,
          it_alias.value AS alias_value,
          CASE
              WHEN it_speed.value ILIKE '%Tbps%' THEN CAST(regexp_replac
              WHEN it_speed.value ILIKE '%Gbps%' THEN CAST(regexp_replac
              WHEN it_speed.value ILIKE '%Mbps%' THEN CAST(regexp_replac
              WHEN it_speed.value ILIKE '%Kbps%' THEN CAST(regexp_replac
              ELSE NULL
          END AS int_speed,
          ht_location.value AS node_location,
          COALESCE(h.name, h.host) AS node_name,
          COALESCE(ht_contact.value, '') AS node_contact
   FROM public.items i
   JOIN public.item_tag it_alias ON i.itemid = it_alias.itemid
   AND it_alias.tag = 'interface_alias'
   LEFT JOIN public.item_tag it_name ON i.itemid = it_name.itemid
   AND it_name.tag = 'interface_name'
   LEFT JOIN public.item_tag it_speed ON i.itemid = it_speed.itemid
   AND it_speed.tag = 'interface_speed'
   JOIN public.hosts h ON i.hostid = h.hostid
   JOIN public.host_tag ht_location ON i.hostid = ht_location.hostid
   AND ht_location.tag = 'location'
   LEFT JOIN public.host_tag ht_contact ON i.hostid = ht_contact.hostid
   AND ht_contact.tag = 'contact'
   WHERE it_speed.value NOT LIKE '0 bps'
     AND (it_alias.value LIKE 'BL5%'
          OR it_alias.value LIKE 'BL4%')
     AND (i.key_ LIKE 'ifInOctets[%]'
          OR i.key_ LIKE 'ifOutOctets[%]'))
```



New Table Report

Create new table report

Interface "{#MVSNMPVALUE1}": Alias -- ifAlias[{#MVSNMPVALUE1}]

Order: 1 | Macros: {#MVSNMPVALUE1} | Column name: Alias

Interface "{#MVSNMPVALUE1}": Speed -- ifHighSpeed[{#MVSNMPVALUE1}]

Order: 2 | Macros: {#MVSNMPVALUE1} | Column name: Speed | Consolidation function: Max | Percentile

Interface "{#MVSNMPVALUE1}": In Throughput -- ifInOctets[{#MVSNMPVALUE1}]

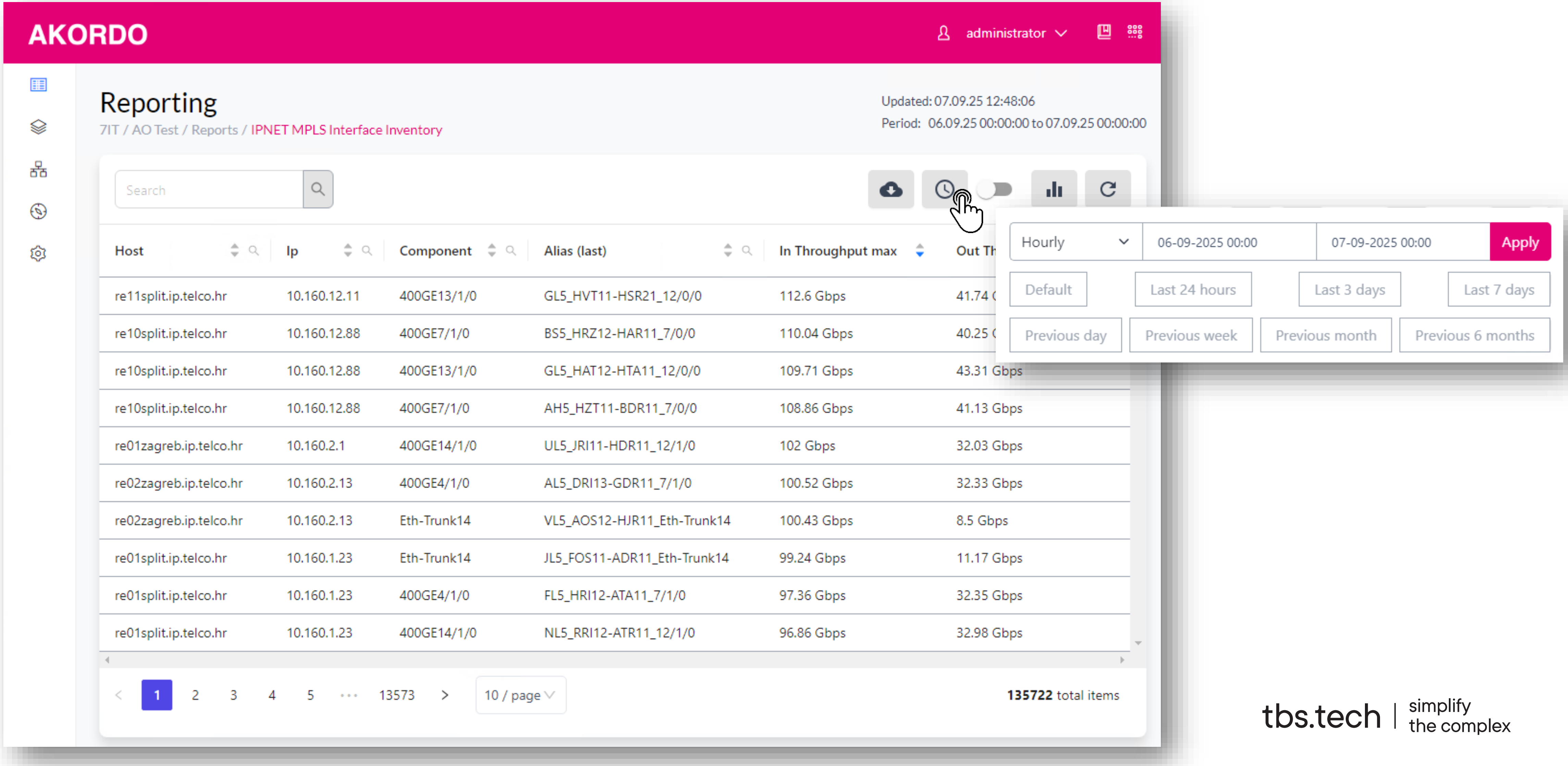
Order: 1 | Macros: {#MVSNMPVALUE1} | Column name: In Throughput | Consolidation function: Max | Percentile

Interface "{#MVSNMPVALUE1}": Out Throughput -- ifOutOctets[{#MVSNMPVALUE1}]

Order: 1 | Macros: {#MVSNMPVALUE1} | Column name: Out Throughput | Consolidation function: Max | Percentile

telelink business services

Scalable Live Reports: Search, Sort, Navigate, Schedule, Export



Reporting

7IT / AO Test / Reports / IPNET MPLS Interface Inventory

Updated: 07.09.25 12:48:06
Period: 06.09.25 00:00:00 to 07.09.25 00:00:00

06-09-2025 00:00 – 07-09-2025 00:00

Default | Last 24 hours | Last 3 days | Last 7 days
Previous day | Previous week | Previous month | Previous 6 months

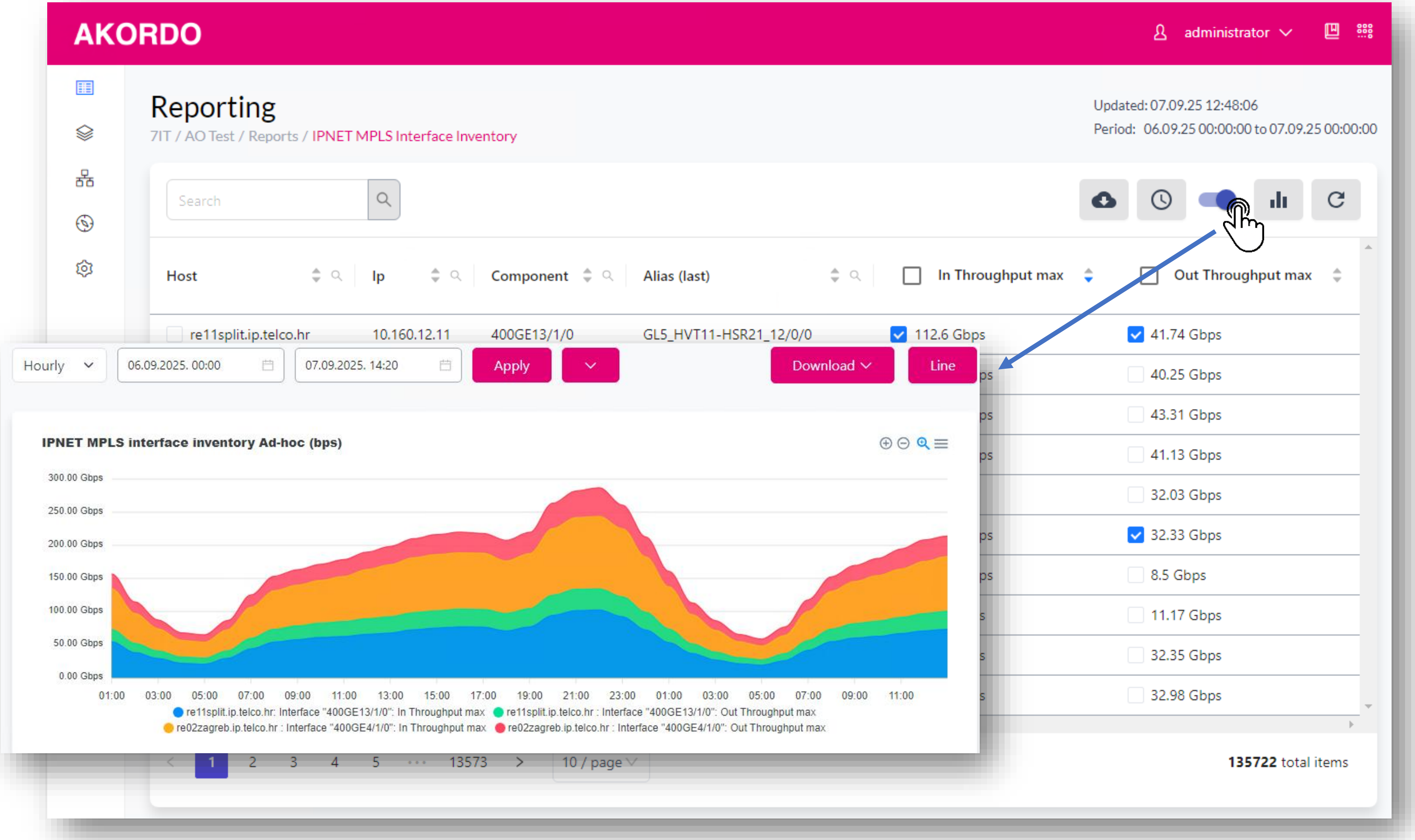
Host	Ip	Component	Alias (last)	In Throughput max	Out Th
re11split.ip.telco.hr	10.160.12.11	400GE13/1/0	GL5_HVT11-HSR21_12/0/0	112.6 Gbps	41.74
re10split.ip.telco.hr	10.160.12.88	400GE7/1/0	BS5_HRZ12-HAR11_7/0/0	110.04 Gbps	40.25
re10split.ip.telco.hr	10.160.12.88	400GE13/1/0	GL5_HAT12-HTA11_12/0/0	109.71 Gbps	43.31 Gbps
re10split.ip.telco.hr	10.160.12.88	400GE7/1/0	AH5_HZT11-BDR11_7/0/0	108.86 Gbps	41.13 Gbps
re01zagreb.ip.telco.hr	10.160.2.1	400GE14/1/0	UL5_JRI11-HDR11_12/1/0	102 Gbps	32.03 Gbps
re02zagreb.ip.telco.hr	10.160.2.13	400GE4/1/0	AL5_DRI13-GDR11_7/1/0	100.52 Gbps	32.33 Gbps
re02zagreb.ip.telco.hr	10.160.2.13	Eth-Trunk14	VL5_AOS12-HJR11_Eth-Trunk14	100.43 Gbps	8.5 Gbps
re01split.ip.telco.hr	10.160.1.23	Eth-Trunk14	JL5_FOS11-ADR11_Eth-Trunk14	99.24 Gbps	11.17 Gbps
re01split.ip.telco.hr	10.160.1.23	400GE4/1/0	FL5_HRI12-ATA11_7/1/0	97.36 Gbps	32.35 Gbps
re01split.ip.telco.hr	10.160.1.23	400GE14/1/0	NL5_RRI12-ATR11_12/1/0	96.86 Gbps	32.98 Gbps

< 1 2 3 4 5 ••• 13573 > 10 / page

135722 total items

tbs.tech | simplify the complex

Scalable Live Reports: Interactive Drill-Down with Graphs



Reporting

7IT / AO Test / Reports / IPNET MPLS Interface Inventory

Updated: 07.09.25 12:48:06
Period: 06.09.25 00:00:00 to 07.09.25 00:00:00

Host	Ip	Component	Alias (last)	☐ In Throughput max	☐ Out Throughput max
☐ re11split.ip.telco.hr	10.160.12.11	400GE13/1/0	GL5_HVT11-HSR21_12/0/0	☑ 112.6 Gbps	☑ 41.74 Gbps
				ps	☐ 40.25 Gbps
				ps	☐ 43.31 Gbps
				ps	☐ 41.13 Gbps
					☐ 32.03 Gbps
				ps	☑ 32.33 Gbps
				ps	☐ 8.5 Gbps
				s	☐ 11.17 Gbps
				s	☐ 32.35 Gbps
				s	☐ 32.98 Gbps

06.09.2025. 00:00 – 07.09.2025. 14:20

IPNET MPLS interface inventory Ad-hoc (bps)

- ● re11split.ip.telco.hr: Interface "400GE13/1/0": In Throughput max
- ● re11split.ip.telco.hr : Interface "400GE13/1/0": Out Throughput max
- ● re02zagreb.ip.telco.hr : Interface "400GE4/1/0": In Throughput max
- ● re02zagreb.ip.telco.hr : Interface "400GE4/1/0": Out Throughput max

135722 total items

tbs.tech | simplify the complex

telelink
business
services

Thank You!