

● Zabbix Summit 2026

Evolving Zabbix into a decision-making system

The work between an alert and the next action

Marcin Kaźmierczak
Solution Architect, Sycope

**How many of you have received an alert
that told you something was wrong, but
not what to do next?**

- Solution – adding free metadata collector

Network traffic analysis for NOC, SOC and Owners

Collects and analyses NetFlow, IPFIX and sFlow to show who communicates, where, when and how much.

NOC

Find the traffic behind a busy link.

SOC

Inspect communication that needs explaining.

Application owners

Check application health and availability.

Case 1: users report a slow application

Illustrative incident: a business application slows down during normal working hours

THE TASK

Users are waiting. NOC needs to find which part of the service to investigate. Find a cause to test and the right owner to involve.

NOC must find the transfer before it can act

AFTER THE ZABBIX ALERT

01 Check network issues

Network team: any errors or changes?

02 Ask which jobs were running

Service owners: which job matches the interval?

03 Review application logs

Application team: is the affected service healthy?

04 Align records with the alert

Operator: which transfer overlaps the slowdown?

Only then: identify the transfer to validate with its owner.

- NOC – what you have & what you can add

Zabbix shows the symptom and the busy server

Collects and analyses NetFlow, IPFIX and sFlow to show who communicates, where, when and how much.

VISIBLE IN ZABBIX

Number of commits: high

CPU & Memory utilization: high

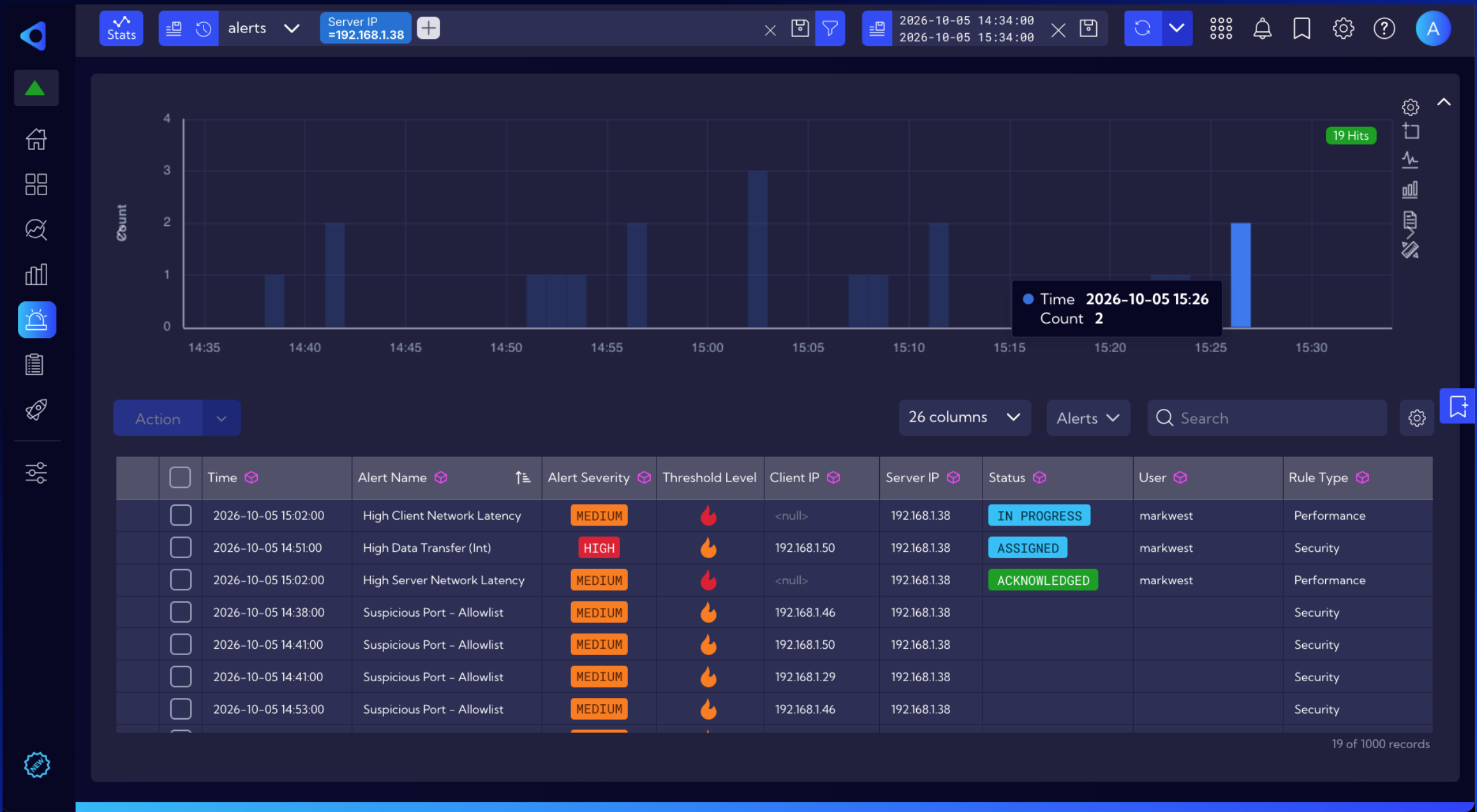
WHAT CAN BE ADDED?

Which transfer uses the link?

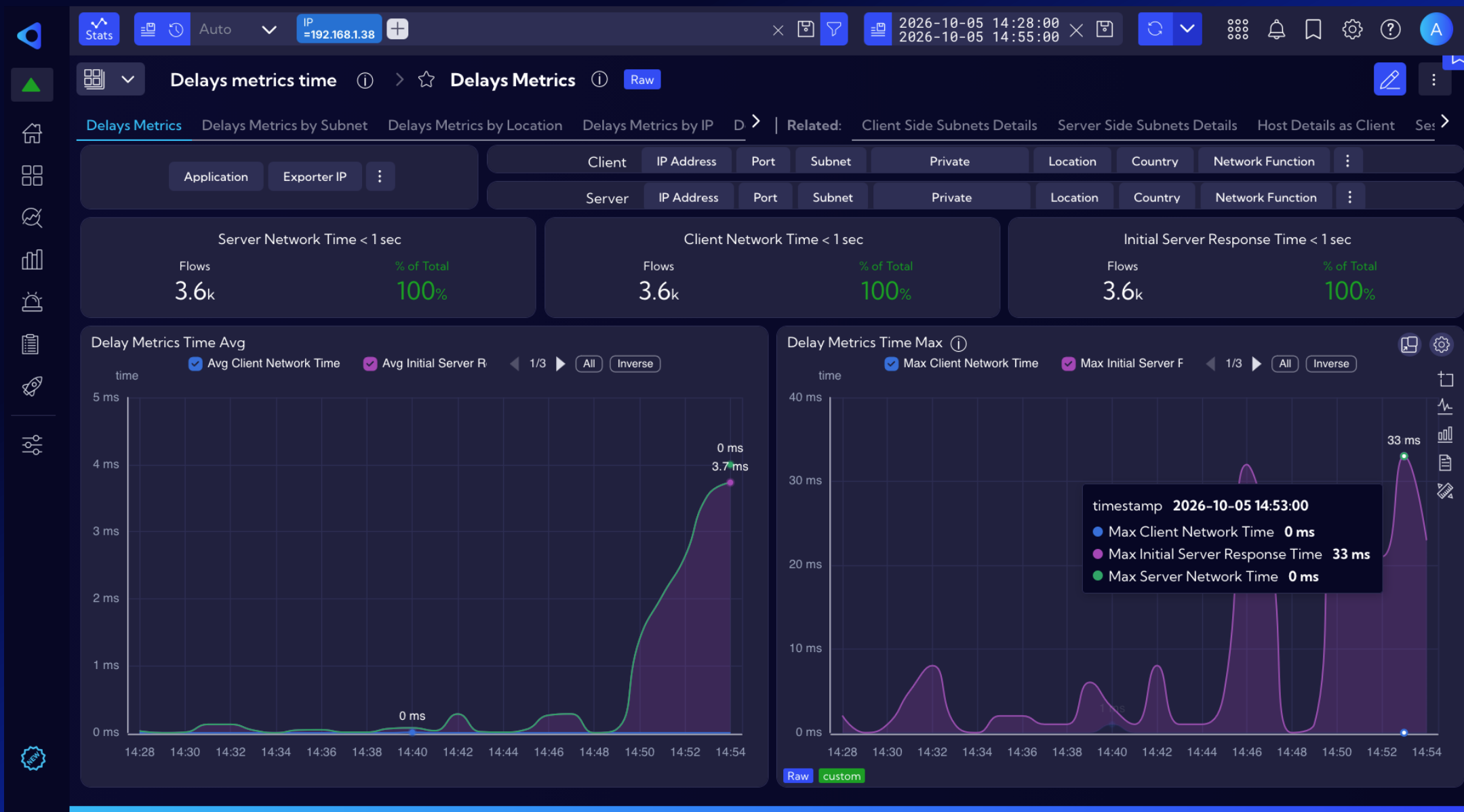
Who sends and receives it?

Client & Server response time

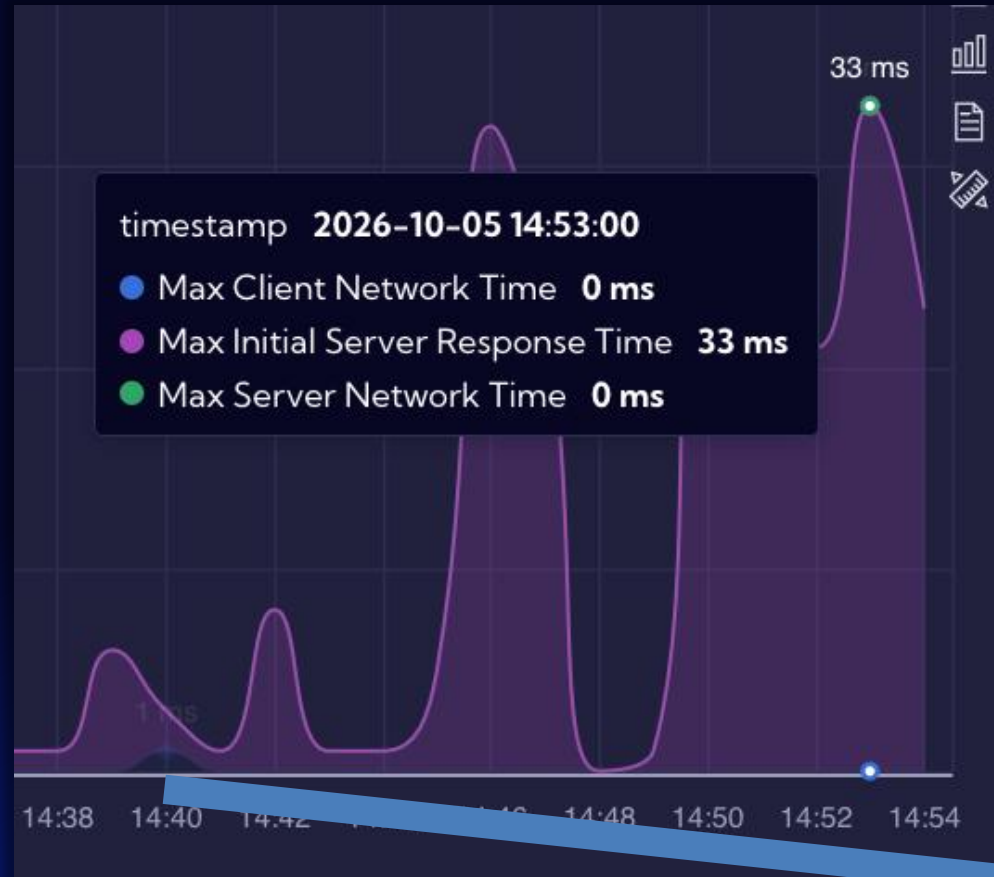
Sycope triggered alert for High Network Latency



Let's check all the delay metrics...



Now we know

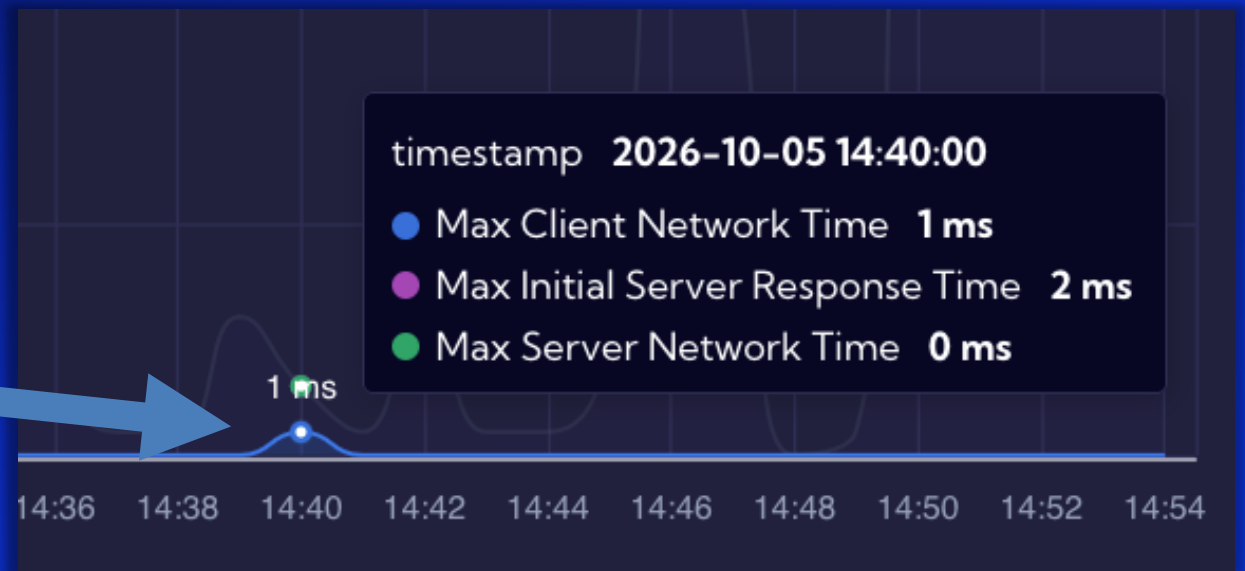


The network is healthy – Client and Server Network Time stay at 0–1 ms

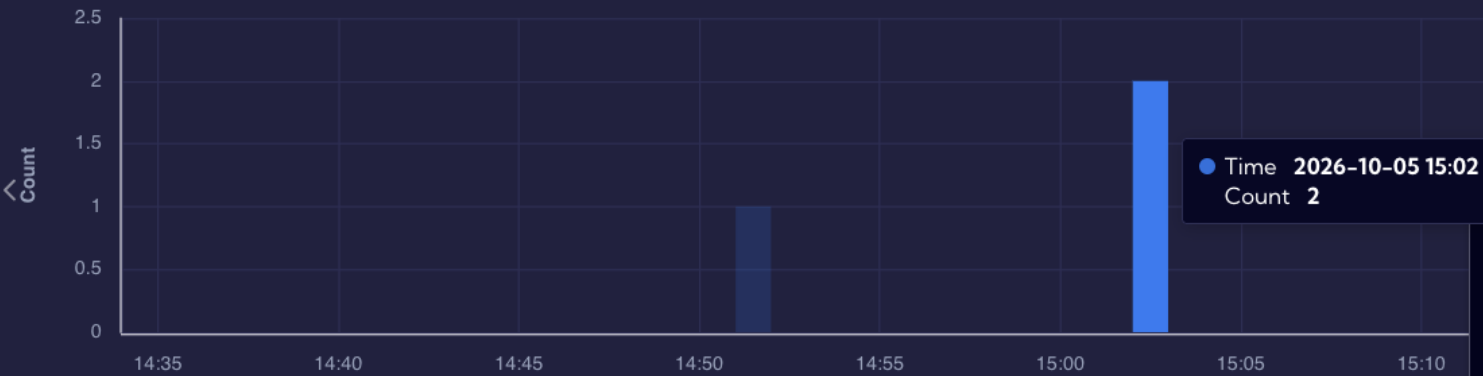
The server is slow to respond – Max Initial Server Response Time jumps from 2 ms to 33 ms

The delay starts after the network – TCP handshake is instant, SQL Server responds later

Only the database server is affected – Other servers are showing no change

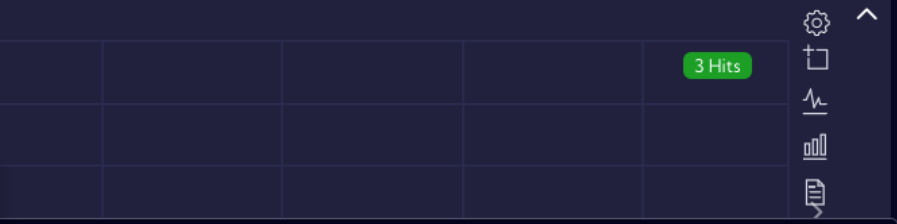


Move from Syclope to Zabbix – Drilldown action



Action ▾

	☐	Time	Alert Name	Alert Severity	Threshold Level	Client IP	Server IP	Status
	☐	2026-10-05 15:02:00	High Client Network Latency	MEDIUM		<null>	192.168.1.38	IN PROGRESS
	☐	2026-10-05 14:51:00	High Data Transfer (Int)	HIGH		192.168.1.50	192.168.1.38	ASSIGNED
	☐	2026-10-05 15:02:00	High Server Network Latency	MEDIUM		<null>	192.168.1.38	ACKNOWLEDGED

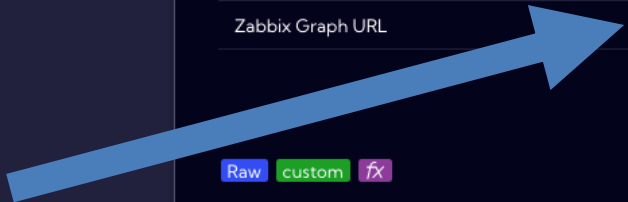


Zabbix Inventory - Drilldown Filtering: Global Local

assetDevices IP address =192.168.1.38

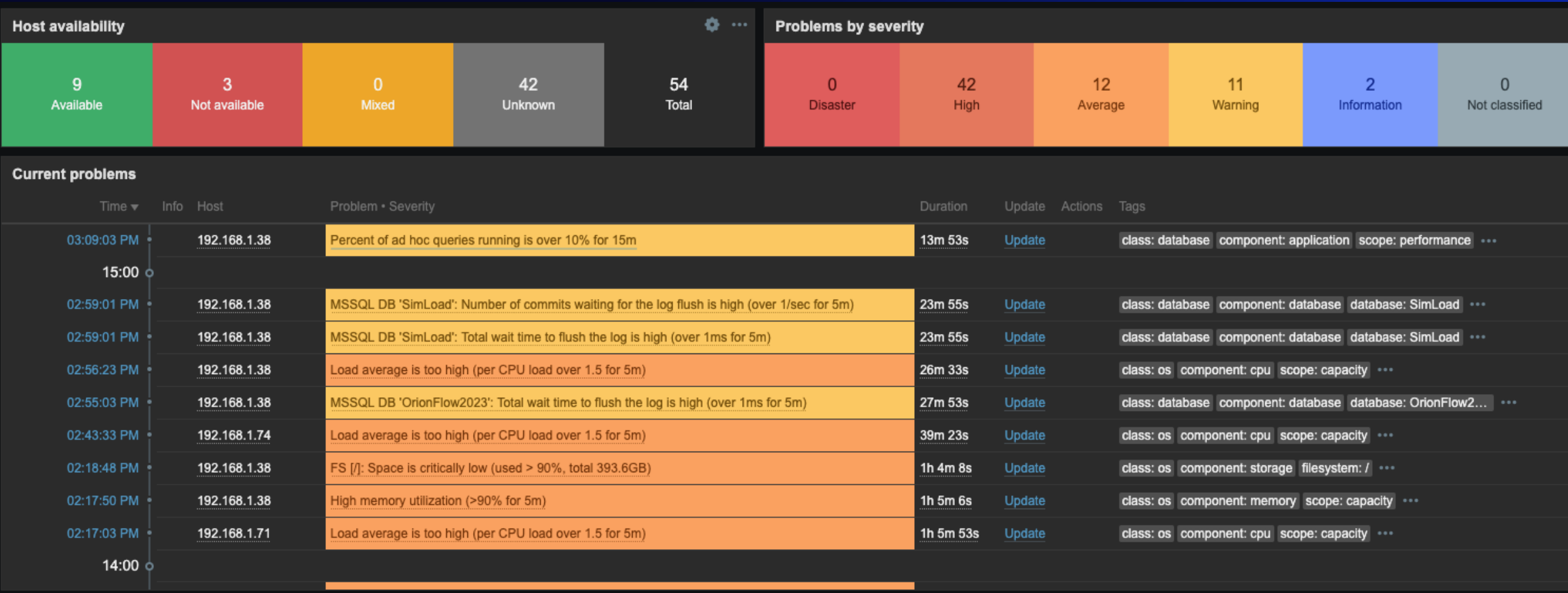
2026-10-05 14:34:00 2026-10-05 15:34:00

Field	Value
IP address	192.168.1.38
Zabbix Name	sqlserver2022
Zabbix Type	SNMP
Zabbix Status	Enabled
Zabbix Group	Databases
Zabbix Notes	SQL Server
Zabbix OS	Linux version 6.14.11-2-pve (build@proxmox) ...
Zabbix Serial No	<blank string>
Zabbix ICMP URL	http://192.168.1.46:8080/history.php?action=show...
Zabbix Graph URL	http://192.168.1.46:8080/zabbix.php?action=charts

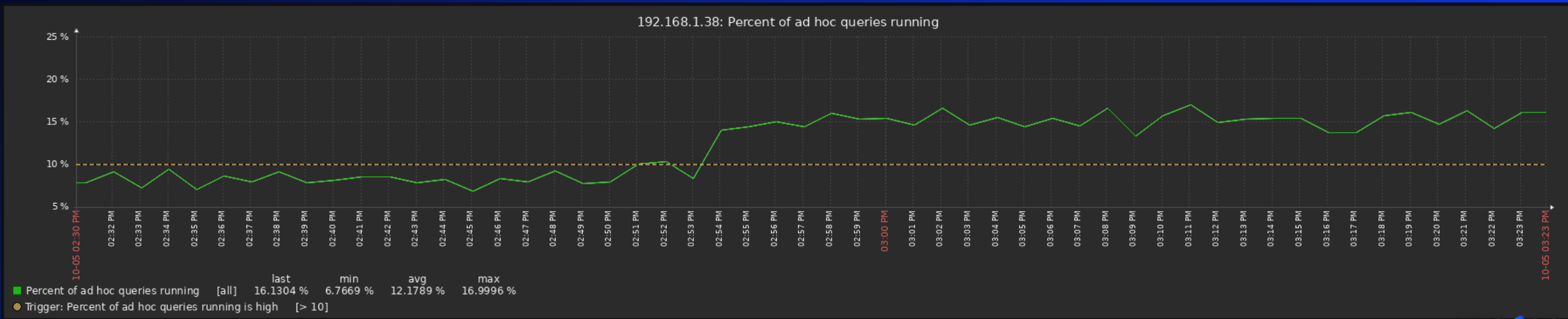
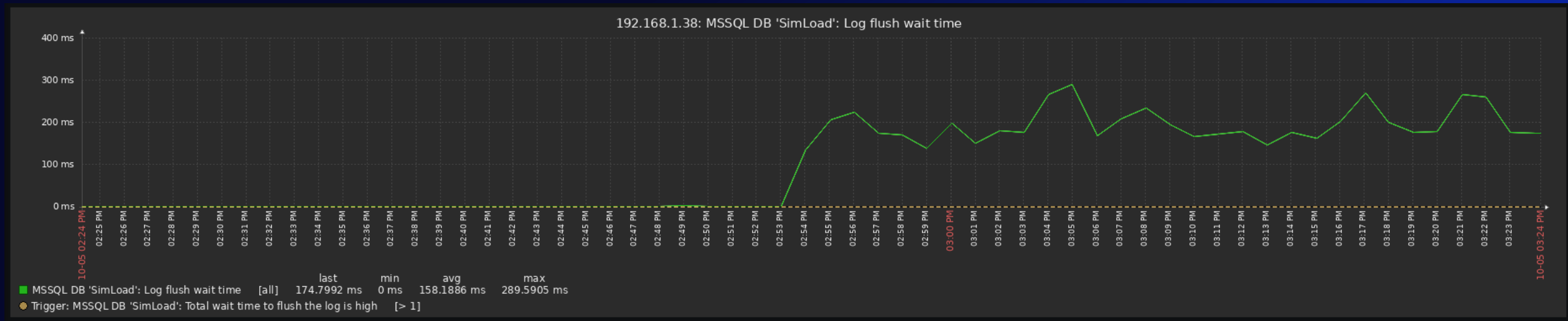


Raw custom fx

Zabbix discovered SQL problems after the network delay



Root cause is visible within SQL statistics



● NOC – what Sycope adds

Sycope identifies the server network delay first

A specific slowdown to verify: new client connects to the database

IN SYCOPE

Client & Server Network Delay

Rank conversations by bytes

Inspect volume over time

WHAT IT ADDS TO THIS ALERT

Quickly verify network vs. application issue

Find the client with the largest transfer

Verify transfers that overlap with the slowdown

NOC reaches the application owner with evidence

Less coordination to identify the transfer. A specific change to test.

WITHOUT SYCOPE

01 Check network issues

02 Ask which jobs were running

03 Review application logs

04 Align records with the alert

WITH SYCOPE - NETWORK FACTS IN ONE ANALYSIS

Sycope: real traffic analysis

Client generating database overload
Application delay on the network
Timing overlaps the slowdown

Next action: Validate the db queries, adjust if appropriate, then check the application.

Case 2: the server sends unusual outbound traffic

Illustrative incident. A bandwidth increase alone does not establish a security event.

THE TASK

Server normally serves internal users. Its outbound traffic has increased. Establish whether this transfer needs security investigation.

SOC assembles the network facts across tools

AFTER THE ZABBIX ALERT

01 Search firewall records

Find server's destination and port.

02 Check available traffic records

Establish direction, volume and interval.

03 Search earlier records

Check whether the same peer appeared before.

04 Combine results for the handoff

Align the host, peer and time across sources.

Only then: ask the owner about this specific transfer.

- SOC – what you have & what you can add

Zabbix shows the increase, but the peer is still unknown

The case starts with a host bandwidth alert. Additional configured checks may add context.

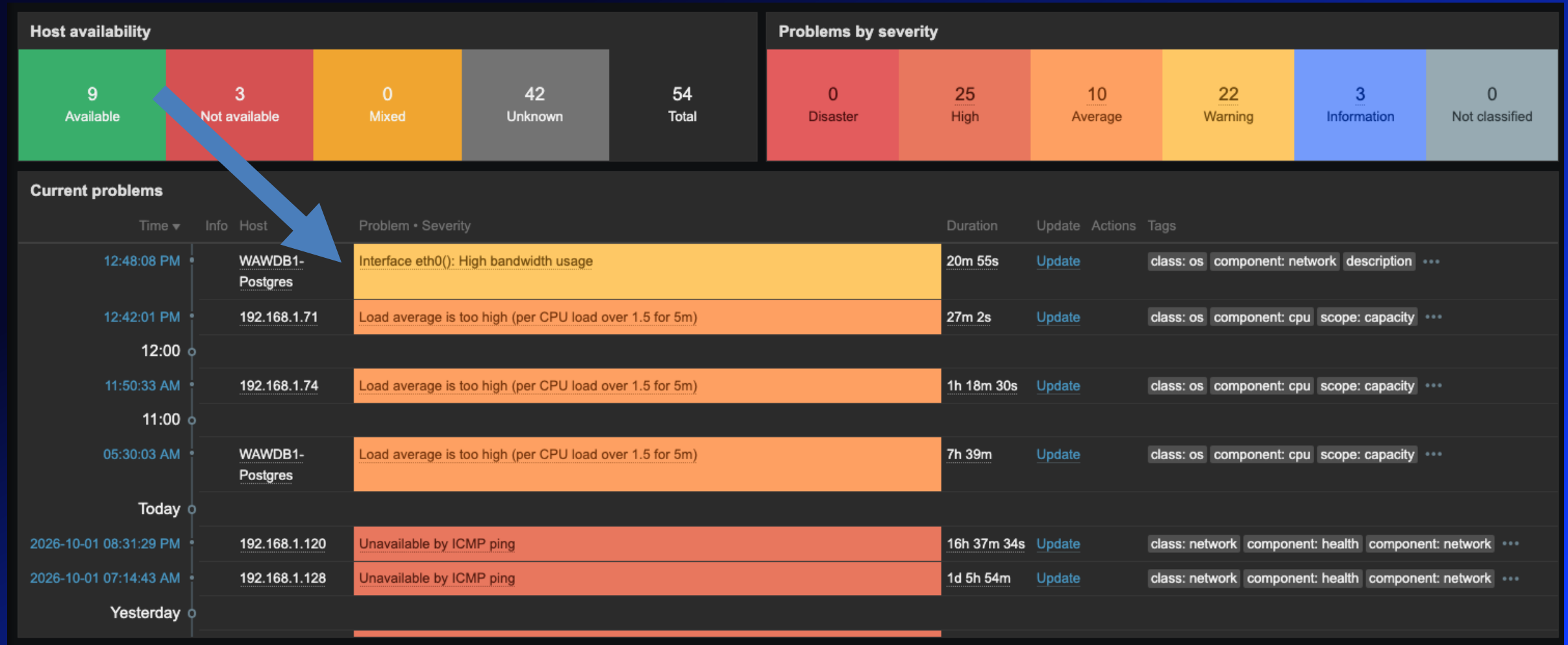
VISIBLE IN ZABBIX

Host: WAWDB1-Postgres
Outbound traffic increase
Event time

WHAT CAN BE ADDED?

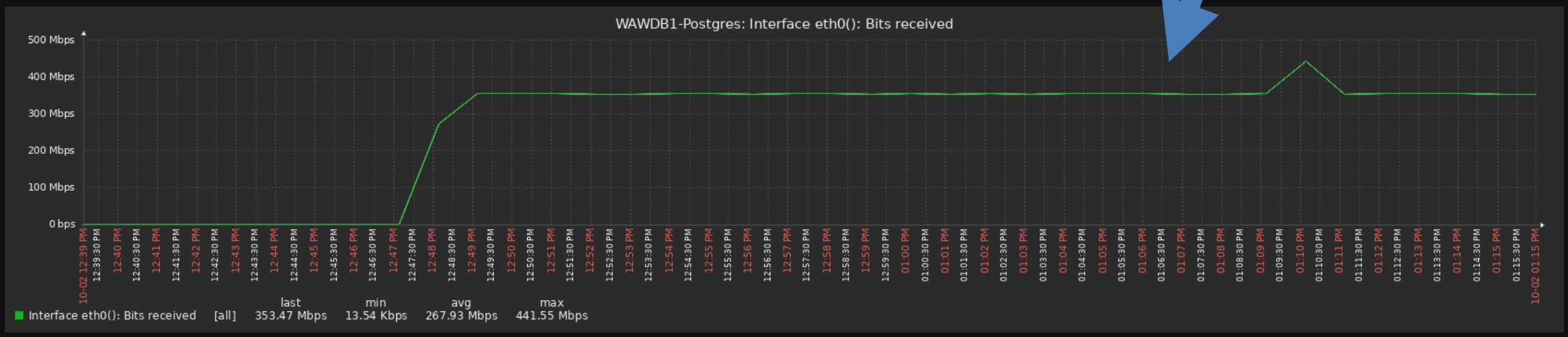
Which destination and port?
How much went to that peer?
Is that communication expected?

Zabbix discovered high interface utilization via triggered problem

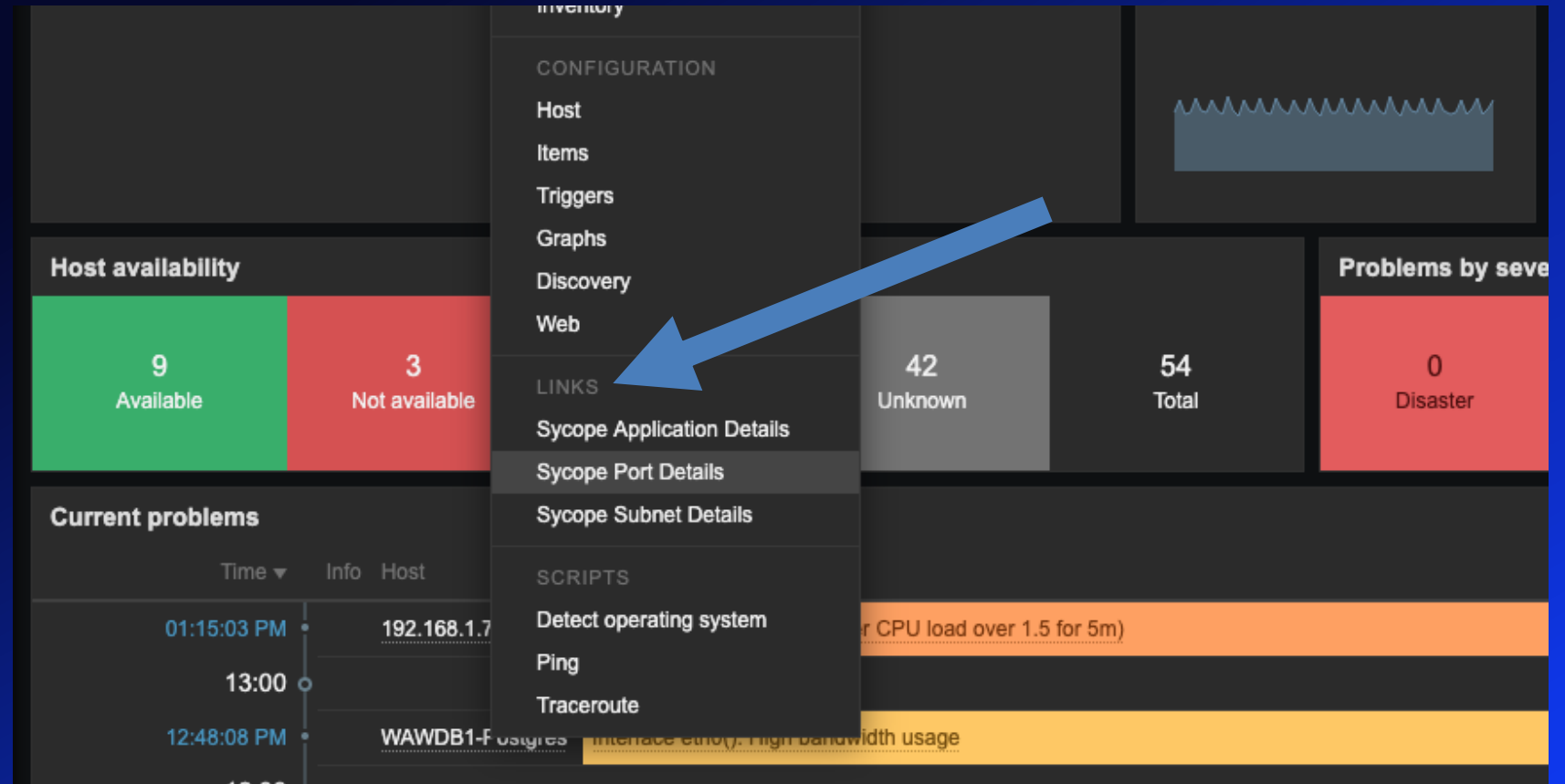


SNMP Interface Item confirms high traffic

Current problems			
Time ▼	Info	Host	Problem • Severity
12:48:08 PM	WAWDB1-Postgres	Interface eth0(): High bandwidth usage	
12:00			
11:50:33 AM	192.168.1.74	Load average is	
11:00			
05:30:03 AM	WAWDB1-Postgres	Load average is	
Today			
2026-10-01 08:31:29 PM	192.168.1.120	Unavailable by I	



Using Links to quickly move to Flow Analysis in Sycop

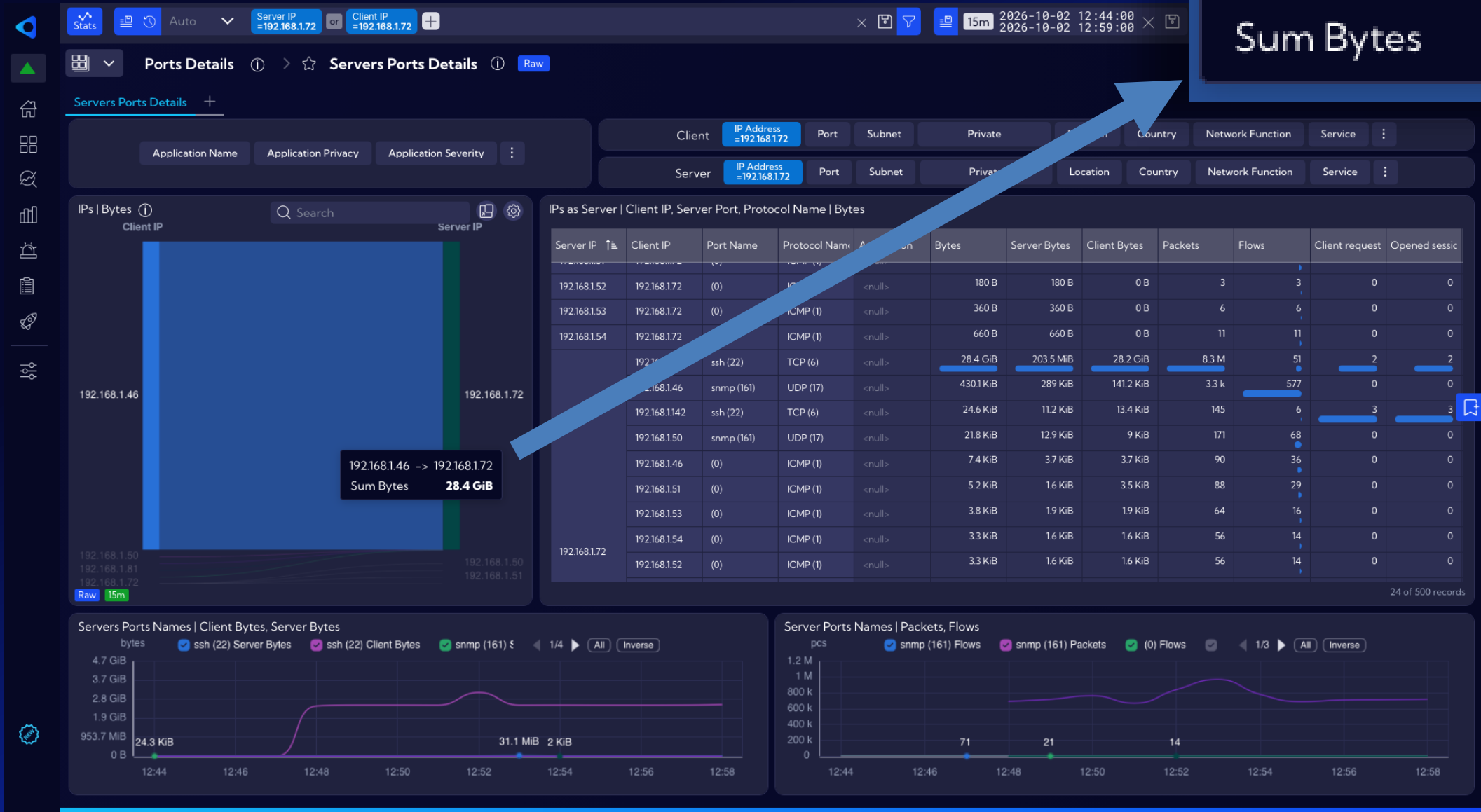


Custom Hyperlink in Zabbix:

<https://192.168.1.14/panel/dashboards/view/64673cdd-5cef260a-789e748d/64008ba2-4c7ffb9c-a4cad412?visualizationModalId=64439ace-815c89a6-1ca8756e&gq=%7B%22query%22:%7B%22source%22:%22%22,%22nql%22:%22serverIp%20%3D%20%5C%22192.168.1.72%5C%22%20%20or%20clientIp%20%3D%20%5C%22192.168.1.72%5C%22%22,%22advanced%22:false%7D,%22timerange%22:%7B%22from%22:%22now-15minutes%22,%22to%22:%22now%22,%22roundTo%22:%22minute%22%7D%7D>

Flow Analysis in Sycopo

28,4 GB transferred using SSH over 15 minutes



192.168.1.46 -> 192.168.1.72
Sum Bytes **28.4 GiB**

Taking actions...

IPs as Server | Client IP, Server Port, Protocol Name | Bytes

Server IP	Client IP	Port Name	Protocol Name	Application	Bytes	Server Bytes	Client Bytes	Packets	Flows	Client request	Opened sessio
192.168.1.52	192.168.1.72	(0)	ICMP (1)	<null>	180 B	180 B	0 B	3	3	0	0
192.168.1.53	192.168.1.72	(0)	ICMP (1)	<null>	360 B	360 B	0 B	6	6	0	0
192.168.1.54	192.168.1.72	(0)	ICMP (1)	<null>	660 B	660 B	0 B	11	11	0	0
192.168.1.72	192.168.1.46	ssh (22)	TCP (6)	<null>	28.4 GiB	203.5 MiB	28.2 GiB	8.3 M	51	2	2
	192.168.1.46	ssh (22)	TCP (6)	<null>	430.1 KiB	289 KiB	141.2 KiB	3.3 k	577	0	0
	192.168.1.46	ssh (22)	TCP (6)	<null>	24.6 KiB	11.2 KiB	13.4 KiB	145	6	3	3
	192.168.1.46	ssh (22)	TCP (6)	<null>	21.8 KiB	12.9 KiB	9 KiB	171	68	0	0
	192.168.1.46	ssh (22)	TCP (6)	<null>	7.4 KiB	3.7 KiB	3.7 KiB	90	36	0	0
	192.168.1.46	ssh (22)	TCP (6)	<null>	5.2 KiB	1.6 KiB	3.5 KiB	88	29	0	0
	192.168.1.46	ssh (22)	TCP (6)	<null>	3.8 KiB	1.9 KiB	1.9 KiB	64	16	0	0
	192.168.1.46	ssh (22)	TCP (6)	<null>	3.8 KiB	1.9 KiB	1.9 KiB	64	16	0	0

24 of 500 records

1/4 All Inverse

12:54 12:56 12:58

1 M 800 k 600 k 400 k 200 k 0

12:44

(0) Flows 1/3 All Inverse

12:52 12:54 12:56 12:58

14

Copy

Quick Actions

Drilldown

Actions

Send externally

Show

Tools

Manage shortcuts

IP Reputation

Block IP and SSH in BECS

Unblock IP in BECS

Block IP in BECS

Open a ticket in Jira

Block host by IP (MACMON)

Add external destination

How to see traces of the server outbound communication

A specific transfer for the owner to confirm or SOC to investigate.

IN SYCOPE	WHAT IT ADDS TO THIS ALERT
Filter the server's traffic + event interval	Communication from the host that raised the alert
Inspect outbound peers and ports	The public destination and TCP/22
Inspect bytes and traffic history	Transfer volume, interval and earlier observations

● SOC – the workflow with Sycope

SOC starts with the transfer already established

Less time assembling network facts. SOC can focus on the investigation.

WITHOUT SYCOPE

01 Search firewall records

02 Check available traffic records

03 Search earlier records

04 Combine results for the handoff

WITH SYCOPE – NETWORK FACTS IN ONE ANALYSIS

Sycope: server + event interval

Public peer and TCP/22

Direction, bytes and timing

Earlier observations

Next action: Ask the owner to confirm this transfer. Escalate with evidence if unexplained.

What changes for the operator

Less work between the alert and the decision

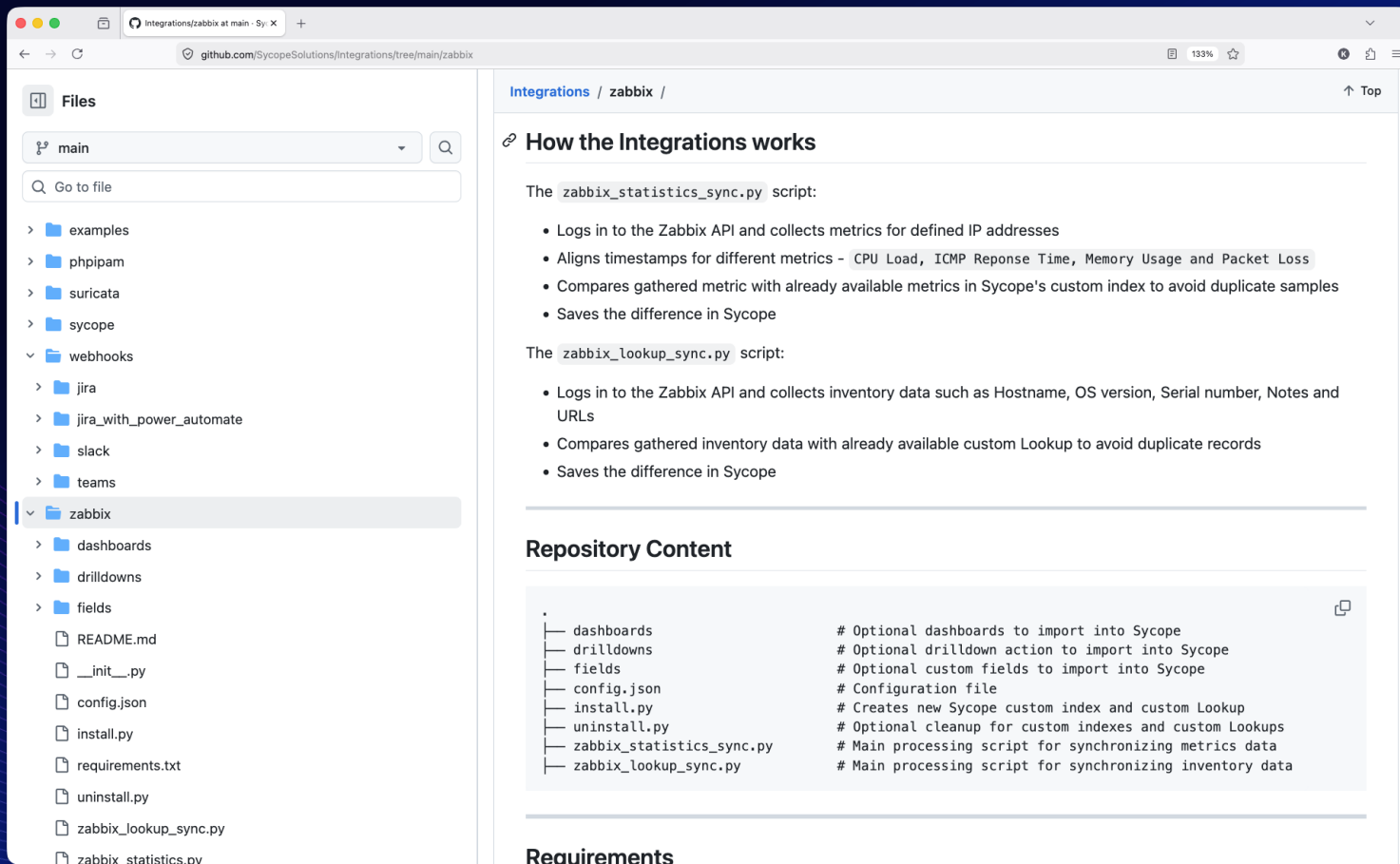
NOC / SLOW APPLICATION

Identify the additional transfer before involving its owner.

SOC / UNUSUAL OUTBOUND TRAFFIC

Hand over the communication record with the alert.

Extend Zabbix with Network Flow Data and integrate Zabbix with Sycope easily



SYCOPE GITHUB REPOSITORY



[https://github.com/
SycopeSolutions/](https://github.com/SycopeSolutions/)

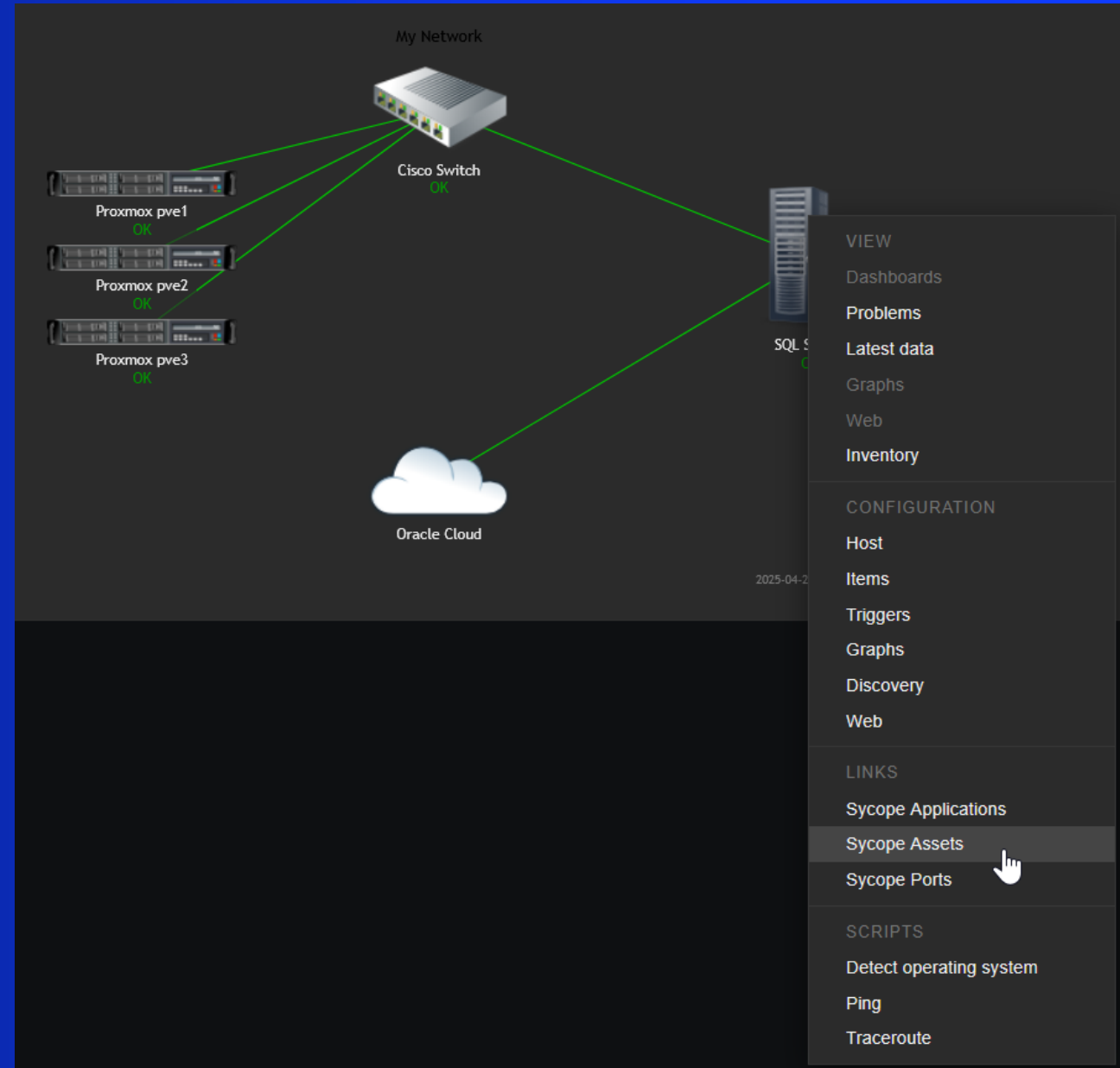
Ability to place anything on the Map

Add Sycope URLs to any built-in or custom dashboards (+define an automatic filter for an IP address or other value)

- Multiple hyperlinks to every Sycope module

Use Zabbix Templates for presentation (labels with macros):

- Alert counter
- Servers with Internet access
- Public connections "from" and "to" the Host
- Number of connections, sessions
- Open ports



SYN TCP Flag

8.00

Visibility - Only SYN Client ...

Public Init Conns

0.00

Visibility - Initial connections from Publi...

Horizontal Scan

0.00

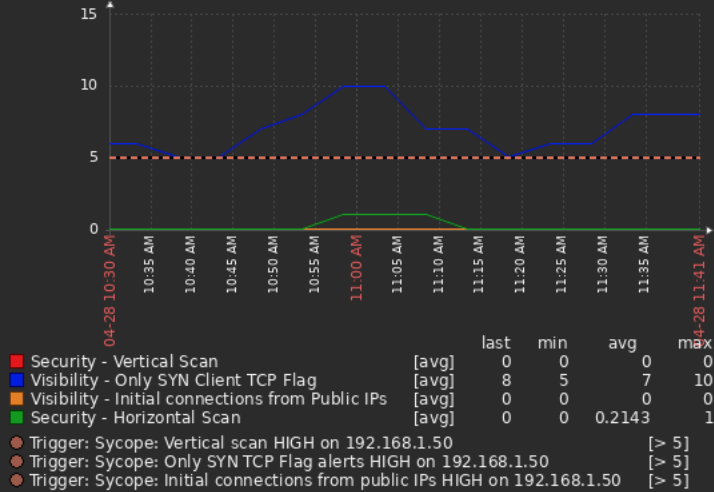
Security - Horizontal Scan

Vertical Scan

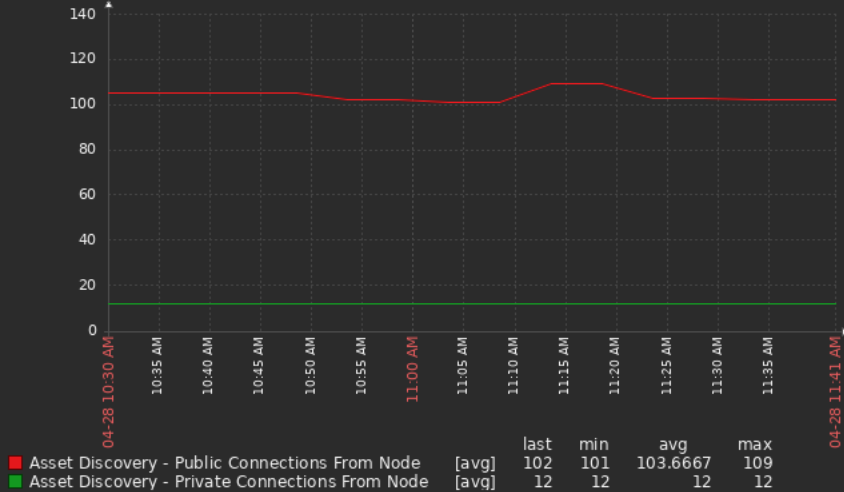
0.00

Security - Vertical Scan

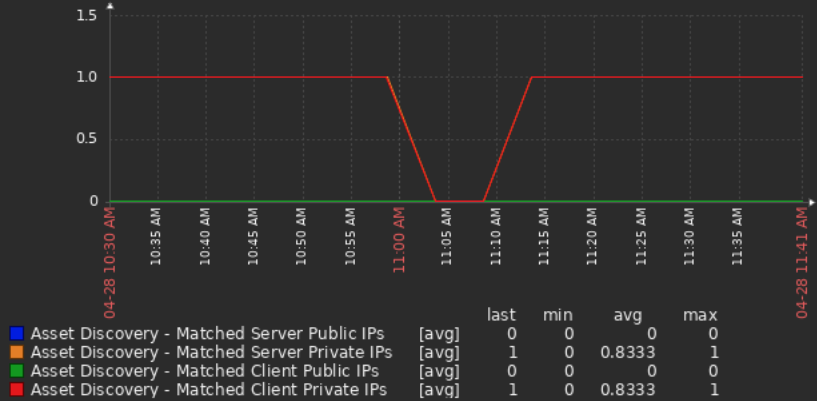
Security Alerts



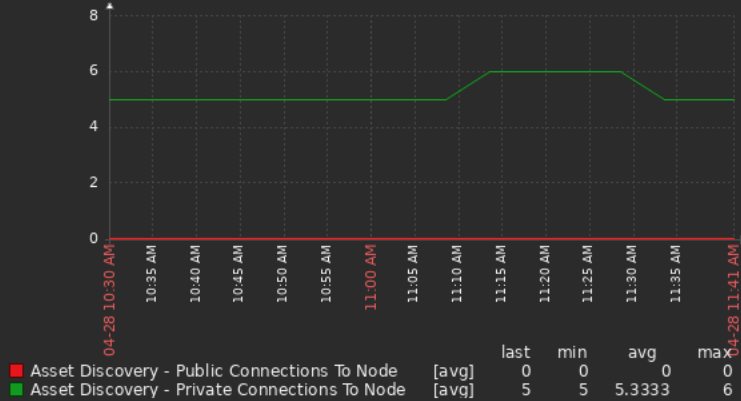
Connections From Node



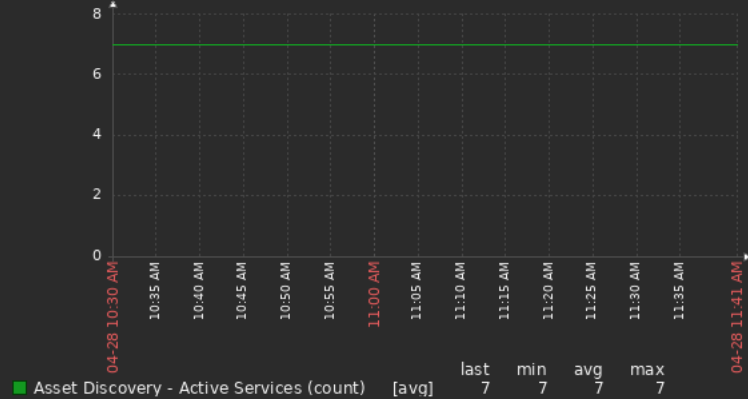
Matched IPs



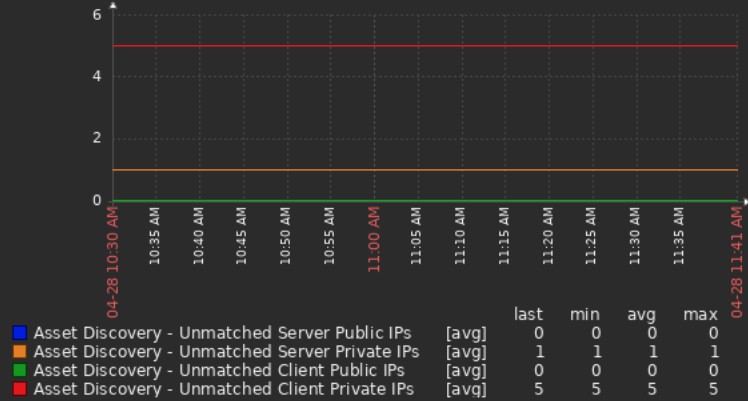
Connections To Node



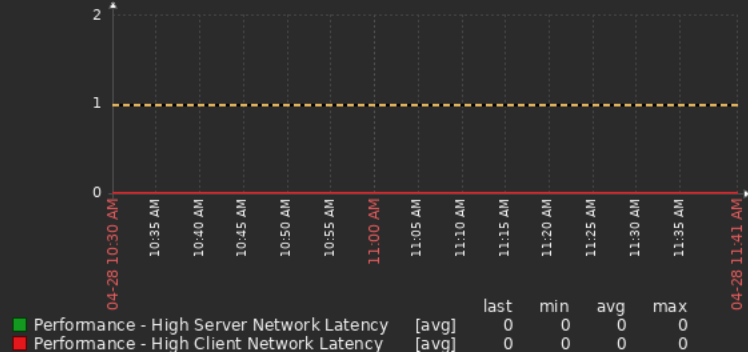
Active Services



Unmatched IPs



Performance Alerts





	Host	Name ▲	Last check	Last value	Change	Tags	Info
	192.168.1.50	Asset Discovery - Active Services (count)	4m 58s	7		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Active Services (port list)	4m 57s	22 (not defined), 23 (...)		component: asset_di...	History
	192.168.1.50	Asset Discovery - Matched Client Private IPs	4m 39s	1	22 (not defined), 23 (not defined), 80 (not defined), 443 (not defined), 2055 (NETFLOW), 2055 (not defined), 10050 (not defined)		
	192.168.1.50	Asset Discovery - Matched Client Public IPs	4m 38s	0			
	192.168.1.50	Asset Discovery - Matched Server Private IPs	4m 37s	1		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Matched Server Public IPs	4m 36s	0		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Private Connections From Node	4m 43s	12		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Private Connections To Node	4m 43s	5	-1	component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Public Connections From Node	4m 41s	102	-1	component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Public Connections To Node	4m 41s	0		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Unmatched Client Private IPs	4m 34s	5		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Unmatched Client Public IPs	4m 33s	0		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Unmatched Server Private IPs	4m 33s	1		component: asset_di...	Graph
	192.168.1.50	Asset Discovery - Unmatched Server Public IPs	4m 32s	0		component: asset_di...	Graph
	192.168.1.50	Performance - High Client Network Latency	4m 56s	0		component: performa...	Graph
	192.168.1.50	Performance - High Client Network Latency (detail)	4m 50s	Total: 0, Acknowledge...		component: performa...	History
	192.168.1.50	Performance - High Server Network Latency	4m 55s	0		component: performa...	Graph
	192.168.1.50	Performance - High Server Network Latency (detail)	4m 48s	Total: 0, Acknowledge...		component: performa...	History
	192.168.1.50	Security - Horizontal Scan	4m 53s	0		component: security	Graph
	192.168.1.50	Security - Horizontal Scan (detail)	4m 48s	Total: 0, Acknowledge...		component: security	History
	192.168.1.50	Security - Vertical Scan	4m 51s	0		component: security	Graph
	192.168.1.50	Security - Vertical Scan (detail)	4m 45s	Total: 0, Acknowledge...		component: security	History
	192.168.1.50	Visibility - Initial connections from Public IPs	4m 53s	0		component: visibility	Graph
	192.168.1.50	Visibility - Initial connections from Public IPs (detail)	4m 47s	Total: 0, Acknowledge...		component: visibility	History
	192.168.1.50	Visibility - Only SYN Client TCP Flag	4m 51s	8	+2	component: visibility	Graph
	192.168.1.50	Visibility - Only SYN Client TCP Flag (detail)	4m 45s	Total: 8, Acknowledge...		component: visibility	History

Extend Zabbix with Network Flow Data and find answers for your alerts for free

SYCOPE FREE LICENSE



<https://free.syclope.com>

- No credit card required
- Ready to use right after installation
- Threat and anomaly detection
- Up to 5,000 flows/s
- Data retention limited to 14 days

**Zabbix flags the change.
Sycope shows the traffic behind it.**

Thank you!