

# Sample report

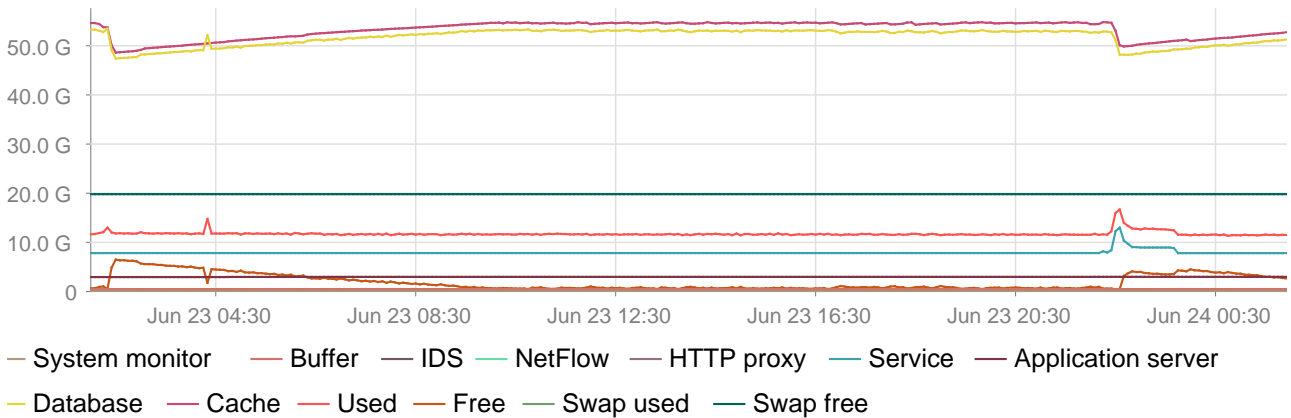
---

↓  
2026-06-23 02:00 CEST - 2026-06-24 02:00 CEST

[www.greycortex.com](http://www.greycortex.com)

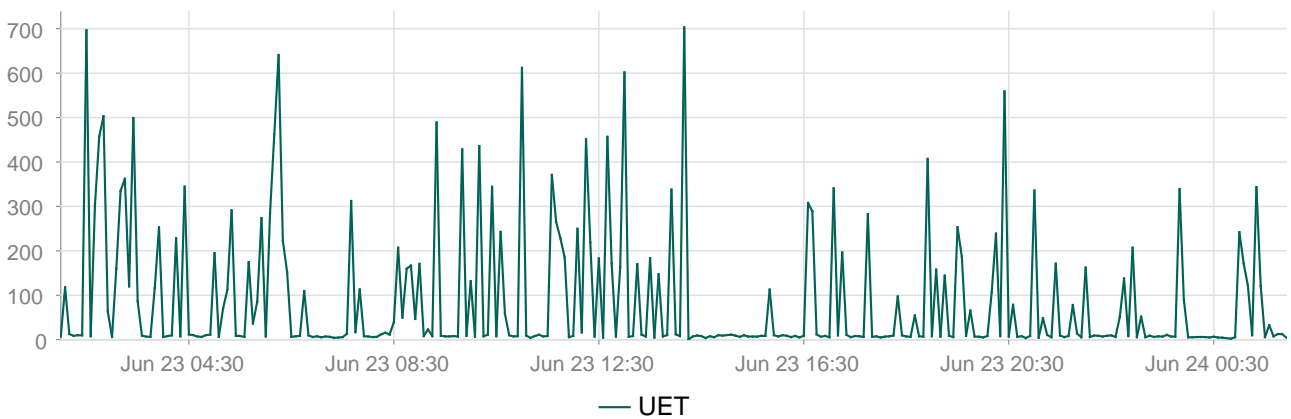
## Memory detailed overview

The chart shows detailed information of memory usage by processes.



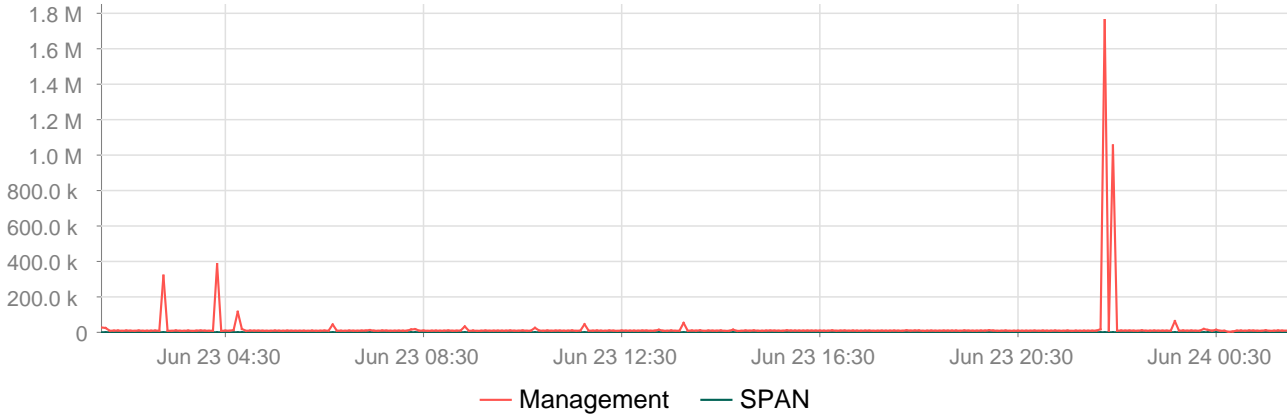
## User experience time

The line chart shows user experience time measured in seconds.



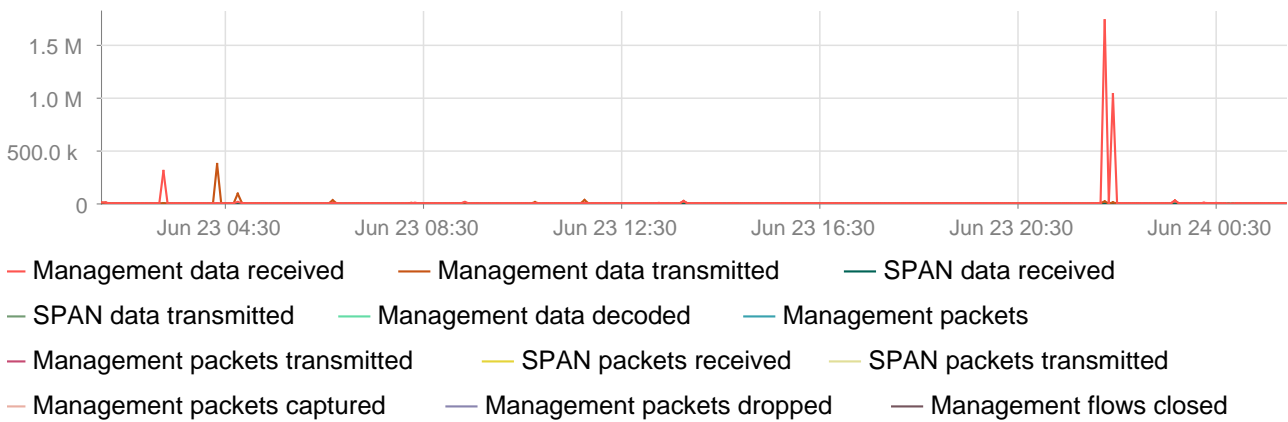
## Traffic overview

The chart shows how much traffic is received on the network interface. SPAN is traffic measured on mirrored ports and Management shows amount of traffic received on the management interface.



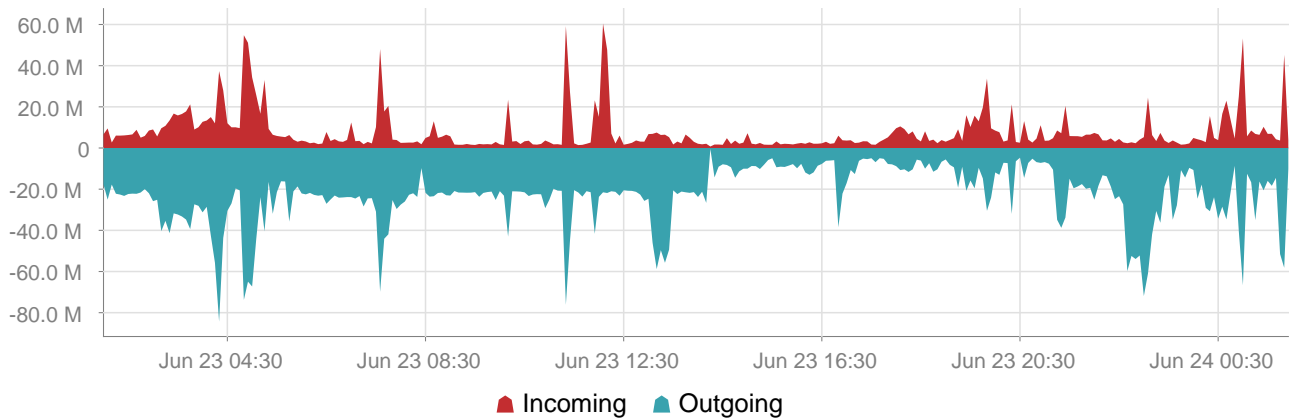
## Traffic detailed overview

The chart shows detailed information about incoming traffic to the network interfaces.



## Traffic by direction

The chart shows incoming and outgoing network traffic.



## Total network traffic

The line chart shows overall network traffic.













## Top users by events

The table shows users ordered by number of events occurred related to a user.

Risk	User	Events
Low	Kelly Howard (khoward_3630)	2
Info	Joe Medina (jmedina_988)	5











## Top source hosts

The table shows source hosts ordered by its risk. Source means the hosts that originated the event. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	 anhur.greycortex.com (10.22.10.107)	75
High	 jiangyin (10.22.8.85)	908
High	 fd00:dead:beef:e8d:5f76:dbff:fb58:d218	7
High	 bes-12 (10.22.182.253)	6
High	 fd00:dead:beef:e8d:2b0:5c6:75e8:7837	4
High	 fd00:dead:beef:e8e8:0:48a7:0:3f	4
High	 fd00:dead:beef:e8d:cb7:5526:a881:ab30	2
High	 10.22.10.107	67
High	 10.22.10.124	64
High	 10.22.10.189	60

## Top source countries

The table shows source countries ordered by its risk. Source means origin country in occurred events. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
High	 United States	534	1.0 k
High	 China	224	545
High	 Korea, Republic of	67	79
High	 Philippines	10	14
Medium	 Japan	46	87
Medium	 Czech Republic	203	403
Medium	 Netherlands	29	395
Medium	 France	37	223
Medium	 Taiwan	136	217
Medium	 Ireland	72	106

## Top services by traffic

The table shows services ordered by highest data traffic.

Service	Type	Traffic
RTSP (554)	LOCAL	127.24 G
HTTPS (443)	LOCAL	77.97 G
HTTPS (443)	REMOTE	37.5 G
NDL-AAS (3128)	LOCAL	16.02 G
NDL-AAS (3128)	REMOTE	16.0 G
HTTP (80)	REMOTE	14.29 G
Rsync (873)	LOCAL	12.7 G
HTTP (80)	LOCAL	12.68 G
SSH (22)	LOCAL	5.86 G
Rsync (873)	REMOTE	2.56 G

## Top services by risk

The table shows services by its risk. Risk is based on severity and number of events. Hosts column means how many hosts are engaged in the event.

Risk	Service	Hosts	Events
Critical	HTTP (80)	57	218
High	DNS (53)	67	3.0 k
High	IMAPS (993)	4	123
High	Socalia (5100)	2	17
High	32738	1	4
High	49001	4	4
High	17400	1	1
High	48513	1	1
High	51413	1	1
High	TELNET (23)	8	592

## Top sensors

The table shows top sensors ordered by number of events.

Severity	Sensor	Events
9	demo	8.1 k

## Top operating systems

The table shows top operating systems used in the network ordered by the number of hosts on which the system was detected.

Operating system	Hosts
Windows 10	37
Windows 7	1
Windows 10/Server 2016/Server 2019/Server 2022 (NT 10.0)	63
Windows 8.1/Server 2012/R2 (NT 6.3)	51
Windows 8/Server 2012 (NT 6.2)	13
Windows 7/Server 2008 R2 (NT 6.1)	494
Windows 7 and newer	1
Windows Vista/Server 2008 (NT 6.0)	16
Windows 2000/XP/Server 2003 (NT 5.x)	4
Windows	2

## Top hosts by traffic at web services

The table shows hosts ordered by highest traffic at web services (HTTP or HTTPS).

Host	Service	Traffic
🌐 10.22.176.33	HTTPS (443)	14.13 G
🌐 10.22.15.195	HTTPS (443)	9.28 G
🌐 10.22.15.229	HTTPS (443)	9.27 G
🌐 10.22.15.20	HTTPS (443)	8.07 G
🌐 10.22.176.147	HTTP (80)	7.91 G
🌐 10.22.15.177	HTTPS (443)	6.58 G
🌐 10.22.15.55	HTTPS (443)	6.15 G
🌐 10.22.15.156	HTTPS (443)	6.08 G
🌐 fd00:dead:beef:e8e8:0:48a7:0:64e8	HTTP (80)	5.53 G

Host	Service	Traffic
🌐 10.22.15.1	HTTPS (443)	4.78 G

## Top hosts by traffic at mail services


The table shows hosts ordered by highest traffic at mail services (IMAP, IMAPS, POP3, SPOP3, SMTP, SMTPS).

Host	Service	Traffic
🌐 10.22.176.107	IMAPS (993)	560.14 M
🌐 10.22.176.107	IMAP (143)	271.73 M
🌐 10.22.8.224	IMAPS (993)	266.05 M
🌐 fd00:dead:beef:e8d:39d7:4972:9aa3:fb8	IMAPS (993)	62.36 M
🌐 10.22.8.224	IMAP (143)	39.13 M
🌐 10.22.8.224	SMTP (25)	27.4 M
🌐 fd00:dead:beef:a85b:b015:2494:b82:b7f9	IMAPS (993)	20.43 M
🌐 fd00:dead:beef:e8d:e231:407d:fc13:f057	POP3S (995)	17.57 M
🌐 fd00:dead:beef:a85b:d4cf:ee9c:2a2:f6c7	IMAP (143)	12.62 M
🌐 10.22.8.224	SMTPS (465)	9.15 M

## Top hosts by traffic










The table shows hosts ordered by network traffic. Highest network traffic is on the top and the number of the rows is adjustable.

Host	Traffic
🌐 10.22.14.27	125.54 G
🌐 fd00:dead:beef:e811:0:48a7:0:1129	16.94 G
🌐 10.22.176.33	15.3 G
🌐 10.22.10.242	10.96 G
🌐 fd00:dead:beef:4ff0:c97:f0a1:4d8a:fc47	9.92 G
🌐 10.22.15.195	9.28 G
🌐 10.22.15.229	9.27 G
🌐 10.22.15.20	8.07 G

Host	Traffic
 10.22.176.147	7.91 G
 10.22.15.177	6.58 G







## Top hosts by risk





The table shows hosts ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	 10.22.10.107	147
High	 10.22.8.85	929
High	 10.22.10.189	880
High	10.22.10.190	191
High	 10.22.10.124	104
High	 10.22.10.246	97
High	 10.22.10.233	57
High	 10.22.182.253	11
High	 fd00:dead:beef:e8d:5f76:dbff:fb58:d218	7
High	 fd00:dead:beef:e8d:2b0:5c6:75e8:7837	4

## Top external sources









The table shows external hosts, which originated communication with internal hosts. External hosts are ordered by its risk.

Risk	Host	Events
High	 173.8.236.98	3
High	 222.186.30.136	3
High	 68.102.166.186	2
High	 122.54.145.102	2
High	 175.210.24.232	2
High	 222.39.145.189	2

Risk	Host	Events
High	 71.40.85.218	1
Medium	 218.47.103.99	9
Medium	 62.24.68.85	45
Medium	 195.146.128.61	15




## Top external hosts





The table shows external hosts ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Host	Events
Critical	 174.36.215.20	1
High	 0.0.0.0	1.9 k
High	 128.227.150.11	5
High	 79.118.182.202	4
High	 2a00:1450:400c:c07::10	4
High	 2a00:1450:400c:c09::6c	2
High	 2001:569:79eb:d700:4db5:9355:c714:8254	1
High	 2001:56a:f111:6700:b9a4:355d:b545:b44e	1
High	2002:5f47:6dc0::5f47:6dc0	1
High	2002:7076:b94a:10:2996:7b52:168d:822f	1

## Top external destinations

The table shows external hosts, when internal hosts originated communication. External hosts are ordered by its risk.

Risk	Host	Events
Critical	 174.36.215.20	1
High	 128.227.150.11	5
High	 79.118.182.202	4

Risk	Host	Events
High	 2a00:1450:400c:c07::10	4
High	2001:67c:e0::85	2
High	 2a00:1450:400c:c09::6c	2
High	 2001:569:79eb:d700:4db5:9355:c714:8254	1
High	 2001:56a:f111:6700:b9a4:355d:b545:b44e	1
High	2002:5f47:6dc0::5f47:6dc0	1
High	2002:7076:b94a:10:2996:7b52:168d:822f	1











## Top events

The table shows events ordered by severity and their number of occurrences. Hosts column means how many hosts are engaged in the event.

Severity	Name	Hosts	Occurrences
<b>9</b>	Adware-pup: W32/Toolbar.WIDGI User-Agent (WidgiToolbar-)	2	1
<b>8</b>	Discovery: New Host (forbidden by policies)	8	58
<b>8</b>	Periodic: Repetitive Connections (every 30 minutes in 6 hours)	16	19
<b>8</b>	Correlation: TOR communication	2	4
<b>7</b>	Limit: Peers at Host	10	341
<b>7</b>	Periodic: Possible Malware Check-in on HTTP/S	7	9
<b>7</b>	Telnet: TELNET login failed	8	7
<b>7</b>	Scan: Radmin Port Sweep (4899)	2	3
<b>7</b>	Limit: Data at Host	2	2
<b>7</b>	Adware-pup: Win32/BrowseFox.H Checkin 2	2	2











## Top destination hosts

The table shows destination hosts ordered by its risk. The destination means the hosts that are targeted in the event. Risk calculation is based on severity and number of events.

Risk	Host	Events
High	 10.22.10.189	820
High	 10.22.10.190	187
High	 10.22.10.246	44
High	 10.22.10.124	39
High	 10.22.10.107	4
High	 10.22.10.232	2
High	 10.22.10.233	1
High	 10.22.10.249	107
High	 10.22.10.163	48
Medium	 10.22.10.110	66











## Top destination countries

The table shows destination countries ordered by its risk. Destination means target country in occurred events. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
Critical	 United States	17	62
High	 Belgium	7	18
High	 Canada	3	5
High	 Romania	1	4
High	 Germany	11	33
Medium	 China	2	7
Medium	 Hungary	1	40
Medium	 Ireland	5	18
Medium	 United Kingdom	2	5
Medium	 Czech Republic	3	4











## Top countries by traffic

The table shows top countries ordered by their data traffic.

Country	Flows	Traffic
 France	222.3 k	127.3 G
 Czech Republic	551.0 k	56.2 G
 Slovakia	70.3 k	11.6 G
 United States	1.2 M	8.7 G
 Ireland	380.4 k	8.1 G
 Poland	24.6 k	6.9 G
 Russian Federation	105.7 k	3.1 G
 Germany	11.8 M	2.8 G
 Sweden	50.6 k	1.6 G
 Estonia	1.9 k	1.1 G

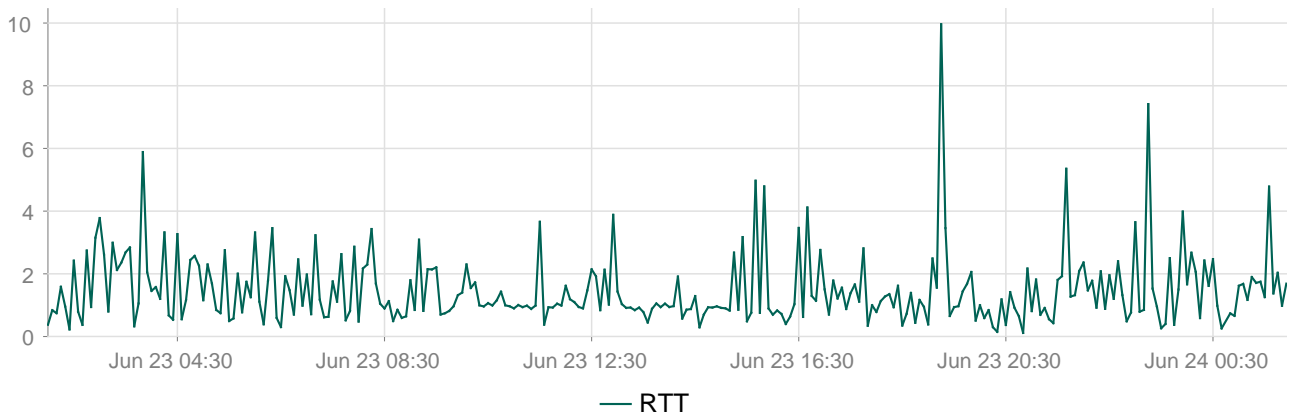
## Top countries

The table shows countries ordered by its risk. Risk calculation is based on severity and number of events.

Risk	Country	Hosts	Events
Critical	 United States	551	1.1 k
High	 Canada	29	39
High	 Belgium	7	18
High	 Romania	1	4
High	 China	226	552
High	 Germany	65	128
High	 Korea, Republic of	67	79
High	 Philippines	10	14
Medium	 Japan	46	87
Medium	 Czech Republic	206	407

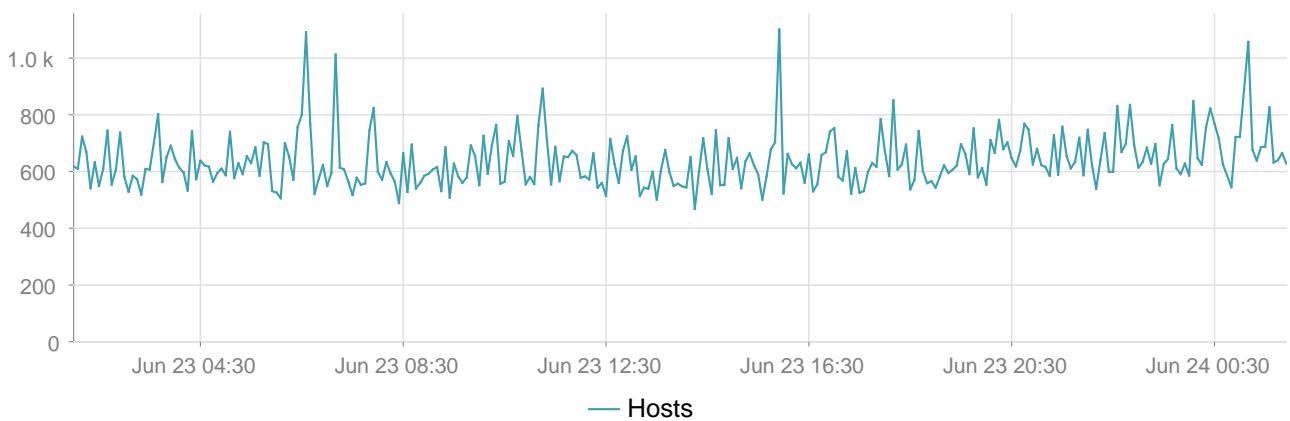
## Round trip time

The line chart shows round trip time measured in seconds.



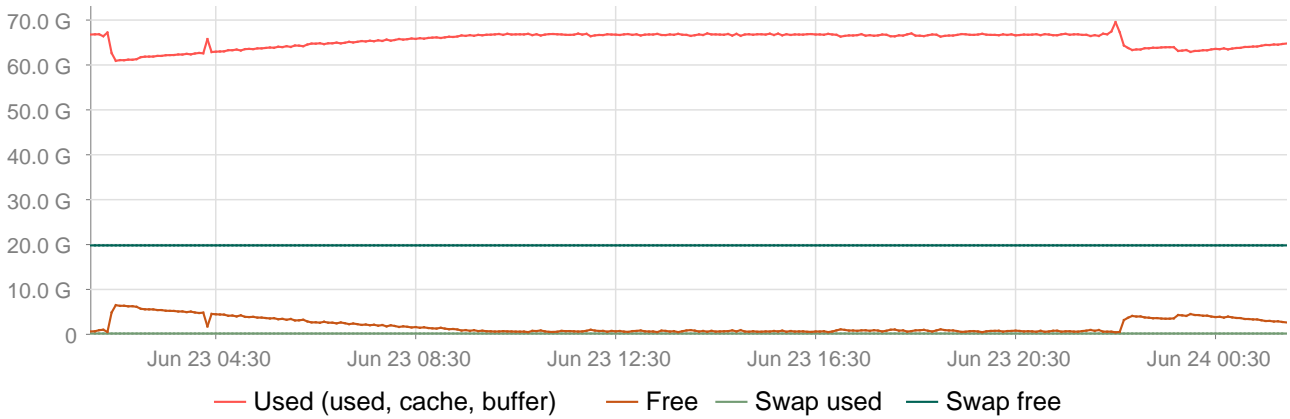
## Number of monitored hosts

The line chart shows the number of active hosts on the network.



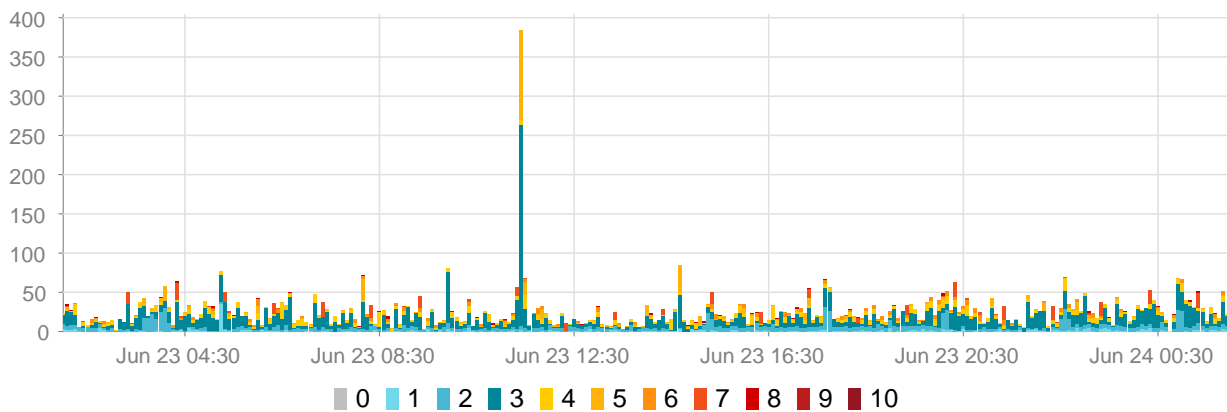
## Memory overview

The chart shows information about memory usage. It shows the total available RAM, the amount of used memory and also the maximum size of swap and the amount of swapped memory.



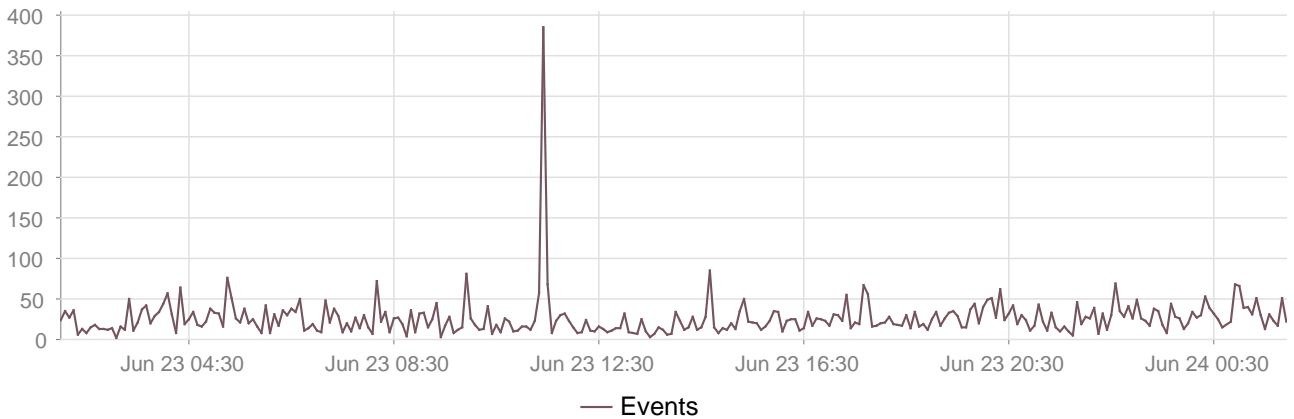
## Events with severities

The bar chart shows number of events by severity.



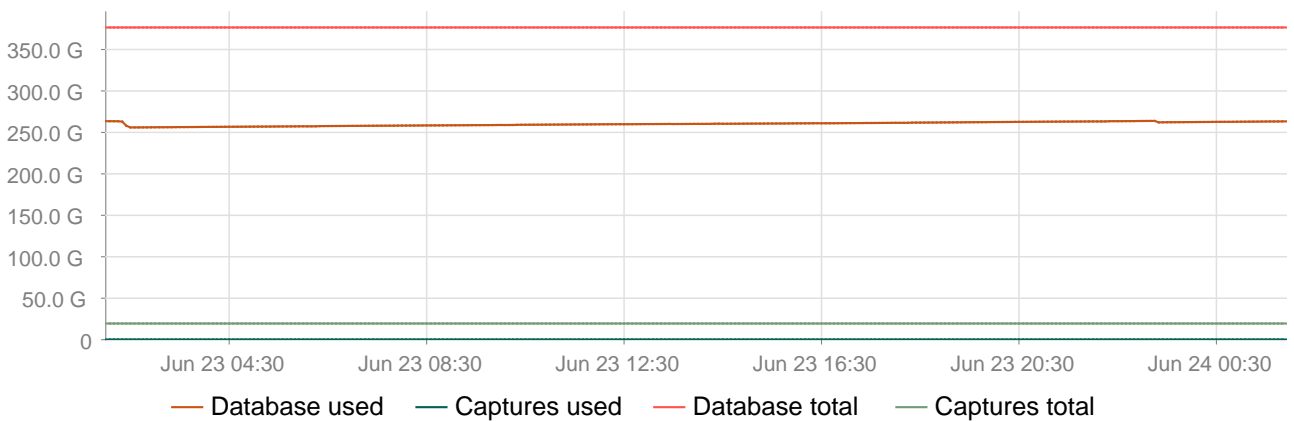
## Events

The line chart shows number of detected events.



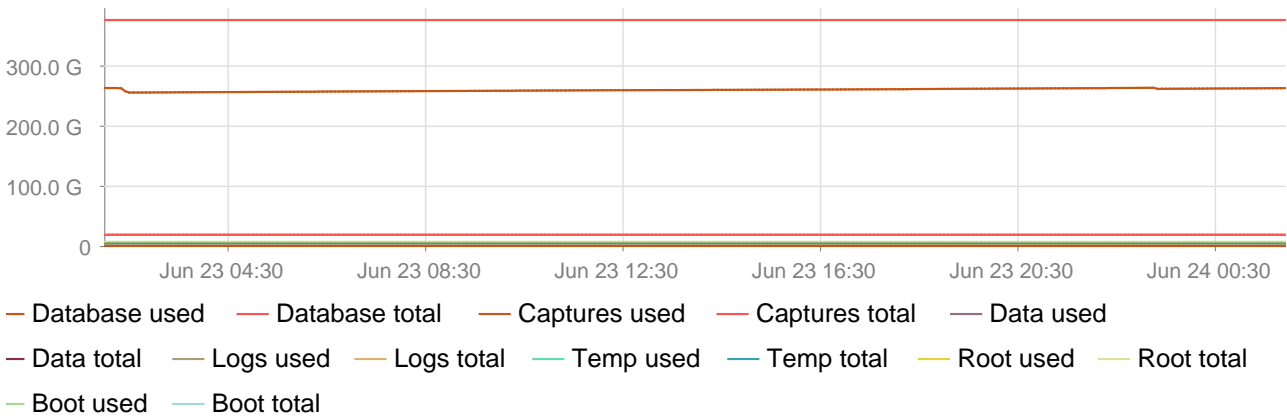
## Disk overview

The chart shows information about database space and its usage.



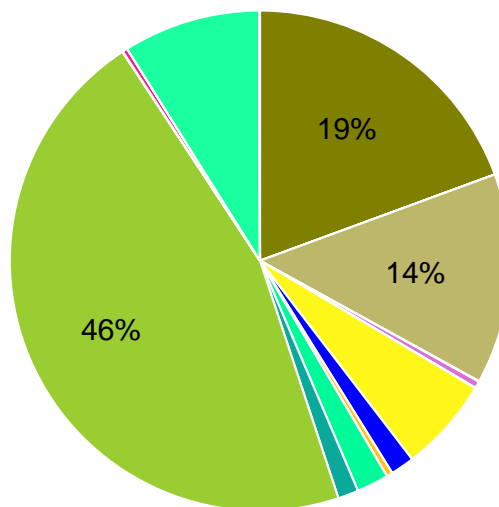
## Disk detailed overview

The chart shows detailed information about space usage of system partitions.



## Data traffic by subnets

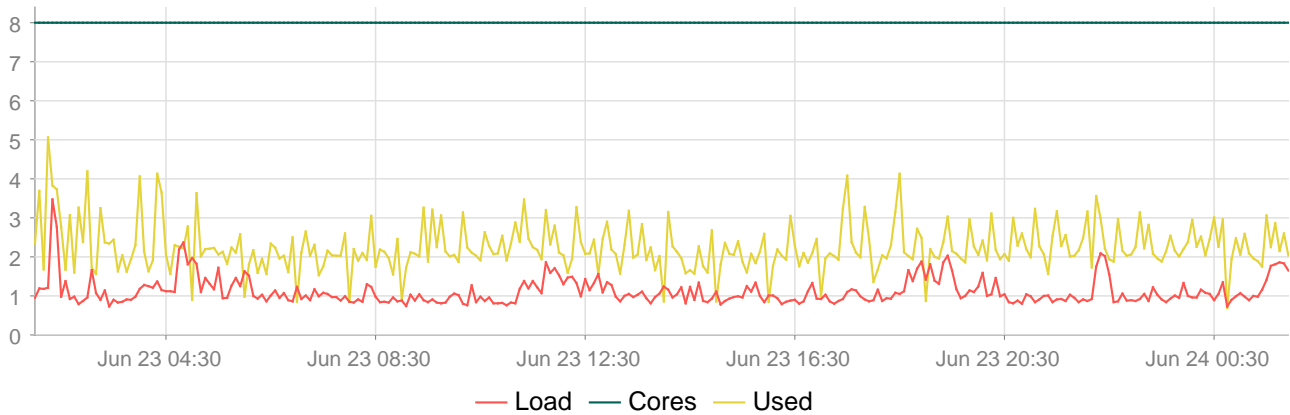
The pie chart shows data traffic by subnets.



- Servers
- Important LAN
- IPv6 segment
- Datacenter B
- GWs
- 3. Floor
- DB servers
- WiFi zone 2
- WEB APPs 2
- Admin
- Admins
- Web servers
- External VPN
- 10. Floor
- Net dev
- App servers
- 9. Floor
- Users
- Testing
- Local net

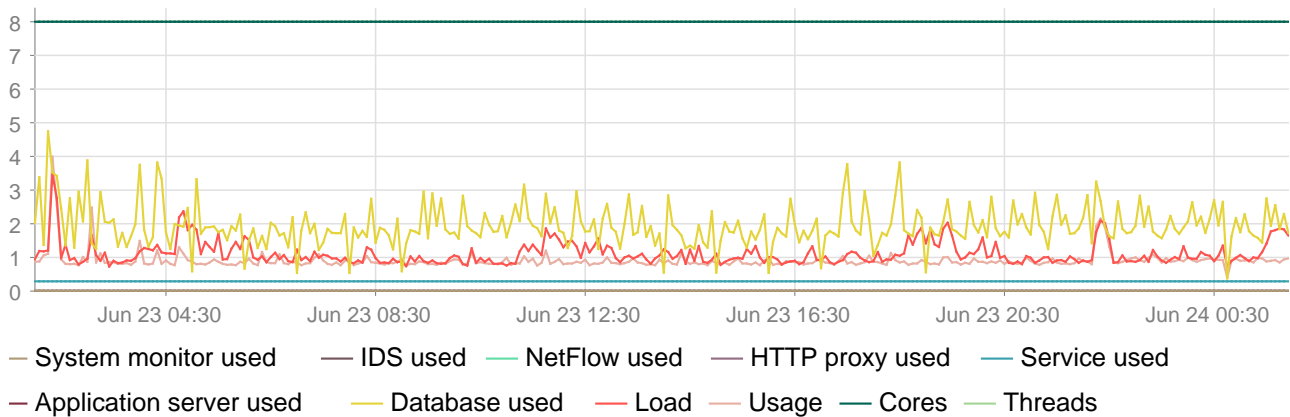
## CPU overview

The chart shows utilization of CPU. Cores value indicates the number of physical cores. The load represents total load of all cores including virtual threads.



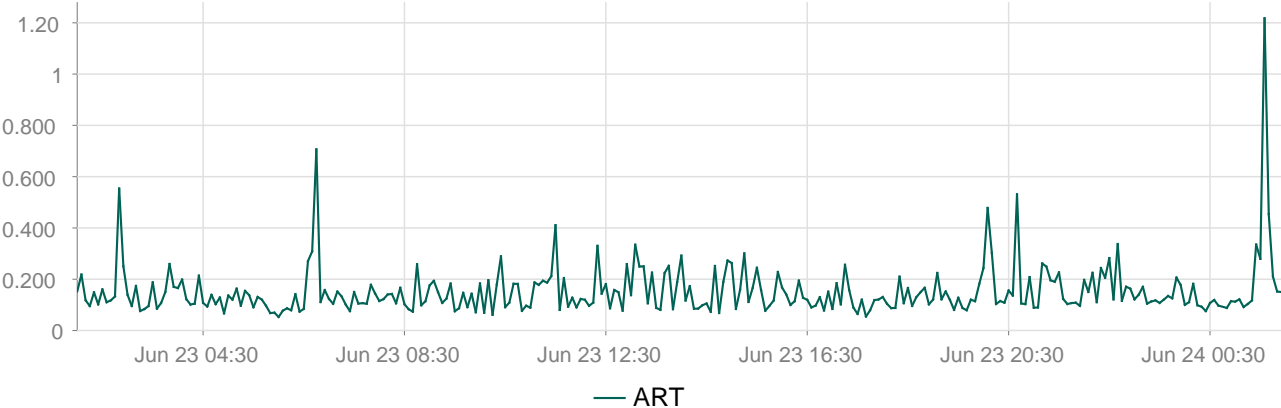
## CPU detailed overview

The chart shows utilization of CPU with detailed information about load of processes.



# Application response time

The line chart shows application response time measured in seconds.



## About this report:

Generated: 2026-06-24 11:50 CEST  
Sensor: demo  
Interval: 2026-06-23 02:00 CEST - 2026-06-24 02:00 CEST  
Appliance Type: all-in-one  
Licensed To: test@greycortex.com  
License Expiration: 2026-12-31  
Current Version: 4.6.0

**NETWORK DETECTION  
AND RESPONSE**



**GREYCORTEX**

[www.greycortex.com](http://www.greycortex.com)