WAZUH | Modules | Security events

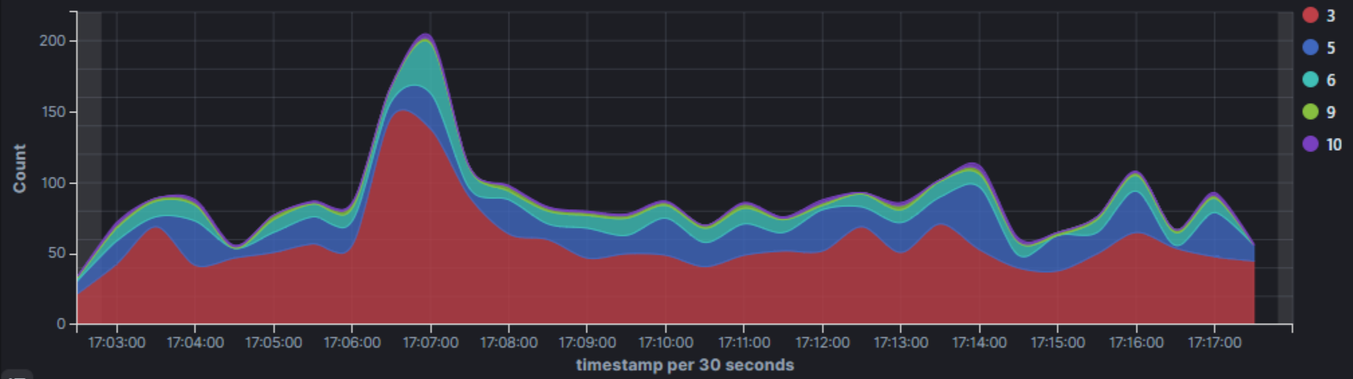
Dashboard | Events | Explore agent | Generate report

Search | KQL | Last 15 minutes | Show dates | Refresh

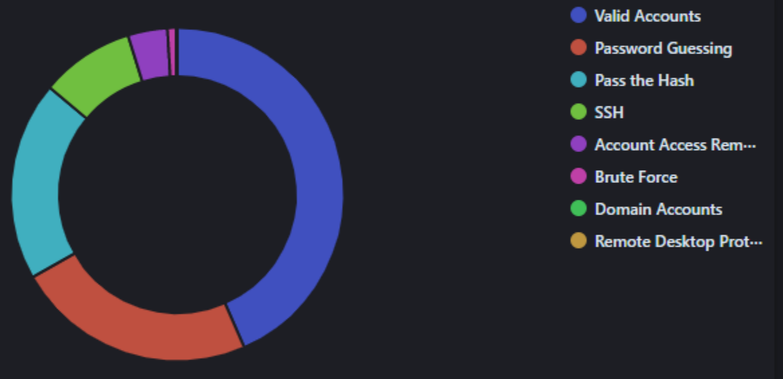
manager.name: smartlog.localdomain | + Add filter

Total	Level 12 or above alerts	Authentication failure	Authentication success
2733	0	414	842

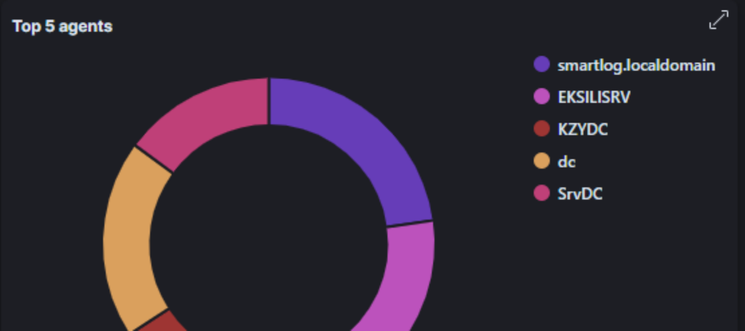
Alert level evolution



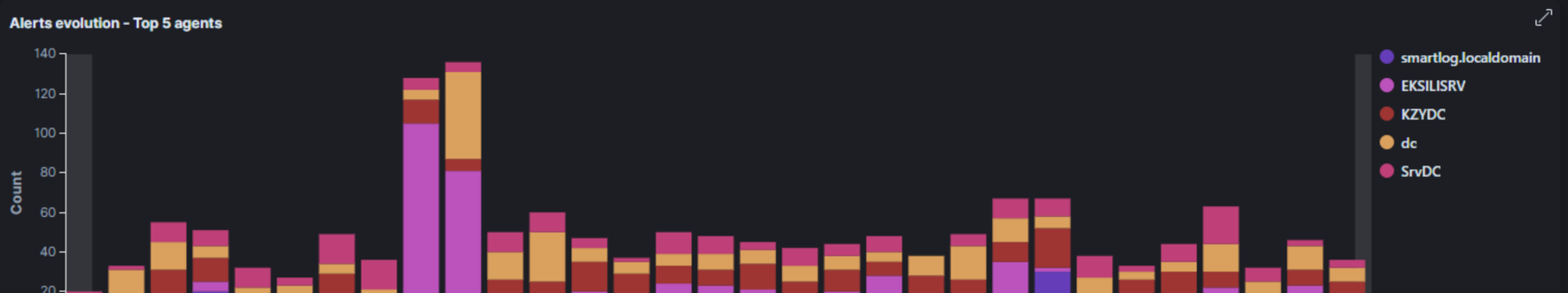
Top MITRE ATT&CKS



Top 5 agents



Alerts evolution - Top 5 agents



Search | KQL | Last 15 minutes | Show dates | Refresh

manager.name: smartlog.localdomain | + Add filter

wazuh-alerts-*

Search field names

Filter by type 0

Selected fields

- agent.name
- rule.description
- rule.id
- rule.level

Available fields

- agent.id
- agent.ip
- data.dstuser
- data.euid
- data.srcip
- data.srcport
- data.srcuser
- data.tty
- data.uid
- data.win.eventdata.authenticationPackageName
- data.win.eventdata.binary
- data.win.eventdata.data
- data.win.eventdata.dCName
- data.win.eventdata.elevatedToken
- data.win.eventdata.errorCode
- data.win.eventdata.errorDescription
- data.win.eventdata.failureReason
- data.win.eventdata.filePath
- data.win.eventdata.gPOCNName
- data.win.eventdata.impersonationLevel
- data.win.eventdata.ipAddress

2,745 hits

Aug 5, 2022 @ 17:03:17.711 - Aug 5, 2022 @ 17:18:17.711 Auto

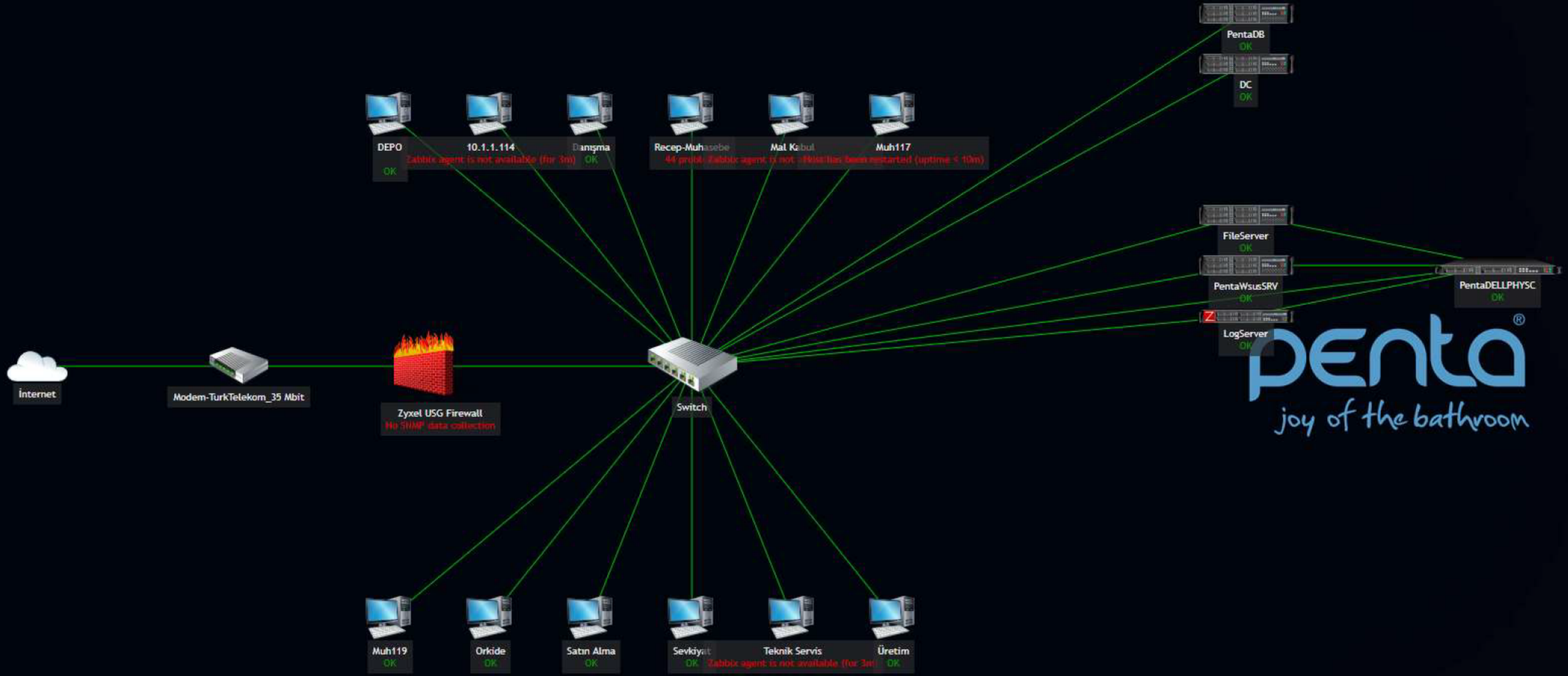
Time	agent.name	rule.description	rule.level	rule.id
Aug 5, 2022 @ 17:18:11.905	SrvADC	Windows logon success.	3	60106

Expanded document

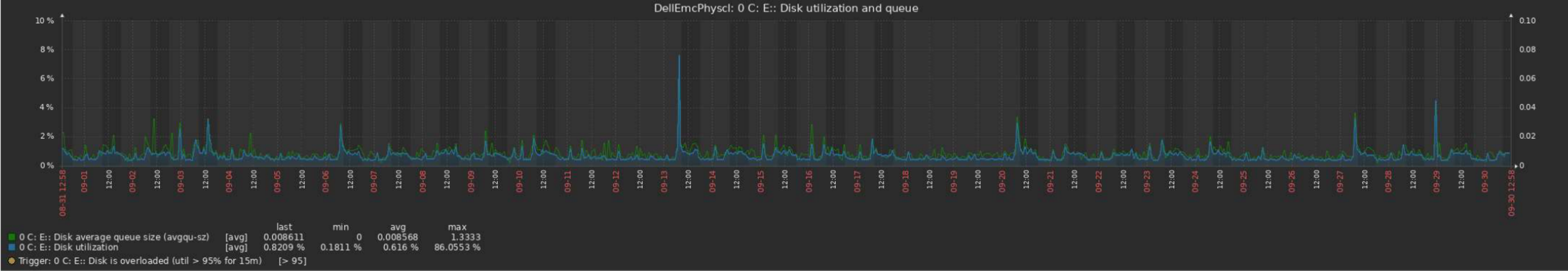
View surrounding documents | View single document

Table | JSON

_id	KUZeboIBJPBuu65d9Ax1
_index	wazuh-alerts-4.x-2022.08.05
_score	-
_type	_doc
agent.id	023
agent.ip	192.168.80.7
agent.name	SrvADC
data.win.eventdata.authenticationPackageName	Kerberos
data.win.eventdata.elevatedToken	%%1842
data.win.eventdata.impersonationLevel	%%1833
data.win.eventdata.ipAddress	fe80::d192:8c71:426:abaa
data.win.eventdata.ipPort	65156


PentaDB
OK
DC
OK
DEPO
OK
10.1.1.114
Zabbix agent is not available (for 3m)
Danışma
OK
Recep-Muhasebe
Mal Kabul
Muh117
44 probl: Zabbix agent is not available, has been restarted (uptime < 10m)
FileServer
OK
PentaWsusSRV
OK
PentaDELLPHYSC
OK
LogServer
OK
İnternet
Modem-TurkTelekom_35 Mbit
Zyxel USG Firewall
No SNMP data collection
Switch
Muh119
OK
Orkide
OK
Satın Alma
OK
Sevkiyat
OK
Teknik Servis
Zabbix agent is not available (for 3m)
Üretim
OK
penta
joy of the bathroom

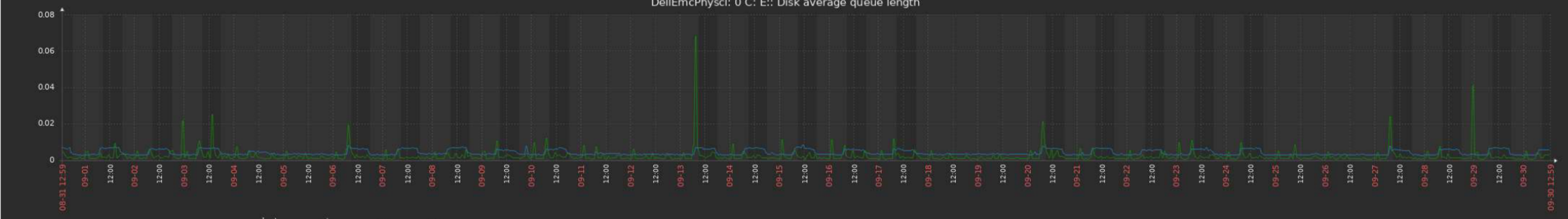
DellEmcPhyscl: 0 C: E:: Disk utilization and queue



		last	min	avg	max
0 C: E:: Disk average queue size (avgqu-sz)	[avg]	0.008611	0	0.008568	1.3333
0 C: E:: Disk utilization	[avg]	0.8209 %	0.1811 %	0.616 %	86.0553 %

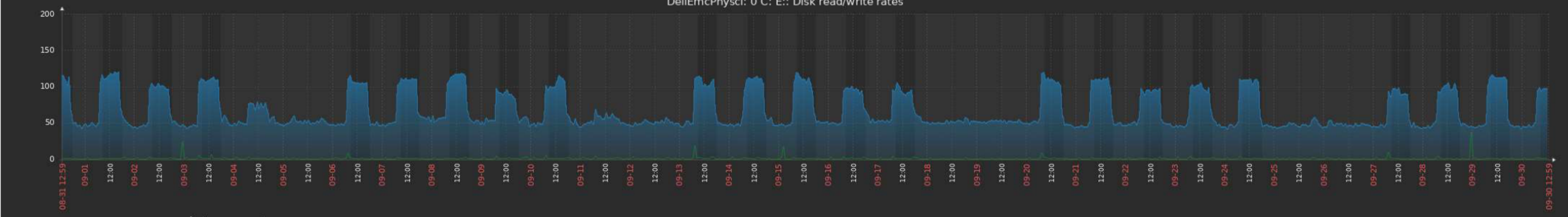
Trigger: 0 C: E:: Disk is overloaded (util > 95% for 15m) [> 95]

DellEmcPhyscl: 0 C: E:: Disk average queue length



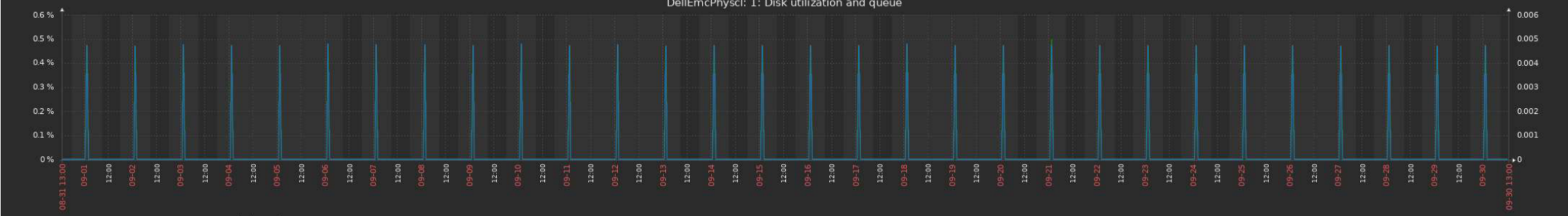
		last	min	avg	max
0 C: E:: Average disk read queue length	[avg]	0.002684	0	0.002121	0.8561
0 C: E:: Average disk write queue length	[avg]	0.005582	0.001787	0.004039	0.18

DellEmcPhyscl: 0 C: E:: Disk read/write rates



		last	min	avg	max
0 C: E:: Disk read rate	[avg]	1.2216 r/s	0 r/s	0.9369 r/s	1336.3576 r/s
0 C: E:: Disk write rate	[avg]	95.7051 w/s	28.665 w/s	65.7176 w/s	648.0363 w/s

DellEmcPhyscl: 1: Disk utilization and queue

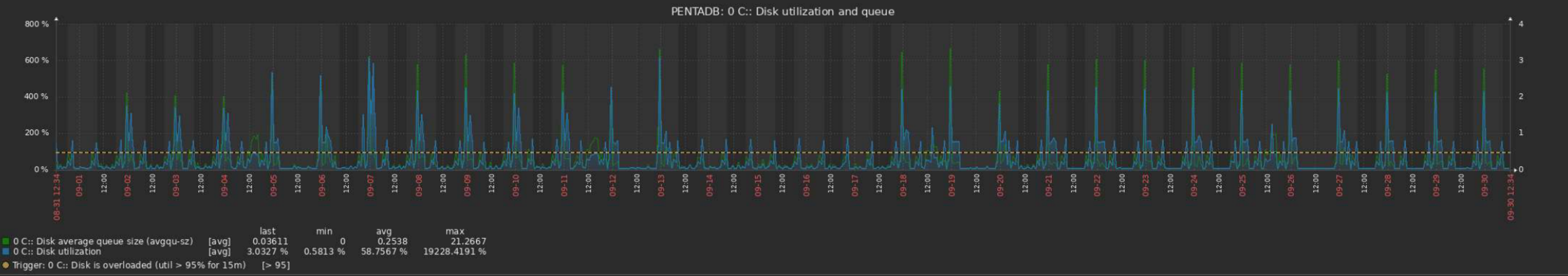


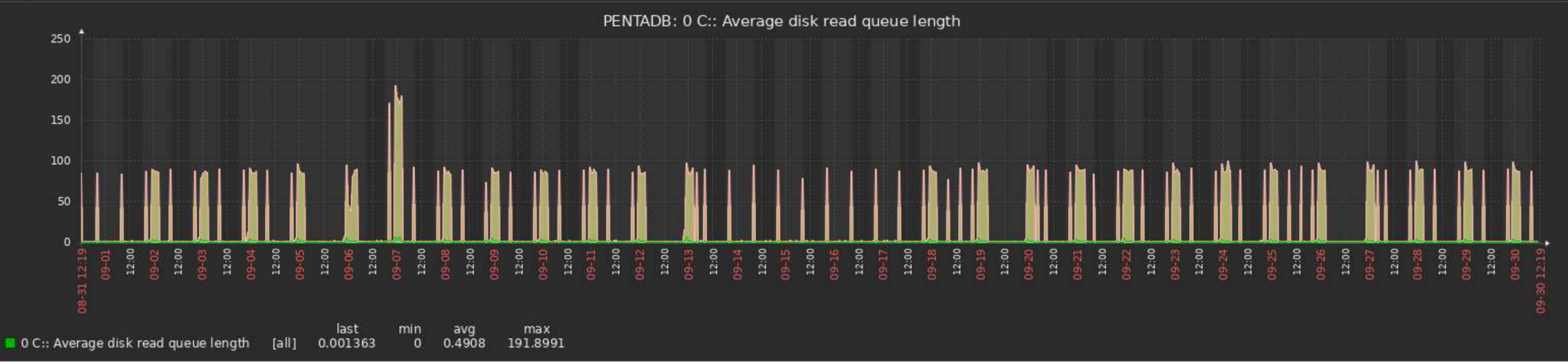
		last	min	avg	max
1: Disk average queue size (avgqu-sz)	[avg]	0	0	0.0001974	0.3
1: Disk utilization	[avg]	0 %	0 %	0.01962 %	28.5128 %

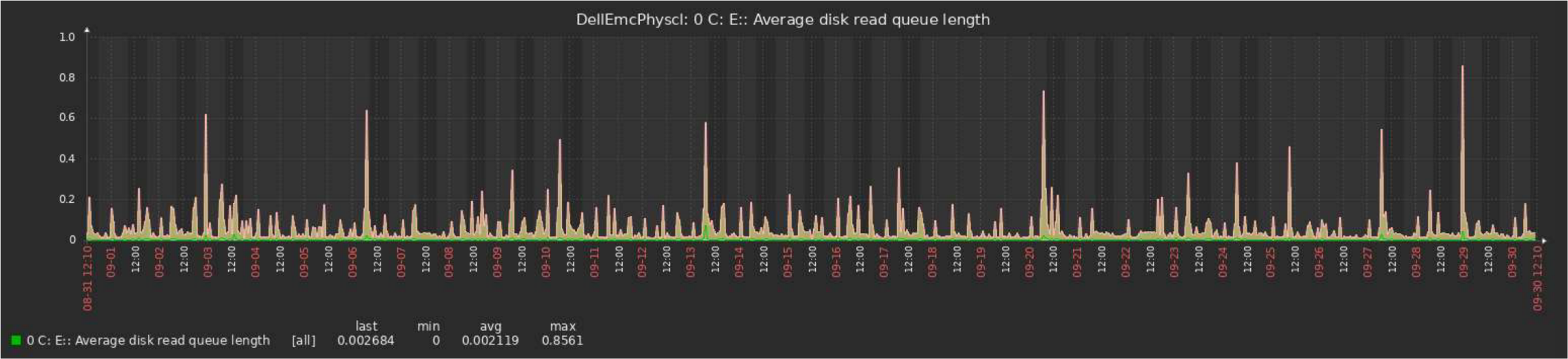
Trigger: 1: Disk is overloaded (util > 95% for 15m) [> 95]

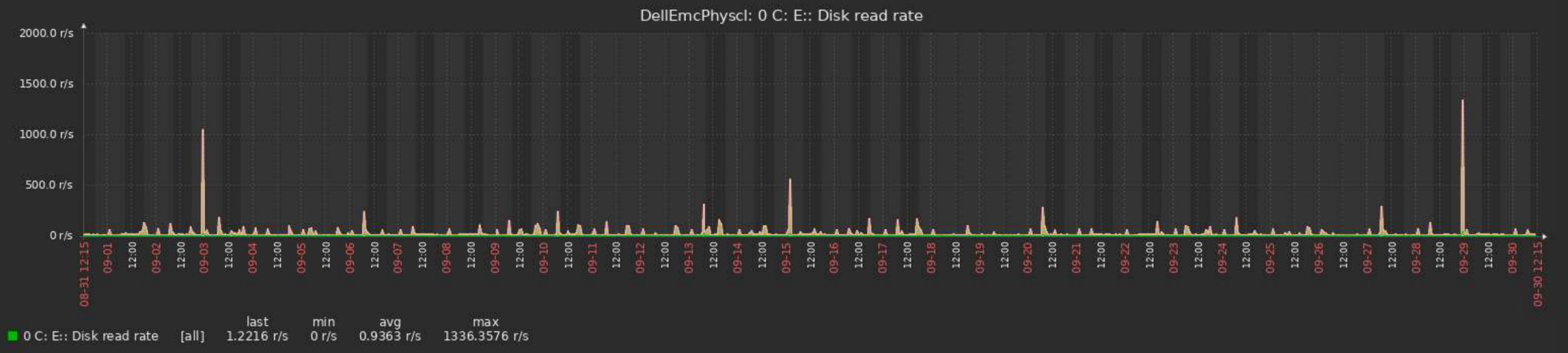
10.1.1.114	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 5	Dashboards 2	Web
DANISMA112	ZBX SNMP JMX IPMI	74	Enabled	Latest data	Problems 74	Graphs 32	Dashboards 2	Web
DC	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 11	Dashboards 2	Web
DC_ACTIVE	ZBX SNMP JMX IPMI		Enabled	Latest data	Problems	Graphs 5	Dashboards 2	Web
DELLEMC	ZBX SNMP JMX IPMI		Enabled	Latest data	Problems	Graphs 5	Dashboards 2	Web
DellEmcPhyscl	ZBX SNMP JMX IPMI	2	Enabled	Latest data	Problems 2	Graphs 19	Dashboards 2	Web
depo138	ZBX SNMP JMX IPMI	70	Enabled	Latest data	Problems 70	Graphs 27	Dashboards 2	Web
DWL-3200AP	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs	Dashboards 1	Web
FILESERVER	ZBX SNMP JMX IPMI	2	Enabled	Latest data	Problems 2	Graphs 11	Dashboards 2	Web
finans118	ZBX SNMP JMX IPMI	67 1	Enabled	Latest data	Problems 68	Graphs 18	Dashboards 2	Web
HavvaSonmez	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 11	Dashboards 2	Web
HP	ZBX SNMP JMX IPMI	65	Enabled	Latest data	Problems 65	Graphs 54	Dashboards 2	Web
malkabul142	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 5	Dashboards 2	Web
MF410 Series	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs	Dashboards 1	Web
MF410 Series1	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs	Dashboards 1	Web
MUH117	ZBX SNMP JMX IPMI	64 1	Enabled	Latest data	Problems 65	Graphs 12	Dashboards 2	Web
MUH119	ZBX SNMP JMX IPMI	44	Enabled	Latest data	Problems 44	Graphs 33	Dashboards 2	Web
ORKIDE-116	ZBX SNMP JMX IPMI	13	Enabled	Latest data	Problems 13	Graphs 21	Dashboards 2	Web
PENTAADDC_ACTIVE	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 5	Dashboards 2	Web
PENTADB	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 33	Dashboards 2	Web
PENTAWSUSSRV	ZBX SNMP JMX IPMI	3	Enabled	Latest data	Problems 3	Graphs 11	Dashboards 2	Web
SATINALMA2	ZBX SNMP JMX IPMI	71	Enabled	Latest data	Problems 71	Graphs 20	Dashboards 2	Web
satis4	ZBX SNMP JMX IPMI	94	Enabled	Latest data	Problems 94	Graphs 15	Dashboards 2	Web
SEVKIYAT	ZBX SNMP JMX IPMI	72	Enabled	Latest data	Problems 72	Graphs 11	Dashboards 2	Web
TEKNIKSERVIS	ZBX SNMP JMX IPMI	68	Enabled	Latest data	Problems 68	Graphs 27	Dashboards 2	Web
URETIM1	ZBX SNMP JMX IPMI	76	Enabled	Latest data	Problems 76	Graphs 11	Dashboards 2	Web
USG110	ZBX SNMP JMX IPMI	1	Enabled	Latest data	Problems 1	Graphs 8	Dashboards 1	Web
www.pentabanyokeyfi.com	ZBX SNMP JMX IPMI		Enabled	Latest data	Problems	Graphs	Dashboards	Web 1
Zabbix server	ZBX SNMP JMX IPMI	1 2	Enabled	Latest data	Problems 3	Graphs 25	Dashboards 3	Web

Displaying 29 of 29 found


PENTADB: 0 C:: Disk utilization and queue
800 %
600 %
400 %
200 %
0 %
4
3
2
1
0
08-31 12:34
09-01
09-02
09-03
09-04
09-05
09-06
09-07
09-08
09-09
09-10
09-11
09-12
09-13
09-14
09-15
09-16
09-17
09-18
09-19
09-20
09-21
09-22
09-23
09-24
09-25
09-26
09-27
09-28
09-29
09-30
09-30 12:34
last min avg max
0 C:: Disk average queue size (avgqu-sz) [avg] 0.03611 0 0.2538 21.2667
0 C:: Disk utilization [avg] 3.0327 % 0.5813 % 58.7567 % 19228.4191 %
Trigger: 0 C:: Disk is overloaded (util > 95% for 15m) [> 95]


PENTADB: 0 C:: Average disk read queue length
250
200
150
100
50
0
08-31 12:19
09-01
09-02
09-03
09-04
09-05
09-06
09-07
09-08
09-09
09-10
09-11
09-12
09-13
09-14
09-15
09-16
09-17
09-18
09-19
09-20
09-21
09-22
09-23
09-24
09-25
09-26
09-27
09-28
09-29
09-30
09-30 12:19
last min avg max
0 C:: Average disk read queue length [all] 0.001363 0 0.4908 191.8991


DellEmcPhyscl: 0 C: E:: Average disk read queue length
1.0
0.8
0.6
0.4
0.2
0
08-31 12:10
09-01
12:00
09-02
12:00
09-03
12:00
09-04
12:00
09-05
12:00
09-06
12:00
09-07
12:00
09-08
12:00
09-09
12:00
09-10
12:00
09-11
12:00
09-12
12:00
09-13
12:00
09-14
12:00
09-15
12:00
09-16
12:00
09-17
12:00
09-18
12:00
09-19
12:00
09-20
12:00
09-21
12:00
09-22
12:00
09-23
12:00
09-24
12:00
09-25
12:00
09-26
12:00
09-27
12:00
09-28
12:00
09-29
12:00
09-30
09-30 12:10
last
min
avg
max
0 C: E:: Average disk read queue length
[all]
0.002684
0
0.002119
0.8561


DellEmcPhyscl: 0 C: E:: Disk read rate
2000.0 r/s
1500.0 r/s
1000.0 r/s
500.0 r/s
0 r/s
08-31 12:15
09-01
12:00
09-02
12:00
09-03
12:00
09-04
12:00
09-05
12:00
09-06
12:00
09-07
12:00
09-08
12:00
09-09
12:00
09-10
12:00
09-11
12:00
09-12
12:00
09-13
12:00
09-14
12:00
09-15
12:00
09-16
12:00
09-17
12:00
09-18
12:00
09-19
12:00
09-20
12:00
09-21
12:00
09-22
12:00
09-23
12:00
09-24
12:00
09-25
12:00
09-26
12:00
09-27
12:00
09-28
12:00
09-29
12:00
09-30
09-30 12:15
last
min
avg
max
0 C: E:: Disk read rate
[all]
1.2216 r/s
0 r/s
0.9363 r/s
1336.3576 r/s

All files
Recent
Favorites
Shares
Tags

Deleted files
22.8 MB used
Settings

Add notes, lists or links …

Notlar
Recently edited

Talk
Recently edited

Reasons to use Nextclo… .pdf
Recently edited


Vineyard.jpg
Recently edited


Nextcloud community.jpg
Recently edited

Name	Size	Modified
Documents	391 KB	4 ay önce
Notlar	0 KB	4 ay önce
Photos	5,4 MB	4 ay önce
Talk	0 KB	4 ay önce
Templates	178 KB	4 ay önce
Nextcloud.png	49 KB	4 ay önce
Nextcloud intro.mp4	3,8 MB	4 ay önce
Nextcloud Manual.pdf	12,1 MB	4 ay önce
Reasons to use Nextcloud.pdf	954 KB	4 ay önce
5 folders and 4 files	22,8 MB	