DevOps 2TIN

Chapter 9

Monitoring & Reporting

DE HOGESCHOOL MET HET NETWERK

Elfde-Liniestraat 24, 3500 Hasselt, www.pxl.be

Monitoring & Reporting

Monitoring
Metrics
Logs
Monitoring History
Monitoring Tools
Low Risk Releases

HOGESCHOOL PXL

Wat is monitoren?

Dictionary

Search for a word

monitor

/ˈmɒnɪtə/

See definitions in:

All | Intelligence | Broadcasting | Electronics

verb

gerund or present participle: **monitoring**

observe and check the progress or quality of (something) over a period of time; keep under systematic review.
"equipment was installed to monitor air quality"

Similar: observe | watch | keep an eye on | keep track of | track

- maintain regular surveillance over.
  "he was a man of routine and it was easy for an enemy to monitor his movements"
- listen to and report on (a foreign radio broadcast or a phone conversation).
  "listening devices were used to monitor conversations"

Definitions from Oxford Languages

Feedback

Translations and more definitions

Wat is monitoren?

Dictionary

Search for a word

monitor

/ˈmɒnɪtə/

See definitions in:

All | Intelligence | Broadcasting | Electronics

verb

gerund or present participle: **monitoring**

observe and check the progress or quality of (something) over a period of time; keep under systematic review.

"equipment was installed to monitor air quality"

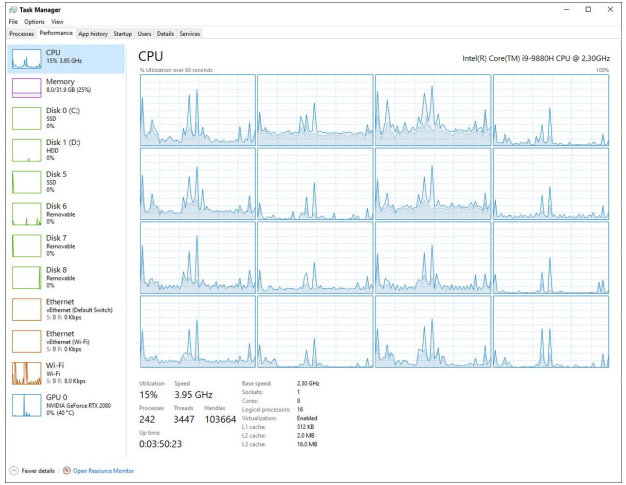
Similar: observe | watch | keep an eye on | keep track of | track

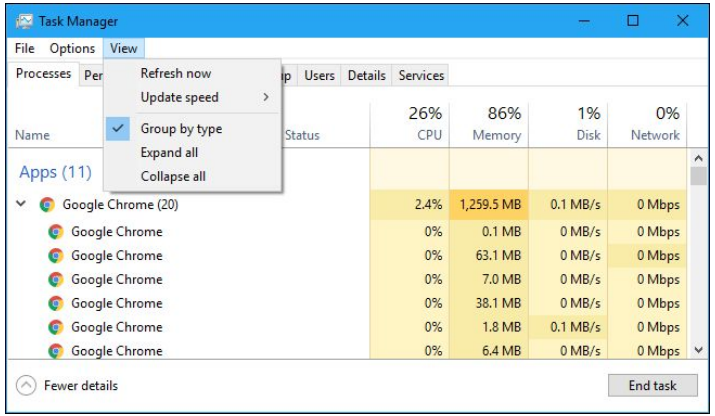
- maintain regular surveillance over.
  "he was a man of routine and it was easy for an enemy to monitor his movements"
- listen to and report on (a foreign radio broadcast or a phone conversation).
  "listening devices were used to monitor conversations"

Definitions from Oxford Languages

Feedback

Translations and more definitions





Metrics

Metrics? -> Meet punten

Dingen zoals:

- Temperatuur van HDDs
- CPU percentage
- Netwerksnelheden
- IO van een HDD

Maar ook:

- Programma logging
- Netwerk logging
- ...

Dictionary

Search for a word

metric[1]

/ˈmɛtrɪk/

See definitions in:

All | Commerce | Mathematics | Physics | Prosody

noun

plural noun: **metrics**

1. TECHNICAL
   a system or standard of measurement.
   "the levels of branching are arbitrary and no precise metric is applied to distance between the nodes"
2. INFORMAL
   the metric system.
   "it's easier to work in metric"

Definitions from Oxford Languages *Feedback*

Translations and more definitions

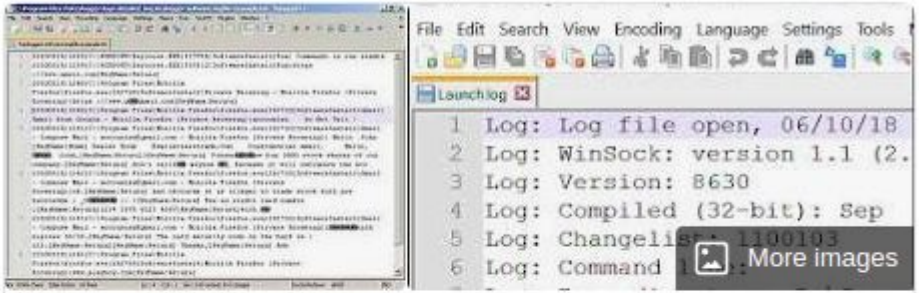
Log files

- /var/log/syslog

```
Dec  4 08:53:45 ip-172-31-42-222 agent[59527]: 2020-12-04 09:53:45 CET | CORE | WARN | (pkg/coll
ector/python/datadog_agent.go:120 in LogMessage) | disk:e5dffb8bef24336f | (disk.py:93) | Unable
 to get disk metrics for /run/docker/netns/c69b319490b4: [Errno 13] Permission denied: '/run/doc
ker/netns/c69b319490b4'. You can exclude this mountpoint in the settings if it is invalid.
Dec  4 08:53:45 ip-172-31-42-222 agent[59527]: 2020-12-04 09:53:45 CET | CORE | WARN | (pkg/coll
ector/python/datadog_agent.go:120 in LogMessage) | disk:e5dffb8bef24336f | (disk.py:93) | Unable
 to get disk metrics for /var/lib/docker/overlay2/bdd2e865c3b8ea3d668fd56cd2468b589eddb92ec2d3cc
cf8994f3d3a0bc4dc4/merged: [Errno 13] Permission denied: '/var/lib/docker/overlay2/bdd2e865c3b8e
a3d668fd56cd2468b589eddb92ec2d3cccf8994f3d3a0bc4dc4/merged'. You can exclude this mountpoint in
the settings if it is invalid.
Dec  4 08:53:45 ip-172-31-42-222 agent[59527]: 2020-12-04 09:53:45 CET | CORE | WARN | (pkg/coll
ector/python/datadog_agent.go:120 in LogMessage) | disk:e5dffb8bef24336f | (disk.py:93) | Unable
 to get disk metrics for /run/docker/netns/7c998a975dda: [Errno 13] Permission denied: '/run/doc
ker/netns/7c998a975dda'. You can exclude this mountpoint in the settings if it is invalid.
^C
ubuntu@ip-172-31-42-222:/var/log$ `
```

- /var/log/kern

```
name="snap-update-ns.lxd" pid=53437 comm="apparmor_parser"
Dec  2 07:54:29 ip-172-31-42-222 kernel: [47617.716403] audit: type=1400 audit(1606895669.218:108): appa
rmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"
name="snap.lxd.activate" pid=53438 comm="apparmor_parser"
Dec  2 07:54:29 ip-172-31-42-222 kernel: [47617.720163] audit: type=1400 audit(1606895669.222:109): appa
rmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"
name="snap.lxd.benchmark" pid=53439 comm="apparmor_parser"
Dec  2 07:54:29 ip-172-31-42-222 kernel: [47617.723771] audit: type=1400 audit(1606895669.226:110): appa
rmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"
name="snap.lxd.buginfo" pid=53440 comm="apparmor_parser"
Dec  2 07:54:29 ip-172-31-42-222 kernel: [47617.727273] audit: type=1400 audit(1606895669.230:111): appa
rmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"
name="snap.lxd.check-kernel" pid=53441 comm="apparmor_parser"
Dec  2 07:54:29 ip-172-31-42-222 kernel: [47617.736972] audit: type=1400 audit(1606895669.238:112): appa
rmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"
name="snap.lxd.daemon" pid=53442 comm="apparmor_parser"
```



Logfile

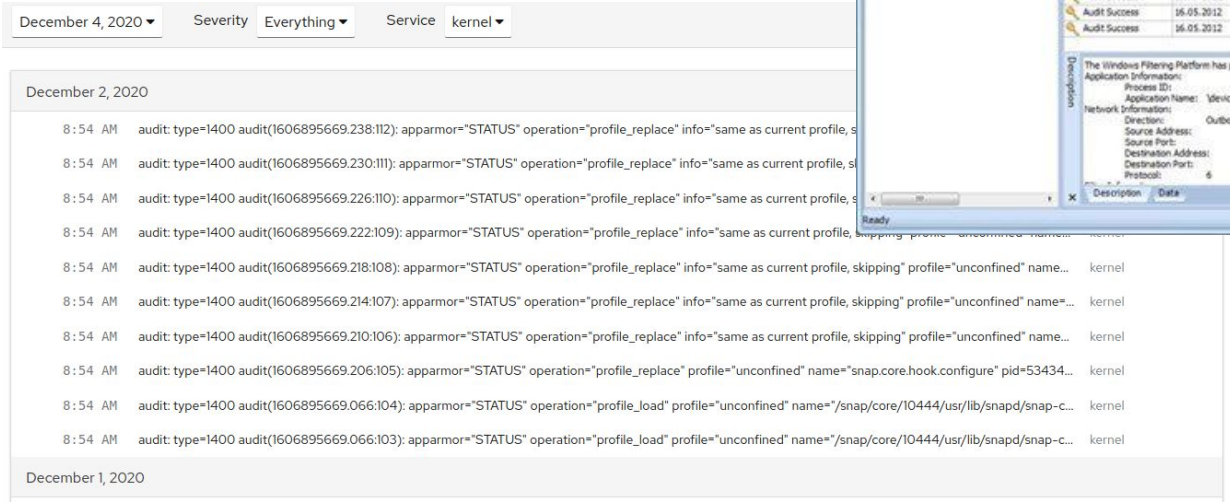
Software type

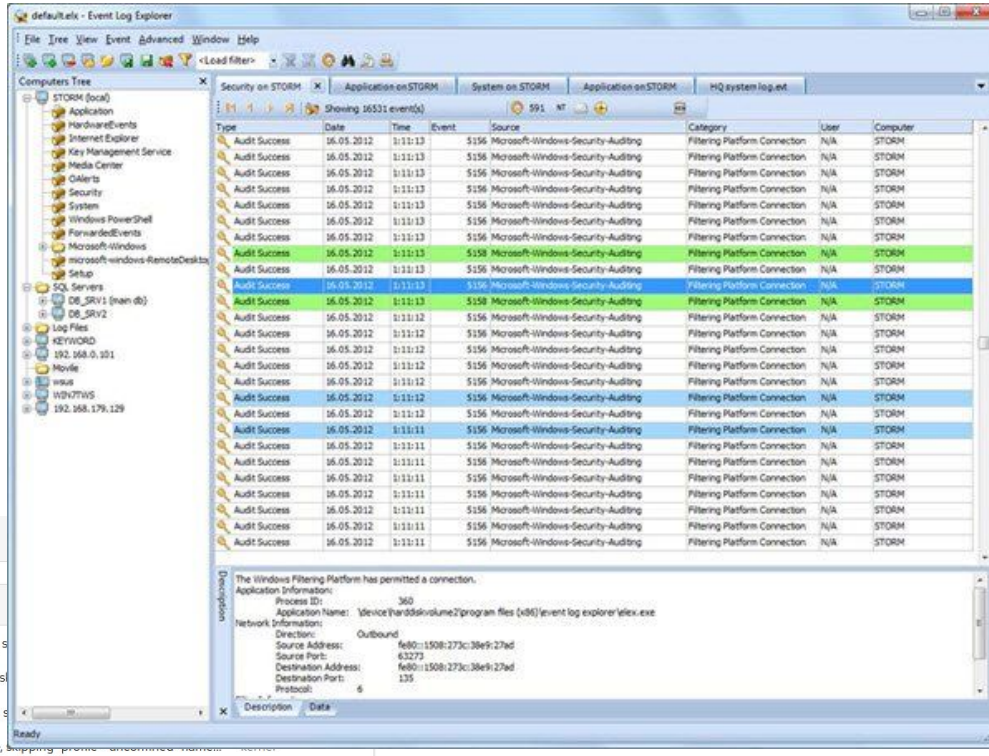
In computing, a log file is a file that records either events that occur in an operating system or other software runs, or messages between different users of a communication software. Logging is the act of keeping a log. In the simplest case, messages are written to a single log file. Wikipedia

Local logs

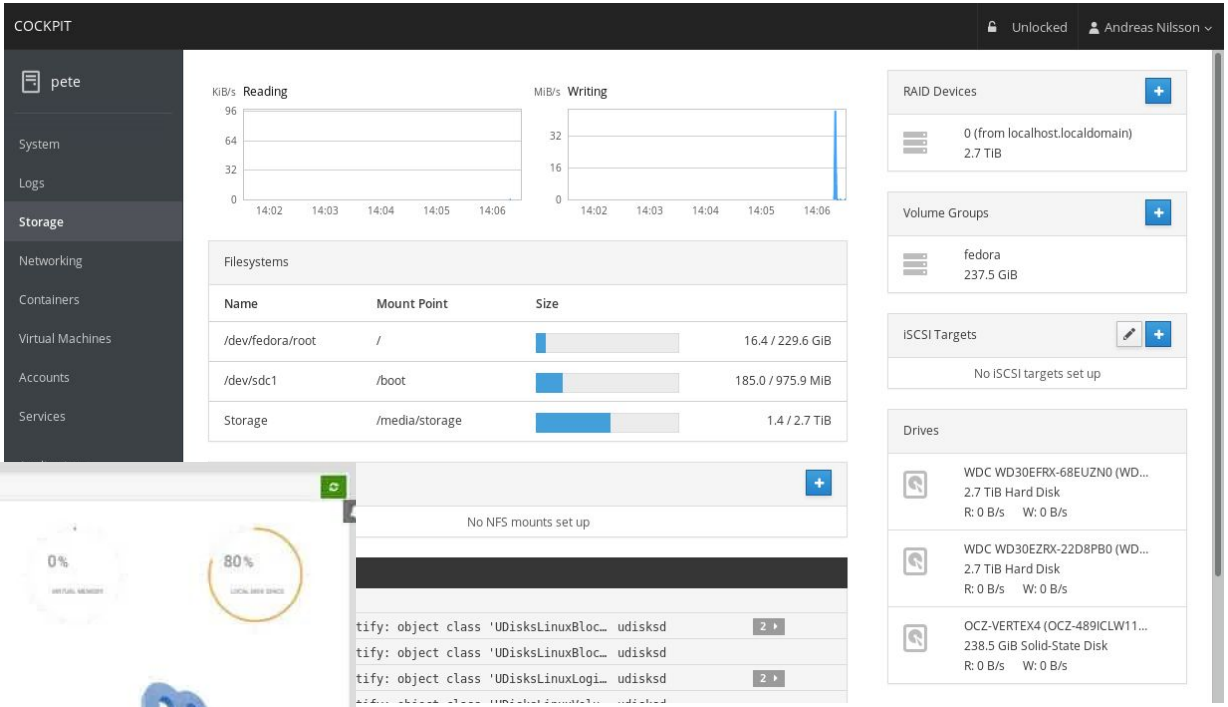
Hoe bekijken?

- **Windows:**
  - **Event viewer**
- ***nix:**
  - **Cockpit**
  - **Webmin**





Local logs

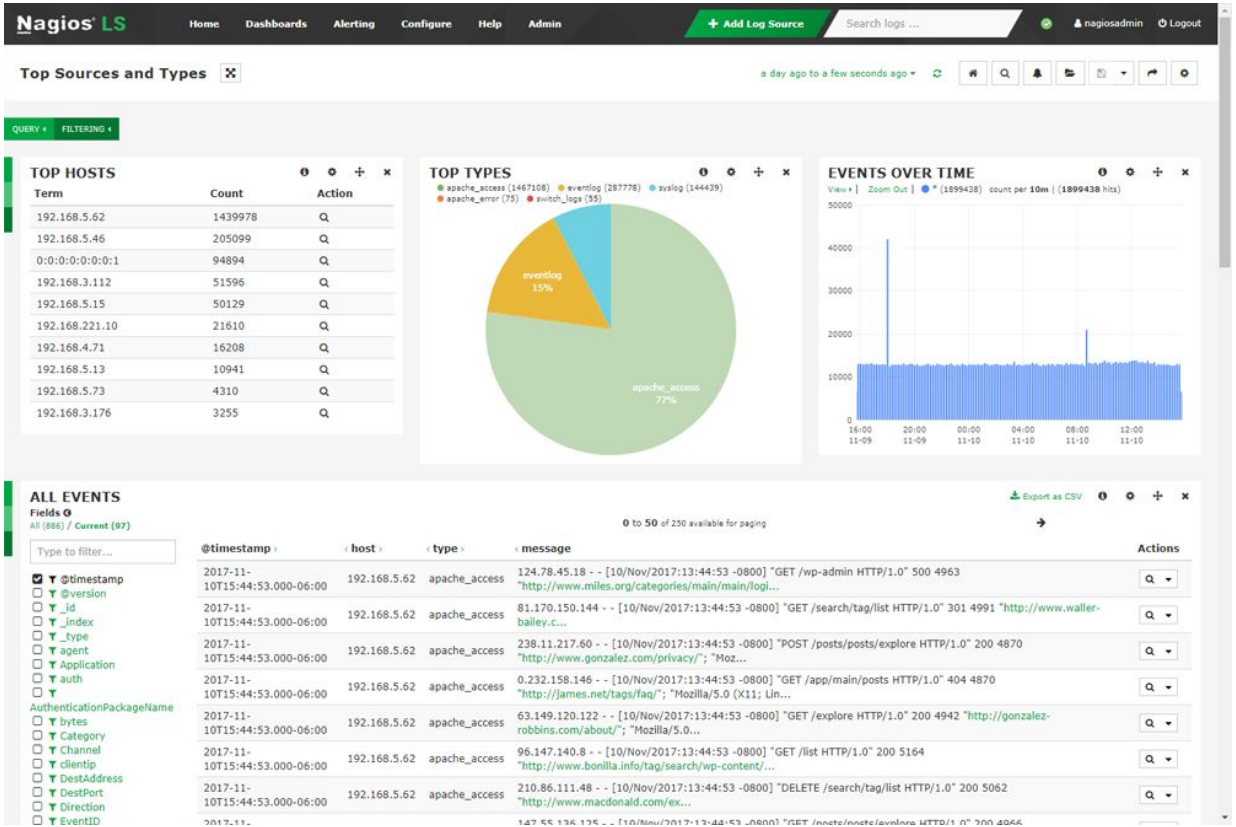

COCKPIT
Unlocked
Andreas Nilsson
pete
System
Logs
Storage
Networking
Containers
Virtual Machines
Accounts
Services
KiB/s Reading
MiB/s Writing
Filesystems
Name
Mount Point
Size
/dev/fedora/root
/
16.4 / 229.6 GiB
/dev/sdc1
/boot
185.0 / 975.9 MiB
Storage
/media/storage
1.4 / 2.7 TiB
No NFS mounts set up
RAID Devices
0 (from localhost.localdomain)
2.7 TiB
Volume Groups
fedora
237.5 GiB
iSCSI Targets
No iSCSI targets set up
Drives
WDC WD30EFRX-68EUZN0 (WD...
2.7 TiB Hard Disk
R: 0 B/s W: 0 B/s
WDC WD30EZRX-22D8PB0 (WD...
2.7 TiB Hard Disk
R: 0 B/s W: 0 B/s
OCZ-VERTEX4 (OCZ-489ICLW11...
238.5 GiB Solid-State Disk
R: 0 B/s W: 0 B/s


Dashboard
System Information
Webmin
System
Servers
Others
Networking
Hardware
Cluster
Un-used Modules
Refresh Modules
72%
30%
0%
80%
System hostname
Operating system
Webmin version
Theme version
Time on system
Kernel and CPU
Processor information
System uptime
Running processes
CPU load averages
Real memory
Virtual memory
Local disk space
Package updates
Recent Webmin logins
webmin

Log aggregatie

Hoe bekijken?

- ELK Stack
  - Graylog
  - Nagios Log server
  - Splunk



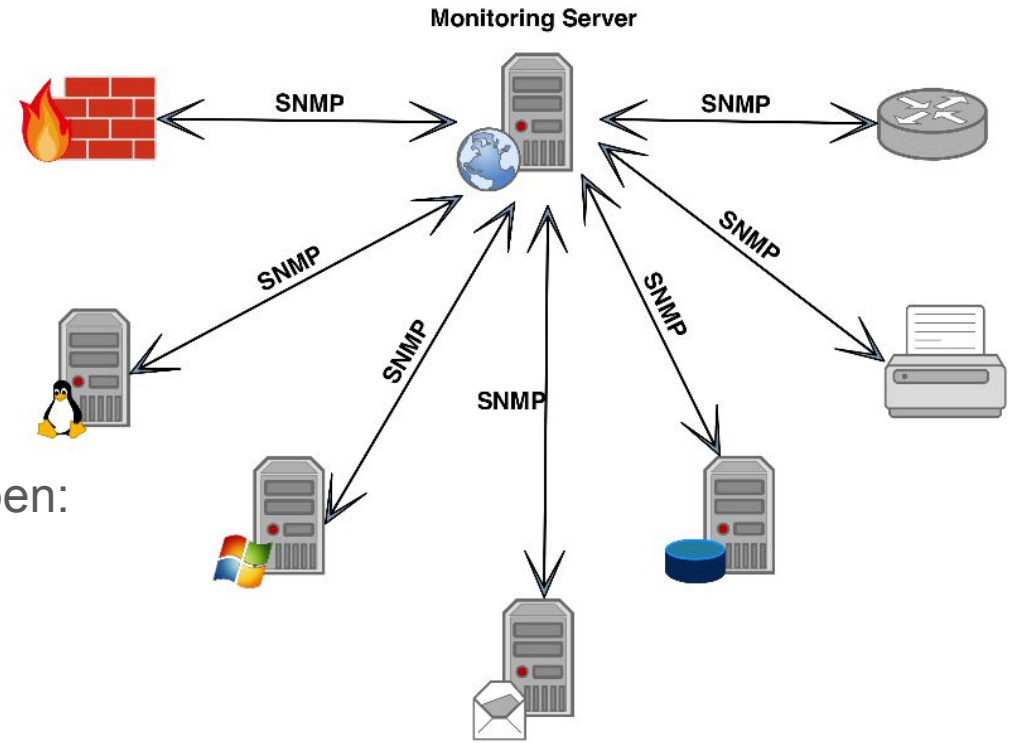
splunk>

Monitoring History

Van hardware monitoring tot AI-Ops.

Waar het begon ->
Simple **N**etwork **M**onitoring **P**rotocol
Est. 1988

Elk apparaat/software kon MiBs hebben:
Management **i**nformation **B**ase file:
Definieert metrics



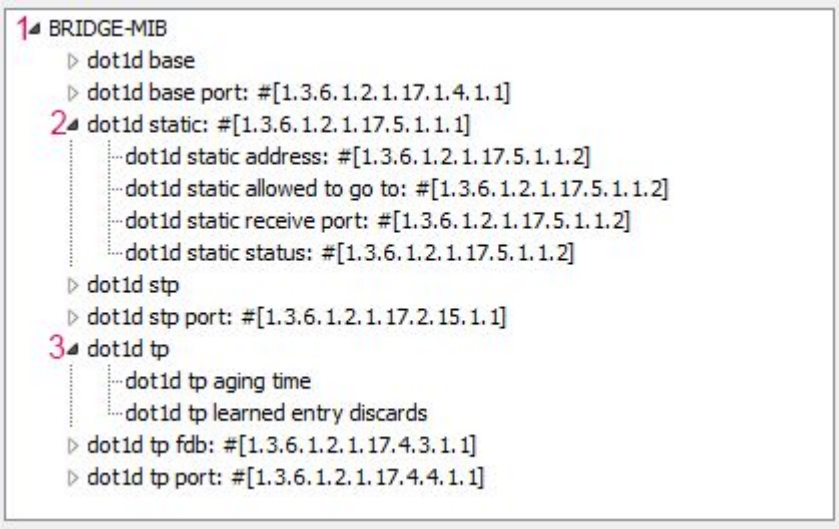
Source: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

Monitoring History

Van hardware monitoring tot AI-Ops.

Waar het begon ->
Simple **N**etwork **M**onitoring **P**rotocol
Est. 1988

Elk apparaat/software kon MiBs hebben:
Management **i**nformation **B**ase file:
Definieert metrics



Source: https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol

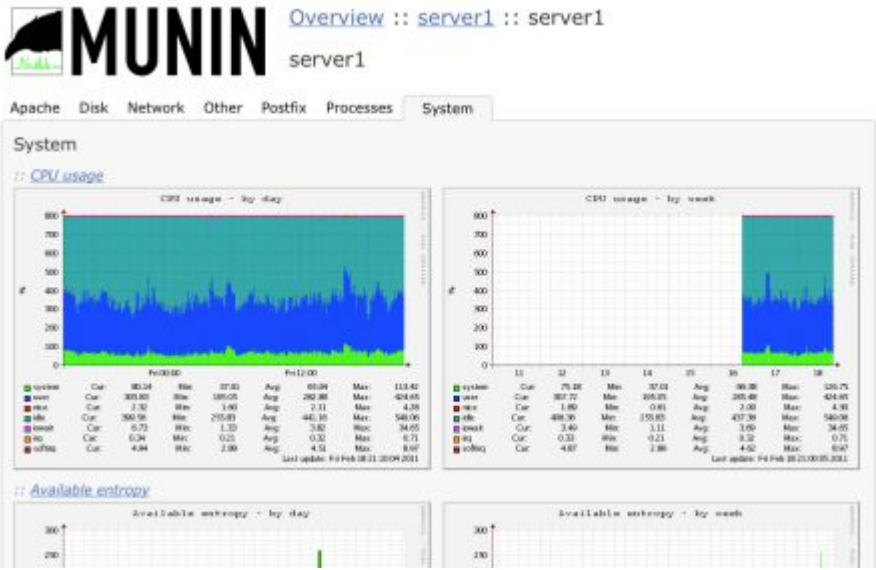
Monitoring Tools

Eerste tools aggregeerde enkel (SNMP) data en toonde die

Voorbeelden:

- Munin
- PRTG (in het begin)

Monitoring Tools



Monitoring Tools

Volgende generatie ging ook iets met de monitoring data doen:

Maar nog steeds heel erg focussed op hardware en “klassieke” servers

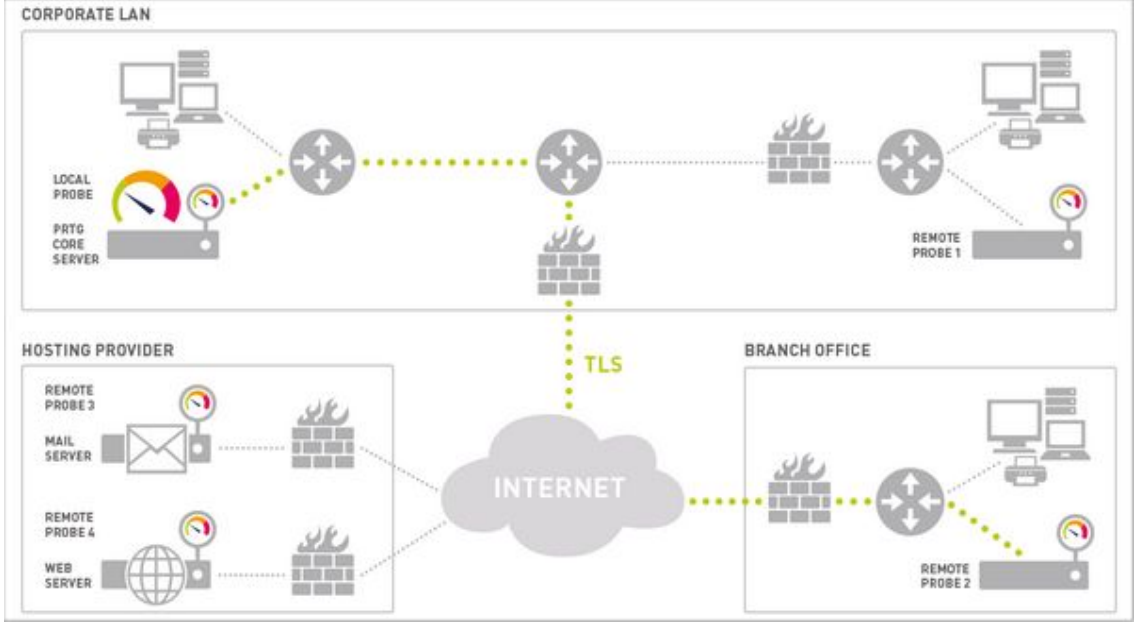
Alerting Tools

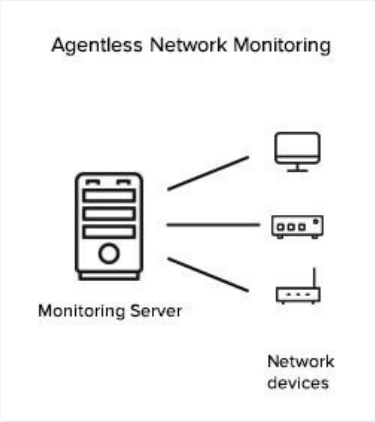
Voorbeelden:

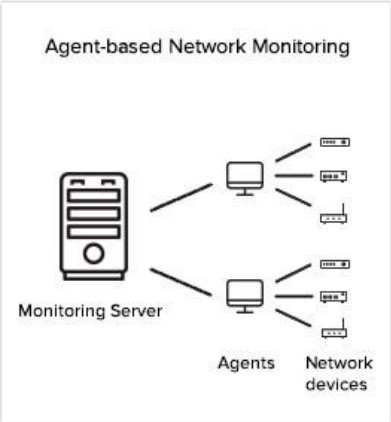
- PRTG (nu)
- Nagios
- Check_mk

Monitoring Tools

Om beter en diepgaander te kunnen monitoren:
Introductie **Agent software**







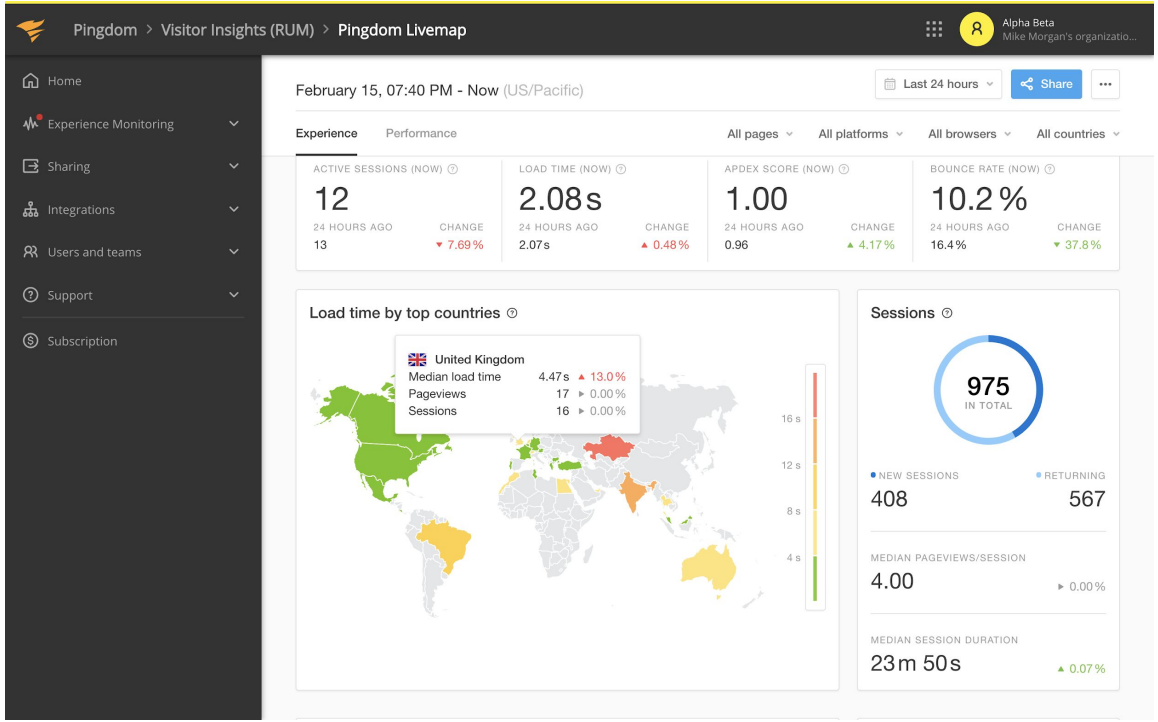
Monitoring Tools

Volgende generatie ging meer op “internet” tools focussen en dus external monitoring doen

Voorbeelden:

- Pingdom
- Freshping
- Uptimerobot

Overlap met testtools
Zoals Webpagetest.org

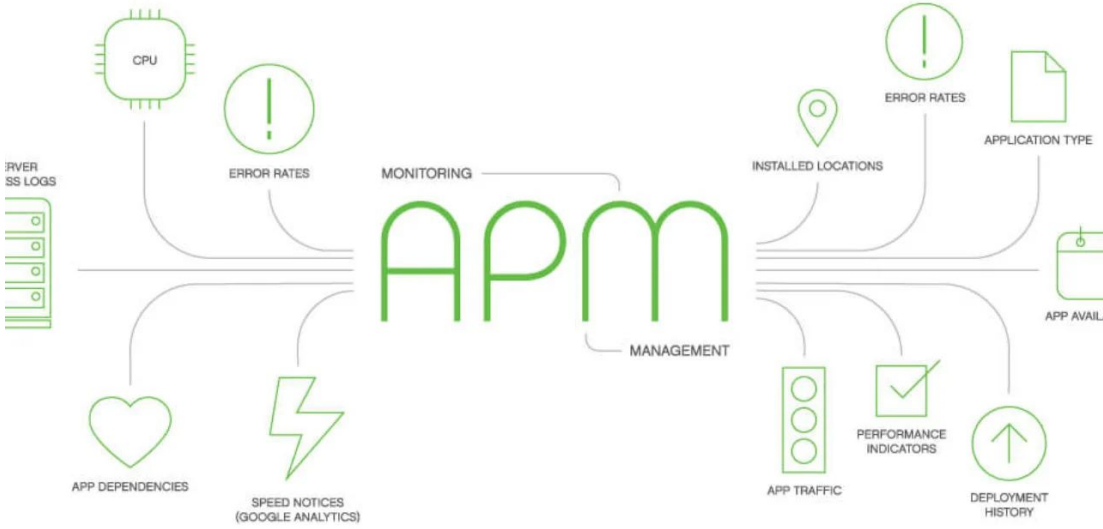


Monitoring Tools

APM is born!
Est +-2012

Mix van voorgaande met Business Logic en predictive /proactive monitoring

-Zabbix/Datadog/New Relic ...

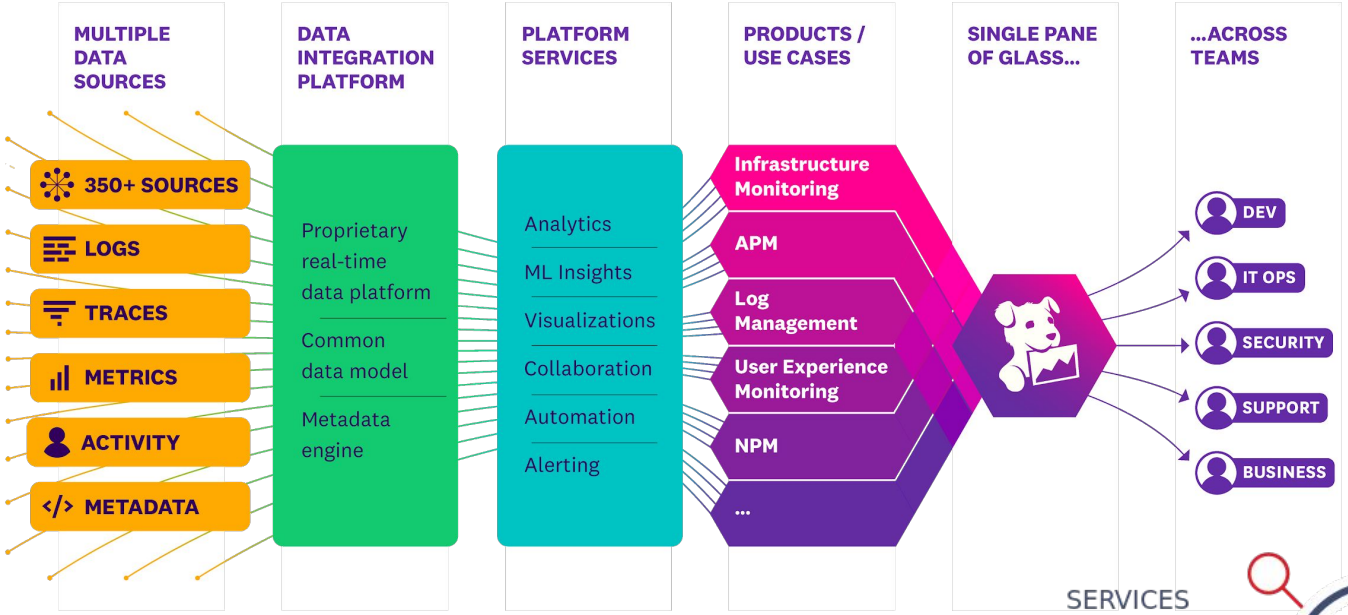


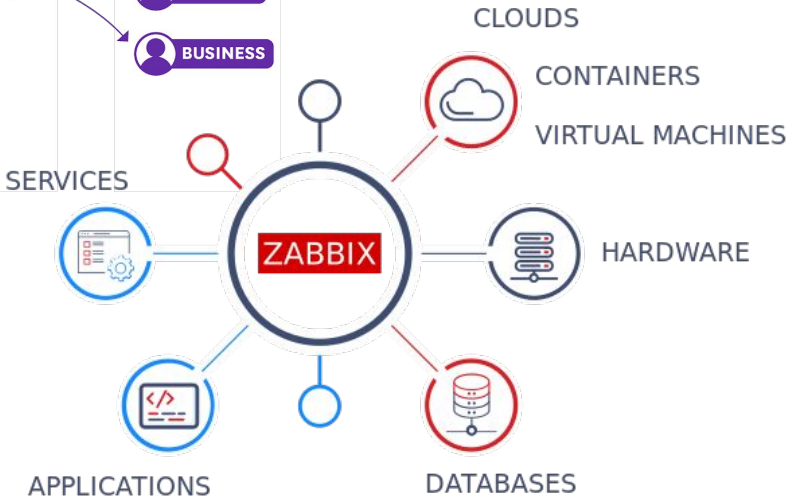
Application performance management

In the fields of information technology and systems management, application performance management is the monitoring and management of performance and availability of software applications. APM strives to detect and diagnose complex application performance problems to maintain an expected level of service. Wikipedia

Source:
https://en.wikipedia.org/wiki/Application_performance_management

Monitoring Tools



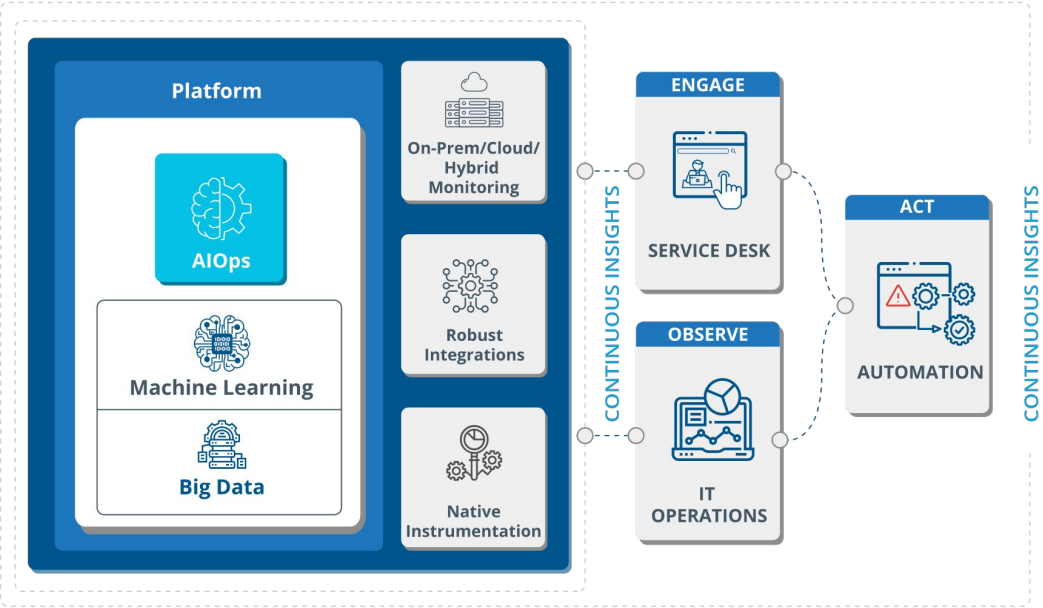


Monitoring Tools

AI ops
Est +-2016

Mix van voorgaande met Business Logic en predictive /proactive monitoring

- BigPanda/Dynatrace/Anodot ...



Source:
https://en.wikipedia.org/wiki/Artificial_Intelligence_for_IT_Operations

Monitoring Tools

Doel van logging:

Generating real-time feedback!

Monitoring in functie van deployment

- Applicaties updaten brengen extra uitdagingen met zich mee
  - Downtime tijdens update (of na update?)
  - Bugs
  - Rollback is niet eenvoudig
  - Alles of niets
- Naast klassieke monitoring van servers, services, logs, .. monitoren in functie van deployments
  - Extra data & real time feedback op de deploy fase

    => **Low(er) risk releases!**

Low Risk releases - Bringing it together

Classic deploys

Pros: Simple, fast, cheap

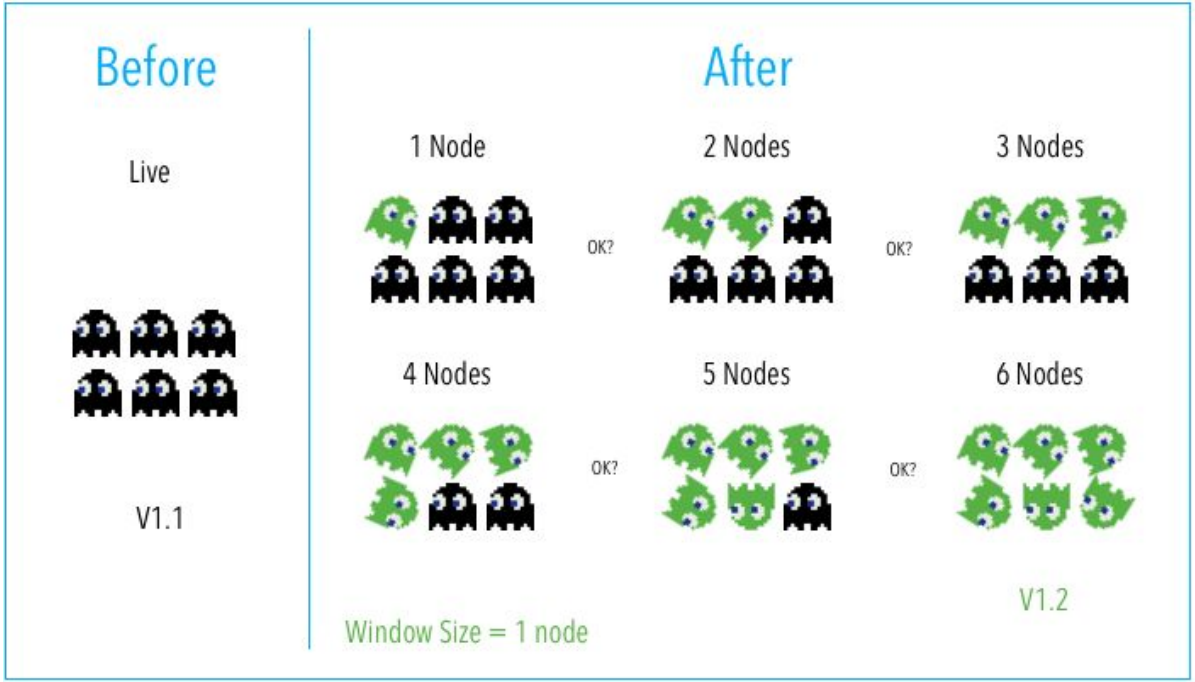
Cons: Risk, outages, slow rollback, unemployment

Low Risk releases - Bringing it together

Rolling deploys

Pros: Simple, cheap, relatively simple to rollback, less risk than basic deployment.

Cons: App/DB needs to support both new and old artifacts. Manual checks/verification at each increment could take a long time.



Low Risk releases - Bringing it together

Testing as a Metric!

Blue/Green deploys

Pros:

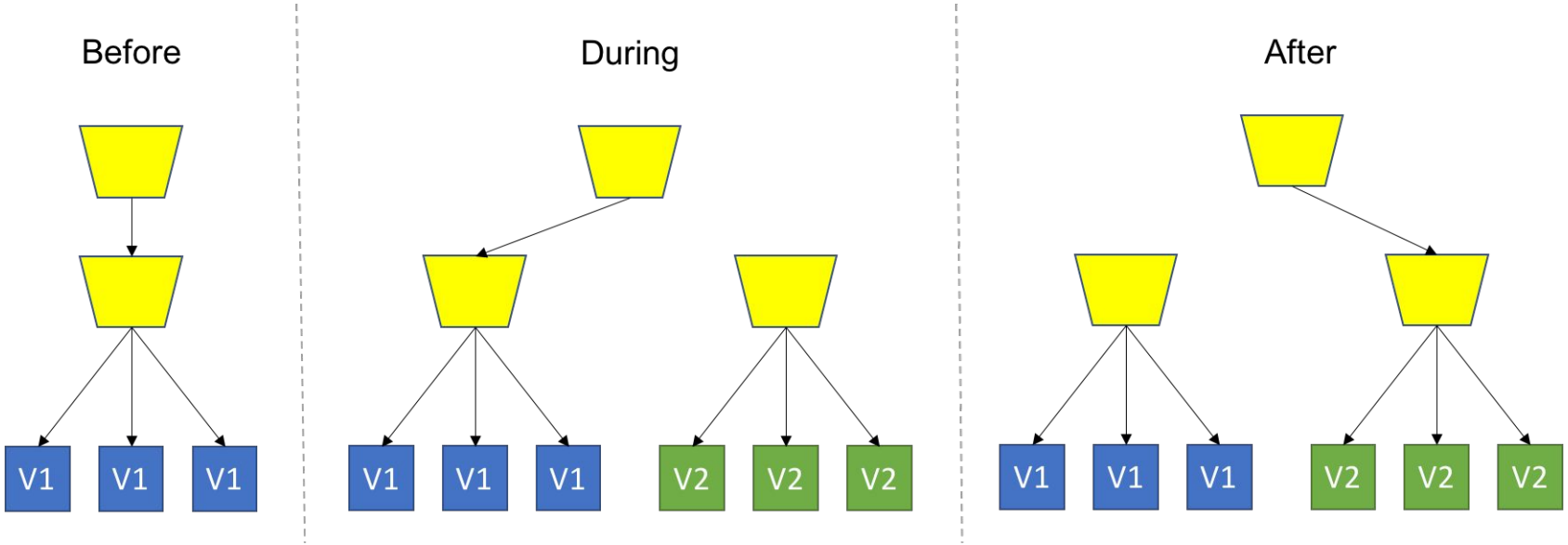
- Simple, fast, well understood.
- Less risk relative to other deployment strategies
- Rapid rollback

Cons:

- complex and expensive
- coverage may not identify all anomalies

Low Risk releases - Bringing it together

Blue/Green deploys



Low Risk releases - Bringing it together

Testing as a Metric!

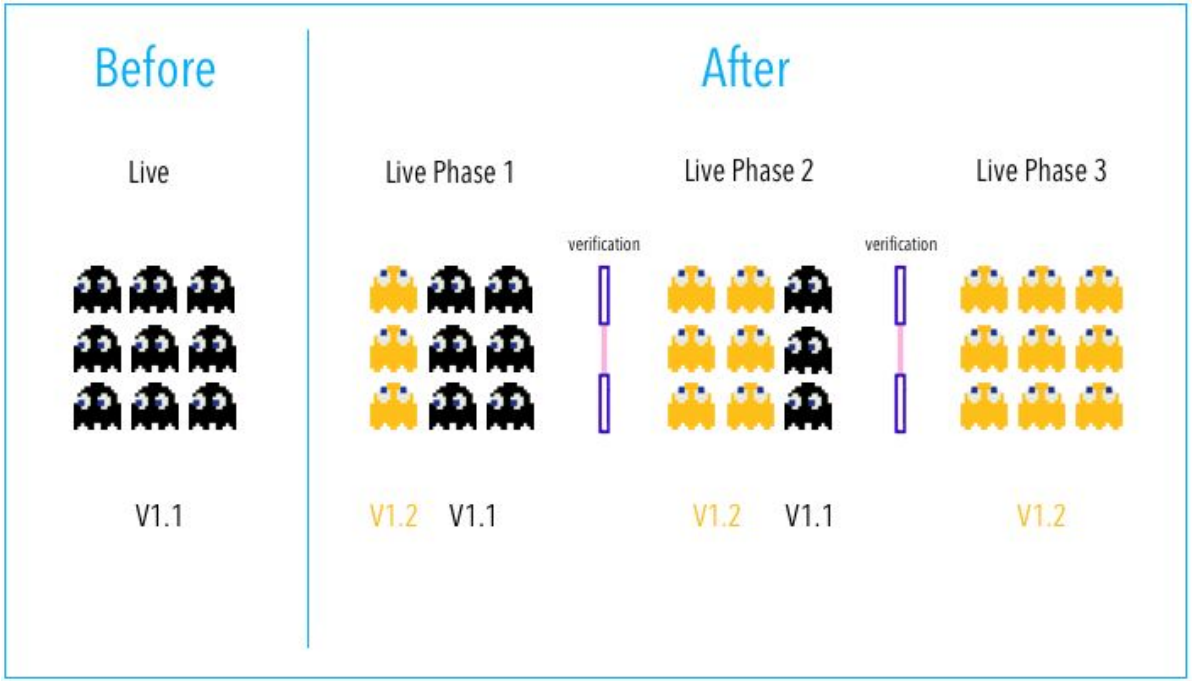
Canary deploys

Pros:

- Deploy in small phases
- Test in production with real users & use cases
- Cheaper than blue/green,Fast and safe rollback

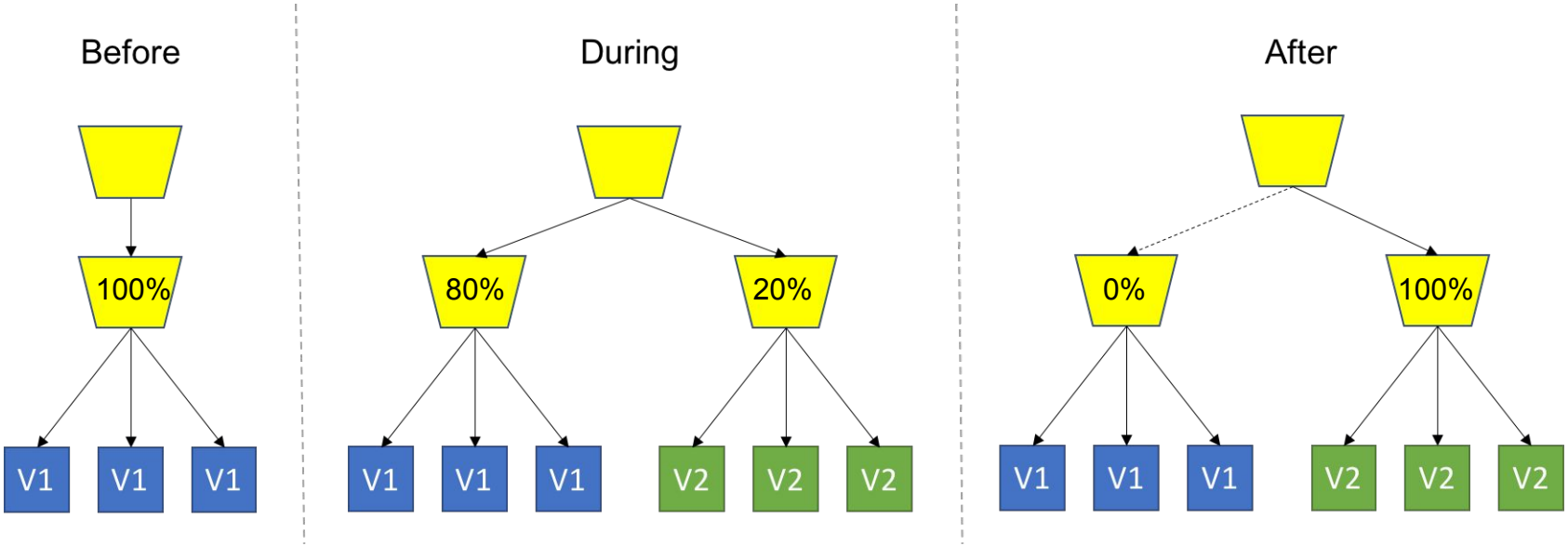
Cons:

- Scripting canary deployments can be complex
- Required monitoring & instrumentation (APM, Log, Infra, End User, …) for testing in production



Low Risk releases - Bringing it together

Canary deploys



Low Risk releases - Bringing it together

Testing as a Metric!

A/B Testing

Pros:

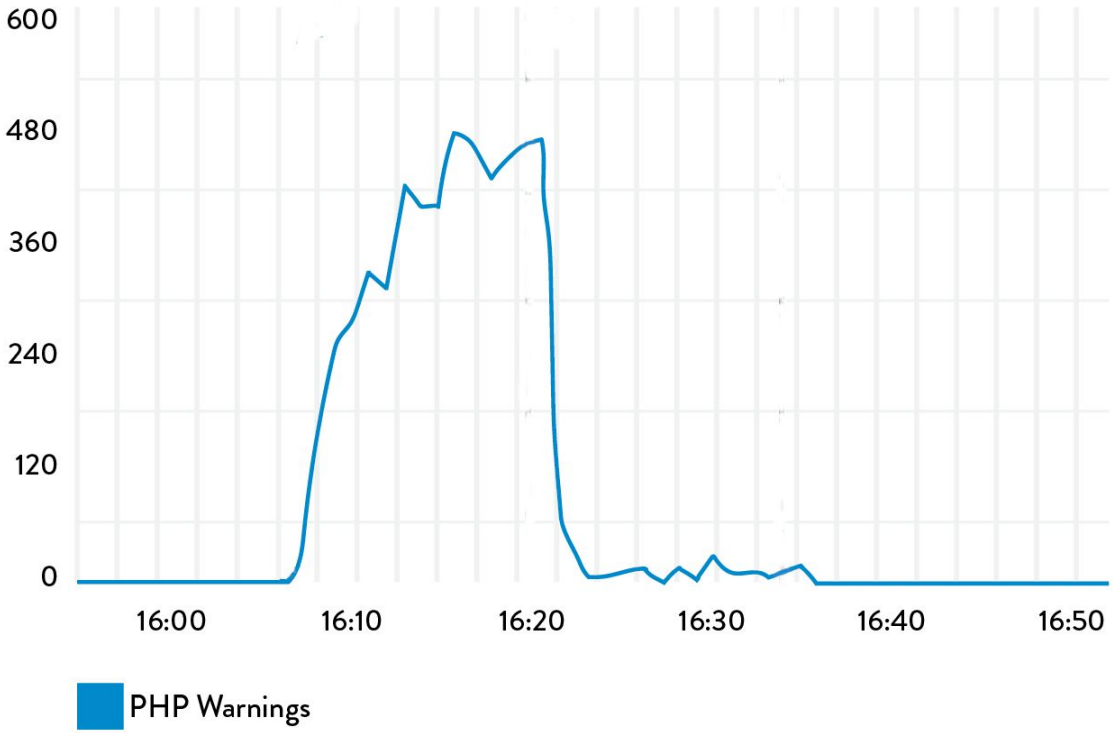
Fast, easy, and cheap way to test new features in production. Lots of tools exist to enable this.

Cons:

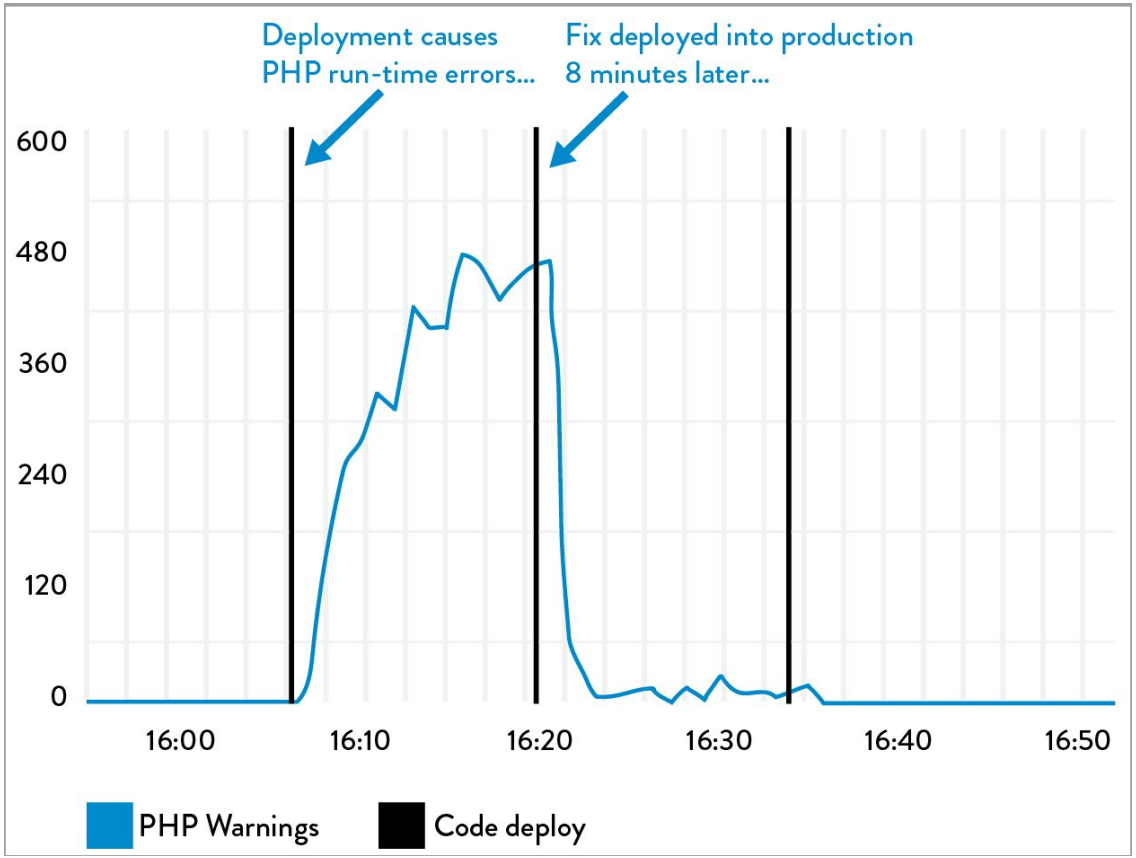
- Experiments can sometimes break the app/service/user experience.
- Scripting AB tests can be complex.
- Database compatibility (schema changes, backward compatibility)

Source: https://harness.io/2018/02/blue-green-vs-canary-deployments/

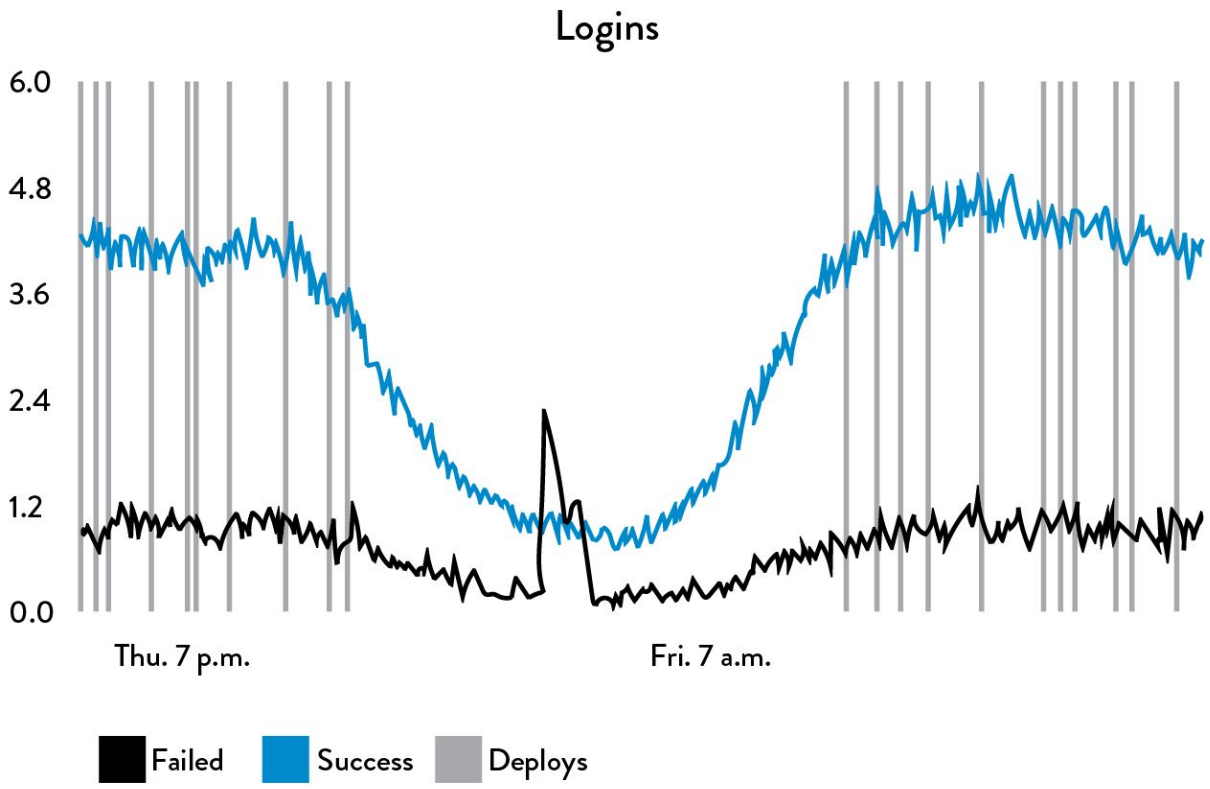
Low Risk releases - Bringing it together



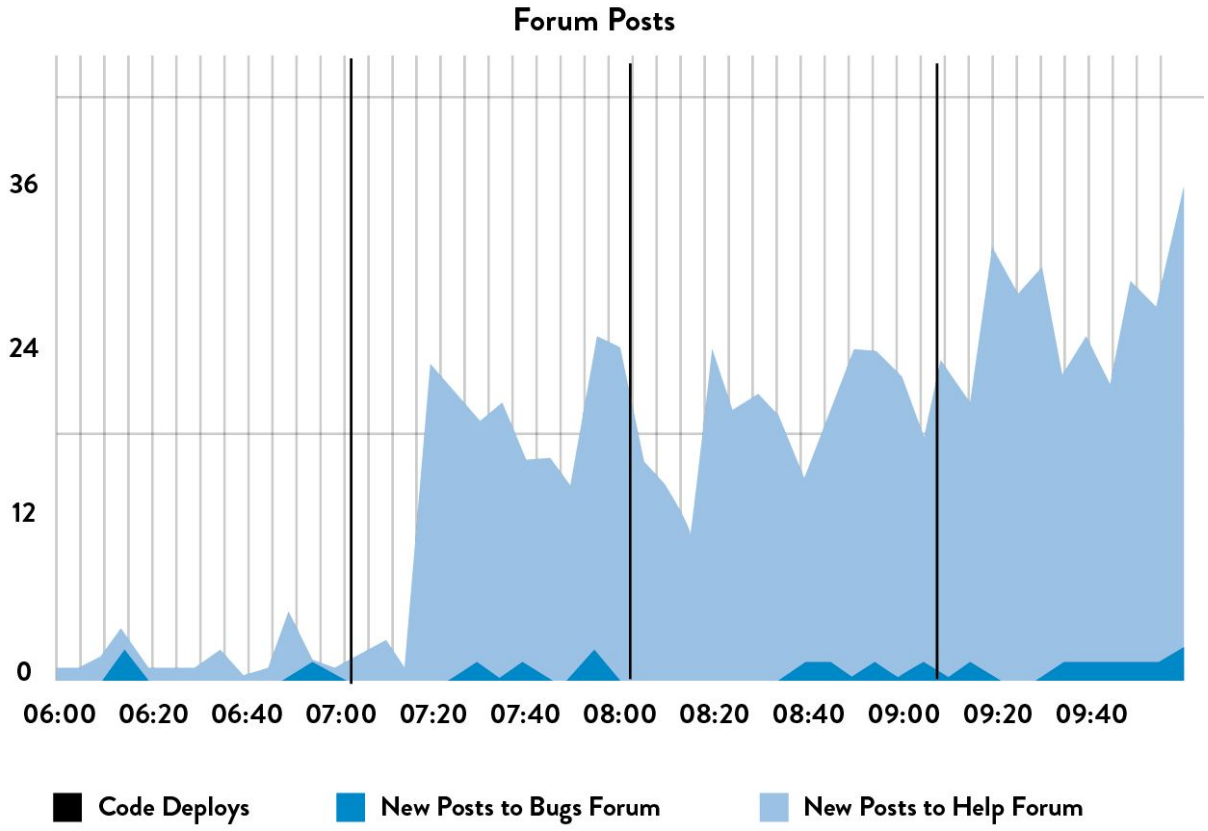
Low Risk releases - Bringing it together



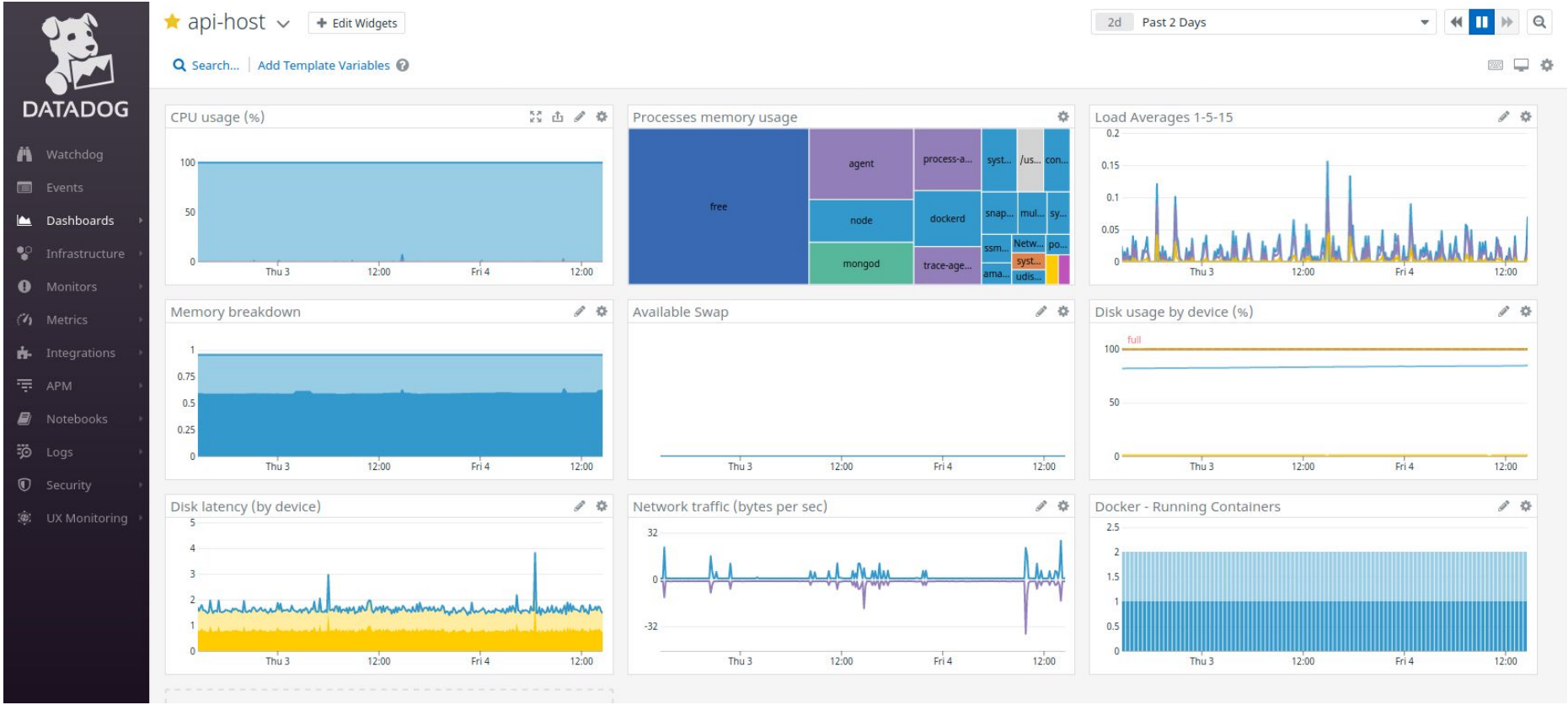
Low Risk releases - Bringing it together



Low Risk releases - Bringing it together



Recap


DATADOG
Watchdog
Events
Dashboards
Infrastructure
Monitors
Metrics
Integrations
APM
Notebooks
Logs
Security
UX Monitoring
api-host
Edit Widgets
Search...
Add Template Variables
2d
Past 2 Days
CPU usage (%)
Processes memory usage
free
agent
node
mongod
process-a...
dockerd
trace-age...
syst...
/us...
con...
snap...
mul...
sy...
ssm...
Netw...
po...
syst...
ama...
udis...
Load Averages 1-5-15
Memory breakdown
Available Swap
Disk usage by device (%)
full
Disk latency (by device)
Network traffic (bytes per sec)
Docker - Running Containers
Thu 3
12:00
Fri 4

PLURALSIGHT

Title: **Continuous Monitoring: The Big Picture**

Big picture overview of Monitoring in the DevOps story. [45mins]

Title: **Centralized Logging with the Elastic Stack**

Introduction to the ELK stack. [2h21mins]

Assignments?

No assignments!

HOGESCHOOL PXL