

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

Wat is monitoren?



Dictionary

Search for a word



monitor

/ˈmɒnɪtər/

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).

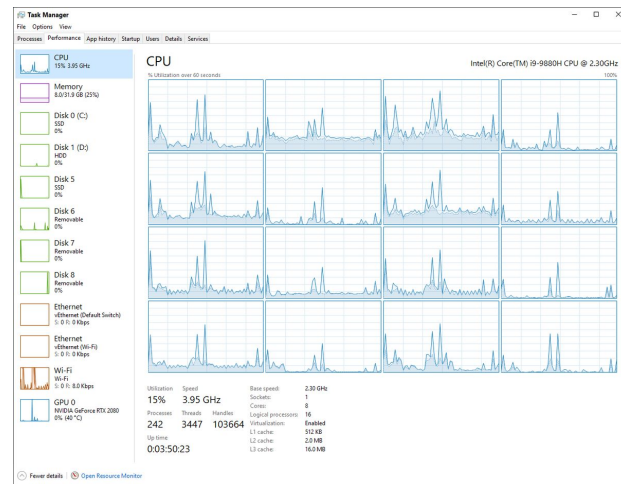
"listening devices were used to monitor conversations"

Definitions from Oxford Languages

Feedback



Translations and more definitions



The screenshot shows the Windows Task Manager window with the 'View' tab selected. A context menu is open over the 'View' tab, showing options: 'Refresh now', 'Update speed', 'Group by type' (checked), 'Expand all', and 'Collapse all'. The main window displays a list of running applications. The first application is Google Chrome (20), which is expanded to show 20 instances. The table below shows the resource usage for these instances.

Name	Status	CPU	Memory	Disk	Network
Apps (11)					
Google Chrome (20)		2.4%	1,259.5 MB	0.1 MB/s	0 Mbps
Google Chrome		0%	0.1 MB	0 MB/s	0 Mbps
Google Chrome		0%	63.1 MB	0 MB/s	0 Mbps
Google Chrome		0%	7.0 MB	0 MB/s	0 Mbps
Google Chrome		0%	38.1 MB	0 MB/s	0 Mbps
Google Chrome		0%	1.8 MB	0.1 MB/s	0 Mbps
Google Chrome		0%	6.4 MB	0 MB/s	0 Mbps

Metrics

Metrics? -> Meet punten


Dingen zoals:


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


Maar ook:

- Programma logging
- Netwerk logging
- ...

Dictionary







metric¹
/'metrik/

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

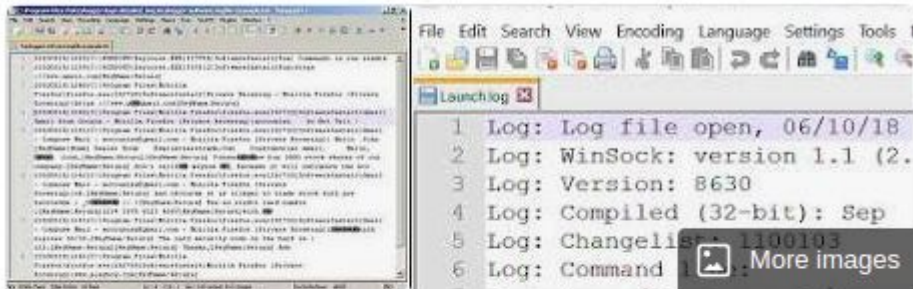
Log files

- /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:e5dff8b8ef24336f | (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:e5dff8b8ef24336f | (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:e5dff8b8ef24336f | (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  
rmer="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  
rmer="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  
rmer="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  
rmer="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  
rmer="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined"  
name="snap.lxd.daemon" pid=53442 comm="apparmor_parser"
```



Logfile

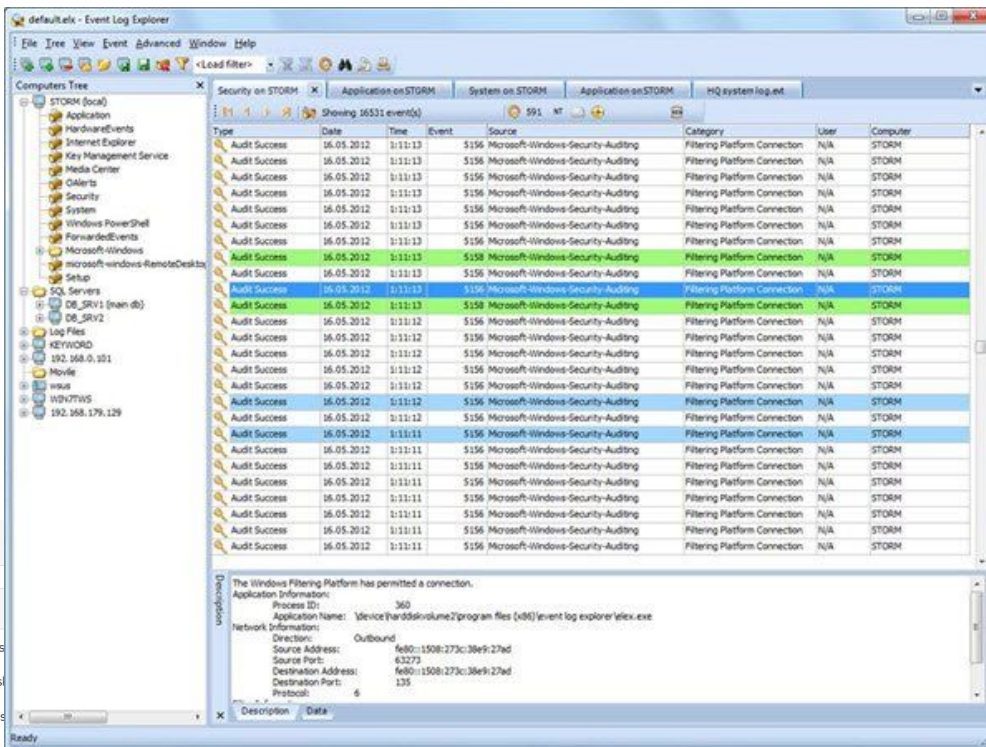
Software type

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



December 4, 2020 ▾

Severity ▾ Everything ▾

Service ▾ kernel ▾

December 2, 2020

```
8:54 AM audit: type=1400 audit(1606895669.238:112): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.230:111): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.226:110): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.222:109): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.218:108): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.214:107): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.210:106): apparmor="STATUS" operation="profile_replace" info="same as current profile, skipping" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.206:105): apparmor="STATUS" operation="profile_replace" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c... pid=53434...
8:54 AM audit: type=1400 audit(1606895669.066:104): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
8:54 AM audit: type=1400 audit(1606895669.066:103): apparmor="STATUS" operation="profile_load" profile="unconfined" name="/snap/core/10444/usr/lib/snapd/snap-c...
```

December 1, 2020

Local logs

COCKPIT

pete

System

Logs

Storage

Networking

Containers

Virtual Machines

Accounts

Services

KiB/s Reading

MiB/s Writing

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

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

Webmin Dashboard

CPU 72%

REAL MEMORY 30%

VIRTUAL MEMORY 0%

LOCAL DISK SPACE 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

1.803

Authentic Theme 13.02

Friday, June 24, 2016 5:39 PM

Linux 3.13.0-43-generic on x86_64

Intel(R) Xeon(R) CPU E5-2630L v2 @ 2.40GHz; 2 cores

3 days, 22 hours, 14 minutes

107

0.03 (1 min) 0.11 (5 mins) 0.13 (15 mins)

1.91 GB total / 602.75 MB used

1000 MB total / 2.42 MB used

39.25 GB total / 7.99 GB free / 31.56 GB used

19 package updates are available

webmin

Recent Webmin logins

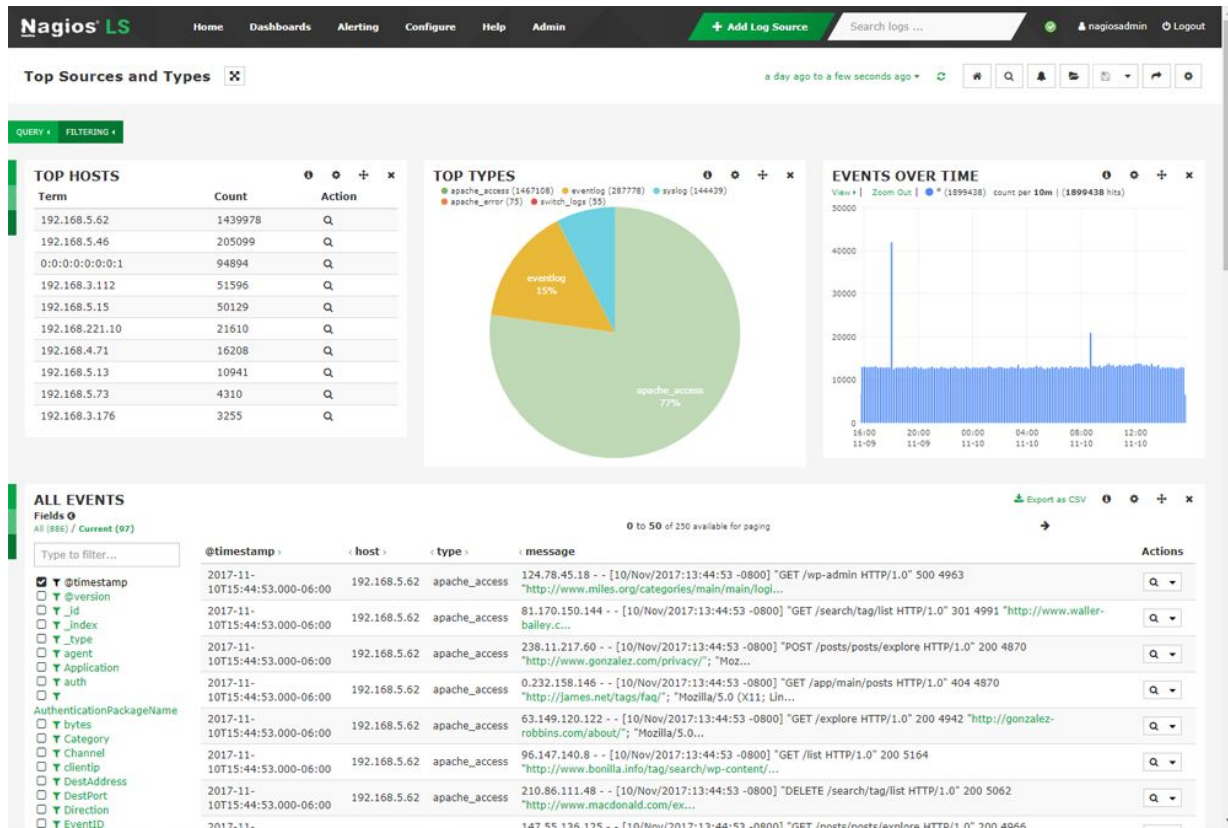
Log aggregatie



Hoe bekijken?

- ELK Stack
 - Graylog
 - Nagios Log server
 - Splunk

splunk>



Monitoring History

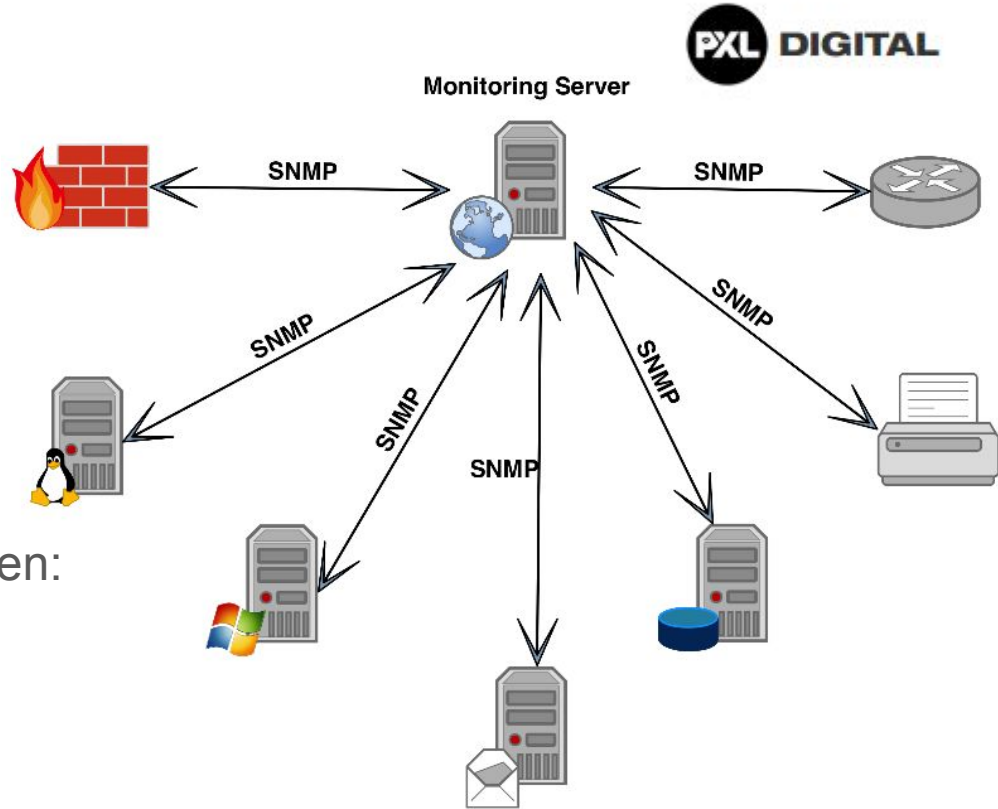
Van hardware monitoring tot AI-Ops.

Waar het begon ->

Simple **N**etwork **M**onitoring **P**rotocol
Est. 1988

Elk apparaat/software kon MiBs hebben:

Management information **B**ase file:
Definieert metrics



Monitoring History



Van hardware monitoring tot AI-Ops.

Waar het begon ->

Simple Network Monitoring Protocol
Est. 1988

Elk apparaat/software kon MiBs hebben:

Management information Base file:
Definieert metrics

```
1 BRIDGE-MIB
  > dot1d base
  > dot1d base port: #[1.3.6.1.2.1.17.1.4.1.1]
2 dot1d static: #[1.3.6.1.2.1.17.5.1.1.1]
  ...dot1d static address: #[1.3.6.1.2.1.17.5.1.1.2]
  ...dot1d static allowed to go to: #[1.3.6.1.2.1.17.5.1.1.2]
  ...dot1d static receive port: #[1.3.6.1.2.1.17.5.1.1.2]
  ...dot1d static status: #[1.3.6.1.2.1.17.5.1.1.2]
  > dot1d stp
  > dot1d stp port: #[1.3.6.1.2.1.17.2.15.1.1]
3 dot1d tp
  ...dot1d tp aging time
  ...dot1d tp learned entry discards
  > dot1d tp fdb: #[1.3.6.1.2.1.17.4.3.1.1]
  > dot1d tp port: #[1.3.6.1.2.1.17.4.4.1.1]
```

Monitoring Tools

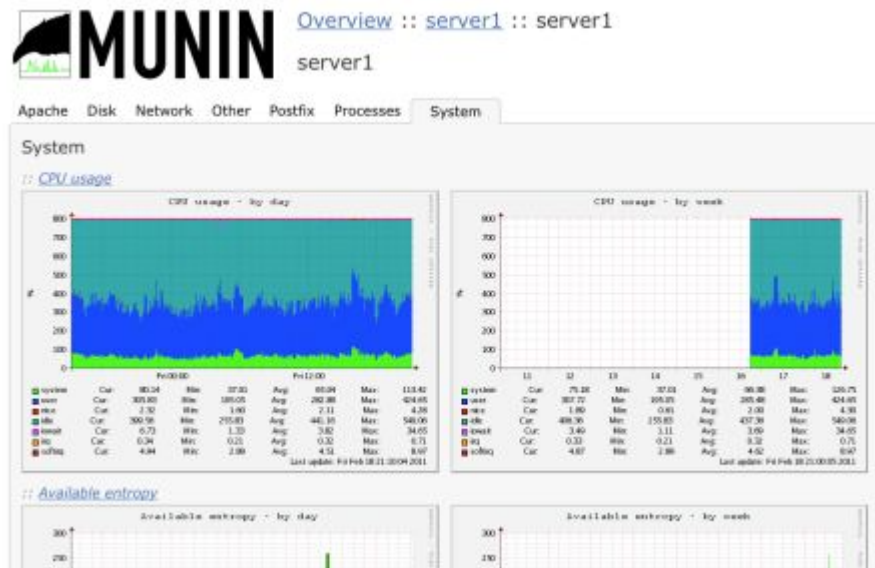


Eerste tools aggregeerde enkel (SNMP) data en toonde die

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

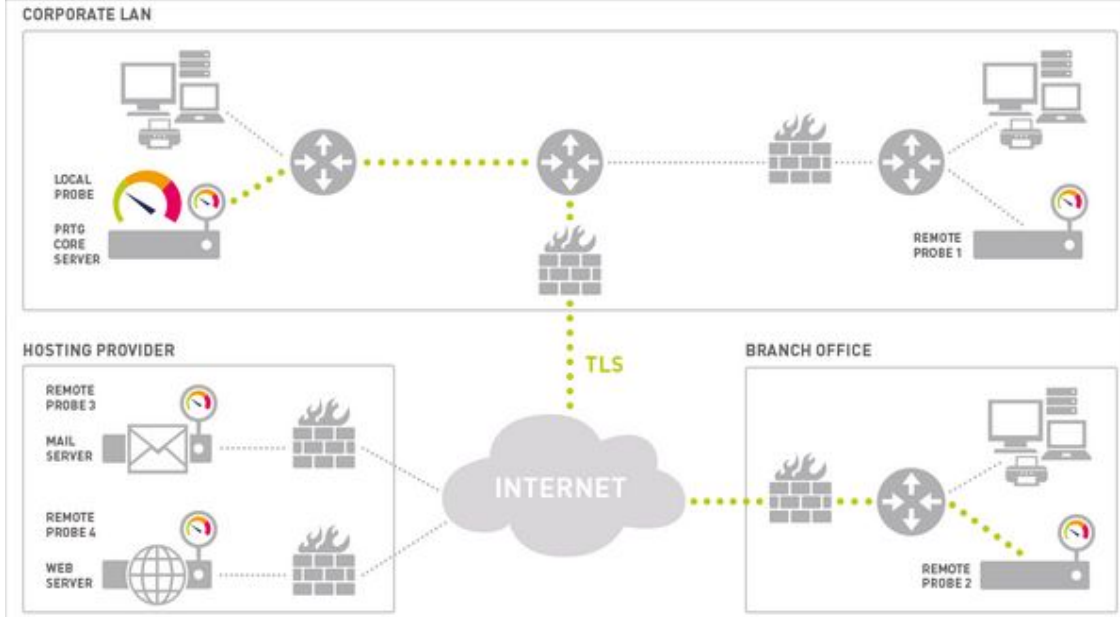
Voorbeelden:

- PRTG (nu)
- Nagios
- Check_mk

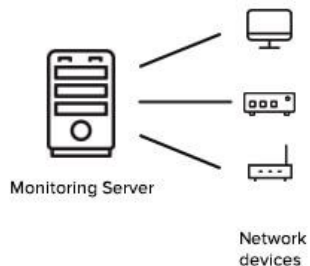


Monitoring Tools

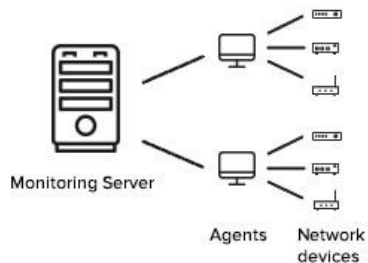
Om beter en diepgaander te kunnen monitoren:
Introductie **Agent** software



Agentless Network Monitoring



Agent-based Network Monitoring



Monitoring Tools



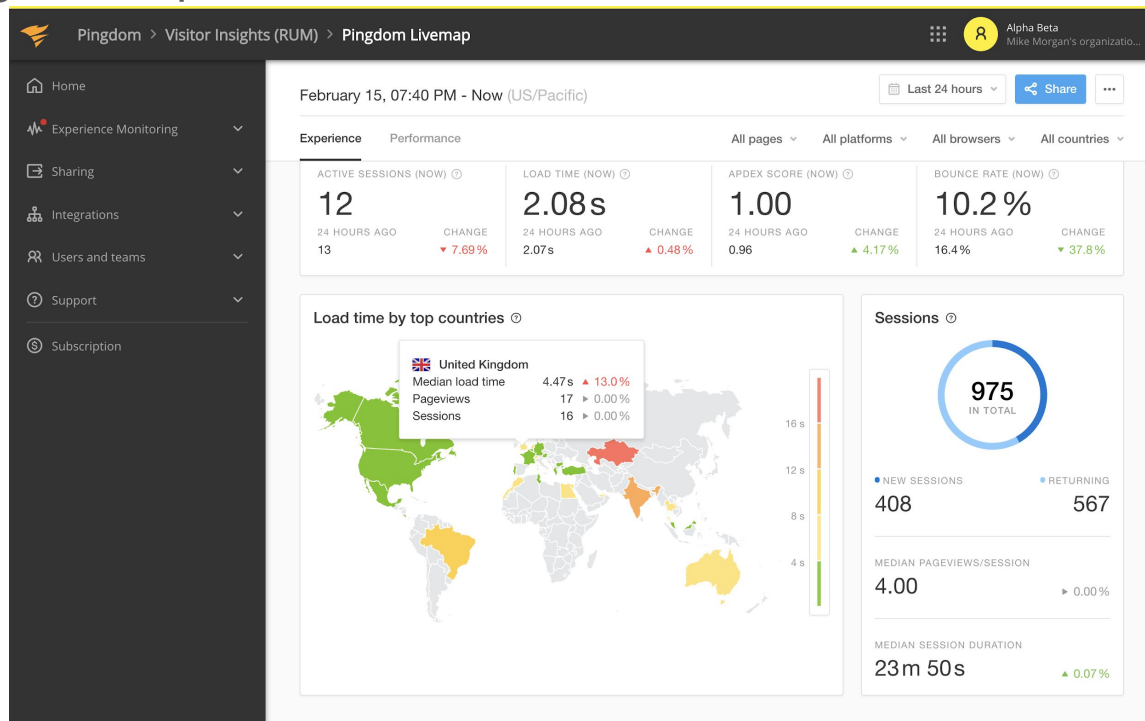
Volgende generatie ging meer op “internet” tools focussen en dus external monitoring doen

Voorbeelden:

- Pingdom
- Freshping
- Uptimebot

Overlap met testtools

Zoals Webpagetest.org

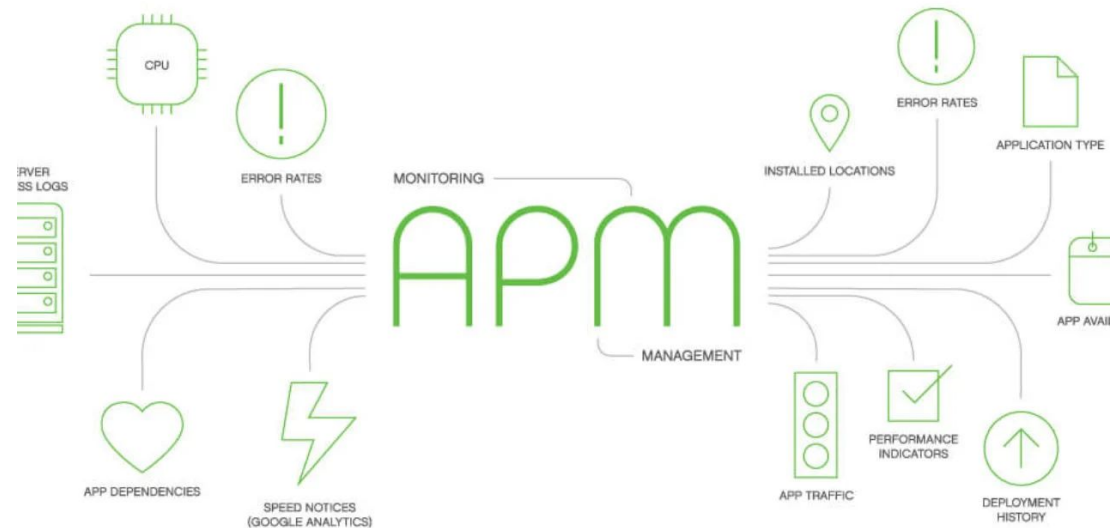


Monitoring Tools

APM is born!
Est +-2012

Mix van voorgaande met
Business Logic en predictive
/proactive monitoring

-Zabbix/Datadog/New Relic ...



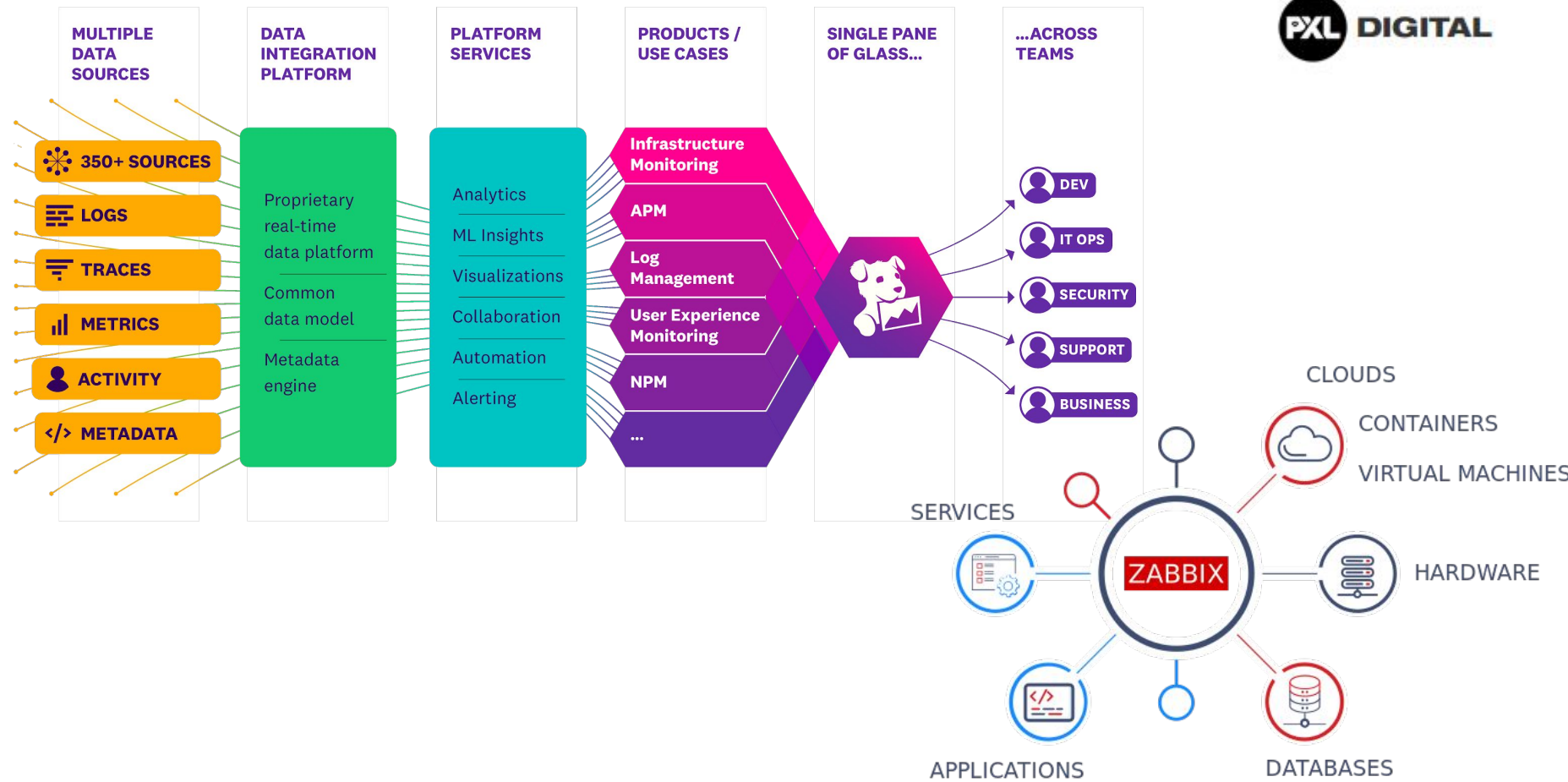
Application performance management

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](https://en.wikipedia.org/wiki/Application_performance_management)

Source:

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

Monitoring Tools

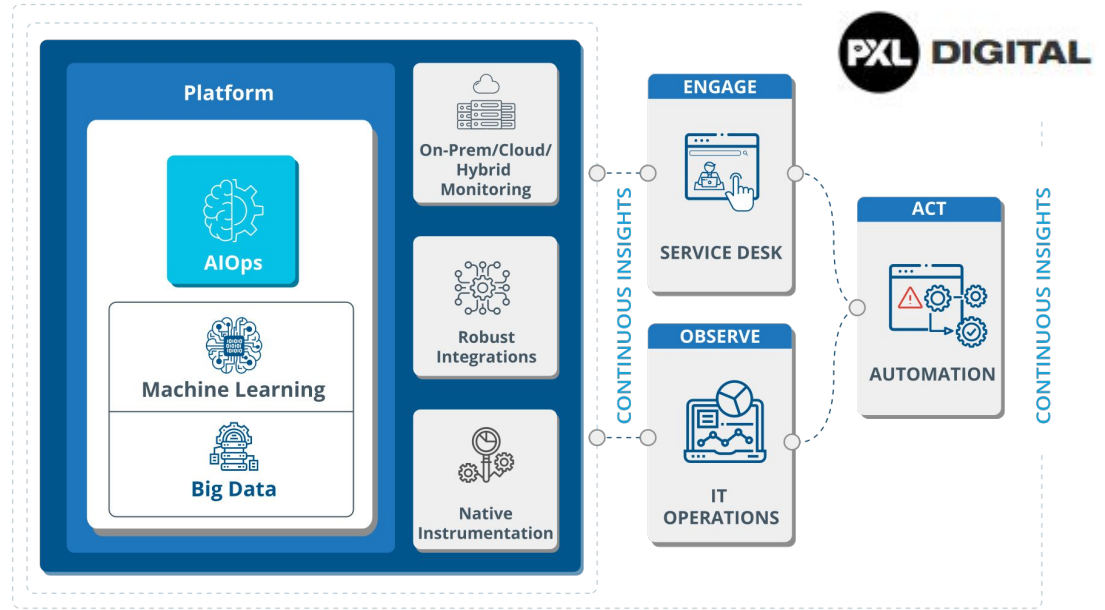


Monitoring Tools

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



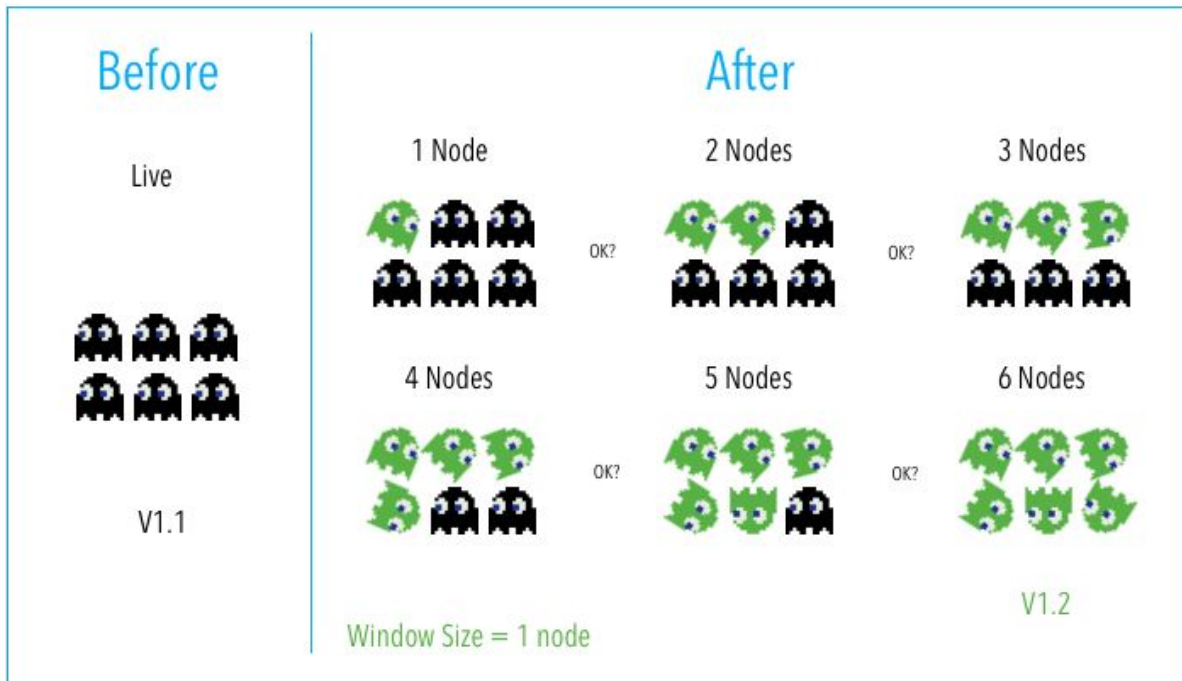
Low Risk releases - Bringing it together



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



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

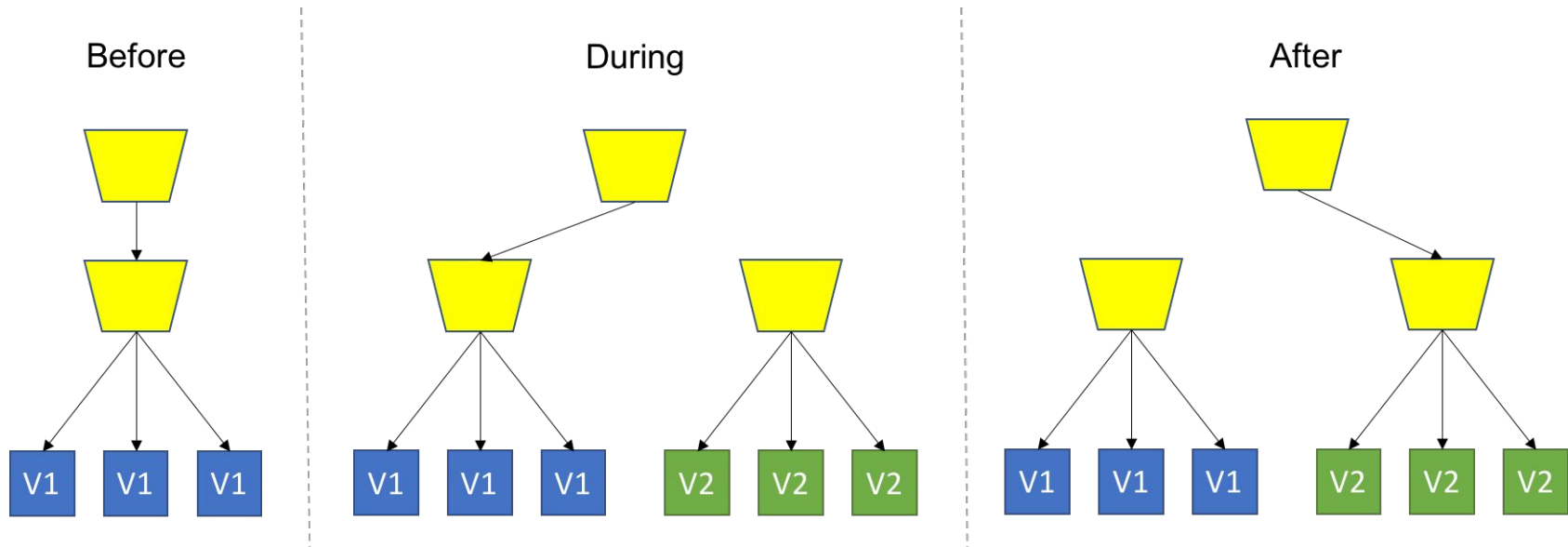
Testing as a Metric!



Low Risk releases - Bringing it together



Blue/Green deploys



Low Risk releases - Bringing it together



Testing as a Metric!

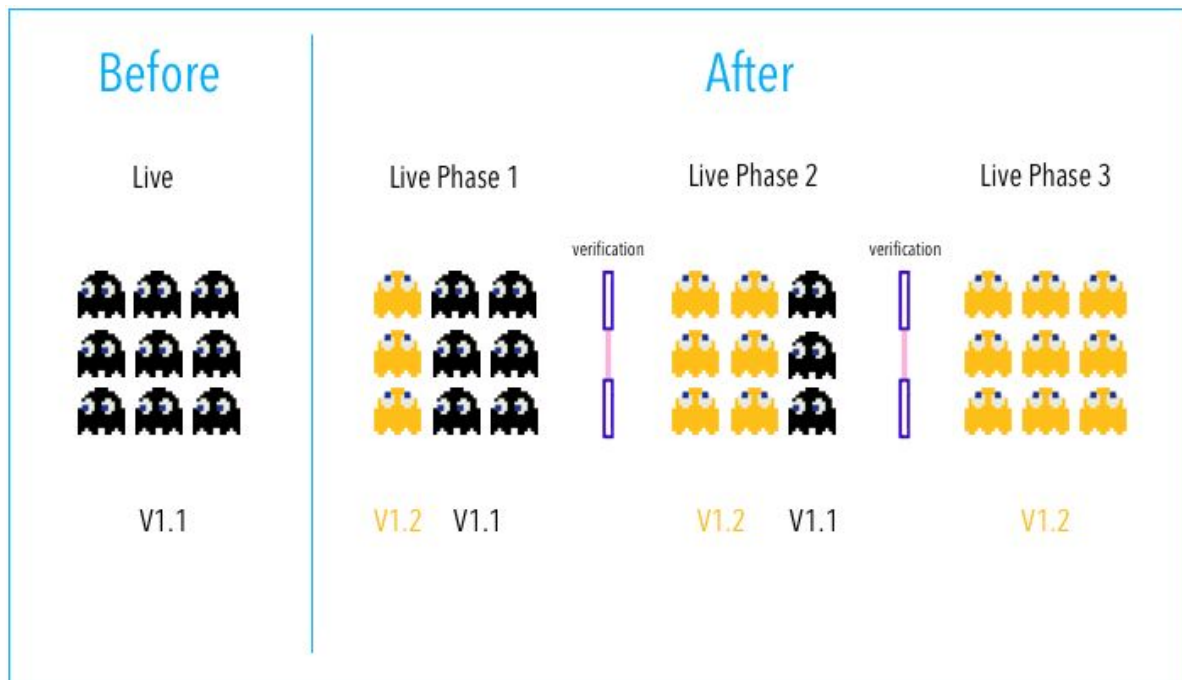
Canary deploys

Pros:

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

Cons:

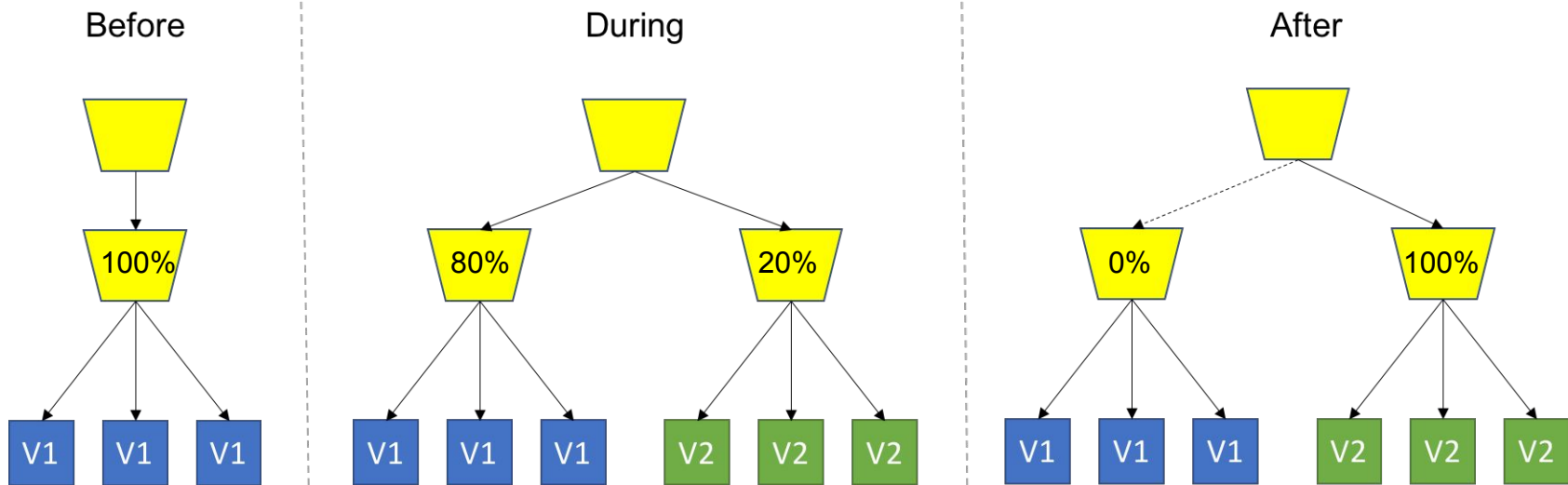
- Scripting canary deployments can be complex
- Required monitoring & instrumentation (APM, Log, Infra, End User, ...) for testing in production



Low Risk releases - Bringing it together



Canary deploys



Low Risk releases - Bringing it together



A/B Testing

Pros:

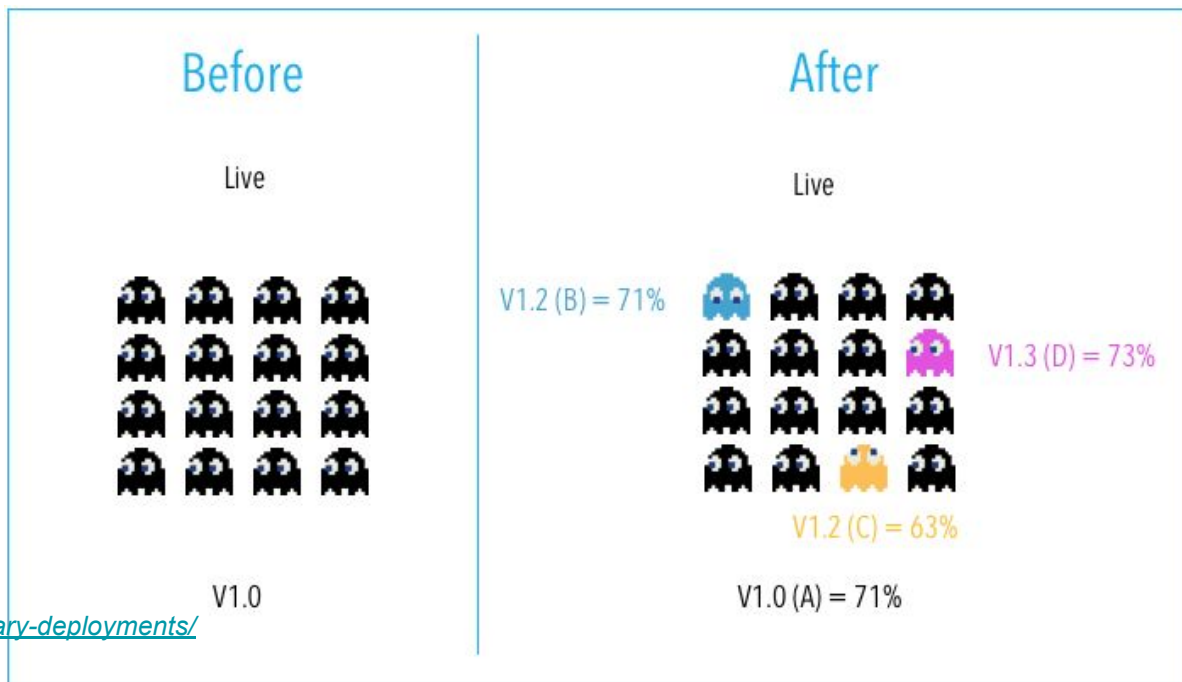
Fast, easy, and cheap way to test new features in production. Lots of tools exist to enable this.

Cons:

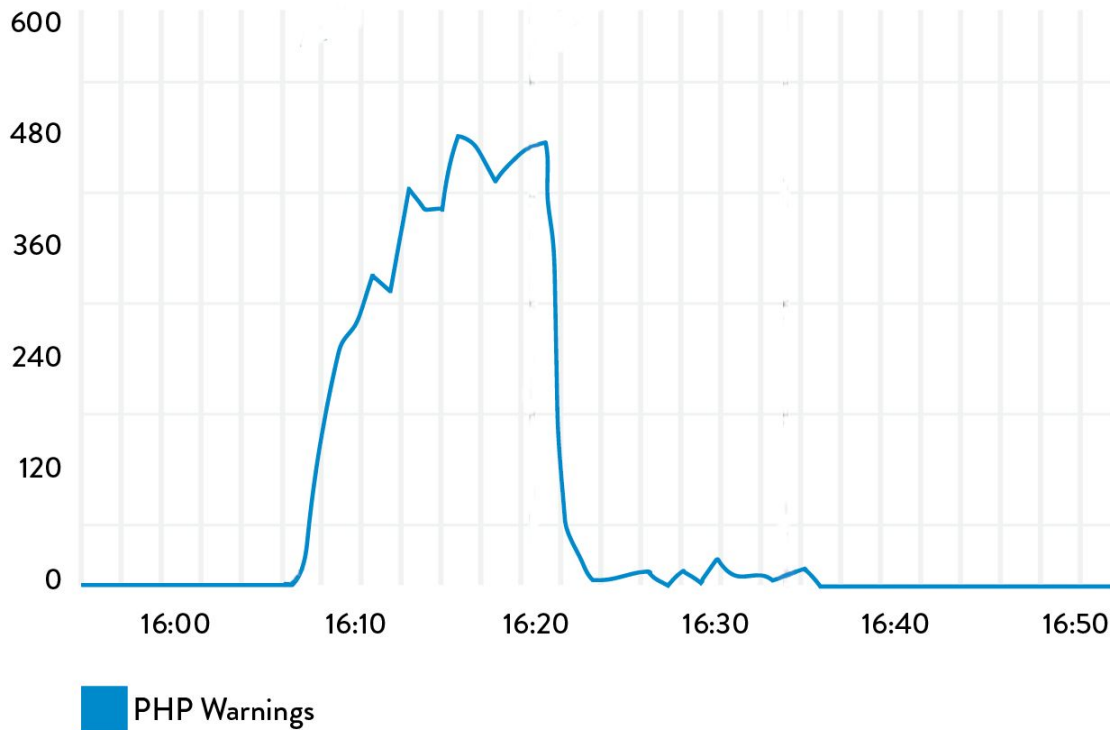
- Experiments can sometimes break the app/service/user experience.
- Scripting AB tests can be complex.
- Database compatibility (schema changes, backward compatibility)

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

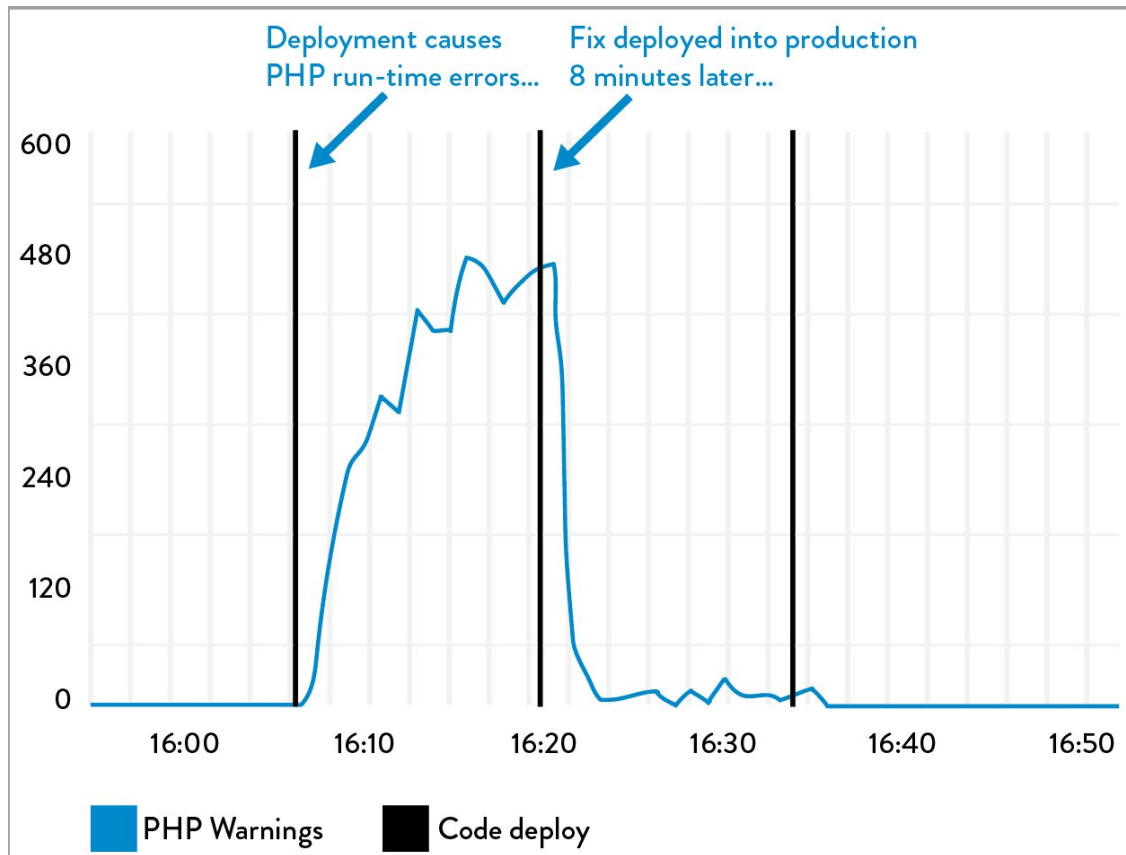
Testing as a Metric!



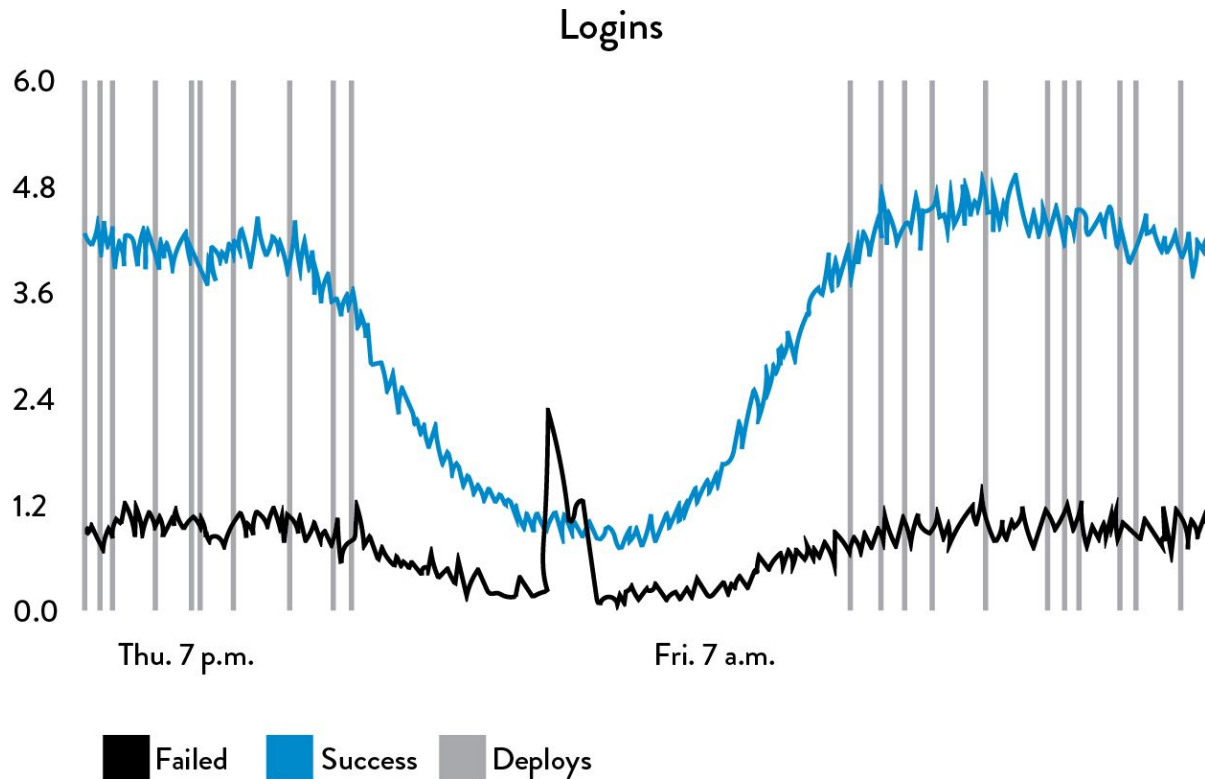
Low Risk releases - Bringing it together



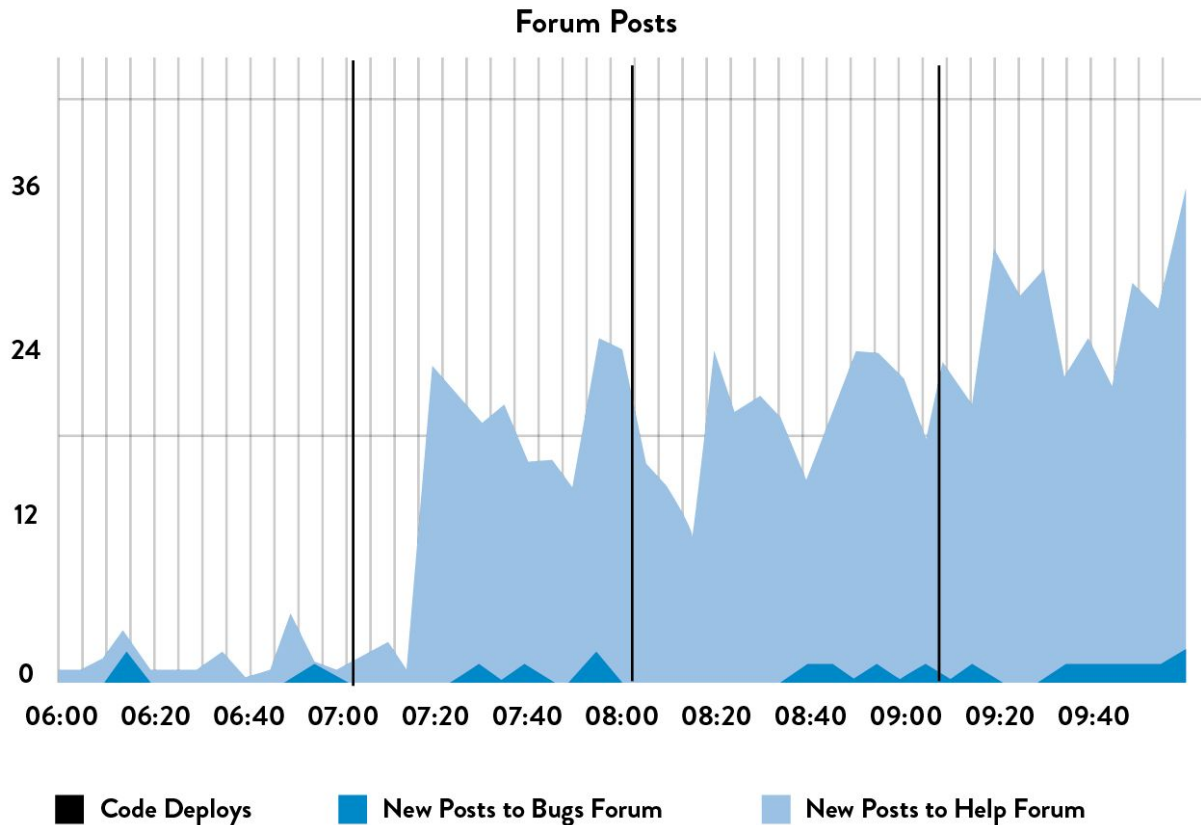
Low Risk releases - Bringing it together



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 ▾

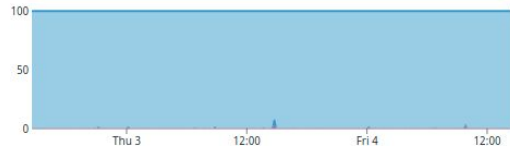
+ Edit Widgets

🔍 Search... | Add Template Variables ?

2d Past 2 Days



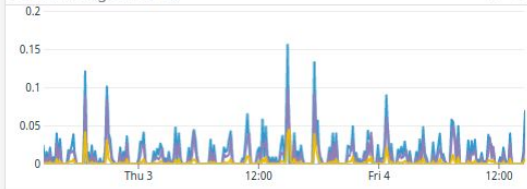
CPU usage (%)



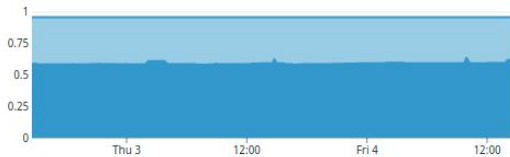
Processes memory usage



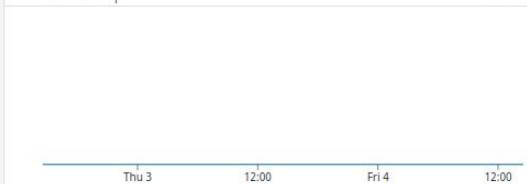
Load Averages 1-5-15



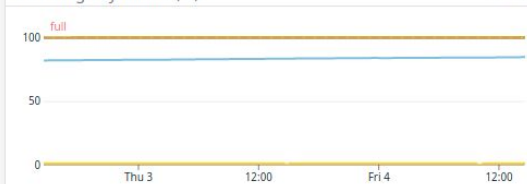
Memory breakdown



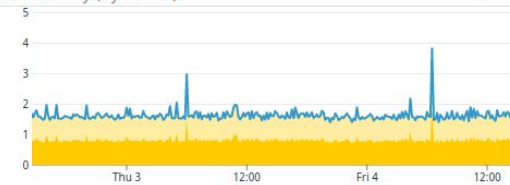
Available Swap



Disk usage by device (%)



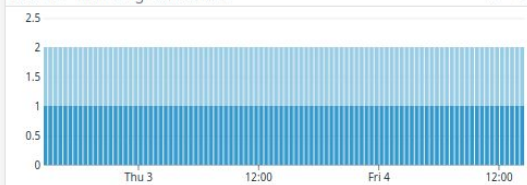
Disk latency (by device)



Network traffic (bytes per sec)



Docker - Running Containers





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!

