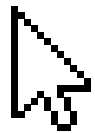
Monitorització d'aplicacions i serveis web

ASW - 12D



Sergi Casaú | Berta Fitó | Arnau Giménez | Marc Heras

01 Què és i per què és important?

Per què necessitem monitoritzar els nostres serveis web?

02 Com podem monitoritzar?

Quines eines podem fer servir per a la monitorització?

03 Nivells de Monitorització

Un cop tenim les eines, com podem definir què controlem?

04 Beneficis i Inconvenients

Té inconvenients? Quins? Com es relacionen amb els beneficis?

05 Conclusions

Cloenda, bibliografia i organització.

El servidor ha caigut???

01

Què és i per què és important?

Per què necessitem monitoritzar els nostres serveis web?

“La monitorització és el procés de testejar i verificar que l‘usuari final pot interactuar amb el producte tal i com s’esperaria.”

Tipus de monitorització

Interna

Detecta problemes interns de l'app

Externa

Detecta problemes fora del servidor

Objectiu

Maximitzar la disponibilitat i oferir als usuaris la millor experiència possible.

Què es monitoritza?

Seguretat

Busca vulneracions i vulnerabilitats.

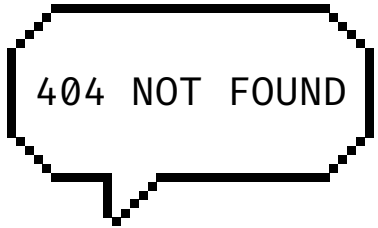
Rendiment

Inclou disponibilitat, detecció de bugs, eficiència i temps de resposta.

Funcionalitat

Observar components, proveir alertes i *dashboards*, detecció d'anomalies, rastreig distribuit, dependència i *flow mapping*.

02

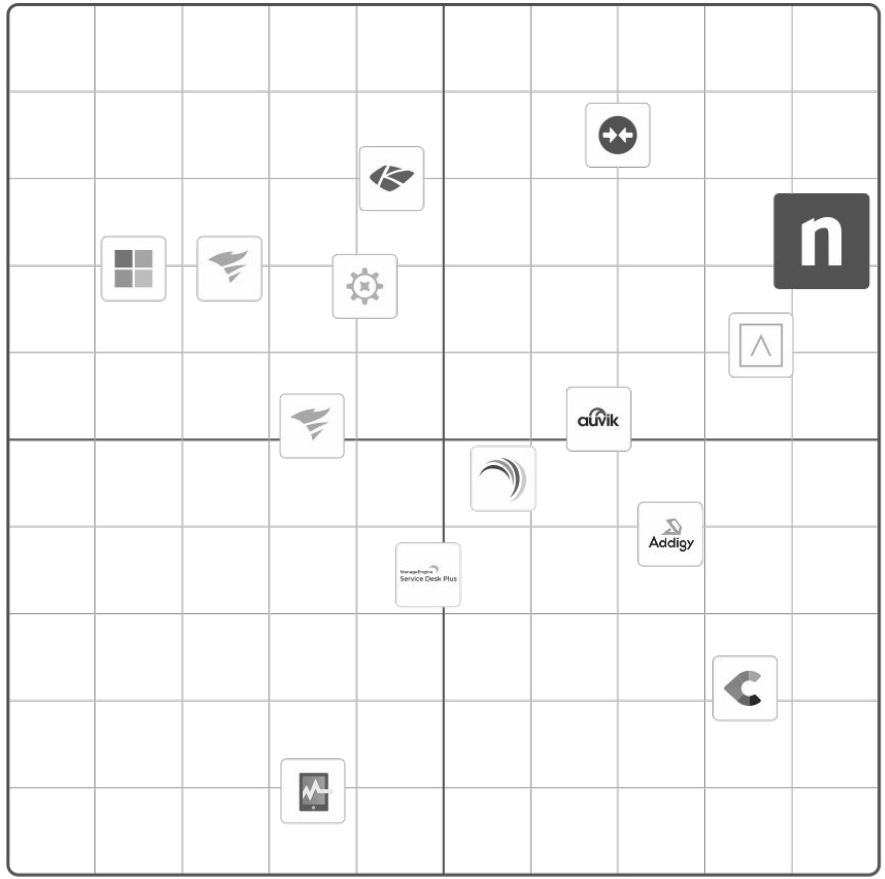


Com podem monitoritzar?

Quines eines podem fer servir per a la monitorització?

Eines

- Existeixen diverses eines dedicades a la monitorització d'aplicacions i serveis web.
- Ofereixen diferents nivells de complexitat.
- No analitzen codi com *SonarQube*.
- Creen mètriques, gràfics, taules, etc.



Exemples d'Eines

NinjaOne

Rendiment en directe amb generació d'alertes i automatització

ClickCease

Eina de prevenció de *clicks* i anuncis fraudulents

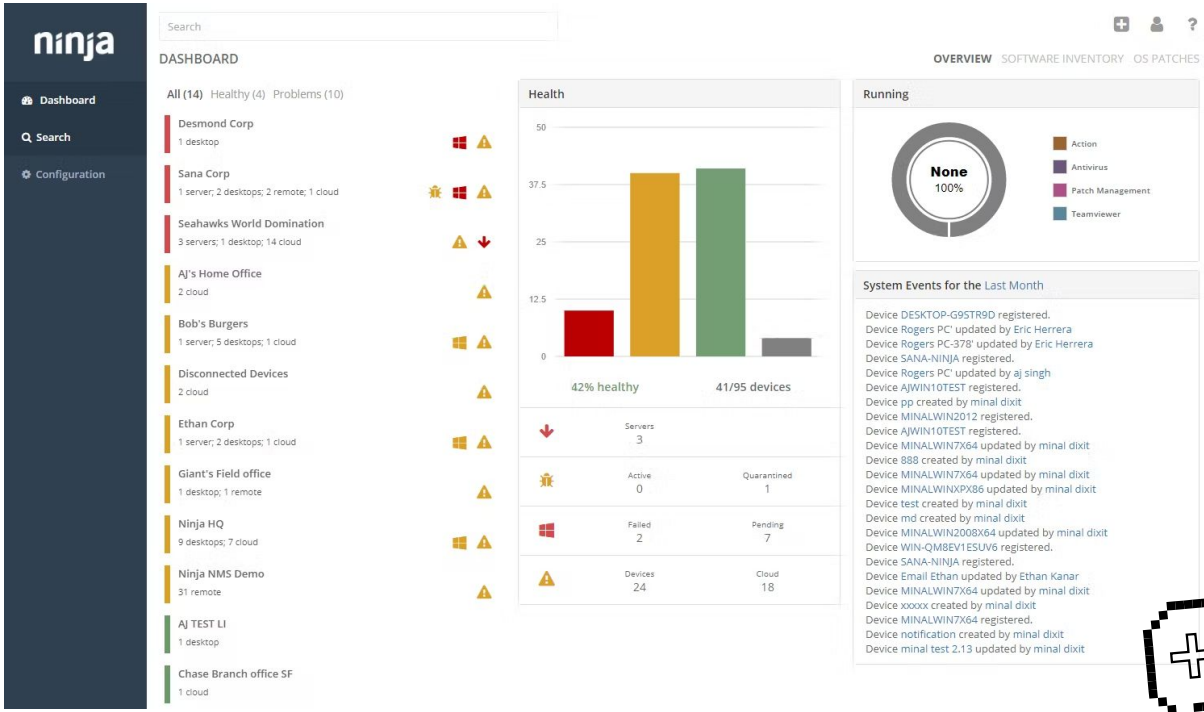
SolarWinds

Monitorització completa i mesures de seguretat avançades

Datadog

Proveeix coneixement en directe del rendiment del web

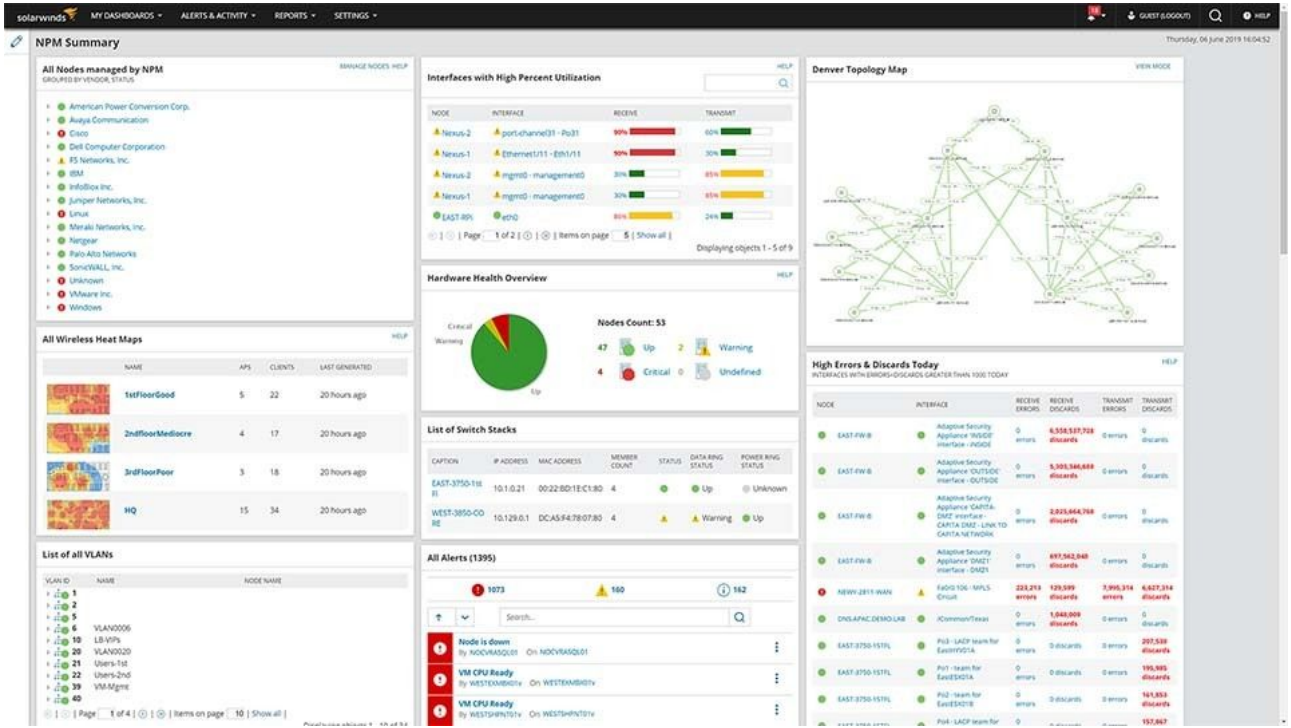
NinjaOne


ninja
Search
Dashboard
Search
Configuration
DASHBOARD
OVERVIEW SOFTWARE INVENTORY OS PATCHES
All (14) Healthy (4) Problems (10)
Desmond Corp
1 desktop
Sana Corp
1 server; 2 desktops; 2 remote; 1 cloud
Seahawks World Domination
3 servers; 1 desktop; 14 cloud
AJ's Home Office
2 cloud
Bob's Burgers
1 server; 5 desktops; 1 cloud
Disconnected Devices
2 cloud
Ethan Corp
1 server; 2 desktops; 1 cloud
Giant's Field office
1 desktop; 1 remote
Ninja HQ
9 desktops; 7 cloud
Ninja NMS Demo
31 remote
AJ TEST LI
1 desktop
Chase Branch office SF
1 cloud
Health
50
37.5
25
12.5
0
42% healthy
41/95 devices
Servers 3
Active 0
Quarantined 1
Failed 2
Pending 7
Devices 24
Cloud 18
Running
None
100%
Action
Antivirus
Patch Management
Teamviewer
System Events for the Last Month
Device DESKTOP-G9STR9D registered.
Device Rogers PC' updated by Eric Herrera
Device Rogers PC-378' updated by Eric Herrera
Device SANA-NINJA registered.
Device Rogers PC' updated by aj singh
Device AJWIN10TEST registered.
Device pp created by minal dixit
Device MINALWIN2012 registered.
Device AJWIN10TEST registered.
Device MINALWIN7X64 updated by minal dixit
Device 888 created by minal dixit
Device MINALWIN7X64 updated by minal dixit
Device MINALWINXPX86 updated by minal dixit
Device test created by minal dixit
Device md created by minal dixit
Device MINALWIN2008X64 updated by minal dixit
Device WIN-QM8EV1ESUV6 registered.
Device SANA-NINJA registered.
Device Email Ethan updated by Ethan Kanar
Device MINALWIN7X64 updated by minal dixit
Device xxxxx created by minal dixit
Device MINALWIN7X64 registered.
Device notification created by minal dixit
Device minal test 2.13 updated by minal dixit

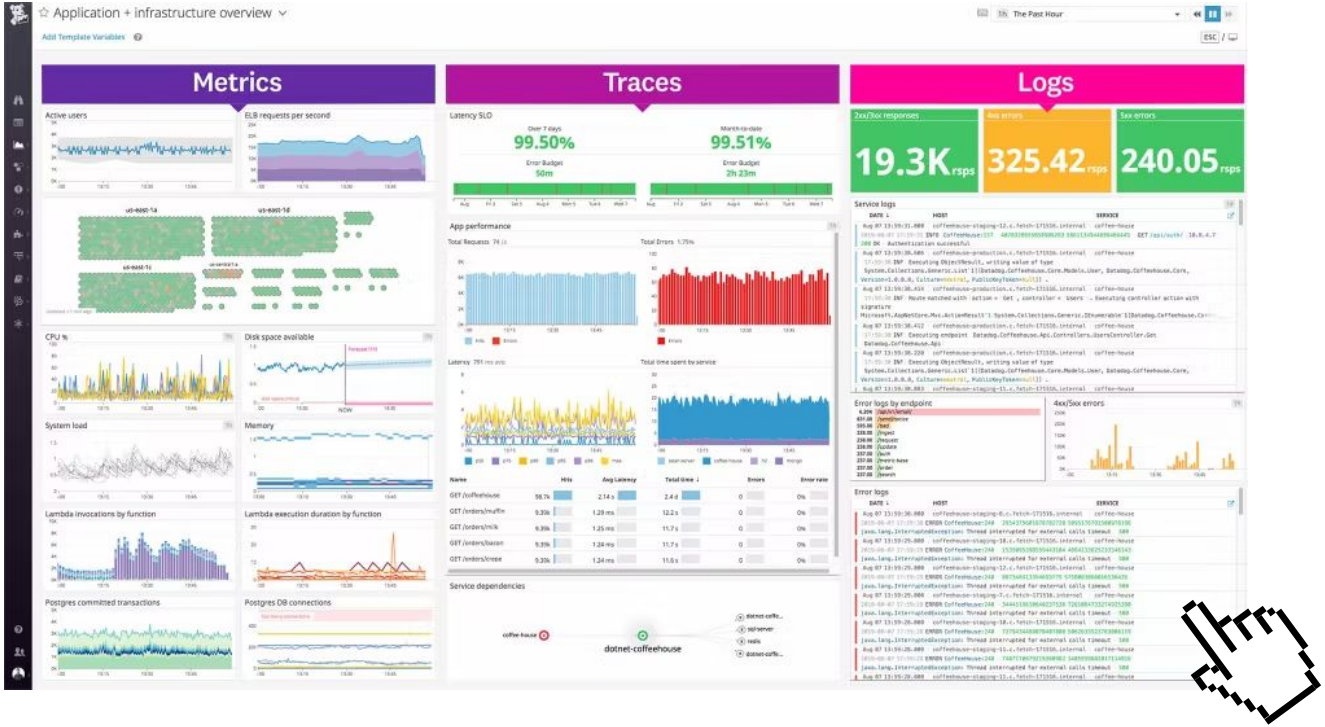
ClickCease

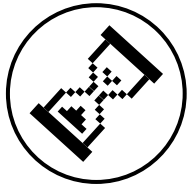

Visitors and Click Analytics
Ad Clicks
6,216
Blocked IPs
2,140
Unique Visitors
5,632
Clicks Per Visitor
1.1
Daily
Hourly
Traffic
Blocked IPs
Blocked IPs
Ad Clicks
Visitors from Ads
Who's Clicking
Genuine Leads
66%
Competitors
1%
Bots
33%
Fraud by Device
Mobile
70%
6%
Desktop
19%
6%

SolarWinds


solarwinds
MY DASHBOARDS
ALERTS & ACTIVITY
REPORTS
SETTINGS
NPM Summary
All Nodes managed by NPM
Interfaces with High Percent Utilization
Denver Topology Map
Hardware Health Overview
Nodes Count: 53
All Wireless Heat Maps
List of Switch Stacks
High Errors & Discards Today
List of all VLANs
All Alerts (1395)

Datadog


Application + infrastructure overview
Add Template Variables
The Past Hour
Metrics
Traces
Logs
Active users
ELB requests per second
CPU %
Disk space available
System load
Memory
Lambda invocations by function
Lambda execution duration by function
Postgres committed transactions
Postgres DB connections
Latency SLO
99.50%
99.51%
App performance
Total Requests
Total Errors
Latency
Total time spent by service
Service dependencies
coffee-house
dotnet-coffeehouse
2xx/3xx responses
19.3K rsps
4xx errors
325.42 rsps
5xx errors
240.05 rsps
Service logs
Error logs by endpoint
4xx/5xx errors
Error logs

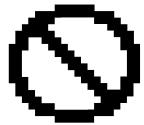


03

Nivells de Monitorització

Un cop tenim les eines, com podem definir què controlem?

“No és necessari monitoritzar tota aplicació web de la mateixa manera.”



Nivells

1

Uptime

Disponibilitat d'una pàgina crítica

2

Transacció

Disponibilitat d'un procés crític

3

Rendiment

Rendiment d'una pàgina crítica

4

Sintètica

Rendiment d'un procés crític

5

Customer Journey

Tots els nivells anteriors i informació de seguretat

04

Beneficis i Inconvenients

Té inconvenients? Quins? Com es relacionen amb els beneficis?

Contrastació

Beneficis

- Coneixement del comportament del nostre sistema
- Detecció d'intrusions
- Permet escalar adequadament el sistema

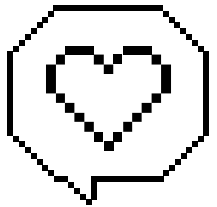
Inconvenients

- Major consum de recursos
- Necessitat de revisar els *logs*
- Realitzar accions no desitjades

05

Conclusions

Cloenda, bibliografia i organització.



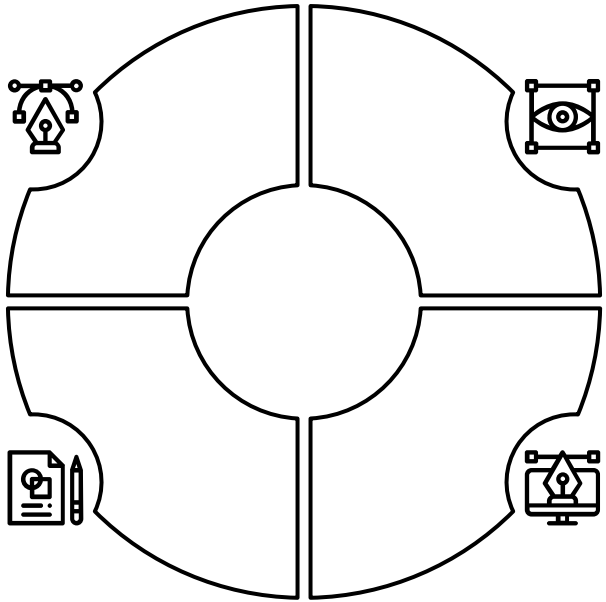
Conclusió

Seguretat

Les eines han de poder proveir una certa protecció.

Funcionalitat

Les eines haurien d'ajudar a mantenir i millorar el sistema.



Alertes

Les alertes haurien de ser a temps real i informades.

Rendiment

Les eines haurien de ser capaces de trobar els detractors de rendiment amb precisió.

“La monitorització és una eina molt valuosa pels desenvolupadors: permet assegurar la protecció i el bon funcionament dels seus productes.”

—La nostra opinió

Recursos

Pàgines web

- https://www.crowdstrike.com/cybersecurity-101/observability/application-monitoring/
- https://www.paessler.com/web-service-monitoring
- https://en.wikipedia.org/wiki/Website_monitoring
- https://www.ninjaone.com/
- https://www.solarwinds.com/
- https://www.datadoghq.com
- https://en.wikipedia.org/wiki/Application_performance_management
- https://en.wikipedia.org/wiki/Synthetic_monitoring
- https://en.wikipedia.org/wiki/Passive_monitoring
- https://pandorafms.com/blog/es/herramientas-de-monitoreo-de-redes/
- https://www.crowdstrike.com/cybersecurity-101/observability/log-management/
- https://www.clickcease.com

Organització

	Sergi*	Berta	Arnau*	Marc
Secció 01	Diapositives	Informació i diapositives	*Seguretat* i diapositives	*Aspectes* i diapositives
Secció 02			*Eines*	Informació i diapositives
Secció 03		Informació i diapositives		Informació i diapositives
Secció 04	*Beneficis*	*Desafiaments*	*Desavantatges* i diapositives	
Secció 05		Diapositives		

* Presentadors