ESET Inspect on-prem server – Optimizacija i debug / trace logovi

Tema

Optimizacija ESET Inspecta.

Postavljanje ESET Inspect on-prem servera u debug / trace mode.

Prikupljanje logova.

Važno

ESET Inspect server može zapisati vrlo veliku količinu podataka u kratko vrijeme i “zagušiti” server na kojemu je baza podataka. Ovaj postupak koristite samo u kratkom periodu radi prikupljanja podataka za podršku.

Napravite disk-image backup i / ili puni snapshot.

Prije bilo koje promjene postavki zapišite trenutačno stanje kako biste ih mogli kasnije vratiti.

Optimizacija

Prvo provjerite jesu li serveri ESET Inspecta i baze podataka hardverski odgovarajući i optimizirani:

https://help.eset.com/ei_deploy/latest/en-US/hardware_requirements.html

https://help.eset.com/ei_deploy/latest/en-US/reduce_database_size.html

https://help.eset.com/ei_navigate/latest/en-US/?optimize_server.html

https://help.eset.com/ei_navigate/latest/en-US/optimize_server.html?performance_check.html

EIconnector performanse:
https://support.eset.com/en/kb8539-check-performance-in-eset-inspect-and-eset-inspect-on-prem

---

Debug/trace postupak

[1] Dashboard >> Events screenshot

Otvorite https://esetserver:4433/console/dashboard/events i napravite sliku ekrana (screenshot01.jpg)

[2] Dashboard >> Server screenshot

Otvorite https://esetserver:4433/console/dashboard/server i napravite sliku ekrana (screenshot02.jpg)

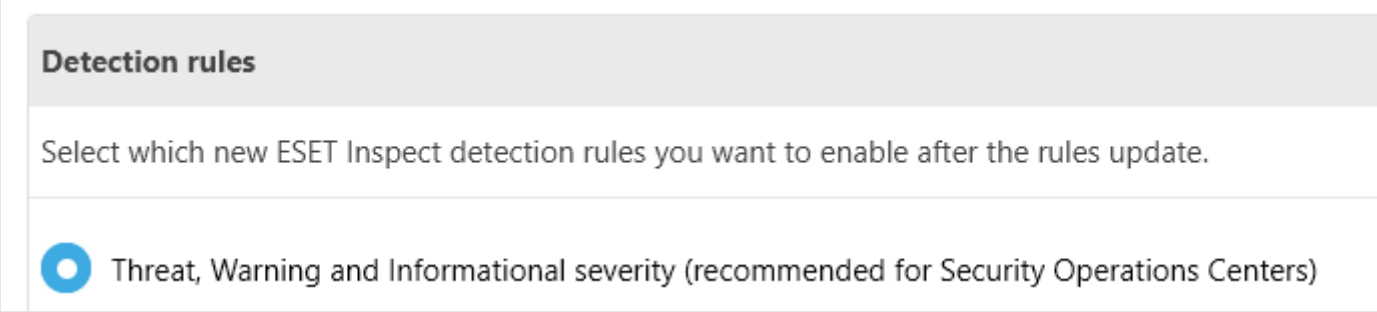
[3] More.. >> Settings

Otvorite https://esetserver:4433/console/settings >> Logging

i postavite “Trace log verbosity” na “Debug”

[4] Ako se radi o problemu s detekcijama..

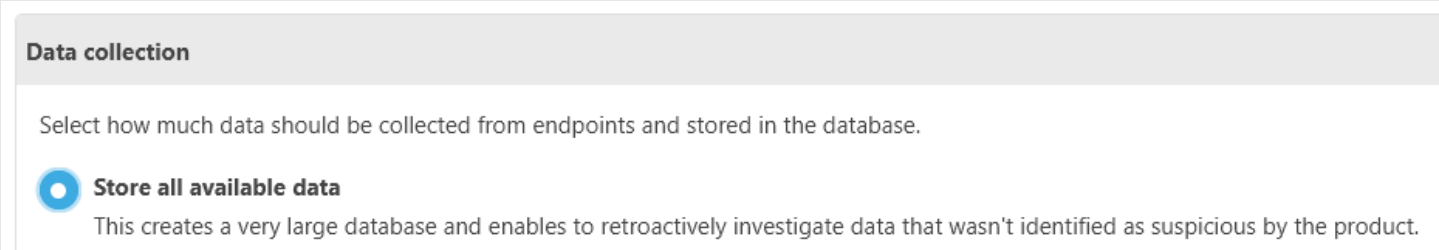
..uključite Detection rules >> Threat, warning and informational severity



[5] Ako se radi o problemu s detekcijama..

..uključite Data Collection >> Store all available data

(obratite pozornost na napomenu uz ovu stavku!)



[6] Pričekajte da se problem pojavi

..ili ga “isprovocirajte” ako je izvedivo.

[7] Ponovno napravite slike ekrana

../dashboard/server i ../dashboard/events (screenshot03.jpg i screenshot04.jpg)

Logovi

Nakon što se pojavi ili isprovocirate problem, prikupite:

[A] ELC logove sa servera na kojem je ESET Inspect server https://www.nod32.com.hr/podrska/kb8275

[B] sve slike ekrana

[C] disk IOPS sa servera na kojemu je database za ESET Inspect
https://help.eset.com/ei_deploy/https://www.nod32.com.hr/podrska/kb8275/en-US/hardware_requirements.html >> The disk IOPS

Nakon toga vratite postavke na početno stanje.

Napomena: zamijenite “esetserver” adresom svoga ESET Protect servera.

ESET Inspect esetinspect on-prem onprem eei eix debug trace mode xmode logging xESET xInspect xesetinspect xon-prem xonprem xeei xeix xdebug xtrace xlogging dnevnik xdnevnik