

EEALx ESET Endpoint Antivirus for Linux - Troubleshooting TrblSht

Tema

Priprema Linux računala za prikupljanje dijagnostičkih logova u slučaju kada sumnjate da Endpoint Security for Linux uzrokuje probleme u radu ili kad ne blokira nešto što bi trebao blokirati.

Postupak

- pripremite okolinu za replikaciju problema
 - postavite policy za Linux Endpoint prema sl.1
 - pripremite TCPdump naredbu:
 - `sudo tcpdump -i <%eth0%> -s 0 -w tcpdump.log`
(umjesto <%eth0%> stavite naziv mrežne kartice s 'problematicnog' LAN-a; za info o mrežnim karticama v. naredbe `ip -a i route`)
 - ako je u problem uključena dodatna aplikacija - uključite diagnostic / debug logove i u njoj
 - pokrenite TCPdump
 - zapišite točno vrijeme
 - pokrenite problematični postupak (npr. aplikaciju koja ne radi ako je neki modul ESET Securityja aktivan i sl.)
 - kad se pojavi pogreška, pričekajte desetak sekundi
 - ponovite problematični postupak
 - zaustavite TCPdump
 - isključite "Diagnostic records" (Sl.1) - vratite na "Informative records"
 - po potrebi isključite dijagnostičko zapisivanje u aplikaciji
-

Prikupljanje logova

v. <https://www.nod32.com.hr/podrska/kb8275>

Slanje logova

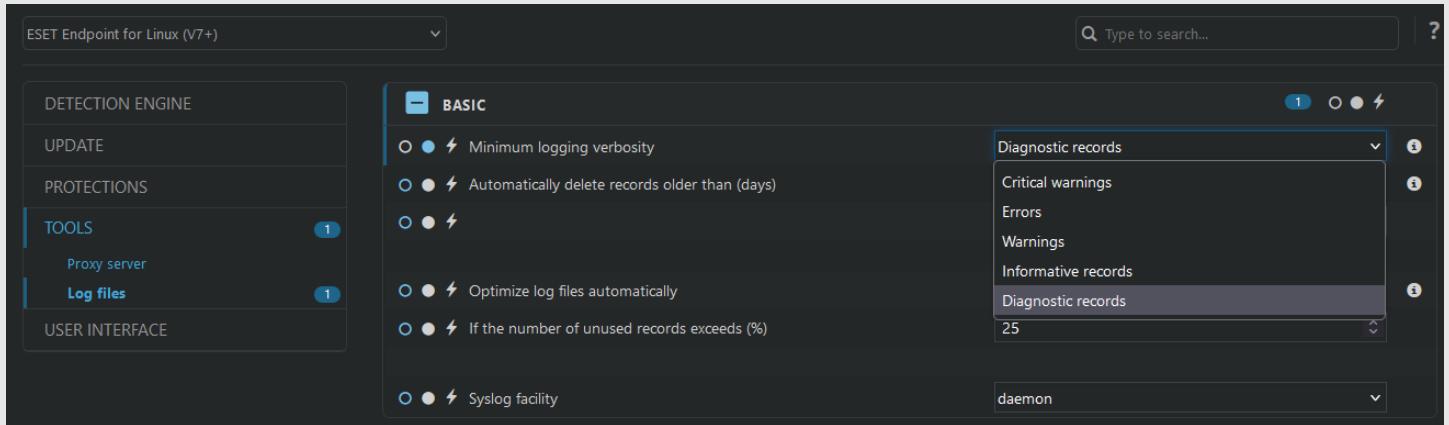
- sve datoteke spremite u arhivu (ZIP, 7z) s lozinkom i stavite na online disk (Microsoft OneDrive, DropBox, i sl.):
 1. `tcpdump.log`
 2. datoteku koju je kreirala skripta `collect_logs.sh`
 3. po potrebi i datoteku koju je kreirala skripta `info_get`

4. dijagnostičke logove "problematične" aplikacije

- pošaljite nam mailom link za preuzimanje
 - (!) obavezno u poruci navedite točno vrijeme pojave problema
-

Slike

Sl.1 "Minimum logging verbosity" = "Diagnostic records"



diagnostics dijagnostika xdiagnostics xdijagnostika troubleshooting trblsht xtroubleshooting xtrblsht eealx
endpoint security linux logovi tcpdump infoget xeealx xendpoint xsecurity xlinux xlogovi xtcpdump xinfoget elc
debug xdebug trace xtrace