ESET Protect
Dijagnostika

Tema

Prikupljanje dijagnostičkih logova za analizu problema u radu sljedećih dijelova sustava:

• ESET Protect (EPx) server / konzola
• ERAAgent
• Endpoint / File Security / Mail Security
• Komunikacija između računala
• Komunikacija s računalima na Internetu
• Komunikacija s ESET-ovim serverima na Internetu

Uvod

Najbrži načini da ustanovite utječe li vaša konfiguracija ili konfiguracija vaše mreže na ponašanje pojedinih dijelova ESET-ova sustava:

• Izdvojite računalo iz mreže (fizički ili ga spojite na “hotspot”)
• Izdvojite EPx iz mreže (fizički ili ga spojite na “hotspot”)
• Instalirajte probno okruženje “od nule” i isprobajte; ako se problem ne pojavljuje – kopirajte postavke sustava jednu po jednu dok ne nađete koja stavka ga uzrokuje

Postupak – Kratko (tl;dr)

Ako gornji testovi ne daju rezultat i problemi se i dalje pojavljuju – prikupite dnevnike programa iz popisa u nastavku i nastojat ćemo u njima pronaći uzrok.

Postupak – Detaljno

Poželjno je da odaberete barem dva klijenta s kojima ima problema.

[A1] Postavite EPx tako da zapisuje “Trace” razinu događaja
(v.→sl. EPx server – Trace log)

[A2] Postavite policy ERAAgenta za testirane klijente tako da zapisuje “Trace” razinu događaja
(v.→sl. ERA Agent – Trace log)

[A3] Postavite policy Endpoint za testirane klijente tako da bilježi dijagnostičke zapise u dnevnik
(v.→sl. Endpoint – Diagnostic log)

[A4] Uključite odgovarajuće napredne dnevnike
(v.→sl. Endpoint – Advanced log)

[A5] Pokrenite Wireshark

(https://support.eset.com/en/kb6446-how-to-create-wireshark-log)

[A6] Uključite dijagnostičko *logiranje* i na firewallu, proksiju, .. perimetra

[A7] Zapišite točan datum i vrijeme pokretanja testa

[A8] Pokrenite proceduru koja dovodi do problema
(ili pričekajte da se problem pojavi ako ga nije moguće replicirati po želji)

[A9] Zapišite vrijeme pojave problema
(ako je problem vidljiv)

[A10] Isključite trace, diagnostic, advanced zapisivanje

[A11] Zaustavite Wireshark
(v.→[B4]!)

Razno

[B1] Prikupite zapise programa ESETLogCollector sa EPx servera
(https://www.nod32.com.hr/podrska/kb8275)

[B2] Prikupite zapise programa ESETLogCollector sa klijenata
(https://www.nod32.com.hr/podrska/kb8275)

[B3] Izvezite policyje za ERAAgenta i Endpoint
(https://www.youtube.com/watch?v=lYiQsREEEJw)

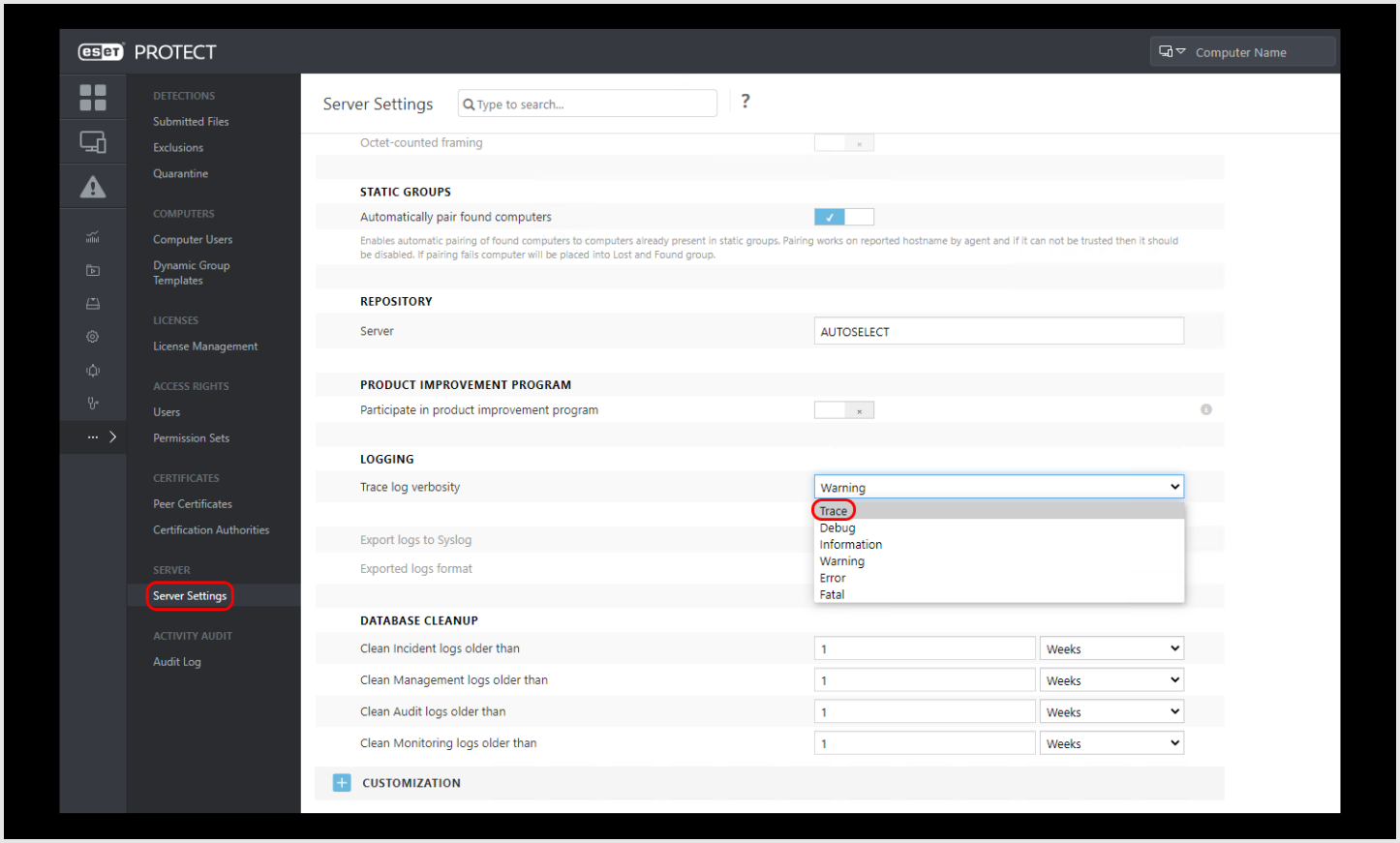
[B4] Spremite Wireshark zapise u dva oblika – .pcapng i .csv (bilo je više slučajeva da Wireshark nije dobro zatvorio datoteke, pa su testovi "propali")

[B5] Spremite zapise firewalla, proksija

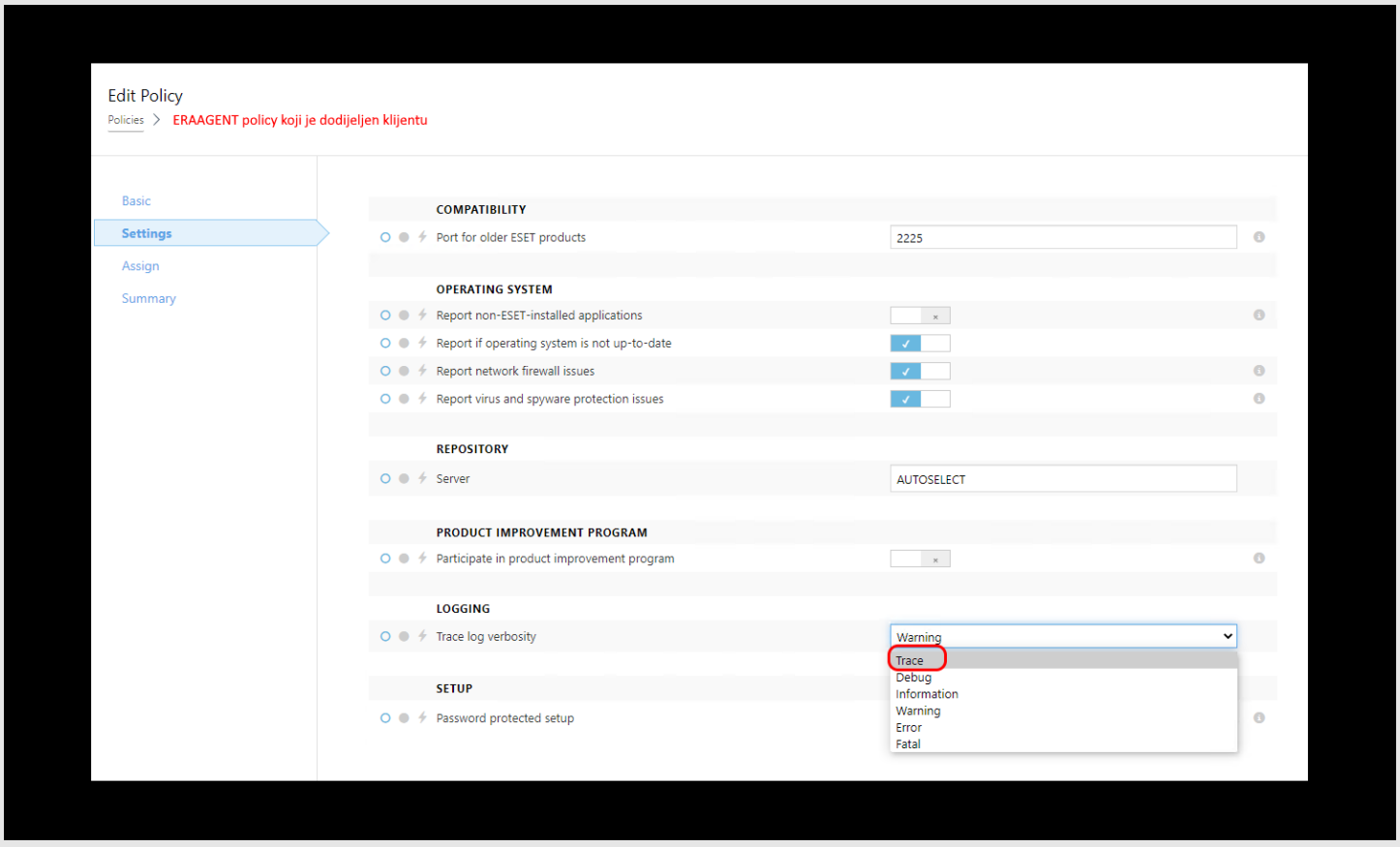
• Datoteke spremite u ZIP, 7z, RAR, … ili nekom drugom općeprihvaćenom obliku komprimirane arhive s lozinkom
• Označite ih jasno da znamo koji paket pripada kojem računalu
• Priložite točno vrijeme pokretanja testa (i vrijeme pojave problema ako je bio vidljiv)
• Spremite na svoj *cloud* disk ili na naš FTP (zatražite podatke ako već unaprijed nismo dogovorili)
• Pošaljite nam link kako bismo preuzeli paket
• Pošaljite nam i lozinku za arhive

Slike

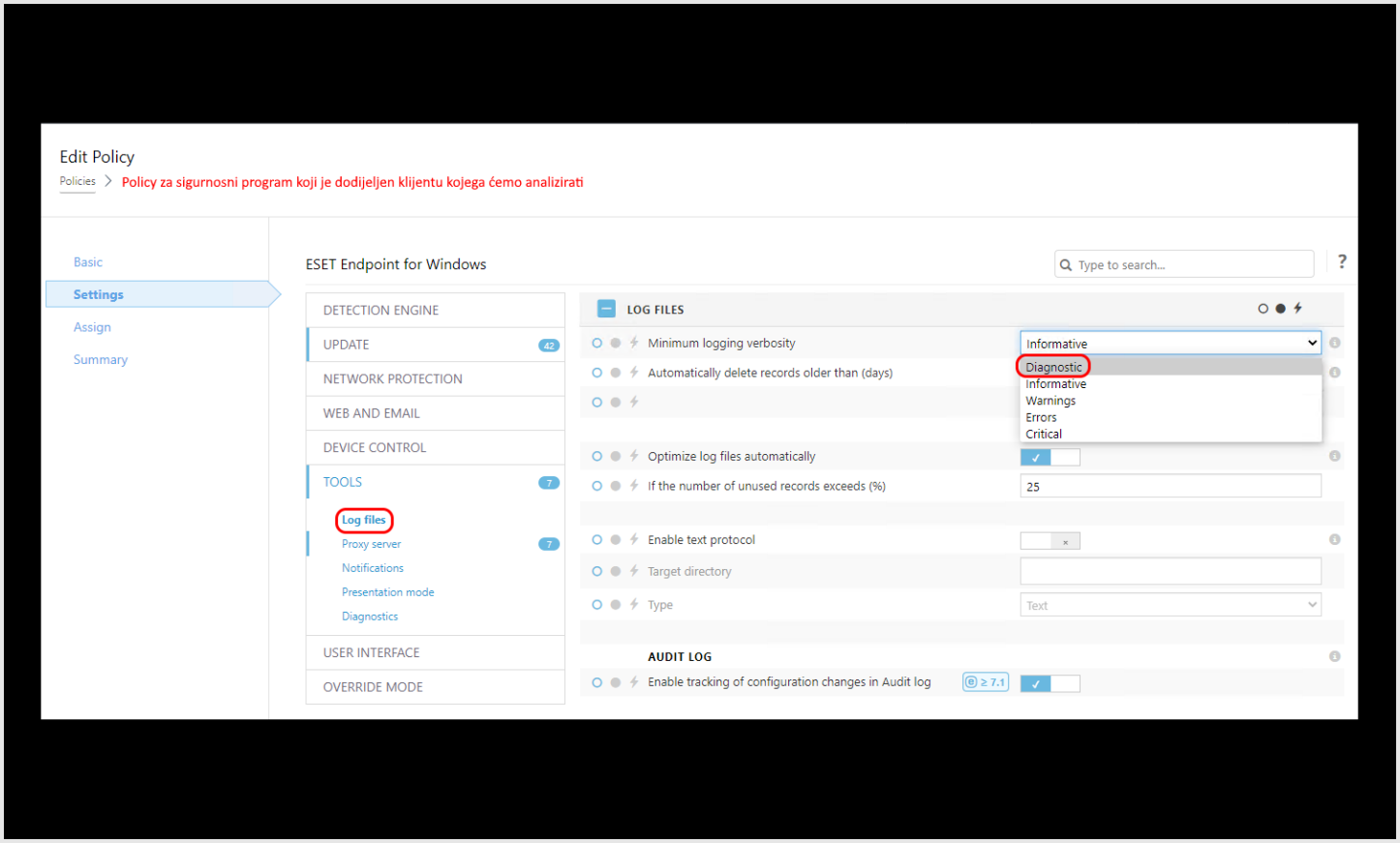
• EPx server – Trace log



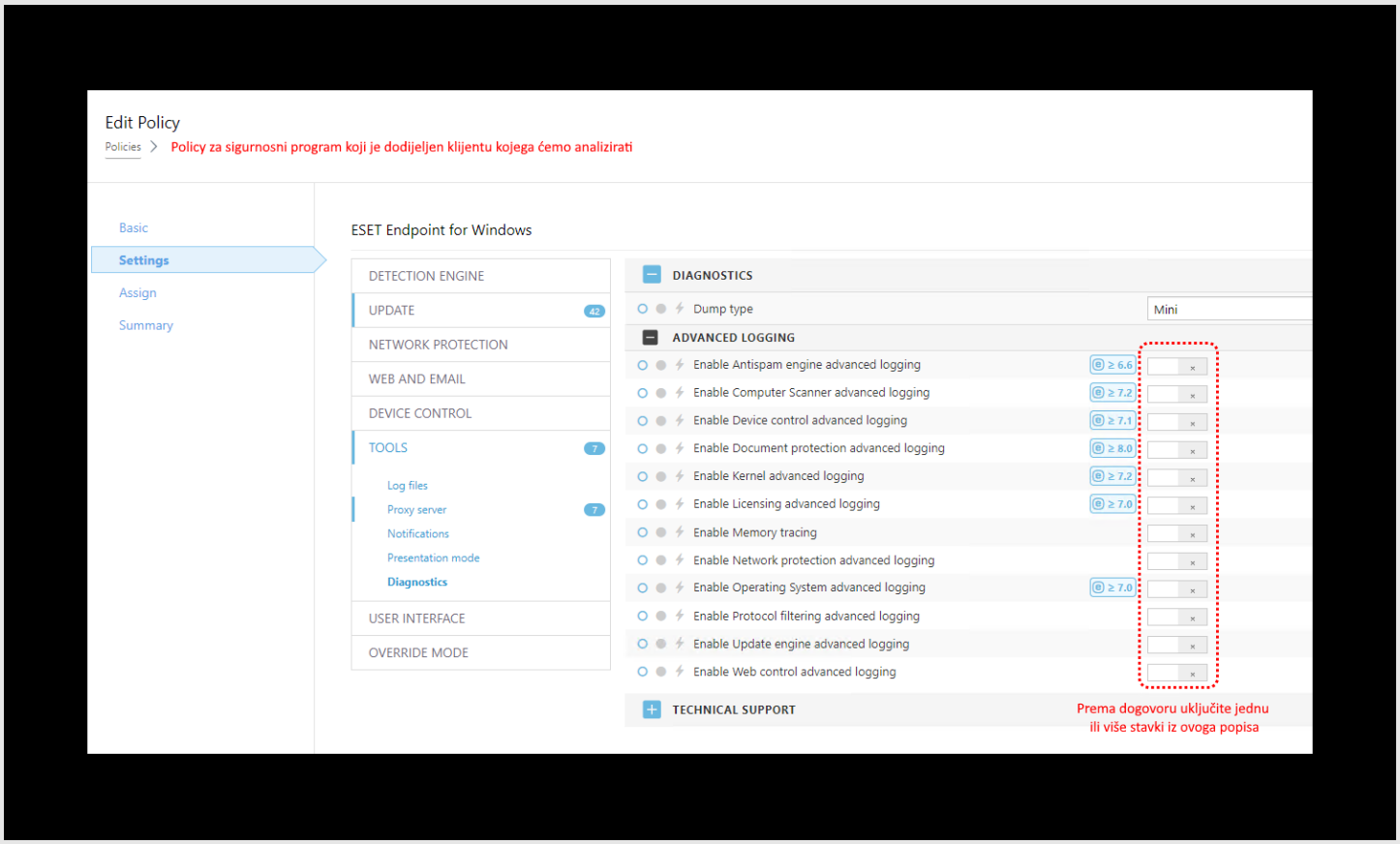
- ERAAgent – Trace log



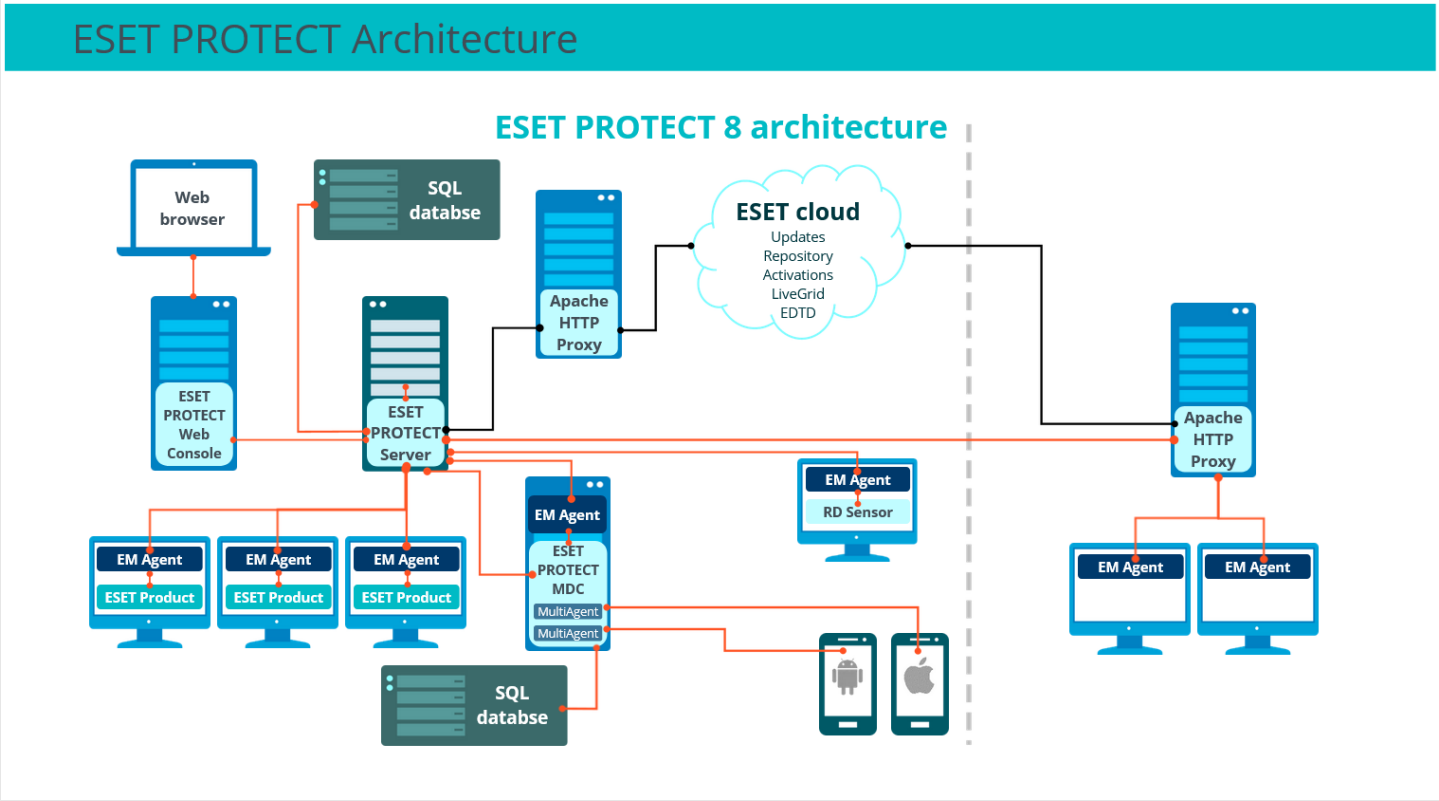
- Endpoint – Diagnostig log



- Endpoint – Advanced log



- EPx arhitektura



ESET Security Management Center ESMC – ESET Protect EPx – Architecture

Video

.

---

dijagnostika xdiagx xtrblshtx xepxx xep8x xesmcx xerax diag xepxdiagx epxdiag xtroubleshootingx