

ESET Protect Dijagnostika

Tema

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

- ESET Protect (EPx) server / konzola
- EMagent (ESET Management Agent)
- Endpoint / File Security / Server Security / Mail Security
- Komunikacija između računala u mreži
- Komunikacija s računalima na Internetu
- Komunikacija s ESET-ovim serverima na Internetu

Uvod

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

- Provjerite ima li problematično računalo (ili grupa) isto mrežno okruženje (isti segment, gateway, proxy, firewall profil, ...)
- Provjerite ima li problematično računalo (ili grupa) instalirane iste programe i konfiguraciju
- Izdvojite problematično računalo iz mreže (fizički ili ga spojite na *ad-hoc hotspot* mobitela)
 - ako to nije moguće - upotrijebite neki VPN klijent (ProtonVPN glasi za pouzdanog)
- Izdvojite EPx iz mreže (fizički ili ga spojite na *ad-hoc hotspot* mobitela)
 - ako to nije moguće - upotrijebite neki VPN klijent (ProtonVPN glasi za pouzdanog)
- 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.

[A] 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 EMAgenta za testirane klijente tako da zapisuje "Trace" razinu događaja
(v.→sl. [EMAgent - Trace log](#))

[A3] Postavite policy Endpoint za testirane klijente tako da bilježi dijagnostičke zapise u dnevnik
(v.→sl. [Endpoint - Logging verbosity](#))

[A4] Uključite odgovarajuće napredne dnevnike
(v.→sl. [Endpoint - Advanced logging](#))

[A5] Pokrenite Wireshark
(<https://support.eset.com/en/kb64446-how-to-create-wireshark-log>)
v.→video
v.→[B4]

[A5b] Po potrebi ili po dogovoru, uključite i Procmon
(<https://support.eset.com/en/kb6308-using-process-monitor-to-create-log-files>)
v.→video
v.→[B4b]

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

[A7] Zapišite točan datum i vrijeme pokretanja testa

[A8] [v.A9!] Pokrenite proceduru koja dovodi do problema:
Npr. pošaljite instalacijski task ili pošaljite task za aktiviranje programa (ili to učinite na računalu) i sl.
Ako ne možete po želji "isprovocirati" pojavu problema, pričekajte da se pojavi.

[A9] Obavezno zapišite točno vrijeme pojave problema! Logovi sadrže gigabajte teksta i nije moguće pronaći gdje se pojavio problem ako ne znamo točno vrijeme jer i svako potpuno funkcionalno računalo i program imaju tisuće poruka o pogreškama, a koje nikako ne utječu na rad

[A10] Isključite trace, diagnostic, advanced zapisivanje

[A11] Zaustavite Wireshark
(v.→[B4]!)

[A12] Pokrenite naredbu netstat na ESET Protect serveru, ovisno o operacijskom sustavu:

[A12A] Linux EPX:

```
netstat --all --wide --numeric-hosts --numeric-ports --verbose --extend  
--listening --context
```

[A12B] Windows EPX:

```
Get-NetUDPEndpoint | select  
LocalAddress,LocalPort,CreationTime,OwningProcess,@{Name="Process";Expression  
={{(Get-Process -Id $_.OwningProcess).ProcessName}} | Format-Table
```

[B] Slanje logova

[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 EMAgenta i Endpoint
(<https://www.youtube.com/watch?v=IYiQsREEEJw>)

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

[B4b] Ako ste koristili i Procmon, spremite i te logove

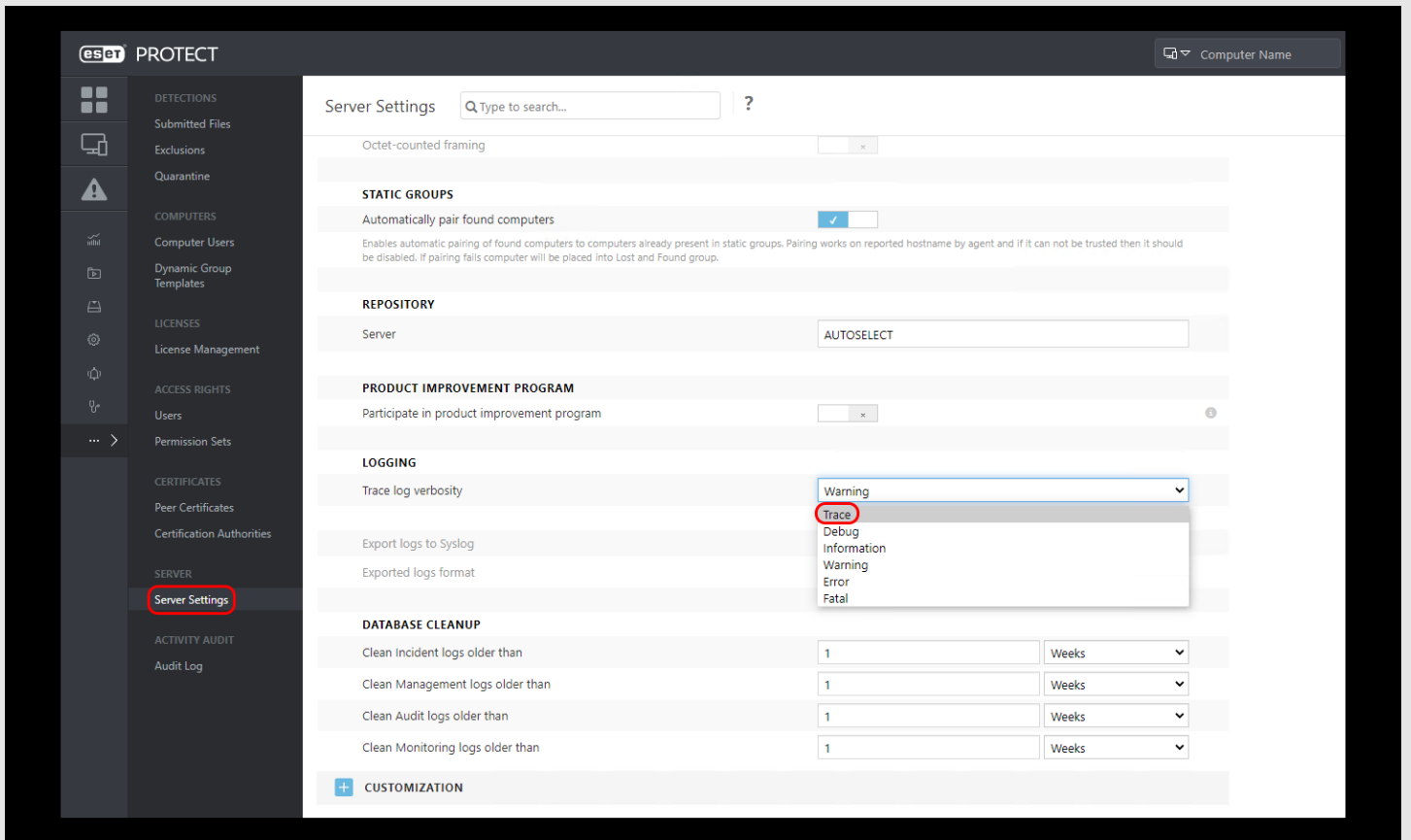
[B5] Spremite zapise firewalla, proksija perimetra

[B6] Dodajte rezultat narebe **netstat** [v.A12]

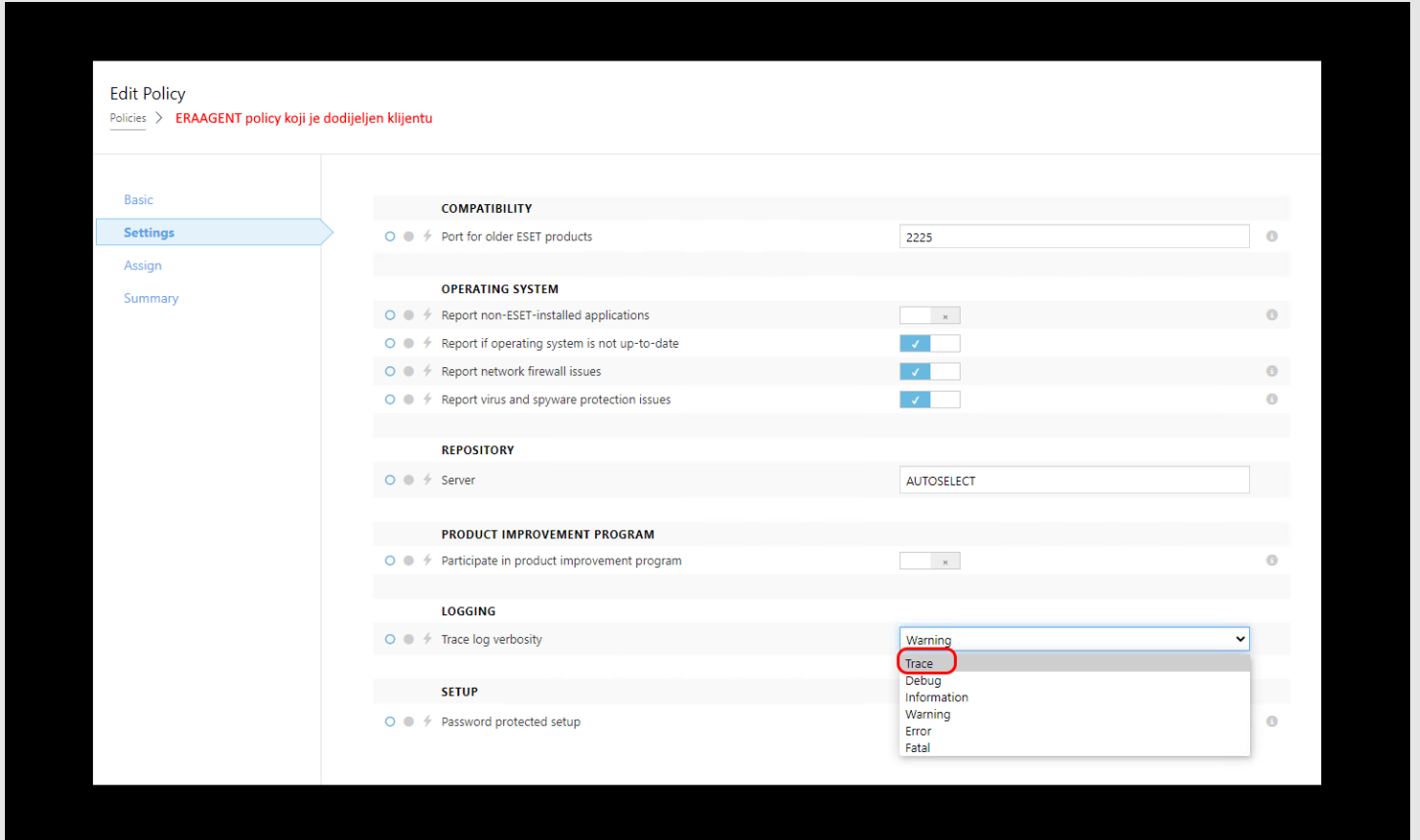
- Datoteke spremite u ZIP, 7z, RAR, ... ili neki drugi općeprihvaćeni oblik komprimirane arhive s lozinkom
- Označite ih jasno da znamo koji paket pripada kojem računalu
- Priložite točno vrijeme pokretanja testa (i vrijeme pojave problema ako je bio vidljiv)
- Spremite na svoj *cloud* disk ili na naš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

Slike

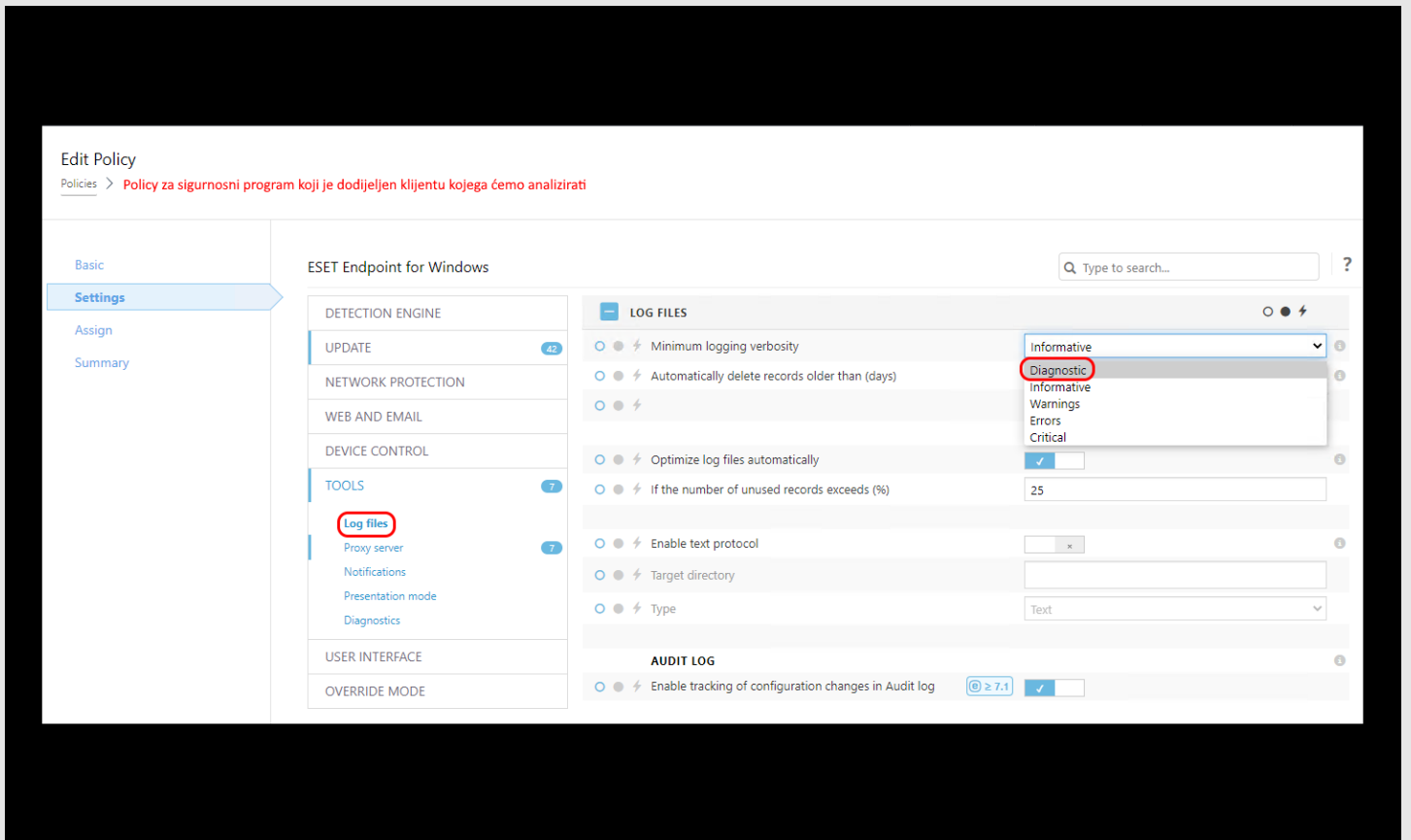
- EPx server - Trace log



- EMAGENT - Trace log



- Endpoint - Logging verbosity



• Endpoint - Advanced logging

Endpoint EN:

Advanced setup



Detection engine **7**

Update **2**

Protections **1**

Tools

Log files

Presentation mode

Diagnostics

Connectivity

User interface **3**

Notifications **13**

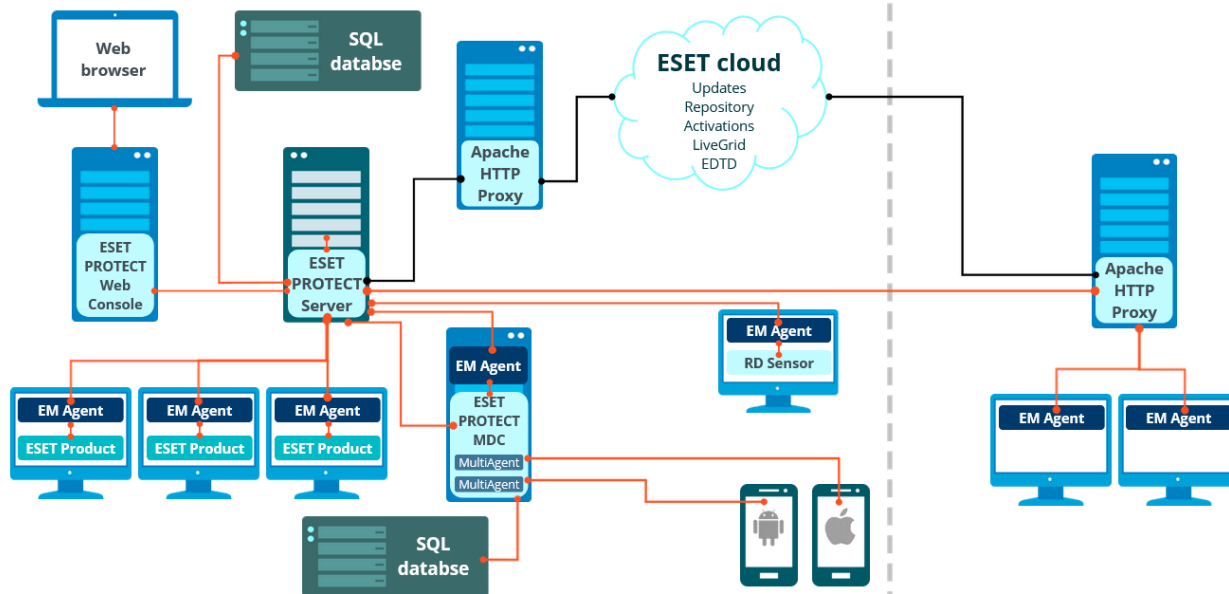
Advanced logging

- Enable Antispam engine advanced logging
- Enable Computer Scanner advanced logging
- Enable Device control advanced logging
- Enable Direct Cloud advanced logging
- Enable Document protection advanced logging
- Enable Email client protection advanced logging
- Enable ESET LiveGuard advanced logging
- Enable Kernel advanced logging
- Enable Licensing advanced logging
- Enable Memory tracing
- Enable Network protection advanced logging
- Enable Network traffic scanner advanced logging
- Enable Operating System advanced logging
- Enable push messaging advanced logging
- Enable Real-time file system protection advanced logging
- Enable Secure Browser advanced logging
- Enable Update engine advanced logging
- Enable Vulnerability & Patch Management advanced logging
- Enable Web control advanced logging

- EPx arhitektura

ESET PROTECT Architecture

ESET PROTECT 8 architecture



ESET Protect EPx - Architecture

Video

Primjer upotrebe programa ProcMon i WireShark.

Prikazuje pripremu okoline za početak snimanja tek neposredno prije replikacije problema (u ovom slučaju je za primjer odabrana instalacija Agenta):

<https://www.nod32.com.hr/podrska/wp-content/uploads/1012-opt.mp4>

diagnostics dijagnostika xdiagnostics xdijagnostika troubleshooting trblsht xtroubleshooting xtrblsht xepxx ep
xepxdiax epxdiax xtroubleshootingx xprocmon procmon wireshark xwireshark sysinternals xsysinternals
emagent xemagent