

# Apache HTTP proxy - Dijagnostika

Kao i uvijek, "Korak " u aktivnostima na bilo kojem serveru: prije ikakve radnje napravite disk-image backup / snapshot / checkpoint / ...

Što detaljnije provedete testove i što više preciznih podataka pošaljete "u prvom naletu" - to kraće će trajati dijagnosticiranje i to manje potpitanja ćemo imati.

---

## Restart servera (ne samo servisa)

Prije nastavka - prvo restartajte cijeli ESET Protect server (nemojte restartati samo Apache httpd servis).

Ako se problem pojavljuje i dalje, slijedite donje upute.

---

## Dijagnostika httpd servisa (proxy)

---

### Provjera proxyja

- Radi li servis?
- Imate li drugi proxy putem kojega se ovaj spaja na internet? Je li sve u redu konfigurirano?
- Traži li drugi proxy username/password?
- Propušta li firewall sav promet s ovog proxyja?

### Ako je Apache instaliran na Windows - test v1

start >> run >> [ Firefox | Chrome | MSEdge ]  
otvorite `http://<$ProxyIP>:<$ProxyPort>/index.html`  
mora prikazati stranicu s tekstem "It works!"

### Ako je Apache instaliran na Windows - test v2

• powershell -command Test-NetConnection -ComputerName <\$ProxyIP> -Port <\$ProxyPort> -  
InformationLevel Detailed | Format-List \*

ili

- `powershell -command Test-NetConnection -ComputerName <$ProxyIP> -Port <$ProxyPort> -InformationLevel Detailed | Format-List *`

## Ako je Apache instaliran na Windows - test v3

- `powershell -command Invoke-WebRequest https://edf.eset.com/edf -verbose`
- `powershell -command Invoke-WebRequest -Proxy http://<$ProxyIP>:<$ProxyPort> -uri https://edf.eset.com/edf -verbose`
- `powershell -command Invoke-WebRequest -Proxy http://<$ProxyIP>:<$ProxyPort> -uri https://www.google.com -verbose`

## Ako je Apache instaliran na Linux/VA - test v1L

- `wget -no-check-certificate -e use_proxy=yes -e http_proxy=<$ProxyIP>:<$ProxyPort> www.eset.com`
- `wget -no-check-certificate -e use_proxy=yes -e http_proxy=<$ProxyIP>:<$ProxyPort> www.google.com`

## Ako je Apache instaliran na Linux/VA - test v2L

- `curl -proxy <$ProxyIP>:<$ProxyPort> -include -silent https://edf.eset.com/edf`
- `curl -proxy <$ProxyIP>:<$ProxyPort> -include -silent https://bing.com`

Nakon svakog testa snimite sliku ekrana i pošaljite tako da se vidi naredba i rezultat.

---

## Pregled sadržaja u cacheu

- Windows:  
`"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -v -a -p`  
`"C:\ProgramData\Apache HTTP Proxy\cache"`
- Linux/VA:  
`htcacheclean -v -a -p /var/cache/httpd/proxy`

---

# Čišćenje cachea

## Apache instaliran na Windows

- pokrenite CMD kao administrator
- `net stop ApacheHttpProxy`
- `"C:\Program Files\Apache HTTP Proxy\bin\htcacheclean.exe" -v -t -p"C:\ProgramData\Apache HTTP Proxy\cache" -l500M -L24`
- `dir "C:\ProgramData\Apache HTTP Proxy\cache" /A/S/B`
- `net start ApacheHttpProxy`

Ako ne uspije, probajte "brutalnom" metodom ukloniti cache:

- `RD /Q /S "C:\ProgramData\Apache HTTP Proxy\CACHE\"`
- `MD "C:\ProgramData\Apache HTTP Proxy\CACHE\"`

## Apache instaliran na Linux/VA

- `service httpd stop (ili systemctl stop httpd)`
- `htcacheclean -v -t -p'/var/cache/httpd/proxy/' -l500M -L24`
- `service httpd start (ili systemctl start httpd)`

Napomena: vrijednosti `500M` i `24` prilagodite prema svojim potrebama i/ili dokumentaciji ([https://help.eset.com/protect\\_deploy\\_va/latest/en-US/enable\\_apache\\_http\\_proxy.html](https://help.eset.com/protect_deploy_va/latest/en-US/enable_apache_http_proxy.html))

### Legenda:

- `<$ProxyIP>` ... IP adresa proxy servera (za httpd koji dolazi s ESET Protect serverom je to IP adresa ESET protecta)
- `<$ProxyPort>` ... Port proxy servera (za httpd koji dolazi s ESET Protect serverom je to obično: 3128)

---

# Prikupljanje logova

- napravite kopiju datoteke "httpd.conf"
  - Windows:  
`copy "C:\Program Files\Apache HTTP Proxy\conf\httpd.conf" "C:\Program Files\Apache HTTP Proxy\conf\httpd.conf.bkp"`
  - Linux/VA:  
`cp /etc/httpd/conf/httpd.conf /etc/httpd/conf/httpd.conf.BKP`

- otvorite "httpd.conf" u tekst editoru
  - Windows:
 

```
notepad "C:\Program Files\Apache HTTP Proxy\conf\httpd.conf"
```
  - Linux/VA:
 

```
nano /etc/httpd/conf/httpd.conf
```
- pronađite i umjesto "LogLevel warn" stavite "LogLevel debug"
- spremite datoteku
- restartajte HTTPD servis
  - Windows:
 

```
net stop ApacheHttpProxy
net start ApacheHttpProxy
```
  - Linux/VA:
 

```
systemctl restart httpd
```
- obavezno provjerite httpd.conf je li ostao na "debug"
- pokrenite Wireshark (<https://support.eset.com/en/kb6446-how-to-create-wireshark-log>)
- zapišite točno vrijeme
- forsirajte 2-3 puta update da se zabilježi pokušaj komunikacije u logovima
- isključite Wireshark i spremite logove
- komprimirajte logove zadnjih barem 48 sati (\*1)
  - Windows:
 

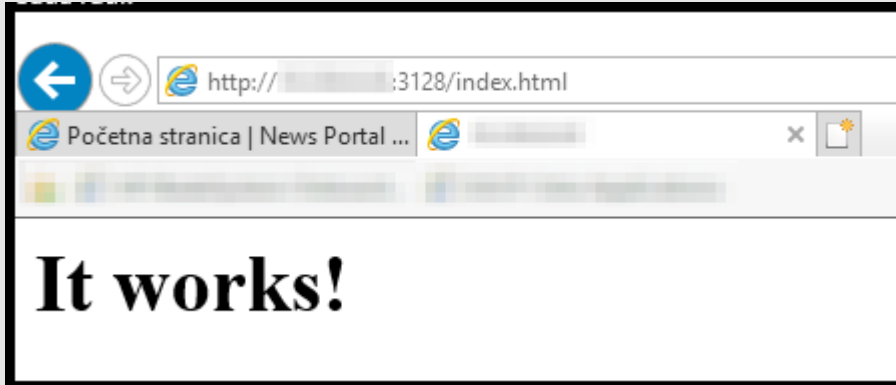
```
C:\Program Files\Apache HTTP Proxy\logs\*.*
```
  - Linux/VA:
 

```
/var/log/httpd/*
```
- vratite "httpd.conf" iz backupa ili promijenite "debug" u "warn"
- restartajte proxy servis (v.gore)
- pošaljite nam [ 7Z / ZIP / ARJ / RAR ] datoteku s logovima
  - ako je datoteka prevelika za e-mail (>5MB) - stavite na svoj *cloud-disk* ili zatražite informacije za upload na naš FTP server
- napišite IP adresu i FQDN sljedećih računala:
  - MDM servera
  - EPX servera
  - HTTP proksija
  - klijenta
  - ... svih ostalih bitnih računala uključenih u testiranje
- napišite točno vrijeme kad ste testirali
- Pošaljite Wireshark, gornje logove i ELC:
  - Windows:
 

```
ESETLogCollector (https://www.nod32.com.hr/podrska/kb672)
```

- Linux/VA:  
`info-get` (<https://support.eset.com/en/kb6159>)

## Slike



```
> Test-NetConnection -ComputerName 192.168.1.100 -Port 3128 -InformationLevel Detailed | format-list *
VERBOSE: 168.192.in-addr.arpa
DEBUG: 196616
DEBUG: "Sort-Object" - "Address" cannot be found in "InputObject".
VERBOSE: Perform operation 'Invoke CimMethod' with following parameters, 'namespaceName' = root\standardcimv2
VERBOSE: Operation 'Invoke CimMethod' complete.

ComputerName           : 192.168.1.100
RemoteAddress          : 192.168.1.100
ResolvedAddresses      : {192.168.1.100}
PingSucceeded         : False
PingReplyDetails      :
TcpClientSocket       :
TcpTestSucceeded      : True
RemotePort            : 3128
TraceRoute            :
Detailed              : True
InterfaceAlias        : Ethernet
InterfaceIndex        : 5
InterfaceDescription  : Realtek PCIe GBE Family Controller
NetAdapter            : MSFT_NetAdapter (CreationClassName = "MSFT_NetAdapter", DeviceID = "{280...}
NetRoute              : MSFT_NetRoute (InstanceID = ";C?8;@...; 55;")
SourceAddress         : 192.168.1.100
NameResolutionSucceeded : True
BasicNameResolution   : {Microsoft.DnsClient.Commands.DnsRecord_PTR}
LLMNRNetbiosRecords  : {}
DNSOnlyRecords       : {}
AllNameResolutionResults : Microsoft.DnsClient.Commands.DnsRecord_PTR
IsAdmin               : False
NetworkIsolationContext : Private Network
MatchingIPsecRules    :
```

httpd trblsht xhttpdx xtrblshtx xapachex xproxyx xproxytestx pwshproxytest troubleshooting proxytest  
testproxy xproxytest xttestproxy itworks xitworks itsworking xitsworking xpowershell