NAP

10. PREDAVANJE

Sadržaj

- Kratak pregled Network Access Protection
- NAP metode prisile
- Konfiguracija NAP-a
- Nadgledanje i rješavanje problema

Kratak pregled Network Access Protection

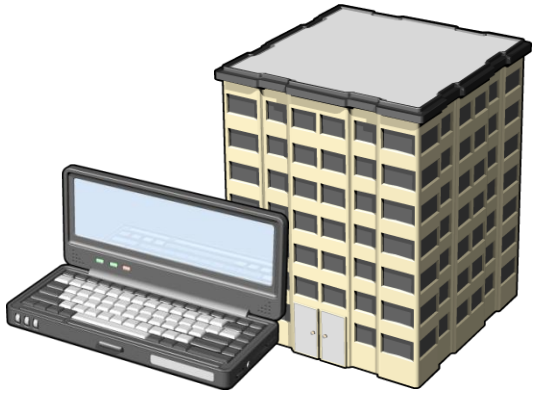
- Što je Network Access Protection?
- NAP scenariji
- NAP metode prisile
- Arhitektura NAP platforme

Što je Network Access Protection?

- NAP može:
  - Prisiliti “health-requirement” politike na klijentska računala
  - Pobrinuti se da su klijentska računala u skladu s politikama
  - Ponuditi mogućnost popravka računalima koja nisu u skladu s politikama
- NAP ne može:
  - Onemogućiti maliciozne radnje autoriziranim korisnicima s računalima koja su u skladu s politikama
  - Onemogućiti pristup mreži računalima koja su izuzeta od djelovanja NAP politika (računala s Windows XP SP2 i ranija) kada su za njih definirana pravila izuzeća

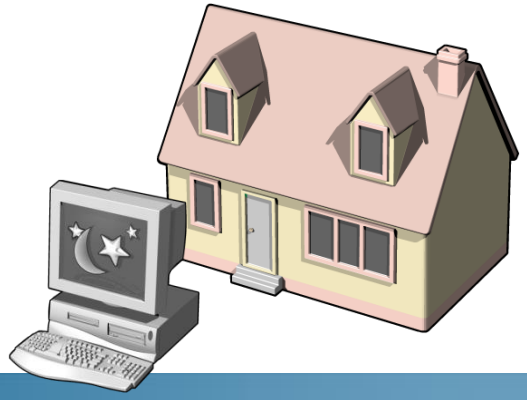
NAP nam pomaže provjeriti zdravstveno stanje:

Prijenosnih računala koja često mijenjaju mreže



Gostujućih prijenosnih računala

Desktop računala

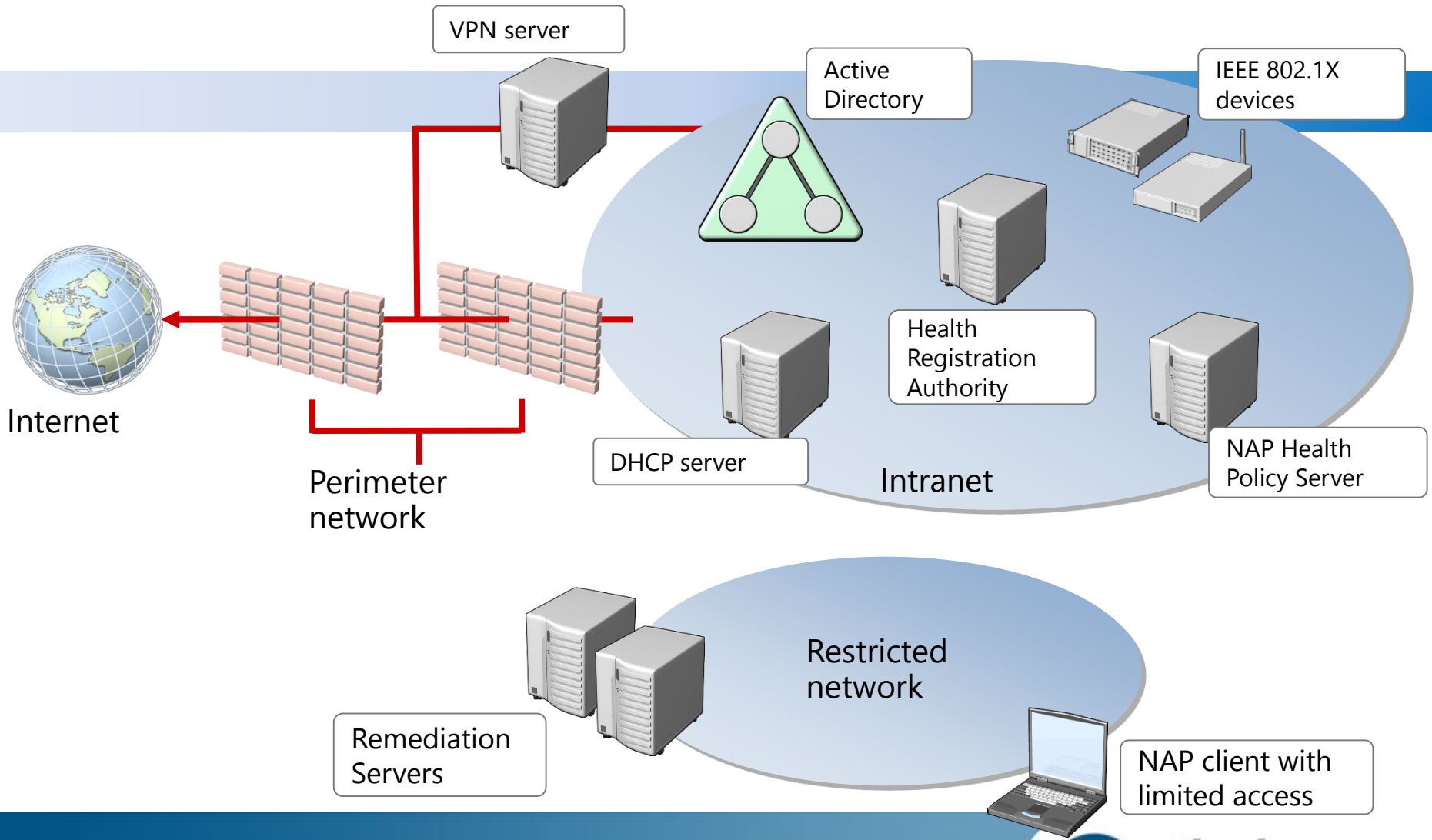


Kućnih računala kojima ne upravljamo

NAP metode prisile

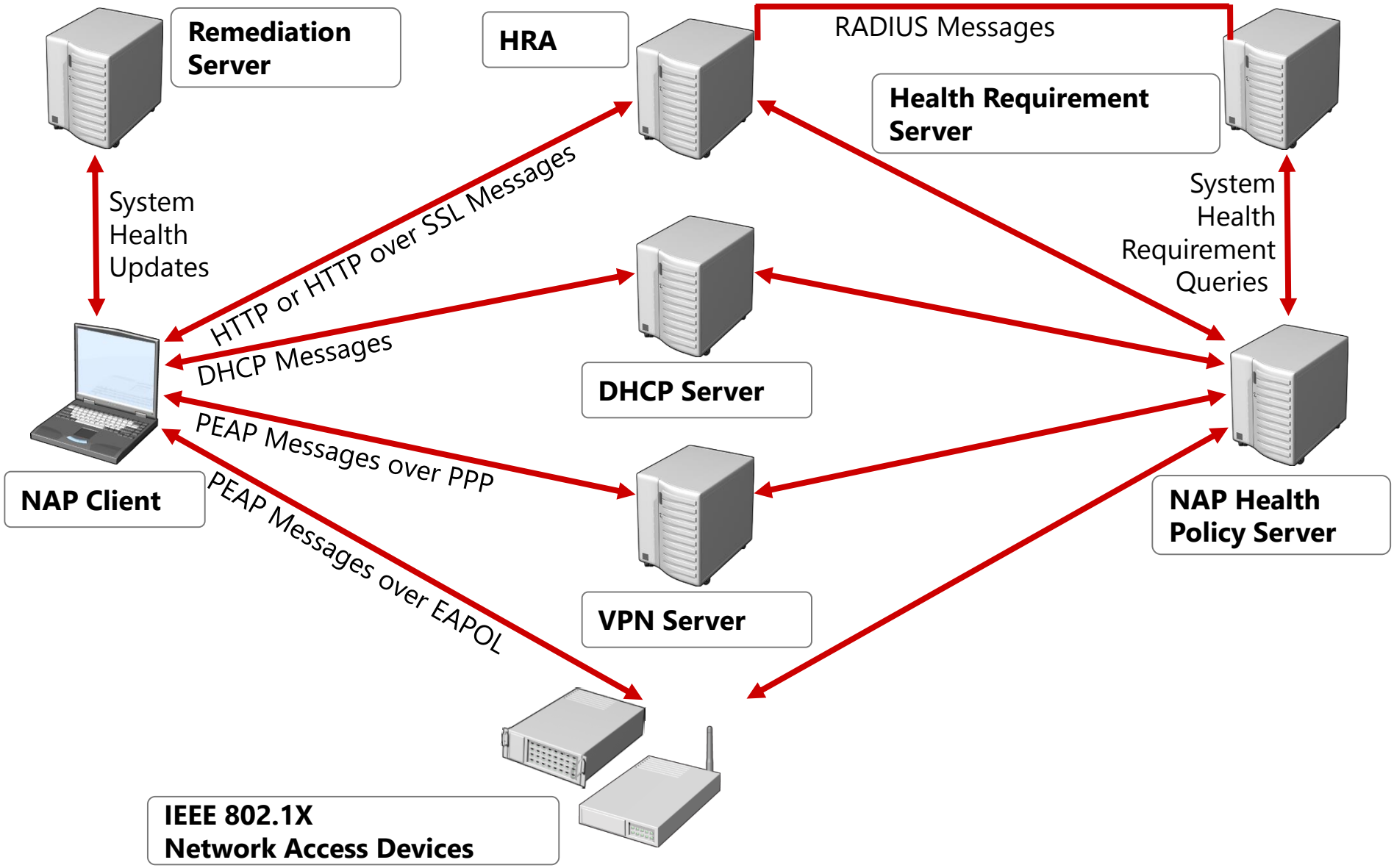
Metoda	Ključne točke
IPsec prisila	• Računalo mora biti u skladu s politikama da bi komuniciralo u mreži • Najjača metoda prisile, može se primijeniti po IP adresama ili portovima protokola
802.1X prisila	• Računalo mora biti u skladu s politikama da bi dobilo pristup mreži preko 802.1X uređaja (autentifikacijski switch ili access point)
VPN prisila	• Računalo mora biti u skladu s politikama da bi dobilo neograničen pristup preko RAS-a
DHCP prislila	• Računalo mora biti u skladu s politikama da bi dobilo ispravnu IPv4 adresu od DHCP • Najslabija metoda prisile

Arhitektura NAP platforme



NAP metode prisile

- NAP proces prisile
- IPsec prisila
- 802.1x prisila
- VPN prisila
- DHCP prisila


Remediation Server
HRA
RADIUS Messages
Health Requirement Server
System Health Updates
HTTP or HTTP over SSL Messages
System Health Requirement Queries
DHCP Messages
DHCP Server
PEAP Messages over PPP
NAP Client
PEAP Messages over EAPOL
NAP Health Policy Server
VPN Server
IEEE 802.1X Network Access Devices

IPsec prisila

- Ključne informacije o IPsec NAP prisili:
  - Sastoji se od health certificate servera i IPsec NAP EC
    - Health certificate server izdaje X.509 certifikate klijentima kada se potvrdi da su u skladu s zdravstvenim politikama
    - Certifikati se koriste za autentikaciju klijenata kada iniciraju IPsec komunikaciju s drugim NAP klijentima na mreži
  - IPsec prisila sužava komunikaciju na mreži na samo one klijente koji su u skladu s zdravstvenim politikama i imaju certifikat
  - Komunikacija između "zdravih" klijenata se može definirati prema IP adresi ili po TCP/UDP portovima

802.1x prisila

- Ključne informacije o 802.1X žičanoj ili bežičnoj prisili :
  - Računalo mora biti u skladu s politikama da bi dobilo pristup mreži preko 802.1X uređaja
  - Računala koja nisu “zdrava” imaju ograničen pristup mreži
  - Pristup mreži se može ograničiti bilo korištenjem filtriranja IP paketa ili VLAN ID -jeva
  - 802.1X prisila aktivno nadgleda klijente i u trenutku kada klijent iz bilo kojeg razloga više nije “zdrav”, stavlja ga u ograničeni dio mreže

VPN prisila

- Ključne informacije o VPN NAP prisili :
  - Računalo mora biti u skladu s politikama da bi dobilo pristup mreži preko VPN konekcije
  - Računalima koja nisu “zdrava” pristup mreži se ograničava filtriranjem IP paketa
  - VPN prisila aktivno nadgleda klijente i u trenutku kada klijent iz bilo kojeg razloga više nije “zdrav”, stavlja ga u ograničeni dio mreže

DHCP prisila

- Ključne informacije o DHCP prisili :
  - Računalo mora biti u skladu s politikama da bi dobilo neograničen pristup mreži i ispravnu IPv4 adresu od DHCP servera
  - Računalima koja nisu “zdrava” pristup mreži se ograničava dodijeljivanjem IP adrese koja vrijedi jedino u ograničenom dijelu mreže
  - DHCP prisila aktivno nadgleda klijente i u trenutku kada klijent iz bilo kojeg razloga više nije “zdrav”, stavlja ga u ograničeni dio mreže

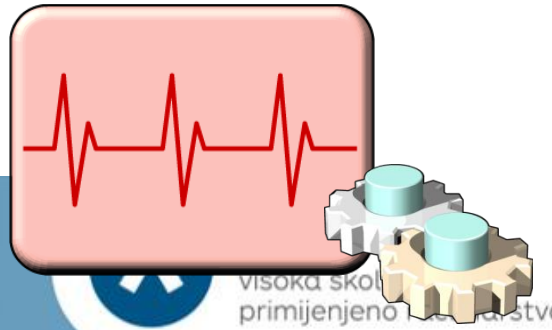
Konfiguracija NAP-a

- Što su System Health Validators?
- Što je Health Policy?
- Što je Remediation Server Grupe?
- NAP Client konfiguracija

Što su System Health Validators?

System Health Validators (SHV) su serverski parnjaci System Health Agentima (SHA) na strani klijenta

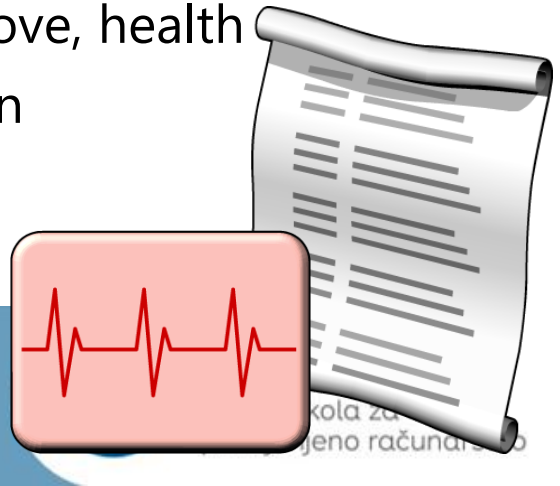
- Svaki SHA na klijentu ima odgovarajući SHV u NPS-u
- SHV ovi omogućavaju NPS da verificira zdravstveno stanje (SoH) generirano od odgovarajućeg SHA na klijentu
- SHV ovi sadrže odgovarajuće konfiguracijske postavke za klijentska računala
- Windows Security SHV odgovara Microsoft SHA na klijentskim računalim



Što su to Health Policy?

Da bi mogli iskoristiti Windows Security Health Validator, moramo konfigurirati Health Policy i dodijeliti joj SHV

- Health policies se sastoje od jednog ili više SHVs i drugih postavki koje omogućavaju da definiramo zdravstvene zahtjeve kojima klijenti moraju udovoljiti da bi neometano mogli pristupiti mreži
- Klijentske health policies možemo definirati u NPS dodavanjem jednog ili više SHV ova
- NPS radi NAP prisilu prema svakoj pojedinačnoj mrežnoj konekciji
- Nakon što kreiramo health policy i dodamo mu SHV ove, health policy možemo dodati u Network policy i na taj način kontrolirati pristup internoj mreži

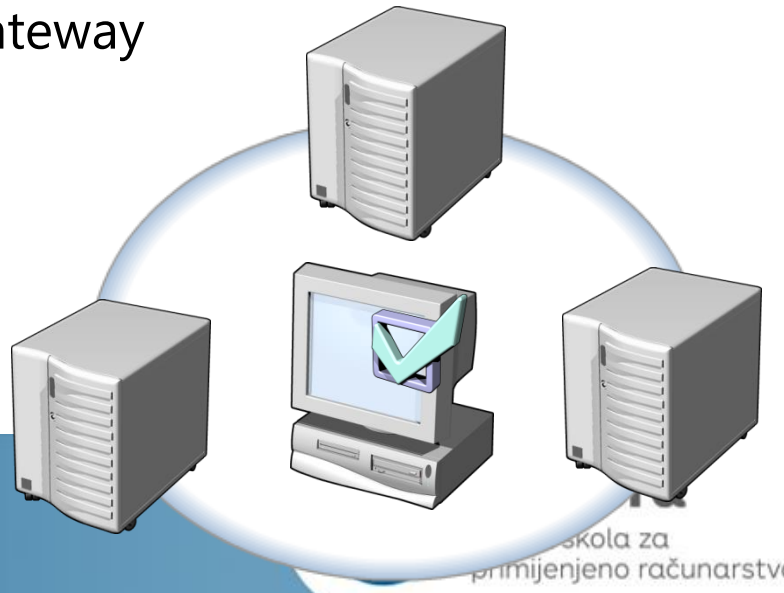


Što su Remediation Server Grupe?

Kada definiramo NAP prisile, trebali bi definirati servere za popravak koji će poslužiti onim klijentima koji nisu u skladu s zdravstvenim politikama

- Server za popravak sadrži nadogradnje i zakrpe koje su nužne da bi klijent s NAP agentom mogao postati sukladan zdravstvenim politikama i da bi neometano mogao komunicirati u mreži
- Serveri za popravak se nalaze u ograničenom dijelu mreže. Oni mogu biti file serveri, WSUS server ili recima gateway

  prema Internetu



NAP Client konfiguracija

- Neki oblici NAP implementacije koji koriste Windows Security Health Validatore zahtijevaju uključivanje Security Centera na klijentu
- Network Access Protection servis mora biti uključen (automatic start) kada implementiramo NAP na klijente koji imaju NAP agenta (servis je inicijalno isključen)
- Moramo konfigurirati i uključiti odgovarajuće NAP enforcement klijente na računalima (napclcfg.msc)
- Većina NAP postavki može biti konfigurirana putem Group Policy objekata

Nadgledanje i rješavanje problema

- Što je NAP Tracing?
- Rješavanje problema
- Rješavanje problema pomoću Event Log zapisa

Što je NAP Tracing?

- NAP tracing identificiran NAP događaje i zapisuje ih u log datoteku ovisno o konfiguriranim postavkama:
  - Basic
  - Advanced
  - Debug
- Tracing zapise možemo koristiti za:
  - Procjenu zdravlja i sigurnosti mreže
  - Rješavanje problema i održavanje
- NAP tracing is je prema zadanoj postavci isključen
- Možemo ga uključiti kroz GUI ili pomoću netsh naredbe
  - netsh nap client set tracing state = enable

Rješavanje problema

Možemo koristiti sljedeće netsh NAP komande da bi pokušali riješiti potencijalne probleme:

- netsh NAP client show state
- netsh NAP client show config
- netsh NAP client show group

Rješavanje problema pomoću Event Log zapisa

Event ID	Značenje
6272	Dogodila se uspješna autentifikacija
6273	Nije se dogodila se uspješna autentifikacija
6274	Postoji konfiguracijski problem
6276	NAP client je u karanteni
6277	NAP client je u probnom roku
6278	NAP client ima puni pristup resursima