Algebra
visoka škola za
primijenjeno računarstvo

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo | Ilica 242 | 10000 Zagreb | Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 | matični broj: 2412926 | IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 | fax. +385 (0)1 2305 004 | info@racunarstvo.hr | www.racunarstvo.hr

KATEDRA ZA OPERACIJSKE SUSTAVE

Operacijski sustavi: mrežna infrastruktura i servisi

Lab 09 – DHCP Network Access Protection

REV 2.0

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo | Ilica 242 | 10000 Zagreb | Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 | matični broj: 2412926 | IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 | fax. +385 (0)1 2305 004 | info@racunarstvo.hr | www.racunarstvo.hr

Sadržaj

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Uvod

Tema današnje vježbe jesu **NAP** (eng. *Network Access Protection*) mehanizmi. NAP je zadužen za provjeru „zdravlja" klijenata koji se žele spojiti na domensku mrežu. Ovisno o zdravlju, NAP će dopustiti pristup mreži, potpuno izolirati klijenta ili mu dopustiti pristup samo najnužnijim resursima. Zdravlje klijenta određuje se prema nekoliko kategorija.

- **Windows vatrozid**: uključen na svim mrežnim vezama i na svim profilima.
- **Antivirusna aplikacija**: uključena i s instaliranim najnovijim definicijama.
- **Antispyware aplikacija**: isto kao i za antivirusnu aplikaciju.
- **Windows ažuriranja**: instalirana ažuriranja operacijskog sustava. Moguće je odrediti i vrstu ažuriranja koja nužno mora biti instalirana (npr. kritične sigurnosne nadogradnje).

Današnja je vježba najkompleksnija do sada i objedinjuje elemente nekoliko vježbi, a izravno se nastavlja na prethodnu. Vježba je predviđena za rad u dva termina. U prvom dijelu vježbe (danas) instaliramo uloge koje nedostaju (DHCP i RRAS) i konfiguriramo DHCP NAP. Opišimo infrastrukturu koju želimo postići.

- **SERVERDC**: domenski kontroler domene racunarstvo.edu kojem smo instalirali uloge certifikacijskih servisa u prošloj vježbi. Na ovo računalo je pred instaliran DHCP poslužitelj a danas ćemo instalirati **NPS** (eng. *Network Policy Server*) ulogu putem koje implementiramo NAP.
- **SERVER1**: ovaj poslužitelj danas ne koristimo.
- **CLI1**: klijentsko računalo s kojeg ćemo testirati funkcionalnost NAP mehanizama. Ovisno o postavljenim opcijama, ovo će računalo imati puni ili djelomični pristup mreži.

Opišimo u par rečenica **DHCP NAP**. Klijenti koji od DHCP poslužitelja traže TCP/IP postavke moraju zadovoljiti uvjete nametnute NAP kriterijima. Ako ne zadovolje, DHCP poslužitelj klijentu će poslati postavke koje će mu onemogućiti komunikaciju s ostalim računalima na mreži (npr. mrežnu masku 255.255.255.255 – IP adresa bez klase). Ova je vrsta NAP-a najlakša za konfiguraciju i ne zahtijeva certifikacijske servise. Klijentima se, eventualno, može dopustiti pristup nužnim resursima (npr. poslužitelju s javnim dijeljenim mapama) dok ne isprave propust u zdravstvenom stanju.

Ovime završava današnji uvod. Krenimo s vježbom.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Prije vježbe

1. Prijavite se na računalo kao **Administrator** s lozinkom **Pa$$w0rd**.
2. Kliknite na **Start**-> **Administrative Tools**-> **Hyper-V Manager**.
3. Provjerite jesu li sva virtualna računala isključena. Podsjetimo se, isključena računala kao oznaku statusa imaju **Off** ili **Saved**. Uključena računala imaju oznaku **Running**.
4. Primijenite *snapshot* **Start** na virtualnom računalu **KZOS-SERVERDC.**
5. Primijenite *snapshot* **Start** na virtualnom računalu **KZOS-CLI1.**

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Pripremne radnje

Kako je opisano u uvodu, prije nego konfiguriramo NAP, moramo instalirati potrebne uloge. Instalacija se minimalno razlikuje od postupaka koje smo prošli u prethodnim vježbama.

Osnovna konfiguracija

U AD ćemo dodati grupu koja će poslužiti za smještaj računala koja podliježu NAP provjeri.

1. Prikažite **Hyper-V Manager** konzolu.
2. Pokrenite virtualno računalo **KZOS-SERVERDC**
3. Prijavite se na računalo **SERVERDC** kao **RACUNARSTVO\Administrator** s lozinkom **Pa$$w0rd**
4. Prikažite ekran **Start** i kliknite na **Active Directory Users and Computers**.
5. Prikazuje se konzola **Active Directory Users and Computers**. Unutar lijevog okna proširite domenu **racunarstvo.edu**.
6. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Racunala** i iz kontekstualnog izbornika odaberite **New**-> **Group**.
7. Prikazuje se ekran **New Object – Group**. U polje **Group name** upišite **NAP_Racunala**.
8. Unutar kategorije **Group Scope** postavite vrijednost **Domain local** i kliknite gumb **OK**.
9. Vraćate se u **Active Directory Users and Computers** konzolu. Unutar desnog okna desnim gumbom miša kliknite na grupu **NAP_Racunala** i iz kontekstualnog izbornika odaberite opciju **Properties**.
10. Prikazuje se ekran **NAP_Racunala Properties**. Kliknite na karticu **Members** i zatim kliknite gumb **Add**.
11. Prikazuje se ekran za odabir objekata. Kliknite gumb **Object Types.**
12. Prikazuje se ekran **Object Types**. Označite stavku **Computers** i kliknite gumb **OK**.
13. Vraćate se na ekran za odabir objekata. U polje **Enter the object names to select** upišite **CLI1** i kliknite gumb **OK**.
14. Vraćate se na ekran **NAP_Racunala Properties**. Kliknite gumb **OK.**
15. Zatvorite **Active Directory Users and Computers** konzolu.

Promijenimo TCP/IP postavke računala CLI1 – postavljamo ih na DHCP.

1. Prikažite **Hyper-V Manager** konzolu.
2. Pokrenite virtualno računalo **KZOS-CLI1**
3. Prijavite se na računalu **CLI1** kao **RACUNARSTVO\Admin1** s lozinkom **Pa$$w0rd**
4. Prikažite ekran **Start**, upišite **ncpa.cpl** te pritisnite gumb **Enter**.
5. Prikazuje se prozor **Network Connections** s popisom mrežnih adaptera.
6. Desnim gumbom miša kliknite na adapter **LAN** i iz kontekstualnog izbornika odaberite opciju **Properties**.
7. Prikazuje se ekran **LAN Properties**. Kliknite na stavku **Internet Protocol Version 4 (TCP/IPv4)** i zatim kliknite gumb **Properties**.
8. Prikazuje se ekran sa postavkama mrežnog adaptera. Uključite opcije **Obtain an IP address automatically** i **Obtain DNS server address automatically** te kliknite gumb **OK**.
9. Vraćate se na ekran **LAN Properties**. Kliknite gumb **Close**.
10. Zatvorite sve prikazane prozore na računalu **CLI1**.

Provjerimo je li Windows Firewall isključen:

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

1. Prikažite ekran **Start**, upišite **`WF.msc`** i pritisnite tipku **Enter**.
2. Prikazuje se **Windows Firewall with Advanced Security** konzola. U lijevom oknu desnim gumbom miša kliknite na **Windows Firewall with Advanced Security** (prva stavka) i iz kontekstualnog izbornika odaberite opciju **Properties**.
3. Prikazuje se ekran sa postavkama vatrozida. Kliknite na karticu **Domain Profile** i iz izbornika **Firewall state** odaberite opciju **Off**. Kliknite gumb **Apply**.
4. Na isti način isključite vatrozid na **privatnom** profilu (kartica **Private Profile**) i na **javnom** profilu (kartica **Public Profile**).
5. Zatvorite sve otvorene prozore na računalu **CLI1**.
6. Na traci izbornika *Virtual Machine Connection* prozora kliknite na **Action** -> **Shut Down**.
7. Virtualno računalo **CLI1** će se isključiti.

-----NAPOMENA-----

Uključenje odnosno isključenje Windows Firewalla zahtijeva prava lokalnog administratora. Osim prethodnim postupkom, Windows Firewall se može isključiti i pomoću naredbe **`netsh advfirewall set allprofiles state off`**. Tu naredbu ćemo koristiti u nastavku vježbe.

Instalacija i konfiguracija potrebnih uloga

Sada možemo instalirati potrebnu ulogu na računalu SERVERDC.

1. Prikažite ekran **Start** i kliknite na **Server Manager**.
2. Prikazuje se **Server Manager** konzola. Kliknite na izbornik **Manage-> Add Roles and Features**.
3. Prikazuje se ekran **Before you begin**. Kliknite gumb **Next**.
4. Prikazuje se ekran **Select installation type**. Ostavite predefinirane opcije i kliknite gumb **Next.**
5. Prikazuje se ekran **Select destination server**. Ostavite predefinirane opcije i kliknite gumb **Next.**
6. Prikazuje se ekran **Select server roles**. Označite stavku **Network Policy and Access Services.**
7. Prikazuje se ekran s informacijama o dodatnim komponentama. Kliknite gumb **Add Features**.
8. Vraćate se na ekran **Select server roles**. Kliknite gumb **Next**.
9. Prikazuje se ekran **Select features**. Kliknite gumb **Next**.
10. Prikazuje se ekran **Network Policy and Access Services**. Kliknite gumb **Next**.
11. Prikazuje se ekran **Select role services**. Ostavite predefinirane opcije i kliknite gumb **Next**.
12. Prikazuje se ekran sa sažetkom odabranih opcija. Kliknite gumb **Install** i pričekajte kraj instalacije.
13. Kliknite gumb **Close** i zatvorite **Server Manager** konzolu.

S obzirom da je DHCP poslužitelj već pred instaliran na računalu SERVERDC ovdje završavamo sa instalacijom uloga.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

DHCP NAP

Jednostavna verzija NAP-a vezana je za DHCP poslužitelj. Kad god klijent na mreži zatraži postavke od DHCP poslužitelja, NAP će provjeriti zdravlje klijenta i odrediti odgovarajuće TCP/IP postavke. Naša infrastruktura je organizirana na način da je DHCP poslužitelj instaliran na računalu SERVERDC i pred konfiguriran sa DHCP rasponom. Krenimo s konfiguracijom NAP-a.

1. Prikažite ekran **Start** i kliknite na **Network Policy Server**.
2. Prikazuje se konzola **Network Policy Server**. U lijevom oknu kliknite na stavku **NPS (local)**. Zatim u središnjem oknu kliknite na opciju (hiperveza) **Configure NAP**.
3. Prikazuje se ekran **Select Network Connection Method For Use with NAP**. Postavite opcije:
    a. **Network connection method**: odaberite Dynamic Host Configuration Protocol (DHCP)
    b. **Policy name**: upišite OSMIS.
4. Kliknite gumb **Next**.
5. Prikazuje se ekran **Specify NAP Enforcement Servers Running DHCP Server**. Kako je NPS poslužitelj ujedno i DHCP poslužitelj, RADIUS nam nije potreban. Kliknite gumb **Next**.
6. Prikazuje se ekran **Specify DHCP Scopes**. Koristimo samo jedan DHCP raspon stoga nije potrebno definirati NAP filtere za DHCP raspone. Kliknite gumb **Next**.
7. Prikazuje se ekran **Configure Machine Groups**. NAP računala ćemo konfigurirati putem Group Policyja. Ostavite predefinirane opcije i kliknite gumb **Next**.
8. Prikazuje se ekran **Specify a NAP Remediation Server Group and URL.** Ove postavke ćemo konfigurirati kasnije u vježbi. Ostavite predefinirane opcije i kliknite gumb **Next**.
9. Prikazuje se ekran **Define NAP Health Policy**. Ostavite predefinirane opcije i kliknite gumb **Next**.
10. Prikazuje se ekran sa sažetkom postavljenih opcija. Kliknite gumb **Finish**.
11. Ne zatvarajte **Network Policy Server** konzolu!

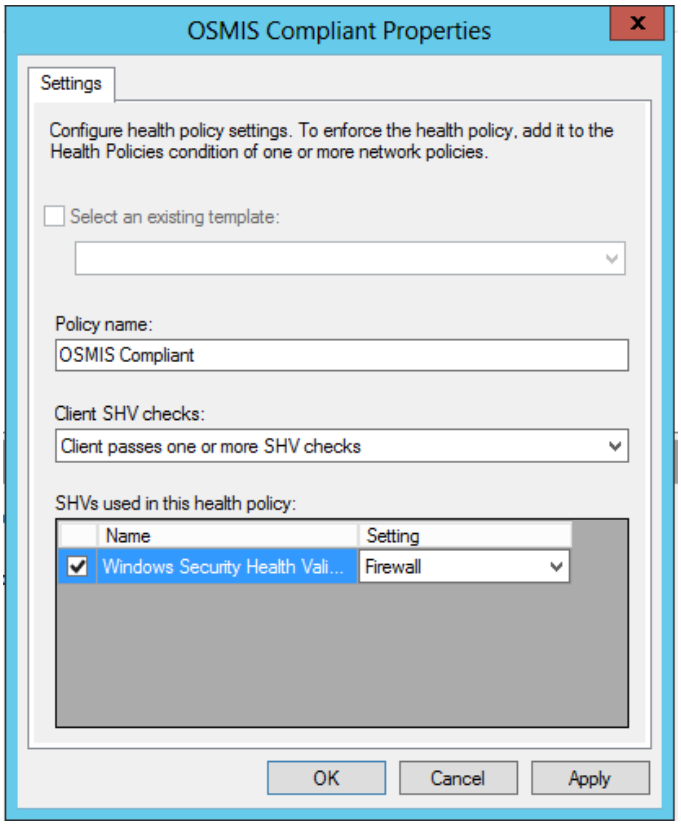
Sada konfiguriramo sigurnosne - zdravstvene uvjete za NAP klijente:

1. U lijevom oknu proširite mapu **Network Access Protection**-> **System Health Validators**-> **Windows Security Health Validator**.
2. Desnim gumbom miša kliknite na stavku **Settings** i iz kontekstualnog izbornika odaberite opciju **New**.
3. Prikazuje se ekran **Configuration Friendly Name**. U polje **Friendly Name** upišite **Firewall** i kliknite gumb **OK.**
4. Prikazuje se ekran **Windows Security Health Validator**. Isključite sve opcije osim one u kategoriji **Firewall Settings**. Kliknite gumb **OK**.
5. Ne zatvarajte **Network Policy Server** konzolu!

Uvjet za vatrozid asocirat ćemo s NAP postavkama:

1. U lijevom oknu proširite mapu **Policies** i kliknite na stavku **Health Policies**.
2. U desnom oknu dvostrukim klikom otvorite svojstva stavke **OSMIS Compliant**.
3. Prikazuje se prozor **OSMIS Compliant Properties**. Postavite opcije:
    a. **Policy name**: ostavite **OSMIS Compliant**
    b. **Client SHV checks**: odaberite opciju **Client passes one or more SHV checks**

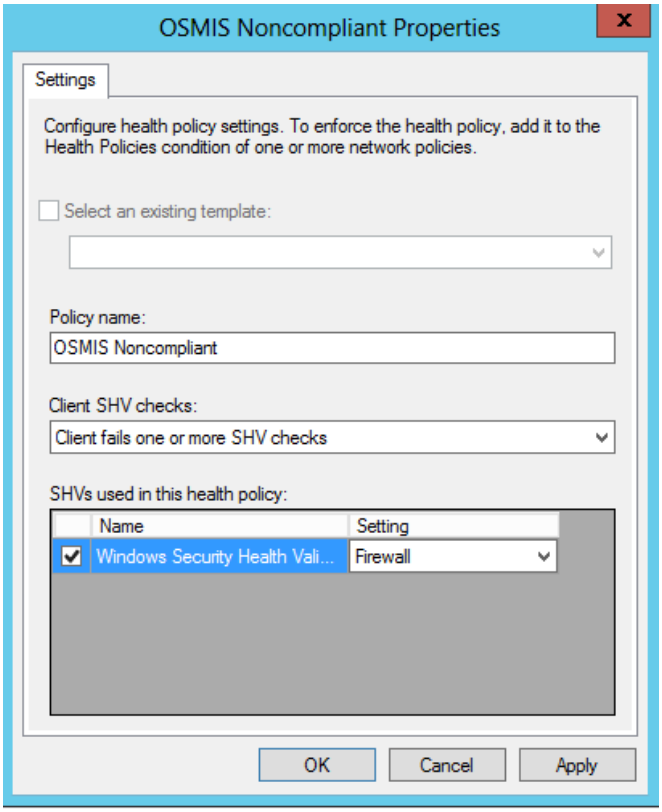
c. **SHVs used in this health policy**: vrijednost u izborniku **Setting** postavite na **Firewall**
d. usporedite svoj ekran s onim na sljedećoj slici.



Slika 1. NAP postavke kad računalo ispunjava zahtjeve

4. Kliknite gumb **OK**.
5. Vraćate se u **Network Policy Server** konzolu.
6. Unutar desnog okna dvostrukim klikom otvorite svojstva stavke **OSMIS Noncompliant.**
7. Prikazuje se prozor **OSMIS Noncompliant Properties**. Postavite opcije:
   a. **Policy name**: ostavite OSMIS Noncompliant
   b. **Client SHV checks**: odaberite opciju Client fails one or more SHV checks
   c. **SHVs used in this health policy**: vrijednost u izborniku Setting postavite na Firewall i
   d. usporedite svoj ekran s onim na slici u nastavku.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 2. NAP postavke kad računalo ne ispunjava zahtjeve

8. Kliknite gumb **OK**.
9. Minimizirajte **Network Policy Server** konzolu.

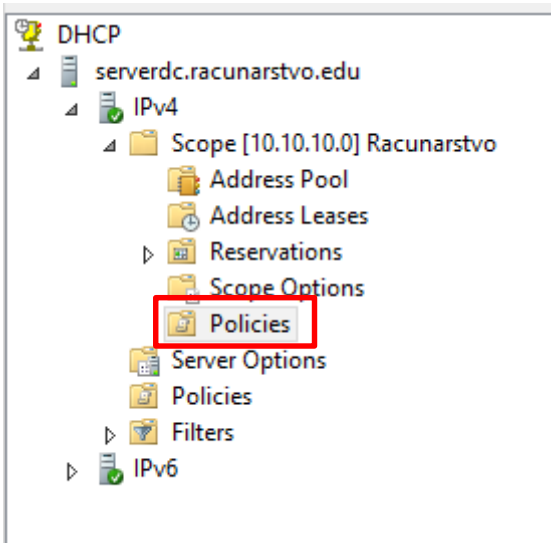
Sada možemo asocirati NAP postavke s DHCP poslužiteljem.

1. Prikažite ekran **Start** i kliknite na **DHCP**.
2. Prikazuje se **DHCP** konzola. Unutar lijevog okna proširite poslužitelj **serverdc.racunarstvo.edu** i zatim proširite stavku **IPv4**.
3. Unutar lijevog okna desnim gumbom miša kliknite na raspon **[10.10.10.0] Racunarstvo** i iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se ekran **Scope [10.10.10.0] Racunarstvo Properties**. Kliknite na karticu **Network Access Protection**.
5. Postavite opcije:
    a. uključite **Enable for this scope**
    b. uključite **Use custom profile**
    c. u polje **Profile name** upišite **OSMIS**.
6. Kliknite gumb **OK**.
7. Ne zatvarajte **DHCP** konzolu!

Konfiguracija DHCP-a za NAP nije potpuna. Definirat ćemo posebne opcije koje će koristiti izolirani klijenti, kako bi ih lakše separirali:

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

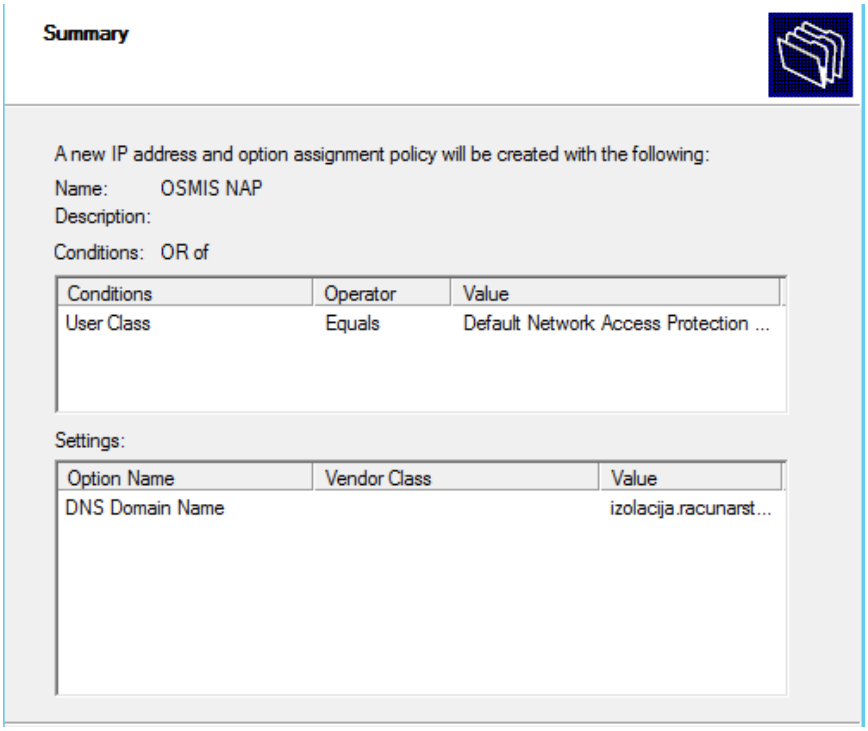
1. Unutar lijevog okna, pod našim DHCP rasponom (provjerite gdje treba kliknuti pomoću donje slike), desnim gumbom miša kliknite na mapu **Policies** i iz kontekstualnog izbornika odaberite opciju **New Policy**.



Slika 3 Definiranje dodatnih opcija

2. Prikazuje se ekran **DHCP Policy Configuration Wizard**. U polje **Policy Name** upišite **OSMIS NAP** i kliknite gumb **Next**.
3. Prikazuje se ekran **Configure Conditions for the policy**. Kliknite gumb **Add**.
4. Prikazuje se ekran **Add/Edit Condition**. Postavite opcije:
    a. Izbornik **Criteria**: odaberite **User class**
    b. Izbornik **Operator**: odaberite **Equals**
    c. Izbornik **Value**: odaberite **Default Network Access Protection Class**
    d. Kliknite gumb **Add**.
5. Kliknite gumb **OK**.
6. Vraćate se na ekran **Configure Conditions for the policy**. Kliknite gumb **Next**.
7. Prikazuje se ekran **Configure settings for the policy**. Označite opciju **No** i kliknite gumb **Next**.
8. Prikazuje se ekran **Configure settings for the policy**. Označite opciju **015 DNS Domain Name**.
9. U polje **String name** upišite **izolacija.racunarstvo.edu** i kliknite gumb **Next**.
10. Prikazuje se ekran sa sažetkom odabranih opcija. Usporedite izgled svog ekrana s onime na sljedećoj slici.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 4 Postavke DHCP NAP izolacije

11. Kliknite gumb **Finish**.
12. Minimizirajte **DHCP** konzolu.

NAP postavke moramo preko Group Policyja povezati s računalima. GP objekt postavljamo na organizacijsku jedinicu **Racunala**. Budući da ta organizacijska jedinica sadržava i poslužitelj SERVER1, primijenit ćemo sigurnosni filtar (sjetite se kolegija AOS) na grupu **NAP_Racunala** koju smo izradili na početku vježbe. Tako smo povezali NAP postavke samo s računalima u grupi NAP_Racunala, a ne sa svim računalima unutar organizacijske jedinice. Jednako ćemo tako u ovom koraku konfigurirati i tekst poruke koju će NAP servis prikazati korisnicima čija računala ne zadovoljavaju sigurnosne kriterije.

1. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
2. Prikazuje se **Group Policy Management** konzola. U lijevom oknu proširite mape **forest: racunarstvo. edu** i **Domains** i na kraju proširite domenu **racunarstvo.edu**.
3. Unutar lijevog okna desnim gumbom miša kliknite na organizacijsku jedinicu **Racunala** i iz kontekstualnog izbornika odaberite opciju **Create a GPO in this domain, and Link it here...**
4. Prikazuje se **New GPO** prozor. U polje **Name** upišite **NAP_DHCP** i kliknite gumb **OK**.
5. U lijevom oknu desnim gumbom miša kliknite na GPO **NAP_DHCP** i iz kontekstualnog izbornika odaberite opciju **Edit**.
6. Prikazuje se **Group Policy Management Editor** konzola. Proširite mapu **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **Network Access Protection**-> **NAP Client Configuration.**
7. U lijevom oknu kliknite na stavku **Enforcement Clients**.
8. U desnom oknu desnim gumbom miša kliknite na stavku **DHCP Quarantine Enforcement Client** te iz kontekstualnog izbornika odaberite opciju **Enable**.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

9. U lijevom oknu kliknite na **User Interface Settings**. Zatim u desnom oknu dvostrukim klikom otvorite stavku **User Interface**.
10. Prikazuje se **User Interface Properties** prozor. Popunite podatke:
    a. **Title**: Obavijest administratora
    b. **Description**: U tijeku je konfiguracija vašeg računala
11. Kliknite gumb **OK**.
12. Zatvorite **Group Policy Management Editor** konzolu.
13. Prikažite se u **Group Policy Management konzolu**.
14. U lijevom oknu označite GPO **NAP_DHCP**. U desnom oknu u kategoriji **Security Filtering** označite grupu **Authenticated User** i kliknite gumb **Remove**.
15. Prikazuje se prozor s potvrdom uklanjanja grupe. Kliknite gumb **OK**.
16. U istoj kategoriji kliknite gumb **Add**.
17. Otvara se ekran za odabir objekata. U polje **Enter the object names to select** upišite **NAP_Racunala** i kliknite gumb **OK**.
18. Zatvorite **Group Policy Management** konzolu.
19. Prikažite ekran **Start**, upišite **`cmd`** i pritisnite tipku **Enter**.
20. Prikazuje se **Command Prompt** prozor. Upišite naredbu **`gpupdate`**
21. Upišite naredbu **`Exit`**

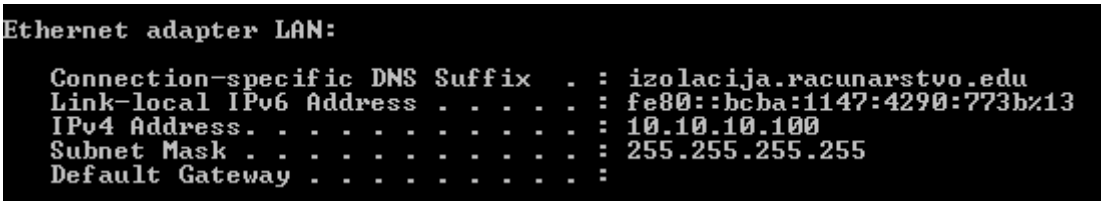
GP objekt je stvoren. Poslije ćemo ga doraditi, ali za sada je konfiguracija dovoljna za isprobavanje DHCP NAP-a.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Testiranje DHCP NAP-a

Podsjetimo se, na početku vježbe smo na CLI1 računalu isključili Windows Firewall i postavili DHCP postavke na TCP/IP konfiguraciji. Sada možemo provjeriti NAP postavke na klijentima koji ne ispunjavaju zdravstvene uvjete:

1. Pokrenite virtualno računalo **CLI1** i prijavite se kao **RACUNARSTVO\admin1** s lozinkom **Pa$$w0rd**.
2. Prikažite ekran **Start** i upišite **cmd**
3. Desnim gumbom miša kliknite na **Command Prompt** i iz trake na dnu ekrana kliknite gumb **Run as administrator**.
4. Prikazuje se **UAC** prozor. Kliknite gumb **Yes**.
5. Prikazuje se **Command Prompt** prozor. Upišite naredbu **ipconfig**
6. Proučite ispis naredbe. Na prvi se pogled postavke ne razlikuju (osim DNS sufiksa) od onih koje smo konfigurirali na DHCP opsegu. Ipak, obratite pozornost na mrežnu masku, kao što prikazuje slika:



Slika 5. TCP/IP postavke računala CLI1

Na DHCP rasponu definirali smo Default Gateway 10.10.10.2 i mrežnu masku 255.255.255.0. Računalo CLI1 dobilo je neispravnu mrežnu masku (odnosno, IP adresu bez klase), a Default Gateway adresu uopće nije dobilo. Prema svemu sudeći, računalo CLI1 izolirano je od ostatka mreže.

7. Upišite naredbu **ping serverdc**
8. Naredba će vratiti odgovor putem **IPv6** protokola.

Na njemu nismo implementirali NAP stoga računalo nije ni stavljenu u izolaciju. Isključimo IPv6 protokol:

9. Upišite naredbu **ncpa.cpl**
10. Prikazuje se prozor **Network Connections** s popisom mrežnih adaptera.
11. Desnim gumbom miša kliknite na adapter **LAN** i iz kontekstualnog izbornika odaberite opciju **Properties**.
12. Prikazuje se ekran **LAN Properties**. Isključite opciju **Internet Protocol Version 6 (TCP/IPv6)** i kliknite gumb **OK**.
13. Zatvorite **Network Connections** prozor.
14. Prikažite **Command Prompt** prozor.
15. Upišite naredbu **ping serverdc**
16. Naredba će ispisati grešku.
17. Ne zatvarajte **Command Prompt**!

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Možemo zaključiti da NAP mehanizam funkcionira u skladu sa uvodnim dijelom vježbe. Vatrozid je isključen i računalo je izolirano. Nameće se zaključak da će uključenje vatrozida računalo CLI1 ukloniti iz izolacije. Provjerimo:

1. Upišite naredbu **`netsh advfirewall set allprofiles state on`**
2. Naredba mora ispisati status **OK**.
3. Upišite naredbu **`ipconfig –release`**
4. Upišite naredbu **`ipconfig –renew`**

Računalo je opet stavljeno u izolaciju. TCP/IP postavke su identične onima na Slika 5. TCP/IP postavke računala CLI1. Pokušajmo otkriti zašto je računalo još uvijek u izolaciji pregledom zapisa u NAP logu.

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite ekran **Start**, upišite **Event** i pritisnite tipku **Enter**.
3. Prikazuje se konzola **Event Viewer**. U lijevom oknu proširite **Custom Views**-> **Server Roles** i kliknite na **Network Policy and Access Services**.
4. Osvježite prikaz konzole pomoću tipke **F5**.
5. U desnom oknu dvostrukim klikom otvorite događaj s oznakom **6276** u stupcu **Event ID**.
6. Pročitajte nekoliko prvih redaka (pronađite informaciju o tome što se dogodilo s računalom CLI1).
7. Zatvorite **Event Viewer** konzolu.

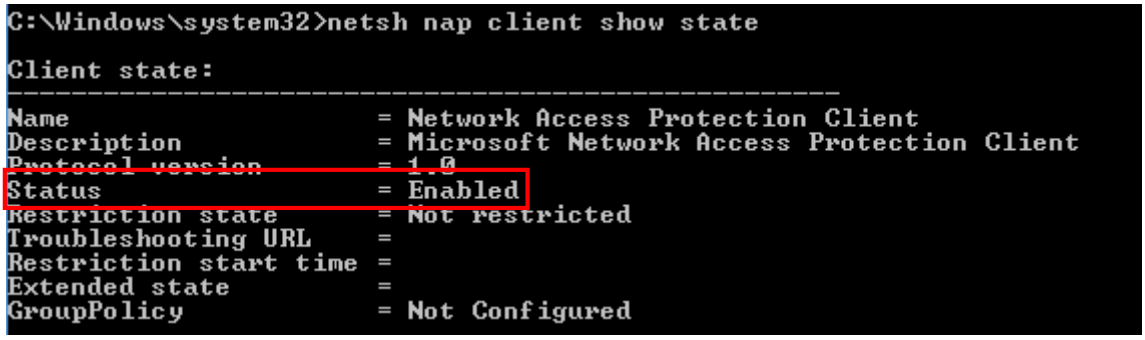
Računalo nije stavljeno u izolaciju zbog isključenog vatrozida nego jer je proglašeno nekompatibilnim sa NAP-om. Iako Windows 8 (i 7) operacijski sustavi podržavaju NAP mehanizam, za njegovo funkcioniranje potrebno je uključiti pripadajući klijentski servis.

NAP klijentski servis

Klijentski NAP servis predefinirano je isključen, a namijenjen je automatskom uključenju sigurnosnih komponenti računala koje zahtijevaju NAP kriteriji, te slanju zdravstvenog stanja računala NPS poslužitelju. Također, tekst koji smo konfigurirali preko Group Policyja se ne prikazuje se jer je vezan za isti servis. Uključit ćemo ga i vidjeti hoćemo li dobiti punu NAP funkcionalnost.

1. Prebacite se na računalo **CLI1**.
2. Prikažite **Command Prompt**.
3. Upišite naredbu **`services.msc`**
4. Prikazuje se **Services** konzola. U desnom oknu pronađite servis **Network Access Protection Agent**.
5. U desnom oknu desnim gumbom miša kliknite na servis **Network Access Protection Agent** te iz kontekstualnog izbornika odaberite opciju **Start**.
6. Pričekajte dok se servis ne pokrene.
7. Minimizirajte **Services** konzolu.
8. Prikažite **Command Prompt**.
9. Upišite naredbu **`netsh nap client show state`**
10. Naredba ispisuje stanje NAP klijentskog servisa. Pronađite redak **Status** i uvjerite se da ima oznaku **Enabled**, kao što prikazuje sljedeća slika.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr



Slika 6. NAP klijentski servis je aktivan

Provjerimo hoće li nas sada NAP staviti u izolaciju:

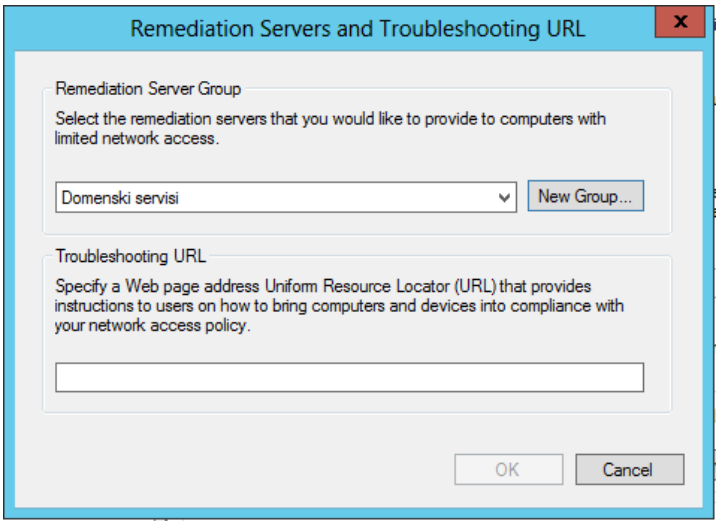
11. Upišite naredbu **`ipconfig –release`**
12. Upišite naredbu **`ipconfig -renew`**
13. Ne zatvarajte **Command Prompt**!

Računalo je još uvijek u izolaciji jer ne može kontaktirati NPS poslužitelj, a samim time niti dojaviti promjenu zdravstvenog stanja. Konfiguracija NAP-a stoga nije završena. Nastavljamo sa konfiguracijom nužnih resursa.

Pristup nužnim resursima

Računalo CLI1 ispunjava zdravstvene uvjete za puni pristup mreži, ali to ne uspijevamo postići. Konfiguraciju nastavljamo u NPS konzoli. Za početak, dopustimo mu pristup (i svim zdravstveno neispravnim računalima) domenskom kontroleru, a koji je ujedno i NPS poslužitelj.

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite **Network Policy Server** konzolu.
3. U lijevom oknu proširite **Policies**-> **Network Policies**.
4. U središnjem oknu dvostrukim klikom otvorite postavke stavke **OSMIS Non NAP-Capable**.
5. Prikazuje se ekran **OSMIS Non NAP-Capable Properties**. Kliknite na karticu **Settings** i zatim u lijevom oknu označite **NAP Enforcement**.
6. U središnjem oknu kliknite gumb **Configure**.
7. Prikazuje se **Remediation Servers and Troubleshooting URL** prozor. Kliknite gumb **New Group**.
8. Prikazuje se **New Remediations Server Group** prozor. Popunite podatke:
    a. **Group Name**: upišite **Domenski servisi**
    b. kliknite gumb **Add**
    c. prikazuje se **Add New Server** prozor. Popunite podatke:
        i. **Friendly name**: upišite **SERVERDC**
        ii. **IP address or DNS name**: upišite **SERVERDC** i kliknite gumb **Resolve**
        iii. U kategoriji IP address označite IPv4 adresu 10.10.10.1
        iv. Kliknite gumb **OK**
    d. Vraćate se na **New Remediation Server Group** prozor. Kliknite gumb **OK**
    e. Vraćate se na ekran **Remediation Servers and Troubleshooting URL**. Provjerite je li u izborniku odabrana stavka **Domenski servisi**, kako prikazuje slika:



Slika 7. Grupa nužnih servisa

    f. kliknite gumb **OK**.
9. Vraćate se na ekran **OSMIS Non NAP-Capable Properties.** Kliknite gumb **OK**.
10. Vraćate se u **Network Policy Server** konzolu.

Istim ćemo postupkom dodati nužne servise i drugom pravilu.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

1. U središnjem oknu dvostrukim klikom otvorite postavke **OSMIS Noncompliant** stavke.
2. Prikazuje se ekran **OSMIS Noncompliant Properties**. Kliknite na karticu **Settings** i zatim u lijevom oknu označite **NAP Enforcement**.
3. U središnjem oknu kliknite gumb **Configure**.
4. Prikazuje se **Remediation Servers and Troubleshooting URL** prozor. Iz izbornika odaberite stavku **Domenski servisi** i kliknite gumb **OK**.
5. Vraćate se na ekran **OSMIS Noncompliant Properties.** Kliknite gumb **OK**.
6. Minimizirajte **Network Policy Server** konzolu.

Provjerimo kakva je promjena na računalu CLI1.

1. Prebacite se na računalo **CLI1**.
2. Prikažite **Command Prompt**.
3. Upišite naredbu **ipconfig –renew**.
4. Na prvi se pogled ništa nije promijenilo. Ipak, upišite naredbu **`ping 10.10.10.1`**.
5. Računalo SERVERDC odgovara na ping zahtjev (ali ne preko pinga DNS imena, jedino ako ste ga „pingali“ preko IP adrese). To je jedino računalo kojem možete pristupiti s računala CLI1. Za provjeru probajte „pingati“ računalo SERVER1, tj. IP adresu 10.10.10.2.
6. Ne zatvarakte **Command Prompt**!

U nastavku vježbe vidjet ćemo kako automatski uključiti sve tražene komponente na klijentskim računalima kako bismo udovoljili NAP zahtjevima, te kako bi dotični funkcionirao transparentno za korisnika.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Automatsko usklađivanje s NAP zahtjevima

Ideja NAP-a nije trajna izolacija korisnika, nego privremena. Drugim riječima, klijenta privremeno smjestimo u izolirani dio mreže dok ne ispuni sve sigurnosne zahtjeve za puni pristup. Najprije ćemo privremeno onemogućiti NAP kako bi klijent mogao primijeniti nove GP postavke.

1. Prebacite se na računalo **SERVERDC**.
2. Prikažite **DHCP** konzolu.
3. Unutar lijevog okna desnim gumbom miša kliknite na raspon **[10.10.10.0] Racunarstvo** i iz kontekstualnog izbornika odaberite opciju **Properties**.
4. Prikazuje se ekran **Scope [10.10.10.0] Racunarstvo Properties**. Kliknite na karticu **Network Access Protection**.
5. Uključite **Use default Network Access Protection profile** i kliknite gumb **Apply**.
6. Uključite opciju **Disable for this scope** i kliknite gumb **Apply** (nije greška u koracima, zaista morate najprije uključiti predefinirani profil pa tek onda isključiti NAP).
7. Ne zatvarajte ovaj prozor! Trebat ćemo ga za nekoliko trenutaka.

Sada možemo preko Group Policyja konfigurirati NAP klijentski servis koji će automatski usuglasiti računalo s NAP stavkama, ali i prikazati poruku koju smo u prethodnoj cjelini konfigurirali za prikaz korisnicima. Iako smo u prethodnoj cjelini taj servis uključili na računalu CLI1, to nije dovoljno. NAP će provjeravati veliki broj računala u produkcijskom okruženju i svako od njih mora imati uključen pripadajući servis.

1. Prikažite ekran **Start** i kliknite na **Group Policy Management**.
2. Prikazuje se **Group Policy Management** konzola. U lijevom oknu desnim gumbom miša kliknite na GPO **NAP_DHCP** i iz kontekstualnog izbornika odaberite opciju **Edit**.
3. Prikazuje se **Group Policy Management Editor** konzola. Proširite mapu **Computer Configuration**-> **Policies**-> **Windows Settings**-> **Security Settings**-> **System Services**.
4. U desnom oknu dvostrukim klikom otvorite servis **Network Access Protection Agent**.
5. Prikazuje se ekran **Network Access Protection Agent Properties**. Uključite opciju **Define this policy setting** i zatim kliknite stavku **Automatic**.
6. Kliknite gumb **OK** i zatvorite sve otvorene prozore na računalu **SERVERDC**.

Ažurirajmo GPO postavke na računalu CLI1:

1. Prebacite se na računalo **CLI1**.
2. Prikažite **Command Prompt** i upišite naredbu **`ipconfig –renew`**.
3. Upišite naredbu **ipconfig**. Uvjerite se da je DNS sufiks sada **racunarstvo.edu**.
4. Upišite naredbu **`gpupdate /force`**.
5. Na pitanje o odjavi korisnika odgovorite s **Y**.
6. Prijavite se na računalo **CLI1** kao **RACUNARSTVO\admin1** s lozinkom **Pa$$w0rd.**
7. Prikažite ekran **Start** i upišite **`cmd`**
8. Desnim gumbom miša kliknite na **Command Prompt** i iz trake na dnu ekrana kliknite gumb **Run as administrator**.
9. Prikazuje se **UAC** prozor. Kliknite gumb **Yes**.
10. Prikazuje se **Command Prompt** prozor. Ne zatvarajte ga!

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Zatim ponovno uključujemo DHCP NAP.

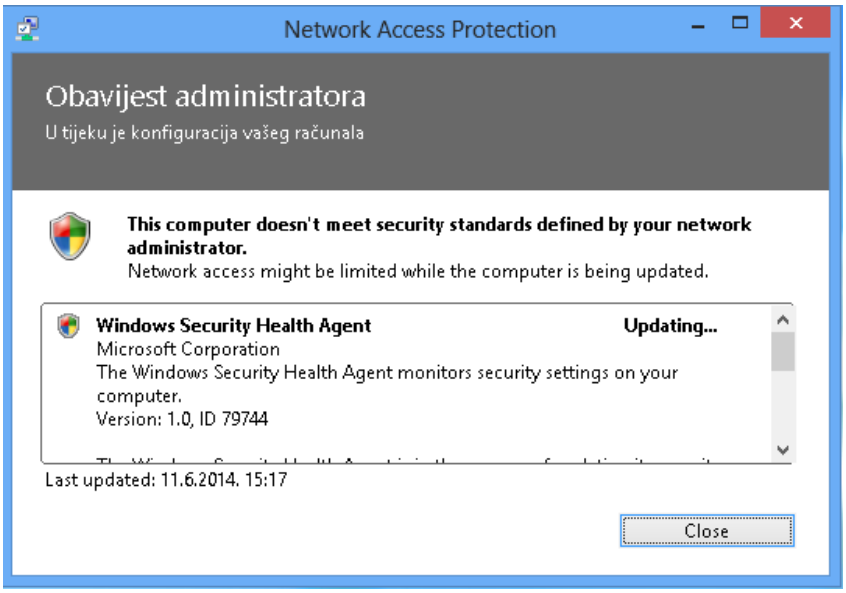
1. Prebacite se na računalo **SERVERDC**.
2. Prozor s NAP postavkama DHCP opsega je prikazan. Kliknite opciju **Enable for this scope**.
3. Kliknite na opciju **Use custom profile** i u polje **Profile name** upišite **OSMIS**.
4. Kliknite gumb **OK**.

Pogledajmo kako se ove promjene pokazuju na računalu CLI1.

1. Prebacite se na računalo **CLI1**.
2. Upišite naredbu **`netsh advfirewall set allprofiles state off`**
3. Upišite naredbu **`ipconfig –renew`**.
4. Nakon sekundu-dvije u obavijesnoj se traci prikazuje **NAP obavijest** kao što je prikazano na slici u nastavku. Kliknite na nju. Ako niste stigli, ponovite prethodna dva koraka i obavijest će se ponovno pojaviti.

Slika 8. Obavijest o NAP konfiguraciji

5. Kad ste kliknuli na obavijest, prikazuju se informacije o postupku usklađivanja računala sigurnosnim zahtjevima NAP-a. Uočite i tekst koji smo definirali preko Group Policyja, kao na slici u nastavku.
6. Kliknite gumb **Close**.



Slika 9. NAP obavijest

Ovime završava današnja vježba. Isključite sva virtualna računala.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo I Ilica 242 I 10000 Zagreb I Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 I matični broj: 2412926 I IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 I fax. +385 (0)1 2305 004 I info@racunarstvo.hr I www.racunarstvo.hr

Rezultat vježbe

Rezultat današnje vježbe jesu izmjene na virtualnim računalima, i to redom:

1. **SERVERDC** izmjene:
    a. grupa NAP_Racunala s računalom CLI1
    b. GP objekt DHCP_NAP s filtriranjem na grupu NAP_Racunala. GP objekt sadržava postavke NAP klijentskog servisa i konfiguraciju teksta poruke koji se prikazuje u slučaju neispravnih zdravstvenih uvjeta.
2. CLI1 izmjene:
    a. TCP/IP postavke promijenjene na automatske
    b. Pokrenut NAP klijentski servis

Današnja vježba ne zahtijeva *snapshot*.

Visoko učilište Algebra - visoka škola za primijenjeno računarstvo | Ilica 242 | 10000 Zagreb | Hrvatska
Upisano kod trgovačkog suda u Zagrebu pod MBS: 080664742
Poslovna banka: Zagrebačka banka d.d. Trg bana Josipa Jelačića 10, 10000 Zagreb, Hrvatska
OIB: 14575159920 | matični broj: 2412926 | IBAN: HR7523600001102036972
tel. +385 (0)1 2222 182 | fax. +385 (0)1 2305 004 | info@racunarstvo.hr | www.racunarstvo.hr

Što treba znati nakon ove vježbe?

1. Konfigurirati DHCP NAP
2. Omogućiti izoliranim klijentima pristup određenim resursima (npr. nekom poslužitelju)
3. Konfigurirati automatsko usklađivanje s NAP standardima

Dodatna literatura

- Technet scenariji za DHCP NAP:

http://technet.microsoft.com/en-us/library/dd125379(v=ws.10).aspx

- Opis Windows Security Health validatora:

http://technet.microsoft.com/en-us/library/cc731260.aspx

- Neke česte pogreške kod NAP-a

http://technet.microsoft.com/en-us/library/dd348494(v=ws.10).aspx