FAKULTA RIADENIA A INFORMATIKY, ŽILINSKÁ UNIVERZITA V ŽILINE

DOKUMENTÁCIA K RIEŠENIU MALEJ FIREMNEJ SIETE

SIEŤOVÉ OPERAČNÉ SYSTÉMY

5ZKS11, Skupina 1
Andrej Kováč
Tomáš Pikna
Stanislav Rusnák
Pavol Tuka

2015

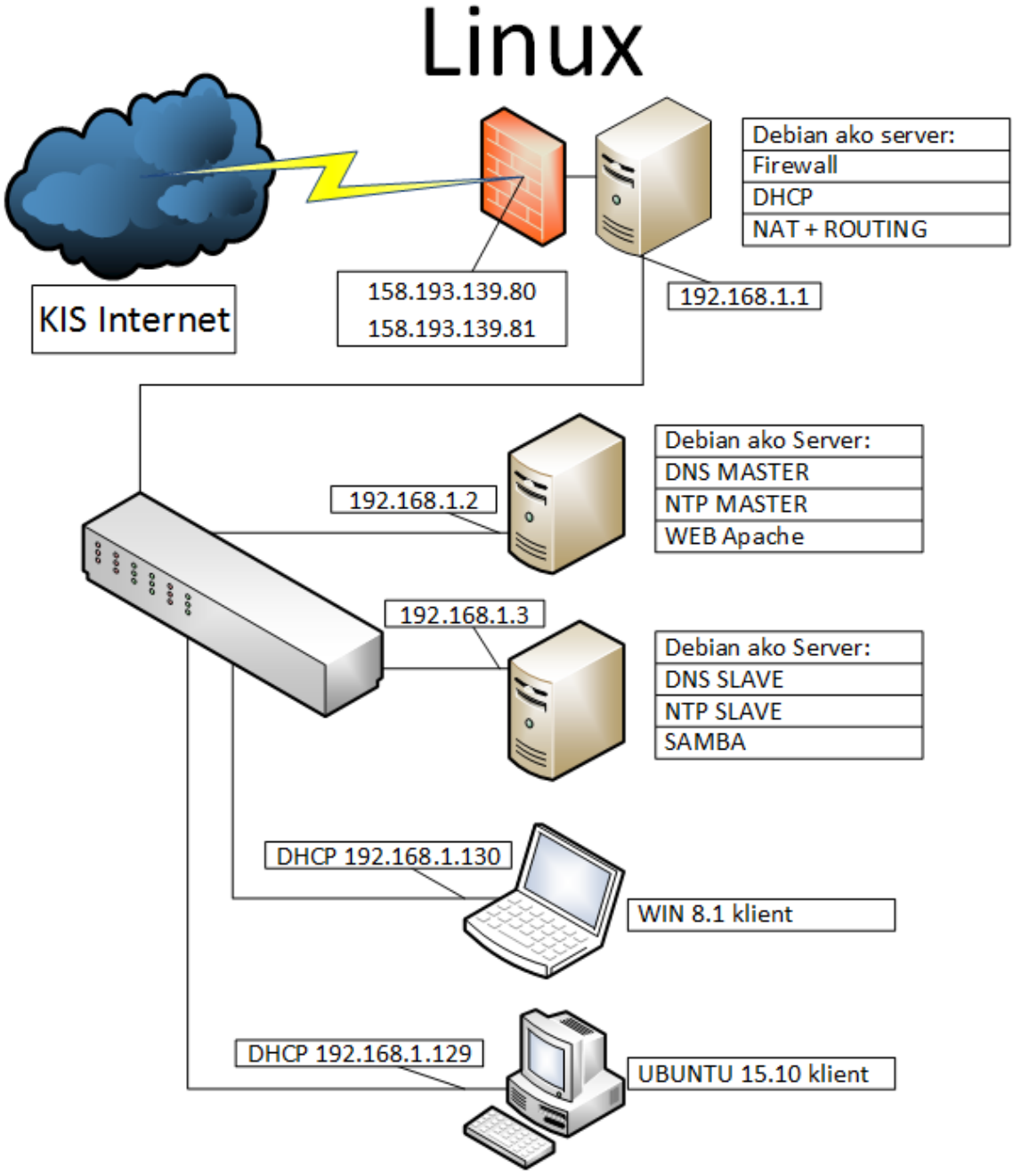
Obsah

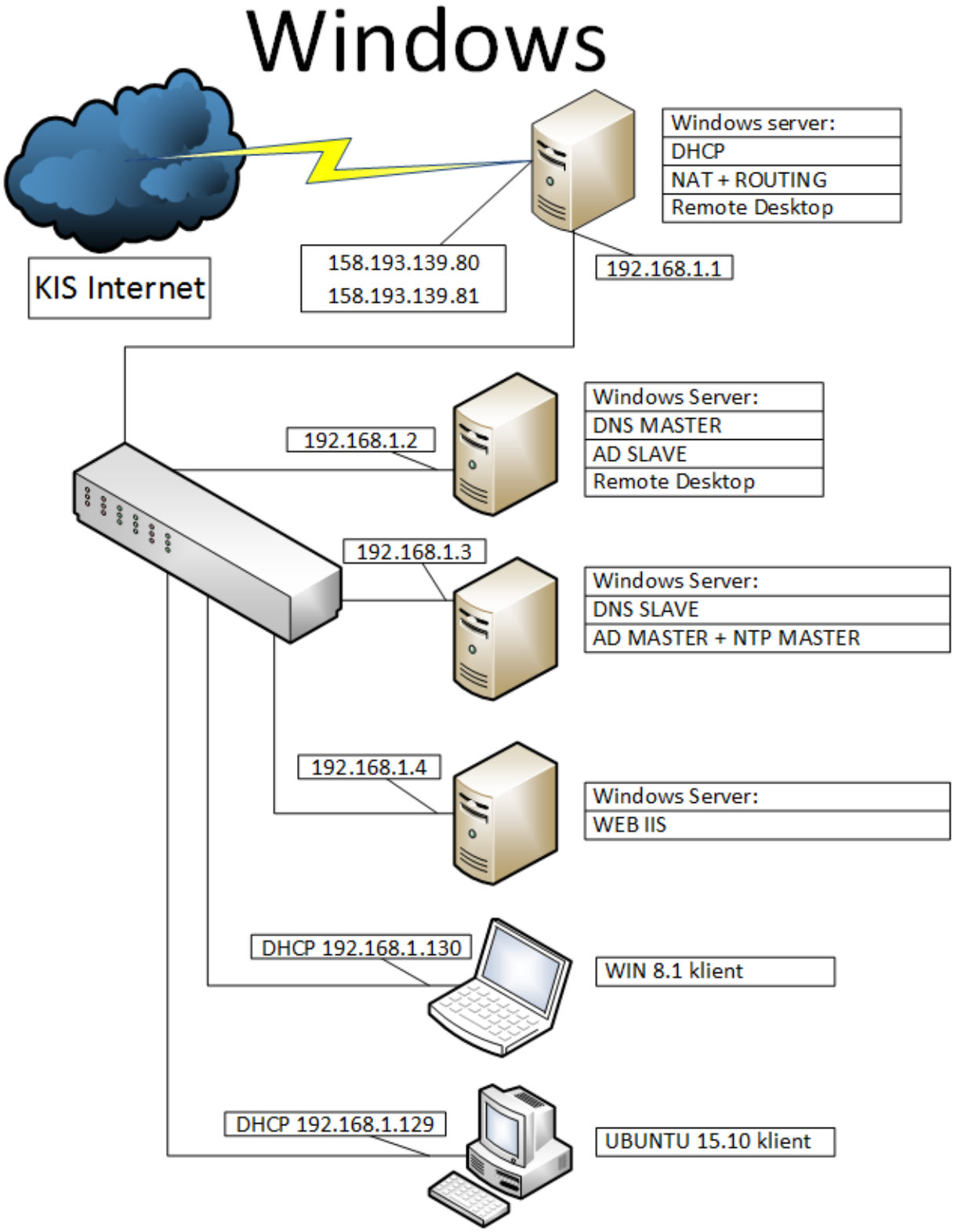
Zadanie

Navrhnite sieť pre malú firmu, v ktorej budú spustené nasledovné služby:

- Firewall (IP Tables)
- DHCP server
- DNS (Bind)
- NTP
- Web (Apache / IIS)
- Zdieľanie súborov (Samba / Active Directory)

Základná topológia




Windows
KIS Internet
158.193.139.80
158.193.139.81
Windows server:
DHCP
NAT + ROUTING
Remote Desktop
192.168.1.1
192.168.1.2
Windows Server:
DNS MASTER
AD SLAVE
Remote Desktop
192.168.1.3
Windows Server:
DNS SLAVE
AD MASTER + NTP MASTER
192.168.1.4
Windows Server:
WEB IIS
DHCP 192.168.1.130
WIN 8.1 klient
DHCP 192.168.1.129
UBUNTU 15.10 klient

Konfigurácia portov serverov

Konfigurácia portov serverov bola jednoduchá, keďže väčšina serverov mala nastavenú len statickú IP adresu. Podľa zadania bolo potrebné mať nastavené dve verejné IP adresy na jednom sieťovom rozhraní servera pripojeného k internetu priamo. Keďže sme zadanie spracovávali na dvoch rôznych OS, tak aj toto nastavenie bolo rôzne.

LINUX

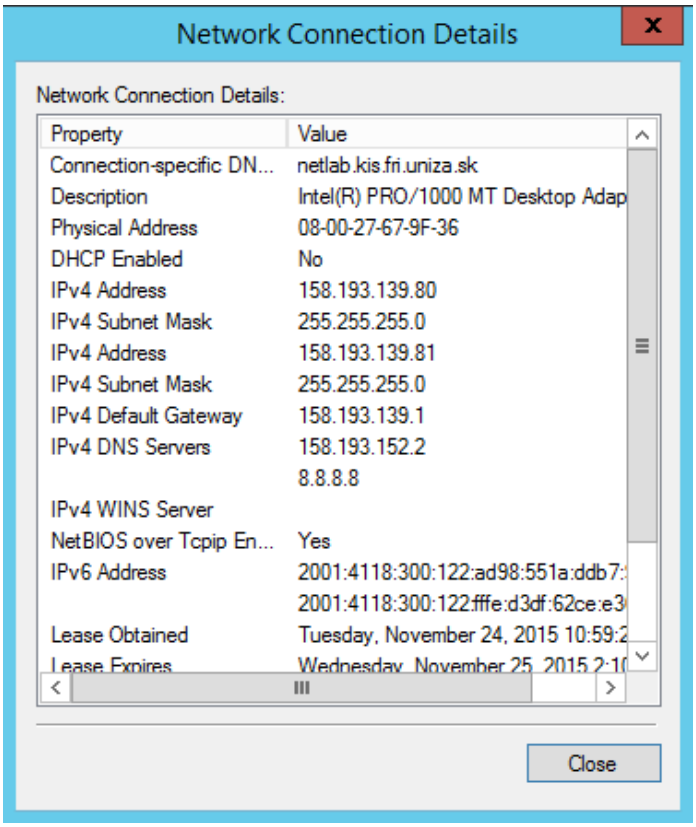
Adaptér sme rozdelili na dva virtuálne adaptéry eth0 a eth0:1. Na každom sme nastavili inú IP adresu ale rovnakú masku a bránu.

/etc/network/interfaces

```
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback
allow-hotplug eth0
iface eth0 inet6 auto
allow-hotplug eth1

iface eth0 inet static
address 158.193.139.80
netmask 255.255.255.0
gateway 158.193.139.1
network 158.193.139.0
broadcast 158.193.139.255

iface eth0:1 inet static
address 158.193.139.81
netmask 255.255.255.0
gateway 158.193.139.1
network 158.193.139.0
broadcast 158.193.139.255

iface eth1 inet static
address 192.168.1.1
netmask 255.255.255.0
broadcast 192.168.1.255
network 192.168.1.0
```

WINDOWS SERVER

Windows ako operačný systém podporoval možnosť použitia viacerých statických IP adries na jednom sieťovom adaptéri, na ktorý sme nastavili dané adresy. Konfigurácia adaptéra vyzerá nasledovne:



DHCP

LINUX

Inštaláciu služby DHCP sme zabezpečili príkazom:

apt-get install isc-dhcp-server

Ďalšie príkazy ktorými sme službu spúštali a zastavovali sú:

service isc-dhcp-server stop
service isc-dhcp-server start

V súbore */etc/dhcp/dhcpd.conf* sme nastavili DNS servery a rozsah adries, ktoré bude DHCP prideľovať klientom:

```
option domain-name "SOSRANO1";
option domain-name-servers 192.168.1.2 192.168.1.3;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.129 192.168.1.254;
 option routers 192.168.1.1;
}
```

Na jednom zo serverov sa vyskytol problém, že po určitom čase sa staticky nastavená IP adresa zmenila. Riešením bolo vypnutie služby *dhclient* príkazom:

kill PID_PROCESU_DHCLIENT

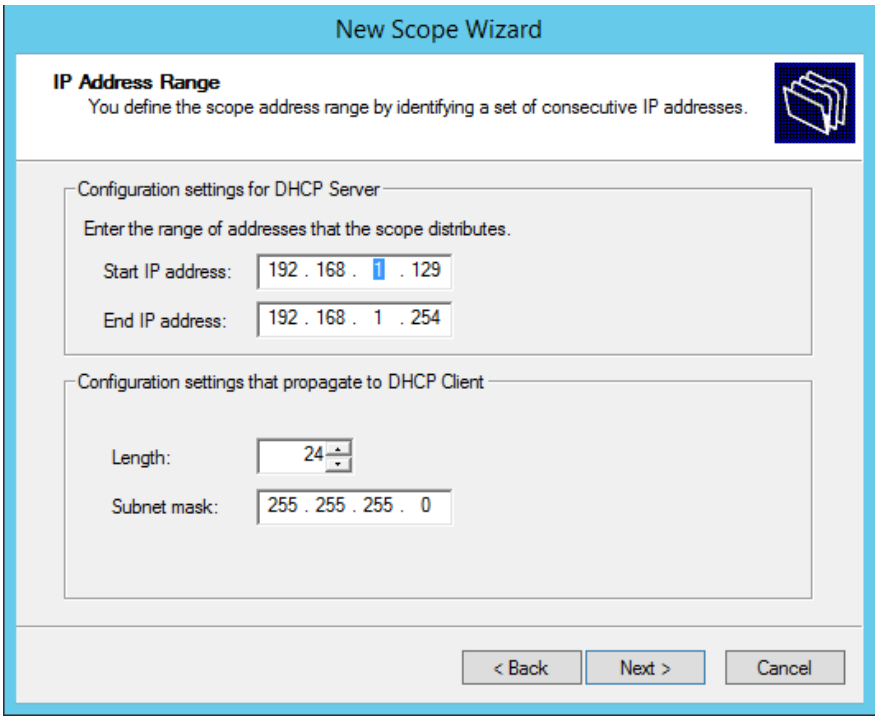
WINDOWS

Inštalácia

Vo windows server managerovi sme cez možnosť *"Add Roles and Features"* pridali DHCP server, potvrdili sme výber služby a naištalovali ju.

Konfigurácia

"Control Panel → Administrative Tools → DHCP"
V ponuke sme rozklikli náš server, v ňom IPv4 a vybrali sme možnosť *"new Scope"* z hornej lišty. Na obrazovke sa zobrazí Install Wizard v ktorom sme zvolili názov pravidla na prideľovanie IP adries, vyberali rozsah IP adries a masku. V našom prípade vyzerala ako na nasledujúcom obrázku.



V ďalšom kroku sme mali možnosť pridať výnimku z predtým zadaného rozsahu, tým sa myslí adresy ktoré prideľovať nebude aj keď sú v rozsahu IP z ktorých má prideľovať. My sme túto možnosť nevyužili, lebo sme mali pevne definované adresy pre klientov a servery. Stačí kliknúť *"Next"*.
Vyberali sme aký dlhý čas si server bude pamätať IP adresy ktoré niekomu pridelil, pre naše potreby stačilo 4 hodiny (dĺžka cvičenia).
V ďalšom kroku sme vybrali možnosť nastaviť DHCP, nastavili sme bránu na „192.168.1.1", pridali sme IP adresy našich DNS serverov, ktoré sú „192.168.1.2" a „192.168.1.3".
Keďže WINS servers nevyužívame tak ďalšie okno týkajúce sa nastavení WINS v DHCP sme preskočili tlačidlom *"Next"* a na poslednom okne inštalátora sme vybrali možnosť aplikovať a spustiť službu.

Vytvorili sme klienta s OS UBUNTU, ktorý po pripojení do siete dostal pridelenú IP adresu z nášho rozsahu.

Konfugurácia prepínača z topológie

1. *sh startup* - ak sa tam vyskytuje, potrebný príkaz : *erase startup*
2. *sh flash* - ak je tam *vlan.dat*, potrebné zmazať príkazom : *delete vlan.dat*
3. *reload*
4. *span mode rapid*

Zadávateľ práce pridal do zadania požiadavku na preverenie možnosti pridať VLAN-y do tejto našej siete. VLAN 10 – servery so statickou adresou VLAN 20 – DHCP klienti
Na prepínači sa porty priradili do daných VLAN.

Zmena nastavenia rozhrania s IP adresou 192.168.1.1. Tento port sme rozdelili na 2 subrozhrania eth1.10 (pre VLAN10) a eth1.20 (pre VLAN20). Postup sme overovali len na Linux serveri a bolo potrebné zmeniť nastavenia rozhraní:

/etc/network/interfaces

Tieto riadky:

```
iface eth1 inet static
address 192.168.1.1
netmask 255.255.255.0
broadcast 192.168.1.255
network 192.168.1.0
```

Sme nahradili týmito:

```
auto eth1.10
iface eth1.10 inet static
address 192.168.1.1
netmask 255.255.255.128
network 192.168.1.0
broadcast 192.168.1.127
vlan_raw_device eth1

auto eth1.20
iface eth1.20 inet static
address 192.168.1.129
netmask 255.255.255.128
network 192.168.1.128
broadcast 192.168.1.255
vlan_raw_device eth1
```

Po vytvorení VLAN bolo potrebné zmeniť nastavenie DHCP servera.

/etc/dhcp/dhcpd.conf

Zmeníme konfiguráciu na:

```
option domain-name "SOSRANO1";
option domain-name-servers 192.168.1.2 192.168.1.3;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.128 netmask 255.255.255.128 {
range 192.168.1.130 192.168.1.254;
option routers 192.168.1.129;
}
```

Firewall a NAT

LINUX

Firewall a NAT sme na OS Linux nastavovali pomocou *iptables*. V postupnom riešení sme mali viaceré verzie. Prvá, určená na testovanie, bola veľmi neefektívna, ale na overenie funkčnosti siete dostačujúca, povolila všetku komunikáciu na všetky porty a nastavené bolo len NAT.
Postupným riešením sme firewall dokončili podľa zadania.

NAT sme na začiatku nastavili len na základný preklad a postupom času sme pridávali statické NAT záznamy na porte 53 pre DNS serveri a na porte 123 pre náš NTP server.

Aby sme každé spustenie Linuxu nemuseli pridávať jednotlivé príkazy IPTABLES tak sme vytvorili samospúšťací script ktorý aplikuje naše FIREWALL a NAT pravidlá pri štarte systému.

/etc/network/iptables_rules.sh

```
################################################################################
# FLUSH ALL RULES IN THE MANGLE, NAT AND FILTER TABLES
################################################################################

iptables -t mangle -F
iptables -t nat    -F
iptables -t filter -F

################################################################################
# DELETE ALL USER-DEFINED (NOT BUILT-IN) CHAINS IN THE TABLES
################################################################################

iptables -t mangle -X
iptables -t nat    -X
iptables -t filter -X

################################################################################
# SET ALL POLICIES FOR ALL BUILT-IN CHAINS TO DROP
################################################################################

iptables -P INPUT   DROP
iptables -P FORWARD DROP

################################################################################
# FW RULES
################################################################################

# OUTPUT

# INPUT

iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A INPUT -p icmp --icmp-type 8 -s 0/0 -d 192.168.1.1 -m state --state
NEW,ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -t filter -A INPUT -p tcp --destination-port 22 -j ACCEPT
```

```
# FORWARD

iptables -t filter -A FORWARD -i eth1 -o eth0 -j ACCEPT      //zo zadania pustiť z dnu smerom von čokoľvek

iptables -t filter -A FORWARD -i eth0 -o eth1 -p icmp -j ACCEPT
iptables -t filter -A FORWARD -i eth0 -o eth1 -m state --state ESTABLISHED,RELATED -j ACCEPT //povolí už vzniknuté spojenia
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --destination-port 53 -j ACCEPT // dns
iptables -t filter -A FORWARD -i eth0 -o eth1 -p udp --destination-port 53 -j ACCEPT // dns
iptables -t filter -A FORWARD -i eth0:1 -o eth1 -p tcp --destination-port 53 -j ACCEPT //dns
iptables -t filter -A FORWARD -i eth0:1 -o eth1 -p udp --destination-port 53 -j ACCEPT //dns
iptables -t filter -A FORWARD -i eth0 -o eth1 -p tcp --destination-port 22 -j ACCEPT //ssh
iptables -t filter -A FORWARD -i eth0 -o eth1 -p udp --destination-port 123 -j ACCEPT //ntp

################################################################################
# NAT
################################################################################

iptables -t nat -A POSTROUTING -o eth0 -j SNAT --to 158.193.139.80

#DNAT
iptables -t nat -A PREROUTING -d 158.193.139.80 -p tcp --dport 53 -j DNAT --to-destination 192.168.1.2:53
iptables -t nat -A PREROUTING -d 158.193.139.81 -p tcp --dport 53 -j DNAT --to-destination 192.168.1.3:53
iptables -t nat -A PREROUTING -d 158.193.139.80 -p udp --dport 53 -j DNAT --to-destination 192.168.1.2:53
iptables -t nat -A PREROUTING -d 158.193.139.81 -p udp --dport 53 -j DNAT --to-destination 192.168.1.3:53

iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 22 -j DNAT --to 192.168.1.2:22
iptables -t nat -A PREROUTING -i eth0:1 -p tcp --dport 22 -j DNAT --to 192.168.1.3:22

iptables -t nat -A PREROUTING -d 158.193.139.80 -p udp --dport 123 -j DNAT --to-destination 192.168.1.2:123

################################################################################
# ENABLE FORWARDING
################################################################################

echo 1 > /proc/sys/net/ipv4/ip_forward
```

WINDOWS

Použitie operačného systému Windows Server 2012 R2 ako firewallu medzi dvomi sieťami (filtrovaním komunikácie medzi dvomi sieťovými kartami - IN, OUT) nie je vhodné. Firewall bol nastavovaný v záložke *Windows Firewall with Advanced Security* (záložky *Inbound* a *Outbound*), lenže daný firewall slúži len pre daný lokálny server. Znamená to, že je schopný filtrovať len komunikáciu určenú preňho a nedokáže filtrovať komunikáciu, ktorá cez neho prechádza. Možnosti a funkcie v záložkách *Network Policy Server, Local Security Policy* taktiež nie sú určené pre firewalling prechádzajúcej komunikácie. Odporúčame použiť

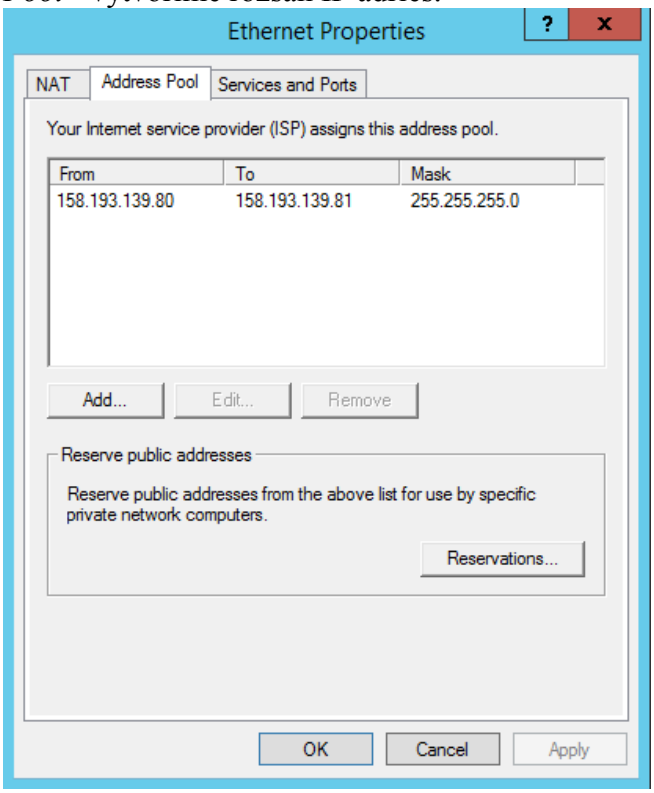
napríklad Debian Firewall, ktorého konfigurácia je uvedená vyššie alebo hardware-ový firewall (Cisco ASA, Juniper, Fortinet …).

Inštalácia NAT

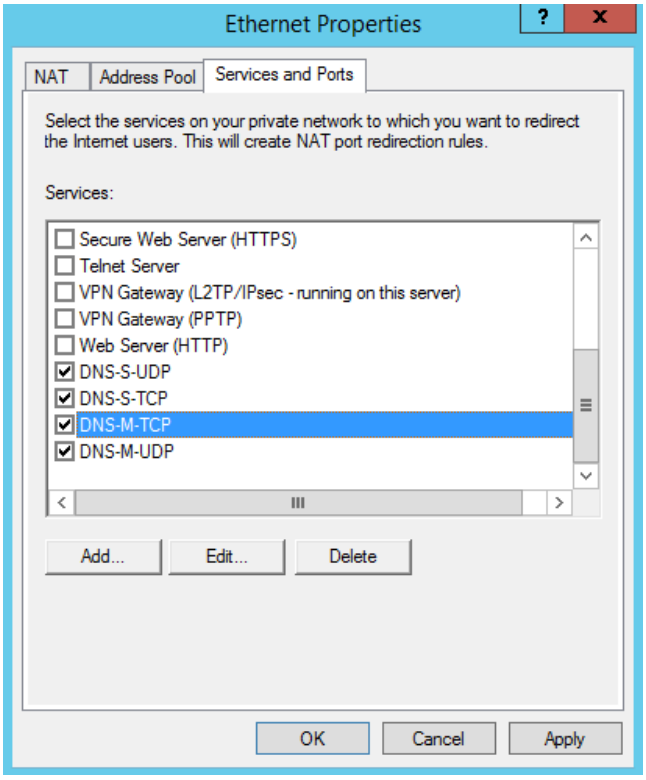
Vo Windows Server Managerovi sme cez možnosť *"Add Roles and Features"* pridali *"Remote Access"*, potvrdili sme výber služby *"Routing"* a nainštalovali ju. Pri inštalácii zvolíme sieťový adaptér, ktorý je pripojený k internetu.
NAT sa spustí a funguje, no je potrebné pridať statické NAT záznamy pre port 53.

Konfigurácia NAT

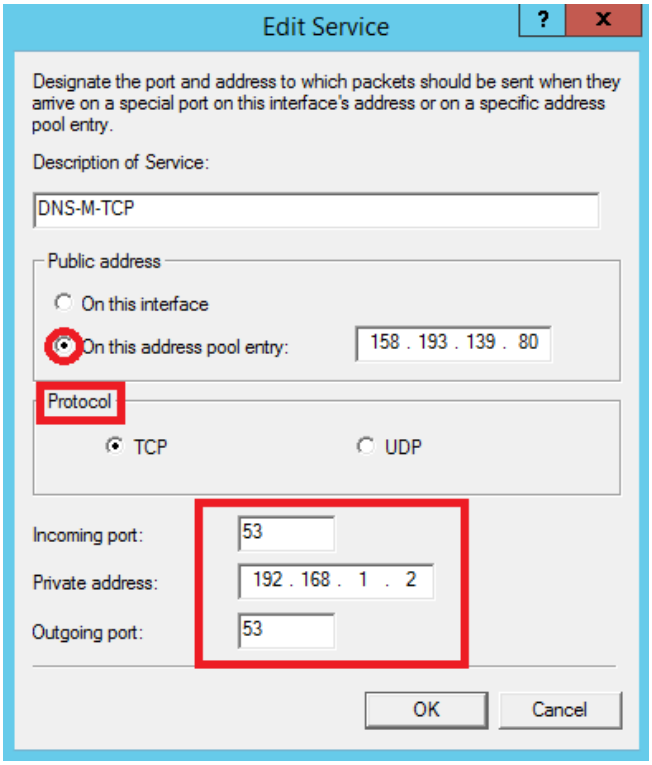
"Control Panel → Administrative Tools → Routing and Remote Access"
Po kliknutí na NAT vyberieme sieťový adaptér pripojený k internetu. V záložke *"Address Pool"* vytvoríme rozsah IP adries.



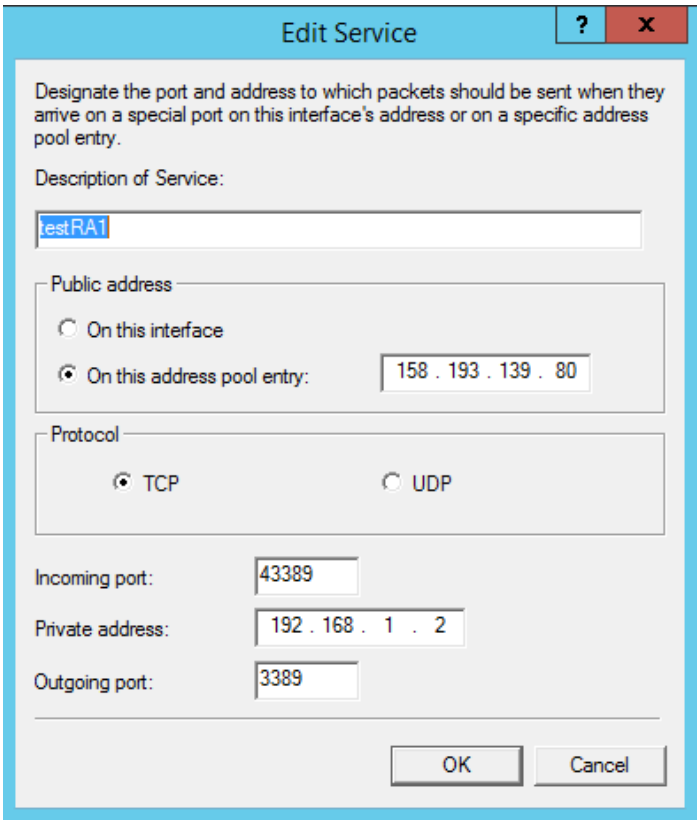
Maska musí mať tvar 255.255.255.0 pre správne fungovanie, ak maska bude mať na poslednom oktete inú hodnotu, v celej sieti padne internet. Pravdepodobne to je spôsobené nastavením sieťového adaptéra, ktorý má dve IP adresy a masku 255.255.255.0.
V karte *"Services and Ports"* musíme pridať 4 nové záznamy NAT pre DNS - Master/Slave - TCP/UDP na porte 53.



Naše záznamy NAT mali takéto nastavenia (červenou sú zvýraznené dôležité nastavenia):



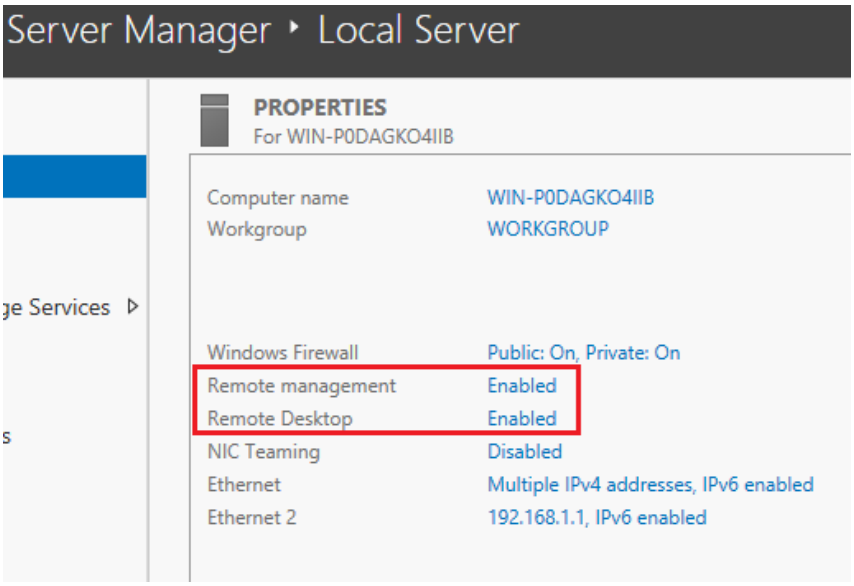
Postupne sme zistili, že treba povoliť statické NAT záznamy pre vzdialený prístup k serverom v sieti, preto sme do NAT pridali takéto pravidlo:



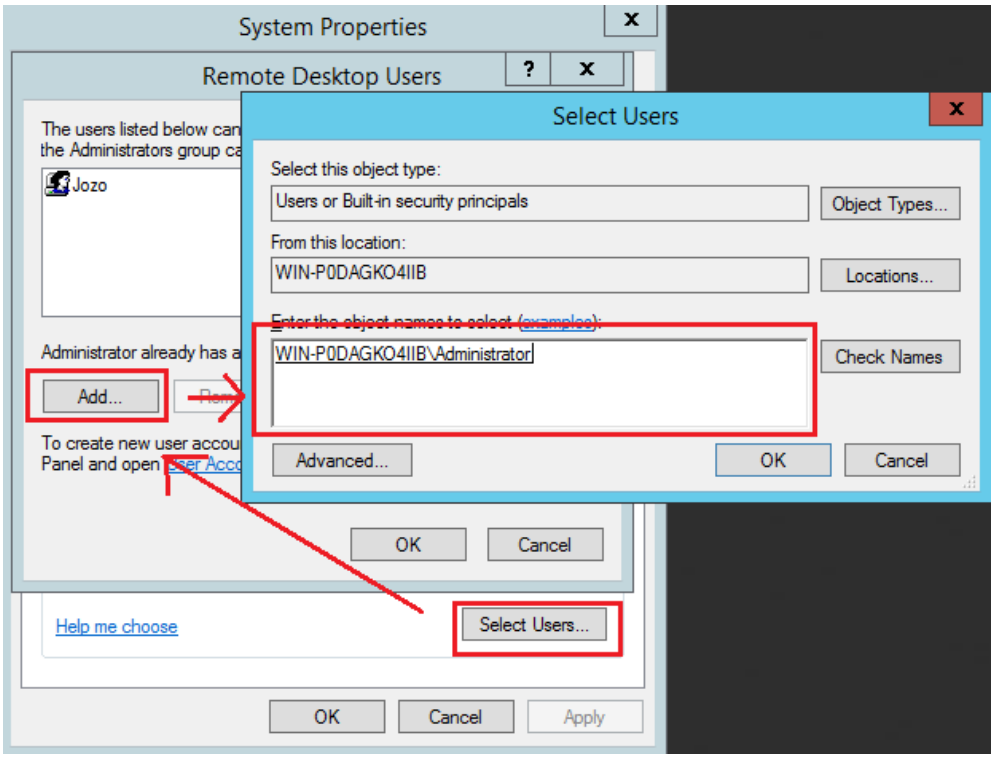
Toto pravidlo zabezpečí že ak sa vzdialeným ovládaním pripojíme na IP 158.193.139.80:43389 tak nás *Remote Access* (port 3389) pripojí na server s IP 192.168.1.2. Takýmto spôsobom by sme vedeli pridávať priame prístupy na ďalších hostov v sieti.

Remote Access

Po pridaní pravidla na vzdialený prístup z vonkajšej siete do 192.168.1.2 stačí na serveri s touto IP povoliť Remote Desktop. "*Windows Server Manager → Local Server → Povoliť Remote Desktop"*

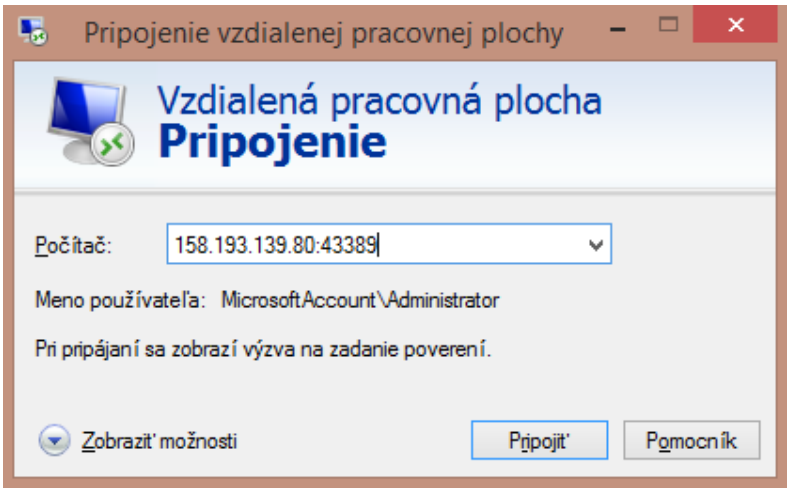


Taktiež je veľmi dôležité pridať používateľa cez tlačidlo *"Select User → Add.. →* Napísať meno Windows používateľa *→ Check Names* (ak nájde)*→ OK*"

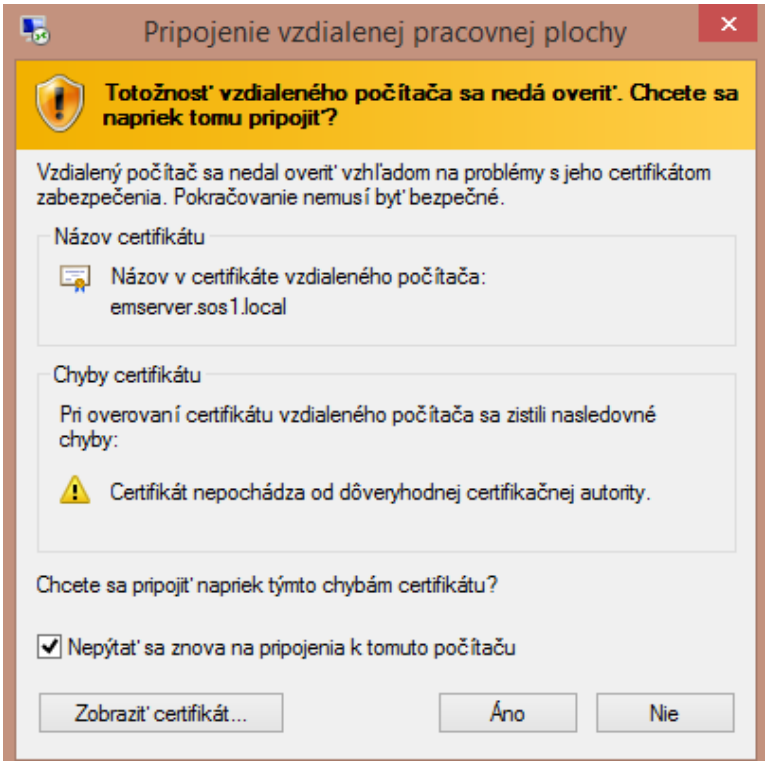


Funkcia je teraz spustená a stačí nasledovne vyskúšať funkčnosť: Client PC Win 8.1 na ovládanie Servera na 192.168.1.2 adrese cez Windows Remote Desktop. Pre overenie funkcionality NAT sme si Client PC pripojili cez WiFi hotspot vytvorený smartfónom.

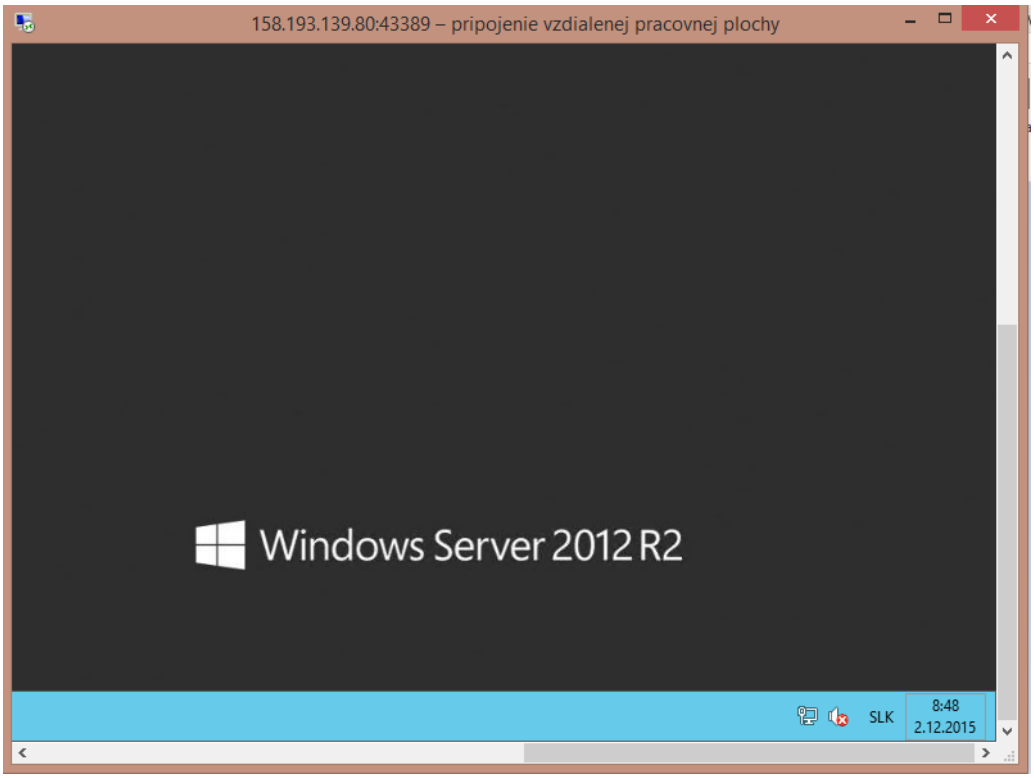
Pripojenie vzdialenej plochy - zadanie adresy ako sme zadefilovali v NAT



Potvrdenie certifikátu.



Orezaný screenshot zo vzdialeného ovládania servera.



Táto služba je veľmi užitočná na správu, počas testovania sa prejavila ako stabilná a efektívna na správu Windows Servera.

DNS (Domain Name System)

LINUX

Náš DNS server spravuje doménu (zónu) *sos1.local*. V tejto zóne sme chceli využívať IPv4 preklady (preklad doménového mena na IP, reverzné preklady sme nepotrebovali). Ako softvérové riešenie DNS sme použili *Bind9*, ktorý sa nachádza v štandardných systémových repozitároch (nainštalovali sme ho pomocou príkazu *apt-get install bind9*). V hlavnom konfiguračnom súbore */etc/bind/named.conf.options* sme nastavili tzv. forwarders - IP adresa DNS, na ktorý sa obrátil náš server ak nebude vedieť splniť požiadavku na preklad. (Môžu to byť DNS providera).

```
forwarders {
158.193.152.2;
};
dnssec-validation no;
```

Do súboru *named.conf.local* sme pridali našu zónu.

```
view "local" {
      match-clients {192.168.1.0/24; 127.0.0.1;};
      zone "sos1.local" {
      type master;
      file "/etc/bind/master/db.sos1.local";
      allow-query {any;};
       allow-transfer {192.168.1.3;};
      };
};
view "public" {
      match-clients {any;};
      zone "sos1.local" {
      type master;
      file "/etc/bind/master/db.sos1.public";
      allow-query {any;};
       allow-transfer {192.168.1.3;};
      };
};
```

Vytvorili sme dva pohľady (view), jeden pre lokálne dotazy (*local*) z našej siete, a druhý pre dotazy z ostatných sietí (*public*). Čo zabezpečí, že ak sa prichádza dotaz na DNS z vonkajšej siete je použitý iný zónový súbor ako keď sa dotazujeme v rámci našej siete. Pre jednoduchšiu orientáciu v adresárovej štruktúre sme vytvorili adresár *master*, kde sme uložili naše zónové súbory.

```
      {@    IN    SOA     ns1.sos1.local. hostmaster.sos1.local. (TREBA MAT
V 1 RIADKU)}
```

súbor *master/db.sos1.local*

```
$TTL    1H
@       IN      SOA     ns1.sos1.local. hostmaster.sos1.local. (
                                2015100601          ; Serial
                                3H          ; Refresh
                                1H          ; Retry
                                2W        ; Expire
                                2H )        ; Negative Cache TTL
                ;
                @       IN      NS      ns1.sos1.local.
                @       IN      NS      ns2.sos1.local.
                ns1     IN      A       192.168.1.2
                ns2     IN      A       192.168.1.3
```

súbor *master/db.sos1.public*

```
$TTL    1H
@       IN      SOA     ns1.sos1.local. hostmaster.sos1.local. (
                                2015100601          ; Serial
                                3H          ; Refresh
                                 1H         ; Retry
                                2W          ; Expire
                                2H )        ; Negative Cache TTL
                ;
                @       IN      NS      ns1.sos1.local.
                @       IN      NS      ns2.sos1.local.
                ns1     IN      A       158.193.139.80
                ns2     IN      A       158.193.139.81
```

Ak sme už raz použili pohľady (*view*) je nutné upraviť všetky zónové súbory (aj tie, ktoré sú defaultne vytvorené - /etc/bind/*named.conf.default-zones*) tak, aby boli "obalené" v pohľade.

```
view "default" {
...
};
```

Po nastavení primárneho (master) DNS sme nastavili aj záložný (slave) server, kde sme v adresári bind vytvorili adresár *slave*, do ktorého sa ukladajú stiahnuté zónové súbory z *master* DNS a bolo potrebné nastaviť prístupové práva (príkaz *chmod*) tohto adresára tak, aby bol do neho umožnený zápis - uloženie stiahnutých súborov.

chmod u+x ./etc/bind/slave

named.conf.local pre slave (pre master je “type master;”, cesta k súboru cez priečinok master a posledný riadok namiesto masters {adresa} je “allow-transfer {192.168.1.3};” (to je ip slave-a))

```
view "local" {
  match-clients {192.168.1.0/24; 127.0.0.1;};
  zone "sos1.local" {
          type slave;
     file "/etc/bind/slave/db.sos1.local";
     allow-query {any;};
     masters {192.168.1.2;};
  };
};

view "public" {
  match-clients {any;};
  zone "sos1.local" {
          type slave;
     file "/etc/bind/slave/db.sos1.public";
     allow-query {any;};
     masters {192.168.1.2;};
  };
};
```

WINDOWS

Master

DNS master nainštalujeme cez Server Manager klikom na *Manage* v pravom hornom rohu → *Add roles and features* → *Role-based or feature-based installation* → zo zoznamu serverov vyberieme náš server → vyberieme službu DNS a dokončíme inštaláciu. Po inštalácií DNS balíka sme vytvorili *primárnu forward lookup* zónu *sos1.local (Tools → DNS → Configure a DNS server → Create a forward lookup zone → This server maintains the zone* keďže tento server bude spravovať zónu → povolili sme aj možnosť pre Active Directory, keďže ho budeme využívať → nastavili sme nech záznamy preposiela na DNS Slave a jeho IP adresu), ktorej záznamy načítame zo súboru, *sos1.local.dns* (defaultne sa zónové súbory ukladajú do *Windows/System32/dns* takže ho odporúčame uložiť tam), ktorého obsah je:

```
;
;  Database file sos1.local.dns for Default zone scope in zone sos1.local.
;      Zone version:  18
;

@                       3600    IN  SOA ns1.sos1.local. hostmaster. (
                                        18          ; serial number
                                        120         ; refresh
                                        300         ; retry
                                        3600        ; expire
                                        600       ) ; default TTL
```

```
;
;  Zone NS records
;

@                NS        ns2.sos1.local.
@                NS        ns1.sos1.local.

;
;  Zone records
;

ns1              A         192.168.1.2
ns2              A         192.168.1.3
www              A  192.168.1.4
www              A  158.193.139.80

```

Pozor: na konci súboru je prázdny riadok.

Po načítaní zónového súboru je ešte potrebné vo vlastnostiach zóny na karte *Zone Transfers* zaškrtnúť *Allow zone transfers* a zvoliť druhú možnosť *Only to servers listed on the Name Servers tab*, čím sa povolí transfer zónových súborov na servery definované na záložke *Name Servers*, ktoré sa v našom prípade načítali zo zónového súboru. (Poznámka: dva *www* záznamy z dvomi rôznymi IP adresami sú kvôli tomu, aby aj DNS požiadavky z verejných sietí boli poslané na náš DNS).

Slave

Po nainštalovaní služby DNS bolo potrebné nastaviť server na slave mode. V pravom hornom rohu v záložke klikneme na *Tools* → *Forward lookup zones* → *New zone* → *Next.* V tomto okne vyberieme možnosť *Secondary zone* → *Next* a meno zóny sme v našom prípade zvolili *sos1.local.* V ďalšom okne máme možnosť určiť a nastaviť *Master DNS server* ktorý má v našom prípade IP *192.168.1.2* po kliknutí na *Next* a *Finish* je služba DNS Slave nainštalovaná a spustená. Po chvíli by si tento server stiahne záznamy z DNS Master servera.

SLUŽBY NA ZDIEĽANIE PRIEČINKOV

LINUX (SAMBA)

Na jednom zo serverov (V našom prípade DNS slave) sme nainštalovali SAMBU príkazom:

apt-get install (libcups2) samba (samba-common cups)

V priečinku */etc/samba/* sme vytvorili zálohu súboru *smb.conf*, vyprázdnili sme ho a vložili sme nasledujúce riadky:

```
[global]
 workgroup = WORKGROUP
 server string = Samba Server %v
 netbios name = debian
 security = user
 map to guest = bad user
 dns proxy = no
```

Následne sme reštartovali SAMBU príkazom:

systemctl restart smbd.service

Pridali sme zdieľané priečinky *allusers* a *anonymous*, ktoré budú prístupné všetkým užívateľom a nastavili sme im práva:

mkdir -p /home/shares/allusers
chown -R root:users /home/shares/allusers/
chmod -R ug+rwx,o+rx-w /home/shares/allusers/

mkdir -p /home/shares/anonymous
chown -R root:users /home/shares/anonymous/
chmod -R ug+rwx,o+rx-w /home/shares/anonymous/

Do súboru *smb.conf* sme pridali nastavenie zdieľaného priečinku *allusers*, ktorý bude prístupný a zapisovateľný pre všetkých užívateľov skupiny:

```
[allusers]
 comment = All Users
 path = /home/shares/allusers
 valid users = @users
 force group = users
 create mask = 0660
 directory mask = 0771
 writable = yes
```

Pre prácu používateľov s domácimi (home) priečinkami prostredníctvom samby sme pridali:

```
[homes]
 comment = Home Directories
 browseable = no
 valid users = %S
 writable = yes
 create mask = 0700
 directory mask = 0700
```

Nastavenie anonymného zdieľaného priečinku, ktorého obsah môžu upravovať všetci užívatelia v sieti:

```
[anonymous]
 path = /home/shares/anonymous
 force group = users
 create mask = 0660
 directory mask = 0771
 browsable =yes
 writable = yes
 guest ok = yes
```

Pre vykonanie zmien sme znovu reštartovali SAMBU:

systemctl restart smbd.service

Pridanie a správa používateľov:

Pridali sme používateľa s menom *samba* a nastavili preňho heslo:

useradd samba -m -G users
passwd samba
zadanie hesla

Prístup k zdieľaným súborom z Windowsu:

Win + R; \\debian

WINDOWS (ACTIVE DIRECTORY)

Active directory master nainštalujeme cez Server Manager klikom na *Manage* v pravom hornom rohu.

Inštalácia:

Add Roles and Features → výber *Role-based or feature-based installation* → *Next* → v tabuľke s výberom cieľového serveru vyberieme náš server a klikneme na *Next* → zo zoznamu vecí, ktoré chceme nainštalovať, vyberieme *Active Directory Domain Services* (V prípade, že DNS server doteraz nebol nainštalovaný, vyberieme aj možnosť *DNS Server*. V našom prípade DNS už bol nainštalovaný takže tento krok môžeme vynechať) → v okne, ktoré nám povie, ktoré funkcie (features) sú potrebné pre AD klikneme na *Add Features* a

ďalej na *Next* → ak chceme pridať nejaké funkcie, tak to môžme urobiť v tomto okne. V našom prípade klikneme iba na *Next* → Okno informujúce o AD DS (Active Directory Domain Services) a jeho požiadavkach ako napríklad potreba DNS. Klikneme na *Next* → Okno ponúkajúce prehľad o inštalovaných súčastiach. Klikneme na *Install* a začne sa proces inštalácie a po jej skončení klikneme na *Close*.

Nastavenie

V Server Managerovi nám naľavo pribudla položka AD DS. Po kliknutí naňho sa nám hore objaví výstražný trojuholník so zvýraznenou žltou farbou a textom *Configuration required for AD DS at ...* Kde klikneme na *More* a následne na *Promote this server to a domain controller under Action.* Keďže potrebujeme vytvoriť nový strom, v tomto okne vyberieme možnosť *Add a new forest* a napíšeme meno root domény, v našom prípade *sos1.local* a klikneme na *Next.* V ďalšom okne sú nastavenia doménového controllera kde vyplníme heslá a klikneme na *Next* → v tomto okne sa objaví upozornenie ktoré môžeme teraz ignorovať a klikneme na *Next* → *NetBIOS domain name* sa vyplní automaticky a môžme kliknúť na *Next* → v okne *Paths* môžeme meniť nastavenia priečinkov databázy, logov a SYSVOL. Necháme default a klikneme *Next* → V tomto okne klikneme na *Install* a počkáme na dokončenie inštalácie a reštartujeme server.

Secondary AD server

Postup pri inštalácii secondary AD je zhodný s primárnym. Rozdiel je v tom, že nevytvára nový strom, ale pripája sa k už existujúcemu. Ako prihlasovacie meno treba použiť: meno užívateľa @ názov domény. V našom prípade *Administrator@sos1.local* a z ponúknutého zoznamu vyberieme našu doménu *sos1.local.*

Sharing na AD DS Master

Kvôli zdieľaniu priečinkov a súborov bolo potrebné na AD Master serveri potrebné pridať *skupinu (group)* a *používateľov (users)* do tejto skupiny. V záložke *Tools* vyberieme možnosť *AD DS Users and Comupters.* V prvom rade vytvoríme novú organizačnú jednotku (u nás *sos1 users*). V nej vytvoríme novú skupinu, ktorej priradíme meno, v našom prípade *Sharing.* Následne vytvoríme jedného alebo dvoch užívateľov. Vyplníme meno a priezvisko a taktiež prihlasovacie meno. V ďalšom okne zadáme dostatočne silné heslo a zaškrtneme možnosť nech heslo nestratí platnosť. Do novovytvorenej skupiny pridáme nového užívateľa - buď v groupe pridáme užívateľa alebo v užívateľovi ho priradíme do groupy.

V záložke *Tools* → *Group policy management* nájdeme v strome naľavo našu organizačnú jednotku a po pravom kliku vyberieme *Create a GPO in this domain* a zvolíme meno *(network_drive)* po jeho pridaní a po pravom kliku naňho zvolíme edit. V strome naľavo nádeme cestu *User configuration* → *Preferences* → *Windows settings* → *Drive maps.* V okne napravo pridáme *New* → *Mapped drive*. Následne si vytvoríme na disku ľubovoľný priečinok a v ňom testovací textový súbor. V nastavení priečinku nastavíme zdieľanie pre našu vytvorenú groupu *(sharing).* V nastavení mapped drive nastavíme :

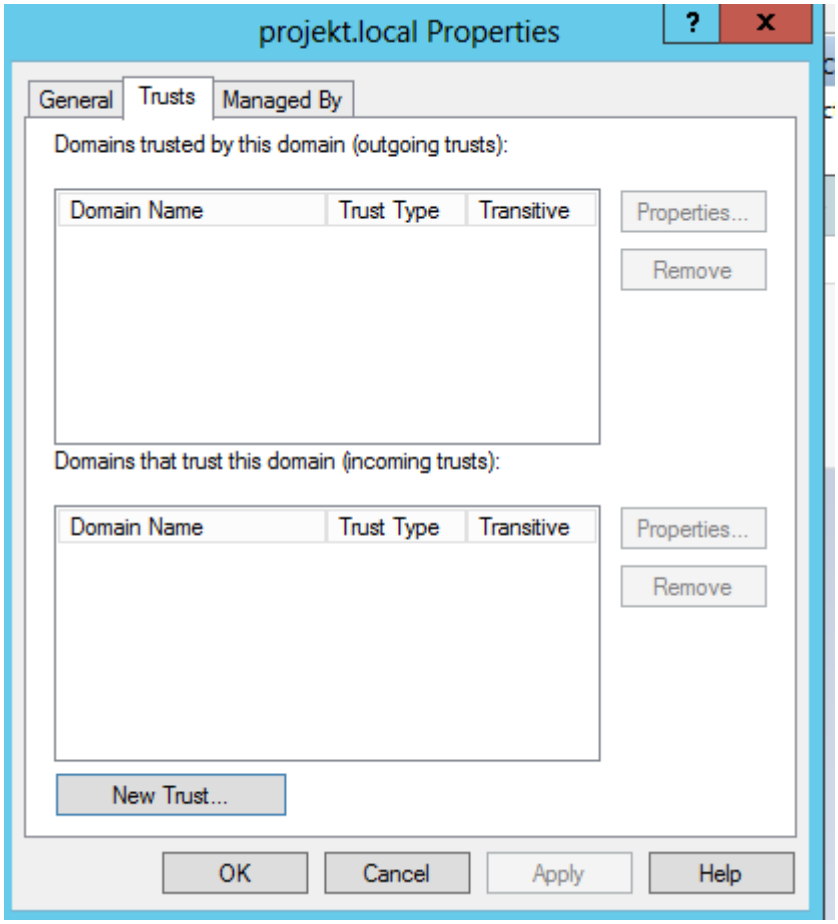
- *Action : Create*
- *Location : cesta k nášmu priečinku*
- *Hide/show this drive : Show this drive*
- *Hide/show all drives : Show all drives*

V záložke *Common* vyberieme možnosť *Item-level targeting* a *Targeting…* Pridáme *New item → Security group* a nájdeme našu groupu (*Sharing*) - v prípade ak bola nastavená ako Primárna groupa, zaškrtneme aj to.

Prihlásime sa ako užívateľ ktorého sme vytvorili v našej groupe do našej domény v tvare : *meno@sos1.local* a v príkazovom riadku vynútime update group policy príkazom : *gpupdate /force* . Po reštartovaní počítača sa v *My computer* objaví v *Network location* náš zdieľaný priečinok.

Trusted zóny

Ďalším krokom bolo vytvorenie trusted vzťahu so susednou doménou (sos2.local). Na nastavení tohto vzťahu sme otvorili *Server Manager → Tools → Active Directory Domains and Trust.* V ponúknutom okne sme zvolili našu doménu. V záložke *Properties → New Trust →* Zadáme doménu s ktorou chceme vytvoriť vzťah, ktorý bol v našom prípade *Two-way forest.*



NTP (Network Time Protocol)

LINUX

Konfigurácia servera a klientov

Protokol NTP slúži na synchronizáciu času všetkých počítačov pripojených do siete. Na to využíva protokol UDP. Klienti (počítače), ktoré chcú zosynchronizovať svoj čas, pošlú dotazy na NTP server(y), ktoré odpovedajú správou s presným časom.

Pre naše potreby sme ako NTP server zvolili server na ktorom už beží DNS Master server s IP adresou 192.168.1.2

Bolo potrebné nainštalovať balíček *ntp* príkazom *apt-get install ntp*. Na konfiguráciu NTP slúži súbor */etc/ntp.conf* . Na počítači, ktorý bude bežať ako NTP server bolo potrebné upraviť tento súbor do tvaru :

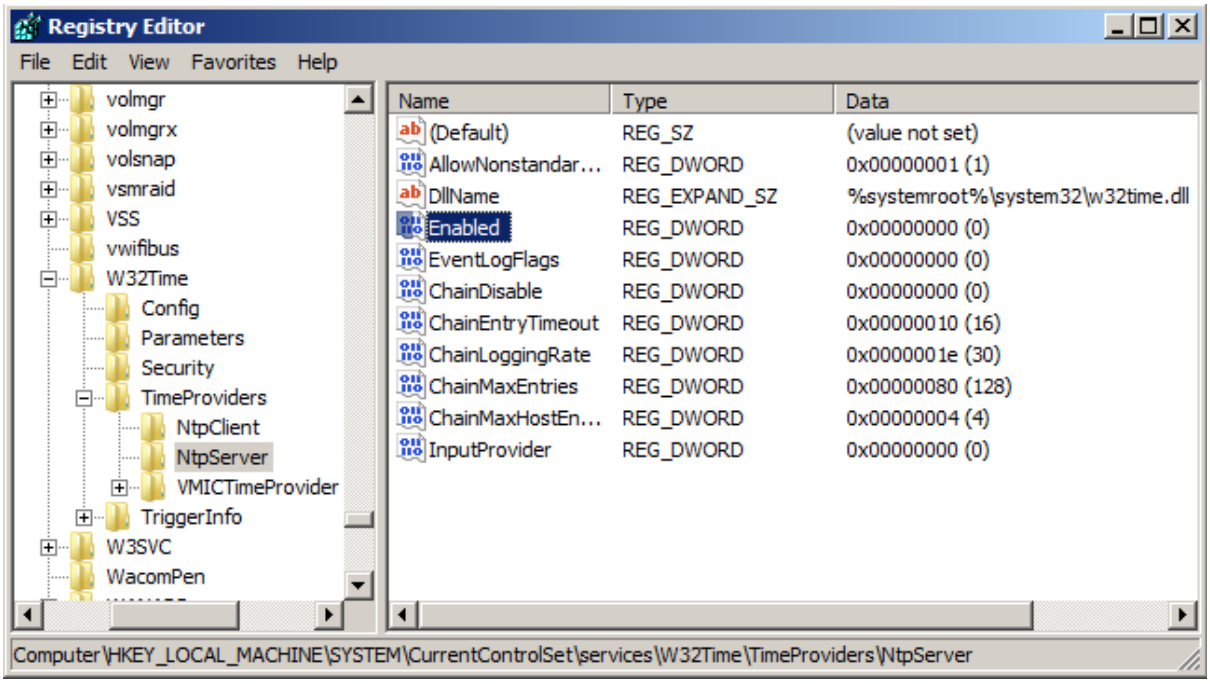
```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift

# You do need to talk to an NTP server or two (or three).
server 3.sk.pool.ntp.org iburst prefer
server 3.europe.pool.ntp.org
server 2.europe.pool.ntp.org

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
```

Na klientských počítačoch bol tento súbor nakonfigurovaný v tvare :

```
# /etc/ntp.conf, configuration for ntpd; see ntp.conf(5) for help
driftfile /var/lib/ntp/ntp.drift

# You do need to talk to an NTP server or two (or three).
server 192.168.1.2

# By default, exchange time with everybody, but don't allow configuration.
restrict -4 default kod notrap nomodify nopeer noquery
```

WINDOWS

Pre nastavenie Windows servera ako NTP server bez použitia Active Directory je potrebné vykonať zmenu v registroch. Do *Registry Editora* sa dostaneme zadaním príkazu *regedit* do spúšťacieho riadku (Win+R). V registroch rozbalíme cestu *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *TimeProviders* | *NtpServer* a hodnotu *Enabled*, ktorá je primárne nastavená na "0", zmeníme na "1".



Následne je potrebné v príkazovom riadku zadať *w32tm /config /update*, ktorý zmení nastanie W32TM - Windows Time engine. Táto zmena spustí NTP server na tomto počítači. Po zadaní *w32tm /query /configuration* si môžme skontrolovať, či NTP server beží správne.

Synchronizácia s NTP serverom

Pre nastavenie synchronizácie systému s NTP serverom treba taktiež vykonávať zmeny v registroch.
V *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *Parameters* nastavíme hodnotu *Type* na "NTP".
V *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *Config* nastavíme hodnotu *AnnounceFlags* na "5".
V *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *TimeProviders* | *NtpServer* nastavíme hodnotu *Enabled* na "1".
V *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *Parameters* nastavíme hodnotu *NtpServer* na zoznam peerov, od ktorých môžme čas prijímať, oddelených medzerou. Môže to byť zoznam IP adries alebo DNS mien, ku ktorým však treba na ich koniec pridať ",0x1".
V *HKEY_LOCAL_MACHINE* | *SYSTEM* | *CurrentControlSet* | *Services* | *W32Time* | *TimeProviders* | *NtpClient* nastavíme hodnotu *SpecialPollInterval*, ktorá určuje čas (v sekundách) medzi každou požiadavkou, na "900" (decimálne), čo je odporúčaná hodnota od Microsoftu.

Pre aplikovanie zmien reštartujeme Windows Time service príkazom
net stop w32time && net start w32time v príkazovom riadku.

WEBOVÉ SERVERY

LINUX (APACHE)

Apache sme nainštalovali zadaním príkazov :

apt-get install apache2
apt-get install mysql
apt-get install php5

v adresári */var/www/* sme vytvorili súbor

v súbore */etc/apache2/sites-available* sme nastavili dva virtuálne servere:

```
<VirtualHost *:80>
<------>ServerName web1.sos1.local
<------>ServerAlias www.web1.sos1.local
<------>ServerAdmin webmaster@localhost
<------>DocumentRoot "/var/www/web1.php"
</VirtualHost>

<VirtualHost *:80>
<------>ServerName web2.sos1.local
<------>ServerAlias www.web2.sos1.local
<------>ServerAdmin webmaster@localhost
<------>DocumentRoot "/var/www/web2.php"
</VirtualHost>
```

Na DNS master serveri bolo potrebné do záznamov dopísať :

db.sos1.local :

```
web1  IN    A       192.168.1.4
web2  IN    A       192.168.1.4
```

db.sos1.public :

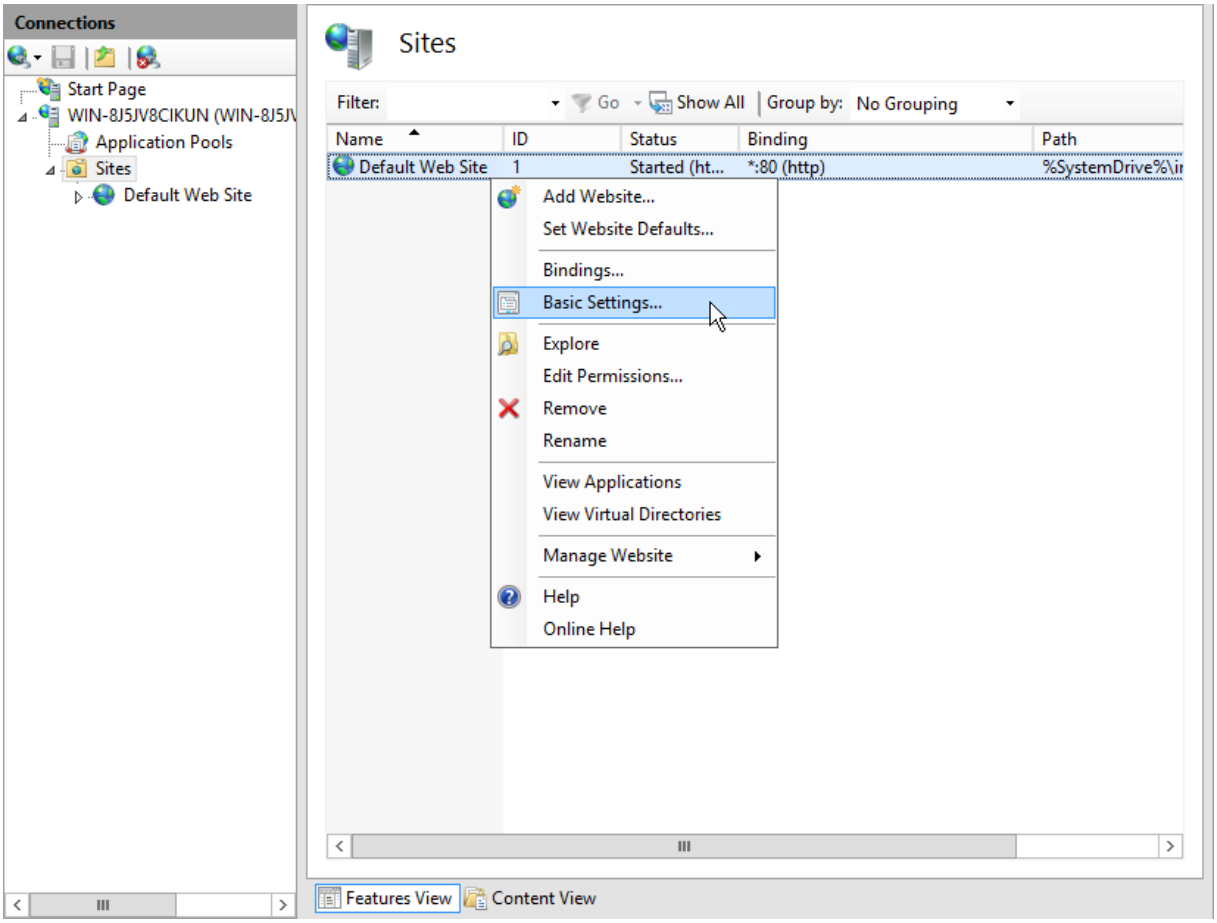
```
web1  IN    A       158.193.139.80
web2  IN    A       158.193.139.80
```

WINDOWS (IIS)

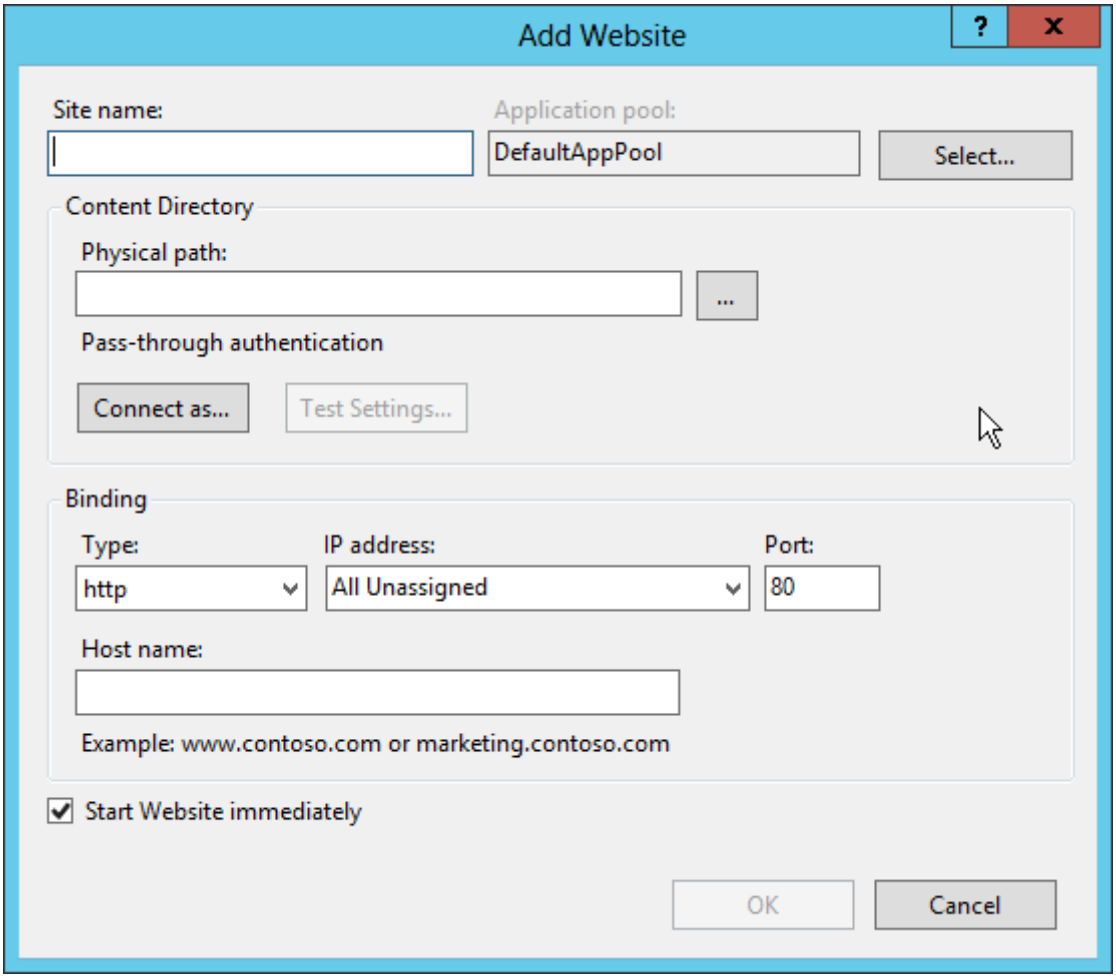
Funkciu IIS (Internet Information Server) sme pridali vo Windows server manager cez tlačidlo *Add roles and features*. Preklikáme sa k zoznamu funkcií, kde zvolíme *Web Server (IIS)* a pokračujeme. Žiadne dodatočné funkcie nie sú potrebné, znova klikáme *Next*, kým sa dostaneme k ponuke *Role Services* a v nej zvolíme požadované služby. Následne klikneme *Next* a *Install*.

Vytvorenie webu

Po úspešnej inštalácii sa IIS objaví na ľavom paneli v server manager-i. Klikneme na ikonu IIS a v zozname dostupných serverov sa zjaví jeden - ten, na ktorom uskutočňujeme konfiguráciu. Klikneme naň pravým tlačidlom myši a z ponuky zvolíme možnosť *Internet Information Services (IIS) Manager*. Otvorí sa nové okno, v ktorého ľavom paneli sa nachádza náš server. Rozbalíme jeho ponuku a klikneme na *Sites*. Pravý klik na *Default Web Site* nám ponúkne viacero možností vrátane nastavenia webstránky a pridania novej.



Ako našu webstránku môžme ponechať defaultnú, ktorá obsahuje logo IIS 8 alebo si vytvoriť vlastnú kliknutím na *Add Website…* V okne pre vytvorenie webstránky zadáme jej názov, cestu k zdrojovým súborom, typ protokolu, port a host name.



Po vytvorení a spustení webu by k nemu mali mať prístup všetci účastníci v sieti zadaním IP adresy/host name do internetového prehliadača.

Kombinovanie Linux a Windows

Linux - DNS - povolenie DDNS + Linux Firewall

Ak chceme použiť Active Directory, ktorý bude komunikovať s DNS, ktorý beží na operačnom systéme Linux je potrebné v konfigurácií služby *bind9* nastaviť, kto môže upravovať dynamické záznamy na DNS. My sme povolili upravovanie zónových súborov všetkým zariadeniam v našej sieti. Toto nastavenie aplikujeme v súbore */etc/bind/named.conf.local,* kde do našej zóny (*sos1.local*) pridáme nasledovný riadok:

```
allow-update {192.168.1.0/24;};
```

Následne sme nastavili plné prístupové práva na adresár, v ktorom sa nachádzali zónové súbory. V našom prípade to bol adresár */etc/bind/master*

```
chmod 777 /etc/bind/master
```

Windows - Active Directory

Pri inštalácii a nastavení Active Directory postupujeme rovnako, je potrebné dbať na to, aby AD používal správny DNS a aby bola vytvorená správna doména (názov domény v AD sa viaže na názov DNS zóny) a v nej pridaný užívateľ, pod ktorým sa môžeme do danej domény prihlásiť.

Problémy a zistenia

Po prihlásení užívateľa do Active Directory domény sa DNS A záznam pošle na DNS, kde sa neuloží priamo do zónového súboru (db.sos1.local), ale vytvorí sa tzv. journal súbor (db.sos1.local**.jnl**). Tento A záznam nie je ihneď dostupný pretože zo súboru *.jnl sa do samotného zónového súboru sa uloží až po určitom čase (defaultne 15 minút, podľa iného zdroja sa vykonáva "hneď ako je to možné"). Ak to chceme vykonať okamžite je potrebné reštartovať službu *bind9* pomocou príkazu *service bind9 restart*. Na diagnostiku problémov sme použili *service bind9 status*, kde sa nám objavili chyby:

- *BADTIME*, čo sme vyriešili aktualizovaním času na oboch zariadeniach pomocou NTP
- *BADKEY*, čo sme vyriešili zrušením akejkoľvek autentifikácie medzi AD a DNS, keďže sme to zabezpečili tým, že upravovať zónové súbory môžu len zariadenia z IP adresou v našej sieti
- *A record for domain not found* - táto chyba sa vyskytla, keď bol daný A záznam len v súbore *.jnl a po reštartovaní služby *bind9* sa už tento záznam načítal do zónového súboru a tým sme chybu odstránili

Zaujímavým zistením bolo, že keď sme použili ako DNS Master *bind9* na Linuxe a DNS Slave na Windows Server 2012 R2 nebol žiadny problém s korektným kopírovaním zónových súborov z *mastra* na *slave*. Je teda zaujímavé, že aj svety Linuxu a Windowsu sa v niektorých častiach dokážu dohodnúť, ak ich k tomu vieme prinútiť. :)