Dokumentácia riešenia

**SOS**

**Skupina 3 Meno a priezvisko:**

**Michal Knapčok**

**Juraj Beleščák**

**Preambula / Účel**

Účelom tohto dokumentu je poskytnúť informácie o riešení SOS.

|  |  |
| --- | --- |
| Dokument: | Dokumentácia riešenia **SOS** |
| Verzia: |  |
| Autor: | Knapčok, Beleščák |

**História dokumentu**

|  |  |  |
| --- | --- | --- |
| Verzia | Dátum verzie | Popis zmien |
| 0.01 | 11.9.2017 | Úvodný draft |
| 0.1 | 1.12. | Vloženie nečistopisu do dokumentu |
| 0.2 | 18.12. | Zdokumentované časti pre Windows: Topolgia, prvotné nastavenia, routovanie, port-forwarding, NTP, DNS a Logovanie |
| 0.3 | 22.12. | Dokumentovanie OS Linux: Topologia, prvotné nastavenia, firewall a NAT |
| 0.4 | 26.12. | Dokumentovanie OS Linux: DNS |
| 0.5 | 27.12. | Dokumentovanie OS Windows: IIS Server, DHCP |
| 0.6 | 28.12. | Dokumentovanie OS Linux: DHCP, Mail Service |
| 0.7 | 29.12. | Dokumentovanie OS Linux: Syslog-ng |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Obsah

[1 Obsah 4](#_Toc502489666)

[2 Zoznam tabuliek 6](#_Toc502489667)

[3 Zoznam obrázkov 7](#_Toc502489668)

[4 Úvod 9](#_Toc502489669)

[5 Riešenie pre OS LINUX 10](#_Toc502489670)

[5.1 Topológia zapojenia 10](#_Toc502489671)

[5.2 Prvotné nastavenia 10](#_Toc502489672)

[5.2.1 Prístupové údaje 10](#_Toc502489673)

[5.2.2 Nastavenie adresovania 10](#_Toc502489674)

[5.3 Firewall 11](#_Toc502489675)

[5.3.1 Návrh riešenia 12](#_Toc502489676)

[5.3.2 Konfigurácia 12](#_Toc502489677)

[5.3.3 SSH 12](#_Toc502489678)

[5.4 NAT 13](#_Toc502489679)

[5.4.1 Výnimky vo firewalle 13](#_Toc502489680)

[5.4.2 Overenie 14](#_Toc502489681)

[5.5 DHCP 16](#_Toc502489682)

[5.5.1 Konfigurácia 16](#_Toc502489683)

[5.5.2 Overenie DHCP 17](#_Toc502489684)

[5.6 DNS 17](#_Toc502489685)

[5.6.1 Konfigurácia 17](#_Toc502489686)

[5.6.2 Výnimky pre Firewall 23](#_Toc502489687)

[5.6.3 Overenie 23](#_Toc502489688)

[5.7 Apache 24](#_Toc502489689)

[5.7.1 HTTP 24](#_Toc502489690)

[5.7.2 HTTPS 26](#_Toc502489691)

[5.8 NTP 28](#_Toc502489692)

[5.9 Mailová služba 28](#_Toc502489693)

[5.9.1 Pridanie RR do DNS zóny 29](#_Toc502489694)

[5.9.2 Konfigurácia SMTP 30](#_Toc502489695)

[5.9.3 Konfigurácia POP3 35](#_Toc502489696)

[5.9.4 Konfigurácia SquirrelMail 35](#_Toc502489697)

[5.9.5 Testovanie Mailovej služby 36](#_Toc502489698)

[5.10 SYSLOG-NG 37](#_Toc502489699)

[5.10.1 Konfigurácia 37](#_Toc502489700)

[5.10.2 Overenie 37](#_Toc502489701)

[6 Riešenie pre OS Windows 40](#_Toc502489702)

[6.1 Topológia zapojenia 40](#_Toc502489703)

[6.2 Prvotné nastavenia 40](#_Toc502489704)

[6.3 Nastavenie routovania na Server-router 42](#_Toc502489705)

[6.4 Port forwarding pre Remote Desktop 48](#_Toc502489706)

[6.5 DNS Server 49](#_Toc502489707)

[6.6 DHCP 51](#_Toc502489708)

[6.7 NTP Server 59](#_Toc502489709)

[6.8 Web Server IIS 60](#_Toc502489710)

[6.9 Logovanie 65](#_Toc502489711)

[7 Literatúra 66](#_Toc502489712)

[7.1 Firewall 66](#_Toc502489713)

[7.2 NAT 66](#_Toc502489714)

[7.3 DHCP 66](#_Toc502489715)

[7.4 DNS 66](#_Toc502489716)

[7.5 Web Server 67](#_Toc502489717)

[7.6 Mail Service 67](#_Toc502489718)

[7.7 NTP 67](#_Toc502489719)

[7.8 Logovanie 67](#_Toc502489720)

[7.9 Iné 67](#_Toc502489721)



# Zoznam tabuliek

[Tabuľka 1: Adresný plan Linux 10](#_Toc502489722)

[Tabuľka 2: Konfigurácia virtual hostov Apache 24](#_Toc502489723)

[Tabuľka 3: Adresný plán Windows 40](#_Toc502489724)

# Zoznam obrázkov

[Obrázok 1: Konfigurácia sieťových rozhraní na Server-router 11](#_Toc502489725)

[Obrázok 2: Skript firewall.sh zabezpečujúci firewall na serveri Server-router 13](#_Toc502489726)

[Obrázok 3: Overenie NAT 15](#_Toc502489727)

[Obrázok 4. DHCP - konfiguračný súbor dhcpd.conf 16](#_Toc502489728)

[Obrázok 5. Súbor interfaces na Server-Router 17](#_Toc502489729)

[Obrázok 6. Príkaz ifconfig na zariadení Klient 17](#_Toc502489730)

[Obrázok 7: Zónový súbor private.sos3.local 19](#_Toc502489731)

[Obrázok 8: Zónový súbor public.sos3.local 19](#_Toc502489732)

[Obrázok 9: Reverzný zónový súbor internal.arpa 20](#_Toc502489733)

[Obrázok 10: Reverzný zónový súbor external.arpa 20](#_Toc502489734)

[Obrázok 11: Súbor Krndc-key.+157+12769.private 22](#_Toc502489735)

[Obrázok 12: Vynimky vo firewalle pre DNS 23](#_Toc502489736)

[Obrázok 13: Overenie funkčnosti DNS serveru 24](#_Toc502489737)

[Obrázok 14: Public DNS záznam pre HTTP 25](#_Toc502489738)

[Obrázok 15: Private DNS záznam pre HTTP 26](#_Toc502489739)

[Obrázok 16. Súbor private.sos3.local 29](#_Toc502489740)

[Obrázok 17. Súbor public.sos3.local 29](#_Toc502489741)

[Obrázok 18. Úprava firewall.sh z dôvodu funkčnosti mailovej služby 30](#_Toc502489742)

[Obrázok 19. Všeobecný typ konfigurácie pošty 30](#_Toc502489743)

[Obrázok 20. Poštový názov systému 31](#_Toc502489744)

[Obrázok 21. Príjemca pošty pre používateľov root a postmaster 32](#_Toc502489745)

[Obrázok 22. Iné destinácie pre príjmanie pošty 33](#_Toc502489746)

[Obrázok 23. Synchrónne aktualizácie pošty 34](#_Toc502489747)

[Obrázok 24. Lokálne siete 34](#_Toc502489748)

[Obrázok 25 Súbor 003-mail.sos3.local.conf 35](#_Toc502489749)

[Obrázok 26. Vytvorenie mailu 36](#_Toc502489750)

[Obrázok 27. Overenie poslaného mailu 36](#_Toc502489751)

[Obrázok 28: Výpis obsahu zložky /var/log/debian-edu 38](#_Toc502489752)

[Obrázok 29: Logy zo serveru 2 uložené na serveri 1 39](#_Toc502489753)

[Obrázok 30: Nastavenie IP adries na serveri Server-router 41](#_Toc502489754)

[Obrázok 31: Nastavenie smerovania na Server-router obr. 1 42](#_Toc502489755)

[Obrázok 32: Nastavenie smerovania na Server-router obr. 2 43](#_Toc502489756)

[Obrázok 33: Nastavenie prekladania NAT na Server-router obr. 1 44](#_Toc502489757)

[Obrázok 34: Nastavenie routovania na Server-router obr. 4 45](#_Toc502489758)

[Obrázok 35: Nastavenie prekladania NAT na Server-router obr. 2 45](#_Toc502489759)

[Obrázok 36: Nastavenie prekladania NAT na Server-router obr. 3 46](#_Toc502489760)

[Obrázok 37: Nastavenie prekladania NAT na Server-router obr. 4 46](#_Toc502489761)

[Obrázok 38: Testovanie NAT na Serveri 1 47](#_Toc502489762)

[Obrázok 39: Nastavenie prekladania NAT na Server-router obr. 5 48](#_Toc502489763)

[Obrázok 40: Nastavenie zónového súbora DNS - Windows 50](#_Toc502489764)

[Obrázok 41: Konfigurácia DNS - Windows 51](#_Toc502489765)

[Obrázok 42. Pridanie role pomocou Add Roles and Features 52](#_Toc502489766)

[Obrázok 43. Notifikácia ohľadom dokončenia konfigurácie DHCP 52](#_Toc502489767)

[Obrázok 44. Vytvorenie nového rozsahu 53](#_Toc502489768)

[Obrázok 45. Vytvorenie nového rozsahu – zadanie názvu 54](#_Toc502489769)

[Obrázok 46. Vytvorenie nového rozsahu – zadanie rozsahu a masky 54](#_Toc502489770)

[Obrázok 47. Vytvorenie nového rozsahu – zadanie IP adresy routera 55](#_Toc502489771)

[Obrázok 48. Lokácia Configure Options... 56](#_Toc502489772)

[Obrázok 49. Pridanie DNS Servera už vytvorenému rozsahu 56](#_Toc502489773)

[Obrázok 50. Služby role pri inštalácií DHCP Relay Agenta 57](#_Toc502489774)

[Obrázok 51. Lokácia „New Routing Protocol...“ 58](#_Toc502489775)

[Obrázok 52. Zvolenie DHCPv4 Relay Agent 58](#_Toc502489776)

[Obrázok 53. Overenie dynamického pridelenia IP adresy 59](#_Toc502489777)

[Obrázok 54: Konfigurácia NTP servera 60](#_Toc502489778)

[Obrázok 55. Pridanie role pomocou Add Roles and Features 61](#_Toc502489779)

[Obrázok 56. Záložka Server Roles pri inštalácii IIS 61](#_Toc502489780)

[Obrázok 57. Lokácia Internet Information Service Manager-a 62](#_Toc502489781)

[Obrázok 58. Vymazanie default-ne vytvorenej stránky 63](#_Toc502489782)

[Obrázok 59. Vytvorenie novej stránky 64](#_Toc502489783)

[Obrázok 60. Definovanie názvu stránky a cesty k súborom 64](#_Toc502489784)

[Obrázok 61. Overenie funkčnosti webového servera 65](#_Toc502489785)

# Úvod

V našej práci sa budeme zaoberať implementáciou a konfiguráciou menšej firemnej siete, ktorá bude pozostávať z 3 serverov a jedného klientského zariadenia. Jeden server bude slúžiť ako router, dva ako servery, na ktoré nainštalujeme aplikácie poskytujúce služby ako DNS, DHCP, Apache či NTP. Klient bude slúžiť na kontrolu funkčnosti nainštalovaných aplikácii, ktoré umožnia firme poskytovať služby pre vnútornú, ale aj vonkajšiu sieť. Tieto riešenia budú nainštalované a otestované v prostredí operačných systémov Linux a Windows.

Dokument popisuje systémovú architektúru riešenia SOS v akademickom roku 2017/18.

# Riešenie pre OS LINUX

Všetky vykonané nastavenia a konfigurácie je nutné vykonávať ako root ak nie je povedané inak.

## Topológia zapojenia

Topológia SOS sa skladá z routera, dvoch serverov a klienta.

|  |  |  |  |
| --- | --- | --- | --- |
| Názov zariadenia | Rozhranie | IP adresa | Popis |
| Server-router | ens3 | 158.193.153.138  158.193.153.154 | Rozhranie pripojené k internetu |
|  | ens4 | 192.168.1.1 | Rozhranie pripojené k sieti so servermi |
|  | ens5 | 192.168.2.1 | Rozhranie pripojené k sieti s klientom |
| Server1 | ens4 | 192.168.1.2 |  |
| Server2 | ens4 | 192.168.1.3 |  |
| Klient | ens5 | 192.168.2.2 |  |

Tabuľka 1: Adresný plan Linux

## Prvotné nastavenia

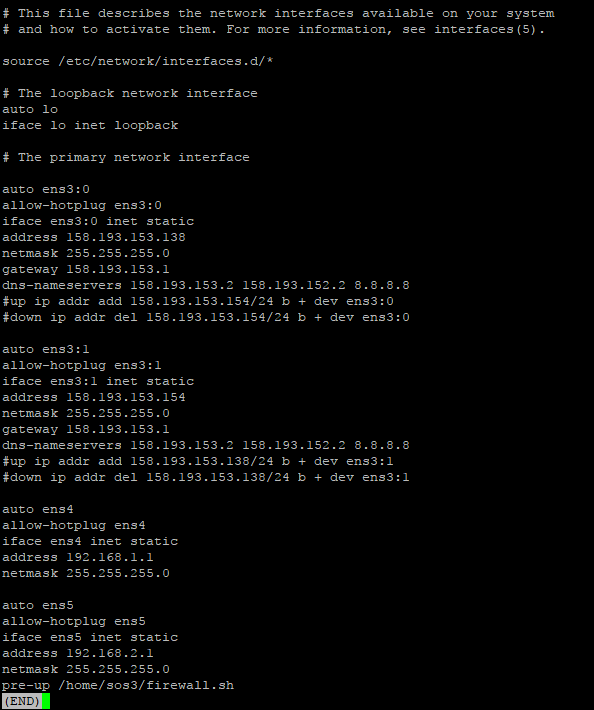
### Prístupové údaje

Ako prvé sme zmenili prístupové údaje k serverom. Zrušili sme defaultného používateľa a vytvorili si používateľa sos3 na všetkých zariadeniach a pridali sme mu nové heslo. Taktiež sme zmenili heslo na roota. Toto sme použili na všetky zariadenia.

### Nastavenie adresovania

Následne sme nastavili statické IP adresy pre zariadenia upravením konfiguračného súboru */etc/network/interfaces*

Na priloženom obrázku je vidieť nastavenie na serveri Server-router.



Obrázok 1: Konfigurácia sieťových rozhraní na Server-router

Na rozhranie ens 3:0 a ens 3:1 sme nastavili verejné IP adresy pridelené pre našu skupinu.

## Firewall

Súčasťou riešenia je aj firewall.

### Návrh riešenia

Firewall na operačnom systéme Linux zabezpečíme pomocou nástroja Netfilter, ktorý je súčasťou kernelového jadra. Používali sme program iptables pomocou ktorého sme vytvárali a vkladali pravidlá do firewallu.

### Konfigurácia

Keďže pravidlá sa do firewallu dajú vkladať len postupne po jednom príkaze rozhodli sme sa vytvoriť bash skript firewall.sh ktorý sme uložili v priečinku: */home/sos3/*

Aby sa skript spustil vždy po spustení systému sme zabezpečili pomocou príkazu

pre-up /home/sos3/firewall.sh

Tento príkaz sme vložili do konfiguračného súboru */etc/network/interfaces* pre rozhranie ens5 na serveri Server-router.

Taktiež treba nastaviť práva na spúšťanie tohto súboru a to príkazom:

chmod a+x firewall.sh

Ako prvé sme v tomto skripte nastavili vymazanie predchádzajucich uložených pravidiel. A to príkazmi:

iptables -F #vymaze filter zaznamy

iptables -F -t nat #vymaze nat zaznamy

Následne sme nastavili predvolenú politiku pre vetvy INPUT, FORWARD a OUTPUT

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

Pre vetvy INPUT a FORWARD je predvolená politika DROP, takže pakety, ktoré nemajú nastavenú výnimku vo firewalle budú zahodené. Vetva OUTPUT sme nastavili na ACCEPT.

Taktiež sme povolili komunikáciu smerujúcu na loopback, ICMP pakety a komunikáciu pomocou už vytvoreného spojenia príkazmi:

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p icmp -j ACCEPT

iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

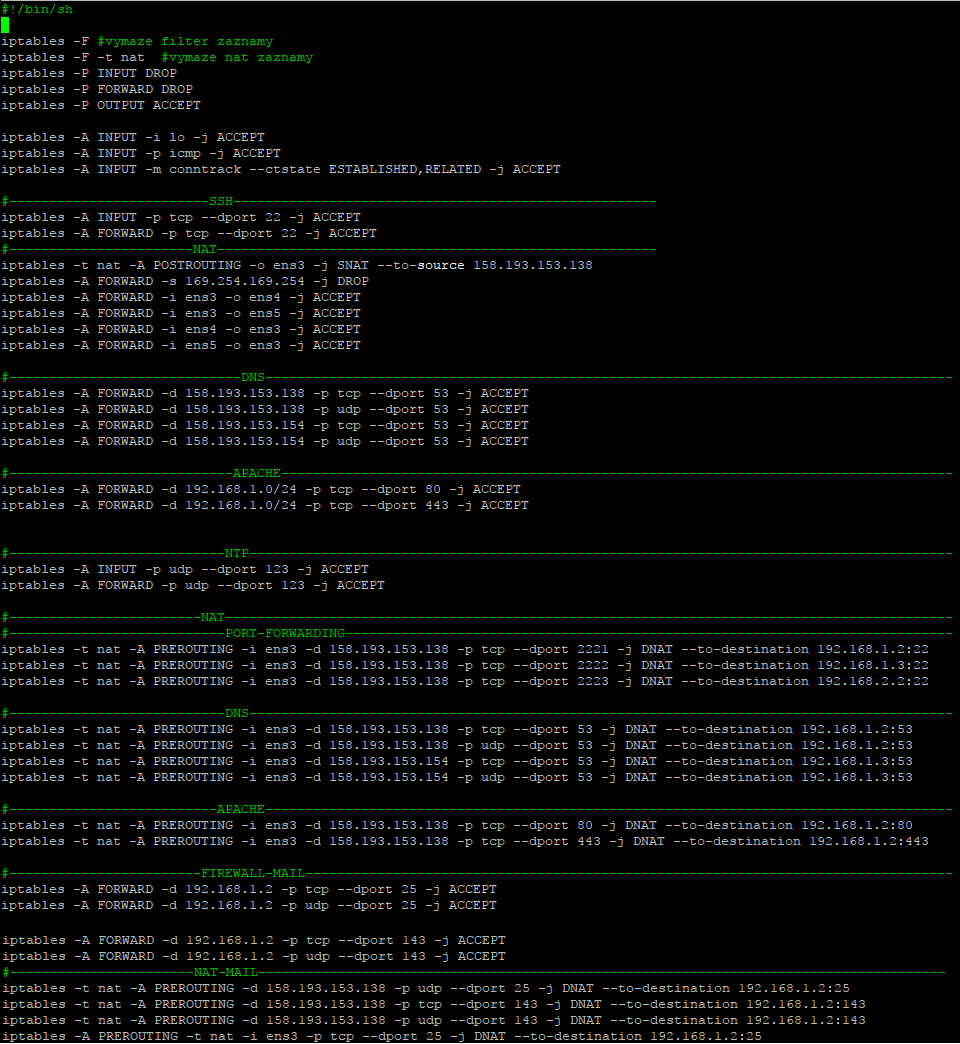
### SSH

Nastavili sme aj výnimku pre port 53, ktorý je vyhradený pre SSH príkazmi:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A FORWARD -p tcp --dport 22 -j ACCEPT

Na nasledujúcom obrázku je vidieť výslednú verziu skriptu, ktorý sme priebežne upravovali počas semestra po inštalácii a konfigurácii rôznych služieb.



Obrázok 2: Skript firewall.sh zabezpečujúci firewall na serveri Server-router

## NAT

V tejto časti uvedieme konfiguráciu NAT mechanizmu.

### Výnimky vo firewalle

Aby mohol NAT fungovať, vo firewalle musíme spustiť prekladanie adries príkazom:

iptables -t nat -A POSTROUTING -o ens3 -j SNAT --to-source 158.193.153.138

Pre každú službu ktorú sme spustili na našom serveri sme museli vytvoriť pravidlá pre NAT. Tie vyzerajú takto:

#------------------------NAT-----------------------------------------------------

#---------------------------PORT-FORWARDING--------------------------------------

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 2221 -j DNAT --to-destination 192.168.1.2:22

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 2222 -j DNAT --to-destination 192.168.1.3:22

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 2223 -j DNAT --to-destination 192.168.2.2:22

#---------------------------DNS--------------------------------------------------

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 53 -j DNAT --to-destination 192.168.1.2:53

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p udp --dport 53 -j DNAT --to-destination 192.168.1.2:53

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.154 -p tcp --dport 53 -j DNAT --to-destination 192.168.1.3:53

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.154 -p udp --dport 53 -j DNAT --to-destination 192.168.1.3:53

#--------------------------APACHE------------------------------------------------

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.2:80

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.2:443

#---------------------------MAIL-------------------------------------------------

iptables -t nat -A PREROUTING -d 158.193.153.138 -p udp --dport 25 -j DNAT --to-destination 192.168.1.2:25

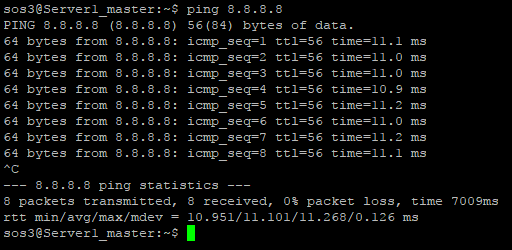
iptables -t nat -A PREROUTING -d 158.193.153.138 -p tcp --dport 143 -j DNAT --to-destination 192.168.1.2:143

iptables -t nat -A PREROUTING -d 158.193.153.138 -p udp --dport 143 -j DNAT --to-destination 192.168.1.2:143

iptables -A PREROUTING -t nat -i ens3 -p tcp --dport 25 -j DNAT --to-destination 192.168.1.2:25

### Overenie

Na overenie môžeme použiť príkaz ping, ktorým overíme konektivitu:



Obrázok 3: Overenie NAT

## DHCP

Pre dynamické prideľovanie IP adries bolo potrebné nainštalovať DHCP Server na serveri 1. Pre správne fungovanie bolo potrebné nakonfigurovať DHCP Relay na server-routeri z dôvodu, že klienti sa nachádzali v inej sieti ako DHCP server.

### Konfigurácia

Na routeri server-router bolo potrebné nainštalovať isc-dhcp-relay pomocou príkazu

apt-get install isc-dhcp-relay

a po úspešnej inštalácii upraviť súbor */etc/default/isc-dhcp-relay*. Do atribútu SERVERS sme pridali IP adresu DHCP servera v úvodzovkách (v prípade viacero serverov, by sme ich oddelili medzerami).

SERVERS="192.168.1.2"

Druhá potrebná úprava sa týkala atribútu INTERFACES, interface-ov na ktorých mal DHCP server prideľovať IP adresy.

INTERFACES="ens4 ens5"

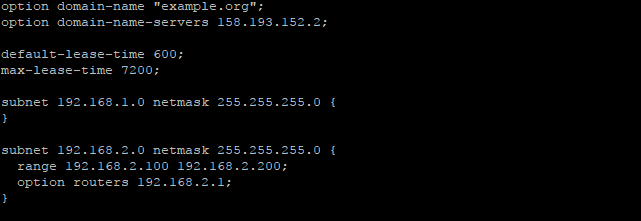
Nasledovne sme nainštalovali a nakonfigurovali DHCP server na zariadení Server 1 (192.168.1.2). Ako prvý krok, bolo potrebné nainštalovať balík DHCP Server, známy aj ako dhcp3-server pomocou príkazu

#apt install isc-dhcp-server

Po úspešnej inštalácií bolo potreba upraviť hlavný konfiguračný súbor pre DHCP */etc/dhcp/dhcpd.conf.* Pred úpravou, je vhodné spraviť si zálohu originálneho súboru pomocou príkazu

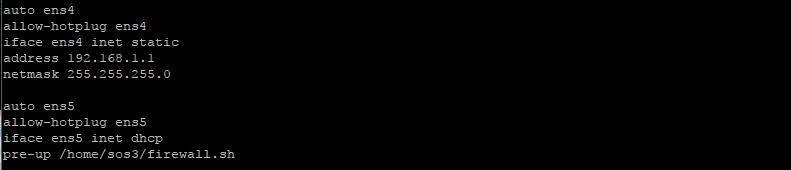
cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpdDEFAULT.conf

Požiadavkou bolo aby náš DHCP server prideľoval dynamicky IP adresu na zariadenie Klient na rozhraní ens5. Preto sme upravili súbor */etc/dhcp/dhcpd.conf* nasledovne ako je ukázané na obrázku. Podľa tejto konfigurácie, by mal server prideľovať IP adresy z rozsahu 192.168.2.100 – 192.168.2.200.



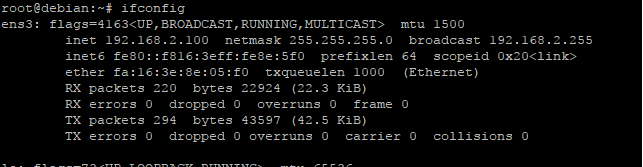
Obrázok 4. DHCP - konfiguračný súbor dhcpd.conf

Rovnako sme museli nastaviť statickú IP adresu pre DHCP server na rozhraní ens4 a povoliť dhcp na rozhranie ens5 v súbore */etc/network/interfaces* na zariadení Server-router.



Obrázok 5. Súbor interfaces na Server-Router

### Overenie DHCP

Po reštartovaní služby isc-dhcp-server a rozhrania eth5 sme otesovali či DHCP správne pridelil IP adresu na zariadení Klient. 

Obrázok 6. Príkaz ifconfig na zariadení Klient

Ako vidieť, zariadeniu Klient bola pridelená IP adresa zo zadaného rozsahu – 192.168.2.100 takže DHCP Server sme nakonfigurovali správne.

## DNS

### Konfigurácia

Ďalšou z našich úloh bolo nainštalovanie DNS serveru. Je potrebné mať DNS na inštalované na 2 serveroch pričom jeden sa bude správať ako Master a druhý ako Slave. Rozhodli sme sa, že Master bude Server 1 a Slave bude Server 2.

Na oba servery sme nainštalovali službu bind9 a nainštalovali balíčky súvisiace s DNS príkazmi:

apt-get install bind9

apt-get install dnsutils

Po úspešnej inštalácii sa nám vytvorili priečinky a súbory v zložke: */etc/bind*

Ako prvé si v tomto priečinku vytvoríme priečinok Master resp. Slave na Serveri 2

mkdir master

V tomto priečinku na serveri Master si vytvoríme zónové súbory:

* external.arpa
* internal.arpa
* private.sos3.local
* public.sos3.local

Sú to obyčajné textové súbory, ktoré budeme následne upravovať. Vytvoríme si prvý a to private.sos3.local príkazom:

nano private.sos3.local

Nasledujúce riadky vložíme na začiatok súboru:

$TTL 604800

@ IN SOA ns1.sos3.cc.uniza.sk. hostmaster.sos3.cc.uniza.sk. (

2017102302 ; Serial

604800 ; Refresh

86400 ; Retry

2419200 ; Expire

604800 ) ; Negative Cache TTL

Za kľúčovým slovom SOA sme použili názov zóny, ktorý je vyhradený pre našu skupinu. Taktiež sme tam dopísali adresu hostmaster.sos3.cc.uniza.sk.

Veľmi dôležitým údajom je hodnota Serial. Vždy, keď upravíme tento zónový súbor, treba zvýšiť hodnotu čísla Serial. Slave server sa pozerá na túto hodnotu a pokiaľ v zónovom súbore Mastra je táto hodnota vyššia ako v aktuálnom zónovom súbore Slave-a Slave server si tento zónovy súbor aktualizuje podľa Mastra. Odporúča sa ju písať vo formáte YYYYMMDDVV kde:

* YYYY znamená rok kedy bola zmena vykonaná
* MM znamená mesiac kedy bola zmena vykonaná
* DD znamená deň kedy bola zmena vykonaná
* VV znamená koľko krát bol súbor upravený v danom dni

Za touto sekciou pridáme nasledovné riadky:

@ IN NS ns1.sos3.cc.uniza.sk.

@ IN NS ns2.sos3.cc.uniza.sk.

Tieto záznamy ukazujú, adresu DNS serverov v našej doméne.

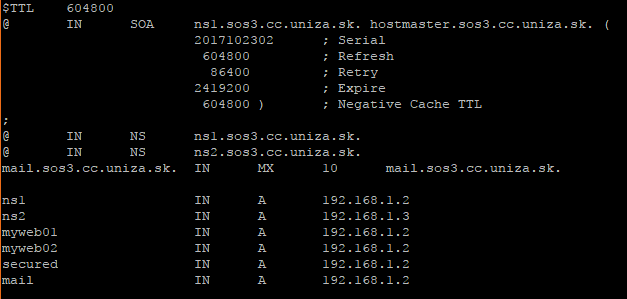
Na koniec dopíšeme tieto riadky:

ns1 IN A 192.168.1.2

ns2 IN A 192.168.1.3

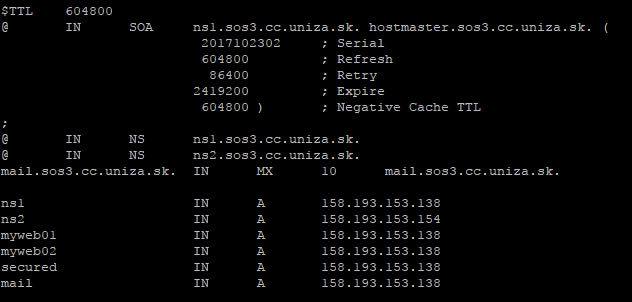
Tu sú konkrétne IP adresy pre DNS servery v našej sieti.

Na nasledujúcom obrázku môžeme vidieť kompletný zónový súbor private.sos3.local, ktorý má doplnené záznamy pre web server a mailový server.



Obrázok 7: Zónový súbor private.sos3.local

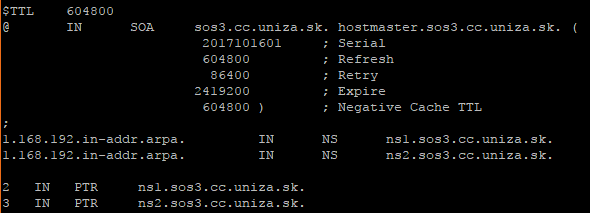
Podobne si vytvoríme aj zónový súbor pre verejnú sieť a to súbor *public.sos3.local*, ktorý bude vyzerať nasledovne.



Obrázok 8: Zónový súbor public.sos3.local

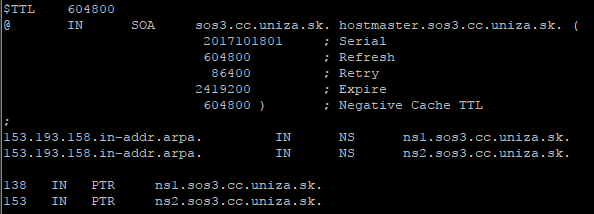
Tento zónový súbor vyzerá podobne lenže namiesto privátnych IP adries sú tu zapísané verejné IP adresy.

Okrem toho si vytvoríme aj reverzné zónové súbory. Reverzný zónový súbor *internal.arpa* bude vyzerať nasledovne.



Obrázok 9: Reverzný zónový súbor internal.arpa

Reverzný zónový súbor *external.arpa* bude vyzerať nasledovne.



Obrázok 10: Reverzný zónový súbor external.arpa

Ďalším krokom je vytvorenie pohľadov. Pohľady pomáhajú pri preklade adries určiť, či vrátia IP adresu z verejného rozsahu alebo so súkromného podľa toho či požiadavka na preklad bola z vnútornej alebo vonkajšej siete. Na Serveri 1 v priečinku */etc/bind* upravíme konfiguračný súbor *named.conf.local* a to vložením nasledujúceho kódu:

key "kinternal" {

algorithm hmac-md5;

secret "4KryvrJV417YLWOjEBV0Ow==";

};

key "kexteranal" {

algorithm hmac-md5;

secret "9IbBLWy6ykOvl3cDbyh6Cw==";

};

acl "internal" {

!key kexternal;

key kinternal;

192.168.0.0/16;

};

acl "external" {

!key kinternal;

//key kexternal;

any;

};

view "Internal" {

match-clients { internal; }; //nazov ACL

allow-transfer{ key kinternal; }; //nazov kluca pre zonu internal

zone "sos3.cc.uniza.sk" { // domena zony

type master; //typ master/slave

file "/etc/bind/master/private.sos3.local";//cesta k zonovemu suboru

allow-query { any; };

//allow-transfer { 192.168.1.3 key kinternal; };

};

zone "1.168.192.in-addr.arpa" {

type master;

file "/etc/bind/master/internal.arpa";

notify yes;

allow-query { any; };

//allow-transfer {192.168.1.3 key kinternal;};

};

};

view "World" {

match-clients {any;};

allow-transfer{ key kexternal; };

zone "sos3.cc.uniza.sk" {

type master;

file "/etc/bind/master/public.sos3.local";

allow-query {any;};

//allow-transfer {192.168.1.3 key kexternal;};

};

zone "153.193.158.in-addr.arpa" {

type master;

file "/etc/bind/master/external.arpa";

notify yes;

allow-query { any; };

//allow-transfer {192.168.1.3 key kexternal;};

};

};

Prvé dve sekcie popisujú kľúče použité pri overení transferov súborov medzi Master a Slave. Je dôležité aby sa hodnota poľa „secret“ zhodovala na serveri Master aj Slave. Tieto kľúče vygenerujeme použitím príkazu:

dnssec-keygen -a HMAC-MD5 -b 128 -n HOST rndc-key

Po zadaní tohto príkazu sme dostali output:

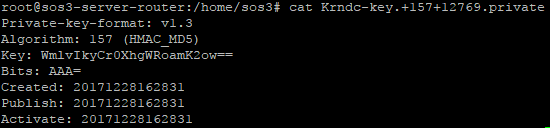
Krndc-key.+157+12769

V priečinku, v ktorom sa práve nachádzame sa vytvorili dva súbory. Krndc-key.+157+12769.key a Krndc-key.+157+12769.private

Otvoríme si súbor Krndc-key.+157+12769.private príkazom:

cat Krndc-key.+157+12769.private

Súbor vyzerá nasledovne:



Obrázok 11: Súbor Krndc-key.+157+12769.private

Skopírujeme hodnotu „Key:“ a uložíme ju do súboru *named.conf.local* do poľa „secret“.

Ďalšie dve sekcie popisujú pravidlá pre ACL. Pre ACL „internal“ špecifikujeme, z akej siete sa môžu dotazovať na DNS záznamy.

V ďalšej sekcii nastavujeme pohľad „Internal“. Nastavíme, ktorý zoznam pravidiel ACL bude použitý, ktorý kľúč bude použitý a pre každú zónu informácie o zóne ako napríklad meno domény, typ servera (Master alebo Slave) alebo cesta k zónovemu suboru. Treba popísať normálny zónový súbor a aj reverzný zónový súbor.

Na Slave serveri by tento súbor vyzeral nasledovne:

key "kinternal" {

algorithm hmac-md5;

secret "4KryvrJV417YLWOjEBV0Ow==";

};

key "kexteranal" {

algorithm hmac-md5;

secret "9IbBLWy6ykOvl3cDbyh6Cw==";

};

acl "internal" {

!key kexternal;

key kinternal;

192.168.0.0/16;

};

acl "external" {

!key kinternal;

//key kexternal;

any;

};

view "Internal" {

match-clients { internal; }; //nazov ACL

zone "sos3.cc.uniza.sk" { // domena zony

type slave; //typ master/slave

file "/etc/bind/slave/private.sos3.local";//cesta k zonovemu suboru

masters{192.168.1.2 key internal;};

allow-query { any; };

};

zone "1.168.192.in-addr.arpa" {

type slave;

file "/etc/bind/slave/internal.arpa";

notify yes;

allow-query { any; };

masters{192.168.1.2 key internal;};

};

};

view "World" {

match-clients {external;};

zone "sos3.cc.uniza.sk" {

type slave;

file "/etc/bind/slave/public.sos3.local";

allow-query {any;};

masters{192.168.1.2 key external;};

};

zone "153.193.158.in-addr.arpa" {

type slave;

file "/etc/bind/slave/external.arpa";

notify yes;

allow-query { any; };

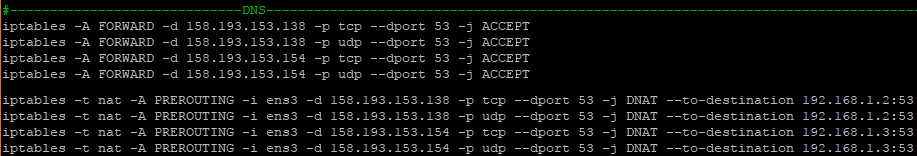
masters{192.168.1.2 key external;};

};

};

### Výnimky pre Firewall

Ďalej pridáme výnimky do skriptu pre firewall firewall.sh na serveri Server-router.



Obrázok 12: Vynimky vo firewalle pre DNS

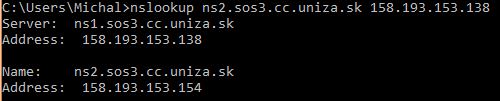
### Overenie

Po vykonaní všetkých potrebných zmien a nastavení je potrebné reštartovať službu bind9 na Serveri 1 a spustiť skript pre firewall na serveri Server-router.

Funkčnosť nášho DNS servera sme overili cez príkazový riadok príkazom:

nslookup ns2.sos3.cc.uniza.sk 158.193.153.138

Výsledok môžeme vidieť na nasledujúcom obrázku.



Obrázok 13: Overenie funkčnosti DNS serveru

## Apache

### HTTP

Ako prvé spravíme update balíčkov a nainštalujeme službu Apache2 na Server1 príkazmi:

apt-get update

apt-get install apache2

Po inštalácii vyvoríme v priečinku */etc/apache2/sites-available* 2 virtualhosty s názvami 001-web1.conf a 002-web2.conf s nasledovonou konfiguráciou:

|  |  |
| --- | --- |
| 001-web1.conf | 002-web2.conf |
| <VirtualHost \*:80>  ServerName web1.sos3.cc.uniza.sk  ServerAdmin webmaster@localhost  DocumentRoot /var/www/web1  ErrorLog ${APACHE\_LOG\_DIR}/web1-error.log  CustomLog ${APACHE\_LOG\_DIR}/web1-access.log combined  </VirtualHost> | <VirtualHost \*:80>  ServerName web2.sos3.cc.uniza.sk  ServerAdmin webmaster@localhost  DocumentRoot /var/www/web2  ErrorLog ${APACHE\_LOG\_DIR}/web2-error.log  CustomLog ${APACHE\_LOG\_DIR}/web2-access.log combined  </VirtualHost> |

Tabuľka 2: Konfigurácia virtual hostov Apache

V pričinku */var/www/* si vytvoríme pričinky web1 a web2 a do oboch priečinkov vytvorím html súbor index.html. Pre testovacie účely sme vytvorili jednoduchú stránku so zdrojovým kódom:

<HTML>

<BODY>

This is web1 test webpage.

</BODY>

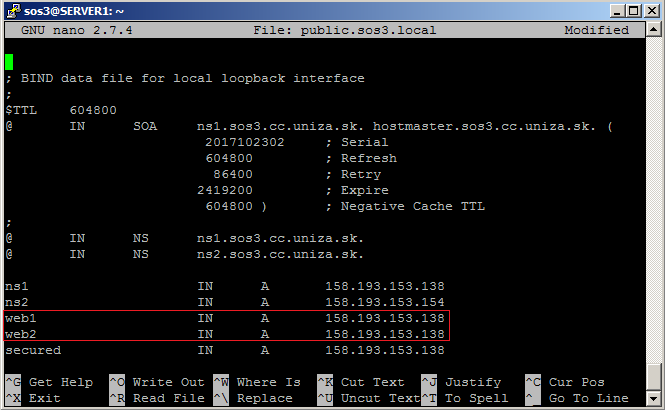
</HTML>

Aby tieto stránky správne fungovali musíme ich v apachi povoliť a to príkazmi:

a2ensite web1.conf

a2ensite web2.conf

Ďalším krokom je nastavenie dns záznamov a výnimky vo firewalle a to úpravou súboru */etc/bind/master/public.sos3.local* podľa nasledujúceho obrázku. Doplníme to, čo je na obrázku v červenom rámčeku.

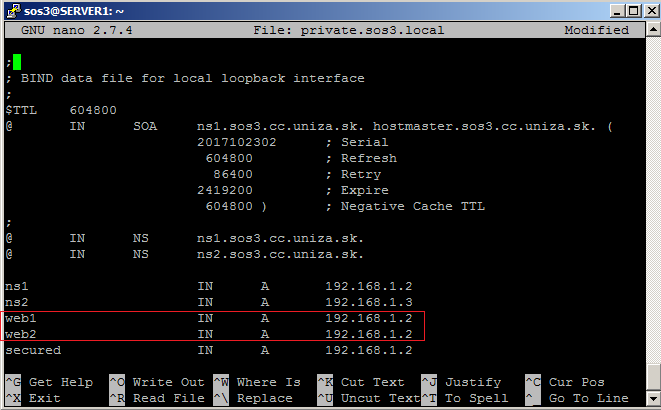


Obrázok 14: Public DNS záznam pre HTTP

Pozn: Treba zvýšiť seriové číslo zonoveho suboru.

Pozn2: Na snímke vidieť záznam secured, ktorý je vytvorený pre HTTPS stránku. Môžme si ho vytvoriť teraz alebo neskôr. Nič sa nestane ak sa vytvorí hneď.

Tak isto treba upraviť aj zónový súbor pre internú sieť */etc/bind/master/private.sos3.local*



Obrázok 15: Private DNS záznam pre HTTP

Ďalej sme upravili konfiguráciu pre firewall na server-router a to pridaním nasledovných riadkov:

iptables -A FORWARD -d 192.168.1.0/24 -p tcp --dport 80 -j ACCEPT

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 80 -j DNAT --to-destination 192.168.1.2:80

Uložíme zmeny a reštartujeme všetky potrebné služby a skripty, pre ktoré sme upravovali konfiguračné súbory. Tj. spustíme skript /home/sos3/firewall.sh a reštartujeme služby bind9 a apache2.

Po týchto úpravách by nám stránka web1.sos3.cc.uniza.sk mala fungovať.

(Treba si dať pozor na DNS, v našom prípade nefungovali glue recordy a museli sme si ručne nastaviť ip adresu DNS servera v nastavenia rozhrania Ethernet).

### HTTPS

Ako prvé musíme aktivovať SSL modul a to príkazom:

a2enmod ssl

Reštartujeme apache2.

Vytvoríme si priečinok kde uložíme certifikát a kľúč.

mkdir /etc/apache2/ssl

Vygenerujeme certifikát a kľúč, ktoré uložíme do */etc/apache2/ssl* a to príkazom:

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/apache2/ssl/apache.key -out /etc/apache2/ssl/apache.crt

Po zadaní tohto príkazu nám bude položených niekoľko otázok: Odpovede budú vyzerať nejako takto:

Country Name (2 letter code) [AU]: SK  
State or Province Name (full name) [Some-State]: Slovakia  
Locality Name (eg, city) []: Zilina  
Organization Name (eg, company) [Internet Widgits Pty Ltd]: sos3  
Organizational Unit Name (eg, section) []: KIS  
Common Name (e.g. server FQDN or YOUR name) []: sos3.cc.uniza.sk  
Email Address []: [webmaster@sos3.cc.uniza.sk](mailto:webmaster@sos3.cc.uniza.sk)

Teraz vytvoríme virtualhosta v priečinku */etc/apache2/sites-available/*

Skopírujeme a upravíme defaultny subor.

cp default-ssl.conf webSSL.conf

Otvoríme a upravíme súbor webSSL.conf nasledovne:

<IfModule mod\_ssl.c>

<VirtualHost \*:443>

ServerAdmin webmaster@localhost

ServerName secured.sos3.cc.uniza.sk

ServerAlias www.secured.sos3.cc.uniza.sk:443

DocumentRoot /var/www/securedweb

ErrorLog ${APACHE\_LOG\_DIR}/error.log

CustomLog ${APACHE\_LOG\_DIR}/access.log combined

SSLEngine on

SSLCertificateFile /etc/apache2/ssl/apache.crt

SSLCertificateKeyFile /etc/apache2/ssl/apache.key

<FilesMatch "\.(cgi|shtml|phtml|php)$">

SSLOptions +StdEnvVars

</FilesMatch>

<Directory /usr/lib/cgi-bin>

SSLOptions +StdEnvVars

</Directory>

#BrowserMatch "MSIE [2-6]" \

# nokeepalive ssl-unclean-shutdown \

# downgrade-1.0 force-response-1.0

</VirtualHost>

</IfModule>

Vyzerá to komplikovane ale našťastie stačí upraviť len niekoľko vecí a to riadky zvýraznené červenou farbou.

Treba vytvoriť html súbor v zložke */var/www/secured* s názvom index.html. Odporúčam použiť podobný kód ako pre stránku web1.

Po týchto všetkých krokoch povolíme stránku príkazom: *a2ensite webSSL.conf*

Reštartujeme apache.

service apache2 restart

Upravíme DNS záznam pridaním nasledovného riadku do súboru /etc/bind/master/public.sos3.local.

secured IN A 158.193.153.138

Obdobnú úpravu spravíme aj pre *private.sos3.local*

Reštartujeme bind9.

Posledná vec ktorú upravíme je skript pre firewall a pridáme príkazy:

iptables -A FORWARD -d 192.168.1.0/24 -p tcp --dport 443 -j ACCEPT

iptables -t nat -A PREROUTING -i ens3 -d 158.193.153.138 -p tcp --dport 443 -j DNAT --to-destination 192.168.1.2:443

Uložíme a spustíme skript.

Webstránka *https://secured.sos3.cc.uniza.sk* by mala fungovať.

Použitý certifikát je self-signed takže bude treba udeliť mu výnimku v prehliadači.

## NTP

Updatetneme balíčky a nainštalujeme ntp príkazmi:

apt-get update

apt-get install ntp

Upravíme konfiguračný súbor služby NTP „*nano /etc/ntp.conf“*

Nastavíme synchronizáciu na 0.sk.pool.ntp.org príkazom

pool 0.sk.pool.ntp.org iburst

Nastavenie obmedzenia prístupu len zo siete 192.168.1.0/24

Do konfiguračného súboru dopíšem riadok:

restrict 192.168.1.0 mask 255.255.255.0 nomodify notrap

Reštartujem službu a nastavím aby sa spustila po reštartovaní systému príkazmi:

systemctl restart ntp

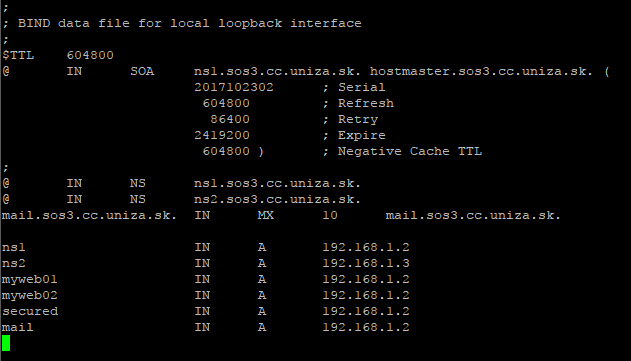
systemctl enable ntp

## Mailová služba

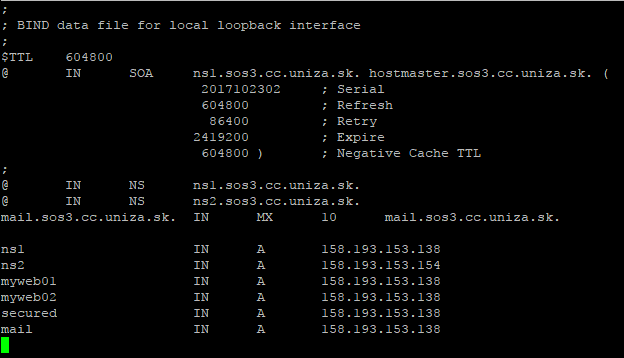
Keď sme nainštalovali webový server, bola nám zadaná úloha vytvoriť mailovú službu na serveri. Rozhodli sme sa, že ju nainštalujeme na server kde už je pripravený webový server Apache, tj. na zariadenie Server1. Medzi používané protokoly pre poskytnutie tejto služby patria SMTP, POP3 a IMAP. Ako SMTP server sme zvolili postfix balík a pre implementáciu POP3, resp IMAP použijeme balík dovecot a pre jednoduchší prístup do mailovej schránky pomocou webového rozhrania sme použili voľne dostupný Squirrelmail.

### Pridanie RR do DNS zóny

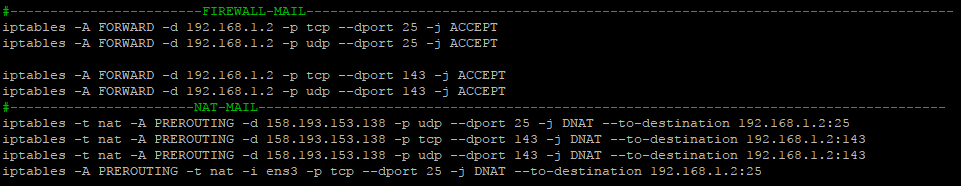
Z dôvodu správneho fungovania sme museli vložiť MX záznam do zónového súboru DNS master servera tak, aby ukazoval na server s nainštalovanou mailovou službou a pridať **NAT** pravidlo do **iptables** z dôvodu aby bol možný verejný prístup.



Obrázok 16. Súbor private.sos3.local



Obrázok 17. Súbor public.sos3.local



Obrázok 18. Úprava firewall.sh z dôvodu funkčnosti mailovej služby

### Konfigurácia SMTP

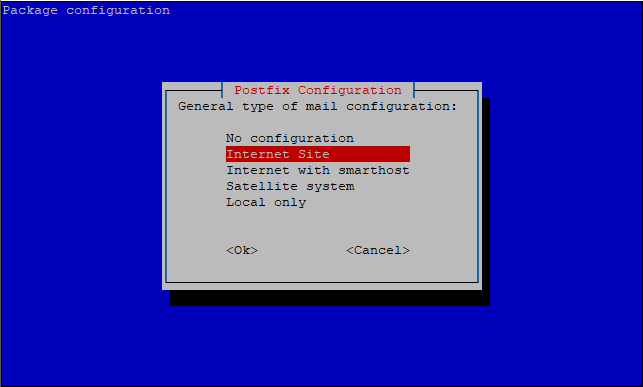
Neskôr sme nainštalovali SMTP server – Postfix pomocou príkazov

#apt-get update

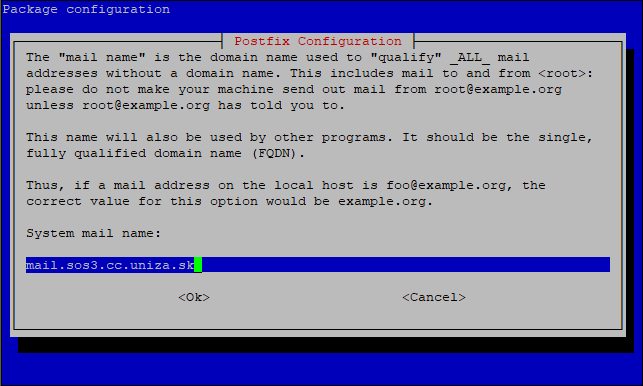
#apt-get install postfix

Pri inštalovaní sa nás systém opýta len dve otázky ohľadne konfigurácie, preto musíme nanovo vyžiadať konfiguráciu tohto balíka po dokončení inštalácie pomocou príkazu

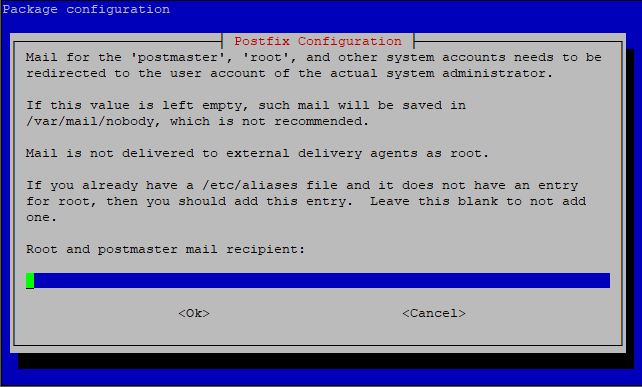
#dpkg-reconfigure -plow postfix

1. Všeobecný typ konfigurácie pošty – Vybrali sme typ „Internetová lokalita“ (Internet Site) ktorá je predvolenou možnosťou a obsahuje základnú konfiguráciu 

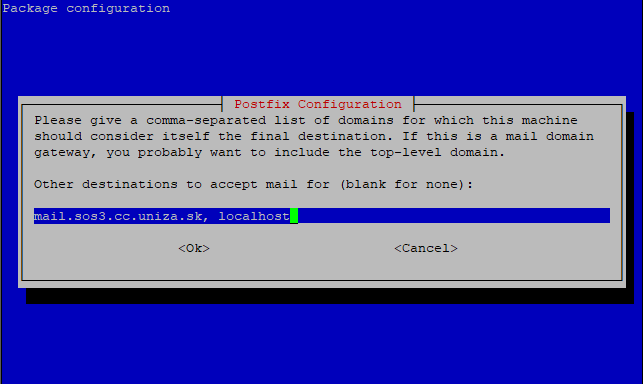
Obrázok 19. Všeobecný typ konfigurácie pošty

1. Poštový názov systému – Názov nášho servera, ktorý uvedieme aj do MX záznamu DNS, mail.sos3.cc.uniza.sk 

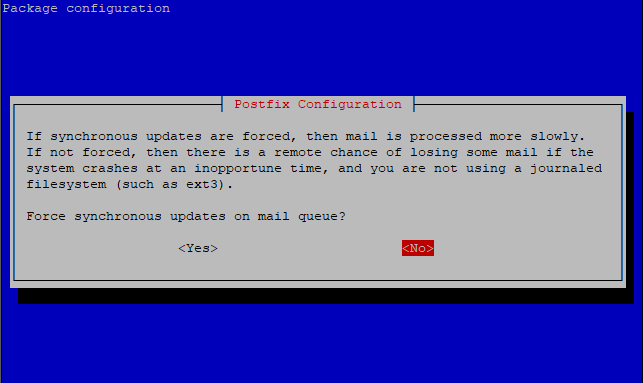
Obrázok 20. Poštový názov systému

1. Príjemca pošty pre používateľov root a postmaster – Slúži na definovanie aliasu pre užívateľov root a postmaster, na ktorý budú smerované správy. Nechávame prázdne. 

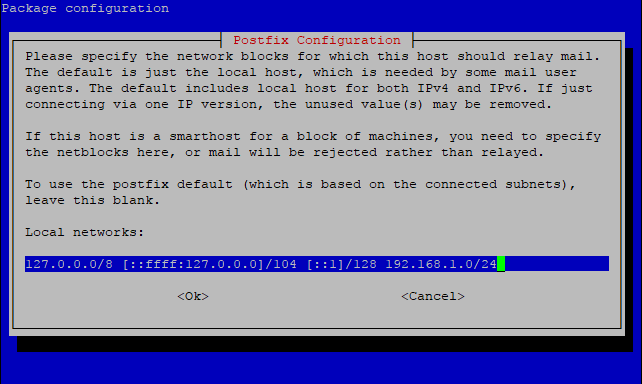
Obrázok 21. Príjemca pošty pre používateľov root a postmaster

1. Iné destinácie pre príjmanie pošty – Domény, ktoré tento server obsluhuje. Pridali sme našu doménu „mail.sos3.cc.uniza.sk“ a „localhost“ 

Obrázok 22. Iné destinácie pre príjmanie pošty

1. Vynútenie synchrónnej aktualizácie poštového frontu – Ak je vynútená, môže byť spracovávanie pošty pomalšie, avšak naopak, je možná strata pošty ak sa systém zrúti v nevhodnom okamihu. Volíme možnosť „Nie“ 

Obrázok 23. Synchrónne aktualizácie pošty

1. Lokálne siete – Táto voľba slúži podobne ako DHCP-Relay, pomocou ktorej je možné zabrániť šíreniu SPAMu. Pridali sme našu lokálnu sieť 

Obrázok 24. Lokálne siete

1. Ostatné otázky – Ponechávame predvolené nastavenia.

Zložka */etc/postfix/* obsahuje konfiguračné súbory pre službu postfix, medzi ktorými nájdeme aj hlavný konfiguračný súbor main.cf ktorý ešte dodatočne upravíme. Otvoríme ho pomocou editora a zmeníme hodnotu parametra **myhostname** na **mail.sos3.cc.uniza.sk**.

### Konfigurácia POP3

Pre správne fungovanie, sme museli nainštalovať POP3 pomocou príkazu

# apt-get install dovecot-pop3d

Konfiguračné súbory pre dovecot môžeme nájsť v zložke */etc/dovecot/.* Pre potrebu bezpečnosti je potrebné zakázať plain-text autentifikáciu cez dovecot pomocou úpravy v súbore */etc/dovecot/conf.d/10-auth.conf* kde zmeníme hodnotu parametra **disable\_plaintext\_auth** na hodnotu „**yes**“.

### Konfigurácia SquirrelMail

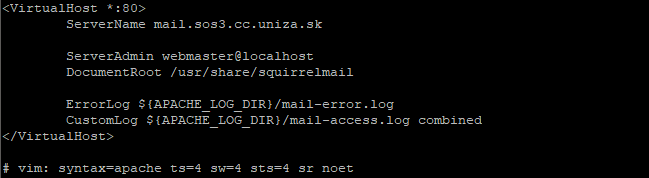
Pre jednoduchší prístup do našej mailovej schránky ako bolo vyššie spomenuté, sme využili voľne dostupný Squirrelmail. Avšak, zo začiatku sa nám nedarilo ho nainštalovať cez príkaz

# apt-get install squirrelmail

Preto sme museli pridať nový záznam do súboru */etc/apt/sources.list* aby mohol systém stiahnuť a nainštalovať požadovaný balík.

deb http://archive.ubuntu.com/ubuntu xenial universe

Konfiguračné súbory pre SquirrelMail nájdeme umiestnené v zložke */etc/squirrelmail*. V tejto zložke je možné nájsť conf.pl skript, pomocou ktorého je možné nakonfigurovať Squirrelmail. Spustíme tento skript a zvolíme predvolenú konfiguráciu (D), nasledovne zvolíme možnosť dovecot pre POP3 server a potvrdíme. Nastavenie domény na našu docielime pomocou postupnosti volieb *2->1* a ako hodnotu napíšeme „**mail.sos3.cc.uniza.sk**“, uložíme (S) a ukončíme (Q).

Aby squirrelmail dokázal komunikovať s webovým serverom (apache2), vytvorili sme samostatnú lokalitu pre našu mailovú službu. V zložke */etc/squirrelmail/* je default-ne vytvorený súbor apache.conf, ktorý sme prekopírovali do zložky */etc/apache2/sites-enabled* pod názvom **003-mail.sos3.local.conf** a upravili ako je na nasledujúcom obrázku 

Obrázok 25 Súbor 003-mail.sos3.local.conf

Pomocou príkazu *a2dissite* sme zakázali ostatné lokality a povolili iba lokalitu týkajúcu sa squirrelmail-u

a2dissite <lokalita.conf>

a2ensite 003-mail.sos3.local.conf

### Testovanie Mailovej služby

Po nainštalovaní a nakonfigurovaní, sme si vytvorili dvoch nových užívateľov mailuser1 a mailuser2 pre overenie funkčnosti mailovej služby pomocou príkazu

# adduser <názov\_užívateľa>

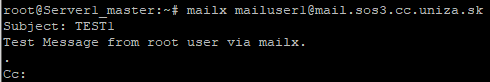
Kvôli bezpečnosti sme týmto novovytvoreným užívateľom odobrali právo používať shell (bash) a prístup k systému pomocou príkazu

# chsh -s /bin/false <názov\_užívateľa>

Po vytvorení „mailových“ užívateľov sme si nainštalovali jednoduchého mailového klienta mailx pomocou príkazu

# apt-get install bsd-mailx

Pre otestovanie posielania správ sme pomocou mailx príkazu skúsili poslať mail na používateľa [mailuser1@mail.sos3.cc.uniza.sk](mailto:mailuser1@mail.sos3.cc.uniza.sk) a kontrolu, či email prišiel sme vykonali cez prehliadač.



Obrázok 26. Vytvorenie mailu

Obrázok, na ktorom je snímka obrazovky

Popis vygenerovaný s veľmi vysokou spoľahlivosťou

Obrázok 27. Overenie poslaného mailu

## SYSLOG-NG

### Konfigurácia

Nainštalovali sme aplikáciu Syslog-ng na serveri, kde tento program nebol nainštalovaný príkazom:

apt-get install syslog-ng

Rozhodli sme sa, že na Server 1 budeme ukladať logy z ostatných serverov. Ako prvé si v sekcii „Options“ v konfiguračnom súbore */etc/syslog-ng/syslog-ng.conf* upravíme alebo doplníme nasledujúce riadky:

keep\_hostname(yes);

create\_dirs(yes);

Na koniec tohto súboru doplníme nasledovné riadky:

destination bindd {file("/var/log/bind.log");}; #kde sa bude logovat

filter filter1 {program("named");}; #filter pre aky program

log {source(s\_src); filter(filter1); destination(bindd); }; #vytvorenie pravidla

Vďaka tomuto kódu nám bude logovať všetko čo sa týka DNS na tomto serveri. Ukladať to bude do súboru */var/log/bind.log.*

Aby sme mohli prijímať logy z iných serverov potrebujeme nastaviť, cestu k súboru kde bude logy zo serverov ukladať a ako ich bude rozpoznávať, že sú určené k uloženiu na tomto serveri. To dosiahneme pripísaním nasledovných riadkov na koniec súboru.

source clients { syslog(ip(192.168.1.2) transport("tcp")); };

destination clientslogs {

file("/var/log/debian-edu/$YEAR$MONTH$DAY/$HOST.auth");

};

Ďalším krokom je nastavenie odosielania logov z iných serverov. Pre testovacie účely sme zvolili Server 2. Na tomto serveri sme upravili konfiguračný súbor */etc/syslog-ng/syslog-ng.conf* a doplnili nasledujúce riadky:

destination d\_network { syslog("192.168.1.2" transport("tcp")); };

log {source(s\_src); destination(d\_network); };

destination d\_local { file("/var/log/messages/logy"); };

log { source(s\_src); destination(d\_local); };

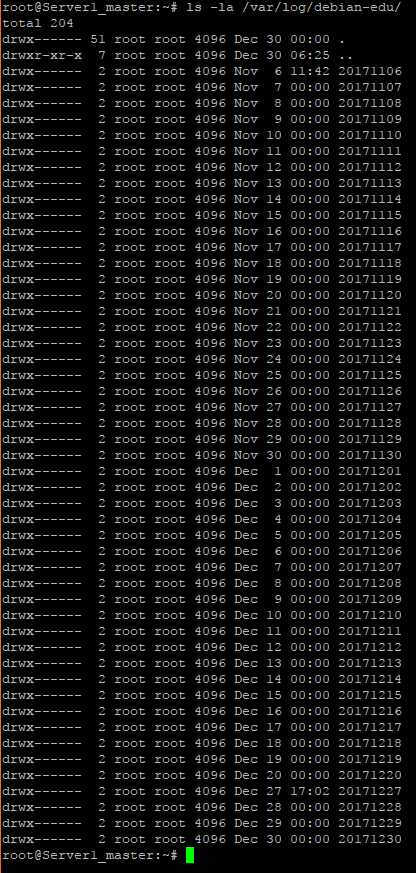
Po vykonaní týchto nastavení a reštartovaní programu syslog-ng na serveroch, kde sa upravovali ich konfiguračné súbory sa spustilo logovanie na Server 1.

### Overenie

Aby sme overili, že logovanie na vzdialený server funguje v poriadku skontrolujeme na Serveri 1 zložku */var/log/debian-edu/* príkazom:

ls –la /var/log/debian-edu

V našom prípade to vrátilo takýto výstup:

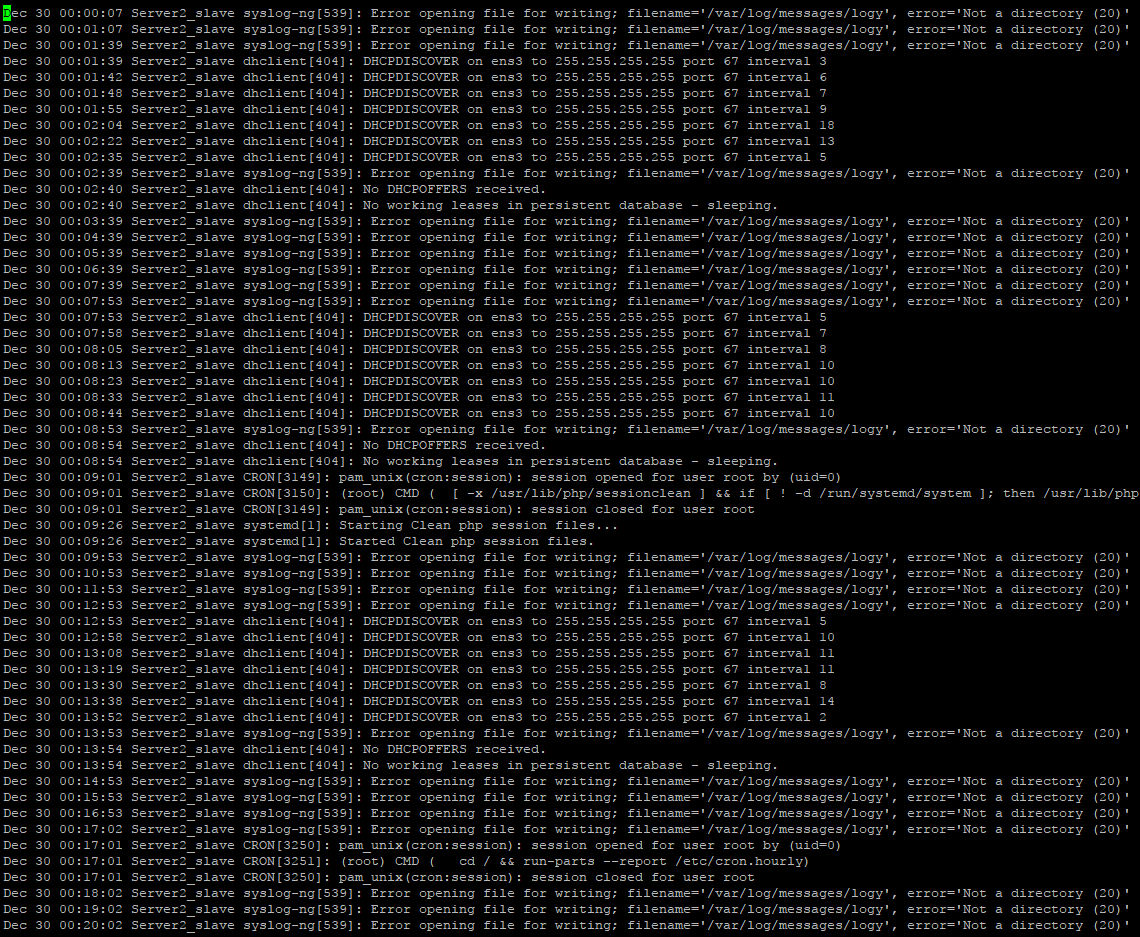


Obrázok 28: Výpis obsahu zložky /var/log/debian-edu

Ak chceme overiť či úspešne zapisuje do týchto súborov otvoríme si napríklad najnovší priečinok. V ňom sa nachádza jeden súbor:

Server2\_slave.auth

V tomto súbore sú zapísané logy a vyzerá to ako na nasledujúcom obrázku:



Obrázok 29: Logy zo serveru 2 uložené na serveri 1

# Riešenie pre OS Windows

## Topológia zapojenia

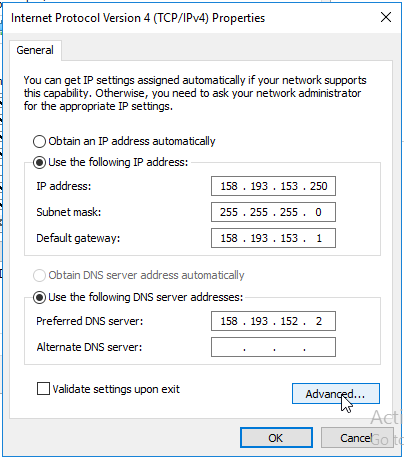
|  |  |  |  |
| --- | --- | --- | --- |
| Názov zariadenia | Rozhranie | IP adresa | Popis |
| Widnows\_server\_router | Ethernet2 | 158.193.153.246  158.193.153.250 | Rozhranie pripojené k internetu |
|  | Ethernet | 192.168.1.1 | Rozhranie pripojené k sieti so servermi |
|  | Ethernet3 | 192.168.2.1 | Rozhranie pripojené k sieti s klientom |
| Server1 | Ethernet | 192.168.1.2 |  |
| Server2 | Ethernet | 192.168.1.3 |  |
| Klient | Ethernet3 | 192.168.2.2 |  |

Tabuľka 3: Adresný plán Windows

## Prvotné nastavenia

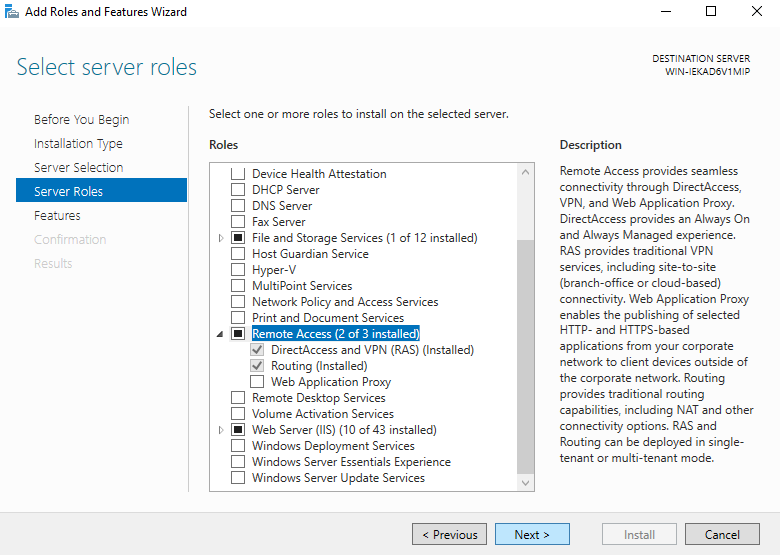
Ako prvé som zmenil heslo na Administrátora na všetkých zariadeniach. Zároveň som nastavil statické IP adresy pre zriadenia Server1, Server2, klient a pre rozhrania smerujúce do privátnej siete na zariadení Server-router.

Pre server-router som nastavil statickú IP adresu 158.193.153.246/24 s bránou 158.193.153.1. Pridal som jej aj druhú IP adresu 158.193.153.250/24 klknutím na tlačidlo Advanced (Viď obrázok) a kliknutím na tlačidlo Add address.

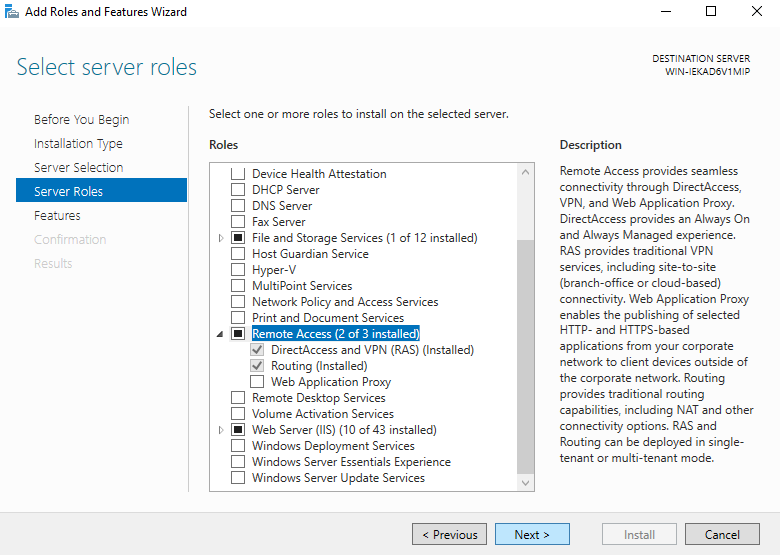


Obrázok 30: Nastavenie IP adries na serveri Server-router

## Nastavenie routovania na Server-router

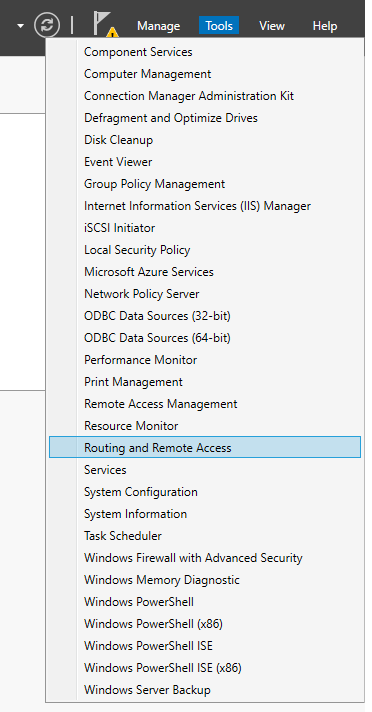
V aplikácii Server Manager klikneme na „Add roles and features“, vyberieme rolu „Remote Access“ a zbehneme inštaláciu. 

Obrázok 31: Nastavenie smerovania na Server-router obr. 1

Následne kliknutím na „Tools“ -> „Services“ zapneme službu „Service routing and remote access“ a nastavíme, aby sa automaticky spúšťal po štarte. 

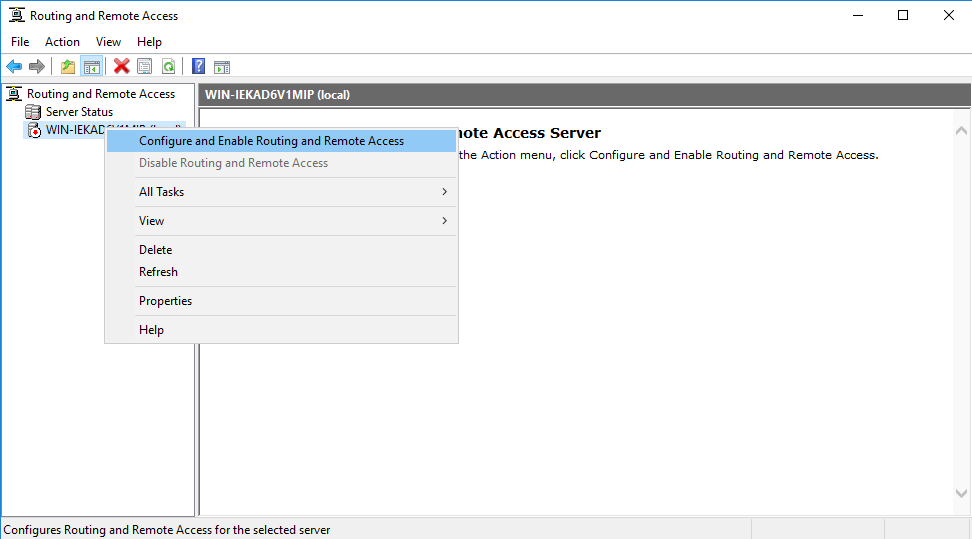
Obrázok 32: Nastavenie smerovania na Server-router obr. 2

Ďalej klikneme na „Tools - Routing and remote access“

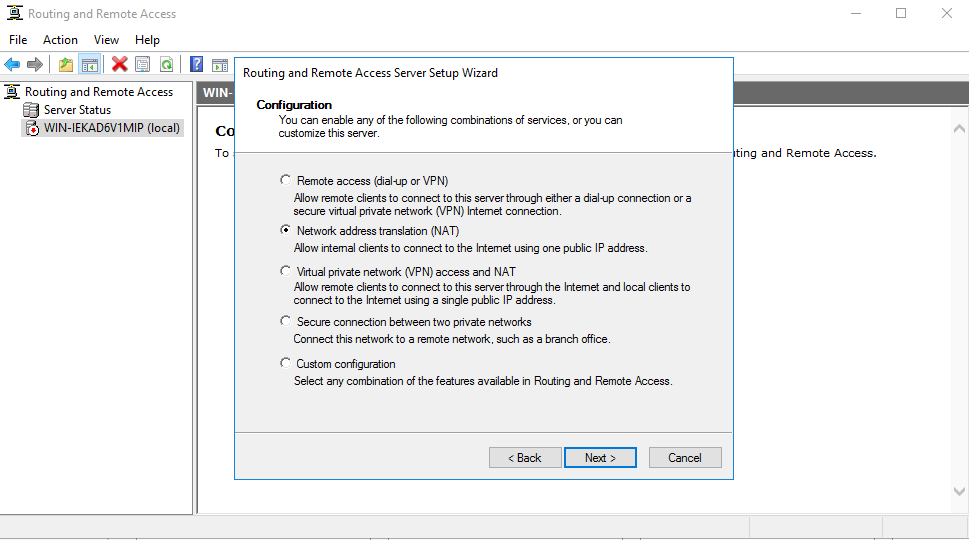


Obrázok 33: Nastavenie prekladania NAT na Server-router obr. 1

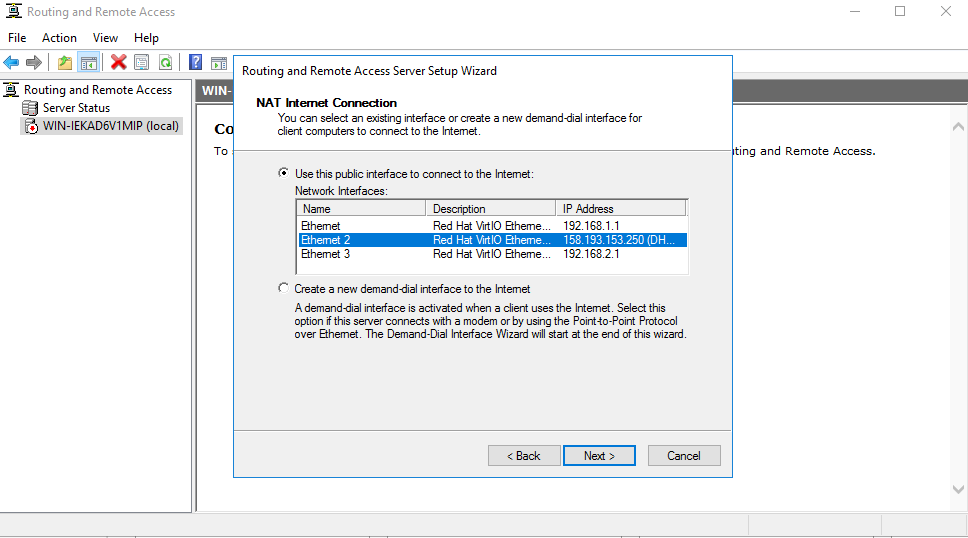
Nakonfigurujem NAT prekladanie pre rozhranie Ethernet.



Obrázok 34: Nastavenie routovania na Server-router obr. 4

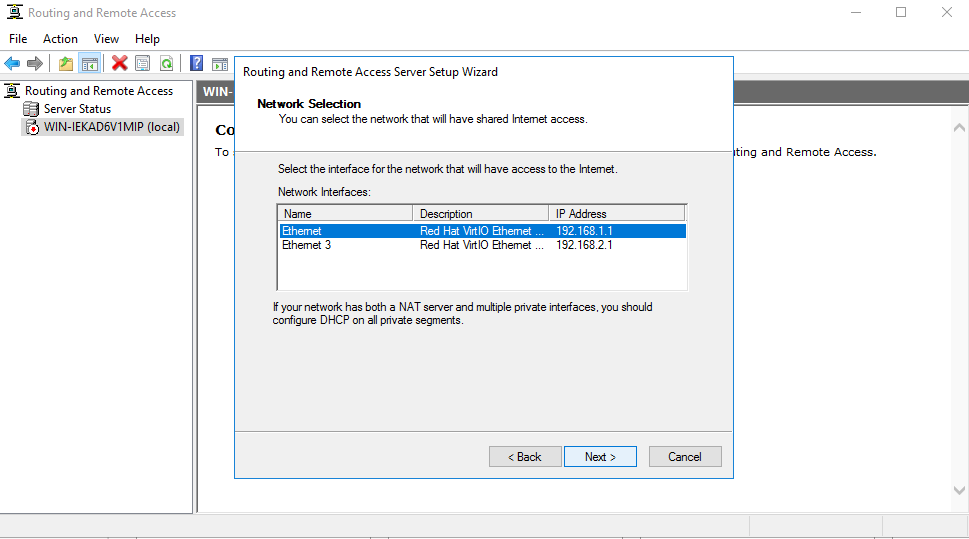


Obrázok 35: Nastavenie prekladania NAT na Server-router obr. 2



Obrázok 36: Nastavenie prekladania NAT na Server-router obr. 3

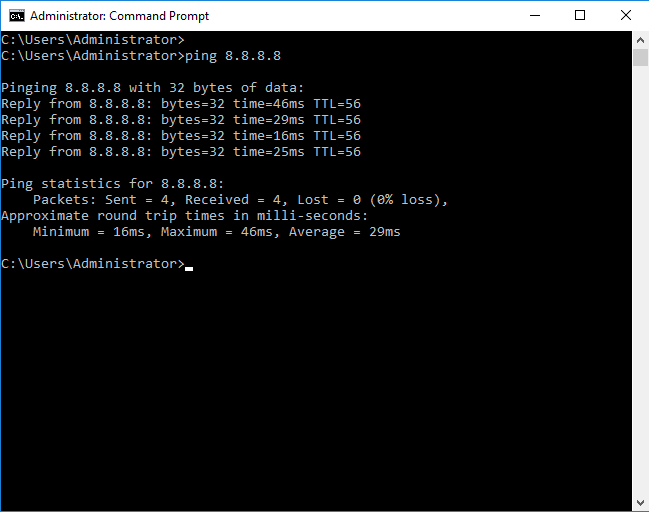
Ako verejné rozhranie nastavím Ethernet2, ktorým sme pripojený do internetu.



Obrázok 37: Nastavenie prekladania NAT na Server-router obr. 4

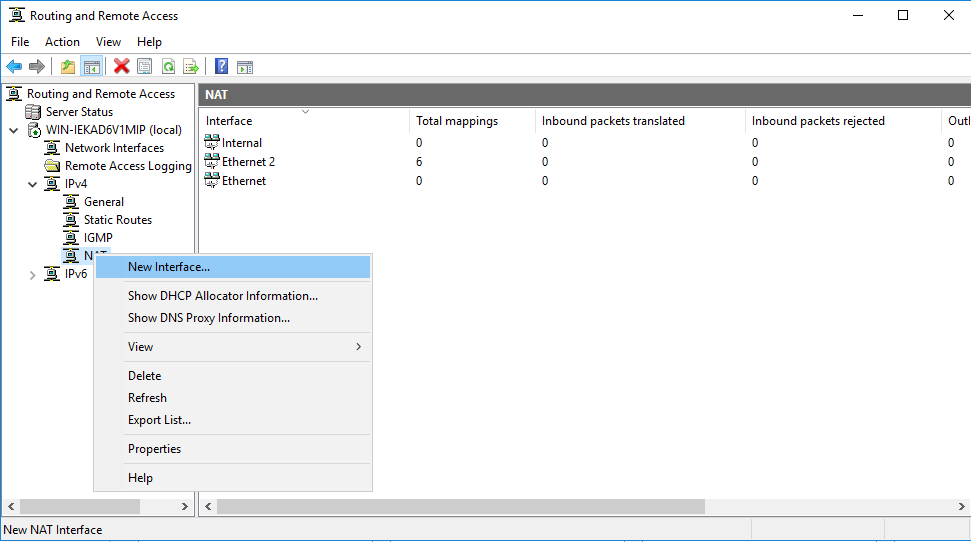
Ako privátne rozhranie nastavím Ethernet, ku ktorému sú pripojené naše servery.

Otestujem konektivitu Serveru 1 príkazom ping 8.8.8.8



Obrázok 38: Testovanie NAT na Serveri 1

Pridáme si aj nové rozhranie pre sieť s klientom (192.168.2.0/24). Nastavíme ho podobne ako v predchádzajucom postupe.



Obrázok 39: Nastavenie prekladania NAT na Server-router obr. 5

Otestujeme konektivitu na zariadenia klienta prikazom ping 8.8.8.8

## Port forwarding pre Remote Desktop

Port forwarding pre používanie služby remote desktop sme spustili na zariadení Server-router pomocou príkazového riadku a to nasledovným príkazom:  
*netsh interface portproxy add v4tov4 listenport=5001 listenaddress=158.193.153.250 connectport=3389 connectaddress=192.168.1.2*

Port na ktorom bude “počúvať” Server-router je 5001 ak sa chceme pripojiť na Server1.

Obdobne nastavíme porty aj pre Server2 (5002) a Klient (5003).

Posledný krok je povoliť porty 5001-5003 na firewalle serveru Server-router. V nastaveniach firewallu vytvoríme nový Inbound rule kde nastavíme povolenie TCP portov 5001-5003. Uložíme a port forwarding funguje.

Pri mojom testovaní aj po správnom nakonfigurovaní Remote Desktop sekal a odpájal sa. Vyriešili sme to nastavením hodnoty MTU pre packety na 1400. Na chvíľu to pomohlo, no nakoniec sa zdá, že problém je niekde inde.

## DNS Server

Ako prvé si vytvoríme výnimky na firewalle server-router. Otvoríme aplikáciu Firewall with Advanced security. V pravo hore klikneme “New rule” a vytvoríme nové pravidlo. Vytvoríme pravidlá pre TCP port 53 a UDP port 53.

Budeme inštalovať DNS server. Master bude Server2 (192.168.1.3) a slave bude Server1(192.168.1.2). Inštalácia služby DNS do prostredia Windows prebieha cez Server Manager, v ktorom zvolíme možnosť Add Roles and Features. Postupným klikaním na tlačidlo Next sa dostaneme až na kartu Roles, v ktorej vyberieme DNS Server a všetky jeho súčasti. Odklikáme next a dokončíme inštaláciu na oboch serveroch.

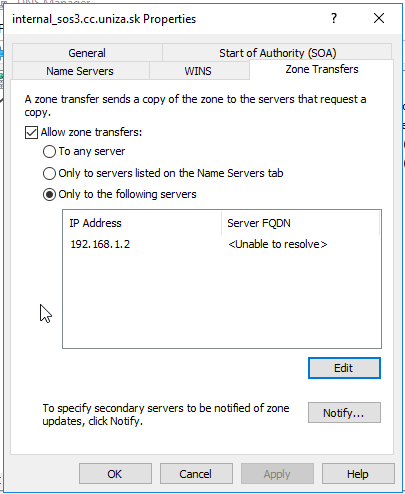
Po úspešnom nainštalovaní pracujeme so službou DNS pomocou DNS Manager-a. V procese inštalácie sa automaticky vygenerujú záložky Forward/Reverse Loopup Zones, Trust Point a Conditional Forwarders. Pre nás budú kľúčové hlavne záložky Forward a Reverse Lookup Zones.

Novú zónu pridáme kliknutím pravého tlačidla myši na záložku Forward Lookup Zones a kliknutim na Add zone. Ak konfigurujeme službu na serveri Master zvolíme možnosť Primary Zone. V nasledujúcom okne je potrebné napísať meno zóny, v našom prípade internal\_sos3.cc.uniza.sk. Po kliknutí na tlačidlo Next sa zobrazí výzva na vytvorenie, prípadne použitie existujúceho zónového súboru. Keďže sa jednalo o prvotnú konfiguráciu zóny, vytvorili sme nový súbor internal\_sos3.cc.uniza.sk.dns, ktorý sa uložil na pevný disk (cesta - C:\Windows\System32\dns). Následne sa systém pýtal na možnosť akceptovania dynamických záznamov, kde sme túto možnosť nepovolili. Po tomto kroku nasleduje rekapitulácia a po kliknutí na talčidlo Finish máme úspešne vytvorenú primárnu zónu internal\_sos3.cc.uniza.sk

Vo vytvorenej zóne bolo potrebné vytvoriť A záznamy pre ns1.internal\_sos3.cc.uniza.sk (192.168.1.3) a ns2.internal\_sos3.cc.uniza.sk (192.168.1.2). A záznamy vytvoríme pravým kliknutím myši na zónu sos3.cc.uniza.sk a vyberieme možnosť New Host (A or AAAA). V otvorenom okne je potrebné vyplniť položky name (ns1) a IP address (192.168.1.3).

Pri vytvorení reverznej zóny sme postupovali rovnakým spôsobom ako pri Forward Lookup Zone. Vytvárali sme reverznú zónu pre IPv4, potrebné bolo zadať Network ID (192.168.1.), vytvoriť reverzný zónový súbor a tlačidlom Finish potvrdiť.

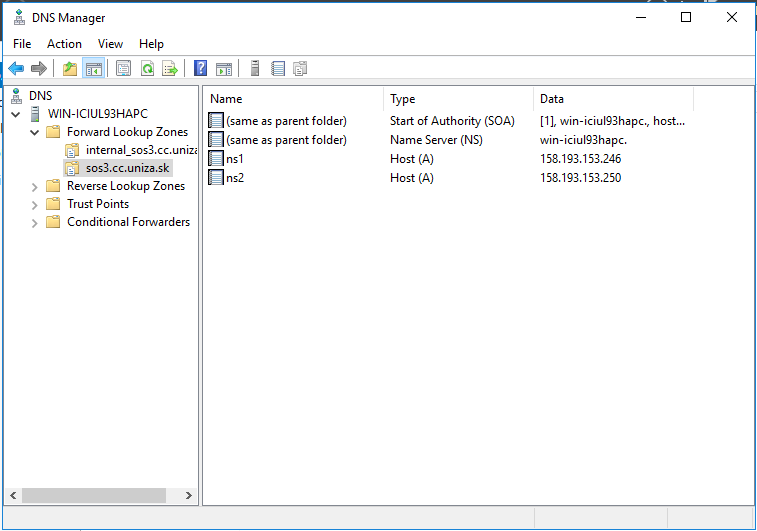
Aby sa povolilo odosielanie zony z master na slave musíme nastaviť na mastrovi povolenie, na server s akou IP môže posielať zonu. Klikneme pravým tlačidlom na zónu a otvoríme properties. Na karte zone transfer prepneme možnosť povolenia odosielania na “Only to the following servers” a ručne pridáme IP adresu serveru s DNS Slave. Ak to bolo úspešné, malo by to vyzerať ako na obrazku.



Obrázok 40: Nastavenie zónového súbora DNS - Windows

Ak server pracuje ako DNS Slave kroky sú podobné ako pri Mastrovi, jediný rozdiel je vo výbere typu zóny. Miesto Primary Zone ako tomu bolo doteraz, je potrebné zvoliť možnosť Secondary Zone. Následne zadať meno zóny (internal\_sos3.cc.uniza.sk) a úspešne kontaktovať server DNS Master.

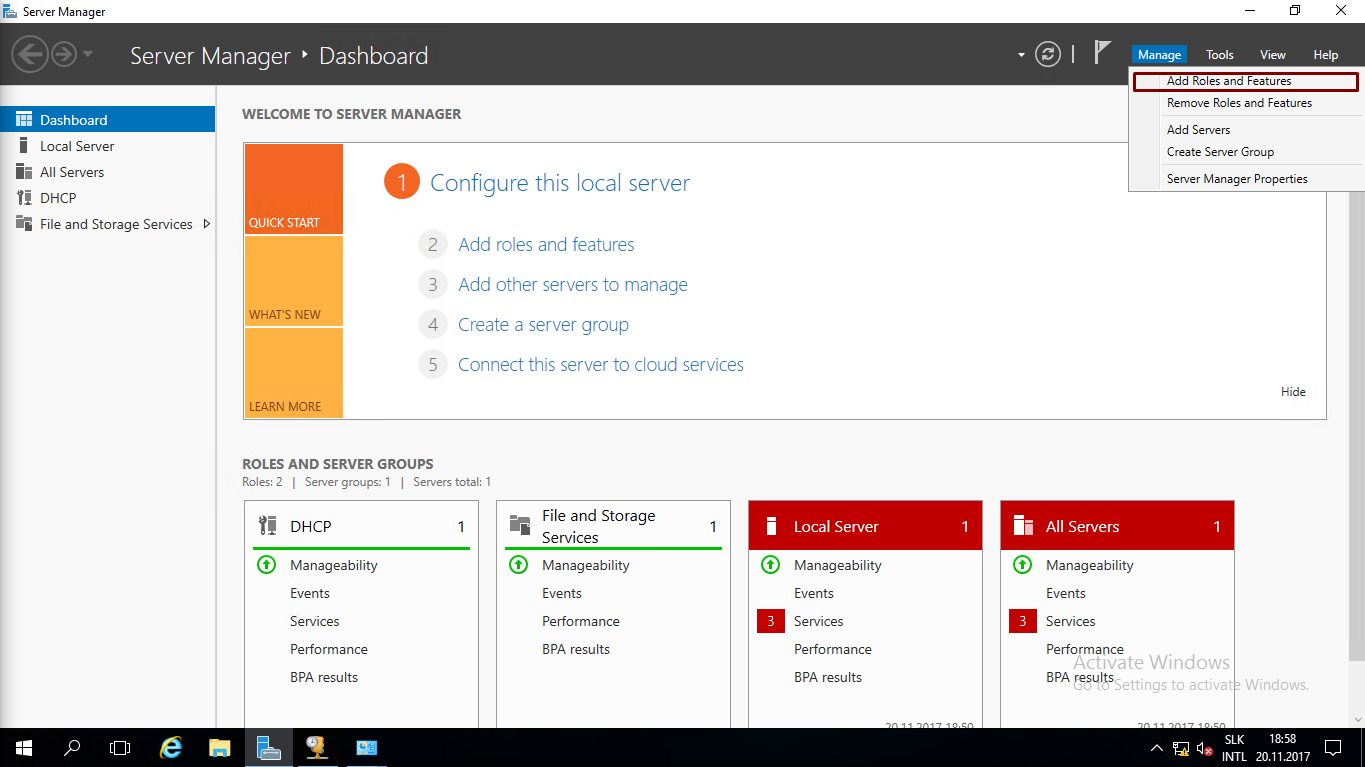
V ďalšom kroku vytvoríme zónu pre externé siete. Na serveri DNS Master vytvoríme novú forward zónu s názvom sos3.cc.uniza.sk a vytvoríme ns1 a ns2 záznamy odkazujúce na IP adresy 158.193.153.246 a 158.193.153.250.

Po úspešnej konfigurácii to vyzerá takto: 

Obrázok 41: Konfigurácia DNS - Windows

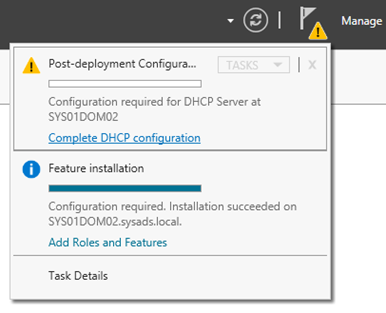
## DHCP

Na Serveri 1 sme nainštalovali protokol DHCP. Začali sme pridaním role cez možnosť Add Roles and Features Wizard ktorú nájdeme v Manage v pravom honom rohu. Po spustení wizardu, nemeníme nič a dostaneme sa pomocou tlačítka Next na záložku Server Roles.



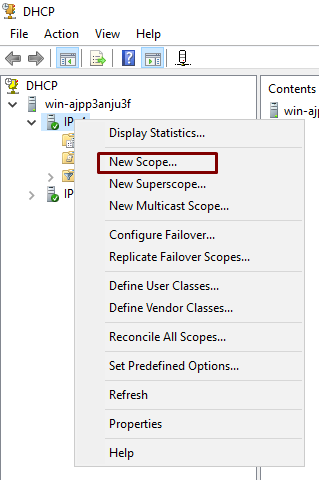
Obrázok 42. Pridanie role pomocou Add Roles and Features

Na záložke Server Roles v zozname Roles nájdeme DHCP Server, ktorý označíme a pokračujeme tlačítkom Next. Po úspešnom nainštalovaní avšak musíme ešte dokončiť DHCP konfiguráciu na ktorú nás upozorňuje aj notifikácia v Server Manageri. Klikneme na notifikáciu a následne na „Complete DHCP configuration“.



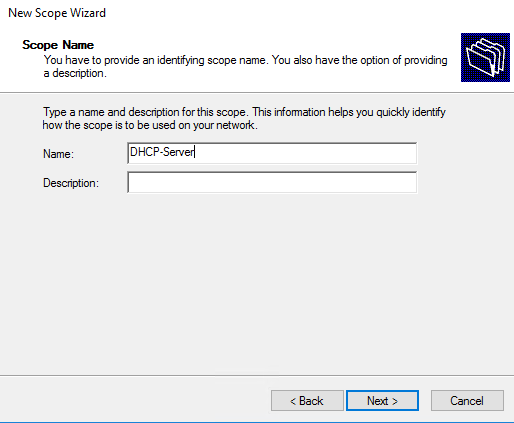
Obrázok 43. Notifikácia ohľadom dokončenia konfigurácie DHCP

Po dokončení konfigurácie sme si otvorili DHCP ( Start – Windows Administrative Tools – DHCP ). Vytvorili sme nový rozsah (New Scope...).



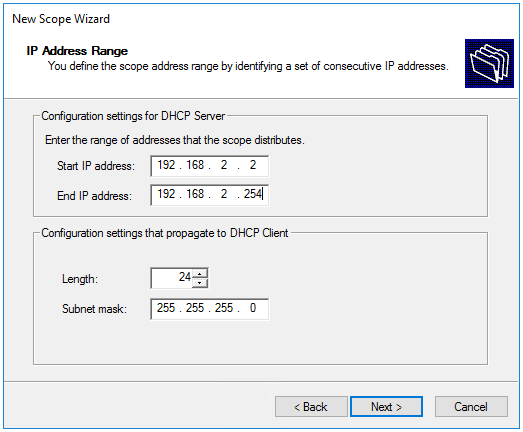
Obrázok 44. Vytvorenie nového rozsahu

Názov sme zadali ľubovolný, v našom prípade DHCP-Server



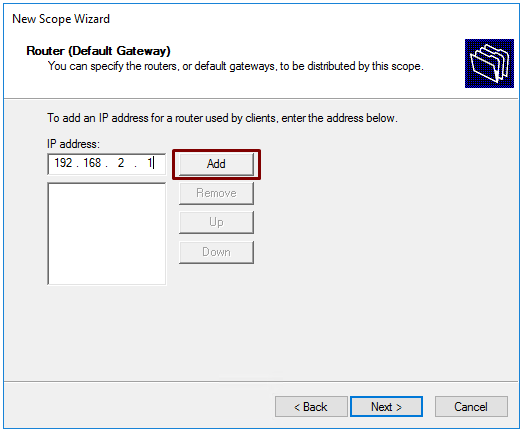
Obrázok 45. Vytvorenie nového rozsahu – zadanie názvu

V ďalšom kroku sme zadali rozsah IP adries aké má DHCP prideľovať. V našom prípade to bol rozsah od 192.168.2.2 po 192.168.2.254 s maskou /24 – 255.255.255.0



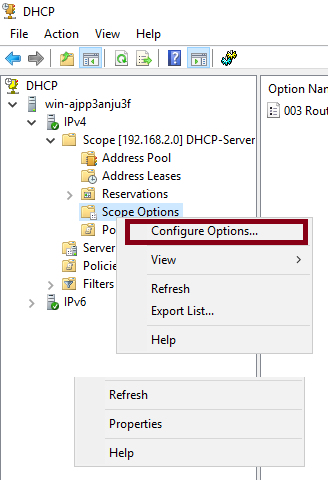
Obrázok 46. Vytvorenie nového rozsahu – zadanie rozsahu a masky

Pokračujeme tlačidlom Next, pokým sa nedostaneme na nastavenia routera a zadáme IP adresu (v našom prípade 192.168.2.1) pomocou tlačidla Add a pokračujeme bez zmien až do konca.

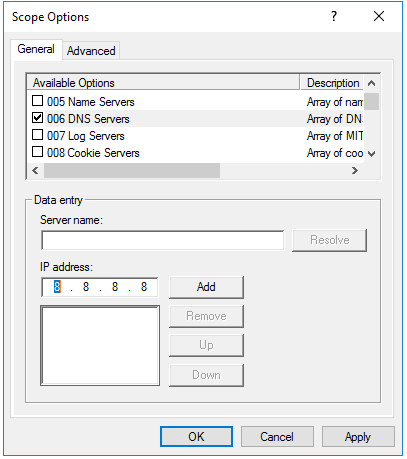


Obrázok 47. Vytvorenie nového rozsahu – zadanie IP adresy routera

V prípade ak nám automaticky nepridalo DNS server, pridáme ho manuálne. Klikneme na Scope Options pravým tlačidlom myši a vyberieme možnosť Configure Options... Nájdeme v zozname možností DNS Server a pomocou tlačidla Add pridávame záznamy.

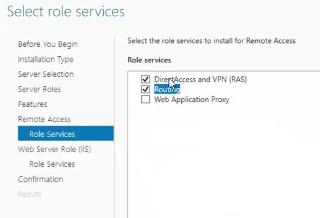


Obrázok 48. Lokácia Configure Options...



Obrázok 49. Pridanie DNS Servera už vytvorenému rozsahu

Pre funkčnosť DHCP bolo potrebné ešte nainštalovať DHCP Relay Agent na server-router. Pomocou Add Roles and Features Wizard (na úvodnej obrazovke Server Manager alebo v pravom hornom menu Manage – Add Roles and Features Wizard) nainštalujeme rolu Remote Access ktorú nájdeme v zozname Roles. V Role Services zvolíme DirectAccess and VPN(RAS) a Routing a pokračujeme až do konca bez zmien.

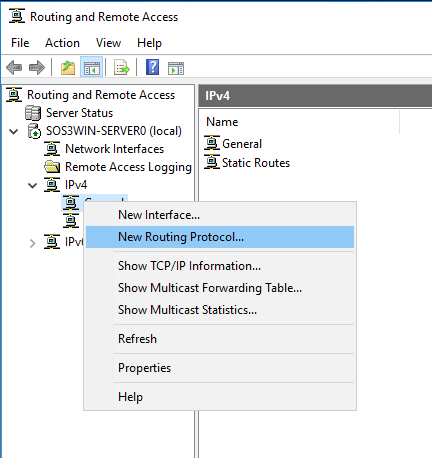


Obrázok 50. Služby role pri inštalácií DHCP Relay Agenta

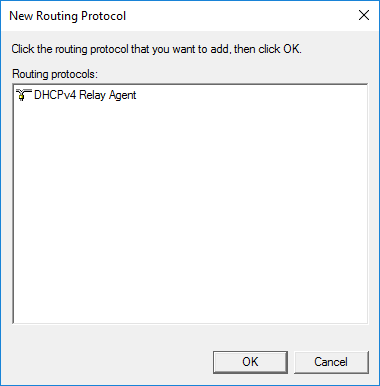
Po nainštalovaní si otvoríme Routing and Remote Access (Start – Windows Administrative Tools

Routing and Remote Access). Pravým tlačidlom klikneme na lokálny server (v našom prípade SOS3WIN-SERVER0) a zvolme možnosť Configure and Enable Routing and Remote Access. Otvorí sa nám inštalácia, klikneme Next a zvolíme možnosť Custom configuration a znova Next kde zvolíme LAN routing a dokončíme inštaláciu.Pri spýtaní či chceme spustiť Routing and Remote access service, klikneme Start service.

Pravým tlačidlom klikneme na General (SOS3WIN-SERVER0 - IPv4 – General) a zvolíme New Routing Protocol... a následne zvolíme možnosť DHCPv4 Relay Agent.



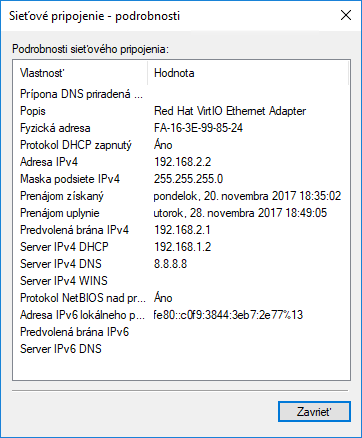
Obrázok 51. Lokácia „New Routing Protocol...“



Obrázok 52. Zvolenie DHCPv4 Relay Agent

Pod IPv4 sa nám vytvorí DHCP Relay Agent (SOS3WIN-SERVER0 – Ipv4 – DHCP Relay Agent), klikneme pravým tlačidlom a vyberieme možnosť Properties. Pridáme IP DHCP servera (u nás 192.168.1.2) pomocou Add a potvrdíme – OK. Znova klikneme pravým tlačidlom myši na DHCP Relay Agent a vyberieme možnosť New Interface... Zo zoznamu zvolíme interface na ktorý chceme uplatniť DHCP (u nás Ethernet 3) a pokračujeme do konca bez zmien.

Následne môžeme na klientovi otestovať.



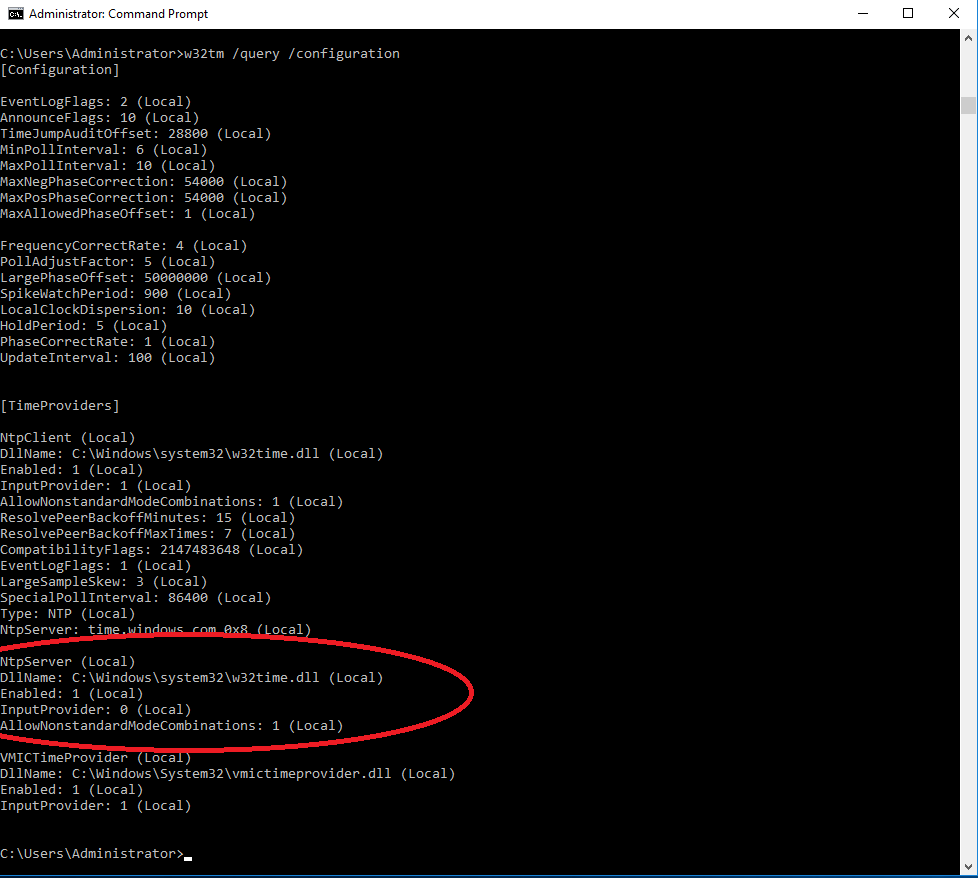
Obrázok 53. Overenie dynamického pridelenia IP adresy

## NTP Server

Na spustenie NTP na Windows servery sme museli vykonať zmeny v registroch. Spustíme okno RUN (WIN+R) , kde napíšeme regedit. Následne sa dostaneme cestou HKEY\_LOCAL\_MACHINE | SYSTEM | CurrentControlSet | Services | W32Time | TimeProviders | NtpServer až k hodnote Enabled , ktorá bola nastavená na 0 , a my ju zmeníme na 1.

V príkazovom riadku, zadáme príkaz *w32tm /config /update*, čím spustíme NTP server na danom zariadení. Následne použijeme príkaz *net stop w32time && net start w32time*

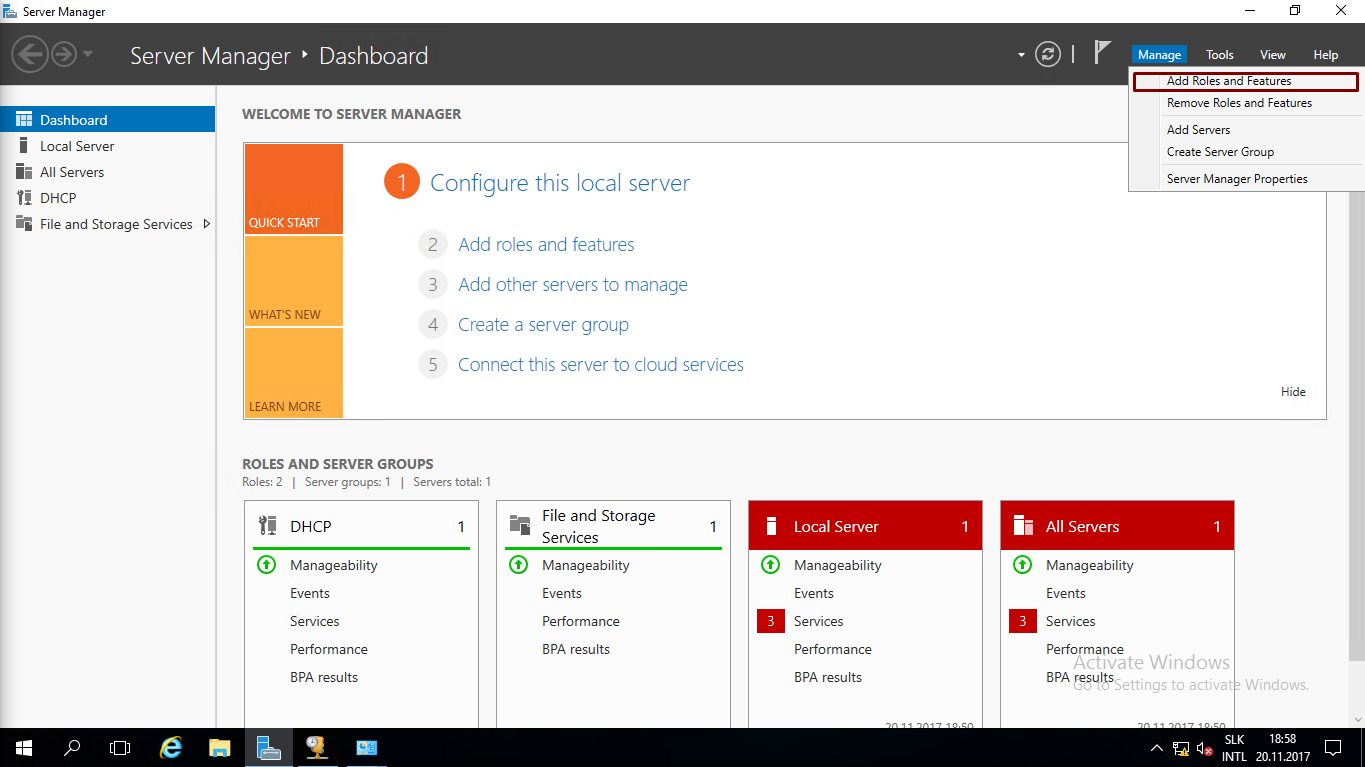
Ak boli všetky príkazy úspešne použité skontrolujeme, či NTP server beží a to príkazom: *w32tm /query /configuration*

**

Obrázok 54: Konfigurácia NTP servera

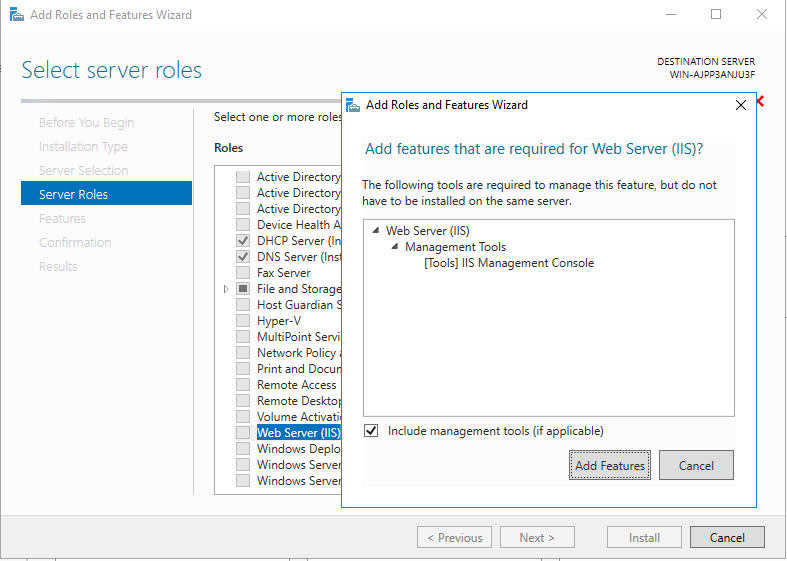
## Web Server IIS

Na server1 (192.168.1.2) sme sa rozhodli nainštalovať webový server. Začíname znova pridaním role (Add Roles and Features Wizard).



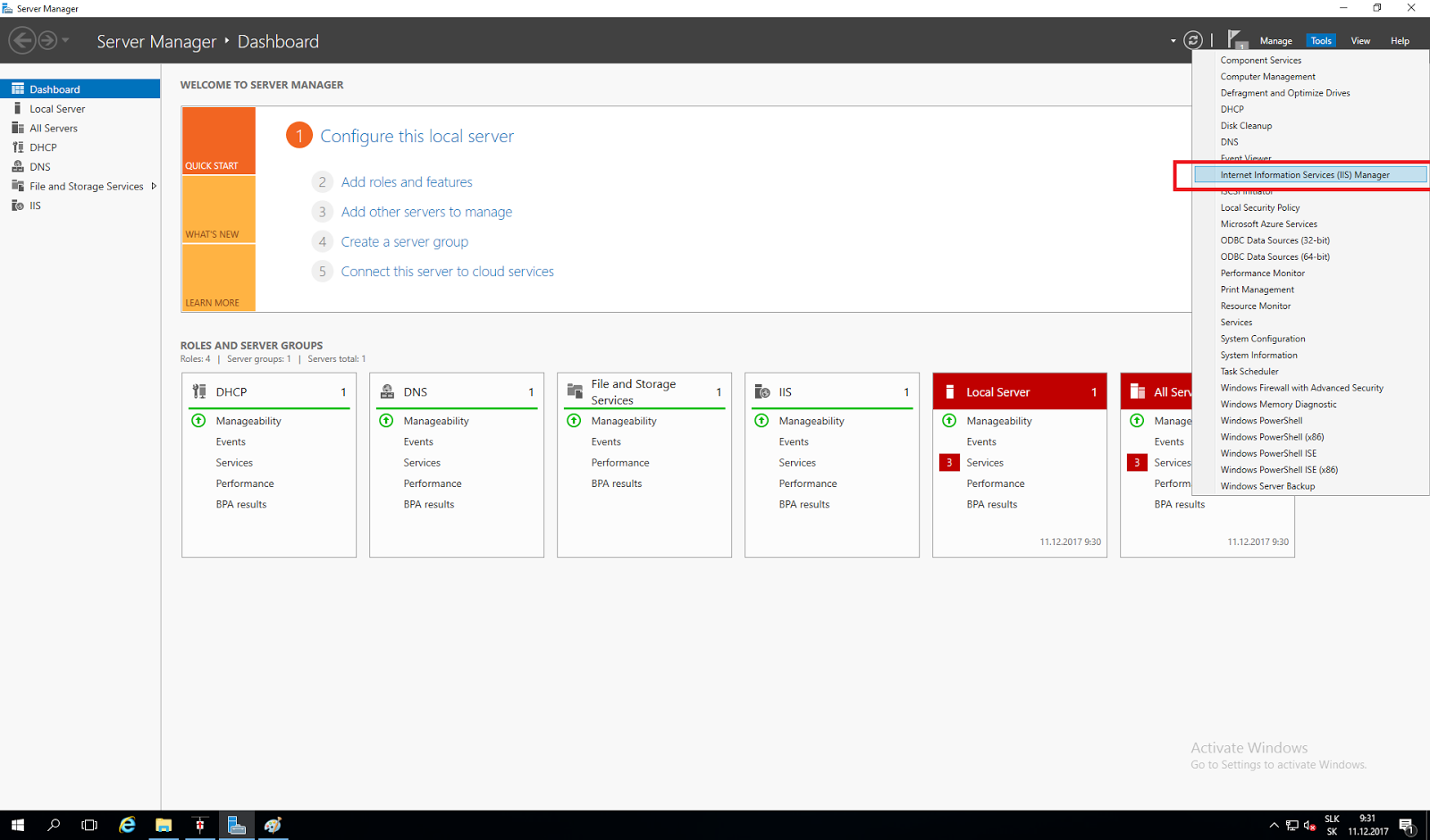
Obrázok 55. Pridanie role pomocou Add Roles and Features

V danom okne pokračujeme až po záložku Serve Roles kde v zozname Roles zaklikneme „Web Server (IIS)“ a spýta sa nás či vážne chceme pridať všetky komponenty týkajúce sa tejto role, stlačíme Add Features.



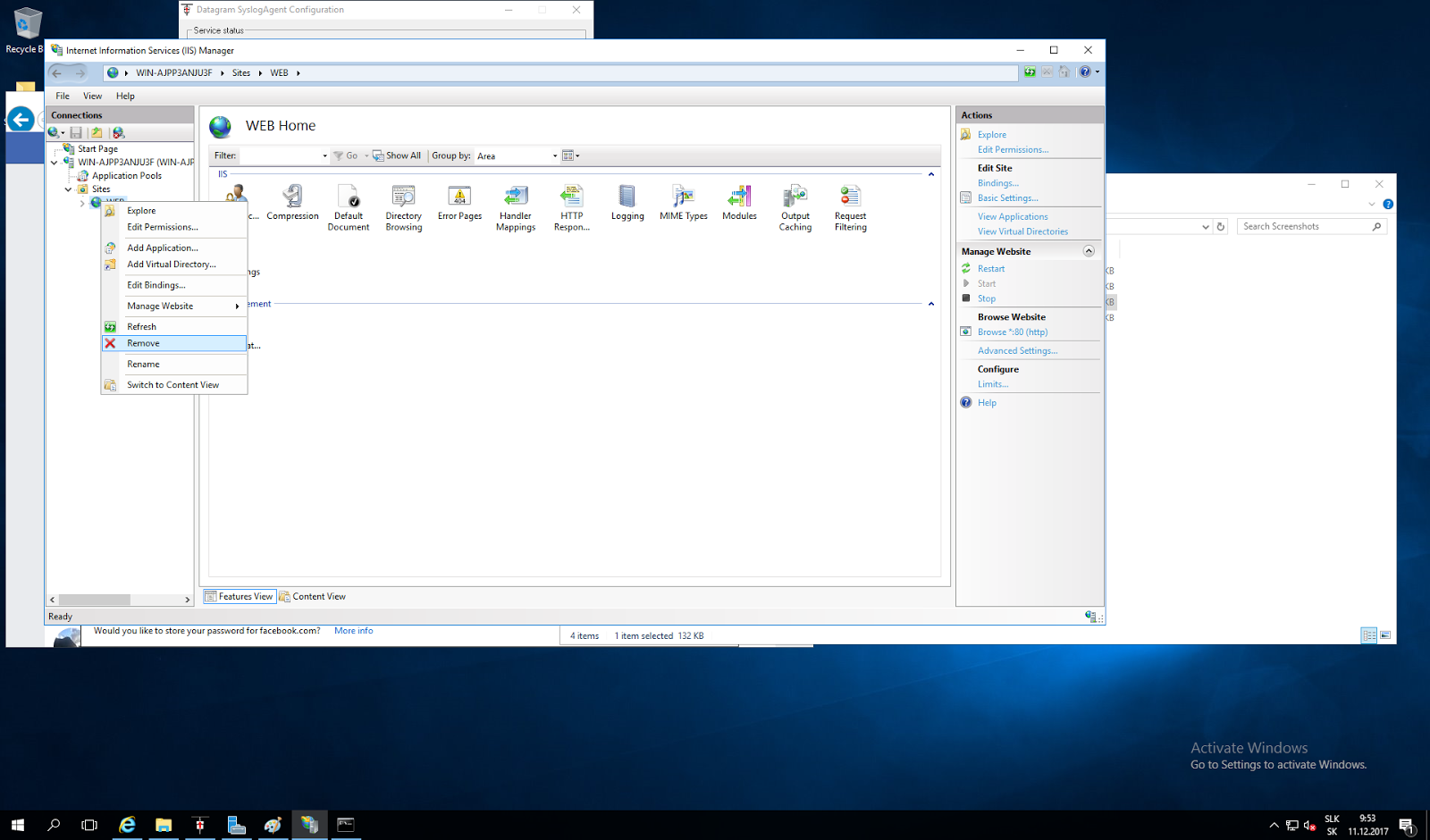
Obrázok 56. Záložka Server Roles pri inštalácii IIS

Pomocou tlačidla Next pokračujeme až do konca inštalácie bez ďalších zmien. Po dokončení inštalácie v pravom hornom rohu vyberieme možnosť Manage – Internet Information Service (IIS) Manager.



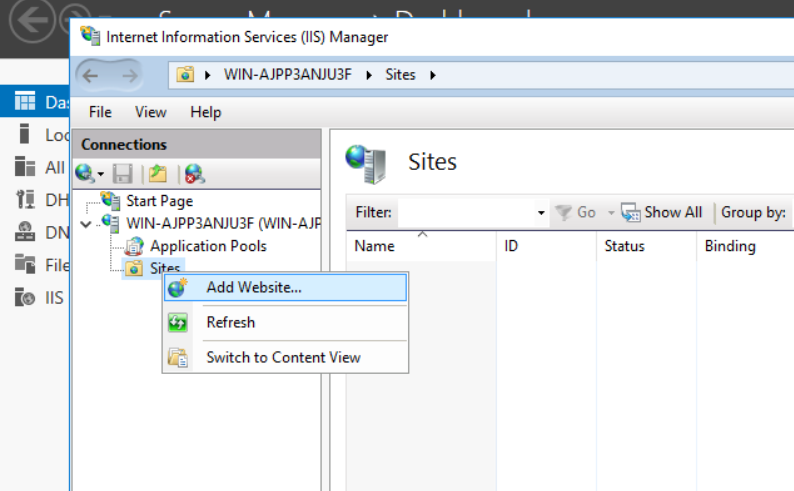
Obrázok 57. Lokácia Internet Information Service Manager-a

Vidíme v zozname už default-ne vytvorenú web stránku, ktorú ale vymažeme.



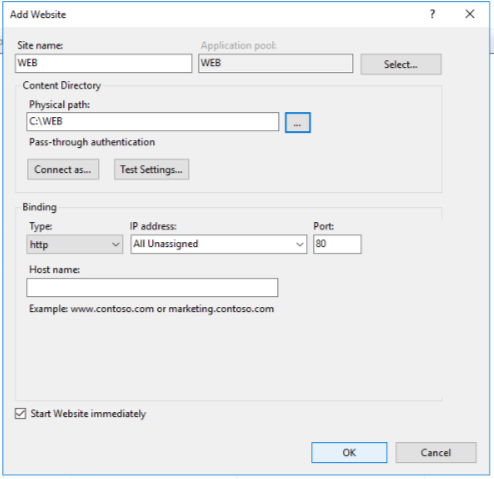
Obrázok 58. Vymazanie default-ne vytvorenej stránky

Vytvoríme si nový ľubovolný adresár (v našom prípade C:\WEB) v ktorom vytvoríme súbor index.html do ktorého zapíšeme ľubovolný text pre možné následné otestovanie. V IIS Manageri zvolíme možnosť Add Website...



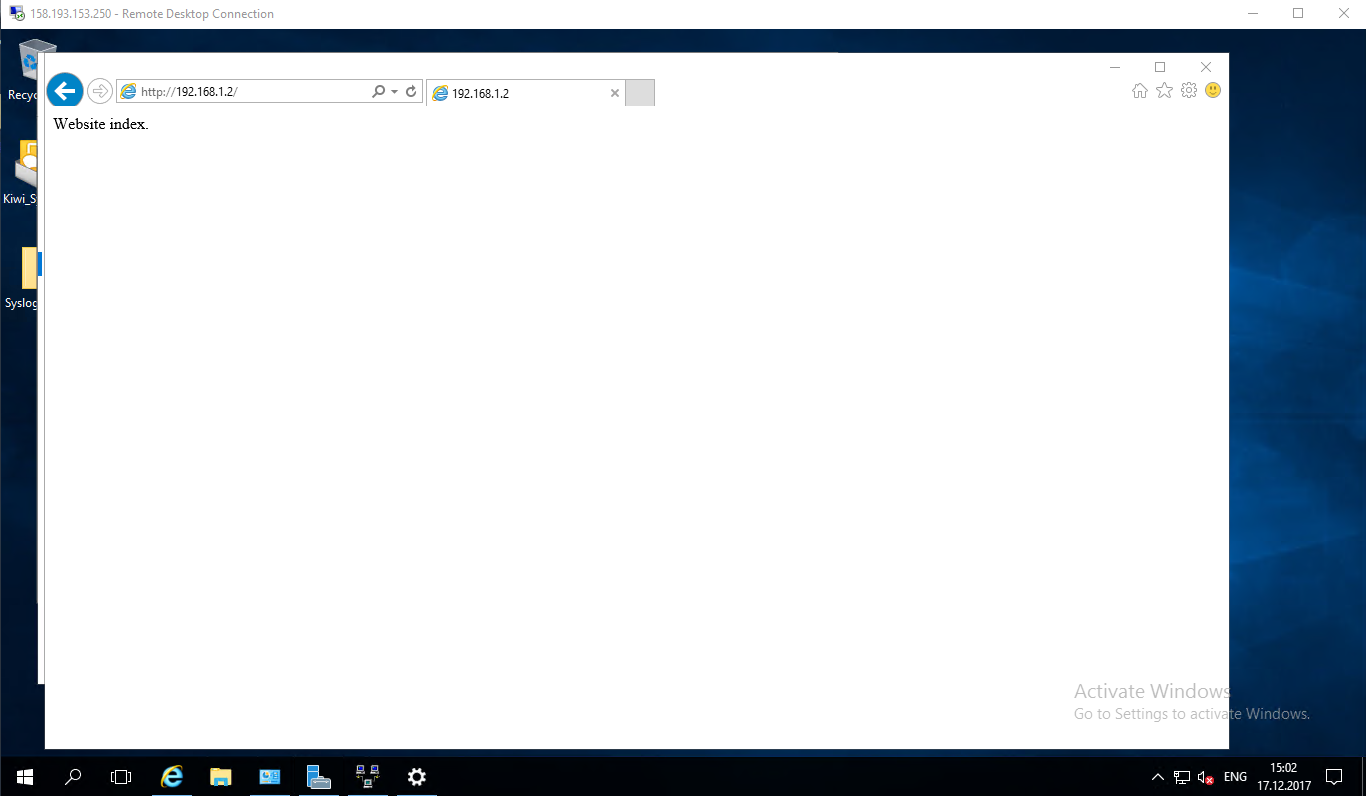
Obrázok 59. Vytvorenie novej stránky

V následujúcom kroku zadáme názov a fyzickú cestu k danej stránke (C:\WEB) a potvrdíme tlačidlom OK.



Obrázok 60. Definovanie názvu stránky a cesty k súborom

Následne sme otestovali na klientovi túto webstránku na adrese 192.168.1.2 kde bol vytvorený IIS.

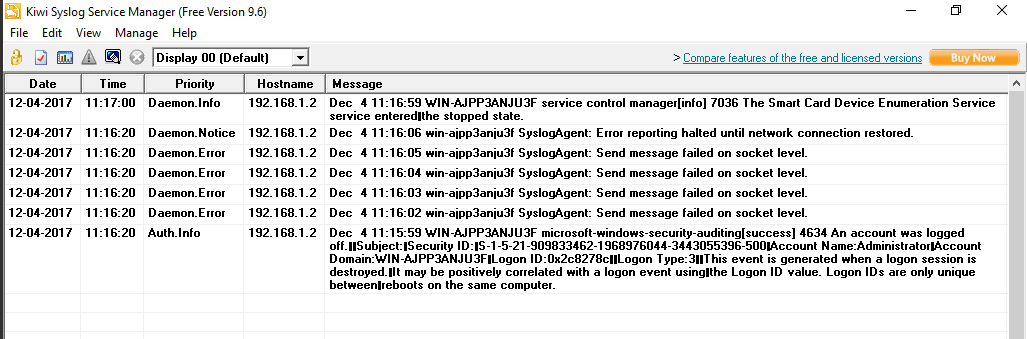


Obrázok 61. Overenie funkčnosti webového servera

## Logovanie

Na Serveri 2 sme nainštalovali logovací server Kiwi. Podmiekou k inštalácii bolo NET framework 3.5. Ten sme nainštalovali cez Server Manager - Add roles and features. Na každý server, z ktorého chceme odosielať logy nainštalujeme aplikáciu SyslogAgent. Po spustení nastavíme protokol a IP adresu serveru, na ktorý chceme odosielať logy a službu spustíme.

Prijaté logy sa zobrazia na konzole aplikácie Kiwi (Viď obrázok)



# Literatúra

* <https://debian-handbook.info/browse/stable/>
* <https://docs.microsoft.com/en-us/windows-server/windows-server>

## Firewall

* <https://wiki.debian.org/iptables>
* <https://wiki.debian.org/DebianFirewall>
* <https://www.digitalocean.com/community/tutorials/how-to-set-up-a-firewall-using-iptables-on-ubuntu-14-04>
* <https://www.lammertbies.nl/comm/info/iptables.html>

## NAT

* <https://www.revsys.com/writings/quicktips/nat.html>
* <https://www.howtoforge.com/nat_iptables>
* <http://www.bctes.com/nat-linux-iptables.html>

## DHCP

* <https://www.isc.org/downloads/dhcp/>
* <https://wiki.debian.org/DebianFirewall>
* <https://wiki.debian.org/DHCP_Server>
* <https://support.cumulusnetworks.com/hc/en-us/articles/201787526-Configuring-DHCP-Relays>
* <https://blogs.technet.microsoft.com/teamdhcp/2012/08/31/installing-and-configuring-dhcp-role-on-windows-server-2012/>
* <https://technet.microsoft.com/en-us/library/dd469685(v=ws.11).aspx>
* <https://technet.microsoft.com/en-us/library/hh831538(v=ws.11).aspx>

## DNS

* Bind Best practise: <https://kb.isc.org/article/AA-00892/0/Best-Practices-for-those-running-Authoritative-Servers.html>
* Bind response rate limiting : <https://kb.isc.org/article/AA-01000/0>
* Bind Security: Transaction Signatures (TSIG) Configuration: <https://www.cyberciti.biz/faq/unix-linux-bind-named-configuring-tsig/>
* <https://www.digitalocean.com/community/tutorials/how-to-configure-bind-as-a-private-network-dns-server-on-ubuntu-14-04>
* <https://technet.microsoft.com/en-us/library/cc771031(v=ws.11).aspxhttps://technet.microsoft.com/en-us/library/cc725925(v=ws.11).aspx>

## Web Server

* <http://httpd.apache.org>
* <https://www.eventtracker.com/Eventtracker/media/Eventtracker/files/support-docs/How-to-Install-and-Customize-IIS-Web-Server.pdf>
* <https://www.digitalocean.com/community/tutorials/how-to-configure-the-apache-web-server-on-an-ubuntu-or-debian-vps>
* <https://www.digitalocean.com/community/tutorials/how-to-set-up-apache-virtual-hosts-on-ubuntu-16-04>

## Mail Service

* <http://squirrelmail.org/docs/admin/admin-3.html>
* <https://wiki.debian.org/Postfix>

## NTP

* <https://support.microsoft.com/en-us/help/816042/how-to-configure-an-authoritative-time-server-in-windows-server>
* <https://social.technet.microsoft.com/Forums/windows/en-US/c28d6fd3-d7b9-4ed1-bbc6-f509015c2eca/ntp-server-configuration-on-server-2016?forum=winserver8gen>
* <https://linuxconfig.org/how-to-setup-ntp-server-and-client-on-debian-9-stretch-linux>
* <https://www.tecmint.com/install-and-configure-ntp-server-client-in-debian/>

## Logovanie

* <https://wiki.debian.org/DebianEdu/HowTo/syslog-ng>
* <http://oscarhjelm.com/blag/?p=1193>

## Iné

* <http://www.mobzystems.com/blog/windows-server-port-forwarding-from-the-command-line/>
* <https://technet.microsoft.com/en-us/library/cc770798(v=ws.10).aspx>