Implementácia firemnej siete

Semestrálna práca

Andrej Hucík, Miroslav Kozák, Andrej Šišila

Katedra informačných sietí
Žilinská Univerzita v Žiline - Fakulta riadenia a informatiky
Žilina
2017

Obsah

Zoznam obrázkov

Zoznam tabuliek

Kapitola 1

Úvod

Základom každej firmy, či už malej, strednej alebo veľkej, je stabilná a bezpečná sieťová infraštruktúra.

V našej práci sa budeme zaoberať implementáciou a konfiguráciou menšej firemnej siete, ktorá bude pozostávať z jedného smerovača, jedného prepínača, dvoch serverových systémov a dvoch pracovných staníc. Potom na potrebných uzloch nastavíme potrebné služby, ktoré umožnia firme poskytovať služby pre vnútornú, ale aj vonkajšiu sieť.

Kapitola 2

Ciele práce

Hlavným cieľom našej práce je vytvorenie jednoduchej sieťovej infraštruktúry, ktorú bude možné nasadiť do podnikového prostredia. Vytvorenie a konfigurácia takejto siete si vyžadovalo splnenie nasledovných čiastkových cieľov:

- Inštalácia operačného systému na serverové systémy, pracovné stanice a smerovač, a ich následná základná konfigurácia
- DNS: Master/Slave riešenie s replikáciou a overením
- Podpora viacerých virtuálnych web serverov a s inštaláciou niektorej z web aplikácii typu CMS or Wiki
- Firewall na smerovači cez netfilter s NAT
- Firewall na server systémoch
- NTP čas pre firmu
- SSH prístup
- DHCP
- Email

Služby bolo potrebné sprevádzkovať najprv na linuxovej distribúcií Debian 8.6.0 x64 Stable a potom aj na Windows Server 2016, preto je aj táto práca rozdelená na dve hlavné časti: konfiguráciu v prostredí Windows a Linux.

Kapitola 3

Topológia siete

Naša topológia siete pozostáva z firewallu ku ktorému je na jednom rozhraní pripojený prepínač ku ktorému su napojené dva servery a dva počítače. Na druhom rozhraní je Internet. Na linuxoch aj na windowsoch bola rovnaká topológia s výnimkou, že pri pracovaní s linuxom sa nachádzali počítače a servery v rozdielnych VLAN: Servery vo VLAN-e 10 a desktopy vo VLAN-e 20.

Keďže si Windows Server nerozumel s VLAN-ami, topológia siete sa líši v tom, že všetky koncové uzly sú v defaultnej VLAN-e.

Kapitola 4

Linux

4.1 Inštalácia operačného systému Debian 8.6.0 x64

4.1.1 Inštalácia serverov

netinst Stiahnut image
vytvoriť virtuálku
nastaviť virtuálku
nainštalovať debian

Stiahli sme si obraz disku Debian 8.6.0 stable 64 bitovú verziu . Obraz disku (iso súbor) sme pripojili k diskovej mechanike VM a spustili sme inštaláciu OS. Hostname–každá VM má svoje meno odvodené od jej funkcie napr. všetky servery majú označenie „SX“ a desktopy „DX“, kde X je poradové číslo servera/desktopu. Domain – nastavili sme pridelenú doménu: sos3.local. Servery nemajú grafické rozhranie, iba textové.

b. Študent prejde postupne jednotlivými nastaveniami, ktoré ponúka nástroj VB. c. Pre jednotlivé VM sme správne nastavili sieťové adaptéry a virtualizačné parametre, napríklad PAE/NX a paravirtualizačné rozhranie v SYSTEM ACCELERATION. d. Každej VM sme nastavili správny počet a funkčnosť sieťových adaptérov: 2 pre firewall, 1 pre servery a desktopy e. Zdieľaný adresár sme na VM nepridávali.

4.1.2 Inštalácia desktopov

rovnako ako servery, akurát s xfce

4.2 Základná konfigurácia

nejaké balíčky, čo sme inštalovali na všetky počítače

4.3 Firewall

ako sme robili firewall v iptables

4.3.1 Spúšťanie iptables skriptu po štarte

iptables skript po štarte

4.4 VLAN

Servery sú vo VLAN 10, desktopy vo VLAN 20. Smerovanie medzi VLANami je vykonávané na FW. Preto sme na FW museli nainštalovať balíčky „isc-dhcp-server“ a „vlan“ t.j. „apt-get installisc-dhcp-server vlan“. Potom sme editovali súbor „/etc/network/interfaces“ tak, že sme odstránili adresné informácie z vnútorného interfacu eth1, ale nechali sme „auto eth1“, aby sa port zapol (UP). Následne sme pridali subinterface eth1.10 pre VLAN 10 (servery) a eth1.20 pre VLAN 20 (desktopy). Adresný rozsah pre jednotlivé VLAN bola sieť 192.168.0.0/24 rozdelená na dve /25 siete: 192.168.0.0 - 192.168.0.127 pre VLAN 10 a 192.168.0.128 - 192.168.0.255 pre VLAN 20

FW je DHCP relay server. Všetky DHCP požiadavky prepošle FW DHCP serveru, ktorý pridelí klientovi IP adresu a ďalšie nakonfigurované informácie. Týmto spôsobom je FW zodpovedný iba za filtrovanie premávky a server za služby poskytované na sieti. IP adresa DHCP servera sa do konfiguračného súboru „/etc/default/isc-dhcp-relay“ DHCP relay agenta musí zadať BEZ úvodzoviek a musíme počúvať na obidvoch subinterfacocht.j. eth1.10 aj eth1.20.

4.5 DNS

Systém názvov domén alebo systém mien domén, alebo systém doménových mien (Domain Name System), skr. DNS, je systém, ktorý ukladá prístup k informácii o názve stroja (hostname) a názve domény v istej distribuovanej databáze v počítačových sieťach ako internet. Najdôležitejšie je, že poskytuje mechanizmus získania IP adresy pre každé meno stroja (lookup) a naopak (reverse), a uvádza poštové servery (MX záznam) akceptujúce poštu pre danú doménu.

DNS poskytuje na internete všeobecne dôležitú službu, pretože kým počítače a sieťový hardvér pracujú s IP adresami, ľudia si vo všeobecnosti ľahšie pamätajú mená strojov a domén pri použití napr. v URL a e-mailovej adrese (obzvlášť nepríjemné by to bolo pri IPv6 adrese). DNS tak tvorí prostredníka medzi potrebami človeka a softvéru.

V rámci našej doménovej zóny „sos3.local“ sme si museli nastaviť dva DNS servery: Master (S1) a Slave (S2). Slave zrkadlí hlavný DNS server a v prípade poruchy ho zastúpi. Keďže si Slave DNS server všetko stiahne z Master DNS servera, netreba ho primárne konfigurovať, ale stačí mu nastaviť „allow-transfer“ na privátnu IP Master DNS.

Na obidva servery sme nainštalovali DNS server a nástroje na overenie jeho funkčnosti príkazom „apt-get install bind9 bind9utils dnsutils“.

Master DNS serveru sme upravovali súbory „/etc/resolv.conf“ (konfigurácia adries DNS serverov), „/etc/bind/master/db.sos3.local“ (view-lokálny), „/etc/bind/master/db.sos3.extern (view-verejný), „/etc/bind/named.conf.local“ (definovanie lokálnych a verejných DNS View). Obsah súboru „/etc/resolv.conf“ je uvedený nižšie.

```
domain sos3.local
nameserver 192.168.0.2
nameserver 192.168.0.3
```

V adresári „/etc/bind“ na S1 sme vytvorili adresár „master“, do ktorého sme ukladali zónové súbory pre DNS.

Viewy sme nastavovali na Master DNS serveri súbormi „/etc/bind/named.conf.local“, „/etc/bind/master/db.sos3.local“, „/etc/bind/master/db.sos3.external“. Pri dotazovaní na doménové meno nášho DNS zvnútra sa použijú privátne adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.local“. Pri dotazovaní na doménové meno nášho DNS zvonku sa použijú verejné adersy DNS serverov zo súboru „/etc/bind/master/db.sos3.ext O tom, aký súbor sa použije, rozhoduje súbor „/etc/bind/named.conf.local“

Počítače v lokálnej sieti sa dokážu navzájompingať pomocou svojich hostname. Preklad hostname názvov na IP adresy je definovaný v súbore „/etc/bind/master/db.sos3.local“

Firewall bol nakonfigurovaný tak, aby prepúšťal DNS požiadavky na lokálnej sieti, a tiež aby prepúšťal požiadavky z internetu na obidva DNS servery t.j. aby boli obidva DNS servery viditeľné zvonku (PREROUTING). Záznamy pre DNS sú pre obidve verejné IP adresy pre udp aj tcp port 53 (zdrojový aj cieľový).

V prípade, že sa vyskytli problémy, skúšali sme vypnúť firewall, kontrolovali sme konfiguračné súbory Master DNS servera príkazmi „named-checkconf“ a „named-checkzone“ a príkazom „tcpdump“ sme monitorovali prenášané správy. Pri každej zmene konfiguračných súborov bolo treba reštartovať bind9 / isc-dhcp-server / interface.

Zdroje:
https://www.howtoforge.com/two_in_one_dns_bind9_views

4.6 DHCP

DHCP server (S2) sme museli upraviť tak, aby prideľoval aj DNS adresy serverov. Súbor „/etc/dhcp/dhcpd.conf“ na S1 sme upravili tak, že sme doň pridali privátne IP adresy DNS serverov (option domain-name-servers). Do časti pre podsieť sme definovali názvy týchto serverov. Voľbu „optionhost-name“ sme zmenili z pôvodného

„example.org“ na „sos3.local“. Tým, že sme nastavili DNS server, nemusíme meniť na jednotlivých hostoch súbor „/etc/resolv.conf“.

Dynamic Host Configuration Protocol (DHCP) je súbor zásad, ktoré využívajú komunikačné zariadenia (počítač, router alebo sieťový adaptér), umožňujúci zariadeniu vyžiadať si a získať IP adresu od servera, ktorý má zoznam adries voľných na použitie.DHCP Server (Dynamic Host Configuration Protocol) vykonáva automatické pridelenie IP adries svojim klientom. Môžu to byť akékoľvek systémy, podporujúce DHCP. DHCP je štandardný protokol, môžu ho využívať aj systémy mimo Microsoft. Z Microsoft operačných systémov podporujú funkciu DHCP klienta všetky až na veľmi exotický LAN Manager pre OS / 2.V rámci siete potom máme DHCP Server - prideľujúca adresy a počítače - ktoré je od neho preberajú (DHCP Clients). V sieti môžu byť aj počítače, ktoré majú tieto adresy nastavené manuálne.

4.7 NTP

NTP(Network Time Protocol) je protokol na sychronizáciu všetkých počítačov pripojených do vnutornej siete. Tento protokol zaisťuje, aby všetky počítače v sietei mali rovnaký a presný čas. Bol nvrhnutý aby odolával následkom premenlivého zdržania pri doručovaní paketov. NTP používa UDP na porte 123. NTP server sme zvolili server2, ktorý má ip adresu 192.168.0.3. Nainštalovali sme NTP príkazom apt-get install ntp. Na klientoch sme nainštalovali NTP pomocou príkazu apt-get installntpntpdate. V súbore na serveri s2 /etc/ntp.conf sme pridali slovenské servery zo stránky www.pool.ntp.org/zone/sk. a ostatné servery sme zakomentovali. Klienti si z master serveru aktualizujú čas.

4.8 Web server

Apache HTTP Server je softwarový webový server s Opensource licenciou pre Linux, BSD, Microsoft Windows a iné platformy.

PHP (PHP: Hypertext Preprocessor) je populárny opensource skriptovací jazyk, ktorý sa používa najmä na programovanie klient-server aplikácií (na strane servera) a pre vývoj dynamických webových stránok.

MySQL je slobodný a otvorený viacvláknový, viacužívateľský SQL relačný databázový server. MySQL je podporovaný na viacerých platformách (ako Linux, Windows či Solaris) a je implementovaný vo viacerých programovacích jazykoch ako PHP, C++ či Perl. Databázový systém je relačný, typu DBMS (database management system). Každá databáza je v MySQL tvorená z jednej alebo z viacerých tabuliek, ktoré majú riadky a stĺpce. V riadkoch sa rozoznávajú jednotlivé záznamy, stĺpce udávajú dátový typ jednotlivých záznamov, pracuje sa s nimi ako s poľami. Práca s MySQL databázou je vykonávaná pomocou takzvaných dotazov, ktoré vychádzajú z programovacieho jazyka SQL (StructuredQueryLanguage).

Na webový server sme použili apache. Apache HTTP Server je softwarový webový server s Opensource licenciou pre Linux, BSD, Microsoft Windows a iné platformy. V dnešnej dobe je najrozšírenejším na celom svete. Pre plnú fukncionalitu webového servera sme museli nainštalovať nainštalovaťapache, mysql, php príkazom:

apt-get install apache2 mysql php5ň

V adresári /var/www/ sme vytvorili priečinky s názvami web1 a web2. Kde web1 a web2 predstavovali dva virutálne webové servery. Následne sme v etc/apache2/sites-available 003-wiki.sos3.local.conf sme pridali cestu ku web stránke /var/www/web1 a ServerName web2.sos3.local. Pre joomlu v súbore 002-joomla.sos3.local.conf sme pridlai cestu k adresaru ked uz DocumentRoot /var/www/web1 a ServerName web1.sos3.local

Následne do DNS záznamov sme museli pridať:

db.sos1.local
web1 IN A 192.168.0.4
web2 IN A 192.168.0.4

db.sos1.public
web1 IN A 158.193.139.74
web2 IN A 158.193.139.74

4.8.1 Joomla

V priečinku /var/www/web2 sme stiahli joomlu verziu 3.6 pomocou príkazuň

wget https://github.com/.../Joomla_3.6.0-Stable-Full_Package.zip

V ďalšom kroku sme odzipovali tento súbor príkazom

unzip Joomla_3.6.0-Stable-Full_Package.zip

Následne sme v prehliadači otvorili web1.sos3.local a podľa príslušných krokov sme nainštalovali joomlu. Ake su tam prava? Root:root nefunguje

4.8.2 Mediawiki

V priečinku var/www/web1 sme stiahli Wikimedia pomocou príkazu

wgethttps://www.mediawiki.org/wiki/Download/mediawiki-1.2.8.zip

Následne sme odzipovali tento súbor príkazom

unzip mediawiki-1.2.8.zip

A v poslednom kroku sme v prehliadači web2.sos3.local nainštalovali mediawiki.

4.9 Poštový server

Na poštový server sme použili postfix.Postfix je počítačový program pre unixové systémy pro prepravu elektronickej pošty (MTA).

Najprv bolo ptorebné nainštalovať postfix príkazom apt-get installpostfix prešli sme inštaláciou kde sme nastavili hostname sos3.local. Následne sme museli reštartovať postfixservicepostfixrestart. V súbore /etc/postfix/main.cf je potrebné upraviť myhostname = sos3.local, odkomentovať

pridat konfigurak

Kapitola 5

Windows

5.1 DHCP

Inštaláciu sme vykonali vo Windows service manager - Add Roles and Features, vybrali si možnosť DHCP server.

Pre konfiguráciu sme klikli na TOOLS a následne DHCP.Zobrazilo sa nám okno s ponukou , my sme vybrali náš server, IPv4 a možnosť new scope. Spustil sa New ScopeWizard. V prvom kroku sme napisali názov pravidla na prideľovanie IP adries. Ďalej sme zvolili rozsah IP adries a masku.

Rozsah IP adries od 192.168.0.1 po 192.168.0.254
Maska 255.255.255.0

Následne sme využili možnosti pridať výnimku z predtým zadaného rozsahu, teda adresy ktoré sa nebudu prideľovať napriek tomu, že sú zo nami zadaného rozsahu v predchádzajúcom kroku. Ide o adresy serverov 192.168.0.2 a 192.168.0.3.

Potom sme zvolili aký dlhý čas si server bude pamätať IP adresy ktoré niekomu pridelil. Stačilo nám 5 hodín (dĺžka cvičenia aj s rezervou).

Nakoniec sme nastavili bránu na „192.168.1.1", pridali sme IP adresy našich DNS serverov, teda „192.168.1.2" a „192.168.1.3". , a dokončili inštaláciu kliknutím na Finish.

5.2 DNS

V prvom rade sme si zvolili Master a Slave. Master je server1 (192.168.0.2) a Slave server2 (192.168.0.1)

DNS master nainštalujeme pomocou Windows Server Manager. Klikneme na Manage , vyberieme možnosť Add roles and features daľej Role-based or feature-basedinstallation, zobrazí sa zoznam serverov, my vyberieme náš server a zvolímezo zoznamu rolesDNS Server a dokončíme inštaláciu.

Po inštalácií DNS balíka sme sa dostali cez Tools -> DNS -> Configure a DNS server -> Create a forward lookupzone k vytvoreniuprimárnej forward lookupzóny sos1.local , nastavili sme aj nech záznamy preposiela na Slave 192.168.0.3.

Prešli sme k inštalácii DNS Slave.Postup ako pri DNS Master avšak DNS server bolo potrebné nastaviť na slavemode. Vybrali sme Tools -> Forward lookupzones -> New zone. Hneď v prvom kroku sme vybrali možnosť nie Primaryzone ale Secondaryzone a taktiež meno zóny .V ďalšom kroku určíme DNS Masterserver,v našom riešení ma IP 192.168.0.2 .Dokončíme vytváranie zóny pomocou Next a Finish. Onedlho si Slave stiahne záznamy z DNS Master servera.

5.3 NTP

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.Využijeme opäť win+R , zadáme w32tm /config /update,čím vlastne spustíme NTP server na danom zariadení.

Na aplikáciu zmien sme reštartovali Windows Timeservice príkazom zadaným do commandline:

net stop w32time && net start w32tim.

5.4 NAT

Nainštalovanie sme vykonali vo Windows Server Manageri, kde cez Add Roles and Features. Pridali sme

imidž

potvrdili sme službu Routing a následne sme ju nainštalovali. Pri inštalácii zvolíme sieťový adaptér eth0, ktorý je pripojený k internetu. Po inštalácii je NAT plne funkčné, ale je potrebné pridať NAT záznamy na porte 53. Ďalej sme ho potrebovali nakonfigurovať v control panel -> Administrative tools -> Routing and Remote Access. Po kliknutí na NAT, vyberieme záložku s adaptérom, ktorý je pripojený k internet. V Address Pool je potrebné nastaviť from, čo znamená našu počiatočnú public adresu 158.193.139.74 a to, čo je naša koncová adresa 158.193.139.75 a maska 255.255.255.0. V záložke services and ports je potrebné pridať 4 nové záznamy NAT pre DNS(Master-Slave, TCP-UDP).

5.5 Web server

Webserver ISS (Internet Information Server) sme pridali cez windows server manager tlačidlom Addroles and features, kde sme vyhľadali Web Server ISS a po-

kračujeme ďalej. Pri ponuke Role Services

Následne nainštalujeme služby na server. 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.

Po inštalácii sa nachádza ISS v ľavom paneli vo Windows Server Manager-i. Po kliknutí na tools v pravom hornom rohu klikneme Internet Information Services (ISS) manager. A po rozkliknutí na ľavom rohu je už vytvorená default sites. Otvoriť ju je možné zadaním do browseru “localhost”.

5.6 Poštový server

V server manageri klikneme na tools a v záložne DNS, nasmerujume sa ku DNS severu a vytvoríme nové záznamy pre mail server. Cname záznam mail 158.193.139.74, dva MX(Mail exchanger) záznamy 0 mail sos3.local a 10 mail sos3.local.

Zo stránky mailenable.com stiahneme standart edition. Začneme inštaláciou stiahnutého balíčka, zaklikneme web mail service(server). V nasledujúcich krokoch napíšeme do Domain Name: sos3.local a DNS host: 192.168.0.2 a smtp port: 25. Počas inštalácie nám vybehne tabuľká, kde odklikneme aby sa mailserver inštaloval ako webserver ISS. V server manageri po kliknutí servers -¿ localhost -¿ system -¿ diagnose si skontrolujeme či všetky políčka sú pass, čo nám značí že mail enable funguje. V ďalšom kroku servers -¿ localhost -¿ services and connectors a na SMTP klikneme pravým tlačidlom a klikneme na properties. V záložne general nastavíme default mail domain name čo je v našom prípade mail.sos3.local. Ďalej v záložke smart host nastavíme IP/DOMAIN 158.193.139.74. Po reštarte serveru vidíme že, všetky service sú running.

Kapitola 6

Záver

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (**latexcompanion**).

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (**knuthwebsite**).

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum (**einstein**).