LATVIJAS UNIVERSITĀTE
DATORIKAS FAKULTĀTE

UZŅĒMUMA INFORMĀCIJAS SISTĒMAS IZVEIDE IZMANTOJOT ATVĒRTĀ PIRMKODA PROGRAMMATŪRU.

KVALIFIKĀCIJAS DARBS

Autors: **Braijens Staškevičs**
Studenta apliecības nr.: bs13004
Darba vadītājs: Juris Smirnovs

RĪGA 2015

ANOTĀCIJA

Kvalifikācijas darba "**Uzņēmuma informācijas sistēmas izveide izmantojot atvērtā pirmkoda programmatūru**" mērķis bija izveidot uzņēmuma SIA "Aerobs" informācijas sistēmu, kurā uzņēmuma darbinieki varētu droši glabāt datus, koplietot tos, bet galvenais - sistēmas izveidē jāizmanto atvērtā pirmkoda programmatūra.

Darba gaitā informācijas sistēma tika izveidota izmantojot virtualizāciju, tajā tika iekļauti sekojoši atvērtā pirmkoda risinājumi – Endian, Samba, BackupPC, Zabbix. Mērķis bija izveidot informācijas sistēmu, ko gala lietotāji var lietot izmantojot operētājsistēmas, kuru lietošanai nepieciešams iegādāties licenci, piemēram Windows 7.

Rezultātā tika izveidota informācijas sistēma atbilstoši tehniskajām prasībām. Šī sistēma ir viegli piepildināma ar jauniem risinājumiem, kā arī pielāgojama citiem uzņēmumiem.

ABSTRACT

The main goal of the qualification work "**Creating business information system by open source software**" is to create companies SIA "Aerobs" information system, where employees can share and save their documents. The main rule is to create this system using Open Source software.

This system was created using virtualization and used following Open Source solutions – Endian, Samba, BackupPC, Zabbix. The target was to create Open Source information system, which can use employees who may have computer's operating system which can use only if license is already bought, for example Windows 7.

As a result, was created information system which conform technical specification which was written by SIA "Aerobs". This information system is easy to supplement with new solutions, adjust it to another company.

SATURA RĀDĪTĀJS

APZĪMĒJUMU SARAKSTS

DNS - (Domain Name Server - angļu v.) Dalītu datu bāzu (domēnu vārdu serveru) kopums, kas nodrošina atbilstību starp domēnu vārdu adresēm un skaitliskajām IP adresēm. Sistēma DNS atbrīvo interneta lietotājus no nepieciešamības atcerēties garus skaitlisko adrešu sarakstus.[3]

IP adrese – (Internet Protocol Address - angļu v.) ir unikāls kādas ierīces (parasti datora) identifikators (tīkla slāņa protokola IP adrese), kurš ir pieslēgts lokālajam tīklam vai internetam[1].

SMNP - TCP/IP protokolu saimes sastāvdaļa, kas veic datoru tīkla mezglu un iekārtu (piem., tiltu, maršrutētāju) pārvaldību un konfigurācijas pārraudzību. [3]

DHCP - Protokols, kurš ļauj tīkla administratoriem centralizēti pārvaldīt un automatizēt IP adrešu organizāciju datoru tīklos. Organizācijai, apgādājot tās datoru lietotājus ar pieslēgumiem internetam, jānodrošina katram datoram sava IP adrese. Protokols DHCP ļauj tīkla administratoram pārraudzīt un izplatīt IP adreses no centrālā vadības punkta un automātiski nosūtīt jaunu IP adresi, ja dators tiek pieslēgts kādai citai vietai tīklā. [3]

SSH - (Secure Shell - angļu v.) SSH ir tīkla protokols, kurš ļauj drošu datu apmaiņu starp divām tīkla ierīcēm[5]. Šis protokols nodrošina šifrēšanu. Savienojumam tiek izmantot TCP protokols, 22. ports.

VPN - (Virtual Private Network - angļu v.) Publiska datoru tīkla mezglu kopa, kas, izmantojot dažādas sistēmas, izveidota tā, lai kā datu pārsūtīšanas vidi izmantotu internetu. Šīs sistēmas izmanto šifrēšanu un citus drošības pasākumus, lai piekļuve tīklam būtu nodrošināta tikai autorizētiem lietotājiem un neviens cits datus nevarētu pārķert. [3]

HTTP - (Tīkla Internet standartprotokols, kas nodrošina informācijas apmaiņu globālajā tīmeklī WWW. Protokolu HTTP izmanto hipersaišu veidošanai starp hiperteksta dokumentiem. Noklikšķinot peli uz kādas no hipersaitēm, ar šī protokola starpniecību tiek atvērts attiecīgais dokuments neatkarīgi no tā, kur šis dokuments tīklā Internet ir izvietots[3].

MAC adrese – (media access control address – angļu v.)ir unikāls identifikators, kas ir piešķirts tīkla adapterim, lai komunicētu fiziskajā tīkla segmentā. MAC adreses tiek izmantotas dažādās tīkla tehnoloģijās, lielākajā daļā no IEEE 802 standartu tīkla tehnoloģijām, tai skaitā Ethernet. MAC adreses tiek iekļautas un izmantotas OSI etalonmodeļa MAC protokola apakšslānī[4].

FTP – (File Transfer Protocol – angļu v.) CP/IP protokolu sistēmas sastāvdaļa, kas aptuveni atbilst atvērto sistēmu sadarbības bāzes etalonmodeļa lietojumslānim. Izmantojot protokola TCP pakalpojumus, protokols FTP ļauj tīkla lietotājiem apskatīt attālu datoru direktorijus, nolasīt, pārsūtīt vai atjaunot to datnes[3].

LAN – (Local Area Network – angļu v.) Lokālais tīkls. Datoru tīkls, kas izvietots nelielā teritorijā un atrodas lietotāja pārziņā. Lokālais tīkls sastāv no sakaru līnijām, kas savieno personālos datorus un citas elektroniskās koplietošanas iekārtas (printerus, ploterus, datu uzkrāšanas un glabāšanas ierīces)[3].

WAN – (Wide Area Network – angļu v.) Datoru tīkls, kas savieno attālus lietotājus, kuri var atrasties citās pilsētās vai valstīs un kuri parasti izmanto vispārējās lietošanas vai speciālus sakaru līdzekļus[3].

RAM – (Random Access Memory – angļu v.) Operatīvā atmiņa. Datora primārās (operatīvās) atmiņas daļa, kurā uzglabātajām programmu instrukcijām un datiem ir iespējama tieša piekļuve no centrālā procesora, izmantojot ātrdarbīgo ārējo kopni. Atšķirībā no otra primārās atmiņas komponenta - lasāmatmiņas - no brīvpiekļuves atmiņas centrālais procesors var ne tikai nolasīt datus, bet var datus tajā arī ierakstīt[3].

UDP – (User Datagram Protocol – angļu v.) Lietotāja diagrammu protokols. TCP/IP protokolu komplekta protokols, kas ļauj lietojumprogrammai nosūtīt ziņojumu vienam vai vairākiem kāda datora lietojumiem. Ja, lietojot protokolu UDP, nepieciešama droša pārraide, tad lietojumprogrammā jābūt ietvertai pakešu secības pārbaudei un kļūdu notifikācijai[3].

OS – (Operating System – angļu v.) Operētājsistēma. Programmu komplekss, kas vada datu organizēšanu un programmu izpildi datorā, nodrošina aparatūras un programmatūras kopdarbību, resursu racionālu izmantošanu, kā arī sadarbību ar lietotāju[3].

OID – (Object Identifier – angļu v.) Objekta identifikators. Numurs, kas identificē objektu klasi vai atribūtu. To izmanto veicot monitoringu, piemēram ar SMNP protokolu[3].

SSL – (Secure Sockets Layer – angļu v.) Drošligzdu slānis. Firmas Netscape Communications izstrādāts protokols drošas un privātas saziņas nodrošināšanai internetā. Kad seanss, kurš izmanto drošligzdu slāni, ir sācies, serveris aizsūta publisko atslēgu pārlūkprogrammai. Pārlūkprogramma to izmanto, lai nosūtītu patvaļīgi ģenerētu slepeno atslēgu atpakaļ serverim, tādējādi nodrošinot iespēju apmainīties ar slepenajām atslēgām seansa laikā[3].

NAT – (Network Address Translation – angļu v.) Tīkla adrešu translēšana. Interneta standarts, kas lokālajos tīklos nodrošina vienas IP adrešu kopas izmantošanu iekšējam trafikam,

bet otras - ārējā trafika adresēm. Standarts NAT izveido specifisku ugunsmūri iekšējo IP adrešu apslēpšanai un ļauj apvienot vairākus tīkla ISDN savienojumus vienā interneta savienojumā[3].

RSA – RSA šifrēšanas. Patentēts publiskās atslēgšifrēšanas algoritms, ko izstrādājuši RSA Data Security, Inc. darbinieki Rivest, Shamir un Adelman 1978.gadā. Šis algoritms ir šifrēšanas tehnikas PGP pamatā[3].

SMB - Servera ziņojumu bloka protokols. protokols, kas nodrošina klienta datora lietojumprogrammu ierakstīšanu servera datnēs un datņu nolasīšanu no tā, kā arī iespēju pieprasīt servera pakalpojumus datoru tīklā. Protokols SMB tiek izmantots internetā virs TCP/IP protokoliem. Izmantojot protokolu SMB lietojumprogrammām to lietotājiem tiek nodrošināta gan piekļuve datnēm attālos serveros, gan iespējas izmantot arī citus resursus, piem., printerus[3].

IEVADS

Mūsdienās ļoti aktuāla tendence ir veidot mazos uzņēmumus, kuru viena kalendārā gada apgrozījums nepārsniedz 100 000 EUR[2] . Šie uzņēmumi tiek veidoti dažādu preču pārdošanai, kā arī ar mērķi sniegt pakalpojumus. Galvenais iemesls, kāpēc daudzi uzņēmēji izvēlās dibināt mikrouzņēmums ir tā salīdzinoši zemās dibināšanas izmaksas, kā arī atvieglinātā nodokļu politika salīdzinot ar uzņēmumu, kurš likumā noteiktā kārtībā nespēj būt mikrouzņēmums.

Mikrouzņēmums bieži dibina personas, kuras iepriekš nav bijušas uzņēmēji vai kāda cita veida saimnieciskās darbības veicēji, tādejādi uzsākot savas gaitas uzņēmējdarbībā. Bieži šo jauno uzņēmēju rīcībā uzsākot darbību nav iespējams atvēlēt pietiekoši lielu naudas summu licencētu informācijas sistēmu izveidē, tāpēc aplūkosim uzņēmuma informācijas sistēmas izveides iespējas izmantojot atvērtā pirmkoda programmatūru.

Darba mērķis ir izstrādāt biznesa informācijas sistēmas projektu, izmantojot atvērtā pirmkoda programmatūru, uzņēmumam SIA "Aerobs", kurš nodarbojās ar pakalpojumu sniegšanu un ir mikrouzņēmuma nodokļa maksātājs.

Izstrādē netiks izmantotas+ specifiski šī uzņēmuma darbības sfērai veidotas atvērtā pirmkoda programmatūras, tāpēc šo sistēmu būs iespējams pielāgot lielākai daļai jaundibināto uzņēmumu.

Darba uzdevums ir, izmantojot atvērtā pirmkoda programmatūru, izveidot informācijas sistēmu ar tai nepieciešamajiem drošības elementiem, mūsdienu populārākajām tendencēm un inovatīvākajiem risinājumiem, kas apmierina uzņēmuma SIA "Aerobs" biznesa prasības, praktisko pielietojumu gala lietotājiem, un nodrošina uzņēmuma datu drošību.

Darba strukturēšana notiks vadoties pēc Latvijas Universitātes izdotas un 03.02.2012. apstiprināta resursa "PRASĪBAS NOSLĒGUMA DARBU IZSTRĀDĀŠANAI UN AIZSTĀVĒŠANAI LATVIJAS UNIVERSITĀTĒ", kā arī Latvijas Universitātes Datorikas fakultātes apstiprināta resursa “KVALIFIKĀCIJAS DARBA IZSTRĀDES UN AIZSTĀVĒŠANAS METODISKIE NORĀDĪJUMI”.

1. BIZNESA INFORMĀCIJAS SISTĒMAS IZVEIDES IZPĒTE

1.1. **Biznesa prasības**

Uzņēmums, kuram tiek projektēta konkrētā biznesa informācijas sistēma nodarbojas ar pakalpojumu sniegšanu, tajā strādā 4 darbinieki, uzņēmuma apgrozījums katru gadu aug, tāpēc tuvākā nākotnē plānots pieņemt darbā vēl papildus darbiniekus. Svarīgākais uzņēmuma darbības nodrošināšanai ir failu koplietošana, centralizēta glabāšana, datu aizsardzība, piekļuve failiem atrodoties ārpus biroja telpām.

1.2. **Tehniskās un funkcionālās prasības**

Tehniskās prasības, kuras noteikti jānodrošina projektējamai sistēmai:

- failu koplietošanas iespēja,
- gala lietotāji izmantos Microsoft Windows ražoto operētājsistēmu Windows 7 64bit,
- neatkarīgi vai gala lietotājs izvēlēsies lietot galda darbstaciju vai portatīvo datoru, iekštīklā tas izmantos tikai kabeļus ar RJ45 savienojuma kontaktu,
- jānovērš jebkāda veida savienojumu iespējamība ar neautorizētiem pieslēgumiem jeb uzbrukumi sistēmai,
- jāveic sistēmas uzraudzība un potenciālo draudu novēršana,
    - serveriem:
        - procesora noslodze,
        - operatīvās atmiņas daudzums – pieejamais un izlietotais,
        - cietā diska atmiņas daudzums – pieejamais un izlietotais,
        - sistēmas darbības laiks (laiks, kopš ieslēgšanas),
        - ienākošā un izejošā datu plūsma,
        - sasniedzamība no monitoringa servera,
    - darbstacijām:
        - procesora noslodze,
        - operatīvās atmiņas daudzums – pieejamais un izlietotais,
        - cietā diska atmiņas daudzums – pieejamais un izlietotais,
        - sasniedzamība no monitoringa servera,

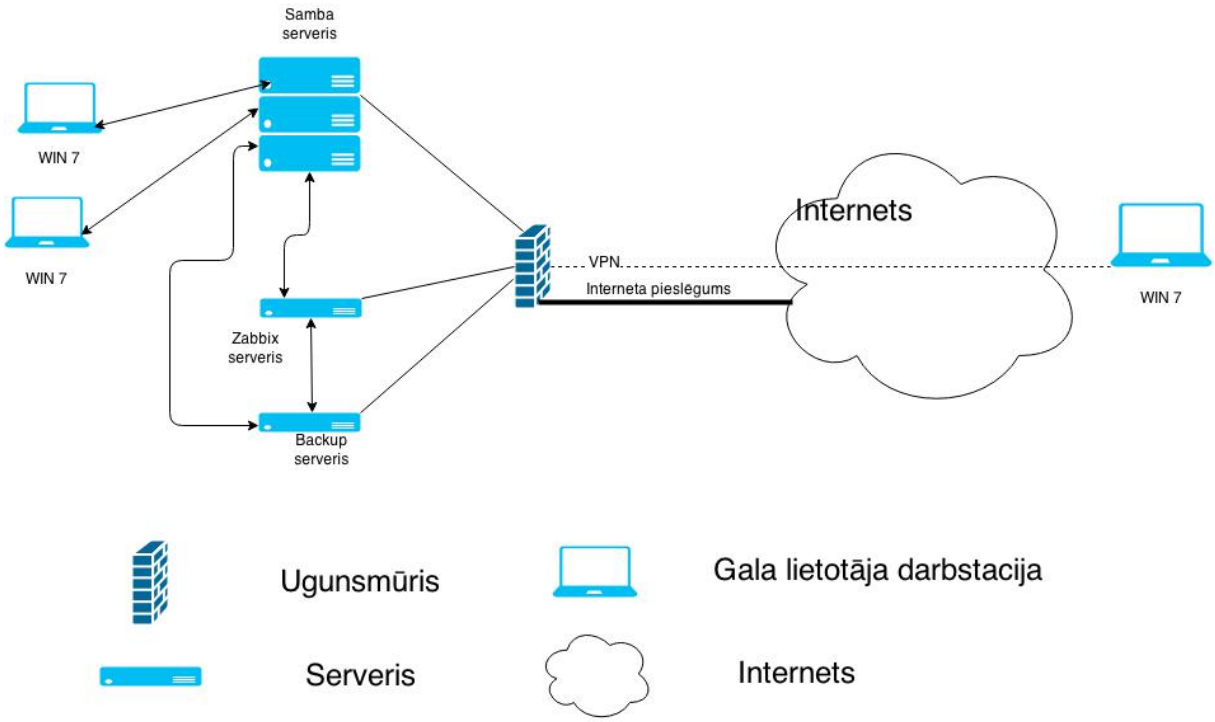
- iespēja, izmantojot Interneta starpniecību, pieslēgties iekštīklam ar VPN savienojumu,
- statiska IP ārējā adrese,
- regulāra rezerves kopiju izveide:
    - pilnās rezerves kopijas izveide katru Pirmdienu pulksten 01:00;
    - inkrementālā rezerves kopija katru dienu pulksten 00:00;
    - tiek saglabātas 5 pilnās un 6 inkrementālās rezerves kopijas;
- lietotāju grupu izveide, grupu – administratori, uzņēmuma vadība, lietotāji,
- sistēmas lietotāju izveide – lietotājs Braijens Staškevičs grupā administratori, Juris Ozols – uzņēmuma vadība, Ieva Liepa un Agris Kalniņš – lietotāji.

Neskatoties uz to, ka gala lietotāji izmantos operētājsistēmu, kuras lietošanai nepieciešams iegādāties licenci, topošajai informācijas sistēmai jābūt atvērtā pirmkoda un bezmaksas risinājumiem, lai šo sistēmu potenciāli varētu pielāgot un izmantot arī citi uzņēmumi.

1.3. **Sistēmas lietotāji**

Atkarībā no grupas, kurā lietotāji tiks pievienoti, piemēram, “administratori”, “vadītāji” vai “lietotāji”, to piekļuves tiesības dažādām mapēm un datnēm jānodrošina atšķirīgas, jo uz servera uzņēmuma vadītājs glabās datus, kuri satur komercnoslēpumu un tos nedrīkst ne lasīt, ne rediģēt uzņēmuma darbinieki. Tieši šādu, kā arī citu iemeslu dēļ ne tikai lietotāju grupām būs atšķirīgas piekļuves tiesības, bet arī pašiem darbiniekiem tās būs atšķirīgas. Lietotājs Braijens Staškevičs šinī informācijas sistēmā ir paredzēts kā sistēmas administrators, tāpēc tam tiek nodrošinātas tiesības visos sistēmas serveros. Kā administrators, tas drīkst arī pārlūkot visus koplietotos failus, rediģēt uzstādījumus, dzēst, pievienot tos jebkurā mapē. Katram lietotājam - Jurim Ozolam, Ievai Liepai un Agrim Kalniņam sistēmā tiek izveidota mape, kurā tas var glabāt savus dokumentus, tomēr bez īpašām atļauju piešķiršanām, citi lietotāji šinīs mapēs neredz to saturu, līdz ar ko nevar rediģēt to. Tiek izveidota arī mape, kurā glabājas uzņēmuma dokumenti, kurā ikviens darbinieks redz saturu, var pievienot failus, tomēr dzēst tos drīkst tikai sistēmas administrators, kā arī uzņēmuma vadītājs, un tiek izveidota mape, kurā darbinieki var koplietot savus failus – ievietot tos, dzēst, labot, tomēr visiem darbiniekiem ir vienādās tiesības, tāpēc kolēģis varēs izdzēst cita kolēģa ievietotos failus.

1.4. **Projektējuma skice**



1.4.1. att. **Biroja informācijas sistēmas projektējums**

1.5. **Programmatūras izvēlē**

1.5.1. **Atvērtā pirmkoda programmatūra**

Atvērtā pirmkoda programmatūra (Open Source Software - angļu v.) ir programmatūra, kuras pirmkodu atklāti izmanto tās veidotāji un lietotāji. Šādas programmatūras priekšrocība ir iespēja tās programmētājiem un izmantotājiem jau programmas izstrādes gaitā attīstīt un pielāgot programmu specifisku uzdevumu risināšanai. [3] Programmatūru ar šādu licenci drīkst izmantot, modificēt, papildināt, bez tās pirmatnējā izstrādātāja ziņas. Kā arī tās izmantošana ir bez maksas. Lai gan tas skan mazliet dīvaini - izmantot kāda cita radītu produktu bez maksas, tomēr bieži vien ražotāji, kuri piedāvā daļu savas programmatūras bez maksas, lai lietotāji to izmantotu, atklātu kļūdas un par to ziņotu, tai pašā laikā šis uzņēmums pārdod arī programmatūras maksas versiju, kurā tas sola mazāk kļūdu, iespējams kādus citus labumus, piemēram telefonisku atbalstu 24 stundas dienā. Tirgū ir pieejamas ne tikai lietojumprogrammas ar atvērtā pirmkoda licenci, bet pat operētājsistēmas.

1.5.2. **Serveru operētājsistēma**

Sākot plānot serveru ieviešanu, uz kuriem būs izvietota gan failu koplietošanas sistēma, gan pārraudzības sistēma, gan rezerves kopiju veidošanas sistēma, pirmais ar ko saistās atvērtā pirmkoda programmatūra ir Linux. Kaut arī tam ir daudz distributīvi, vietnē www.distrowatch.com atrodamajā topā redzams, ka pats populārākais[28] distributīvs ir Mint, kam seko Ubuntu un Debian. Tā kā šinī topā ir apskatītas, gan operētājsistēmas lietotāju datoriem, gan serveriem, tad nākas secināt, ka Ubuntu ir operētājsistēma, kura ir pieejama gan personālo datoru lietotājiem, gan serveriem. Papētot Ubuntu serveru iespējas un priekšrocības, secināts, ka tam ir pieejami risinājumi, kurus nepieciešams, lai radītu šo plānoto informācijas sistēmu. Kā arī aparatūras prasības, kuras ir uzrādījis operētājsistēmas ražotājs, nav pārāk lielas, kas savukārt veicina šīs informācijas sistēmas izveides mērķi - radīt informācijas sistēmu mazajiem uzņēmumiem. Lai instalētu šos sistēmu nebūs nepieciešams pirkt jaunus, dārgus serverus, bet pietiek ar jau lietošanā esošu datoru, kura tehniskie parametri atbilst operētājsistēmas ražotāja izvirzītajām prasībām.

Ubuntu operētājsistēma ir radīta 2004. gadā[20].Versijas šī distributīva operētājsistēmām iznāk pietiekoši bieži. Par to, cik veca ir konkrētā versija var spriest pēc versijas nosaukuma, piemēram, 14.04., kur pirmais skaitlis apzīmē gadu, kurā izdota (t.i. 14 nozīmē 2014. gadā), bet otrs skaitlis liecina par ceturksni kurā iznākusi versija. Jaunas versijas iznāk reizi 6 mēnešos, un katra 4. versija pie nosaukuma iegūst papildinājumu "LTS" (long-term support - angļu v.), kas tulkojumā jāsaprot, kā ilgstoši tehniski atbalstītā jeb Ubuntu šai versijai vismaz 2 gadus sola nodrošināt atjauninājumus, kā arī tehnisko atbalstu.

Mūsu izstrādājamai informācijas sistēmai izvēlēsimies "Ubuntu Server 14.04. LTS". Ražotāja mājaslapā atrodamajās prasībās norādīts, ka standarta instalācijai nepieciešams, ka iekārtai, uz kuras uzstādīs šo operētājsistēmu "Ubuntu Server 14.04. LTS", nepieciešams vismaz[27] - 1 GHz procesors, 512 MB brīvpiekļuves atmiņa, 1,75 GB cietā diska atmiņas.

1.5.3. **Pārraudzības sistēma**

Mūsdienās ir radītas ļoti daudz sistēmu pārraudzības programmatūras. Tirgū ir pieejamas gan atvērtā pirmkoda programmas, gan tādas, kuru lietošanai jāiegādājas licence. Neatkāpjoties no projekta mērķa, meklējam piemērotāko. Veicot piemērotākās sistēmas izvēli, ļoti uzskatāmi par populārākajām pārraudzības sistēmām ir izveidota tabula Interneta enciklopēdijā

www.wikipedia.org.[13] Aplūkojot šo tabulu, jāsecina, ka Latvijā radītā Zabbix pārraudzības sistēma ir viena no labākajām, tāpēc tuvākai sistēmas izpētei tiek izmantota produkta mājaslapa. Iepazīstoties ar mājaslapā www.zabbix.com atrodamo informāciju, secinu, ka šis produkts tieši piemērots projektam, jo tas nodrošina visu nepieciešamo sistēmas pārraudzību - izmantojot SNMP protokolu, PROXY servera atbalsts, kas ir būtisks lai veiktu monitoringu iekārtā, kura atrodas ārpus biroja vai kādu brīdi nevar sazināties ar pārraudzības serveri, kurā tiek uzkrāti un analizēti dati. Šim produktam ir daudz, citu lietotāju radīti risinājumi efektīvai sistēmu pārraudzībai.

Izpētot Zabbix piedācātās monitorēšanas iespējas, secināts, ka ir pieejami risinājumi darbstacijām, kuras neatrodas nepārtraukti tīklā vai ir paredzēts lietot darbstaciju bez tīkla pieslēguma kādu laika posmu, tas atbalsta šīs biznesa informācijas sistēmas projektā izvirzīto lietojamo operētājsistēmu lietojumu - gan Linux (tātad arī Ubuntu), gan Windows (tikai kā aģents, nevis serveris). Apkopojot secināts, ka projekta pārraudzībai tiks izmantota Zabbix programmatūra, kas ir radīta Latvijā.

1.5.4. **Ugunsmūris, maršrutētājs, VPN**

Lai izveidotu datortīklu, ar pienācīgu aizsardzību pret datu zādzībām, par tā aizsardzību jārūpējas pienācīgi - jālieto ugunsmūri, jāierobežo dažādas piekļuves tiesības, jālieto šifrētie savienojumi, utt. Arī plānotājā informācijas sistēmā paredzēts glabāt failus un dokumentus, kuru nonākšana trešo pušu rīcībā nav pieļaujama, tāpēc jāvadās pēc labās prakses informācijas sistēmu drošības nodrošināšanā.

Meklējot ugunsmūri topošai informācijas sistēmai, uzmanību piesaistīja kompānijas Endian risinājums. Kompānija Endian piedāvā gan atvērtā pirmkoda (ar ierobežotām iespējām), gan risinājumus, kura lietošanai nepieciešama licences iegāde. Papētot sīkāk atvērtā pirmkoda risinājumu, secināju, ka tas nodrošina visus nepieciešamos drošības risinājumus, kā arī ir ērts lietošanā - to var lietot gan kā virtuālo mašīnu, gan uzstādīt tīkla iekārtā, kā tās operētājsistēmu. Endian risinājums piedāvā visus svarīgos servisus - DHCP, DNS, ugunsmūri, VPN, dažādus filtrus, portu pārvirzīšanu, utt. Tāpēc pieņemts lēmums, ka aizsardzībai, kā arī funkcionalitātes nodrošināšanai tiks izmantots Endian atvērtā pirmkoda risinājums.

1.5.5. **Failu koplietošana**

Failu koplietošanas servisam, kurš tiks uzstādīts uz Linux operētājsistēmas Ubuntu distributīva, jānodrošina piekļuve failiem no Microsoft ražotajām Windows 7 PRO 64bit operētājsistēmām. Tieši šī ir pati svarīgākā prasība failu koplietošanas serverim.

Ubuntu mājaslapā ievietotā informācija liecina, ka failu un drukas iekārtas koplietošanai jāizmanto Samba serveris. Tieši tas izmanto protokolus, kurus saziņai ar to izmanto Windows operētājsistēma, līdz ar ko ir iespējama failu apmaiņa. Tā kā šis viennozīmīgi ir tas, kas projektam ir nepieciešams un ir ļoti būtisks, tad Samba serveris tiks izmantots, lai nodrošinātu failu koplietošanu starp darbiniekiem.

Failu koplietošanas, apskates, rediģēšanas un piekļuves tiesības ir noteiktas informācijas sistēmas tehniskajās prasībās.

1.5.6. **Rezerves kopiju veidošana**

Rezerves kopiju veidošana ir būtisks aizsardzības mehānisms pret datu zaudēšanu informācijas sistēmā. Ar to iespējams samazināt datu zaudēšanu līdz niecīgam līmenim. Būtiski ir izstrādāt datu kopiju veidošanas shēmu – kurā dienā, cikos, kāda tipa kopija jāveido. Lai pēc iespējas labāk izvairītos no datu pazaudēšanas, arī izstrādājamajā informācijas sistēmā tiek ieviests rezerves kopiju veidojošais serveris.

Meklējot piemērotāko atvērtā pirmkoda programmatūru, tika apskatīts Interneta enciklopēdijā izveidotais rezerves kopiju veidošanai izmantojamās programmatūras salīdzinājums[15]. Tika secināts, ka līdzvērtīgākie konkurenti ir BackupPC un Bacula, kas nodrošina visplašākās iespējas – gan komandrindas saskarni, gan grafisko, kā arī piedāvā rezerves kopiju veidošanu Windows sistēmām, kas var būt noderīgi, ja nepieciešams izveidot datu rezerves kopiju Windows darbstacijai vai serverim, ja papildinot un pielāgojot šo informācijas sistēmu, tādi tiktu ieviesti, tomēr Bacula par Windows operētājsistēmu kopiju veidošanu ir nepieciešama licence, tāpēc šinī informācijas sistēmā tiks izmantot BackupPC piedāvātais atvērtā pirmkoda risinājums datu rezerves kopiju veidošanai.

Informācijas sistēmas tehniskā specifikācija paredz, ka jāveido divu veida rezerves kopijas - pilnā un inkrementālā. Pilnā rezerves kopija paredz visu norādīto datu dublēšanu, tomēr inkrementālā – izmainīto vai papildināto, vai dzēsto datu jeb veikto izmaiņu dublēšanu.

1.6. **Projekta tehniskā realizācija**

Informācijas sistēmas izstrādei ir nepieciešami vismaz trīs serveri. SIA “Aerobs” plāno izmantot tā rīcībā esošo datortehniku un tam nav iespējas veikt lielas investīcijas aparatūrā. Lai nodrošinātu optimālu finanšu un aparatūras resursu izmantošanu, fizisko serveru vietā tiks izmantotas virtuālās mašīnas. Efektivitāte, elektroenerģijas ekonomija, mobilitāte, uzskatāmība, gandrīz identiska realizācija salīdzinot ar aparātu risinājumiem - tieši tādi ir lielākie virtualizācijas izmantošanas plusi.

1.6.1. **Virtualizācija**

Virtuālo mašīnu izveidei, kā arī darbināšanai tiks izmantots Oracle radīts "virtualizātors" ar nosaukumu "Virtualbox", kurš nodrošina pilnu virtualizāciju[21] jeb operētājsistēma, kuru uzstādīs virtuālajā mašīnā, "domās", ka tā darbojas uz pilnīgi neatkarīgas ierīces.

Izvēle taisīt šo projektu ar virtuālo mašīnu palīdzību tika pieņemta, lai iegūtu efektīvāku resursu izmantošanu, tomēr saglabātu funkcionalitāti. Tādejādi, ja šo projektu nolemtu attīstīt tālāk un veikt idejas pārdošanu citiem uzņēmumiem, to būtu iespējams viegli prezentēt un tam būtu nepieciešama tikai 1 fiziska iekārta, uz kuras uzstādīta virtuālajām mašīnām nepieciešamā programmatūra.

"Virtualbox" ir atvērtā pirmkoda programmatūra, kuru iespējams uzstādīt uz populārākajām operētājsistēmām - Windows, Linux, Mac OS X, Solaris.

Šis Oracle produkts nodrošina arī nepieciešamos uzstādījumus, kuri būs jākonfigurē, lai virtuālo mašīnu darbību maksimāli pietuvinātu to reālajai darbībai dzīvē. Tas nodrošina dažādas tīkla konfigurācijas, kas būs ļoti svarīgi šī projekta izstrādē.

1.6.2. **Datortīkla uzbūve un tīkla adrešu dalīšana**

Datortīkla uzbūve plānota slēgta – tai nevarēs pieslēgties jebkurš, neatrodoties biroja telpās un fiziski neizveidojot savienojumu ar maršrutētāju izmantojot, datortīkla kabeli ar RJ45 savienojuma kontaktu datoram, tomēr to būs iespējams izdarīt, ja lietotājam tik izveidota pieeja informācijas sistēmai izmantojot VPN savienojumu. Datortīkla iekštīklā izmantos kabeļus, kuri savienos lietotāja darbstaciju ar Endian maršrutētāju, kas savukārt ir savienots ar serveriem un Internetu, tādejādi nodrošinot lietotājiem piekļuvi gan serveriem, kas atradīsies iekštīklā, gan

Internetam. Nav plānots birojā izvietot bezvadu interneta piekļuves punktus. Atrodoties ārpus biroja, informācijas sistēmai būs iespējams tikai noteiktiem lietotājiem, kuriem tiks piešķirts lietotājvārds un parole, lai izveidotu VPN savienojumu.

IPv4 adrešu dalīšanu serveriem un datoriem nodrošinās DHCP serviss, tam tiks norādīts konkrēts apgabals, kuru tas varēs piešķirt lietošanā kādai iekārtai, kura veiks pieprasījumu DHCP serverī. Šis apgabals, kurā tiks piešķirtas IP adreses būs no 10.0.0.2 līdz 10.0.0.199, kurām apakštīkla maskas adrese būs 255.255.255.0. Šis būs C klases tīkls. Tīkla vārtejas adrese būs 10.0.0.1, kas vienlaicīgi būs arī "Firewall" adrese. Tieši virtuālā mašīna "Firewall" nodrošinās tīkla adrešu izdalīšanu, jo tajā darbosies DHCP serviss.

VPN serverī arī adreses tiks dalītas izmantojot DHCP serveri, adrešu apgabals, kurā tiks piešķirtas IP adreses būs no 10.0.0.200 līdz 10.0.0.254, kurām apakštīkla maska būs 255.255.255.0, kas arī ir C klases tīkls. Kad tiks izveidots VPN savienojums, lietotājam netiks ierobežota pieeja nevienam resursam, tas varēs piekļūt tieši tā pat kā to varētu izdarīt atrodoties biroja telpās.

Tā kā informācijas sistēmas ārējā adrese jeb adrese, kuru piešķirs Interneta servisa piegādātājs, būs statiska (to paredz tehniskā specifikācija), tad to būs tikai vienreiz jāuzkonfigurē.

Serveru viena no svarīgākajām prasībām ir, ka tīkla adrese ir statiska jeb nemainīga. Tas ir ļoti būtiski, lai spētu nodrošināt veiksmīgu klientu (darbstaciju) pieslēgšanos pie īstā servera. Piemēram monitoringa sistēmas "Zabbix" servera adrese nedrīkst būt dinamiska, jo konfigurējot Zabbix aģentus, kuri atradīsies piemēram "Samba" serverī, tiem būs jānorāda konkrēta IP adrese vai DNS vārds, no kuras Zabbix serveris varēs nolasīt monitoringa vērtības.

Ieplānotās jeb rezervētās IP adreses, kuras tik inicializētas izmantojot MAC adreses rezervāciju, jeb brīdī, kad tiks veikt pieprasījums DHCP serverī, tas pārbaudīs, vai MAC adrese nesakrīt ar kādu no tām, kuras ievadītas rezervācijas sarakstā, ja tā notiks, tad tiks atgriezta rezervētā IP adrese.

2. BIROJA INFORMĀCIJAS SISTĒMAS PRAKTISKĀ REALIZĀCIJA

2.1. **Virtualbox konfigurēšana**

2.1.1. **Virtuālo mašīnu nosaukumi**

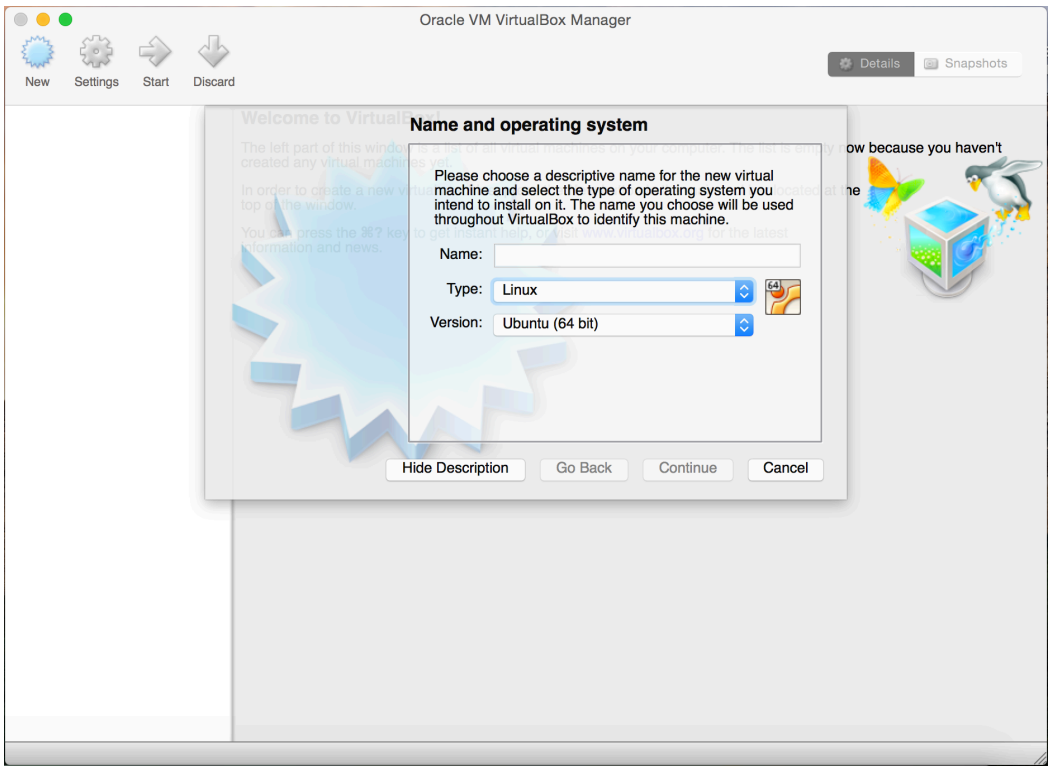
Veidojot virtuālās mašīnas, tām būs jāpiešķir nosaukumi, tāpēc jau iepriekš tām tiks izvēlēti nosaukumi, kuri vēlāk konfigurēšanas laikā tiks piešķirta katrai mašīna. Tie tiks veidoti atbilstoši virtuālās mašīnas funkcijai vai servisam, kuru tā veiks, lai turpmāk to varētu vieglāk identificēt.

Nosaukumi:

- Firewall – virtuālajā mašīnā tiks uzstādīts Endian ugunsmūris, kurš nodrošinās arī citas funkcijas;
- Samba – serveris, kurš tiks izmantos failu koplietošanai;
- Zabbix – serveris, kuru izmantos informācijas sistēmas monitoringam ar Zabbix palīdzību;
- Backup – serveris, ar kuru tiks veidotas rezerves kopijas citiem serveriem un/vai darbstacijām, lai datu zaudēšanas gadījumā datus būt iespējams atgūt.

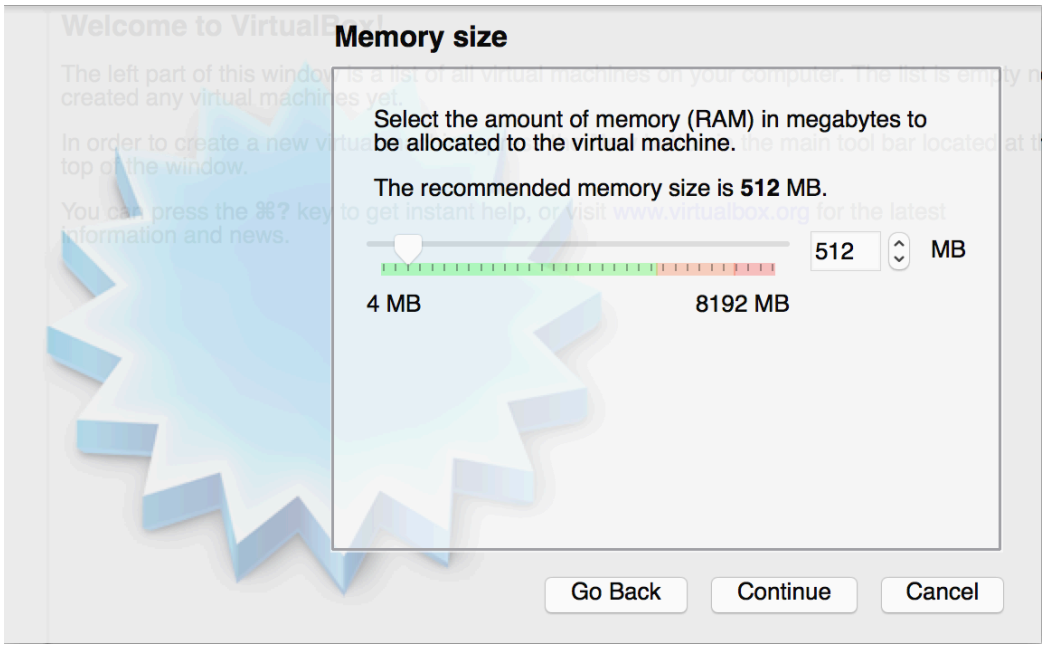
2.1.2. **Virtuālo mašīnu izveide**

Sākumā jāizveido 4 tukšas virtuālās mašīnas, kuras vēlāk modificēsim katra servera/servisa vajadzībām. Katrai no šīm mašīnām izvēlamies nosaukumu (name – angļu v.), tālāk jāizvēlas tips (type - angļu v.) jāuzstāda "Linux", bet versija (version – angļu v.) "Ubuntu 64bit", jo gan visi serveri, gan ugunsmūris ir bāzēti uz Linux sistēmu.



2.1.2.1 att. **Virtualbox virtuālās mašīnas nosaukuma ievadīšana, OS tipa un versijas izvēle**

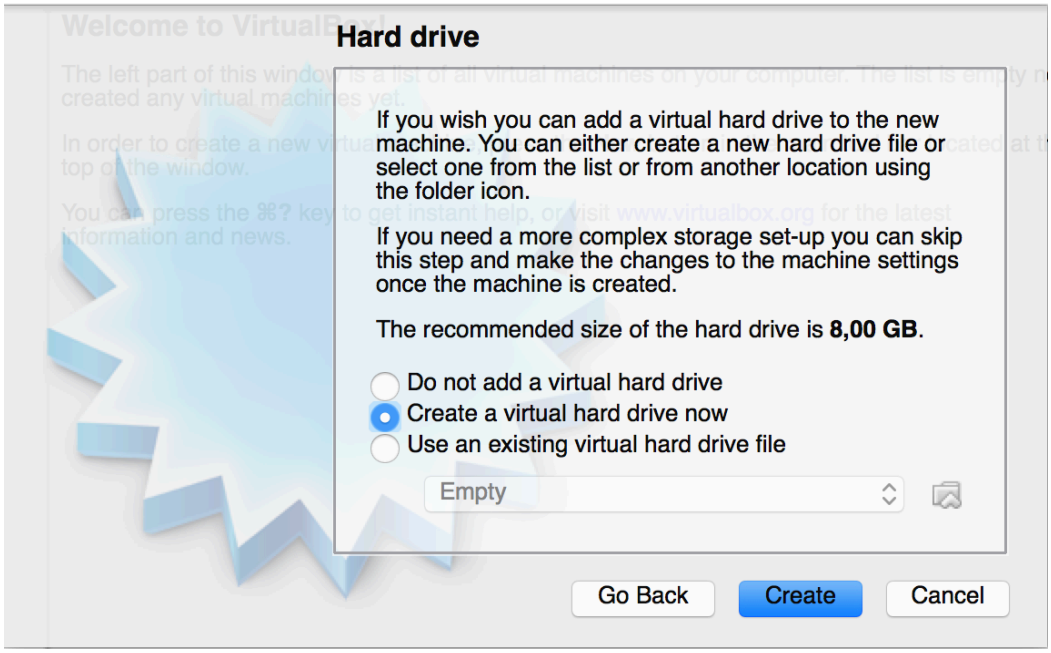
Katrai no šīm mašīnām sākumā iedalām 512MB brīvpiekļuves atmiņu (skat. 2.1.2.2. attēlu) un 8GB diska vietu. Ar to ir pietiekami, lai nodrošinātu katras mašīnas darbību bez traucējumiem, tomēr vajadzības gadījumā to vēlāk var mainīt.



2.1.2.2. att. **Brīvpiekļuves atmiņas (RAM) daudzuma izvēle virtuālajai mašīnai**

Kad ir definēts virtuālās mašīnas nosaukums, OS tips un versija, brīvpiekļuves atmiņas daudzums, ir pienācis laiks izveidot tās cieto disku, tā kā līdz šim to neesam veidojuši un mums

tas būs nepieciešams katrai no šīm četrām virtuālajām mašīnām, tad nākošajā solī izvēlamies *Veidot jaunu virtuālo cieto disku tagad* (Create a virtual hard drive now – angļu v.) (skat. 2.1.2.3. attēlu).

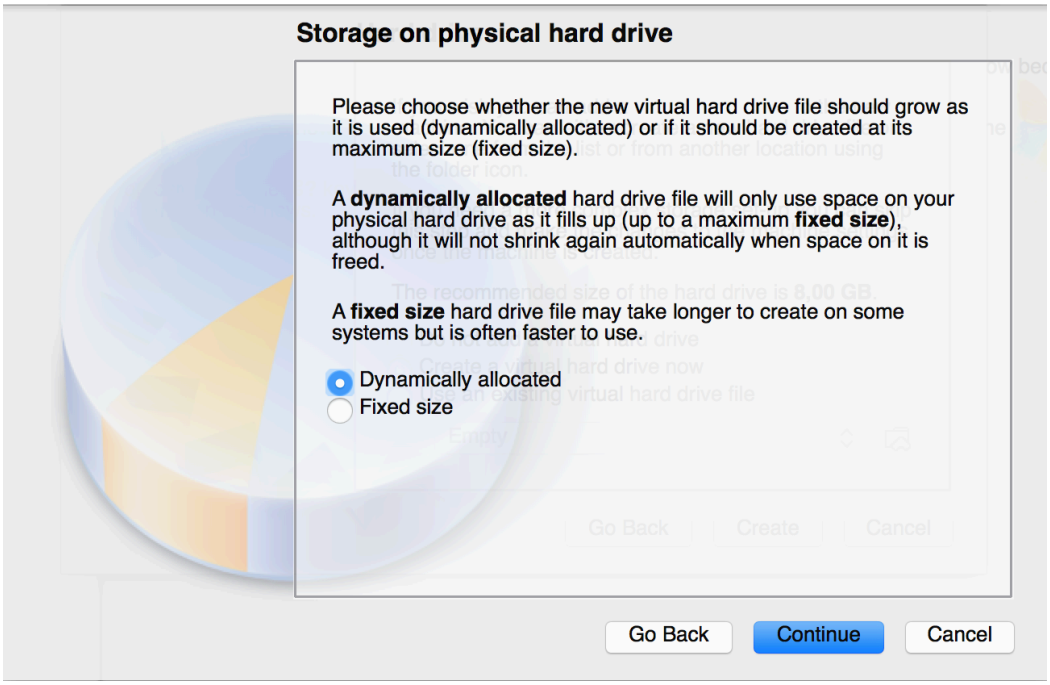


2.1.2.3. att. **Cietā diska izvēlne**

Nākošajā izvēlnē ir jāizvēlas cietā diska faila tips (Hard drive file type – angļu v.), kas nozīmē, ka jāizvēlas formāts, kādā tiks veidots cietais disks, kuru izmantos virtuālā mašīna. Šis virtuālās mašīnas cietais disks sistēmā, uz kuras tiek darbināts Virtualbox izveidos failu, kuru pievienojot virtuālajai mašīnai, tā uzskata, ka tā ir tās fiziska sastāvdaļa. Atkarībā no vajadzībām ir jāizvēlas šis tips. Tā kā neplānojam šīs virtuālās mašīnas pārvietot uz citiem virtuālo mašīnu dziņiem, tad izvēlamies *Virtualbox Disk Image* (skat. 2.1.2.4. attēlu), jo tad ir Oracle veidotais tips priekš tā produkta Virtualbox, kā arī tajā potenciāli varētu būt mazāk risku ar nesaderību ar Virtualbox.

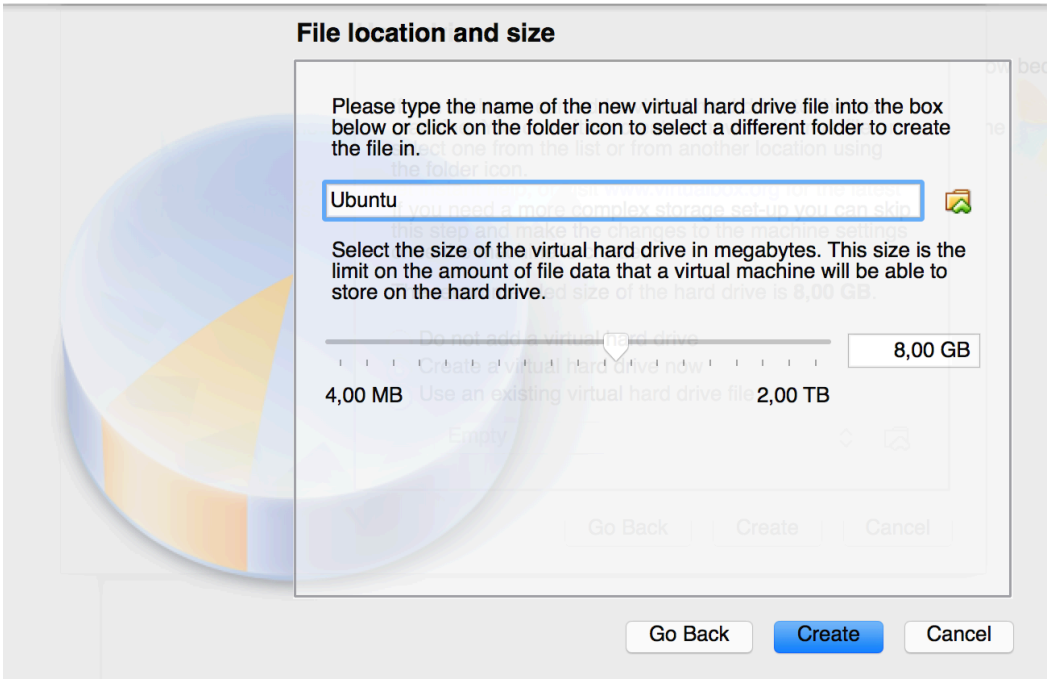
2.1.2.4. att. **Cietā diska faila tipa izvēle**

Kad ir izvēlēts cietā diska faila tips, jāizvēlas veids, kā šī datne tiks veidota. Šeit var izvēlēties dinamiski piešķirtu izmēru (Dynamically allocated – angļu v.) vai noteikts izmērs (Fixed size – angļu v.). Atšķirība ir veids, kā tiks veidots šis cietais disks virtuālajai mašīnai. Izmantojot dinamisko izmēra piešķiršanu, tiks veidots fails, kura izmērs dinamiski pieaugs vai samazināsies atkarībā no tā, vai virtuālā mašīna aizņems vairāk šī diska vietu vai nē, bet izvēloties noteikta tipa cieto disku, datorā, kurā būs uzstādīts Virtualbox, un uz kura tiks startētas virtuālās mašīnas, tiks izveidots noteikta lieluma fails, kura izmēra lielums nemainīsies atkarībā no veiktajām darbībām konkrētajā mašīnā. Šī izvēle ir ļoti lietderīga, ja tiek veidotas virtuālās mašīnas uz datora, kura cietā diska lielums nav tik liels, lai varētu veidot noteikta izmēra cietā diska failus. Arī šī darba veidošanai, visām četrām virtuālajām mašīnām izvēlamies *dinamiski piešķirtu izmēru* (skat. 2.1.2.5. attēlu).



2.1.2.5. att. **Cietā diska faila glabāšanas veida izvēle**

Pēdējā solī jāizvēlas šī cietā diska faila nosaukumu un diska lielumu (skat. 2.1.2.6. att.). Tā kā ugunsmūra un sistēmas monitoringa sistēmai nebūs nepieciešami cietie diski ar lielu atmiņas daudzumu, tad to lielumu izvēlamies 8,00 GB. Tomēr Samba serverim, kā arī Backup serverim izvēlēsimies 500,00 GB lielus cietos diskus, jo tiem būs nepieciešams glabāt failus un ar 8,00 GB lielu krātuve būs pārāk maza.



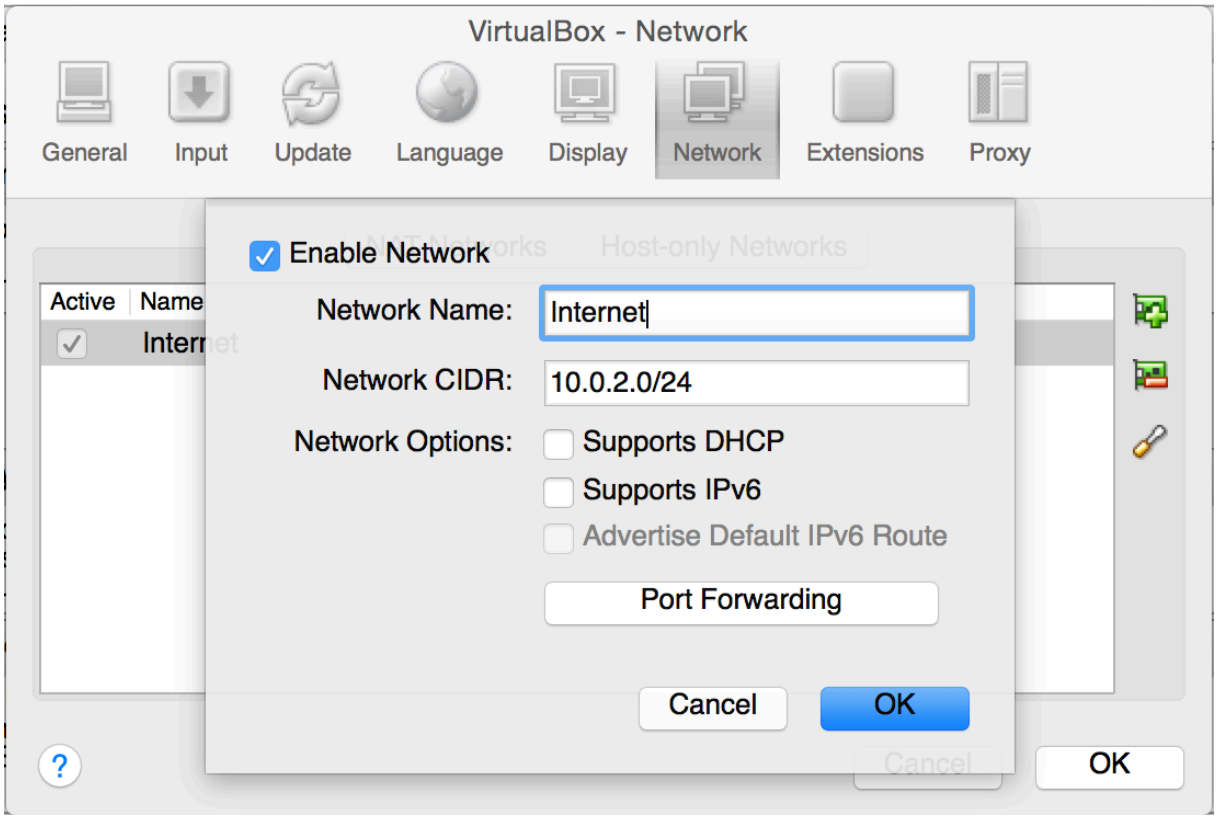
2.1.2.6. att. **Cietā diska nosaukuma un lieluma izvēle**

Priekš Windows 7 darbstacijām izvēlas *Windows 7 (64 bit)*, brīvpiekļuves atmiņas daudzums izvēlās 2048 MB, tas būs pietiekami, lai lietotu šo virtuālo mašīnu bez aizķeršanās, kā arī cietā diska lielumu izvēlamies vismaz 60 GB, lai neaptrūktos atmiņas daudzums.

2.1.3. **Tīkla konfigurēšana**

Pēc sekmīgas virtuālās mašīnas izveides, nākamais, tomēr ļoti būtisks solis ir izvēlēties tīkla adaptera/-u (Network adapter – angļu v.) uzstādījumus, lai virtuālās mašīnas darboties atbilstoši tehniskai specifikācijai un tiktu pietuvināta realitātei.

Tā kā būs nepieciešam imitēt Interneta darbību šinī darbā, kas būs nepieciešama VPN tunelim, konfigurējam speciālu tīklu iekš Virtualbox. Atverot Virtualbox uzstādījumos sadaļu *network* jāizveido jauns NAT *network*, kura nosaukums būs Internet, jo tas imitēs Interneta darbību. NAT network izveido tīklu, kurš ir pieejams tikai darbstacijas ietvaros, kurā uzstādīts Virtualbox[30].



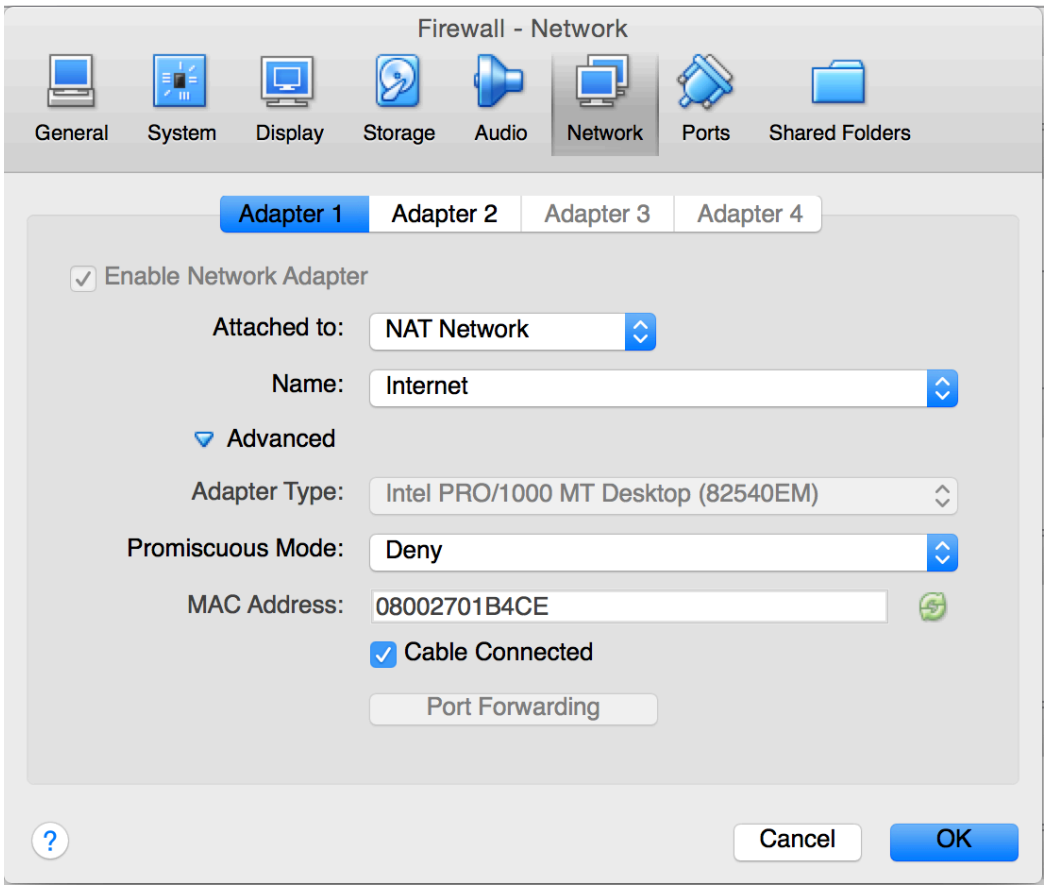
2.1.3.1.att. **NAT network konfigurēšana**

Pēc nosaukuma izveides, izvēlamies tīkla adrešu diapazonu, šeit atstāj noklusēto vērtību, jo tā atbilst vajadzībām, tomēr pēc noklusējuma ir ieslēgts DHCP, šo atspējo, jo adreses tiks

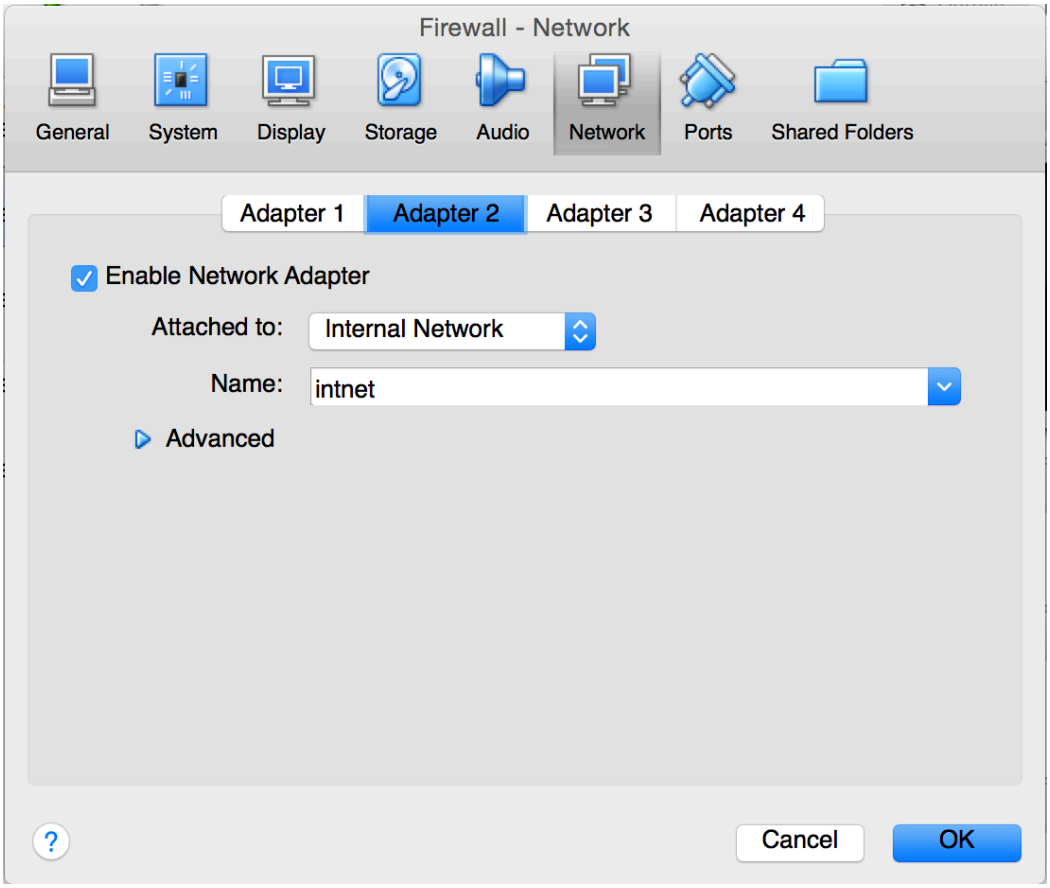
izvēlētas statiskas un ievadītas manuāli, lai sekmīgāk imitētu Interneta izmantošanu VPN savienojuma nodibināšanai.

2.1.3.1. Firewall

Ugunsmūra virtuālajai mašīnai jāieslēdz (Enable Network Adapter – angļu v.), 2 tīkla adapteri, jo pirmais tiks izmantots, lai no datora, uz kuras uzstādīts Virtualbox, varētu piekļūt tīklam un Internetam, tam sadaļā pievienots (Attached to – angļu v.) jāizvēlas NAT Network (skat. 2.1.3.1.1. attēlu), kas nodrošina, ka mašīna piekļūst tīklam un Internetam, tomēr tā neiegūst reālu MAC un IP adresi, savukārt otrs tīkla adapteri jāuzstāda kā *Internal Network* tipa adapteris, kā arī tā nosaukums ir "*intnet*" (skat. 2.1.3.1.2. attēlu). Ar šādu konfigurācijas izvēli tiek nodrošināts, ka šī virtuālā mašīna darbosies līdzīgi kā fizisks maršrutētājs.



2.1.3.1.1. att. **Pirmā tīkla adaptera uzstādījumi**



2.1.3.1.2. att. **Otrā tīkla adaptera uzstādījumi**

2.1.3.2. Samba, Zabbix, Backup, Windows 7 darbstacijas

Visiem citiem datoriem, kuri darbosies šinī informācijas sistēmā jāieslēdz tikai 1 tīkla adapteris, kurš jāuzstāda kā *Internal Network* tipa adapteris, kā arī tā nosaukums ir "*intnet*".

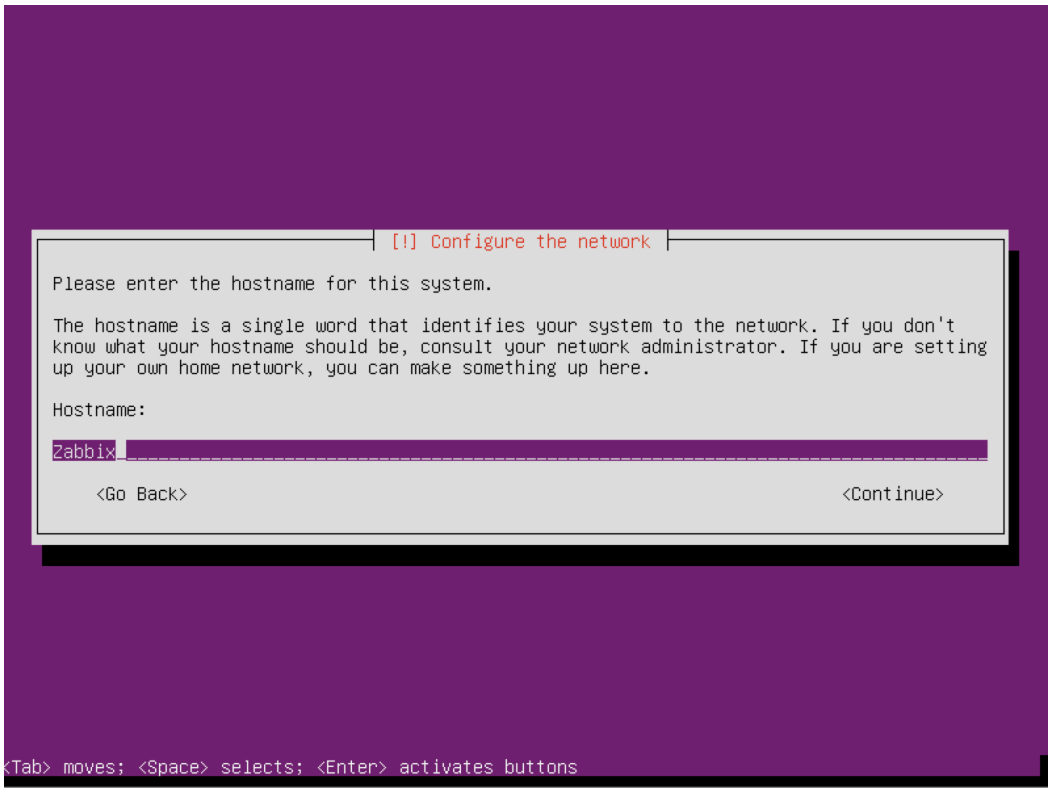
2.2. Operētājsistēmu instalēšana

2.2.1. Ubuntu uzstādīšana

Virtuālajās mašīnās "Zabbix", "Samba", "Backup" uzstādām Ubuntu 14.04. Uzstādīšanas process visās šinīs virtuālajās mašīnas ir identisks, tāpēc apskatīsim tikai vienas uzstādīšanu un konfigurēšanu. Instalēšanai izmantosim Ubuntu 14.04. failu ar .iso[26] paplašinājumu.

Startējam virtuālo mašīnu "Zabbix", kur līdzīgi kā ar "Firewall" izvēlamies lejupielādēto instalāciju. Kad tas izdarīts, izvēlās valodu, izvēlamies angļu valodu, lai personīgu iemeslu dēļ būtu vieglāk veikt uzstādīšanu.

Tālāk nākošajā izvēlnē izvēlamies opciju *instalēt Ubuntu serveris* (Install Ubuntu server – angļu v.). Pēc šī soļa tiks piedāvāts izvēlēties valodu, kādā vēlaties veikt instalēšanas procesu, arī šeit izvēlamies angļu valodu. Nākošajā izvēlnē jānorāda atrašanās vieta – valsts. Tas ir būtiski, lai atjauninājumi tiktu iegūti no tuvākā servera. Izvēlamies – *Latvia*. Tālāk tiks piedāvāts izvēlēties klaviatūras izkārtojumu atrast vai izvēlēties no saraksta. Mēs izvēlēsimies no saraksta *English (US),* jo tad varam būt droši, ka mūsu klaviatūra funkcionēs tieši kā mums nepieciešams. Pēc instalācijas pabeigšanas to ir iespējams nomainīt. Nākošajā solī prasīts, lai ievadām *hostname,* tas ir viens vārds, kurš identificēs šo serveris mūsu tīklā.

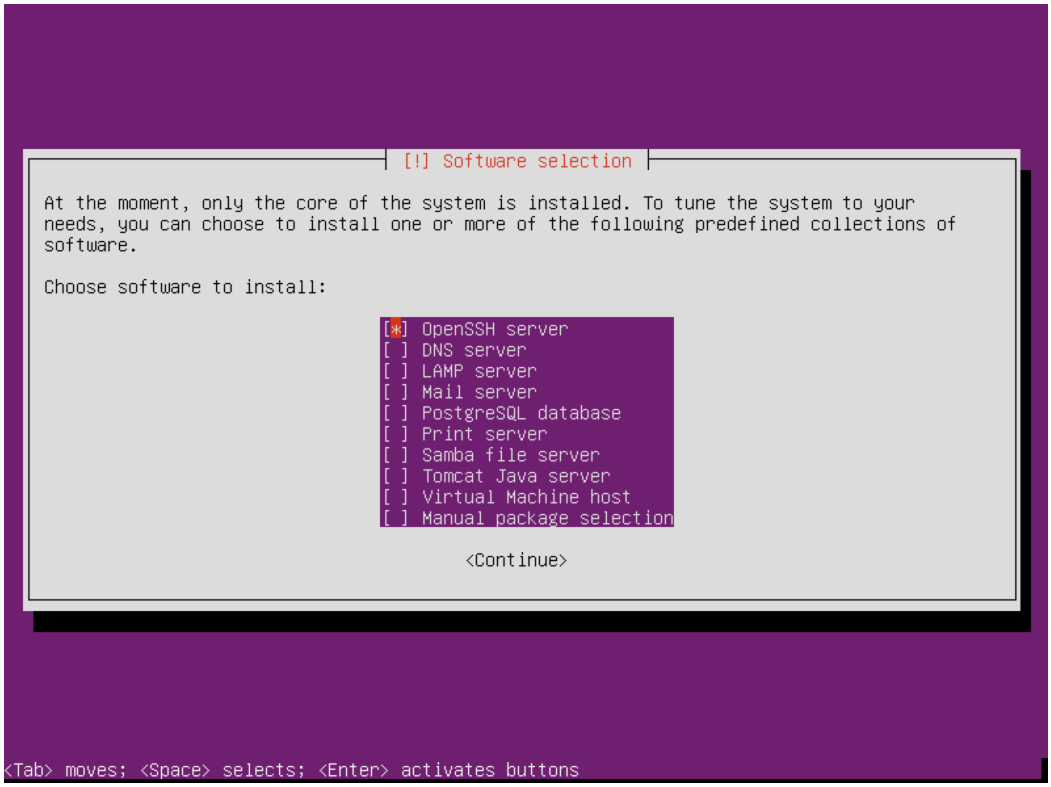


2.2.1.1. att. ***Hostname uzstādīšana***

Pēc *hostname* uzstādīšanas, jāievada lietotāja pilnais vārds (Full user name – angļu v.), kam savukārt sekos lietotājvārds kontam, kuru atstājam tādu pašu, kā pilno vārdu, tālāk mums jāievada parole, tomēr jāatceras, ka parolei jābūt drošai – tādai, ko nevarētu viegli uzminēt. Parole tiek izvēlēta vismaz 10 simbolu garumā, tajā iekļaujot lielos un mazos latīņu alfabēta burtus, kā arī skaitļus un simbolus.

Pēc šo darbību pabeigšanas, jāizvēlas šifrēt vai nešifrēt mājas direktoriju. Drošības palielināšanai, mēs izvēlamies šifrēt, jo cietā diska zādzības gadījumā, tie nebūs izlasāmi. Nākošā solī jāizvēlas laika zona (time zone – angļu v.), kas ir būtiski, lai sistēma strādātu bez pārpratumiem, jo tieši nepareizas laika zonas izvēle var traucēt atjauninājumu saņemšanai, savienojumu izveidošanai, u.c. Tā kā šīm instalācijām nav nepieciešams dalīt cieto disku

partīcijās, tad izvēlamies izmantot visu disku un uzstādīt šifrētu LVM (Use entire disk and set up encrypted LVM). Nākošā solī izvēlamies disku (mums pieejams tikai viens disks, jo tikai vienu esam pievienojuši virtuālajai mašīnai), kurā vēlamies instalēt Ubuntu un izveidot masīvus un piekrītam rakstīt izmaiņas diskā un izveidot loģiskos masīvus. Tālāk jāievada kriptēšanas frāze, kuru sistēma izmantos, lai varētu piekļūt failiem. Tā jāizveido pēc iespējas sarežģītāka – lielo, mazo burtu, skaitļu un simbolu virkne, garumā ieteicams garāka par 20 simboliem. Tālāk apstiprinām izmaiņas un sāksies instalēšanas process, kura laikā sistēma automātiski veiks ierakstus cietajā diskā un veidos operētājsistēmu. Instalēšanas procesā mums piedāvās uzstādīt *Proxy serveri* tomēr mums tas nav nepieciešams un tāpēc to atstājam tukšu. Izvēlamies, lai netiktu veikti automātiski atjauninājumi, jo tādejādi centīsimies paši kontrolēt, kurus atjauninājumus uzstādīsim, kurus nē, jo ne vienmēr svaigākie atjauninājumi ir labākā aizsardzība sistēmām. Šinīs atjauninājumos var atrasties nozīmīgas kļūdas, kuras var kaitēt sistēmas drošībai. Atjauninājumus uzstādīsim pašrocīgi. Nākošā solī mums piedāvās izvēlēties, kādas pakotnes vēlamies instalēt, izvēlamies *OpenSSH*, lai no jebkuras operētājsistēmas darbstacijas varētu pieslēgties serverim izmantojot SSH savienojumu.



2.2.1.2. att. **Pakotņu izvēle instalācijas procesā**

Pēdējā instalācijas solīt vaicās, vai vēlamies izveidot *Master Boot Record*, kur piekritīsim, jo šis izveidos diskā ierakstu, kā startēt šo operētājsistēmu.

Kad instalēšana pabeigta, startējam virtuālo mašīnu, ievadam konkrētās virtuālās mašīnas lietotāja vārdu un paroli. Tālāk ievadām komandu *sudo su,* ar šīs komandas palīdzību iegūstam *root* lietotāja tiesības Linux Ubuntu sistēmā, kuras nepieciešamas, lai varētu veikt tālākās darbības. Pēc šīs komandas ievadīšanas, būs jāievada lietotāja parole un uz sesijas laiku, lietotājs iegūst *root* lietotāja tiesības. Kad tas izdarīts ievadām komandas *apt-get update* un *apt-get upgreide*, katru atdalot ar *Enter* taustiņu:

Komanda *apt-get update* pārbauda, kādi atjauninājumi, kādās lietojumprogrammām, vai datubāzēm ir pieejami, savukārt komanda *apt-get upgrade* lejupielādē un uzstāda šos atjauninājumus, kuris tika atrasti ar *apt-get update* komandu.

Šī procedūra jāveic, lai uzstādītajai Ubuntu operētājsistēmai pārbaudītu, vai nav pieejami atjauninājumi, ar kuru palīdzību iespējams ir novērti kādi sistēmas ievainojamības *caurumi.* Šīs komanda jāievada manuāli, jo sistēmas instalēšanas procesā izvēlējāmies, ka nevēlamies automātiskos atjauninājumus.

2.2.2. **Windows 7**

No Microsoft operētājsistēmas Windows 7 versijām jāizvēlas Professional, Enterprise vai Ultimate[14], jo tikai šie varianti atbalsta darbstacijas pievienošanai domēnam, kas būs nepieciešams, lai pieslēgtu failu koplietošanas serverim "Samba". Uzstādīsim Windows 7 Ultimate.

Vispirms jāizvēlas instalēšanas procesa valoda, šeit var izvēlēties tikai angļu valodu, laika un naudas vienību formātā (time and currency format – angļu v.) izvēlamies Latviešu (Latvian – angļu v.), klaviatūras izkārtojumu vai ievades metodi (Keyboard or input method – angļu v.) izvēlamies US, lai nebūtu aizķeršanās ar simboliem.

Tālāk jāizlasa licences nosacījumi un piekrītot var turpināt instalēšanas procesu. Tālāk izvēlamies *Custom* sadaļu, jo šī būs pirmā instalācija, nevis, piemēram Windows XP jaunināšanu uz Windows 7. Tālāk jāizvēlas cietais disks, kurā tiks instalēta Windows 7 operētājsistēma, tā kā virtuālās mašīnas izveides procesā izveidojām tikai vienu cieto disku, tad šeit arī uzrādās tikai viens pieejams cietais disks, kuru arī izvēlamies. Tālāk sekos 2-3 minūšu garš instalācijas process. Kad tas būs pabeigts, būs jāievada datora nosaukums un lietotāja vārds.

Nākamajā solī ir jāuzstāda lietotāja parole, būtu jāatceras, ka jāizmanto droša parole – lielo, mazo latīņu alfabēta burtu, skaitļu un simbolu virkne, tās garumā vēlams vismaz 8

simboliem. Kad tas ir izdarīts, nākošā solī jāizvēlas, kādā veidā instalēt uzstādījumus. Izvēlamies ieteicamos uzstādījumus (Use recommended settings – angļu v.), tieši šāda ir izvēle, jo tā ir darbstacija nevis serveris, kura darbība spēj ietekmēt visa biroja darbību. Visus šos uzstādījumus vēlāk būs iespējams rediģēt. Pēc tam jāpārliecinās, ka ir pareiza laika zona, kā arī laiks un kalendārs atbilst patiesībai, kad tas būs izdarīts, tad nākošajā solī jāizvēlas tīkla tips, kur šoreiz izvēlēsimies *work network*, tomēr uzstādīšanas brīdī tas nav tik būtiski.

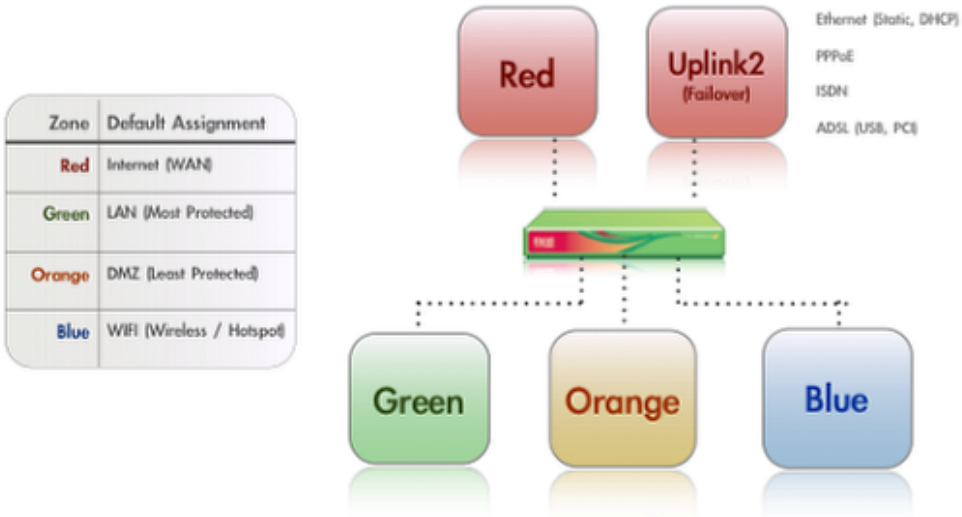
Windows darbstaciju paredzēts izmantot gan Samba servera, gan Zabbix, gan Endian konfigurēšanā, kā arī pārvaldībā. Lai to būtu ērtāk lietot, uzstādām lietojumprogrammu Putty, kuru lejupielādējam no Interneta[22].

2.2.3. **Endian (ugunsmūra) uzstādīšana**

Endian ugunsmūra uzstādīšanu un konfigurēšanu saskaņā ar ražotāja dokumentāciju[9]. Instalēšanu veiksim uz virtuālās mašīnas "Firewall", kurai neuzstādījām nekādu operētājsistēmu – ne Windows, ne Linux. Jāatceras, ka šinī virtuālajā mašīnā speciāli tika ieslēgti 2 tīkla kastes – *NAT network* ar tīkla nosaukumu *Internet* un *Internal Network* ar tīkla nosaukumu *intnet*.

2.2.3.1. Zonu iedalījums

Pirms Endian uzstādīšanas, izpētot ražotāja dokumentāciju, secināts, ka ļoti būtiski ir zināt noklusēto interfeisu sadalījumu (skat. 2.2.3.1.1. attēlu[11])



2.2.3.1.1. att.[11] **Endian zonu jeb interfeisu sadalījums**

- RED – teritoriālais datoru tīkls (WAN jeb Wide Area Network – angļu v.) – datortīkls, kurš nodrošina piekļuvi Interneta jeb šinī interfeisā tik pieslēgts interneta servisa piegādātāja nodrošinātais pieslēgums, tātad - Virtualbox pirmais tīkla adapteris NAT network "Internet";
- GREEN – lokālais tīkls (LAN jeb Local Area Network – angļu v.) – šinī interfeisā tiks pieslēgti visi serveri un datori, tātad – Virtualbox otrais tīkla adapteris *Internal Network* ar nosaukumu *intnet*;
- ORANGE – demilitarizētā zona (DMZ jeb demilitarized zone – angļu v.) – šinī darbā netiks izmantota, tomēr tā lieliski noderētu pielāgojot šo informācijas sistēmu kādam uzņēmumam, kurš vēlās izvietot savu mājas lapu vai demonstrācijas klientiem, no tās pēc noklusējuma nav atļauti savienojumi ar *GREEN* un *BLUE* zonu;
- BLUE – bezvadu tīkla iekārtu zona (Wireless/Hotspot – angļu v.) – arī šo zonu šinī darbā neizmantos un neapskatīs, tomēr pielāgojot kāda cita uzņēmuma vajadzībām, šinī zonā pieslēgtu bezvadu interneta raidītājus un/vai piekļuves punktus.

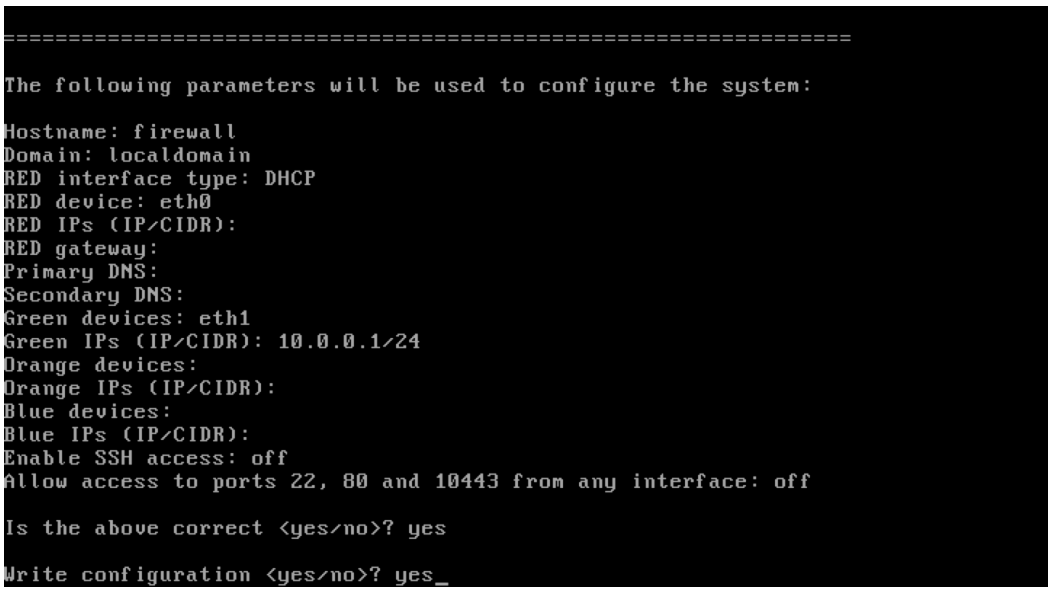
2.2.3.2. Endian instalēšana un konfigurēšana

Pēc iepazīšanās ar zonām, Endian mājaslapā lejupielādē failu ar .iso[8] paplašinājumu, kuru būs ļoti ērti uzstādīt uz virtuālās mašīnas. Izvēlamies 3.0.5 versiju. Pēc .iso instalācijas faila lejupielādes, startējam virtuālo mašīnu "Firewall" un izvēlamies vietu, kurā atrodas šī nupat lejupielādētā .iso instalācija, pēc šīs darbības veikšanas, startējam virtuālo mašīnu. Instalēšanas procesā jāizvēlas IP adrese *GREEN* interfeisam. *GREEN* interfeisu izmantos iekštīkla vajadzībām – serveriem un darbstacijām. IP adresi uzstādām 10.0.0.1 ar C klases apakštīkla makstu 255.255.255.0., tomēr šādas IP adreses izvēle nav obligāta, var izvēlēties arī piemēram 192.168.0.1.

2.2.3.2.1. att. **IP adreses un apakštīkla maskas izvēle GREEN interfeisam**

Kad instalēšanas process sekmīgi noslēdzies, startējam virtuālo mašīnu un pirmais, kas veicams ir *root* lietotāja paroles nomaiņa. Tas ir ļoti būtisks process no drošības aspekta, jo noklusētā Endian parole ir pieejama Internetā, kā arī atrodama dokumentācijā. Paroles nenomainīšana rada potenciālus draudus sistēmas drošībai, jo uzbrukuma gadījumā, ja lauzējs zina vai noskaidro, ka tiek izmantots Endian risinājums, tas var pārbaudīt noklusēto paroli, kura ir pieejama ikvienam. Sekmīgas autorizācijas gadījumā tas pārņem kontroli pār iekārtu, jo ar *root* tiesībām var konfigurēt pilnīgi visus uzstādījumus. Šī iemesla dēļ nomaināms noklusēto *root* lietotāja paroli "endian" uz "drošu" paroli ar pietiekami lielu simbolu skaitu. Tieši tāda pati darbība jāveic ar administratora paroli, kuru izmanto, lai pieslēgtos grafiskajai saskarnei.

Pēc sekmīgas paroles maiņas un drošības uzlabošanas, nākošais solis ir konfigurēšana, kuru veiksim ar komandrindas palīdzību (izvēlnē sadaļa *Shell*). Pirmā komanda, kuru ievadām komandrindā ir *netwizard*. Ar tās palīdzību, izmantojot vienkāršu veidni, tik izveidoti būtiskākie konfigurācijas uzstādījumi, pēc kuriem jau varēs pieslēgties no iekštīklā izvietotas darbstacijas un tālāko konfigurāciju veikt ar grafisko saskarni.



2.2.3.2.2. att. **Konfigurācijas izveide izmantojot komandrindas komandu netwizard**

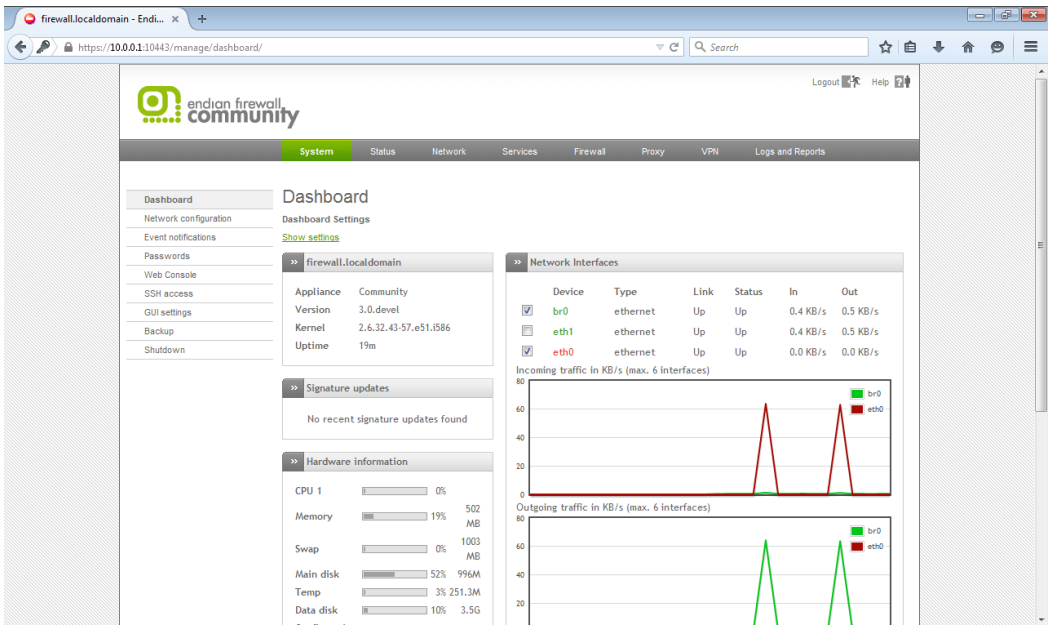
Komanda *netwizard* piedāvā konfigurēt sekojošus parametrus:

- Hostname – iekārtas nosaukums, to izvēlās brīvi, lai vēlāk varētu identificēt iekārtas, ja tādas ir vairākas tīklā;
- Domain – domēna nosaukums, sakarā ar to, ka vēl domēns nav izveidots, tad šeit atstāj noklusējamo vērtību – *localhost;*
- RED interfeisa tips (RED interface type – angļu v.) – veids, kā tiks noteikta vai izvēlēta *RED* interfeisa IP adrese – izmantojot DHCP serveri vai ievadot statisku adresi, šeit konfigurācijas sākumā izvēlamies DHCP, jo to nodrošina Virtualbox, tomēr vēlāk to būs iespējams arī mainīt uz statisku, ko arī darīsim, jo tāda ir tehniskās specifikācijas prasība;
- RED iekārta (RED device – angļu v.) – tīkla kartes, kurā tiks pieslēgts *RED* interfeiss, izvēle, tā kā konfigurējot virtuālās mašīnas tika ieslēgtas 2 tīkla kartes šai virtuālajai mašīnai un tieši pirmais tīkla adapteris ir atbildīgs par ienākošo tīklu jeb savienojumu Interneta provaideri, tad izvēlamies *eth0*, jo šeit tīkla portus numurē sākot ar 0 nevis 1, kā tas ir Virtualbox uzstādījumos;
- GREEN iekārta (GREEN device – angļu v.) – tīkla karte, kurā tiks pieslēgts GREEN interfeiss, izvēlamies Virtualbox otro adapteri, kuram ir uzstādīts tips *Internal Network* ar nosaukumu *intnet*, kura nosaukums Endian attēlojās kā *eth1*;

- GREEN IP adreses (GREEN IPs) – *GREEN* interfeisa adreses (šo ievadījām jau instalācijas procesā, tāpēc tas piedāvā jau iepriekš ievadīto) ar C klases apakštīklu;
- ORANGE iekārtas (ORANGE device – angļu v.) – konfigurācijas sākumā nav paredzēts izmantot *ORANGE* interfeisu, tāpēc to atstājam neaizpildītu;
- BLUE iekārta (BLUE device – angļu v.) – arī *BLUE* interfeisu nav paredzēts izmantot, tāpēc atstājam neaizpildītu;
- Atļaut SSH savienojumu (Enable SSH access) – tā kā turpmāko konfigurāciju paredzēts veikt izmantojot grafisko saskarni, tad neatļaujam veidot SSH savienojumus (vajadzības gadījumā to vēlāk varēs atļaut), līdz ar ko, arī iegūstam drošības papildinājumu, jo, ja kāds mēģinās pieslēgties pie 22 porta, tad savienojums tiks noraidīts, jo esam izvēlējušies neatļaut šādus savienojumus;
- Atļaut piekļuvi 22, 80 un 10443 portam no jebkura interfeisa (Allow access to port 22, 80 and 10443 from any interface – angļu v.) – drošības nolūkos neatļaujam veidot savienojumus uz minētajiem portiem no jebkura interfeisa, noklusēti ir definētas zonas, no kurām varēs veikt konkrētus savienojumus ar portiem.

Kad izvēlēti visi augstākminētie konfigurācijas uzstādījumi, jāpiekrīt, ka tie ir ievadīti korekti, kā arī šo uzstādījumu saglabāšanai. Kad tas izdarīts veicam iekārtas restartēšanu (reboot – angļu v.)

Tālāko konfigurēšanu veic izmantojot grafisko saskarni, tāpēc nepieciešams startēt sagatavoto Windows 7 darbstaciju, kurai manuāli uzstāda IP adresi, kura ietilpst nupat izveidotajā tīklā, piemēram 10.0.0.2, apakštīkla maska 255.255.255.0, vārteja 10.0.0.1, primārā DNS adrese 10.0.0.1, sekundārā Google DNS servera adrese – 8.8.8.8. Manuāli jāuzstāda tīkla adreses darbstacijā, jo pēc noklusējuma DHCP serviss ir izslēgts. Pēc adrešu ievadīšanas pārlūkprogramma atver grafisko saskarni, kurai var piekļūt ievadot "Firewall" IP adresi un pievienojot portu – 10443. Šeit jāievada autorizācijas dati – lietotājvārds "admin" un administratora parole. Pēc sekmīgas autorizācijas, atvērsies Endian grafiskā saskarne (skat. 2.2.3.2.3. attēlu), kuru turpmāk izmantosim tālākā konfigurēšanas gaitā.



2.2.3.2.3.. att. **Endian grafiskā saskarne**

2.3. Sistēmu uzstādīšana un konfigurēšana

2.3.1. Endian

Visas turpmākā Endian konfigurēšana notiks izmantojot grafisko saskarni, izmantojot Interneta pārlūkprogrammu.

Pirmais veicamais darbs ir statiskas IP adreses norādīšana *RED* interfeisam, ja tas nav izdarīts konfigurēšanas procesā izmantojot komandrindu. Jāuzstāda statiska IP adrese, kā arī jāvienojas arī ar Interneta servisa piegādātāju, ka tas nodrošinās statisku IP adresi, lai varētu veikt pieslēgumu izmantojot VPN. Uzstādot uz reālas sistēmas tai būtu jāuzstāda Interneta servisa piegādātāja norādītie parametri – IP, apakštīkla, DNS un vārtejas adreses, bet tā kā darbs tiek realizēts ar Oracle Virtualbox palīdzību, tad, izmantojot dokumentāciju[29], uzstādām Endian *eth0* tīkla kartes statisko IP, apakštīkla, DNS (primāro un sekundāro) un vārtejas adreses (skat. 2.3.1.1. tabulu).

2.3.1.1 tabula

Endian eth0 tīkla adaptera adrešu uzstādījumi

Skaidrojums	Adrese
IP	10.0.2.6
Apakštīkla maska	255.255.255.0
Vārteja	10.0.2.2
Primārais DNS	10.0.2.3
Sekundārais DNS	8.8.8.8

Kā sekundāro DNS adresi ievadījām, līdz ar ko uzstādījām Google publisko DNS serveri[12]. Ja primārais DNS neatbildēs, tad atbildi dos sekundārais, tomēr, ja tiks pieprasīta iekšējā adrese, piemēram 10.0.0.3 (Zabbix), tad sekundārais nespēs atgriezt īsto atbildi uz mūsu izsaukumu. Tomēr sekundārais DNS spēs sekmīgi atbildēt par Interneta domēnu izsaukumiem, jo Google DNS serveris ir viens no lielākajiem pasaulē.

2.3.1.1. DHCP

Tā kā tīkla projektējumā ir paredzēts, ka iekārtām – darbstacijām un serveriem – IP adreses iedalīs DHCP serveris, tad aktivizējam to, jo pēc noklusējuma tas ir izslēgts. Pēc tā ieslēgšanas, Windows darbstacijai, kuru izmantojām Endian konfigurēšanai, jānoņem manuāli ievadītās IP, apakštīkla, vārtejas un DNS serveru adreses, tāpēc, ka tagad jebkura iekārta – dators vai serveris – pieslēdzoties saņems IP adresi, kuru iedalīs DHCP, ja tajā nebūs speciāli rezervētas adreses konkrētām iekārtām. Tā kā projektējumā ir paredzēts un realitātē ir būtiski, ka serveriem ir statiskās nevis dinamiskās IP adreses, lai vienmēr pieslēgtos pie pareizā servera, tad tiem rezervē IP adreses. Rezervēšanu veic balstoties uz šo serveru tīkla adapteru MAC adresēm.

2.3.1.1.1. tabula

IP adrešu rezervēšanas tabula serveriem

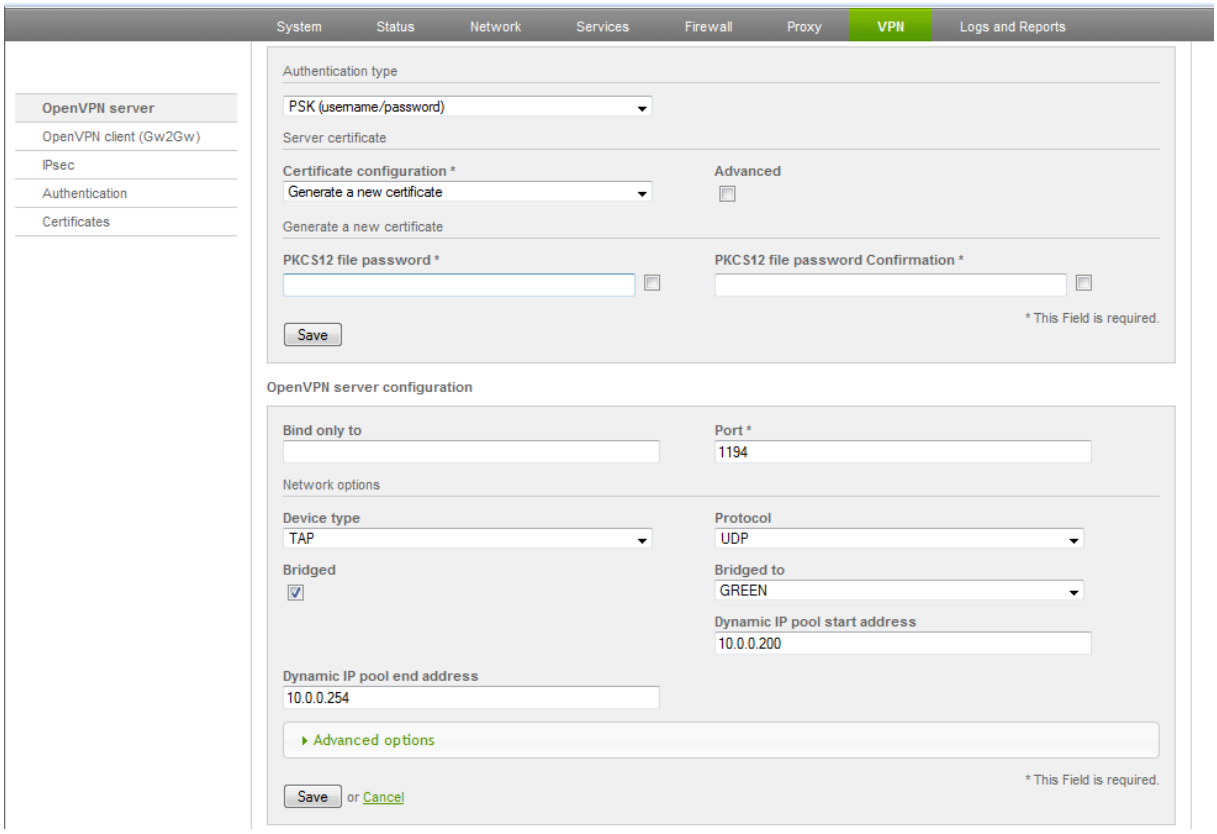
Servera nosaukums	IP adrese	MAC adrese
Samba	10.0.0.2.	08002751FE60
Zabbix	10.0.0.3	080027F731E5
Backup	10.0.04	0800278737EC

Lai nenotiktu konflikts starp DHCP un VPN serveriem, DHCP serverī ievieš IP adrešu izdalīšanas ierobežojumus. DHCP konfigurācija paredz, ka IP adreses tas drīkst dalīt apgabalā no 10.0.0.2 līdz 10.0.0.199, tomēr pirms DHCP tīkla iekārtai uz tās pieprasījumu atbild ar iedalīto IP adresi, tā pārliecinās, ka vaicājošās tīkla iekārtas MAC adrese nav atrodama rezervēto IP adrešu tabulā, ja tā notiek, tad tiek piešķirta rezervētā IP adrese, pretējā gadījumā tas pēc nenoteiktas izvēles var izdalīt IP adreses. Tieši pateicoties IP adrešu rezervēšanai balstoties uz tīkla iekārtas MAC adresi, katrā serverī nebūs manuāli jāuzstāda statiskā servera IP adrese.

2.3.1.2. VPN

Virtuālais privātais tīkls (Virtual Private Network – angļu v.) ir publiska datoru tīkla mezglu kopa, kas, izmantojot dažādas sistēmas, izveidota tā, lai kā datu pārsūtīšanas vidi izmantotu internetu[3]. Arī šinī informācijas sistēmā tiek ieviests VPN serveris, lai tās resursiem varētu piekļūt atrodoties ārpus biroja telpām izmantojot Interneta starpniecību.

Endian atvērtā pirmkoda risinājumā pēc noklusējuma ir uzstādīts OpenVPN serveris, līdz ar ko nekādas papildus instalācijas nav jāveic, tikai jāveic precīza konfigurācija. Visa VPN servera konfigurēšana tiek veikta izmantojot Endian grafisko saskarni, kura pieejama adresē https://10.0.0.1:10443 sadaļā VPN. Lai sāktu konfigurēšanu, vispirms startē OpenVPN serveri (Enable OpenVPN server – angļu v.) un tālāko konfigurēšanu veic vadoties pēc Endian mājaslapā sagatavotā konfigurēšanas apraksta[10].



2.3.1.2.1.att. **Endian VPN servera konfigurācija**

- Autorizācijas tips – (Authentification type – angļu v.) visdrošākais noteikti ir divu līmeņu autorizācija, izmantojot sertifikātu un lietotājvārdu kopā ar paroli, tomēr šī nav parocīgākā konfigurācija parastam lietotājam, tomēr rūpīgi attiecoties ar lietotājvārdu un paroli, to neglabājot visiem pieejamā vietā, arī šis ir pietiekoši drošs risinājums, tāpēc izvēlas autorizāciju tikai ar lietotāja vārdu un paroli.
- Sertifikāta konfigurācija – (Certificate configuration – angļu v.), lai gan pēc noklusējuma sistēma ir uzģenerējusi sertifikātu un piedāvā lietotājam vienkārši to lejupielādēt, tomēr šinī gadījumā izvēle tiek izdarīta par labu jauna sertifikāta ģenerēšanai, arī potenciālai drošības risku samazināšanai. Drošības nolūkos šo sertifikātu ik pēc kāda laika, piemēram 90 dienām var pārģenerēt un izsniegt atkārtoti lietotājiem, lai gadījumā, ja kāda trešā persona ir piekļuvusi vecajam sertifikātam, pēc jaunā uzģenerēšanas vairs nevarētu piekļūt VPN tunelim, līdz ar ko pieslēgties informācijas sistēmai.
- PKC S12 faila parole – (PKC S12 file password – angļu v.) ir parole, kas aizsargā PKC S12 failu.
- Atbildēt uz – (Bind to – angļu v.) atstāj tukšu, jo VPN tunelim drīkstēs pieslēgties no jebkuras IP adreses.

- Ports – (Port – angļu v.) atstāj noklusēto – 1194.
- Iekārtas tips – (Device Type – angļu v.) izvēlās TAN tipu, jo tas ļauj veidot savienojumus no VPN uz kādu no zonām.
- Protokols – (Protocol – angļu v.), atstāj noklusēto un informācijas sistēmas VPN tuneļa mērķiem piemēroto UDP protokolu, nevis izvēlas TCP protkolu.

Savienojums uz – (Bridged to – angļu v.), tā kā iekārtas tipu izvēlējāmies TAN, un tieši tas ir nepieciešams, tad norāda, ka izveidojot VPN savienojumu, lietotājs tiek *iekļauts* zaļajā zonā, līdz ar ko uz to attiecās zaļās zonas likumi.

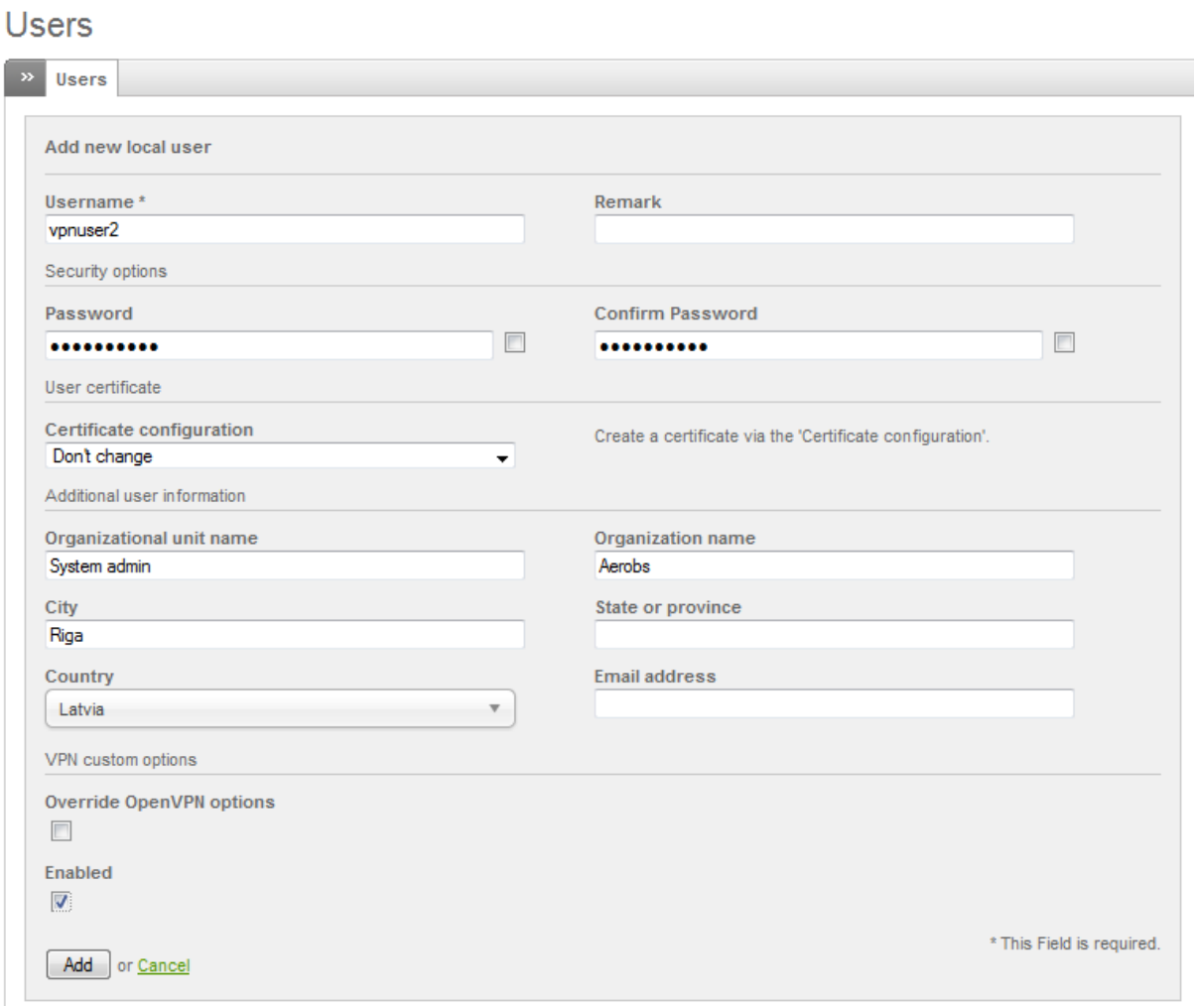
- Dinamisko IP adrešu sākuma un beigu uzstādīšana – (Dynamic IP pool start address – angļu v.; Dynamic IP pool end address – angļu v.) šo IP adrešu apgabalu uzstāda tādu, lai tas nekonfliktētu ar DHCP serveri jeb netiktu izdalīta viena IP adrese divām iekārtām, tāpēc šeit uzstāda divus neatkarīgus apgabalus. Sākuma adrese 10.0.0.200, bet beigu – 10.0.0.254, kas nozīmē, ka var nodefinēt 54 VPN tuneļus, tomēr šī projekta ietvaros tāda nepieciešamība nebūs.

Kad šī konfigurācija pabeigta un izmaiņas saglabātas, veic CA sertifikāta lejupielādēšanu un ar zibatmiņas vai cita veida datu nesēju palīdzību šo sertifikāta failu ar .pem paplašinājumu pārvieno uz datoru, no kura tik veikta VPN savienojuma izveide.

2.3.1.3. VPN lietotāju izveide

Kad visi iestatījumi ievadīti, izmaiņas saglabā un tālāk ir jāizveido lietotājs, kuram būs tiesības pieslēgties VPN tunelim. Tomēr šādas tiesības netiks piešķirtas katram lietotājam. Tās piešķirs tikai sistēmas administratoram un uzņēmuma īpašniekam, tomēr vēlāk pēc uzņēmuma vadītāja mutiska vai rakstiska rīkojuma VPN tuneļus var izveidot arī citiem darbiniekiem. VPN tuneļi netiek veidoti visiem darbiniekiem drošības nolūkos, jo tie var attālināti piekļūt uzņēmuma sensitīvai informācijai un rīkoties ne uzņēmuma interesēs, tāpēc attālināto piekļuvi informācijas sistēmai nodrošinās sistēmas administratoram, kurš neatrodoties birojā varēs veikt informācijas sistēmas labošanas darbus, jauninājumu ieviešanu, un tā tālāk, kā arī uzņēmuma vadītājam, kuram vajadzības gadījumā būs piekļuve uzņēmuma informācijas sistēmai.

Lietotāja izvēle notiek VPN sadaļas apakšsadaļā *Authentification*. Šeit izveido tikai VPN serverī definētu lietotāju, kurš varēs pieslēgties informācijas sistēmai izmantojot VPN savienojumu.



2.3.1.3.1.att. **VPN lietotāja izveide**

- Lietotājvārds – (Username – angļu v.), vārds, kurš identificēs lietotāju un tik izmantot autorizācijas procesā.
- Parole – (Password – angļu v.), šeit sistēmas drošības risku samazināšanā ieteicams izvēlēties sarežģītu jeb *drošu* paroli.
- Sertifikāta uzstādījumi – (Certificate configuration – angļu v.), sakarā ar to, ka nav paredzēts izmantot sertifikātus lietotāju autorizācijas procesā, tad šeit atstāj uzstādījumu nemainīt (Don't change – angļu v.).
- Papildinformāciju – (Additional informatio – angļu v.) pēc sistēmas administratora ieskatiem ievada papildinformāciju par lietotāju (nav obligāti), tomēr lai sistēmas administratoram būtu vieglāk identificēt lietotājus, papildus informācija tika ievadīta.

- Ieslēgt – (Enable – angļu v.) pēc noklusējuma šī opcija nav aktivizēta, tomēr tā kā uzreiz pēc lietotāja izveides tam jābūt strādājošam, tad ieslēdzam šo lietotāju jeb aktivizējam tā piekļuvi VPN tunelim.

Ja kādam lietotājam ir izveidota piekļuve, tomēr laika gaitā sistēmas administrators saprot, ka lietotājs to neizmanto, drošības risku samazināšanas nolūkos ieteicams šo pieeju izslēgt vai izdzēst.

2.3.2. **Samba**

Failu koplietošanas servera Samba uzstādīšanu un konfigurēšanu veic vadoties pēc Jay Ts, Robert Eckstein un David Collier-Brown grāmatas "Using Samba"[16] un organizācijas "Samba" izveidotās Wiki[25] mājas lapas.

Samba servera uzstādīšanu veic virtuālajā mašīnā "Samba", izmantojot komandrindu Sambas serverī vai pieslēdzoties ar SSH savienojumu pie servera (piemērma, izmantojot Putty Windows operētājsistēmā). Būtiski ir atcerēties, ka lai instalētu kādu pakotni Ubuntu serverī, jābūt *root* tiesībām. Samba servera pakotņu instalēšanu veic ar komandu *apt-get install samba*, pēc kuras serverī automātiski tiks instalētas visas nepieciešamās pakotnes Samba serverim. Instalēšanas procesā tiek izveidos Samba servera konfigurācijas fails ar faila paplašinājumu *.conf*, kura atrašanās vieta serverī ir */etc/Samba/smb.conf*, tā kā tas ir ģenerēts automātiski, izdzēšam šo failu, jo veidosim savu konfigurācijas failu, nevis labosim automātiski izveidoto. Tomēr pirms šī faila izdzēšanas, noteikti ir jāaptur Samba servisa darbība Ubuntu serverī, to panāk ar komandu *service samba stop*. Kad sekmīgi apturēts serviss un izdzēst noklusētais konfigurācijas fails, var sākt Samba servera konfigurēšanu. Tās veikšanai izmantosim *Sabma-tool*[24] ar tā palīdzību būs jāievada informācija konkrētajās vietās un konfigurācijas fails tik uzģenerēts automātiski. Papildus informāciju par komandas iespējām var uzzināt ievadot komandu *samba-tool domain proviosion --help*.

Pēc iepazīšanās ar *Samba-tool* iespējām gan organizācijas Samba Wiki lapā, gan Ubuntu servera instrukcijām veicam samba servera konfigurēšanu ievadot komandu *samba-tool domain proviosion --use-rfc2307 –interactive.* Šī komanda ir papildināta ar papildus atribūtu *--use-rfc2307*, kas iespējos iespēju veikt domēna konfigurēšanu izmantojot Microsoft Windows Active Directory administrēšanas rīkus[23]. Savukārt papildinājums *–interactive* palīdzēs vizuāli vieglāk un saprotamāk veidot Samba konfigurāciju[24].

```
root@Samba:/home/samba# samba-tool domain provision --use-rfc2307 --interactive
Realm: aerobs.local
 Domain [aerobs]:
 Server Role (dc, member, standalone) [dc]:
 DNS backend (SAMBA_INTERNAL, BIND9_FLATFILE, BIND9_DLZ, NONE) [SAMBA_INTERNAL]:
 DNS forwarder IP address (write 'none' to disable forwarding) [10.0.0.1]:
Administrator password:
Retype password:
Looking up IPv4 addresses
Looking up IPv6 addresses
No IPv6 address will be assigned
Setting up share.ldb
Setting up secrets.ldb
Setting up the registry
Setting up the privileges database
Setting up idmap db
Setting up SAM db
Setting up sam.ldb partitions and settings
Setting up sam.ldb rootDSE
Pre-loading the Samba 4 and AD schema
Adding DomainDN: DC=aerobs,DC=local
Adding configuration container
Setting up sam.ldb schema
Setting up sam.ldb configuration data
Setting up display specifiers
Modifying display specifiers
Adding users container
Modifying users container
Adding computers container
Modifying computers container
Setting up sam.ldb data
Setting up well known security principals
Setting up sam.ldb users and groups
Setting up self join
Adding DNS accounts
Creating CN=MicrosoftDNS,CN=System,DC=aerobs,DC=local
Creating DomainDnsZones and ForestDnsZones partitions
Populating DomainDnsZones and ForestDnsZones partitions
Setting up sam.ldb rootDSE marking as synchronized
Fixing provision GUIDs
A Kerberos configuration suitable for Samba 4 has been generated at /var/lib/samba/private/krb5.conf
Setting up fake yp server settings
Once the above files are installed, your Samba4 server will be ready to use
Server Role:           active directory domain controller
Hostname:              Samba
NetBIOS Domain:        AEROBS
DNS Domain:            aerobs.local
DOMAIN SID:            S-1-5-21-3225674345-3755085567-4038626843
```

2.3.2.1. att. **Samba servera konfigurēšana izmantojot Samba-tool ar papildus parametriem**

Tā kā esam izvēlējušies komandu *samba-tool domain provision* papildināt ar *interactive*, tad veicot konfigurēšanu, uzreiz aiz lauka nosaukuma kvadrātiekavās tiks piedāvāta vērtība šim laukam[24], ja to nevēlās mainīt, tad attiecīgajā logā jānospiež taustiņš *Enter*.

Konfigurācijā ievadītie parametri:

- Realm – tas ir Kerberos lauks[24], to izmantos kā *Active Directory DNS* vārdu, ievadītā vērtība "aerobs.local";
- Domain – domēna nosaukums garumā līdz 15 simboliem neizmantojot pieturzīmes[24], vērtība – konfigurācijas piedāvātā;
- Server role – servera loma[24], tā kā šis ir pirmais domēna kontrolieris, ko uzstādām šim domēnam, tad tā loma būs *dc* jeb domēna kontrolieris (domain cotroler – angļu v.), vērtība – konfigurācijas piedāvātā;
- DNS backend – sistēma, kura nodrošinās DNS servisu[24], tā kā šī sistēma paredzēta mazam uzņēmuma, tad nav nepieciešams pēc atsevišķa DNS servisa nodrošināšanas sistēmas, pilnīgi pietiekami ir ar *SAMBA_INTERNAL*, ko arī izvēlamies;
- DNS forwarder – tā kā darbstacijās kā primārais DNS serveris tiek norādīta Samba servera IP adrese, bet lietotāji vēlās pieslēgties arī Internetam ne tikai iekšējiem

resursiem, tad kā DNS pieprasīju pārsūtīšanu[24] uzstādām uz adresi 10.0.0.1, kas ir Endian Firewall IP adrese, kura vienlaicīgi strādā arī kā DNS serveris pieprasījumiem uz Interneta adresēm;

- Administrator password – administratora parole tiks izmantota, lai pievienotu vismaz pirmo darbstaciju domēnam, vēlāk būs iespējams deleģēt citu lietotāju vai lietotājus, kuriem būs šādas tiesības. Būtiski atcerēties, ka parole jāizvēlas droša – vismaz 8 simboli, lielie un mazie burti, cipari un simboli[24].

Kad izmantojot šo konfigurēšanas metodi ir aizpildīti visi lauki, sekmīgas konfigurēšanas rezultātā tas attēlo konfigurācijas parametrus uz ekrāna (skat. 2.3.2.1. attēlu). Kad tas sekmīgi izdarīts, tiek automātiski ģenerēts konfigurācijas fails, kurš atrodas */etc/Samba/snb.conf*.

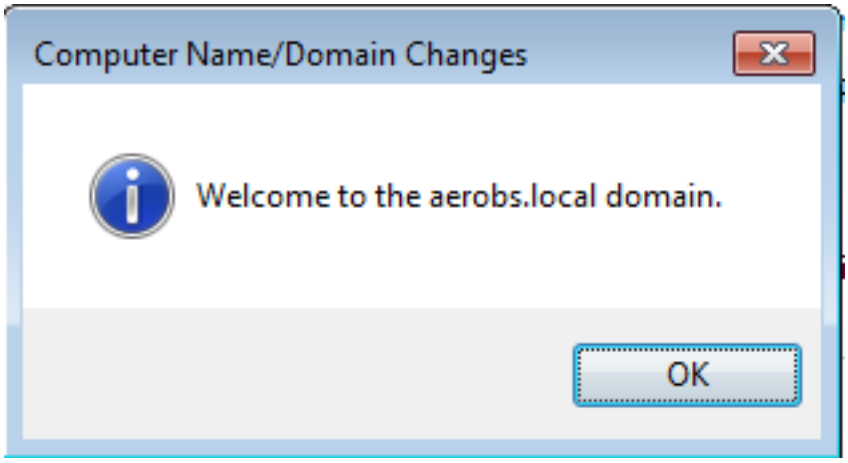
2.3.2.1. Endian DHCP veicamās izmaiņas pirms datoru pievienošanas domēnā

Darbstacijas nevarēs pievienot domēnam ar šī brīža DHCP servera uzstādījumiem, jo meklējot Samba serveri darbstacija nesaņem atbildi, jo DNS serverī 10.0.0.1 nav atbilstošu ierakstu. Tāpēc Endian Firewall grafiskajā saskarnē veicam izmaiņas DHCP servera uzstādījumos – primārā DNS servera adrese 10.0.0.2, bet sekundārā 8.8.8.8. Tas nozīmē, ka veicot datora un/vai lietotāja pievienošanu domēnam, pieprasījums, ja Samba serveris būs aktīvs, tik veikts uz 10.0.0.2, kas ir Samba servera IP adrese, līdz ar ko notiks sekmīga datora vai lietotāja pievienošana. Šo vērtību nemainīsim pēc datoru un lietotāju pievienošanas domēnā, jo veicot pieprasījumu piemēram kādai Interneta domēnam, tad pirmais pieprasījums, ja Samba serveris būs aktīvs, tiks veikts uz 10.0.0.2, ja šis DNS serveris nezinās atbildi, tas to automātiski pārsūtīs 10.0.0.1 kā tas tika paredzēts konfigurējot Samba serveri, tālāk, ja Endian DNS serveris nezinās atbildi, tas veiks pieprasījumu nākošajam DNS serverim, kas konfigurācijā ir paredzēts Interneta servisa piegādātāja DNS serveris.

2.3.2.2. Darbstacijas pievienošana domēnam

Kad ir sekmīgi pabeigta Samba servera konfigurēšana, tad var pievienot darbstaciju domēnam, tomēr, lai datoru varētu pievienot domēnam tam vispirms jānomaina DNS servera adrese, pretējā gadījumā sistēma ziņos, ka tā nevar pievienoties konkrētajam domēnam. Tā kā DHCP serverī vēl nav norādīts, ka primārā DNS servera adresei jābūt Samba servera IP adresei,

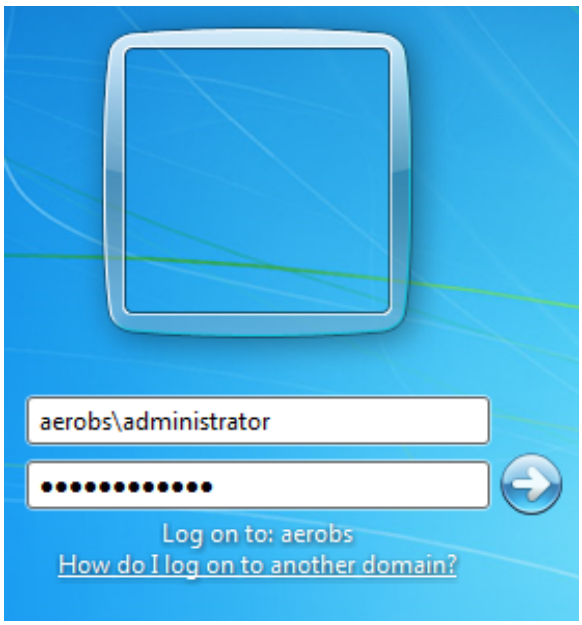
tad pirmajai darbstacijai, kuru pievienosim domēnam, pašrocīgi norādām, ka primārā DNS servera adrese ir 10.0.0.2, bet sekundāro izvēlamies Endian Firewall adresi 10.0.0.1. Kad tas izdarīt var sākta datora pievienošanu domēnam. Atverot Windows operētājsistēmā sadaļu dators (computer – angļu v.), tad sistēmas rekvizīti (system properties – angļu v.) sadaļā datora vārds, domēns un darba grupas uzstādījumi (Computer name, domain, and workgroup settings – angļu v.) izvēlamies mainīt uzstādījumus, tālāk sadaļā domēns (domain – angļu v.) ievadam domēna nosaukumu "aerobs.local" un tālāk sekos lietotājvārda un paroles pieprasījuma logs, kurā ievadam lietotājvārdu "administrator" un paroli to, kuru ievadījām domēna konfigurēšanas procesā. Sekmīgas autorizācijas gadījumā dators tiks pievienots domēnam un par to tiks parādīts attiecīgs paziņojums (skat. 2.3.2.1.1. attēlu).



2.3.2.2.1. att. **Apstiprinājuma paziņojums, ka darbstacija ir pievienota domēnam**

Pēc šī loga aizvēršanas, sistēma aicinās lietotāju restartēt datoru, lai tas iegūtu domēna grupas politiku (group policies – angļu v.) jeb noteikumus, kā sistēmai strādāt, ko tai ir atļaut atvērt, kas aizliegts, un citus uzstādījumus, kurus būs konfigurējis domēna administrators. Lai arī līdz šim nav veikti nekādi domēna konfigurēšanas darbi, tomēr sistēmas restartu ir jāveic.

Pieslēgšanās datoram izmantojot domēna lietotāju nevis lokālo notiek vispirms ievadot domēna vārdu, tad atpakaļ vērstu slīpsvītru, aiz kuras seko domēna lietotāja vārds. Piemēram, aerobs\administrator (skat. 2.3.2.1.2. attēlu).



2.3.2.2.2. att. **Pieslēgšanās datoram izmantojot domēna lietotāja profilu**

2.3.2.3. Rīki Samba servera administrēšanai

Samba servera administrēšanai izmantosim rīkus, kuri pieejami Windows darbstacijās, arī Windows 7, kas ir šīs informācijas sistēmas pamatprasībās iekļautā lietotāju darbstaciju operētājsistēma. Iespēja konfigurēt Samba serveri no Windows darbstacijas tika aktivizēta, kad konfigurēja Samba serveri un tika pievietots komandai *--use-rfc2307*. Šī komanda atļauj izmantot Windows rīku Active Directory Users and Computers, kuru uzstāda Sambas servera administratora Windows 7 darbstacijai. Pēc noklusējuma šis rīks nav iekļauts Windows 7 instalācijā, tādēļ to lejupielādē no Microsoft mājas lapas[6] un uzstāda atbilstoši Microsoft sniegtajām instrukcijām[6].

2.3.2.4. Domēna lietotāju un grupu izveidošana

Domēna lietotājus un grupas izveide un administrēšana notiks izmantojot rīku Active Directory Users and Computers sistēmas administratora Windows 7 darbstacijā. Šis nav vienīgais veids, kā to var darīt. Lai administrētu lietotājus un grupas var izmantot Linux serverī komandrindu, Webmin un citus rīkus.

Lietotājus un grupas, kā arī lietotāju sadalīšanu grupās notiks vadoties pēc informācijas sistēmas izveides prasībām. Pēc prasībām izriet, ka ir jāizveido 3 grupas – administratori,

uzņēmuma vadība. Šobrīd šajās grupās nebūs liels lietotāju skaits, tomēr augot uzņēmumam šo grupu un lietotāju skaits var pieaugt un tā nebūs problēma Samba serverim.

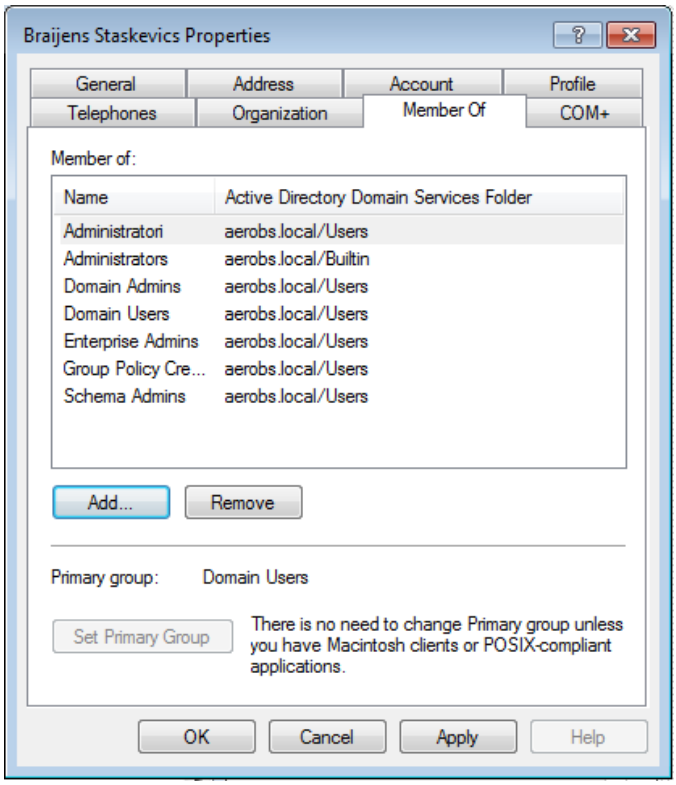
Atverot Active Directory Users and Computers rīku, redzams, ka noklusēti jau ir izveidotas grupas, kā arī lietotāji, tos atstājam nemainīgus, pievienosim jaunas grupas. Šinī rīkā atveram *Action-New-Group* logu, kurā ievadam grupas nosaukumu un apstiprinām to. Pēc šīs darbības tiks izveidota jauna grupa, tieši pēc šāda principa izveidojam arī atlikušās divas grupas. Lietotāju izvēle notiek diez gan līdzīgi, atverot *Action-New-User.* Tālāk jāievada lietotāja vārds, uzvārds un lietotāja vārds, kuru veidosim pēc politikas – vārda pirmais burts un pilns uzvārds, protams var gadīties, ka uzņēmuma strādā divi Andri Bērziņi, tomēr šādās situācijās sistēmas administrators, kurš veic darbinieku domēna lietotāju izveidi var ieviest atkāpes no šīs politikas. Nākošajā solī prasīts ievadīt paroli un pēc noklusējuma ir izvēlēts, ka nākošajā pieslēgšanās reizē lietotājam jānomaina parole (User must change password at next logon – angļu v.), šī ir ļoti ērta iespēja sistēmas administratoriem, kuri var uzģenerēt paroli, to iedot lietotājam, kuram pie pirmās pieslēgšanās. Paroles sarežģītību nosaka noklusētās domēna grupas politika (Group Policy – angļu v.), tādēļ sistēma neļaus ievadīt vienkāršas paroles, kuras sastāv tikai no cipariem vai burtiem. Šinī solī iespējams iespējot vēl papildus parametrus, kurus konkrētajā konfigurācijā gan neiespējosim:

- lietotājs nevar nomainīt paroli – (User cannot change password – angļu v.), kādā uzņēmumā iespējams šāda konfigurācija ir paredzēta drošības politikā, tomēr šī ir subjektīva sistēmas administratora izvēle,
- paroles lietošanas laiks nekad nebeidzās - (Password never expires – angļu v.), arī šī ir subjektīva sistēmas administratora izvēle, tomēr no drošības viedokļa drošāk būtu, ja paroles lietošanas laiks ir ierobežots un ik pēc konkrēta laika tā ir jānomaina, tas samazina drošības riskus,
- konts ir izslēgts – (Account is dissable – angļu v.), pēc noklusējuma šī iespēja ir atspējota, tomēr tā arī to atstāsim, jo nav nepieciešamības pēc konta izslēgšanas, arī šo iespēju var izmantot dažādu drošības risinājumu realizēšanai.

Pēc sekmīgas parametru apstiprināšanas lietotāja konts ir izveidots un tagad to var pieslēgt darbstacijai, pievienot kādai grupai, kā arī veikt daudz citu papildus parametru rediģēšanu izvēlētajam lietotājam vai grupai uzklikšķinot ar labo peles pogu un izvēloties *Labot* (Edit – angļu v.).

Lietotājs Braijens Staškevičs ir šīs jaunizveidotās sistēmas administrators (pēc tehniskajām prasībām), tad šim lietotājam piešķir tieši tādas pašas tiesības kā noklusētajam

lietotājam *Administrator (skat. 2.3.2.4.1. attēlu)*, kuru pēc lietotāja bstaskevics tiesību piešķiršanas, izslēdz (disable – angļu v.). Šādu darbību veic, lai samazinātu iespējamību trešajai personai iekļūt sistēmā – atslēdzot noklusētos lietotājus.

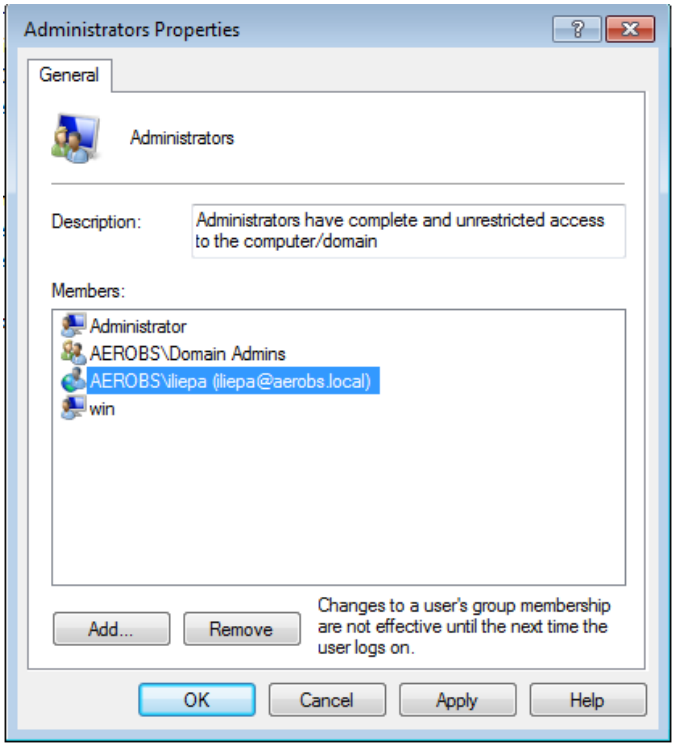


2.3.2.4.1. att. **Lietotāja Braijens Staškevičs pievienoto grupu saraksts**

2.3.2.5. Datora administratora tiesību piešķiršana domēna lietotājam

Tā kā lietotājs administrator ir arī grupā domēna administratori (Domain Admins – angļu v.), tad tam būs administratora tiesības šinī datorā, tomēr pārējiem darbiniekiem - Juris Ozolam, Ievai Liepai un Agrim Kalniņam tikai standarta lietotāja tiesības. Tā kā uzņēmums neparedz ierobežot darbinieku datoru izmantošanu, tas būtu – dažādu bezmaksas programmatūru instalēšanu, piemēram, Skype, tad šiem darbiniekiem jāpiešķir administratora tiesības datorā. To var izdarīt ar datora lokālā lietotāja, kuram ir administratora tiesības vai domēna administratoru (Domain Admins – angļu v.) grupā esošie lietotāji. Ar labo peles klikšķi spiežot uz *Computer* un izvēloties *Manage* apakšsadaļu *Local Users and Group*, kur Administrator grupai pievieno konkrēto darbinieku, kuram šinī konkrētajā datorā tiek piešķirtas administratora tiesības. Ja lietotāja, kuram tiek piešķirtas administratora tiesības, pirms tiesību

piešķiršanas jau bija autorizējies sistēmā, tad lai saņemtu veiktās izmaiņas, viņam jāatslēdzas no sistēmas pilnībā un jāautorizējas no jauna.

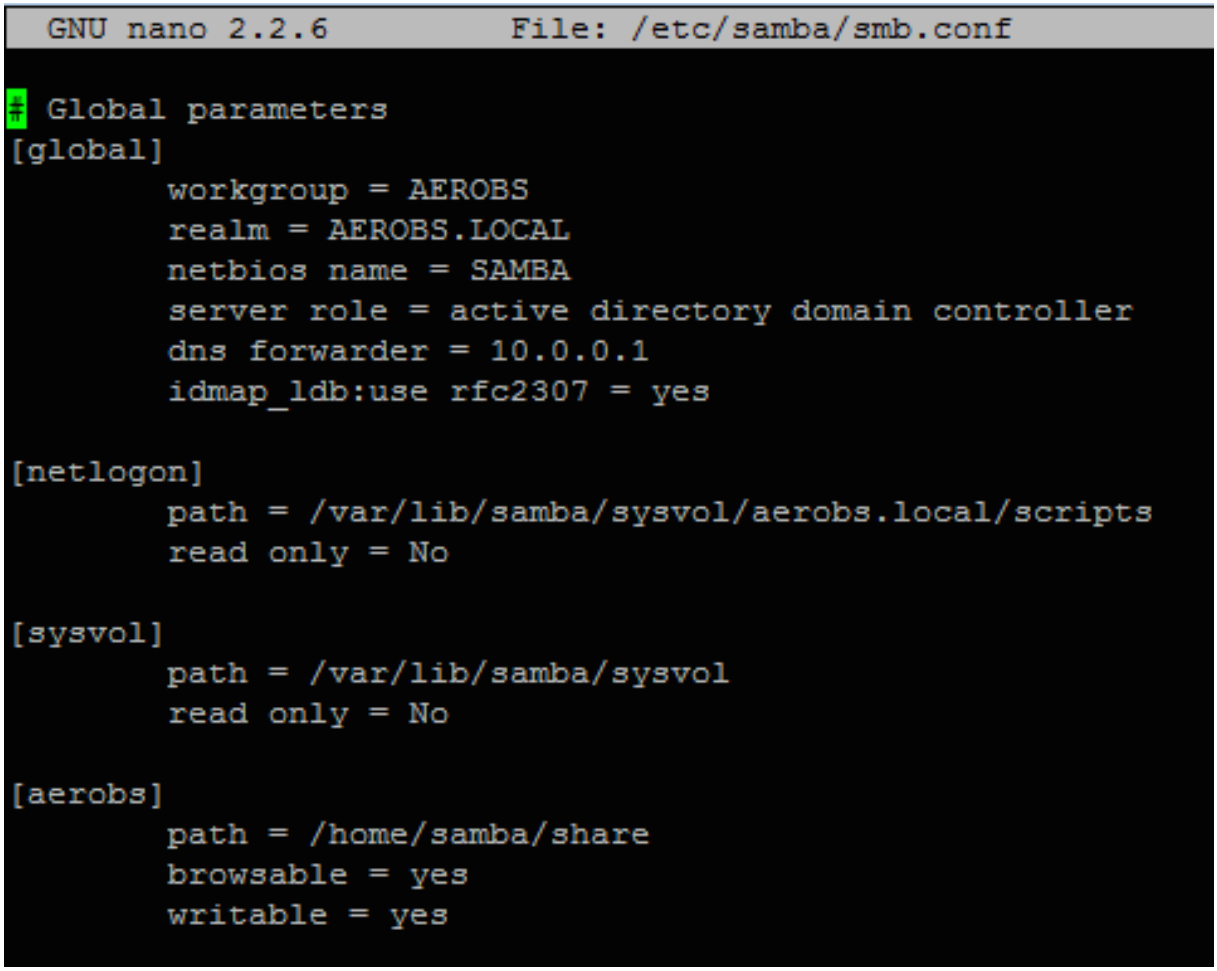


2.3.2.5.1. **Datora administratora tiesību piešķiršana domēna lietotājam**

2.3.2.6. Failu koplietošanas sistēmas izveide

Failu koplietošanas sistēmas izveide tiek veikta vadoties pēc tehniskajās prasībās izvirzītās specifikas, tā izveide tiks veikta vadoties pēc Jay Ts, Robert Eckstein un David Collier-Brown grāmatas "Using Samba"[16], kā arī organizācijas Samba izveidotās Wiki mājaslapas[25].

Koplietošanas sistēmas izveidi sāk mapes, kas būs krātuves bāzes vieta, izveidi ar komandas *mkdir /home/samba/share* palīdzību, kam seko izmaiņu veikšana Sambas servera konfigurācijas failā, kas tiek papildināts ar papildus konfigurāciju.

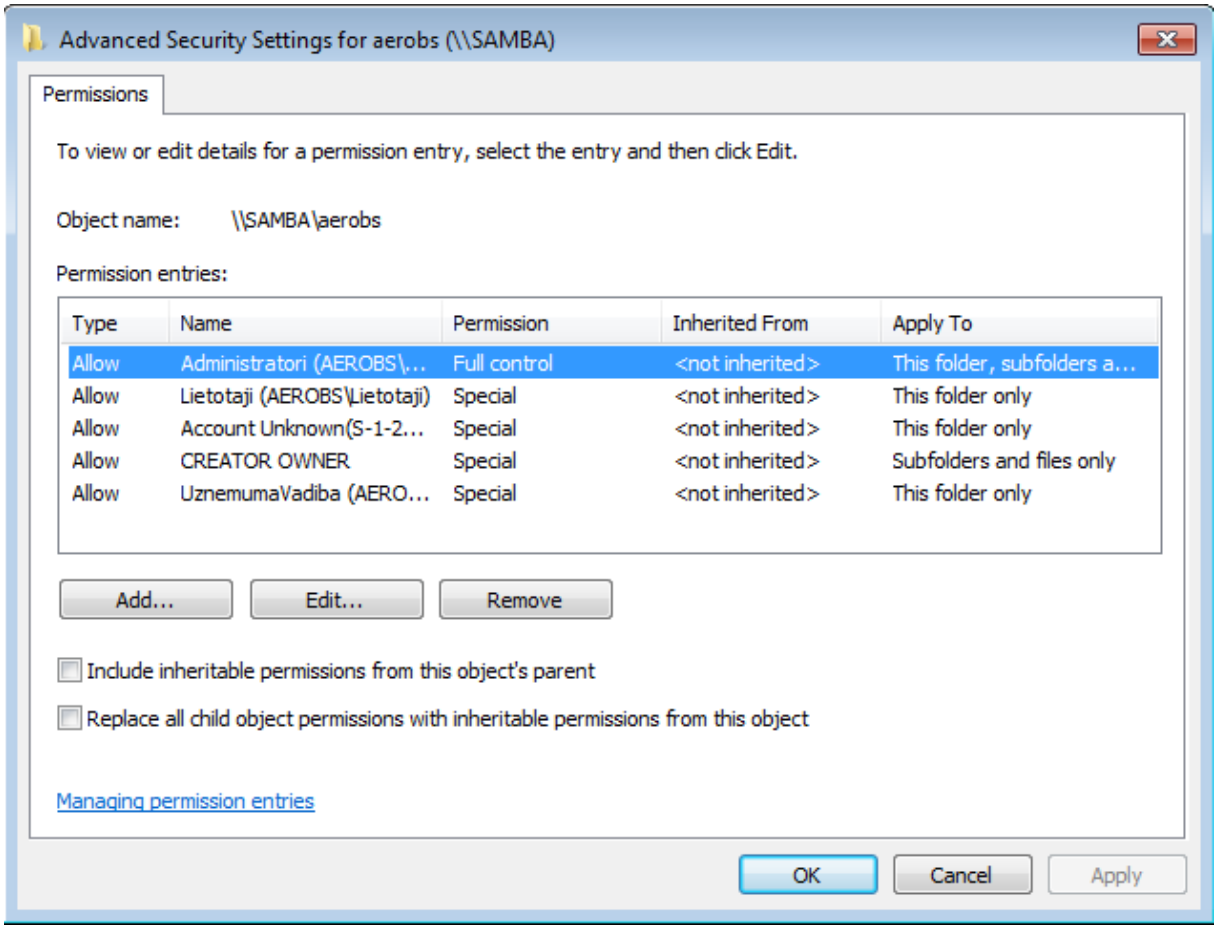


2.3.2.6.1.att. **Sambas konfigurācijas faila saturs**

Failu koplietošanas mapi definē pēdējā kvadrātiekava, kā arī teksts zem tās, kur kvadrātiekavās tiek rakstīts koplietošanas resursa nosaukums, ceļā (path – angļu v.) norāda resursa atrašanās vietu cietajā diskā. Šeit ievada tikko izveidotās mapes atrašanās vietu */home/samba/share.* Pārlūkojams (browsable – angļu v.), kā papildparametrs tiek norādīts, lai veicot tīkla skanēšanu, ikvienai darbstacijai, kas ir tīklā šis resurss būtu redzams, savukārt parametrs, kurš nosaka, vai tiek atļauts saglabāt izmaiņas (writable – angļu v.) noteikt, jā kā, tomēr turpmākajā konfigurācijā šī vērtība tiks ierobežota, jo tiks rediģētas resursa tiesības atkarībā no personas un grupas.

Tālāk konfigurēšana tiek veikta izmantojot Windows 7 operētājsistēmu, kurā tiek atvērts *Computer Manager*, sadaļā *Action* atverot apakšsadaļu *Connect to another computer...* Ar šī rīka palīdzību iespējams pilnībā nokonfigurēt failu koplietošanas serveri izmantojot darbstaciju ar Windows operētājsistēmu. Izveido savienojumu ar Samba serveri adreses laukā ievadot "Samba" servera IP adresi *\\10.0.0.2* vai DNS vārdu *\\samba.* Pēc sekmīga savienojuma nodibināšanas, sāk definētā koplietošanas resursa *aerobs* konfigurēšanu. To veic Computer

Managment/*Shared Folders/Shares* izvēloties koplietojamo resursu *aerobs*. Koplietošanas tiesības piešķir visas tiesības visām trīs grupām – Administratori, Lietotāji un UzņēmumaVadiba, tomēr tas nenozīmē, ka visi lietotāji iegūst tiesības pār šo sistēmu, tāpēc veic papildkonfigurācijas *Security* sadaļas apakšsadaļā *Advanced Security*, kur izveido likumus, pēc kādiem sistēma atļaus/neatļaus piekļuvi resursiem.



2.3.2.6.2.att. **Noteiktumi, pēc kuriem sistēma atļauj/neatļauj piekļuvi koplietošanas resursam**

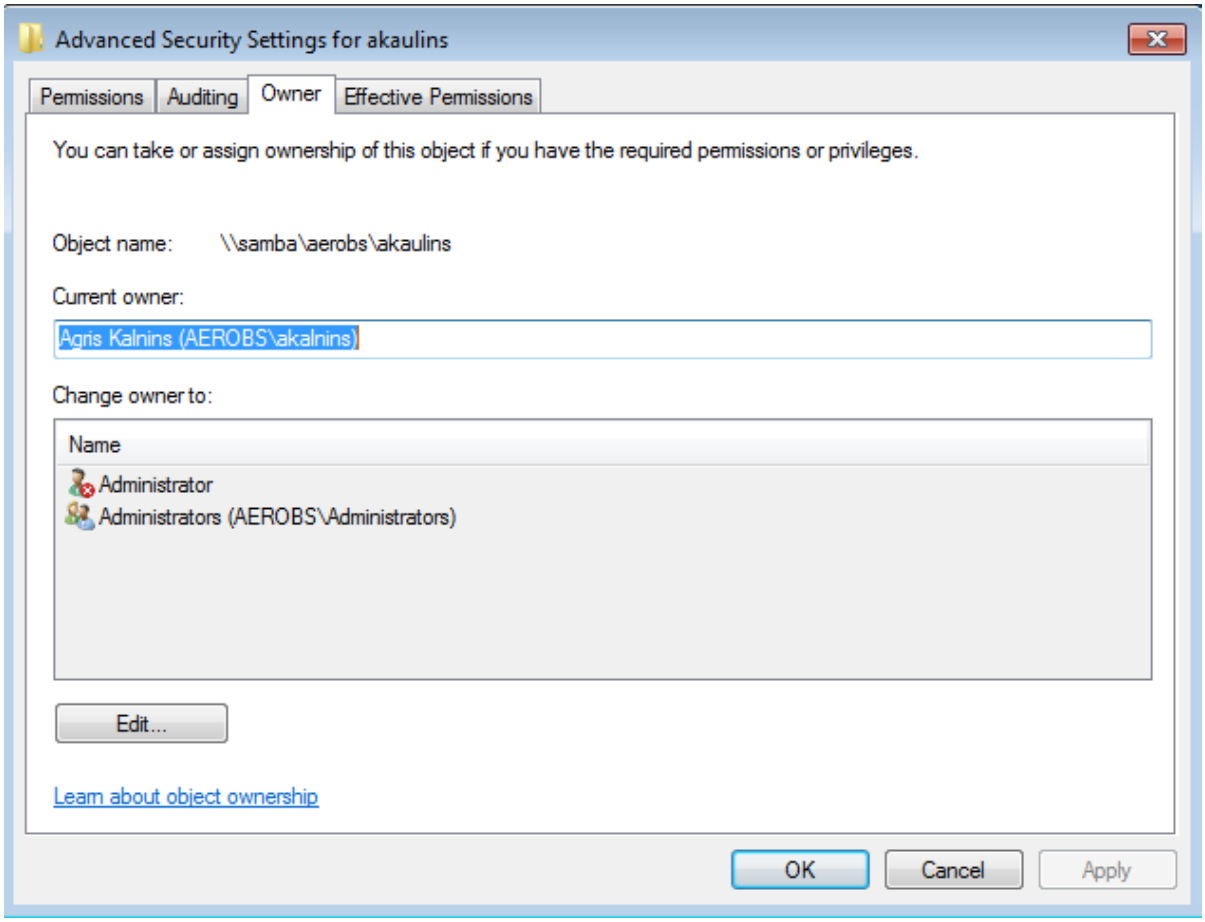
Šeit tiek definēti noteikumi mapei *aerobs*, tās apakšmapēm un failiem. Šie likumi automātiski tiek mantoti jaunizveidotajiem failiem vai mapēm.

- Administratori – tiem tiek piešķirtas visas tiesības pārvaldīt šo resursu – dzēst, pievienot, apskatīt visas apakšmapes, visus failu. Tiem nodrošina pilnīgas pārvaldības tiesības.
- Radītāja, īpašnieks – (Ceator Owner – angļu v.) šis likums nosaka, ka visām apakšmapēm un failiem, kas tik izveidoti koplietošanas resursa mapē *aerobs* saglabās *CREATOR OWNER* likumu, kas paredz, ka mapes īpašnieks, kurš izveido failu mapē, kurā tas ir īpašnieks, iegūst pilnīgas pārvaldes tiesības – dzēst,

labot, pievienot, utt. Šis likums tieši mapi *aerobs*, kurai tiek uzstādītas šīs tiesības neietekmēs, tomēr tās ir nepieciešamas turpmākajām mapēm un failiem, jo tās mantos šo likumu.

- Lietotaji un UznemumaVadiba – šīm divām grupām tiek uzstādīts likumi, kas paredzēti tikai mapei *aerobs*, ar ko lietotāji, kuri iekļauti šinīs mapēs varēs apskatīt *aerobs* apakšmapju un failu nosaukumus, tomēr nevarēs tās atvērt, izlasīt, rediģēt, utt. Apakšmapes šos likumus nemanto.

Tālāk mapē *aerobs* veido apakšmapes, kuru nosaukums ir ekvivalents personas domēna lietotājvārdam, lai būtu vieglāk identificēt katra darbinieka personīgie krātuvi, kurām nevarēs piekļūt neviens cits darbinieks izņemot sistēmas administrators, kā to paredzēja tehniskā specifikācija. Šīs jaunizveidotās mapes manto divus likumus – Administratori un CREATOR OWNER. Mapes īpašnieku uzstāda paredzēto lietotāju (skat. 2.3.2.6.3. attēlu), ar to ir pietiekami, lai nodrošinātu prasību, ka neviens cits izņemot sistēmas administratoru nevar apskatīt tās saturu un veikt jebkādas izmaiņas.



2.3.2.6.3. att. **Mapes īpašnieka uzstādīšana**

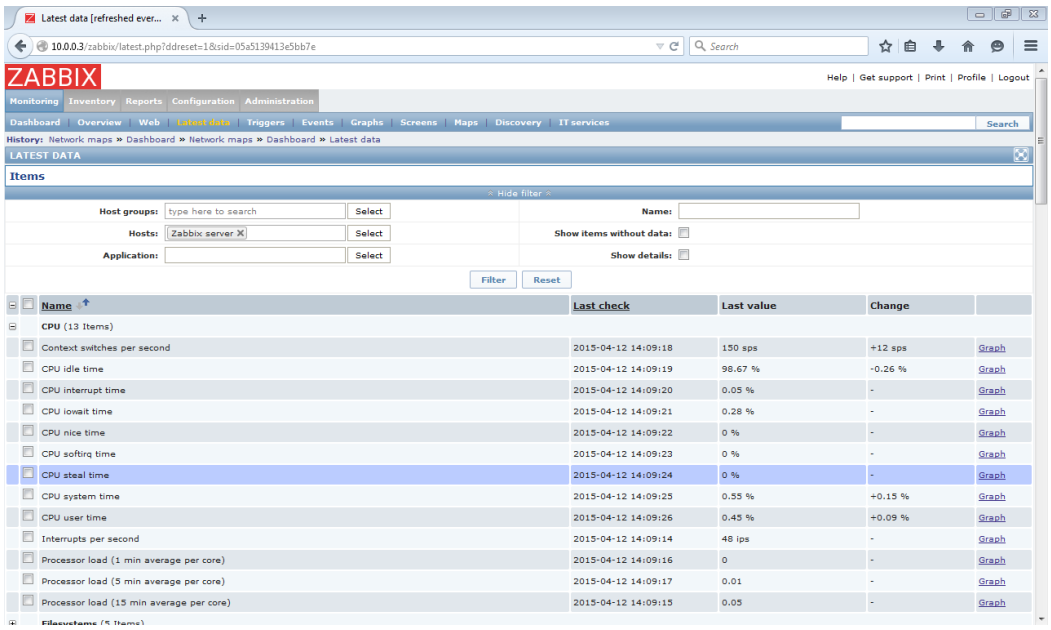
2.3.3. **Zabbix**

Zabbix monitoringa sistēma sastāv no servera un aģenta. Serveris uzkrāj datus, veido grafikus, pārbauda, vai iegūtie monitoringa dati no aģenta nepārsniedz definētās vērtības, kas varētu palīdzēt ātrāk un sekmīgāk prognozēt, novērts un konstatēt problēmas sistēmas.

Zabbix servera un aģenta instalēšana notiek saskaņā ar ražotāja mājaslapā ievietoto instrukciju[32]. Tajā precīzi norādīts, kā uzstādīt monitoringa serveri un aģentu uz Ubuntu 14.04. operētājsistēmas. Tieši šo operētājsistēmu esam sagatavojuši jau iepriekš, tāpēc to uzstādīsim virtuālajā mašīnā "Zabbix". Kad ir noslēgusies Zabbix instalēšana, turpmāko konfigurāciju galvenokārt veiks ar grafisko saskarni, kurai var piekļūt no darbstacijas, kas atrodas tajā pašā tīklā. Izmantosim Windows darbstaciju, kur pārlūkprogrammā ievadīsim adresi http://10.0.0.3/zabbix, kur 10.0.0.3 ir Zabbix servera IP adrese.

Atverot grafisko saskarni, lai rediģētu konfigurāciju, vispirms ir jāautorizējas, bet lai to izdarītu ir jāizmanto Zabbix ražotāja noklusētie autorizācijas dati – lietotājvārds "admin" un parole "zabbix". Tā kā šī ir ražotāja noklusētie autorizācijas dati un tie ir atrodami dokumentācijā, tad pirms lietošanas, rūpējoties par drošību, jānomaina parole, lai gadījumā ja potenciālais uzbrucējs iekļūst informācijas sistēmas tīklā, nevarētu piekļūt monitoringa sistēmai izmantojot ražotāja noklusētos autorizācijas datus. Pēc "drošas" paroles uzstādīšanas var turpināt konfigurēšanu.

Tā kā instalēšanas procesā tika instalēts arī aģents pašam Zabbix serverim, tad sadaļā *Svaigākie dati* (Latest data – angļu v.) jau var apskatīt monitoringa rezultātus (skat. 2.3.3.1. attēlu), kurus Zabbix serveris iegūst no Zabbix serverī uzstādītā aģenta, kurš ir uzkonfigurēts automātiski Zabbix serverī un tam ir uzstādīta ražotāja izveidota veidne (template – angļu v.).



2.3.3.1. att. **Zabbix aģenta iegūtie monitoringa dati par Zabbix servera darbību**

Ražotājs ir sagatavojis vairākas veidnes, kuras ievietojis Zabbix standarta instalācijā. Tās var izmantot dažādu serveru, darbstaciju, tīkla iekārtu, un citu iekārtu monitoringam, tomēr šīs veidnes var labot, papildināt un dzēst pēc sistēmas administratora ieskatiem un vajadzībām. Ir pieejamas veidnes, kas tiks izmantotas šinī darbā sistēmu monitoringā – *Template OS Linux, Template OS Windows, Template App Zabbix Server, u.c.*

2.3.3.1. Monitorings izmantojot Zabbix aģenta interfeisu

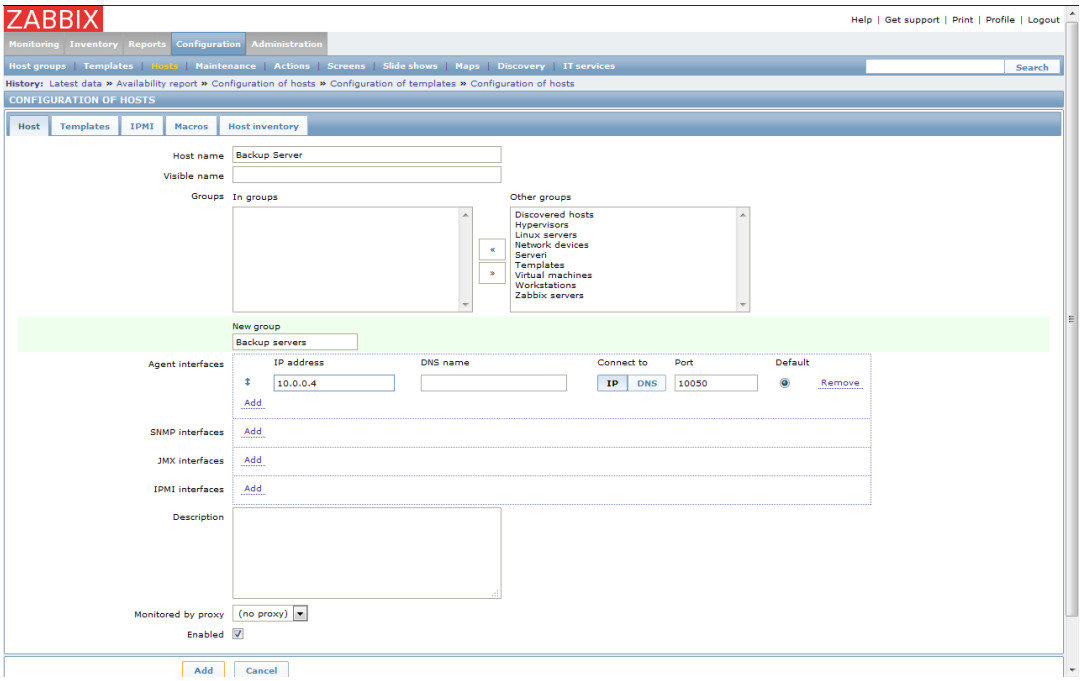
Monitoringu izmantojot Zabbix aģenta interfeisu izmanto galvenokārt serveru, darbstaciju monitoringam. Tie ir pieejami konkrētām operētājsistēmām[33], tādām kā Windows, Linux, Mac OS, Solaris, u.c. Noklusējuma ports monitoringam ar aģenta interfeisa palīdzību ir 10050.

Zabbix divu veidu aģenti – pasīvie un aktīvie[31]. Pasīvie aģenti saņem no Zabbix vai Proxy servera pieprasījumu, par vērtību, kuras lielumu vēlās noskaidrot, aģents tam atbild šo vērtību. Savukārt aktīvais aģents saņem sarakstu no Zabbix servera ar vērtībām, kuras vēlās noskaidrot. Darbā tiks izmantoti tikai pasīvie aģenti.

Tā kā Zabbix programma tik izmantota, lai veiktu vienkāršu sistēmas pārraudzību, tam jāiegūst dati par parametriem, kuru pārraudzību jau veic sistēmas noklusēti uzstādītās veidnes (Templates – angļu v.), tad izmantosim tās, uzstādot konkrētam resursam, atkarībā no operētājsistēmas, konkrētu sagatavi.

2.3.3.2. Resurss

Pirms veidņu izmantošanas un sistēmu monitoringa, vispirms jāizveido *resurss* (host – angļu v.) jeb jādefinē monitorējamās iekārtas adrese (IP, DNS vārds), veids, kā tiks monitorēts (aģents, SNMP, u.c.), vai tiks izmantots Proxy, jādefinē grupa. Lai izveidotu to izdarītu jāatver sadaļas *Configuration* apakšsadaļā *Hosts* un jāizvēlas *Create host.*



2.3.3.2.1. att. **Zabbix resursa veidošanas veidne Backup serverim**

Backup servera *resurss* tiek nosaukts "Backup Server", lai to varētu turpmāk nepārprotami identificēt, tas tika pievienots jau esošā grupā "Serveri", tika norādīts, ka pārraudzība notiks izmantojot aģentu, kurš atrodas IP adresē 10.0.0.4, kas ir virtuālās mašīnas "Backup" IP adrese, izmantojot standarta Zabbix TPC/IP portu 10050. Ar šādu paņēmienu veidojam arī Samba serverim, jo arī tas tiks pārraudzīts izmantojot Zabbix aģentu. Zabbix serveris neveiks pārraudzību Endian Firewall, kaut arī tam ir paredzēts SNMP pārraudzības protokola atbalsts. Tā monitorings tiks veikts izmantojot Endian grafisko saskarni, tomēr kā resurss tas jāizveido, lai to varētu iekļaut sistēmas savienojumu kartē.

2.3.3.2.1 tabula

Zabbix resurss parametru konfigurācijas atspoguļojums ar tiem uzstādītajām vērtībām

Resurss (virtuālās mašīnas nosaukums)	Parametrs	Vērtība
Firewall	Host vārds (host name –angļu v.)	Endian Firewall
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Network devices
	Interfeiss	Netiks monitorēts, jo Endian ir izveidojis rīkus, ar kuriem to var monitorēt izmantojot grafisko saskarni
	IP adrese vai DNS vārds	10.0.0.1
	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	JĀ
Samba	Host vārds (host name –angļu v.)	Samba server
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Serveri
	Interfeiss	Aģents
	IP adrese vai DNS vārds	10.0.0.2
	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	JĀ
Zabbix	Host vārds (host name –angļu v.)	Zabbix server
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Zabbix servers

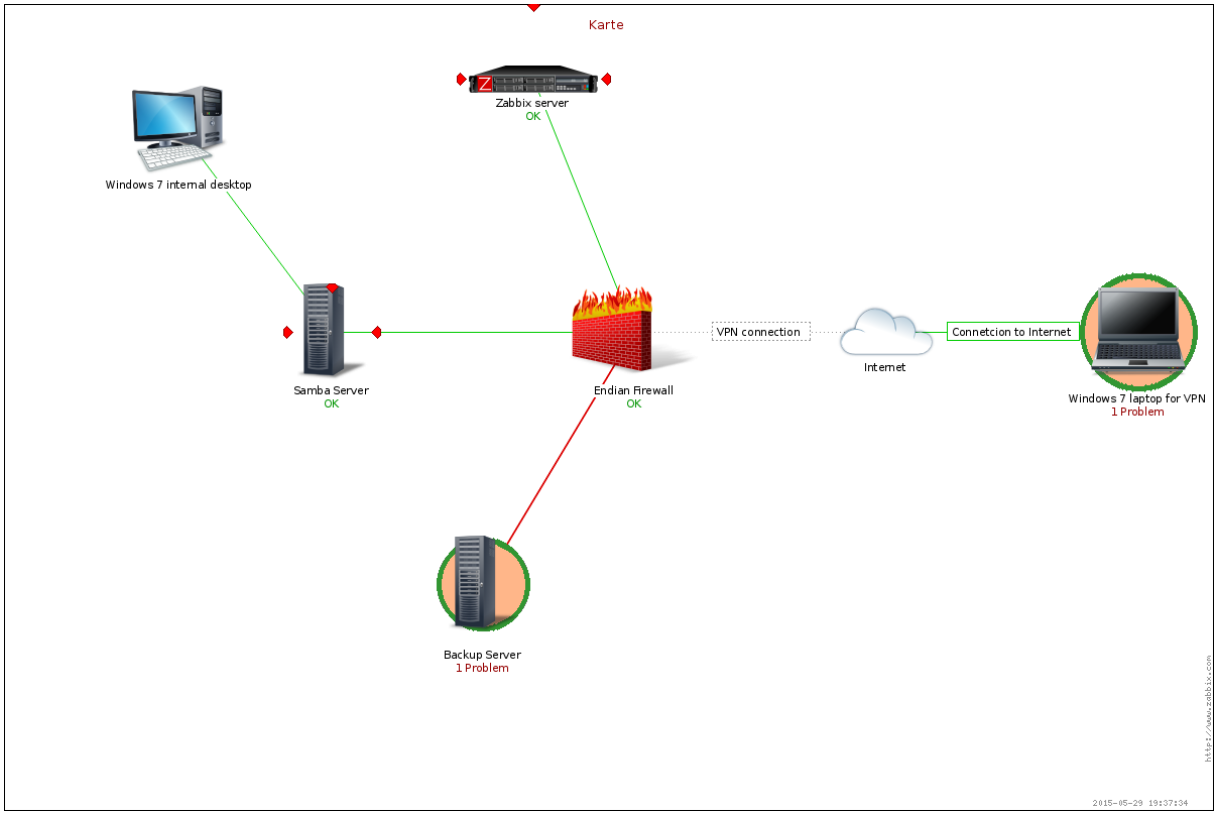
	Interfeiss	Aģents
	IP adrese vai DNS vārds	127.0.0.1 (localhost)
	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	JĀ
Backup	Host vārds (host name –angļu v.)	Backup server
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Zabbix servers
	Interfeiss	Aģents
	IP adrese vai DNS vārds	10.0.0.4
	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	JĀ
Windows 7 internal desktop	Host vārds (host name –angļu v.)	Backup server
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Zabbix servers
	Interfeiss	Aģents
	IP adrese vai DNS vārds	10.0.0.4
	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	JĀ
Windows 7 laptop for VPN	Host vārds (host name –angļu v.)	Backup server
	Redzamais nosaukums (visible name – angļu v.)	-
	Grupa (group – angļu v.)	Zabbix servers
	Interfeiss	Aģents
	IP adrese vai DNS vārds	10.0.0.4

	Monitorings izmantojot *Proxy* (Monitoring by proxy)	Nē (no proxy – angļu v.)
	Ieslēgts (Enable)	Nē (no proxy – angļu v.)

2.3.3.3. Karte

Kartes līdzīgi kā grafikus veido, lai vieglāk būtu uztvert Zabbix servera saņemtos datus, kā arī atklātās problēmas. Ar to palīdzību iespējams vizuāli attēlot notiekošos procesus visā informācijas sistēmā. Tajā shematiski iespējams attēlot pat iekārtu izvietojumu piemēram ēkā, izmantojot iespēju fonā ieliekt bildi, piemēram ēkas plānojumu.

Tīkla pārraudzības nolūkam tiek izveidota, kurā attēlo sistēmā iesaistītos serverus un divas darbstacijas, kas paredzētas tikai vizuālam uzskatam, tomēr ārpus šī projekta ietvariem to ir iespējams papildināt, gan ar monitorējamām iekārtām, gan parametriem, kas tiek pārraudzīti.



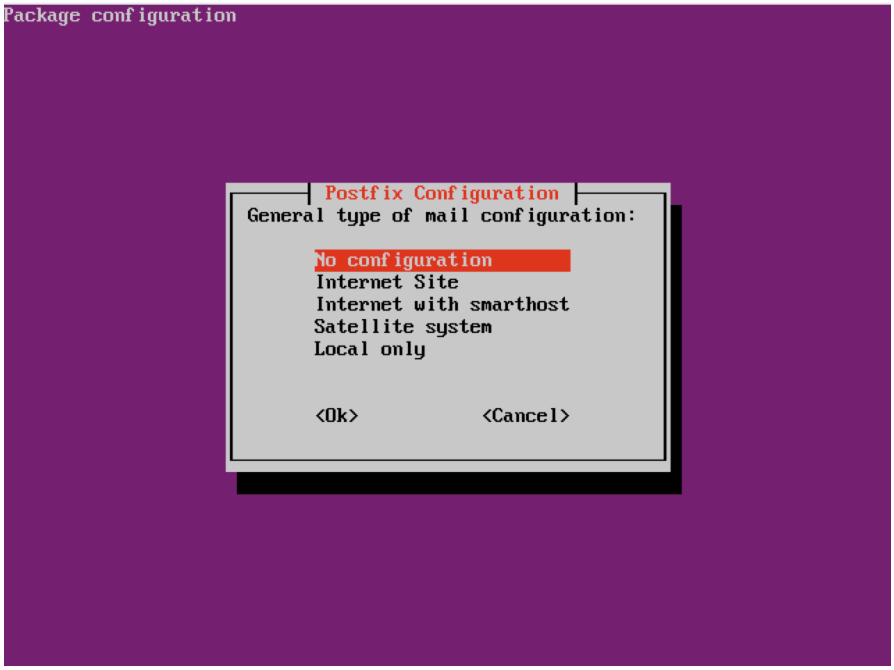
2.3.3.3.1.att. **Izveidotā Zabbix karte, kas attēlo iekārtu pieejamību tīklā**

Kartē starpsavienojumi ir zaļā krāsā, ja tie ir sasniedzami, tomēr sarkani, ja nav. Aplīši, kas iezīmējušies ar "Bakcup Server" un "Windows 7 laptop for VPN" norāda uz kādu problēmu. Aplīšu fona krāsa iekrāsojās atkarībā no problēmas svarīgumu (to paredz noklusētā

konfigurācija). Problēmas var būt visdažādākās –nesasniedzamība jeb nepieejamību lokālajā tīklā, piepildītu cietā diska atmiņu, u.c.

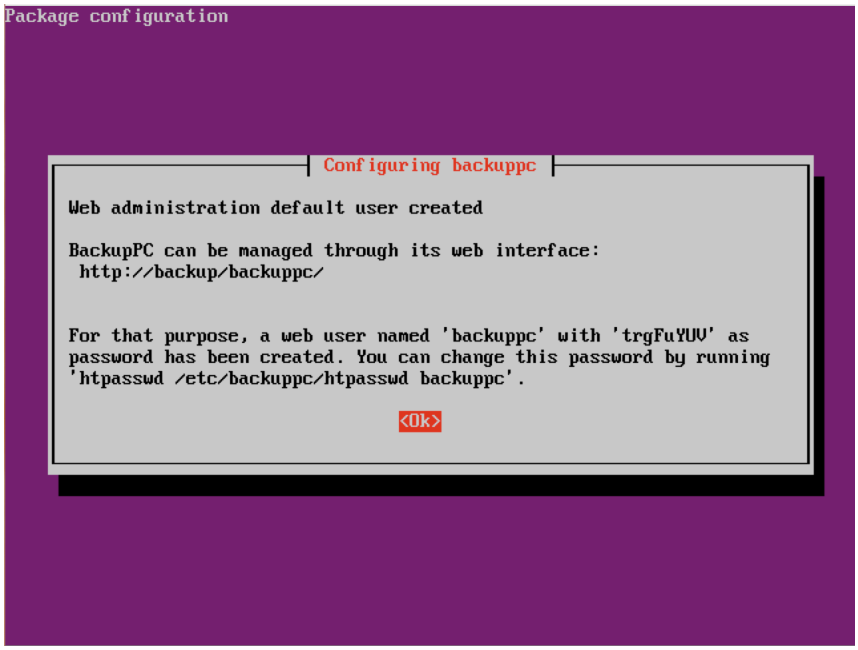
2.3.4. **Backup**

Backup servera uzstādīšana tiek veikta vadoties pēc ražotāja dokumentācijas[7]. Uzstādīšana tiek veikta virtuālajā mašīnā "Backup", uz kuras iepriekš tika sagatavota Linux Ubuntu distributīva operētājsistēma 14.04. LTS. Pirms sistēmas instalācijas, vēlreiz pārliecinās, ka ir uzstādīti jaunākie atjauninājumi un sistēma tiek lietota ar *root* lietotāja tiesībām, pēc tam sāk konfigurēšanu ievadot komandrindā ievada komandu *apt-get install backuppc*, pēc kuras sāksies instalēšanas process, kura laikā sistēma piedāvā konfigurēt e-pasta adresi, kuru izmantot, lai sūtītu paziņojumus par problēmās rezerves kopiju veidošanas procesā (skat. 2.3.4.1 attēlu).



2.3.4.1.att. **E-pasta konfigurēšanas veidne**

Instalēšanas procesā e-pasts netiks konfigurēts, jo nav nepieciešams pēc šāda rīka, tāpēc to nekonfigurē šobrīd, tomēr ja vajadzība vēlāk rodas, to var nokonfigurēt izmantojot grafisko saskarni. Tālāk turpinās sistēmas automātiska instalēšana, kuras noslēgumā parādās svarīgs paziņojums, kurā ietverts lietotājvārds un parole, lai pieslēgtos rezerves kopiju veidošanas sistēmai, kā arī aprakstīti veicamie soļi, lai nomainītu šo paroli (skat. 2.3.4.2. attēlu).



2.3.4.2.att. **Konfigurācijas noslēgums ar ietvertu lietotājvārdu un paroli**

Tālāk konfigurāciju veic grafiskajā saskarnē izmantojot Interneta pārlūkprogrammu, tajāievadot servera adresi http://10.0.0.4/backuppc un komandrindā.

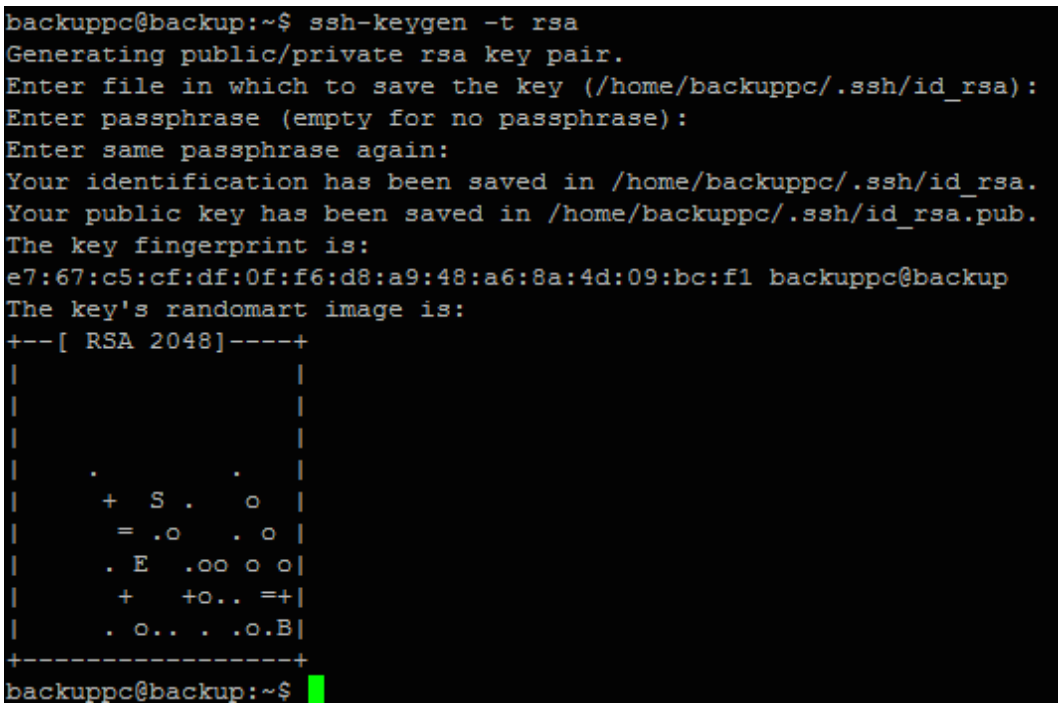
BackupPC programmatūra piedāvā vairākus veidus, kā veikt datu dublēšanu – ar izmantojot SMB protokolu, FTP protokolu, saspiežot un saglabājot arhīvā, kā arī *rsync*, kas ir failu sinhronizācijas rīks, kas izmanto SSH protokolu. Tieši *rsync* metode tiks pielietota šīs informācijas sistēmas rezerves kopiju veidošanas procesā. Tā kā ekonomijas nolūkos dublēt pilnībā visu cietā diska saturu nav iespējams nodrošināt, jo nepieciešams vismaz tik pat ietilpīgs cietais disks, cik ir sistēmai, tad tiek dublētas tikai mapes, kurās glabājās sistēmas konfigurācija, kā arī lietotāju dati, katram serverim šīs mapes ir dažādas. Tās ir atkarīgas no veiktās instalēšanas, kā arī programmatūras uzbūves.

BackupPC, lai veiktu rezerves kopiju veidošanu, izmanto tā izveidotu lietotāju *backuppc*, kas veic programmatūras veiktos uzdevumus – dublēšanu. Tomēr veidojot un plānojot dublēšanas sistēmu jāizvēlas stratēģija, kā to darīt – piešķirot BackupPC serverim pilnas tiesības pār dublējamo serveri, tas būtu, *root* lietotāja tiesības, kas ļautu tam dublēt mapes, kurām var piekļūt tikai ar *root* lietotāja tiesībām, tomēr šādam risinājumam ir savs risks, kas jāņem vērā to izvēloties. Šādā gadījumā BackupPC programma iegūst pilnas tiesības pār otru datoru/serveris, tādejādi, piemēram programmatūras kļūdas dēļ, tā var nodzēst visus datus datorā/serverī vai pat izveidotās kopijas, tādejādi pazaudējot datus neskatoties uz izveidotajām rezerves kopijām. Šāds risinājums ietver sevī arī potenciālus riska draudus, ja BackupPC, kas ir atvērtā pirmkoda programmatūra, līdz ar ko, tās kods ir pieejams ikvienam un atrodot

ievainojamību, tas var ļoti būtiski apdraudēt datu drošību. Otrs risinājums, kā varētu veidot rezerves kopijas, BackupPC programmatūrai nepiešķirot *root* lietotāja tiesības, būtu definēt šo lietotāju, ar kuru tiks veidots pieslēgums datoram/serverim tādejādi liekot sistēmai veikt dažādus procesus un norādīt, ka dublējamos failus ievieto mapē, kurai tiek nodrošinātas piekļuves tiesības šim lietotājam, ar kuru pieslēdzās no BackupPC programmatūras. Šis risinājums ir daudz sarežģītās, kā arī darbietilpīgāks realizēšanas ziņā, tomēr tas ir drošāks, jo samazina iespēju pazaudēt datus. Risinājuma, kurā BackupPC programmatūrai tiek piešķirtas *root* lietotāja tiesības lielākie plusi ir tā salīdzinoši vienkāršā izveide, efektivitāte, iespēja ar sekmīgu darbību kompleksu īsā laikā, piemēram atlikt lietotāja izdzēstu failu dublējamā resursā.

Rezerves kopiju veidošanu BackupPC programmatūrā veic lietotājs *backuppc*, kas tiek izveidots pēc noklusējuma programmatūras instalēšanas procesā. Tā kā rezerves kopiju veidošanai tiks izmantots SSH savienojums, tad vispirms jāsakonfigurē SSH savienojums "Backup" serverim ar "Samba" un "Zabbix" serveri. Šī konfigurācija paredzēs, ka "Samba" un "Zabbix" serveri, brīdī, kad "Backup" serveris pieslēgsies pie tiem, uzticēsies tiem, tādejādi neprasīs paroli, kas varētu būt apgrūtinājums veidojot rezerves kopijas izmantojot SSH savienojumu. Ar šādu paņēmienu tiks nodrošināta sistēmas neatkarīga un automatizēta darbība, kurā sistēmas administratoram nebūs nepieciešams katrā kopijas veidošanas brīdī iejaukties. Lai to panāktu šādu risināju, jāveic secīgas darbības serveros ar komandrindas palīdzību, protams tās var veikt ar grafisko saskarni, piemēram Webmin, ja tāds ir uzstādīts. Šī risinājuma nodrošināšanai tiek izmantoti SSL sertifikātus – publiskos un privātos.

"Backup" serverī ar komandu *mkdir* home/backuppc/.ssh izveido mapi, kurā tik ģenerēti sertifikāti – publiskais un privātais. Lai tos uzģenerētu izmanto komandu *ssh-keygen –t rsa*, kas papildināta ar papildparametru *–t rsa*, kas norāda, ka tiks izmantots RSA šifrēšanas metode. Kad serveris sāk izpildīt komandu, tas uzdod jautājumus par sertifikātu saglabāšanas vietu, kā arī paroli, ar kuru tas tiktu aizsargāts. Šo var izmantot gadījumos, ja nepieciešams uzlabot drošību, tomēr šī projekta ietvaros nav nepieciešams uzstādīt šo paroli.



2.3.4.3.att. **SSL sertifikāta ģenerēšana**

Pēc sekmīgas sertifikātu izveides, mapē */home/backuppc/.ssh* tiek izveidoti vairāki faili, no kuriem *id_rsa* ir privātais sertifikāts, bet *id_rsa.pub* ir publiskais. Tagad serveros, kuriem veidosim rezerves kopijas – "Zabbix" un "Samba", mapē */root* ar komandu *mkdir /root/.ssh* izveido *.ssh* mapi, kurā veidojot pieslēgumu, sistēma pārbaudīs, vai savienojumu veidojošā sistēma ir pazīstama un, vai drīkst to laist sistēmā pat neprasot paroli. Šo pārbaudi sistēma veiks failā /root/.ssh/*authorized_keys*, kas sākumā tiek izveidots un tad tiek iekopēts "Backup" servera faila */home/backuppc/.ssh/id_rsa.pub* faila saturs. Tā ir publiskā atslēga, kas tiks pārbaudīta ar privāto, atbilstības gadījumā sistēma atļaus SSH savienojumu bez jebkādas papildus autorizācijas, kā arī BackupPC programmatūra ar SSH savienojuma palīdzību iegūst *root* lietotāja tiesības serveros "Zabbix" un "Samba", kas ļaus rezerves kopiju serverim veikt kopijas, kā arī vajadzības gadījumā sistēmas administratoram ļoti īsā laikā atgriezt piemēram lietotāja izdzēstos failus. Kad publiskās atslēgas ir iekopētas, pirmā pieslēgšanās veic izmantojot komandrindu, lai pārliecinātos, ka savienojums tiek sekmīgi nodibināts, kā arī netiek pieprasīta autorizācija. Pieslēgšanos veic no "Backup" servera ar komandu "Samba" serverim *ssh root@10.0.0.2* un "Zabbix" – *ssh root@10.0.0.3*. Kad SSH savienojums sekmīgi nodibināts, ir gūta pārliecība, ka turpmāk nevajadzētu būt problēmām ar pieslēgšanos un rezerves kopiju veidošanu tieši savienojuma izveides dēļ.

Tālāko konfigurēšanu veic izmantojot grafisko saskarni, kurā tiek definēts, konkrētās mapes, kurām katrā serverī jāveic dublēšana, laiks, cikos tiks veikta dublēšana, kā arī veids, kā

no tiks kopiju izveide. Vispirms tiek definēti, kurām sistēmām tiks veidoti dublējumi, kā arī norāda, ar kādu lietotājvārdu BackupPC varēs pieslēgties pie šīm sistēmām. Tā kā pirms tam tiks sakonfigurēts SSH savienojums, kas paredz, ka "Backupc" serveris varēs pieslēgties kā *root* lietotājs, tad attiecīgi šo lietotāju norāda kā *root*. Katrā dublējamā resursa konfigurācijā norāda, ka pilnais dublējums jāveic periodā 6,97 dienās, kā to rekomendē ražotājs[7] nevis 7, jo šinī laikā, kas ir 0,03 dienas tik veikta sistēmas startēšana, savienojuma izveide, inkrementālo kopiju gan veic, ik pēc 0.97 dienas. Uzstāda visas tehniskajā specifikācijā paredzētās vērtības – kopiju biežumu, tipu, glabāšanas ilgumu, u.c. Vēlāk šos sistēmas uzstādījumu var pielāgot atkarībā no uzņēmuma vajadzības, tomēr izstrādātā dublēšanas stratēģija ir pietiekami sekmīga un neprasa uzstādīt papildus parametrus.

Xfer sadaļā definē metodi, ar kādu tiks veikta dublēšana, kā arī dublējamās mapes, kas katram serverim ir atšķirīgas. Samba serverim jādublē mapes - */etc, /home/samba, /root, /var*. /etc mapē glabājās sistēmas konfigurācijas faili, piemēram *snm.conf*, kas ir atbildīgs par Samba servera konfigurāciju, */home/Samba* mapē glabājās koplietotie faili Samba serverim, */var* mapē ir log faili, kurus vēlāk var izmantot problēmas diagnosticēšanā, savukārt */root* mapē glabājās SSH savienojuma izveides atslēga. Šīs ir būtiskākās mapes, kuras nepieciešamas, lai atjaunotu servera darbību pēc iespējas ātrāk ar vismazākajiem datu zaudējumiem, kā arī maksimāli taupot vietu cietajā diskā, kurā tiks veikta dublēšana. Līdzīgi kā "Samba" serverim, "Zabbix" serverim dublē mapes - */root, /etc, /var*.

Šos dublējumus vēlams veikt uz cietā diska, kuram tiek nodrošināts arī dublējums, kas tiek glabāts kādā citā datu krātuvē, piemēram pie mākoņpakalpojumu sniedzējiem, vai ārējā datu nesējā – ārējā cietā diskā, zibatmiņā. Tādā veidā arī papildus nodrošinoties pret dabas katastrofām vai ugunsnelaimēm, vai citiem faktoriem, kas var iznīcināt informācijas sistēmas fiziskās iekārtas. Šie ir tikai daži ieteikumi, kā *labāk* nodrošināties pret datu zudumiem, tomēr, ja tos nav iespējams realizēt, vai izmaksas ir pārāk lielas, tad šādā, salīdzinoši mazā informācijas sistēmā, kāda ir šī var izveidot cieto disku masīvu vai masīvus, kas palīdz nodrošināties pret datu zudumu, ja cietais disks fizisku iemeslu dēļ pārstāj darboties, tomēr šī metode nepasargā datus, piemēram no ugunsnelaimes.

3. INFORMĀCIJAS SISTĒMAS LIETOŠANA GALA LIETOTĀJIEM

3.1. **Endian Firewall**

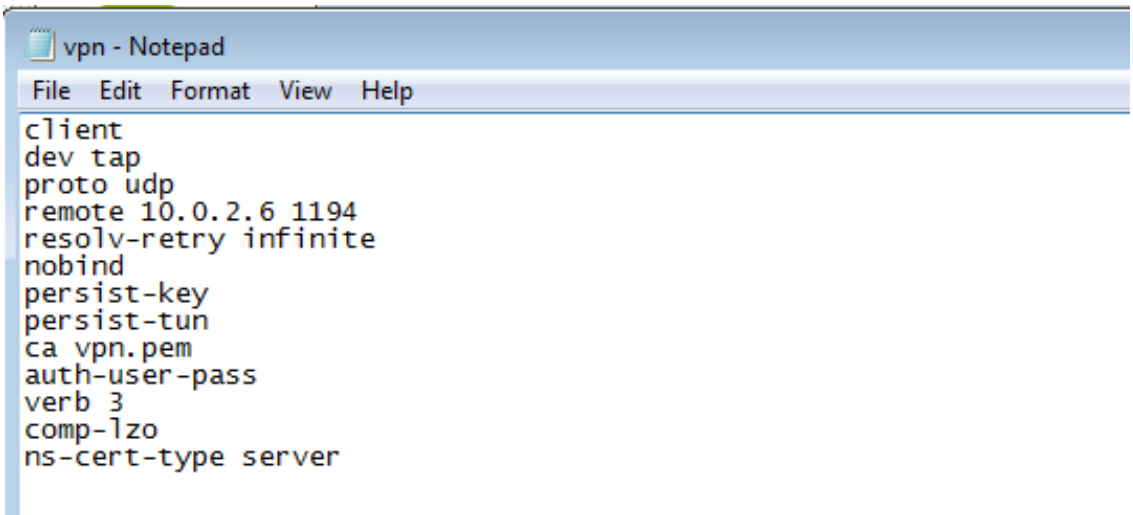
Informācijas sistēmas gala lietotājiem, izņemot sistēmas administratoru nav jābūt piekļuvei Endian Firewall grafiskajam interfeisam, kas pieejams adresē 10.0.0.1, kā arī komandrindai. Šeit sistēmas administrators var ieviest izmaiņas datortīkla konfigurācijā, pievienot papildus pieslēgšanās iespējas informācijas sistēmai izmantojot VPN savienojumu, u.c.

Sistēmas administratora konfigurēšanas iespējas ar komandrindu un grafisko saskarni ir funkcionāli līdzvērtīgas. Ar katru no tām var veikt sistēmas tādu konfigurāciju, kāda tā tiek izmantota šinī informācijas sistēma.

3.1.1. **Pieslēgšanās izmantojot VPN**

Lai pieslēgtos informācijas sistēmai izmantojot VPN savienojumu, vispirms jālejupielādē atvērtā pirmkoda OpenVPN klienta programmatūru un konfigurē to atbilstoši ražotāja pamācībai[18], kas pēc sekmīgas konfigurācijas uzstādīšanas tiks izmantota, lai pieslēgtos informācijas sistēmai.

Kad OpenVPN GNU jeb grafiskā saskarne ir uzstādīta Windows 7 darbstacijā, mapē C:\Program Files\OpenVPN\config ievieto lejupielādēto CA sertifikāta faila ar .pem paplašinājumu kopiju. Līdzās sertifikāta failam šinī mapē izveido jaunu ar paplašinājumu .ovpn, kurā tiek ierakstīta konfigurācija. Šo failu var rediģēt ar Windows 7 iebūvēto rīku Notepad vai kādu citu.

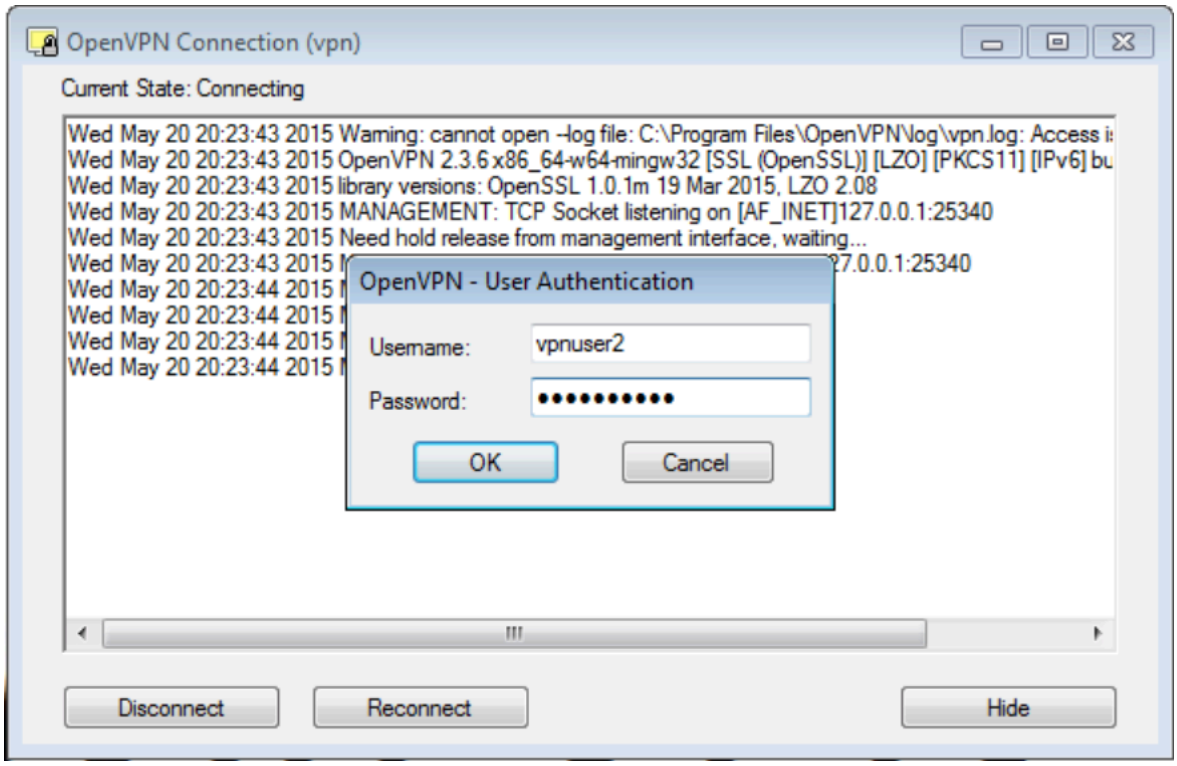


3.1.1.1. att. **VPN klienta konfigurācijas fails**

Konfigurācijas fails tiek veidots vadoties pēc ražotāja izveidotas parauga un skaidrojumiem[17].

- client – norāda, ka šis ir klients nevis serveris, kas cenšas pieslēgties pie VPN servera.
- dev tap – iekārtas tips TAP, tieši TAP izvēlējās kā iekārtas tipu veicot servera konfigurēšanu, tāpēc arī klienta konfigurācijā izvēlās tieši tādu pašu tipu.
- proto udp – savienojuma veids izvēlēts tieši tāds pats kā serverī – UDP protokols savienojuma nodrošināšanai.
- remote 10.0.2.6 1194 – norāda servera adresi un portu, pie kura jāslēdzas, lai izveidotu VPN tuneli. IP adresi ir Endian *red* zonas jeb ārējā IP adrese, kuru nodrošina Interneta provaideris, tieši šī iemesla dēļ ir nepieciešama statiska IP adrese.
- resolve-retry infinite – bezgalīgi ilgi mēģina izveidot savienojumu ar serveri, noderīgi, ja dators nedarbojās tikai vienā tiklā, bet laiku pa laikam maina tīklu, piemēram portatīvais dators, tā kā VPN paredzēts izmantot ar datoru, kas atrodas gan birojā, gan ārpus tā, tātad – portatīvais dators, tad šis tiek iespējots konfigurācijā.
- nobind – tā kā nav nepieciešams konfigurāciju saistīt ar specifisku portu, tad tiek aktivizēts konfigurācijas parametrs *nobind.*
- persist-key un persist-tun – šo parametru izmanto, lai maksimāli saglabātu stāvokli restarta gadījumā, iespējams bez tā var iztikt, tomēr jebkura nodrošināšanās pret negaidītām izmaiņām nozīmē mazāk jūtamu problēmu lietotājiem.
- ca vpn.pem – sertifikāta atrašanās vieta un nosaukums. Tā kā sertifikātu saglabājām tajā pašā mapē, kur atrodas konfigurācijas fails, tad pietiek, ja norāda tikai sertifikāta nosaukumu ar faila paplašinājumu.
- auth-user-pass – autentifikācijas metode, klienta konfigurācijas failā norāda tādu pašu kā serverī uzstādīto – lietotājvārda un paroles metodi.
- verb 3 – uzstāda log faila rakstīšanas līmeni jeb uzstāda līmeni, cik sīki jāveido log faili par savienojumiem.
- ns-cert-type server – ar šo komandu papildina konfigurācijas failu, lai samazinātu riskus no potenciālajiem uzbrukumiem, tas veic servera sertifikāta pārbaudi.

Pēc konfigurācijas faila izveides, sertifikāta ievietošanas līdzās konfigurācijas failam mapē C:\Program Files\OpenVPN\config var startēt OpenVPN grafisko interfeisu un savienot klientu ar serveri.



3.1.1.2. att. **OpenVPN klienta VPN savienojuma izveide ar VPN serveri - lietotājvārda un paroles ievade**

Kad savienojums sekmīgi izmantot, lietotājs var lietot visus serverus tieši tāpat kā atrodoties birojā. Pateicoties izveidotajai konfigurācijai, pieslēdzoties informācijas sistēmai izmantojot VPN savienojumu, netiek ierobežotas nekādas lietotāja darbības. Tas var piekļūt koplietošanas serverim, piemēram sistēmas administrators grafiskajiem serveru vadības rīkiem.

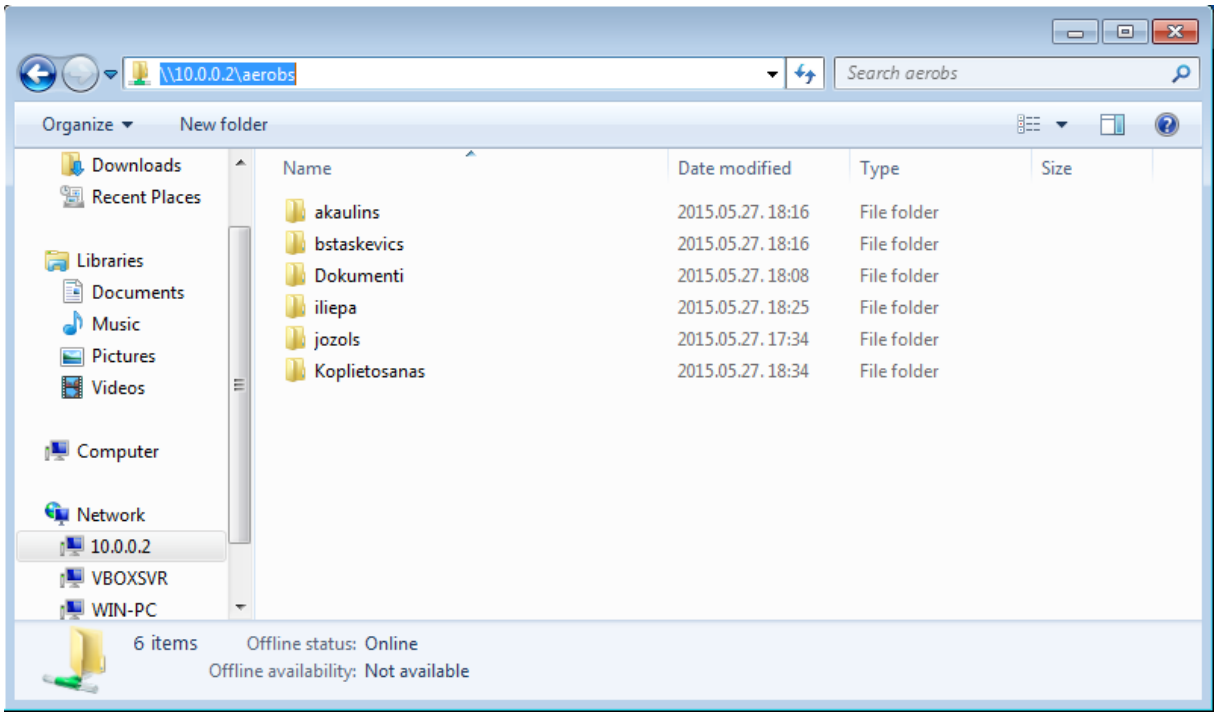
3.2. **Samba**

Samba serveri izmanto gan darbinieki, gan uzņēmuma vadība, gan sistēmas administrators. Šinī sistēmā tiek glabāti faili, kā arī tiek nodrošināta domēna darbība. Līdzīgi kā citi Ubuntu serveri, arī šo var lietot un veikt konfigurāciju izmantojot komandrindu (ko sistēmas administrators konfigurēšanas procesā noteikti izmanot), gan grafisko saskarni. Mūsdienās ir radīto ļoti daudzi grafiskie rīki, ar kuru palīdzību ir iespējams konfigurēt sistēmas, tomēr ne vienmēr šie rīki spēj nodrošināt ekvivalentu funkcionalitāti komandrindai, tomēr iepazīstoties ar Samba serveri un tā iespējām, tika atklāti jauni administrēšanas rīki un

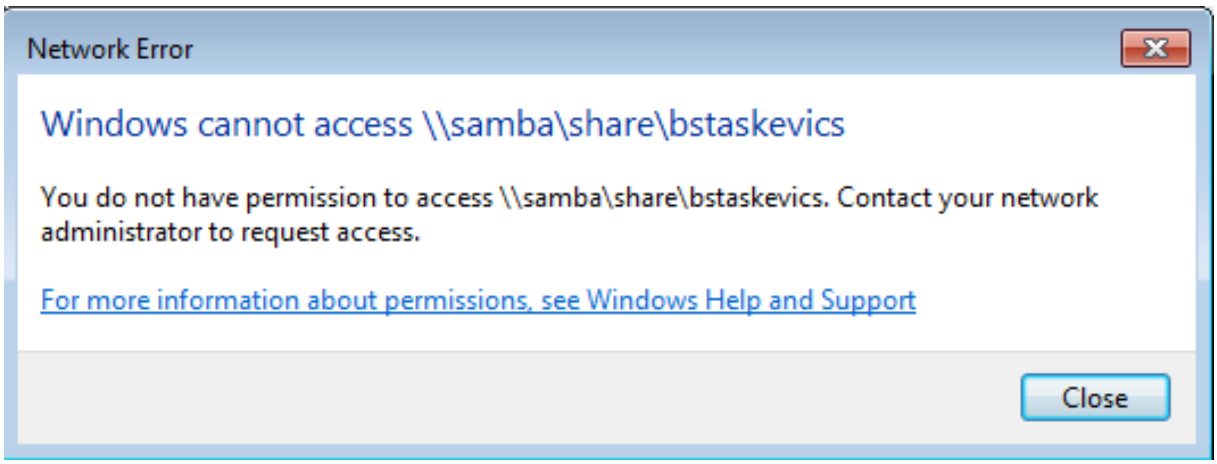
paņēmieni, kar kuriem administrēšanas process notiek jūtami vienkāršāk salīdzinot ar komandrindu, tomēr bez tās pilnībā nav iespējams iztikt. Protams visu šo konfigurāciju var veikt ar citiem paņēmieniem un rīkiem, tomēr šīs sistēmas izbūvē tika izmēģināti grafiskie rīki.

Samba serveri nav iespējams konfigurēt izmantojot Interneta pārlūkprogrammu, jo tam nav uzstādīts attiecīgs grafiskās saskarnes rīks, piemēram Webmin. To iespējams administrēt izmantojot divus Microsoft rīkus – Computer Management (instalēts pēc noklusējuma) un Active Directory Users and Computers (jālejupielādē no Microsoft mājas lapas[6]). Ar to palīdzību sistēmas administrators izmantojot Windows darbstaciju var pārvaldīt domēna lietotājus un koplietošanas resursus.

Sistēmas lietotāji, lai pieslēgtos pie koplietošanas resursa ievada servera IP adresi *\\10.0.0.2\aerobs* vai DNS vārdu \\samba\aerobs. Tādejādi tiks izveidots savienojums un lietotājs redzēs visu informāciju, kas tam ir pieejams (skat. 3.2.1. attēlu). Mēģinot pieslēgties mapēm vai failiem, kuriem tiem nav paredzēts pieslēgties parādīsies attiecīgs kļūdas paziņojums, ka nav tiesību veikt konkrēto darbību (skat. 3.2.2. attēlu).



3.2.1.att. **Skats pieslēdzoties koplietošanas resursam**



3.2.2.att. **Paziņojuma paraugs par aizliegumu piekļūt konkrētam resursam**

3.3. **Zabbix**

Zabbix monitoringa sistēma ir paredzēta tikai sistēmas administratoram, tomēr laika gaitā attīstot un ieviešot jaunus risinājumus, to var sākt izmantot arī uzņēmuma darbinieki, piemēram lai pārraudzītu temperatūras izmaiņas iekštelpās. Zabbix grafiskajā saskarnē tiek izveidots lietotājs sistēmas administratoram, kuram tiek piešķirtas tiesības identiskas kā noklusētajam administratoram, pēc izveides un tiesību piešķiršanas, noklusētais lietotājs jāatslēdz, šī darbība jāveic, lai samazinātu iespējamību, ka kāds varētu piekļūt Zabbix servera grafiskajai videi un gūt kaut vismazāko priekšstatu par informācijas sistēmas uzbūvi un parametriem, kas savukārt var palīdzēt ļaundarim veikt ielaušanos informācijas sistēmā un datu zādzību. Piekļūt Zabbix grafiskajai saskarnei, monitoringa datiem, grafikiem, kartēm un citiem uzstādījumiem var adresē http://10.0.0.3/zabbix. Lai arī tiek izmantots nešifrēts HTTP protokola savienojums, protokola šifrēšana var būt kā papildus drošības instruments, tomēr nav kritiski, jo piekļuve iespējama tikai no iekštīkla vai izmantojot VPN savienojumu, kas tiek šifrēts. Protams ieteicams būtu uzstādīt kaut atvērtā pirmkoda SSL sertifikātu.

3.4. **Backup**

BackupPC programmatūru un serveri var konfigurēt izmantojot komandrindu (SSH) vai grafisko saskarni (http://10.0.0.4/backuppc). Šinī sistēmā piekļuve jānodrošina tikai sistēmas administratoram, kurš var veikt labojumus konfigurācija, pārbaudīt kopiju izveidi, veikt labojumus, utt. Nepieciešamības gadījumā sistēmas administrators var startēt rezerves kopijas izveidi nekavējoties, nesagaidot brīdi, kad tā ir ieplānota. BackupPC grafiskā saskarne ir

izveidota ļoti pārskatāmi, kā arī viegli konfigurējama, kā arī tajā ir iekļauta ražotāja mājaslapā atrodamā dokumentācija, kura pieejama arī neatrodoties tiešsaistē, tādejādi sniedzot papildus informāciju un skaidrojumus par katru no ievadāmajām vērtībām. Grafiskā saskarne piedāvā arī neizmantojot komandrindu izlasīt log failu, kurā sistēma veic ierakstus par katrām savām darbībām – uzsāktajiem procesiem, problēmām, neveiksmīgajiem dublējumiem, utt.

Kopumā saskarne ir izveidota ļoti pārskatāma un funkcionāli ļoti labi nodrošināta, lai ar to varētu veikt gandrīz visas darbības, ko varētu veikt izmantojot komandrindu, tādejādi nodrošinot ērtu un saprotamu vidi, kurā strādāt sistēmas administratoram, kā arī viegli apmācīt informācijas sistēmas lietotāju, kurš uzņemas sistēmas administratora lomu, kaut zināšanas nav tik augstā līmenī.

4. DROŠĪBA

Jebkuru informācijas sistēmu nedrīkst uzstādīt nevadoties pēc labās prakses IS drošības nodrošināšanā. Sistēmu administratoriem, kuri veic sistēmu uzstādīšanu un konfigurēšanu vienmēr jāiepazīstas ar sistēmas uzbūvi, potenciālai vājajām vietām, u.c. Ar vārdu "drošība" nav jāsaprot tikai *drošas* paroles izvēle, tajā ietilpst arī neizmantoto portu bloķēšanu, paaugstinātas drošības risinājumu izvēli, u.c.

Viens no būtiskākajiem jautājumiem, ko apskatīt drošības aspektā ir paroles izvēle. Vienmēr jāatceras, ka ne tikai sistēmu administratoriem ir jāizvēlas drošas paroles, bet to jādara arī sistēmas lietotājiem. Protams nevajag domāt, ka arī izvēloties *drošu* paroli, to neviens nekad neuzzinās vai neuzlauzīs. Izvēloties paroli vienmēr ieteicams izvēlēties to pēc iespējas garāku (vismaz 8 simbolu garumā), iekļaujot tajā gan lielos, gan mazos burtus, kā arī ciparus un simbolus, tādā veidā to padarot grūtāk uzminamu. Parole ir simbolu virkne, kuru drīkst zinās tās lietotājs un to nedrīkst jebkādā veidā nodot lietošanā citiem.

Fakts, ka sistēmu administratori un lietotāji būs izvēlējušies sarežģītas paroles nenozīmē, ka sistēma ir droša. Vienmēr, kad ir izvēles iespēja starp šifrētu un nešifrētu datu pārraides savienojumu, jāizvēlas šifrētu, piemēram HTTPS, FTPS, SSH, u.c., tādejādi vēl vairāk samazinot potenciālo datu noplūdi.

Katrai sistēmai jābūt vismaz minimālām drošības prasībām, tomēr nedrīkst aizmirst par pašas sistēmas lietotājiem, kuri būtu jāinstruē, kā lietot sistēmas resursus, kā glabāt un dalīties ar datiem, kā tos apstrādāt. Šādu apmācību būtu vēlams veikt katram sistēmas lietotājam neatkarīgi no viņa zināšanām IT nozarē, jo tieši sociālā inženierija mūsdienās ir populārs veids, kā trešās personas iegūst datus. Sistēmu administratoriem regulāri jāatgādina sistēmas lietotājiem par drošību, jo tas ir ne tikai viņu interesēs, bet arī uzņēmuma un tā vadītāja.

Nedrīkst aizmirst par sistēmas *veselīguma* monitoringu jeb sistēmas uzraudzību. Nevienu sistēmu nedrīkst uzstādīt un atstāt nepieskatītu, vienmēr ir jāseko līdzi sistēmas darbībai, atjauninājumu uzlikšanai, drošības caurumu novēršanai, sistēmas lietotāju darbībām sistēmā, u.c. Tas ir būtiski, lai samazinātu potenciālos draudus sistēmas uzlaušanai. Nelielā uzņēmumā kā SIA "Aerobs", sistēmu administratoram būtu jāuzņemas iniciatīva un konsultējoties ar uzņēmuma vadību ir jāizstrādā drošības politika. Tajā iekļaujot punktus, kuri jāievēro attīstot sistēmas, risinot problēmas, veicot profilaktisku darbus, u.c. Šinī politikā jāiekļauj tādi punkti kā piemēram:

- rezerves kopijas atjaunināšanas izmēģināšana – piemēram reizi divos mēnešos testa vidē jāizmēģina rezerves kopijas atjaunināšana, lai pārliecinātos, vai vispār ir iespējams atjaunot datus no izveidotajām rezerves kopijām;
- paroļu sarežģītības noteikšana – jānosaka cik sarežģītas paroles lietotājiem jāizvēlas, ja tas iespējams uzstādīt sistēmā, tad jādefinē, cik sarežģītai tai jābūt un cik bieži tā jāmaina;
- piekļuves tiesību noteikšana – neatļaut "visiem darīt visu" jeb ierobežot piekļuvi lietotājiem vietām, kur tiem nav jāpiekļūst, piemēram konfigurācijas failiem, veidnēm;
- ierobežot sistēmu lietotāju darbības – piemēram aizliegt instalēt dažādas programmas, aizliegt piekļūt dažādām mājas lapām utt.

Šie ir tikai daži no iespējamajiem drošības politikas punktiem, vienmēr jārūpējas, lai tie būtu aktuāli un vajadzības gadījumā tiktu papildināti.

5. INFORMĀCIJAS SISTĒMAS UZSTĀDĪŠANA UZ FIZISKĀM IEKĀRTĀM

Neskatoties, ka šīs informācijas sistēmas izveide notika uz virtuālajām mašīnām izmantojot Oracle ražoto atvērtā pirmkoda pilno virtualizāciju nodrošinošo programmu "Virtualbox", šo risinājumu bez īpaši lielām grūtībām ir iespējams pārvietot uz fiziskiem serveriem. Metodes, kā to paveikt ir daudz un dažādas, tomēr vispirms jāizdomā stratēģija attiecībā uz fiziskajiem serveriem, piemēram vai katram virtuālās mašīnas serverim atbildīs fizisks serveris vai tomēr arī fiziskā serverī var uzstādīt virtualizācijas risinājumu, ar kura palīdzību nodrošina vairāku serveru darbību vienā fiziskā iekārtā. Šādu risinājumu mūsdienās izvēlās ļoti daudz, gan lieli, gan mazi uzņēmumi. Lielākais ieguvums no tā ir uzturēšanas izmaksas, jo fiziski tas aizņem mazāk vietas, patērē mazāk elektroenerģiju.

Šīs sistēmas realizācijai izmantojot virtualizāciju nav nepieciešami ļoti jaudīgi un dārgi serveri, jo kopumā sistēma nepatērē pārāk daudz resursus – RAM, HDD diska vietas, procesora resursus. Tā kā sistēmas lietotāju skaits ir ļoti mazs, tajā netiek palaisti milzīgi, resursietilpīgi procesi, piemēram datubāžu serveri. Linux serveru minimālās prasības[27] - 1 GHz procesors, 512 MB brīvpiekļuves atmiņa, 1,75 GB cietā diska atmiņas, tā kā informācijas sistēmā darbojās trīs šādi serveri un Endian ražotais Firewall ir diez gan līdzvērtīgs resursu patēriņa ziņā, jo tas arī ir būvēts uz Linux bāzes, tad veicot vienkāršus aprēķinu, ir skaidrs, ka šīs informācijas sistēmas nodrošināšanu spētu nodrošināt lietotāja darbstacijas dators ar piemēram Intel Core 2 Quad procesoru, 8GB RAM un 1TB cieto disku, kas izveidots masīvā, lai nodrošinātos pret datu zudumiem viena cietā diska fiziska defekta dēļ. Šāda datora iegāde ir salīdzinoši lēta, līdz ar ko tas būtiski nesamazinātu informācijas sistēmas izveides izmaksas.

Pati migrēšana no izstrādes vides uz faktisko vidi, neatkarīgi no izvēlētā fiziskā risinājuma – fiziski serveri vai virtualizācija, nav īpaši sarežģīta. Virtualizācijas gadījumā vienkārši jāeksportē virtuālā mašīna vienā vidē un jāimportē otrā, pārvietojot uz fizisku iekārtu, ir vairāki risinājumi – klonēšana, atjaunošana no rezerves kopijas, u.c.

REZULTĀTI

Kvalifikācijas darba izpētes un izstrādes laikā izveidota informācijas sistēma, izmantojot atvērtā pirmkoda programmatūru, tādejādi sasniedzot izvirzīto darba mērķi. Informācijas sistēmā iekļauta sekojoša programmatūra:

- Samba,
- Endian,
- BackupPC,
- Zabbix.

Izstrādes procesā daudz tika domāts un meklēti drošības risinājumi. Ļoti liela uzmanība tika pievērta mūsdienīgiem risinājumiem, to iespējām, līdz ar ko izveidotā informācijas sistēma ir ar pašreiz tirgū modernākajiem un vienlaikus arī praktiskākajiem atvērtā pirmkoda risinājumiem. Sistēmā tika iekļautas vairāk iespēju, nekā to paredzēja sistēmas tehniskās prasības, jo tas būtiski neiespaido sistēmas ātrdarbību, tomēr palielina sistēmas funkcionalitāti un lietošanas ērtumu.

Pēc sekmīgas informācijas sistēmas izveides, konfigurācijas uzstādīšanas tika radīta vienkārša, gala lietotājiem ērta informācijas sistēma. Īpaši tika domāts par sistēmas administratora lietošanas ērtumu, jo uzņēmumos, kuru apgrozījums nepārsniedz 100 000 EUR visdrīzāk nebūs iespējams algot sistēmas administratoru. Šī iemesla dēļ galvenokārt tika izmantoti grafisko saskaņu rīki – saskarnes, kurām piekļūst izmantojot Interneta pārlūku vai uzstādot speciālu programmatūru datorā.

Darbs tika izstrādāts uz virtuālajām mašīnām, kas bija papildus izaicinājums, jo bija jāveic konkrētā risinājuma darbības izpēte, labākā risinājuma piemeklēšana, tomēr tika izveidota informācijas sistēmas izmantojot mūsdienu tendenci – virtualizāciju. Līdz ar ko tika izpētītas tās iespējas, kā arī secināts, ka šādas sistēmas izveidi un lietošana ir daudz izdevīgāk veikt tieši izmantojot virtuālo infrastruktūru nevis fiziskos serverus.

Kopumā sistēmas izveide vērtējama sekmīgi un prasībām atbilstoša, tomēr šo sistēmu savā uzņēmumā var ieviest ne tikai SIA "Aerobs" jeb uzņēmums, kuram tika veidota šī sistēma. Lai gan informācijas sistēma tika veidota uzņēmumam, kurā strādā tikai četri darbinieki, darbinieku skaita palielināšanās nav problemātiska sistēmai. Šo sistēmu var papildināt un pielāgot gandrīz ikviena uzņēmuma vajadzībām, īpaši uzņēmumiem, kas maksā mikrouzņēmuma nodokli un kuru apgrozījums, kā arī peļņa neatļauj veidot dārgas un sarežģītas

informācijas sistēmas, kuru uzturēšanai speciāli jāalgo darbinieki, kas administrēs tās, jāiegādājas programmatūras lietošanas licences, kā arī jāiegādājas dārga infrastruktūra.

ATSAUCES

1. IP skaidrojums, Interneta enciklopēdija [tiešsaiste] – [atsauce 17.03.2015.] – pieejams: http://lv.wikipedia.org/wiki/IP_adrese
2. Latvijas Republikas tiesību akti [tiešsaiste]. - [atsauce 02.03.2015.] pieejams: http://likumi.lv/doc.php?id=215302
3. LZA TK ITTEA terminu datubāze [tiešsaiste]. - [atsauce 02.03.2015.] pieejams: www.termini.lza.lv
4. MAC skaidrojums, Interneta enciklopēdija [tiešsaiste] – [atsauce 17.03.2015.] – pieejams: http://lv.wikipedia.org/wiki/MAC_adrese
5. SSH skaidrojums, Interneta enciklopēdija [tiešsaiste] – [atsauce 17.03.2015.] – pieejams: http://lv.wikipedia.org/wiki/Secure_Shell
6. Active Directory Users and Computers lejupielādēšanas vieta un uzstādīšanas instrukcija [tiešsaiste] – [atsauce 26.04.2015.] – pieejams: https://www.microsoft.com/en-us/download/details.aspx?id=7887
7. Backuppc dokumentācija [tiešsaiste] – [atsauce 02.05.2015.] – pieejams: http://backuppc.sourceforge.net/faq/BackupPC.html#Step-2:-Installing-the-distribution
8. Endian .iso faila iegūšanas avots [tiešsaiste] - [atsauce 15.03.2015.] - pieejams: http://www.endian.com/us/community/download/efw/
9. Endian konfigurēšanas dokumentācija [tiešsaiste] – [atsauce 05.04.2015.] – pieejams: http://docs.endian.com/3.0/utm/system.html
10. Endian VPN servera konfigurēšana [tiešsaistē] – [atsauce 30.04.2015.] – pieejams: http://docs.endian.com/3.0/utm/vpn/server.html
11. Endian zonu jeb interfeisu sadalījums [tiešsaiste] – [atsauce 05.04.2015.] – pieejams: http://help.endian.com/entries/20272066-Network-Configuration-Wizard-Part-2-of-3-
12. Google publiskā DNS servera adrese [tiešsaiste] – [atsauce 06.04.2015.] – pieejams: https://developers.google.com/speed/public-dns/docs/using
13. Interneta enciklopēdija [tiešsaiste] - [atsauce 15.03.2015.] - pieejams: http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
14. Interneta enciklopēdija [tiešsaiste] – [atsauce 24.03.2015.] – pieejams: http://en.wikipedia.org/wiki/Windows_7_editions

15. Interneta enciklopēdija, Backup programmatūras saraksts [tiešsaiste] – [atsauce 22.04.2015.] – pieejams: http://en.wikipedia.org/wiki/List_of_backup_software
16. Jay Ts, Robert Eckstein un David Collier-Brown grāmatas "Using Samba", O'Reilly, 2000.
17. OpenVPN klienta konfigurācijas paraugs ar skaidrojumiem [tiešsaiste] – [atsauce 02.05.2015.]a – pieejams: https://openvpn.net/index.php/open-source/documentation/howto.html#examples
18. OpenVPN konfigurēšanas pamācīga [tiešsaitē] – [atsauce 01.05.2015.] – pieejams: https://openvpn.net/index.php/open-source/documentation/howto.html#install
19. OpenVPN lejupielādes vieta [tiešsaiste] – [atsauce 01.05.2015.] – pieejams: https://openvpn.net/
20. Par Ubuntu distributīvu [tiešsaiste] - [atsauce 15.03.2015.] - pieejams: http://www.ubuntu.com/about/about-ubuntu
21. Par Virtualbox [tiešsaiste] - [atsauce 15.03.2015.] - pieejams: https://www.virtualbox.org/wiki/Virtualization
22. Putty instalācijas faila iegūšanas avots [tiešsaiste] – [atsauce 01.04.2015.] – pieejams: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
23. RFC2307 skaidrojums [tiešsaiste] – [atsauce 21.04.2015.] – pieejams: https://wiki.samba.org/index.php/Using_RFC2307_on_a_Samba_DC
24. Samba servera konfigurēšanas pamācība [tiešsaiste] – [atsauce 21.04.2015.] – pieejams: https://wiki.samba.org/index.php/Samba_AD_DC_HOWTO
25. Samba Wiki mājas lapa – [tiešsaiste] – [atsauce 19.04.2015.] – pieejams: https://wiki.samba.org/index.php/Main_Page
26. Ubuntu 14.04. faila iegūšanas avots [tiešsaiste] – [atsauce 19.03.2015.] – pieejams: http://www.ubuntu.com/download/server
27. Ubuntu servera minimālās prasības [tiešsaiste] - [atsauce 15.03.2015.] - https://help.ubuntu.com/lts/serverguide/preparing-to-install.html
28. Vietnē ievietotais un regulāri atjauninātais populārāko Linux distributīvu tops [tiešsaiste]. - [atsauce 15.03.2015.] -http://distrowatch.com/index.php?dataspan=52
29. Virtualbox NAT adaptera adrešu konfigurēšana [tiešsaiste] – [atsauce 06.04.2015.] – pieejams: https://www.virtualbox.org/manual/ch09.html#idp100683904
30. Virtualbox NAT network [tiešsaistē] – [atsauce 06.04.2015.] – pieejams: https://www.virtualbox.org/manual/ch06.html#network_nat

31. Zabbix aktīvie un pasīviem aģenti – [tiešsaiste] – [atsauce 12.04.2015.] – pieejams: https://www.zabbix.com/documentation/2.4/manual/appendix/items/activepassive
32. Zabbix instalēšanas norādes ražotāja mājaslapā [tiešsaiste] – [atsauce 11.04.2015.] – pieejams: https://www.zabbix.com/documentation/2.4/manual/installation/install_from_packages
33. Zabbix serveru un aģentu lejupielādes vietne – [tiešsaiste] – [atsauce 12.04.2015.] – pieejams: http://www.zabbix.com/download.php

Kvalifikācijas darbs „**Uzņēmuma informācijas sistēmas izveide izmantojot atvērtā pirmkoda programmatūru**” izstrādāts Latvijas Universitātes Datorikas fakultātē.

Ar savu parakstu apliecinu, ka darbs izstrādāts patstāvīgi, izmantoti tikai tajā norādītie informācijas avoti un iesniegtā darba elektroniskā kopija atbilst izdrukai.

Autors: ***Braijens Staškevičs*** _____ ___.05.2015.

Rekomendēju darbu aizstāvēšanai

Darba vadītājs/a: **sociālo zinātņu bakalaurs vadībzinātnē, Juris Smirnovs**

_____ ___.05.2015.

Recenzents: _____

Darbs iesniegts **___.___.2015**.

Kvalifikācijas darbu pārbaudījumu komisijas sekretārs: _____

Darbs aizstāvēts kvalifikācijas darbu pārbaudījuma komisijas sēdē

___.06.2015. prot. Nr. _____

Komisijas sekretārs(-e): _____