Petteri Olkinuora

Kerberoitu NFSv4-protokolla Jyväskylän yliopiston Linux-työasemaympäristössä

Tietotekniikan pro gradu -tutkielma

16. huhtikuuta 2018

Jyväskylän yliopisto

Informaatioteknologian tiedekunta

Tekijä: Petteri Olkinuora

Yhteystiedot: petteri.olkinuora@jyu.fi

Ohjaaja: Timo Hämäläinen

Työn nimi: Kerberoitu NFSv4-protokolla Jyväskylän yliopiston Linux-työasemaympäristössä

Title in English: Kerberized NFSv4-protocol in University of Jyväskylä Linux-desktop environment

Työ: Pro gradu -tutkielma

Suuntautumisvaihtoehto: Ohjelmistotekniikka

Sivumäärä: 57+4

Tiivistelmä: NFS-protokollaa käytetään Linux-tietokoneiden väliseen tiedostojen jakoon. NFS-protokolla on perinteisesti ollut tietoturvan kannalta ongelmallinen ja se soveltuu huonosti moderneihin avoimiin verkkoihin, joissa vaaditaan käyttäjäntunnistusta, tiedon salausta ja tiedon eheyden tarkistamista. Kerberoitu NFSv4-protokolla on NFS-protokollan tietoturvallinen uudempi versio, joka tukee näitä ominaisuuksia. Tässä tutkimuksessa esitellään Jyväskylän yliopistossa käytössä olevaa NFSv4-protokollan teknistä toteutusta.

Avainsanat: Linux-työasema, NFSv4-protokolla, Kerberos

Abstract: NFS-protocol is used to share data between Linux hosts. NFS-protocol has several security issues and it is problematic in modern open networks, which requires user authentication, data encryption and integrity verification. Kerberized NFSv4-protocol is newer version of NFS-protocol that support these features. This research presents technical overview of NFSv4-protocol in University of Jyväskylä.

Keywords: Linux-workstation, NFSv4, Kerberos

Kuviot

Sisältö

1 Johdanto

Lähiverkot ovat olleet olemassa hieman laskentatavasta ja määritelmästä riippuen 20-40 vuotta. Keskustietokoneiden aikakaudelta siirryttäessä 1980-luvulla mikrotietokoneiden aikakaudelle tieto ja tietokoneilla suoritettavat tehtävät hajautuivat keskustietokoneilta käyttäjien työpöydillä sijaitseville mikrotietokoneille. Yksi modernin tietotekniikan suurista murroksista on 1980-luvulla yleistynyt PC eli Personal Computer eli henkilökohtainen tietokone. Jatkossa käytän tästä nimitystä työasema.

Lähiverkot koostuvat työasemista ja työasemille tarjottavista verkon palveluista. Työasemat ovat yleensä yhden käyttäjän henkilökohtaisia tai muutaman käyttäjän jakamia tietokoneita, joissa on asennettuna esimerkiksi Windows-, Linux- tai macOS -käyttöjärjestelmä. Lähiverkon palveluita työasemille tarjoavat palvelimet. Tyypillisiä lähiverkon palvelimia ovat tulostuspalvelimet, tiedostonjakopalvelimet, sähköpostin säilömiseen, lukemiseen ja välittämiseen erikoistuneet palvelimet sekä WWW-palvelimet.

Palveluiden keskittäminen erillisille palvelimille on perusteltua. Jokaisen palvelun asentaminen ja konfiguroiminen jokaiselle lähiverkon työasemalle on työlästä ja se syö työaseman resursseja. Esimerkiksi käyttäjien tiedostojen keskittäminen erilliselle tiedostonjakopalvelimelle vapauttaa työasemasta tallennustilaa ja yksinkertaistaa tiedostojen varmistuskopiontia ja ryhmätyötilanteissa mahdollistaa tiedostojen yhtäaikaisen käytön usean käyttäjän kesken.

Tässä tutkimuksessa keskitytään tiedostopalveluihin ja erityisesti Linux-käyttöjärjestelmien tiedostonjakopalveluiden tietoturvaan. Tietoturva tiedostonjakopalvelun yhteydessä käsittää kysymyksiä kuten, kenellä on lupa käsitellä tiedostoa tai onko käyttäjä tunnistettu, ennen kuin hän pääsee käsittelemään tiedostoa? Tietoturvaan liittyy myös kysymyksiä, kuten pitääkö tiedonsiirtoyhteys salata?

Yleisin lähiverkoissa käytössä oleva mekaniikka käyttäjän identiteetin tunnistamiseen on Kerberos-protokolla. Kerberos-protokolla on Massachusetts Institute of Technology:ssä 1980-luvulla kehitetty avoimiin verkkoihin suunniteltu käyttäjäntunnistusprotokolla. Se yleistyi lähiverkoihin, kun Microsoft liitti Kerberos-protokollan osaksi Windows 2000 -käyttöjärjestelmää (Butler ym. 2006). Kerberos on yleisesti käytössä Windows-työasemaverkoissa ja sen

avulla käyttäjä voidaan tunnistaa niin tiedosto-, tulostus-, sähköposti-, kuin vaikkapa Skype -palveluihin.

Linux-verkoissa Kerberos-protokolla on myös hyvin tuettu, mutta huonosti hyödynnetty. Yksi tietoturvan kannalta heikoin Linux-palvelu on Linux-käyttöjärjestelmän NFS-tiedostonjakoprotokolla. NFS-protokollassa ei ollut ilmestyessään lainkaan tietoturvan kannalta olennaisia ominaisuuksia, kuten käyttäjän tunnistusta tai tiedon salausta. Vasta 2000-luvulla julkaistu NFS-protokollan neljäs versio, niin kutsuttu NFSv4-protokolla sisältää tuen Kerberos-protokollalle (Bhat ja Quadri 2013).

Kerberos-protokollan ja NFSv4-protokollan yhteiskäyttöä kutsutaan kerberoiduksi NFSv4 -protokollaksi. Kerberoitu NFSv4-protokolla on tietoturvallinen tiedostonjakoprotokolla Linux-lähiverkoissa. Vaikka protokolla on melkein kaksikymmentä vuotta vanha, siitä on tehty todella vähän tutkimusta. Julkaisuja toimivista Linux-työasemaympäristöistä, joissa hyödynnettäisiin kerberoitua NFSv4-protokollaa ei löydy. Jyväskylän yliopistolla on tehty yksi pro gradu -tutkielma aiheesta nimeltään Kerberos ja NFS (Kautto 2008). Tutkielmassa rakennetaan testiympäristö ja tarkastellaan, onko kerberoitu NFSv4-protokolla jo riittävän kypsä sovellettavaksi tuotantoympäristöihin.

Tässä tutkimuksessa käsitellään reaalimaailman tuotantoympäristöä. Jyväskylän yliopiston työasemaympäristö on Windows-ympäristö. Jyväskylän yliopistolla on kuitenkin satoja Linux-työasemia, ja niihin tulee tarjota samat palvelut, kuin Windows-työasemille. Ei ole kustannustehokasta pystyttää Windows-verkon rinnalle Windows-työasemille tarjottavat palvelut vastaavina Linux-työasemaverkon palveluina, vaan on pyritty hyödyntämään Windows-työasemaverkon palveluita muille käyttöjärjestelmille aina, kuin se vain on teknisesti mahdollista. Esimerkiksi Kerberos-käyttäjäntunnistuspalveluita tarjoavat Windows-palvelimet. Tulostuspalveluita tarjoavat Windows-tulostuspalvelut. Tiedostonjakopalveluita tarjoaa kolmannen osapuolen valmistama kaupallinen NAS-järjestelmä (Network Attached Storage). Kyseinen NAS-järjestelmä palvelee erikseen Windows-työasemia ja Linux-työasemia tietoturvallisesti hyödyntäen Kerberos-protokollaa. Jyväskylän yliopiston työasemaverkko on moniprotokollainen sekaympäristö, jossa eri käyttöjärjestelmät sulautuvat yhteen muodostaen monipuolisen, mutta myös monimutkaisen lähiverkon.

Tämä tutkimus on luonteeltaan konstruktiivinen. Konstruktiivisen tutkimuksen piirteitä on kuvattu seuraavasti (Lukka 2000): tutkimus liittyy reaalimaaliman ongelmaan, tutkimus tuottaa innovatiivisen konstruktion, tutkijan ja käytännön edustajien oletetaan tekevän tiimityötä, jossa syntyy kokemuksellista oppimista, tutkimus on kytketty olemassa olevaan teoreettiseen taustaan ja tutkimusten tulokset reflektoidaan takaisin teoreettiseen taustaan. Tutkimuksen kohteena on Jyväskylän yliopiston lähiverkko. Konstruktioksi määritellään kerberoidun NFSv4-protokollan sovellettu käyttö Jyväskylän yliopistolla ja tutkimuksen tulokset ovat yleistettävissä laajemmin kysymykseen, miten toteutetaan tietoturvalliset tiedostonjakopalvelut Linux-työasemista koostuvissa lähiverkoissa, joissa koko lähiverkkoa ei ole rakennettu vain Linux-työasemia silmällä pitäen.

Tässä tutkimuksessa käydään ensin läpi Kerberos-käyttäjäntunnistusprotokollaa siltä osin, kun se on tämän tutkimuksen aiheen kannalta järkevää. Sen jälkeen käydään läpi NFS-protokollan historiaa ja sen nykyisen neljännen version ominaisuuksia. Tutkimuksen empiirisessä osassa yhdistetään NFS-protokolla ja Kerberos-protokolla ja selitetään, miten Linux-työasemaverkossa voidaan toteuttaa tietoturvalliset tiedostonjakopalvelut käyttäen kerberoitua NFSv4 -protokollaa. Tässä tutkimuksessa tuotantoympäristö, Jyväskylän yliopiston lähiverkko, vastaa reaalimaailman tuotantoympäristöä. Kuten aina reaalimaailman tuotantoympäristöissä, kaikki rakennuspalikoita ei voi aina itse valita.

2 Kerberos-protokolla

Kerberos-protokolla on turvallinen, kolmannen osapuolen varmistama kertakirjausjärjestelmä identiteettien tunnistamiseen lähiverkoissa. Kerberos-protokolla on turvallinen, koska se ei ikinä lähetä salasanoja suojaamattomasti lähiverkossa eikä se tallenna salasanoja muistiin. Kerberos-protokollassa on kolmas osapuoli, jonka tehtävänä on varmistaa, että käyttäjä on se, joka hän väittää olevansa ja palvelu on se, mikä se väittää olevansa. Kerberos-protokolla on lisäksi kertakirjausjärjestelmä, eli käyttäjä voi samalla käyttäjätunnuksella ja salasanalla käyttää useita lähiverkon palveluita.

Tässä luvussa käydään läpi käyttäjäntunnistusta Kerberos-protokollalla. Aluksi käsitellään Kerberos-protokollan historiaa. Seuraavaksi käydään läpi Kerberos-protokollan keskeisiä käsitteitä, kuten kertakirjaus, Kerberos-tiketti, Kerberos-prinsipaali ja Kerberos-toimialue. Luvussa käsitellään myös yleisellä tasolla autentikointiprosessi ja tietoturvaan liittyviä huomioita.

2.1 Mikä on Kerberos-protokolla

Kerberos-protokolla on verkon protokolla, jonka tehtävänä on varmistaa identiteettejä suojaamattomissa verkoissa ja huolehtia pääsynhallinnasta verkon palveluihin. Identiteettillä tarkoitetaan tässä käyttäjää tai palvelua verkossa. Kerberos on suunniteltu avoimiin verkkoihin. Avoimella verkolla tässä tarkoitetaan verkkoa, joissa kuka tahansa voi kuunnella ja/tai häiritä verkon liikennettä. Tyypillinen esimerkki avoimesta verkosta on Internet. Internetissä kuka tahansa voi kuunnella verkon liikennettä, varastaa liikennettä tai muokata sitä ja uudelleen lähettää väärennettyä liikennettä eteenpäin.

Kerberos-protokolla on hyvin tuettu useilla eri käyttöjärjestelmäalustoilla. Se käyttää symmetristä salausta käyttäjän ja palvelun identiteetin varmistamiseen ja se on suunniteltu toimimaan palomuurien molemmin puolin. Kerberos tarjoaa myös kertakirjauspalvelun (Neuman ja Ts‘o 1994).

2.2 Historia

Nimi Kerberos tulee Kreikan mytologiasta. Kerberosta on kuvattu usein kolmipäiseksi koiraa muistuttavaksi hirviöksi, joka vartio manalan porttia. Kreikan mytologian mukaan kuoleman jälkeen ihminen päätyy manalaan, jota hallitsevat Haades-jumala ja hänen vaimonsa Persefone. Manalan porttia valvoo kolmipäinen koira nimeltä Kerberos, jonka tehtävänä on varmistaa, etteivät kuolleet pääse karkaamaan manalasta ja etteivät elävät pääse tunkeutumaan manalaan (Graves 1992).

Tietotekniikassa Kerberoksen juuret sijaitsevat Massachusets Institute of Technology:ssä eli MIT:ssä. Alunperin Project Athenan tuotoksena syntyneen käyttäjäntunnistusprotokollan kehitys alkoi 1980-luvun alussa (Neuman ja Ts‘o 1994). MIT:ssä ymmärrettiin, että keskustietokoneiden aikakausi oli päättymässä ja oltiin siirtymässä jaettuihin verkkoihin ja palvelin-asiakas-arkkitehtuuriin. Jaetussa verkossa tyhmä pääte ja keskustietokone eivät enää keskustele keskenään yhtä väylää käyttäen vaan samalla väylällä on nyt muitakin toimijoita. Kerberos-protokollan versiot yksi, kaksi ja kolme olivat kehitysversioita. Kerberoksen neljäs versio julkaistiin 1980-luvun lopulla. Kerberoksen nykyinen versio viisi on syntynyt uusista tarpeista, joita neljännessä versiossa ei ollut (Neuman ja Ts‘o 1994).

Nykyään referenssiversio MIT Kerberos v5 protokollasta on julkisesti saatavilla verkossa osoitteessa `https://web.mit.edu/kerberos/`. Se on myös RFC 4120 (Neuman ym. 2005). Kerberos-protokollasta on olemassa myös muita vapaita ja kaupallisia versioita. Kerberoksen suosio kasvoi valtavasti, kun Microsoft ilmoitti ottavansa Kerberos v5. protokollan Windows 2000 -verkkojen käyttäjäntunnistusjärjelmäksi (Butler ym. 2006). Nykyään useimmat käyttöjärjestelmät tukevat Kerberos v5. -protokollaa. Tästä eteenpäin käytän tässä tutkielmassa Kerberos v5. protokollasta lyhennettä Kerberos.

Kerberoksessa on neljä pääperiaatetta. Se on turvallinen, se on kertakirjausjärjestelmä (engl. Single Sign On, SSO), siinä on aina luotettu kolmas osapuoli ja se tarjoaa keskinäisen luottosuhteen palvelimen ja asiakkaan välillä (Neuman ja Ts‘o 1994). Seuraavaksi käydään tiivistetysti läpi, mitä nämä tarkoittavat:

- Kerberos on turvallinen käyttää. Kerberos ei koskaan lähetä verkossa salasanoja suojaamattomana

- Kerberos on kertakirjausjärjestelmä. Tämä tarkoittaa sitä, että käyttäjän pitää todistaa henkilöllisyytensä kirjautumalla järjestelmään. Onnistuneen sisäänkirjautumisen jälkeen käyttäjä voi käyttää kaikkia verkon Kerberosta hyödyntäviä resursseja samalla kirjautumisella. Käyttäjän ei siis tarvitse kirjautua jokaiseen verkon palveluun erikseen.
- Kerberos rakentuu asiakkaista ja palveluista sekä keskitetystä Kerberos-palvelusta. Jokainen kirjautuminen tapahtuu erillisen keskitetyn Kerberos-palvelun kautta. Mallissa on siis aina asiakas, palvelu ja kolmannen osapuolen Kerberos-palvelu.
- Kerberos tarjoaa keskinäisen luottosuhteen palvelun ja asiakkaan välillä. Tämä tarkoittaa sitä, että sekä asiakkaan, että palvelun luotettavuus tarkistetaan kirjautumisen yhteydessä keskitetyssä Kerberos-käyttäjätunnistuspalvelussa. Näin verkon palvelu voi luottaa asiakkaan olevan se joka se väittää olevansa ja asiakas taas voi luottaa siihen, että verkon palvelu on se, mikä se väittää olevansa.

Kerberos perustuu salaisuuteen, jonka molemmat osapuolet tietävät. Kerberos salaa kaiken arkaluontoisen verkossa välitettävän viestinnän salausavaimilla, jotka ovat molempien osapuolien tiedossa, mutta joita on vaikea ulkopuolisen saada tietoonsa (Neuman ja Ts‘o 1994).

2.3 Kerberos prinsipaali, -instanssi ja -toimialue

Jokainen Kerberos-ympäristö koostuu asiakkaista, palveluista ja Kerberos-käyttäjäntunnistuspalvelusta. Asiakkaaksi usein mielletään käyttäjä ja käyttäjän työasema. Palveluksi taas mielletään palvelin tai siinä pyörivä palvelu. Kerberos-käyttäjäntunnistusjärjestelmä koostuu kahdesta erillisestä palvelusta, joista myöhemmin lisää.

Kaikilla toimijoilla tässä ympäristössä on oma prinsipaali. Prinsipaali yksilöi toimijan Kerberosta hyödyntävässä ympäristössä. Prinsipaaliin liittyy aina avain. Tämä avain on salasana tai salalause. Prinsipaali on aina uniikki. Toisella käyttäjällä, työasemalla, palvelimella tai palvelulla ei voi olla samaa prinsipaalia. Jokainen prinsipaali alkaa käyttäjätunnuksella tai palvelun nimellä. Sitä seuraa valinnaiset instanssit. Näitä valinnaisia instansseja käytetään kahdessa tapauksessa. Palveluprinsipaalien tapauksessa sekä erillisten ylläpitotunnusten kanssa.

Kerberokseen liittyy prinsipaalin ja valinnaisten instanssien lisäksi toimialue (engl. realm). Kerberos-toimialue sisältää kaikki palvelut, palvelimet, työasemat ja käyttäjätunnukset, jotka kuuluvat saman ympäristön piiriin eli kaikki verkon palvelut, jotka käyttävät samoja Kerberos-käyttäjäntunnistuspalveluita. Kerberos-toimialue eli Kerberos-REALM nimetään yleensä organisaation DNS-nimen perusteella, mutta isoilla kirjaimilla kirjoitettuna. Esimerkiksi Helsingin yliopistolla on DNS-nimi helsinki.fi. Heidän Kerberos-REALM olisi silloin HELSINKI.FI.

Toimialueen nimi ei ole pakko olla DNS-nimi. Esimerkiksi Jyväskylän yliopiston DNS-nimi on jyu.fi, mutta Microsoft Active Directoryn tarjoama Kerberos-ympäristön toimialue on historiallisista syistä nimeltään AD.JYU.FI. Ennen keskitettyä IT-palvelua Jyväskylän yliopistolla oli käytössä useampia Kerberos-toimialueita. Palveluiden keskittämisen myötä muista Kerberos-toimialueista on luovuttu, ja jäljelle on jäänyt AD.JYU.FI -niminen Kerberos-toimialue.

Kerberos v.5 -protokollan mukainen prinsipaalin rakenne on seuraava:

```
kayttajatunnus[/vi1/vi2.../vin]@KERBEROS.REALM
palvelu/dns-nimi[vi1/vi2.../vin]@KERBEROS.REALM
```

Prinsipaali koostuu prinsipaalin nimestä, jota seuraa `n`-määrä valinnaisia instansseja `vi`, joita seuraa `@`-merkki ja lopuksi isoilla kirjaimilla kirjoitettu Kerberos-toimialueen nimi. Esimerkiksi käyttäjäntunnukset `matti` prinsipaali toimialueessa AD.JYU.FI voisi olla vaikka

```
matti@AD.JYU.FI
```

2.4 Avaintenjakelukeskus

Kerberos-Avaintenjakelukeskus (engl. Key Distribution Center, KDC) on keskeinen osa Kerberos-ympäristöä. Avaintenjakelukeskus koostuu kolmesta komponentista: Kerberos-tikettienmyöntämispalvelusta (engl. Ticket Granting Service, TGS), Kerberos-käyttäjäntunnistuspalvelusta (engl. Authentication Server, AS) sekä tietokannasta, joka sisältää kaikki Kerberos-prinsipaalit sekä niiden avaimet (salasanat tai salalauseet) (Butler ym. 2006). Käytännön toteutuksissa nämä kolme komponenttia on yleensä yhdistetty samaksi palvelinsovel-

lukseksi.

Ilman avaintenjakelukeskusta Kerberos-järjestelmä ei voi toimia. Siksi ainakin tuotantoympäristöissä avaintenjakelukeskukset ovat poikkeuksetta monistettuja palveluita (Neuman ja Ts‘o 1994). Verkko, joka sisältää monta avaintenjakelukeskusta toteutetaan siten, että Kerberos synkronoi kaikki prinsipaalit ja niiden avaimet kaikille avaintenjakelukeskuksille. Tämä tarkoittaa sitä, että kaikkien käyttäjien salasanat, kaikkien palveluiden salasanat ja kaikkien palvelimien ja työasemien salasanat sijaitsevat kaikilla avaintenjakelukeskuksilla.

2.5 Tiketti

Kerberos-käyttäjäntunnistusjärjestelmässä käyttäjän tunnistamiseen käytetään tikettiä. Kerberos-tiketti tai tiketti on avaintenjakelukeskuksen myöntämä salattu tietue, joka sisältää sessioavaimen, erilaisia lippuja sekä muita kenttiä. Tiketillä on kaksi tehtävää. Ensinnäkin se varmistaa asiakkaan identiteetin palvelulle ja palvelun identiteetin asiakkaalle. Toiseksi tiketti sisältää lyhytkestoisen suojatun sessioavaimen, jonka avulla asiakas ja palvelu salaavat välitettävää tietoa verkossa.

Tikettiä voidaan verrata vaikka passiin. Passissa on tietoja henkilöstä, kauanko passi on voimassa ja mitä rajoitteita passin käytöllä on. Kerberos-tiketti sisältää vastaavia tietoja. Kerberos-tikettejä on erilaisia. Seuraavat tiedot löytyvät kaikista Kerberos-tiketeistä:

- Palvelua haluavan asiakkaan prinsipaali tai palvelua tarjoavan palvelun palveluprinsipaali
- Aikaleimat, milloin tiketti astuu voimaan ja milloin voimassaolo päättyy
- Lista IP-osoitteista, joista kyseistä tikettiä voi käyttää
- Salattu sessioavain asiakkaan ja palvelun väliseen kommunikointiin

Avaintenjakelukeskus myöntää tiketin. Se kerää tietoja palvelua pyytävältä asiakkaalta, lisää omia tietoja tikettiin ja asettaa lippujen arvoja ja salaa tiketin ja toimittaa sen perille asiakkaalle. Kerberos-tiketti pitää salata riittävän hyvin, jotta ulkopuoliset tahot kaapattuaan tiketin eivät saa sitä auki ja muutettua sieltä asioita, kuten voimassaoloaikaa, käyttäjän prinsipaalia tai palvelun palveluprinsipaalia.

Tiketillä on lyhyt voimassaoloaika. Usein tiketin voimassaoloaika määritellään esimerkiksi työpäivän pituiseksi. Näin vaikka tiketti varastettaisiinkin, siitä ei ole varastajalleen pitkäksi ajaksi iloa. Tiketin salauksen pitää olla riittävän hyvä ja voimassaoloajan riittävän lyhyt, jottei mahdollinen hyökkääjä pääse purkamaan tiketin voimassaoloajan sisällä tikettiä auki ja muuttamaan tietoja sieltä tai varastamaan tiketin sisältämää sessioavainta.

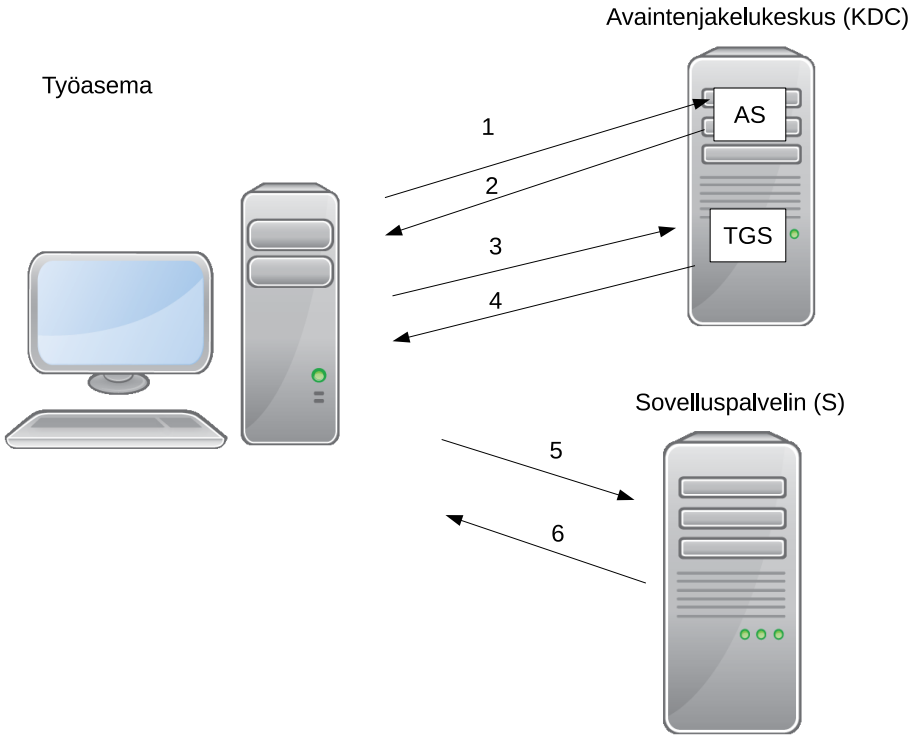
Kerberoksen kertakirjausominaisuus on toteutettu erityisellä tiketinmyöntämistiketillä (engl. Ticket Granting Ticket, TGT). Tiketinmyöntämistiketin avulla käyttäjä voi käyttää verkon palveluita ilman, että hänen täytyy joka kerta kirjautua jokaiseen palveluun erikseen. Tiketinmyöntämistiketin avulla käyttäjä voi pyytää avaintenjakelukeskukselta yksittäisiä tikettejä verkon eri palveluihin. Tällöin käyttäjä ei lähetä avaintenjakelukeskukselle käyttäjätunnusta ja salasanaa vaan tiketinmyöntämistiketin. Avaintenjakelukeskuksen työnjako menee siten, että Kerberos-käyttäjäntunnistuspalvelu myöntää pelkästään Tiketinmyöntämistikettejä ja Kerberos-tikettienmyöntämispalvelu myöntää tikettejä verkon muihin palveluihin.

2.6 Autentikointiprosessi

Yksinkertaistettu malli Kerberos käyttäjäntunnistuksesta etenee kuvion 1 mukaisesti (Neuman ja Ts‘o 1994).

Kohdassa 1. käyttäjä kirjautuu työasemaan. Käyttäjä antaa käyttäjätunnuksen ja salasanan työaseman sisäänkirjautumisprosessille. Työasema välittää käyttäjän tunnistautumispyynnön avaintenjakelukeskuksen (KDC) käyttäjäntunnistuspalvelulle (AS). Mikäli käyttäjätunnus ja salasana olivat oikein, kohdassa 2. AS palauttaa tiketinmyöntämistiketin (TGT) työasemalle. Kun käyttäjä haluaa käyttää työasemaltaan verkon palvelua (S), lähettää työasema kohdassa 3. tikettienmyöntämispalvelulle (TGS) käyttäjän tiketinmyöntämistiketin (TGT) ja pyynnön saada käyttää verkon palvelua (S). Kohdassa 4. TGS palauttaa palvelutiketin käyttäjän työasemalle. Kohdassa 5. käyttäjä haluaa käyttää verkossa olevaa palvelua (S). Työasema lähettää TGS-palvelulta saamansa palvelutiketin sovelluspalvelimelle (S). Kohdassa 6. sovelluspalvelin kuittaa käyttäjätunnistuksen onnistuneeksi ja käyttäjä voi alkaa käyttää sovelluspalvelimella olevaan verkon palvelua (S).

Sovelluspalvelimessa sijaitseva verkon palvelu voi olla esimerkiksi tiedostonjakopalvelu tai



Kuvio 1. Kerberoksen yksinkertaistettu malli.

tulostuspalvelu. Kerberoksen avulla käyttäjän ei tarvitse tunnistautua sovelluspalvelimeen erikseen. Koska Kerberos on kertakirjausjärjestelmä, käyttäjän ei tarvitse syöttää käyttäjätunnusta ja salasanaa jokaiseen verkon palveluun erikseen vaan käyttäjän työasemalla tallessa oleva tiketinmyöntämistiketti (TGT) tunnistaa käyttäjän identiteetin verkon palveluille automaattisesti.

Butler ym. (2006) sekä (Neuman ym. 2005) kuvaavat tätä prosessia hieman tarkemmin, mutta silti vielä yleisellä tasolla seuraavasti. Käyttäjän (K) kirjautuessa työasemaan (T) työaseman sisäänkirjautumisprosessi siis pyytää tiketinmyöntämistikettiä (TGT) avaintenjakelukeskukselta. Kohdassa 1. pyynnön rakenne sisältää käyttäjän prinsipaalin Pk, aikaleiman T1, tikettienmyöntämispalvelun prinsipaalin Ptgs sekä pyynnön tiketin voimassaoloajasta V:

```
Kohta 1.
K -> AS : Pk,T1,Ptgs,V
```

Tämä viesti on nimeltään KRB_AS_REQ. Kun käyttäjätunnistuspalvelu (AS) saa pyynnön,

se tarkistaa löytyykö käyttäjän prinsipaali (Pk) Kerberos-tietokannasta ja onko pyynnössä oleva aika (T1) järkevä. Koska Kerberos on aikariippuvainen, ei aika (T1) saa poiketa kovin paljoa avaintenjakelukeskuksen ajasta. Yleensä Kerberos sallii viiden minuutin heiton järjestelmien kelloissa. Kaikkien verkon palveluiden pitää siis olla samassa ajassa, jotta käyttäjätunnistus onnistuu.

Jos käyttäjän prinsipaali (eli käyttäjän käyttäjätunnus) löytyy Kerberos-tietokannasta ja pyynnössä oleva aikaleima on sallittujen rajojen sisäpuolella, alkaa avaintenjakelukeskus rakentaa käyttäjälle vastausviestiä. Vastausviesti koostuu kahdesta osasta. Avaintenjakelukeskus luo satunnaisen sessioavaimen käyttäjän ja tikettienmyöntämispalvelun välistä kommunikointia varten (Stgs). Ensimmäinen osa vastausviestiä koostuu sessioavaimesta (Stgs), tiketinmyöntämispalvelun prinsipaalista (Ptgs) sekä tiedon tiketinmyöntämistiketin voimassaoloajasta (Vtgt). Viestiosa salataan Kerberos-tietokannasta löytyvällä käyttäjän salaisella avaimella (Ak). Toinen osa vastausviestiä sisältää sekin vasta luodun sessioavaimen (Atgs), käyttäjän prinsipaalin Pk, tiketin voimassaoloajan Vtgt, uuden aikaleiman T2, sekä asiakkaan IP-osoitteen. Tämä osa vastausviestiä on itseasiassa tiketinmyöntämistiketti. Se salataan Kerberos-tietokannasta löytyvällä tikettienmyöntämispalvelun avaimella (Atgs). Tämä kaksiosainen vastausviesti on nimeltään KRB_AS_REP:

```
Kohta 2.
AS -> K : Ak{Stgs,Ptgs,Vtgt},Atgs{Stgs,Pk,Stgt,T2,IP}
```

Tiketinmyöntämistiketin (Stgt) saatuaan käyttäjä on kirjautunut onnistuneesti työasemaan. Kerberos on kertakirjausjärjestelmä. Tämä tarkoittaa nyt sitä, että käyttäjä voi käyttää muita verkon palveluita kirjautumatta niihin enää erikseen uudestaan. Tämä tehdään käyttäjän kirjautumisvaiheessa saaman tikettienmyöntämistiketin avulla.

Seuraavaksi käyttäjä haluaa käyttää sovelluspalvelimen (S) palvelua. Tämä palvelu on määritelty sellaiseksi turvalliseksi verkon palveluksi, joka vaatii käyttäjän tunnistamista. Käyttäjä pyytää tikettienmyöntämispalvelulta palvelutikettiä, joka sallii hänen käyttävän sovelluspalvelimen (S) palvelua. Tämä pyyntö on nimeltään KRB_TGS_REQ ja se koostuu seuraavista paloista: sovelluspalvelimen (S) prinsipaalista Ps, Pyydetystä voimassaoloajasta Ts, käyttäjän tiketinmyöntämistiketistä Stgt sekä käyttäjän työaseman senhetkisestä ajasta Tk, joka on

salattu sessioavaimella Stgs:

```
Kohta 3.
K -> TGS : Ps,Ts,Atgs{Stgs,Pk,Vtgt,T2,IP},Stgs{Tk}
```

Tikettienmyöntämispalvelin purkaa käyttäjän tikettienmyöntämistiketin omaa salaista avaintaan käyttäen (Atgs) ja aikaleiman (Tk) käyttäjän tiketinmyöntämistiketistä löytyvällä sessioavaimella (Stgs). Seuraavaksi tiketinmyöntämispalvelu tarkistaa käyttäjän tiketinmyöntämistiketin aikaleiman (Vtgt) sekä pyynnössä olleen senhetkisen ajan Tk. Jos molemmat ajat ovat sallittujen rajojen sisäpuolella luo tiketinmyöntämispalvelu käyttäjälle palvelutiketin sovelluspalvelimen (S) käyttämistä varten.

Palvelutiketti koostuu uudesta istuntoavaimesta Rtgs, käyttäjän prinsipaalista Pk, palvelutiketin voimassaoloajasta(Trtgs), TGS-palvelimen uudesta aikaleimasta T3 sekä asiakkaan IP-osoitteesta sovelluspalvelimen (S) salaisella avaimella SO salattuna.

Käyttäjälle tiketinmyöntämispalvelu lähettää paluuviestin KRB_TGS_REP, joka on taas kaksiosainen. Toinen osa koostuu juuri luodusta istuntoavaimesta Rtgs, sovelluspalvelimen (S) prinsipaalista Ps sekä palvelutiketin voimassaoloajasta (Trtgs) ja nämä kolme asiaa salataan tiketinmyöntämistiketin sessioavaimella. Toinen osa paluuviestistä on juuri luotu istuntoavain:

```
Kohta 4.
TGS -> K : Stgs{Rtgs,Ps,Trtgs},SO{Rtgs,Pk,Trtgs,T3,IP}
```

Tällä paluuviestillä käyttäjä voi käyttää sovelluspalvelimen (S) palvelua. Käyttäen autentikointipalvelun istuntoavainta Stgs käyttäjä voi avata paluuviestin. Seuraavaksi käyttäjä muodostaa uuden viestin, joka sisältää aikaleiman T4 sekä palvelulipun ja salaa viestin kohdassa 4. saadulla istuntoavaimella. Tätä viestiä kutsutaan KRB_AP_REQ ja sen muoto on:

```
Kohta 5.
K -> S : Stgs{T4},SO{Rtgs,Pk,Trtgs,T3,IP}
```

Halutessaan käyttäjä voi vaatia sovelluspalvelimelta molemminpuolista autentikointia. Tällöin sovelluspalvelimen täytyy todistaa identiteettinsä käyttäjälle. Sovelluspalvelin avaa asiak-

kaan aikaleiman T4, käsittelee sitä sovitulla tavalla (T4+V) missä V=vakio, salaa sen istuntoavaimella ja lähettää vastausviestin käyttäjälle. Tämä viesti on autentikoinnin viimeinen osa ja sitä kutsutaan KRB_AP_REP-viestiksi ja sen muoto on

```
Kohta 6.
S -> K : Stgs{T4+v}
```

Tässä esiteltiin Kerberos-autentikoinnin yksinkertainen malli. Protokollan sisällä tapahtuu vielä lisää toimintoja, mutta niiden yksityiskohtainen esittely ei ole tämän tutkielman kannalta olennaista.

2.7 Tiketin lisäominaisuuksia

Kerberos-tiketillä on lukuisia lisäominaisuuksia. Tiketti voi olla "Renewable"tai "Forwardable", se voi olla myös "Proxiable", tunnistamisen sijaan tiketillä voidaan vain testata tulevaa mahdollista käyttäjätunnistusta tai tunnistus voidaan käyttäjän sijaan liittää alla olevaan rautaan käyttäjän, palvelun tai käyttöjärjestelmän sijaan. Lista on pitkä ja kasvaa protokollaan kehitettävien uusien ominaisuuksien myötä. Ajantasainen lista lisäominaisuuksista löytyy Kerberoksen RFC dokumentista (Neuman ym. 2005) Tämän tutkimuksen kannalta tällainen olennainen lisäominaisuus on "Renewable", joka käsitellään seuraavaksi.

Joskus sovellukset vaativat tiketiltä pidempää voimassaoloaikaa, kuin esimerkiksi kahdeksan tuntia. Renewable eli uusittava tiketti on sellainen tiketti, joka tietyn aikavälin sisällä voidaan uusia ilman, että koko käyttäjätunnistusprosessia tarvitsee läpikäydä uudelleen. Uusittavalla tiketillä on kaksi voimassaoloaikaa. Toinen on varsinainen voimassaoloaika (yleensä 8-24 tuntia) ja toinen, kuinka kauan tikettiä voi uusia (tyypillisesti yksi viikko). Tikettiä voi siis uusia voimassaoloajan sisällä uusinta-ajan verran (Neuman ym. 2005). Jos esimerkiksi tiketin voimassaoloaika on kahdeksan tuntia ja sitä saa uusia viikon ajan, niin jokaisen kahdeksan tunnin aikana sovelluksen on muistettava käydä pyytämässä tiketin uusintaa avaintenjakelukeskukselta. Kun tiketin uusinta-aika päättyy, tiketti lakkaa olemasta voimassa ja uutta tikettiä varten koko käyttäjätunnistusprosessi pitää aloittaa alusta.

2.8 Tietoturva

Vaikka Kerberosta pidetään turvallisena, se ei takaa turvallisuutta kaikissa tilanteissa. On tärkeä ymmärtää protokollan rajoitteet, jotta käyttöönoton suunnittelussa kohdeympäristössä osataan ottaa oikeat asiat huomioon.

Ensinnäkään Kerberos ei osaa suojautua Denial of Service (DoS) -hyökkäyksiltä. Kerberoksessa ei ole mekanismia havaita tällaisia hyökkäyksiä vaan tällaiset hyökkäykset on estettävä verkossa muilla menetelmillä. Toiseksi prinsipaalien avaimet on pidettävä turvassa. Prinsipaalin avaimen avulla ulkopuolinen taho voi esiintyä toisena käyttäjänä, työasemana, palvelimena tai palveluna. On erittäin tärkeää suojata avaintenjakelukeskus, jottei prinsipaalien avaimet pääse vuotamaan ulkopuolisen tahon haltuun (Neuman ym. 2005). Kolmanneksi Kerberos ei voi huonoille salasanoille tai salalauseille mitään. Jos hyökkääjä arvaa käyttäjän salasanan tai salalauseen, hän voi varastaa kyseisen käyttäjän identitetin. Neljänneksi Kerberoksessa ei ole mekaniikkaa varmentaa kerberoitujen ohjelmien aitoutta. Jos esimerkiksi käyttäjän työasemalle on asennettu haittaohjelma, joka kerää käyttäjän kaikki näppäinpainallukset, saa hyökkääjä käyttäjän salasanan selville (Neuman ja Ts‘o 1994).

2.9 Mitä salausalgoritmeja Kerberos hyödyntää

Kerberos perustuu salaisuuteen, jonka molemmat osapuolet tietävät ja tätä yhteistä salaisuutta siirretään verkossa vain salatussa muodossa. Kerberos salaa tiedonsiirron symmetrisellä salausalgoritmilla (Neuman ja Ts‘o 1994).

Alun perin Kerberos v5. rakentui DES-salausalgoritmin (Data Encryption Standard) ja MD5-tiivistealgoritmin ympärille. Kerberos RFC määrittelee salausalgoritmit, joita Kerberoksen pitää tukea. Jotta Kerberos-ympäristö olisi taaksepäin yhteensopiva vanhempien asiakasohjelmien kanssa, RFC suosittelee seuraavien salausalgoritmien tukemista: AES128-CTS-HMAC-SHA1-96, DES-CBC-MD5 sekä DES3-CBC-SHA1-KD (Neuman ym. 2005). Nykyään DES-salausalgoritmia pidetään yleisesti aivan liian turvattomana (Joseph, Krishna ja Arun 2015). Myös DES-salausalgoritmin seuraajaa nk. kolminkertaista DES-salausta (3DES) sekä MD5-tiivistealgoritmia pidetään nykyään turvattomina (Joseph, Krishna ja Arun 2015). Tätä tutkielmaa kirjoittaessani talvella 2018 Microsoft Windows -käyttöjärjestelmät eivät

oletuksena enää tue DES-pohjaisia salausalgoritmeja ollenkaan (Microsoft 2012) vaan oletuksena Microsoft Windows käyttää AES256-CTS-HMAC-SHA1-96-salausalgoritmia Kerberoksen kanssa. Tällä hetkellä AES-salausalgoritmia pidetään sekä suorituskykyisenä, että turvallisena. Se kuitenkin tarkoittaa vain sitä, että salausalgoritmin vikoja ei vielä tunneta (Joseph, Krishna ja Arun 2015).

2.10 GSSAPI

GSSAPI (tai GSS-API) on lyhenne sanoista Generic Security Application Program Interface. GSSAPI on IETF-standardi RFC 2078, joka tarjoaa ylätason API-rajapinnnan erilaisiin käyttäjäntunnistus- ja tiedonsuojauspalveluihin. GSSAPI määrittelee abstraktin ohjelmointirajapinnan ottamatta kantaa alla oleviin tietoturvakäytäntöihin tai käyttäjäntunnistusprotokolliin (Fuchsberger 1998). Kerberos ei ole GSSAPI eikä GSSAPI ole Kerberos, mutta moderneissa Linux-järjestelmissä GSSAPI tarjoaa sovellustason rajapinnan Kerberoksen käyttöön (Kautto 2008). Monet Kerberosta käyttävät palvelut eivät käytä Kerberos-kirjastoja suoraan vaan ne käyttävät GSSAPI-rajapintaa, joka taas voi hyödyntää Kerberosta tai jotain muuta käytäjäntunnistusjärjestelmää.

GSSAPI on asiakas-palvelin järjestelmä, joka voi, kuten Kerberoskin, varmistaa käyttäjän tai palvelun identiteetin verkossa, validoida jokaisen välitetyn viestin verkossa ja osapuolten näin halutessaan salata kaiken viestinnän verkossa. RFC 4121 kuvaa Kerberoksen käyttöä GSSAPI:n kanssa. GSSAPI:n rajapintakutsut ovat ohjelmointikieliriippumattomia. GSSAPI on tuettuna monessa ohjelmointikielessä. GSSAPI-standardi C-ohjelmointikielelle löytyy RFC 2744 -dokumentista ja tuki Java-ohjelmointikielelle RFC 2853 -dokumentista. Linux-palveluista mm. SSH ja NFS tukevat GSSAPI-rajapintaa.

3 Network File System

Tiedostonjakopalvelimen tehtävä on jakaa käyttäjien tiedostoja lähiverkossa työasemien välillä eli mahdollistaa käyttäjien tiedostojen yhteiskäyttö. Tarve tiedostojen yhteiskäyttöön seuraa työn luonteesta ja tiettyjen ohjelmistojen toimivuuksien edellytyksistä. Tiedostonjakopalvelin sisältää hakemistopuun, jonka osia verkon muilla laitteilla, eli asiakkailla, on lupa liittää osaksi oman tiedostojärjestelmän hakemistopuuta (Izquierdo ym. 2004).

Tässä kappaleessa esitellään Sun Microsystems:n kehittämää Network File System -protokollaa. Aluksi käydään läpi hieman historiaa ja verkkoprotokollan kehitysvaiheita. Sitten esitellään NFS-protokollan toimintamekanismit niiltä osin, kuin se on tämän tutkimuksen kannalta olennaista. Luvun lopussa käydään läpi NFS-protokollan uusinta versiota ja sen Kerberosta hyväksi käyttävää tietoturvallista toteutusta.

3.1 Historia

Sun Microsystems kehitti NFS-protokollan 1980-luvun alussa. Se oli ensimmäisiä kaupallisia tiedostonjakoprotokollia markkinoilla. NFS-protokollan arkkitehtuuri on palvelin-asiakasmalli. NFS-protokollan ensimmäinen versio jäi Sun Microsystems:n sisäiseksi prototyypiksi. NFS-protokollan versio kaksi julkaistiin SunOS2 UNIX-käyttöjärjestelmän mukana vuonna 1984. Sun Microsystems:n NFS-protokolla lisensoitiin pian moniin UNIX-käyttöjärjestelmiin. NFS-protokollan toinen versio on RFC 1094. Vuosien saatossa protokollaan on tehty joitain korjauksia ja parannuksia ja vuonna 1996 siitä julkaistiin kolmas versio NFSv3. NFSv3 tuki muun muassa TCP-yhteyksiä ja suurempaa tiedoston kokoa. NFSv3 on viimeinen Sun Microsystems:n julkaisema versio NFS-protokollasta ja se on RFC 1813. Kolmannen version jälkeen protokollan kehitys on jatkunut IETF:n toimesta ja vuonna 2000 IETF julkaisi neljännen version NFS-protokollasta, joka poikkeaa monilta osin edeltäjistään (Kautto 2008). Tämä NFSv4-protokolla on RFC 7530.

Alun perin Sun Microsystems suunnitteli NFS-protokollan käyttöjärjestelmäriippumattomaksi tavaksi jakaa tiedostoja verkossa eri laitteiden välillä. Se oli tilaton, toimintavarma, lähiverkkoihin suunniteltu UDP/IP-yhteyden päälle rakennettu järjestelmä, joka saavutti suur-

ta suosiota erityisesti UNIX-käyttöjärjestelmien keskuudessa (Sadi 2016). Sun julkisti protokollan suunnitteluperiaatteet, jotta muut valmistajat ja akateeminen yhteisö voisivat kehittää omat ohjelmistonsa tukemaan NFS-protokollaa. Kolmekymmentä vuotta myöhemmin NFS-protokollasta on tullut de facto -standardi monessa käyttöjärjestelmässä (Izquierdo ym. 2004).

3.2 RPC, XDR ja Portmapper

NFS-protokolla perustuu Sun Microsystemsin kehittelemään Remote Procedure Call (RPC) -etäohjelmakutsuihin sekä Exernal Data Representation (XDR) -standardiin (Kautto 2008). Remote Procedure Call on nimensä mukaisesti etäohjelmakutsu. Järjestelmä mahdollistaa komennon suorittamisen toisessa koneessa (Thurlow 2009). External Data Representation on standardi tiedon koodaukseen ja tiedon rakenteen kuvaamiseen. Se on kehitetty tiedon siirtoon eri tietokonearkkitehtuurien välillä. RPC-etäohjelmakutsut ja NFS-protokolla käyttävät XDR-standardia välitettävän tiedon kuvaamiseen (Eisler 2006). Tästä eteenpäin käytän Remote Procedure Call -termistä sen lyhennettä RPC ja External Data Representation -standardista sen lyhennettä XDR.

RPC-etäohjelmakutsuja ovat esimerkiksi, avaa tiedosto, siirry hakemistoon, suorita komento palvelimella, avaa tiedosto ja kirjoita tiedostoon. Näitä kutsuja yhdistämällä voidaan luoda komentosarjoja, joilla työasemasta voidaan käskeä palvelimen suorittamaan haluttuja operaatiota (Thurlow 2009). RPC-etäohjelmakutsut voidaan välittää työasemasta palvelimelle esimerkiksi luotettavan TCP/IP- tai epäluotettavan UDP/IP-yhteyden avulla. Jos RPC-etäohjelmakutsu välitetään epäluotettavan UDP/IP-yhteyden avulla, pitää sovellusohjelmoijan huolehtia, että RPC-etäohjelmakutsu saapuu perille palvelimelle tai mitä tehdään, jos se ei saavu. Jos RPC-etäohjelmakutsu välitetään luotetun TCP/IP-yhteyden avulla, ei tätä työtä sovellusohjelmoijan tarvitse tehdä. RPC-etäohjelmakutsu ei ota kantaa käytettävään siirtoyhteyteen (Thurlow 2009).

Useat verkon palvelut, kuten vaikka http tai ssh palvelevat tietyssä TCP/UDP-portissa. RPC-etäohjelmakutsuille ei ole kiinnitetty yhtä porttia tai porttialuetta, vaan tilanne on hieman monimutkaisempi. RPC-etäohjelmakutsu käynnistyessään varaa palvelimelta TCP- ja/tai UDP-

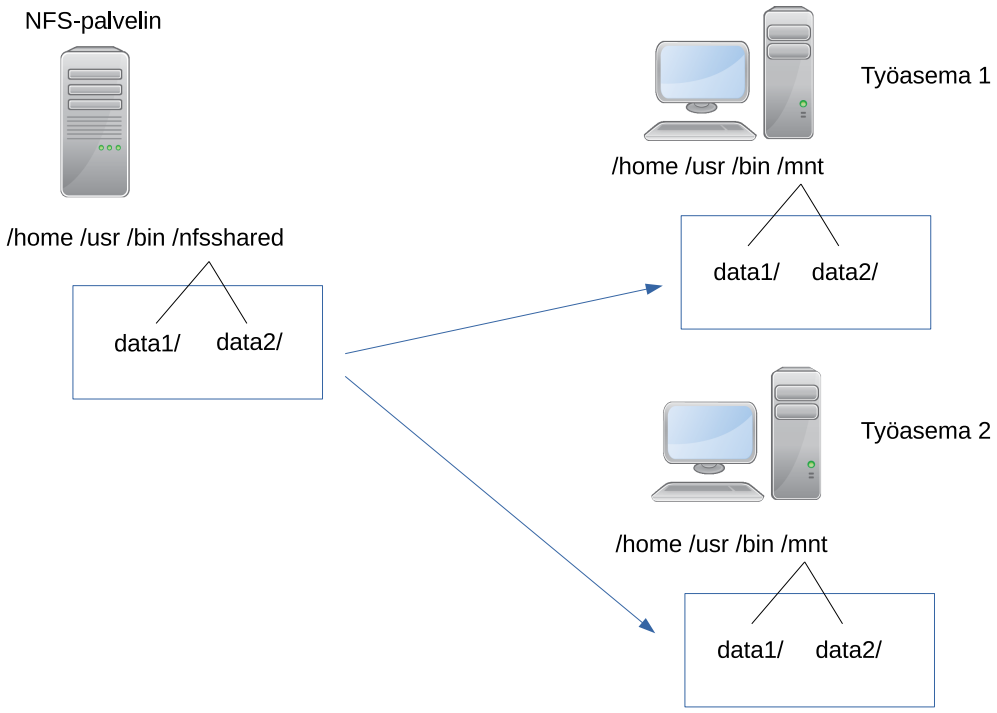
portin ja rekisteröi sen paikallisen tietokoneen portmapper-palveluun (portmapper tunnetaan uudemmissa Linux-käyttöjärjestelmissä nimellä rpcbind). Portmapper-palvelu palvelee asiakkaita määrätyssä TCP/UDP-portissa 111. Kun työaseman RPC-etäohjelmakutsua käyttävä ohjelma haluaa muodostaa yhteyden palvelimen RPC-palveluun, kysyy työasema palvelimen portmapper-palvelulta, missä TCP/UDP-portissa haluttu RPC-palvelu palvelee. Vastauksen saatuaan työasema osaa muodostaa yhteyden palvelimen haluttuun RPC-palveluun (Kautto 2008).

3.3 NFS-protokolla

Sun Microsystems suunnitteli NFS-protokollan tiedostojen jakamiseen lähiverkon laitteiden kesken. Suunnitteluperiaatteisiin kuului, että järjestelmän piti olla käyttäjille läpinäkyvä, vikasietoinen ja sen piti olla helposti implementoitavissa eri tietokonearkkitehtuureille ja käyttöjärjestelmäalustoille. Yksinkertaistettuna NFS-protokolla on ohjelma, joka on rakennettu RPC-etäohjelmakutsujen päälle.

NFS-protokollalla voidaan tuottaa lähiverkossa tiedostonjakopalvelut. Tiedostonjakopalvelimena toimii NFS-palvelin ja asiakkaana työasema. NFS-palvelimelle on asennettu NFS-palvelinohjelmisto ja työasemalle on asennettu NFS-asiakas-ohjelmisto. Työasemat ottavat yhteyden palvelimelle ja liittävät palvelimesta jaettuja hakemistorakenteita osaksi työaseman omaa hakemistopuuta. Näin tiedostonjakopalvelimella sijaitsevat tiedostot ovat työasemien yhteiskäytössä.

NFS-protokolla jakautuu kahteen osaan. Mount-protokollaan ja NFS-protokollaan (Levy ja Silberschatz 1990). Mount-protokollaa käytetään, kun asiakas (työasema) muodostaa ensimmäisen kerran yhteyden tiedostonjakopalvelimelle (NFS-palvelimelle). NFS-palvelimella sijaitsee exports-niminen tiedosto, jossa listataan, mitä NFS-palvelimen hakemistorakenteen osia voidaan jakaa eli exportoida millekin työasemalle kiinnitettäväksi eli mountattavaksi osaksi työaseman omaa hakemistorakennetta. Kuviossa 2 on esitetty tämä tilanne. Lisäksi NFS-palvelin ylläpitää listaa siitä, mitkä hakemistot palvelimelta on liitetty millekin työasemille. Näin NFS-palvelin voi ilmoittaa asiakkaille, jos palvelin esimerkiksi sammutetaan tai uudelleen käynnistetään. Koska NFS-protokolla on suunniteltu tilattomaksi, tämä lista



Kuvio 2. NFS-palvelimelta jaetut hakemistot data1 ja data2 mountattuna työasemiin.

on vain suuntaa antava. Se ei välttämättä esitä koko tilannetta tietyllä ajanhetkellä (Levy ja Silberschatz 1990).

NFS-protokolla jatkaa siitä, mihin Mount-protokollan suoritus päättyy. NFS-protokollalla työasema voi esimerkiksi listata NFS-palvelimen hakemistoja, siirtyä toisiin hakemistoihin, avata tai sulkea tiedostoja ja luoda tai muokata tiedostoja. Kaikki kommunikaatio työaseman ja NFS-palvelimen välillä tapahtuu RPC-etäohjelmakutsuilla, jotka välitetään lähiverkossa joko epäluotettavan UDP/IP-yhteyden, tai luotettavan TCP/IP-yhteyden avulla avulla.

3.4 NFS-protokolla ja tietoturva

NFS-protokollan vanhemmat versiot kaksi (NFSv2) ja kolme (NFSv3) sisältävät lukuisia tietoturvan kannalta ongelmallisia piirteitä. Ensinnäkään NFS-protokollassa ei ole luotettua käyttäjäntunnistamista. Protokolla tarjoaa kaksi käyttäjäntunnistusmenetelmää: ei ollenkaan käyttäjäntunnistusta tai käyttäjäntunnistuksen perustuen asiakkaan työaseman UID

(UserID) ja GID (GroupID) tietokantaan (Izquierdo ym. 2004). Linux-järjestelmissä käyttäjän identiteetin määrää käyttäjätunnus, käyttäjätunnuksen UID-numero ja käyttäjätunnuksen GID-numero. Käyttäjätunnus on yleensä aakkosista koostuva kirjainjoukko, UID- ja GID-numerot ovat positiivisia kokonaislukuja, joista UID-numero on käyttäjän identifioimiseen tarkoitettu henkilökohtainen numero ja GID-numero käyttäjän ensimmäisen ryhmän numero. Linux-järjestelmässä käyttäjä kuuluu vähintään yhteen ryhmään ja tämä ryhmä on käyttäjän ensimmäinen eli nk. primääriryhmä. Työaseman tietokantaan perustuva käyttäjätunnistus siis tarkoittaa sitä, että työasema ja NFS-palvelin jakavat saman UID/GID-tietokannan ja näillä UID/GID-määrityksillä säädellään, mihin tiedostoihin ja hakemistoihin käyttäjällä on lupa päästä käsiksi. Jos työasemalla käyttäjä "matti"lisätään ryhmään "talous", pääsee käyttäjä "matti"kaikkiin ryhmän "talous"omistamiin tiedostoihin ja hakemistoihin. Jos käyttäjä "matti"on työaseman pääkäyttäjä, voi "matti"itse lisätä itsensä mihin tahansa NFS-palvelimen ryhmään ja näin päästä mihin tahansa tiedostoihin tai hakemistoihin käsiksi. NFS-palvelimessa ei ole mitään mekaniikkaa estää työaseman käyttäjän pääsemästä käsiksi mihin tahansa jaettuun hakemistoon, koska UID/GID-tarkistus tehdään työaseman päässä. Lisäksi NFS-protokollan yhteys ei ole salattu. Potentiaalinen hyökkääjä voi kuunnella NFS-protokollan liikennettä lähiverkossa ja saada selville, mitä UID/GID-yhdistelmiä NFS-palvelin käyttää ja sitä kautta saada pääsy NFS-palvelimen tiedostoihin ja hakemistoihin (Izquierdo ym. 2004). Jos hyökkääjä pääsee käsiksi työasemaan ja onnistuu saamaan pääkäyttäjän oikeudet, hyökkääjä voi luoda käyttäjätunnuksen "sirpa"ja lisätä "sirpa"kaikkiin NFS-palvelimen ryhmiin ja näin päästä mihin tahansa NFS-palvelimen tiedostoihin käsiksi.

Toinen ongelma NFS-protokollassa on se, että se luottaa NFS-palvelimen exports-tiedostossa oleviin tietoihin työasemasta (Bhat ja Quadri 2013). Jos potentiaalinen hyökkääjä varastaa lähiverkossa olevan työaseman IP-osoitteen ja DNS-nimen, voi hyökkääjä esiintyä tänä työasemana ja liittää eli mountata NFS-palvelimen resursseja. NFS-palvelin ei tee mitään tarkistuksia liittämisprosessissa. NFS-palvelimelle riittää, että työasema todistaa identiteettinsä IP-osoitteensa ja DNS-nimensä perusteella.

NFS-protokolla on rakenteeltaan kokoelma RPC-kutsuja, joiden avulla palvelin ja asiakas keskustelevat lähiverkossa (Bhat ja Quadri 2013). Suurin tietoturvaongelma NFS-protokollassa on, että RPC-etäohjelmakutsut eivät sisällä sellaisia tietoturvan kannalta olennaisia var-

mennuksia tai tarkistuksia, joita pidämme 2010-luvulla itsestään selvinä. Kun asiakas ottaa ensimmäisen kerran yhteyttä palvelimelle RPC-etäohjelmakutsulla, ei asiakkaan identiteettiä varmenneta millään lailla. Lisäksi sekä yhteyden muodostamisvaiheessa, että myöhemmin asiakkaan ja palvelimen välisessä viestien välityksessä ei RPC-etäohjelmakutsuja salata. Lähiverkkoa kuuntelemalla hyökkääjä voi hyödyntää RPC-etäohjelmakutsuista saamaansa informaatiota omiin tarkoituksiinsa.

Yhdeksi ongelmaksi muodostuu myös organisaation palomuuri. Koska NFS-protokolla tarvitsee RPC-etäohjelmakutsujen takia avukseen portmapper-palvelua ja portmapper-palvelu taas arpoo RPC-etäohjelmakutsuille TCP/UDP-portteja satunnaisesti, on NFS-palvelua vaikea käyttää palomuurien kanssa. Palomuuri ei voi tietää, mitä portteja portmapperille pitäisi olla auki. Näistä tietoturvaongelmista johtuen NFS-protokollaa on jatkokehitetty ja ongelmia on korjattu ja joitain ongelmia on kierretty NFS-protokollan neljännessä (NFsv4) versiossa.

3.5 NFSv4-protokolla

NFSv4-protokolla eli NFS-protokollan neljäs versio on jatkokehitetty Sun Microsystems:n alkuperäisestä NFS-protokollasta ja sen versioista kaksi ja kolme. Versiossa neljä on pyritty säilyttämään NFS-protokollan suunnitteluperiaatteita, kuten hyvä suorituskyky, nopea virheistä toipuminen, protokollan yksinkertaisuus, ja protokollan siirrettävyys eri käyttöjärjestelmäalustoille. NFSv4-protokollassa on lisäksi otettu huomioon aikaisemmin protokollaa vaivanneet tietoturvaongelmat ja protokollan suorituskykyä on myös parannettu.

3.5.1 Delegointi

Yksi uusi ominaisuus NFSv4-protokollassa on tuki tiedostojen delegoinnille. Delegoinnin tarkoituksena on vähentää verkon liikennettä ja sitä kautta lisätä NFS-protokollan suorituskykyä. Kuvitellaan tilanne, jossa käyttäjä haluaa käsitellä tiedostoa, joka sijaitsee NFS-palvelimella. Delegoinnissa työasema lataa NFS-palvelimelta tiedoston paikallisesti omaan välimuistiinsa. Palvelimella olevan tiedoston sijaan työasema siirtyy käsittelemään tiedoston paikallista kopioita. Tämä vähentää verkkoliikennettä ja nopeuttaa tiedoston käsittelyä. NFS-palvelin siis delegoi tiedoston käsittelyoikeudet väliaikaisesti työasemalle (Sadi 2016).

Delegointi voidaan tarvittaessa purkaa. Tilanteessa, jossa toinen käyttäjä haluaa käsitellä samaa tiedostoa, purkaa NFS-palvelin delegaation ensimmäisen käyttäjän työaseman kanssa ja tiedoston käsittely jatkuu normaalisti NFS-protokollan yli palvelimella ilman delegaatiota. Delegaatio toimii parhaiten tilanteessa, jossa vain yksi työasema käyttää NFS-palvelimen jakoa tai monta työasemaa käyttää NFS-palvelimen jakoa, mutta NFS-palvelimen jaolle on määritelty vain luku -tyyppiset oikeudet. Tässäkin tilanteessa ongelmana on se, että työasemalla ei välttämättä ole käytössään tiedoston uusinta versiota vaan työasemalla on käytössään vain se versio, jonka NFS-palvelin on delegoinut työaseman välimuistiin (Sadi 2016).

Työasema ei pyydä NFS-palvelimelta delegaatiota tiedostolle, vaan NFS-palvelin päättää, milloin delegointi voidaan toteuttaa. NFS-palvelin voi esimerkiksi antaa usealle työasemalle luku-delegaation, mutta kirjoitus-delegaation vain yhdelle työasemalle kerrallaan konfliktien välttämiseksi (Sadi 2016).

3.5.2 RPCSEC_GSS

Yksi suurimmista NFSv4-protokollan eroista vanhempiin NFS-protokollan versioihin on mahdollisuus käyttää Kerberosta NFS-protokollan kanssa. NFSv4-protokollan kerberoiminen tarkoittaa NFS-protokollan RPC-kutsujen kerberoimista. Tähän tarkoitukseen NFSv4-protokolla käyttää RPCSEC_GSS-protokollaa, joka on RFC 5403.

RPCSEC_GSS-protokolla mahdollistaa vahvan käyttäjätunnistuksen RPC-etäohjelmakutsuja hyödyntäville protokollille antamalla RPC-etäohjelmakutsuille pääsyn GSS-API-rajapintaan (Eisler 2009). Mikäli NFSv4-protokollan kanssa halutaan käyttää Kerberosta, konfiguroidaan NFS-palvelin ja NFS-asiakastyöasema käyttämään RPCSEC_GSS-protokollaa. Koska GSS-API tukee myös tiedon salausta ja tiedon eheyden varmistamista, voidaan NFSv4-protokollan kanssa ottaa myös nämä ominaisuudet käyttöön.

3.5.3 NFSv4-protokolla ja palomuuri

NFS-protokollan versiot kaksi ja kolme ovat tilattomia ja tarvittaessa lisäksi yhteydettömiä. Vanhempia versioita on mahdollista käyttää sekä UDP/IP-, että TCP/IP-yhteyden kanssa. NFS-protokolla sisältää lukuisan määrän portteja, joita portmapper-palvelu varaa. NFSv4-

protokolla on tilallinen ja yhteydellinen protokolla, joka toimii vain TCP/IP-yhteyden avulla. Lisäksi kaikki yhteydet on rajattu yhteen TCP-porttiin 2049. NFSv4-protokolla tekee portmapper-palvelusta tarpeettoman ja NFSv4-protokolla toimii hyvin palomuurin takana, sillä sekä työasema, että NFS-palvelin liikennöivät yhden tiedossa olevan TCP-yhteyden avulla (Cheng ym. 2015).

Näiden ominaisuuksien lisäksi on syytä mainita, että NFSv4-protokolla pakottaa käyttämään UTF-8 Unicode merkistöstandardia. NFSv4-protokolla julkaistiin IETF:n toimesta vuonna 2000. Protokolla on kuitenkin jatkuvan kehityksen kohteena. Tätä tutkimusta kirjoittaessa talvella 2018 NFSv4-protokollasta on julkaistu jo kolme täydentävää versiota NFSv4.0, NFSv4.1 ja NFSv4.2. Kukin täydentävä versio on tuonut NFSv4-protokollaan uusia ominaisuuksia.

3.5.4 Hienojakoiset käyttöoikeudet

Perinteisessä UNIX-käyttöjärjestelmässä tiedostot on tallennettu hakemistoista koostuvaan puumaiseen hiearkiseen rakenteeseen. Puun juurena on nk. juurihakemisto ja juurihakemisto sisältää lisää hakemistoja ja tiedostoja. UNIX-käyttöjärjestelmässä jokainen tiedostojärjestelmään tallennettu objekti on tiedosto ja jokaisella tiedostolla on käyttäjäoikeuksia. Käyttäjäoikeudet koskevat siis sekä tiedostoja, ajettavia binäärejä, UNIX-soketteja, putkia, hakemistoja, symbolisia linkkejä ja kovia linkkejä. Jokaiselle tiedostolle on määritelty kolme oikeusluokkaa: tiedoston omistajan oikeudet (User), tiedoston ryhmän oikeudet (Group) ja muiden järjestelmän käyttäjien oikeudet (Other). Näillä kolmella oikeusluokalla on kolme käyttöoikeusattribuuttia: lupa lukea tiedostoa (r), lupa kirjoittaa tiedostoon (w) ja lupa suorittaa tiedosto (x) (Mellander 2002). Yleensä tiedoston luoja on sen omistaja ja tiedoston luoja voi määritellä tiedostolleen muita käyttöoikeuksia. Näiden perinteisten tiedosto-oikeuksien ongelmaksi tulee se, että tiedostolla voi olla vain yksi ryhmä ja vain yksi omistaja. Jos käyttäjä matti kuuluu ryhmään talous, voi käyttäjä matti luoda tiedoston ostot.xls ja antaa ryhmälle talous luku ja kirjoitusoikeudet tiedostoon. Käyttäjä matti ei voi antaa myös ryhmälle johto lukuoikeuksia ostot.xls-tiedostoon tai ryhmälle myynti sekä luku-, että kirjoitusoikeuksia samaan tiedostoon, sillä perinteinen UNIX-käyttöjärjestelmä ei tue näin monimutkaista oikeusrakennetta.

NFSv4-protokolla korjaa tätä ongelmaa esittelemällä Access Contol List (ACL)-rakenteen tiedoston oikeuksien määrittelemiseen. NFSv4-protokolla tukee hienojakoisempaa tiedosto-oikeusrakennetta, jossa jokaisella tiedostolla on ACL-lista. ACL-lista koostuu Access Control Entry (ACE) -säännöistä (Haynes ja Noveck 2015). Perinteisellä UNIX-käyttöjärjestelmän tiedostolla on User, Group ja Other käyttöoikeusluokat ja näillä luokille on määritelty lukuoikeus, kirjoitusoikeus ja suoritusoikeus tiedostoon. NFSv4-protokollan ACL-lista sisältää ACE-sääntöjä, joilla voidaan määritellä monta ryhmää ja monta omistajaa ja jakaa näille oikeuksia huomattavasti monipuolisemmin. NFSv4 ACL oikeudet tukevat myös oikeuksien perintää. Jos jollain hakemistolla on määrätyt ACE-säännöt, niin hakemiston sisälle luodut tiedostot ja alihakemistot voivat tarvittaessa periä (tai olla perimättä) ylähakemiston oikeudet. Järjestelmä tukee myös oikeuksia kieltäviä sääntöjä, eli sääntöjoukkoon voidaan määritellä tunnuksia tai ryhmiä joilla ei ole oikeuksia tiedostoon tai hakemistoon. Kuvaan tilannetta seuraavaksi esimerkin avulla.

Linux-komennolla `ls -la` voidaan listata tiedoston perinteiset UNIX-käyttöjärjestelmän oikeudet. Tuloste voisi näyttää vaikka seuraavalta:

```
[tunnus@kone ~]$ ls -la tiedosto.txt
-rw-------. 1 tunnus ryhma 0 Mar 21 19:34 tiedosto.txt
```

Tässä tunnus-käyttäjätunnuksella on rw-oikeudet, eli luku- ja kirjoitusoikeudet tiedostoon tiedosto.txt. Ryhmällä ryhma ja ryhmällä other ei ole mitään oikeuksia tiedostoon. NFSv4-protokollalla toteutetussa jaossa käyttäjäoikeuksia ei voi listata tällä komennolla, sillä `ls`-komento ei osaa esittää tiedoston käyttöoikeuksia. NFSv4-ympäristöön tallennetun tiedoston käyttöoikeudet voidaan listata komennolla `nfs4_getfacl`. Komento tulostaa saman tiedoston oikeudet seuraavasti:

```
[tunnus@kone ~]$ nfs4_getfacl tiedosto.txt
A::tunnus@DOMAIN:rwadtTnNcCoy
```

Tiedostolla voi olla myös enemmän omistajia ja ryhmiä ja näillä voi olla erilaisia oikeuksia tiedostoon:

```
[tunnus@kone ~]$ nfs4_getfacl tiedosto2.txt
```

```
A::tunnus@DOMAIN:rwadtTnNcCoy
A::tunnus2@DOMAIN:watTNcCy
A:g:ryhma1:rwaxtTnNcCy
A:g:ryhma2:rwadxtTnNcCoy
```

Lisää tietoa NFSv4-protokollan monipuolisista tiedostojen oikeuksista löytyy Linux-työasemasta komennolla `man nfs4_acl`.

4 Microsoft Active Directory

Lähiverkossa sijaitsevien työasemien, palvelinten, tulostimien ja käyttäjien keskitetty hallinta on haastavaa. Kun kone-, ja käyttäjämassat kasvavat, kasvaa hallittavien objektien määrä helposti liian suureksi. Keskitettyjen lähiverkkojen hallintaan on kehitetty vuosien saatossa erilaisia hakemistopalveluita jäsentämään lähiverkkoja. Hakemistopalvelut helpottavat käyttäjiä löytämään lähiverkon palveluita ja ylläpitoa hallitsemaan niitä. Modernit Windows-lähiverkot sisältävät usein Microsoftin kehittämän hakemistopalvelun Microsoft Active Directoryn (Tankard 2012).

Tässä luvussa esitellään yleisellä tasolla Microsoft Active Directoryn piirteitä ja toiminnallisuuksia niiltä osin, kuin se on tämän tutkimuksen kannalta olennaista. Microsoft Active Directory on hyvin laaja kokonaisuus lähiverkon palveluita sekä lähiverkon hallintaan suunniteltuja työkaluja. Tässä luvussa esitellään Microsoft Active Directory -hakemistopalvelua vain Kerberoksen näkökulmasta.

4.1 Historia

Microsoft kehitti Active Directoryn 1990-luvulla ja se julkaistiin osana Windows 2000 -käyttöjärjestelmää (Paddock 2003). Active Directory -hakemistopalvelu on syntynyt tarpeesta koota lähiverkon eri palvelut, kuten tulostuspalvelut, tiedostonjakopalvelut, sähköpostipalvelut, työasemat, käyttäjätunnukset ja ryhmät yhdeksi hallittavaksi kokonaisuudeksi. Microsoft ei keksinyt Active Directory -hakemistopalvelua tyhjästä. Se perustuu jo aiemmin julkaistuun Windows NT4 -hakemistopalveluun, mutta Microsoft Active Directory on edeltäjäänsä paljon laajempi ja monipuolisempi kokonaisuus (Pittaway 1999).

Ensimmäinen versio Microsoft Active Directorystä julkaistiin Windows 2000 -käyttöjärjestelmän osana. Se on kehittynyt Windows-käyttöjärjestelmän mukana ja kun Microsoftin tuoteperheeseen on tullut uusia ominaisuuksia, myös Microsoft Active Directoryyn on tullut näitä ominaisuuksia vastaavia hallintatyökaluja. Tätä tutkimusta kirjoittaessa talvella 2018 uusin versio Microsoft Active Directory -hakemistopalvelusta sisältyy Windows 2016 Server -käyttöjärjestelmään.

4.2 Tietokanta ja palvelut

Microsoft Active Directory -hakemistopalvelu voidaan ajatella olevan yksi iso LDAP-tietokanta, joka sisältää kaiken lähiverkon rakenteesta lähtien lähiverkon laitteiden DNS-nimistä, käyttäjistä, ryhmistä, tietokoneista, tiedostonjakopalveluista, tulostimista, sertifikaateista, palomuureista, käyttöoikeuksista, sähköpostin hallintatyökaluista ja niin edelleen. Microsoft Active Directory jakautuu lähiverkon eri palveluiksi, kuten esimerkiksi Kerberos-käyttäjäntunnistuspalveluksi, Internet nimipalveluksi (DNS, Domain Name Service) ja LDAP-hakemistopalveluksi (LDAP, Lightweight Directory Access Protocol) (Microsoft 2014b).

Microsoft Active Directory -hakemistopalvelun ydin on Domain Controller -palvelin. Kerberoksen näkökulmasta Domain Controlller -palvelin toimii lähiverkossa myös avaintenjakelukeskuksena roolissa(Pittaway 1999). Domain Controllerit sisältävät Kerberos REALM:n prinsipaalit sekä Kerberos-tietokannan. Domain Controller -palvelimet tarjoavat Kerberos-käyttäjäntunnistuspalvelun lähiverkossa.

4.3 Metsä ja toimialue

Microsoft Active Directory ryhmittelee objekteja hiearkisiin loogisiin kokonaisuuksiin. Korkeimmalla hierarkiassa on metsä. Metsä on säiliö, joka sisältää toimialueita. Toimialue on puumainen säiliö, joka sisältää objekteja. Objektit ovat esimerkiksi käyttäjätilejä, tulostimia, tietokonetilejä ja organisaatioyksiköitä. Esimerkki metsästä voisi olla kansainvälinen yritys. Esimerkki toimialueesta voisi olla tämän kansainvälisen yrityksen Euroopan tai vaikka Helsingin osasto. Toimialueesta käytetään usein sen englanninkielistä nimeä Domain.

Toimialue kasaa yhteen objektit puumaiseksi rakenteeksi. Toimialueen objektit ovat konkreettisia asioita, kuten käyttäjätunnuksia, tulostimia ja tietokonetilejä. Tällaisten konkreettisten objektien lisäksi toimialue voi sisältää objekteja, joiden tehtävänä on varastoida toisia objekteja. Tällaisia säiliöobjekteja kutsutaan organisaatioyksiköksi. Organisaatioyksiköt voivat sisältää muita organisaatioyksiköitä ja muita toimialueen objekteja. Toimialueen organisaatioyksikkö voidaan ajatella olevan analogia hakemistolle tiedostojärjestelmässä. Organisaatioyksikkö kasaa samankaltaisia objekteja ryhmiksi ja näitä ryhmiä voidaan hallita kokonaisuuksina. Organisaatioyksikön objekteille voidaan luoda sääntöjä ja toimialueen si-

sällä voidaan määritellä käyttäjät tai käyttäjäryhmät, joilla on oikeus muuttaa organisaatioyksikön ominaisuuksia. Organisaatioyksiköstä käytetään usein sen englanninkielisestä nimestä johdettua lyhennettä OU eli Organizational Unit (Microsoft 2014b).

Kerberos on sisäänrakennettu Microsoft Active Directory -hakemistopalveluun. Kerberoksen toiminnan kannalta voidaan ajatella, että Kerberos REALM eli Kerberos toimialue on sama asia, kuin Microsoft Active Directory -toimialue (Microsoft 2014b).

4.4 Objekti

Microsft Active Directory -hakemistopalvelun perusyksikkö on objekti ja sekin on säiliö. Objekti rakentuu attribuuteista ja objekti on säiliö objektin attribuuttien arvoja. Kun toimialueeseen luodaan uusi objekti, objektin attribuuteille annetaan erilaisia arvoja. Esimerkiksi käyttäjätunnus-objektia luotaessa käyttäjätunnus-objektin attribuuteille annetaan arvoja, kuten käyttäjätunnus, sukunimi, etunimi, sähköpostiosoite ja niin edelleen. Osa arvoista määritellään objektia luotaessa, toiset luodaan automaattisesti, eikä niihin voi vaikuttaa. Toimialueen pakottamia attribuutteja ovat Globally Unique Identifier (GUID) ja Security Identifier (SID) (Microsoft 2014a).

GUID on 128-bittinen numerosarja, jonka toimialue luo objektille objektin luontivaiheessa. Objektin GUID-attribuuttia ei voi luonnin jälkeen muuttaa. Microsoft Active Directory käyttää GUID-numeroa vain sisäisesti. Kaikilla objekteilla on aina GUID-numero. GUID-numeron lisäksi muun muassa käyttäjätunnus-objekteille ja tietokonetili-objekteille luodaan SID-attribuuttiin henkilökohtainen SID-numero. SID-numeron omaavat objektit voivat osallistua käyttäjäntunnistusprosessiin ja tällaisilla objekteilla voi olla myös käyttöoikeuksia toimialueessa. Esimerkiksi toimialueella, tietokonetilillä, ryhmällä ja käyttäjätilillä on aina oma henkilökohtainen SID-numero. SID-numero on toimalueriippuvainen ja voi muuttua jos objekti siirretään esimerkiksi toimialueesta toiseen saman metsän sisällä (Microsoft 2014a).

4.5 Objektin nimi

Toimialueen objekteihin viitataan objektien nimillä. Microsoft Active Directory -hakemistopalvelun objekteihin voi viitata sekä objektin LDAP-nimellä, että nk. logon-nimellä (Microsoft 2014a). Kuvitellaan, että käyttäjä Matti on töissä yrityksessä Firma. Firman Microsoft Active Directory -toimialueen nimi on firma.com. Kuvitellaan, että Firma jakaantuu organisaatioyksiköiksi johto, markkinointi, palkanlasku. Lisäksi kuvitellaan, että käyttäjä Matti on töissä markkinoinnissa. Käyttäjän Matti LDAP-nimi firma.com-toimialueessa olisi silloin

```
cn=matti,ou=Markkinointi,dc=firma,dc=com
```

Yksinkertainen esimerkki logon-nimestä on käyttäjätunnus tai tietokoneen nimi (Microsoft 2014a). Äskeisen esimerkin mukaisesti käyttäjän Matti logon-nimi olisi matti. Käyttäjän LDAP-nimi voi muuttua. Jos Matti ylennetään Firma-yrityksen johtoon, siirrettäisiin käyttäjän objekti organisaatioyksikköön johto. Käyttäjän Matti uusi LDAP-nimi on silloin

```
cn=matti,ou=Johto,dc=firma,dc=com
```

Myös objektin logon-nimi voidaan vaihtaa. Samoin objektin SID-numero voi vaihtua, jos objekti siirretään toimialueesta toiseen saman metsän sisällä. Vain objektin GUID-numero pysyy muuttumattomana objektin elinkaaren ajan. Microsoft Active Directory -hakemistopalvelussa logon-nimeä käytetään Kerberos-käyttäjäntunnistuspalveluiden kanssa. (Microsoft 2014a). Käyttäjä Matti käyttää logon-nimeä matti kirjautuessaan esimerkiksi työasemaansa.

Lähiverkon tietokoneita varten Microsoft Active Directory -hakemistopalveluun on varattu oma objekti nimeltään tietokonetili. Tietokonetili koostuu GUID ja SID -numeroista, LDAP-nimestä, logon-nimestä, tietokoneen DNS-tiedoista sekä palveluprinsipaaleista (engl. Service Principal Name, SPN). Palveluprinsipaali on attribuuttisäiliö, jota käytetään Kerberoksen kanssa. Yhdellä tietokonetilillä voi olla monta palveluprinsipaalia. Palveluprinsipaalin avulla työasema tai palvelin todistaa identiteettinsä Kerberos-avaintenjakelukeskukselle.

5 Kerberoitu NFSv4-toteutus Jyväskylän yliopistossa

Tämän tutkimuksen tarkoituksena on esitellä, miten Kerberoitu NFSv4-protokolla on saatu toimimaan tuotantoympäristössä joka koostuu kaupallisesta Kerberoksesta, kaupallisesta NFSv4-palvelimesta sekä näitä hyödyntävistä Linux-työasemista. Jyväskylän yliopiston lähiverkko on tyypillinen korkeakouluverkko, johon kuka tahansa voi kytkeytyä omalla päätelaitteellaan. Tällainen ympäristö on avoin lähiverkko ja siellä tarvitaan vahvaa käyttäjäntunnistamista ja tiedon salausta.

Tässä luvussa esitellään, miten Microsoft Active Directory -hakemistopalvelua hyödynnetään Linux-työasemien käyttäjäntunnistuksessa ja miten kaupallinen NFSv4-palvelin toimii Microsoft Active Directory Kerberoksen kanssa ja miten kerberoitu NFSv4 -protokolla toimii Linux-työaseman kanssa.

5.1 Jyväskylän yliopiston toimialue AD.JYU.FI

Jyväskylän yliopiston Microsft Active Directory -hakemistopalvelussa ei varsinaisesti hyödynnetä metsän käsitettä. Jyväskylän yliopistossa on vain yksi toimialue ja sen nimi on ad.jyu.fi. Toimialue sisältää kaikki yliopiston käyttäjät, ryhmät, tietokonetilit mukaanlukien työasemat ja palvelimet, sekä joukon muita objekteja.

Linux-työaseman kannalta kerberoitu NFSv4 -protokolla toimii vain, jos NFS-palvelinta vastaava tietokonetili on määritelty toimialueeseen, Linux-työasemaa vastaava tietokonetili on määritelty toimialueeseen, ja palvelua Linux-työasemassa käyttävä loppukäyttäjä on määritelty toimialueeseen.

5.2 Jyväskylän yliopiston työasemaympäristö

Tässä tutkielmassa termillä työasema tarkoitetaan käyttäjän henkilökohtaista tietokonetta. Työasema voi olla pöytäkone tai kannettava tietokone. Kannettavat ja pöytäkoneet saavat asennuspalvelimelta saman levykuvan, jonka mukaan työasemat asennetaan. Jyväskylän yliopiston työasemaympäristö koostuu noin 5000 Windows-työasemasta, noin 400 Linux-työ-

asemasta ja noin 400 macOS-työasemasta. Työasemat ovat keskitetysti ylläpidetty It-palveluiden toimesta. It-palveluiden vastuulla on työasemien keskitetty asentaminen, asiakaspalvelu ja käyttöopastus, ohjelmistojen levitys, tietoturvasta ja päivityksistä huolehtiminen sekä huollon koordinointi.

Jyväskylän yliopiston Linux-työaseman käyttöjärjestelmä on tätä tutkimusta kirjoittaessa talvella 2018 RedHat Enterprise Linux 7.4. Linux-työasemia hallitaan Red Hat Satellite 6.2 Server -tuotteella. Red Hat Satellite tarjoaa ylläpidolle työasemien ja palvelinten keskitetyt asennus- ja päivityspalvelut, auditointipalvelut, etäkomentojen suorituspalvelut sekä työasemien ja palvelinten konfiguraatioiden hallintapalvelut.

5.3 Jyväskylän yliopiston NFS-palvelut

Tiedostonjakopalveluita Jyväskylän yliopistossa tarjoaa EMC VNX5700 Unified Storage. EMC VNX5700 on multiprotokolla Block- ja NAS-järjestelmä eli se tukee sekä Microsoftin kehittämää Windows-järjestelmien tukemaa CIFS-protokollaa (CIFS, Common Internet Filesystem), että Linux-järjestelmien tukemaa NFS-protokollaa. Lisäksi EMC VNX5700 Unified Storage tarjoaa raakaa kovalevypintapalvelua (FC, Fibre Channel) SAN-verkkoon (SAN, Storage Area Network) kytketyille palvelimille. Seuraavaksi esitellään, miten kerberoitu NFSv4-protokolla on konfiguroitu EMC VNX5700 Unified Storage NAS -järjestelmään.

EMC VNX5700 Unified Storage on Jyväskylän yliopiston konfiguraatiossa NFS-palvelin, joka tarjoaa kerberoidulla NFSv4-protokollalla tiedostonjakopalveluita Jyväskylän yliopiston Linux-työasemille. Kuten missä tahansa kerberoitua NFSv4-protokollaa tukevassa palvelimessa, NFS-palvelun tulee olla käynnistetty, palvelun tulee tukea NFSv4-protokollaa ja sen tulee jakaa yhteinen salaisuus avaintenjakelukeskuksen kanssa. Toisin sanoen EMC VNX5700 Unified Storage NAS-järjestelmälle tulee olla luotuna toimialueen sopivaan organisaatioyksikköön tietokonetili, jossa on etukäteen neuvoteltuna palveluprinsipaali NFSv4-palvelulle.

5.4 Konfiguraatiot Linux-työasemassa

Jyväskylän yliopiston Linux-työasemat konfiguroidaan automaattisesti asennuksen yhteydessä. Linux-työasema tuntee käyttäjän, Kerberos-palvelut verkossa ja työasema jakaa tarvittavan NFS-palveluprinsipaalin Kerberos-palveluiden kanssa. Työasemalla on tieto, missä lähiverkossa sijaitsevat nimipalvelut ja aikapalvelut. Työasema tietää myös, missä lähiverkossa sijaitsee NFS-palvelut ja erityisesti kerberoidut NFSv4 -palvelut.

5.4.1 Aikapalvelut ja nimipalvelut

Työaseman DNS-tiedot pitää olla oikein määritelty. Jyväskylän yliopiston Linux-työasemat ovat konfiguroitu päivittämään DNS-tiedot lähiverkosta DHCP-palvelun avulla automaattisesti. Ohitan testiympäristön DHCP-asetukset ja DNS-asetukset. Totean vain, että ne tulevat Linux-työasemaan automaattisesti lähiverkosta.

Kerberos on aikariippuvainen palvelu. Työaseman kellon pitää olla oikeassa ajassa. Työaseman kelloa ylläpitää NTP-palvelu (NTP, Network Time Protocol). NTP on määritelty seuraavasti:

```
[root@test-ws ~]# cat /etc/ntp.conf
disable monitor

# Permit time synchronization with our time source, but do not
# permit the source to query or modify the service on this system.
restrict default kod nomodify notrap nopeer noquery
restrict -6 default kod nomodify notrap nopeer noquery
restrict 127.0.0.1
restrict -6 ::1

# Set up servers for ntpd with next options:
# server - IP address or DNS name of upstream NTP server
# iburst - allow send sync packages faster if upstream unavailable
# prefer - select preferrable server
# minpoll - set minimal update frequency
# maxpoll - set maximal update frequency
server ntp1.jyu.fi
```

```
server ntp1.jyu.fi
server ntp1.jyu.fi

# Driftfile.
driftfile /var/lib/ntp/drift
[root@test-ws ~]#
```

Aikapalvelimina käytetään siis ntp1.jyu.fi, ntp2.jyu.fi ja ntp3.jyu.fi -palvelimia. On tärkeää, että koko kerberoitu ympäristö käyttää samoja aikapalvelimia. Kuvitellaan tilanne, jossa työasema käyttäisi sisäverkon aikapalvelimia ja sovelluspalvelin ulkoverkon aikapalvelimia. Jos sisäverkon ja ulkoverkon välinen linkki katkeaa, toimii työasemissa edelleen kello ja se käy "sisäverkon aikaa". Sovelluspalvelin, joka käyttää ulkoverkon aikapalvelimia, ei tässä tilanteessa voi enää päivittää omaa kelloaan ja sovelluspalvelimen kello voi alkaa edistää tai jätättää. Kerberos on aikariippuvainen järjestelmä. Kun sovelluspalvelimen kello on riittävän eri ajassa työasemien kelloon suhteutettuna, ei työasemat voi enää käyttää sovelluspalvelun palvelua. Kerberos kieltää yhteydenotot sovelluspalvelimelle aikaristiriidan takia.

5.4.2 Linux-työaseman NFS-palvelut

Seuraavassa on listattu Linux-työasemassa käynnissä olevat käyttöjärjestelmän palvelut:

```
[root@test-ws ~]# systemctl list-unit-files --type=
  service | grep enabled
accounts-daemon.service                       enabled
atd.service                                   enabled
auditd.service                                enabled
autofs.service                                enabled
autovt@.service                               enabled
bluetooth.service                             enabled
crond.service                                 enabled
cups.service                                  enabled
dbus-org.bluez.service                        enabled
dbus-org.freedesktop.NetworkManager.service   enabled
dbus-org.freedesktop.nm-dispatcher.service    enabled
display-manager.service                       enabled
gdm.service                                   enabled
```

```
getty@.service                                enabled
goferd.service                                enabled
initial-setup-reconfiguration.service         enabled
iptables.service                              enabled
irqbalance.service                            enabled
iscsi.service                                 enabled
ksm.service                                   enabled
ksmtuned.service                              enabled
lvm2-monitor.service                          enabled
microcode.service                             enabled
multipathd.service                            enabled
netcf-transaction.service                     enabled
NetworkManager-dispatcher.service             enabled
NetworkManager.service                        enabled
ntpd.service                                  enabled
postfix.service                               enabled
puppet.service                                enabled
puppetagent.service                           enabled
rhsmcertd.service                             enabled
rsyslog.service                               enabled
rtkit-daemon.service                          enabled
spice-vdagentd.service                        enabled
sshd.service                                  enabled
sysstat.service                               enabled
systemd-readahead-collect.service             enabled
systemd-readahead-drop.service                enabled
systemd-readahead-replay.service              enabled
tuned.service                                 enabled
```

Kuten listasta on nähtävissä, työaseman NFS-asiakkaan palveluita ei ole oletuksena käyttöjärjestelmässä päällä. Palvelut käynnistyvät tarvittaessa. Toisin, kuin monissa Linux-jakeluissa, Red Hat Enterprise Linux 7.4 -jakelussa käyttäjän tai ylläpitäjän ei tarvitse huolehtia käynnistyvistä NFS-palveluista työasemassa (Navrátil ym. 2017, luku 8.3). Työasema neuvottelee automaattisesti NFS-palvelimen kanssa protokollan versiosta ja tietoturvamäärityksistä ja käynnistää tarvittavat NFS-palvelut, kun mount-komento suoritetaan. Linux-työasemasta pitää löytyä rpm-paketti nfs-utils, joka sisältää tarvittavat ohjelmistot ja konfigu-

raatiotiedostot NFS-palveluiden käyttämiseen. NFS-protokollan vanhemmat versiot (eli versiot kaksi ja kolme) tarvitsevat lock.d ja stat.d -palvelut tiedostojen lukituksien hallitsemiseen ja palvelimelta tulevien viestien välitykseen. Lisäksi Linux-työasema tarvitsee portmapper-ohjelman RPC-etäohjelmakutsujen varaamien UDP/TCP-porttien neuvotteluun. NFSv4-protokolla on tilatietoinen ja kaikki RPC-etäohjelmakutsut välitetään yhden TCP/IP-portin avulla. Siksi NFSv4-protokollan kanssa ei tarvita rpcbind-palvelua. stat.d ja lock.d -palveluiden toiminnallisuudet ovat sisäänrakennettu NFSv4-protokollaan eikä niitäkään enää tarvita. Sen sijaan NFSv4-protokolla tarvitsee kaksi uutta palvelua, idmapd ja rpcsecgssd. Idmapd-palvelu yksilöi Linux-työaseman UID/GID numeroita NFSv4-protokollan käyttäjätunnuksiin ja ryhmiin. Rpcsecgssd-palvelu mahdollistaa Kerberoksen käytön NFSv4-protokollan kanssa.

5.4.3 Kerberos-konfiguraatio

Jyväskylän yliopiston käyttämä Linux-jakelu on Red Hat Enterprise Linux 7.4 Tässä testissä käytössä oleva Kernelin versio on:

```
[root@test-ws ~]# uname -s -r
Linux 3.10.0-693.17.1.el7.x86_64
```

Jotta Kerberos-palveluita voidaan hyödyntää, tarvitsee Linux-työasema Kerberos-asiakasohjelmistot. Ohjelmistojen nimet ja versiot tässä tutkimuksessa ovat:

```
krb5-libs-1.15.1-8.el7.x86_64
krb5-workstation-1.15.1-8.el7.x86_64
pam_krb5-2.4.8-6.el7.x86_64
```

NFS-asikasohjelmistojen versiot ovat:

```
nfs-utils-1.3.0-0.48.el7.x86_64
nfs4-acl-tools-0.3.3-15.el7.x86_64
```

Työaseman sisäänkirjautumisprosessia muokataan Linux-työasemassa authconfig-työkalulla. Työkalun versio tässä tutkimuksessa on:

```
authconfig-6.2.8-30.el7.x86_64
```

Linux-työasema konfiguroidaan käyttämään Kerberosta seuraavasti. Asetukset, kuten Ker-

beros REALM ja KDC-palvelinten DNS-osoitteet sekä millaisia tikettejä KDC-palvelimelta pyydetään, konfiguroidaan tiedostoon `/etc/krb5.conf`. Tiedoston sisältö näyttää tältä:

```
[root@test-ws ~]# cat /etc/krb5.conf
[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 dns_lookup_realm = false
 dns_lookup_kdc = false
 ticket_lifetime = 10h
 renew_lifetime = 7d
 forwardable = true
 rdns = false
 default_realm = AD.JYU.FI
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 AD.JYU.FI = {
  kdc = dc2.ad.jyu.fi
  kdc = dc3.ad.jyu.fi
  kdc = dc4.ad.jyu.fi
  kdc = dc1.ad.jyu.fi
  admin_server = dc3.ad.jyu.fi
 }

[domain_realm]
 .ad.jyu.fi = AD.JYU.FI
 ad.jyu.fi = AD.JYU.FI
[root@test-ws ~]#
```

Tiedosto kertoo Linux-työaseman Kerberos-ohjelmistolle, mikä on Kerberos REALM, mitkä ovat KDC-palvelinten DNS-osoiteet, mikä on oletuksena tiketinmyöntämistiketin voimassaoloaika ja kuinka monta päivää tiketinmyöntämistikettiä voi uusia renew-ominaisuuden avulla.

Automaattisen asennusprosessin yhteydessä Linux-työasema konfiguroidaan siten, että se osaa käyttää Kerberosta käyttäjän tunnistamiseen. Tämä vaatii yllä olevan konfiguraatiotiedoston lisäksi Linux-käyttöjärjestelmän PAM-modulien konfiguroimisen. PAM-modulit ovat vastuussa sisäänkirjautumisprosessista. Sisäänkirjautumisprosessi muokataan käyttämään Kerberos-käyttäjäntunnistusjärjestelmää authconfig-työkalulla seuraavasti:

```
authconfig --useshadow --passalgo=sha256 --enablekrb5 --update
```

Tämä komento ajetaan työaseman asennusvaiheessa. Komento kertoo työasemalle, että kun käyttäjä kirjautuu sisään työasemaan, yritetään yhtenä vaihtoehtona käyttäjäntunnistusta Kerberoksella.

5.4.4 Käyttäjä

Mahdollisimman automaattisessa ympäristössä Linux-työasemaan ei luoda paikallisia käyttäjätunnuksia, vaan käyttäjätunnukset luetaan keskitetystä tietokannasta, kuten Microsoft Active Directory -hakemistopalvelusta. Tässä tutkimuksessa keskitytään kerberotuun NFSv4 -protokollaan, joten en ota tässä kantaa hakemistopalveluiden konfiguroimisesta Linux-työasemaan. Totean vain, että moderni Linux-työasema tukee monia kaupallisia ja avoimeen lähdekoodiin perustuvia hakemistopalveluita. Ohitan hakemistopalvelut tässä testitapauksessa ja luon käsin työasemaan paikallisen testitunnuksen ja näytän, miten Kerberoitu NFSv4 -protokolla toimii normaalilla paikallisella käyttäjätunnuksella, joka tunnistetaan Kerberoksen avulla. Paikallinen testitunnus topeolk0 on luotu Linux-työasemaan komennolla:

```
useradd –u 257655 –g 100 –c "Testitunnus Olkinuora" topeolk0
```

Seuraavaksi voidaan testata sisäänkirjautumisprosessin toimivuutta. Kun käyttäjä topeolk0 kirjautuu työasemaan, käyttäjä tunnistetaan Microsoft Active Directoryn avaintenjakelukeskuksen avulla. Käyttäjä saa Kerberos-tiketinmyöntämistiketin, jolla on oletuksena määritelty voimassaoloaika. Sekä Linux-, Windows-, että macOS -käyttöjärjestelmissä on työkaluja Kerberos-tiketin hallintaan. Komento `klist` ilman parametreja näyttää tiketin voimassaoloajan, kuinka kauan tikettiä voi uusia ja mihin tiketti on kakutettu. Ohitetaan tässä kohdassa SSH-etäkirjautuminen ja kirjautuminen graafisen kirjautumisruudun avulla. Seuraavaksi suoritetaan sisäänkirjautuminen suoraan Linux-työaseman konsolilta:

```
Red Hat Enterprise Linux
Kernel 3.10.0-693.17.1.el7.x86_64 on an x86_64

test-ws login: topeolk0
Password:
Last login: Mon Feb 12 12:38:29 on :0
[topeolk0@test-ws ~]$
```

Sisäänkirjautuminen onnistui. Seuraavaksi tarkastellaan, saimmeko tiketinmyöntämistiketin sisäänkirjautumisen yhteydessä:

```
[topeolk0@test-ws ~]$ klist
Ticket cache: KEYRING:persistent:257655:krb_ccache_xwHo5eQ
Default principal: topeolk0@AD.JYU.FI

Valid starting     Expires            Service principal
02/13/18 14:59:24  02/14/18 00:59:24  krbtgt/AD.JYU.FI@AD.JYU.FI
        renew until 02/20/18 14:59:24
[topeolk0@test-ws ~]$
```

Komento `klist` tulostaa näytölle tietoja käyttäjän Kerberos-tiketeistä. Sisäänkirjautumisen jälkeen käyttäjällä on ensimmäinen Kerberos-tiketti, tiketinmyöntämistiketti. Tulosteesta näemme, että tiketinmyöntämistiketti on nimeltään `krbtgt/AD.JYU.FI@AD.JYU.FI`, se on voimassa 14.2.2018 kello 00:59:24 saakka. Tiketinmyöntämistiketillä on lisäksi renew-ominaisuus, ja tikettiä voidaan uusia 20.2.2018 kello 14:59:24 asti. Käyttäjä voi kirjautua tällä tiketinmyötämistiketillä lähiverkon Kerberosta hyödyntäviin palveluihin.

5.4.5 NFSv4 domain

Linux-käyttöjärjestelmässä käyttäjä identifioidaan UID ja GID -numeroiden perusteella. Perinteisesti NFS-protokollassa autentikointi on toiminut myös UID ja GID -numeroiden perusteella. Järjestelystä tekee ongelmallisen se, että sekä NFS-palvelimen, että Linux-työaseman pitää jakaa sama UID ja GID -numeroavaruus. NFSv4-protokolla ei käytä perinteisiä UID ja GID -numeroita tiedosto-oikeuksien määrittelemiseen vaan NFSv4-protokolla käyttää käyttäjänimiä ja ryhmänimiä. NFSv4-protokollassa tätä kutsutaan NFSv4 domainiksi.

NFSv4 domain on NFS-palvelimen ja Linux-työaseman jakama avaruus käyttäjänimiä ja ryhmänimiä. NFSv4-domain määritellään työasemassa tiedostossa `/etc/idmapd.conf` ja sen tulee olla sama, kuin NFS-palvelimella. Esimerkki tiedostosta on liitteessä A

`/etc/idmapd.conf`-tiedostolla on merkitystä idmapper-ohjelmalle, joka tulkitsee työaseman UID ja GID -numeroita NFS-palvelimen käyttäjiin ja ryhmiin. Tiedostolla voi säätää idmapper-ohjelman toimintaa myös erilaisissa poikkeustapauksissa. Jyväskylän yliopiston idmapper-ohjelman konfiguraatiossa kerrotaan vain NFSv4 domain. Jyväskylän yliopistossa NFSv4 domain on ad.jyu.fi. Huomattavaa on, että NFSv4 domain ei ole sama asia, kuin Microsoft Active Directoryn toimialue eikä se ole sama asia, kuin Kerberos REALM.

Joissain Linux-jakeluissa idmapper-ohjelma on käyttöjärjestelmän erillinen palvelu, joka pitää konfiguroida käynnistymään työaseman käynnistyksen yhteydessä. Red Hat Enterprise Linux 7.4 -jakelussa idmapper-palvelu on osa Kerneliä ja erillistä käyttöjärjestelmän palvelua ei tarvita (Navrátil ym. 2017, luku 8.1.1).

5.4.6 Kerberos-palveluprinsipaali NFSv4-palveluja varten

Kerberoidun NFSv4 -protokollan käyttö tarkoittaa RPC-etäohjelmakutsujen kerberoimista ja siihen RPC käyttää GSSD-rajapintaa, eli toisin sanoen kerberoidun NFSv4 -protokollan konfiguroiminen tarkoittaa RPCGSSD-palvelun konfiguroimista. RPCGSSD-palvelu vaatii työasemalta palveluprinsipaalin, jonka työasema ja avaintenjakelukeskus ovat etukäteen neuvotelleet. Palveluprinsipaali, jota kerberoitu NFSv4 -protokolla käyttää on nimeltään nfs. Jyväskylän yliopiston tuotantoympäristössä tarvitaan siis Linux-työasema ja työasemaa vastaava tietokonetili Microsoft Active Directory -hakemistopalveluun. Lisäksi Linux-työasemaan tarvitaan Kerberos-avaintiedosto, jossa on nfs-palveluprinsipaali ja sen salaisuus.

Ensin Microsoft Active Directory -hakemistopalveluun luodaan tietokonetili työasemaa varten. Tietokonetilin voi luoda monella tavalla, mutta tyypillisesti konetili luodaan automatiikalla tai skripteillä. Manuaalisesti konetili voidaan luoda Microsoft PowerShell -komentotulkissa seuraavalla komennolla:

```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
```

```
PS C:\> New-ADComputer -Name "test-ws" -Path
  "OU=Workstations-Linux,DC=ad,DC=Jyu,DC=fi" -Description
  "Testityoasema Petteri Olkinuora"
PS C:\>
```

Komennolla New-ADComputer luodaan uusi konetili test-ws toimialueen ad.jyu.fi organisaatioyksikköön Workstations-Linux . Komento tulee käynnistää käyttäjätunnuksella, jolla on luontioikeudet kyseiseen organisaatioyksikköön ja työasemalle tai palvelimelle, jossa komento ajetaan, pitää olla asennettuna Remote Server Administration Tools -niminen ohjelmisto. Ohjelmisto on ladattavissa ilmaiseksi Microsoftin WWW-sivuilta.

Seuraavaksi Linux-työaseman ja Microsoft Active Directory Kerberoksen välille neuvotellaan yhteinen salaisuus, joka tallennetaan työasemaan tiedostoon `/etc/krb5.keytab`. Tämä voidaan luoda Microsoftin omilla työkaluilla tai Linux-työasemasta löytyvillä työkaluilla. Tässä esimerkissä käytetään msktutil-ohjelmaa. msktutil-ohjelmalla voi luoda tietokonetilejä Microsoft Active Directory -hakemistopalveluun ja muokata niitä. Jvyäskylän yliopistossa tietokonetilit luodaan tietyn prosessin mukaisesti toimialueeseen ja ne liitetään tiettyihin organisaatioyksiköihin. Tässä esimerkissä msktutil-työkalulla muokataan jo olemassa olevaa tietokonetiliä. Valmiiseen tietokonetiliin pitää lisätä nfs-palveluprinsipaali ja tämä palveluprinsipaali pitää tuoda Linux-työasemaan.

Seuraavaksi kirjaudutaan sisään Linux-työasemaan admintunnus-tunnuksella, jolla on oikeus tehdä muutoksia tietokonetiliin. Tarkistetaan vielä, että kirjautuminen onnistui ja saimme tiketinmyöntämistiketin:

```
[admintunnus@test-ws ~]$ klist
Ticket cache: KEYRING:persistent:100002:krb_ccache_Gx81LUl
Default principal: admintunnus@AD.JYU.FI

Valid starting     Expires            Service principal
02/19/18 11:43:12  02/19/18 21:43:12  krbtgt/AD.JYU.FI@AD.JYU.FI
renew until 02/26/18 11:43:12
```

Seuraavaksi työasemassa ajetaan komento msktutil, joka lisää nfs-palveluprinsipaalin avain-

tenjakelukeskuksessa olevaan työasemaa vastaavaan konetiliin. msktutil neuvottelee myös jaetun salaisuuden työaseman ja avaintenjakelukeskuksen kanssa ja tallentaa salaisuudesta kopion komennon syötteenä annettavaan tiedostoon. Testikoneemme nimi on test-ws.cc.jyu.fi ja se sijaitsee ad.jyu.fi domainissa Workstations-Linux-nimisessä organisaatioyksikössä. msktutil tarvitsee nämä tiedot komennon suorittamiseksi:

```
[admintunnus@test-ws ~]$ /usr/sbin/msktutil -b "ou=Workstations-Linux,
dc=ad,dc=jyu,dc=fi" --computer-name test-ws.cc.jyu.fi
-s nfs/test-ws.cc.jyu.fi -s nfs/test -h test-ws.cc.jyu.fi
--server dc1.ad.jyu.fi --upn nfs/test-ws.cc.jyu.fi
--enctypes 0x10 -k tiedosto.keytab
[admintopeolki@test-ws ~]$
```

Komento on tässä pilkottu useammalle riville. Komennolle annetaan parametreiksi organisaatioyksikkö, työaseman nimi ja minkä nimiset palveluprinsipaalit työasemaa varten luodaan. Lisäksi komennolle kerrotaan Kerberos-palvelimen nimi, mitä salausmekanismia halutaan tukea sekä tiedoston nimi, johon palveluprinsipaali ja sen salausavain kirjoitetaan. Komento ajetaan admintunnus-tunnuksella, jolla on Microsoft Active Directory -hakemistossa määritelty oikeudet muokata organisaatioyksikön Workstations-Linux objekteja. Seuraavaksi tarkastellaan `klist` komennolla syntynyttä tiedostoa:

```
[admintopeolki@test-ws ~]$ klist -k -e tiedosto.keytab
Keytab name: FILE:tiedosto.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   3 test-ws$@AD.JYU.FI (aes256-cts-hmac-sha1-96)
   3 nfs/test-ws.cc.jyu.fi@AD.JYU.FI (aes256-cts-hmac-sha1-96)
   3 nfs/test-ws@AD.JYU.FI (aes256-cts-hmac-sha1-96)
```

msktutil loi tiedoston tiedosto.keytab. Tiedosto sisältää nfs-palveluprinsipaalit. Molempien palveluprinsipaalien salaisuudet on salattu AES256-CTS-HMAC-SHA1-96-salausalgoritmilla.

Seuraavaksi siirretään tiedosto.keytab oikeaan paikkaan. Oletuksena Linux-työaseman rpc-secgssd-palvelu etstii Kerberos-keytab-tietoja tiedostosta `/etc/krb5.keytab`. Siirretään tiedosto oikealle paikalleen ja uudelleen nimetään se oikean nimiseksi. Sitten muutetaan sen

oikeudet siten, että vain pääkäyttäjä pääsee siihen käsiksi:

```
[root@test-ws ~]# chown root:root /etc/krb5.keytab
[root@test-ws ~]# chmod 0600 /etc/krb5.keytab
[root@test-ws ~]# ls -la /etc/krb5.keytab
-rw-------. 1 root root 1514 Feb 19 12:07 /etc/krb5.keytab
[root@test-ws ~]#
```

Keytab-tiedosto on syytä suojata, jottei tiedostossa olevaa salaisuutta pääse väärinkäyttämään. Kun keytab-tiedosto on paikallaan, voidaan kokeilla NFS-protokollan `mount`-komentoa, joka liittää NFSv4-palvelimen hakemiston osaksi työaseman hakemistorakennetta. Luodaan hakemisto `/mnt/testmount`, johon liitos halutaan tehdä. Komennon paremetreiksi annetaan, minkä tyyppinen tiedostojärjestelmä ollaan liittämässä hakemistoon, NFS-protokollan versio, haluttu salaustapa eli Kerberos, NFSv4-palvelimen osoite ja palvelimen hakemisto joka halutaan liittää sekä hakemisto Linux-työasemassa, johon liitos halutaan tehdä:

```
[root@test-ws ~]# mkdir /mnt/testmount
[root@test-ws ~]# mount -t nfs -o nfsvers=4.0 -o sec=krb5
nfs4.ad.jyu.fi:/test_fs /mnt/testmount/
[root@test-ws ~]# cd /mnt/testmount/
```

`mount`-komento onnistui eikä palauttanut virheitä. Mahdollisissa virhetilanteissa komennolla `dmesg` voi selvittää virhekoodeista, missä virhe on tapahtunut. Toinen paikka etsiä virheitä on Linux-työaseman `/var/log/messages`-tiedosto. Linux-työasemalta voidaan myös kysyä, millä parametreilla liitos on tehty. Nämä löytyvät `/proc/mounts`-tiedosto:

```
[root@test-ws ~]$ cat /proc/mounts | grep nfs4.ad.jyu.fi
nfs4.ad.jyu.fi:/test_fs on /mnt/testmount type nfs4
(rw,relatime,vers=4.0,rsize=131072,wsize=131072,namlen=255,hard,
proto=tcp,port=0,timeo=600,retrans=2,sec=krb5,
clientaddr=130.234.30.143,local_lock=none,addr=130.234.0.44)
```

Tiedosto kertoo, mitkä kaikki NFS-protokollan parametrit liitoksessa on käytössä.

NFSv4-palvelimella on testihakemisto topeolk0, jonka omistaa käyttäjätunnus eikä muilla käyttäjätunnuksilla tai ryhmillä ole oikeuksia hakemistoon. Testataan, pääseekö Linux-työaseman pääkäyttäjä kyseiseen hakemistoon:

```
[root@test-ws testmount]# ls -la
total 24
drwxrwxrwx. 6 root          root  1024 Feb 19 13:42 .
drwxr-xr-x. 3 root          root    23 Feb 19 13:46 ..
dr-xr-xr-x. 2 root          bin   1024 Feb 19 13:21 .etc
drwxr-xr-x. 2 root          root  8192 Feb 12 14:50 lost+found
d---------. 2 topeolk0      90198   80 Feb 19 13:42 topeolk0
[root@test-ws testmount]# cd topeolk0/
-bash: cd: topeolk0/: Permission denied
[root@test-ws testmount]#
```

Linux-työaseman pääkäyttäjä ei pääse hakemistoon, sillä pääkäyttäjällä ei ole topeolk0-tunnuksen Kerberos-tiketinmyöntämistikettiä. Katsotaanpa, millaiset oikeudet topeolk0-hakemistolla on:

```
[root@test-ws testmount]# nfs4_getfacl topeolk0/
A:fd:topeolk0@ad.jyu.fi:rwaDdxtTnNcCoy
```

Seuraavaksi kirjaudutaan topeolk0-tunnuksella Linux-työasemaan, ja testataan pääseekö käyttäjä topeolk0 siirtymään hakemistoon. Katsotaan `klist`-ohjelman tuloste ennen hakemistoon siirtymistä ja sen jälkeen:

```
[topeolk0@test-ws ~]$ klist
Ticket cache: KEYRING:persistent:257655:krb_ccache_ns4UYfo
Default principal: topeolk0@AD.JYU.FI

Valid starting     Expires            Service principal
02/19/18 14:12:53  02/20/18 00:12:53  krbtgt/AD.JYU.FI@AD.JYU.FI
renew until 02/26/18 14:12:53
[topeolk0@test-ws ~]$ cd /mnt/testmount/
[topeolk0@test-ws testmount]$ klist
Ticket cache: KEYRING:persistent:257655:krb_ccache_ns4UYfo
Default principal: topeolk0@AD.JYU.FI

Valid starting     Expires            Service principal
02/19/18 14:12:58  02/20/18 00:12:53  nfs/nfs4.ad.jyu.fi@AD.JYU.FI
renew until 02/26/18 14:12:53
02/19/18 14:12:53  02/20/18 00:12:53  krbtgt/AD.JYU.FI@AD.JYU.FI
```

```
renew until 02/26/18 14:12:53
[topeolk0@test-ws testmount]$
```

`klist`-komennon tulosteesta voidaan nähdä, että käyttäjällä topeolk0 on tiketinmyöntämistiketti `topeolk0@AD.JYU.FI`. Kun topeolk0 siirtyi hakemistoon, alkoi hän käyttämään kerberoitus NFSv4-palvelua. Linux-työasema haki avaintenjakelukeskukselta topeolk0-tunnuksen tiketinmyöntämistiketillä palvelutiketin NFSv4-palvelua varten. Jäljemmästä `klist`-komennon tulosteesta voidaan nähdä, että tiketinmyöntämistiketin lisäksi käyttäjä on saanut nfs-nimisen palvelutiketin `nfs/nfs4.ad.jyu.fi@AD.JYU.FI` NFS-palvelimelle nfs4.ad.jyu.fi.

Siirrytään topeolk0-hakemistoon, johon vain topeolk0-tunnuksella on oikeuksia. Kokeillaan luoda tiedosto Linux-käyttöjärjestelmän touch-komennolla ja tarkastellaan tiedoston oikeuksia:

```
[topeolk0@test-ws topeolk0]$ touch tiedosto.txt
[topeolk0@test-ws topeolk0]$ ls -la
total 16
d---------. 2 admintopeolki 90198 1024 Feb 19 14:13 .
drwxrwxrwx. 6 root          root  1024 Feb 19 13:55 ..
-rwx------. 1 topeolk0      users    0 Feb 19 14:13 tiedosto.txt
[topeolk0@test-ws topeolk0]$

[topeolk0@test-ws topeolk0]$ nfs4_getfacl tiedosto.txt
A::OWNER@:rwadxtTnNcCoy
```

Tiedosto saa oikeudet, jotka näkyvät osittain oikein `ls -la` ja täsmällisesti `nfs4_getfacl`-komennolla. Linux-työasemassa on nyt käytössä kerberoidulla NFSv4-protokollalla jaettu hakemisto.

5.5 Kerberos-tiketin voimassaoloajan haasteet

Kerberos-tiketin turvallisuus perustuu symmetriseen salaukseen ja siihen, että tiketillä on voimassaoloaika, jonka umpeuduttua tiketistä tulee hyödytön. Protokollan standardissa on määritelty tiketille kahdeksan tunnin voimassaoloaika. Mikäli avaintenjakelukeskus sallii ti-

ketin uusimisen (standarin mukaan näin on, mutta organisaation tietoturvapolitiikan takia tätä ominaisuutta on voitu rajoittaa), voi tikettiä uusia kahdeksan tunnin sisällä, jolloin käyttäjä saa lisää aikaa uuden kahdeksan tuntia. Protokollan standardi määrittelee, että yhtä tikettiä voi uusia seitsemän päivän ajan. Tiketin uusiminen ei aiheuta salasanakyselyä. Monissa organisaatioissa on voitu rajoittaa tietoturvasyistä esimerkiksi kirjautumisaikoja eli mihin aikaan päivästä käyttäjien oletetaan olevan työasemillaan ja mihin aikaan työaika loppuu eikä käyttäjien ole enää syytä käyttää järjestelmiä. Kerberos soveltuu tällaisiin käyttötarkoituksiin oikein hyvin. Standardin mukaan tiketinmyöntämistiketti on voimassa kahdeksan tunnin ajan, eli voidaan ajatella työntekijän tulevan töihin yhdeksään ja lähtevän kello viisi, jolloin hänellä on yhden tiketinmyöntämistiketin voimassaolon ajan lupa käyttää verkon palveluita. Organisaatioissa, joissa käyttäjät voivat olla päiväkausia kirjautuneena sisään, seitsemän päivän rajoitus voi tulla vastaan ja rajoittaa työntekoa. Esimerkiksi tutkimuslaitoksissa, joissa käyttäjä ajaa työasemallaan raskasta laskentaan tai vaikkapa tietokonesimulaatioihin liittyviä viikkokausia kestäviä eräajoja, voi protokollan kahdeksan tunnin ja seitsemän päivän rajoitukset tulla vastaan. Kun tiketin voimassaoloaika päättyy, päättyy lupa käyttää verkon palveluita ja mikäli eräajo hyödyntää Kerberos-käyttäjäntunnistuksesta riippuvia resursseja, voi eräajo katketa kesken suorituksen. Tällaisiin käyttökohteisiin Kerberos soveltuu huonosti. Yleensä ratkaisuna on eristää pitkät eräajot erillisiin laboratorioympäristöihin, joissa Kerberosta ei käytetä, vaan tietoturvasta on huolehdittu muilla tavoin.

Kerberos ei uusi tiketinmyöntämistikettiä käyttäjän puolesta, vaan käyttäjän tulee huolehtia siitä itse. Organisaatiotasolla voidaan määritellä työskentelypolitiikka, joka sanelee, että käyttäjän pitää kirjautua päivän päätteeksi työasemaltaan. Tällaisessa tilanteessa tikettiä ei koskaan tarvitsekaan uusia. Tiketti on voimassa työpäivän ajan ja seuraavana päivänä käyttäjä kirjautuu uudelleen työasemaan saaden näin uuden tiketin. Ongelmalliseksi asian tekee, mikäli käyttäjä tekee töitä työasemallaan kauemmin, kuin kahdeksan tuntia kerrallaan. Linux-työasemassa tiketin uusinta voidaan hoitaa esimerkiksi sisäänkirjautumisen yhteydessä käyttäjän oikeuksilla ajettavalla pienellä skriptillä, joka uusii tikettiä, kunnes seitsemän päivän raja tulee vastaan ja avaintenjakelukeskus evää uusimispyynnön. Yksinkertainen esimerkki tästä skriptistä on esitetty tässä. Komennolla `kinit` käyttäjä voi noutaa itselleen salasanaa vastaan avaintenjakelukeskukselta tiketinmyöntämistiketin. `kinit -R` puolestaan uusii olemassa olevaa tiketinmyöntämistikettiä. `kinit -R` ei kysy salasanaa, joten skripti

voi pyöriä taustalla käyttäjältä piilossa. Skriptin alussa käytetään toista Kerberos-komentoa `klist` kertomaan, onko kyseisellä käyttäjällä tikettiä. Jos tikettiä ei ole, while-silmukkaa ei suoriteta. Jos tiketti on olemassa, yritetään se uusia ja jäädään tunniksi nukkumaan `sleep 3600`. Tunnin päästä yritetään tiketin uusintaa jälleen. while-silmukka päättyy, kun klist palauttaa arvon epätosi eli tiketinmyöntämistiketti on lakannut olemasta voimassa. `kinit` ja `klist` toimivat kaikissa käyttöjärjestelmissä, jotka on yhdistetty Kerberos REALM:iin ja joissa Kerberos-komentorivityökalut on asennettu.

```
while ( klist &>/dev/null ) do
  kinit -R &> /dev/null;
  sleep 3600;
done
```

Kyseinen skripti voidaan käynnistää työaseman login-prosessin yhteydessä. Olkoon skriptin nimi vaikka `renew_kerberos_ticket.sh` ja sijainti `/usr/local/bin`. Skriptiä voidaan kutsua laittamalla toinen pieni skripti `jyu-krb5.sh` `/etc/profile.d` hakemistoon ja sen sisällöksi yksinkertaisesti vain

```
#!/bin/bash
/usr/local/bin/renew_kerberos_ticket.sh &
```

Kaikki `.sh`-päätteiset tiedostot, jotka sijaitsevat `/etc/profile.d`-hakemistossa käynnistetään käyttäjän sisäänkirjautumisen yhteydessä. Yllä oleva esimerkki käynnistää taustalle ajoon Kerberos-tiketinmyöntämistikettiä uusivan skriptin, joka herää tunnin välein uusimaan käyttäjän tiketinmyöntämistikettiä. Kun tiketinmyöntämistiketin uusinta-aika päättyy, skripti poistuu while-silmukasta, ja skriptin ajo päättyy.

5.6 Teknologian tulevaisuuden käyttökohteita

Jyväskylän yliopistossa kerberoitua NFSv4-protokollaa käytetään tuotannossa kotihakemistoissa ja testataan ryhmähakemistoissa. Jyväskylän yliopiston NAS-järjestelmää ei alun perin suunniteltu ryhmähakemistojen käyttöön NFSv4-protokollan kanssa, joten Jyväskylän yliopistossa isoja ryhmähakemistoja ei voi käyttää NFSv4-protokollalla. Pienten tutkimusryhmien testiympäristöjä on kuitenkin jaettu kerberoidulla NFSv4-protokollalla ja tästä jär-

jestystä on vaihtelevia käyttökokemuksia. Suurimmat muutokset NFSv3-protokollan ja kerberoidun NFSv4-protokollan välillä ovat muuttuneet tiedosto-oikeudet ja Kerberos-tiketti. Linux-käyttäjä ei välttämättä tiedä tai ymmärrä muuttuneita tiedosto-oikeuksia tai ei muista pitää huolta oman Kerberos-tikettinsä voimassaolosta. Osa ohjelmistoista ei ymmärrä muuttuneita tiedosto-oikeuksia. Useat Linux-ohjelmistot olettavat, että ne voivat kirjoittaa hakemistoon X ja muuttaa sitten kirjoittamiensa tiedostojen oikeuksia. Jos hakemisto X sijaitseekin oikeasti NFS-palvelimella ja se on jaettu Linux-työasemaan kerberoidulla NFSv4-protokollalla voi syntyä ongelmia.

Ensimmäisen ryhmän ongelmat aiheuttavat erilaiset kääntäjät ja make-tyyppiset ohjelmistot, jotka luovat paljon väliaikaistiedostoja ja symbolisia linkkejä ja kovia linkkejä ja muuttavat näiden väliaikaistiedostojen oikeuksia. Koska NFSv4-protokollalla jaetussa hakemistossa ei välttämättä toimi normaalit tiedostojen oikeuksien muokkauskomennot, kuten chown ja chmod, voi kääntäjä tai make-tyyppinen ohjelma keskeytyä virheeseen, vaikka varsinaista virhettä ei ole tapahtunut. Korjauksena tähän on ollut antaa käyttäjälle kaikki mahdolliset oikeudet hakemistoon. Joskus tämä riittää, mutta aina ei. Tällaisissa tilanteissa ohjelmien kääntäminen ja make-tyyppisten ohjelmien ajo on suoritettava hakemistossa, joka ei sijaitse NFSv4-protokollan tarjoamassa hakemistossa, vaan työaseman paikallisella kovalevyllä sijaitsevassa hakemistossa.

Toisen ryhmän ongelmat muodostavat ohjelmat, jotka haluavat ajon aikana varmistua siitä, että käyttäjä omistaa hakemiston X ja että vain käyttäjällä on oikeudet hakemistoon X. Tällaisia ohjelmia ovat esimerkiksi Linux-käyttöjärjestelmän pulseaudio-äänijärjestelmä ja SSH-palvelu. Molemmat näistä ohjelmista olettavat, että tiedostolla ja hakemistolla on vain yksi omistaja. NFSv4-protokollalla jaetussa hakemistossa on käytössä hienojakoiset NFSv4 ACL -oikeusrakenteet ja yksittäisellä tiedostolla voi olla monta omistajaa ja monta ryhmää, ja näillä voi olla erilaisia oikeuksia tiedostoihin ja hakemistoihin. Jos tiedostolla tai hakemistolla on laajoja ACL-määrityksiä, voi osa Linux-työaseman ohjelmistoista kieltäytyä toimimasta. Ratkaisuna on yrittää yksinkertaistaa NFSv4-protokollalla jaettujen tiedostojen ACL-määrityksiä. Tällä tavalla valitettavasti menetetään hienojakoisten käyttöoikeuksien tuomat hyödyt.

Kerberoidulla NFSv4-protokollalla voidaan toteuttaa korkeakoulussa Linux-mikroluokka,

jossa jokaiselle mikroluokan Linux-työasemalle on konfiguroitu sama jaettu verkkohakemisto ja käyttäjien kotihakemistot löytyvät tästä verkkohakemistosta. Näin käyttäjän ei tarvitse muistaa millä mikroluokan työasemalla käyttäjä on viimeksi ollut kirjautuneena sisään ja käyttäjän sama kotihakemisto ja samat tiedostot löytyvät joka kerta, kun käyttäjä kirjautuu jollekin mikroluokan koneista sisään. Tässä konfiguraatiossa kotihakemistojen hienovaraiset oikeudet on säädettävä siten, että kaikki halutut Linux-työaseman ohjelmistot toimivat. Esimerkiksi Jyväskylän yliopistossa nimenomaan tässä kotihakemistokonfiguraatiossa käyttäjän kotihakemistojen hienovaraisten oikeuksien asettamisessa jouduttiin lukuisiin kompromisseihin tietoturvan, ylläpidettävyyden ja käytettävyyden välillä.

Kerberoitu NFSv4-protokolla ei sovi ympäristöihin, joissa suoritetaan pitkiä eräajoja. Esimerkiksi joihinkin laskentaympäristöihin kerberoidut sovellukset eivät sovi, jos Kerberostiketti lakkaa olemasta voimassa ennen, kuin laskutoimitus valmistuu. Tällaisissa ympäristöistä tietoturvasta tulee huolehtia muilla tavoilla. Toisinaan laskentaympäristö voi vaatia myös niin paljon suorituskykyä tietokoneen tiedostojärjestelmältä, että lähiverkossa tiedostonjakopalvelimelta jaettu hakemisto laskentaympäristön tallennustilana ei ylipäänsä voi tulla kysymykseen.

Kerberoitu NFSv4-protokolla soveltuu hyvin Linux-työasemaympäristöön, jossa vaaditaan korkeaa tietoturvaa ja jossa tiedostojen käsittelytarpeet ovat rajalliset. Jaettu hakemisto työasemassa ei koskaan käyttäydy ihan samalla tavalla, kuin tietokoneen paikallisen kovalevyn hakemisto. Teknologiassa on rajoitteita, jotka on syytä huomioida suunnitteluvaiheessa.

6 Yhteenveto

Tässä tutkimuksessa käsiteltiin lähiverkon tiedostonjakopalveluita Linux-työasemaympäristössä. Tutkimuksessa esiteltiin Kerberoksen ja NFS-protokollan eri versioiden toimintaa. Tutkimuksessa todettiin, että vanhempi NFSv3-protokolla ei sovellu käytettäväksi moderneissa avoimissa lähiverkoissa sen heikon tietoturvan takia. Sen sijaan lähiverkoissa tulisi käyttää uudempaa NFSv4-protokollaa, joka lisää protokollaan Kerberoksen tarjoamat tietoturvapalvelut. Tutkimuksessa todettiin, että kerberoitu NFSv4-protokolla tarjoaa tietoturvalliset tiedostonjakopalvelut Linux-työasemaympäristössä ja että teknologia on tuotannossa Jyväskylän yliopiston lähiverkossa, jossa on muun muassa käytössä kolmannen osapuolen NFSv4-palvelin, Microsoft Active Directory -hakemistopalvelun tarjoama Kerberos-käyttäjäntunnistusjärjestelmä sekä Linux-työasemia. Teknologia on perinteiseen NFS-protokollaan verrattuna monimutkainen ja vaatii kaikkien rakennuspalikoiden ymmärtämistä. Tämän tutkimuksen yksi tarkoitus oli purkaa nämä rakennuspalikat auki, jotta järjestelmä olisi mahdollista rakentaa myös johonkin toiseen ympäristöön.

Pyrin käyttämään tutkimuksessa uusinta mahdollista lähdemateriaalia taustoittamaan teknologioita. Kuitenkin sekä Kerberos-protokolla, että NFS-protokolla ovat 1980-luvulla kehitettyjä teknologioita, joten osa lähdemateriaalista on kyseiseltä ajalta. Uutta lähdemateriaalia edustavat uudemmat NFSv4-protokollan ominaisuuksiin ja suorituskykyyn liittyvät tutkimukset sekä Kerberoksen formalisointiin liittyvä tutkimus. Microsoft Active Directory -hakemistopalvelun ja Linux-työaseman osalta osa materiaalista on niin yksityiskohtaista, että jouduin tukeutumaan valmistajien käyttöohjeisiin tieteellisten artikkeleiden sijaan. Muutamissa teknisissä yksityiskohdissa jouduin taustoittamaan teoriaosuutta myös IETF Working Group:n RFC-dokumenteilla, koska en löytänyt kaipaamiani yksityiskohtia muualta.

Jatkotutkimuskohteita voisi olla tarkastella protokollan tiedonsiirtoväylälle asettamia vaatimuksia, miten Kerberos-protokollalla salattua tiedonsiirtoa saisi tehostettua, miten laskentapalvelinten Kerberos-tikettiin liittyvät ongelmat saataisiin ratkottua ja miten ryhmähakemistoja olisi järkevä toteuttaa tällä teknologialla. Kerberoitu NFSv4-protokolla on käytössä Jyväskylän yliopiston lähiverkossa enkä näe mitään syytä, miksi se ei voisi olla käytössä myös muissa korkeakouluissa tai yrityssektorilla.

Lähteet

Bhat, Wasim Ahmad, ja Smk Quadri. 2013. “Understanding and mitigating security issues in Sun NFS”. *Network Security* 2013 (1): 15–18.

Butler, Frederick, Iliano Cervesato, Aaron D. Jaggard, Andre Scedrov ja Christopher Walstad. 2006. “Formal analysis of Kerberos 5”. *Theoretical Computer Science* 367 (1): 57–87.

Cheng, Ming, Dean Hildebrand, Geoff Kuenning, Soujanya Shankaranarayana, Bharat Singh ja Erez Zadok. 2015. “Newer Is Sometimes Better: An Evaluation of NFSv4.1”. *ACM SIGMETRICS Performance Evaluation Review* 43 (1): 165–176.

Eisler, Mike, toimittanut. 2006. *XDR: External Data Representation Standard: Request for Comments: 4506.* The Internet Society, Network Working Group, maaliskuu. Viitattu 7. helmikuuta 2018. `https://tools.ietf.org/html/rfc4506`.

———. 2009. *RPCSEC_GSS Version 2: Request for Comments: 5403.* The Internet Society, Network Working Group, helmikuu. Viitattu 20. maaliskuuta 2018. `https://tools.ietf.org/html/rfc5403`.

Fuchsberger, Andreas. 1998. “GSS-API”. *Information Security Technical Report* 2 (4): 54–61.

Graves, Robert. 1992. *The Greek Myths: Complete Edition.* Combined Edition. Penguin Books.

Haynes, Thomas, ja David Noveck, toimittaneet. 2015. *Network File System (NFS) Version 4 Protocol: Request for Comments: 7530.* The Internet Society, Network Working Group, maaliskuu. Viitattu 20. maaliskuuta 2018. `https://tools.ietf.org/html/rfc7530`.

Izquierdo, Antonio, Jose María Sierra, Julio César Hernández ja Arturo Ribagorda. 2004. “Security Issues in Network File Systems”. *Computational Science And Its Applications - Iccsa 2004, Pt 1* 3043:812–820.

Joseph, D Paul, M Krishna ja K Arun. 2015. “Cognitive Analytics and Comparison of Symmetric and Asymmetric Cryptography Algorithms”. *International Journal of Advanced Research in Computer Science* 6 (3).

Kautto, Tuomas. 2008. “Kerberos ja NFS”. Tutkielma, Jyväskylän yliopisto.

Levy, Eliezer, ja Abraham Silberschatz. 1990. “Distributed File System: Concepts and Examples”. *ACM Computing Surveys* 22 (4).

Lukka, K. 2000. “Management expertise for the new millenium : in commemoration of the 50th anniversary of the Turku School of Economics and Business Administration”. Luku The Key Issues of Applying the Constructive Approach to Field Research, toimittanut Reponen T. Turku School of Economics / Business Administration.

Mellander, Jim. 2002. “Unix Filesystem Security”. *Information Security Technical Report 2002, Vol.7(1), pp.11-25* 7 (1): 11–25.

Microsoft. 2012. *Network security: Configure encryption types allowed for Kerberos.* Microsoft, 15. marraskuuta. Viitattu 23. marraskuuta 2017. `https://technet.microsoft.com/en-us/library/jj852180(v=ws.11).aspx`.

———. 2014a. *How Domains and Forests Work.* Microsoft, 19. marraskuuta. Viitattu 14. helmikuuta 2018. `https://technet.microsoft.com/en-us/library/cc783351(v=ws.10).aspx`.

———. 2014b. *What Are Domains and Forests?* Microsoft, 19. marraskuuta. Viitattu 13. helmikuuta 2018. `https://technet.microsoft.com/en-us/library/cc759073(v=ws.10).aspx`.

Navrátil, Milan, Jacquelynn East, Don Domingo, Josef Bacik, Kamil Dudka, Hans de Goede, Harald Hoyer ym. 2017. *Red Hat Enterprise Linux 7 Storage Administration Guide.* RedHat, Inc., 11. joulukuuta. Viitattu 9. helmikuuta 2018. `https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/index`.

Neuman, B. Clifford, ja Theodore Ts‘o. 1994. “Kerberos: An Authentication Sewice for Computer Networks”. *Communications Magazine, IEEE IEEE Communications Magazine* 32 (9): 33–38.

Neuman, Clifford, Tom Yu, Sam Hartman ja Kenneth Raeburn. 2005. *The Kerberos Network Authentication Service (V5): Request for Comments: 4120.* The Internet Society, Network Working Group, heinäkuu. Viitattu 2. marraskuuta 2017. `https://tools.ietf.org/html/rfc4120`.

Paddock, Douglas A. 2003. “Delegation of Authority in Active Directory”. *EDPACS* 30 (8): 9–15.

Pittaway, Glenn. 1999. “Distributed security services in microsoft Windows NT 5.0 — Kerberos and the active directory”. *Information Security Technical Report* 4:20–21.

Sadi, Ghania Al. 2016. “Tuning and Optimizing Network File System Server Performance”. *International Journal of Computer Applications* 134 (10): 25–29.

Tankard, Colin. 2012. “Taking the management pain out of Active Directory”. *Network Security* 2012 (4): 8–11.

Thurlow, Robert. 2009. *RPC: Remote Procedure Call Protocol Specification Version 2: Request for Comments: 5531.* The Internet Society, Network Working Group, maaliskuu. Viitattu 7. helmikuuta 2018. `https://tools.ietf.org/html/rfc5531`.

Liitteet

A Esimerkki idamapd.conf

```
[root@test-ws ~]# cat /etc/idmapd.conf
# ------------------------------ #
# Managed by puppet, DO NOT EDIT. #
# ------------------------------ #

[General]
#Verbosity = 0
# The following should be set to the local NFSv4 domain name
# The default is the host's DNS domain name.
Domain = ad.jyu.fi

# The following is a comma-separated list of Kerberos realm
# names that should be considered to be equivalent to the
# local realm, such that <user>@REALM.A can be assumed to
# be the same user as <user>@REALM.B
# If not specified, the default local realm is the domain name,
# which defaults to the host's DNS domain name,
# translated to upper-case.
# Note that if this value is specified, the local realm name
# must be included in the list!
#Local-Realms =

[Mapping]

Nobody-User = nobody
Nobody-Group = nobody

[Translation]

# Translation Method is an comma-separated, ordered list of
# translation methods that can be used.  Distributed methods
# include "nsswitch", "umich_ldap", and "static".  Each method
```

```
# is a dynamically loadable plugin library.
# New methods may be defined and inserted in the list.
# The default is "nsswitch".
Method = nsswitch

# Optional.  This is a comma-separated, ordered list of
# translation methods to be used for translating GSS
# authenticated names to ids.
# If this option is omitted, the same methods as those
# specified in "Method" are used.
#GSS-Methods = <alternate method list for translating GSS names>

#----------------------------------------------------------------#
# The following are used only for the "static" Translation Method.
#----------------------------------------------------------------#
[Static]

# A "static" list of GSS-Authenticated names to
# local user name mappings

#someuser@REALM = localuser


#----------------------------------------------------------------#
# The following are used only for the "umich_ldap" Translation Method.
#----------------------------------------------------------------#

#[UMICH_SCHEMA]

# server information (REQUIRED)
#LDAP_server = ldap-server.local.domain.edu

# the default search base (REQUIRED)
#LDAP_base = dc=local,dc=domain,dc=edu

#--------------------------------------------------------#
# The remaining options have defaults (as shown)
```

```
# and are therefore not required.
#-------------------------------------------------------------#

# whether or not to perform canonicalization on the
# name given as LDAP_server
#LDAP_canonicalize_name = true

# absolute search base for (people) accounts
#LDAP_people_base = <LDAP_base>

# absolute search base for groups
#LDAP_group_base = <LDAP_base>

# Set to true to enable SSL - anything else is not enabled
#LDAP_use_ssl = false

# You must specify a CA certificate location if you enable SSL
#LDAP_ca_cert = /etc/ldapca.cert

# Objectclass mapping information

# Mapping for the person (account) object class
#NFSv4_person_objectclass = NFSv4RemotePerson

# Mapping for the nfsv4name attribute the person object
#NFSv4_name_attr = NFSv4Name

# Mapping for the UID number
#NFSv4_uid_attr = UIDNumber

# Mapping for the GSSAPI Principal name
#GSS_principal_attr = GSSAuthName

# Mapping for the account name attribute (usually uid)
# The value for this attribute must match the value of
# the group member attribute - NFSv4_member_attr
#NFSv4_acctname_attr = uid
```

```
# Mapping for the group object class
#NFSv4_group_objectclass = NFSv4RemoteGroup

# Mapping for the GID attribute
#NFSv4_gid_attr = GIDNumber

# Mapping for the Group NFSv4 name
#NFSv4_group_attr = NFSv4Name

# Mapping for the Group member attribute (usually memberUID)
# The value of this attribute must match the value of NFSv4_acctname_attr
#NFSv4_member_attr = memberUID
```