Jussi Osamaa

KIOSK-PC VMWARE YMPÄRISTÖSSÄ

Tietotekniikan koulutusohjelma
2016

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

Tiivistelmä

Kiosk-PC VMWare ympäristössä

Osamaa, Jussi
Satakunnan ammattikorkeakoulu
Tietotekniikan koulutusohjelma
Toukokuu 2016
Ohjaaja: Trast, Ismo
Sivumäärä: 48
Liitteitä:1

Asiasanat: Kiosk-PC, Windows, VMWare, AD

Osaamisen testaaminen suoritetaan oppilaitoksissa pääsääntöisesti valvotussa ympäristössä suoritetussa kokeessa. Valvonta ja kokeiden järjestäminen kuormittaa organisaatiota ja aiheuttaa jäykkyyttä opintojen sujuvaan etenemiseen.

Tässä työssä rakennetaan järjestelmä, jota voidaan esimerkiksi hyötykäyttää oppilaitoksissa sähköisen tenttijärjestelmän pohjana. Työn menetelmänä on projekti, jossa luodaan Kiosk-PC ympäristö.

Alussa käsitellään verkkojen perusteet, käydään läpi ohjelmia ja työkaluja. Sitten käydään läpi virtuaalikoneiden luominen, käyttöjärjestelmien asentaminen ja Domainin luominen. Lopussa käydään läpi mitä kaikkia asetuksia Kiosk-koneen luominen vaatii ja todennetaan kokoonpanon toimivuus.

Abstract

Kiosk-PC in VMWare environment

Osamaa, Jussi
Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2016
Supervisor: Trast, Ismo
Number of pages: 48
Appendices: 1

Keywords: Kiosk-PC, Windows, VMWare, AD

In educational institutions, testing of competence is mainly carried out in controlled environment and closed tests. Supervision and organizing the tests strains the organization and causes some stiffness in smooth progress of the studies.

In this work we build a system that can – for example – be used in educational institutions for the basis for electronic exam systems. Purpose of the thesis is to build a project in which we create a Kiosk-PC environment.

In the beginning of the thesis we go through the basics of the network, programs and tools. Then we go through the creation of the virtual machine, settings of the operating system and creation of the domain. At the end we go through which settings the creation of the Kiosk-machine requires and verify functionality of the device configuration.

SISÄLLYSLUETTELO

1 Johdanto

Tässä työssä rakennetaan järjestelmä, jota voidaan esimerkiksi hyötykäyttää oppilaitoksissa sähköisen tenttijärjestelmän pohjana. Työn menetelmänä on projekti, jossa luodaan Kiosk-PC ympäristö. Järjestelmää hallinnoidaan ja rajoitetaan palvelimen kautta.

Työ toteutetaan virtuaaliympäristössä VMWare nimisellä ohjelmalla. VMWarella on tarkoitus luoda yksinkertainen perusverkko, johon sisältyy palvelin ja palvelimelta hallitut tietokoneet. Hallittuja tietokoneita nimitetään Kiosk-PC:iksi, jotka soveltuvat myös esimerkiksi nettikahviloihin tai muihin käyttötarpeisiin, jossa tarvitaan järjestelmää, jonka käyttöä on rajoitettu. Palvelin toimii Windows Server 2012 R2 käyttöjärjestelmällä ja Kiosk-PC:t Windows 10 käyttöjärjestelmällä.

Kiosk-PC tai Kiosk-ohjelmisto on yleisesti ottaen käyttöliittymä, joita käytetään nettikahviloissa tai esimerkiksi esittelynäyttöinä. Käyttöliittymässä on suljettu ominaisuuksia, jotka estävät käyttäjiä tekemästä muutoksia itse käyttöjärjestelmään.
Jos Windows halutaan saada suljetuksi, niin pitää ottaa huomioon esimerkiksi seuraavia asioita:

- Pikanäppäinyhdistelmät pitää estää kuten Ctrl+Alt+Delete, Win+X-näppäimet, F1-F12 näppäimiä ja monia muita. Käytännössä pitää estää kaikki pikanäppäimet, jotka mahdollistaisivat käyttäjälle pääsyn Windows-asetuksiin.

- Kansioihin ja itse kiintolevylle pitää tehdä estot, jotta käyttäjä ei saa tallennettua tiedostoja minne haluaa.

- Internet-selaimeen pitää tehdä estoja, jotka eväävät pääsyn selaimen asetuksiin ja estää halutessa pääsy tietyille verkkosivuille.

- Ulkoisten laitteiden käyttö kuten USB-tikut ja CD-levyt pitää estää.

- Käyttäjätili pitää määrittää siten, että edellisen käyttäjän tiedot eivät jää koneen muistiin vaan tyhjentyvät.

- Videovalvonta

2 Verkkojen perusteet

2.1 TCP/IP

TCP/IP on protokolla yhdistelmä, joka pitää sisällään monta eri protokollaa. Pääkomponentit kuitenkin ovat nimensä mukaisesti TCP- ja IP-protokollat. IP-protokolla huolehtii käytännössä informaation ja osoitteiden reitittämisestä eri laitteille. Tämä pitää sisällään mm. IP-osoitteet, aliverkon peitteen, oletusyhdyskäytävän, DNS-osoitteen ja DHCP:n. TCP/IP on reititysprotokolla, joka tarkoittaa että käyttäjän on mahdollisuus jakaa verkkoja moniin eri aliverkkoihin.

Ei-reitittävissä protokollissa kaikki laitteet, jotka kytketään samaan verkkoon, ovat suoraan yhteydessä toisiinsa, joka on jo pelkästään tietoturvan kannalta iso riskitekijä. OSI-mallissa IP-protokolla sijoittuu kolmanteen kerrokseen, eli verkkokerrokseen. (Kuva 1)

TCP-protokolla puolestaan pitää huolen siitä, miten laitteet kommunikoivat toistensa kanssa. Tämä käytännössä tapahtuu liukuvan ikkunoinnin avulla, eli dataa lähetetään niin paljon kuin toinen osapuoli pystyy vastaanottamaan.

Esimerkki 1. Kone A lähettää Kone B:lle paketteja, joille on määritetty tietty koko, Kone B lähettää aina kuittauksen takaisin kun on saanut vastaanotettua koko paketin. Tämän jälkeen Kone A lähettää uuden paketin ja kasvattaa samalla tiedonsiirron määrää. Datapakettien kokoa voidaan säädellä kasvattamalla ikkunan kokoa. [1] [9]

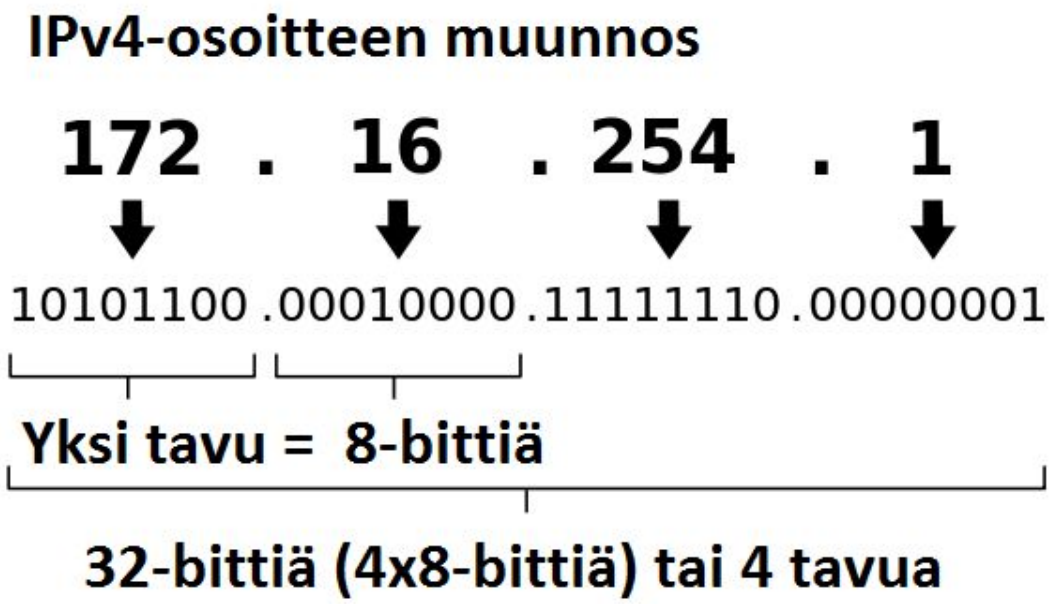
TCP-protokolla sijoittuu OSI-mallissa neljänteen kerrokseen, eli kuljetuskerrokseen (Kuva 1)

Kuva 1. OSI-Malli [7]

2.1.1 IPv4-osoitteet

IPv4-osoite on 32-bittinen osoite, joka täytyy olla kaikissa laitteissa, jotka toimivat TCP/IP-protokollan alla. Osoite voidaan ilmaista binääri- tai desimaalimuodossa. Yleisin muoto on kuitenkin desimaalimuoto ja se on huomattavasti vaivattomampi kirjoittaa.

IP-osoite erotellaan neljään eri oktettiin. Yksi oktetti sisältää 8 binäärilukua, joiden yksittäinen arvo voi olla 0 tai 1. IP-osoitteiden verkkoavaruus on välillä 0.0.0.0-255.255.255.255. (Kuva 2)



Kuva 2. IPv4-osoite [8]

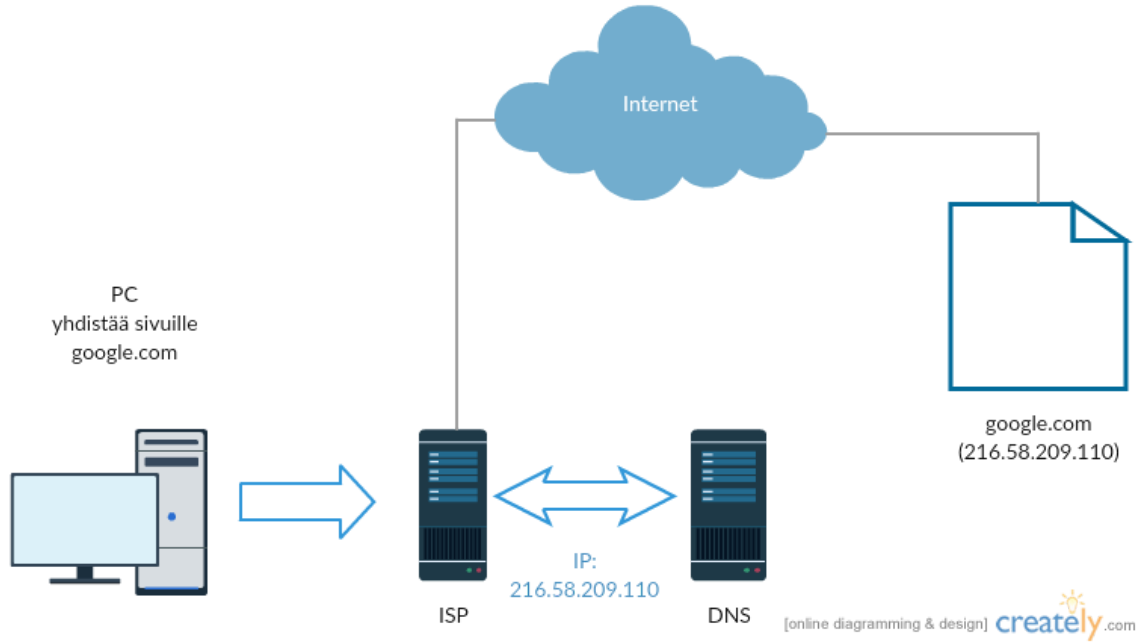
Seuraavassa taulukossa käsitellään yksittäisen oktetin muuntaminen binääristä desimaalimuotoon.
Binäärimuodossa lukuarvo kaksinkertaistuu oikealta vasemmalle tultaessa, alkaen numerosta 1 ja päättyen numeroon 128. Jos halutaan esimerkiksi luku 192. Niin annetaan lukujonon kahdelle viimeiselle merkille vasemmalla binääriarvo 1 ja lopuille 0. Tämän jälkeen täytyy yhteenlaskea kaikki arvot joissa on binääriarvona 1, joten tässä tapauksessa 128+64 = 192.

Potenssi[i]	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Desimaali	128	64	32	16	8	4	2	1
Binääri	1	1	0	0	0	0	0	0

2.1.2 DNS

DNS (Domain Name Server) eli nimipalvelin, on järjestelmä joka muuntaa verkkotunnukset IP-osoitteiksi. Tämä on siksi pakollinen, koska jos käyttäjä yrittää esimerkiksi mennä sivuille www.google.com, niin kone ei osaisi navigoida sivulle suoraan, koska kone ymmärtää vain, mihin IP-osoitteeseen sen pitää yhdistää.

Yksinkertaistettuna, kun kone yrittää yhdistää Internet-sivulle, se tarkistaa ensin DNS-palvelimelta Internet-sivun IP-osoitteen, jonka jälkeen koneen on mahdollista saada Internetin kautta yhteys itse sivulle. (Kuva 3)



Kuva 3. DNS-kaavio

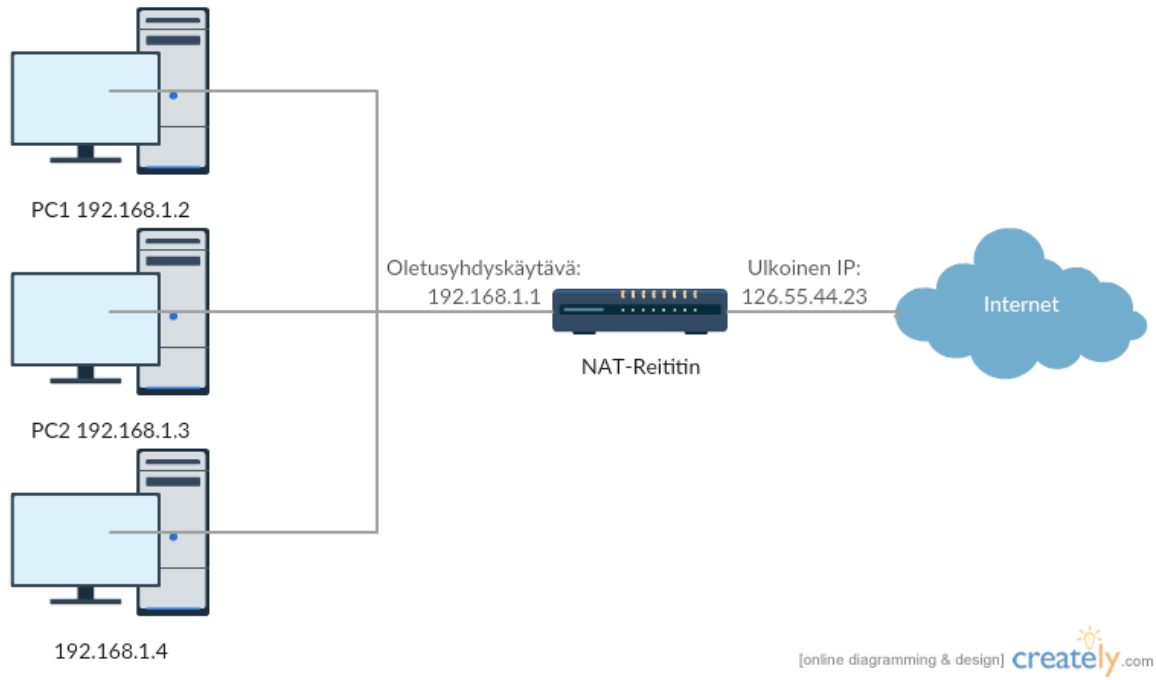
2.1.3 DHCP

DHCP (Dynamic Host Configuration Protocol) on verkkoprotokolla, joka pystyy automaattisesti määrittämään lähiverkon uusille laitteille esimerkiksi IP-osoitteita, oletusyhdyskäytävän ja nimipalvelin-osoitteita. DHCP pystyy jakamaan käytännössä lähes mitä tahansa asetuksia.
DHCP:lle määritellään tietty IP-osoiteavaruus, josta lähiverkon laitteet saavat halutun IP-osoitteen. Tätä kutsutaan yleensä DHCP Scopeksi. DHCP:lle määritellään myös erikseen voimassaoloaika, että kuinka kauan IP-osoitteet ovat voimassa kunnes ne vaihtuvat. [2] [1]

2.1.4 NAT

NAT (Network Address Translation) eli osoitteenmuunnos tarkoittaa sitä, että ulkoinen IP muutetaan NAT:n avulla omaan lähiverkkoon sopivaksi. Kuvassa on normaali 192.168.1.0-verkko jolle reititin muuntaa IP-osoitteet sisäverkossa.
Internettiin yhdistäessä reititin kuitenkin antaa ulkoisen, eli julkisen IP-osoitteen. (Kuva 4)

Tämä verkkotekniikka on luotu sen takia, koska IP-osoitteita ei riittäisi läheskään kaikille koneille, jos niitä ei muunnettaisi omaan lähiverkkoon sopiviksi.



Kuva 4. NAT-malli

2.1.5 Aliverkotus

Yrityksissä ja yleensäkin organisaatioissa jaetaan usein osoiteavaruuksia aliverkkoihin. Aliverkkojen tarkoitus on helpottaa ylläpitoa ja tällä tavoin pystytään pitämään työasemaverkot erillään toisistaan. [3]

Aliverkotuksessa pitää ottaa huomioon se, että kuinka suuri verkko on, eli kuinka monta työasemaa ja reititintä se tarvitsee. Aliverkon verkkoavaruudesta täytyy varata osoitteet työasemille, aliverkolle, broadcastille ja reittimille.

Aliverkon peite = Subnet Mask

Broadcast-osoite = Viimeinen mahdollinen IP-osoite verkkoavaruudesta.
Reitittimen osoite = Oletusyhdyskäytävä (Default Gateway)

Esimerkki 1.

Koko verkolle on annettu osoiteavaruus 192.168.1.0 /24, eli 255.255.255.0 on aliverkon peite, joka pitää sisällään 256 = 2^8 osoitetta, eli binäärimuodossa sen viimeinen oktetti on kokonaan käytettävissä. Verkkoavaruuteen luodaan kolme työasemaverkkoa, joiden suuruudet ovat A=36 työasemaa, B=10 työasemaa ja C=29 työasemaa.
Aliverkotustaulukko on hyödyllinen apuväline tähän tarkoitukseen.

CIDR	Host bits	Netmask	Addresses in subnet
/24	8	255.255.255.0	$256 = 2^8$
/25	7	255.255.255.128	$128 = 2^7$
/26	6	255.255.255.192	$64 = 2^6$
/27	5	255.255.255.224	$32 = 2^5$
/28	4	255.255.255.240	$16 = 2^4$
/29	3	255.255.255.248	$8 = 2^3$
/30	2	255.255.255.252	$4 = 2^2$
/31	1	255.255.255.254	$2 = 2^1$
/32	0	255.255.255.255	$1 = 2^0$

Verkko A	Verkko B	Verkko C
36 työasemaa	29 työasemaa	10 työasemaa
Aliverkko-osoite	Aliverkko-osoite	Aliverkko-osoite
Broadcast-osoite	Broadcast-osoite	Broadcast-osoite
Reittimen-osoite	Reittimen-osoite	Reittimen-osoite
Yhteensä 39 osoitetta	**Yhteensä 32 osoitetta**	**Yhteensä 13 osoitetta**

Aliverkotustaulukosta katsotaan, että Verkko A:n kriteerit täyttää /26-verkko, jossa on varattu kuusi viimeistä bittiä osoitteille, eli 64 = 2^6. Aliverkon osoitteeksi tulee 255.255.255.192.

Verkko B:lle varataan verkko /27, johon mahtuu täsmälleen 32 osoitetta.
Verkkoon ei tämän jälkeen saa lisättyä yhtään laitetta. Aliverkon osoite 255.255.255.224.

Verkko C:n kriteerit täyttää /28-verkko, joten aliverkon osoitteeksi varataan 255.255.255.240.

Kun työasemaverkkojen aliverkko-osoitteet on määritetty niin ne jaotellaan haluttuun 192.168.1.0-192.168.1.254 verkkoon. Osoitteet varataan suuruusjärjestyksessä suurimmasta alkaen.

Verkko A:lle määritetään ensimmäiseksi verkko-osoitteet, koska se on suurin verkko. Luodaan taulukko, johon listataan mahdollisia osoiteavaruuksia. Periaatteessa verkon osoitteet voi valita mistä kohtaa vaan, mutta loogisinta on aloittaa alusta.

Verkko A

Subnet addr	**First host**	**Last host**	**Subnet mask**	**Broadcast**
192.168.1.0	**192.168.1.1**	**192.168.1.62**	**255.255.255.192**	**192.168.1.63**
192.168.1.64	192.168.1.65	192.168.1.126	255.255.255.192	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.190	255.255.255.192	192.168.1.191

Verkko B

Subnet addr	**First host**	**Last host**	**Subnet mask**	**Broadcast**
192.168.1.64	**192.168.1.65**	**192.168.1.94**	**255.255.255.224**	**192.168.1.95**
192.168.1.96	192.168.1.97	192.168.1.126	255.255.255.224	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.158	255.255.255.224	192.168.1.159

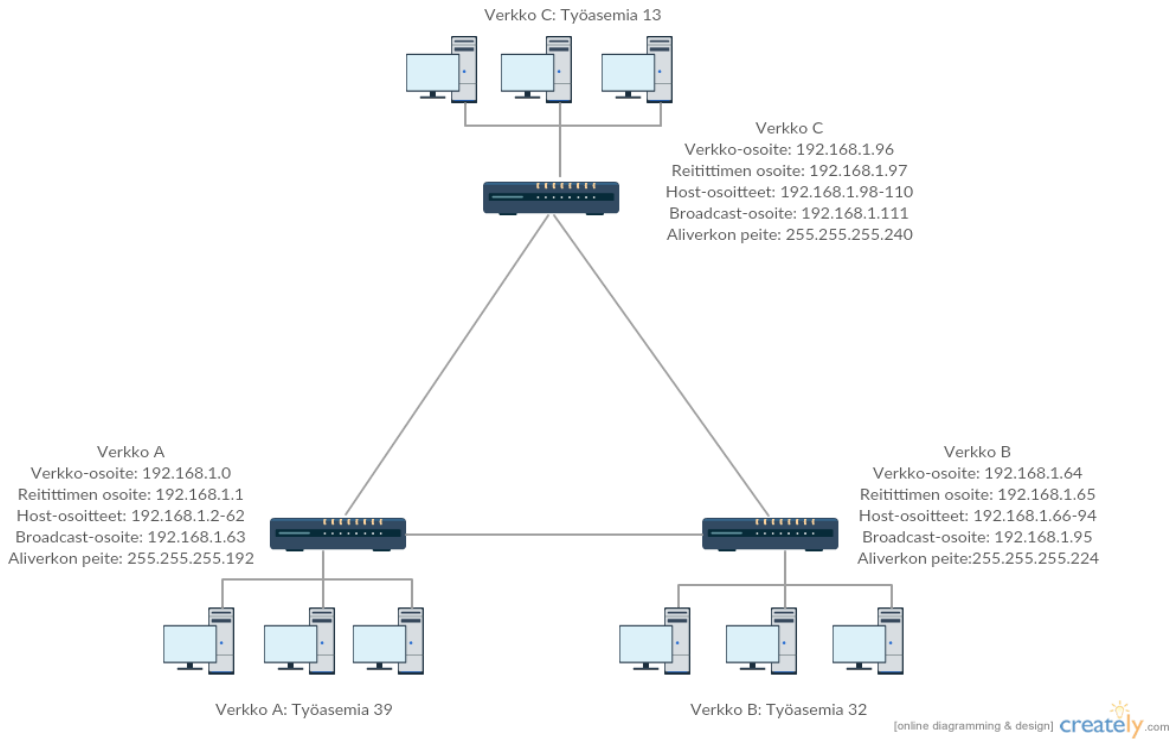
Verkko C

Subnet addr	**First host**	**Last host**	**Subnet mask**	**Broadcast**
192.168.1.96	**192.168.1.97**	**192.168.1.110**	**255.255.255.240**	**192.168.1.111**
192.168.1.112	192.168.1.113	192.168.1.126	255.255.255.240	192.168.1.127
192.168.1.128	192.168.1.129	192.168.1.142	255.255.255.240	192.168.1.143

Jokaiselle verkolle määritetään ensimmäinen mahdollinen osoiteavaruus.
Järjestyksessä Verkko A, Verkko B ja Verkko C.

Osoitteiden jakamisen jälkeen jää käytettäväksi 192.168.1.112 - 192.168.256 väliltä verkko-osoitteita, joita on mahdollisuus käyttää jos luodaan uusia työasemaverkkoja. (Kuva 5)

Verkko A	Verkko B	Verkko C
Verkko-osoite: 192.168.1.0	Verkko-osoite: 192.168.1.64	Verkko-osoite: 192.168.1.96
Reitittimen osoite: 192.168.1.1	Reitittimen osoite: 192.168.1.65	Reitittimen osoite: 192.168.1.97
Host-osoitteet: 192.168.1.2-62	Host-osoitteet: 192.168.1.66-94	Host-osoitteet: 192.168.1.98-110
Broadcast-osoite: 192.168.1.63	Broadcast-osoite: 192.168.1.95	Broadcast-osoite: 192.168.1.111
Aliverkon peite: 255.255.255.192	Aliverkon peite:255.255.255.224	Aliverkon peite: 255.255.255.240



Kuva 5. Työasemaverkot

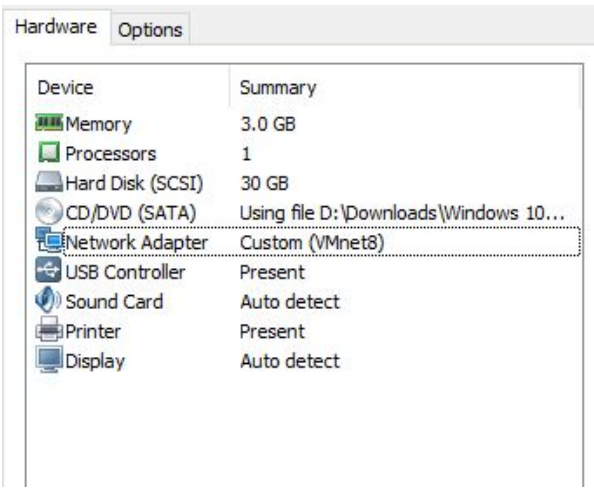
3 Järjestelmät ja työkalut

3.1 VMWare

Opinnäytetyössä käytetään VMware Workstation nimistä ohjelmistoa virtuaalitietokoneiden luontiin ja ajamiseen. Virtualisointi tässä tapauksessa tarkoittaa sitä, että luodaan ympäristö joka on tehty ohjelmallisesti, mutta vastaa fyysistä tietokone ja palvelin kokoonpanoa.

VMwaressa luodaan pohja, johon määritellään millaisia laiteresursseja sen pitää virtualisoida. Opinnäytetyön Server- ja Workstation-työkoneille on esimerkiksi varattu 3 GB keskusmuistia ja 30 GB kiintolevytilaa työasemaa kohden. VMware virtualisoi muitakin peruskomponentteja käyttäen fyysisen koneen resursseja.

Koneen tarvitsee olla melko tehokas, koska virtualisointi vaatii koneelta paljon resursseja varsinkin, jos montaa virtuaalikonetta ajetaan samanaikaisesti. (Kuva 6)

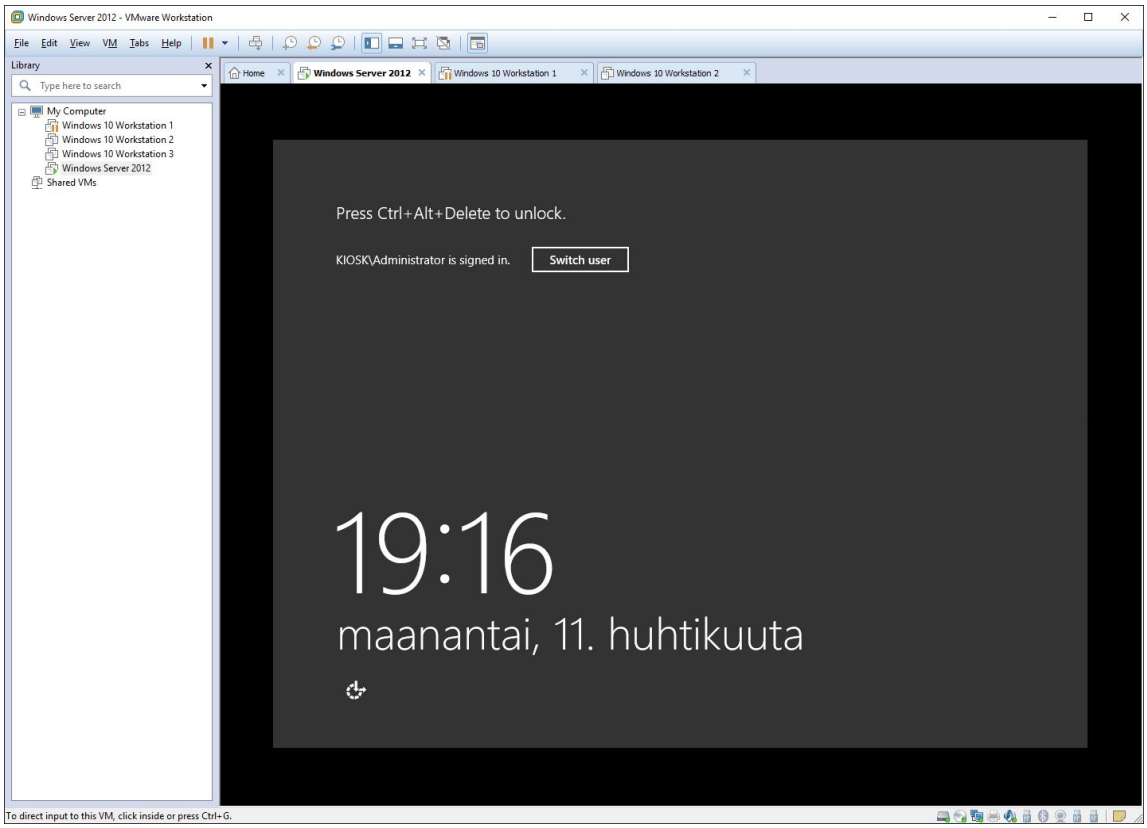


Kuva 6. Virtuaalikoneen laitteistotiedot

VMwaren käyttöliittymä on varsin yksinkertainen. Vasempaan palkkiin on listattu luodut virtuaalikoneet, jotka saa helposti päälle esimerkiksi klikkaamalla haluamansa koneen aktiiviseksi ja painamalla yläpalkista Play-painiketta.

Oikeassa ruudussa on varsinainen näyttöruutu, josta käytetään virtuaalikoneita, kuten tavallistakin PC:tä. Sen yläpuolella on välilehdet, josta voi lennossa vaihtaa toiseen virtuaalikoneeseen.

Oikealla alhaalla on erilaisia indikaattoreita, jotka kuvaavat esimerkiksi että onko ulkoisia laitteita kytketty ja saako kone verkkoyhteyden. (Kuva 7)



Kuva 7. VMware käyttöliittymä

3.2 Windows Server 2012 R2

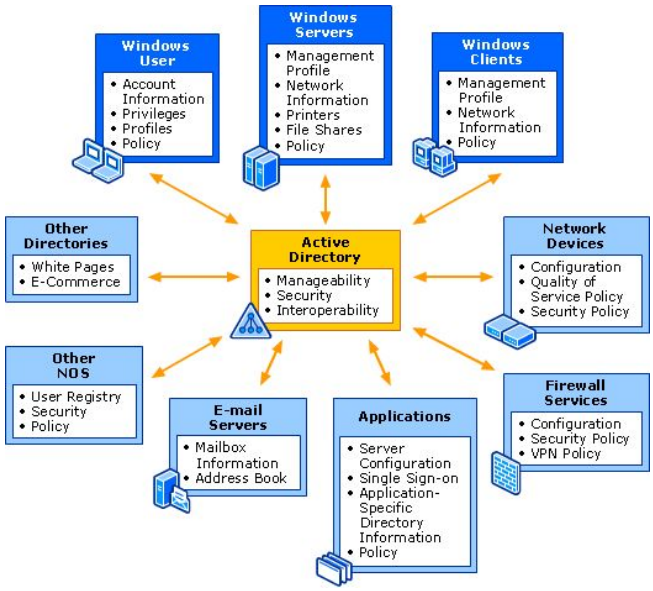
Windows Server 2012 on kuudes julkaisu Windows Server-tuoteperheessä. Se pohjautuu Windows 8:n ohjelmakoodiin, jossa on merkittäviä uudistuksia edeltäjäänsä nähden. Windows Server on nimensä mukaisesti palvelinkäyttöjärjestelmä, joka eroaa tavallisesta Windows-käyttöjärjestelmä siten, että siihen on integroitu kattava määrä työkaluja, joilla voidaan hallinnoida isompiakin yritysverkkoja.

3.2.1 Active Directory

Active Directory on joukko palveluita, joita käytetään käyttäjien, tietokoneiden ja verkkoresurssien hallinnointiin. Active Directorylle voi määrittää erilaisia rooleja, jotka pitävät sisällään erilaisia palvelukokonaisuuksia. Active Directory Services yhdistää siis tietokannan ja tarjoaa palvelut, joilla tietokantaan pääsee käsiksi. [5] (Kuva 8)

Palveluihin sisältyvät:
Active Directory Domain Services (ADDS)
Active Directory Certificate Services (ADCS)
Active Directory Federation Services (ADFS)

Active Directory Right Management Services (ADRMS)
Active Directory Lightweight Directory Services (ADLDS)

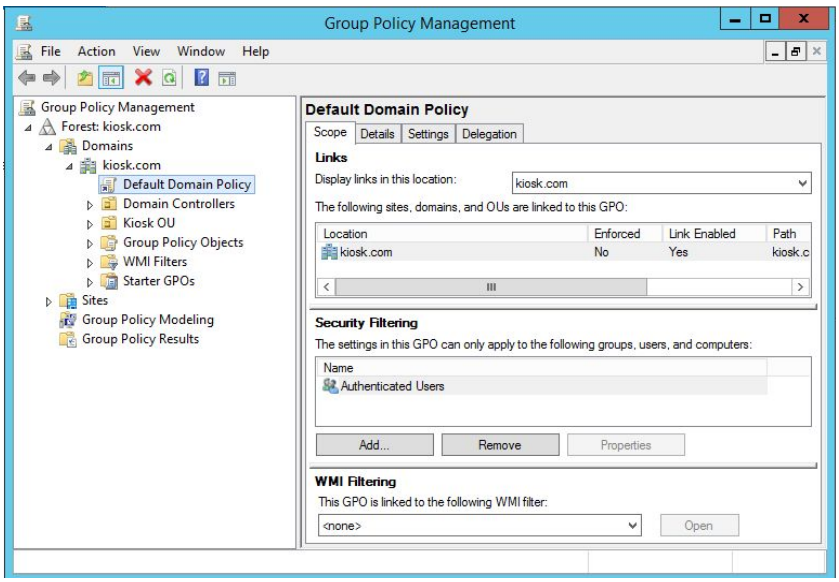


Kuva 8. Active Directory [6]

Opinnäytetyössä käytetään perinteistä Active Directory Domain Services palvelinroolia, joka tarjoaa tunnistuspalvelut, hakemistopalvelut ja ja tallennuspalvelun erilaisista objekteista.

3.2.2 Group Policy Management

Palvelinroolia määrittäessä asennetaan erikseen Group Policy Management Tool, joka tuo käytettäväksi hallintakonsolin, jolla voidaan hallita forestin kaikkien toimialueiden ja toimipaikkojen ryhmäkäytäntöobjekteja. Hallintakonsolin saa auki Server Managerin Tools-valikosta. [5] (Kuva 9)



Kuva 9. Group Policy Management

4 VMware ja Windows Server asennus

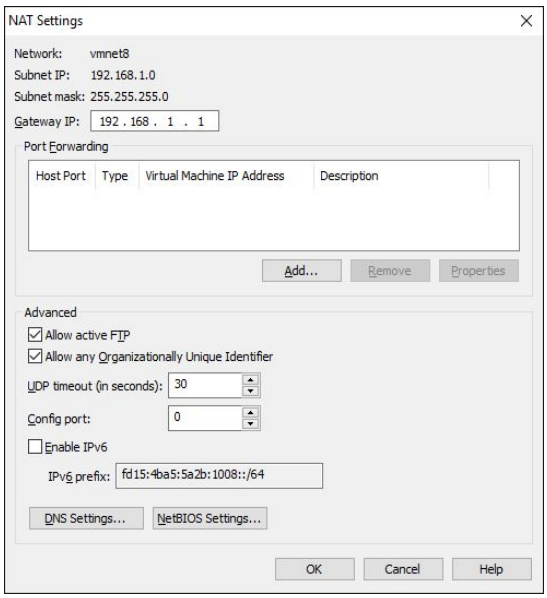
4.1 VMware verkon määritys

VMwaren Virtual Network Editorista määritellään alkuun verkkoasetukset. Kaikki virtuaalikoneet tulevat toimimaan 192.168.1.0 verkossa.

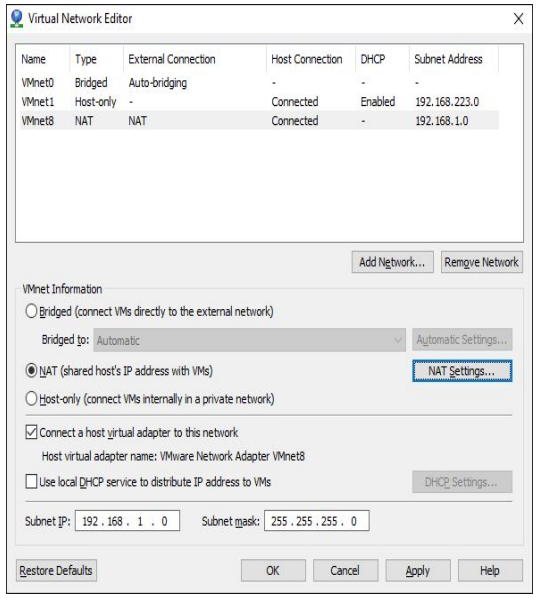
Network Editorin avulla luodaan virtuaalinen reititin, jonka kautta Internet-yhteys kulkee. Eli fyysiseltä pohjakoneelta tulee Internet-yhteys virtuaaliseen reittimeen, joka ohjaa IP-osoitteet NAT:n avulla virtuaalikoneille.

Tässä vaiheessa DHCP:tä ei oteta käyttöön, vaikka sen saisikin määritettyä VMwaren verkkoasetuksiin. Tarkoitus on luoda oma DHCP-palvelin Windows palvelimen kautta. (Kuvat 10, 11 ja 12)

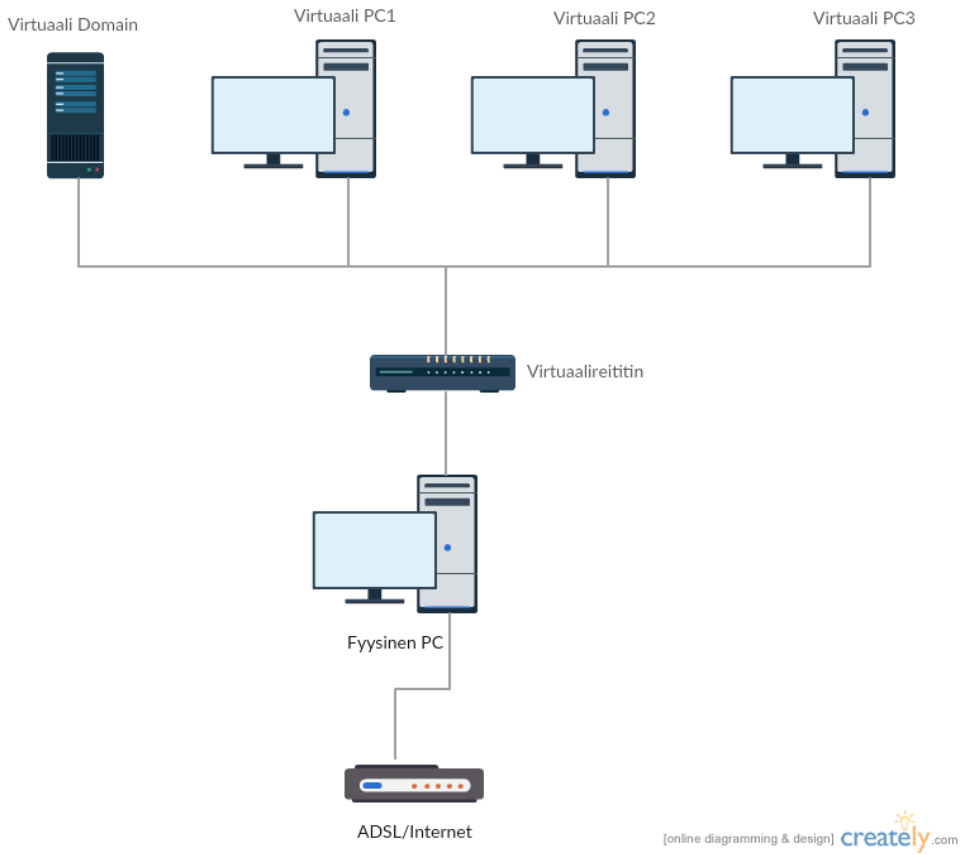
Verkko: 192.168.1.0
Oletusyhdyskäytävä: 192.168.1.1
Aliverkon peite: 255.255.255.0
NAT: Enabloitu
DHCP: Disabloitu
IPv6: Disabloitu



Kuva 10. Verkko-asetukset

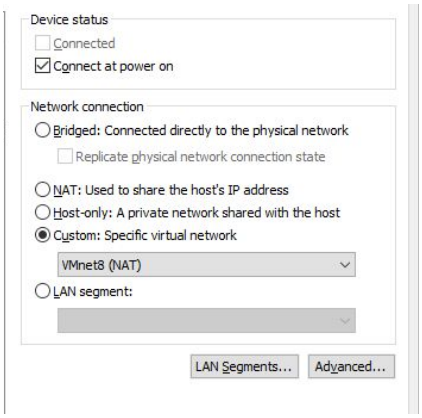


Kuva 11. NAT-asetukset



Kuva 12. Verkkokaavio

Virtuaalikoneiden asetuksiin määritetään tämän jälkeen, että kaikki käyttävät VMnet8 (NAT) verkkoa. (Kuva 13)

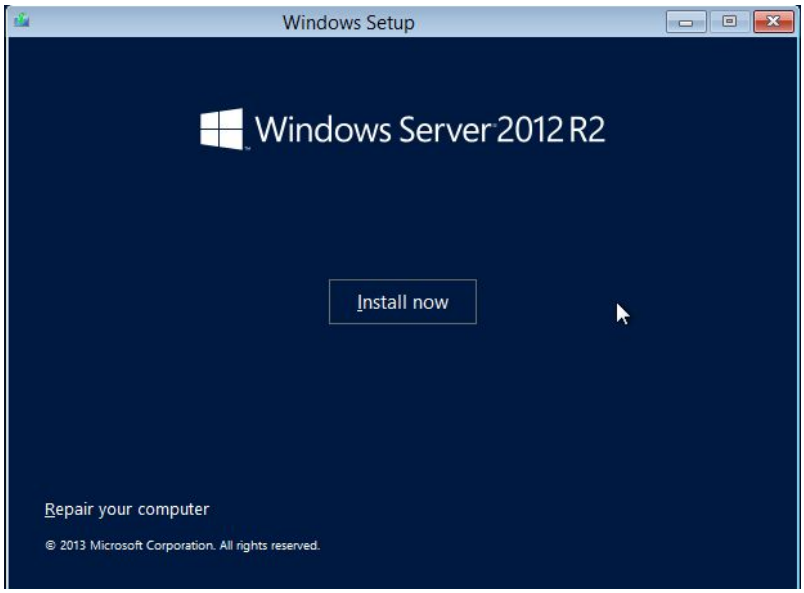


Kuva 13. VMnet 8 (NAT)

4.2 Windows Server ja Windows 10 asennus

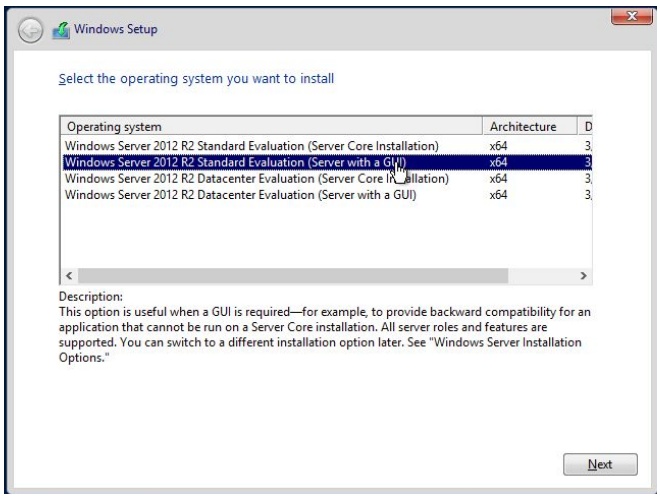
Asennetaan käyttöjärjestelmät omille virtuaalikoneilleen. Käydään läpi ainoastaan Windows Server-asennus, koska asennusprosessi on molemmissa käyttöjärjestelmissä hyvin samanlainen.

1. Bootataan virtuaalikone Windows Server 2012 R2 imagella.
Tämän jälkeen avautuu asennusikkuna, josta valitaan Install Now. (Kuva 14)



Kuva 14. Asennus-ikkuna

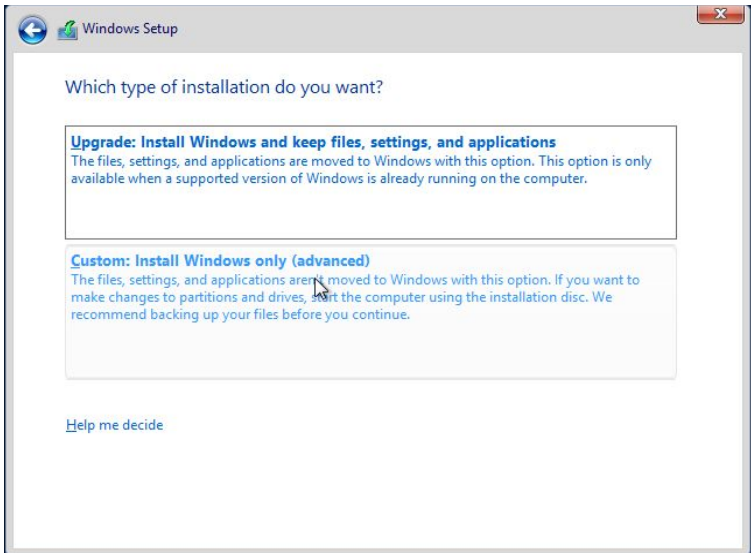
2. Valittavaksi tulee eri versiota, Standard ja Datacenter versio, joko graafisella käyttöliittymällä (GUI) tai ilman. Valitaan Standard-versio graafisella käyttöliittymällä. (Kuva 15)



Kuva 15. Version valinta

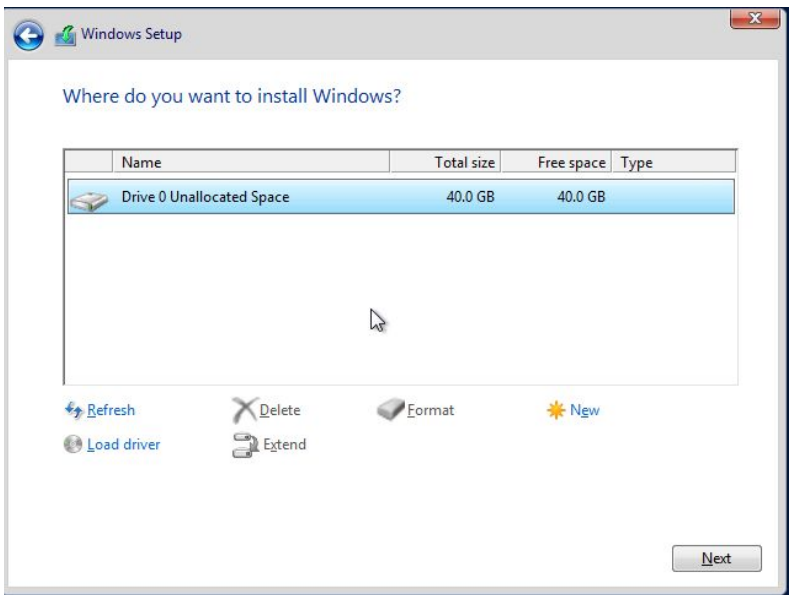
3. Seuraavaksi sinua pyydetään hyväksymään lisenssioikeudet. Valitaan “I accept licence terms” ja painetaan Next.

4. Vaihtoehdoiksi tulee joko Upgrade- tai Custom-asennus. Valitaan Custom-asennus. Upgrade-asennus on käytettävissä ainoastaan, jos koneelle olisi asennettu aikaisemmin vanhempi versio Windows Server-käyttöjärjestelmästä. (Kuva 16)



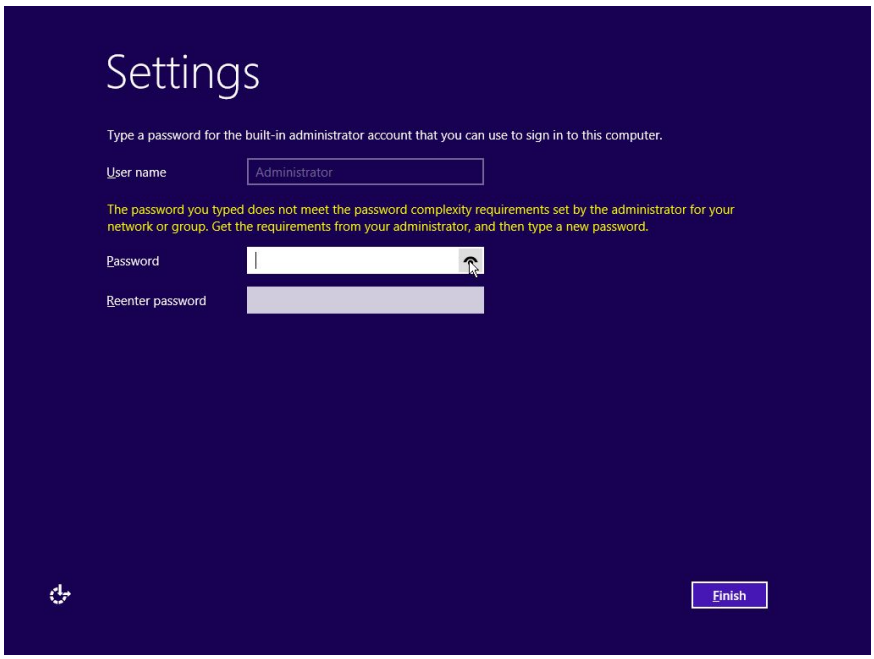
Kuva 16. Upgrade- ja Custom-asennus

5. Seuraavaksi valitaan kiintolevy, johon käyttöjärjestelmä halutaan asentaa. Halutessaan voi myös osioida kiintolevyn pienempiin osiin. Tässä tapauksessa ei osiointia tarvita vaan asennetaan käyttöjärjestelmä koko kiintolevylle. (Kuva 17)



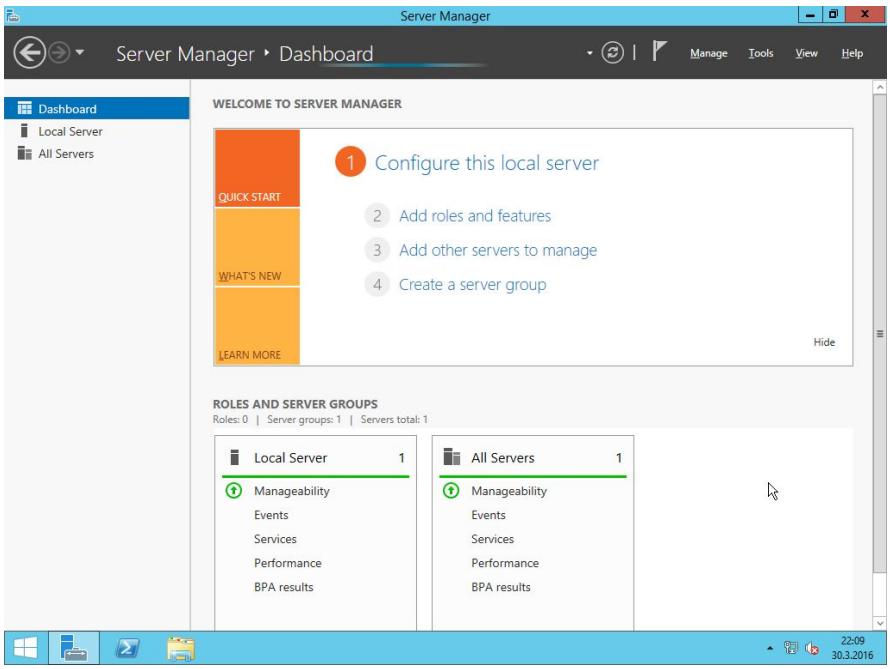
Kuva 17. Kiintolevyn osiointi

6. Edellisten toimenpiteiden jälkeen Windows alkaa asentumaan. Asennuksen jälkeen tulee Asetukset-ikkuna, jossa määritetään käyttäjätunnus ja salasana, jonka täytyy täyttää Windowsin turvallisuusvaatimukset. Salasanan täytyy sisältää pieniä tai suuria kirjaimia, numeroita, erikoismerkkejä ja oltava vähintään 8-merkkiä pitkä. (Kuva 18.)



Kuva 18. Admin-käyttäjän luonti

7. Asennus on suoritettu loppuun ja Windows Server on asennettu onnistuneesti. Näytölle avautuu työpöytä ja Server Manager-hallinnointi sovellus. (Kuva 19)

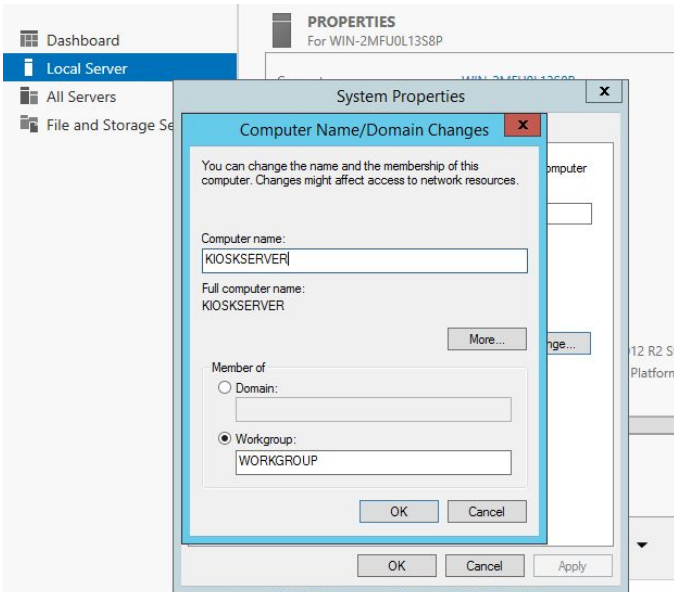


Kuva 19. Windows Server 2012 R2 alkunäkymä

5 Active Directory ja Domain Controller

5.1 Palvelinkoneen nimeäminen

Koneelle kannattaa määrittää uusi nimi, joka helpottaa myöhemmin asetusten tekoa. Tämä saadaan muutettua menemällä Server Managerissa välilehdelle Local Server, klikataan Computer Name kohdassa tietokoneen nykyistä nimeä ja valitaan Change. Tänne syötetään nimikenttään KIOSKSERVER, joka tulee olemaan palvelintietokoneen nimi. (Kuva 20)

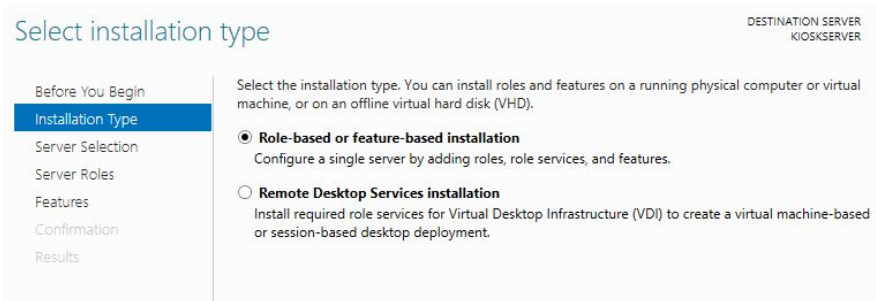


Kuva 20. Koneen nimeäminen

5.1.1 AD:n luonti

1. Server Managerista valitaan Manage välilehdeltä Add Roles and Features ja klikataan Next.

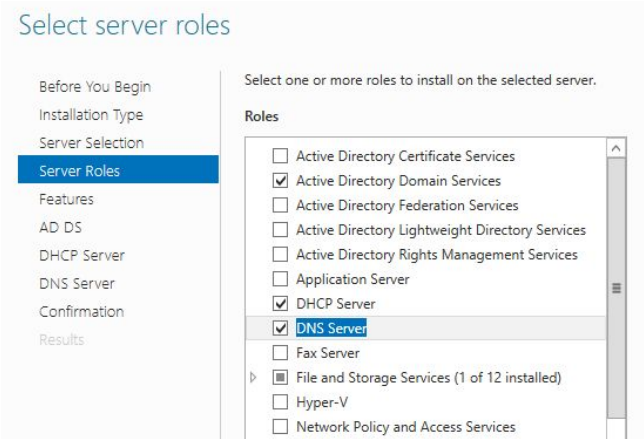
2. Asennustyypiksi valitaan Role-based or feature-based installation. (Kuva 19)



Kuva 21. Asennustyyppi

3. Server Selection kohdassa valitaan Server Pool kohdassa KIOSKSERVER-palvelin, jonka pitäisi olla automaattisesti valittavissa, jos kone saa verkkotiedot normaalisti reitittimen kautta.

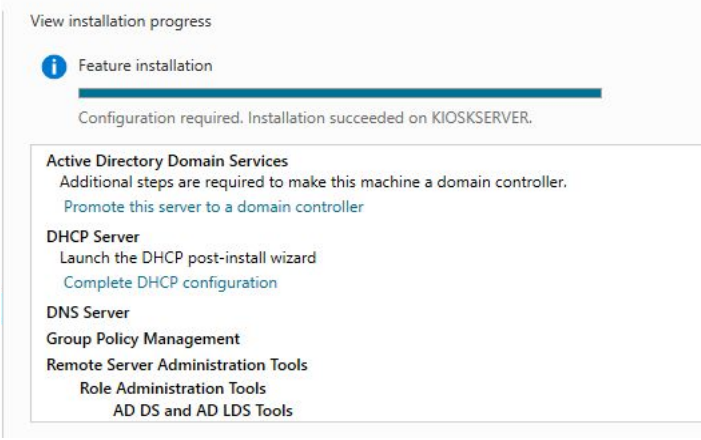
4. Server Roles välilehdellä valitaan aktiivisiksi Active Directory Domain Services, DHCP Server ja DNS Server. (Kuva 22)



Kuva 22. Palvelinroolit

5. Add Features kohdassa voi valita mahdollisia lisäominaisuuksia jotka haluaa asentaa. Valitaan Group Policy Management työkalu, jolla myöhemmin määritetään rajoituksia Kiosk-tietokoneille.

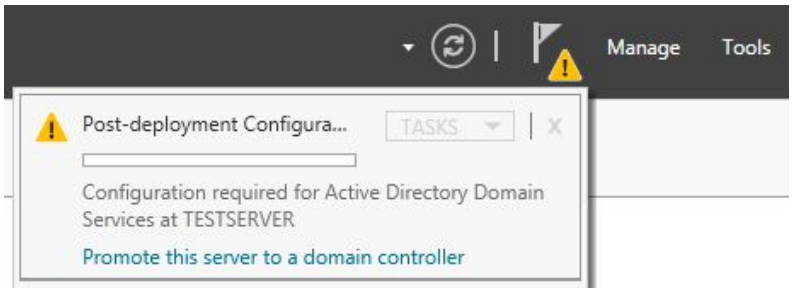
6. DHCP- ja DNS-server välilehdillä ei tarvitse painaa kuin Next ja kaikki aiemmin määritetyt asetukset asentuvat painamalla Install. Kun asennus on valmis, kone pitää käynnistää uudelleen. (Kuva 23)



Kuva 23. Asennusprosessi

5.1.2 Domain Controller

Kun Active Directory on asennettu, niin sen jälkeen palvelin ylennetään Domain Controlleriksi. Tämän saa tehtyä Server Managerin ilmoitusikkunasta, josta tehdään Post-deployment Configuration. (Kuva 24)

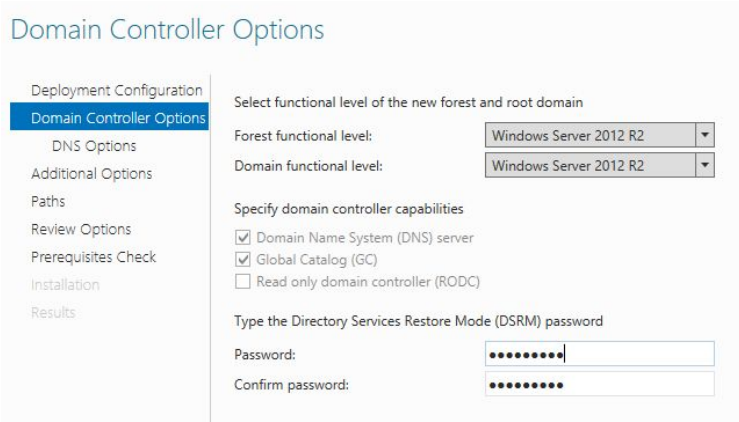


Kuva 24. Post-deployment Configuration

1.Luodaan uusi metsä ja määritetään Root-domainille nimi kiosk.com. (Kuva 25)

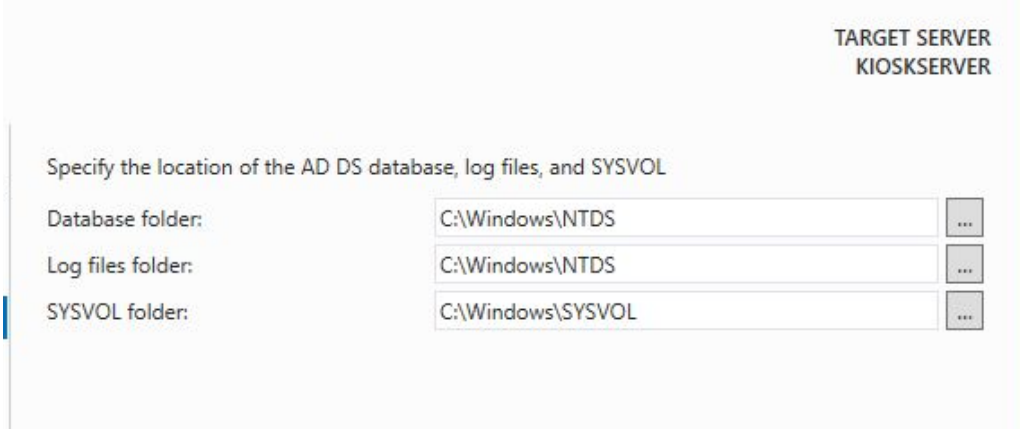
Kuva 25. Deployment Configuration

2. Annetaan domainin ja metsän toiminnallisuustasot, joihin valitaan Windows Server 2012 R2. Määritellään Administrator-käyttäjän salasana, jonka avulla ohjauspalvelin voidaan käynnistää Directory Services Restore Mode-tilassa, joka on domain controllerin vikasietotila. Tämän jälkeen DNS-välilehdellä on mahdollisuus valtuuttaa erillisiä DNS-palvelimia, jos verkossa niitä on. (Kuva 26)



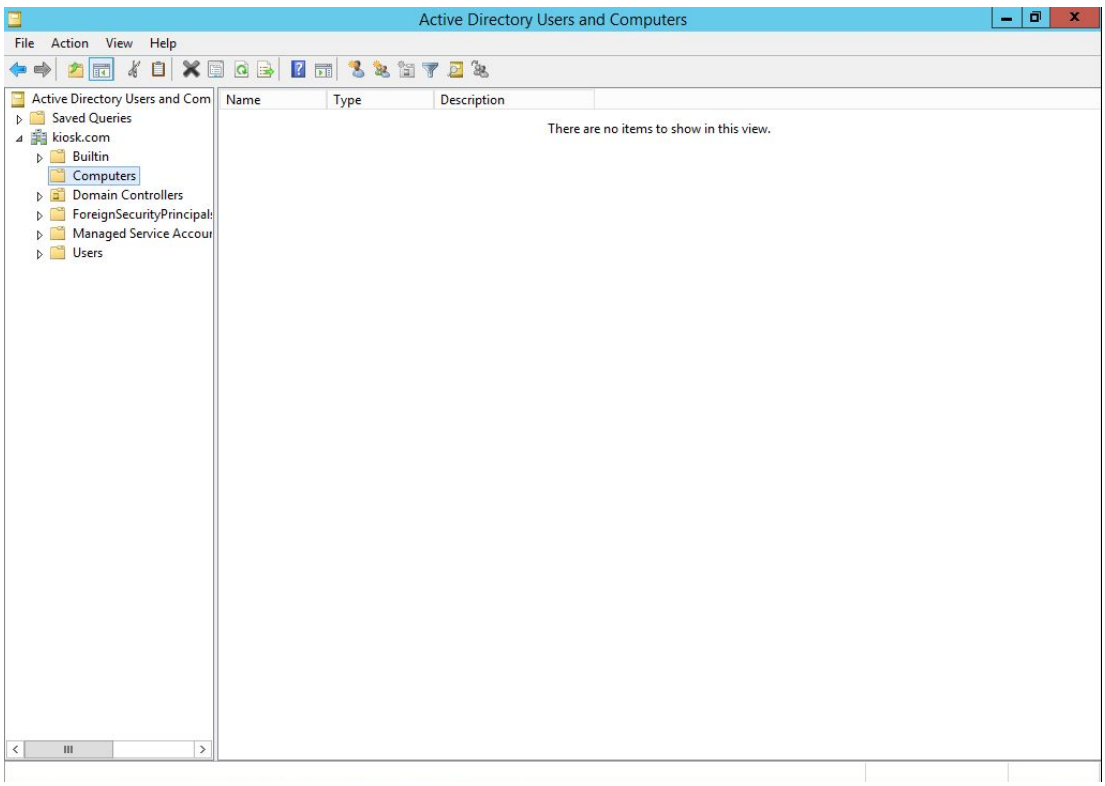
Kuva 26. Domain Controller-asetukset

3. Määritellään NETBIOS-nimi, jonka maksimipituus saa olla 15 merkkiä, isoilla kirjaimilla ja hyväksytään painamalla Next. Seuraavaksi määritetään Database (tietokannat), Log files (logit) ja SYSVOL (julkisten tiedostojen sijainti) kansiot. Suorituskyvyn kannalta nämä siirretään usein ulkoiselle asemalle, mutta tässä tapauksessa jätetään oletuskansiot.(Kuva 27)



Kuva 27. Hakemistojen määrittäminen

4. Asetusten teon jälkeen käyttäjälle tulee ikkuna, jossa on yhteenveto asetuksista. Klikataan Install ja varsinainen asennus alkaa. Kone käynnistetään uudelleen ja tämän jälkeen Server Managerin Tools-valikosta avataan Active Directory Users and Computers-konsoli. Työkalulla voidaan hallita toimialueita, ominaisuuksia, käyttäjiä, ryhmiä, tietokoneita, organisaatioyksiköitä ja ryhmäkäytäntöjä.(Kuva 28)

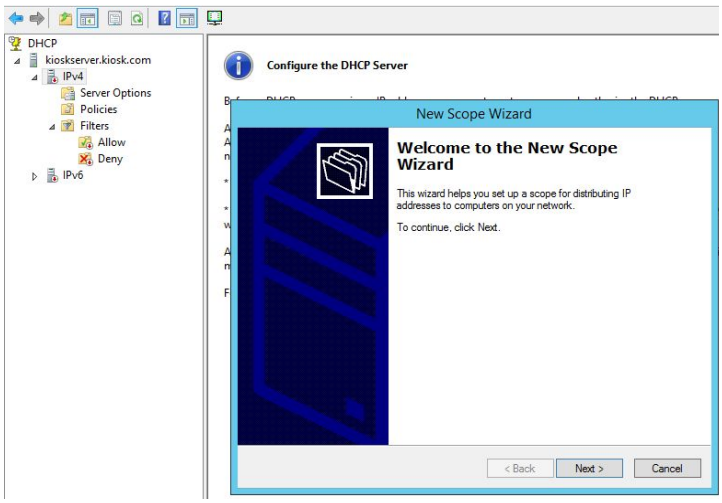


Kuva 28. Active Directory-hallintakonsoli.

5.1.3 DHCP-Scope

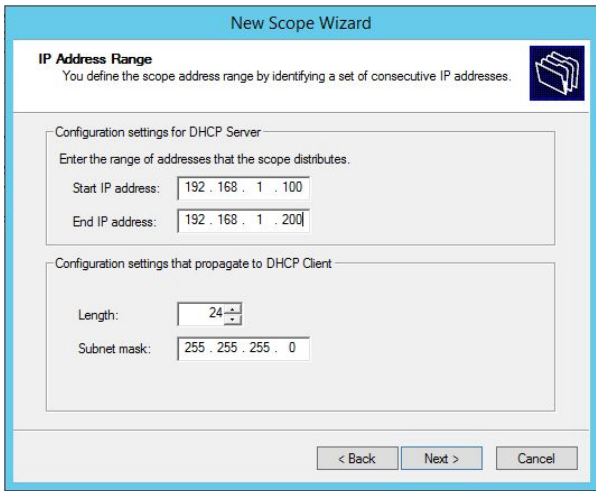
Tarkoitus on määritellä DHCP-Scope, joka antaa 192.168.1.100-192.168.1.200 alueelta IP-osoitteet Kiosk-työasemille. Toimivuus tarkistetaan käynnistämällä myöhemmin Kiosk-työasema. Käynnistyksen jälkeen katsotaan, onko se saanut DHCP:n kautta määritetyt asetukset.

1.Server Managerin Tools-valikosta avataan DHCP. DHCP-konsolissa klikataan IPv4-kenttää oikealla hiiren painikkeella ja valitaan New Scope, jonka jälkeen käynnistyy asennusvelho. (Kuva 29)



Kuva 29. DHCP-Scope

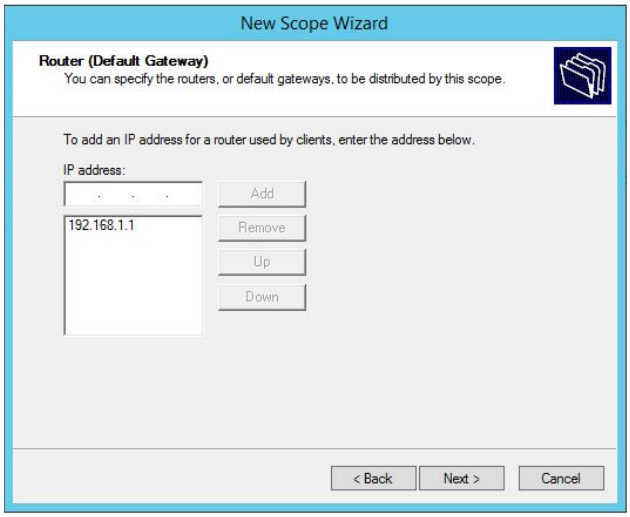
2. Määritellään seuraavaksi Scopelle nimi, joka tulee olemaan Basic. Tämän jälkeen tulee ikkuna, jossa määritellään verkko-alue. Annetaan aiemmin määritetyt arvot ja klikataan Next. (Kuva 30)



Kuva 30. IP-osoitteiden määritys

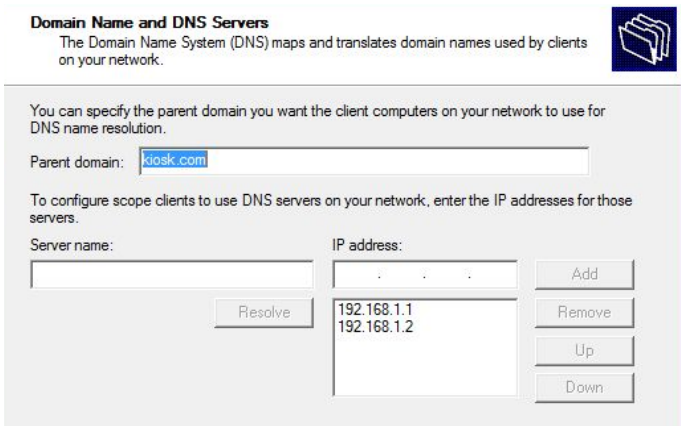
3. Seuraavissa ikkunoissa voidaan määritellä, jos halutaan lisätä poikkeuksia tietyille IP-osoitteille ja mahdollinen lease-duration, eli kuinka kauan IP-osoite pysyy käyttäjällä, kunnes se vaihtuu. Poikkeuksia ei tehdä ja lease-time jätetään vakioksi, eli 8 päivää.

4. Seuraavaksi tulee ikkuna, jossa kysytään, haluaako käyttäjä tehdä muutoksia Default Gateway, DNS ja WINS-palvelin asetuksiin. Valitaan “Yes, I want to configure these options Now”, koska tänne saadaan määriteltyä reitittimen oletusyhdyskäytävä. Kirjoitetaan IP address-kenttään 192.168.1.1 ja lisätään painamalla Add. (Kuva 31)



Kuva 31. Default Gatewayn määrittäminen

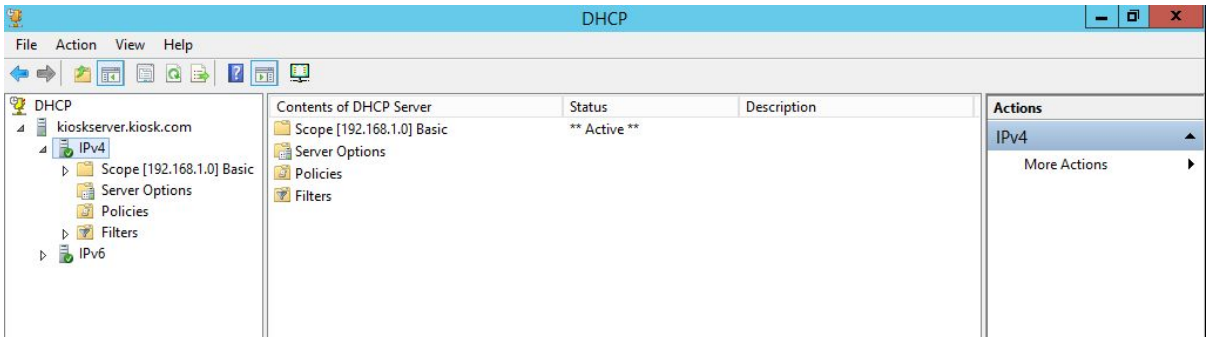
5. DNS-ikkunassa varmistetaan, että Parent domain-kohdassa on kiosk.com ja IP-osoitteet on oikein määritelty. WINS-ikkuna jätetään tyhjäksi, koska sitä ei käytetä. (Kuva 32)



Kuva 32. DNS-palvelin osoitteet

6. Jatketaan asennus loppuun valitsemalla “Yes, I want to activate this scope now” ja painetaan Finish. Viimeinen tehtävä on valtuuttaa DHCP-palvelin, jotta luvattomat DHCP-palvelimet eivät pystyisi palvelemaan toimialueen asiakkaita. Klikataan oikealla hiiren klikkauksella domain-nimeä (kioskserver.kiosk.com) ja valitaan Authorize.

Tämän jälkeen voidaan tarkastella Address Leases kentästä, että DHCP-scope on aktivoitunut.(Kuva 33)



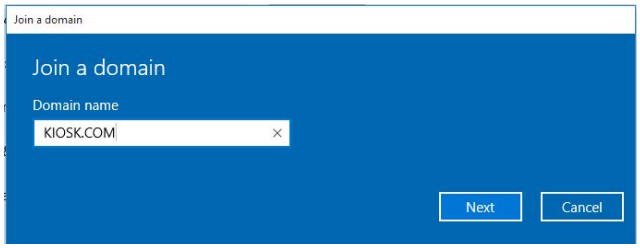
Kuva 33. DHCP-scope

5.2 Kiosk työasemien yhdistäminen AD:hen

Tarkoitus on liittää Windows 10 Kiosk-työasemat Windows Server 2012 domainiin. Työasemista tarkistetaan, että ne ovat yhteydessä domainiin ja saavat tarvittavat osoitteet DHCP:n kautta.

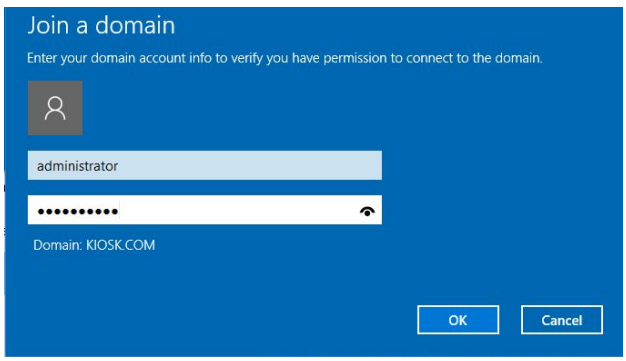
1. Avataan Windows 10:n kautta Settings -> System -> About.

2. Valitaan “Join a Domain” ja kirjoitetaan kenttään domain-osoite KIOSK.COM. (Kuva 34)



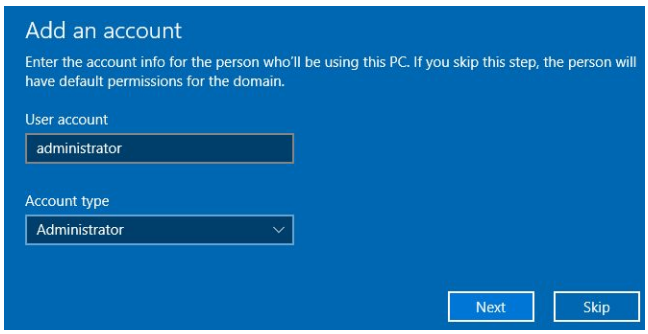
Kuva 34. Join a domain

3. Kirjoitetaan Domainin käyttäjätunnus ja salasana. (Kuva 35)



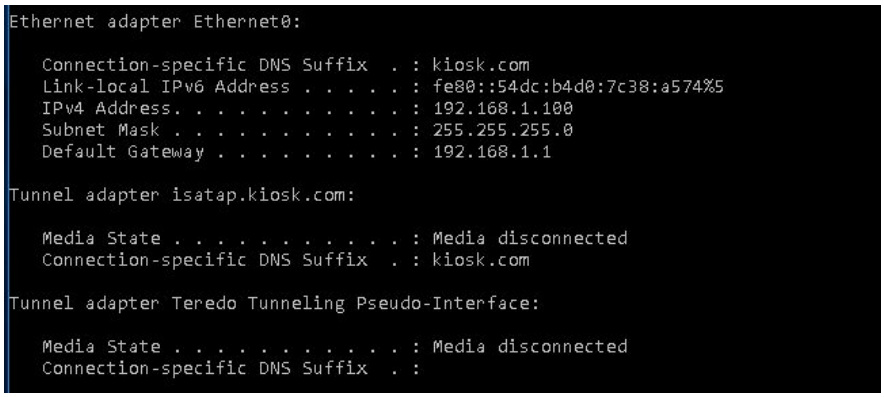
Kuva 35. Käyttäjätunnukset

3. Määritetään käyttäjätili tyyppi ja jatketaan painamalla Next, jonka jälkeen kone käynnistetään uusiksi ja työasema on liitetty onnistuneesti domainiin. (Kuva 36)



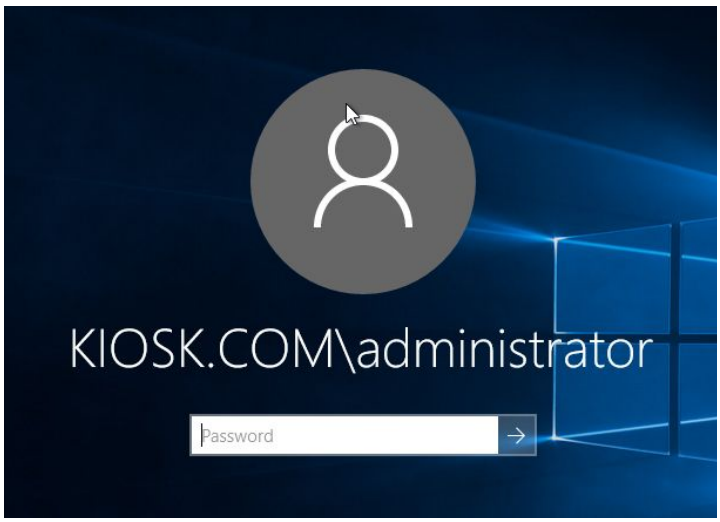
Kuva 36. Tilityyppi

4. Varmistetaan Windowsin Command Promptissa ipconfig komennolla, että työasema on yhdistetty domainiin ja saa tarvittavat osoitteet, eli kone saa DHCP:n avulla DNS:n, Default Gatewayn, IP-osoitteen ja Subnet Maskin. (Kuva 36)



Kuva 36. Ipconfig

5. Tämän jälkeen työasemalle pääsee kirjautumaan domainin tunnuksilla. (Kuva 37)

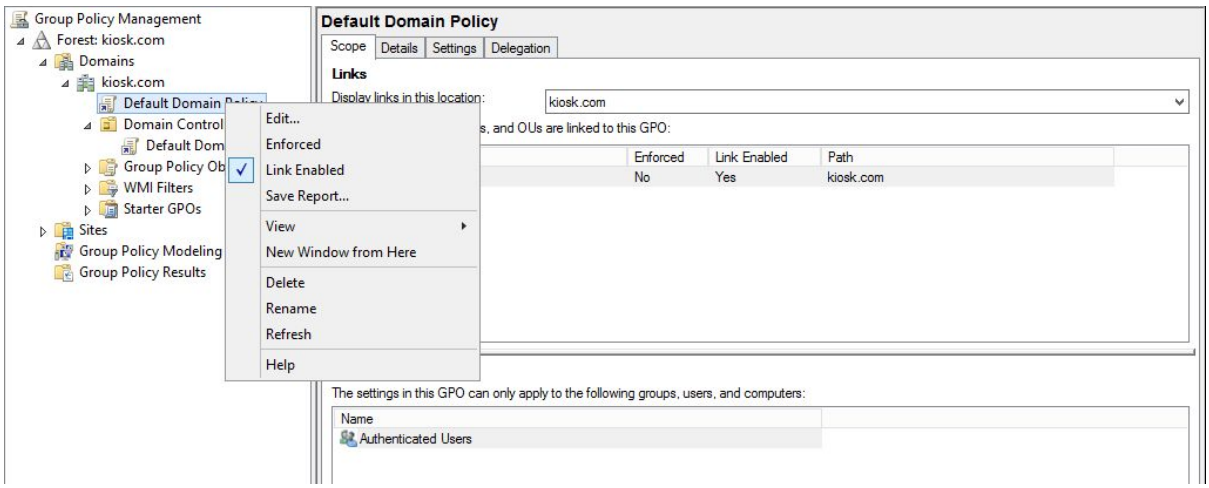


Kuva 37. Kirjautumiskonsoli

5.3 Salasanan disablointi ja uuden käyttäjän luonti Windows Serverissä

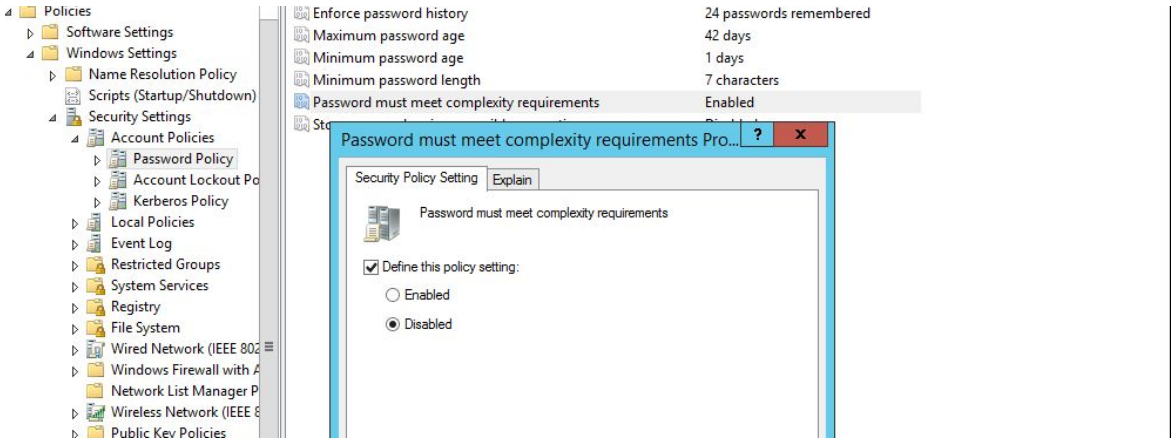
Oletuksena Windows Server vaatii salasanan käyttäjätiliä luotaessa, mutta tässä tilanteessa kun luodaan Kiosk-työasemaa niin halutaan, ettei salasanaa ole ja kone kirjautuu automaattisesti sisään.

1. Avataan Group Policy Management, josta klikataan Default Domain Policy- painiketta oikealla hiiren näppäimellä ja valitaan Edit. (Kuva 38)



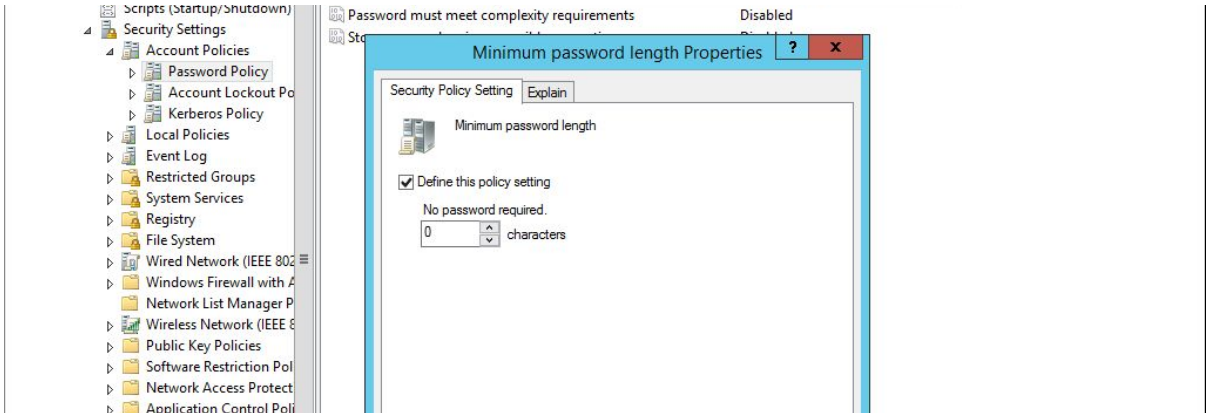
Kuva 38. Group Policy Management

2. Security Settings - > Password Policy kohdasta annetaan “Password must meet complexity requirements”-asetukselle arvo Disabled. (Kuva 39)



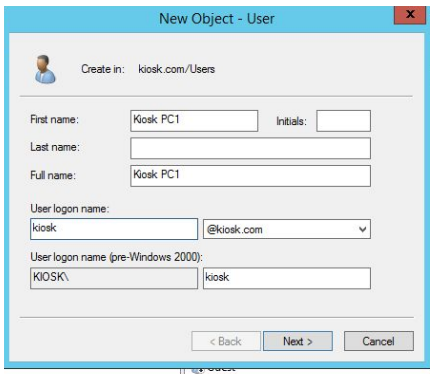
Kuva 39. Password

3. Määritetään salasanan maksimipituudeksi nolla merkkiä asetuksesta “Minimum password length”. (Kuva 40)



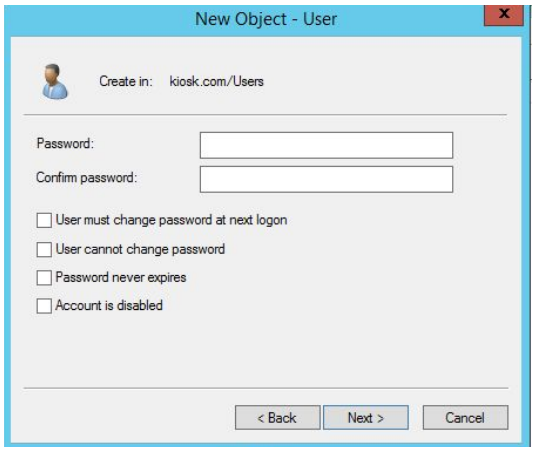
Kuva 40. Minimum password length

4. Määritetään uusi käyttäjä luomalla uusi käyttäjä objekti. (Kuva 41)



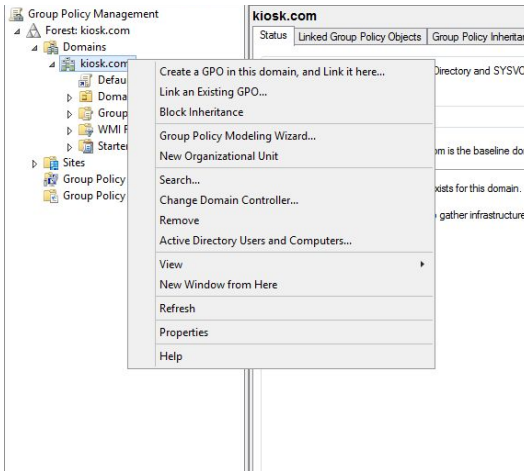
Kuva 41. Käyttäjän luonti

5. Jätetään salasanakentät tyhjäksi painetaan Next.
Finish painikkeella hyväksytään tehdyt asetukset. (Kuva 42)



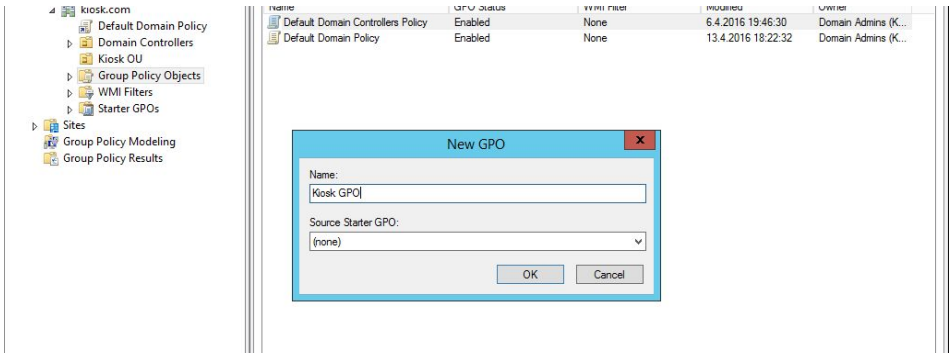
Kuva 42. Käyttäjän salasana

6. Seuraavaksi luodaan uusi Organizational Unit johon liitetään Kiosk-työasemat. Valitaan New Organizational Unit Group Policy Managementista ja nimetään se Kiosk OU:ksi. (Kuva 43)



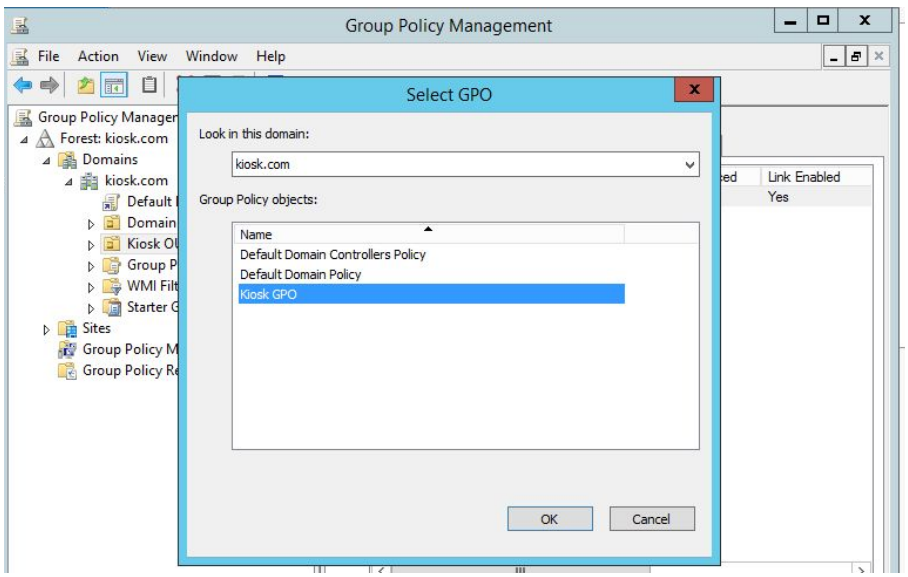
Kuva 43. Kiosk OU

7. Luodaan uusi Group Policy-objekti kohtaan Group Policy Objects ja nimetään se Kiosk GPO:ksi. (Kuva 44)



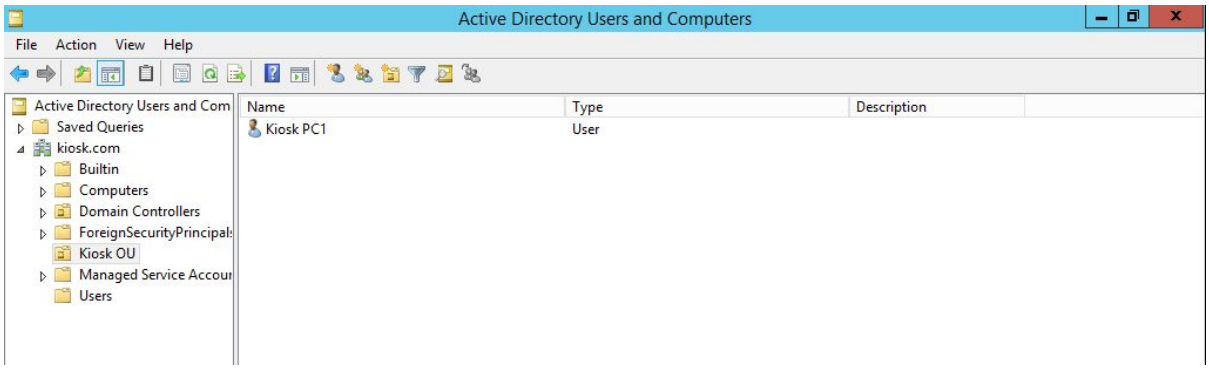
Kuva 44. Kiosk GPO

8. Liitetään juuri luotu GPO-objekti Kiosk OU-ryhmään. Valitsemalla oikealla hiiren painikkeella Kiosk OU:sta Link an existing GPO. (Kuva 45)



Kuva 45. GPO-linkitys

9. Siirretään aiemmin luotu Kiosk PC1 käyttäjä Kiosk OU-ryhmään. (Kuva 46)



Kuva 46. Kiosk PC1-käyttäjä

Luodaan vielä Kiosk PC2-käyttäjä, jolle tehdään sama operaatio kuin PC1-käyttäjälle. Tämän vaiheen jälkeen on luotu perus pohja ja käyttäjärajoituksia annetaan työasemille Group Policy Managementin kautta.

6 Kiosk-PC:n luonti ja rajoitukset

Luodaan aluksi yksinkertaisin variaatio ilman sen ihmeellisempiä rajoituksia.
Koneen on tarkoitus käynnistyä niin, että pelkkä selainikkuna aukeaa kokoruututilaan. Eikä käyttäjä voi tehdä koneella muuta kuin navigoida selaimen kanssa.

6.1 Kiosk PC1

Avataan Group Policy Management ja tehdään seuraavat asetukset Kiosk PC1:lle.

1. Pakotetaan Internet Explorer avautumaan kokoruututilassa.

Computer Configuration – Administrative Templates – Windows Components – Internet Explorer

Enforce full-screen mode - Enabled

2. Pakotetaan Internet Explorer käynnistymään muiden ohjelmien sijaan

User Configuration\Policies\Administrative Templates\System

Enable Custom User Interface - Enabled
c:\Program Files\Internet Explorer\iexplore.exe

3. Määritetään kotisivuksi **http://www.wikipedia.fi**

Windows Components\Internet Explorer

“Disable changing home page settings” - Enabled
http://www.wikipedia.fi

4. Poistetaan Task Manageri käytöstä.
System\CTRL+ALT+DEL
Remove Task Manager - Enabled

5. Luodaan 3 rekisteriavainta, jotka mahdollistavat käyttäjän automaattisen kirjautumisen

Computer Configuration\Preferences\Windows Settings\Registry.

\[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\]

"DefaultUserName"="Kiosk PC1"

"AutoAdminLogon"="1"

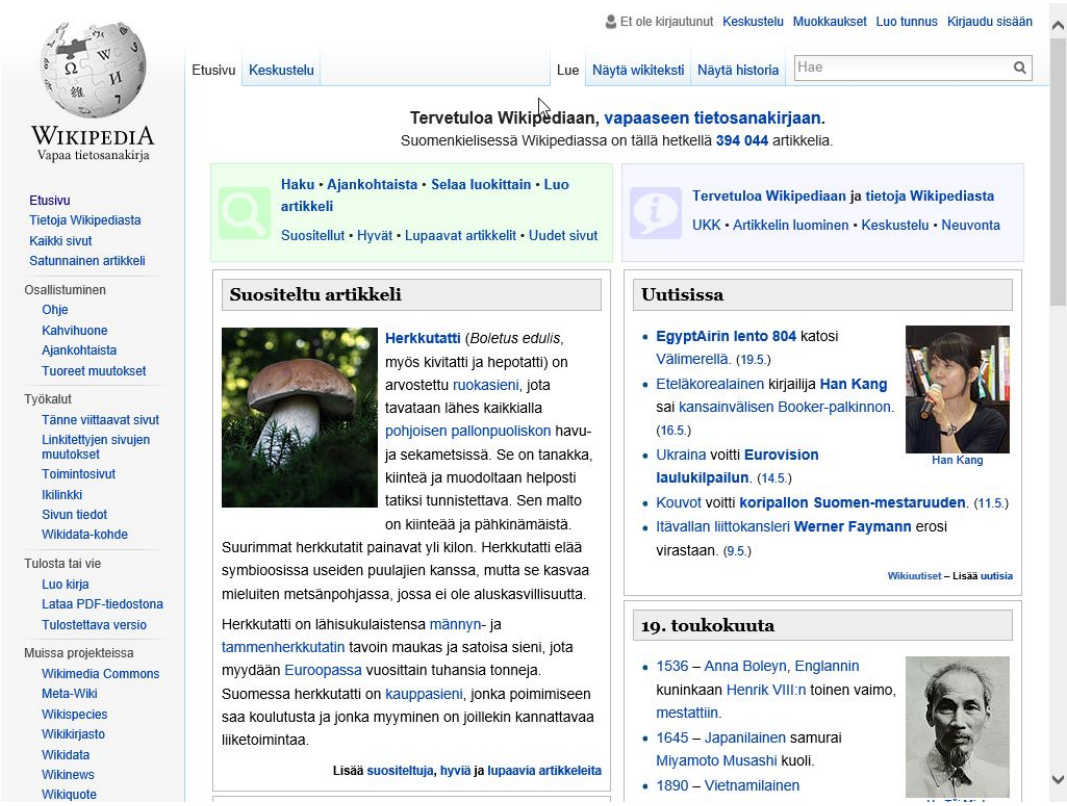
"DefaultPassword"=" "

6. Disabloidaan CTRL+ALT+DELETE näppäinyhdistelmä rekisteriasetuksella, joten käyttäjä ei pääse vaihtamaan käyttäjätunnusta tai pääse muihinkaan asetuksiin.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Keyboard Layout]
"Scancode Map"=hex:00,00,00,00,00,00,00,00,05,00,00,00,38,00,38,00,1d,00,1d,00,
38,e0,38,e0,1d,e0,1d,e0,00,00,00,00

7. Kun asetukset on määritetty niin päivitetään asetukset Command Promptissa komennolla gpupdate /force.

Käynnistetään Kiosk-työasema ja kone käynnistyy suoraan Internet Explorerin kokoruutu-tilaan ja käyttäjällä ei ole käytettävissään kuin itse nettiselain. (Kuva 47)



Kuva 47. Kiosk PC1-käyttöliittymä

6.2 Kiosk PC2

Tarkoitus on tehdä monimutkaisempi variaatio, jossa käyttäjästä otetaan webkameralla valokuva hänen kirjautuessaan sisään. Tähän käytetään ohjelmaa nimeltä CommandCam, jolle luodaan skripti joka käynnistää ohjelman heti, kun käyttäjä on kirjautunut.

Käyttäjältä estetään pääsy kaikkialle muualle paitsi My Documents, My Music, My Pictures, My Videos ja Downloads kansioihin. Jos käyttäjä luo tänne tiedostoja, niin ne tyhjentyvät kun käyttäjä kirjautuu ulos.

Käyttäjällä on käytettävissään Chrome-selain, johon asennetaan Kiosk-lisäosa, joka pakottaa Chromen kokoruututilaan ja estää Chromen omien pikanäppäinten käytön.
Asennetaan Windows Taskbarin tilalle erillinen launcheri, koska muuten Chrome peittää koko taskbarin eikä käyttäjä pääse pois Chromesta.

Asennetaan AutoHotkey ohjelma ja luodaan skripti, joka estää oikean hiiren klikkauksen. Tämä estää käyttäjää tekemästä muutoksia launcheriin.

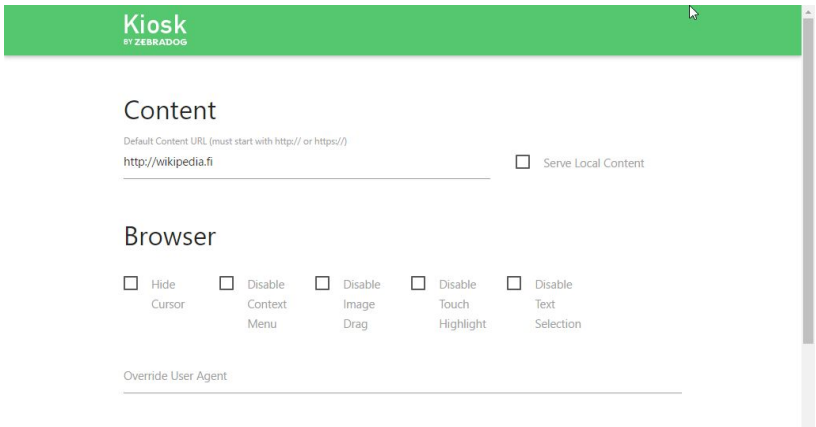
Määritetään verkkosivuille Whitelist-suodatin, joka estää pääsyn kaikkiin verkkosivuihin, joita ei ole määritetty listaukseen.

Kaikki muut ohjelmat estetään paitsi Paint, AutoHotKey, Nexus Launcher, Wordpad, Google Chrome ja CommandCam.

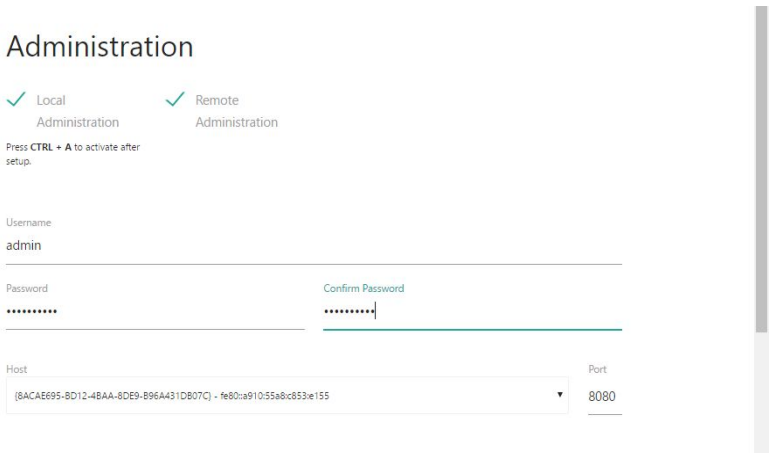
6.2.1 Työaseman valmistelu

1. Aloitetaan asentamalla tarvittavat ohjelmistot, eli AutoHotKey, Nexus Launcher, Google Chrome, Kiosk-lisäosa Chromeen ja CommandCam. Tämän voi tehdä, joko asentamalla .MSI-paketit suoraan Group Policy Managementin kautta taikka suoraan työasemalta.

2. Kun ohjelmat on asennettu niin määritetään asetukset Kiosk-lisäosaan. Määritetään aloitussivu http://wikipedia.fi, annetaan käyttäjätunnus, salasana ja määritetään etäkäytön mahdollisuus. (Kuva 48 ja Kuva 49)

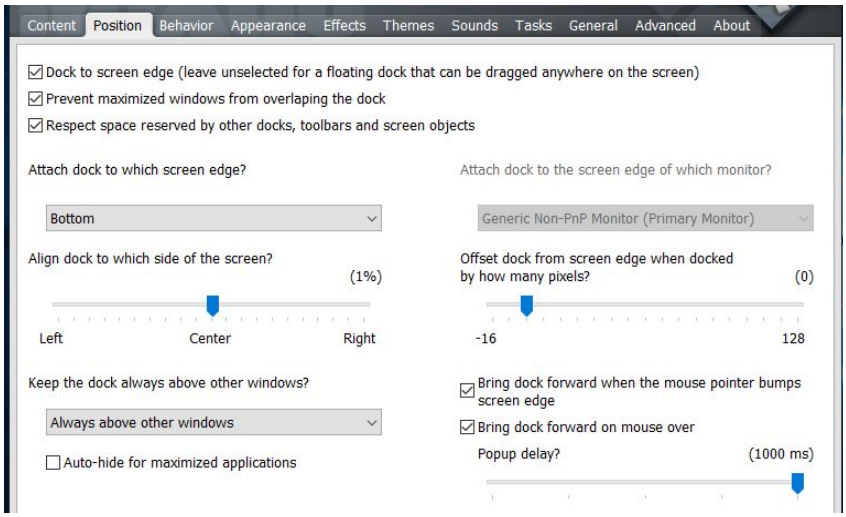


Kuva 48. Kiosk-lisäosan asentaminen



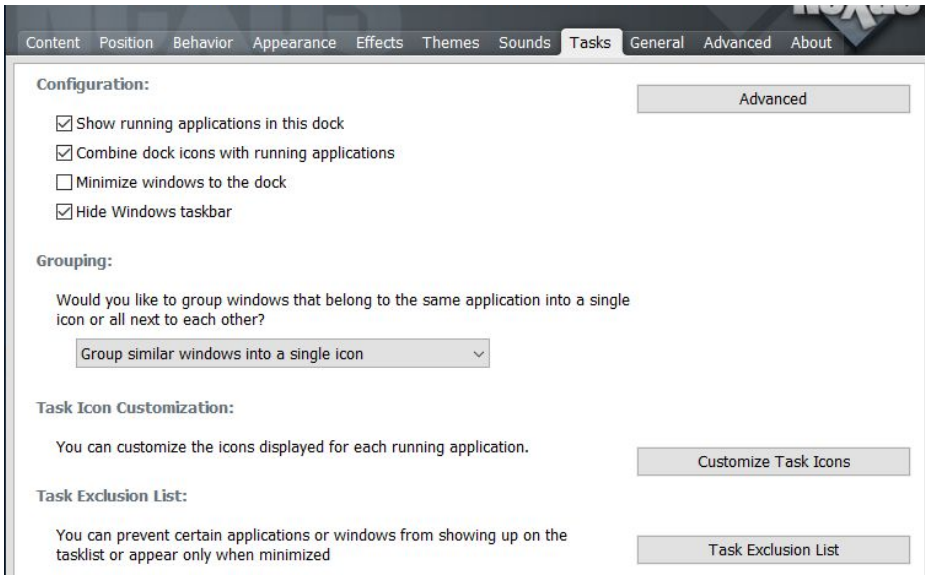
Kuva 49. Kiosk-lisäosan määrittely

3. Määritetään Nexus-launcheriin asetukset. Valitaan Position kentästä, että Launcher sijoittuu aina keskelle ruudun alalaitaan ja on aina päällimmäisenä. (Kuva 50)



Kuva 50. Nexus-asetukset

4. Määritetään vielä Tasks-välilehdeltä, kohta “Hide Windows Taskbar”, jonka jälkeen Windowsin oma Taskbar katoaa. (Kuva 51)



Kuva 51. Nexus-asetukset Tasks-välilehti

5. Määritetään tarvittavat pikakuvakkeet Launcheriin raahaamalla ne siihen. Launcherissa ovat pikakuvakkeet Kello, Kiosk-selain, Wordpad, Paint, Tyhjennyskripti- ja Uloskirjautumis-painike. (Kuva 52)

Kuva 52. Nexus Launcher

6. Tyhjennys-skripti painikkeesta Kiosk-selain sulkeutuu pois kokoruuduntilasta ja tyhjentää samalla selaimen sivuhistorian, evästeet ja välimuistin. (Kuva 53)

```
ECHO ---------------------------------------
ECHO **** Clearing Chrome cache
taskkill /F /IM "chrome.exe">nul 2>&1

set ChromeDataDir="C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default"
set ChromeCache=%ChromeDataDir%\Cache>nul 2>&1
del /q /s /f "%ChromeCache%\*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*Cookies*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*History*.*">nul 2>&1


set ChromeDataDir="C:\Users\%USERNAME%\Local Settings\Application Data\Google\Chrome\User Data\Default"
set ChromeCache=%ChromeDataDir%\Cache>nul 2>&1
del /q /s /f "%ChromeCache%\*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*Cookies*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*History*.*">nul 2>&1
ECHO **** Clearing Chrome cache DONE
```

Kuva 53. Tyhjennys-skriptin koodi

7. Luodaan C-levylle Kuvat-kansio, jonka sisälle laitetaan CommandCam.exe, jolle määritetään myöhemmin skripti, joka ottaa kuvan käyttäjästä sisäänkirjautuessa. Kansio jaetaan Windows Server-koneelle valitsemalla kansion asetuksista kohta Sharing ja määritetään käyttöoikeus koneelle KIOSKSERVER.

6.2.2 Group Policy-asetusten teko ja skriptien määrittäminen

1. Luodaan sisäänkirjautumis skripti, joka mahdollistaa valokuvan ottamisen sisäänkirjautuessa.
Skripti toimii niin, että se käynnistyy kahden sekunnin kuluttua, kun kone on käynnistynyt ja tallentaa kuvan nimellä, joka on riippuvainen päivästä ja ajasta.(Kuva 54)

script2.ps1

```
start-sleep -s 2
    while($TRUE)
    {
    $dateString = Get-Date -Format yyyyMMddhhmm

    C:\Kuvat\CommandCam.exe /filename Image$dateString.bmp

    break
    }
```

Kuva 54. Valokuvaus-skriptin koodi

2. Tämän jälkeen luodaan tyhjennys-skripti, joka tyhjentää kaikki tiedostot Documents-,Downloads-, Music-, Videos- ja Pictures-kansioista. Skripti tyhjentää myös Chromen välimuistin, evästeet ja historian. Käytännössä skripti kertoo koneelle, että sen pitää mennä määrättyihin kansioihin ja poistaa sieltä kaikki tiedostot ja alikansiot. (Kuva 55)

```
set folder="%USERPROFILE%\Documents\"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

set folder="%USERPROFILE%\Downloads\"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

set folder="%USERPROFILE%\Music\"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

set folder="%USERPROFILE%\Videos\"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)

set folder="%USERPROFILE%\Pictures\"
cd /d %folder%
for /F "delims=" %%i in ('dir /b') do (rmdir "%%i" /s/q || del "%%i" /s/q)


set ChromeDataDir="C:\Users\%USERNAME%\AppData\Local\Google\Chrome\User Data\Default"
set ChromeCache=%ChromeDataDir%\Cache>nul 2>&1
del /q /s /f "%ChromeCache%\*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*Cookies*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*History*.*">nul 2>&1


set ChromeDataDir="C:\Users\%USERNAME%\Local Settings\Application Data\Google\Chrome\User Data\Default"
set ChromeCache=%ChromeDataDir%\Cache>nul 2>&1
del /q /s /f "%ChromeCache%\*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*Cookies*.*">nul 2>&1
del /q /f "%ChromeDataDir%\*History*.*">nul 2>&1
ECHO **** Clearing Chrome cache DONE
```

Kuva 55. Tyhjennys-skripti

3. Seuraavaksi tehdään kaikki estot Group Policy Management-asetuksilla.
Aloitetaan tekemällä asetukset Control Panel- ja Desktop-osioihin. Estetään pääsy ohjauspaneeliin ja estetään käyttäjää muuttamasta erinäisiä asetuksia, kuten taustakuvaa, ääniasetuksia, työpöydän pikakuvakkeita ja poistetaan Roskakori-kuvake työpöydältä. (Kuva 56)

Policy	Setting	
Automatic certificate management	Enabled	
Option		Setting
Enroll new certificates, renew expired certificates, process pending certificate requests and remove revoked certificates		Disabled
Update and manage certificates that use certificate templates from Active Directory		Disabled
Show certificate expiry notifications	Disabled	

Administrative Templates

Policy definitions (ADMX files) retrieved from the local machine.

Control Panel

Policy	Setting
Prohibit access to the Control Panel	Enabled

Control Panel/Personalization

Policy	Setting
Prevent changing color scheme	Enabled
Prevent changing desktop background	Enabled
Prevent changing desktop icons	Enabled
Prevent changing mouse pointers	Enabled
Prevent changing screen saver	Enabled
Prevent changing sounds	Enabled
Prevent changing theme	Enabled
Prevent changing window color and appearance	Enabled
Prevent changing visual style for windows and buttons	Enabled
Prohibit selection of visual style font size	Enabled

Control Panel/Programs

Policy	Setting
Hide "Programs and Features" page	Enabled
Hide the Programs Control Panel	Enabled

Desktop

Policy	Setting
Prohibit adjusting desktop toolbars	Enabled
Prohibit User from manually redirecting Profile Folders	Enabled
Remove Recycle Bin icon from desktop	Enabled

Kuva 56. Control Panel ja Desktop GPO-asetukset

4. Määritetään Start Menu and Taskbar-lohkosta asetuksia, jotka vaikuttavat käynnistysvalikon painikkeisiin ja Windowsin Taskbarin muokkaamiseen. Asetukset jättävät periaatteessa käynnistysvalikon melkein kokonaan tyhjäksi ja Taskbariin ei voi enää tehdä muutoksia.

Nämä ei ole välttämättä pakollisia, koska käytössä on erillinen launcher. Mutta esimerkiksi vikatilanteessa jossa launcher kaatuisi, niin on hyvä olla nämä asetukset varalla, ettei käyttäjä pääse tekemään muutoksia. (Kuva 57)

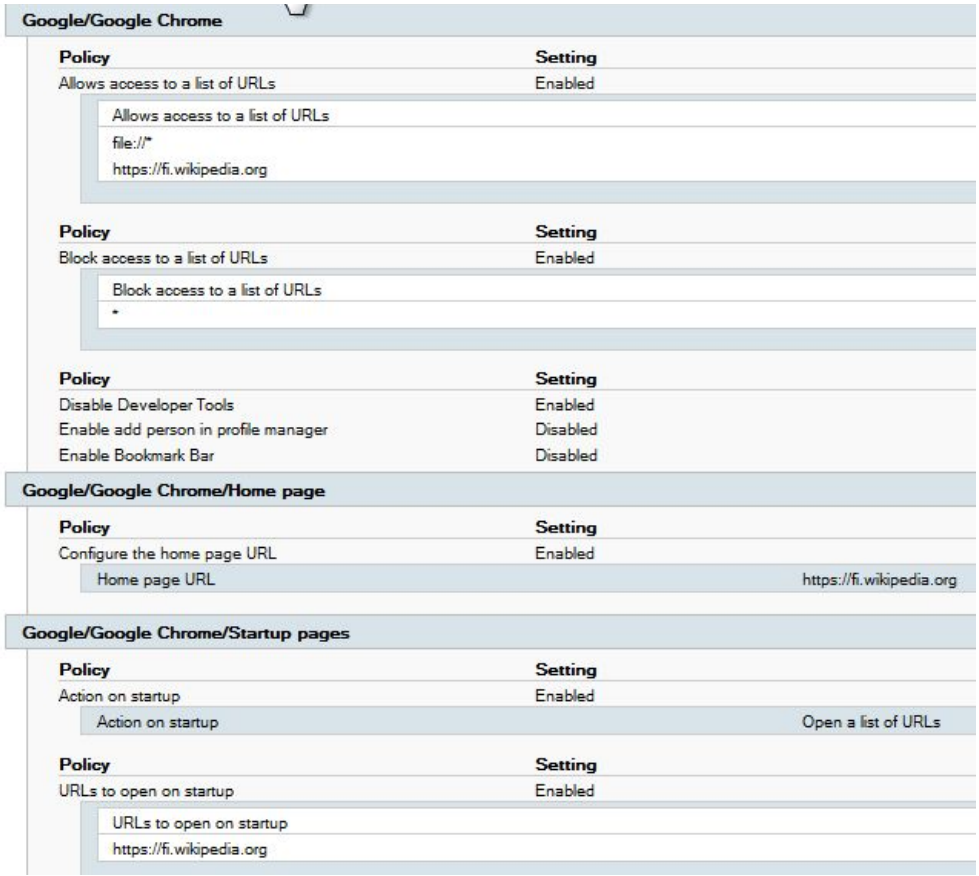
Start Menu and Taskbar

Policy	Setting
Clear history of recently opened documents on exit	Enabled
Clear the recent programs list for new users	Enabled
Do not allow pinning items in Jump Lists	Enabled
Do not search communications	Enabled
Do not search for files	Enabled
Do not search programs and Control Panel items	Enabled
Hide the notification area	Enabled
Lock all taskbar settings	Enabled
Lock the Taskbar	Enabled
Prevent changes to Taskbar and Start Menu Settings	Enabled
Prevent users from adding or removing toolbars	Enabled
Prevent users from moving taskbar to another screen dock location	Enabled
Prevent users from rearranging toolbars	Enabled
Prevent users from resizing the taskbar	Enabled
Remove All Programs list from the Start menu	Enabled
Remove and prevent access to the Shut Down, Restart, Sleep, and Hibernate commands	Enabled
Remove Balloon Tips on Start Menu items	Enabled
Remove Default Programs link from the Start menu.	Enabled
Remove Documents icon from Start Menu	Enabled
Remove Favorites menu from Start Menu	Enabled
Remove frequent programs list from the Start Menu	Enabled
Remove Games link from Start Menu	Enabled
Remove Help menu from Start Menu	Enabled
Remove Music icon from Start Menu	Enabled
Remove Network Connections from Start Menu	Enabled
Remove Network icon from Start Menu	Enabled
Remove Pictures icon from Start Menu	Enabled
Remove programs on Settings menu	Enabled
Remove Run menu from Start Menu	Enabled
Remove Search Computer link	Enabled
Remove Search link from Start Menu	Enabled
Remove the volume control icon	Enabled
Turn off all balloon notifications	Enabled

Kuva 57. Start Menu and Taskbar GPO-asetukset

5. Seuraavaksi määritetään Google Chromelle GPO-asetukset. Windows Serverissä ei ole suoraan asennettuna Chromen GPO-asetuksia, vaan ne pitää ladata erikseen Googlen omalta palvelimelta http://dl.google.com/dl/edgedl/chrome/policy/policy_templates.zip.
Tiedostot puretaan Windowsissa **\\kiosk.com\SYSVOL\kiosk.com\Policies\PolicyDefinitions** kansioon.

Asetuksiin määritetään, että fi.wikipedia.org alkuiset sivut sallitaan ja jos käyttäjä yrittää esimerkiksi mennä toisille sivuille niin selain estää sen. File://*-komennolla käyttäjä pystyy lataamaan silti esimerkiksi kuvaliitteitä halutessaan, muuten se olisi estetty. (Kuva 58)



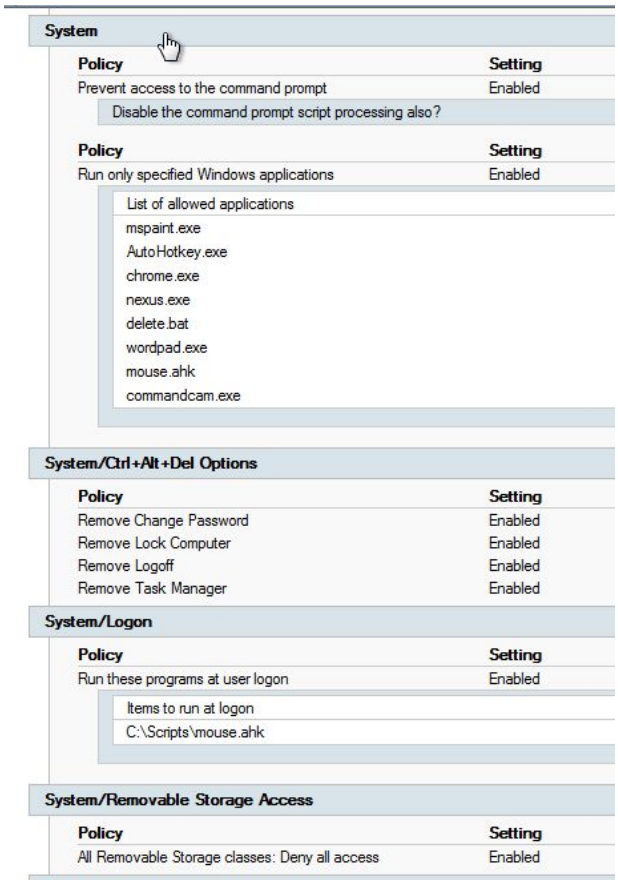
Kuva 58. Chrome GPO-asetukset

6. Määritetään AutoHotKey-skripti, joka estää oikean hiiren klikkauksen ja valitaan ohjelmat, joita voi työasemalta käynnistää. Nimetään skripti tiedostonimellä mouse.ahk, joka pitää sisällään koodin.

RButton::LButton

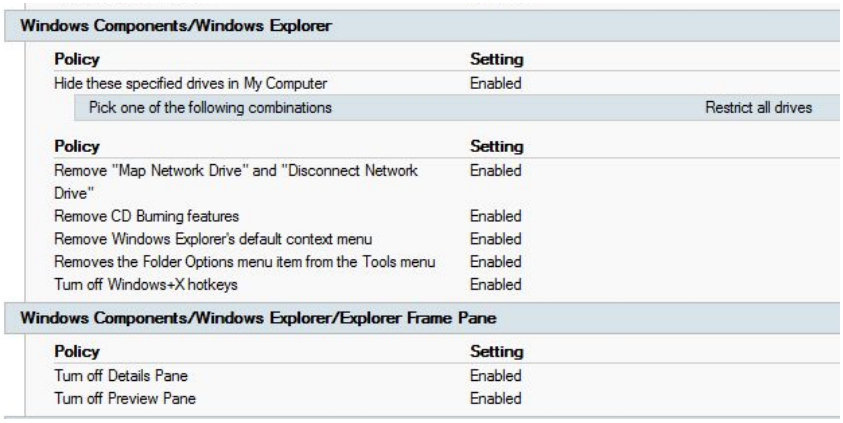
Tämä tekee sen, että oikea hiiren klikkaus korvataan vasemmalla hiiren klikkauksella. Eli launcherin asetuksiin ei pääse käsiksi.

Skripti määritetään käynnistymään koneen käynnistyksen yhteydessä. Estetään käyttäjää kytkemästä ulkoisia tallennusmedioita koneelle ja pääsy Command Promptiin.
Varmuuden vuoksi estetään myös Ctrl+Alt+Del näppäinyhdistelmällä löytyvät valinnat.
(Kuva 59)



Kuva 59. System GPO-asetukset

7. Estetään pääsy kaikille asemille ja poistetaan ominaisuuksia Windowsin File Explorerista. (Kuva 60)



Kuva 60. Windows Explorer GPO-asetukset

8. Määritetään vielä automaattinen kirjautuminen ja CTRL+ALT+DELETE disablointi KIOSK PC1-variaation tapaan.

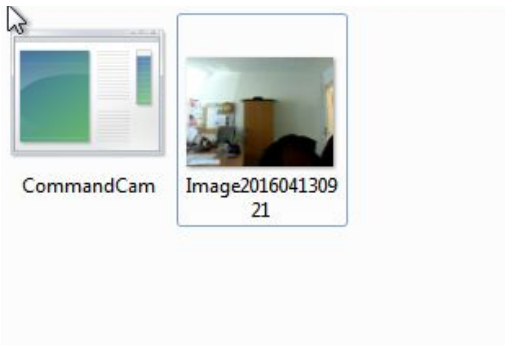
6.2.3 Toimivuuden testaaminen

Koneen toimivuus testataan ja pyritään katsomaan täyttyvätkö kaikki kriteerit.

1. Kone käynnistyy suoraan työpöydälle ja Windows Taskbarin tilalla on erillinen Nexus Launcher. (Kuva 61)

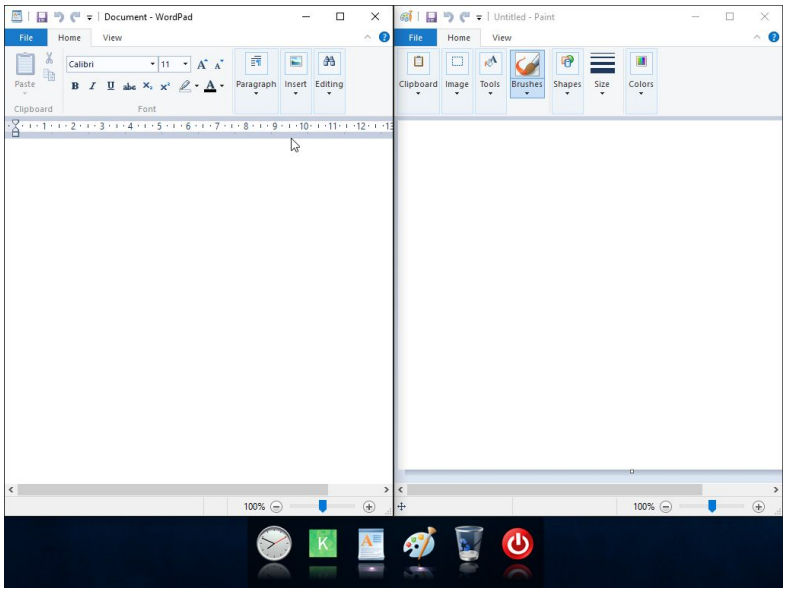
Kuva 61. Kiosk PC2-käyttöliittymä

2. Todetaan, että kone on ottanut onnistuneesti käyttäjästä kuvan, navigoimalla Windows Server koneelta Kuvat kansioon. (Kuva 62)



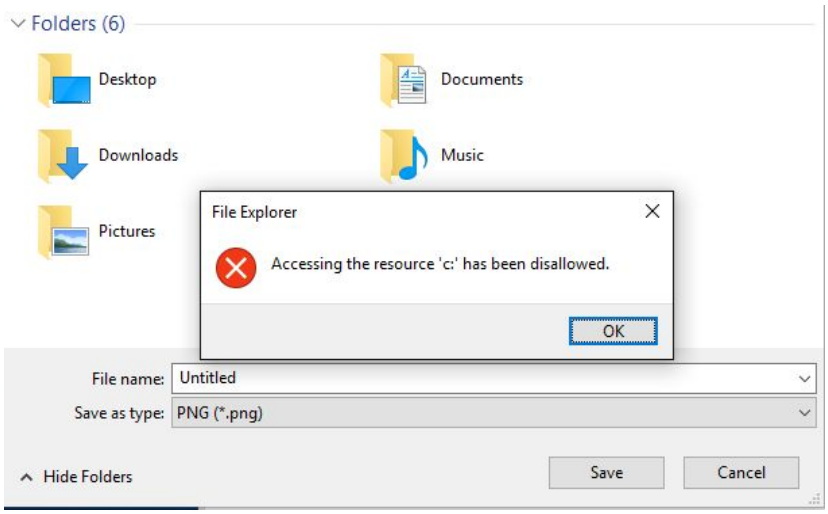
Kuva 62. CommandCam-kuvat

3. Avataan Wordpad ja Paint onnistuneesti. (Kuva 63)



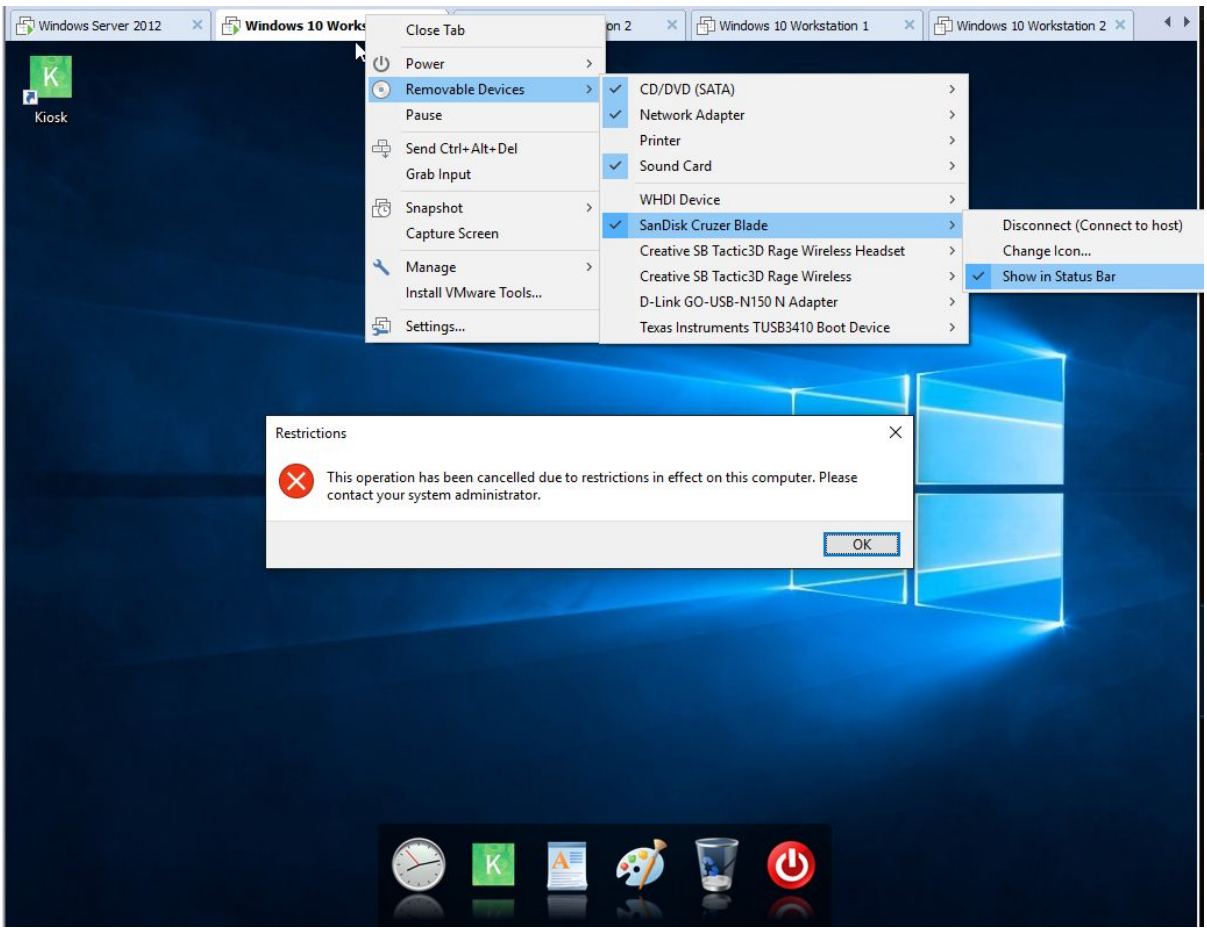
Kuva 63. Wordpad ja Paint

4. Navigoidaan Paint-ohjelman kautta File Exploreriin ja yritetään päästä C-asemalle. Todetaan, että pääsy on kielletty ja valittavissa ei ole mitään muita kansioita kuin Desktop, Downloads, Documents, Music, Pictures ja Videos. (Kuva 64)



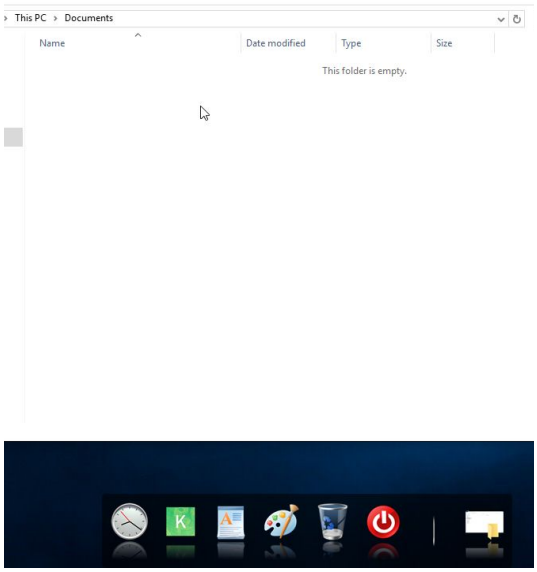
Kuva 64. C-levylle pääsy estetty.

5. Kytketään VMWaren kautta USB-tikku virtuaalikoneeseen ja todetaan, että käyttö on estetty. Sama virheilmoitus syntyy jos yrittää painaa Win+X-näppäinyhdistelmiä. CTRL+ALT-näppäimillä alkavat yhdistelmät ei myöskään toimi, koska ne on disabloitu. (Kuva 65)



Kuva 65. USB-Tikun asentaminen

6. Todetaan, että kansiot tyhjenevät kun käyttäjä kirjautuu ulos. (Kuva 66)



Kuva 66. Kansion tyhjennys

7. Avataan Kiosk-selain joka aukaisee Wikipedian aloitussivuna. Roskakori-painikkeesta selaimen saa suljettua kokonaan. (Kuva 67)

Kuva 67. Kiosk-selain ja Nexus Launcher

8. Yritetään vaihtaa Wikipedian oletuskieltä ja todetaan, että selain estää sen aikaisemmin määritetyllä Whitelist-suodattimella, joka blokkaa kaikki muut paitsi fi.wikipedia.org alkuiset sivustot. (Kuva 68)

Kuva 68. Pääsy estetty sivuille

7 Yhteenveto

Työ oli kokonaisuudessaan suhteellisen haastava ja asetuksia sai testata paljon, jotta kaikki saatiin varmuudella toimimaan. Haastavinta oli löytää oikeanlainen valokuvaus-ohjelma, jolla onnistuttiin toteuttamaan valokuvan ottamisen siten, että näkyvillä ei ole graafista käyttöliittymää.

CommandCam-ohjelma oli suunniteltu käytettäväksi komentokehotteen kautta, ja siinä oli itsessään sellainen bugi, että se ottaa vain yhden kuvan kerrallaan nimellä image.bmp. Tähän piti luoda erikseen PowerShell-skripti, joka määrittää tiedostolle aina uuden nimen.

Omia haasteita toi myös Windows Taskbarin saaminen näkyviin päällimmäisenä, kun nettiselain on kokoruututilassa. Tämä on onnistunut vanhemmassa Windows XP-versiossa asetusten kautta, mutta tämä ominaisuus on poistettu Windows Vista-versiosta alkaen. Vaihtoehtoiseksi ratkaisuksi löysin lopulta erillisen launcherin, joka korvaa Windowsin Taskbarin.

Työssä sai käyttää runsaasti omaa luovuuttaan, koska variaatioita on paljon erilaisia ja yleensä asetukset luodaan tarpeiden mukaan. Kokonaisuudessaan työ oli erittäin mielenkiintoinen. Seuraavaksi olisi aikomus pyrkiä ohjelmoimaan oma Kiosk-sovellus, jossa on kaikki integroituna ja Windows Server-käyttöjärjestelmää ei tarvita.

LÄHTEET

[1] Cisco Networking Academy Program., and Cisco Networking Academy Program. *Introduction to Networks: Companion Guide*. Indianapolis, Indiana: Cisco Press, 2014. Viitattu 12.04.2016.
[2] https://fi.wikipedia.org/wiki/DHCP Viitattu 12.04.2016.
[3] http://www.cs.tut.fi/tlt/npg/vyo/Subnets/subnets_3.swf Viitattu 12.04.2016.
[4] Understanding Active Directory. Viitattu 13.04.2016.
https://www.youtube.com/watch?v=Tvp88xYf5Es
[5] Kivimäki J. Windows Server 2008 R2: Tehokas Hallinta. 2009. Viitattu 13.04.2016
[6] Technet Mircrosoft. AS DS on a Windows Server Network. Viitattu 13.04.2016
[7] https://fi.wikipedia.org/wiki/OSI-malli Viitattu 12.04.2016.
[8] https://upload.wikimedia.org/wikipedia/commons/7/74/Ipv4_address.svg Viitattu 12.04.2016.
[9]Dye, Mark A., Rick McDonald, Antoon W. Rufi, Inc Cisco Systems, and Cisco Networking Academy. *Network Fundamentals: CCNA Exploration Companion Guide*. Indianapolis (IN): Cisco Press, 2008. Viitattu 12.04.2016.

LIITTEET

AutoHotKey

AutoHotKey on ilmainen avoimen lähdekoodin ohjelmisto. Ohjelmalla voidaan luoda skriptejä Windows-käyttöjärjestelmissä, joilla voidaan esimerkiksi ohjelmallisesti luoda erilaisia kansion avaamis skriptejä tai luoda näppäinyhdistelmille yksittäinen macro-näppäin.

Winstep Nexus Launcher

On WinStepin julkaisema ilmainen launcheri, jolla voidaan korvata Windowsin Taskbar. Ohjelmalle on luotu monia erilaisia teemoja, joista on pyritty saamaan visuaalisesti näyttäviä.

CommandCam

On Ted Burken ohjelmoima yksinkertainen ohjelma valokuvien ottamiseen. Ohjelma käyttää Microsoftin Directshow API-kirjastoja päästäkseen käsiksi Web-kameroihin Ohjelma toimii komentokehoitteen kautta.

Google Chrome

On Googlen kehittämä selainohjelma, joka pohjautuu Chromium-nimiseen avoimen lähdekoodin projektiin. Se on maailman toiseksi suosituin selain Internet Explorerin jälkeen.