

# **Windows Server 2012 -palvelimen standardiperusteinen koven- taminen**



Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Hämeenlinna, syksy, 2017

Antti Silvola

TIETOJENKÄSITTELY  
VISAMÄKI, HÄMEENLINNA

---

<b>Tekijä</b>	Antti Silvola	<b>Vuosi</b> 2017
<b>Työn nimi</b>	Windows Server 2012 -palvelimen standardiperusteinen koventaminen	
<b>Työn ohjaaja</b>	Lasse Seppänen	

---

## TIIVISTELMÄ

Opinnäytetyössä tehtiin Windows Server 2012 -palvelimen standardiperusteisen koventamisohjeistus eli palvelimen tietoturvamäärityksien tarkistaminen ja muuttaminen oletusmäärityksistä tietoturvallisempiin määrityksiin. Työn tavoitteena oli kuvailla, mitä CIS-Standardin mukaan tehdyn Windows Server 2012 -palvelinkäyttöjärjestelmän palvelinkoventaminen pitää sisältään.

Eri lähteissä (esimerkiksi VAHTI ja KATAKRI) on määritetty vaatimustasoja, joiden mukaan palvelimet tulee asentaa järjestelmällisesti, niin että lopputuloksena on kovenettu palvelin. Lähteissä ei ole kuvattuna mikä on menettelytapa, jolla uudet järjestelmät asennetaan järjestelmällisesti.

Opinnäytetyössä on käytetty PDCA-tutkimusmenetelmää, jonka avulla voidaan tehdä palvelinkoventamismäärityksiä. Työn lopussa olevassa liitteessä on kuvattu tutkimustyölopputulokset yksityiskohtaisesti. Taulukossa näkyvät palvelinkohtaiset oletusasetukset, CIS-standardin mukainen arvo sekä suositus siitä, mikä asetus tulee määrittää palvelimelle, jotta palvelin on standardin mukaan kovenettu tietoturvallisesti.

**Avainsanat** Windows Server 2012, koventaminen, CIS

**Sivut** 39 sivua, joista liitteitä 34 sivua

BUSINESS INFORMATION TECHNOLOGY  
VISAMÄKI, HÄMEENLINNA

---

<b>Author</b>	Antti Silvola	<b>Year</b> 2017
<b>Subject</b>	Windows Server 2012 Standard Based Hardening	
<b>Supervisor</b>	Lasse Seppänen	

---

ABSTRACT

The topic for my thesis is to do Windows Server 2012 Standard Based Hardening guide. The thesis main point is to give an understanding to the reader what is hardening to the Windows Server 2012 operation system. The goal is to provide what should be changed in a Windows Server 2012 server, so that the server is hardened by CIS standards. The thesis describes how to check and change the server's security definitions from the default settings so that the definitions are more secure.

Different sources (for example VAHTI and KATAKRI) have defined requirements, so that the server needs to be installed systematically so that the end result is a hardened server. In the requirement sources there has not been defined on which procedure the new server is installed systematically.

PDCA-research methods were used in this thesis and the methods can be used to make server hardening definitions. The Appendix, that is in the end of the thesis, describes the results of the research work in details. The appendix table shows the server default settings, the CIS standard value and the recommended secure setting which should be defined to the server so that the server would be securely hardened to the standard.

**Keywords** Windows Server 2012, hardening, CIS.

**Pages** 39 pages including appendixes 34 pages

# SISÄLLYS

1	JOHDANTO.....	1
2	WINDOWS SERVER 2012 .....	2
3	PALVELINKOVENTAMINEN .....	3
4	PLAN-DO-CHECK-ACT (PDCA) THE DEMING MODEL-VIITEKEHYS .....	4
5	KOVENTAMISEEN LIITTYVÄT STANDARDIT.....	5
5.1	Center for Internet Security .....	5
5.2	CIS Security benchmarks for Windows (The Center for Internet Security) .....	6
5.3	Microsoft Security Compliance Manager.....	6
5.4	Organisaatiotason määrittämät parhaat käytännöt.....	6
6	KOVENTAMISEEN LIITTYVÄT TOIMENPITEET .....	7
6.1	Toimintatavan määrittäminen .....	7
6.2	Perustason tietoturvatason määrittäminen .....	7
6.3	Roolikohtainen tietoturvatason määrittäminen.....	7
6.4	Palvelinkoventamisen poistaminen .....	8
7	PALVELINKOVENTAMISTYÖKALUJA.....	9
7.1	Local security policy .....	9
7.2	Local Group Policy Editor .....	9
7.3	Security configuration and analysis .....	9
7.4	Group Policy Management .....	9
7.5	Järjestelmähallinta työkalut kuten SCCM tai BSA.....	9
8	PALVELINKOVENTAMISEEN LIITTYVÄT LISÄTOIMENPITEET.....	11
9	PALVELIMEN TIETOTURVATASON TARKISTUSTYÖKALUJA.....	13
9.1	Cis-Cat Pro .....	13
9.2	Nessus .....	13
9.3	Microsoft Baseline Security Analyzer.....	13
10	PALVELINKOVENTAMISMÄÄRITYKSET.....	14
10.1	Account Policies .....	14
10.1.1	Password Policy .....	14
10.1.2	Account Lockout Policy.....	15
10.2	Local Policies .....	15
10.2.1	Audit Policy .....	15
10.2.2	User Rights Assignment.....	16
10.2.3	Security Options .....	17
10.3	Windows Firewall with Advanced Security .....	20
10.3.1	Domain Profile .....	20
10.3.2	Private Profile .....	21

10.3.3	Public Profile .....	21
10.4	System Audit Policies .....	22
10.5	Administrative Templates .....	23
10.5.1	Personalization .....	24
10.5.2	MSS (Legacy) Security Options .....	24
10.5.3	Microsoft Peer-to-Peer Networking Services.....	25
10.5.4	Network Connections .....	25
10.5.5	Network Provider .....	26
10.5.6	Windows Connect Now .....	26
10.5.7	Windows Connection Manager .....	26
10.5.8	Pass the Hash Mitigations .....	27
10.5.9	Audit Process Creation .....	27
10.5.10	Early Launch Antimalware .....	27
10.5.11	Logging and tracing .....	27
10.5.12	Internet Communication settings .....	28
10.5.13	Locale Services.....	28
10.5.14	Logon .....	29
10.5.15	Remote Procedure Call.....	29
10.5.16	Microsoft Support Diagnostic Tool.....	29
10.5.17	Windows Performance PerfTrack.....	29
10.5.18	User Profiles.....	30
10.5.19	Time Providers.....	30
10.5.20	App runtime.....	30
10.5.21	AutoPlay Policies .....	30
10.5.22	Credential User Interface .....	31
10.5.23	EMET.....	31
10.5.24	Event Log Service.....	32
10.5.25	Previous Versions .....	32
10.5.26	Location and Sensors.....	32
10.5.27	OneDrive (formerly SkyDrive).....	33
10.5.28	RemoteFX USB Device Redirection.....	33
10.5.29	Device and Resource Redirection.....	33
10.5.30	Security .....	34
10.5.31	Session Time Limits.....	34
10.5.32	RSS Feeds.....	34
10.5.33	OCR .....	35
10.5.34	Software Protection Platform .....	35
10.5.35	Store .....	35
10.5.36	Consent.....	35
10.5.37	Windows Logon Options .....	36
10.5.38	Windows PowerShell.....	36
10.5.39	WinRM Client.....	36
10.5.40	WinRM Service .....	36
10.5.41	Windows Remote Shell.....	36
10.5.42	Defer Windows Updates .....	37
10.5.43	Personalization .....	37
10.5.44	Notifications .....	37
10.5.45	Internet Communication settings .....	38
10.5.46	Attachment Manager .....	38

10.5.47 Network Sharing.....	38
10.5.48 Playback.....	38
11 YHTEENVETO .....	39
LÄHTEET .....	40

Liitteet

Liite 1 CIS-KOVENTAMISMÄÄRITYKSET

## 1 Johdanto

Tämän opinnäytetyön tavoitteena oli nostaa Windows Server 2012 -palvelimen käyttöjärjestelmän perustietoturvasoaa CIS-standardia hyödyntäen. Työssä selvitettiin, mitä standardin mukaisia tietoturvamutoksia tulisi tehdä asennettavaan palvelimeen. Tavoitteena oli nostaa palvelimen perustason (baseline) tietoturvasoaa. Opinnäytetyön pääasiallisena tietoperustana käytettiin Center for Internet Securityn luomia viitekehysä CIS Microsoft Windows Server 2012 Benchmark v1.0.0 ja CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1 muita koventamiseen liittyviä tietolähteitä. Koventamisen määrittämisen kohteena käytettiin Windows Server 2012 R2 -käyttöjärjestelmän omaavaa palvelinta, joka ei ole vielä liitettyä toimialueeseen.

Opinnäytetyön tutkimusmenetelmä oli kehittämisprojekti, jonka tarkoituksena oli miettiä miten parantaa palvelimen tietoturvasoaa. Julkisen ja yksityisen sektorin organisaatiot ovat alkaneet vaatimaan, että palvelinkoventaminen tehdään kansainvälisen viitekehysten, ei toimittajan ohjeistuksen mukaan. Vaaditaan myös, että käytössä on menettelytapa, jolla järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus. Tutkimusmenetelmänä on käytetty W. Edward Demingin PDCA-kehityssykliä, joka on ongelmanratkaisumalli ja kehittämismenetelmä. Opinnäytetyössäni tämä tutkimusmenetelmä on kertaluontoinen prosessi, kun taas organisaatiossa tämän tulisi olla päättymätön prosessi, jolla tietoturvaa kehitetään sekä parannetaan.

Tutkimuskysymyksenä oli vastata julkisen sektorin vaatimukseen. Mitä palvelinkoventaminen pitää sisällään, kun käytetään luotettavaa ja ulkopuolista koventamislähdettä. Miten lähteestä saadaan koventamiseen liittyvä tiedot ulos. Miten tulisi koventamisessa tietoturvamäärityksiä muuttaa, jonka avulla organisaatiolla olisi menettelytapa, jonka lopputuloksena on kovennettu asennus.

Opinnäytetyön tuloksena osoitettiin, miten voi nostaa tietoturvan tasoa Microsoftin ensiasennuksen jälkeisistä oletusasetuksista tietoturvallisemmaksi sekä pienentää palvelimeen kohdistuvia ulkopuolisia tietoturvauhkia. Opinnäytetyö voi myös toimia tietoturvaohjeena yrityksissä ja organisaatioissa. Työ opastaa miten, Windows Server 2012 -palvelin voidaan koventaa, niin että välttytään tietoturvauhkilta ja kohotetaan palvelin-kohtaista tietoturvasoaa.

## 2 Windows Server 2012

Windows Server 2012 on Microsoftin kehittämä palvelinkäyttöjärjestelmää, joka on Windows Server 2008 R2-palvelinkäyttöjärjestelmän seuraaja. Käyttöjärjestelmä on julkaistu syyskuussa 2012. Windows Server 2012 R2 on (Windows Server 2012 päivitys) Microsoftin uusin Windows-palvelinkäyttöjärjestelmä. Sen päivitys on julkaistu loka-kuussa 2013. Windows Server 2012 R2 on Microsoftin ensimmäinen pilvikäyttöjärjestelmä (Cloud Operating System).

Windows Server 2012 on hyvin samankaltainen käyttöjärjestelmä kuin Windows 8, koska nämä järjestelmät olivat osana samaa kehitysprojektia. Käyttöliittymä on kummassakin samanlainen ja suurin osa asetuksista löytyy samoista paikoista. Windows Server 2012:ssa on vähemmän virranhallintaominaisuuksia, sillä palvelinkäyttöjärjestelmää ei voida laittaa esimerkiksi nukkumaan (sleep) virran säästämiseksi.

Microsoftin Windows Server 2012:ssa on aikaisempien viiden version sijasta neljä: Standard, Datacenter, Essentials ja Foundation. Versiot ovat perustoiminnaltaan hyvin samanlaiset. Standard-versiosta puuttuu joitakin ominaisuuksia, mitä Datacenterissä on. Standard-versiossa esimerkiksi virtuaalikoneiden määrä on rajoitettu kahteen, kun Datacenter-versiossa määrää ei ole rajoitettu.

Windows tarjoaa myös erityiskäyttöön Essentials- ja Foundation-versiot, jotka ovat karstittuja versioita. Kumpikaan versio ei tue virtualisointia, mutta niillä pystytään tuottamaan yksittäisiä palveluita. Essentials-versio tukee 25:tä käyttäjää ja sisältää yksinkertaistetun käyttöliittymän. Foundation-versio tukee vain 15:tä käyttäjää. Nämä versiot sopivat esimerkiksi pienille yrityksille.

Kaikissa versioissa voidaan valita Server Core- tai Server with a Graphical User Interface (GUI) asennuksen. Server Core sisältää vain palvelimen palveluille tärkeimmät ominaisuudet. Server Core sopii tilanteisiin, joissa palvelimen tiedetään tuottavan vain tiettyä palvelua kuten Active Directory- tai DNS-palvelua. Server with a Graphical User Interface -asennuksessa palvelimeen tulee graafinen käyttöliittymä, jolla palvelinta on helpompi hallita. Palvelimeen voidaan asentaa yhdistelmä kaikkia sallittuja rooleja ja ominaisuuksia. Tätä asennusvaihtoehtoa suositellaan, jos palvelimen roolit vaihtuvat sen käyttöaikana. (Windows Server 2012 Editions comparison, 2014.)



### 3 Palvelinkoventaminen

Palvelinkoventaminen (Server Hardening) on turvallisuutta parantava prosessi, jonka avulla palvelin on konfiguroitu tietoturvallisesti vähentämällä niin monta turvallisuusriskiä kuin on mahdollista.

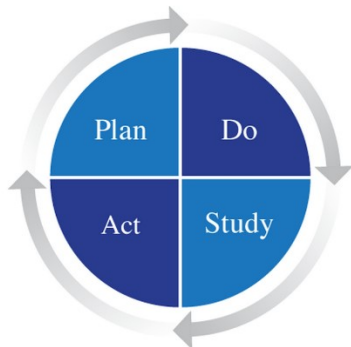
Vaikka palvelimen oletusasetukset ja -määritykset ovat parantuneet huomattavasti vuosien varrella, monia asetuksia tulee tietoturvallisesti nostaa, jotta palvelimesta saadaan tietoturvallinen. Helppokäyttöisyyden mukaan määritetty asetus ei normaalisti takaa, että asetus on turvallinen, mikä avaa tietoturvahkamahdollisuuden erityyppisille tietoturvahyökkäyksille.

Palvelinkoventaminen on hyvä tehdä samassa yhteydessä asennuksen kanssa. Tämän jälkeen kannattaa ottaa käyttöön palvelimen muita ominaisuuksia, rooleja tai ohjelmistoja. (Server Hardening, 2015.)

## 4 Plan-Do-Check-Act (PDCA) The Deming Model-viitekehys

Palvelinkoventamistutkimustyöhän on käytetty PDSA-ympyrää, joka tunnetaan myös Deming model viitekehystenä (Kuva 1). Deming Model on ongelmanratkaisumalli ja kehittämismenetelmä, jonka perusta jatkuvan laadun parantamiselle: ensin suunnitellaan (Plan), sitten tehdään (Do). Tekemisen jälkeen tarkistetaan (Check) ja tehdään tarvittaessa korjaukset (Act). Korjausten jälkeen ympyrässä palataan alkuun eli suunnitteluun. Viitekehysten on kehittänyt Tohtori W. Edwards Deming. (Deming, 2016).

- Plan. Suunnitteluvaiheessa määritetään muutoksen tavoite ja suunnitellaan muutos (Define and plan the change.).
- Do. Tekovaiheessa tehdään suunnitellut muutokset kohteeseen. (Implement the change.).
- Check. Tarkistusvaiheessa tarkistetaan tehdyt muutokset ja tarkistetaan niiden toiminnallisuus (Monitor the change, analyzing the effectiveness of the change.).
- Act. Korjausvaiheessa tehdään mahdolliset korjaukset muutokseen, jotta saavutetaan haluttu tavoite (Adjust based on the analysis, initiating appropriate improvement activities).



Kuva 1. PDCA-ympyrä, (Deming PDCA Cycle, 2016.)

## 5 Koventamiseen liittyvät standardit

Koventamiseen liittyvät julkiset standardit pohjautuvat johonkin konkreettiseen tapaan käydä palvelimen asetuksia läpi tietoturvallisen lopputuloksen saavuttamiseksi. Standardeja ei vielä ole paljon olemassa.

Eräs standardeja laatinut taho on Center for Internet Security. Voittoa tavoittelematon organisaatio on dokumentoinut useita standardeja, jotka löytyvät helposti sen verkkosivuilta.

Toinen taho on toimittajan omat määrytykset. Windows Server 2012 tapauksessa määrytykset tulevat Microsoftilta, jonka on kehittänyt Security Compliance Manager 3.0 (SCM 3.0) -työkalun. Työkalun avulla voidaan nopeasti määrittää sekä hallita eri laitteisiin kohdistuvia tietoturva-asetuksia.

### 5.1 Center for Internet Security

Center for Internet Security (CIS) on voittoa tavoittelematon organisaatio. CIS pyrkii parantamaan globaalia internet-tietoturvaa. Sen päämäärä on luoda ja edistää julkiselle ja yksityiselle sektorille luotettava ja turvallinen toimintaympäristö eri käyttökohteille, kuten Windows Server 2012-palvelinkäyttöjärjestelmä.

CIS Securityn määrittämät standardit (benchmarks) sisältävät suositeltavat tekniset määrytykset käyttöjärjestelmille, sovelluksille, ja ohjelmistoille. Määrytysten avulla CIS pyrkii luomaan maailmanlaajuiset yhteiset pelisäännöt tietoturvan parantamiseksi.

CIS Securityn määrittämät kriteerit ovat ainoita yhteisymmärryksessä määritettyjä konfiguraatio ohjeistuksia. Niiden kehittämiseen ja hyväksymiseen ovat osallistuneet eri organisaatiot, jotka edustavat hallintoa, yritysmaailmaa, teollisuutta ja koulutusta. Ne ovat globaaleja standardeja, joiden tarkoitus on antaa organisaatioille viitekehyksen tietoturvan parantamiseen.

Standardit on luonut laaja-alainen asiantuntijaryhmä, ja ryhmän edustajat edustavat eri aihealueita kuten konsultaatiota, sovelluskehitystä, auditointia, tietoturvakehitystä.

Standardit käyvät läpi kaksivaiheisen tarkastuksen ennen kuin ne hyväksytään. Ensimmäisen vaiheen aikana CIS-asiantuntijat keskusteleval, suunnittelevat sekä luovat luonnokset standardille. Ensimmäinen vaihe päättyy, kun asetusten määrytyksissä on päästy yksimielisyyteen.

Toinen vaihe alkaa, kun standardit on julkaistu. Tässä vaiheessa kaikki standardeihin annettu palaute tarkistetaan ja selvitetään, onko joitakin lisäasetuksia seuraavaan versioon. (CIS Center for Internet Security, 2014.)

## 5.2 CIS Security benchmarks for Windows (The Center for Internet Security)

CIS Microsoft Windows Server 2012 R2 Benchmark v2.2.1 on CIS:n määrittämä viimeisin viitekehys, jonka avulla voidaan parantaa organisaation tietoturvaa. CIS Security Benchmarks pyrkii kuvaamaan määrittämät käytännöllisesti sekä järkevästi. Se tarjoaa myös selkeän tietoturvallisuuden edun eikä heikennä teknologian käytettävyyttä.

CIS Security Benchmarks for Windows sisältää määrittämät kahden eri roolin mukaiselle palvelimelle. Domain Controller -roolikohtaiset määrittämät ovat tarkoitettu toimialueen ohjaukselle, jolla hallitaan Active Directorya (Hakemistopalvelu). Member Server -roolikohtaiset määrittämät ovat tarkoitettu toimialueelle liitettävälle palvelimelle. Palvelin voi pitää sisällään seuraavia rooleja tai ominaisuuksia: AD Certificate Services, DHCP Server, DNS Server, File Server, Hyper-V, Network Policy and Access Services, Print Server, Remote Access Services, Remote Desktop Services sekä Web Server. (CIS Benchmarks, 2014.)

## 5.3 Microsoft Security Compliance Manager

Security Compliance Manager 3.0 (SCM 3.0) on Microsoft Solution Accelerator-tiimin luoma ilmainen työkalu. Sen avulla voi nopeasti määrittää sekä ylläpitää työasemia. Työkalun merkittävä uudistus edelliseen versioon verrattuna on, että se tarjoaa uusia perustason Internet Windows Server 2012-, Windows 8- ja Internet Explorer 10-tietoturvaasetuksia.

SCM tarjoaa valmiin käyttöönotettavan tietoturvakäytäntö DCM-kokoonpanon pakauksessa, jotka on testattu ja täysin tuettu. Nämä lähtökohdat perustuvat Microsoft Security oppaan suosituksiin ja alan parhaisiin käytäntöihin. Suositusten avulla on mahdollista hallita konfiguraatiokokoonpanoja, määrittää yhteensopivuusvaatimukset sekä vähentää turvallisuusuhkia. (Microsoft Security Compliance Manager, SCM, 2016.)

## 5.4 Organisaatiotason määrittämät parhaat käytännöt

Organisaation tulisi määrittää omat ns. parhaat käytännöt eri käyttöjärjestelmille sekä niiden käyttäjille ohjelmistoille. Käytännöt sisältävät yleensä organisaation sisäisiä hyväksi havaittuja toimintatapoja eri osa-alueilla. Käytännöissä kiinnitetään huomiota tietoturvallisuuden sekä palveluiden toiminnallisuuteen.

## 6 Koventamiseen liittyvät toimenpiteet

Palvelinkoventamisen on yleensä projektiluonteista työtä, jossa määritetään tietty aihe sekä sen laajuus, henkilöt ja aikaraja jolloin työn tulee olla tehtynä. Aiheen laajuudessa määritetään mihin osa-alueeseen koventaminen tehdään ja mitä standardia tulee noudattaa. Työhön valitaan organisaatiosta kunkin osa-alueen parhaimmat asiantuntijat. Aikarajassa määritetään kesto, joka tarvitaan itse työn tekemiseen, jotta koventamis-määritykset saadaan organisaation käyttöön.

### 6.1 Toimintatavan määrittäminen

Palvelinkoventamisen aloittaminen tulisi tehdä määrittämällä hyvä toimintatapa, jonka avulla palvelinkoventamiset tehdään. Yksi hyvä tapa on käyttää Plan-Do-Check-Act (PDCA) the Deming Model-ongelmanratkaisumallia ja kehittämismenetelmää.

Mikä tahansa toimintatapa valitaankin, tulee toimenpiteet, määritykset sekä muutokset dokumentoida. Dokumentaation avulla voidaan PDCA Check-vaiheessa löytää juurisyy ja muuttaa tietoturvamääritys oikeaksi tai tuotantovaiheessa ongelmaselvityksessä löytää juurisyy.

### 6.2 Perustason tietoturvatason määrittäminen

Palvelinkoventaminen olisi hyvä aloittaa määrittämällä perustason tietoturva (ns. baseline) määrityksille, jotka määritetään kaikille palvelimelle käyttöönoton yhteydessä. Perustason tietoturva-asetukset olisi hyvä testata toimivaksi kokoonpanoksi organisaatiolle.

Windows Server 2012 on suunniteltu turvalliseksi oletuksena. Kuitenkin jokaisen organisaation olisi harkittava, millainen turvallisuustaso sekä toiminnallisuus tarvitaan. Siksi voidaan joutua tekemään erityisiä kokoonpanon muutoksia täyttämään oman ympäristöön annettuja, esim. valtiohallinnon vaatimuksia, kuten VAHTI/KATAKRI. (Baseline Server Hardening, 2014.)

### 6.3 Roolikohtainen tietoturvatason määrittäminen

Perustason tietoturvatason määrittämisen jälkeen voidaan palvelimelle määrittää ns. roolikohtaiset tietoturvatason koventamiset, kuten toimialueen ohjauskoneille, että IIS-, tietokanta- tai tiedostopalvelimelle.

Roolikohtaiset tietoturvamääritykset ajetaan perustason tietoturvamäärityksien päälle. Roolikohtaisten tietoturvamääritysten tekoon voidaan käyttää CIS Security standardeista löytyviä tietoturvaohjeistuksia.

CIS Security -standardeista löytyy eri tuotteille vastaavanlaisia koventamisviitekehyksiä kuten, Apache HTTP Server, Apache Tomcat Server, BIND DNS Server, FreeRADIUS, Microsoft IIS Server, IBM DB2 Server, Microsoft Exchange, Microsoft SharePoint Server,

Microsoft SQL Server, MIT Kerberos, MySQL Database Server, Novell eDirectory, OpenLDAP Server, Oracle Database Server, Sybase Database Server, Xen Server.

#### 6.4 Palvelinkoventamisen poistaminen

Palvelimilta tehtyjen koventamisen poistaminen on hankalaa, ellei muutoksia ole dokumentoitu (Plan-vaihe, Plan-Do-Check-Act (PDCA) the Deming Model). Tietoturva-asetuksien muuttaminen onnistuu määrittämällä asetus uudestaan, tosin tietoturva-asetuksissa on paljon määrittelemättömiä (ns. Not configured) -kohteita, joiden muuttaminen takaisin ei onnistu muuten kuin oletusasetukset palauttamalla. Tietoturva-asetuksien palauttaminen niiden oletusasetuksiksi onnistuu ajamalla oletusasetukset ole-massa olevien asetusten päälle.

Oletusasetukset, ns. Security template-tiedosto sijaitsevat Windows Server 2012-palvelimella %systemroot%\inf -kansioissa. Oletusasetustiedostoja Windows Server 2012-palvelimelle on kaksi: Defltbase.inf ja Defltsv.inf. Molemmissa tiedostoissa on samat asetukset. Ne soveltuvat myös Windows Server 2008-palvelimelle, jota varten ne on luotu, mutta yhteensopivat Windows Server 2012-palvelimien kanssa. Oletusasetuksien palauttaminen onnistuu helpoiten Security Configuration and Analysis (Secedit.exe) -työkalun avulla. (Kommento: secedit /configure /cfg %windir%\inf\defltbase.inf /db defltbase.sdb /verbose). (Suojausasetusten palauttaminen niiden oletusasetuksiksi, 2017.)

## 7 Palvelinkoventamistyökaluja

### 7.1 Local security policy

Local security policy (secpol.msc) on graafinen työkalu, jonka avulla voidaan hallita ja määrittää järjestelmä- ja tietoturvamäärityksiä paikalliselle palvelimelle. Kaikkia järjestelmä- ja tietoturvamäärityksiä ei voida Local Security Policy työkalulla määrittää. Työkalu on hieman suppea määritys kohteiltaan. Rajautuu vain ns. Security Settings asetuksiin. Työkalun avulla voidaan viedä (export) olemassa olevat tietoturvamääritykset ulos palvelimelta tai tuoda (import) esimääritettyjä tietoturva-asetuksia palvelimelle. (Local Security Policy, 2017.)

### 7.2 Local Group Policy Editor

Local Group policy Editor (gpedit.msc) on graafinen työkalu, jonka avulla voidaan hallita ja määrittää järjestelmä- ja tietoturvamäärityksiä paikallisella palvelimelle. Local Group policy Editorin avulla voidaan määrittää kaikkia palvelin kohtaisia järjestelmä- ja tietoturvamäärityksiä. (Local Group Policy Editor, 2017.)

### 7.3 Security configuration and analysis

Security Configuration and Analysis on Microsoft Management Console (MMC.exe) hallintakonsolin sisällä oleva graafinen Snap-in työkalu, jonka avulla voidaan hallita ja määrittää järjestelmä- ja tietoturvamäärityksiä paikallisella palvelimelle. Työkalun avulla voidaan voi ajaa sisään esimääritettyjä tietoturva konfiguraatiota palvelimelle. Security Configuration and Analysis työkalun avulla voi verrata paikallisen käyttäjärjestelmän asetuksia tietoturvapohjaisiin määrityksiin, jotka on määritelty erilliseen .inf tiedostoon

Security Configuration and Analysis (Secedit.exe) on merkkipohjainen työkalu, jolla voidaan järjestelmällisesti määrittää esimääritettyjä tietoturva määrityksiä paikallisella palvelimelle komentojono pohjaisesti. (Using the Windows Server 2012 Security Configuration and Analysis Tool, 2017.)

### 7.4 Group Policy Management

Group Policy Management, GPO (gpmc.msc) on graafinen työkalu, jonka avulla voidaan keskitetysti hallita ja määrittää järjestelmä, että tietoturva määrityksiä toimialueella oleville palvelimelle sekä työasemille. Työkalu asennettuna automaattisesti Active Directory Domain Service roolin käyttöönoton yhteydessä. Tietoturvamäärityksiä voi myös tehdä käyttäjä- että ryhmäkohtaisesti. (Group Policy Management Console, 2017.)

### 7.5 Järjestelmähallinta työkalut kuten SCCM tai BSA

Järjestelmähallinta työkalut kuten BMC:n BladeLogic Server Automation (BSA) ja Microsoftin System Center Configuration Manager (SCCM) työkaluilla voidaan keskitetysti

hallita ja määrittää järjestelmä- ja tietoturvamäärityksiä järjestelmien piirissä oleville laitteille. Järjestelmähallintatyökalua ovat yleensä maksullisia, ja edellyttää että järjestelmähallinta-agentti asennetaan kohde laitteelle. (Microsoft System Center and BMC Management Tools Integration and Interaction, 2017.)



## 8 Palvelinkoventamiseen liittyvät lisätoimenpiteet

Palvelimelle olisi hyvä tehdä myös muita toimenpiteitä kuin käyttöjärjestelmäkohtaisia koventamismäärityksiä, joilla voidaan myös parantaa palvelimen tietoturvaa. Alla on kuvattu muita toimenpiteitä, jotka parantavat tietoturvaa. Näitä lisätoimenpiteitä ei ole kuvattu CIS Benchmarkeissa, mutta ne olisi hyvä huomioida palvelinkoventamisia tehdessä.

Asennusvaiheessa tulisi aina olla Windows NTFS -tiedostojärjestelmä otettu käyttöön, jonka avulla voidaan käyttöoikeuksia ja suojauksia tehdä tiedostojärjestelmäpohjaisesti. Oletuksena palvelimen asennusvaiheessa palvelimen levy alustetaan automaattisesti NTFS -tiedostojärjestelmäpohjaiseksi.

Palvelimen automaattisesti käynnistyvät palvelut tulisi ottaa muuttaa Disabled tilaan, jos eivät ole käytössä tai tarpeellisia palvelimella. Oletuksena palvelut käynnistyvät automaattisesti ja ovat toiminnassa taka-alalla. Myös palvelut tulisi käynnistää erillisillä palvelukohtaisilla tunnuksilla.

Palvelimelle tulisi määrittää tietoturvapäivitykset asentumaan automaattisesti. Tietoturvapäivitykset asennetaan automaattisesti palvelimille kerran kuukaudessa erikseen sovittuna ajankohtana. Organisaation tulisi määrittää oma käytäntö, miten tietoturvapäivityksiä asennetaan. Palvelimella tulisi myös olla asennettuna viimeisin Service Pack versio, joka on asennettu erikseen suunnitellun päivityskäytäntö aikataulun mukaan. Käytäntö edellyttää, että asennukset olisi testattu testipalvelimilla, ennen kuin asennus tehdään tuotantopalvelimelle.

Palvelimelle tulisi olla asennettuna ajan tasalla oleva virustorjuntaohjelma, joka hakee ajan tasalla olevat päivitykset automaattisesti. Virustorjunnan avulla torjutaan verkossa leviävistä haittaohjelmista tai palvelimelle ladatuissa tiedostoissa olevista tietoturvaohjelmista.

Palvelimella tulisi olla käytössä palvelimen paikallinen palomuurin (Windows Firewall). Palomuurilla on avattu vain tarpeelliset portit sekä mahdollisesti myös eri palvelut tai ohjelmat.

Palvelin tulisi sijaita suojaetuissa verkkovyöhykkeissä, jotka tulisi sijaita mieluummin erillisissä verkkovyöhykkeistä missä muuta verkon aktiivilaitteet sijaitsevat. Liikennöinti vaatii aina säätömuutoksia palomuurissa. Palomuurisäätö muutokset tehdään palvelujen välille, yhteen suuntaa ja vain käyttötarpeen vaatima portit ja protokolla luvutetaan.

Palvelimesta tulisi ottaa säännöllisin väliajoin vähintään täysvarmistus, missä varmuuskopioitava data kopioidaan täydellisesti ulkoisille varmistusmedioille. Varmistuksen avulla voidaan palautua aikaisempaan tilaan.

Fyysiselle palvelimelle tulisi olla asennettuna palvelinhallinta-agentit ajan tasalle. Jos palvelin on virtuaalinen palvelin, tulee siihen asentaa hallintatyökalut –ohjelmisto ajan tasalle. (The Windows Server Hardening Checklist, 2017.)

## 9 Palvelimen tietoturvatason tarkistustyökaluja

Palvelimen tietoturvatason on hyvä testata eri tavoilla säännöllisin väliajoin. Tietoturvatarkistus olisi myös hyvä tehdä palvelinkoentamisoluvaiheessa, jotta havaitaan mahdollisia uusia tietoturvavahko kohtia käyttöjärjestelmästä. Nämä kohdat on hyvä ottaa mukaan palvelinkoentamisoluvaiheessa, jotta ne tulisi muutettua tietoturvalisemmaksi.

Alla on lueteltu eri työkaluja, joiden avulla voidaan tehdä tietoturvaan liittyviä tarkistuksia.

### 9.1 Cis-Cat Pro

CIS-CAT PRO on tietoturvan asetuksien arviointi ja vertailu työkalu, jonka on kehittänyt CIS Security. Työkalu hyödyntää CIS Security Benchmarkkeja. Ohjelmisto on maksullinen. (CIS-CAT Pro, 2017.)

### 9.2 Nessus

Nessus on kattava tietoturvaan liittyvien haavoittuvuuksien skannausohjelmisto, jonka on kehittänyt Tenable Network Security. Nessus voidaan tehdä erilaisia tarkistuksia, kuten eri hakkereiden käyttämien haavoituuksien skannauksen, tietoturvapäivityksien puuttumisen, mahdolliset väärin tietoturva konfiguroinnit sekä salasanakäytäntöihin liittyviä tarkistuksia. Ohjelmisto on maksuton henkilökohtaiseen käyttöön. (Nessus, 2017.)

### 9.3 Microsoft Baseline Security Analyzer

Microsoft Baseline Security Analyzer (MBSA) on tietoturvan arviointityökalu, minkä on kehittänyt Microsoft. Ohjelma tarkistaa järjestelmän turvallisuuden tason. Ohjelma osaa myös tarkistaa onko palvelimen viimeisemmät tietoturvapäivitykset ajantasalla sekä ovatko palvelimen tietoturva-asetukset kunnossa. (Microsoft Baseline Security Analyzer, 2017.)

## 10 Palvelinkoventamismääritykset

Alla olevissa kohdissa käydään läpi tietoturva-asetuksia, joihin tehdään tietoturva-asetuksien muuttamisia. Olen kuvannut tietoturva-asetuskohdat, jotka muutetaan oletusasetuksista tietoturvallisemmaksi. Jos oletusasetus on saman kuin CIS MS Windows Server 2012 R2 Benchmark viitataan, asetusta ei ole kuvattuna tähän kohtaa. Kaikki kohdat löytyvät tämän opinnäytetyön liitteestä. Opinnäytetyön tutkimustyön tulokset olen koonnut tiedot yhteen taulukkoon. Tuloksien läpikäynnissä olen tarkistanut Windows Server 2012 R2 -palvelimen määrityksen Oletusarvon, CIS MS Windows Server 2012 R2 Benchmark -ohjeellisen asetuksen, sekä suositus asetuksen joka tulee ottaa käyttöön, jotta palvelin on tietoturvallisesti kovennettu.

CIS MS Windows Server 2012 R2 Benchmark ohjeellinen asetuksena on käytetty Level 1 - Member Server asetuksesta joka soveltuu Member Server rooliin omaavan palvelimen roolin.

### 10.1 Account Policies

Tämän kohdan alla on määritykset tunnuksen liittyvät käytännöt. Tämä kohta on jaettu kahteen osaan. Password Policy-osaan jossa, määritellään salamääritykset sekä Account lockout policy-osaan, jossa määritetään uloskirjauskäytännöt.

#### 10.1.1 Password Policy

Enforce password history -kohta on oletuksena 0, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 24 tai enemmän salasanaa muistaa. Suositukseni koventamisarvoksi on 24 salasanaa muistaa, kunnes aikaisemmin käytetty salasanaa voidaan ottaa käyttöön uudestaan.

Maximum password age -kohta on oletuksena 42 päivää, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 60 tai vähemmän päivää, mutta ei 0 päivää. Suositukseni koventamisarvoksi on 60 päivä välein salasana tulee vaihtaa.

Minimum password age -kohta on oletuksena 0 päivää, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 1 tai enemmän. Suositukseni koventamisarvoksi on 1 päivä päästä salasana voidaan vaihtaa toiseksi.

Minimum Password Length -kohta on oletuksena 0 merkkiä, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 15 tai enemmän merkkiä. Suositukseni koventamisarvoksi on 14 merkkiä tulisi salasanan olla.

Password Complexity Requirements -kohta on oletuksena Disabled, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Enabled. Suositukseni koventamisarvoksi on Enabled, salasana tulee olla.

Store Passwords using reversible encryption -kohta on oletuksena Disabled, CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Enabled.  
Suositukseni koventamisarvoksi on Disabled, jätetään oletus asetus voimaan.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Account Policies>Password Policy.

### 10.1.2 Account Lockout Policy

Account lockout duration -kohta on oletuksena asetukseen ei ole määritettyä arvoa., CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 15 minuuttia tai enemmän.  
Suositukseni koventamisarvoksi on 15 minuuttia kun salasana on lukossa.

Account lockout threshold duration -kohta on oletuksena 0 Invalid logon attempts. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 10 tai vähemmän väärin kirjautumisyrityksiä.  
Suositukseni koventamisarvoksi on 10 väärin kirjautumisyritystä.

Reset account lockout counter after duration -kohta on oletuksena asetukseen ei ole määritettyä arvoa., CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on 15 minuuttia tai enemmän.  
Suositukseni koventamisarvoksi on 15 minuuttia jonka, jälkeen salasana laskuri nollataan.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy.

## 10.2 Local Policies

Local Policies on jaettu kolmeen osaan, Audit Policy-, User Rights Assignment- sekä Security Options-osaan. Audit Policy-osan alla määritetään auditointi määrittelyt, User Rights Assignment-osa alla määritetään paikallisen palvelimen käyttöoikeudet sekä Security Options-osa alla määritetään paikallisten palvelimen tietoturva-asetuksiin liittyvät asetukset.

### 10.2.1 Audit Policy

Auditointi ei tee palvelin turvallisemmaksi, ja CIS MS Windows Server 2012 R2 Benchmarkin ei ota kantaa auditointi määrittelyihin. Suositukseni ovat, että koventamisen yhteydessä määritetään Auditointi määrittelyt, jotka auttavat löytämään ongelmanratkaisussa juurisyyn.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Local.

## 10.2.2 User Rights Assignment

Access this computer from the network duration -kohta on oletuksena Every-one, Administrators, Users, Backup Operators ryhmät. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators, Authenticated Users.

Suositukseni koventamisarvoksi kohtaan määritetään vain Administrators, Authenticated Users ryhmät.

Add workstations to domain -kohta on oletuksena tyhjä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators, ryhmä, jonka jäsenet voi vain liittää toimialueelle työasemia tai palvelimia.

Allow log on locally -kohta on oletuksena Administrators, Users, Backup Operators ryhmät. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators, ryhmän jäsenet jota voivat kirjautua paikallisesti palvelimelle.

Back up files and directories -kohta on oletuksena Administrators, Backup Operators ryhmät. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators, ryhmän jäsenet voivat vain ottaa varmistuksia.

Create symbolic links -kohta on oletuksena Administrators, NT VIRTUAL MACHINE\Virtual Machines. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators, ryhmän jäsenet voivat vain luoda Symbolic linkkejä.

Deny log on as a batch job -kohta on oletuksena Guests. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Guests, Local account and member of Administrators group.

Suositukseni koventamisarvoksi kohtaan määritetään Guests.

Deny log on as a batch job -kohta on oletuksena No one. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Guests.

Suositukseni koventamisarvoksi kohtaan määritetään Guests.

Deny log on as a service -kohta on oletuksena No one. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Guests.

Suositukseni koventamisarvoksi kohtaan määritetään Guests.

Deny log on through Remote Desktop Services service -kohta on oletuksena No one. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Guests, Local account.

Suositukseni koventamisarvoksi kohtaan määritetään Guests, Local account.

Log on as a batch job service -kohta on oletuksena Administrators, Backup Operators, Performance Log Users. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators.

Restore files and directories -kohta on oletuksena Administrators, Backup Operators. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators.

Shut down the system directories -kohta on oletuksena Administrators, Backup Operators. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus on Administrators.

Suositukseni koventamisarvoksi kohtaan määritetään Administrators.

Synchronize directory service data -kohta on oletuksena tyhjä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus No one.

Suositukseni koventamisarvoksi kohtaan määritetään No one.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Local Policies\User Rights Assignment.

### 10.2.3 Security Options

Accounts: Administrator account status -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled, oletus Administrator tunnus on pois käytössä ja erillinen ylläpitäjä tunnus on luotuna.

Accounts: Block Microsoft accounts status -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Users can't add or log on with Microsoft accounts.

Suositukseni koventamisarvoksi kohtaan määritetään Users can't add or log on with Microsoft accounts.

Accounts: Rename administrator account -kohta on oletuksena Administrator. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Rename this account to something that does not indicate its purpose.

Suositukseni koventamisarvoksi kohtaan määritetään Rename this account to something that does not indicate its purpose.

Accounts: Rename guest account -kohta on oletuksena Guest. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Rename this account to something that does not indicate its purpose.

Suositukseni koventamisarvoksi kohtaan määritetään Rename this account to something that does not indicate its purpose.

Audit: Force audit policy subcategory settings (Windows Vista or later) to over-ride audit policy category settings -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Devices: Allowed to format and eject removable media -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Administrators.  
Suositukseni koventamisarvoksi kohtaan määritetään Administrators.

Interactive logon: Display user information when the session is locked -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Interactive logon: Machine inactivity limit -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 900 tai vähemmän, mutta or fewer second(s), but not 0.  
Suositukseni koventamisarvoksi kohtaan määritetään 900 sekuntia.

Interactive logon: Number of previous logons to cache (in case domain controller is not available) limit -kohta on oletuksena 10 logons. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 4 or fewer logons.  
Suositukseni koventamisarvoksi kohtaan määritetään 4 kirjatumista muistetaan.

Interactive logon: Prompt user to change password before expiration -kohta on oletuksena 5 days. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus between 5 and 14 days.  
Suositukseni koventamisarvoksi kohtaan määritetään 14 päivää, jolloin tulee ilmoitus salasana vanhenemisesta.

Interactive logon: Require Domain Controller authentication to unlock workstation ration -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Interactive logon: Smart card removal behaviour ration -kohta on oletuksena No Action. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Lock Workstation.  
Suositukseni koventamisarvoksi kohtaan määritetään Lock Workstation.

Microsoft network client: Digitally sign communications (always) -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Microsoft network server: Digitally sign communications (always) -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.



Microsoft network server: Digitally sign communications (if client agrees) -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Microsoft network server: Server SPN target name validation level -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Accept if provided by client.

Suositukseni koventamisarvoksi kohtaan määritetään Accept if provided by client.

Network access: Allow anonymous SID/Name translation -kohta on oletuksena Enabled Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Network access: Do not allow anonymous enumeration of SAM accounts and shares -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Network access: Do not allow storage of passwords and credentials for network authentication shares -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Network access: Do not allow storage of passwords and credentials for network authentication-kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Network security: Allow Local System to use computer identity for NTLM authentication -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Network security: Allow LocalSystem NULL session fallback authentication -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Network security: Force logoff when logon hours expire -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Network security: LAN Manager authentication level -kohta on oletuksena Not Defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Send NTLMv2 response only. Refuse LM & NTLM.

Suositukseni koventamisarvoksi kohtaan määritetään Send NTLMv2 response only. Refuse LM & NTLM.

Network security: Minimum session security for NTLM SSP based (including secure RPC) clients -kohta on oletuksena Require 128-bit encryption. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Require NTLMv2 session security, Require 128-bit encryption.

Suositukseni koventamisarvoksi kohtaan määritetään Require NTLMv2 session security, Require 128-bit encryption.

Network security: Minimum session security for NTLM SSP based (including secure RPC) servers -kohta on oletuksena Require 128-bit encryption. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Require NTLMv2 session security, Require 128-bit encryption.

Suositukseni koventamisarvoksi kohtaan määritetään Require NTLMv2 session security, Require 128-bit encryption.

User Account Control: Admin Approval Mode for the Built-in Administrator account authentication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

User Account Control: Behavior of the elevation prompt for standard users -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

User Account Control: Only elevate executables that are signed and validated -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options.

### 10.3 Windows Firewall with Advanced Security

Windows Firewall with Advanced Security on jaettu kolmeen osaan, Domain Profile-, Private Profile- sekä Public Profile-osa. Domain Profile-osan alla määritetään palomuuriasetukset toimialue liikennöintiä varten, Private Profile-osa alla määritetään palomuuriasetukset tunnetussa verkossa liikennöintiä varten sekä Public Profile-osa alla määritetään palomuuriasetukset julkisen paikkojen verkossa liikennöintiä varten.

#### 10.3.1 Domain Profile

Domain: Logging: Size limit (KB)-kohta on oletuksena 4096 KB. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 16,384 KB or greater.

Suositukseni koventamisarvoksi kohtaan määritetään 16,384 KB

Domain: Logging: Log dropped packets -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes.

Domain: Logging: Log successful connections -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security.

### 10.3.2 Private Profile

Private: Logging: Size limit (KB)-kohta on oletuksena 4096 KB. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 16,384 KB or greater.

Suositukseni koventamisarvoksi kohtaan määritetään 16,384 KB.

Private: Logging: Log dropped packets -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes

Private: Logging: Log successful connections -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes.

Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security.

### 10.3.3 Public Profile

Public: Logging: Size limit (KB) -kohta on oletuksena 4096 KB. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 16,384 KB or greater.

Suositukseni koventamisarvoksi kohtaan määritetään 16,384 KB.

Public: Logging: Log dropped packets -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes.

Public: Logging: Log successful connections -kohta on oletuksena No. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Yes.

Suositukseni koventamisarvoksi kohtaan määritetään Yes.

Computer Configuration\Windows Settings\Security Settings\Windows Firewall with Advanced Security.

## 10.4 System Audit Policies

Account Logon: Audit Credential Validation -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Account management: Audit Computer Account Management-kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Account management: Audit Other Account Management Events -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Account management: Audit Security Group Management -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Account management: Audit User Account Management -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Detailed Tracking: Audit Process Creation -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success.  
Suositukseni koventamisarvoksi kohtaan määritetään Success.

Logon/Logoff: Audit Account Lockout -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success.  
Suositukseni koventamisarvoksi kohtaan määritetään Success.

Logon/Logoff: Audit Logoff -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success.  
Suositukseni koventamisarvoksi kohtaan määritetään Success.

Logon/Logoff: Audit Logon -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Logon/Logoff: Audit Other Logon/Logoff Events -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.  
Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Logon/Logoff: Audit Special Logon -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Object Access: Audit Removable Storage -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Policy Change: Audit Audit Policy Change -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Policy Change: Audit Authentication Policy Change -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Priviledge Use: Audit Sensitive Privilege Use -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

System: Audit IPsec Driver -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

System: Audit Other System Events -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

System: Audit Security State Change -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

System: Audit Security System Extension -kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

System: Audit System Integrity-kohta on oletuksena No auditing. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Success and Failure.

Suositukseni koventamisarvoksi kohtaan määritetään Success and Failure.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Security Settings\Advanced Audit Policy Configuration\System Audit Policies

## 10.5 Administrative Templates

Administrative Templates alla on useita osia. Näiden osien alla määritetään eri asetuksia käyttöjärjestelmän eri osa-alueille. Osa asetuksista vaikuttaa käytettävyyteen, osa toiminnallisuuteen, osa turvallisuuteen.

### 10.5.1 Personalization

Prevent enabling lock screen camera -kohta on oletuksena Not Configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Prevent enabling lock screen slide show -kohta on oletuksena Not Configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Control Panel\Personalization.

### 10.5.2 MSS (Legacy) Security Options

MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Highest protection, source routing is completely disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Highest protection, source routing is completely disabled.

MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Highest protection, source routing is completely disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Highest protection, source routing is completely disabled.

MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 300,000 or 5 minutes(recommended).

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 300,000.

MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default Gateway addresses (could lead to DoS) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

MSS: (SafeDllSearchMode) Enable Safe DLL search mode (recommended) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default) -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 5 or fewer seconds.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 5 seconds.

MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning -kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 90% or less.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 90%.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\MSS (Legacy).

### 10.5.3 Microsoft Peer-to-Peer Networking Services

Turn off Microsoft Peer-to-Peer Networking Services -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\ Network\ Microsoft Peer-to-Peer Networking Services.

### 10.5.4 Network Connections

Prohibit installation and configuration of Network Bridge on your DNS domain network -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

'Require domain users to elevate when setting a network's location' is set to 'Enabled - kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Network\Network Connections.

#### 10.5.5 Network Provider

Hardened UNC Paths -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Network\Network Provider.

#### 10.5.6 Windows Connect Now

Configuration of wireless settings using Windows Connect Now -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Prohibit access of the Windows Connect Now wizards -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\ Network\Windows Connect Now

#### 10.5.7 Windows Connection Manager

Minimize the number of simultaneous connections to the Internet or a Windows Domain kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Prohibit connection to non-domain networks when connected to domain authenticated network -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\ Network\ Windows Connection Manager



### 10.5.8 Pass the Hash Mitigations

Apply UAC restrictions to local accounts on network logons - kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\ Network\Pass the Hash Mitigations.

### 10.5.9 Audit Process Creation

Include command line in process creation events - kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\System\Audit Process Creation

### 10.5.10 Early Launch Antimalware

Boot-Start Driver Initialization Policy - kohta on oletuksena Not defined/Ei määritettynä. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: Good, unknown and bad but critical.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: Good, unknown and bad but critical.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Early Launch Antimalwar.

### 10.5.11 Logging and tracing

Configure registry policy processing: Do not apply during periodic background processing -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: FALSE.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: FALSE.

Configure registry policy processing: Process even if the Group Policy objects have not changed -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: TRUE.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: TRUE.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Group Policy.

### 10.5.12 Internet Communication settings

Turn off access to the Store -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off downloading of print drivers over HTTP -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off handwriting personalization data sharing -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off handwriting recognition error reporting -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off Internet download for Web publishing and online ordering wizards -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off printing over HTTP -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off Registration if URL connection is referring to Microsoft.com -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication settings.

### 10.5.13 Locale Services

Disallow copying of user input methods to the system account for sign-in Now -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Locale Services.

#### 10.5.14 Logon

Do not display network selection UI -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Do not enumerate connected users on domain-joined computers -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off app notifications on the lock screen -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Logon.

#### 10.5.15 Remote Procedure Call

Enable RPC Endpoint Mapper Client Authentication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Remote Procedure Call.

#### 10.5.16 Microsoft Support Diagnostic Tool

Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider-kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Microsoft Support Diagnostic Tool\

#### 10.5.17 Windows Performance PerfTrack

Enable/Disable PerfTrack provider -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Troubleshooting and Diagnostics\Windows Performance PerfTrack\.

#### 10.5.18 User Profiles

Turn off the advertising ID -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\User Profiles\.

#### 10.5.19 Time Providers

Enable Windows NTP Client tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\System\Windows Time Service\Time Providers\.

#### 10.5.20 App runtime

Allow Microsoft ac-counts to be optional tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\App runtime\.

#### 10.5.21 AutoPlay Policies

Disallow Autoplay for non-volume devices tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Set the default behavior for AutoRun tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Do not execute any auto-run commands.

Suositukseni koventamisarvoksi kohtaan määritetään Do not execute any auto-run commands.

Turn off Autoplay' tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: All drives.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: All drives.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies\

#### 10.5.22 Credential User Interface

Do not display the password reveal button tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Credential User Interface\

#### 10.5.23 EMET

EMET 5.51-kohta on oletuksena Not defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Install EMET 5.51 or higher.  
Suositukseni koventamisarvoksi kohtaan määritetään Install EMET 5.51.

Default Action and Mitigation Settings -kohta on oletuksena User configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Default Protections for Internet Explorer-kohta on oletuksena Not configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Default Protections for Popular Software-kohta on oletuksena Not configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Default Protections for Recommended Software-kohta on oletuksena Not configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

System ASLR-kohta on oletuksena Not configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

System DEP'-kohta on oletuksena Not configured. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

System SEHOP'-kohta on oletuksena Not defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Windows Settings\Administrative Templates\ Network\Windows Connect Now\Configuration of wireless settings using Windows Connect Now.

#### 10.5.24 Event Log Service

Application: Specify the maximum log file size (KB) -kohta on oletuksena 20,480. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 32,768 or greater. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 32,768.

Security: Specify the maximum log file size (KB) -kohta on oletuksena 20,480. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 32,768 or greater. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 32,768.

Setup: Specify the maximum log file size (KB) -kohta on oletuksena 20,480. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 32,768 or greater. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 32,768.

System: Specify the maximum log file size (KB) -kohta on oletuksena 20,480. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 32,768 or greater. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 32,768.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Event Log Service\Setup\.

#### 10.5.25 Previous Versions

Configure Windows SmartScreen tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off Data Execution Prevention for Explorer-kohta on oletuksena Not defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled. Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Turn off shell protocol protected mode -kohta on oletuksena Not defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled. Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\File Explorer\

#### 10.5.26 Location and Sensors

Turn off location tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Location and Sensors\

#### 10.5.27 OneDrive (formerly SkyDrive)

Prevent the usage of OneDrive for file storage tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Prevent the usage of OneDrive for file storage on Windows 8.1 tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\OneDrive\.

#### 10.5.28 RemoteFX USB Device Redirection

Do not allow pass-words to be saved tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Connection Client\

#### 10.5.29 Device and Resource Redirection

Do not allow COM port redirection tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Do not allow drive redirection tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Do not allow LPT port redirection tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Do not allow supported Plug and Play device redirection tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Device and Resource Redirection\.

#### 10.5.30 Security

Always prompt for password upon connection tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Require secure RPC communication tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Set client connection encryption level tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: High Level. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: High Level

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Security\.

#### 10.5.31 Session Time Limits

Set time limit for active but idle Remote Desktop Services sessions -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 15 minutes or less'. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 15 minutes.

Set time limit for disconnected sessions tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 1 minute'. Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 1 minute.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Remote Desktop Services\Remote Desktop Session Host\Session Time Limits\.

#### 10.5.32 RSS Feeds

Prevent downloading of enclosures tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled. Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\RSS Feeds\.



### 10.5.33 OCR

Set what information is shared in Search-kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: Anonymous info  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled: Anonymous info.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Search\.

### 10.5.34 Software Protection Platform

Turn off KMS Client Online AVS Validation tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Software Protection Platform\

### 10.5.35 Store

Turn off the offer to update to the latest version of Windows -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Turn off the Store application -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Store\.

### 10.5.36 Consent

Automatically send memory dumps for OS-generated error reports application -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Error Reporting\Consent\

### 10.5.37 Windows Logon Options

Sign-in last interactive user automatically after a system-initiated restart tication -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Logon Options\.

### 10.5.38 Windows PowerShell

Turn on PowerShell Script Block Logging tication -kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows PowerShell\.

### 10.5.39 WinRM Client

Disallow Digest authentication tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Client\.

### 10.5.40 WinRM Service

Disallow WinRM from storing RunAs credentials -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Remote Management (WinRM)\WinRM Service.

### 10.5.41 Windows Remote Shell

Allow Remote Shell Access-kohta on oletuksena Enabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Disabled.

Suositukseni koventamisarvoksi kohtaan määritetään Disabled.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Administrative Templates\Windows Components\Windows Remote Shell\

#### 10.5.42 Defer Windows Updates

Configure Automatic Updates: Scheduled install day tication -kohta on oletuksena Not Defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus 0 - Every day'.

Suositukseni koventamisarvoksi kohtaan määritetään 0 - Every day'.

Asetukset löytyvät Local security policy kohdasta Computer Configuration\Policies\Administrative Templates\Windows Components\Windows Update\.

#### 10.5.43 Personalization

Enable screen saver tication -kohta on oletuksena User Defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Force specific screen saver: Screen saver executable name tication -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: scrn-save.scr'.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: scrn-save.scr.

Password protect the screen saver tication -kohta on oletuksena User Defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Screen saver timeout -kohta on oletuksena User Defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled: 900 seconds or fewer, but not 0'.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled: 900 seconds.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\Control Panel\Personalization\.

#### 10.5.44 Notifications

Turn off toast notifications on the lock screen -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.

Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\Start Menu and Taskbar\Notifications\

#### 10.5.45 Internet Communication settings

Turn off Help Experience Improvement Program -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\System\Internet Communication Management\Internet Communication Settings\

#### 10.5.46 Attachment Manager

Notify antivirus programs when opening attachments -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\Windows Components\Attachment Manager\

#### 10.5.47 Network Sharing

Prevent users from sharing files within their profile -kohta on oletuksena Disabled. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\Windows Components\Network Sharing\.

#### 10.5.48 Playback

Prevent Codec Download -kohta on oletuksena User defined. CIS MS Windows Server 2012 R2 Benchmarkin ohjeellinen suositus Enabled.  
Suositukseni koventamisarvoksi kohtaan määritetään Enabled.

Asetukset löytyvät Local security policy kohdasta User Configuration\Policies\Administrative Templates\Windows Components\Windows Media Player\Playback\

## 11 Yhteenveto

Opinnäytetyön tutkimustyön pohjalta voidaan todeta, että Windows Server 2012 palvelun on turvallinen käyttöjärjestelmä, kun siihen otetaan mukaan CIS Microsoft Windows Server 2012 R2 Benchmark-standardin tuomat tietoturva-asetukset mukaan. Tutkimustyön lopputuloksena on tarkistettu yhteensä 288 Windows tietoturva-asetusta, joista 135 on muutettu Windows Server oletusmäärittämisestä tietoturvalisemmäksi määrittämisiksi. Loput 153 asetusta on tarkistettu ja hyväksytty, niin että oletusasetus on riittävän turvallinen asetusta perustuen CIS Microsoft Windows Server 2012 R2 Benchmark-standardiin.

Palvelinkoventamisessa tulee suunnitella etukäteen työn kulku ja peruslähteenä käytettävä koventamislähde. Koventamistyön tulee olla dokumentoitu, jotta nähdään mitä on muutettu oletusasetuksiin verrattuna. Työhön tulee ottaa mukaan organisaation eri osastoilta useampia asiantuntijoita, jotka voivat selvittää ja tarkistaa toiminnallisuusvaikutuksia eri osa-alueiden osalta. Palvelinkoventaminen tulee myös tiedottaa organisaatiolle, että on käytössä olemassa olevat tapa tehdä palvelimista tietoturvallisia. Myös organisaation johdon pitää tukea palvelinkoventamista, jotta työaika voidaan käyttää työn tekemiseen, sekä erilaisia työkaluja, joiden avulla voidaan jalkauttaa palvelinkoventamiset käyttöönoton yhteydessä.

Palvelinkoventaminen tulisi ottaa osaksi palvelimien käyttöönottoprosessia, jotta palvelimet tulisivat aina asennettua, niin että lopputuloksena olisi kovennettuna käyttöjärjestelmä. Uusiin palvelimiin palvelinkoventamisen käyttöönotto on helpompaa kuin tuotannossa olevaan. Jälkimmäisessä tapauksessa tulee selvittää etukäteen vaikuttaako koventamisasetus johonkin olemassa olevaan toiminnallisuustoimintaan.

## Lähteet

Werner, F. (2014). Windows Server 2012 Editions comparison. Haettu 15.6.2014 osoitteesta

[https://www.thomas-krenn.com/en/wiki/Windows\\_Server\\_2012\\_Editions\\_comparison](https://www.thomas-krenn.com/en/wiki/Windows_Server_2012_Editions_comparison)

Hammell, J. (2015). Server Hardening. Haettu 14.7.2015 osoitteesta

<http://www.serverhardening.com/>

Deming (n.d.). Deming model. Haettu 14.12.2016 osoitteesta

<http://Deming.org>

Deming (n.d.). Deming PDCA Cycle. Haettu 14.12.2016 osoitteesta

<https://deming.org/explore/p-d-s-a>

CIS Center for Internet Security (n.d.). CIS Center for Internet Security. Haettu 14.6.2014 osoitteesta

<https://www.cisecurity.org/>

CIS Center for Internet Security (n.d.). CIS Benchmarks. Haettu 14.6.2014 osoitteesta

<https://benchmarks.cisecurity.org/>

Microsoft (n.d.). Microsoft Security Compliance Manager (SCM). Haettu 14.6.2016 osoitteesta

<http://social.technet.microsoft.com/wiki/contents/articles/774.microsoft-security-compliance-manager-scm.aspx>

Microsoft (n.d.). Baseline Server Hardening. Haettu 14.6.2014 osoitteesta

<https://technet.microsoft.com/en-us/library/cc526440.aspx>

Microsoft (n.d.). Suojausasetusten palauttaminen niiden oletusasetuksiksi (2017). Haettu 14.4.2017 osoitteesta

<https://support.microsoft.com/fi-fi/help/313222/how-do-i-restore-security-settings-to-a-known-working-state>

Microsoft (n.d.). Local Security Policy. Haettu 14.5.2017 osoitteesta

<https://technet.microsoft.com/en-us/library/dd277395.aspx>

Microsoft (n.d.). Local Group Policy Editor. Haettu 14.5.2017 osoitteesta

[https://technet.microsoft.com/en-us/library/cc725970\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc725970(v=ws.11).aspx)

Petri D. (n.d.). Using the Windows Server 2012 Security Configuration and Analysis Tool. Haettu 14.5.2017 osoitteesta

<https://www.petri.com/using-windows-server-2012-security-configuration-and-analysis-tool>

Microsoft (n.d.). Group Policy Management Console. Haettu 14.5.2017 osoitteesta [https://technet.microsoft.com/en-us/library/cc753298\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc753298(v=ws.11).aspx)

Microsoft (n.d.). Microsoft System Center and BMC Management Tools Integration and Interaction Haettu 14.5.2017 osoitteesta <https://blogs.technet.microsoft.com/andrew/2012/02/14/microsoft-system-center-and-bmc-management-tools-integration-and-interaction/>

UpGuard (n.d.) The Windows Server Hardening Checklist. Haettu 14.5.2017 osoitteesta <https://www.upguard.com/blog/the-windows-server-hardening-checklist>

CIS Center for Internet Security (n.d.). CIS-CAT Pro. Haettu 14.5.2017 osoitteesta <https://www.cisecurity.org/tools/cis-cat-pro/>

Tenable (n.d.) Nessus. Haettu 14.5.2017 osoitteesta <http://www.tenable.com/products/nessus>.

Microsoft (n.d.). Microsoft Baseline Security Analyzer. Haettu 14.5.2017 osoitteesta <https://technet.microsoft.com/fi-fi/security/cc184924.aspx>

CIS Center for Internet Security (n.d.). CIS Microsoft Windows Server 2012 R2 Benchmark versio 2.2.1. Haettu 14.3.2017 osoitteesta <https://www.cisecurity.org/cis-benchmarks/>

## Liite 1

## CIS Koventamis määrittymiset

Liitteessä on kuvattu kaikki CIS Microsoft Windows Server 2012 r2 Benchmark 2.2.1 -dokumentissa kuvatut tietoturva-asetukset. Taulukkoon on tuotu palvelimelta tietoturva-asetuksen Oletusarvo, viitekehysdokumentista saatu arvo, sekä arvo joka tulisi ottaa käyttöön, kun halutaan asetukseen tehdä koventaminen.

## Account Policies

- Password Policy

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Enforce password history	0	24 or more password(s)	24	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.1
Maximum password age	42	60 or fewer days, but not 0	60	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.2
Minimum password age	0	1 or more day(s).	1	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.3
Minimum Password Length	0	14 or more character(s)	14	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.4
Password Complexity Requirements	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.5
Store Passwords using reversible encryption	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.1.6

- Account Lockout Policy

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Account lockout duration	N/A	15 or more minute(s)	15	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.2.1



Account lockout threshold	N/A	10 or fewer invalid logon attempt(s), but not 0.	10	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.2.2
Reset account lockout counter after	0	15 or more minute(s)	15	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 1.2.3

## Local Policies

- Audit Policy

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Audit account logon events	No Auditing	N/A	Success, Failure	Logitietojen kerääminen ei tee ei tee palvelinta tietoturvallisemmaksi, vaan auttaa ongelmahallinnassa
Audit account management	No Auditing	N/A	Success, Failure	Kts. peruste yllä
Audit directory service access	No Auditing	N/A	No Auditing	Kts. peruste yllä
Audit logon events	No Auditing	N/A	Success, Failure	Kts. peruste yllä
Audit object access	No Auditing	N/A	Success, Failure	Kts. peruste yllä
Audit privilege use	No Auditing	N/A	Success, Failure	Kts. peruste yllä
Audit process tracking	No Auditing	N/A	No Auditing	Kts. peruste yllä
Audit system events	No Auditing	N/A	No Auditing	Kts. peruste yllä

- User Rights Assignment

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Access Credential Manager as a trusted caller	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.1

Access this computer from the network	Everyone, Administrators, Users, Backup Operators	Administrators, Authenticated Users	Administrators, Authenticated Users	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.2
Act as part of the operating system	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.3
Add workstations to domain	N/A	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.4
Adjust memory quotas for a process	LOCAL SERVICE, NETWORK SERVICE, Administrators	Administrators, Local Service, Network Service	Administrators, Local Service, Network Service	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.5
Allow log on locally	Administrators, Users, Backup Operators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.6
Allow log on through Remote Desktop Services	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users	Administrators, Remote Desktop Users	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.7
Back up files and directories	Administrators, Backup Operators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.8
Change the system time	LOCAL SERVICE, Administrators	LOCAL SERVICE, Administrators	LOCAL SERVICE, Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.9
Change the time zone	LOCAL SERVICE, Administrators	LOCAL SERVICE, Administrators	LOCAL SERVICE, Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.10
Create a pagefile	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.11
Create a token object	N/A	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.12

Create global objects	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	LOCAL SERVICE,NETWORK SERVICE,Administrators,SERVICE	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.13
Create permanent shared objects	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.14
Create symbolic links	Administrators,NT VIRTUAL MACHINE\Virtual Machines	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.15
Debug programs	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.16
Deny access to this computer from the network	Guests	Guests, Local account and member of Administrators group	Guests	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.17
Deny log on as a batch job	No One	Guests	Guests	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.18
Deny log on as a service	No One	Guests	Guests	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.19
Deny log on locally	Guests	Guests	Guests	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.20
Deny log on through Remote Desktop Services	No One	Guests, Local account	Guests, Local account	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.21
Enable computer and user accounts to be trusted for delegation	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.22

Force shutdown from a remote system	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.23
Generate security audits	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE	LOCAL SERVICE, NETWORK SERVICE	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.24
Impersonate a client after authentication	LOCAL SERVICE, NETWORK SERVICE, Administrators, SERVICE	LOCAL SERVICE, NETWORK SERVICE, Administrators, SERVICE	LOCAL SERVICE, NETWORK SERVICE, Administrators, SERVICE	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.25
Increase scheduling priority	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.26
Load and unload device drivers	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.27
Lock pages in memory	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.28
Log on as a batch job	Administrators, Backup Operators, Performance Log Users	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.29
Manage auditing and security log	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.30
Modify an object label	No One	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.31
Modify firmware environment values	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.32
Perform volume maintenance tasks	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.33

Profile single process	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.34
Profile system performance	Administrators,NT SERVICE\WdiServiceHost	Administrators,NT SERVICE\WdiServiceHost	Administrators,NT SERVICE\WdiServiceHost	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.35
Replace a process level token	Local Service, Network Service	Local Service, Network Service	Local Service, Network Service	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.36
Restore files and directories	Administrators,Backup Operators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.37
Shut down the system	Administrators,Backup Operators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.38
Synchronize directory service data	N/A	No One	No One	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.39
Take ownership of files or other objects	Administrators	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.2.40

## Security Options

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Accounts: Administrator account status	Enabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.1
Accounts: Block Microsoft accounts	Not Defined	Users can't add or log on with Microsoft accounts.	Users can't add or log on with Microsoft accounts.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.2
Accounts: Guest account status	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.3

Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.4
Accounts: Rename administrator account	Administrator	Rename this account to something that does not indicate its purpose	Rename this account to something that does not indicate its purpose	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.5
Accounts: Rename guest account	Guest	Rename this account to something that does not indicate its purpose	Rename this account to something that does not indicate its purpose	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.1.6
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Not Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.2.1
Audit: Shut down system immediately if unable to log security audits	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.2.2
Devices: Allowed to format and eject removable media	Not Defined	Administrators	Administrators	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.4.1
Devices: Prevent users from installing printer drivers	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.4.2
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.2

Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.2
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.3
Domain member: Disable machine account password changes	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.4
Domain member: Maximum machine account password age	30 days	30 or fewer days, but not 0	30 days	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.5
Domain member: Require strong (Windows 2000 or later) session key	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.6.6
Interactive logon: Display user information when the session is locked	Not Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.1
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.2
Interactive logon: Machine inactivity limit	Not Defined	900 or fewer second(s), but not 0	900 or fewer seconds	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.3
Interactive logon: Message text for users attempting to log on	Not Defined	Org.Taso viesti	Org.Taso viesti	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.4
Interactive logon: Message title for users attempting to log on	Not Defined	Org.Taso viesti	Org.Taso	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.5

Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10 logons	4 or fewer logons	4 or fewer logons	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.6
Interactive logon: Prompt user to change password before expiration	5 days	between 5 and 14 days	14	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.7
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Enabled.	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.8
Interactive logon: Smart card removal behavior	No Action	Lock Workstation	Lock Workstation	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.7.9
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.8.1
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.8.2
Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.8.3
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 or fewer minute(s), but not 0	15 minutes	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.9.1
Microsoft network server: Digitally sign communications (always)	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.9.2
Microsoft network server: Digitally sign communications (if client agrees)	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.9.3



Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.9.4
Microsoft network server: Server SPN target name validation level	Not Defined	Accept if provided by client	Accept if provided by client	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.9.5
Network access: Allow anonymous SID/Name translation %CHECK%	Enabled	Disabled.	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.1
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.2
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.3
Network access: Do not allow storage of passwords and credentials for network authentication	Disabled	Enabled.	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.4
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.5
Network access: Named Pipes that can be accessed anonymously	Disabled, None	None	None	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.6
Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions, System\CurrentControlSet\Control\Server Applications, Software\Microsoft\Windows	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Serv	System\CurrentControlSet\Control\ProductOptions System\CurrentControlSet\Control\Server	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.7

	NT\CurrentVersion	er Applications Software\Microsoft\Windows NT\CurrentVersion	Applications Software\Microsoft\Windows NT\CurrentVersion	
Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlSet\Control\Print\Printers, System\CurrentControlSet\Services\Eventlog, Software\Microsoft\OLAP Server, Software\Microsoft\Windows NT\CurrentVersion\Print, Software\Microsoft\Windows NT\CurrentVersion\Windows, System\CurrentControlSet\Control\ContentIndex, System\CurrentControlSet\Control\Terminal Server, System\CurrentControlSet\Control\Terminal Server\Us-erConfig, System\CurrentControlSet\Con-	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server	System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.8

	trol\Terminal Server\DefaultUserConfiguration,Software\Microsoft\Windows NT\CurrentVersion\Perflib,System\CurrentControlSet\Services\SymonLog	trol\Terminal Server		
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.9
Network access: Shares that can be accessed anonymously	Not Defined	No one	No one	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.10
Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	Classic - local users authenticate as themselves	Classic - local users authenticate as themselves	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.10.11
Network security: Allow Local System to use computer identity for NTLM	Not Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.1
Network security: Allow LocalSystem NULL session fallback	Not Defined	Disabled.	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.2
Network security: Allow PKU2U authentication requests to this computer to use online identities.	Disabled.	Disabled.	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.3
Network security: Configure encryption types allowed for Kerberos	Not Defined %CHECK%	RC4_HMAC_MD5, AES128_HMAC_SHA1,	RC4_HMAC_MD5, AES128_HMAC_SHA1,	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.4

		AES256_HMAC_SHA1, Future encryption types.	AES256_HMAC_SHA1, Future encryption types.	
Network security: Do not store LAN Manager hash value on next password change	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.5
Network security: Force logoff when logon hours expire	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.6
Network security: LAN Manager authentication level	Not Defined	Send NTLMv2 response only. Refuse LM & NTLM	Send NTLMv2 response only. Refuse LM & NTLM	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.7
Network security: LDAP client signing requirements	Negotiate signing	Negotiate signing	Negotiate signing	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.8
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.9
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption	Require NTLMv2 session security, Require 128-bit encryption	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.11.10
Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.13.1

System objects: Require case insensitivity for non-Windows subsystems	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.15.1
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.15.2
User Account Control: Admin Approval Mode for the Built-in Administrator account	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.1
User Account Control: Allow UIAccess applications to prompt for elevation without using the secure desktop	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.2
User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode	Prompt for consent for non-Windows binaries	Prompt for consent for non-Windows binaries	Prompt for consent for non-Windows binaries	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.3
User Account Control: Behavior of the elevation prompt for standard users	Prompt for credentials	Automatically deny elevation requests	Automatically deny elevation requests	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.4
User Account Control: Detect application installations and prompt for elevation	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.5
User Account Control: Only elevate UIAccess applications that are installed in secure locations	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.6
User Account Control: Run all administrators in Admin Approval Mode	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.7
User Account Control: Switch to the secure desktop when prompting for elevation	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.8

User Account Control: Virtualize file and registry write failures to per-user locations	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 2.3.17.9
---	---------	---------	---------	---

## Windows Firewall With Advanced Security

### Domain Profile

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Domain: Firewall state	Not Configured	On	On (recommended)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.1
Domain Profile: Inbound Connections	Not Configured	Enabled:Block (Default)	Enabled:Block (Default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.2
Domain: Outbound connections	Not Configured	Allow (default)	Allow (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.3
Domain: Display a notification'	Not Configured	No	No	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.4
Domain: Apply local firewall rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.5
Domain: Apply local connection security rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.6
Domain: Logging	Not Configured	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\domainfw.log	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.7
Domain: Logging: Size limit (KB)	Not Configured	16,384 KB or greater.	16,384 KB	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.8
Domain: Logging: Log dropped packets	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1

				Paragraph 9.1.9
Domain: Logging: Log successful connections	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.1.10

## Private Profile

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Private: Firewall state	Not Configured	On	On (recommended)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.1
Private Profile: Inbound Connections	Not Configured	Enabled: Block (Default)	Enabled: Block (Default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.2
Private: Outbound connections	Not Configured	Allow (default)	Allow (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.3
Private: Display a notification'	Not Configured	No	No	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.4
Private: Apply local firewall rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.5
Private: Apply local connection security rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.6
Private: Logging	Not Configured	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log.	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.7
Private: Logging: Size limit (KB)	Not Configured	16,384 KB or greater.	16,384 KB	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.8
Private: Logging: Log dropped packets	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.9

Private: Logging: Log successful connections	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.2.10
--	----------------	------	------	--

## Public Profile

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Public: Firewall state	Not Configured	On	On (recommended)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.1
Public Profile: Inbound Connections	Not Configured	Enabled: Block (Default)	Enabled: Block (Default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.2
Private: Outbound connections	Not Configured	Allow (default)	Allow (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.3
Public: Display a notification'	Not Configured	No	No	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.4
Public: Apply local firewall rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.5
Public: Apply local connection security rules	Not Configured	Yes (default)	Yes (default)	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.6
Public: Logging	Not Configured	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log.	Enabled: %SYSTEMROOT%\System32\logfiles\firewall\privatefw.log	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.7
Public: Logging: Size limit (KB)	Not Configured	16,384 KB or greater.	16,384 KB	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.8
Public: Logging: Log dropped packets	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.9



Public: Logging: Log successful connections	Not Configured	Yes.	Yes.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 9.3.10
---	----------------	------	------	--

### System Audit Policies

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Account Logon: Audit Credential Validation	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.1
Account management: Audit Computer Account Management	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.2
Account management: Audit Other Account Management Events	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.2.4
Account management: Audit Security Group Management	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.2.5
Account management: Audit User Account Management	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.2.6
Detailed Tracking: Audit Process Creation	No auditing	Success	Success	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.3.1
Logon/Logoff: Audit Account Lockout	No auditing	Success	Success	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.5.1
Logon/Logoff: Audit Logoff	No auditing	Success	Success	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.5.2
Logon/Logoff: Audit Logon	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.5.3
Logon/Logoff: Audit Other Logon/Logoff Events	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.5.4

Logon/Logoff: Audit Special Logon	No auditing	Success	Success	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.5.5
Object Access: Audit Removable Storage	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.6.1
Policy Change: Audit Audit Policy Change	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.7.1
Policy Change: Audit Authentication Policy Change	No auditing	Success	Success	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.7.2
Privilege Use: Audit Sensitive Privilege Use	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.8.1
System: Audit IPsec Driver	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.9.1
System: Audit Other System Events	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.9.2
System: Audit Security State Change	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.9.3
System: Audit Security System Extension	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.9.4
System: Audit System Integrity	No auditing	Success and Failure	Success and Failure	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 17.9.5

## Administrative Templates

### Personalization

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Prevent enabling lock screen camera	Not configured	Enabled	Enabled:	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.1.1.1
Prevent enabling lock screen slide show	Not configured	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.1.1.2

## MSS (Legacy) Security Options

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
MSS: (AutoAdminLogon) Enable Automatic Logon (not recommended)	Not defined	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.1
MSS: (DisableIPSourceRouting IPv6) IP source routing protection level (protects against packet spoofing)	Not defined	Highest protection, source routing is completely disabled	Highest protection, source routing is completely disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.2
MSS: (DisableIPSourceRouting) IP source routing protection level (protects against packet spoofing)	Not defined	Highest protection, source routing is completely disabled	Highest protection, source routing is completely disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.3
MSS: (EnableICMPRedirect) Allow ICMP redirects to override OSPF generated routes	Not defined	Disabled.	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.4
MSS: (KeepAliveTime) How often keep-alive packets are sent in milliseconds	Not defined	Enabled: 300,000 or 5 minutes (recommended).	300,000 ms	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.5
MSS: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers	Not defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.6
MSS: (PerformRouterDiscovery) Allow IRDP to detect and configure Default	Not defined	Disabled.	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.7

Gateway addresses (could lead to DoS)				
MSS: (SafeDllSearch-Mode) Enable Safe DLL search mode (recommended)	Not defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.8
MSS: (ScreenSaverGracePeriod) The time in seconds before the screen saver grace period expires (0 recommended)	5 seconds	Enabled: 5 or fewer seconds	Enabled: 5	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.9
MSS: (TcpMaxDataRetransmissions IPv6) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	5	Enabled: 3	Enabled: 3	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.10
MSS: (TcpMaxDataRetransmissions) How many times unacknowledged data is retransmitted (3 recommended, 5 is default)	5	Enabled: 3	Enabled: 3	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.11
MSS: (WarningLevel) Percentage threshold for the security event log at which the system will generate a warning	Not defined	Enabled: 90% or less	90 %	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.3.12

## Link-Layer Topology Discovery

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Turn on Mapper I/O (LLTDIO) driver	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.9.1
Turn on Responder (RSPNDR) driver	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.9.2

## Microsoft Peer-to-Peer Networking Services

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Turn off Microsoft Peer-to-Peer Networking Services	Disabled	Enabled.	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.10.2

## Network Connections

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Prohibit installation and configuration of Network Bridge on your DNS domain network	Disabled	Enabled.	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.11.2
Require domain users to elevate when setting a network's 'location' is set to 'Enabled'	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.11.3

## Network Provider

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Hardened UNC Paths	Disabled	Enabled.	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.14.1

## TCP/IP Settings

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Disable IPv6	All IPv6 components are enabled and Windows prefers IPv6 over IPv4	CIS Benchmarks for Windows arvo	Disabled-Components - 0xff (255).	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.19.2.1

## Windows Connect Now

Asetus	Oletusarvo palvelimella	CIS Benchmarks for	Koven-tamis su-ositusarvo	Peruste/Lähde

		Windows arvo		
Configuration of wireless settings using Windows Connect Now	Enabled	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.20.1
Prohibit access of the Windows Connect Now wizards	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.20.2

## Windows Connection Manager

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Minimize the number of simultaneous connections to the Internet or a Windows Domain	None	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.21.1
Prohibit connection to non-domain networks when connected to domain authenticated network	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.4.21.2

## Pass the Hash Mitigations

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Apply UAC restrictions to local accounts on network logons	None	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.6.1
WDigest Authentication'	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.6.2

## Audit Process Creation

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Include command line in process creation events	None	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.3.1

## Early Launch Antimalware

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Boot-Start Driver Initialization Policy	None	Enabled: Good, unknown and bad but critical.	Enabled: Good, unknown and bad but critical..	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.12.1

## Logging and tracing

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Configure registry policy processing: Do not apply during periodic background processing	Disabled.	Enabled: FALSE	Enabled: FALSE.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.19.2.
Configure registry policy processing: Process even if the Group Policy objects have not changed	Disabled	Enabled: TRUE	Enabled: TRUE	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.19.3.
Turn off background refresh of Group Policy'	Disabled.	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.19.4

## Internet Communication settings

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Turn off access to the Store	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.1
Turn off downloading of print drivers over HTTP'	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.2
Turn off handwriting personalization data sharing	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.3
Turn off handwriting recognition error reporting	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.4

Turn off Internet Connection Wizard if URL connection is referring to Microsoft.com'	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.5
Turn off Internet download for Web publishing and online ordering wizards	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.6
Turn off printing over HTTP	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.7
Turn off Registration if URL connection is referring to Microsoft.com	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.8
Turn off Search Companion content file updates	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.9
Turn off the "Order Prints" picture task'	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.10
Turn off the "Publish to Web	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.11
Turn off the Windows Messenger Customer Experience Improvement Program		Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.12
Turn off Windows Customer Experience Improvement Program		Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.13
turn off Windows Error Reporting	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.20.1.14

## Locale Services

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Disallow copying of user input methods to the system account for sign-in	Enabled	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.24.1

## Logon



Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Do not display network selection UI	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.25.1
Do not enumerate connected users on domain-joined computers	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.25.2
Enumerate local users on domain-joined computers	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.25.3
Turn off app notifications on the lock screen'	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.25.4
Turn on convenience PIN sign-in'	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.25.5

## Sleep Settings

Asetus	CIS Benchmarks for Windows arvo	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Require a password when a computer wakes (on battery)	Enabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.29.5.1
Require a password when a computer wakes (plugged in)'	Enabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.29.5.2

## Remote Assistance

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Configure Offer Remote Assistance	Disabled	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.31.1
Configure Solicited Remote Assistance'		Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.31.2

## Remote Procedure Call

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Enable RPC Endpoint Mapper Client Authentication	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.32.1
Restrict Unauthenticated RPC clients	Enabled: Authenticated.	Enabled: Authenticated.	Enabled: Authenticated.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.32.2

## Microsoft Support Diagnostic Tool

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Microsoft Support Diagnostic Tool: Turn on MSDT interactive communication with support provider	Enabled	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.39.5.1

## Windows Performance PerfTrack

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Enable/Disable PerfTrack	Enabled	Disabled	Disabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.39.11.1

## User Profiles

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
Turn off the advertising ID	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.41.1

## Time Providers

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koventamis suositusarvo	Peruste/Lähde
--------	-------------------------	---------------------------------	-------------------------	---------------

Enable Windows NTP Client	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.44.1.1
Enable Windows NTP Server	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.8.44.1.2

## App runtime

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Allow Microsoft accounts to be optional	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.6.1

## AutoPlay Policies

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Disallow Autoplay for non-volume devices'	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.8.1
Set the default behavior for AutoRun	Disabled	Do not execute any autorun commands.	Do not execute any autorun commands.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.8.2
Turn off Autoplay'	Disabled	Enabled: All drives.	Enabled: All drives.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.8.3

## Credential User Interface

Asetus	Oletusarvo palvelimella	CIS Benchmarks for Windows arvo	Koven-tamis su-ositusarvo	Peruste/Lähde
Do not display the password reveal button	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.15.1
Enumerate administrator accounts on elevation	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.15.2

## EMET

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
EMET 5.51	None	Install EMET 5.51 or higher.	Install EMET 5.51 or higher..	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.1
Default Action and Mitigation Settings	User configured.	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.2
Default Protections for Internet Explorer	Not configured	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.3
Default Protections for Popular Software	Not configured	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.4
Default Protections for Recommended Software	Not configured	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.5
System ASLR	Not configured	Enabled: Application Opt-In	Enabled: Application Opt-In	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.6
System DEP'	Not configured	Enabled: Application Opt-In	Enabled: Application Opt-In	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.7
System SEHOP'	Not configured	Enabled: Application Opt-In	Enabled: Application Opt-In	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.24.8

## Event Log Service

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Application: Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.1.1
Application: Specify the maximum log file size (KB)	20,480	Enabled: 32,768 or greater	Enabled: 32,768	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.1.2
Security: Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.2.1

Security: Specify the maximum log file size (KB)'	20,480	196,608 or greater'	196,608	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.2.2
Setup: Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.3.1
Setup: Specify the maximum log file size (KB)'	20,480	Enabled: 32,768 or greater	Enabled: 32,768	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.3.2
System: Control Event Log behavior when the log file reaches its maximum size	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.4.1
System: Specify the maximum log file size (KB)'	20,480	Enabled: 32,768 or greater	Enabled: 32,768	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.26.4.2

## Previous Versions

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Configure Windows SmartScreen	Disabled	Enabled: Require approval from an administrator before running downloaded unknown software	Enabled: Require approval from an administrator before running downloaded unknown software.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.30.2
Turn off Data Execution Prevention for Explorer	None	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.30.3
Turn off heap termination on corruption	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.30.4
Turn off shell protocol protected mode	None	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.30.5

## Location and Sensors

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
--------	-------------------------	----------------------------	----------------------------------	---------------

Turn off location	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.37.1
-------------------	----------	---------	----------	--

## OneDrive (formerly SkyDrive)

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Prevent the usage of OneDrive for file storage	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.47.1
Prevent the usage of OneDrive for file storage on Windows 8.1	Disabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.47.2

## RemoteFX USB Device Redirection

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Do not allow passwords to be saved	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.2.2

## Connections

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Restrict Remote Desktop Services users to a single Remote Desktop Services session	Enabled	Enabled	Enabled.	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.2.1

## Device and Resource Redirection

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Do not allow COM port redirection	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.3.1
Do not allow drive redirection	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.3.2

Do not allow LPT port redirection	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.3.3
Do not allow supported Plug and Play device redirection	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.3.4

## Security

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Always prompt for password upon connection	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.9.1
Require secure RPC communication	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.9.2
Set client connection encryption level	Disabled	Enabled: High Level.	Enabled: High Level	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.9.3

## Session Time Limits

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Set time limit for active but idle Remote Desktop Services sessions'	Disabled	Enabled: 15 minutes or less'	Enabled: 15 minutes	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.10.1
Set time limit for disconnected sessions	Disabled	Enabled: 1 minute'	Enabled: 1 minute'	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.52.3.10.2

## Temporary folders

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Do not delete temp folders upon exit	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 8.9.52.3.11.1
Do not use temporary folders per session'	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 8.9.52.3.11.2

## RSS Feeds

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Prevent download-ing of enclosures	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.53.1

OCR

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Allow indexing of en-crypted files	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.54.2
Set what infor-mation is shared in Search	Disabled	Enabled: Anony-mous in-fo'	Enabled: Anony-mous info'	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.54.3

Software Protection Platform

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Turn off KMS Client Online AVS Valida-tion	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.59.1

Store

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Turn off Automatic Download and Install of updates	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.61.1
Turn off the offer to update to the latest version of Windows	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.61.2
Turn off the Store application	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Bench-mark v2.2.1 Paragraph 18.9.61.3

MAPS

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
--------	-------------------------	----------------------------	----------------------------------	---------------



Join Microsoft MAPS	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.69.3.1
---------------------	----------	----------	----------	--

## Consent

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Configure Default consent	Always ask before sending data.	Enabled: Always ask before sending data	Enabled: Always ask before sending data	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.70.2.1
Automatically send memory dumps for OS-generated error reports	Enabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.70.2.1

## Windows Installer

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Allow user control over installs	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.74.1
Always install with elevated privileges	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.74.1

## Windows Logon Options

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Sign-in last interactive user automatically after a system-initiated restart	Enabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.75.1

## Windows PowerShell

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Turn on PowerShell Script Block Logging	Enabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.84.1

Turn on PowerShell Transcription	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.84.2
----------------------------------	----------	----------	----------	--

## WinRM Client

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Allow Basic authentication	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.1.1
Allow unencrypted traffic	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.1.2
Disallow Digest authentication	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.1.3

## WinRM Service

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Allow Basic authentication	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.2.1
Allow remote server management through WinRM	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.2.2
Allow unencrypted traffic	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.2.3
Disallow WinRM from storing RunAs credentials	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.86.2.4

## Windows Remote Shell

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Allow Remote Shell Access	Enabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.87.1

## Defer Windows Updates

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Configure Automatic Updates'	Enabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.90.2
Configure Automatic Updates: Scheduled install day	Not Defined	0 - Every day'	0 - Every day'	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.90.3
No auto-restart with logged on users for scheduled automatic updates installations	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 18.9.90.4

## Personalization

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Enable screen saver	User Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.1.3.1
Force specific screen saver: Screen saver executable name	Disabled	Enabled: scrn-save.scr'	Enabled: scrn-save.scr'	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.1.3.2
Password protect the screen saver'	User Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.1.3.3
Screen saver timeout	User Defined	Enabled: 900 seconds or fewer, but not 0'	Enabled: 900 seconds	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.1.3.4

## Notifications

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
Turn off toast notifications on the lock screen	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.5.1.1

## Internet Communication settings

Asetus	Oletusarvo palvelimella	Koven-tamis su-osi-tusarvo	CIS Bench-marks for Windows arvo	Peruste/Lähde
--------	-------------------------	----------------------------	----------------------------------	---------------

Turn off Help Experience Improvement Program	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.6.5.1.1
--	----------	---------	---------	---

## Attachment Manager

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Do not preserve zone information in file attachments'	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.7.4.1
Notify antivirus programs when opening attachments	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.7.4.2

## Network Sharing

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Prevent users from sharing files within their profile.	Disabled	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.7.26.1

## Windows Installer

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Always install with elevated privileges	Disabled	Disabled	Disabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.7.39.1

## Playback

Asetus	Oletusarvo palvelimella	Koventamis suositusarvo	CIS Benchmarks for Windows arvo	Peruste/Lähde
Prevent Codec Download	User Defined	Enabled	Enabled	Lähde: CIS MS Windows Server 2012 R2 Benchmark v2.2.1 Paragraph 19.7.43.2.1