

Tietoturvan ylläpito

Saatesanat	1
Virtuaalipalvelimet	1
Symantec Endpoint Protection Manager sovelluksen asennus	2
Symantec Endpoint Protection sovelluksen asennus	8
Nessus Essentials asennus	14
Nessus Essentials auditointi	20
Tietoturva demo: / AD User -> Domain Admin	22

Saatesanat

Tulen kuvaamaan ja kertomaan tietoturva sovelluksen asennuksen ja sen jakamisen työasemille, tietoturva auditointi käyttäen valmista sovellusta sekä merkityksen miksi on tärkeää että on eritelty käyttäjätunnuksen roolin mukaan ja miksi ei tule käyttää liian järeitä tunnuksia laitteiden ylläpitoon.

Tämä merkityksen tulen näyttämän tämän dokumentin Tietoturva demo osiossa, jossa ”ylennän” itseäni normaalisti Active Directory käyttäjästä Domain Administrator tason käyttäjäksi.

Tulen myös kertomaan miten tämä voidaan estää, varsin helpoilla toimenpiteillä toimialueen sekä tietoturvan parannuksilla työasema tasolla.

Virtuaalipalvelimet

Palvelin ympäristö on asennettu Oracle Virtualbox sovelluksen päälle joka on asennettu Windows 10 1909 koneelle.

Fyysisessä koneessa on muistia 24GB ja suorittimena on Intelin i6700k -suoritin, jossa on neljä ydintä. Kiintolevynä Virtualbox palvelimille toimii Kingston merkinen SSD-levy, jolla kokoa n. 960GB. Itse virtuaalipalvelimet vievät levytilaa n. 181GB

Verkkoalueena toimii 10.0.10.0/24 ja Gateway roolissa toimii Untangle -palomuri virtuaalipalvelin IP-osoitteella 10.0.10.1

Palvelimet jotka ovat asennettu tähän jarno.local -nimiseen Active Directory toimialueeseen sekä niiden roolit lyhyesti kuvattuna seuraavaksi.

INF-DC01 / 10.0.10.2 / Windows Server 2019 Core

-Domain Controller (FSMO roolien omistaja), DNS-palvelin, DHCP-palvelin, tiedosto palvelin, tulostus - palvelin.

INF-DC02 / 10.0.10.10 / Windows Server 2016 Core

-Domain Controller sekä DNS-palvelin

INF-SEPM01 / 10.0.10.3 / Windows Server 2019 GUI
- Symantec Endpoint Protection Manager-palvelin

INF-SEC01 / 10.0.10.4 / Windows Server 2019 GUI
- Nessus Essentials-palvelin.

Olen myös asentanut oheiset työasema käyttöjärjestelmäiset virtuaalikoneet, jotka saavat ip -osoitteensa INF-DC01 palvelimet DHCP palvelua käyttäen. Nämä työasemat ovat osana jarno.local toimialuetta.

Windows 10 v1909 Desktop (x64)
Windows 10 v1909 Laptop (x64)
Windows 7 Professional (x64)
Windows XP Professional (x86)

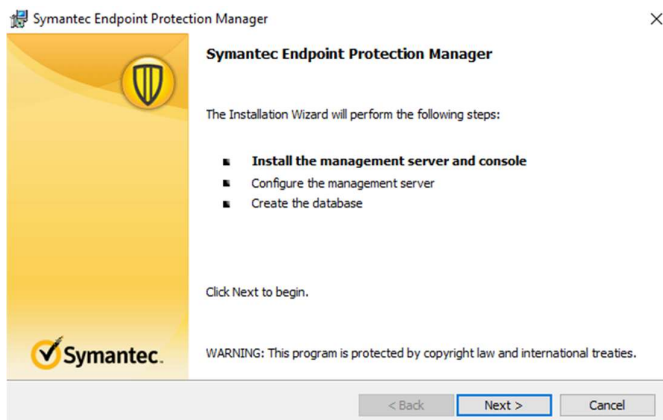
Symantec Endpoint Protection Manager sovelluksen asennus

Seuraavaksi tulen kuvaamaan kuinka tapahtuu Symantec Endpoint Protection Manager (jäljempänä SEPM) palvelimen asennus Windows Server 2019 ympäristöön.

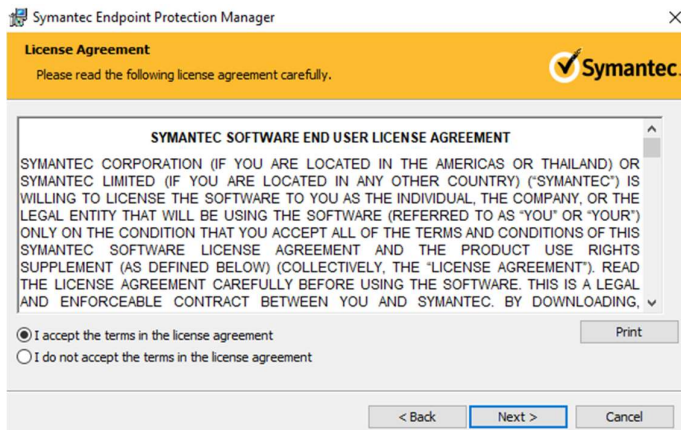
SEPM palvelin tarkoitus on toimia keskitettynä tietoturva sovelluksen hallinta ja ylläpito -palvelimena jarno.local toimialueella.

Tällä palvelimella voidaan jakaa tietoturva sovelluksia erilaisilla komponenteilla työasemille ja palvelimille sekä muuttaa sääntöjä keskitetysti, miten tietoturva -sovellus toimii työasemilla ja palvelimilla.

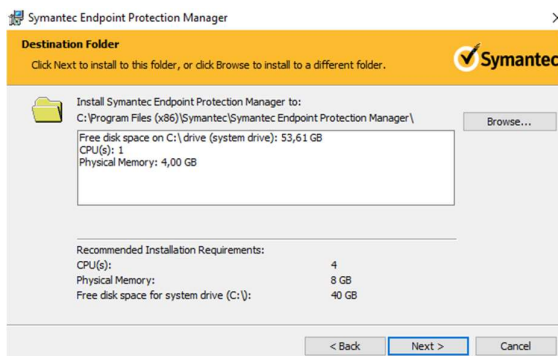
Olen ladannut trial -version jonka tulen asentamaan.



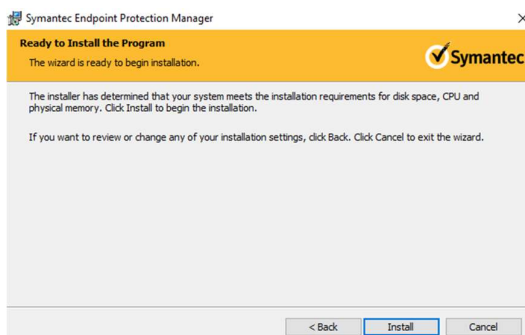
Asennuksen käynnistyksessä tulee ensimmäiseksi ikkuna joka kertoo mitä tulemme asentamaan ja missäkin järjestyksessä. **Next.**



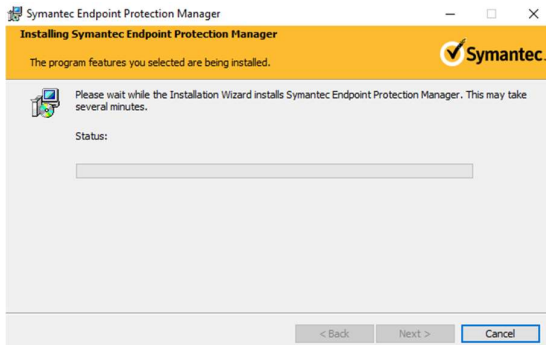
Seuraavaksi luemme tarkasti lisenssi ehdot. **Next.**



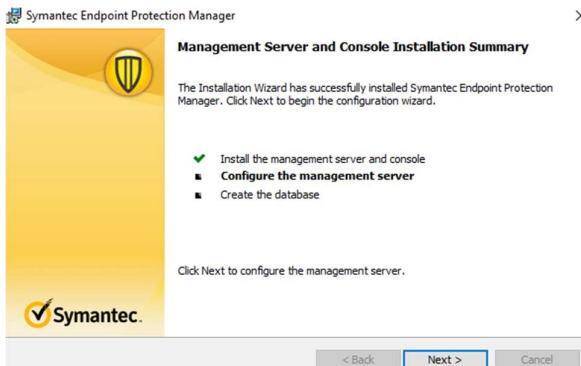
Tämän jälkeen ohjelma ehdottaa asennus kansiota sekä tarkistaa että palvelimella on tarpeeksi resursseja, jotta asennus voidaan suorittaa. Tässä tapauksessa minulla on vain 4GB muistia, vaikka Symantec suosittaa, että olisi 8GB muistia, mutta voimme jatkaa tästä huolimatta asennusta. **Next.**



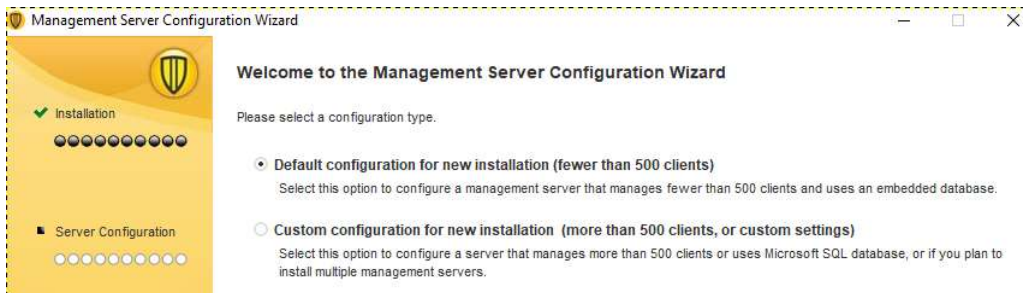
Seuraavaksi ryhdymme itse asennukseen, kun asennus on varmistanut, että kaikki tarpeellinen resurssi on saatavilla. **Install.**



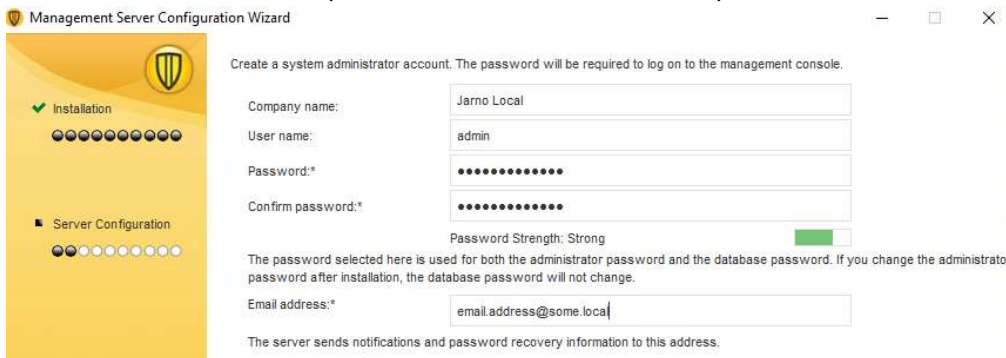
Oheinen asennus dialogi ilmestyy seuraavaksi ja odotamme että se valmistuu.



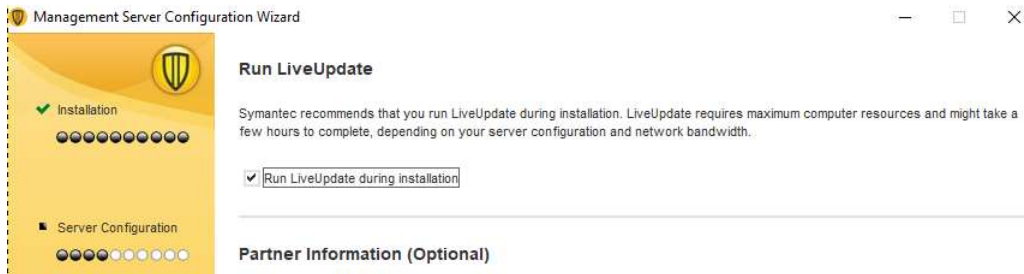
Nyt kun olemme saaneet asennettua palvelimen ja konsolin, niin jatkamme tietokannan asennukseen. **Next.**



Seuraavaksi valitsemme oletuksen, eli meillä on alle 500 työasemaa jota haluamme hallinnoida. Voimme myös määrittää, että luomme oman SQL-tietokannan mutta tässä tapauksessa Symantecin oma sisäänrakennettu tietokanta palvelin riittää meidän asennus tarpeisiin. **Next**



Tämän jälkeen määritämme yrityksen tiedot, sekä pääkäyttäjän tunnuksen sekä salasanan. Myös tässä kohtaa pitää määrittää sähköpostiosoite mihin voidaan lähettää viestejä järjestelmästä. Huomio, että tässä tapauksessa olen antanut tähän keksityn sähköpostiosoitteen. **Next.**



Tässä määritämme seuraavaksi, että Symantec hakee tuoreimmat sovelluspäivityksen sekä virustietokantakuvakset asennuksen aikana. **Next.**

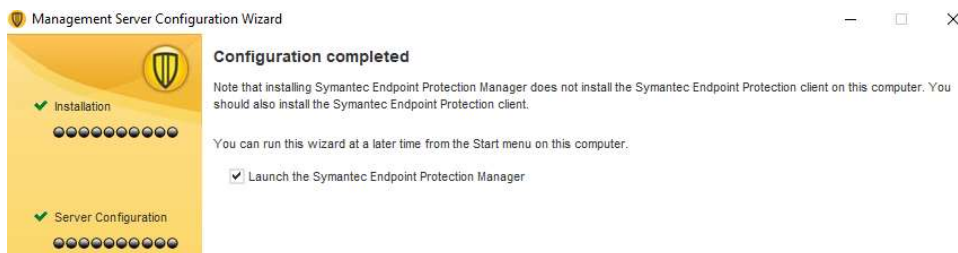


Nyt voimme sallia, että meidän palvelin lähettää pseudonymisuus tietoa Symantecin palvelimelle. Tämä mahdollisesti voi parantaa myös tietoturvaä yleisellä tasolla. **Next.**

The database is being created and initialized. Depending on your environment and bandwidth, it can take some time to complete. Please be patient while the process completes. Initializing Database...



Seuraavaksi tapahtuu itse tietokannan luonti. Tässä voi kestää tovikin, joten tässä välissä voi käydä ottamassa esimerkiksi kupin kahvia tai teetä.



Ja lopuksi kun tietokanta on muodostettu onnistuneesti, voimme asennuksen lopuksi käynnistää Symantec Endpoint Protection Manager sovelluksen. **Finish.**



**Symantec
Endpoint Protection Manager**

User name:

Password:

Server: 

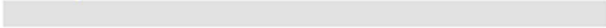
[Forgot your password?](#)

Kun valitsemme että asennuksen jälkeen käynnistetään SEPM sovellus automaattisesti, niin seuraavaksi meitä pitäisi hetken päästä kohdata tällainen ikkuna.

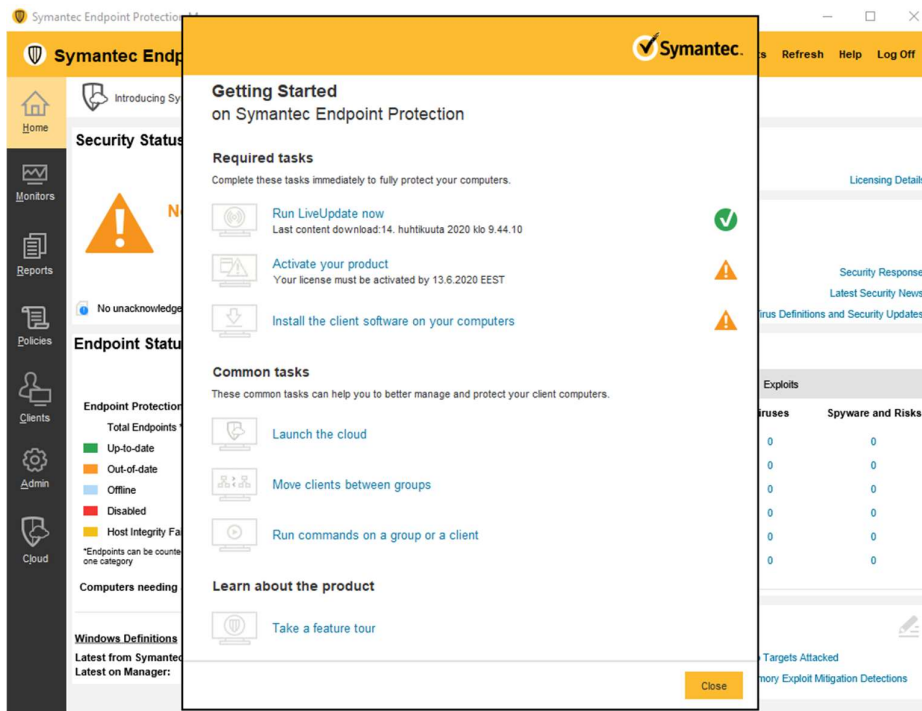
Tähän annamme asennuksen aikana luodut pääkäyttäjän tunnukset. **Log On**

Logging on to the management server

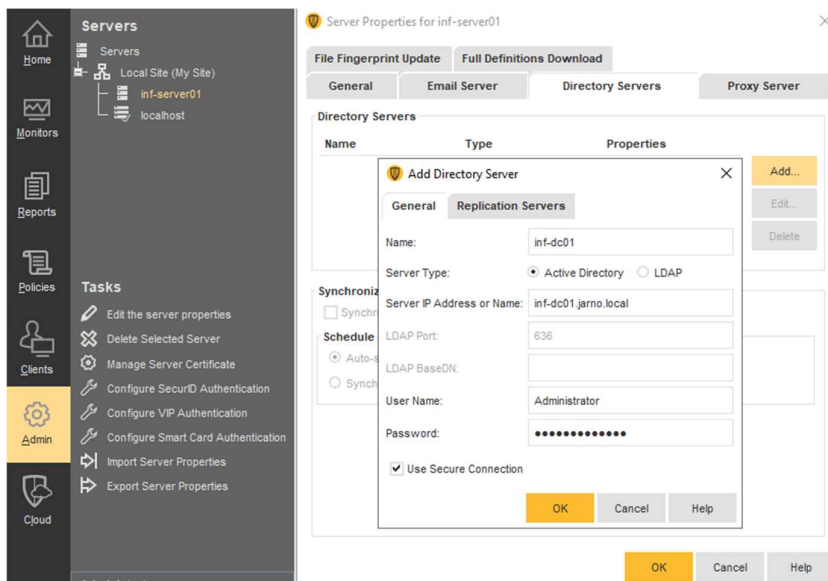
This may take several seconds...



Tämän jälkeen odotamme hetken, kun kirjaudumme sisälle järjestelmään.

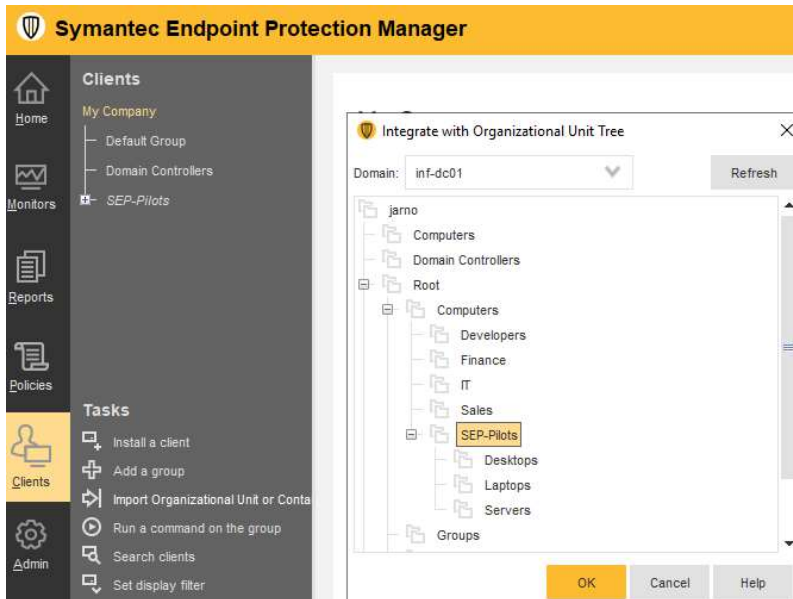


Meille avautuu nyt päänäköymä, jolla voimme hallinnoida SEPM palvelua ja siihen liitettyä työasemia. **Close**
Vasemmalla sivupalkissa on navigointi painikkeet, joilla saamme valittua eri hallinta näkymiä.



Meidän pitää tuoda olemassa oleva Active Directory tieto SEPM sovellukseen, jotta voimme hallinnoida koneita Active Directory Organisaatio Yksikkö tasolla. Pääsemme tähän määrittelyyn vasemmalta Admin -> Servers -> Local Site -> inf-server01 -> Edit server properties -> Directory Servers -> Add

Jossa annamme sitten tiedot toimialueesta, kuten palvelin sekä tunnuksen jolla luomme Active Directorystä tietoa. Tähän voinee käyttää muutakin tunnusta kuin Administrator, riittänee tunnus joka voi lukea vain tietoa, tyyliliin Domain Users tason tunnus. **OK**



Tämän jälkeen voimme vasemmalta Import Organizational Unit or Container kautta valita domain ->inf-dc01 ja valita jarno -> Root -> Computer -> SEP-Pilots Organisaatio Yksikön jonka jäseniä voimme hallinnoida sekä asentaa SEP tietoturva sovelluksen. **OK.**



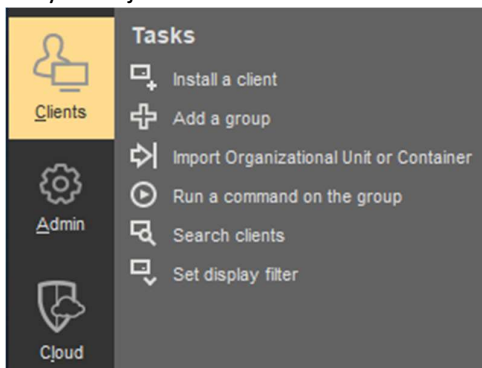
Ja nyt meillä näkyy tämän valitun Organisaatio Yksikkö puu vasemmalle Clients näkymässä.

Tässä vaiheessa olemme siis saaneet asennettua SEPM sovelluksen.

Seuraavassa osiossa luomme asennus paketin ja asennamme sen etänä työasemille SEPM hallinnan kautta.

Symantec Endpoint Protection sovelluksen asennus

Avaamme siis SEPM hallinta paneelin, ellei sitä ole jo valmiiksi avattu ja menemme vasemmalta Clients näkymään ja valitsemme **Install a Client.**



Client Deployment Wizard

Select Deployment Type

Welcome to the Client Deployment Wizard

Use this wizard to install the protection client on computers in your network or update existing client communication settings.

[Click to view the Install Client tour](#)

Note: For instructions to install the client on a computer that runs Symantec Mail Security or Symantec Scan Engine, see the Symantec Technical Support knowledge base article:

[Click here](#)

☒ New Package Deployment

Select packages from the server and specify client group and features.

Tämän jälkeen meille avautuu määrittämisvelho, jossa ensimmäiseksi valitsemme New Package Deployment (oletus) **Next**.

Client Deployment Wizard

Select Group and Install Feature Sets

Install Packages: Windows - Symantec Endpoint Protection version 14.2.5569.2100 - English

This selection includes:
 WIN64BIT: Windows - Symantec Endpoint Protection version 14.2.5569.2100 - English (14.4.2020)
 WIN32BIT: Windows - Symantec Endpoint Protection version 14.2.5569.2100 - English (14.4.2020)

Group: My Company\SEP-Pilots [Browse...](#)

Install Feature Sets: Protection for Active Directory

Installs Symantec Endpoint Threat Defense for Active Directory. Network, web, and behavior protection technologies are not installed.
 Some security features are not supported on some platforms. Please refer to product documentation for details.

Install Settings: Default Standard client installation settings for Windows [Options...](#)

Content Options: ☐ Include virus definitions in the client installation package.

Uncheck this option to create a smaller client installation package that does not include virus definitions but does include all other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions.

Seuraavaksi voimme määrittää ominaisuuksia, mutta tässä tapauksessa menemme valinnalla Protection for Active Directory sekä Default Standard client installation settings for Windows. **Next**.

Client Deployment Wizard

Install Symantec Endpoint Protection to Remote Computers

Choose your preferred installation method.

☐ Save Package

Creates an executable installation package, but does not distribute protection software to remote computers.

☒ Remote Push

Creates a client installation package and pushes the package onto client computers. The package installs automatically on the computers.

[Preparing for Remote Push Installation](#)

☐ Web Link and Email

Creates a client installation package and an email template so you can send an email notification with download instructions to users.

 The web link installs the latest installation package that you specified. If you re-run the wizard and select a different installation package, the web link directs to the latest selection only. You cannot assign more than one installation package to the same group.

Nyt vielä määritämme tavan jolla asennamme paketin työasemalla, tässä tapauksessa valitsemme etäasennusta varten Remote Push. **Next**.

Computer Selection
Select the computers to receive the client installation package or the communication settings.

Browse or search the network for computers on which you want to install the protection client.

Available Computers:
Configure Network Timeout ...

Browse Network Search Network

Microsoft Windows Network
JARNO
INF-DC02
INF-SEC01
INF-SEPM01

>> <<

Install Protection Client on:

Computer	Type	Current Protection
INF-DC02		

Login Credentials

The default Administrator account on the client computer INF-DC02 (10.0.10.10) must be used to install Symantec Endpoint Protection.

Login Credentials

User name: Administrator

Password:

Domain or Workgroup: jarno.local

OK Cancel

Valitsemme INF-DC02 lisäämme sen asennettavien koneiden joukkoon klikkaamalla kahta hakasulje nappia oikealla. Tämän jälkeen saamme vielä ikkunan jossa kysytään tunnuksia jolla voidaan asennus tehdä tälle palvelimelle. **OK**.

Install Protection Client on:

Computer	Type	Current Protection
inf-dc02 (10.0.10.10)	64-Bit	Unprotected

Tämän jälkeen palvelin ilmestyy oikealle ikkunassa ja myös kertoo tiedot palvelimelta (perus) sekä on siellä jo asennettu olemassa olevaa tietoturvasovellusta. **Next**.

Client Deployment Wizard

Install Symantec Endpoint Protection Client
Install the client software or communication updates on the computers listed below.

You are about to send client software to the following computers:

Computer	Description	Type	Current Protection
inf-dc02 (10.0.10.10)	Windows Server 2016 Standard Evaluation...	64-Bit	Unprotected

Lopuksi saamme vielä vahvistus ikkunan jossa näkyy koneet johon olemme asentamassa SEP-sovellusta. **Send**.

Deploying Client Remotely
Protection software is being sent to your computers now.

Deployment time varies depending on the network speed and the number of computers that you have selected to receive the software.

Total progress: 0% finished. 0 out of 1 clients are deployed.

0%

Computer	Description	Type	Status
inf-dc02 (10.0.10.10)	Windows Server 2016 Stan...	64-Bit	0

Seuraavaksi tulee ikkuna jossa nähdään, että SEPM palvelin yrittää lähettää ja asentaa SEP sovellusta inf-dc02 palvelimelle.

 Client Deployment Wizard ✕

Deployment Summary 

Symantec Endpoint Protection Manager sent software to the selected computers.

Symantec Endpoint Protection Manager sent the installation files to the selected computers. Review whether the installation succeeded on the Clients tab. You can also check the Deployment Reports, at Reports > Computer Status.

Client protection deployment summary: 1 succeeded, 0 failed.

Computer	Description	Type	Deployment Status
 inf-dc02 (10.0.10.10)	Windows Server 2016 Stan...	64-Bit	Successful

Ja nyt asennuksen jälkeen näemme, että asennus on onnistunut. **Next.**

 Client Deployment Wizard ✕

Client Deployment Wizard Complete 

The installation files were sent to the computers that you selected.

Ja lopuksi tulee vielä vahvistus, että kaikki asennuksen onnistuneet. **Finish.**

Clients

My Company

- Default Group
- Domain Controllers**
- SEP-Pilots
 - Desktops
 - Laptops
 - Servers

Domain Controllers Policy serial number: 2799-04/15/2020 17:45:07 641

Clients Policies Details **Install Packages**

View: Default view All users and computers Filter

Name	Health State	Logon User or Computer	Last Time Status Changed	Virus Definition
 INF-DC01	Online	Administrator	17. huhtikuuta 2020 13:24	Not available
 inf-dc02	Online	None	17. huhtikuuta 2020 13:24	Not available

Voimme nyt vielä varmistaa, että asennus on onnistunut, kun tämä palvelin ilmestynyt SEPM hallinnassa Clients näkymään ja palvelin nimen kohdalla on vihreä pallo, joka tarkoittaa, että sillä on myös yhteys meidän SEPM palvelimelle ja voimme sitä hallinnoida.

Tässä tapauksessa inf-dc02 palvelin ilmestyi Default Group kansioon, kun se ei ollut SEP-Pilots Organisaation Yksikön alla, kun se oli Domain Controllers kansiossa Active Directoryssä. Joten jouduin hiiren oikealle ottamaan Move inf-dc02 ja siirtämään sen Domain Controllers (jonka olen myös käsin luonut SEPM hallintaan) kansioon, yhdessä jo toisen Domain Controller koneen kanssa inf-dc01.

Voimme myös luoda ns. manuaalisia asennus paketteja, mikäli emme voi tai halua asentaa Remote Push toimintoa käyttäen.

Tämä tapahtuu menemällä vasemmalla Admin -> Install Packages näkymään

Symantec Endpoint Protection Manager Latest Alerts Refresh Help Log Off

Install Packages

- Client Install Package
- Client Install Settings
- Client Install Feature Set

Tasks

- Export a Client Install Package...
- Delete Client Install Package
- Edit Client Install Package Properties...
- Upgrade Clients with Package
- Add a Client Install Package...
- Set User Information Collection...

Client Install Package

Package Name	Platform	Type	Version	Created Time
Symantec Endpoint Pr...	Windows 64bit	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Windows 32bit	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Mac	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Linux RPM	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Linux DPKG	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...

Package Symantec Endpoint Protection version 14.2.5569.2100 for WIN64BIT has been assigned to the following groups:

- My Company\SEP-Pilots\Laptops
- My Company\SEP-Pilots\Servers
- My Company\SEP-Pilots\Desktops

Josta sitten hiiren oikealla valitsemme esimerkiksi ylimmän paketin SEP x64 version ja otamme Export

Client Install Package

Package Name	Platform	Type	Version	Created Time
Symantec Endpoint Pr...	Windows 64bit	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Windows 32bit	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Mac	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Linux RPM	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...
Symantec Endpoint Pr...	Linux DPKG	Symantec Endpoint Pr...	14.2.5569.2100	14. huhtikuuta 2020 kl...

 Export Package: Symantec Endpoint Protection version 14.2.5569.2100 for WIN64BIT

Use exported packages to manually install a client, or to serve the package from a URL for auto-upgrade. Note: for auto-upgrade installation, do not create a single .EXE file.

Export folder: Browse...

☒ Create a single .EXE file for this package

Installation Features and Settings

Select the security features for this package:

Full Protection for Clients

Some security features are not supported on some platforms. Please refer to product documentation for details.

Select the installation settings for this package:

Default Standard client installation settings for Windows

☒ Include virus definitions in the client installation package.

Uncheck this option to create a smaller client installation package that does not include virus definitions but does include all other content. After the client is installed, run LiveUpdate immediately on the clients to download the virus definitions.

Policy Mode

Computer mode applies the policies to all users of the protected computer. User mode applies the policies based on which user is logged on to the protected computer.

☒ Computer mode ☐ User mode

Export Settings

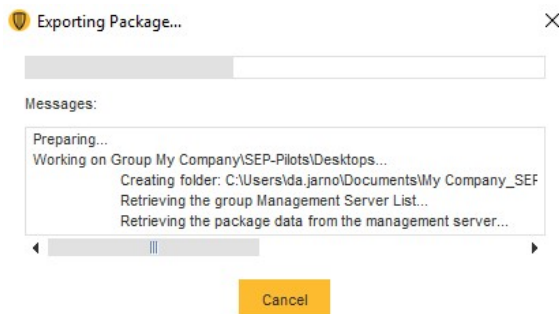
☒ Export a managed client

☐ Export an unmanaged client

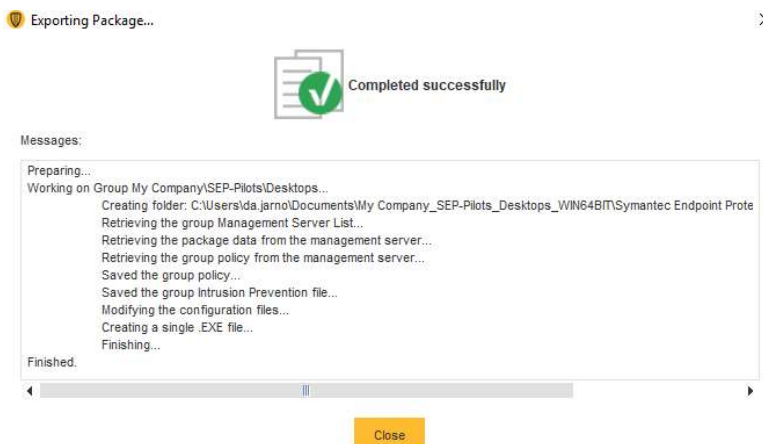
☒ Export packages with policies from the following groups:

- ☐ My Company
 - ☐ Default Group
 - ☐ Domain Controllers
- ☐ SEP-Pilots
 - ☒ Desktops
 - ☐ Laptops
 - ☐ Servers

Tässä ensin valitsemme kansion jonne paketin luodaan (Export Folder), sen jälkeen mikä ominaisuus ja asetus asetukset tulee paketilla (Full Protection for Clients), sitten valitsemme mihin kansioon nämä koneet ilmestyvät SEPM hallinnassa, tässä tapauksessa Desktop. Sekä asennus tapana valitsemme Default Standard client installation settings for Windows. Policy Mode: en pidämme oletuksena, eli Computer mode. **Ok.**



Tämän jälkeen SEPM alkaa luomaan asennuspakettia meidän valitsemilla asetuksilla.



Ja tämän jälkeen vielä tulee vahvistus, että kaikki on mennyt onnistuneesti läpi ja paketti on luotu. **Close.**

Ja voimme vielä lopuksi tarkistaa SEPM palvelimen kansiota C:\Users\da.jarno\Documents\My Company_SEP-Pilots_Desktops_WIN64BIT\Symantec Endpoint Protection version 14.2.5569.2100 – English, että sinne on generoitunut asennus paketti.

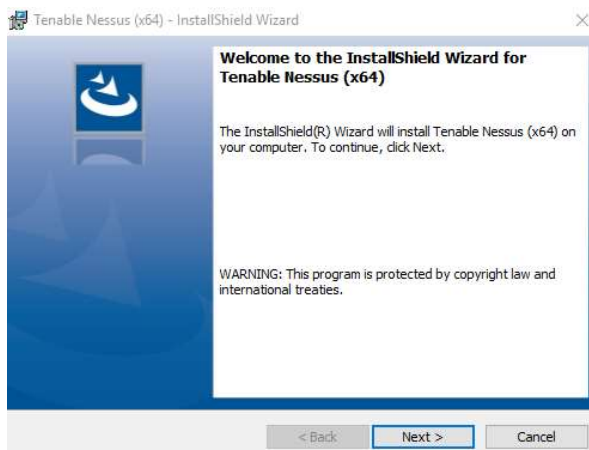


Näin olemme siis asentaneet etänä ja luoneen asennuspaketin SEP asennuksia varten. Seuraavaksi kerron miten voimme auditoida meidän toimialueen tietoturvaa käyttäen Nessus Essentials sovellusta.

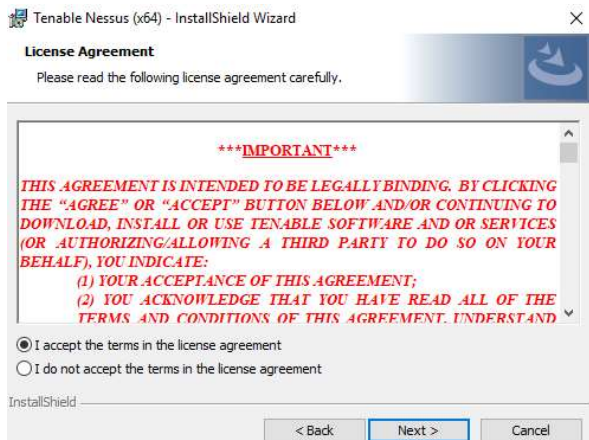
Nessus Essentials asennus

Tulen asentamaan Nessus Essentials tietoturvakartoitus sovelluksen INF-SEC01 Windows Server 2019 palvelimelle. Tällä sovelluksella voimme auditoida toimialueen koneita ja luoda näkemystä olemassa olevasta tietoturvasta ja mahdollista uhista siihen liittyen.

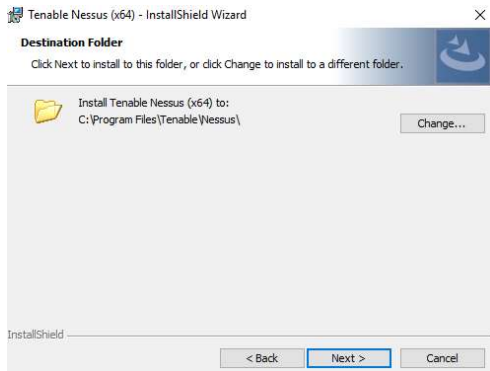
Asennus paketin saa vapaasti ladata <https://www.tenable.com/products/nessus/nessus-essentials> sivulta, ainoa mitä pitää tehdä on anoa ilmainen aktivointi tunnus asennusta varten.



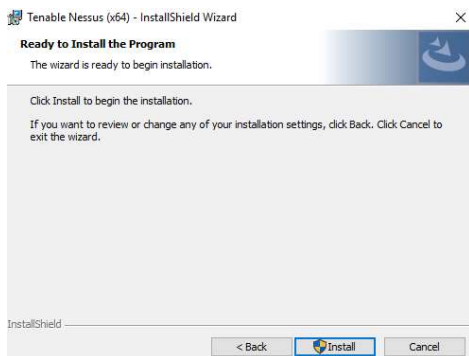
Käynnistämme asennus paketin, jolloin saamme oheisen dialogin. **Next.**



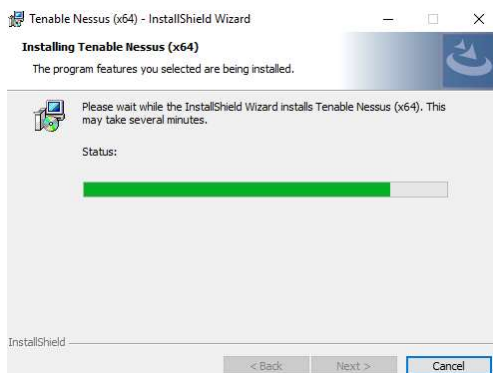
Luomme lisenssi ehdot tarkasti läpi. **Next.**



Valitsemme asennus kansion, menemme oletuksella. **Next.**



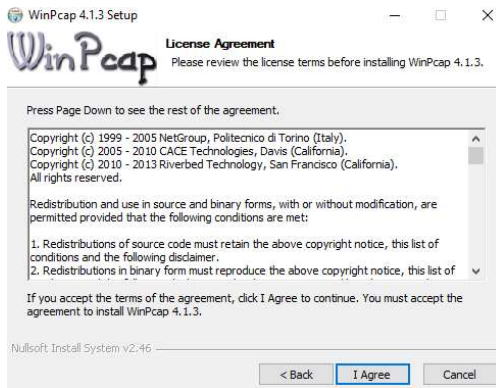
Tämän jälkeen olemme valmis asennukseen. **Install.**



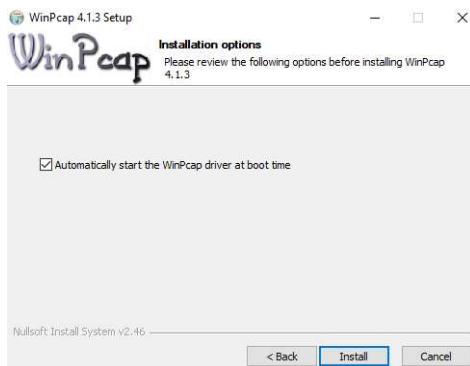
Nyt odotamme, että asennus valmistuu.



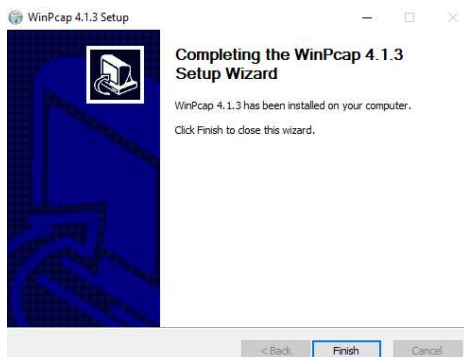
Asennuksen aikana joudumme asentamaan osana Nessusta WinPcap -sovelluksen. Tämä on osana verkon ja niiden pakettien analysointia varten. **Next.**



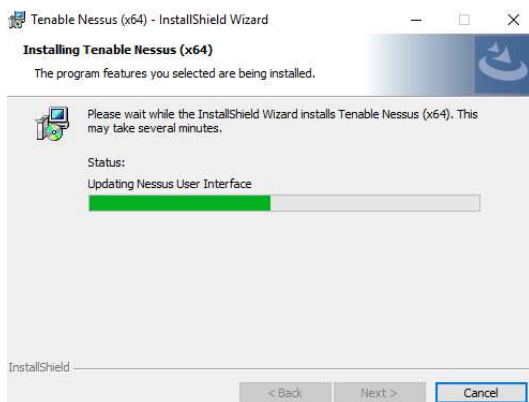
Luomme jälleen tarkasti lisenssiehdot. **I Agree**



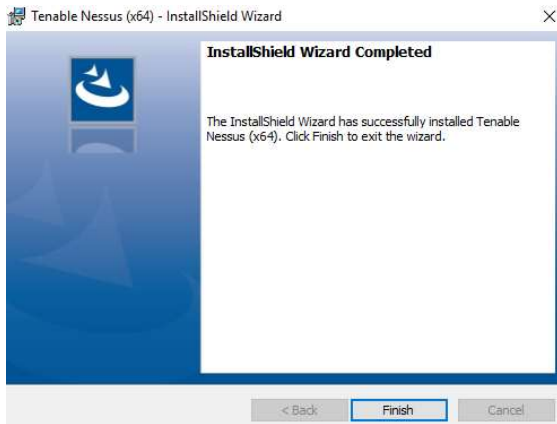
Ja vielä varmistamme, että winPcap käynnistyy palvelimen käynnistytksen aikana. **Install.**



Ja hetken päästä asennus on suoritettu. Nyt voimme jatkaa taas itse Nessus sovelluksen asennusta. **Finish.**



Nyt siis jatkuu taas itse Nessus sovelluksen asennus.

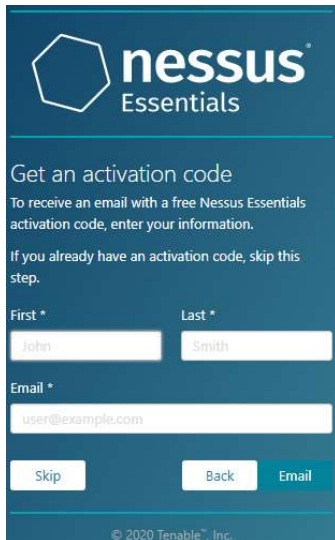


Ja lopuksi asennus on suoritettu onnistuneesti loppuun. **Finish.**

Tämän jälkeen käynnistyy automaattisesti oletus Internet -selain ja avaa osoitteen <http://localhost:8834/WelcomeToNessus-Install/welcome> jossa voimme jatkaa asennusta.



Seuraavaksi valitsemme tuotteen jonka haluamme asentaa. Tässä tapauksessa Nessus Essentials. **Continue**



Tässä annamme tiedot jolla luomme ilmaisen aktivointikoodin. Anna tähän sopivat tiedot. **Email**



nessus
Essentials

Register Nessus

Enter your activation code.

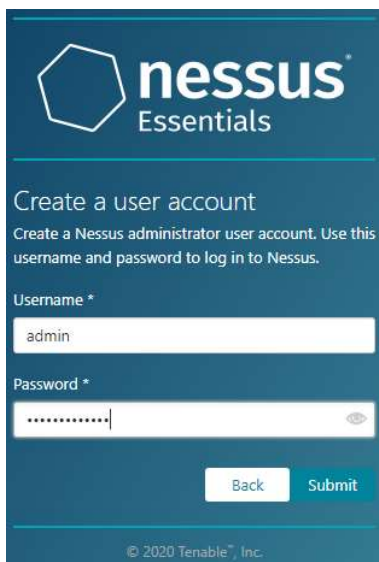
Activation Code *

☐ Register Offline

[Settings](#) [Back](#) [Continue](#)

© 2020 Tenable™, Inc.

Kun olemme antaneet tiedot niin syötämme tähän Activation Code kenttään koodin, jonka olemme saaneet sähköpostilla mitä käytimme edellisessä ikkunassa. **Continue.**



nessus
Essentials

Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

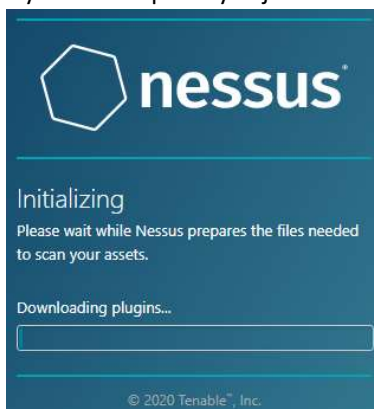
Username *

Password *

[Back](#) [Submit](#)

© 2020 Tenable™, Inc.

Nyt luomme pääkäyttäjän tunnuksen ja salasanan Nessus Essentials hallintaa varten. **Submit.**



nessus

Initializing

Please wait while Nessus prepares the files needed to scan your assets.

Downloading plugins...

© 2020 Tenable™, Inc.

Tämän jälkeen asennus käy vielä lataamassa tietoja Nessuksen palvelimelta, kun pluginsit. Tässä menee hetki ja voit taas käydä tässä välissä hakemassa lisää kahvia tai teetä. Myös lounaskin on mahdollista.



Kun tarvittavat komponentit on saatu ladattua, niin tehdään vielä pluginien rakentaminen. Tässäkin menee se toinen tovinen.

Kun tämä on mennyt läpi, olemme onnistuneesti asentaneet Nessus Essentials sovelluksen.

Seuraavaksi aloitamme auditoinnin asennuksen jälkeen.

Nessus Essentials auditointi

Welcome to Nessus Essentials

To get started, launch a host discovery scan to identify what hosts on your network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets

10.0.10.0/24

Close

Submit

Kun nämä komponentit on ladattu ja rakennettu, avautuu tervetuloa ikkuna eteemme. Tähän voimme antaa skannattavien koneiden ip -osoitteet tai vaihtoehtoisesti koko aliverkon mitä halutaan skannata. Tässä tapauksessa annan oman jarno.local toimialueen aliverkon 10.0.10.0/24 **Submit**.

My Host Discovery Scan Results

Nessus found the following hosts listed below from your list of targets (10.0.10.0/24).

To launch your first basic network scan, select the hosts you want to scan. These hosts count towards the 16 host limit on your license.

☐	IP	DNS
☐	10.0.10.3	inf-sepm01.jarno.local
☐	10.0.10.4	INF-SEC01.jarno.local
☐	10.0.10.10	inf-dc02.jarno.local
☐	10.0.10.1	firewall.jarno.local
☐	10.0.10.2	INF-DC01.jarno.local
☐	10.0.10.50	win10desktop.jarno.local
☐	10.0.10.52	WIN10LAPTOP.jarno.local
☐	10.0.10.54	winxp-pro.jarno.local
☐	10.0.10.55	Win7Pro.jarno.local

Discovery Complete!

Back

Run Scan

Kun kartoitus on tehty, niin näimme koneet jota tullaan skannaamaan. **Run Scan**.

My Basic Network Scan

Configure

Back to My Scans

Hosts 9

Vulnerabilities 9

History 1

Filter

Search Hosts

9 Hosts

Host	Vulnerabilities	%
10.0.10.10	32	4%
10.0.10.2	28	0%
10.0.10.3	27	4%
10.0.10.4	18	4%
10.0.10.55	16	0%
10.0.10.50	13	0%
10.0.10.52	13	0%
10.0.10.54	10	3%
10.0.10.1	3	0%

Scan Details

Policy: Basic Network Scan

Status: Running

Scanner: Local Scanner

Start: Today at 4:01 PM

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

Tämän jälkeen avautuu Network Scan ikkuna, jossa voi seurata skannauksen edistymistä. Tässä menee tovi, jos toinenkin, riippuen montako konetta käydään läpi.



Ja kun skannaus on ohitse, näemme meidän yleiskuvan meidän tietoturvatilanteesta.

My Basic Network Scan / Plugin #73182

← Back to Vulnerabilities

Configure Audit Trail

Hosts 9 Vulnerabilities 47 History 1

CRITICAL Microsoft Windows XP Unsupported Installation Detection

Description

The remote host is running Microsoft Windows XP. Support for this operating system by Microsoft ended April 8th, 2014.

Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities. Furthermore, Microsoft is unlikely to investigate or acknowledge reports of vulnerabilities.

Solution

Upgrade to a version of Windows that is currently supported.

See Also

<http://www.nessus.org/u?2f80aef2>
<http://www.nessus.org/u?321523eb>
<https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
<http://www.nessus.org/u?8dcab5e4>

Output

No output recorded.

Port	Hosts
N/A	10.0.10.54

Ja kun avaamme Vulnerabilites välilehden, niin voimme nähdä, että ainakin yksi Critical tason tietoturvaravitius tulee meidän toimialueen Windows XP koneesta.

Tietoturva demo: / AD User -> Domain Admin

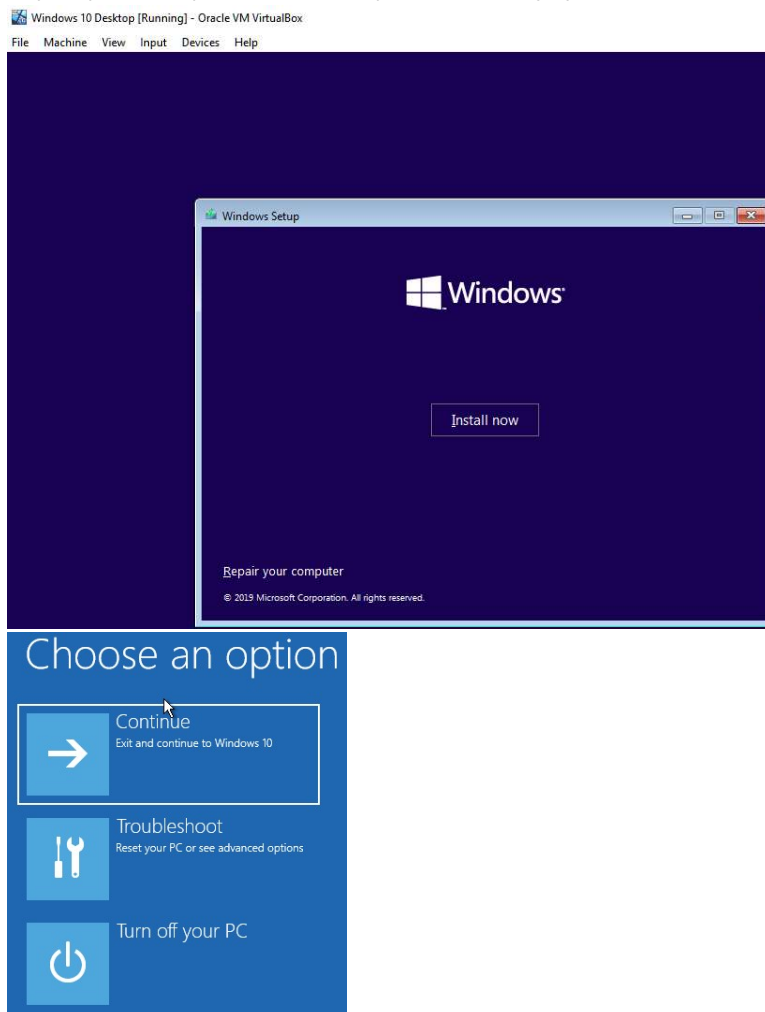
Eli lähtötilanne on se, että meillä Win10Desktop tietokone johon meillä ei ole paikallista Administrator tason tunnusta.

Käytämme kirjautumiseen jarno.nousiainen@jarno.local joka on normaali Domain Users ryhmän jäsen Active Directoryssä.

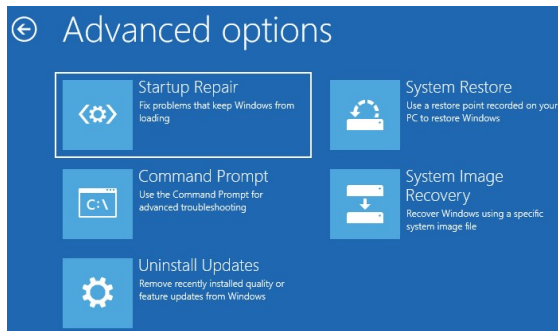
Eli haluamme aluksi saada tietokoneelle Win10Desktop Administrator tason tunnukset. Tähän voidaan käyttää joko työkalua jolla voimme nollata Win10Desktop Administrator käyttäjän salasanan, tai vaihtoehtoisesti korvata ns. Stickey Keys toiminnon Command Prompt sovelluksella.

Tämä siksi, kun tämä Stickey Keys voidaan jo käynnistää ennen kirjautumista koneelle ja tämä Stickey Keys suoritetaan System -tason tunnuksesta. Tällöin voimme esimerkiksi komennolla "net user Administrator password!!" resetoita Administrator käyttäjän salasanan ja voimme sitten kirjautua paikallisesti Administrator tunnuksesta.

Eli aloitamme käynnistämällä Win10Desktop Windows 10 käynnistys .ISO imagella ja menemällä sieltä Repair your computer toimintoa pitkin tiedostojärjestelmään kiinni.



Josta valitsemme Troubleshoot



Seuraavaksi valitsemme Command Prompt, jotta pääsemme tiedostojärjestelmään käsiksi.

```
Windows 10 Desktop [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Administrator: X:\windows\SYSTEM32\cmd.exe
X:\Sources>c:
C:\>dir
Volume in drive C is System Reserved
Volume Serial Number is B0E1-DD52

Directory of C:\

04/17/2020  06:17 PM                0 Recovery.txt
             1 File(s)                0 bytes
             0 Dir(s)  121,974,784 bytes free

C:\>d:
D:\>dir
Volume in drive D has no label.
Volume Serial Number is D0E2-6C49

Directory of D:\

03/18/2019  08:52 PM    <DIR>          PerfLogs
04/16/2020  02:22 AM    <DIR>          Program Files
04/14/2020  09:22 AM    <DIR>          Program Files (x86)
04/14/2020  09:56 AM    <DIR>          TEMP
04/14/2020  09:14 AM    <DIR>          Users
04/16/2020  09:20 AM    <DIR>          Windows
             0 File(s)                0 bytes
             6 Dir(s)  42,600,460,288 bytes free

D:\>
```

Ja kuten tästä huomaamme, levykirjaimen D:\ alta löytyy Windows asennuksemme

```
D:\>dir
Volume in drive D has no label.
Volume Serial Number is D0E2-6C49

Directory of D:\

03/18/2019  08:52 PM    <DIR>          PerfLogs
04/16/2020  02:22 AM    <DIR>          Program Files
04/14/2020  09:22 AM    <DIR>          Program Files (x86)
04/14/2020  09:56 AM    <DIR>          TEMP
04/14/2020  09:14 AM    <DIR>          Users
04/16/2020  09:20 AM    <DIR>          Windows
             0 File(s)                0 bytes
             6 Dir(s)  42,600,460,288 bytes free

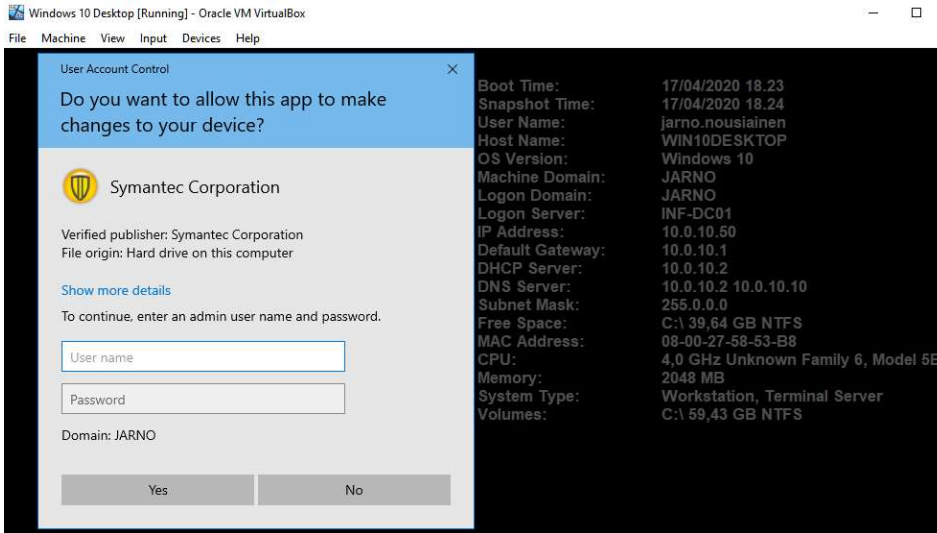
D:\>copy d:\Windows\System32\sethc.exe d:
1 file(s) copied.

D:\>copy /y d:\Windows\System32\cmd.exe d:\Windows\System32\sethc.exe
1 file(s) copied.

D:\>
```

Eli ensimmäiseksi kopioimme sethc.exe d:\ juuren talteen, jonka jälkeen kopioimme cmd.exe sethc.exe nimiseksi.

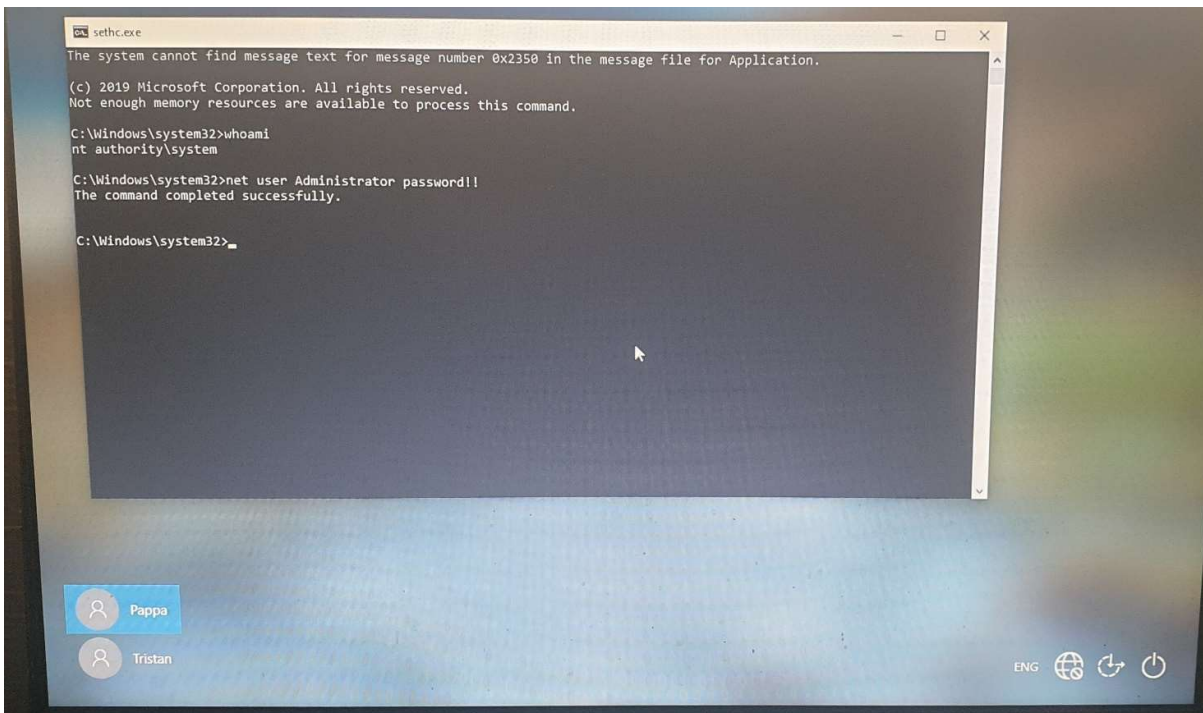
Tämän jälkeen voimme käynnistää tietokoneen uudelleen normaalisti takaisin Windows 10 tilaan.



Eli voin vielä havainnollistaa, tunnus joka minulla on käytössä Win10Desktop.jarno.local toimialue koneelle on jarno.nousiainen ei ole oikeutta suorittaa Järjestelmänvalvojan tason tehtäviä, kun käynnistää Symantec Endpoint Protection ylläpitotasolla.

Olen myös bginfo nimisellä sovelluksella luonut taustakuvan joka käynnistyksellä mikä kertoo koneen tiedot, eli tuo valkoinen teksti mustalla taustalla oikealla puolella.

Tässä kohtaa tuli vastaan Virtualbox sovelluksen rajallisuus syöttää Shift komentoa, joten joudun tätä jatkamaan aivan fyysisessä tietokoneessa



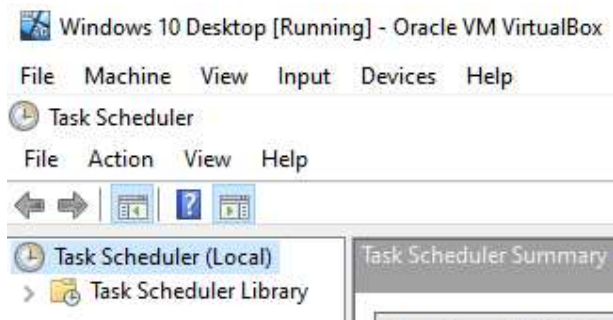
Ja nyt kun meillä on halussa Järjestelmänvalvojan tason tunnus Win10Desktop koneella, voimme seuraavaksi korottaa itsemme Domain Administrator ryhmän jäseneksi.

Tämä vaatii jo hieman suunnittelua ja sitä että jarno.local toimialueen ylläpitäjät käyttävät Administrator tunnusta myös tietokoneiden hallintaa, toki voi myös olla mahdollista, että heillä on omat Administrator tason tunnukset, kuten esimerkiksi da.jarno jarno.local toimialueella.

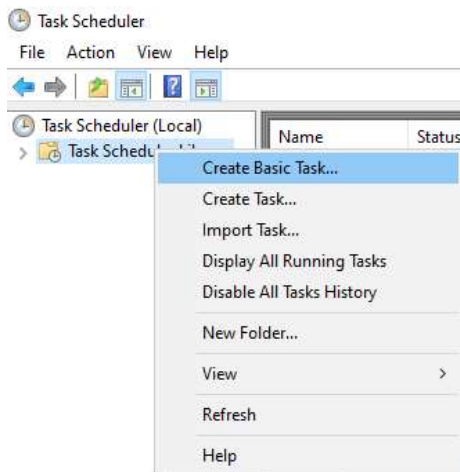
Ja jos vielä tämä ylläpitäjä käyttää työasemienkin ylläpitoon tätä da.jarno tunnusta niin silloin voimme suhteellisen helposti korottaa itsemme Domain Administrator ryhmän jäseneksi. Tämä tosiaan vaatii myös hieman sosiaalisen puolen hakkerointia 😊

Eli aluksi luomme Scheduled Taskin omalle Win10Desktop koneelle, joka suorittaa tietyn komennon, kun da.jarno kirjautuu esimerkiksi Remote Desktop yhteydellä antamaan etäapua keksityssä vikatilanteessa.

Aluksi avaamme Task Schedulerin polusta Windows Administrative Tools



Valitsemme hiiren oikealla Task Scheduler Library kohdalla ja otamme Create Basic Task



Annetaan nimi ja kuvaus oman maun mukaan. **Next.**

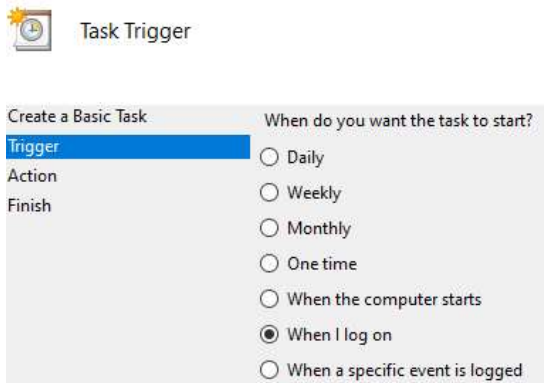
Create Basic Task Wizard



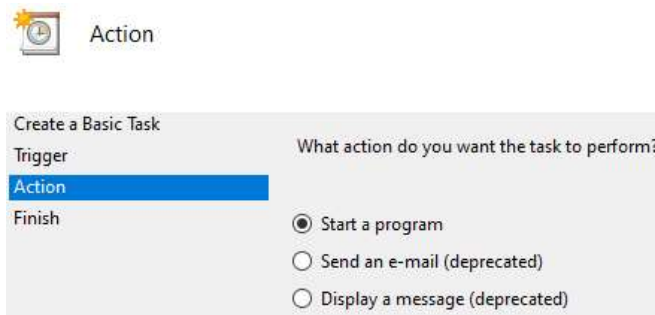
Create a Basic Task

Create a Basic Task	
Trigger	Use this wizard to quickly schedule a common task. For more advanced options or settings such as multiple task actions or triggers, use the Create Task command in the Actions pane.
Action	Name: Add Jarno to Domain Admins
Finish	Description: I own the Domain now

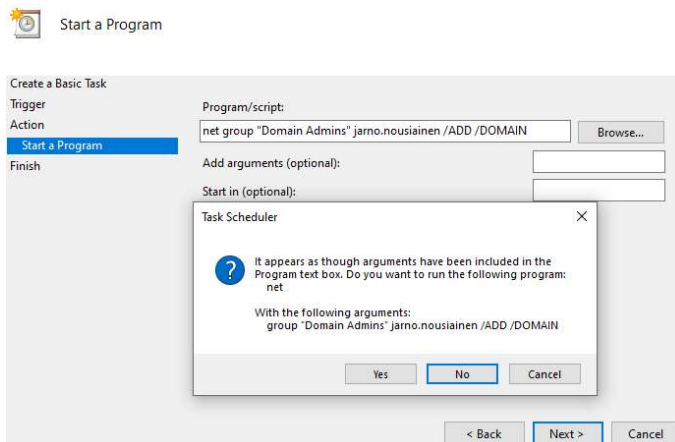
Valitaan When I log on, milloin tämä meidän taski tullaan ajamaan. **Next.**



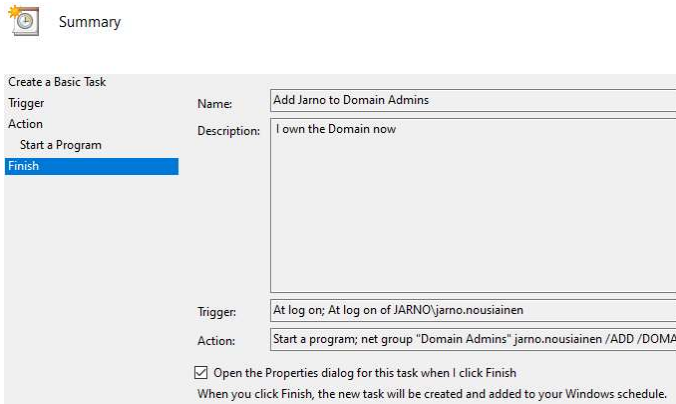
Toimintona valitaan, että suoritetaan sovellus tai komento. **Next.**



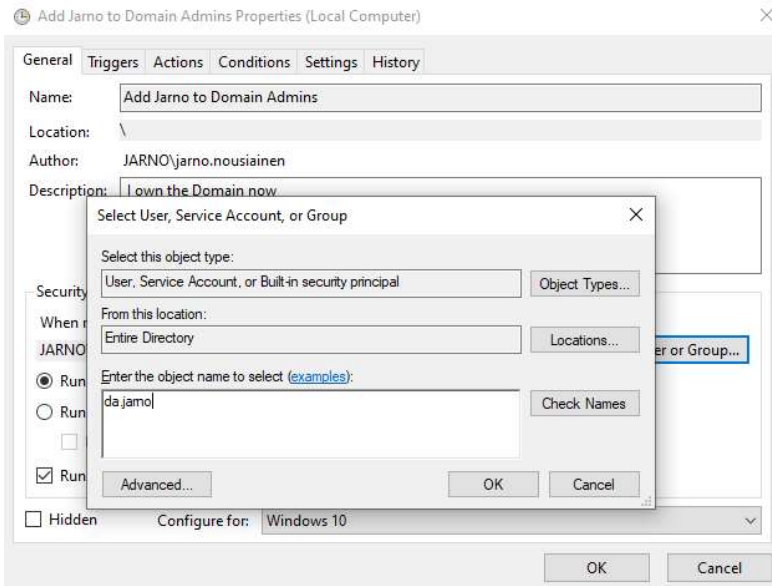
Komennoksi annetaan "net group "Domain Admins" jarno.nousiainen /ADD /DOMAIN" ilman siis hapsuja. Jonka jälkeen Task Scheduler ehdottaa hieman muutosta, valitaan **Yes** ja sen jälkeen **Next**



Lopuksi saamme vielä yhteenvedon tehtävästä ajastetusta tehtävästä. Tässä kohtaa ruksaamme ”Open the Properties dialog for this task when I click Finish”. **Finish.**

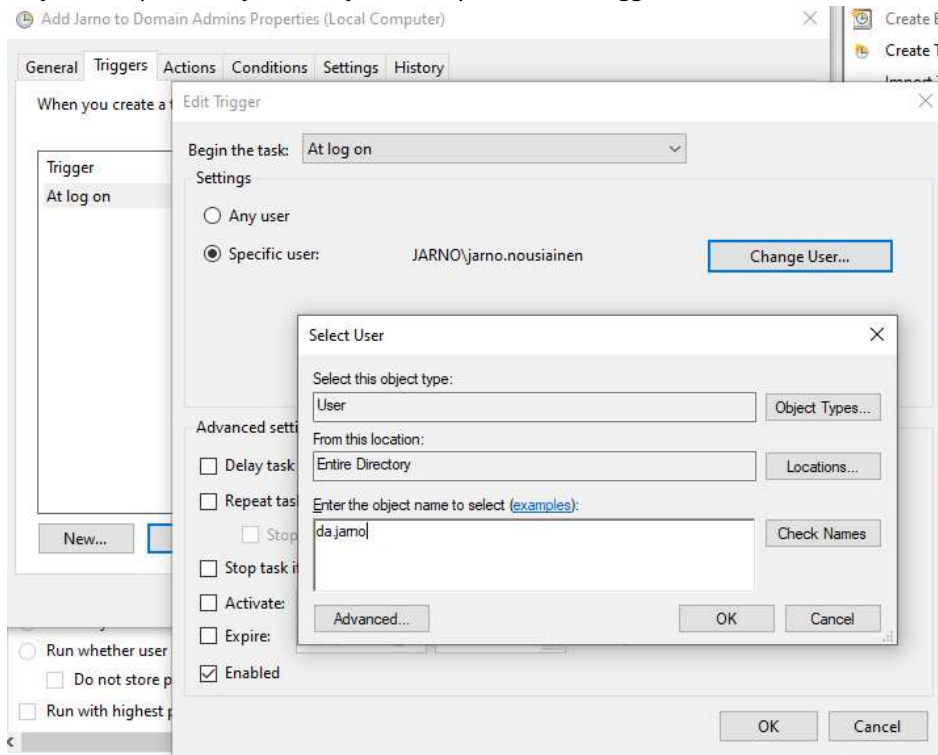


Lisäämme ruksin Run with highest privileges sekä valitsemme Configure for ”Windows 10”. Tämän jälkeen avaamme Change User and Group valitsemme Locations kohdasta Entire Directory ja kirjoitamme kenttään da.jarno ja valitsemme OK



Seuraavaksi menemme Triggers välilehdelle ja valitsemme Edit.

Täällä muutamme valitsemme taas Change User sekä Locations kohdaksi Entire Directory ja käyttäjäksi da.jarno. Lopuksi OK ja tämän jälkeen myös OK Edit Triggers välilehdeltä.



Tämän jälkeen meillä on valmiina komento joka suoritetaan, kun da.jarno kirjautuu koneelle, millä lisää meidän Active Directory Domain Admins ryhmään.

Seuraavaksi meidän pitää saada kirjautumaan da.jarno koneelle, esimerkiksi Remote Desktop yhteyden avulla. Voidaan vaikka pyytää apua jonkun sovelluksen kanssa tai mahdollisesti jokin vika muu keksitty vika tilanne.

Tein tästä videon jolta selviää parhaiten tämä, miten saadaan tämän jälkeen Domain Admins tason oikeudet haltuun.

Olen tämän videon ladannut OneDriveen kansioon

<https://iukky->

[my.sharepoint.com/:v:/g/personal/jarno_nousiainen_student_careeria_fi/EUD7RCYDwKdGm0u2qm1lQaUBZc8yOH566dLpzU0ZAO64ZQ?e=xXbGxF](https://iukky-my.sharepoint.com/:v:/g/personal/jarno_nousiainen_student_careeria_fi/EUD7RCYDwKdGm0u2qm1lQaUBZc8yOH566dLpzU0ZAO64ZQ?e=xXbGxF)

Eli nyt olemme päässeet normaalisti käyttäjästä muutamalla työvaiheella Domain Admins tason käyttäjäksi.

Se miten tätä voidaan estää on ensimmäiseksi estää millä medially oman koneensa käynnistys ja/tai määrittää Bitlocker levyn kryptaus pakolliseksi kaikille työasemille, jolloin emme voi tehdä mitään muutoksia systeemi levyille ilman että meillä on tiedossa Bitlocker avain.

Tämä myös edellyttää sitä, ettemme anna käyttäjille paikallisen pääkäyttäjän tason oikeuksia, jolloin he ovat jo ohittaneet tuon ensimmäisen vaiheen jolla elevoidaan itsemme koneen pääkäyttäjäksi.

Toinen mikä on ehdottoman tärkeää, että emme missään nimessä ylläpidä työasemia tai kirjaudu niille Domain Admins tason tunnuksella.

Eli mielellään luomme esim. erilliset käyttäjät joilla ylläpidämme työasemia joille on määritelty koneille ylläpito oikeudet, mutta ei toimialueen ylläpito oikeuksia.

Voimme esimerkiksi luoda käyttäjä wa.jarno jolla ylläpidämme vain työasemia (wa -> Workstation Admin)

Toiseksi voisimme luoda sa.jarno nimisen käyttäjän jolla ylläpidämme vain palvelimia (sa -> Server Admin)

ja lopuksi luoda erillisen da.jarno tunnuksen, jolla vain ja ainoastaan kirjaudumme ja ylläpidämme toimialue palvelimia, Domain Controller koneita (da-> Domain Admin)