



# Devops & Security : Structure & Security with Group Policies

**Ilias Latifine (r0847060)**

**Opleiding**  
Elektronica-ICT

# Inhoud

|          |                                                            |           |
|----------|------------------------------------------------------------|-----------|
| <b>1</b> | <b>Inleiding .....</b>                                     | <b>3</b>  |
| <b>2</b> | <b>OU/AGDLP structuur.....</b>                             | <b>4</b>  |
| 2.1      | Domein.....                                                | 4         |
| 2.2      | Organization Unit (OU) .....                               | 5         |
| 2.3      | Groups .....                                               | 6         |
| <b>3</b> | <b>Bedrijfseisen/Group Policys.....</b>                    | <b>7</b>  |
| 3.1      | Toepassen juiste bedrijfsbureaublad .....                  | 7         |
| 3.2      | Marketing afdeling moet NodeJS geïnstalleerd krijgen. .... | 8         |
| 3.3      | Rechten op de map Invoices.....                            | 9         |
| 3.4      | Overzicht .....                                            | 10        |
| <b>4</b> | <b>Resultaten .....</b>                                    | <b>11</b> |
| 4.1      | Eis 1.....                                                 | 11        |
| 4.2      | Eis 2.....                                                 | 13        |
| 4.3      | Eis 3.....                                                 | 14        |
| <b>5</b> | <b>Browser security.....</b>                               | <b>16</b> |
| 5.1      | Link naar demo video .....                                 | 16        |
| <b>6</b> | <b>Besluit .....</b>                                       | <b>17</b> |

## 1 Inleiding

Ik ben Ilias Latifine tweede jaar student aan de Thomas More hogeschool te Geel. Ik volg de opleiding Electronica-ICT. Voor het vak Devops & Security hebben we de mogelijkheid gekregen om een casestudy te maken uit een aantal verschillende cases die we vooraf gekregen hadden. Ik heb gekozen voor Case 2: Structure & Security with Group Policies.

De bedoeling van deze case was dat je OU, AGDLP en GPO opstelling uitwerkte die aan een aantal bedrijfs-/securityeisen moest voldoen.

In dit verslag zal u kunnen lezen hoe ik deze case opgelost heb.

Veel lees plezier.

*Ilias Latifine*

## 2 OU/AGDLP structuur

### 2.1 Domein

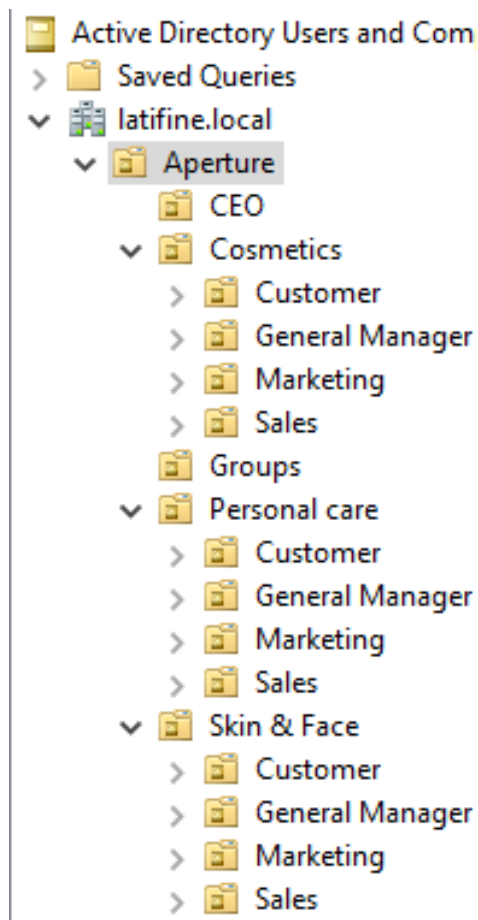
Ik heb gekozen om mijn domain **latifine.local** te noemen en binnen dit domein is de hele structuur uitgewerkt.

In de screenshot ziet u het resultaat van het powershell cmdlet Get-ADDomain. Hier kan u de naam van u domain bekijken.

```
PS C:\Users\Administrator> Get-ADDomain

AllowedDNSSuffixes      : {}
ChildDomains            : {}
ComputersContainer      : CN=Computers,DC=latifine,DC=local
DeletedObjectsContainer : CN=Deleted Objects,DC=latifine,DC=local
DistinguishedName       : DC=latifine,DC=local
DNSRoot                 : latifine.local
DomainControllersContainer : OU=Domain Controllers,DC=latifine,DC=local
DomainMode              : Windows2016Domain
DomainSID               : S-1-5-21-3267819097-1248804844-3022877967
ForeignSecurityPrincipalsContainer : CN=ForeignSecurityPrincipals,DC=latifine,DC=local
Forest                  : latifine.local
InfrastructureMaster     : WIN-P08LGSTLK51.latifine.local
LastLogonReplicationInterval : 
LinkedGroupPolicyObjects : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=latifine,DC=local}
LostAndFoundContainer    : CN=LostAndFound,DC=latifine,DC=local
ManagedBy               : 
Name                     : latifine
NetBIOSName              : LATIFINE
ObjectClass              : domainrole3
ObjectGUID               : 82a20eb6-b821-4c5a-aab1-8c539bc81065
ParentDomain             : 
PDCEmulator              : WIN-P08LGSTLK51.latifine.local
PublicKeyRequiredPasswordRolling : True
QuotasContainer          : CN=NTDS Quotas,DC=latifine,DC=local
ReadOnlyReplicaDirectoryServers : {}
ReplicaDirectoryServers  : {WIN-P08LGSTLK51.latifine.local}
RIDMaster                : WIN-P08LGSTLK51.latifine.local
SubordinateReferences    : {DC=ForestDnsZones,DC=latifine,DC=local, DC=DomainDnsZones,DC=latifine,DC=local, CN=Configuration,DC=latifine,DC=local}
SystemsContainer         : CN=System,DC=latifine,DC=local
UsersContainer           : CN=Users,DC=latifine,DC=local
```

## 2.2 Organization Unit (OU)



Ik heb gekozen om als eerste een OU aan te maken met de naam van het bedrijf om dan hier binnen de volledige bedrijfsstructuur toe te voegen.

Daarna heb ik gekozen om voor elke division binnen het bedrijf ook een OU aan te maken zodat ik policies kan toepassen die gelden binnen een bepaalde division. Heb de CEO ook als division genomen zodat we daar ook apart policies op kunnen toepassen.

Hierna heb ik binnen de divisions telkens nog 4 OU's gemaakt voor elke afdeling: General Manager, Sales, Customer & Marketing. Dit geeft me de mogelijkheid om voor elke afdeling andere policies toe te passen.

Tot slot heb ik aan elke OU de juiste user toegevoegd zodat de juiste persoon binnen de juiste division en afdeling zit.

We hebben ook nog een OU waar alle Global en Domain Local Groups inzitten.

## 2.3 Groups

| Name                                                                                                   | Type                          |
|--------------------------------------------------------------------------------------------------------|-------------------------------|
|  DL_Invoices_Modify   | Security Group - Domain Local |
|  DL_Invoices_Read     | Security Group - Domain Local |
|  DL_Software_Modify   | Security Group - Domain Local |
|  DL_Software_Read     | Security Group - Domain Local |
|  DL_Wallpapers_Modify | Security Group - Domain Local |
|  DL_Wallpapers_Read   | Security Group - Domain Local |
|  GG_CEO               | Security Group - Global       |
|  GG_Customer          | Security Group - Global       |
|  GG_General Manager   | Security Group - Global       |
|  GG_Marketing         | Security Group - Global       |
|  GG_Sales             | Security Group - Global       |

Om een goede AGDL structuur te gebruiken moeten we Global Groups en Domain Local Groups aanmaken.

Als eerste heb ik voor elke afdeling en de CEO een global group aangemaakt en hierin de juist personen toegevoegd.

Daarna heb ik voor alle gedeelde mappen 2 Domain local groups gemaakt. Eén voor Read rechten en één voor Modify rechten.

Aan de hand van de gevraagde eisen kan je dan bepaalde Global Groups member maken van deze domain local groups en dan kan je deze gebruiken om NFTS rechten mee aan te passen.

## 3 Bedrijfseisen/Group Policys

### 3.1 Toepassen juiste bedrijfsbureaublad

Het eerste eis was dat iedereen van de Cosmetics divisie een rode achtergrond kregen en al de rest een blauwe.

Dit heb ik gerealiseerd door 2 group policy objects te maken 1 voor een rode achtergrond en 1 voor een blauwe.

In het screenshot ziet u welke policy hiervoor nodig was.

|                                                                    |                                                                     |         |      |
|--------------------------------------------------------------------|---------------------------------------------------------------------|---------|------|
| User Configuration (Enabled)                                       |                                                                     |         | hide |
| Policies                                                           |                                                                     |         | hide |
| Administrative Templates                                           |                                                                     |         | hide |
| Policy definitions (ADMX files) retrieved from the local computer. |                                                                     |         |      |
| Desktop/Desktop                                                    |                                                                     |         | hide |
| Policy                                                             | Setting                                                             | Comment |      |
| Desktop Wallpaper                                                  | Enabled                                                             |         |      |
| Wallpaper Name:                                                    | \\192.168.1.1\Aperture Shared\Wallpapers\Aperture wallpaper red.jpg |         |      |
| Example: Using a local path: C:\windows\web\wallpaper\home.jpg     |                                                                     |         |      |
| Example: Using a UNC path: \\Server\Share\Corp.jpg                 |                                                                     |         |      |
| Wallpaper Style:                                                   | Fill                                                                |         |      |

|                                                                    |                                                                      |         |      |
|--------------------------------------------------------------------|----------------------------------------------------------------------|---------|------|
| User Configuration (Enabled)                                       |                                                                      |         | hide |
| Policies                                                           |                                                                      |         | hide |
| Administrative Templates                                           |                                                                      |         | hide |
| Policy definitions (ADMX files) retrieved from the local computer. |                                                                      |         |      |
| Desktop/Desktop                                                    |                                                                      |         | hide |
| Policy                                                             | Setting                                                              | Comment |      |
| Desktop Wallpaper                                                  | Enabled                                                              |         |      |
| Wallpaper Name:                                                    | \\192.168.1.1\Aperture Shared\Wallpapers\Aperture wallpaper blue.jpg |         |      |
| Example: Using a local path: C:\windows\web\wallpaper\home.jpg     |                                                                      |         |      |
| Example: Using a UNC path: \\Server\Share\Corp.jpg                 |                                                                      |         |      |
| Wallpaper Style:                                                   | Fill                                                                 |         |      |

De policy haalt de achtergrond uit een shared map waar de rode en de blauwe achtergrond in staan.

De objects pas ik dan toe aan de nodige OU's.

### 3.2 Marketing afdeling moet NodeJS geïnstalleerd krijgen.

Het tweede eis was dat de marketing afdeling de software van NodeJS geïnstalleerd moest krijgen bij het inloggen.

Heb hiervoor 1 object aangemaakt.

In het screenshot ziet u welke policy hiervoor nodig was.

|                                                                         |                                                             |      |
|-------------------------------------------------------------------------|-------------------------------------------------------------|------|
| User Configuration (Enabled)                                            |                                                             | hide |
| Policies                                                                |                                                             | hide |
| Software Settings                                                       |                                                             | hide |
| Assigned Applications                                                   |                                                             | hide |
| Node.js                                                                 |                                                             | hide |
| Product Information                                                     |                                                             | show |
| Deployment Information                                                  |                                                             | hide |
| General                                                                 | Setting                                                     |      |
| Deployment type                                                         | Assigned                                                    |      |
| Deployment source                                                       | \\192.168.1.1\Aperture Shared\Software\node-v17.3.0-x64.msi |      |
| Installation user interface options                                     | Maximum                                                     |      |
| Uninstall this application when it falls out of the scope of management | Disabled                                                    |      |
| Do not display this package in the Add/Remove Programs control panel    | Disabled                                                    |      |
| Install this application at logon                                       | Enabled                                                     |      |

De policy haalt een .msi bestand uit een shared map en gebruikt dit om de software te installeren bij login.

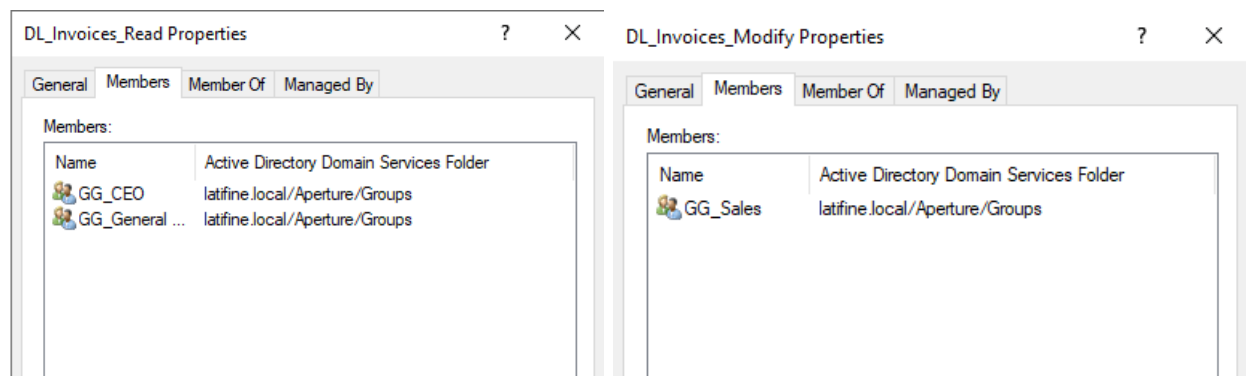
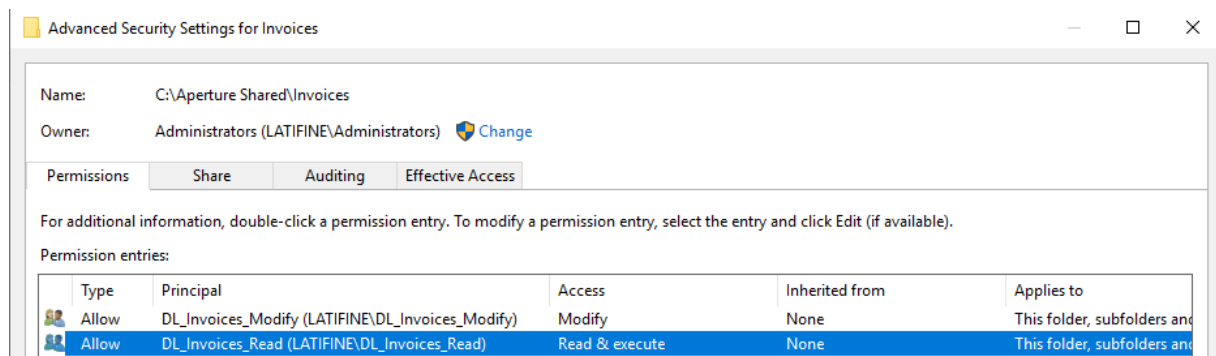
De objects pas ik dan toe aan de nodige OU's.

### 3.3 Rechten op de map Invoices

Het derde eis was dat afdeling Sales read/write rechten had op de shared map Invoices en het hoger management enkel read rechten.

Hiervoor heb ik de juist NFTS rechten moeten toepassen op de map en de juiste global groups memebers moeten maken van de juiste domain local group.

In de screenshots ziet u de rechten van de map en de members van de domain local groups.

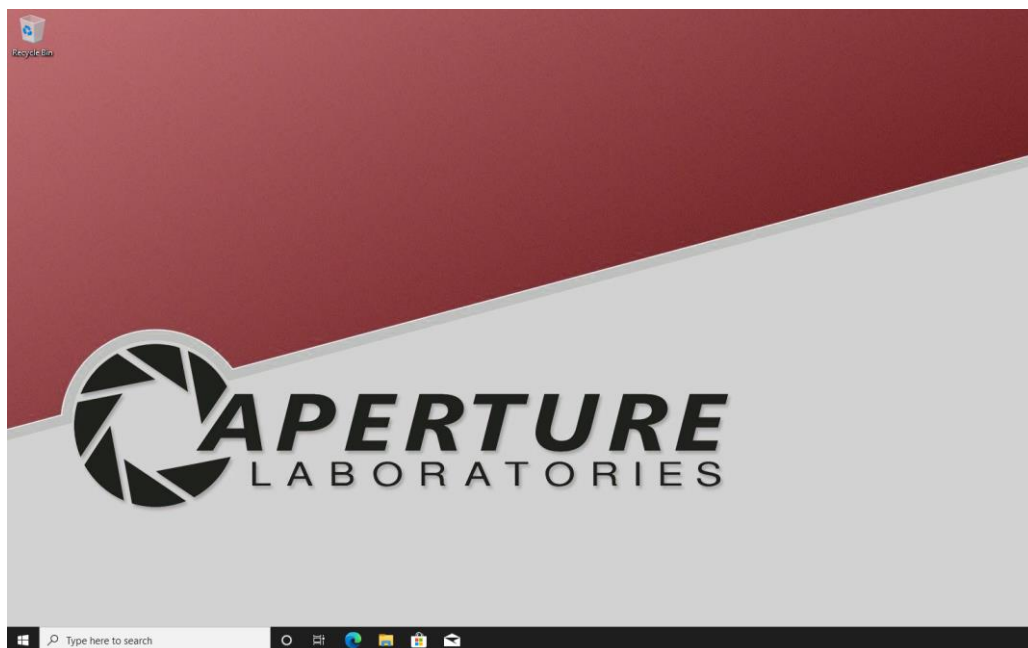
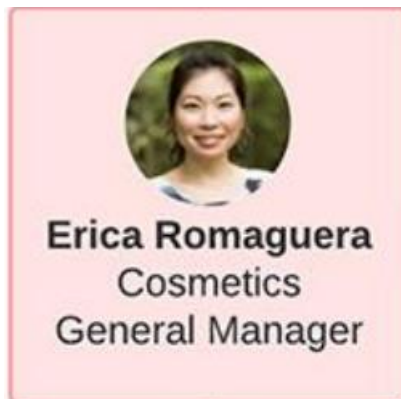


### 3.4 Overzicht

- ▼  CEO
  -  Wallpaper Blue
- ▼  Cosmetics
  -  Wallpaper Red
  -  Customer
  -  General Manager
  - ▼  Marketing
    -  NodeJS
  - >  Sales
  -  Groups
- ▼  Personal care
  -  Wallpaper Blue
  - >  Customer
  - >  General Manager
  - ▼  Marketing
    -  NodeJS
  - ▼  Sales
- ▼  Skin & Face
  -  Wallpaper Blue
  -  Customer
  - >  General Manager
  - ▼  Marketing
    -  NodeJS
  -  Sales

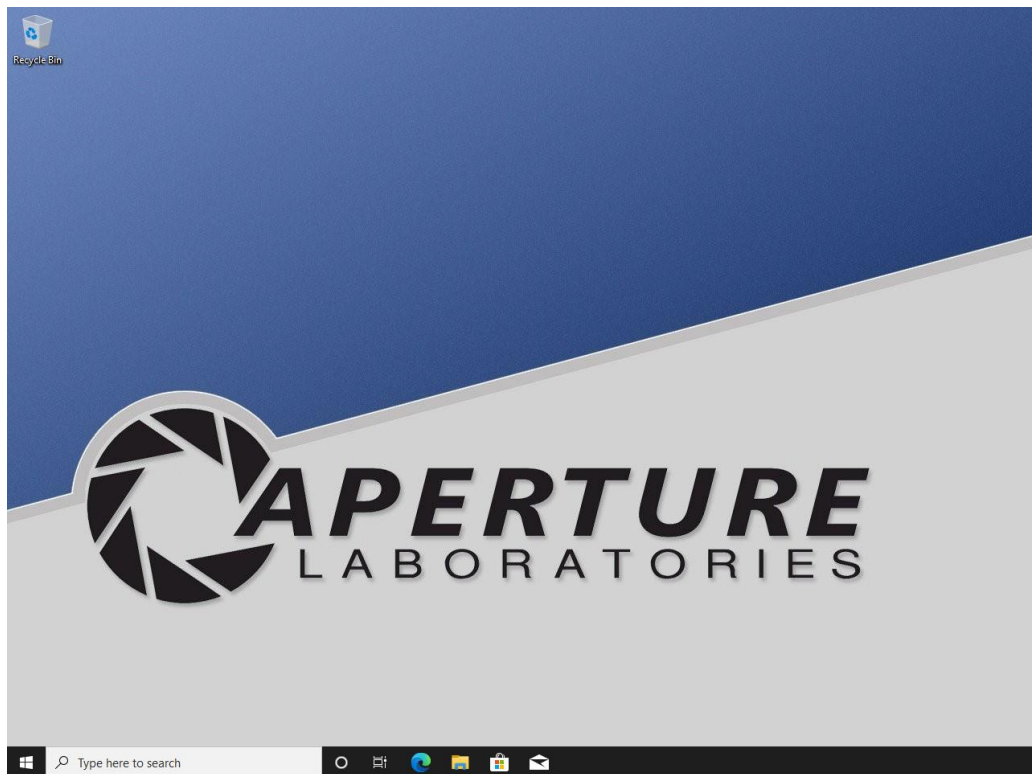
## 4 Resultaten

### 4.1 Eis 1

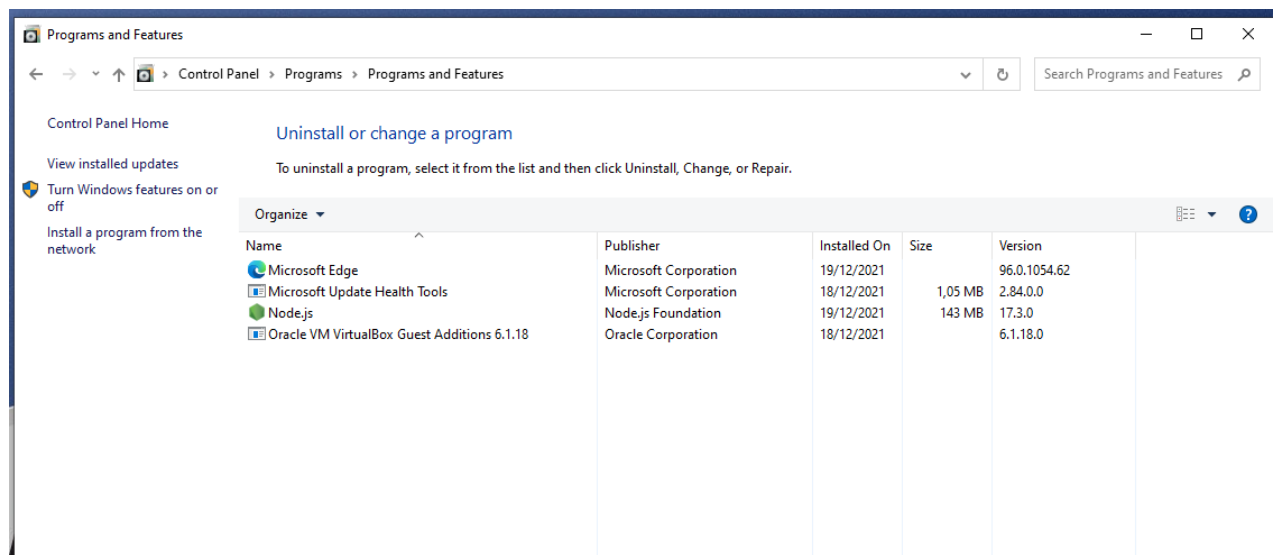




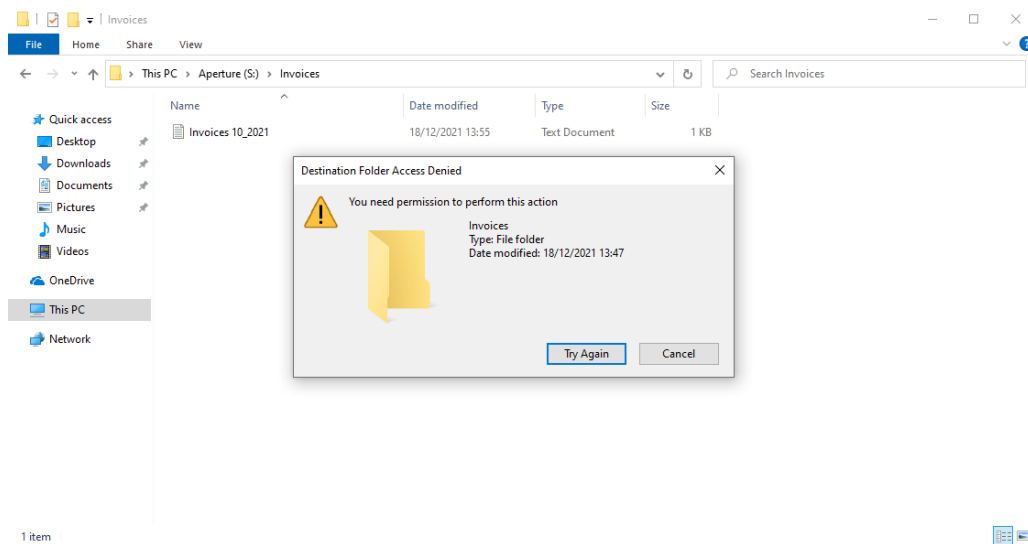
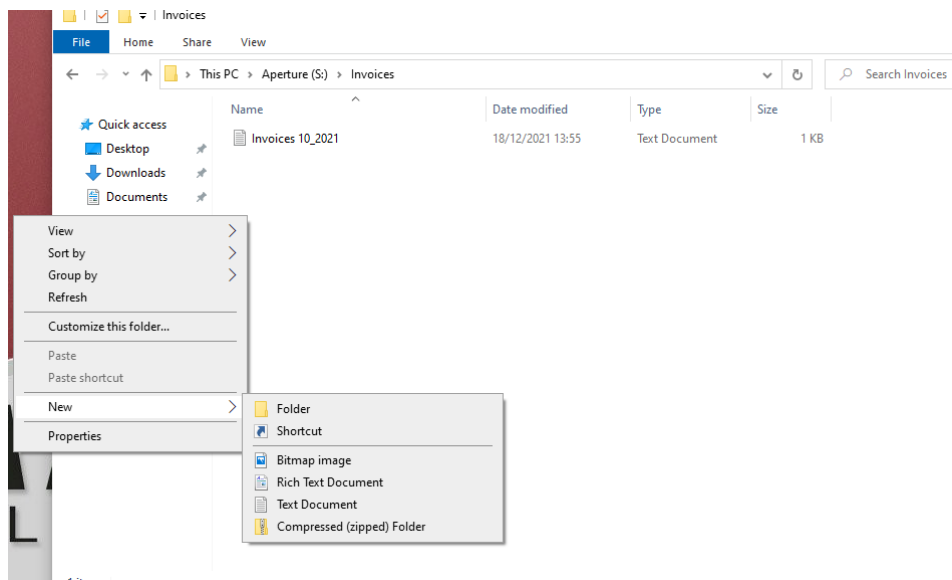
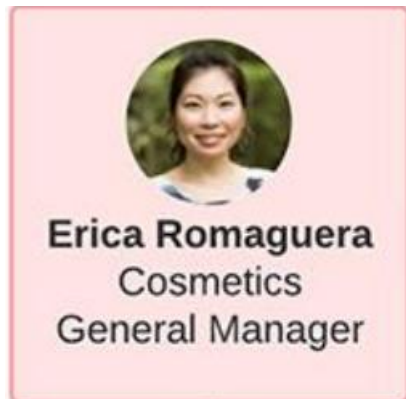
**Gianni Block**  
Sales Director

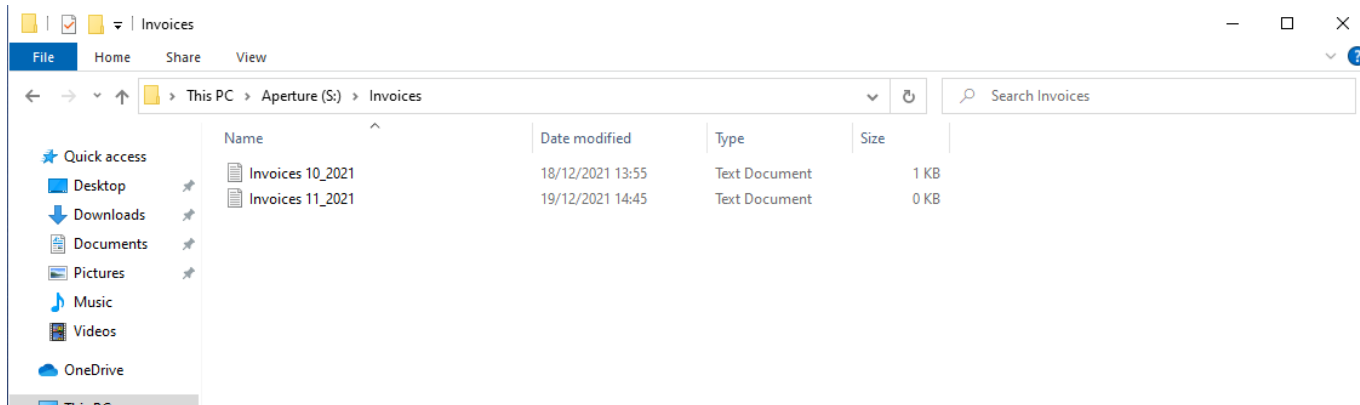
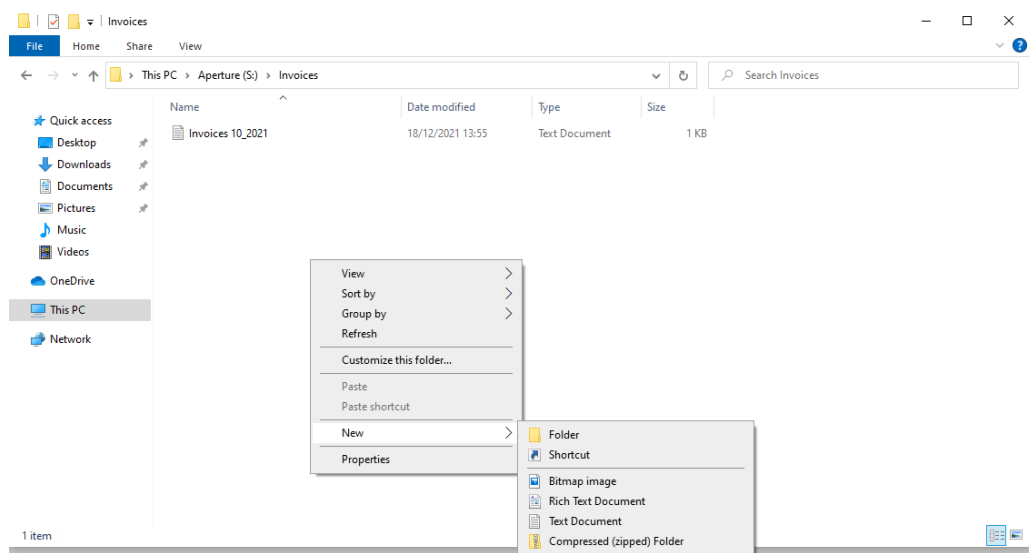
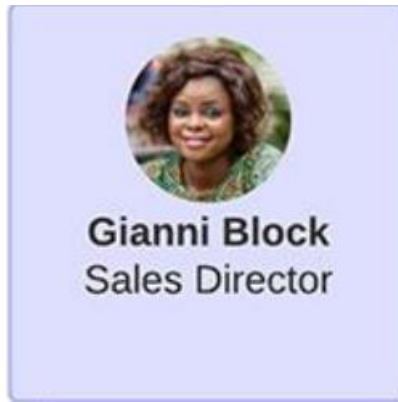


## 4.2 Eis 2



## 4.3 Eis 3





## **5 Browser security**

### **5.1 Link naar demo video**

[https://www.youtube.com/watch?v=v\\_kSiFofrkE](https://www.youtube.com/watch?v=v_kSiFofrkE)

## 6 Besluit

Na hard werken met vallen en opstaan is dit mijn resultaat geworden voor mijn case study voor het vak devops en security. Ik ben zeer blij en trots dat ik een mooi eind resultaat heb kunnen verwezenlijken en vond het zeer interessant en zeker voor herhaling vatbaar.