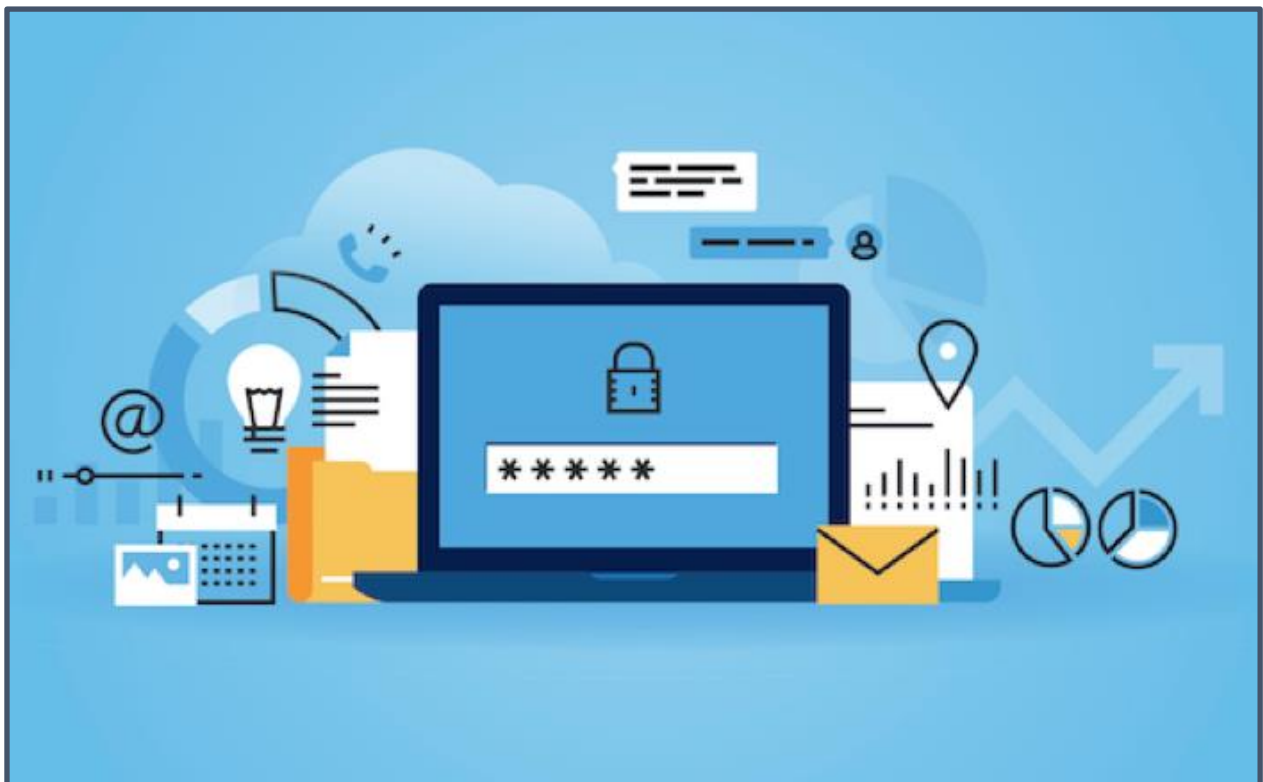


Livrable 3 :

Administration du Système d'Information



Sommaire

I.	Résumé	2
II.	Introduction	2
	<i>Contexte</i>	<i>2</i>
	<i>Problématique.....</i>	<i>2</i>
III.	Présentation de la maquette	2
	1. <i>Active Directory.....</i>	<i>2</i>
	2. <i>Sécurité.....</i>	<i>6</i>
	3. <i>Conteneurisation et automatisation du système.....</i>	<i>11</i>
	4. <i>Supervision et infrastructure.....</i>	<i>16</i>
IV.	Plan de formation et de protection des utilisateurs du S.I	18
	Mise en évidence des dangers :.....	19
	<i>Propositions</i>	<i>20</i>
	<i>Etape 1 : Test des failles actuels dans l'entreprise :.....</i>	<i>20</i>
	<i>Etape 2 : Formation des employés sur site</i>	<i>21</i>
	<i>Etape 3 : évaluation des améliorations.....</i>	<i>22</i>
V.	Devis et coût	23
	<i>Devis.....</i>	<i>23</i>
	<i>Facture</i>	<i>32</i>
VI.	Améliorations Possibles	33
VII.	Conclusion.....	38
VIII.	Table de Figures	39
IX.	Bibliographie	40

I. Résumé

Lors de dernier livrable on a étudié toutes les notions qu'on va mettre l'accent sur pour bien améliorer notre système d'information Abstergo, Nous avons faire la maquette de nouveau système et on a donné un devis et des propositions d'améliorations possibles.

II. Introduction

Contexte

Dans le cadre de notre projet, nous nous concentrons sur la conception d'une solution informatique complète pour répondre aux besoins de notre client. Cette solution vise à optimiser l'infrastructure informatique de l'entreprise, en mettant en place une architecture réseau solide, des mesures de sécurité renforcées et une gestion efficace des ressources informatiques. Dans ce livrable l'objectif principal est d'améliorer la performance, la sécurité et la disponibilité des systèmes informatiques de l'entreprise, tout en réduisant les coûts opérationnels.

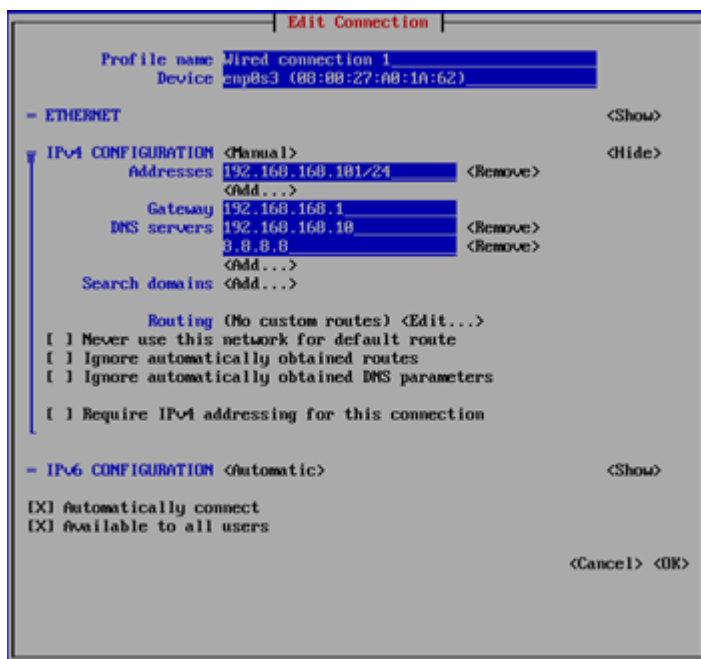
Problématique

Comment concevoir et mettre en œuvre une solution informatique complète qui répond aux besoins de l'organisation en matière d'architecture Active Directory, de sécurité, de cryptographie des données, de supervision, de virtualisation, et de gestion des coûts, tout en garantissant une maquette fonctionnelle démontrant la faisabilité et l'efficacité de la proposition ?

III. Présentation de la maquette

1. Active Directory

Tout d'abord, nous avons deux serveurs ayant le rôle d'AD DS (Active Directory Domain Services) : le serveur principal « Serveur ABSTERGO », contrôleur du domaine « abstergo.local » et le serveur secondaire « Serveur R&D », contrôleur du domaine « rdlyon.local ».



Rôles

Nous attribuons les rôles suivants aux deux serveurs :

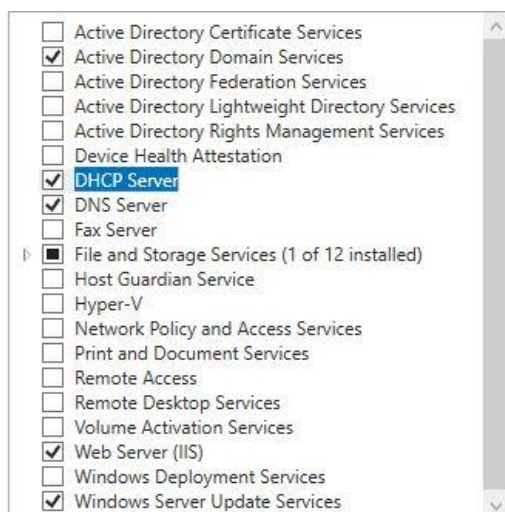


Figure 1: Rôles attribués

- **AD DS** : Pour l'administration des utilisateurs, des groupes et des ressources réseau. Permet d'avoir une gestion centralisée des utilisateurs, des ordinateurs et des politiques de sécurité au sein d'un réseau.
- **DHCP** : Permet de simplifier la gestion des adresses IP en attribuant dynamiquement des adresses aux périphériques lors de leur connexion au réseau.
- **DNS** : Permet de traduire les noms de domaine en adresse IP. Fondamental pour la résolution des noms de domaine en adresses IP, facilitant ainsi l'identification des ressources réseau.
- **WSUS** : Permet de gérer la distribution des mises à jour logicielles publiées par Microsoft aux ordinateurs clients dans un réseau. Cela assure la sécurité et la cohérence du système.
- **Web Server (IIS)** : Fournit un serveur web pour héberger des sites web et des applications. Essentiel puisque la société

ABSTERGO est spécialisée dans la conception de capteurs et de solutions IOT.

Relation D'approbation

Le système originel d'ABSTERGO comprenait deux sites distants : le site principal et le site R&D de Lyon. Il fallait rapprocher ces deux en permettant aux administrateurs de « abstergo.local » d'avoir accès aux ressources de « rdlyon.local » sans avoir l'accès inverse. Nous avons fait ceci en utilisant une relation d'approbation unidirectionnelle et transitive avec « abstergo.local » étant l'approuvant et « rdlyon.local » étant l'approuvé.

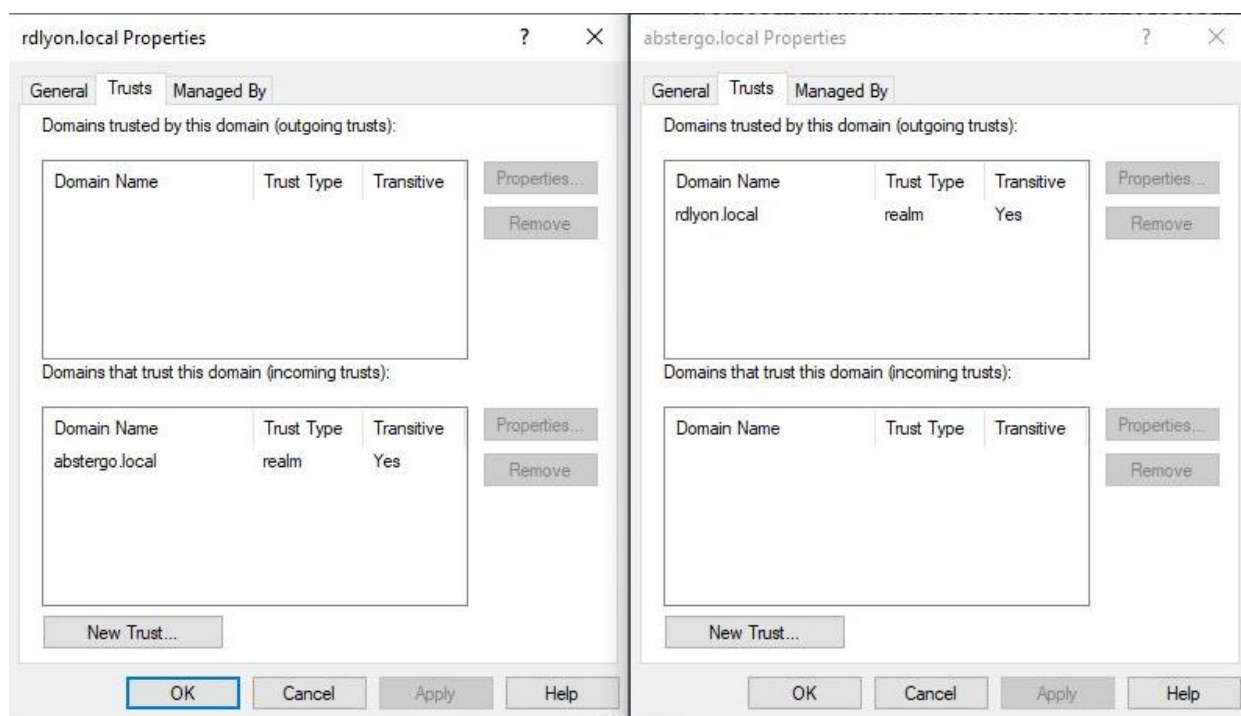


Figure 2: Relation approbation unidirectionnelle

Organisation de l'AD

L'entreprise d'ABSTERGO est composée de six services : Direction, Administratif, Production, R&D et Commercial. Nous organisons notre Active Directory de façon de répartir les utilisateurs dans les services tout en pouvant facilement attribuer les GPO à ces premiers.

L'organisation choisie permet de lier les GPO aux Unités Organisationnelles de la région ou uniquement à celui du service puis de l'attribuer aux groupes de service. Ces derniers permettent d'éviter de devoir attribuer les GPO aux utilisateurs individuellement. De plus, cette organisation facilite l'ajout de régions et de secteurs à l'AD de l'entreprise.

Les GPO que nous ajoutons sont :

- **Raccourcis-Utilisateur** : Créer un raccourci sur le Bureau du poste de travail des utilisateurs concernés au ERP Dolibarr en accédant au lien « erp-dolibarr.fr ».
- **LecteurRéseau** : Créer un lecteur réseau Z: partagé aux utilisateurs concernés.
- **InstallAntivirus** : Permet de télécharger l'antivirus Eset (version gratuite pour cette démonstration) sur les machines concernées en accédant l'application d'installation partagée sur le réseau et en exécutant un script PowerShell.

```

1  ### Variables
2  $SharedFolder = "\\win-q4nnsq22h6t.abstergo.local\applications$"
3
4  $LocalFolder = "C:\TEMP"
5
6  $ExeName = "avast_free_antivirus_setup_online.exe"
7
8  $ExeArgument = "/S"
9
10 if (Test-Path "$SharedFolder\$ExeName"){
11
12     New-Item -ItemType Directory -Path "$LocalFolder" -ErrorAction SilentlyContinue
13     Copy-Item "$SharedFolder\$ExeName" "$LocalFolder" -Force
14
15     if (Test-Path "$LocalFolder\$ExeName"){
16         Start-Process -Wait -FilePath "$LocalFolder\$ExeName" -ArgumentList "$ExeArgument"
17     }
18
19     Remove-Item "$LocalFolder\$ExeName"
20
21 }else{
22     Write-Warning "L'exécutable ($ExeName) est introuvable sur le partage !"
23 }
24
25 if (Get-Package -Name "Avast Free Antivirus") {
26     Write-Output "Le logiciel Avast est déjà présent"
27 }
28

```

Figure 3: Script PowerShell de InstallAntivirus

Nous obtenons l'Active Directory suivant :

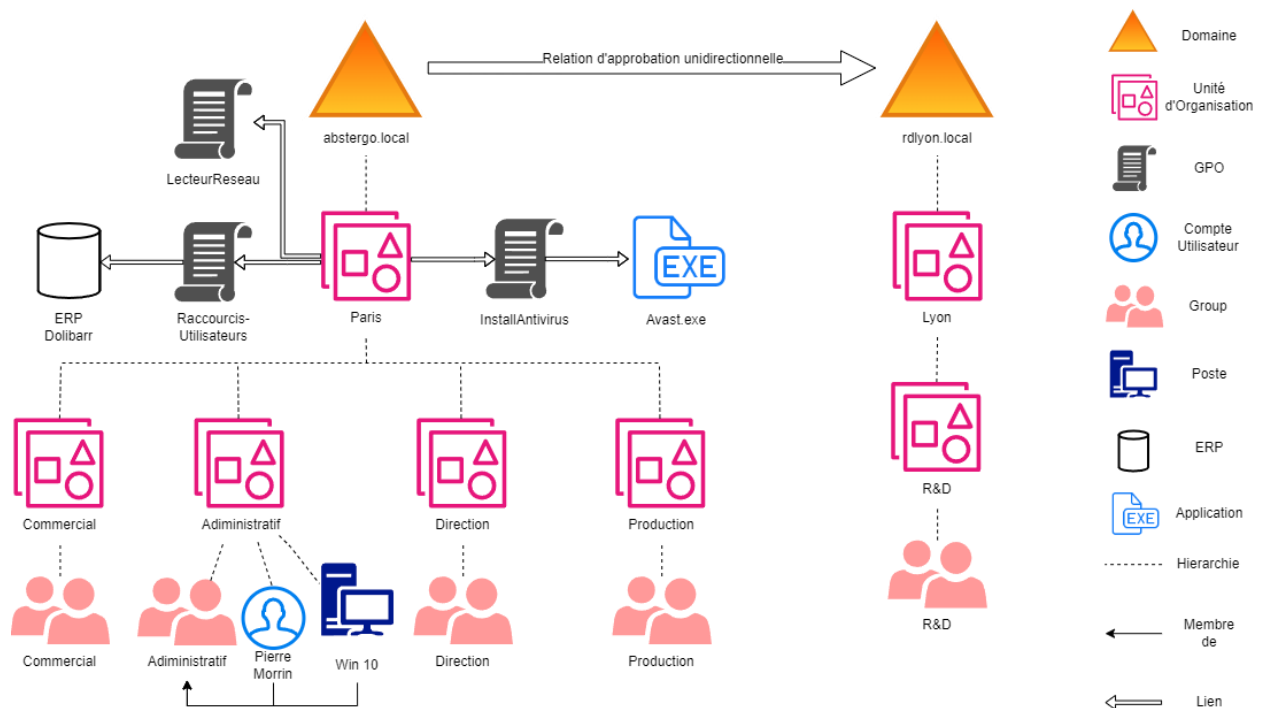


Figure 4: Schématisation de l'Active Directory

2. Sécurité

Pare-feu

Nous avons utilisé le pare-feu open-source Pfsense pour mettre en place les règles de filtrages sur les paquets entrants sur ses interfaces. Ainsi, nous configurons les adaptateurs du pare-feu de manière qu'ils soient : NAT, LAN-Abstergo et DMZ-Abstergo.

Nous nous sommes concentrés sur les risques que peuvent rencontrer nos utilisateurs sur internet. Pour cela, nous avons créé des règles de filtrages sur les paquets entrants par la WAN. Nous avons tout d'abord créé une règle pour bloquer l'accès aux sites http. En effet, ces derniers ne sont pas chiffrés, facilitent les attaques de type MITM (Man-In-The-Middle) et sont plus susceptibles de distribuer du contenu malveillant.

D'autre part, nous utilisons le package PfBlocker. Celui-ci permet de créer automatiquement des règles de filtrages qui bloquent une liste d'adresses IP de sites malicieux ou non-sécurisés prédéfinis. Nous avons bloqué les listes PRI1 et PRI3, deux listes de haute qualité, qui se réactualisent souvent et qui contiennent peu de faux positifs.

Figure 5: Configuration PRI3

Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
<input checked="" type="checkbox"/>	0/0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	0/0 B	IPv4 *	pfB_PRI1_v4	*	*	*	*	none		pfB_PRI1_v4 auto rule	
<input type="checkbox"/>	0/0 B	IPv4 *	pfB_PRI3_v4	*	*	*	*	none		pfB_PRI3_v4 auto rule	
<input type="checkbox"/>	0/0 B	IPv4 UDP	*	*	*	1191	*	none		Acces Internet -> OpenVPN	
<input type="checkbox"/>	0/0 B	IPv4+6 TCP	*	*	LAN address	80 (HTTP)	*	none		Bloque HTTP	

Figure 6: Règles de filtrage WAN

VPN

Nous utilisons le paquet OpenVPN dans Pfsense. Celui-ci nous a permis de mettre en place un serveur VPN qui établit une connexion sécurisée et cryptée entre les utilisateurs certifiés par ABSTERGO et la WAN. Ceci est fait en créant un tunnel crypté avec l'algorithme de hachage SHA512 et en attribuant l'adresse IP 192.168.168.0/24 aux clients afin de dissimuler les adresses réelles.




VPN / OpenVPN / Servers					
Servers Clients Client Specific Overrides Wizards Client Export					
OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 1194 (TUN)	192.168.168.0/24	Mode: Remote Access (SSL/TLS) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA512 D-H Params: 2048 bits	VPN	  

Figure 7 : Serveur VPN

Proxy

Nous utilisons le paquet SquidGuard de Pfsense afin d'avoir un proxy transparent sur HTTP/HTTPS. Celui-ci, d'une part, permet de surveiller le trafic HTTP/HTTPS en temps réel des utilisateurs ce qui permet de détecter les activités suspectes, analyser le comportement des utilisateurs ou encore générer des rapports sur l'utilisation d'Internet au sein de l'organisation. D'autre part, nous utilisons le proxy transparent pour bloquer des sites spécifiques, pour l'instant « facebook.com » et « twitter.com », en utilisant les règles ACL.

Squid Access Table					
Date	IP	Status	Squid - Access Logs Address	UserDestination	
12.11.2023 15:25:49	192.168.100	TCP_REFRESH_MODIFIED/200	http://www.msftconnecttest.com/connecttest.txt	-	104.123.50.170
12.11.2023 15:09:32	192.168.101	TCP_MISS/206	http://2.au.download.windowsupdate.com/d/msdownload/update/software/updt/2023/09/windows10.0-kb5031005-x64_28695ad07af69031af976d9b7079484bac846ebb-ca-b	-	2.21.132.186
12.11.2023 15:09:31	192.168.101	TCP_MISS/206	http://2.au.download.windowsupdate.com/d/msdownload/update/software/updt/2023/10/windows-kb890830-x64-v5.118_1898d7783231ed14970911d2c4d815be13e2a4a.exe	-	2.21.132.208
12.11.2023 15:09:31	192.168.101	TCP_MISS/206	http://2.au.download.windowsupdate.com/d/msdownload/update/software/updt/2023/10/windows-kb890830-x64-v5.118_1898d7783231ed14970911d2c4d815be13e2a4a.exe	-	2.21.132.186
12.11.2023 15:09:31	192.168.101	TCP_MISS/200	http://download.windowsupdate.com/phf/d/dod/ph/pro-d5/msdownload/update/software/updt/2023/10/1024/windows-kb890830-x64-v5.118_1898d7783231ed14970911d2c4d815be13e2a4a.exe.json	-	95.100.203.137
12.11.2023 15:09:31	192.168.101	TCP_MISS/206	http://2.au.download.windowsupdate.com/d/msdownload/update/software/updt/2023/09/windows10.0-kb5031005-x64_28695ad07af69031af976d9b7079484bac846ebb-ca-b	-	2.21.132.208
12.11.2023 15:09:31	192.168.101	TCP_MISS/200	http://download.windowsupdate.com/phf/d/dod/ph/pro-d5/msdownload/update/software/updt/2023/09/1024/windows10.0-kb5031005-x64_28695ad07af69031af976d9b7079484bac846ebb-ca-b.json	-	95.100.203.177
12.11.2023 15:09:31	192.168.101	TCP_MISS/206	http://3.au.download.windowsupdate.com/d/	-	8.247.205.126

Figure 8: Table de logs

Blacklist

facebook.com
twitter.com

Destination domains that will be blocked for the users that are allowed to use the proxy. Put each entry on a separate line. You can also use regular expressions.

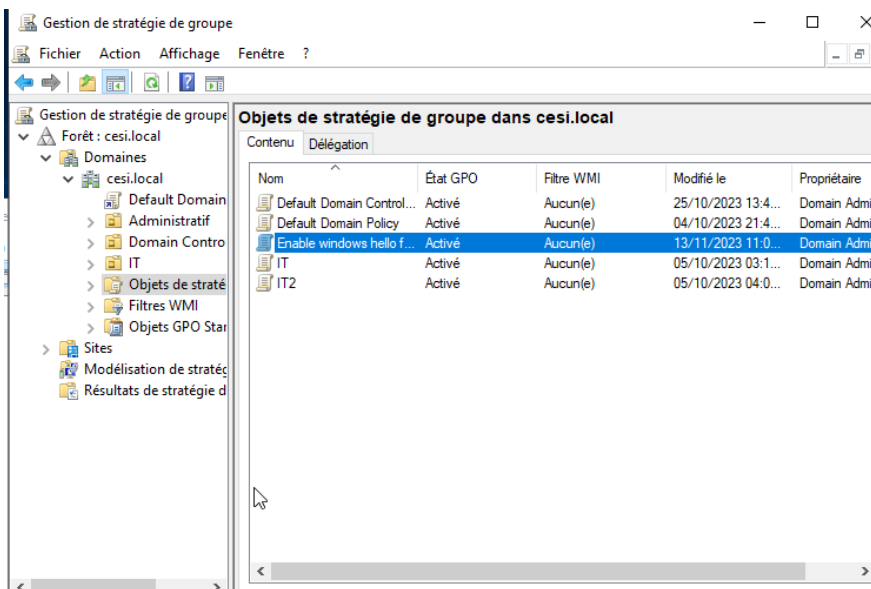
Figure 9: Règles ACL

Authentification

Windows Hello :

Dans le livrable 2, nous avons évalué que la meilleure solution était de mettre en place une authentification windows hello + mot de passe, afin de nous assurer du bon fonctionnement de cette méthodes nous allons suivre les étapes suivantes :

En premier lieu, nous devons créer une nouvelle stratégie de groupe :



Nous avons nommé cette stratégie : Enable windows hello for business

Une fois cela fait, il faut simplement configurer la stratégie de groupe en passant par :

User Configuration > Politiques > Administrative Templates > Windows Component > Windows Hello for Business

Figure 10: Creation GPO windows hello

Une fois arrivé sur cette page nous devrions obtenir la page suivante :

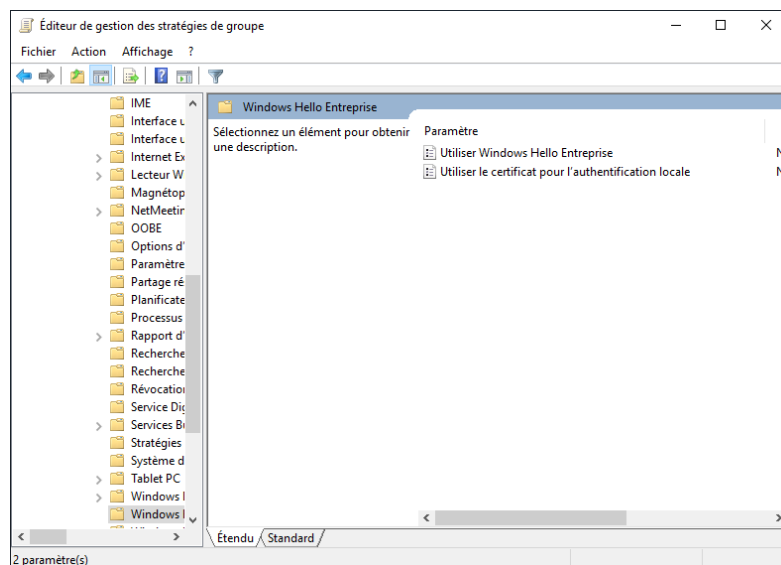
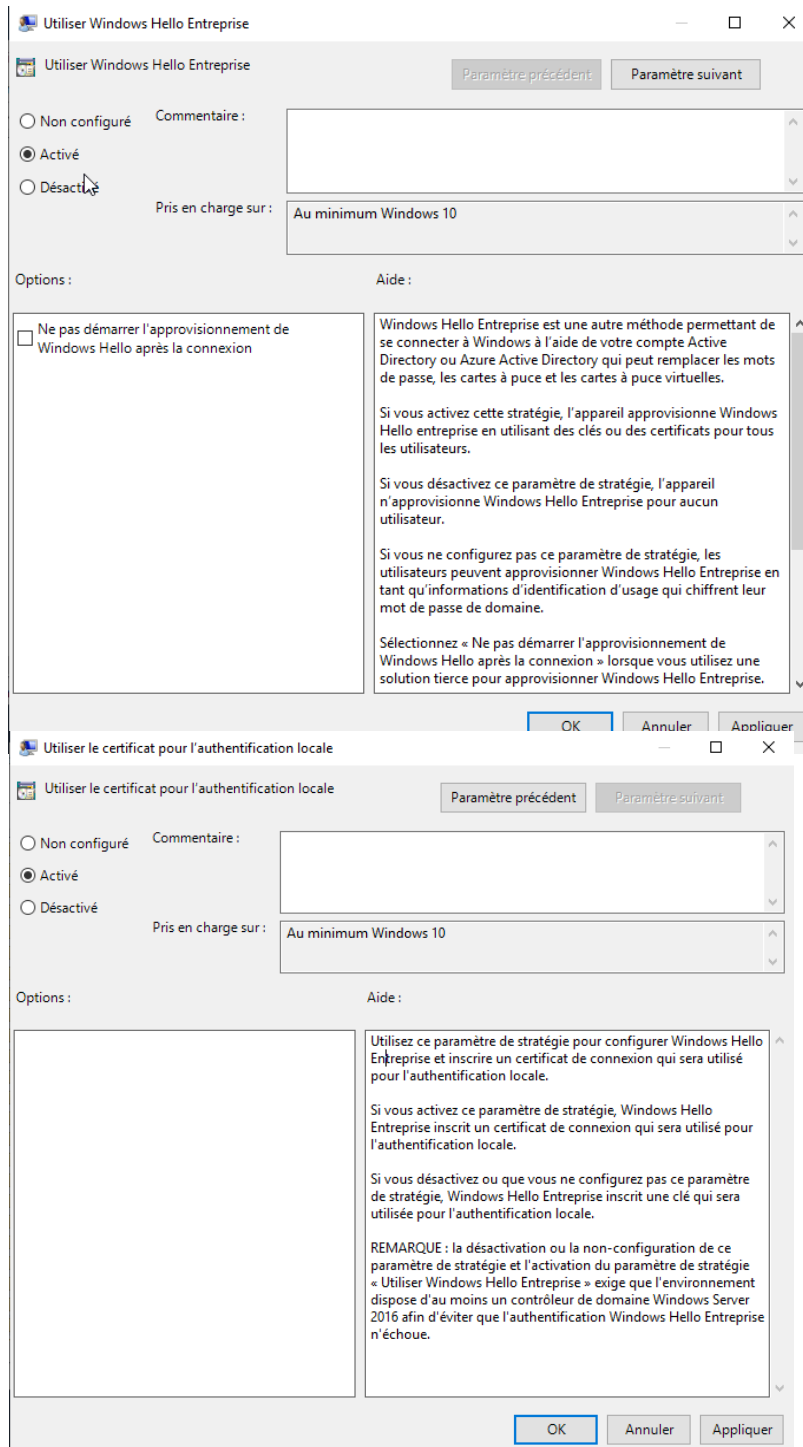


Figure 11 : Configuration GPO

Une fois cela fait, nous double cliquons sur « Utiliser Windows Hello Entreprise » :



Nous sélectionnons activer et cliquons sur OK

Il faut ensuite faire la même manipulation sur utiliser le certificat pour l'authentification locale :

Figure 12 : Règle Windows Hello Enterprise

En suite, nous devons naviguer dans: **Windows Settings > Security Settings > Public Key Policies**

Figure 13: Règle certificat authentication locale

Nous arriverons sur le panneau suivant :

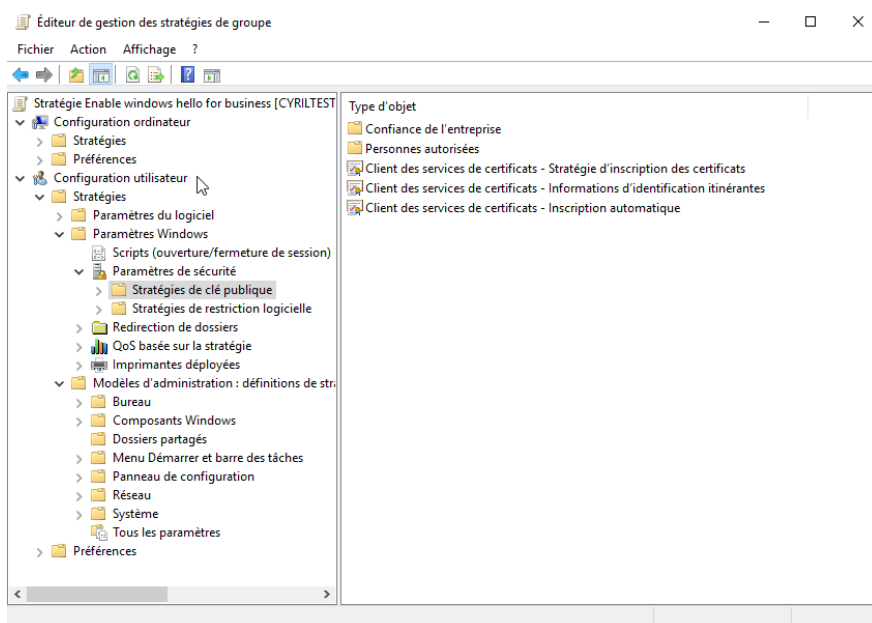
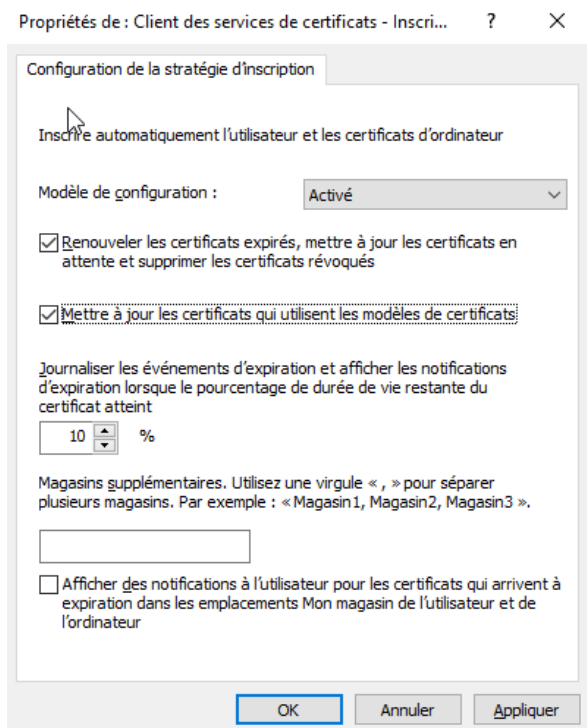


Figure 14: Stratégie de clés publique

Dans le quel il faudra sélectionner : « Client des services de certificats – Inscription automatique »



Dans ce menu nous avons mis en Modèle de configuration : Activé

Et sélectionner :

- Renouveler les certificats expirés
- Mettre à jour les certificats

Puis nous avons validé.

Cette configuration permettra aux utilisateurs qui ont des postes de travail avec caméras compatibles de s'authentifier avec la reconnaissance faciale.

Figure 15: Clients des services de certificats

D'autre part, pour les systèmes qui ne peuvent pas être accédés avec les caméras, nous utilisons l'application Keepass pour générer et garder les mots de passe du système d'information. Nous

choisissons de générer des mots de passes de 15 caractères en total, composé de caractères spéciaux, de majuscules et de minuscules. Nous voyons que ces mots de passes prennent de centaines d'années pour être décryptés par brute force. La base de mots de passe est elle-même protégée par un mot de passe.

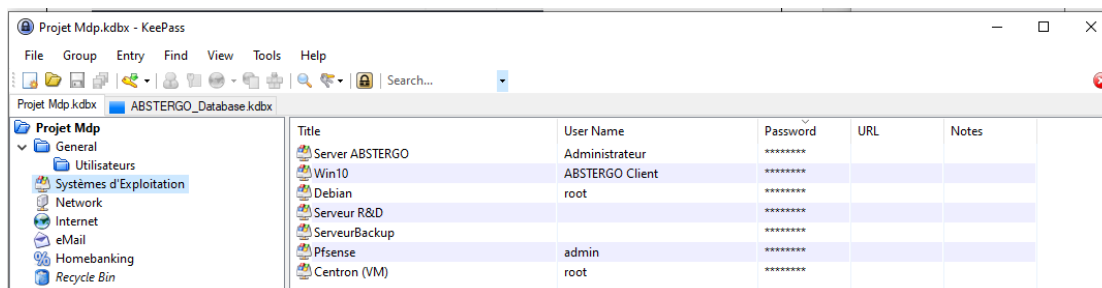


Figure 16: Base de mot de passe KeePass

3. Conteneurisation et automatisation du système

Conteneurisation

Nous avons essayé d'utiliser Docker et Ansible afin de faire la conteneurisation et l'automatisation du système. Nous avons tenté de déployer un conteneur pour lister les GPO appliqués à un utilisateur. Nous avons tout d'abord créé un Dockerfile et un programme python que nous utilisons pour créer l'image « gpouser:latest » dans le conteneur « GPOUser »

```
GNU nano 7.2 Dockerfile
FROM python:latest
WORKDIR /app

COPY . /app

CMD ["python", "app.py"]
```

Figure 17: Dockerfile

```
GNU nano 7.2 app.py
import subprocess

def get_applied_gpos(username):
    try:
        result = subprocess.run(['gpresult', '/USER', username, '/SCOPE', 'USER'])
        output = result.stdout
        print(output)
    except subprocess.CalledProcessError as e:
        print(f"Erreur lors de l'exécution de gpresult : {e}")

if __name__ == "__main__":
    username = 'utilisateur_test'
    get_applied_gpos(username)
```

Figure 18: app.py

Nous écrivons un playbook.yml afin de déployer le conteneur « GPOUser ». Cependant, nous avons besoin de d'installer Docker et configurer WinRM pour qu'il puisse accéder à l'Active Directory du Windows Serveur.

```

GNU nano 7.2                                playbook.yml
---
- name: Manage Docker Container with Ansible
  hosts: 192.168.168.10
  connection: local
  become: true
  tasks:
    - name: Pull gpouser Docker Image
      command: docker pull gpouser:latest

    - name: Run GPOUser Container
      command: docker run -d --name GPOUser -p 8080:80 gpouser:latest
  
```

Figure 19: playbook.yml

Il est conseillé d'utiliser les scripts PowerShell afin d'automatiser l'Active Directory et les autres éléments du système d'information.

Scripts

Afin d'automatiser au mieux possible notre active directory, nous avons mis en place des scripts powershell permettant de créer des utilisateurs à l'aide d'un simple fichier excel, mais aussi de les supprimer, le tout en ayant une liste d'exclusion permettant de s'assurer qu'aucun compte important est effacé, ce qui pourrait tuer la machine (oui, c'est déjà arrivé sur une de nos VM) :

```

Install-Module -Name ImportExcel

# Importation des données Excel
$CSVData = Import-Excel -Path 'C:\Users\vboxuser\Downloads\Users.xlsx' -
HeaderName Nom,Prenom,OU,Groupe -StartRow 2

# Collecter tous les utilisateurs AD actuels
$AllADUsers = Get-ADUser -Filter * | Select-Object -ExpandProperty SamAccountName

# Liste des comptes à ne pas supprimer
$ExcludedAccounts = @("admin", "vboxuser", "autres_comptes_importants")

foreach($User in $CSVData)
{
    $UserNom = $User.Nom
    $UserPrenom = $User.Prenom
    $UserOU = $User.OU
    $UserGroupe = $User.Groupe
    $UserLogin = (($UserPrenom.Substring(0,1)).ToLower() +
    $UserNom.ToLower()).replace(' ','')

    if ($UserLogin.Length -gt 20)
    {
  
```

```

    $UserLogin = $UserLogin.substring(0,20)
  }

  $UserMotDePasse = "ChangeMe2024"

  # Vérifier l'existence de l'OU
  if (-not (Get-ADOrganizationalUnit -Filter {ou -eq $UserOU}))
  {
    New-ADOrganizationalUnit $UserOU -ProtectedFromAccidentalDeletion $false
  }

  # Vérifier l'existence du groupe
  if (-not (Get-ADGroup -Filter {SamAccountName -eq $UserGroupe}))
  {
    New-ADGroup -Name $UserGroupe -GroupScope Global -Path "OU=$UserOU,
DC=Abstergo, DC=local"
  }

  # Vérifier si l'utilisateur existe déjà
  if (-not (Get-ADUser -Filter {SamAccountName -eq $UserLogin}))
  {
    New-ADUser -Name "$UserNom $UserPrenom" `
      -DisplayName "$UserNom $UserPrenom" `
      -GivenName $UserPrenom `
      -Surname $UserNom `
      -SamAccountName $UserLogin `
      -UserPrincipalName "$UserLogin@cesi.local" `
      -Path "OU=$UserOU,DC=cesi,DC=local" `
      -AccountPassword (ConvertTo-SecureString $UserMotDePasse -
AsPlainText -Force) `
      -ChangePasswordAtLogon $true `
      -Enabled $true

    Add-ADGroupMember -Identity $UserGroupe -Members $UserLogin
    Write-Output "Création du nouvel utilisateur : $UserLogin"
  }
  else
  {
    Write-Warning "L'utilisateur $UserLogin existe déjà dans l'Active
Directory"
  }

  # Supprimer l'utilisateur de la liste $AllADUsers
  $AllADUsers = $AllADUsers | Where-Object { $_ -ne $UserLogin }
}

# Supprimer les utilisateurs qui ne sont pas dans le fichier Excel et qui ne sont
pas dans la liste d'exclusion

```

```
foreach ($UserLogin in $AllADUsers)
{
    if ($UserLogin -notin $ExcludedAccounts)
    {
        Remove-ADUser -Identity $UserLogin -Confirm:$false
        Write-Output "Utilisateur supprimé : $UserLogin"
    }
    else
    {
        Write-Output "L'utilisateur $UserLogin est dans la liste d'exclusion et ne sera pas supprimé."
    }
}
```

Explication du code :

Installation du module ImportExcel :

« Install-Module -Name ImportExcel »

Ce module est utilisé pour importer des données depuis un fichier Excel. Il simplifie la lecture des fichiers Excel dans PowerShell.

Importation des données Excel :

« \$CSVData = Import-Excel -Path 'C:\Users\vboxuser\Downloads\Users.xlsx' -HeaderName Nom,Prenom,OU,Groupe -StartRow 2 »

Cette commande importe les données d'un fichier Excel. Les colonnes sont spécifiées par les noms **Nom**, **Prenom**, **OU** (unité organisationnelle), et **Groupe**. Le traitement commence à partir de la deuxième ligne du fichier.

Collecte des utilisateurs AD actuels :

“\$AllADUsers = Get-ADUser -Filter * | Select-Object -ExpandProperty SamAccountName”

Récupère tous les comptes utilisateurs existants dans Active Directory, en ne sélectionnant que leurs noms de compte (SamAccountName).

Liste des comptes à ne pas supprimer :

« \$ExcludedAccounts = @("admin", "vboxuser", "autres_comptes_importants") »

Crée une liste de comptes qui ne doivent pas être supprimés, comme les comptes administrateurs et les comptes système.

Boucle de traitement des utilisateurs du fichier Excel :

« foreach(\$User in \$CSVData) { ... } »

Cette boucle traite chaque utilisateur listé dans le fichier Excel.

- **Extraction et traitement des informations de l'utilisateur :** À l'intérieur de cette boucle, le script extrait les informations de chaque utilisateur (nom, prénom, OU, groupe) et génère un nom de connexion.
- **Vérification et création de l'OU :** Le script vérifie si l'unité organisationnelle spécifiée existe. Si elle n'existe pas, elle est créée.
- **Vérification et création du groupe :** De manière similaire, le script vérifie l'existence du groupe spécifié et le crée si nécessaire.
- **Création de l'utilisateur dans AD :** Si l'utilisateur n'existe pas déjà dans Active Directory, il est créé avec les informations fournies.
- **Retrait de l'utilisateur de la liste des utilisateurs AD :** Après le traitement de chaque utilisateur, son nom de connexion est retiré de la liste **\$AllADUsers**. Cette étape est cruciale pour la suppression des utilisateurs non listés dans le fichier Excel.

Suppression des utilisateurs non listés dans le fichier Excel :

« foreach (\$UserLogin in \$AllADUsers) { ... } »

Cette boucle parcourt la liste des utilisateurs AD restants (ceux qui ne sont pas mentionnés dans le fichier Excel) et les supprime, à condition qu'ils ne soient pas dans la liste des comptes exclus (**\$ExcludedAccounts**).

Une fois ce code exécuté, nous obtenons cela :

```

10 $UserGroupe = $User.Groupe
11 $UserLogin = ((($UserPrenom.Substring(0,1)).ToLower() + $UserNom.ToLower()))
12 $UserLogin = $UserLogin.replace(' ', '')
13 if ($UserLogin.Length -gt 20)
14 {
15     $UserLogin.remove($UserLogin.Length - 1)
16 }
17 $UserMotDePasse = "ChangeMe2024"
18
19 #Check si l'OU existe
20 if (Get-ADOrganizationalUnit -Filter {ou -eq $UserOU })
21 {
22 }
23 else
24 {
25     #Creation de l'OU
26     New-ADOrganizationalUnit $UserOU -ProtectedFromAccidentalDeletion $false
27
28     New-ADUser -Name $UserNom $UserPrenom `
29     -DisplayName "$UserNom $UserPrenom" `
30     -GivenName $UserPrenom `
31     -Surname $UserNom `
32     -SamAccountName $UserLogin `
33     -UserPrincipalName "$UserLogin@cesi.local" `
34     -Path "OU=$UserOU,DC=cesi,DC=local" `
35     -AccountPassword (ConvertTo-SecureString $UserMotDePasse -AsPlainText -Force) `
36     -ChangePasswordAtLogon $true `
37     -Enabled $true
38
39     Add-ADGroupMember -Identity $UserGroupe -Members $UserLogin
40     Write-Output "Création du nouvel utilisateur : $UserLogin"
41 }
42 }
43
44 Création du nouvel utilisateur : ctilhou
45
46 PS C:\Windows\system32>
  
```

Ce qui permet de rapidement et visuellement maintenir une liste des utilisateurs encore actifs sur le système

La liste doit impérativement être en fichier XLS et sous le format suivant :

Nom	Prenom	OU	Groupe
Tilhou	Cyril	IT	IT

Piste d'amélioration :

Il est possible d'utiliser le Task Scheduler de Windows pour automatiquement mettre à jour la liste à minuit.

4. Supervision et infrastructure

Supervision

(Centreon sur l'interface LAN ou SolarWinds NPM sur Windows Serveur)

Dans cette partie pour bien améliorer notre system d'information il faut utiliser un outil de supervision pour superviser l'état de performance de réseau dans un Dashboard. On a utilisé le Centreon quand doit installer et configurer les adresses afin d'avoir une interface graphique pour la supervision.

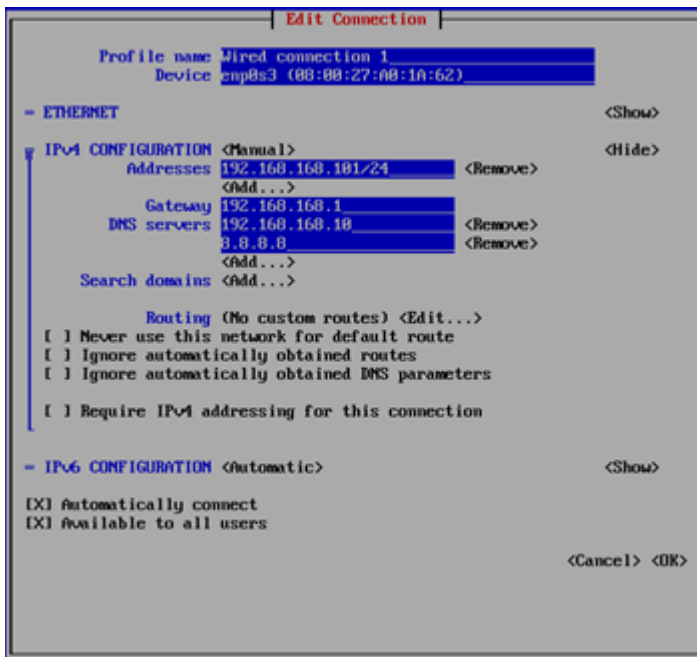


Figure 20: Configuration Réseau Centreon

→ Pour aller plus loin dans l'amélioration de votre système d'information on va utiliser un outil de supervision qui est assez performante et applicable à nos besoins car on a 100 machines et deux serveurs distants (Paris et Lyon)

→ On a choisi pour cette partie SolarWinds Network Performance Monitor qu'on installe pour tester durant la période d'essai qui dure 30 jours et qui a approuvé son efficacité pour assurer l'amélioration sur votre système d'information.

→ Toute information de Network Performance Monitor est bien expliquée dans la partie devis et cout.

Infrastructure

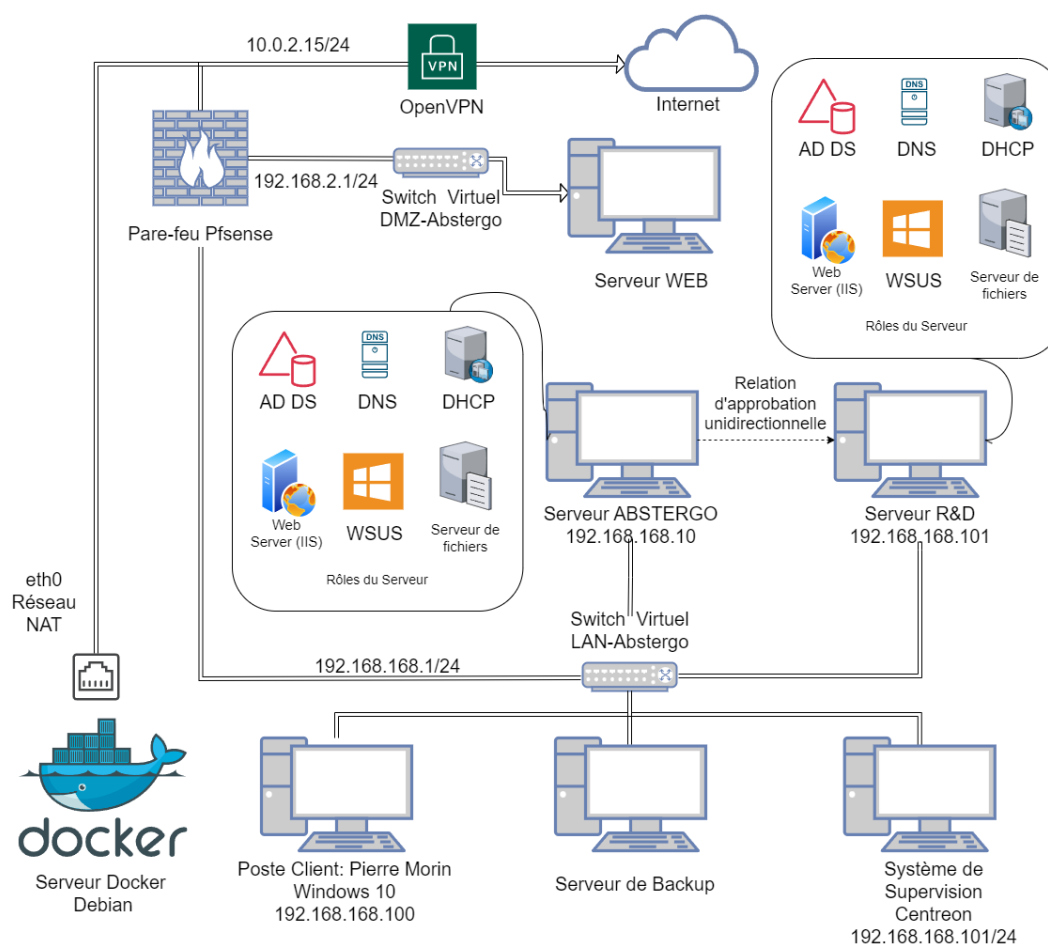


Figure 21: Schématisation finale

IV. Plan de formation et de protection des utilisateurs du S.I

Un bon S.I est un système complexe méticuleusement produit pour assurer la sécurité de toutes les informations qui transitent à travers celui-ci, mais aucun S.I n'est infallible, et souvent dans les bons S.I, si toutes les précautions sont prises, les failles ne sont pas d'origine matérielle ni logicielle, mais humaine.

En effet, une attaque relativement basse compétence utilisant du « Social engineering » peut faire de très gros dégâts si les utilisateurs du S.I ne sont pas au courant des risques pour eux même et leurs entreprises.

Mise en évidence des dangers :

Sun Tzu aurait écrit dans son fameux livre : l'art de la guerre, « Connaissez l'ennemi et connaissez-vous vous-même ; en cent batailles vous ne courrez jamais aucun danger. ». bien que ces affirmations soient un peu douteuses quant à la sécurité, l'idée reste ici bien valide il faut voir le point de vue de notre « ennemis » et les failles de notre système et comprendre les vecteurs d'attaque possible afin de former au mieux nos « alliés » à pallier ce danger.

Pour ce faire, nous allons étudier en détails les vecteurs d'attaque les plus communs dans un système d'information.

Liste des dangers les plus communs pour les S.I :

1. **Hameçonnage (Phishing)** : Tentatives d'obtenir des informations sensibles en se faisant passer pour une entité de confiance.
2. **Attaque par déni de service (DDoS)** : Inonde un système avec un volume de données trop important pour qu'il puisse y répondre ou fonctionner normalement.
3. **Attaque par injection SQL** : Insertion de code malveillant dans une base de données via une faille dans le traitement des requêtes SQL.
4. **Attaque par force brute** : Tentatives répétées de deviner un mot de passe ou une clé cryptographique.
5. **Malware** : Logiciel malveillant conçu pour endommager ou exploiter un système informatique.
6. **Ransomware** : Type de malware qui crypte les données de l'utilisateur et exige une rançon pour les débloquent.
7. **Ingénierie sociale** : Manipulation des personnes pour obtenir des informations confidentielles.
8. **Attaque par homme du milieu (MitM)** : Intercepte et modifie la communication entre deux parties sans leur consentement.
9. **Zero-day exploit** : Exploite une vulnérabilité inconnue des développeurs du logiciel ou du système.
10. **Attaque sur le réseau sans fil (Wi-Fi eavesdropping)** : Écoute clandestine sur un réseau sans fil pour voler des informations.
11. **Cross-site scripting (XSS)** : Injecte du code malveillant dans des sites web pour l'exécuter dans le navigateur de l'utilisateur.
12. **Drive-by download** : Téléchargement automatique de malware lors de la visite d'un site web compromis.
13. **Attaque par répudiation** : Destruction des journaux pour empêcher le suivi des activités malveillantes.
14. **Spoofing** : Usurpation d'identité ou d'adresse IP pour gagner la confiance ou accéder à un réseau.
15. **Attaque de l'intercepteur de clavier (Keylogger)** : Surveillance des frappes au clavier pour voler des informations telles que les identifiants de connexion.

16. **Attaque de logique d'application** : Exploite la logique d'une application pour effectuer des opérations non prévues par le développeur.
17. **Attaque de l'annuaire (Directory traversal)** : Accède aux fichiers stockés en dehors de la racine du serveur web.
18. **Session hijacking** : Exploitation d'une session utilisateur valide pour obtenir un accès non autorisé.
19. **Cryptojacking** : Utilisation non autorisée des ressources informatiques d'une victime pour miner des cryptomonnaies.
20. **Attaque de dépôt de fichiers (File dumping)** : Accès non autorisé et récupération de fichiers à partir de systèmes compromis.

Toutes les attaques **surlignées en jaune** sont des attaques qui peuvent être en partie causées par une interaction utilisateur.

Comme vous pouvez le voir, beaucoup de celles-ci sont causées directement ou indirectement par l'utilisateur, elles représentent donc en même temps, les erreurs les plus simples à corriger, mais les plus difficiles. En effet, il faut mettre en place tout un programme d'entraînement des utilisateurs du SI pour assurer que le réseau est utilisé correctement et de manière sécurisée.

Propositions

Nous pouvons remarquer dans cette liste qu'il y a 3 grands vecteurs d'attaque qui peuvent être utilisés par nos utilisateurs pour s'infiltrer dans le réseau :

- Les attaques logicielles : tout type de virus téléchargeable
- Les attaques physiques : les intrusions dans les bureaux
- Les attaques visant le manque de formation : phishing et autres attaques spécialisées dans la manipulation des utilisateurs.

Afin de mettre en place une formation couvrant tous les points que les utilisateurs doivent connaître, nous devons établir des procédures de formation. Pour ce faire, nous proposons une formation complète en trois étapes :

Etape 1 : Test des failles actuels dans l'entreprise :

Dans le cadre de notre test de sécurité nous tenterons au cours des 2 prochains mois d'accéder aux systèmes de l'entreprise en utilisant différents moyens :

- **Phishing** :
 - Description : Tentatives d'obtenir des informations sensibles (comme les identifiants de connexion et les mots de passe) en se faisant passer pour une entité de confiance via des communications électroniques.

- Méthodologie : Envoi d'e-mails ou de messages ciblés qui semblent provenir de sources légitimes (par exemple, la direction de l'entreprise, des partenaires commerciaux) pour inciter les employés à divulguer des informations confidentielles.
 - Objectifs : Évaluer la sensibilisation du personnel aux tentatives d'hameçonnage et la robustesse des protocoles de sécurité en place pour prévenir de telles attaques.
- **Piratage par envoi de pièces jointes frauduleuses ou site web infecté :**
- Description : Utilisation de logiciels malveillants dissimulés dans des pièces jointes ou via des sites web compromis pour infiltrer le réseau de l'entreprise.
 - Méthodologie : Création de documents ou de liens apparemment inoffensifs qui, une fois ouverts ou cliqués, installent des logiciels malveillants permettant l'accès non autorisé au réseau de l'entreprise.
 - Objectifs : Tester la capacité des systèmes de sécurité de l'entreprise à détecter et à neutraliser les logiciels malveillants et évaluer l'efficacité des formations des employés à reconnaître et à éviter les menaces potentielles.
- **Accès physique aux bureaux pour obtenir des informations :**
- Description : Tentative d'accès non autorisé aux locaux de l'entreprise pour obtenir des informations sensibles ou accéder directement aux systèmes informatiques.
 - Méthodologie : Utilisation de techniques telles que le tailgating (suivre quelqu'un pour entrer dans un espace sécurisé) ou le social engineering (manipuler les employés pour qu'ils accordent un accès physique) pour pénétrer dans les locaux.
 - Objectifs : Évaluer la sécurité physique des bureaux, y compris les contrôles d'accès, la surveillance et la sensibilisation du personnel à la sécurité.

Etape 2 : Formation des employés sur site

Afin de garantir que tous les employés soient conscients des risques liés à l'informatique, il serait judicieux d'organiser une journée de sensibilisation. Cette journée mettra l'accent sur les dangers informatiques et les bonnes pratiques à adopter. L'objectif est de s'assurer que les employés comprennent ces risques et soient en mesure d'agir en connaissance de cause.

Pour renforcer l'impact de cette formation et sensibiliser davantage les employés, nous envisageons de présenter un reportage détaillant diverses méthodes utilisées pour infiltrer notre système. Ce reportage servira d'exemple concret pour illustrer la réalité des menaces.

Durant cette formation, il sera crucial d'aborder plusieurs points clés :

Pratiques Sécurisées en Ligne :

- **Prudence avec les e-mails et pièces jointes :** Apprendre aux utilisateurs à ne pas ouvrir des pièces jointes ou cliquer sur des liens dans des emails non sollicités ou suspects.

- **Utilisation sécurisée des navigateurs** : Encourager l'utilisation de fonctionnalités de sécurité dans les navigateurs, comme les avertissements de sites web non sécurisés ou frauduleux.

Gestion des Mots de Passe :

- **Utilisation de mots de passe forts** : Former les utilisateurs à créer des mots de passe robustes et uniques pour chaque compte.
- **Changement régulier des mots de passe** : Encourager les utilisateurs à changer leurs mots de passe régulièrement et à ne jamais les partager.

Sécurité des Appareils Personnels :

- **Protection des appareils mobiles** : Sensibiliser les utilisateurs à l'importance de sécuriser leurs appareils mobiles, notamment par des mots de passe, la reconnaissance faciale ou les empreintes digitales.
- **Mise à jour des appareils personnels** : Encourager les utilisateurs à maintenir leurs appareils personnels à jour avec les derniers systèmes d'exploitation et logiciels de sécurité.

Réseau Sécurisé :

- **Utilisation prudente des réseaux Wi-Fi publics** : Éduquer les utilisateurs sur les risques des réseaux Wi-Fi publics et promouvoir l'utilisation de réseaux privés virtuels (VPN) lors de l'accès à des informations sensibles.

Sensibilisation aux Médias Sociaux :

- **Prudence sur les réseaux sociaux** : Informer les utilisateurs des risques liés au partage d'informations sensibles sur les réseaux sociaux et les sensibiliser à l'importance de la confidentialité et des paramètres de sécurité.

Reporting et Réaction aux Incidents :

- **Encouragement au reporting** : Inciter les utilisateurs à signaler immédiatement toute activité suspecte ou tout problème de sécurité à l'équipe IT.
- **Connaissance des procédures d'urgence** : Assurer que tous les utilisateurs connaissent les procédures à suivre en cas de détection d'une menace ou d'une violation de la sécurité.

Etape 3 : évaluation des améliorations

Afin d'évaluer l'efficacité de la formation, il est crucial de procéder à un nouveau test du système. Nous envisageons donc d'attendre entre 3 et 4 mois avant de tenter à nouveau une infiltration.

Après cette tentative, nous évaluerons les performances des utilisateurs face à nos attaques. Cela nous permettra de vérifier s'il y a eu une amélioration notable. Si nécessaire, nous élaborerons un plan de remédiation spécifiquement adapté aux services les plus vulnérables ou les plus affectés.

V. Devis et coût

Devis

Ces améliorations et propositions vont couter de l'argent. Le cout dépend de la technologie souhaitée et de la période d'utilisation.

Cout de Windows Server 2022

Nous ne pouvons actuellement qu'acheter les licences de Windows Serveur 2022, nous allons donc substituer son prix avec celui de Windows Serveur 2019.

Édition de Windows Server 2022	Idéal pour	Modèle de licences	Conditions relatives aux licences d'accès client ^[1]	Prix de détail suggéré (PDSF) ^[4]
Centre de données ^[2]	Centres de données et environnements cloud hautement virtualisés	Basé sur les cœurs	Licence d'accès client Windows Server	6 155 \$
Standard ^[2]	Environnements physiques ou faiblement virtualisés	Basé sur les cœurs	Licence d'accès client Windows Server	1 069 \$
Essentials	Petites entreprises avec jusqu'à 25 utilisateurs et 50 appareils	Serveurs spécialisés (licence serveur) ^[3]	Aucune licence d'accès client n'est obligatoire	501 \$

Figure 11: Tarification Windows Server 2022 [1]

Cout de Licence Windows 10 Pro

Professionnel



Windows 10

Microsoft

WINDOWS 10 PROFESSIONNEL - (64BITS)

99,00 € TTC

~~189,95 € TTC~~

-90,95 €

82,50 € HT

- ✓ Licence d'activation type OEM (avec mises à jour)
- ✓ Fichier d'installation ISO de Windows (64 bits)
- ✓ Version Multilingue & Française
- ✓ Support technique inclus 7/7 + guide d'installation et activation
- ✓ Licence et lien de téléchargement livrés par mail 24h/24

Quantité :

Figure 22: Tarification Windows 10 pro [2]

Authentification

Afin de donner un accès rapide et sécurisé à nos utilisateurs, nous proposons l'utilisation de la reconnaissance faciale Windows hello, afin d'utiliser cette méthode d'authentification, il nous faut du matériel adapté s'il ne l'est pas déjà : une webcam compatible Windows Hello.

Nous proposons donc le produit suivant :

Livraison Rapide

Webcam Lenovo Performance Full HD

★★★★★ 4.5 (4)

Référence : 4XC1D66055

74,00 €


TVA incluse

Ajouter au panier

Départ livraison dans 1-2 jours ouvrés

Gagnez 1€ en récompenses [S'inscrire maintenant !](#)

☐ Comparer



● ○ ○ ○ ○ ○ ○ ○

Figure 23: Webcam Lenovo [3]

Pour 74€ par post, cette webcam offre une qualité FHD pour les meetings en ligne et est compatible avec Windows hello.

Prenant en compte que nous aurons un total de 100 posts, Nous devons allouer un budget de 7400 euros pour équiper toute l'entreprise en webcam

Le produit est disponible à l'adresse suivante :

https://www.lenovo.com/fr/fr/p/accessories-and-software/webcams-and-video/webcams-and-video_webcams/4xc1d66055

Anti-virus

Nous allons utiliser un antivirus dans chaque machine pour mieux sécuriser notre environnement, éviter toute probabilité d'attaque et protéger le flux des données entre deux machines et entre le serveur et les machines.

Nous allons utiliser l'antivirus ESET qui est fiable et sécurisé et a de nombreux avantages dont :

- **Protection Proactive** : ESET est réputé pour sa protection proactive, comprenant des capacités avancées d'heuristique et d'analyse comportementale, permettant de détecter et bloquer les menaces émergentes avant qu'elles ne puissent causer des dommages.
- **Léger et Efficace** : ESET est conçu pour être léger et efficient en termes de ressources système. Il vise à fournir une sécurité robuste sans affecter significativement les performances de votre ordinateur.
- **Détection Efficace des Logiciels Malveillants** : L'antivirus ESET est reconnu pour son efficacité à détecter un large éventail de logiciels malveillants, y compris les virus, chevaux de Troie, rançongiciels et autres types de logiciels malveillants.
- **Anti-Phishing et Anti-Spam** : ESET inclut souvent des fonctionnalités pour se protéger contre les attaques de phishing et les courriels indésirables, aidant les utilisateurs à éviter de tomber victimes de sites Web frauduleux et d'arnaques par hameçonnage.
- **Contrôle des Périphériques** : Certains produits ESET offrent des fonctionnalités de contrôle des périphériques, permettant aux utilisateurs de gérer et contrôler les dispositifs externes connectés à leur ordinateur, ajoutant une couche de sécurité supplémentaire.
- **Protection Pare-feu** : ESET Internet Security et les produits associés comprennent généralement un pare-feu qui surveille et contrôle le trafic réseau, offrant une protection supplémentaire contre les accès non autorisés.
- **Mises à Jour Régulières** : ESET met régulièrement à jour sa base de données de signatures de virus et son logiciel pour assurer une protection contre les dernières menaces. Les mises à jour régulières sont cruciales pour une sécurité efficace.
- **Interface Conviviale** : Les produits ESET présentent souvent des interfaces conviviales, facilitant la navigation et la gestion des paramètres de sécurité pour les utilisateurs.
- **Support de Plusieurs Plateformes** : ESET propose des solutions de sécurité pour différentes plateformes, notamment Windows, macOS, Android et Linux, offrant une approche complète de la sécurité multi-appareils.
- **Sécurité des Transactions Bancaires et des Achats en Ligne** : Certains produits ESET incluent des fonctionnalités spécifiquement conçues pour sécuriser les transactions en ligne, protégeant les utilisateurs lors des opérations bancaires et des achats en ligne.

ESET est donc un choix fiable, sécurisé et compatible avec Windows et Linux. Il est donc adapté avec nos besoins.

	eset PROTECT ENTRY	eset PROTECT ADVANCED	RECOMMANDÉE eset PROTECT COMPLETE	eset PROTECT ELITE
	Protection moderne multicouche de vos endpoints couplée avec du machine learning puissant et facile à administrer	la meilleure protection des endpoints contre les ransomwares et les menaces de type "zero-day", soutenue par une puissante sécurité des données	Sécurité des applications dans le Cloud, des endpoints et des emails grâce à une protection multicouche	Prévention, détection et réponse tout-en-un combinant une technologie XDR de haut niveau et une protection multicouche complète
Console ①	✓	✓	✓	✓
Protection moderne pour endpoint ①	✓	✓	✓	✓
Protection des serveurs ①	✓	✓	✓	✓
Chiffrement des données ①	✗	✓	✓	✓
Sandboxing Cloud ①	✗	✓	✓	✓
Protection des applications Cloud ①	✗	✗	✓	✓
Protection des serveurs de messagerie ①	✗	✗	✓	✓
Vulnérabilité & patch management ①	✗	✗	✓	✓
Détection & Réponse ①	✗	✗	✗	✓
Authentification Multifacteur ①	+	+	+	✓
Managed Detection & Response (MDR) ①	+	+	+	+
	<div> <div>5</div> <div>+</div> </div> <div>APPAREILS</div> <div>1</div> <div>+</div> <div>ANNÉE</div> <div>182,50€ HT</div>	<div> <div>5</div> <div>+</div> </div> <div>APPAREILS</div> <div>1</div> <div>+</div> <div>ANNÉE</div> <div>237,50€ HT</div>	<div> <div>5</div> <div>+</div> </div> <div>APPAREILS</div> <div>1</div> <div>+</div> <div>ANNÉE</div> <div>292,00€ HT</div>	Laissez-nous vos coordonnées pour recevoir une offre qui correspond aux besoins de votre entreprise
	J'ACHÈTE	J'ACHÈTE	J'ACHÈTE	CONTACTEZ-NOUS
	OBTENIR UNE VERSION D'ESSAI	OBTENIR UNE VERSION D'ESSAI	OBTENIR UNE VERSION D'ESSAI	En savoir plus
	Déjà client ? Renouvelez votre licence	Déjà client ? Renouvelez votre licence	Déjà client ? Renouvelez votre licence	

Figure 24: Tarification de ESET [4]

Routeur / Pare-feu

Pour le pare-feu, nous avons utilisé Pfsense qui est une technologie gratuite mais a des limites et pour une société comme Abstergo nous devrions utiliser un routeur/pare-feu qui est performant, fiable et capable de supporter les serveurs et les machines des employés.

La proposition de notre équipe technique est celle de Cisco la fameuse entreprise informatique spécialisée en matériel du réseau.

On va choisir le routeur/pare-feu **Cisco FirePOWER 1010 ASA – firewall**

1. Fiche technique globale

Tableau 1: Fiche technique Cisco FirePower

Description du produit	Cisco FirePOWER 1010 ASA – firewall
Type de périphérique	Firewall
Format	Bureau
Disque dur	200 Go x 1
Performances	Débit du pare-feu (UDP) : 2 Gbps Débit de pare-feu multi-protocole : 1,4 Gbps Débit VPN IPsec (test 450B UDP L2L) : 500 Mbps
Capacité	Connexions simultanées : 100000 Nouvelles connexions par seconde : 25000 Homologues VPN : 75
Alimentation	CA 120/230 V (50/60 Hz)
Dimensions (LxPxH)	19.9 cm x 20.5 cm x 4.62 cm
Poids	1.36 kg
Garantie du fabricant	90 jours de garantie

2. Éléments Clés

Cisco FirePOWER 1010 ASA - Firewall – bureau offre en particulier:

- Une protection contre les menaces avancées
- Des performances exceptionnelles et une haute fiabilité
- Une inspection renforcée du trafic chiffré
- La puissance de la gamme

Voici quelques-uns des avantages de Cisco FirePOWER :

- **Idéal pour les collaborateurs travaillant à distance** : Prise en charge pré-intégrée des fonctionnalités de sécurité Cisco supplémentaires, notamment le VPN d'accès à distance Cisco anyconnect et l'authentification multifacteur Duo de Cisco.
- **Silencieux** : Compact et sans ventilateur, ce pare-feu est idéal pour les petits bureaux et les espaces de travail.
- **Performances sans compromis** : Les pare-feux de la gamme Firepower 1000 sont équipés de fonctions d'accélération matérielle, qui permettent de maintenir les performances du pare-feu dans toutes les conditions.
- **Configurable** : Grâce au logiciel de base FTD disponible, ajoutez une fonction d'inspection du contenu basée sur le réseau, un système de prévention des intrusions et un filtrage des URL.

- Firepower Threat Defense (FTD) est un système intégré de prévention des intrusions (IPS), de détection de logiciels malveillants (malware) et de gestion des politiques de sécurité proposé par Cisco. Il est souvent intégré aux appareils de sécurité réseau, tels que les pare-feux, pour fournir des fonctionnalités avancées de sécurité.

Cisco FirePOWER 1010 ASA – firewall



CISCO Référence : FPR1010-ASA-K9

1325.76 € HT
prix public conseillé dont 0.00 € d'écopart DEEE
1590.91 € TTC

En stock : 210 pièces,
pour plus d'informations nous contacter

Devis et prix remisé

Afficher les brochures et manuels du produit

24/48h Tarifs BtoB Spécialistes dédiés Haut niveau de certifications

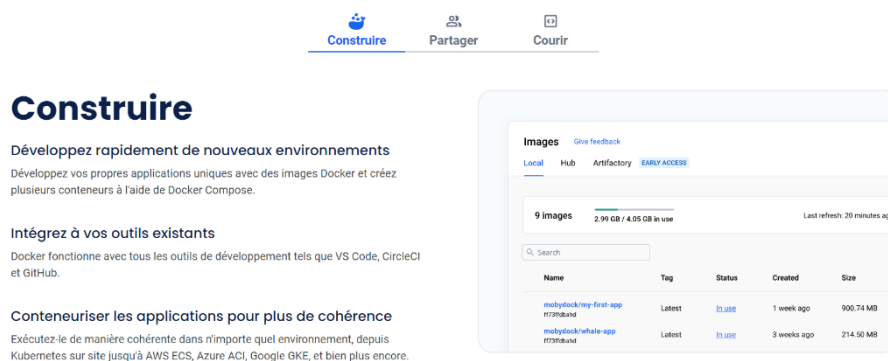
Figure 25: Tarification de Cisco Firewall [5]

Le choix de Cisco est fait par rapport aux futurs besoins d'Abstergo.

CONTENURISATION

Nous devons conteneuriser les données de système d'ABSTERGO, nous allons créer une image et déployer plus rapidement sur demande, l'environnement de conteneurisation nous permet de garantir une grande flexibilité et éviter les surprises lors de l'échange entre les utilisateurs, on parle de dépendances et de détails ça permet de faciliter l'utilisation pour les développeurs et même les normaux utilisateurs.

En cette partie on a travaillé avec la technologie la plus fameuse : Docker. Voici ce qu'elle permet de faire :



Construire Partager Courir

Développez rapidement de nouveaux environnements
Développez vos propres applications uniques avec des images Docker et créez plusieurs conteneurs à l'aide de Docker Compose.

Intégrez à vos outils existants
Docker fonctionne avec tous les outils de développement tels que VS Code, CircleCI et GitHub.

Conteneuriser les applications pour plus de cohérence
Exécutez-le de manière cohérente dans n'importe quel environnement, depuis Kubernetes sur site jusqu'à AWS ECS, Azure ACI, Google GKE, et bien plus encore.

Images Give feedback

Local Hub Artifactory **EARLY ACCESS**

9 images 2.96 GB / 4.05 GB in use Last refresh: 20 minutes ago

Name	Tag	Status	Created	Size
mobydock/tey-first-app	Latest	DLING	1 week ago	900.74 MB
mobydock/whale-app	Latest	DLING	3 weeks ago	214.50 MB

Figure 26: Construire des conteneurs et des images [6]

Partager

Créez avec du contenu vérifié et fiable

Visitez Docker Hub pour parcourir le contenu Docker de confiance de nos éditeurs vérifiés ou des images officielles Docker.

Collaborez avec votre équipe

Extrayez et publiez des images depuis Hub pour un partage facile entre les membres de l'équipe, les organisations ou la communauté au sens large.

Sécurisez vos espaces de travail

Garantissez les meilleures pratiques en matière de gestion de l'accès aux images, de gestion de l'accès au registre et aux référentiels privés.

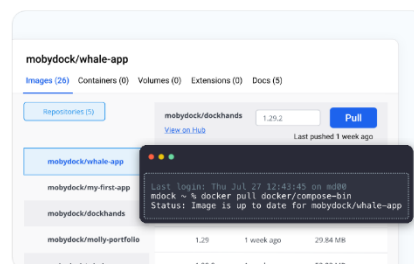


Figure 27: Partager [6]

Courir

Livraison cohérente des applications

Expédiez vos applications en sachant qu'elles fonctionneront de la même manière dans n'importe quel environnement, localement ou dans le cloud.

Développer avec polyvalence

Déployez des applications dans des conteneurs isolés avec prise en charge multilingue, réduisant ainsi les conflits entre les dépendances des applications.

Déployer avec une seule commande

Travaillez dans la CLI Docker Compose pour accélérer le développement et lancer vos applications avec une seule commande.

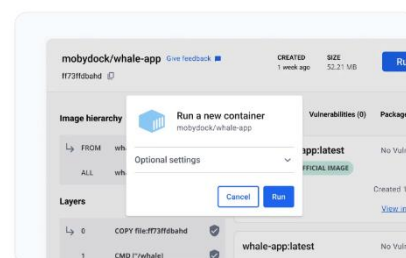


Figure 28: Courir [6]

On va utiliser le Docker Business car il offre beaucoup des avantages par rapport à les autres versions et convenable avec notre utilisation d'Abstergo

Personnel	Pro	Équipe	Entreprise
Idéal pour les développeurs individuels, l'éducation et les communautés open source.	Comprend des outils professionnels pour les développeurs individuels qui souhaitent accélérer leur productivité.	Pour les petites équipes nécessitant des outils de collaboration et de productivité.	Idéal pour les entreprises recherchant une gestion centralisée et des capacités de sécurité avancées.
0 \$	5 \$ par mois	9 \$ par utilisateur* par mois	24 \$ par utilisateur* par mois
<ul style="list-style-type: none"> ✓ Bureau Docker ✓ Dépôts publics illimités ✓ Moteur Docker + Kubernetes ✓ 200 images extraites toutes les 6 heures ✓ Jetons à portée illimitée 	Tout dans Personnel plus : <ul style="list-style-type: none"> ✓ Dépôts privés illimités ✓ 5 000 images extraites par jour ✓ 5 versions simultanées ✓ 300 analyses de vulnérabilités du Hub 	Tout dans Pro plus : <ul style="list-style-type: none"> ✓ Jusqu'à 100 utilisateurs ✓ Équipes illimitées ✓ 15 builds simultanées ✓ Analyses de vulnérabilités illimitées du Hub ✓ Ajouter des utilisateurs en masse ✓ Journaux d'audit 	Tout dans Team plus : <ul style="list-style-type: none"> ✓ Utilisateurs illimités ✓ Bureau Docker renforcé ✓ Gestion centralisée ✓ Gestion de l'accès au registre ✓ Authentification unique (SSO) ✓ Provisionnement des utilisateurs SCIM ✓ Prise en charge du VDI ✓ Achat via facture
Commencez maintenant	Acheter maintenant	Acheter maintenant	Contacter le service commercial Acheter maintenant

Figure 29: Tarification de Docker [7]

On va aussi citer quelques éléments clés pour le choix de Docker Business.

- La gestion de l'image, les dépôts publics et privée sont illimitées.
- La gestion des utilisateurs dont les collaborateurs du référentiel public et les jetons d'accès sont illimitées et les collaborateurs du référentiel privée sont jusqu'à la taille de l'entreprise.

- Le taux d'extraction d'images pour les utilisateurs authentifiés jusqu'à 5000 par jour.

AUTOMATISATION

L'automatisation désigne le processus de réalisation d'une tâche, d'une opération ou d'un processus sans intervention humaine directe. Cela implique l'utilisation de systèmes, de logiciels ou de technologies pour exécuter des actions de manière programmée et répétitive, en suivant des règles prédéfinies. L'objectif principal de l'automatisation est d'améliorer l'efficacité, la rapidité, la cohérence et la fiabilité des opérations.

On va utiliser la technologie Ansible pour l'automatisation. Voici ces avantages [8] :

- **Automatisation simplifiée** : Ansible est une plateforme simple d'utilisation, facile à installer, à configurer et à maîtriser. En moins de 30 minutes, il est possible d'installer et de configurer le système et d'exécuter des commandes ad hoc pour les serveurs pour résoudre un problème spécifique : réglage de l'heure d'été, synchronisation de l'heure d'été, modification du mot de passe racine, mise à jour des serveurs, redémarrage des services, etc.
- **Courbe d'apprentissage basse** : Ansible est facile à déployer, car il n'utilise aucun agent ni aucune infrastructure de sécurité personnalisée supplémentaire. Ansible s'appuie également sur YAML, un langage simple pour décrire votre travail d'automatisation via les playbooks. Les playbooks poussent les paramètres souhaités sur les hôtes définis dans l'inventaire et peuvent même être exécutés ad hoc (via la ligne de commande, sans définition dans les fichiers).
- **Automatisation immédiate** : Dès le moment où vous pouvez envoyer une requête ping aux hôtes via Ansible, vous pouvez commencer à automatiser votre environnement. Commencez par de petites tâches, suivez les bonnes pratiques, hiérarchisez les tâches sources de valeur pour l'entreprise, résolvez des problèmes majeurs, gagnez du temps et améliorez la productivité.

Liste de Prix Publics H.T. conseillés au 01/05/2023

modifiable sans préavis.

Souscription	Référence	Tarif 1 an	Tarif 3 ans
Red Hat Ansible Automation, Standard (100 Managed Nodes)	MCT3691	10 400 €	28 080 €
Red Hat Ansible Automation, Standard (5 000 Managed Nodes)	MCT3692	448 000 €	1 209 600 €
Red Hat Ansible Automation, Standard (10 000 Managed Nodes)	MCT3693	896 000 €	2 419 200 €
Red Hat Ansible Automation, Premium (100 Managed Nodes)	MCT3694	14 000 €	37 800 €
Red Hat Ansible Automation, Premium (5 000 Managed Nodes)	MCT3695	600 000 €	1 620 000 €
Red Hat Ansible Automation, Premium (10 000 Managed Nodes)	MCT3696	1 200 000 €	3 240 000 €

2 niveaux de services incluent de l'assistance technique via le portail web Red Hat et par téléphone

- Standard avec une assistance du lundi au vendredi de 9h à 17h,
- Premium avec une assistance 7j/7 24h/24.

Figure 30: Tarification Ansible [9]

Nodes fait références au nombre d'appareils ou de systèmes que vous êtes autorisées à gérer avec une licence.

On va choisir jusqu'à 100 licences nodes par rapport à notre besoin d'Abstergo qui a deux sites Paris et Lyon.

SUPERVISION

La supervision est une technique industrielle de suivi et de pilotage informatique de procédés de fabrication automatisés. La supervision concerne l'acquisition de données (mesures, alarmes, retour d'état de fonctionnement) et des paramètres de commande des processus généralement confiés à des automates programmables. [10]

Pour bien assurer la supervision de notre système d'information Abstergo on a choisi l'un de plus fameuses technologies qui est Centreon.

On utilise la fameuse technologie qui est gratuite le Centreon.

Facture

NB : Admin système et maintenance par mois

EQUIPE TECHNIQUE CESI

FACTURE

distribuée à

Animus Company
Date: 14 Nov 2023

De

Equipe Technique Cesi
93 Boulevard de la seine , Nanterre ,
92000

DESCRIPTION	Quantite	Prix/unite	Prix Total
Administrateur systeme	1	2916.66	2916.66
Licence Windows 10 Pro	100	99	9900
Licence Windows Server 2022 STA	1	1069	1069
Webcam Lenovo Full Hd	100	74	7400
Cisco FirePower1010 ASA	1	1325.76	1325.76
Docker Entreprise	100/mois	24	2400
Ansible Standard	1/an	10400	10400
Moniteur de performance reseau NPM	1	1785	1785

DESCRIPTION	Quantite	Prix/unite	Prix Total
Maintenance de materiel et logiciels	1/mois	400	400
TOTAL			37,599.42

NB : Admin système et maintenance par an

Le paiement est requis dans les 14 jours
ouvrables à compter de la date de la
facture. Veuillez envoyer le règlement à
l'adresse suivante : equipetech@viacesi.fr
Nous vous remercions de votre
collaboration.


Equipe Technique

EQUIPE TECHNIQUE CESI

FACTURE

distribuée à

Animus Company
Date: 14 Nov 2023

De

Equipe Technique Cesi
93 Boulevard de la seine , Nanterre ,
92000

DESCRIPTION	Quantite	Prix/unite	Prix Total
Administrateur systeme	1	35000	35000
Licence Windows 10 Pro	100	99	9900
Licence Windows Server 2022 STA	1	1069	1069
Webcam Lenovo Full Hd	100	74	7400
Cisco FirePower1010 ASA	1	1325.76	1325.76
Docker Entreprise	100/mois	24	2400
Ansible Standard	1/an	10400	10400
Moniteur de performance reseau NPM	1	1785	1785

DESCRIPTION	Quantite	Prix/unite	Prix Total
Maintenance de materiel et logiciels	1/an	4800	4800
TOTAL			74100.75

VI. Améliorations Possibles

Active Directory :

On peut utiliser l'Active Directory et ses domaines gratuitement donc on peut les déployer sur les machines et les partager mais parlant de votre société qui a des branches et beaucoup d'employées et clients on conseille d'utiliser Azure Active Directory qui est déployer en cloud et on peut les utiliser et les accéder facilement et elle est performante

Le paiement est requis dans les 14 jours ouvrables à compter de la date de la facture. Veuillez envoyer le règlement à l'adresse suivante : equipetech@viacesi.fr
Nous vous remercions de votre collaboration.



Equipe Technique

Vous trouverez ci-dessous un tableau explicatif de cout d’Azure Active Directory

	Standard	Entreprise	Prime
Service de base AAD DS			
Charge d'authentification suggérée (pic, par heure) ¹	0 à 3 000	3 000 à 10 000	10 000 à 70 000
Nombre d'objets suggéré ²	0 à 25 000	25 000 à 100 000	100 000 à 500 000
Fréquence de sauvegarde	Tous les 5 jours	Tous les 3 jours	Quotidien ³
Instances			
Domaine géré ⁴	0,15 \$ /heure/ensemble	0,40 \$ /heure/ensemble	1,60\$ /heure/ensemble
Caractéristiques			
Les répliques		✓	✓
Options de synchronisation supplémentaires ⁵		✓	✓

Figure 31: Tarification Azure Active Directory [11]

Pour le serveur nous allons utiliser Windows Server 2019 et pour le Windows Client nous allons utiliser Windows 10 Professionnel d’où l’achat des licences de Microsoft pour chaque machine.

DNS

DNS signifie Domain Name System, ou système de nom de domaine, en Français. Derrière ce terme vague, ce service informatique né dans les années 80 permet de lier le nom d’un site web à son adresse informatique : son adresse IP.

On va utiliser Google Public Dns qui est parmi des meilleurs et a beaucoup d’avantages dont :

- **Rapidité** : Google Public DNS est connu pour sa rapidité. Il a des serveurs DNS mondiaux bien répartis, ce qui peut entraîner des temps de résolution de noms de domaine plus rapides par rapport aux serveurs DNS fournis par certains fournisseurs d'accès Internet (FAI).
- **Stabilité** : Les serveurs DNS de Google sont généralement stables et fiables, ce qui contribue à minimiser les interruptions de service lors de la résolution des noms de domaine.
- **Sécurité** : Google Public DNS prend en charge DNS over HTTPS (DoH) et DNS over TLS (DoT), ce qui ajoute une couche de chiffrement à la communication DNS, renforçant ainsi la confidentialité et la sécurité.
- **Blocage de Logiciels Malveillants** : Google Public DNS a des fonctionnalités intégrées pour bloquer l'accès à des domaines connus pour héberger des logiciels malveillants. Cela peut contribuer à protéger les utilisateurs contre les menaces en ligne.
- **Facilité de Configuration** : La configuration de Google Public DNS est simple. Les utilisateurs peuvent facilement définir les adresses IP des serveurs DNS de Google dans les paramètres réseau de leur appareil.
- **Accessibilité Mondiale** : Google Public DNS est accessible de manière mondiale, ce qui signifie que les utilisateurs du monde entier peuvent bénéficier de ses fonctionnalités sans restriction géographique.

- **Compatibilité** : Il est compatible avec la plupart des systèmes d'exploitation et des appareils, ce qui permet aux utilisateurs de l'intégrer facilement dans leur configuration réseau, que ce soit sur des ordinateurs, des smartphones, des routeurs, etc.
- **Politiques de Confidentialité Clair** : Google Public DNS a des politiques de conservation des données claires. Selon Google, les journaux d'accès sont supprimés après un certain temps, ce qui peut rassurer ceux qui sont préoccupés par la confidentialité.
- **DNSSEC (DNS Security Extensions)** : Google Public DNS prend en charge DNSSEC, une extension de sécurité du DNS qui vise à authentifier les données DNS afin de garantir leur intégrité.
- **Disponibilité Continue** : En tant que service géré par Google, Google Public DNS bénéficie généralement d'une disponibilité continue, minimisant ainsi les temps d'indisponibilité potentiellement rencontrés avec d'autres serveurs DNS.

Nous choisissons le Google Public Dns Cloud pour que tous les éléments du système d'information doivent être cohérents et nous pourrions déployer tout le système sur cloud pour le manipuler à distance et avoir une copie de backup sur le cloud est très important dans nos jours.

Le tableau suivant présente des modèles d'utilisation de Cloud DNS et leurs coûts potentiels par mois :

Utilisation	Site Web standard	Entreprise	Fournisseur d'hébergement virtuel sur le Web
Zones	5	200	100 000
Coût des zones	5 x 0,20 \$ = 1,00 \$	25 x 0,20 \$ = 5 \$ 175 x 0,10 \$ = 17,50 \$	25 x 0,20 \$ = 5 \$ 9 975 x 0,10 \$ = 997,50 \$ 90 000 x 0,03 \$ = 2 700 \$
Requêtes par mois	10 000 000	50 000 000	100 000 000
Coût des requêtes	10 x 0,40 \$ = 4,00 \$	50 x 0,40 \$ = 20,00 \$	100 x 0,40 \$ = 40,00 \$
Coût total	5 \$/mois	42,50 \$/mois	3 742,50 \$/mois

Figure 32: Tarification de Cloud DNS [12]

VPN

Le VPN (Virtual Private Network) est un système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics. On a travaillé avec OpenVPN sur notre pare-feu Pfsense, mais pour bien sécuriser et pour que le VPN soit fiable et performant avec les besoins de société Abstergo on va mettre l'accent sur un autre VPN qui est le Azure VPN.

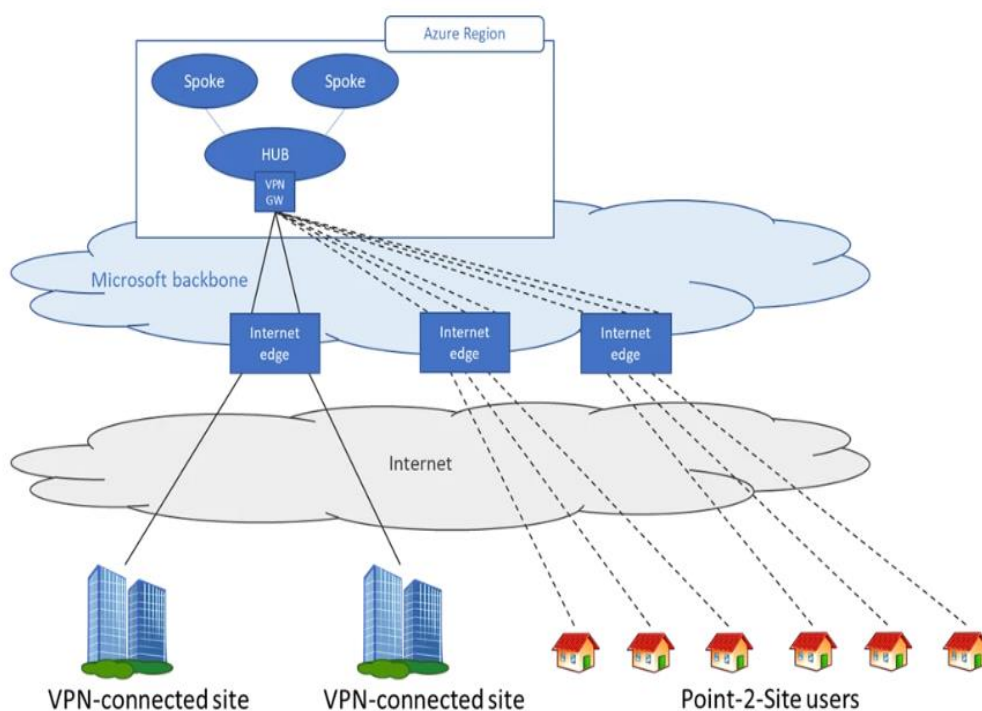


Figure 24 : Fonctionnement de Azure VPN [13]

Le cout du VPN va dépendre de la bande passante l'intervalle de fréquences dans lequel l'affaiblissement du signal est inférieur à une valeur spécifiée et les Tunnels.

Type de passerelle VPN	Tarif	Bande passante	Tunnels S2S	Tunnels P2S
Basic	\$0,04/heure	100 Mbits/s	maximum 10 1-10 : Inclus	maximum 128 1-128 : Inclus
VpnGw1	\$0,19/heure	650 Mbits/s	maximum 30 1-10 : Inclus 11-30: \$0,015/heure par tunnel	maximum 250 1-128 : Inclus 129-250: \$0,01/heure par connexion
VpnGw2	\$0,49/heure	1 Gbits/s	maximum 30 1-10 : Inclus 11-30: \$0,015/heure par tunnel	maximum 500 1-128 : Inclus 129-500: \$0,01/heure par connexion
VpnGw3	\$1,25/heure	1.25 Gbits/s	maximum 30 1-10 : Inclus 11-30: \$0,015/heure par tunnel	maximum 1 000 1-128 : Inclus 129-1 000: \$0,01/heure par connexion
VpnGw4	\$2,10/heure	5 Gbits/s	maximum 100 1-10 : Inclus 11-100: \$0,015/heure par tunnel	maximum 5 000 1-128 : Inclus 129-5 000: \$0,01/heure par connexion
VpnGw5	\$3,65/heure	10 Gbits/s	maximum 100 1-10 : Inclus 11-100: \$0,015/heure par tunnel	maximum 10 000 1-128 : Inclus 129-10 000: \$0,01/heure par connexion

Figure 33: Tarification de Azure VPN

Supervision

Pour bien améliorer le système d'information Abstergo, on va utiliser une technologie performante et assez compatible avec nos besoins car on met l'accent toujours sur la taille de société et qu'il y a deux serveurs distants l'un à Paris et l'autre à Lyon, on va utiliser la technologie SolarWinds .

On va utiliser le produit Surveillance des performances du Réseau (en anglais : SolarWinds Network Performance Monitor NPM).

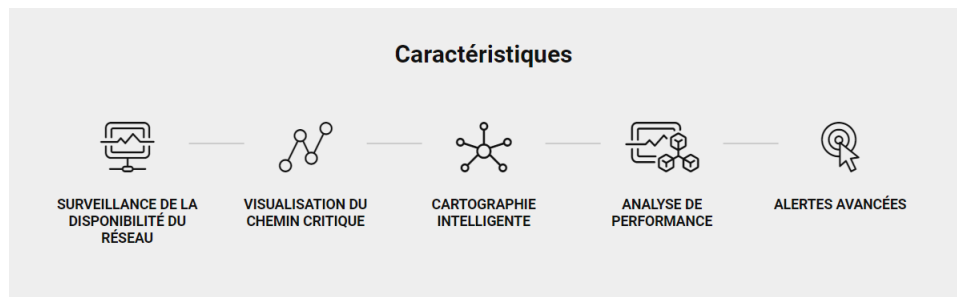


Figure 34: Caracteristiques Solarwinds

- **Surveillance Complète du Réseau** : NPM offre une surveillance en temps réel de l'ensemble du réseau, permettant de détecter rapidement les problèmes de performances, les pannes potentielles, et les goulets d'étranglement.
- **Visualisation de la Topologie** : Il propose des fonctionnalités de cartographie avancées permettant de visualiser la topologie du réseau, les connexions entre les appareils, et d'identifier les relations réseau.
- **Gestion des Alertes Personnalisées** : NPM permet la configuration d'alertes personnalisées, ce qui signifie que les administrateurs peuvent être informés instantanément en cas de problèmes critiques. Les alertes peuvent être envoyées par e-mail, SMS, ou intégrées à d'autres systèmes de gestion.
- **Analyse du Trafic** : Il offre des fonctionnalités d'analyse détaillée du trafic réseau, permettant aux administrateurs de comprendre les modèles de trafic, d'identifier les applications consommatrices de bande passante, et d'optimiser les performances.
- **Supervision des Applications** : NPM ne se limite pas à la supervision du réseau ; il offre également des fonctionnalités de supervision des applications pour identifier les problèmes au niveau de la couche applicative.
- **Tableaux de Bord et Rapports** : Le produit propose des tableaux de bord personnalisables et des rapports détaillés pour analyser les tendances de performance, planifier des mises à niveau, et partager des informations avec les parties prenantes.
- **Intégration avec d'Autres Produits SolarWinds** : Il s'intègre bien avec d'autres produits SolarWinds, offrant une solution plus complète pour la gestion informatique, y compris la surveillance des serveurs, des applications, des bases de données, etc.
- **Simplicité d'Utilisation** : SolarWinds est réputé pour sa facilité d'utilisation, avec une interface utilisateur intuitive et des fonctionnalités qui permettent aux administrateurs de gérer efficacement la supervision du réseau.
- **Évolutivité** : NPM est conçu pour s'adapter aux besoins des réseaux de différentes tailles, offrant une solution évolutive pour les petites, moyennes, et grandes entreprises.

- **Support et Communauté** : SolarWinds offre un support technique solide et une communauté active d'utilisateurs, ce qui facilite l'accès à des ressources utiles et à des solutions en cas de problèmes.

Moniteur de performances réseau

Surveillance de réseau multifournisseur conçue pour évoluer et s'étendre en fonction des besoins de votre réseau.

Principales caractéristiques

- Surveillance de réseau multifournisseur
- Network Insights pour une visibilité plus approfondie
- Cartes intelligentes
- NetPath et PerfStack pour un dépannage facile
- Une évolutivité plus intelligente pour les grands environnements
- Alerte avancée

À partir de 1 785 \$ | [Obtenez un devis](#)

NPM, un module Orion, est construit sur la plateforme SolarWinds

TÉLÉCHARGER L'ESSAI GRATUIT

DÉMO INTERACTIVE

Entièrement fonctionnel pendant 30 jours

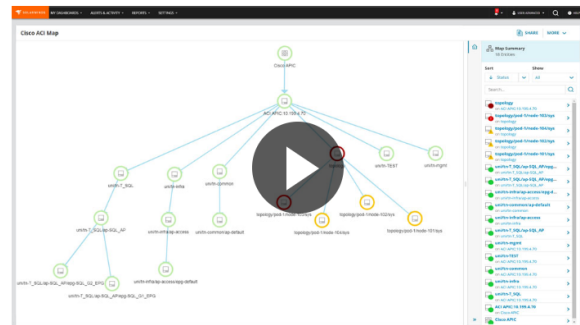


Figure 35: Tarification de Moniteur de performance réseau [15]

VII. Conclusion

Bilan de groupe

En ce qui concerne ce livrable, nous avons établi une liaison entre le premier et le deuxième livrable afin de livrer un document cohérent avec notre travail. Nous avons mis en œuvre tous les points qui ont déjà été proposés dans le livrable 2. Il s'agissait donc d'un livrable entièrement pratique, accompagné bien sûr de justifications de choix. Nous avons également élaboré un devis et une facture approximative, tout en proposant des améliorations.

Bilan Personnel

Sarah KOMBAR :

Ce livrable m'a permis d'approfondir mes connaissances sur le système d'information. Nous avons pu mettre en commun tous les éléments vus pendant ce bloc et donc comprendre le rôle de chacun dans la sécurisation et l'optimisation de celle-ci. Ce livrable a surtout permis d'avoir une vision plus concrète du système d'information.

Ahmad ZIAB :

Ce livrable m'a offert une expérience approfondie dans la conception d'une solution informatique complète, en mettant l'accent sur l'architecture Active Directory, la sécurité réseau, la conteneurisation, la supervision, et la sensibilisation des utilisateurs. La mise en place concrète de la maquette m'a permis d'appliquer les connaissances théoriques acquises, renforçant ainsi ma compréhension pratique des enjeux liés à la sécurité des systèmes d'informations.

Mohamed Amine EL BAH :

Ce livrable m'a aidé à comprendre beaucoup de notions d'administration système d'information. Ce projet m'a globalement aidé techniquement à m'améliorer et m'a également été bénéfique personnellement, car j'occupais le poste de chef d'équipe. Cela m'a permis de gérer une équipe, de définir les priorités et de résoudre les problèmes afin de mettre en place des livrables, tout en maîtrisant les techniques que nous avons acquises durant ce bloc grâce à Mme Bouzarkouna.

Cyril TILHOU-TRIEP :

Ce livrable m'a permis d'explorer des points intéressants de la gestion d'un si, et m'a permis d'approfondir les bases que j'avais déjà acquise. De plus, j'ai eu la chance de pouvoir dans celui-ci explorer le développement en PowerShell, un langage qui m'a toujours intéressé de loin mais que je n'ai jamais eu la chance d'explorer jusqu'à aujourd'hui. J'en ressort grandis et plutôt amusé pour un bloque qui pourtant ne m'intéresse pas spécifiquement.

VIII. Table de Figures

Figure 1: Rôles attribués	3
Figure 2: Relation approbation unidirectionnelle.....	4
Figure 3: Script PowerShell de InstallAntivirus	5
Figure 4: Schématisation de l'Active Directory	5
Figure 5: Configuration PRI3	6
Figure 6: Règles de filtrage WAN	6
Figure 7 : Serveur VPN	7
Figure 8: Table de logs	7
Figure 9: Règles ACL.....	7
Figure 10: Creation GPO windows hello	8
Figure 11 : Configuration GPO	8
Figure 12 : Règle Windows Hello Enterprise.....	9
Figure 13: Règle certificat authentification locale	9
Figure 14: Stratégie de clés publique.....	10
Figure 15: Clients des services de certificats	10
Figure 16: Base de mot de passe Keepass	11
Figure 17: Dockerfile	11
Figure 18: app.py	11
Figure 19: playbook.yml.....	12
Figure 20: Schématisation finale.....	18
Figure : Tarification Windows 10 pro [2]	24
Figure : Webcam Lenovo [3]	24
Figure : Tarification de ESET [4]	26
Figure : Tarification de Cisco Firewall [5]	28
Figure : Construire des conteneurs et des images [6]	28
Figure : Partager [6]	29
Figure : Courir [6]	29
Figure : Tarification de Docker [7]	29
Figure : Tarification Ansible [9]	30

Figure : Tarification Azure Active Directory [11].....	34
Figure : Tarification de Cloud DNS [12].....	35
Figure : Tarification de Azure VPN	36
Figure : Caractéristiques Solarwinds.....	37
Figure : Tarification de Moniteur de performance réseau [15].....	38
 Tableau 1: Fiche technique Cisco FirePower	 27

IX. Bibliographie

- [1] « Tarification et licences Windows Server 2022 | Microsoft ». Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.microsoft.com/fr-fr/windows-server/pricing>
- [2] « Achetez votre licence Windows 10 Professionnel 64 Bits », CoffeeSoft. Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.coffeesoft.fr/systeme-d-exploitation/windows-10-professionnel>
- [3] « Webcam Lenovo Performance Full HD | Lenovo France ». Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: https://www.lenovo.com/fr/fr/p/accessories-and-software/webcams-and-video/webcams-and-video_webcams/4xc1d66055
- [4] « Solutions de sécurité complètes pour votre entreprise | ESET ». Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.eset.com/fr/business/securite-entreprise-pme/>
- [5] C. SARL, « Compufirst - Revendeur de matériel informatique pour les professionnels », Compufirst. Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.compufirst.com/>
- [6] « Docker: Accelerated Container Application Development ». Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.docker.com/>
- [7] « Pricing | Docker ». Consulté le: 13 novembre 2023. [En ligne]. Disponible sur: <https://www.docker.com/pricing/>