

# Epreuve E4

BTS SIO, Lycée Montalembert  
(option SISR)

Années 2020 - 2022

Gaspard  
Malmon

# SOMMAIRE :

- ▶ Présentation du BTS
- ▶ Première année
- ▶ Deuxième année
- ▶ Stages

# PRÉSENTATION DU BTS :

## BTS SIO (Services Informatiques aux Organisations):

2 options disponibles

-> SLAM (solutions logicielles et applications métiers)

-> SISR (solutions d'infrastructures, systèmes et réseaux)

Option SLAM : Conception et développement d'applications

Option SISR : Administration des systèmes et des réseaux

# PREMIÈRE ANNÉE :

(ANNÉE SÉPARÉE EN DEUX SEMESTRES)

Premier semestre :

- ❖ Les bases du système de commande des DOS
- ❖ Les bases de l'active directory et comment la mettre en place
- ❖ Les bases des services réseaux : MAC, IP, Routage...
- ❖ Les différents équipements d'un réseau informatique

Deuxième semestre :

- ❖ Service DHCP (Dynamic Host Configuration Protocol)
- ❖ Service DNS (Domain Name System)
- ❖ Vlan (Virtual LAN) par port
- ❖ Spanning Tree
- ❖ Stage 1<sup>ère</sup> Année

# Système DOS + scripts :

Le système DOS est surtout destiné à la gestion des disques et des fichiers

En connaissant son système de commande, on peut créer des scripts

Scripts pouvant être couplés à une Active Directory

-> Meilleure gestion des répertoires et des fichiers dans l'AD

Exemple de script créé en classe :

```
cd C:\
md C:\TP1\malmon\tp_dos\
cd C:\TP1\
tree
cd C:\TP1\malmon\tp_dos\
echo binaire : 010101 >> lisez.moi.txt | echo decimal : 012345 >> lisez.moi.txt | echo hexadecimal : 0123..ab..ef >> lisez.moi.txt
type lisez.moi.txt
rename lisez.moi.txt lisez1.moi.txt
copy lisez1.moi.txt lisez2.moi.txt
copy lisez1.moi.txt + lisez2.moi.txt >> lisez3.moi.txt
cd C:\TP1\gaucher\
md tp_dos1\
copy tp_dos tp_dos1
del tp_dos
rd tp_dos
tree
pause
```

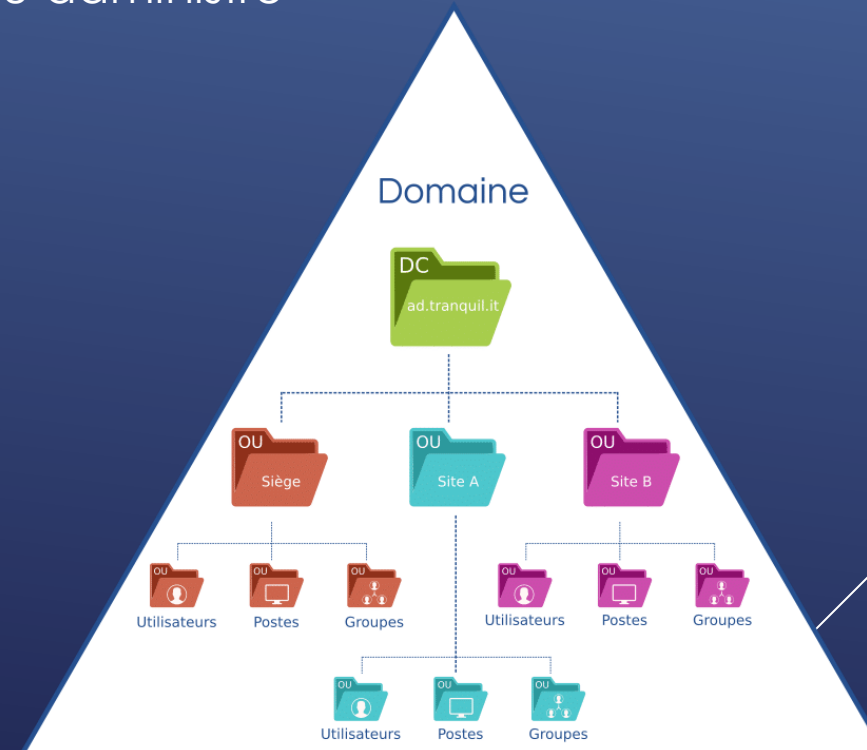
## Active directory :

Une AD est un service d'annuaire proposer par Microsoft

Permet une centralisation des services d'identifications et authentifications

Elle répertorie tout élément d'un réseau administré

Permet aussi le partage de ressources





## Les bases des services réseaux :

Adresse MAC (Media Access Control) :

- Adresse physique stockée dans une carte réseau
- Unique au monde (sauf modifier pas l'utilisateur)

Adresse IP (Internet Protocol) :

- Numéraux d'identification
- Base du système d'acheminement des paquets de données
- 2 versions des IP : IP v4 (32 bits), IP v6 (128 bits)
- IP v4 est plus utilisé actuellement

Le routage :

- Permet de déterminer le chemin pour qu'un paquet aille d'un expéditeur à un receveur
- Permet de faire passer un paquet d'un réseau à un autre
- Fonctionne grâce à une table de routage

```
Adresse physique . . . . . : 5C-3A-45-EA-9B-59
```

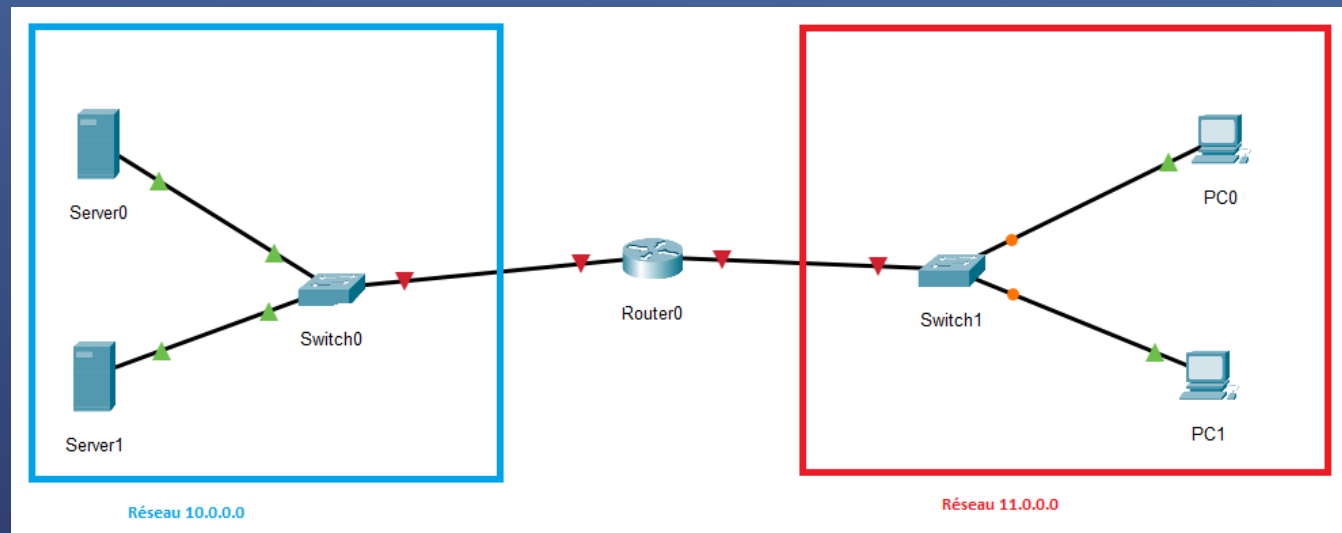
```
Adresse IPv4. . . . . : 192.168.0.9
```

```
Masque de sous-réseau. . . . . : 255.255.255.0
```

```
Passerelle par défaut. . . . . : fe80::160c:76ff:fe60:88bc%11
                                192.168.0.254
```

## Différents équipements d'un réseau informatiques :

- Commutateur (switch)
- Routeur
- Serveurs
- Pc utilisateurs



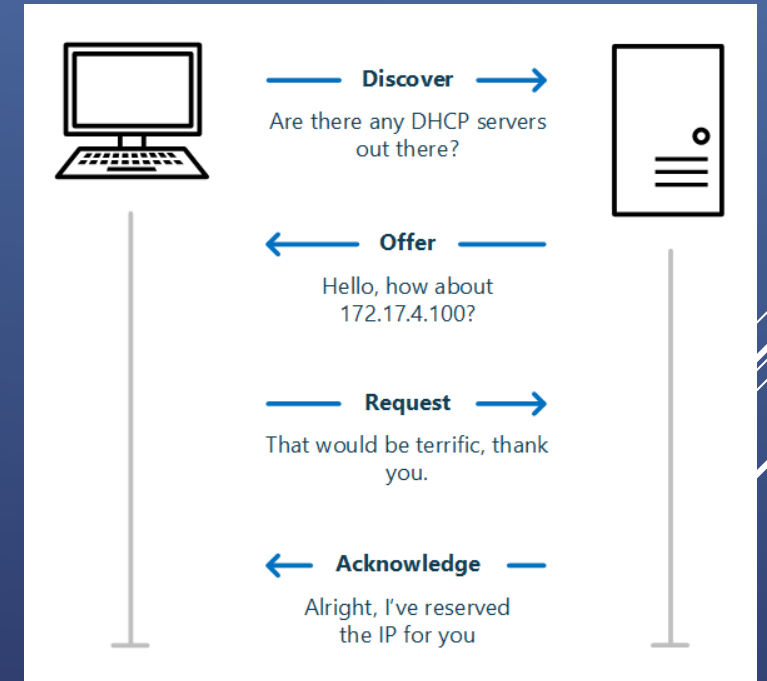
## Service DHCP (Dynamic Host Configuration Protocol) :

Assure la configuration automatique des paramètres IP

Permet de créer des pools d'adresses à distribuer

Peut tous de même réserver une adresse IP spécifique

Plusieurs étapes avant d'attribuer une adresse

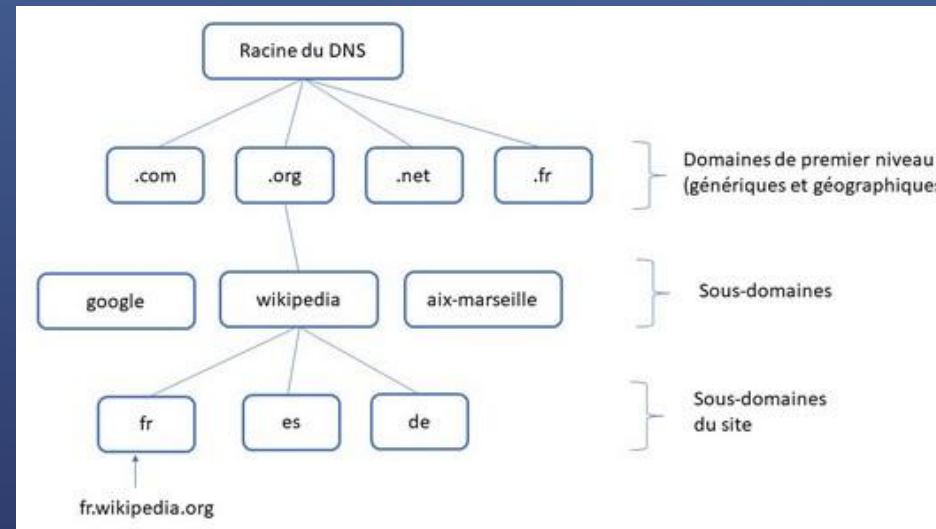
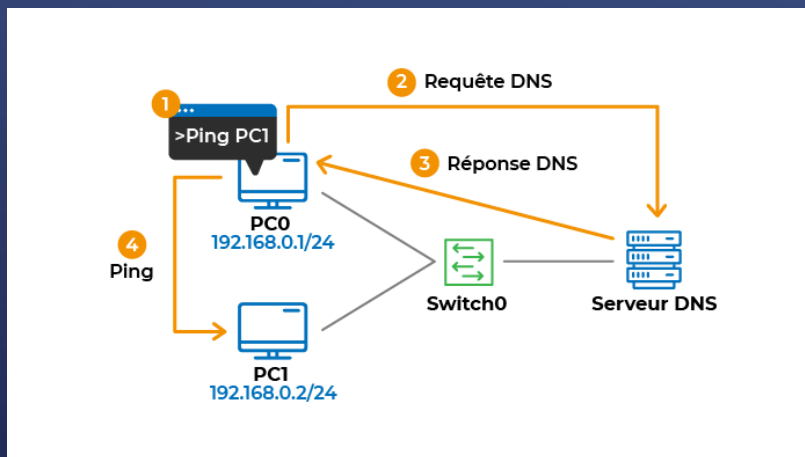


## Service DNS (Domain Name System) :

Permet de traduire les noms de domaines internet en adresses IP  
(ou inversement)

FQDN (Fully Qualified Domain Name) :

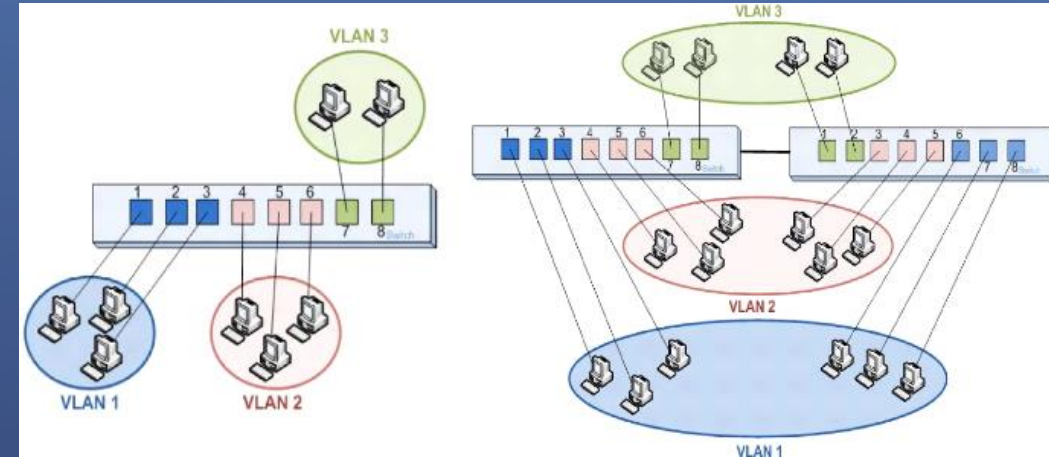
C'est le nom de domaine absolu



## Vlan (Virtual LAN) par port :

Permet de scinder le réseau

Permet une étanchéité maximale des Vlan, donc la sécurité de celles-ci



Différentes configuration de ports :

- Port type Access : ne laisse passer que les paquets untagged
- Port type Trunk : ne laisse passer seulement les paquets tagged
- Port type Hybrid : laisse passer les deux types de paquets

Ports Tagged et Untagged :

Tgged : envoi le paquet sans avoir retiré le tag

Untagged : envoi le paquet après avoir retiré le tag

## Spanning Tree ou STP (Spanning Tree Protocol) :

Permet de contrôler les boucles

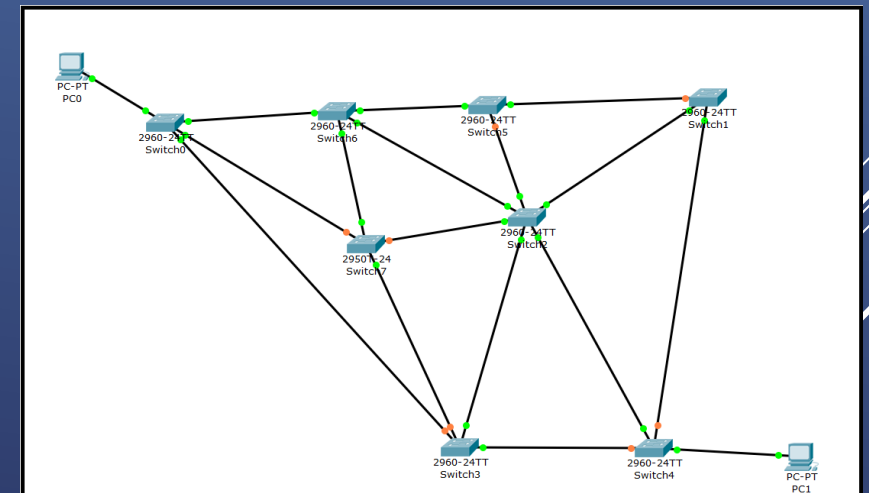
Choisis les routes à bloquer pour optimiser le débit du réseau

Permet de créer de la tolérance aux pannes

Le blocage se fait sur les ports

4 états possibles pour les ports :

- FWD (Forwarding) : port actif
- BLK (Blocking) : port bloqué donc inactif
- LRN (Learning) : port candidat à devenir FWD
- LSN (Listening) : état d'écoute, peut passer en BLK ou en LRN



# DEUXIÈME ANNÉE :

(ANNÉE SÉPARÉE EN DEUX SEMESTRES)

Premier semestre :

- ❖ Protocol HSRP (Hot Standby Router Protocol)
- ❖ Protocol SSH (Secure Shell)
- ❖ Stage 2<sup>ème</sup> année

Deuxième semestre :

- ❖ Service VPN (Virtual Private Network)
- ❖ Service Proxy
- ❖ Service Nagios

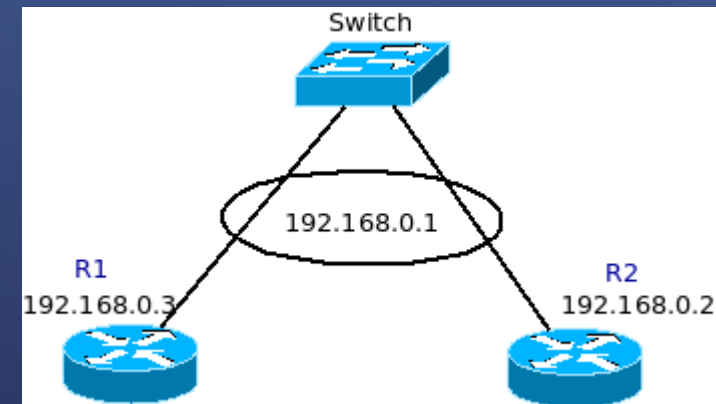


## Protocol HSRP (Hot Standby Router Protocol) :

Protocol propriétaire Cisco

Permet la tolérance aux pannes et la continuité de service

Fonctionne grâce à des sous-réseaux

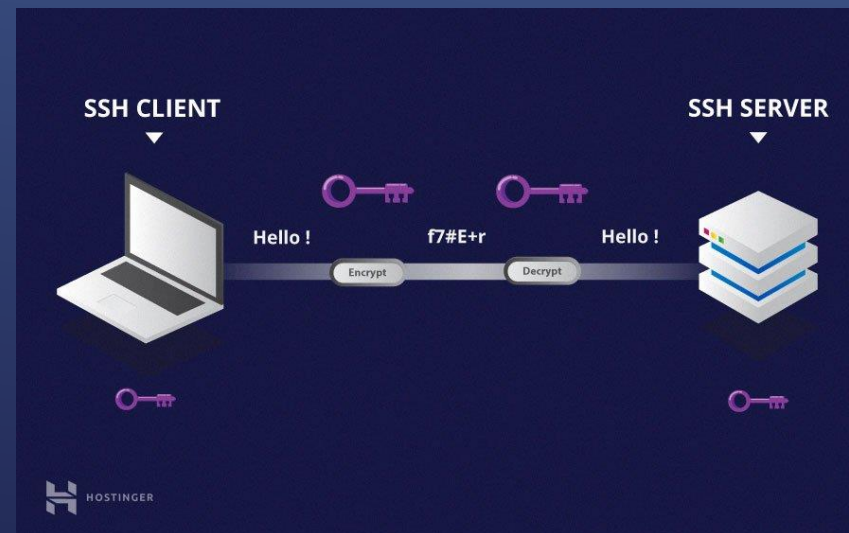


## Protocol HTTP (HyperText Transfer Protocol) :

Permet de prendre le contrôle d'une machine à distance tout en chiffrant les données échanger

Il impose un échange de clés de chiffrement

Il est surtout utilisé afin de se connecter à un serveur Linux



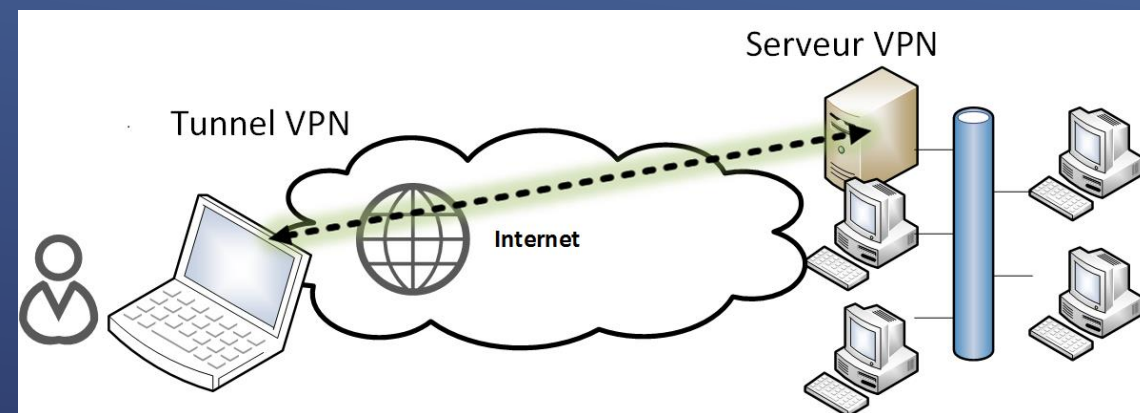
## Service VPN (Virtual Private Network) :

Permet à un appareil situé hors de mon réseau local une connexion à celui-ci

Pour cela il faut la création d'un tunnel entre le client et le serveur VPN

Le VPN Ipsec est le plus utiliser dans le monde

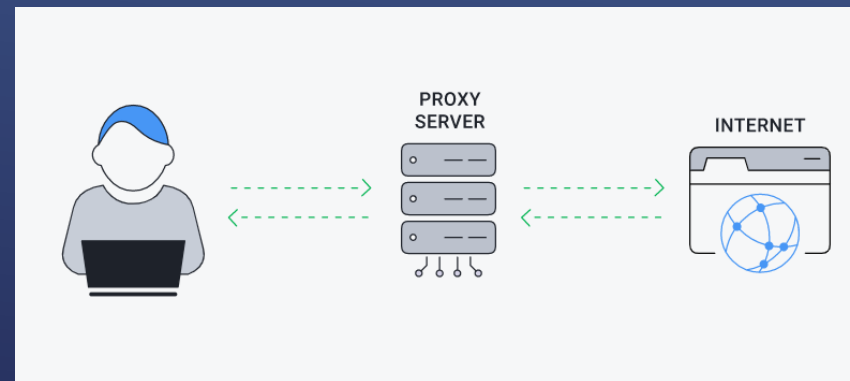
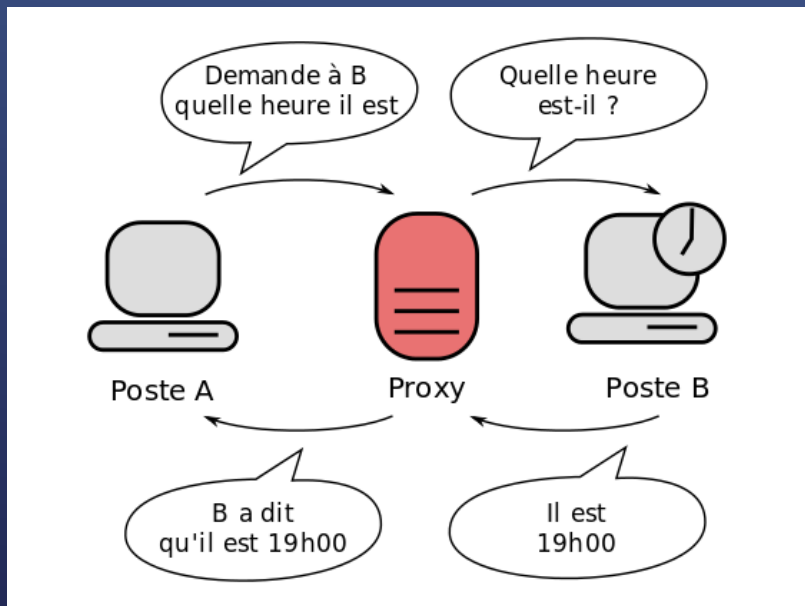
Il nécessite l'installation d'un agent sur le client  
Mais ce tunnel permet de véhiculer différents protocoles de communication (exemple : ssh)



## Service Proxy :

Serveur mandataire servant à faciliter ou surveiller les échanges entre 2 hôtes

Il sert généralement d'intermédiaire pour accéder à un autre réseau, souvent internet



## Service Nagios :

C'est un logiciel de supervision

Cela permet d'avoir une vue d'ensemble sur l'état des différents équipements du réseau

Nagios est un logiciel libre

Il permet de créer ses propres plugins de supervision, ou d'utiliser ceux créés par la communauté

Un équipement supervisé par Nagios peut être dans un des 4 états suivants :

- 0 OK (*tout va bien*)
- 1 WARNING (*le seuil d'alerte est dépassé*)
- 2 CRITICAL (*le service a un problème*)
- 3 UNKNOWN (*impossible de connaître l'état du service*)



# STAGES :

(UN PAR ANNÉE)

## 1<sup>ER</sup> STAGES :

Entreprise : **BH-Technologie**, Nanterre

Maitre de stage : **Jean-François CHAMBREY** (codirecteur de l'entreprise)

Dates : **Du 10 Mai au 11 Juin 2021**

## MISSIONS :

- Réinitialiser et reconfigurer un PC sous Windows 10
- Paramétrage de RK25
- Observation de réparation de serveur



Différents problèmes lors de la reconfiguration du PC :

```

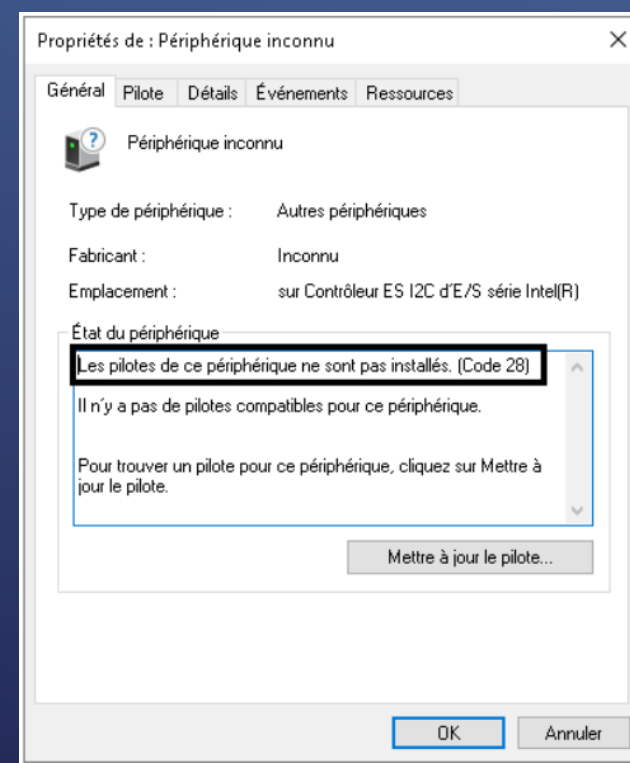
Administrateur : Invite de commandes
Microsoft Windows [version 10.0.19043.1023]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>mklink /j C:\Users\reuni\exemple D:\reuni\exemple
Jonction créée pour C:\Users\reuni\exemple <==> D:\reuni\exemple

C:\Windows\system32>
    
```

Problème de disques

Problème de pilotes



Exemple de ce qu'est un RK25 :



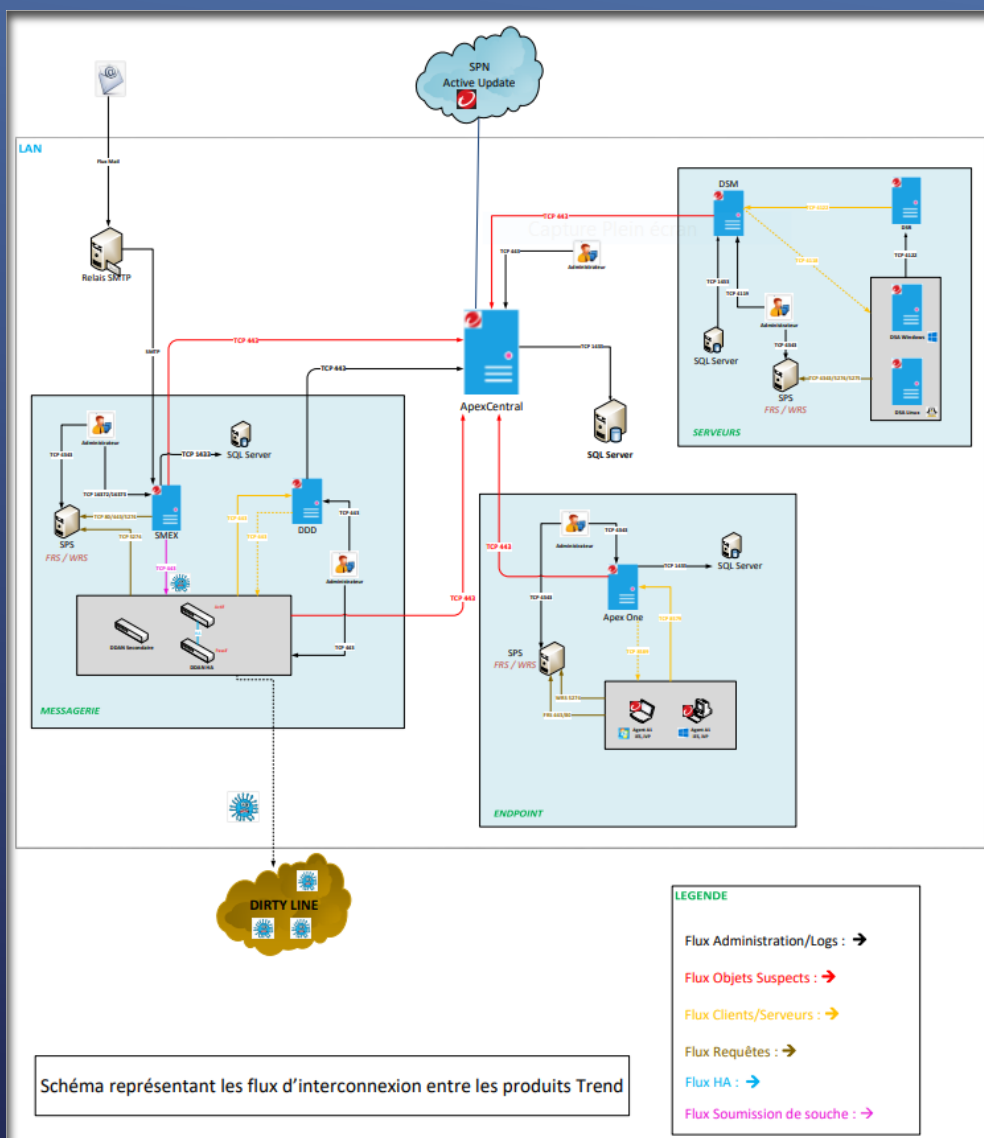
## 2<sup>ÈME</sup> STAGES :

Entreprise : **DSI Pôle Emploi**, montreuil

Maitre de stage : **Julien Chapon** (chargé d'ingénierie et support technique)

Dates : **Du 17 Novembre au 17 Décembre 2021**

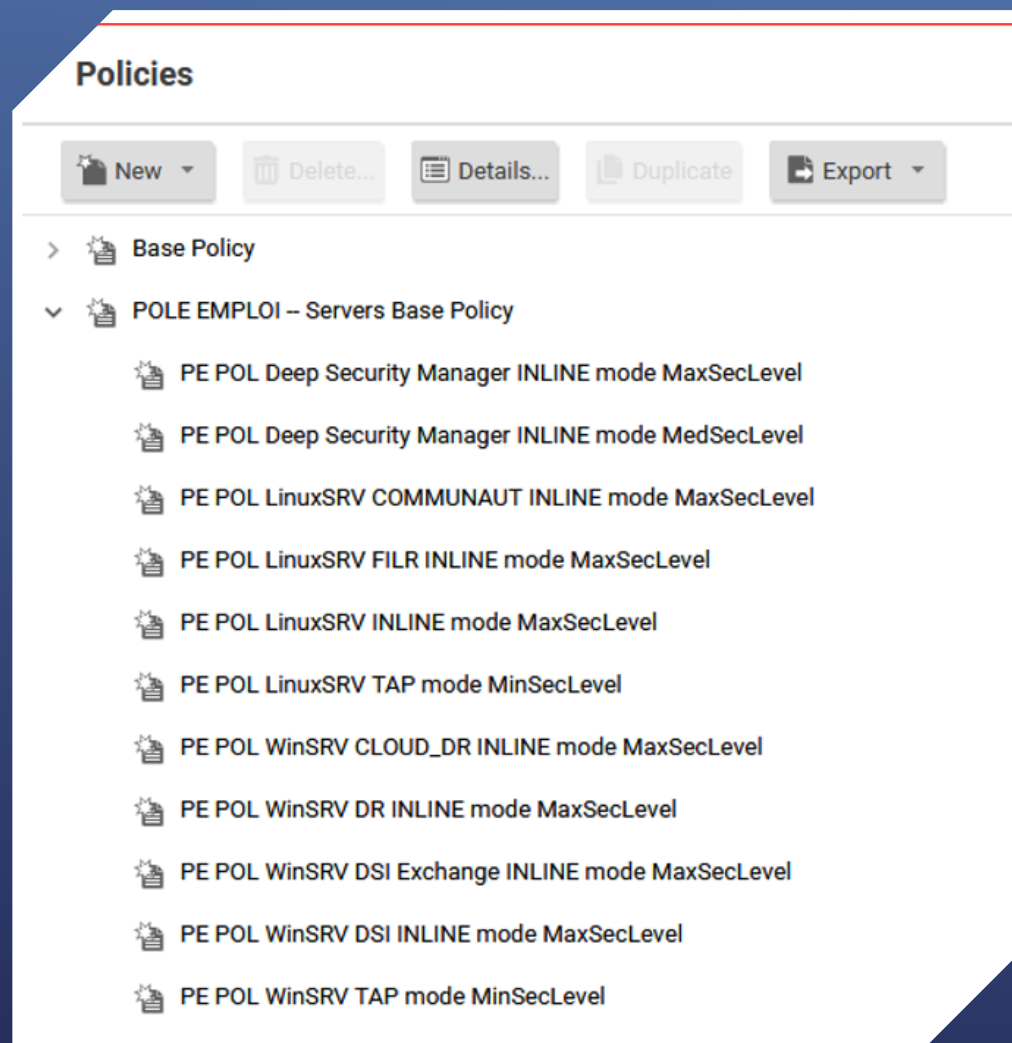
# Schéma réseau :



## MISSIONS :

- Réorganiser des policys
- Créer un cas d'usage de logs
- Créer une doc d'installation de l'antivirus
- Test d'une api
- Patch un serveur

# RÉORGANISER DES POLICYS (GPO) :



- ▶ Les policys sont désorganisées
- ▶ Les noms ne sont pas très explicites
- ▶ Des policys sont redondantes et ne sont utilisées par aucun PC ou Serveurs
- ▶ Et ce pour les deux serveurs deep presents dans le réseau

# arborescence

- > Deep Security manager INLINE (anti-malware = server base) (instruction prévention on + Règles)
- > Linux server base Policy (Anti-malware = server base) (activer + ajout de règles)
  - ° LinuxSRV COMMUNAUT INLINE (anti-malware et instruction prévention = serveur Père)
  - ° LinuxSRV FILR INLINE (anti-malware et instruction prévention = serveur Père)
  - ° LinuxSRV INLINE (anti-malware et instruction prévention = serveur Père)
- > Win server base Policy (Anti-malware = server base)
  - ° WinSRV cloud\_DR INLINE [regroupant Cloud\_DR et DR actuel] (anti-malware = Serveur père)
  - ° WinSRV DSI exchange INLINE (anti-malware = Serveur père) (instruction prévention ON avec règles actuelles)
  - ° WinSRV DSI INLINE (anti-malware = Serveur père) (instruction prévention, integrity monitoring et log inspection ON avec règles actuelles)

General Computer(s) Using This Policy Events

Name: PE POL Deep Security Manager INLINE

Description: Maximum Security Level  
Network Engine Mode INLINE mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode when the Network Engine is in INLINE mode

Inheritance  
Parent Policy: None  
Base Policy  
POLE EMPLOI - Servers Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	Inherited (On)	Real Time
Web Reputation:	On	On
Firewall:	Inherited (Off)	Off, 4 rules
Intrusion Prevention:	Inherited (On)	Detect, 3 rules
Integrity Monitoring:	On	Real Time, no rules
Log Inspection:	On	On, no rules
Application Control:	Inherited (Off)	Off

(regroupe Cloud\_DR et DR actuel)

General Computer(s) Using This Policy Events

Name: PE POL Windows Server Base Policy

Description: Policy parente des serveurs Windows

Inheritance  
Parent Policy: None  
Base Policy  
POLE EMPLOI - Servers Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	On	Real Time
Web Reputation:	Off	Off
Firewall:	Off	Off, no rules
Intrusion Prevention:	Off	Off, no rules
Integrity Monitoring:	Off	Off, 11 rules
Log Inspection:	Off	Off, 11 rules
Application Control:	Off	Off

General Computer(s) Using This Policy Events

Name: PE POL Windows SRV DSI Exchange INLINE

Description: Max Security All Features On  
Network Engine Mode in TAP mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode

Inheritance  
Parent Policy: None  
Base Policy  
PE POL Windows Server Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	Inherited (On)	Real Time
Web Reputation:	Inherited (Off)	Off
Firewall:	Inherited (Off)	Off, no rules
Intrusion Prevention:	On	Prevent, 3 rules
Integrity Monitoring:	Off	Off, 11 rules
Log Inspection:	Off	Off, 11 rules
Application Control:	Inherited (Off)	Off

General Computer(s) Using This Policy Events

Name: PE POL Windows SRV FILR INLINE

Description: Max Security All Features On  
Network Engine Mode in TAP mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode

Inheritance  
Parent Policy: None  
Base Policy  
PE POL Windows Server Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	Inherited (On)	Real Time
Web Reputation:	Inherited (Off)	Off
Firewall:	Inherited (Off)	Off, no rules
Intrusion Prevention:	Inherited (On)	Prevent, 3 rules
Integrity Monitoring:	Inherited (Off)	Off, no rules
Log Inspection:	On	On, 11 rules
Application Control:	Inherited (Off)	Off

General Computer(s) Using This Policy Events

Name: PE POL Linux Server Base Policy

Description: Policy parente des serveurs Linux

Inheritance  
Parent Policy: None  
Base Policy  
POLE EMPLOI - Servers Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	On	Real Time
Web Reputation:	Off	Off
Firewall:	Off	Off, no rules
Intrusion Prevention:	On	Off, no rules
Integrity Monitoring:	Off	Off, 11 rules
Log Inspection:	Off	Off, 11 rules
Application Control:	Off	Off

ajout de règles

General Computer(s) Using This Policy Events

Name: PE POL LinuxSRV COMMUNAUT INLINE

Description: Max Security All Features On  
Network Engine Mode in TAP mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode

Inheritance  
Parent Policy: None  
Base Policy  
PE POL Linux Server Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	Inherited (On)	Real Time
Web Reputation:	Inherited (Off)	Off
Firewall:	Inherited (Off)	Off, no rules
Intrusion Prevention:	Inherited (On)	Prevent, no rules
Integrity Monitoring:	Inherited (Off)	Off, no rules
Log Inspection:	Inherited (Off)	Off, no rules
Application Control:	Inherited (Off)	Off

General Computer(s) Using This Policy Events

Name: PE POL LinuxSRV FILR INLINE

Description: Max Security All Features On  
Network Engine Mode in TAP mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode

Inheritance  
Parent Policy: None  
Base Policy  
PE POL Linux Server Base Policy

Modules

Module	Configuration	Status
Anti-Malware:	Inherited (On)	Real Time
Web Reputation:	Inherited (Off)	Off
Firewall:	Inherited (Off)	Off, no rules
Intrusion Prevention:	Inherited (On)	Prevent, no rules
Integrity Monitoring:	Inherited (Off)	Off, no rules
Log Inspection:	Inherited (Off)	Off, no rules
Application Control:	Inherited (Off)	Off



## arborescence

- > Deep Security Manager INLINE (anti-malware, web reputation, instruction prévention, integrity monitoring et log inspection ON avec ajout de règles)
- > VDI Base Policy (anti-malware, web reputation et instruction prévention ON avec règles actuelles)
  - ° VDI\_Win10 Policy [regroupe NonPerVDI\_Win10 et PerVDI\_Win10 actuel] (anti-malware, web reputation et instruction prévention = VDI Base Policy) (firewall à activer)
  - ° VDI\_Win7 Policy [regroupe NonPerVDI\_Win7 et PerVDI\_Win7 actuel] (anti-malware, web reputation et instruction prévention = VDI Base Policy) (firewall à activer) (Integrity Monitoring et Log Inspection ON mais ajout de règles) (application control ON)

General Computer(s) Using This Policy Events

Name: PE POL Deep Security Manager INLINE

Description: Maximum Security Level  
Network Engine Mode INLINE mode  
Firewall, Intrusion Prevention, and Web Reputation operate in Prevent or Detect mode when the Network Engine is in INLINE mode

Inheritance  
Parent Policy: None  
Base Policy  
POLE EMPLOI - Servers Base Policy - TAP mode

Modules

Module	Setting	Mode
Anti-Malware	On	Real Time
Web Reputation	On	On
Firewall	Off	Off, 4 rules
Intrusion Prevention	On	Detect, no rules
Integrity Monitoring	On	Real Time, no rules
Log Inspection	On	On, no rules
Application Control	Off	Off

ajout de règles

General Computer(s) Using This Policy Events

Name: POLE EMPLOI - VDI Base Policy - INLINE mode

Description:

Inheritance  
Parent Policy: None  
Base Policy  
POLE EMPLOI - Servers Base Policy - TAP mode

Modules

Module	Setting	Mode
Anti-Malware	On	Real Time
Web Reputation	On	On
Firewall	Off	Off, 4 rules
Intrusion Prevention	On	Detect, no rules
Integrity Monitoring	On	Real Time, no rules
Log Inspection	On	On, no rules
Application Control	Off	Off

ajout de règles

# CRÉER UN CAS D'USAGE DE LOGS :

## Problématique :

- ▶ Les logs sont étudiés par une entité externe, et par de l'IA
- ▶ Cas d'usage donc obligatoire afin de permettre à l'IA de bien identifier les problèmes et de faire de bon retour aux équipes de pôle emploi

## Cas d'usage Deep Security

Analyse rapide		Analyse approfondie	
Log brute		Log Brute	
CEF:0 Trend Micro Deep Security Agent 20.0.513 4000000 Eicar_test_file 6 cn1=7 cn1Label=Host ID dvchost=sql2019.vcotrend.lab TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cn2=247 cn2Label=Quarantine File Size filePath=C:\\Users\\administrator.VCOTREND\\Desktop\\virustest.txt act=Delete result=Deleted msg=Realtime TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140		CEF:0 Trend Micro Deep Security Agent 20.0.513 4000000 Eicar_test_file 6 cn1=7 cn1Label=Host ID dvchost=sql2019.vcotrend.lab TrendMicroDsTenant=Primary TrendMicroDsTenantId=0 cn2=247 cn2Label=Quarantine File Size filePath=C:\\Users\\administrator.VCOTREND\\Desktop\\virustest.txt act=Delete result=Deleted msg=Realtime TrendMicroDsFileSHA1=3395856CE81F2B7382DEE72602F798B642F14140	
Champ déterminant		Champs intéressants	
result=Delete	Action final, ici fichier supprimer, mais peut aussi être mis en quarantaine	dvchost=sql2019.vcotrend.lab	Nom du poste infecté
		cn2=247	Taille du fichier
		filePath=C:\\Users\\administrator.VCOTREND\\Desktop\\virustest.txt	Chemin du fichier
		msg=Realtime	Type de scan
		4000000	Type d'événement
Table des types d'événements			
10	Custom Intrusion Prevention (IPS) rule		
20	Log-only Firewall rule		
21	Deny Firewall rule		

# CRÉER UNE DOC D'INSTALLATION DE L'ANTIVIRUS :

## Problématiques :

- ▶ Nouvelle version de MacOS
- ▶ Nouvelle version de l'antivirus obligatoire
- ▶ Différence dans la méthode d'installation
- ▶ Création d'une nouvelle doc à l'intention des techniciens de niveau 2 qui vont installer cette version de l'antivirus dans le futur

# TEST D'UNE API :

► Problématique :

- Permettre aux techniciens de niveau 1 et 2 de rentrer manuellement des objets suspects dans la liste
- Tester l'API afin de voir les différents problèmes et faire des retours aux développeurs



ApexOne

MALMON Gaspard (IGMA2660)

Blocage URL

Deep Security

Envoi de fichier/url  
suspiceux à une Sandbox

Historique

Isolation de poste

Logs

Objets Suspects

Outil Phishing

## Soumission

Environnement : FAB

Fichier

Url

Url à analyser

Soumettre

Consulter

ApexOne

MALMON Gaspard (IGMA2660)

Blocage URL

Deep Security

Envoi de fichier/url  
suspiceux à une Sandbox

Historique

Isolation de poste

Logs

Objets Suspects

Outil Phishing

## Soumission

Environnement : FAB

Fichier

Url

Fichier à analyser

Choisir un fichier ...

Soumettre

Consulter

Ajout d'Objets Suspects

Environnement :

Ajout par :

Liste des Objets Suspects

Environnement :

Ajout d'Objets Suspects

Environnement :

Ajout par :

Type :

Objet :

Action :

Commentaire :

Expiration :

Ajout d'Objets Suspects

Environnement :

Ajout par :

Type :

Objet :

Action :

Commentaire :

Expiration :

Ajout d'Objets Suspects

Environnement :

Ajout par :

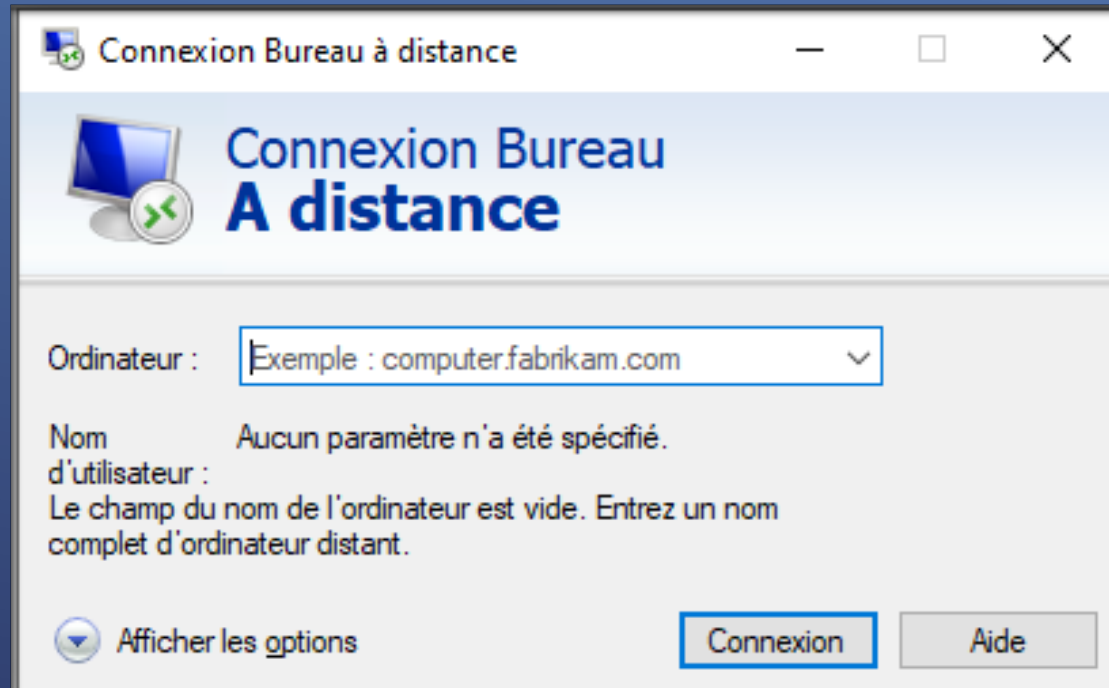
OBJET	TYPE	SCAN ACTION	SCAN PREFILTEI	NOTE	EXPIRATION
Merci de respecter le format de la template du fichier					

Ajout d'Objets Suspects

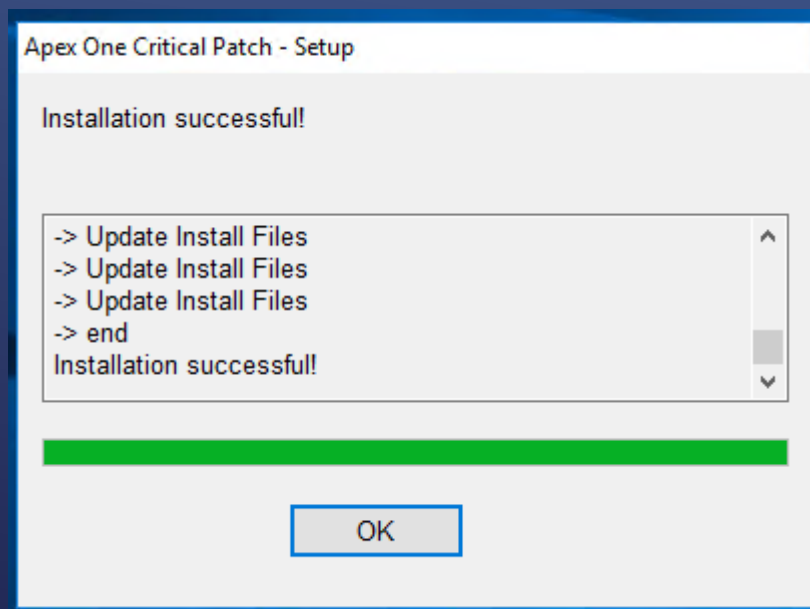
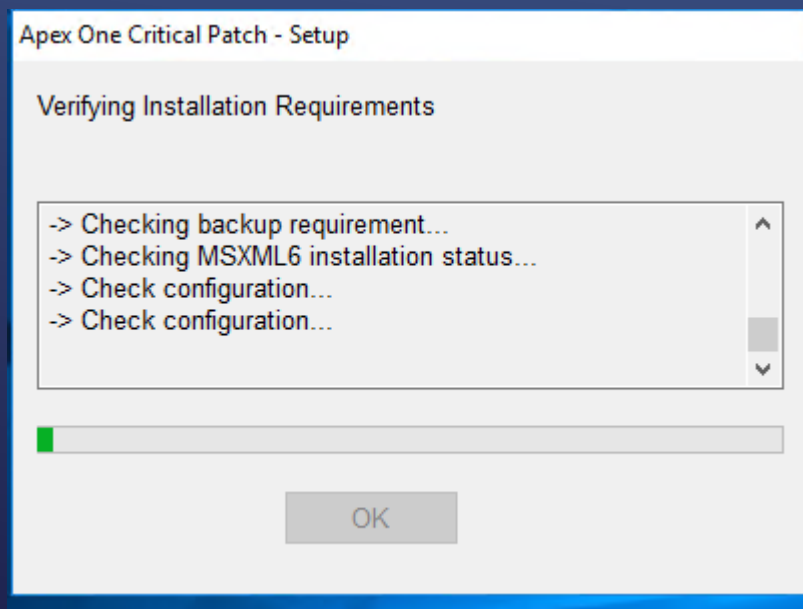
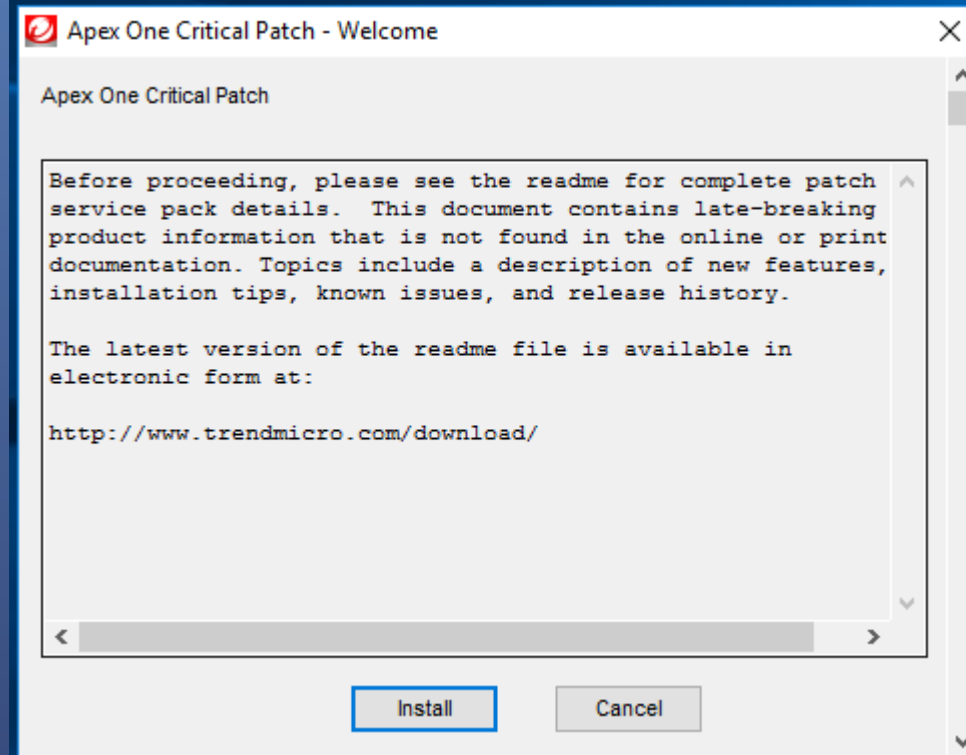
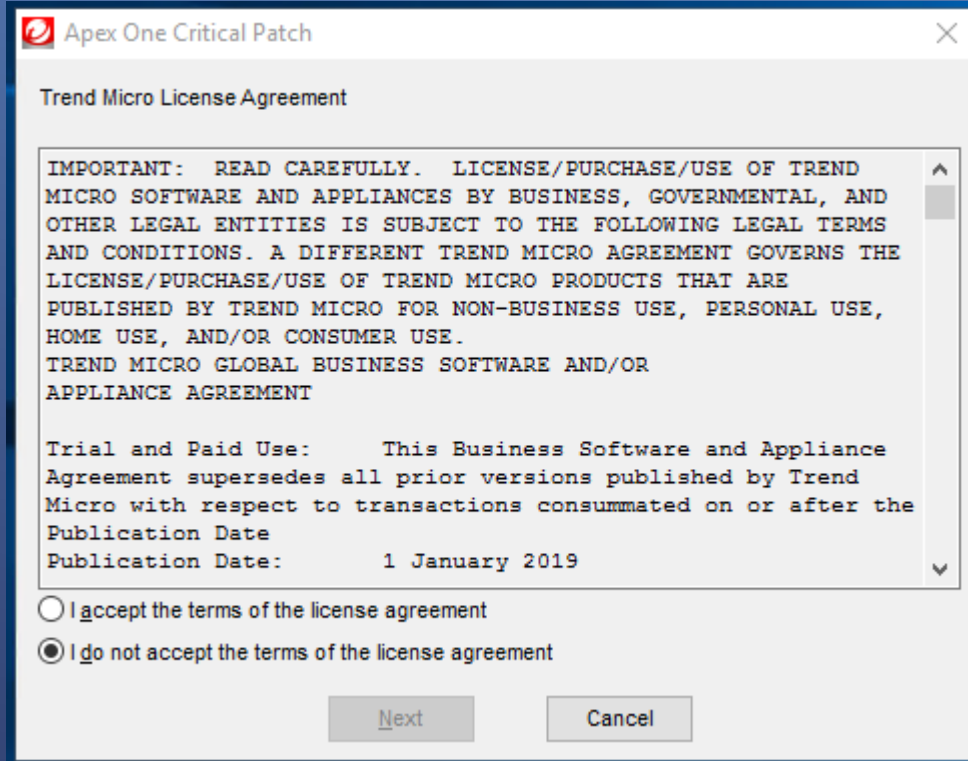
Environnement :

Ajout par :

# PATCH D'UN SERVEUR :

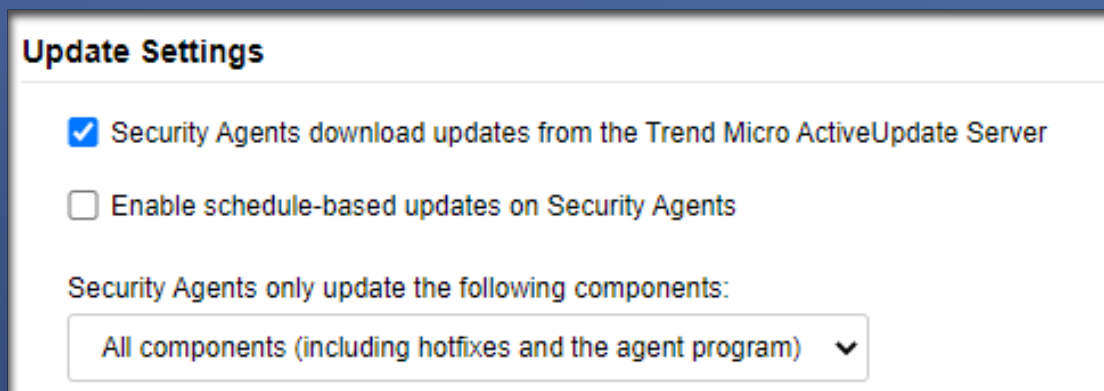


- Connexion au serveur via le bureau à distance de Windows



➤ Suivi des étapes d'installations

- ▶ On vérifie sur l'interface Trend si la mise à jour
- ▶ De plus on programme la décente de la maj sur les posts clients
- ▶ Avec ces paramètres les agents se mettront eux à jour tout seul
- ▶ Sur les posts, il y a 300mo qui redescendent, pour un patch serveur ici de 1,2go



**Update Settings**

☒ Security Agents download updates from the Trend Micro ActiveUpdate Server

☐ Enable schedule-based updates on Security Agents

Security Agents only update the following components:

All components (including hotfixes and the agent program) ▼