



PROJET TUTEURÉ

MAIRIE DE SIGNES

LP Réseaux ASR – 2020/2021

SOMMAIRE

- 1) Présentation des Acteurs
- 2) Objectifs du projet
- 3) Audit & analyse
- 4) Déploiement des solutions
- 5) Mise en place du contexte SSI
- 6) Retour d'expérience

PRÉSENTATION DES ACTEURS



- Cabinet du Maire (validation du projet)
- Direction Informatique (validation technique)
- Service juridique (validation charte et RDPG)
- Responsable informatique (audit – suivi)



Nous-mêmes, « FUTURZO », entreprise d'expertise réseau, intégration de solutions matérielles et logicielles, conseils et formations ainsi que Cyberdéfense.

OBJECTIFS DU PROJET

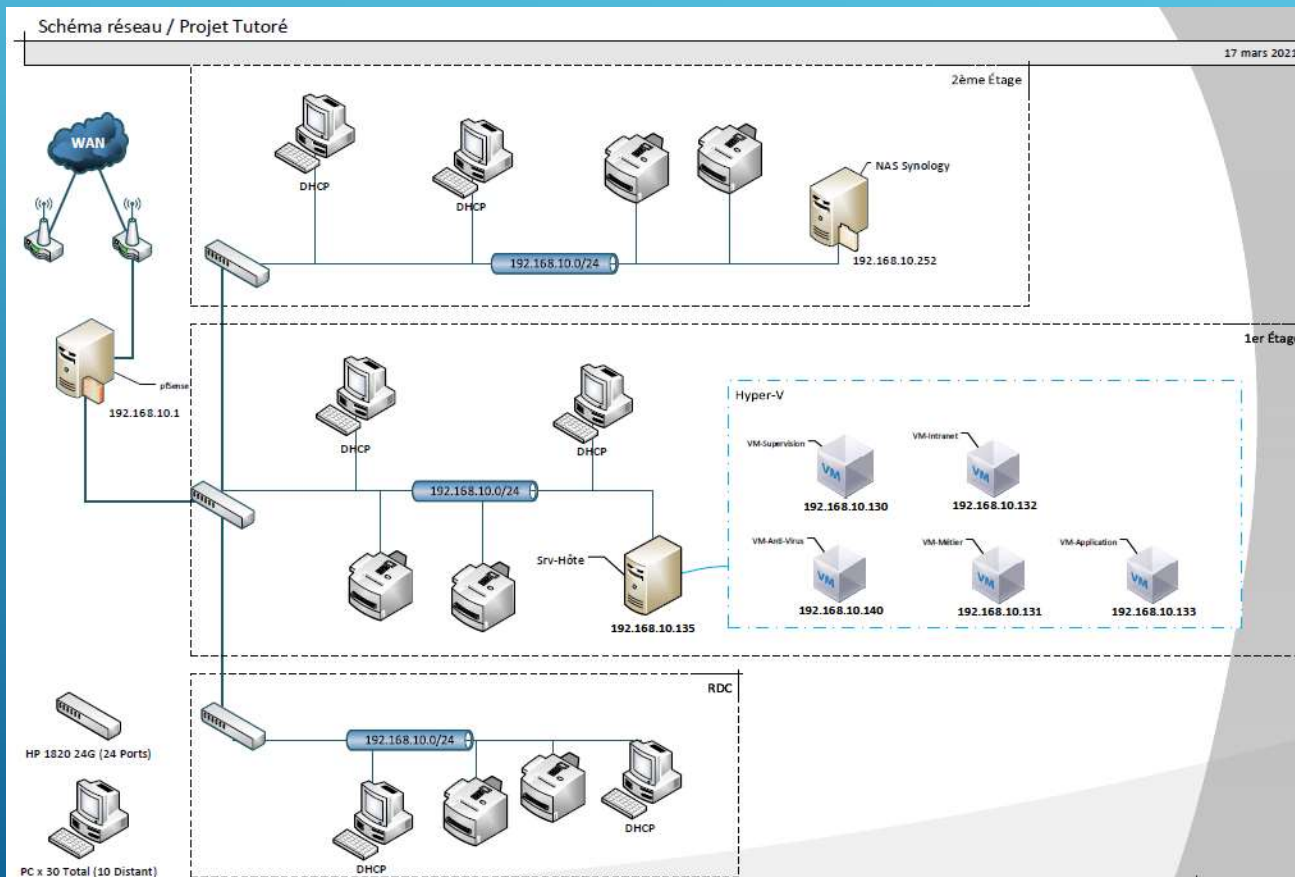
Besoins d'infrastructures :

- Wifi Utilisateurs / Invités
- Accès réseaux Invités
- Accès distant
- Agrégation de deux accès internet
- Recyclage d'ancien serveur en unité de sauvegarde
- Filtrage de l'accès WEB
- Logiciel de messagerie

Besoins cyber :

- Sécuriser les installations
- Sensibilisation du personnel
- Sauvegardes
- PRA

AUDIT DE L'EXISTANT



Adressage IP :

- 192.168.10.0/24
- Pas de VLAN

Existant :

- Pare-feu/Proxy pfSense
- NAS Synology
- Srv-Hôte + 5 VM
- Windows 10-7-XP-S2019

Sécurité:

- BitDefender



ANALYSE

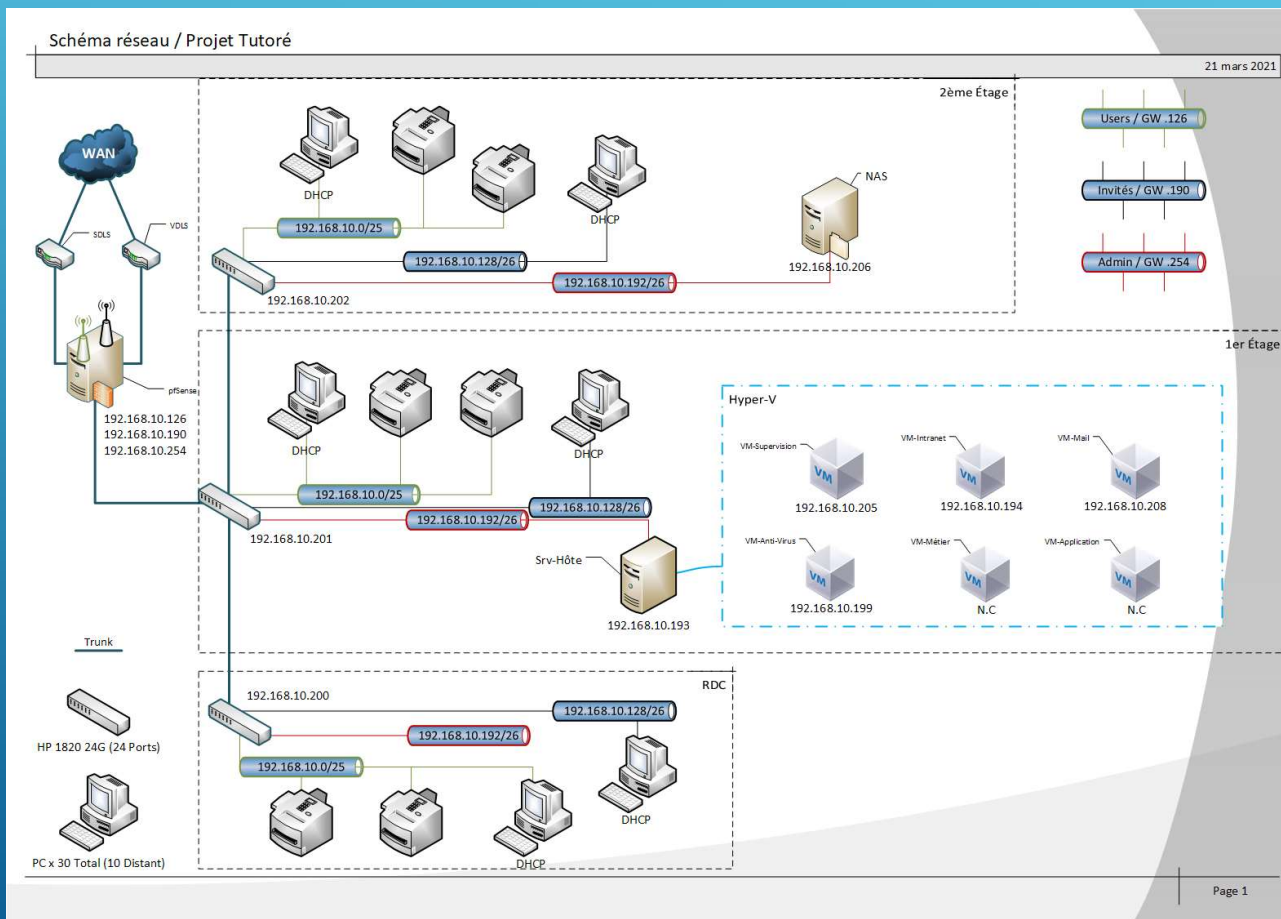
Partie Systèmes/Réseaux :

- ▶ Modification du plan d'adressage IP
- ▶ Architecture sur 3 switches avec VLANs
- ▶ Reconfiguration du pfSense + Agrégation + Filtrage + Proxy + Wifi + VPN
- ▶ Accès sans-fils utilisateurs et invités
- ▶ Accès distant utilisateurs pour le télétravail
- ▶ Mise en place d'une gestion interne des mail
- ▶ Réutilisation de l'ancien serveur pour une unité de sauvegarde

Partie Sécurité :

- ▶ Mise en place d'un plan de sauvegarde + PRA
- ▶ Mise en place d'une solution Anti-virus client/serveur
- ▶ Mise en place d'une station blanche
- ▶ Sensibilisation et formation des utilisateurs
- ▶ Procédure d'exploitation VeraCrypt
- ▶ Charte RGPD

SCÉNARIOS ENVISAGÉS



Adressage IP :

- 192.168.10.0/25 VLAN 100
- 192.168.10.128/26 VLAN 200
- 192.168.10.192/26 VLAN 400

Infrastructure :

- Pare-feu/Proxy pfSense
- Wi-fi pfSense
- Agrégation de lien
- VPN
- Serveur Backup (Ancien)
- NAS Synology
- Srv-Hôte + 5 VM
- BitDefender
- Windows 10-Srv2019

DÉPLOIEMENT DES SOLUTIONS

Matrice des flux effective sur le routeur PfSense

	Source	Dest	Service	Action	Log
Defaut	Inet	Any	*	Détruire	Oui
Bypass proxy	@User/Invité	Inet	HTTP/S	Bloquer	Oui
Invité SRV	@Invité	@Srv/User	*	Bloquer	Oui
Invité Impri	@Invité	@Imprim	*	Autoriser	Non
Invité DNS	@Invité	SRV-Hôte	DNS	Autoriser	Non
Proxy	@User/invité	Inet	Proxy(3128)	Autoriser	Non
Envoi mail	Inet	SRV-Mail	SMTP/POP/IMAP	Autoriser	Non
Réception mail	SRV-Mail	Inet	SMTP	Autoriser	Non
VPN	Inet	VPN	1194(UDP)	Autoriser	Non
Update SRV	@Srv	Inet	HTTP/S + FTP	Autoriser	Non

DÉPLOIEMENT DU PARE-FEU

AGRÉGATION DE LIENS

Système / Routage / Groupes de passerelle / Modifier

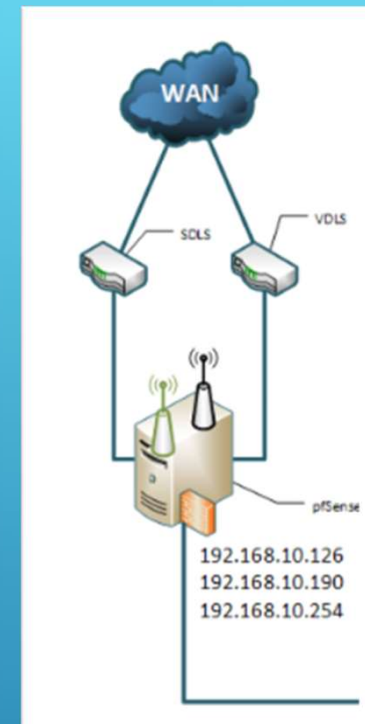
Modifier l'entrée de groupe de passerelle

Nom de groupe: SDSL_VDSL

Priorité de passerelle

WAN_DHCP	Niveau 1	Adresse de l'interface	Interface WAN_DHCP Gateway
WAN2_DHCP	Niveau 1	Adresse de l'interface	Interface WAN2_DHCP Gateway

Passerelle	Niveau	adresse IP virtuelle	Description
Priorité de liaison The priority selected here defines in what order failover and balancing of links will be done. Multiple links of the same priority will balance connections until all links in the priority will be exhausted. If all links in a priority level are exhausted then the next available link(s) in the next priority level will be used.			
adresse IP virtuelle The virtual IP field selects which (virtual) IP should be used when this group applies to a local Dynamic DNS, IPsec or OpenVPN endpoint.			
Seuil de déclenchement Membre tombé Quand déclencher l'exclusion d'un membre			
Description Agrégation WAN Une description peut être saisie ici à des fins de référence administrative (non analysée).			



DÉPLOIEMENT DU PARE-FEU

FILTRAGE

Pare-feu / Règles / BRIDGEINVITES

Flottant(e) WAN VLAN400 WAN2 VLAN100 VLAN200 VPN_USER WIFIUSERS WIFIINVITES BRIDGEUSERS

BRIDGEINVITES OpenVPN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	Filtre d'attente	Ordonnement	Description	Actions
DNS + HTTP/S Proxy											
■	✓	0 / 0 B	IPv4 UDP	BRIDGEINVITES net	*	192.168.10.193	53 (DNS)	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	192.168.10.254	3128	*	aucun	Proxy	📥📏🔄🗑️
Imprimantes											
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.120	*	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.121	*	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.122	*	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.123	*	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.124	*	*	aucun		📥📏🔄🗑️
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	192.168.10.125	*	*	aucun		📥📏🔄🗑️
Block											
■	✗	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	*	80 (HTTP)	*	aucun		📥📏🔄🗑️
■	✗	0 / 0 B	IPv4 TCP	BRIDGEINVITES net	*	*	443 (HTTPS)	*	aucun		📥📏🔄🗑️
■	✗	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	VLAN400 net	*	*	aucun		📥📏🔄🗑️
■	✗	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	BRIDGEUSERS net	*	*	aucun		📥📏🔄🗑️
Allow											
■	✓	0 / 0 B	IPv4 *	BRIDGEINVITES net	*	*	*	*	aucun		📥📏🔄🗑️

Pare-feu / Règles / BRIDGEUSERS

Flottant(e) WAN VLAN400 WAN2 VLAN100 VLAN200 VPN_USER WIFIUSERS WIFIINVITES BRIDGEUSERS

BRIDGEINVITES OpenVPN

Règles (Faire glisser pour changer l'ordre)

	États	Protocole	Source	Port	Destination	Port	Passerelle	Filtre d'attente	Ordonnement	Description	Actions
-> Proxy											
■	✓	27 / 8.76 MB	IPv4 TCP	*	*	Ce pare-feu	*	*	aucun		📥📏🔄🗑️
Proxy obligatoire pour HTTP/HTTPS											
■	✗	0 / 13 KiB	IPv4 TCP	BRIDGEUSERS net	*	*	443 (HTTPS)	*	aucun	Bridge_Bypass_Block_HTTPS	📥📏🔄🗑️
■	✗	0 / 1 KiB	IPv4 TCP	BRIDGEUSERS net	*	*	80 (HTTP)	*	aucun	Proxy_Bypass_Block	📥📏🔄🗑️
Allow											
■	✓	3 / 50.42 MB	IPv4 *	BRIDGEUSERS net	*	*	*	*	aucun		📥📏🔄🗑️

DÉPLOIEMENT DU PARE-FEU

PROXY VIA SQUID ET SQUIDGUARD

SSL Man In the Middle Filtering

HTTPS/SSL Interception ☒ Enable SSL filtering.

SSL/MITM Mode Splice All
The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled.
Default: Splice Whitelist, Bump Otherwise. Click Info for details.

SSL Intercept Interface(s) WAN
VLAN400
WAN2
VLAN100
The interface(s) the proxy server will intercept SSL requests on. *Use CTRL + click to select multiple interfaces.*

SSL Proxy Port
This is the port the proxy server will listen on to intercept SSL while using transparent proxy. *Default: 3129*

SSL Proxy Compatibility Mode Modern
The compatibility mode determines which cipher suites and TLS versions are supported. *Default: Modern. Click Info for details.*

DHParams Key Size 2048 (default)
DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.

AC proxy
Select Certificate Authority to use when SSL interception is enabled.

SSL Certificate Daemon Children
This is the number of SSL certificate daemon children to start. May need to be increased in busy environments. *Default: 5*

Remote Cert Checks Accept remote server certificate with errors
Do not verify remote certificate
Select remote SSL certificate checks to perform. *Use CTRL + click to select multiple options.*

Certificate Adapt Sets the 'Not After' (setValidAfter)
Sets the 'Not Before' (setValidBefore)
Sets CN property (setCommonName)
See [sbloroxxy.cert.adapt directive documentation](#) and [Mimic original SSL server certificate wiki article](#) for details.

Squid General Settings

Enable Squid Proxy ☒ Check to enable the Squid proxy.
Important: If unchecked, ALL Squid services will be disabled and stopped.

Keep Settings/Data ☒ If enabled, the settings, logs, cache, AV defs and other data will be preserved across package reinstalls.
Important: If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade.

Listen IP Version IPv4
Select the IP version Squid will use to select addresses for accepting client connections.

CARP Status VIP aucun
Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status.
Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization.

Proxy Interface(s) WIFIUSERS
WIFIINVITES
BRIDGEUSERS
BRIDGEINVITES
The interface(s) the proxy server will bind to. *Use CTRL + click to select multiple interfaces.*

Outgoing Network Interface Default (auto)
The interface the proxy server will use for outgoing connections.

Port du mandataire (= proxy =) 3128
This is the port the proxy server will listen on. *Default: 3128*

ICP Port
This is the port the proxy server will send and receive ICP queries to and from neighbor caches.
Leave this blank if you don't want the proxy server to communicate with neighbor caches through ICP.

DÉPLOIEMENT DU PARE-FEU

PROXY VIA SQUID ET SQUIDGUARD

Utilisation d'une liste noire mise à disposition par l'Université de Toulouse

Blacklist options

Blacklist ☒ Check this option to enable blacklist

Blacklist proxy

Blacklist upload proxy - enter here, or leave blank.
Format: host:[port login:pass] . Default proxy port 1080.
Example: '192.168.0.1:8080 user:pass'

Blacklist URL

Enter the path to the blacklist (blacklist.tar.gz) here. You can use FTP, HTTP or LOCAL URL blacklist archive or leave blank. The LOCAL path could be your pfsense (/tmp/blacklist.tar.gz).

target Categories

[blk_blacklists_adult]	access	deny	▼
[blk_blacklists_agressif]	access	deny	▼
[blk_blacklists_arjel]	access	---	▼
[blk_blacklists_associations_religieuses]	access	deny	▼
[blk_blacklists_astrology]	access	deny	▼
[blk_blacklists_audio-video]	access	---	▼
[blk_blacklists_bank]	access	---	▼
[blk_blacklists_bitcoin]	access	deny	▼
[blk_blacklists_blog]	access	---	▼
[blk_blacklists_celebrity]	access	---	▼
[blk_blacklists_chat]	access	deny	▼
[blk_blacklists_child]	access	deny	▼
[blk_blacklists_cleaning]	access	---	▼
[blk_blacklists_cooking]	access	---	▼
[blk_blacklists_cryptojacking]	access	deny	▼
[blk_blacklists_dangerous_material]	access	deny	▼
[blk_blacklists_dating]	access	deny	▼

DÉPLOIEMENT DU PARE-FEU

PROXY VIA SQUID ET SQUIDGUARD

```
// If the IP address of the local machine is within a defined
// subnet, send to a specific proxy.
if (isInNet(myIpAddress(), "192.168.10.192", "255.255.255.192"))
    return "DIRECT";

// DEFAULT RULE: All other traffic, use below proxies, in fail-over order.
return "PROXY 192.168.10.254:3128";
```

Configuration automatique
des clients proxy

252 WPAD Standard http://wpad.domaine.lpr/wpad.dat Aucun

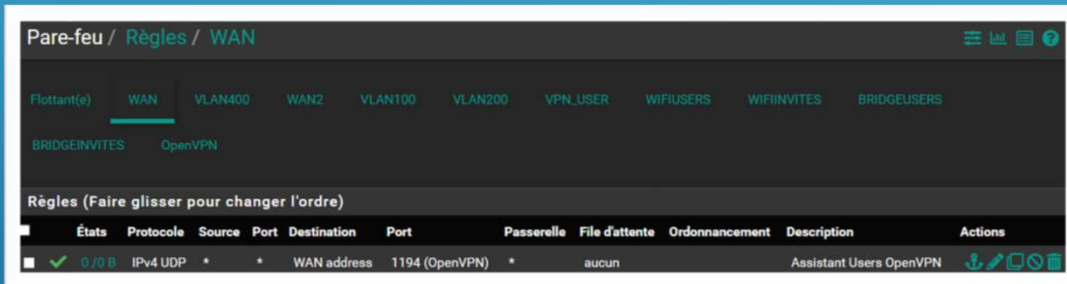
Forçage de l'utilisation de la
fonctionnalité « SafeSearch »

	Nom	Type	Données	Horodateur
WS19-1.domaine.lpr	(identique au dossier parent)	Source de nom (SOA)	[2] ws19-1.domaine.lpr, hostmaster.domaine.lpr.	statique
Zones de recherche directes	(identique au dossier parent)	Serveur de noms (NS)	ws19-1.domaine.lpr.	statique
_msdcs.domaine.lpr	(identique au dossier parent)	Hôte (A)	216.239.38.120	statique
bing.com				
domaine.lpr				
google.fr				
www.bing.com				
www.google.fr				
Zones de recherche inversée				
Redirecteurs conditionnels				

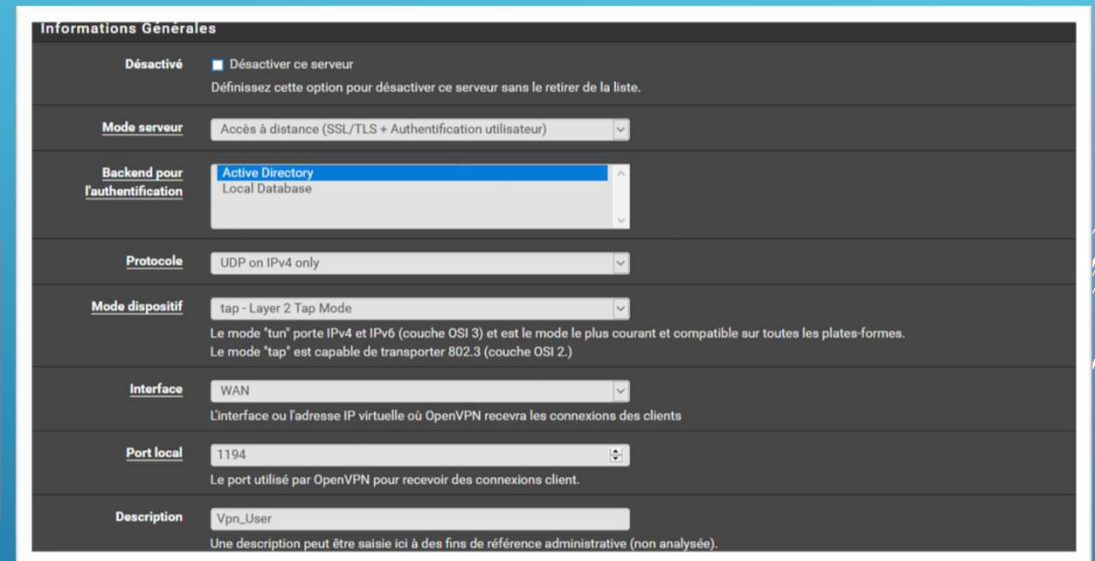
DÉPLOIEMENT DU PARE-FEU

ACCÈS DISTANT

Utilisation d'OpenVPN sécurisé par SSL/TLS en plus de l'authentification AD



Règle de pare-feu à ajouter pour le trafic VPN entrant.







DÉPLOIEMENT DU PARE-FEU

ACCÈS SANS FILS

Interfaces sans fils reliées avec vlan adéquat.

Interfaces sans-fil			
Interface	Mode	Description	Actions
ath1_wlan0	Point d'accès	Wifi-Users	 
ath1_wlan1	Point d'accès	Wifi-Invites	 

Interfaces / Ponts			
Assignations des interfaces Groupes d'interface Sans-fil VLANs QinQs PPPs GREs GIFs <u>Ponts</u> LAGGs			
Interfaces pont			
Interface	Membres	Description	Actions
BRIDGE0	VLAN100, VPN_USER, WIFIUSERS	VLAN100_Bridge	 
BRIDGE1	VLAN200, WIFIINVITES	VLAN200_Bridge	 

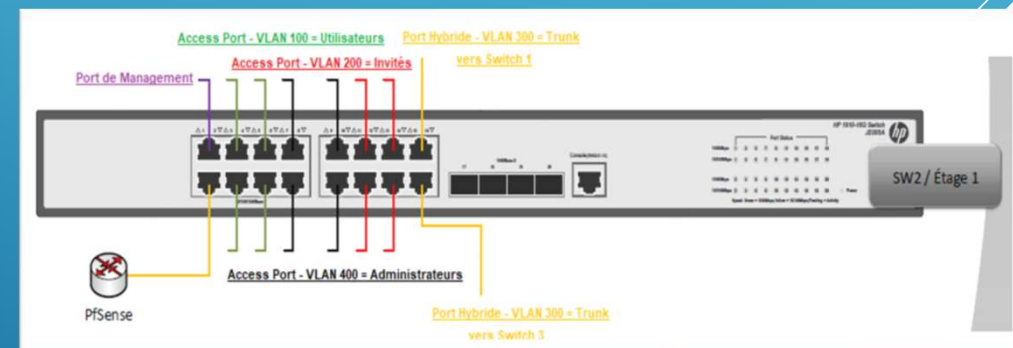
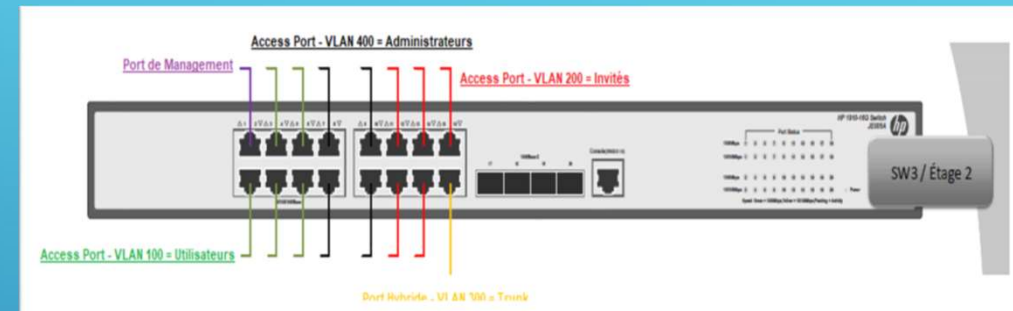
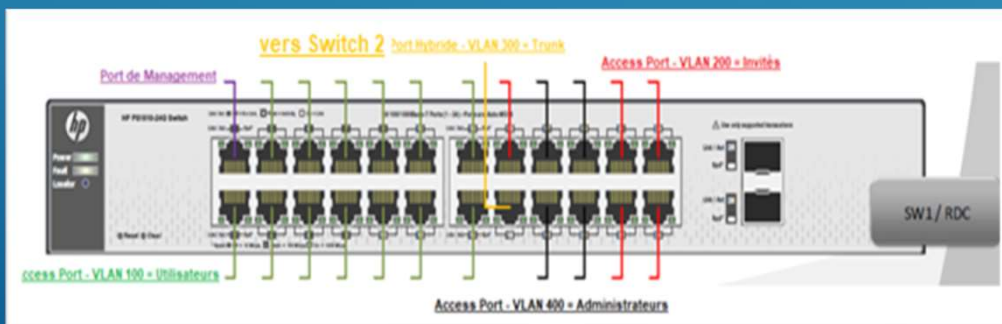
Wifi-Users : WPA2-EAP avec authentification RADIUS (WPA2 uniquement pour la maquette)
Soumis au filtrage Utilisateurs

Wifi-Invités : Ouvert et soumis au filtrage Invités

DÉPLOIEMENT DES SWITCHS

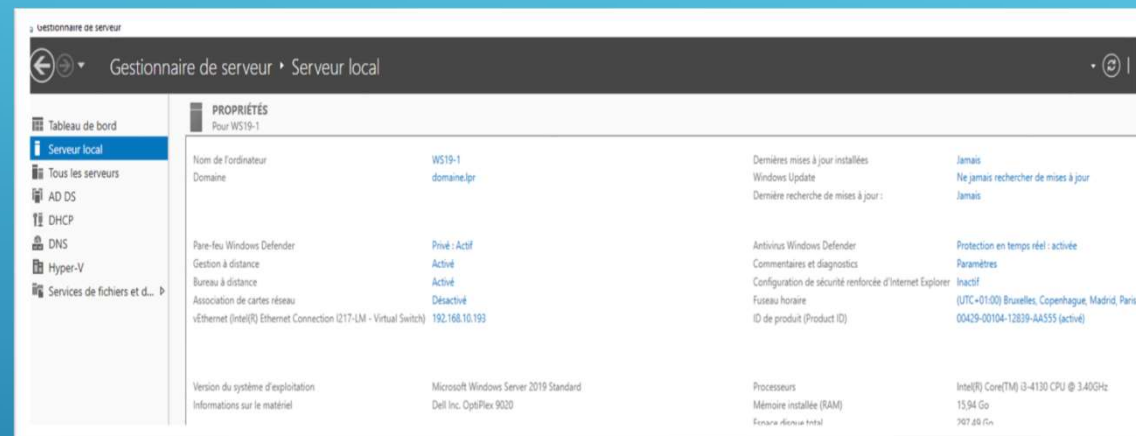
Configuration générique des switchs :

- Réinitialisation du commutateur
- Configuration de l'adresse IP de management
- Sécurisation des accès
- Création de comptes administrateurs nominatifs
- Mise en place de la journalisation
- Configuration du NTP



DÉPLOIEMENT DU SERVEUR HÔTE

Contrôleur de Domaine = serveur Windows 2019
Professionnel



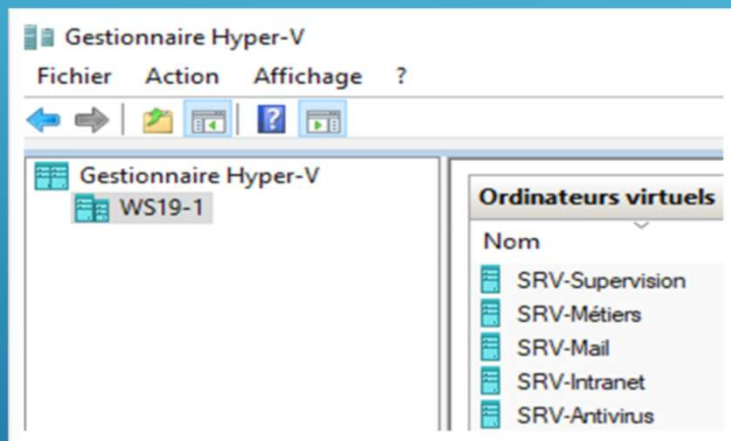
CONTRÔLEUR DE DOMAINE

Domaine créé pour la maquette = « **domaine.lpr** »

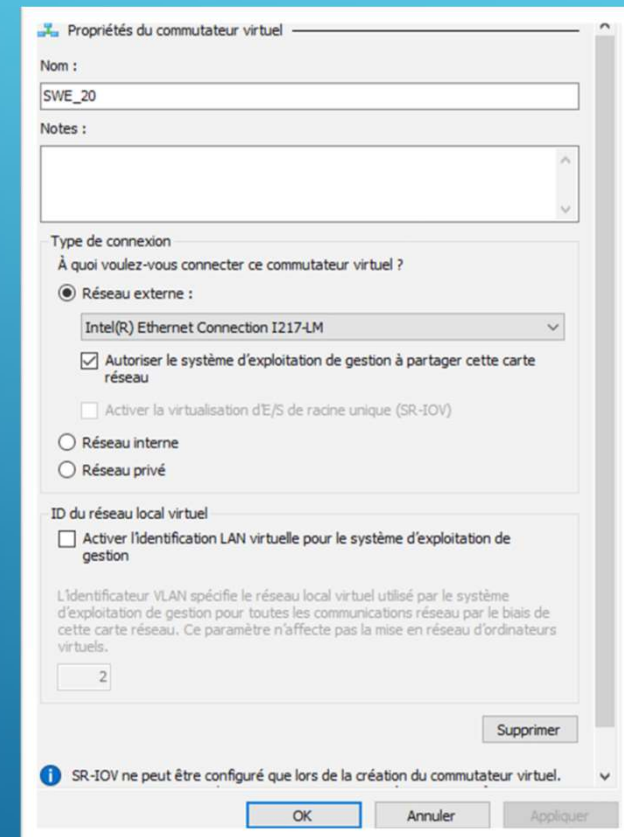
Il ne représente pas le domaine déployé à la mairie de Signes.

DÉPLOIEMENT DU SERVEUR HÔTES

HYPER-V

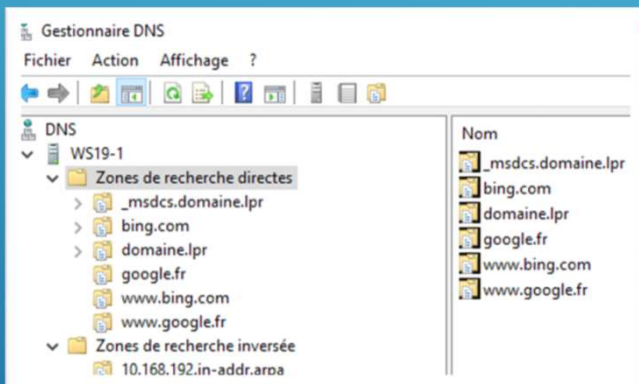


- Création des différentes VM nécessaires
- Création du commutateur virtuel



DÉPLOIEMENT DU SERVEUR HÔTES

DNS



Ajout manuel permettant le filtrage des accès à un contenu explicite (filtrage détaillé plus haut)

- « bing.com »
- « www.bing.com »
- « google.fr »
- « www.google.fr »

DÉPLOIEMENT DU SERVEUR HÔTES

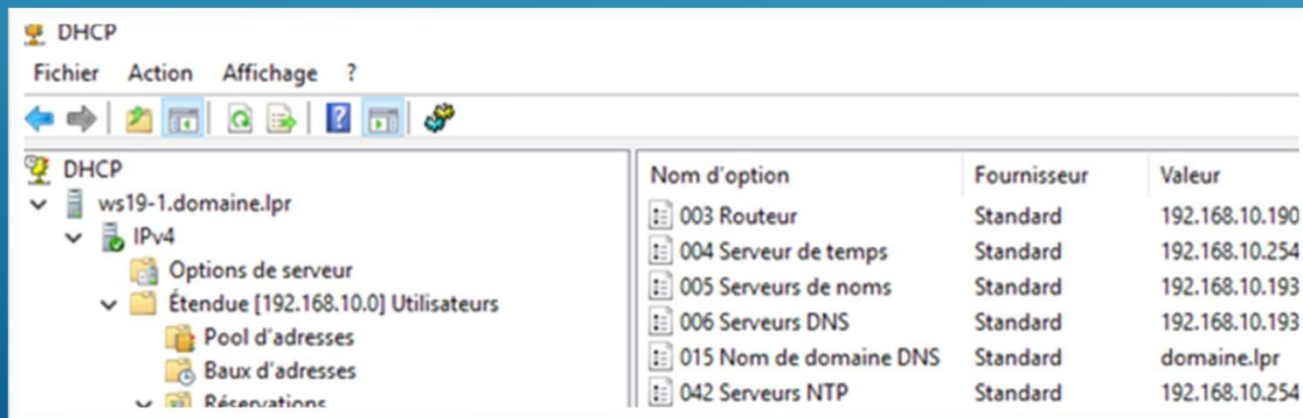
DHCP

Etendue **« Utilisateurs »** : plage d'adresses IP 192.168.10.0/25 = VLAN 100 « Utilisateurs »

Etendue **« Invités »** : plage d'adresses IP 192.168.10.128/26 = VLAN 200 « Invités »

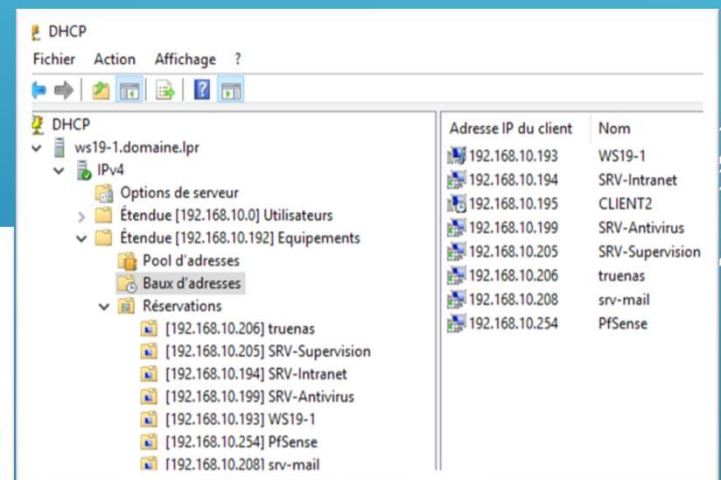
Etendue **« Equipements »** : plage d'adresses IP 192.168.10.192/26 = VLAN 400
« Equipements/admin »

Options d'étendues et réservation de baux :



The screenshot shows the DHCP console for the server 'ws19-1.domaine.lpr'. Under the 'IPv4' section, the 'Options de serveur' are expanded, showing the 'Étendue [192.168.10.0] Utilisateurs'. The 'Pool d'adresses' and 'Baux d'adresses' are also visible. The 'Réservations' section is expanded, showing a list of reservations with their IP addresses and names.

Nom d'option	Fournisseur	Valeur
003 Routeur	Standard	192.168.10.190
004 Serveur de temps	Standard	192.168.10.254
005 Serveurs de noms	Standard	192.168.10.193
006 Serveurs DNS	Standard	192.168.10.193
015 Nom de domaine DNS	Standard	domaine.lpr
042 Serveurs NTP	Standard	192.168.10.254



The screenshot shows the DHCP console for the server 'ws19-1.domaine.lpr'. Under the 'IPv4' section, the 'Options de serveur' are expanded, showing the 'Étendue [192.168.10.192] Equipements'. The 'Pool d'adresses' and 'Baux d'adresses' are also visible. The 'Réservations' section is expanded, showing a list of reservations with their IP addresses and names.

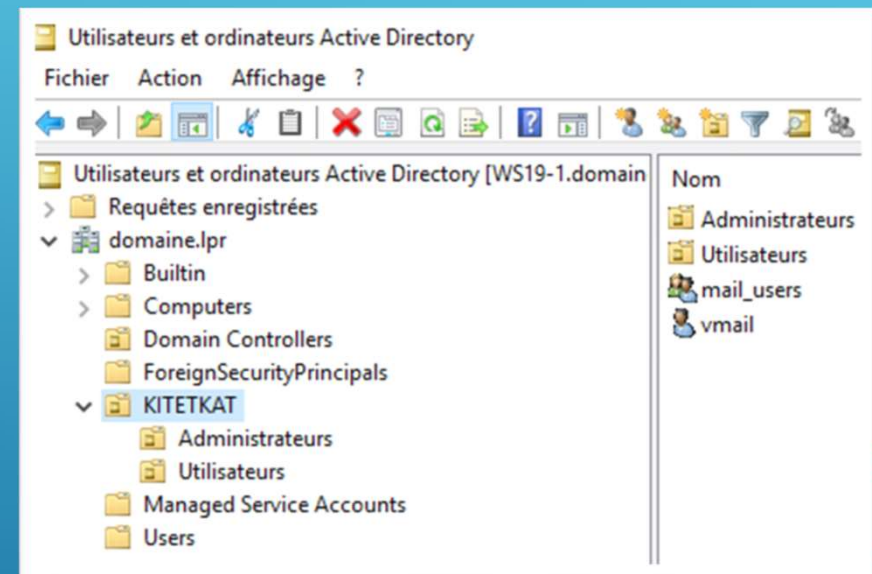
Adresse IP du client	Nom
192.168.10.193	WS19-1
192.168.10.194	SRV-Intranet
192.168.10.195	CLIENT2
192.168.10.199	SRV-Antivirus
192.168.10.205	SRV-Supervision
192.168.10.206	truenas
192.168.10.208	srv-mail
192.168.10.254	PfSense

DÉPLOIEMENT DU SERVEUR HÔTES

AD-DS

Résumé de l'AD de test déployé :

- UO test « **KITETKAT** »
- 2 sous-UO « **Administrateurs** » / « **Utilisateurs** »
- Objectif : monter un partage de fichiers utilisé pour la sauvegarde du serveur de fichiers avec le NAS.



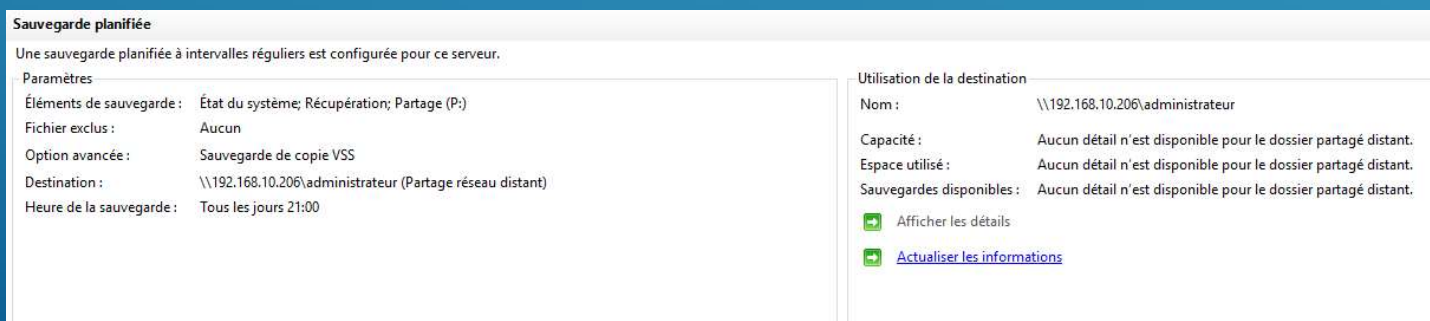
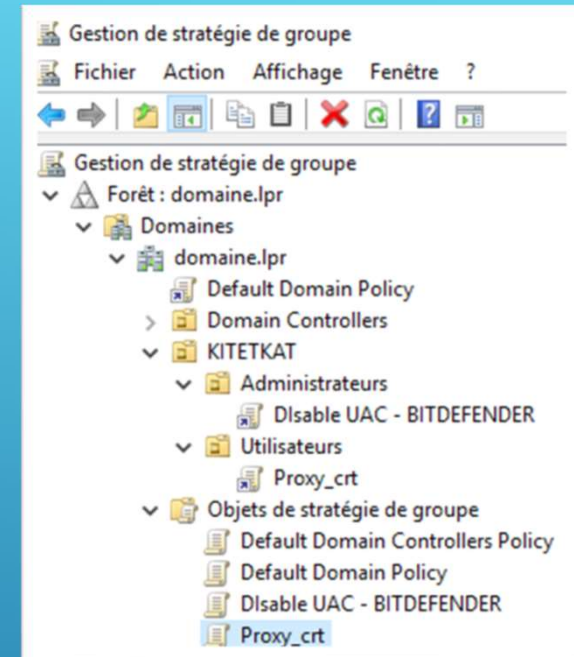
DÉPLOIEMENT DU SERVEUR HÔTES

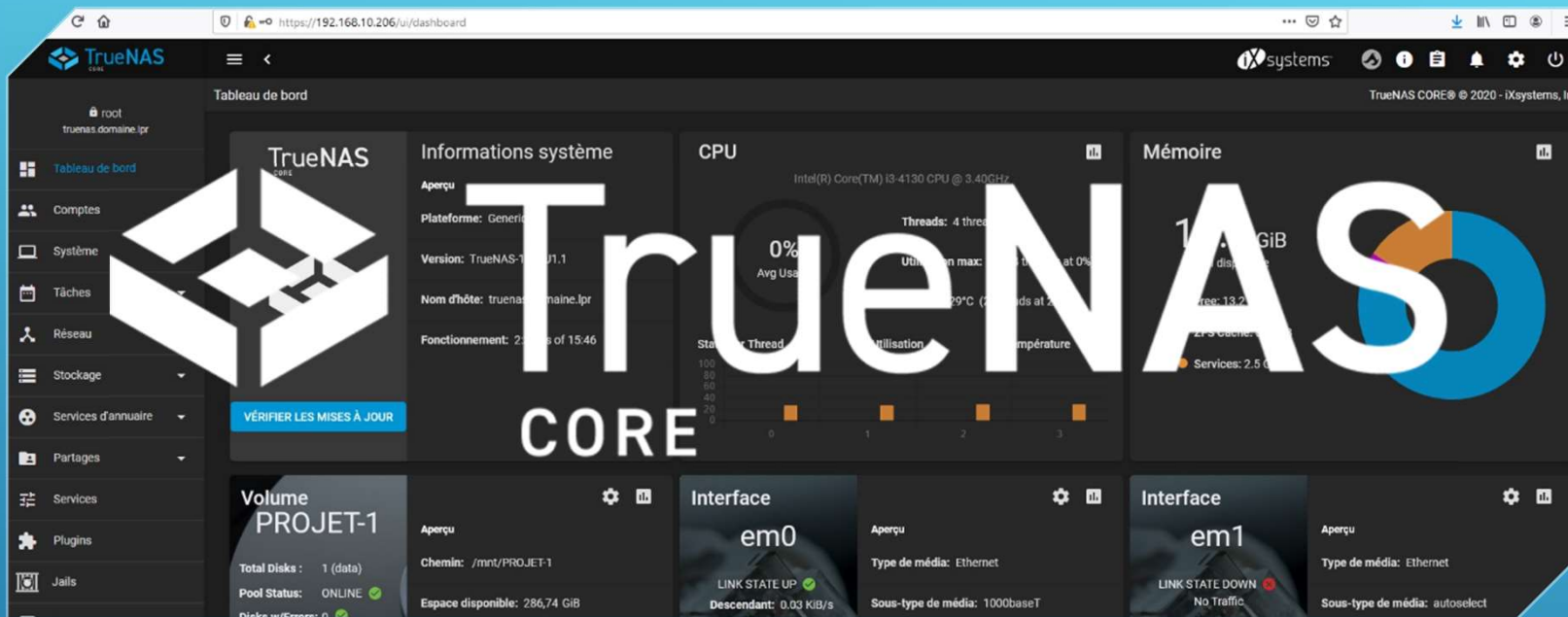
GPO

Proxy crt : ajout d'une autorité de certification sur les machines clientes

Disable UAC - BitDefender : désactivation de l'UAC pour installer l'agent BitDefender sur les postes clients depuis l'appliance GravityZone

SAUVEGARDE DISTANTE





DÉPLOIEMENT DU SERVEUR NAS

DÉPLOIEMENT DU SERVEUR NAS

SYNCHRONISATION AVEC ACTIVE DIRECTORY

- Paramétrage avec informations du Contrôleur de Domaine

Identifiants du Domaine

Nom de domaine *

DOMAINE.LPR

☒ Activer (requiert le mot de passe ou le principal Kerberos) ?

☐ Niveau de journalisation ? ☒ Autoriser les mises à jour DNS ?

☒ Autoriser les domaines approuvés ? ☐ Désactiver le cache FreeNAS ?

☒ Utiliser le domaine par défaut ? ☐ Restreindre PAM ?

Nom du site

DOMAINE.LPR ?

Délai d'attente DNS

10

Realm Kerberos

▼ ?

Winbind NSS Info

Kerberos Principal

TRUENAS\$@DOMAINE.LPR ▼ ?

Nom NetBIOS *

truenas

Compte d'ordinateur OU

?

Alias NetBIOS

Délai d'expiration AD

60 ?

ENREGISTRER OPTIONS DE BASE MODIFIER IDMAP RECONSTRUCTION DU CACHE DU SERVICE D'ANNUAIRE

Informations d'identification du serveur

Nom d'hôte *

WS19-1.domaine.lpr ?

Base DN

DC=domaine,DC=lpr

Bind DN

CN=ldapbind,CN=Users,DC=domaine,DC=lpr

Bind Password

?

☒ Activer ?

☐ Autoriser la liaison anonyme ?

Realms Kerberos

DOMAINE.LPR ▼ ?

Kerberos Principal

▼ ?

Mode de chiffrement

OFF ▼ ?

Certificat

▼ ?

☒ Valider les certificats ?

☐ Désactiver le cache utilisateur/groupe LDAP ?

Délai d'attente LDAP

10

Délai d'attente DNS

10

☐ Samba Schema (DEPRECATED - see help text) ?

Paramètres auxiliaires

Schéma

RFC2307

ENREGISTRER OPTIONS DE BASE MODIFIER IDMAP RECONSTRUCTION DU CACHE DU SERVICE D'ANNUAIRE

DÉPLOIEMENT DU SERVEUR NAS

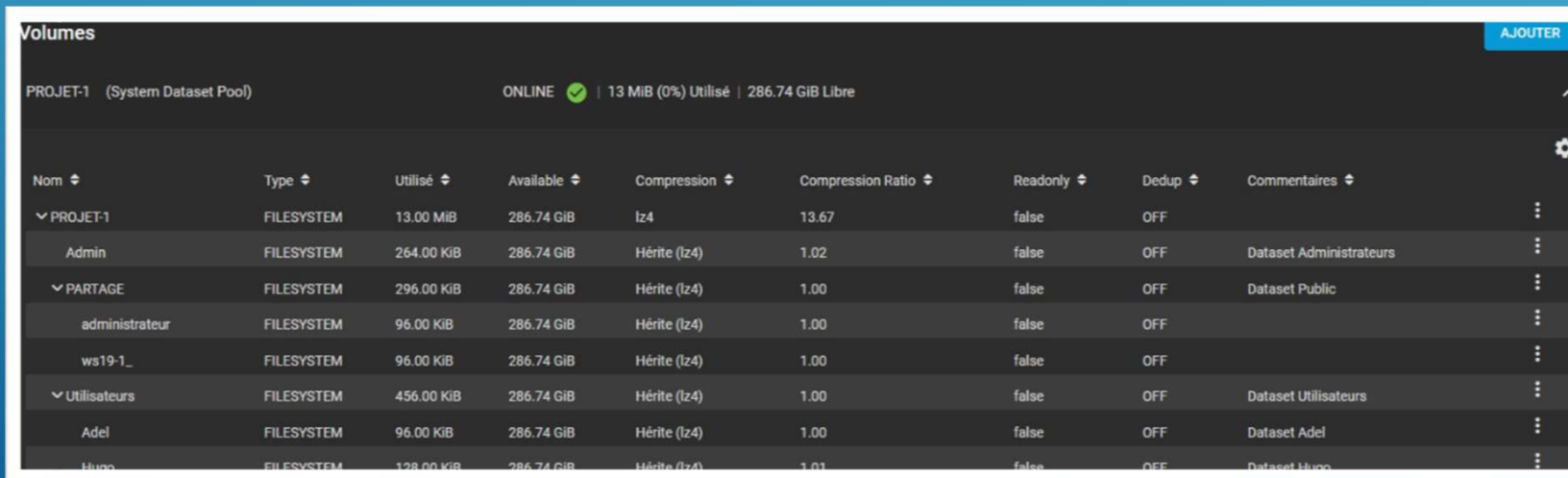
CRÉATION DES VOLUMES

- 3 volumes créés :

Admin : envoi des confs réseaux des différents EAR

Partage : sauvegarde distante du serveur de fichiers

Utilisateurs : pour les répertoires privés des utilisateurs



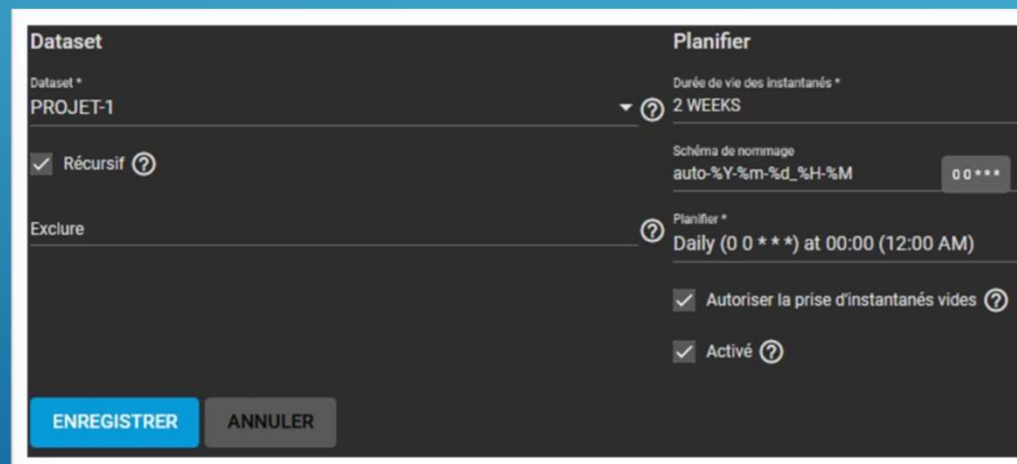
The screenshot shows a web interface for managing volumes. At the top, it says 'Volumes' and 'PROJET-1 (System Dataset Pool)' with a status 'ONLINE' and a green checkmark. Below this is a table with columns: Nom, Type, Utilisé, Available, Compression, Compression Ratio, Readonly, Dedup, and Commentaires. The table lists three main volumes: PROJET-1, PARTAGE, and Utilisateurs, each with its own sub-entries.

Nom	Type	Utilisé	Available	Compression	Compression Ratio	Readonly	Dedup	Commentaires
PROJET-1	FILESYSTEM	13.00 MiB	286.74 GiB	lz4	13.67	false	OFF	
Admin	FILESYSTEM	264.00 KiB	286.74 GiB	Hérite (lz4)	1.02	false	OFF	Dataset Administrateurs
PARTAGE	FILESYSTEM	296.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Public
administrateur	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	
ws19-1_	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	
Utilisateurs	FILESYSTEM	456.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Utilisateurs
Adel	FILESYSTEM	96.00 KiB	286.74 GiB	Hérite (lz4)	1.00	false	OFF	Dataset Adel
Hugo	FILESYSTEM	128.00 KiB	286.74 GiB	Hérite (lz4)	1.01	false	OFF	Dataset Hugo

DÉPLOIEMENT DU SERVEUR NAS

CRÉATION DES INSTANTANÉS

- Sauvegarde automatique 1 fois par jour
- Paramétrage : 2 semaines de rétention de données



The screenshot displays a configuration window for creating snapshots, divided into two main sections: 'Dataset' and 'Planifier'.

Dataset Section:

- Dataset ***: PROJET-1
- ☒ **Récursif** ?
- Exclure**: (Empty list)

Planifier Section:

- Durée de vie des instantanés ***: 2 WEEKS
- Schéma de nommage**: auto-%Y-%m-%d_%H-%M (with a 00**** mask)
- Planifier ***: Daily (0 0 * * *) at 00:00 (12:00 AM)
- ☒ **Autoriser la prise d'instantanés vides** ?
- ☒ **Activé** ?

At the bottom, there are two buttons: **ENREGISTRER** (highlighted in blue) and **ANNULER**.

DÉPLOIEMENT DU SERVEUR DE SUPERVISION



- Surveillance de l'état des divers services réseaux, serveurs et autres matériels réseau
- Production de graphiques dynamiques

Création de comptes
d'administrateurs
nominatifs

A screenshot of the Zabbix web interface's 'Administration' section. On the left is a sidebar menu with 'Administration' selected, showing sub-items: 'Général', 'Proxys', and 'Authentification'. The main area displays a table of users. Each row has a checkbox in the first column. The table columns are: Alias, Prénom, Nom de famille, Type d'utilisateur, and Groupes.

<input type="checkbox"/>	Alias ▲	Prénom	Nom de famille	Type d'utilisateur	Groupes
<input type="checkbox"/>	Admin	Zabbix	Administrator	Super Administrateur Zabbix	Zabbix administrators
<input type="checkbox"/>	adm_h.desouza			Utilisateur Zabbix	Zabbix administrators
<input type="checkbox"/>	adm_j.alba			Utilisateur Zabbix	Zabbix administrators
<input type="checkbox"/>	guest			Utilisateur Zabbix	Disabled, Guests

DÉPLOIEMENT DU SERVEUR DE SUPERVISION

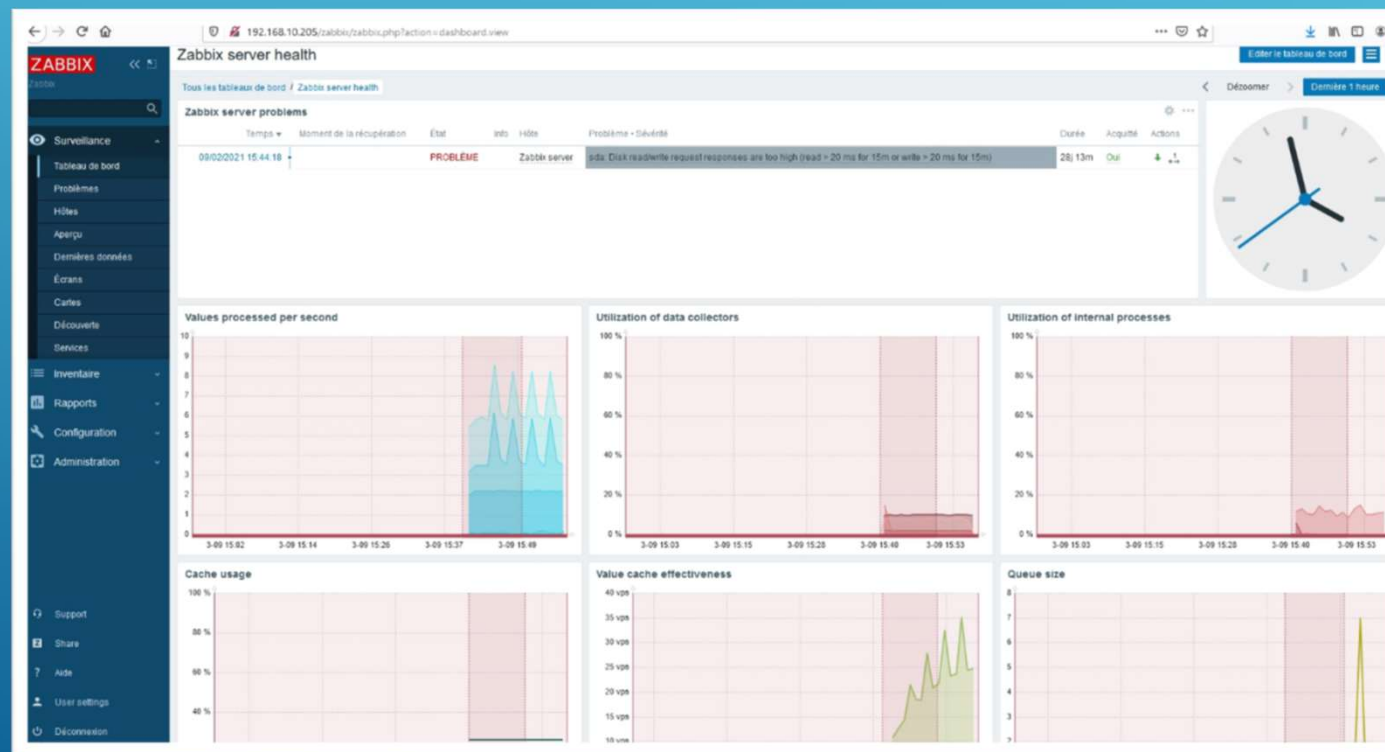
CONFIGURATION DES HÔTES

- Création de templates « machines »
- Déploiement automatique des agents
- Remontée des équipements

	Applications	Éléments	Déclencheurs	Graphiques	Découverte	Web	IP	Interface	Prox	Modules	État	Disponibilité	Comment
<input type="checkbox"/> CLIENT2	Applications 22	Éléments 172	Déclencheurs 105	Graphiques 37	Découverte 4	Web	192.168.10.3:10050			Template OS Windows by Zabbix agent (Template Module Windows CPU by Zabbix agent, Template Module Windows filesystems by Zabbix agent, Template Module Windows generic by Zabbix agent, Template Module Windows memory by Zabbix agent, Template Module Windows network by Zabbix agent, Template Module Windows physical disks by Zabbix agent, Template Module Windows services by Zabbix agent, Template Module Zabbix agent)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> PFSense	Applications 11	Éléments 70	Déclencheurs 16	Graphiques 22	Découverte 2	Web	192.168.10.254:10050			Template OS FreeBSD (Template Module Zabbix agent)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> Srv-Backup	Applications 32	Éléments 138	Déclencheurs 95	Graphiques 29	Découverte 3	Web	192.168.10.208:10050			Template OS Linux by Zabbix agent (Template Module Linux block devices by Zabbix agent, Template Module Linux CPU by Zabbix agent, Template Module Linux filesystems by Zabbix agent, Template Module Linux generic by Zabbix agent, Template Module Linux memory by Zabbix agent, Template Module Linux network interfaces by Zabbix agent, Template Module Zabbix agent)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> Switch 1	Applications 9	Éléments 14	Déclencheurs 9	Graphiques 1	Découverte 8	Web	192.168.10.200:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> Switch 2	Applications 33	Éléments 236	Déclencheurs 109	Graphiques 25	Découverte 8	Web	192.168.10.201:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> Switch 3	Applications 9	Éléments 14	Déclencheurs 9	Graphiques 1	Découverte 8	Web	192.168.10.202:161			Template Net HP Enterprise Switch SNMP (Template Module EtherLike-MIB SNMP, Template Module Generic SNMP, Template Module Interfaces SNMP)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> WS19-1	Applications 22	Éléments 198	Déclencheurs 132	Graphiques 37	Découverte 4	Web	192.168.10.193:10050			Template OS Windows by Zabbix agent (Template Module Windows CPU by Zabbix agent, Template Module Windows filesystems by Zabbix agent, Template Module Windows generic by Zabbix agent, Template Module Windows memory by Zabbix agent, Template Module Windows network by Zabbix agent, Template Module Windows physical disks by Zabbix agent, Template Module Windows services by Zabbix agent, Template Module Zabbix agent)	Activé	ZBX SNMP JMX PM	AUCUN
<input type="checkbox"/> Zabbix server	Applications 17	Éléments 127	Déclencheurs 58	Graphiques 25	Découverte 3	Web	127.0.0.1:10050			Template App Zabbix Server, Template OS Linux by Zabbix agent (Template Module Linux block devices by Zabbix agent, Template Module Linux CPU by Zabbix agent, Template Module Linux filesystems by Zabbix agent, Template Module Linux generic by Zabbix agent, Template Module Linux memory by Zabbix agent, Template Module Linux network interfaces by Zabbix agent, Template Module Zabbix agent)	Activé	ZBX SNMP JMX PM	AUCUN

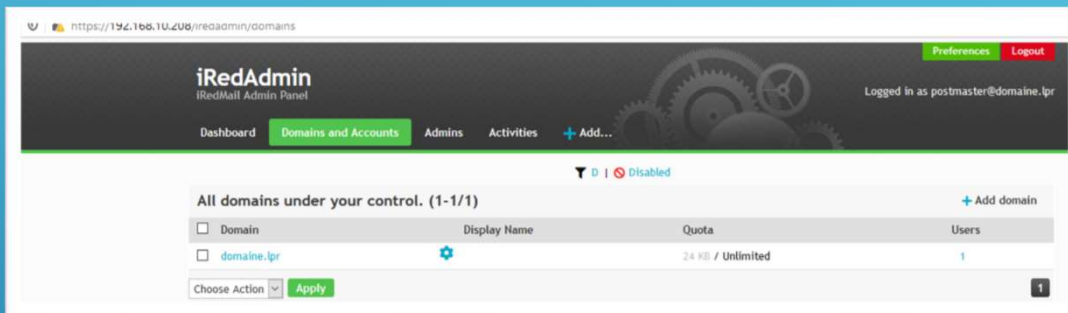
DÉPLOIEMENT DU SERVEUR DE SUPERVISION

INTERFACE TYPE DE MONITORING :



DÉPLOIEMENT DU SERVEUR DE MAIL

SYNCHRONISATION ACTIVE DIRECTORY



- Synchronisation avec AD
- Utilisation du serveur Mail en interface Web



DÉPLOIEMENT DU SERVEUR WEB

- Système de gestion de contenu libre
- Open Source
- Nombreuses fonctionnalités participatives :
 - News
 - Blogs
 - Sondages
 - Flux RSS

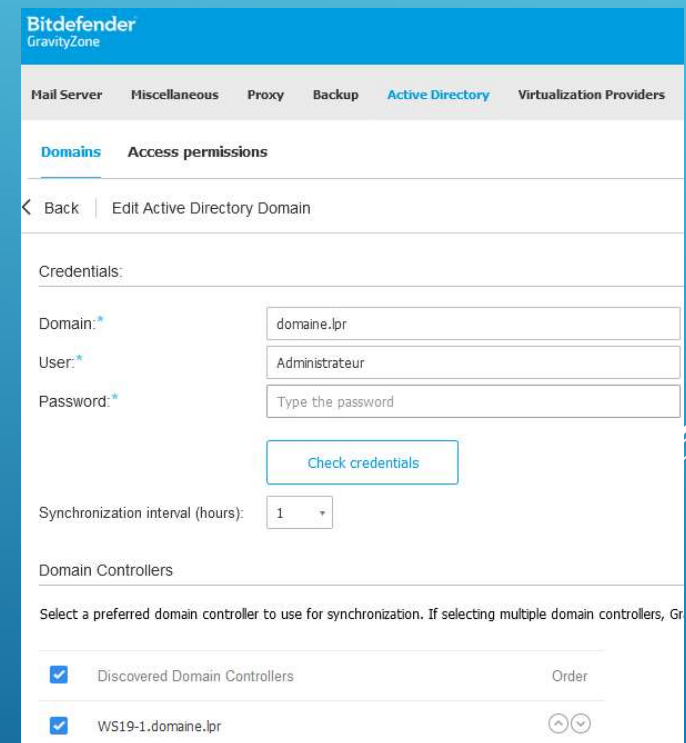
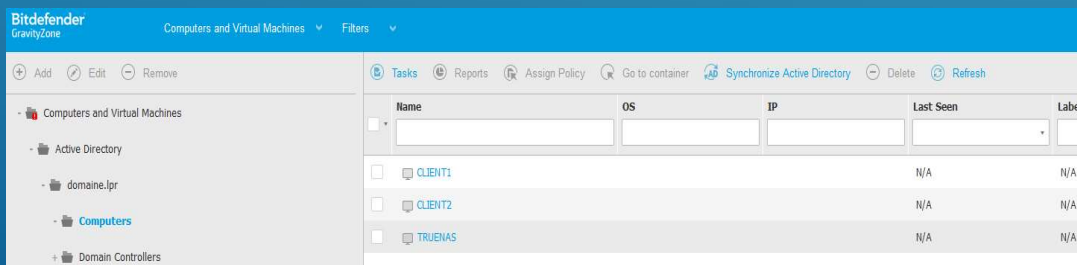


MISE EN PLACE DU CONTEXTE SSI

DÉPLOIEMENT DU SERVEUR ANTI-VIRUS

SYNCHRONISATION ACTIVE DIRECTORY

- Création d'une machine virtuelle sous HYPER-V
- Installation du serveur Anti-Virus,
- Configuration de l'interface Web,
- Création des packages d'installation des agents




```

Fichier  Édition  Affichage  Rechercher  Terminal  Aide
*****
Insérer une clé USB pour commencer...
*****
Clé USB détectée
*****
Début de l'analyse...
*****
/media/analyse/6D07AF9C6C0D0DED/ms.docx: OK
/media/analyse/6D07AF9C6C0D0DED/racie.txt: Eicar-T
/media/analyse/6D07AF9C6C0D0DED/racie.txt: moved to
/media/analyse/6D07AF9C6C0D0DED/text.txt: OK
/media/analyse/Test 1/ist/20180206_105711.jpg: OK
/media/analyse/Test 1/ist/20180206_105810.jpg: OK
/media/analyse/Test 1/ist/20180206_113140.jpg: OK
/media/analyse/Test 1/ist/20180206_131854.jpg: OK
/media/analyse/Test 1/ist/20180206_131914.jpg: OK
/media/analyse/Test 1/ist/20180206_131933.jpg: OK
/media/analyse/Test 1/ist/20180206_132537.jpg: OK
/media/analyse/Test 1/ist/20180206_132617.jpg: OK

----- SCAN SUMMARY -----
Known viruses: 6417252
Engine version: 0.99.3
Scanned directories: 7
Scanned files: 11
Infected files: 1
Data scanned: 20.25 MB
Data read: 20.06 MB (ratio 1.01:1)
Time: 18.985 sec (0 m 18 s)
*****
Analyse terminée !

  Y^
 / \
( ) ( )
 ^
8====|""|====8
   LLLU

CETTE CLE EST INFECTEE !!!

Merci d'insérer de nouveau la clé
pour valider la désinfection
*****
Veuillez retirer la clé...
*****

```

DÉPLOIEMENT DE LA STATION BLANCHE

- Utilitaire antivirscan :
 - scan des supports insérés
- Utilisation antivirus Clamav:
 - mise à jour des définitions de virus hors-ligne

PLAN DE SAUVEGARDES

- LISTING DES PROCEDURES DE SAUVEGARDES DÉTAILLÉ
- FICHES DE TACHES PAS-A-PAS



PLAN DE REPRISE D'ACTIVITÉ

- PROCÉDURES DE RESTAURATION EN CAS DE SINISTRES SUR LES SYSTÈMES ET LES ÉQUIPEMENTS

PROCÉDURE D'EXPLOITATION VERACRYPT



- MISE EN PLACE LOGICIEL DE CRYPTAGE DES DONNÉES
- FORMATION A L'UTILISATION
- PROCÉDURE DÉTAILLÉE

CHARTER RGPD

- MODALITÉS DE MANIPULATION DES DONNÉES
- DROITS INHÉRENTS AUX UTILISATEURS



FICHES-RÉFLEXE

- EN CAS D'INCIDENT SSI
- SIMPLE À METTRE EN OEUVRE



SENSIBILISATION SSI

- LES BONS GESTES À ADOPTER
- UNE HYGIÈNE NUMÉRIQUE À RESPECTER



FORMATION CYBER

- DISPENSÉE PAR LES EXPERTS DE LA « SOCIÉTÉ FUTURZO »



RETOUR D'EXPÉRIENCE

- Capitalisation des connaissances acquises durant le développement du projet
- Obstacles surmontés pendant le déploiement



QUESTIONS ?

