

ANNEXES

DOSSIER PROFESSIONNELLE - ANNEXES - IZABELA KASIAZ - TSSR 2024

Sommaire

1. Assister les utilisateurs en centre de services

- Création d'un cluster VM sous VMWare
- Schéma réseau logique et physique
- Expliquer le fonctionnement des DevEnv via procédure aux utilisateurs

2. Maintenir, exploiter et sécuriser une infrastructure centralisée

- Firewall avec gestion zones WAN, LAN, DMZ
- Maintenir et exploiter un environnement virtualisé : Gérer les différents espaces de stockage
- Maintenir et exploiter un domaine ActiveDirectory et les serveurs Windows : Création et gestion Users, UO, groupes

3. Maintenir et exploiter une infrastructure distribuée et contribuer à sa sécurisation

- Script Linux Backup (Cron –rsync –bucket S3)
- Création de VM sur AWS (Cloud computing)
- Veille technologique - présentation Linux et son fonctionnement

4. Administrer les serveurs Linux

- Développer des scripts d'automatisation
- Créer des utilisateurs ainsi que des groupes et donner accès en SSH
- Mettre une application en production

Activités-type accompagnées d'exemples détaillés

1. Assister les utilisateurs en centre de services

- Création d'un cluster VM sous VMWare

Objectif : La maquette VmWare doit avoir des serveurs fonctionnels et communicants par différents réseaux.

Cluster sous VMWare Workstation :

- 1 server hyperviseur 1
- 1 serveur hyperviseur 2
- 1 serveur SAN (ISCSI)
- 1 serveur AD
- 1 serveur DHCP
- 1 serveur 2019 Ori (clone qui à servi à créer les autres)
- 1 PC win10

4 Réseaux mis en place :

1. Carte réseau NAT = MAJ
2. 192.168.0.0 / 24 = LAN ISCSI

Première machine = 192.168.0.1

Dernière machine = 192.168.0.254

= Network Adapter 2

Segment LAN SAN ISCSI 192.168.0.1

Segment LAN HyperV2 ISCSI 192.168.0.2

Segment LAN HyperV1 ISCSI 192.168.0.3

Segment LAN AD ISCSI 192.168.0.4

Segment LAN PC1 ISCSI 192.168.0.5

3. 192.168.10.0 = LAN PROD

Première machine = 192.168.10.1
Dernière machine = 192.168.10.254

= Network Adapter 3

Segment LAN PROD SAN 192.168.10.1

Segment LAN PROD HyperV1 192.168.10.2

Segment LAN PROD HyperV2 192.168.10.3

Segment LAN PROD AD 192.168.10.4

Segment LAN PROD PC1 192.168.10.5

4. 192.168.20.0 = LAN HEARBEAT

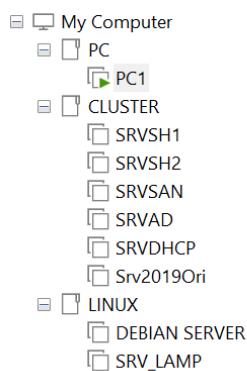
Premiere machine = 192.168.20.1
Derniere machine = 192.168.20.254

= Network Adapter 4

Segment LAN Heartbeat SAN 192.168.20.1
Segment LAN Heartbeat HyperV1 192.168.20.2
Segment LAN Heartbeat HyperV2 192.168.20.3
Segment LAN Heartbeat AD 192.168.20.4
Segment LAN Heartbeat PC1 192.168.20.5



cartes réseaux du SAN



VM listées sur VMWare

Rôle ISCSI sur le NAS

LINUX SRVSAN SRVSH1 SRVSH2

Gestionnaire de serveur

Gestionnaire de serveur > Services de fichiers et de stockage > Volumes >

VOLUMES

Tous les volumes | 5 au total

Volume	Statut	Nom de système...	Allocation	Capacité	Espace libre	Taux de déduplication	Gain de déduplication	Pourcentage u...
SVRSAN (5)								
F:	Quorum	Inconnu	4.98 Go	4.86 Go				
C:		Fixe	39.4 Go	25.3 Go				
E:		StockVm	25.0 Go	24.8 Go				
\?\Volume\63...	Récupération	Fixe	499 Mo	104 Mo				
\?\Volume\29...		Fixe	95.0 Mo	69.1 Mo				

Dernière actualisation : 03/08/2023 14:56:10

RESSOURCES PARTAGÉES

Aucun volume n'est sélectionné.

DISQUE

Aucun volume sélectionné.

DISQUES VIRTUELS iSCSI

Aucun volume sélectionné.

TACHES

LINUX SRVSAN SRVSH1 SRVSH2

Gestionnaire de serveur

Gestionnaire de serveur > Services de fichiers et de stockage > Volumes > Disques >

DISQUES

Tous les disques | 3 au total

Numéro	Disque virt...	État	Capacité	Non alloué	Partition	Lecture se...	En cluster	Sous-systè...	Type de...	Nom
SVRSAN (3)										
0	En ligne	25.0 Go	1.00 Mo	GPT				NVMe	VMware Virtual NVMe Disk	
1	En ligne	5.00 Go	1.00 Mo	GPT				NVMe	VMware Virtual NVMe Disk	
2	En ligne	40.0 Go	0.00 O	GPT				NVMe	VMware Virtual NVMe Disk	

Dernière actualisation : 03/08/2023 14:56:41

VOLUMES

Volumes associés | 1 au total

Volume	Statut	Allocation	Capacité	Espace libre	Taux de déduplication	Gain de déduplication	Pourcentage
SVRSAN (1)							
E:	Fixe	25.0 Go	24.8 Go				

POOL DE STOCKAGE

VMware Virtual NVMe Disk sur SVRSAN

Aucun pool de stockage associé n'existe.

TACHES

DISQUES VIRTUELS iSCSI

Chemin d'accès	État	Statut du disque virtuel	Nom de la cible	Statut de la cible	ID d'initiateur
E:\iSCSI\VirtualDisks\StockVm.vhdx	Connecté	stockvmtarget	Connecté	IPAddress:192.168.0.2; IPAddress:192.168.0.3; IQN:iqn.1991-05.com.microsoft\svrsh1hv; IQN:iqn.1991-05.com.microsoft\svrsh2hv	
F:\iSCSI\VirtualDisks\Quorum.vhdx	Connecté	quorумtarget	Connecté	IPAddress:192.168.0.2; IPAddress:192.168.0.3; IQN:iqn.1991-05.com.microsoft\svrsh1hv; IQN:iqn.1991-05.com.microsoft\svrsh2hv	

CIBLES iSCSI

Nom	Nom du serveur	Nom qualifié cible	Statut de la cible	ID d'initiateur
stockvmtarget	SVRSAN	iqn.1991-05.com.microsoft\svrsan-stockvmtarget-target	Connecté	IPAddress:192.168.0.2; IPAddress:192.168.0.3; IQN:iqn.1991-05.com.microsoft\svrsh1hv; IQN:iqn.1991-05.com.microsoft\svrsh2hv

Configuration des deux disques Quorum (5go) et StockVM (25go)

VIRTUAL MACHINE SETTINGS

Hardware Options

DISQUES VIRTUELS

Chemin d'accès	Summary
E:\iSCSI\VirtualDisks\StockVm.vhdx	2 GB
F:\iSCSI\VirtualDisks\Quorum.vhdx	5 GB

CIBLES iSCSI

Nom	Nom
stockvmtarget	SVRSAN

Memory

Specify the amount of memory allocated to this virtual machine. The memory size must be a multiple of 4 MB.

Memory for this virtual machine: MB

32 GB - 16 GB - 8 GB - 4 GB - 2 GB - 1 GB - 512 MB - 256 MB - 128 MB - 64 MB - 32 MB - 16 MB - 8 MB - 4 MB -

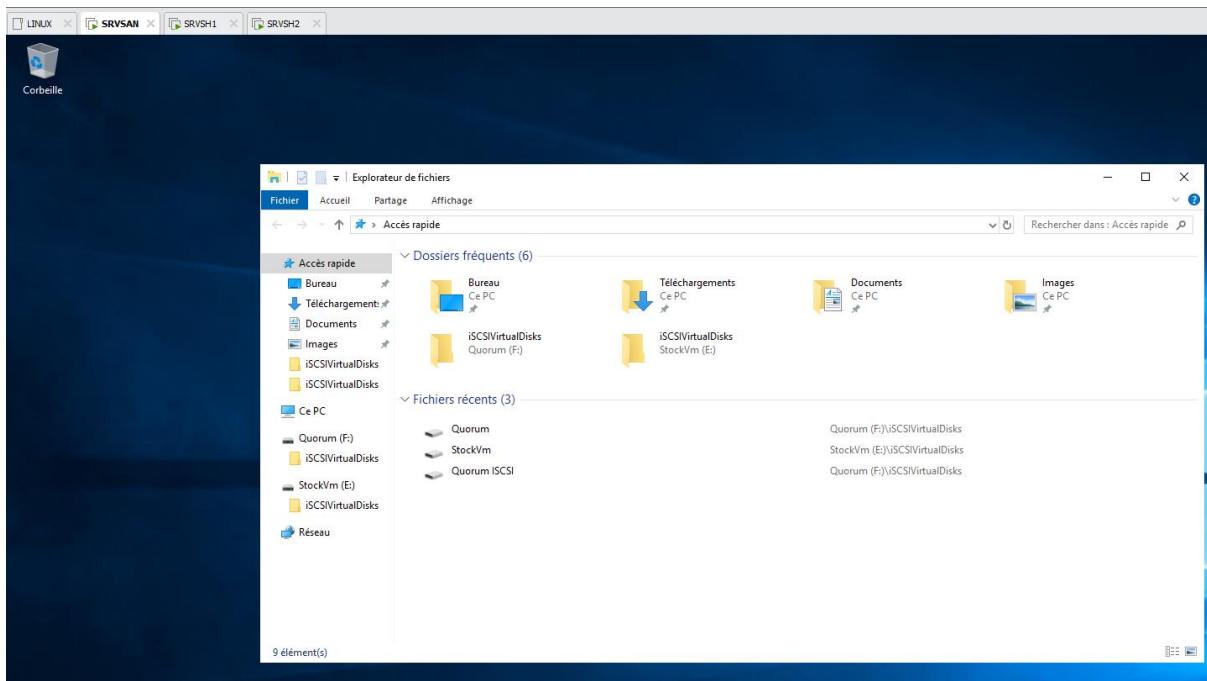
■ Maximum recommended memory
(Memory swapping may occur beyond this size.)

■ Recommended memory
2 GB

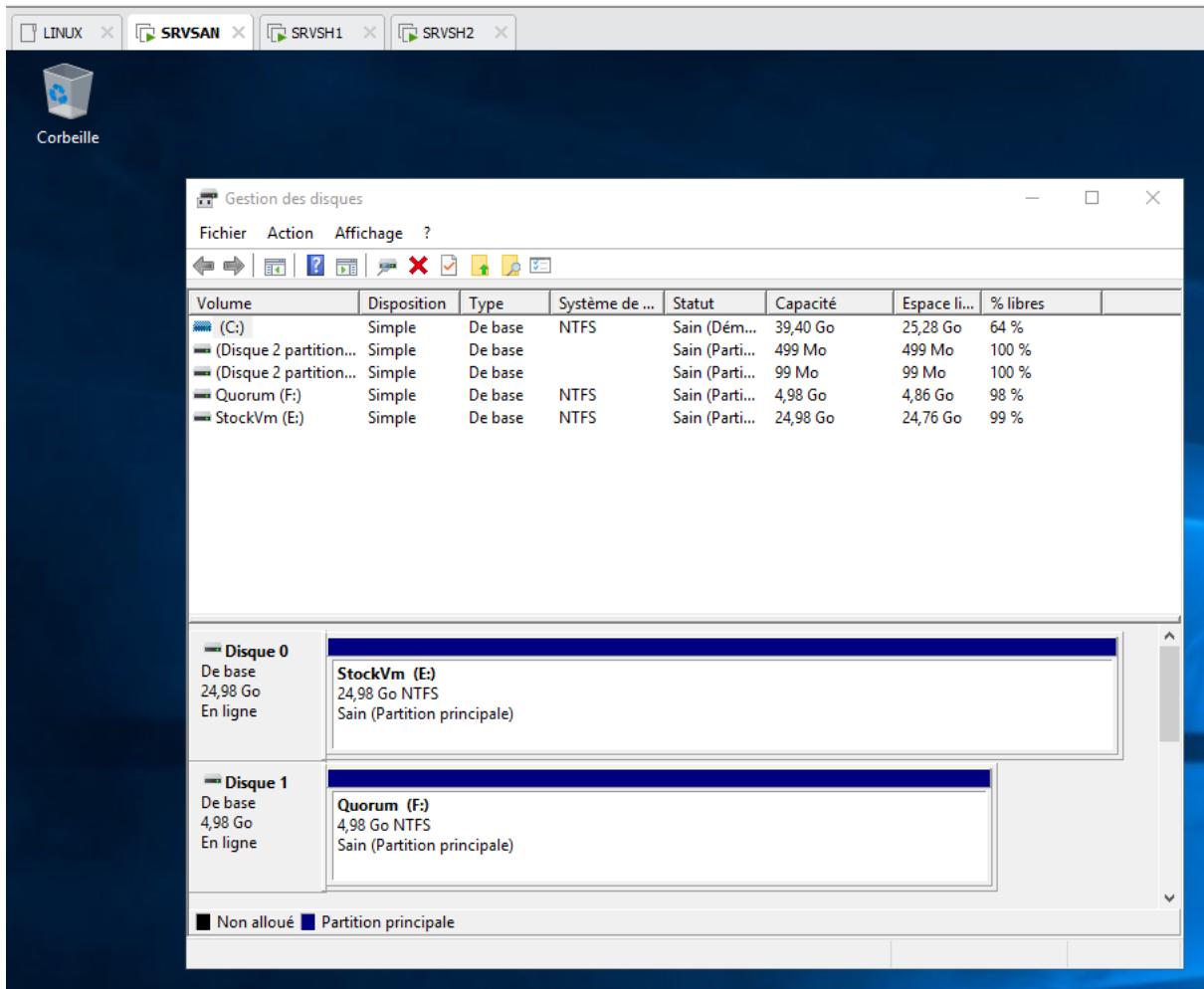
■ Guest OS recommended minimum
1 GB

The virtual machine must be powered off to reduce the amount of memory.

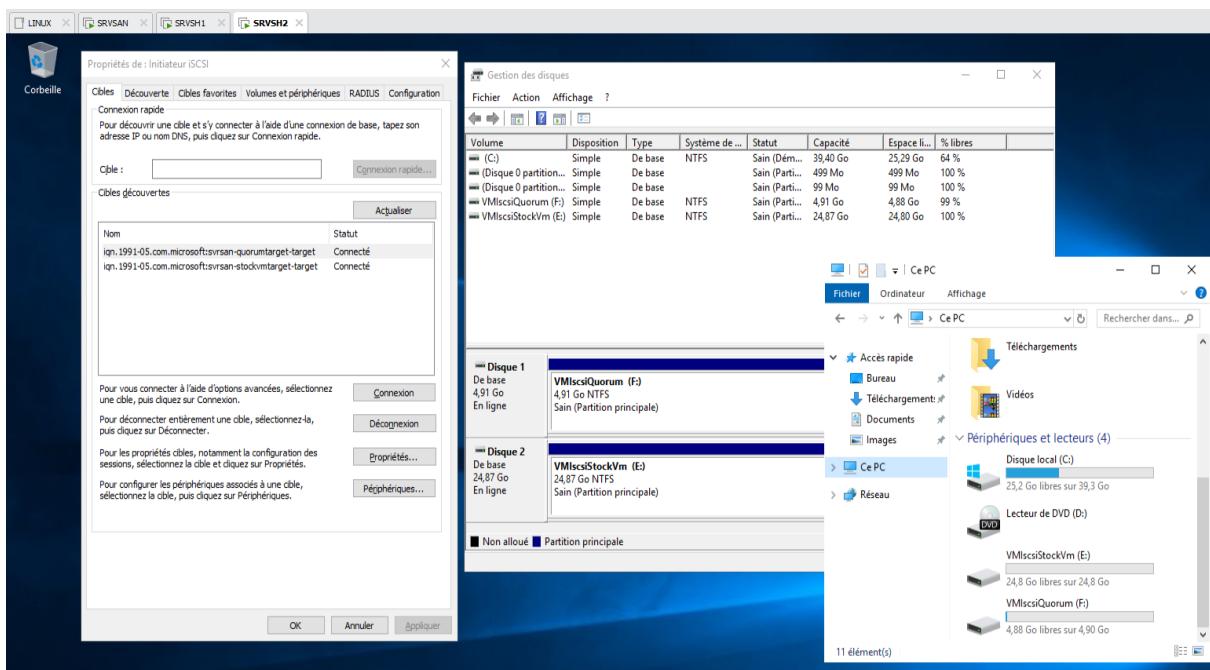
Configuration des disques sur VMWare



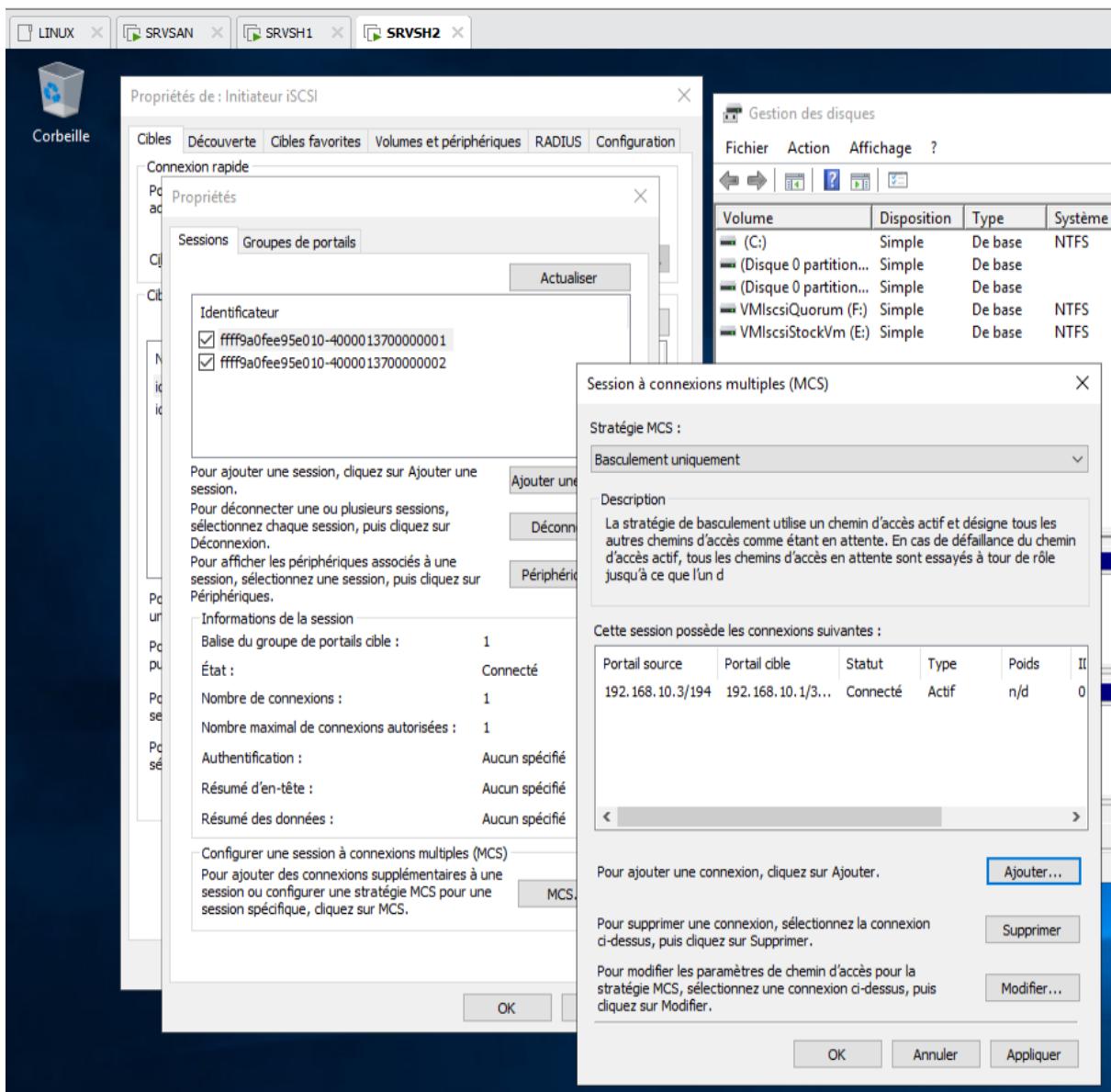
Disques visibles dans l'explorateur de fichiers du NAS



Disques visibles dans le gestionnaire de disques



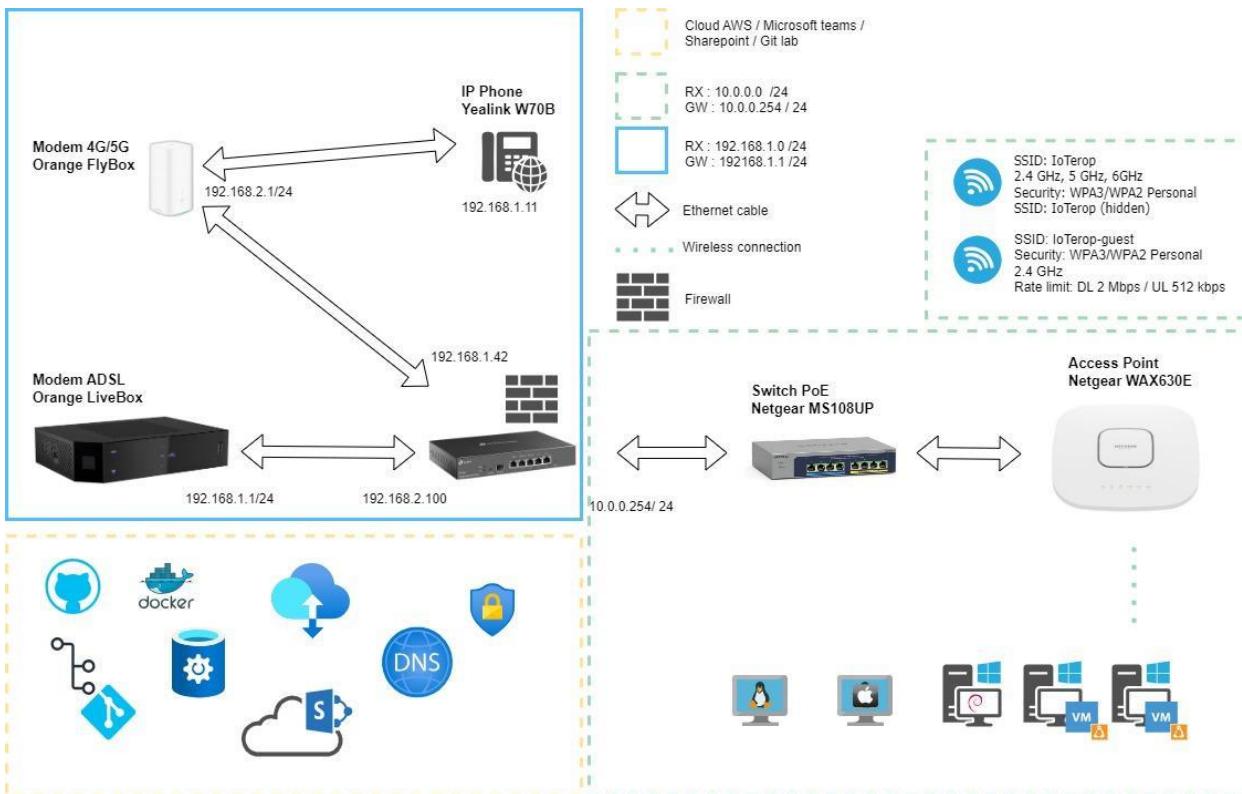
Connection aux cibles par les initiateurs H1 et H2



Stratégie de basculement configuré

- Schéma réseau logique et physique

Logique :



Physique :



Adressage IP

ORGANISATION NOUVEAUX LOCAUX IOTEROP

Tableau adressage IP

Réseaux	Adresse IP	Mask	Gateway	Broadcast	DHCP	DNS	Materiel	IP GUI
loterop	10.0.0.0	/24	10.0.0.254	10.0.0.255	x	10.0.0.254	Modem 4G / 5G Orange flyBox	192.168.2.1
WAN 4G 5G	192.168.1.0	/24	192.168.1.1				Modem ADSL Orange LivBox	192.168.1.1
WAN ADSL	192.168.2.0	/24	192.168.2.1				IP Phone Yeahlink W70B	192.168.1.11
							Router TP-Link ER7206	192.168.1.42
							Switch PoE	
							Netgear MS108UP	10.0.0.254
							Access Point	
							Netgear WAX630E	10.0.0.11

Accès config matériel :

The screenshot shows the Flybox web interface with the following sections:

- Connexion:** Shows connection status (Connected to Orange), roaming status (Roaming désactivé), time elapsed (87:14:11), and network usage (5G).
- Utilisation:** Displays data usage statistics: Mon usage (157.6 Go National, 0 Mo International), Session actuelle (110.8 Go National, 46.7 Go International), and Mon compte (Access to client space).
- Messages:** A section for messaging with a button to connect as administrator.
- Réseaux Wi-Fi:** A section for managing Wi-Fi networks with a connection status icon.

The screenshot shows the Livebox web interface with the following sections:

- authentification:** An authentication form for users with fields for identifiant (Admin) and mot de passe (password).
- mes services:** A status section showing Internet xDSL (green icon) and téléphonie indisponible (red warning icon).

At the bottom, there are links for contact, recommandations, déclaration d'accessibilité, and the copyright notice Orange © copyright 2023.



- Expliquer le fonctionnement des DevEnv via procédure aux utilisateurs

DevEnv

Setup and run tutorial

31.05.2023

Contents

1.1.	Configuration required	4
1.1.1.	First, in WSL / Linux distribution:.....	4
1.1.2.	install the tools :	4
1.2.	AWS configuration.....	5
1.3.	Git clone	5
1.4.	Run DevEnv	6
1.5.	k9s	6
1.5.1.	Utility	6
1.5.2.	Access	6
1.6.	Access to DevEnv Alaska.....	9
1.7.	Rename your DevEnv / Distrib	10
1.8.	Debug	10

1.1. Configuration required

Warnings:

- Before bellow steps, Ops team have to set up an additional AWS account:
 - To access to a DevEnv you will use Access key ID and Secret access key provide by the Op team.
- All information comes from experience and the ops team ([GitLab DevEnv page](#)).
- In this tutorial was used a Debian distribution on WSL2, on Windows 11.
- It is necessary to set WSL2, not WSL1 to use the DevEnvironment.

1.1.1. First, in WSL / Linux distribution:

Create a "devenvironment" folder in your file system. We recommend to use the file architecture available on the loterop gitlab.

```
ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure$ mkdir devenvironment
ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure$ ls
devenvironment
ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure$ cd devenvironment/
ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure/devenvironment$
```



1.1.2. install the tools :

- [AWS CLI](#)
- [Helm](#)
- [Kubectl](#)
- [Terraform](#) (easier with [Homebrew on Linux — Homebrew Documentation](#))

To resolve “-bash: lsb_release: command not found”

\$ sudo apt-get install lsb-release

- [Terragrunt](#)

```
$ wget https://github.com/gruntwork-io/terragrunt/releases/download/v0.45.17/terragrunt_linux_amd64  
$ sudo chmod +x terragrunt_linux_amd64  
$ sudo mv terragrunt_linux_amd64 /usr/local/bin/terragrunt  
• K9S  
$ wget https://github.com/derailed/k9s/releases/download/v0.27.4/k9s_Linux_amd64.tar.gz  
$ tar -xvf k9s_Linux_amd64.tar.gz  
$ sudo mv k9s /usr/local/bin  
• jq
```

1.2. AWS configuration

```
$ helm plugin install https://github.com/hypnoglow/helm-s3.git
```

```
$ aws configure
```

You will set up :

- Access key ID
- Secret access key
- region eu-west-1
- format files: none

```

ikqa@IzabelaM:~/ioterop/PaaS/ops/infrastructure/devenvironment$ cd ..
ikqa@IzabelaM:~/ioterop/PaaS/ops/infrastructure/devenvironment$ helm plugin install https://github.com/hypnoglow/helm-s3.git
Downloading and installing helm-s3 v0.14.0 ...
Checksum is valid.
Installed plugin: s3
ikqa@IzabelaM:~/ioterop/PaaS/ops/infrastructure/devenvironment$ aws configure
AWS Access Key ID [None]: AKIAITP772JXQVZP6L42F4FM.F
AWS Secret Access Key [None]: YPRQNEPPLzyKaaaQqAJP77f5HQTOB480ZsBY
Default region name [None]: eu-west-1
Default output format [None]:
ikqa@IzabelaM:~/ioterop/PaaS/ops/infrastructure/devenvironment$
```

1.3. Git clone

Warning: Do not download the GitLab clone in your Windows files, but in you Linux distribution.

```
$ git clone git@gitlab.com:IoTerop/PaaS/ops/infrastructure-as-code/dev\_environment.git
```

If you need to configure access to Git with SSH keys follow [Using Git with SSH keys - Linux Kamarada](#)

```
$ aws eks update-kubeconfig --name hypernova --region eu-west-1
```

1.4. Run DevEnv

Get the latest version and run

```
$ Make init  
$ make deploy profile=complete  
$ make destroy
```

1.5. k9s

1.5.1. Utility

- Choose which services you need (usually all for QA tests)
- Monitor services and their correct operation
- Restart services
- If a bug occurs, capture it and send it to Ops team for debugging

1.5.2. Access



In the folder containing your DevEnv

Access the global ops view

```
$ k9s
```

Press 0 to see all

Context: arn:aws:eks:eu-west-1:240517794859:cluster/hypernova									<0> all		<>		Attach	
Cluster: arn:aws:eks:eu-west-1:240517794859:cluster/hypernova									<1> hnv-ikqa		<ctrl-d>		Delete	
User: arn:aws:eks:eu-west-1:240517794859:cluster/hypernova									<2> default		<0>		Describe	
KMS Rev: v1.22.17-eks-0a21954									<2>		Edit		Help	
CPU: n/a									<ctrl-k>		Kill		<ctrl-l>	
MEM: n/a									<ctrl-m>		Logs		Metrics	
									Pods(all)[166]		READY		RESTARTS	
									CPU		MEM		NCPU/R	
									CPU/L		CPU/L		CPU/L	
									0		0		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	
									0		n/a		n/a	

```

Context: arn:aws:eks:eu-west-1:248517794859:cluster/hypernova
Cluster: arn:aws:eks:eu-west-1:248517794859:cluster/hypernova
User: arn:aws:eks:eu-west-1:248517794859:cluster/hypernova
K8s Rev: v0.27.6
K8s Rev: v1.22.17-eks-0a21954
CPU: n/a
MEM: n/a

```

<8> all <9> Attach <ctrl-d> Delete []

<1> hnv-ikqa <ctrl-d> Delete []

<2> default <4> Describe []

<6> Edit <7> Help <ctrl-k> Kill []

Pods(hnv-ikqa)[15]

NAME	READY	RESTARTS	STATUS	CPU	MEM	%CPU/R	%CPU/L	%MEM/R	%MEM/L	IP	NODE
alaska-auth-279d90d66-9nhm8	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.104	ip-1
alaska-ceap-65785999c-qkxv9	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.64	ip-1
alaska-definition-659bd0b5f-zzzt9	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.68	ip-1
alaska-frontend-59ef7d0ff89-8tncc	● 1/1	0	Running	0	0	0	0	0	0	10.0.3.109	ip-1
alaska-gateway-7b99a975cb-pppf6	● 2/2	0	Running	0	0	n/a	n/a	n/a	n/a	10.0.3.124	ip-1
alaska-iawx-5bfdbabf5-jd5l5	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.176	ip-1
alaska-network-security-876f85ffff-ws6fr	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.174	ip-1
alaska-network-tcp-0	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.100	ip-1
alaska-network-udp-0	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.11	ip-1
alaska-protocol-manager-78ad699f0a-fchkz	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.69	ip-1
alaska-provisioning-5c880ccccc-69msv	● 2/2	0	Running	0	0	0	0	0	0	10.0.1.131	ip-1
alaska-provisioning-ztdnb8	● 0/1	0	Completed	0	0	n/a	n/a	n/a	n/a	10.0.3.87	ip-1
alaska-security-7e974dd907f-x9x78	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.224	ip-1
alaska-users-6fdc75559-5rcxx	● 2/2	0	Running	0	0	0	0	0	0	10.0.3.43	ip-1

◀load▶

If you need de refresh / restart a microservice to get the latest version, choose the right line and Ctrl+D.

To choose a specific microservices (tag) to test

```
ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure/devenvironment$ cat environment.hcl
# Below are listed all the image tags used by the services.
# Feel free to update tags to match your needs.

alaska_coap_image_tag          = "latest-sec"
alaska_definition_image_tag     = "latest"
alaska_network_security_image_tag= "latest"
alaska_provisioning_image_tag   = "latest"
alaska_auth_image_tag          = "latest"
alaska_campaigns_image_tag     = "latest"
alaska_device_data_image_tag   = "latest"
alaska_devices_image_tag       = "latest"
alaska_file_server_image_tag   = "latest"
alaska_gateway_image_tag       = "latest"
alaska_lm2n_image_tag          = "latest"
alaska_lm2n_firmware_update_image_tag= "latest"
alaska_massachusetts_image_tag = "latest"
alaska_metrics_image_tag       = "latest"
alaska_network_tcp_image_tag   = "latest"
alaska_network_udp_image_tag   = "latest"
alaska_notifications_image_tag = "latest"
alaska_protocol_manager_image_tag= "latest"
alaska_security_image_tag      = "latest"
alaska_users_image_tag         = "latest"
alaska_event_image_tag         = "latest"

ikqa@IzabelaQA:~/ioterop/PaaS/ops/infrastructure/devenvironment$
```

To run a specific microservices, you have to modify the file "environment.hcl" with a text editor, change "lastest" to the tag provided by the R&D team.

You can find all informations to deploy specific tags for each service on the [DevEnv official git page, specifically in the Readme.](#)

1.6. Access to DevEnv Alaska

URL : [https://alaska-\[yournamedistribution\].hypernova.ioterop.com](https://alaska-[yournamedistribution].hypernova.ioterop.com)

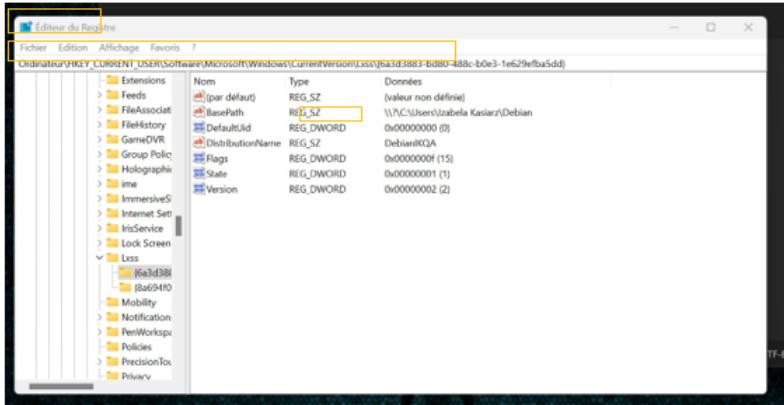
Exemple :

Device TCP : coaps+tcp://stream-alaska-izabelakasiarz.hypernova.ioterop.com

Device UDP : coaps://datagram-alaska-izabelakasiarz.hypernova.ioterop.com

```
{ "Server": { "Operation": "Add", "Ssid": 1, "Uri": "coaps://datagram-alaska-izabelakasiarz.hypernova.iotero.com", "Lifetime": 60, "Security": "Psk", "SecureInfo": {"Identity": "IOWAIKA", "Key": "MD5MzQ1Njc4OQ=="} }}
```

1.7. Rename your DevEnv / Distrib



1.8. Debug

Process

If you detect a bug during the launch, use or destruction of your DevEnv you need to check up the k9s page and contact the Ops Teams. If it's a bug, contact them directly, or create an issue.

Time synchronization default

If AWS does not allow access to devenv due to a synchronization default between WSL and host Windows:

```
$ sudo apt install ntpdate
```

```
$ sudo ntpdate pool.ntp.org
```

Lock files error

Delete files marked as "lock".

```
$ rm : to delete à file
```

```
$ rm -d : for a directory
```

```
$ rm -d -r : for a directory and his files
```

If the device does not disconnect with \$ ctrl x

Put device on pause :

```
$ Ctrl z
```

View current processes and find the device involved

```
$ ps-aux
```

Kill the process

```
$ kill [number of the process]
```

Out of the pause state

```
$ fg
```

Replace logins

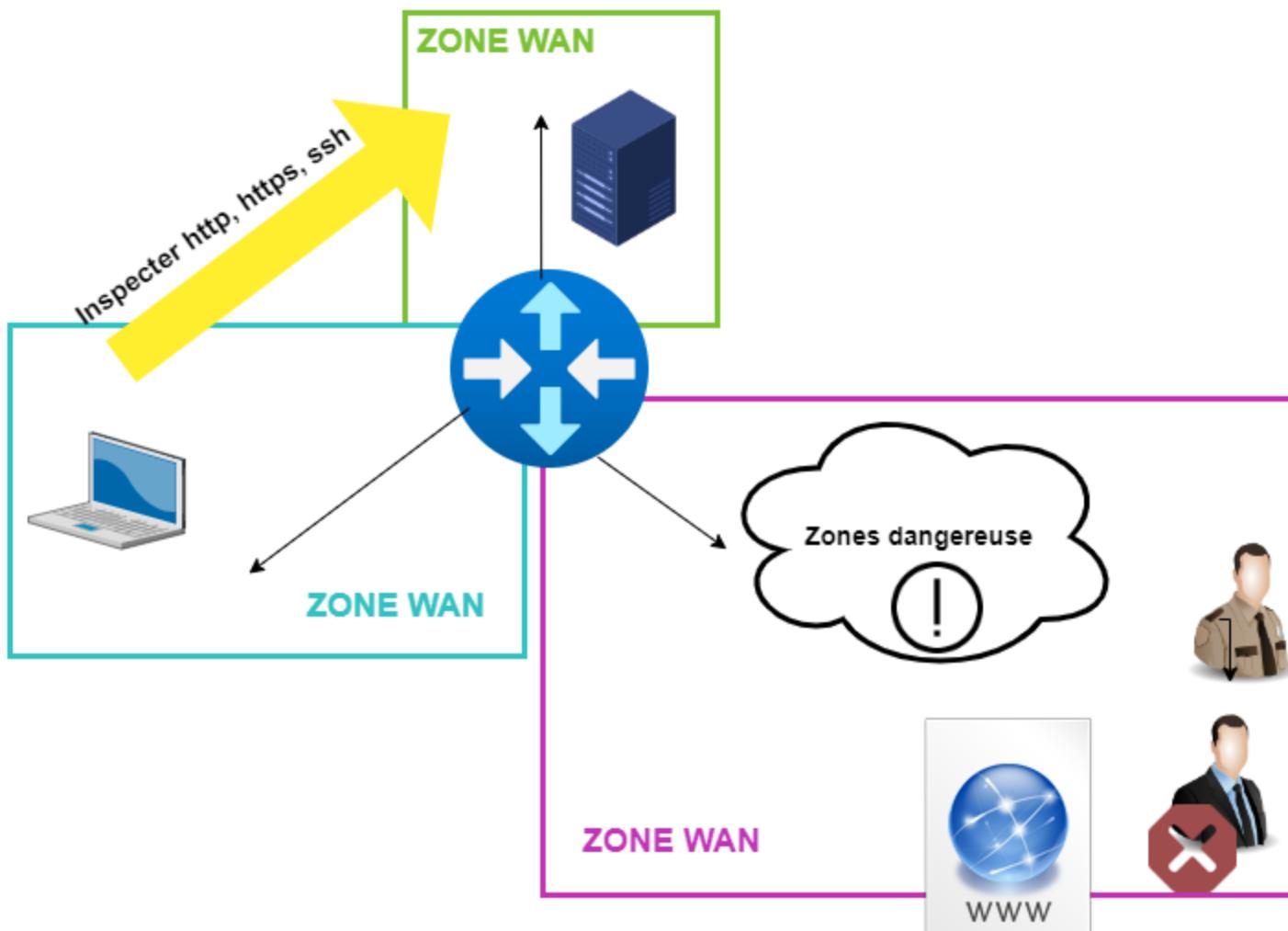
In the DenEnv local directory

Make provisioning

2. Maintenir, exploiter et sécuriser une infrastructure centralisée

- Firewall avec gestion zones WAN, LAN, DMZ et Règles de firewall (ACL standard et étendues)

Schéma d'Architecture réseau :



DAT (Dossier d'Architecture Technique) :

DOSSIER D'ARCHITECTURE TECHNIQUE

IZABELA KASIAZR || TSSR 2023

I. Introduction

L'entreprise HeyAa

La société est une entreprise de e-commerce, ayant besoin d'une infrastructure réseaux sécurisée pour mettre sur le web son e-commerce et donner des outils informatiques à ces salariés.

Nous sommes missionnés pour sécuriser son infrastructure réseau, par la mise en place d'un firewall Fortigate, la définition de politiques de sécurité fines sur les hôtes et serveurs du réseau.

Contexte de sécurité

Résilience, performance et sécurité du SI permettant une interruption de service inexistante, et de ce fait une maintenance et une gestion des risques et monitoring de l'infrastructure transparente.

Objectifs du DAT

- Schemas d'Architecture Réseau logique (Draw.IO),
- Adressage IP du réseau statique et dynamique (excel),
- Versions des systèmes d'exploitation des poste client et serveurs,
- Recommandations pour la sécurité informatiques de la société HeYaA,
- Politique de Pare-Feu avec Fortigate (excel),

Table des matières

I. Introduction	3
II. Schéma d'Architecture Réseau	3
III. Espace d'Adressage IP	4
IV. Version des Systèmes d'Exploitation	4
V. Recommandations pour la Sécurité	4
VI. Politiques de Pare-feu avec Fortigate (Résumé)	5

II. Schéma d'Architecture Réseau

Zone LAN01

Parc informatique :

- postes clients
- dont le PC01 dédié à l'admin administrant le Server Web dans la zone DMZ

Zone LAN02

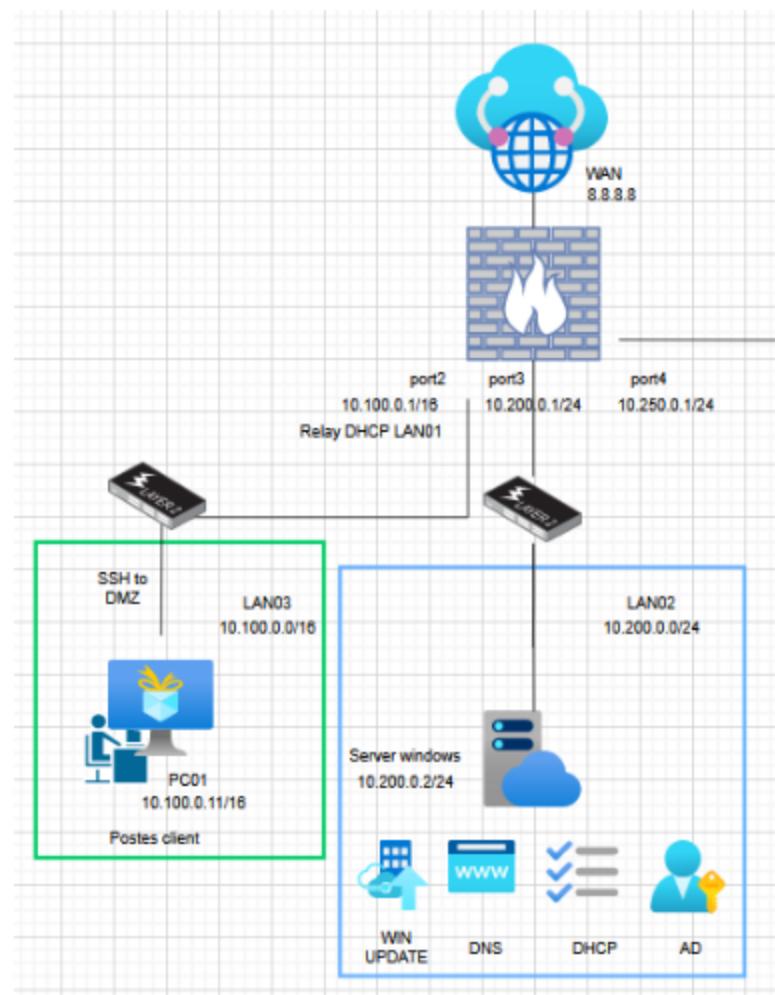
Server Windows

- mises à jour Windows,
- DNS,
- DHCP
- Active Directory.

Zone DMZ

Server Web :

- Ubuntu (accès depuis PC01 en SSH)



III. Espace d'Adressage IP

Vous trouverez l'ensemble de la définition du plan d'adressage dans le tableau ci-dessous.

Spécification des plages d'adresses IP						
Zone	Switch (VMWare)	Port	Subnet	GW	DNS	Commentaires
LAN01	1	2	10.100.0.0/16	10.100.0.1	10.200.0.2	
LAN02	2	3	10.200.0.0/24	10.200.0.1	10.200.0.2	
DMZ	3	4	10.250.0.0/24	10.250.0.1	8.8.8.8	

Baux DHCP						
Zone	Subnet	GW	DNS	Pool DHCP		
LAN01	10.100.0.0/16	10.100.0.1	10.200.0.2	10.100.0.10 - 10.100.0.200		

Spécification VIP								
Type	OS	Zone	Switch (VMWare)	Port	Service	IP	VIP name	VIP
Fortigate	FortiOS 6.4	*	1,2,3	1		10.0.0.70		
PC01Admin	22.04	LAN02	1	2	DHCP, DNS, AD	10.100.0.11		
Ubuntu server	22.04	DMZ	3	4	HTTP/HTTPS	10.250.0.2	VIP_ServerDWeb_HTTP	10.0.0.163
Windows server	OS Version 2	LAN01	2	3	DHCP, DNS, AD	10.200.0.2	VIP_ServerDHCPDNSAD	10.0.0.153

IV. Version des Systèmes d'Exploitation

Spécification des plages d'adresses IP						
Type	OS	Zone	Switch (VMWare)	Port	Service	IP
Fortigate	FortiOS 6.4	*	1,2,3	1		10.0.0.70
PC01Admin	22.04	LAN02	1	2	DHCP, DNS, AD	10.100.0.11
Ubuntu server	22.04	DMZ	3	4	HTTP/HTTPS	10.250.0.2
Windows server	OS Version 22H2...	LAN01	2	3	DHCP, DNS, AD	10.200.0.2

V. Recommandations pour la Sécurité

- Bonnes pratiques de sécurité à suivre pour l'ensemble du réseau.

Tout bloqué en entrant, implicitement bloqué sur toutes les interfaces et on ouvre les services dont on a besoin.

Les ACL sur la couche Switching, isoler le routage inter-vlan par la mise en place d'AC (voir tableau Politiques de Pare-feu avec Fortigate).

- Surveillance du trafic et gestion des journaux. (Syslog → SIEM)
- Politiques de gestion des mots de passe.

VI. Politiques de Pare-feu avec Fortigate (Résumé)

Firewall Rules - Connections from DMZ (port4) to WAN (port1)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
Server Web		10.250.0.2/24	Internet	*	All_ICMP DNS HTTP HTTPS FTP	UDP TCP	53 80 443 20 21	Allow DMZ to WAN
Firewall Rules - Connections from WAN (port1) to DMZ (port4)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
Server Web		*	VM ServerWeb	10.0.0.163	HTTP	UDP TCP	80	Translate Server Web to ServerW
Firewall Rules - Connections from LAN01 (port2) to DMZ (port4)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
PC client		10.100.0.2/16 60:14:B3:AD:45:F6	Server Web	10.250.0.2/24	ICMP SSH	UDP TCP	22 20 21	LAN01_
Firewall Rules - Connections from LAN01 (port2) to LAN02 (port3)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
Poste client		10.100.0.0/16	Server DHCP / DNS / AD	10.200.0.0/24	DHCP DNS AD ICMP	UDP TCP	67 68 53 20 21	Allow LAN01 to LAN02
Firewall Rules - Connections from LAN01 (port2) to WAN (port1)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
Poste client		10.100.0.0/16	Internet	*	ICMP DNS HTTP HTTPS FTP	UDP TCP	53 80 443 20 21	Allow LAN01 to WAN
Firewall Rules - Connections from LAN02 (port3) to WAN (port1)								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
Server DHCP / DNS / AD		10.200.0.0/16	Internet	*	ICMP DNS HTTP HTTPS FTP	UDP TCP	53 80 443 20 21	Allow LAN02 to WAN
Firewall Rules - Implicit								
Source Name	State	Source IP	Destination Name	Destination IP	Service	Protocol	Port	Comment
*	*	*	*	*	*	*	*	Implicit

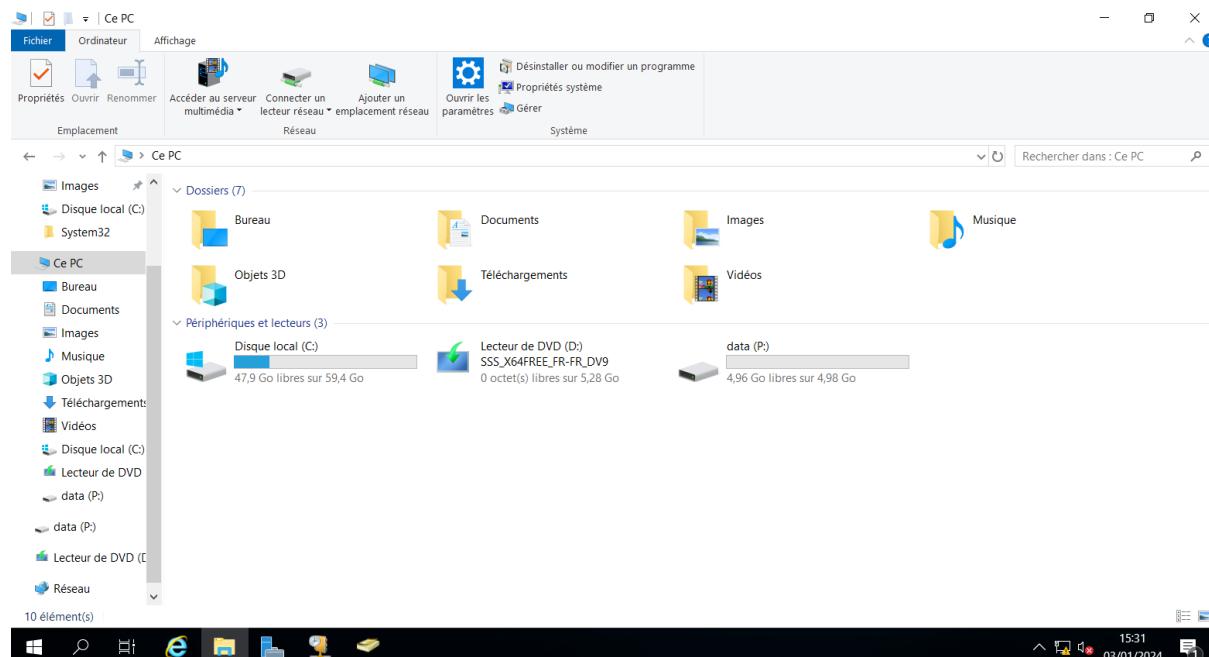
- Maintenir et exploiter un environnement virtualisé : Gérer les différents espaces de stockage

En tant qu'administrateur, sur Windows server je souhaite :

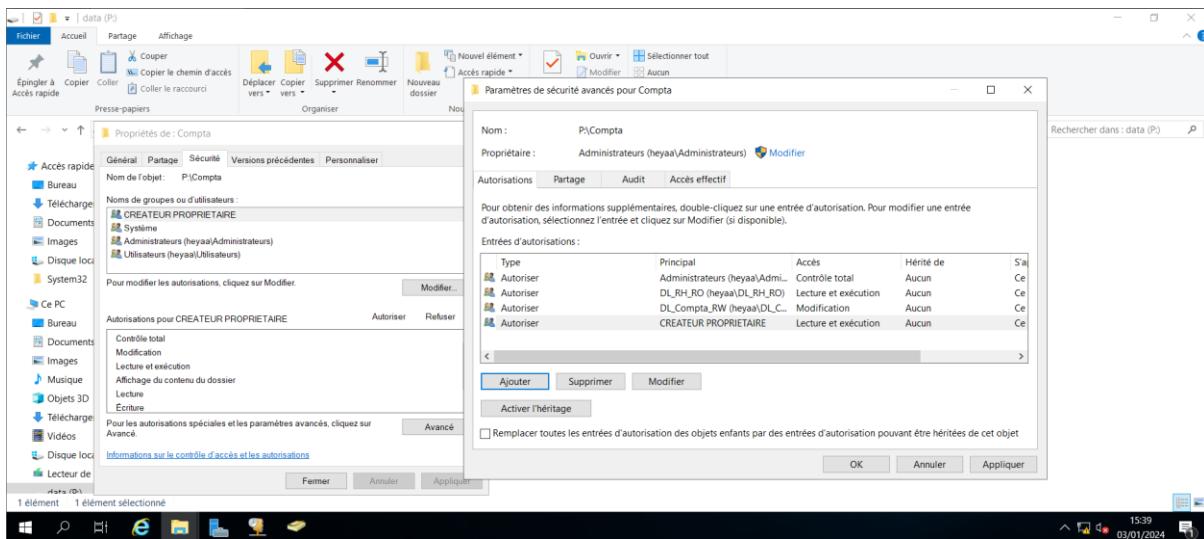
- Ajouter un HDD de 5GO
- Créer des dossiers perso pour les utilisateurs
- Mapper les dossiers perso sur les VM des utilisateurs
- Gestion des quotas de volumes et dossiers

Ajout d'un HDD de 5GO pour partage de fichier comptabilité :

1. Partitionner le disque P

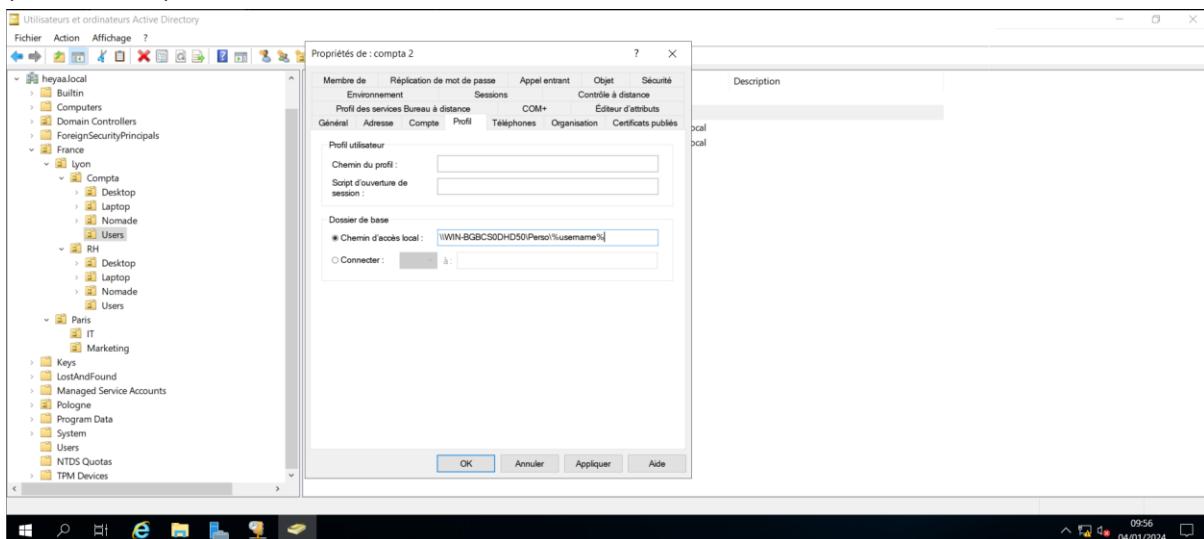


2. Permissions NTFS pour le dossier compta



3. Créer dossier perso dans P et donner accès à GG_Users_Paris

Mapper le dossier perso dans chaque profils utilisateur \\WIN-BGBCS0DHD50\Perso\%username% (chemin UNC)



Script pour mapper dossier personnel pour tous les utilisateurs d'une suite d'UO :

```

script_users_dossier_perso.ps1 X
1 # Importer le module Active Directory
2 Import-Module ActiveDirectory
3
4 # Définir le chemin de l'unité d'organisation contenant les utilisateurs
5 $OU_path = "OU=Users,OU=Compta,OU=Lyon,OU=France,DC=heyaa,DC=local"
6
7 # Définir le chemin du dossier partagé contenant les dossiers personnels
8 $Base_Folder = "\\WIN-BGBCS0DHD50\Personnel"
9
10 # Récupérer la liste des utilisateurs de l'unité d'organisation
11 $users = Get-ADUser -SearchBase $OU_path -Filter *
12
13 # Pour chaque utilisateur
14 foreach ($user in $users) {
15
16     # Récupérer le nom d'utilisateur (sAMAccountName)
17     $username = $user.sAMAccountName
18
19     # Créer le chemin du dossier personnel
20     $Home_Folder = $Base_Folder + $username
21

```

PS C:\Users\Administrateur> C:\script_users_dossier_perso.ps1

Répertoire : \\WIN-BGBCS0DHD50\Personnel

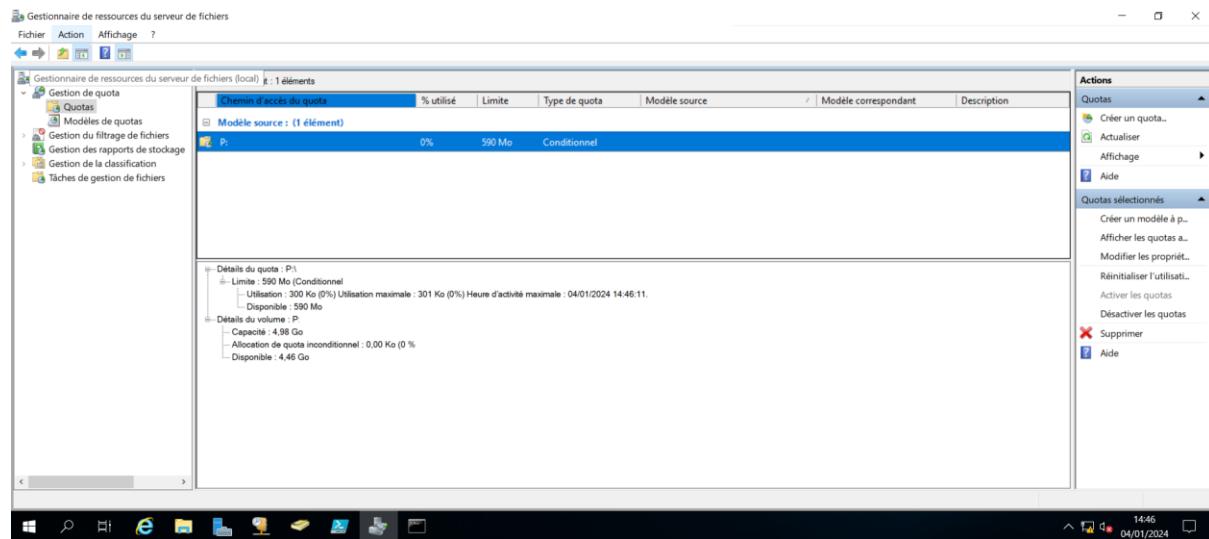
Mode	LastWriteTime	Length	Name
d----	04/01/2024 10:37		compta1
d----	04/01/2024 10:37		compta2

PS C:\Users\Administrateur> |

Version d'évaluation de Windows 10 Entreprise
Licence Windows valide pour 73 jours
Build 19041.vb_release.191206-1409
10:40 04/01/2024

4. Gestion des quotas de volumes et dossiers – Windows Serveur

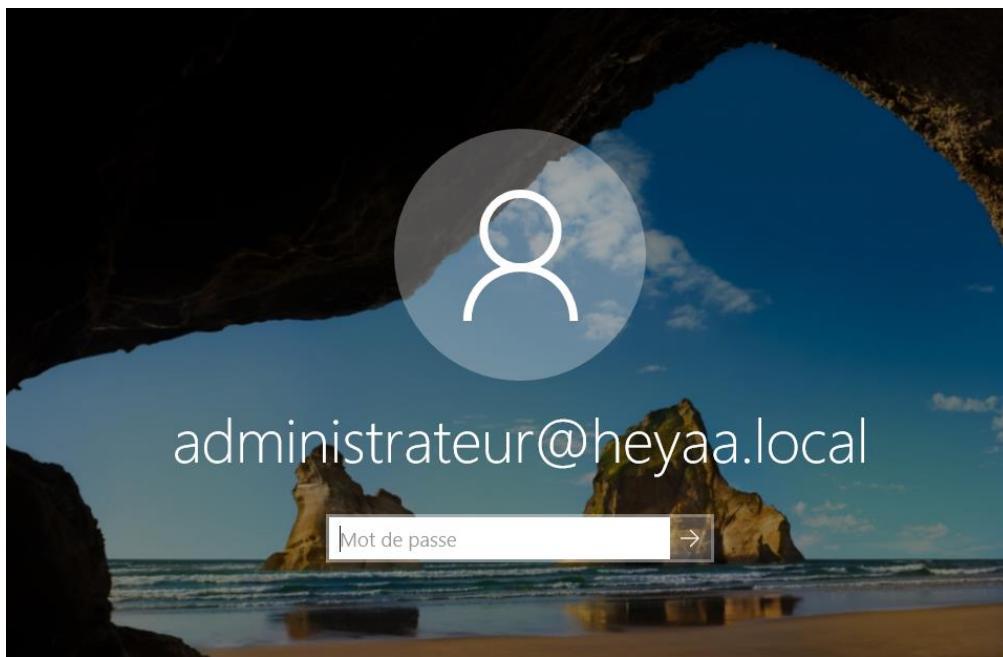
Installation du rôle : Gestionnaire de ressources du serveur de fichiers :



- Maintenir et exploiter un domaine ActiveDirectory et les serveurs Windows

En tant qu'administrateur de l'active Directory, je dois :

- créer des users,
 - des UO,
 - des groupes
 - Ainsi que les administrer



Création de Unité d'Organisation :

- Schémas arborescence des Users et UO

Nom	Type	Description
rh 1	Utilisateur	
rh 2	Utilisateur	

- Fichier texte :

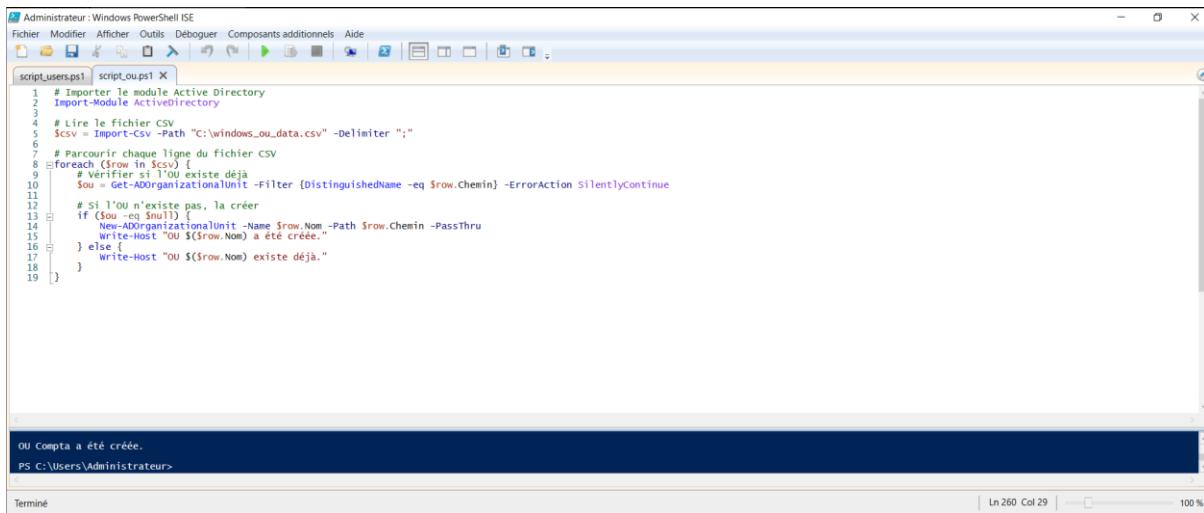
```

Fichier    Modifier    Affichage

Nom;Chemin
Pologne;DC=heyaa,DC=local
Jarslaw;OU=Pologne,DC=heyaa,DC=local
RH;OU=Jarslaw,OU=Pologne,DC=heyaa,DC=local
Compta;OU=Jarslaw,OU=Pologne,DC=heyaa,DC=local
France;DC=heyaa,DC=local
Paris;OU=France,DC=heyaa,DC=local
Lyon;OU=France,DC=heyaa,DC=local
Marketing;OU=Paris,OU=France,DC=heyaa,DC=local
IT;OU=Paris,OU=France,DC=heyaa,DC=local
RH;OU=Lyon,OU=France,DC=heyaa,DC=local
Compta;OU=Lyon,OU=France,DC=heyaa,DC=local

```

- Script :



```

# Importer le module Active Directory
Import-Module ActiveDirectory
# Lire le fichier CSV
$CSV = Import-Csv -Path "C:\windows_ou_data.csv" -Delimiter ";"
# Parcourir chaque ligne du fichier CSV
foreach ($row in $CSV) {
    # Vérifier si l'OU existe déjà
    $OU = Get-ADOrganizationalUnit -Filter {DistinguishedName -eq $row.Chemin} -ErrorAction SilentlyContinue
    if ($OU -eq $null) {
        New-ADOrganizationalUnit -Name $row.Nom -Path $row.Chemin -PassThru
        Write-Host "OU $($row.Nom) a été créée."
    } else {
        Write-Host "OU $($row.Nom) existe déjà."
    }
}

```

OU Compta a été créée.
PS C:\Users\Administrateur>

Création des users dans les Unités Organisationnelles :

- Fichier texte :

Fichier	Modifier	Affichage
heyaa.test3;Toor2024!;OU=Compta,OU=Lyon,OU=France,DC=heyyaa,DC=local;heyaa.Test3;mark.test3@activedirectorypro.com;;Marketing Office;541-213-5443@activedirectorypro.com;346 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test4;Toor2024!;OU=RH,OU=Lyon,OU=France,DC=heyyaa,DC=local;heyaa.Test4;mark.test4@activedirectorypro.com;;Marketing Office;541-213-5444@activedirectorypro.com;347 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test5;Toor2024!;OU=RH,OU=Jaroslaw,OU=Pologne,DC=heyyaa,DC=local;heyaa.Test5;mark.test5@activedirectorypro.com;;Marketing Office;@activedirectorypro.com;348 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test6;Toor2024!;OU=Compta,OU=Jaroslaw,OU=Pologne,DC=heyyaa,DC=local;Heyaa Test6;mark.test6@activedirectorypro.com;;Marketing Office;@activedirectorypro.com;349 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test7;Toor2024!;OU=Compta,OU=Jaroslaw,OU=Pologne,DC=heyyaa,DC=local;Test7;Heyaa Test7;mark.test7@activedirectorypro.com;;Marketing Office;@activedirectorypro.com;350 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test8;Toor2024!;OU=RH,OU=Jaroslaw,OU=Pologne,DC=heyyaa,DC=local;heyaa.Test8;mark.test8@activedirectorypro.com;;Marketing Office;@activedirectorypro.com;351 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test9;Toor2024!;OU=Marketing,OU=Paris,OU=France,DC=heyyaa,DC=local;Test9;Heyaa Test9;mark.test9@activedirectorypro.com;;Marketing Office;@activedirectorypro.com;352 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		
heyaa.test10;Toor2024!;OU=Marketing,OU=Paris,OU=France,DC=heyyaa,DC=local;Test10;Heyaa Test10;mark.test10@activedirectorypro.com;;Marketing Offi@activedirectorypro.com;353 e maple;;Ozark;Mo;65421;Sr Admin;darkmoka		

- Script :

```

# Importe le module active directory pour lancer AD cmdlets
Import-Module ActiveDirectory

# Regarder les données dans le Fichier CSV et remplacer par la variable $ADUsers
$ADUsers = Import-Csv C:\windows_users.data.csv -Delimiter ";"

# Parcourir chaque ligne contenant les détails de l'utilisateur dans le fichier CSV
foreach ($User in $ADUsers) {
    # Lit les données utilisateur de chaque champ de chaque ligne
    $Username = $User.SamAccountName

    # Vérifie si l'utilisateur existe déjà dans AD
    if ((Get-ADUser -Filter {SamAccountName -eq $Username})) {
        # L'utilisateur existe, donner un message d'avertissement
        Write-Warning "Un compte $User existe déjà dans Active Directory."
    }
    else {
        # L'utilisateur n'existe pas, alors créez le nouveau compte $User
    }
}

Le compte utilisateur #SamAccountName=heyaa,test1; password=tour2024; path=OU-BU-01-jarolaw.00-0ologne.0C-heyyaa,DC=local; GivenName=heyya_name; Surname=test8; Initials=h; Name=heyya Test8; DisplayName=heyya Test8; UserPrincipalName=heyaa.test8@activedirectorypro.com; StreetAddress=351 e maple; POBox =; City=Ozark; State=Mo; PostalCode=65421; Title=Sr Admin; Company=darkmoka a été créé.
Le compte utilisateur #SamAccountName=heyaa,test9; password=tour2024; path=OU-Marketing.0U-Paris,0C-heyyaa,DC=local; GivenName=heyya_name; Surname=test9; Initials=h; Name=heyya Test9; DisplayName=heyya Test9; UserPrincipalName=heyaa.test9@activedirectorypro.com; Department=; Description=; Office=Marketing Office; OfficePhone=541-213-5449; EmailAddress=mark.test9@activedirectorypro.com; StreetAddress=352 e maple; POBox =; City=Ozark; State=Mo; PostalCode=65421; Title=Sr Admin; Company=darkmoka a été créé.
Le compte utilisateur #SamAccountName=heyaa,test10; password=tour2024; path=OU-Marketing.0U-Paris,0C-heyyaa,DC=local; GivenName=heyya_name; Surname=test10; Initials=h; Name=heyya Test10; DisplayName=heyya Test10; UserPrincipalName=mark.test10@activedirectorypro.com; Department=; Description=; Office=Marketing Office; OfficePhone=541-213-5450; EmailAddress=mark.test10@activedirectorypro.com; StreetAddress=353 e maple; POBox =; City=Ozark; State=Mo; PostalCode=65421; Title=Sr Admin; Company=darkmoka a été créé.

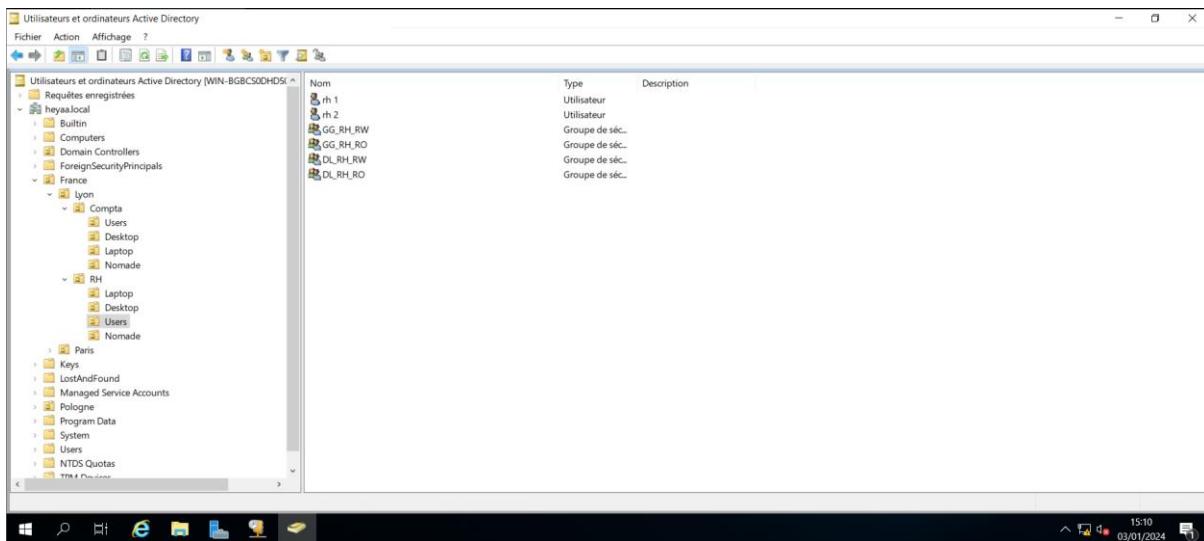
PS C:\Users\Administrateur>

```

Création des groupes (méthode AGDLP pour la gestion de vos ressources) :

- Créer les groupes (DL)
- Créer un groupe Groupe Global (GG)

Nom	Type	Description
compta 1	Utilisateur	
compta 2	Utilisateur	
GG_Compta_RW	Groupe de sec..	
GG_Compta_RO	Groupe de sec..	
DL_Compta_RW	Groupe de sec..	
DL_Compta_RO	Groupe de sec..	



3. Maintenir et exploiter une infrastructure distribuée et contribuer à sa sécurisation

- Script Linux Backup (Cron –rsync –bucket S3)

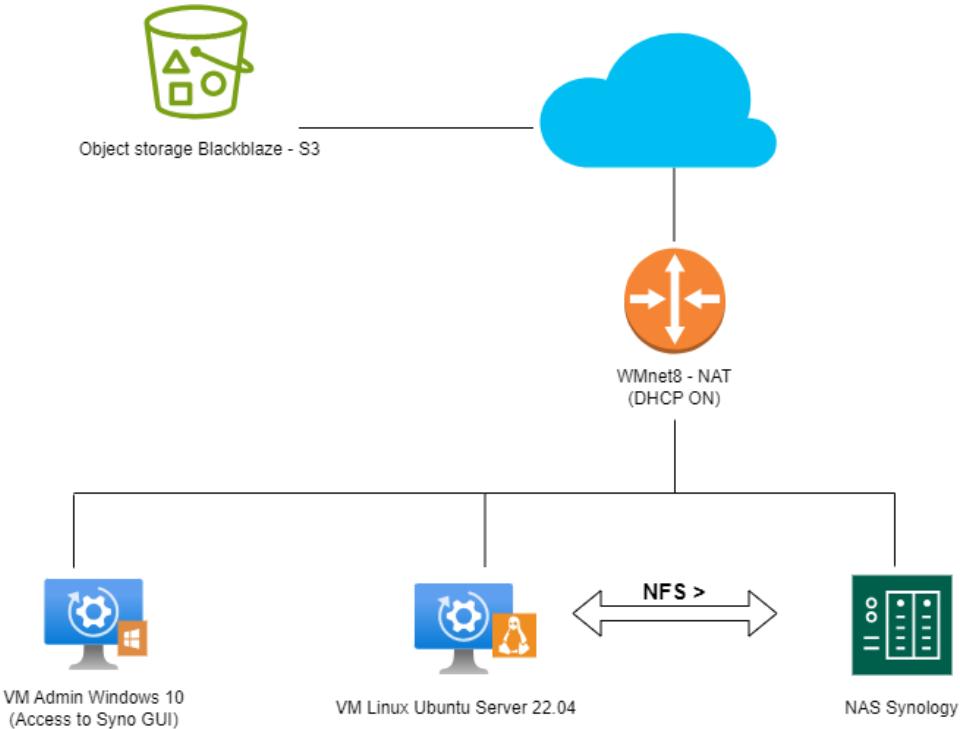
Contexte :

- Créer un partage NFS sur le NAS Synology
- Sur un VM Ubuntu Server 22.04 Mapper le partage NFS
- Je souhaite créer un script sur la VM Ubuntu Server pour que les backup s'effectuent automatiquement

Tâches :

- Installation VM NAS Synology sur VMWare
- Installation VM Ubuntu Server 22.04 sur VMWare
- Connecter les deux VM au même LAN Segment VMware afin qu'ils soient sur le même réseau
- Créer un partage NFS sur NAS Synology
- Mapper le partage NFS sur Ubuntu Server
- Faire en sorte que le point de montage soit en auto-mount à chaque démarrage
- Vérifier le point de montage avec la command fstab
- Mettre en place les backup automatiques depuis Ubuntu Server vers le NAS Synology
 - Créer un script sur l'Ubuntu server afin d'automatiser les backup vers le NAS Synology
 - `$ rsync -auv -r /root/dossier/* /media/nas/volume1/heyaa/barsync -auv -r /root/dossier/* /media/nas/volume1/heyaa/backup`
 - Intégrer le script dans le programme Crontab afin d'automatiser son lancement à date et une heure précise
 - Installer cron
 - Vérifier son état de fonctionnement avec `$systemctl status cron`
 - configurer le fichier cron tab &nano /etc/crontab

- Vérifier que les backup s'effectuent automatiquement sur le NAS Synology avec Hyper backup



```

root@root:~/script      X  Windows PowerShell      X | + | 
darkmoka perso planning pro taches whitemoka
root@root:~/dossier# cd ..
root@root:~#
dossier script
root@root:# cd script/
root@root:~/script# nano backup.sh
root@root:~/script# mount -l
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
udev on /dev type devtmpfs (rw,nosuid,relatime,size=1926776k,nr_inodes=481694,mode=755,inode64)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,noexec,relatime,size=396952k,mode=755,inode64)
/dev/mapper/ubuntu--vg-ubuntu--lv on / type ext4 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev,inode64)
tmpfs on /run/lock type tmpfs (rw,nosuid,nodev,noexec,relatime,size=5120k,inode64)
cgroup2 on /sys/fs/cgroup type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate,memory_recursiveprot)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
bpf on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=780)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs (rw,relatime,fd=29,pgrp=1,timeout=5,minproto=5,maxproto=5,direct,pipe_ino=29144)
hugegetlbfs on /dev/hugepages type hugegetlbfs (rw,relatime,pagesize=2M)
mqqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
traceefs on /sys/kernel/tracing type traceefs (rw,nosuid,nodev,noexec,relatime)
fusectl on /sys/fs/fuse/connections type fusectl (rw,nosuid,nodev,noexec,relatime)
configfs on /sys/kernel/config type configfs (rw,nosuid,nodev,noexec,relatime)
none on /run/credentials/systemd-sysusers.service type ramfs (ro,nosuid,nodev,noexec,relatime,mode=700)
/var/lib/snappy/snaps/core20_1587.snap on /snap/core20/1587 type squashfs (ro,nodev,relatime,errors=continue,x-gdu.hide)
/var/lib/snappy/snaps/snappy_20671.snap on /snap/snappy/20671 type squashfs (ro,nodev,relatime,errors=continue,x-gdu.hide)
/var/lib/snappy/snaps/lxd_22923.snap on /snap/lxd/22923 type squashfs (ro,nodev,relatime,errors=continue,x-gdu.hide)
/dev/sda2 on /boot type ext4 (rw,relatime)
binfmt_misc on /proc/sys/fs/binfmt_misc type binfmt_misc (rw,nosuid,nodev,noexec,relatime)
sunrpc on /run/rpc_pipefs type rpc_pipefs (rw,relatime)
192.168.152.133:/volume1/heya on /media/nas/volume1/heya type nfs (rw,relatime,vers=3,rsize=8192,wsize=8192,namlen=255,hard,proto=tcp,timeo=14,retrans=2,sec=sys,mountaddr=192.168.152.133,mountvers=3,mountport=892,mountproto=udp,local_lock=none,addr=192.168.152.133)
tmpfs on /run/snappy/ns type tmpfs (rw,nosuid,nodev,noexec,relatime,size=396952k,mode=755,inode64)
nsfs on /run/snappy/ns/lxd.mnt type nsfs (rw)
tmpfs on /run/user/1000 type tmpfs (rw,nosuid,nodev,relatime,size=396948k,nr_inodes=99237,mode=700,uid=1000,gid=1000,inode64)
root@root:~/script# 

```

```
x root@root:~/dossier      × + | ~
root@root:~/dossier# systemctl status cron
● cron.service - Regular background program processing daemon
  Loaded: loaded (/lib/systemd/system/cron.service; enabled; vendor preset: enabled)
  Active: active (running) since Wed 2024-01-31 12:41:52 UTC; 10min ago
    Docs: man:cron(8)
   Main PID: 924 (cron)
     Tasks: 1 (limit: 4515)
   Memory: 408.0K
      CPU: 8ms
     CGroup: /system.slice/cron.service
             └─924 /usr/sbin/cron -f -P

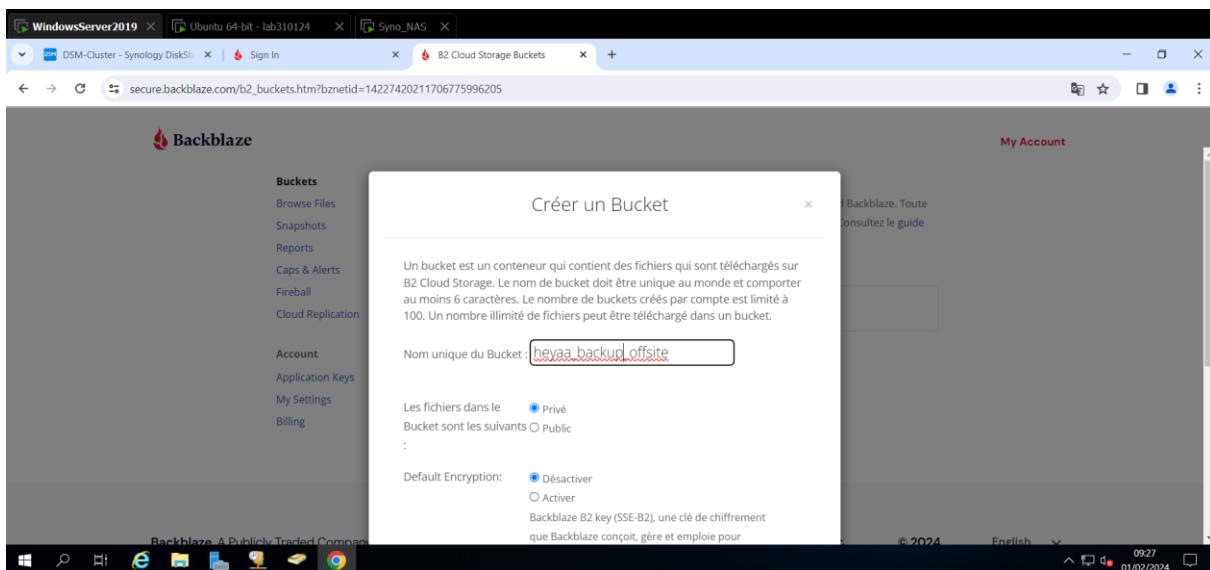
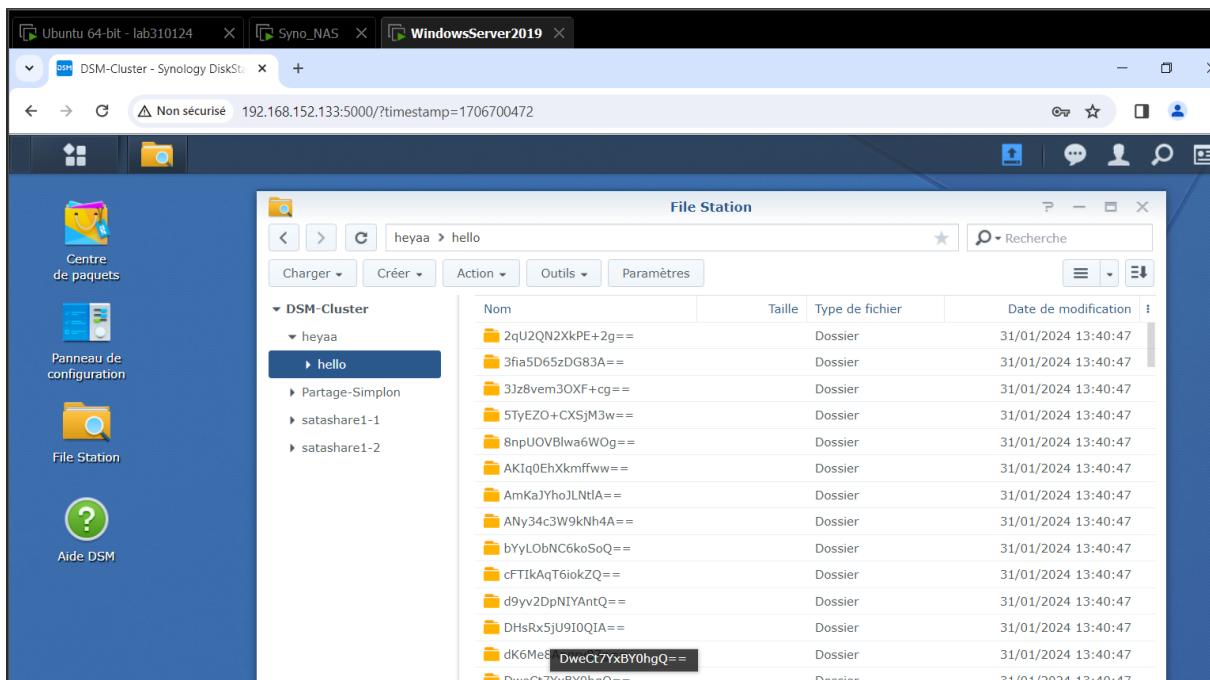
janv. 31 12:41:52 root systemd[1]: Started Regular background program processing daemon.
janv. 31 12:41:52 root cron[924]: (CRON) INFO (pidfile fd = 3)
janv. 31 12:41:52 root cron[924]: (CRON) INFO (Running @reboot jobs)
root@root:~/dossier# |
```

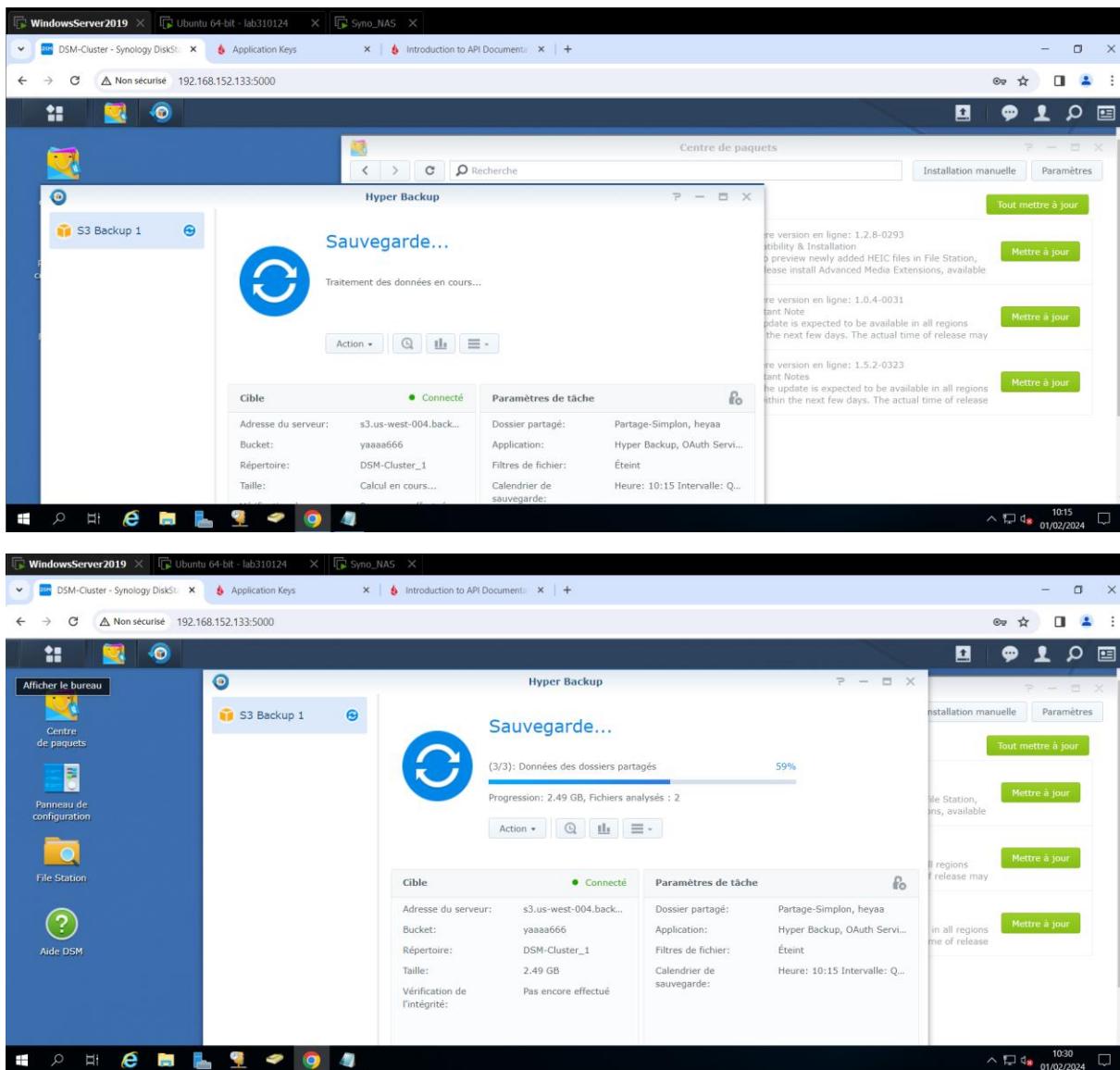
```
root@root:~/script X Windows PowerShell X + - [Read 26 lines]
GNU nano 6.2 /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the 'crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# * * * * * user-name command to be executed
# |----- minute (0 - 59)
# |----- hour (0 - 23)
# |----- day of month (1 - 31)
# |----- month (1 - 12) OR jan,feb,mar,apr ...
# |----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |----- |
# |----- |

# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6 * * 7 root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6 1 * * root test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
#
#
3 * * * * * /root/backup_advanced.sh
```





- Création de VM sur AWS (Cloud computing)

Conditions :

- Je souhaite créer une instance (VM) EC2 Ubuntu 22.04 sur AWS et l'administrer en ligne de commande AWD depuis le terminal.

Tâches :

- Créer un compte AWS (période d'essai) sur <https://aws.amazon.com/fr/free/faqs/>
- Installer AWS CLI sur le PC portable simplon
- Crée une clé d'accès AWS (Access Key) en tant que client
- Accéder à la CLI AWS via avec le terminal

- Créer une instance VM en ligne de commande :
 - ```
aws ec2 run-instances --image-id ami-XXXXXX --count 1 --instance-type t2.nano --key-name votreclefSSH --security-group-ids sg-XXXXXXXXXX --subnet-id subnet-XXXXXXXXXX --associate-public-ip-address --tag-specifications "ResourceType=instance,Tags=[{Key=Name,Value=Un_Petit_Nom}]"
```
- Administrer la/les VM depuis la CLI : Lister les instances running / Résilier l'instance avec son ID / Ajouter une balise TAG Name

The screenshot shows the AWS EC2 Instances launch success page. At the top, there's a green success message: "Succès Lancement de l'instance réussi (i-018bb46a373ff467a)". Below it, a "Journal de lancement" section details the steps: "Initialisation des requêtes Réussi", "Création de groupes de sécurité Réussi", "Création des règles de groupe de sécurité Réussi", and "Début du lancement Réussi". A "Étapes suivantes" section is present at the bottom.

EC2 Instance Connect    Session Manager    **Client SSH**    EC2 Serial Console

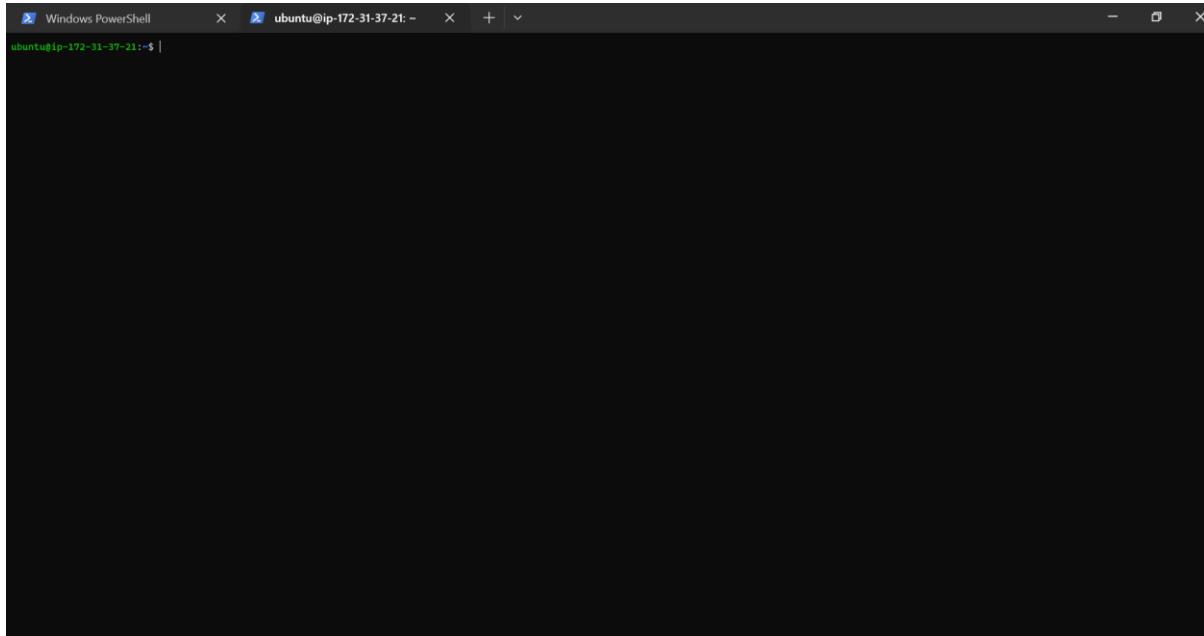
ID d'instance  
i-018bb46a373ff467a (heyaa\_server)

1. Ouvrez un client SSH.
2. Recherchez votre fichier de clé privée. La clé utilisée pour lancer cette instance est heyaa\_key.pem
3. Exécuter, si nécessaire, cette commande pour vous assurer que votre clé n'est pas visible publiquement.  
chmod 400 "heyaa\_key.pem"
4. Connectez-vous à votre instance à l'aide de son DNS public :  
ec2-13-38-216-75.eu-west-3.compute.amazonaws.com

Exemple :

ssh -i "heyaa\_key.pem" ubuntu@ec2-13-38-216-75.eu-west-3.compute.amazonaws.com

**Note:** In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.



```
root@ip-172-31-37-21:~# ls
snap
root@ip-172-31-37-21:~# cd snap/
root@ip-172-31-37-21:~/snap# ls
amazon-ssm-agent lxd
root@ip-172-31-37-21:~/snap# |
```

```

PS C:\Users\utilisateur> aws --version
aws-cli/2.15.16 Python/3.11.6 Windows/10 exe/AMD64 prompt/off
PS C:\Users\utilisateur> aws configure
AWS Access Key ID [None]: AKIA3NX4IY742QLEQOKH
AWS Secret Access Key [None]: zCmwHGreasWdAldyjBgbZj/fJ6/nwJgVrFGpEKU3a
Default region name [None]: eu-west-3
Default output format [None]:
PS C:\Users\utilisateur> aws ec2 describe-instances --query "Reservations[*.Instances[*.{PublicIP:PublicIpAddress,PrivateIP:PrivateIpAddress,Name:Tags[?Key=='Name'][0].Value,Type:InstanceType>Status:State.Name,VpcId:VpcId}]" --filters Name=instance-state-name,Values=running --output table
+-----+-----+-----+-----+-----+-----+
| DescribeInstances |
+-----+-----+-----+-----+-----+-----+
| Name | PrivateIP | PublicIP | Status | Type | VpcId |
+-----+-----+-----+-----+-----+-----+
Limone-Layilla	172.31.0.35	15.237.174.222	running	t2.micro	vpc-0c12f7e3dd0d2378c
heyaa_server	172.31.37.21	13.38.216.75	running	t2.micro	vpc-0c12f7e3dd0d2378c
ServEsteve	172.31.33.179	13.39.155.213	running	t2.micro	vpc-0c12f7e3dd0d2378c
NaomiInstance	172.31.45.195	13.38.117.166	running	t2.micro	vpc-0c12f7e3dd0d2378c
Allaninstance	172.31.41.59	52.47.124.28	running	t2.micro	vpc-0c12f7e3dd0d2378c
production	172.31.37.141	35.180.156.1	running	t2.micro	vpc-0c12f7e3dd0d2378c
Serveur Clement	172.31.25.160	35.180.55.184	running	t2.micro	vpc-0c12f7e3dd0d2378c
KoinKoin_CLI	172.31.31.203	15.237.115.116	running	t2.micro	vpc-0c12f7e3dd0d2378c
Jonathan_SRV	172.31.19.29	35.180.231.16	running	t2.micro	vpc-0c12f7e3dd0d2378c
EC2_Theo	172.31.24.127	15.188.87.89	running	t2.micro	vpc-0c12f7e3dd0d2378c
+-----+-----+-----+-----+-----+-----+

```

- Veille technologique - présentation Linux et son fonctionnement



## SOMMAIRE

### 1 HARDWARE

- E/S Mappées en Mémoire  
L'adresage et communique avec les ordi,imprimante,etc

### 2 KERNEL / SHELL

- Kernel, différences avec Windows
- Distributions
- Dérivés de Linux et exemple

### 3 APPLICATION

## Linux

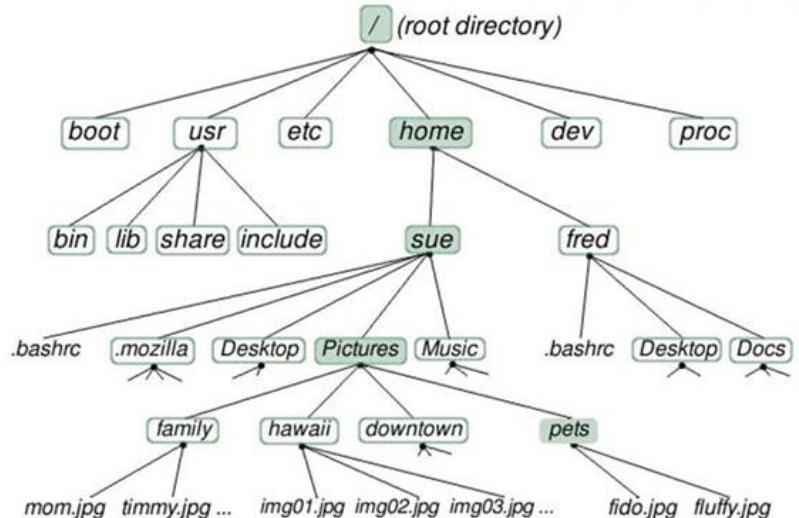
- Système de fichiers de LINUX
- Arborescence
- Fichiers et répertoires
- Editeurs de Texte
- Compression
- Quelques lignes de commandes



# Système de fichiers de LINUX



- Modèle de stockage et de gestion des fichiers
- Organisé en une seule arborescence
- Il permet aux utilisateurs et aux processus d'accéder aux données dont ils ont besoin pour fonctionner.



11

## Fichiers et répertoires



### • Fichiers / fichiers réguliers ou ordinaires

Collection d'informations stockées dans le système de fichiers.

Tout type : texte, des images, des vidéos, binaires et exécutables.

### • Répertoires

Un répertoire est un conteneur qui peut contenir des fichiers et d'autres répertoires.

Peut également contenir des informations sur les fichiers et répertoires qu'il contient : telles que leur nom, leur date de création et leur propriétaire.

### • Fichiers de configuration

Contiennent des informations sur la configuration d'un système, telles que les paramètres réseau, l'emplacement des fichiers et les options d'exécution.

« /etc ».

### • Fichiers de données

Contiennent des informations sur les utilisateurs, les applications et les processus.

« /var ».

### • Fichiers de périphériques

Utilisés pour communiquer avec les périphériques connectés au système, tels que les imprimantes, les disques durs et les claviers.

« /dev ».

### • Liens symboliques

Pointent vers des fichiers ou des répertoires existants. Ils peuvent être utilisés pour créer des raccourcis.

« /usr/bin ».

### • Processus

Fichiers qui sont exécutés par le système.

« /proc ».

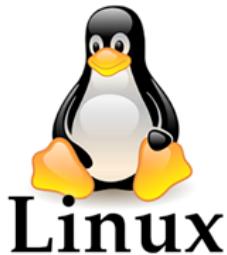
12

# ARBORESCENCE LINUX



## Pour info

Dans **LINUX**, tous les objets de l'arborescence sont considérés comme étant un fichier.



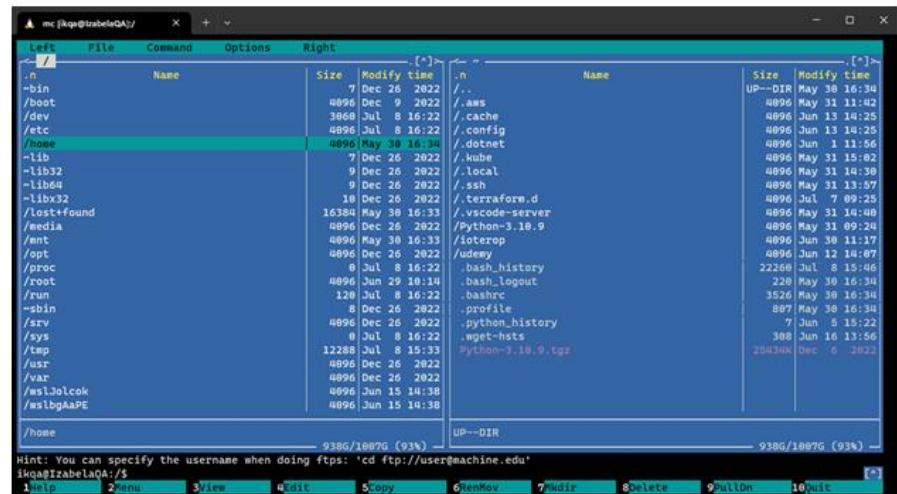
- **/** (La racine de la partition système, root)
- **/bin** (Stock les exécutables et binaires essentiels / Les commandes)
- **/boot** (Stock les fichiers de démarrage de Linux)
- **/dev** (fichiers liés aux périphériques, "devices")
- **/etc** (Les fichiers et la config de linux et des applications)
- **/home** (Les répertoires de base des utilisateurs)
- **/lib** (Les bibliothèques de routines, le module du kernel, "library")
- **/var** (Les journaux systèmes)
- **/mnt** (Les volumes montés temporairement :disquette, CD-ROM)
- **/root** (le répertoire du super utilisateur)
- **/sbin** (Les fichiers systèmes binaires)
- **/tmp** (Le répertoire temporaire)
- **/usr** (les applications utilisateurs)

13

# ARBORESCENCE LINUX



Astuce : Midnight Commander(mc)



14

# ARBORESCENCE LINUX



Astuce : Midnight Commander(mc)

The screenshot shows the mc file manager interface. On the left, there's a tree view of a directory structure. On the right, there's a detailed list view with columns for Name, Size, Modify time, and Right. A terminal window is integrated at the bottom, showing command history and a prompt. A red box highlights the directory path in the tree view.

15

## EDITEUR DE TEXTE - Edition des fichiers de configuration des services

### **La commande Vim** (`sudo apt-get install vim`)

\$ vim {options} {nom\_du\_fichier} pour l'éditer.  
Exemple : `vim -r Informatique`

The screenshot shows the Vim text editor with a configuration file for services. The status bar indicates "New Buffer". The menu bar includes "File", "Edit", "Search", "View", "Insert", "Replace", "Cut", "Paste", "Identify", "Location", "UnDo", "Redo", "Set Mark", "To Bracket", "Copy", and "Where Mark". The bottom status bar shows "VIM - Vi IMproved", "version 8.2.2434", and copyright information. A help message at the bottom of the screen provides instructions for navigating the editor.

16

### **La commande Vi** (`sudo apt-get install Vi`)

\$ vi fichier1

### **La commande Nano** (`sudo apt-get install nano`)

\$ nano fichier1

### **La commande Gedit** (`sudo apt-get install Gedit`)

\$ gedit fichier1

47

# COMPRESSION



- Sur Linux, on utilise la **commande tar** pour **créer des archives au format .tar**
- Par défaut, une archive n'est pas compressée
- Il faudra utiliser un **logiciel de compression** (gzip, bzip2 ou xz) pour compresser l'archive, ce qui donnera une archive au format .tar.gz, .tar.bz2 ou .tar.xz.

*Ex : Compresser le dossier en nom\_archive.tar.gz avec gzip :*

```
$ tar -czf nom_archive.tar.gz le_dossier/
```

## Pour info

- tar est un logiciel d'archivage qui permet de combiner plusieurs fichiers en un seul.
- gzip est un logiciel de compression utilisé pour réduire la taille d'un fichier.
- tar et gzip sont utilisés ensemble pour créer des archives compressées.
- .tar : fichier d'archive non compressé.
- .gz : fichier (archive ou non) compressé avec gzip.
- .tar.gz : fichier d'archive compressé avec gzip.
- Il existe également d'autres logiciels de compression comme bzip2 et xz qui compressent les archives en utilisant d'autres algorithmes de compression.

17

# Quelques lignes de commande



## Pour info

### • ls

permet de lister le contenu du répertoire

### • cd

« Change Directory » et, comme son nom l'indique, vous fait passer au répertoire auquel vous essayez d'accéder.

### • cd ..

Monter d'un niveau

### • cd -

Retourner au répertoire précédent

### • pwd

« print working directory » (afficher le répertoire de travail) et donne le chemin absolu du répertoire dans lequel vous vous trouvez

### • cp

copier des fichiers et des répertoires

### • rm

supprimer des fichiers

### • rm -d -r

supprimer des répertoires et leur contenu

18

# Quelques lignes de commande

## Pour info

- **mv**

déplacer / renommer des fichiers et répertoires

- **mkdir**

créer un dossier

- **touch**

créer un fichier

- **sudo**

« superuser do » et vous permet d'agir en tant que super-utilisateur ou utilisateur root pendant l'exécution d'une commande spécifique

- **cat**

Cat, abréviation de « concatenate », vous permet de créer, d'afficher et de concaténer des fichiers directement depuis le terminal. Il est principalement utilisé pour prévisualiser un fichier sans ouvrir un éditeur de texte graphique

- **ps**

accéder aux processus

- **kill**

Tuer un programme qui ne répond pas en précisant PID

- **history**

Liste numérotée des commandes utilisées dans le passé

19

# SOURCES

- **Theo**

<https://sebsauvage.net/comprendre/linux/>

<https://www.journaldunet.fr/web-tech/guide-de-l-entreprise-digitale/1091588-kernel-linux-open-source-8/>

<https://www.redhat.com/fr/topics/linux/what-is-the-linux-kernel>

[https://fr.wikipedia.org/wiki/Noyau\\_Linux](https://fr.wikipedia.org/wiki/Noyau_Linux)

- **RAJ**

<https://www.computerhope.com/jargon/i/ioport.htm>

<https://www.openai.com>

<https://www.baeldung.com/linux/cli-hardware-info>

- **IZA**

<https://buzut.net/101-commandes-indispensables-sous-linux/>

<https://buzut.developpez.com/tutoriels/101-commandes-indispensables-sous-linux/>

<https://kinsta.com/fr/blog/commandes-linux/>

[https://pixees.fr/informatiquelycee/n\\_site/nsi\\_prem\\_cmd\\_base\\_linx.html](https://pixees.fr/informatiquelycee/n_site/nsi_prem_cmd_base_linx.html)

<https://www.lpmagazine.org/sept-types-fichier-linux/#:~:text=d%20exploitation%20Linux,-Il%20existe%20sept%20types%20de%20fichiers%20et%20%C3%A9pertoires%20Linux%20%3A%20les,stock%C3%A9%20dans%20un%20%C3%A9pertoire%20diff%C3%A9rent.>

[http://hautrive.free.fr/linux/page-systeme-fichier-linux.html#Les\\_URL](http://hautrive.free.fr/linux/page-systeme-fichier-linux.html#Les_URL)

<https://www.malekal.com/les-repertoires-systemes-arborescence-linux/>

20

## 4. Administrer les serveurs Linux

- Développer des scripts d'automatisation

Contexte :

- Je souhaite créer des scripts pour administrer efficacement un parc de VM Linux :
  - Monter automatiquement un point de montage NFS vers un NAS Synology
  - Programmer un point de sauvegarde automatique à date régulière (crontab)
  - Nettoyer le système
  - Mise à jour automatique du système

Tâches :

- Créer scripte point de montage automatique NFS vers NAS Synology :
  - script :

```
rsync -auv -r /root/dossier/* /media/nas/volume1/heyaa/barsync -auv -r /root/dossier/*
/media/nas/volume1/heyaa/backup
```

- Créer script de nettoyage système :

```
#!/bin/bash

Nettoyer les journaux système
find /var/log/ -type f -name "*.log" -delete

Supprimer les fichiers temporaires
find /tmp/ -type f -delete

Vider le cache de la mémoire
sync && echo 3 > /proc/sys/vm/drop_caches
```

- Créer script de mise à jour automatique du système

```
#!/bin/bash
```

```
apt-get update && apt-get upgrade -y
```

- Placer les scripts dans un dossier accessible à l'utilisateur, puis indiquer son chemin dans crontab :
  - nano /etc/crontab

```

GNU nano 6.2 /etc/crontab
/etc/crontab: system-wide crontab
Unlike any other crontab you don't have to run the 'crontab'
command to install the new version when you edit this file
and files in /etc/cron.d. These files also have username fields,
that none of the other crontabs do.

SHELL=/bin/sh
You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

Example of job definition:
*----- minute (0 - 59)
|----- hour (0 - 23)
| |----- day of month (1 - 31)
| | |----- month (1 - 12) OR jan,feb,mar,apr ...
| | | |----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
| | | |

* * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.daily)
47 6 * * 7 root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.weekly)
52 6 1 * * * root test -x /usr/sbin/anacron || (cd / && run-parts --report /etc/cron.monthly)

* * * * * /root/backup_advanced.sh

```

The menu bar at the bottom includes:

- ^G Help
- ^O Write Out
- ^W Where Is
- ^K Cut
- ^U Paste
- [ Read 26 lines ]
- ^T Execute
- ^C Location
- W-U Undo
- M-A Set Mark
- M-B To Bracket
- ^R Read File
- ^P Replace
- ^J Justify
- ^Y Go To Line
- W-B Redo
- M-C Copy
- ^Q Where Was

- Créer des utilisateurs ainsi que des groupes et donner accès en SSH

Conditions :

- Je souhaite ajouter des utilisateurs et des groupes, ainsi que donner accès SSH à un groupe spécifique.

Tâches :

- Configurer les ip statique sur serveur Ubuntu 22.04
  - modifier le fichier :

nano /etc/network/interfaces

```

Fichier Édition Onglets Aide
GNU nano 3.2 /etc/network/interfaces Modifié

This file describes the network interfaces available on your system
and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.*

The loopback network interface
auto lo
iface lo inet loopback

allow-hotplug eth0
iface eth0 inet static
address 192.168.1.20
netmask 255.255.255.0
gateway 192.168.1.1

^G Aide ^O Écrire ^W Chercher ^K Couper ^J Justifier ^C Pos. cur.
^X Quitter ^R Lire fich. ^V Remplacer ^U Coller ^T Orthograp. ^I Aller lig.

```

- Gestion des utilisateurs et des groupes
  - Création de groupes  
addgroup authorized\_ssh\_group
    - Création d'utilisateurs  
adduser user
      - Ajout d'utilisateurs dans les groupes  
usermod -a -G authorized\_ssh\_group user
        - Autoriser un group à avoir des accès SSH :
          - Editer le fichier de configuration du service SSH:  
nano /etc/ssh/sshd\_config
            - Ajouter la ligne suivante:  
AllowGroups authorized\_ssh\_group
          - Redémarrer le service:
            - systemctl restart ssh
          - Accorder les droits SUDO à un utilisateur:  
usermod -a -G sudo user
          - Accès SSH via terminal :  
ssh user@192.168.X.X

```

root@debian12:~# adduser luc_sassion
Ajout de l'utilisateur « luc_sassion » ...
Ajout du nouveau groupe « luc_sassion » (1005) ...
Ajout du nouvel utilisateur « luc_sassion » (1005) avec le groupe « luc_sassion » (1005) ...
Création du répertoire personnel « /home/luc_sassion » ...
Copie des fichiers depuis « /etc/skel » ...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd : mot de passe mis à jour avec succès
Modifier les informations associées à un utilisateur pour luc_sassion
Entrer la nouvelle valeur, ou appuyer sur ENTER pour la valeur par défaut
 NOM []: Luc
 Numéro de chambre []: 13
 Téléphone professionnel []: 0989098765
 Téléphone personnel []: 09876789
 Autre []: commentaire
Cette information est-elle correcte ? [0/n]o
Ajout du nouvel utilisateur « luc_sassion » aux groupes supplémentaires « users » ...
Ajout de l'utilisateur « luc_sassion » au groupe « users » ...
root@debian12:~#

```

- Mettre une application en production

Contexte :

- Je souhaite créer un serveur web avec Apache2 sur mon serveur Ubuntu afin de mettre en ligne un site web.

Tâches :

- Installer les paquets Git et Apache2 : apt-get update & apt-get install apache2 & apt-get install git
- Supprimer le contenu de /var/www/html/ : rm -R /var/www/html/\*
- Importer le site web dans /root
  - git clone <https://github.com/SiteWeb/Contenu>
- Se placer dans le répertoire du site web importé et déplacer son tenu vers /var/www/html
  - Vérifier que le site web s'affiche bien en tapant l'adresse ip du server Ubuntu

