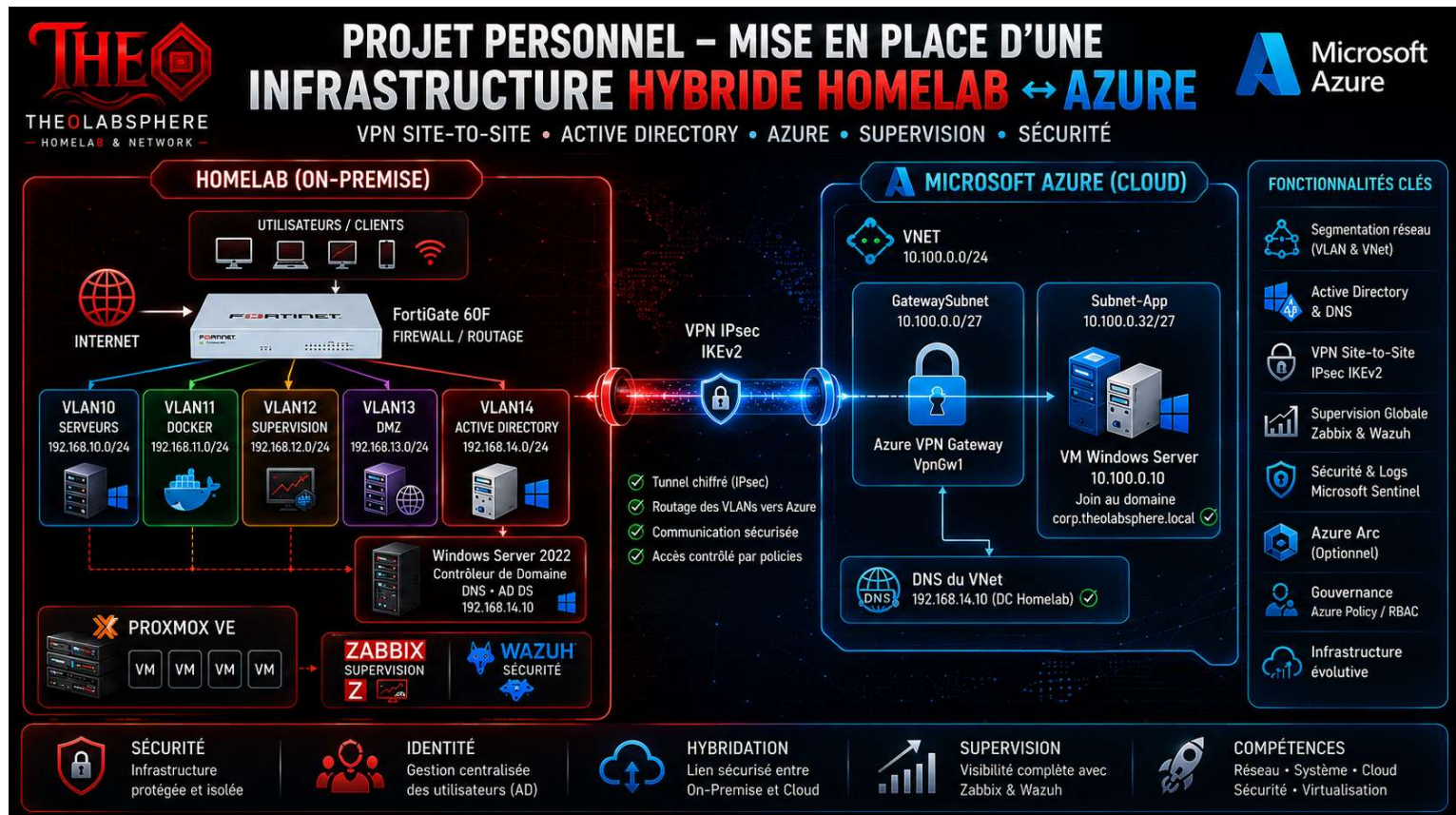


BRETON Théo

Projet N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE MON HOMELAB ET MICROSOFT AZURE

FORTIGATE • VLAN • ACTIVE DIRECTORY • DNS • VPN IPSEC • AZURE • WAZUH • ZABBIX



CAMPUS CARLO ACUTIS

Je tiens à remercier le Campus Carlo Acutis pour les moyens mis à ma disposition dans le cadre de ma formation en BTS SIO, notamment l'accès à la plateforme Microsoft Azure, qui m'ont permis de mettre en pratique et d'approfondir mes compétences en Cloud Computing dans de bonnes conditions.



PROJET PERSONNEL – Théo BRETON

PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

Contexte du Projet

Dans le cadre de mon apprentissage, j'ai décidé de mener ce projet afin de relier mon infrastructure personnelle aux services Cloud de Microsoft Azure et d'acquérir de nouvelles compétences en Cloud Computing. Je souhaite mettre en place une architecture hybride interconnectant mon environnement Homelab, hébergé sur Proxmox, avec Microsoft Azure. L'objectif est de reproduire une architecture proche de celle rencontrée en entreprise, en mettant en œuvre une segmentation réseau, une infrastructure Active Directory, une interconnexion sécurisée entre les environnements On-Premise et Cloud, ainsi que des solutions de supervision et de sécurité.

Segmentation réseau

Une VLAN dédiée à l'Active Directory est créée sur le FortiGate, avec son propre plan d'adressage et ses propres règles de filtrage, afin d'isoler les services d'identité du reste de l'infrastructure. Une seconde VLAN, dédiée aux postes clients, est également créée afin de séparer les serveurs des postes de travail, à l'image d'une segmentation réseau d'entreprise.

Active Directory et DNS

Un Windows Server 2022 est déployé sous Proxmox, promu contrôleur de domaine d'une nouvelle forêt, avec le rôle DNS. Une structure de base (unités d'organisation, groupes, comptes) et quelques GPO sont mises en place pour tester l'administration centralisée.

Interconnexion VPN Site-to-Site

Un tunnel VPN IPsec Site-to-Site relie le FortiGate 60F à une Azure VPN Gateway. Il permet aux deux environnements de communiquer de façon sécurisée via Internet, tout en restant logiquement séparés.

Infrastructure Microsoft Azure

Un groupe de ressources dédié est créé sur Azure afin de regrouper l'ensemble des éléments du projet. Un réseau virtuel (VNet) y est déployé, avec un plan d'adressage distinct de celui du Homelab afin d'éviter tout conflit de routage.

Ce VNet est divisé en deux sous-réseaux : un GatewaySubnet, réservé à la passerelle VPN, et un sous-réseau applicatif destiné à héberger les ressources.

Une Azure VPN Gateway (SKU VpnGw1, en mode routé) est déployée dans le GatewaySubnet et associée à une adresse IP publique statique.

Une Local Network Gateway est configurée pour représenter le FortiGate côté Azure, avec son adresse IP publique et les plages d'adresses des VLAN du Homelab à router à travers le tunnel. Cette configuration complète, côté Azure, l'interconnexion VPN Site-to-Site décrite précédemment.

Une machine virtuelle Windows Server est ensuite déployée dans le sous-réseau applicatif. La configuration DNS du VNet est modifiée pour pointer vers le contrôleur de domaine situé dans le Homelab, ce qui permet à cette VM de résoudre le nom de domaine Active Directory à travers le tunnel et de rejoindre le domaine existant. Cette étape valide l'ensemble de la chaîne technique — routage, règles de pare-feu et VPN — en s'appuyant sur les échanges réels générés par Active Directory (DNS, Kerberos, LDAP, SMB).

Synchronisation des identités et inscription des appareils

Afin d'étendre la gestion des identités au Cloud, Microsoft Entra Connect est déployé pour synchroniser les comptes de l'annuaire Active Directory local vers Microsoft Entra ID.

Deux machines virtuelles Windows 10/11 sont déployées sur le VLAN dédiée aux postes clients et jointes au domaine Active Directory local, au même titre que des postes de travail d'entreprise. Une fois la synchronisation Entra Connect opérationnelle, ces postes sont configurés en Hybrid Azure AD Join, ce qui leur permet d'être à la fois membres du domaine local et enregistrés dans Microsoft Entra ID.

Cette configuration est validée à l'aide de la commande `dsregcmd /status`, qui doit confirmer simultanément les états "AzureAdJoined" et "DomainJoined". Une politique d'accès conditionnel (Conditional Access) est ensuite testée afin de mettre en pratique un scénario de sécurité basé sur la conformité des appareils.

Supervision et sécurité

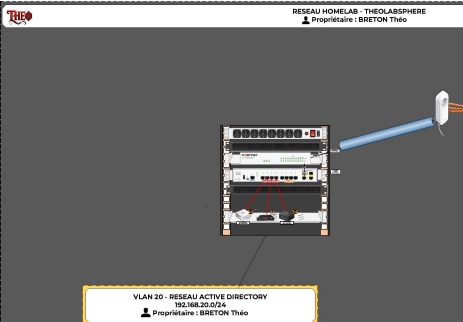
Le contrôleur de domaine est intégré à Zabbix pour la supervision, et à Wazuh pour la collecte des événements de sécurité.

Évolutions envisagées

Second contrôleur de domaine dans Azure, supervision de sécurité Cloud avec Microsoft Sentinel, intégration du Homelab via Azure Arc.
J'ai retiré "synchronisation des identités avec Entra ID" de cette dernière partie puisqu'elle fait maintenant partie du cœur du projet, avec la nouvelle section dédiée.
Dis-moi si tu veux ajuster autre chose, ou si on passe au montage Word.



Schéma Réseau



FreeboxDelta
@IP : 192.168.1.254

LOCAL GATEWAY

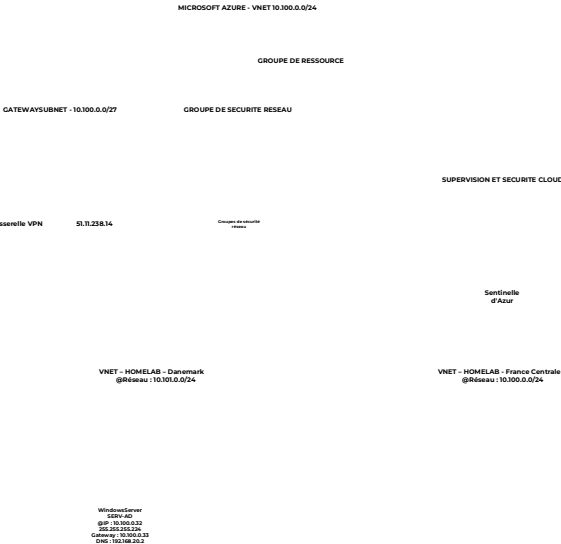
Passerelle Freebox
@IP Public
88.X.X.X

CONNEXION VPN - Fortigate

Clé partagée

WindowsServer
SRV-AD
@IP : 192.168.20.2
@MAC : 08:00:27:5A:19:16
192.168.20.24

SRV-PROXIMOX-THEOLABSPHERE
@IP : 192.168.3.10/24



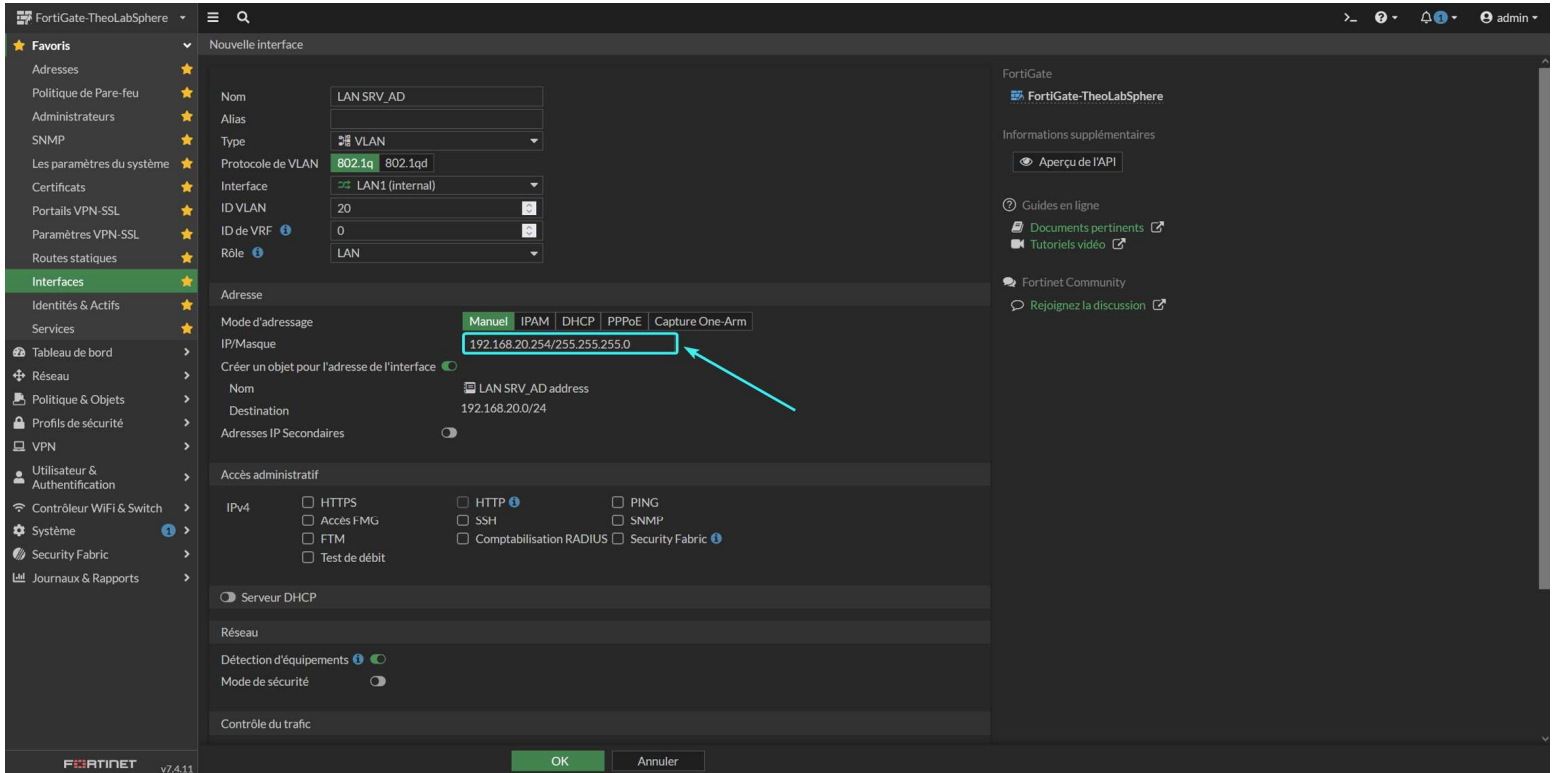
PROJET PERSONNEL – Théo BRETON
PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

PARTIE 1 : OPERATION AU NIVEAU DU HOMELAB

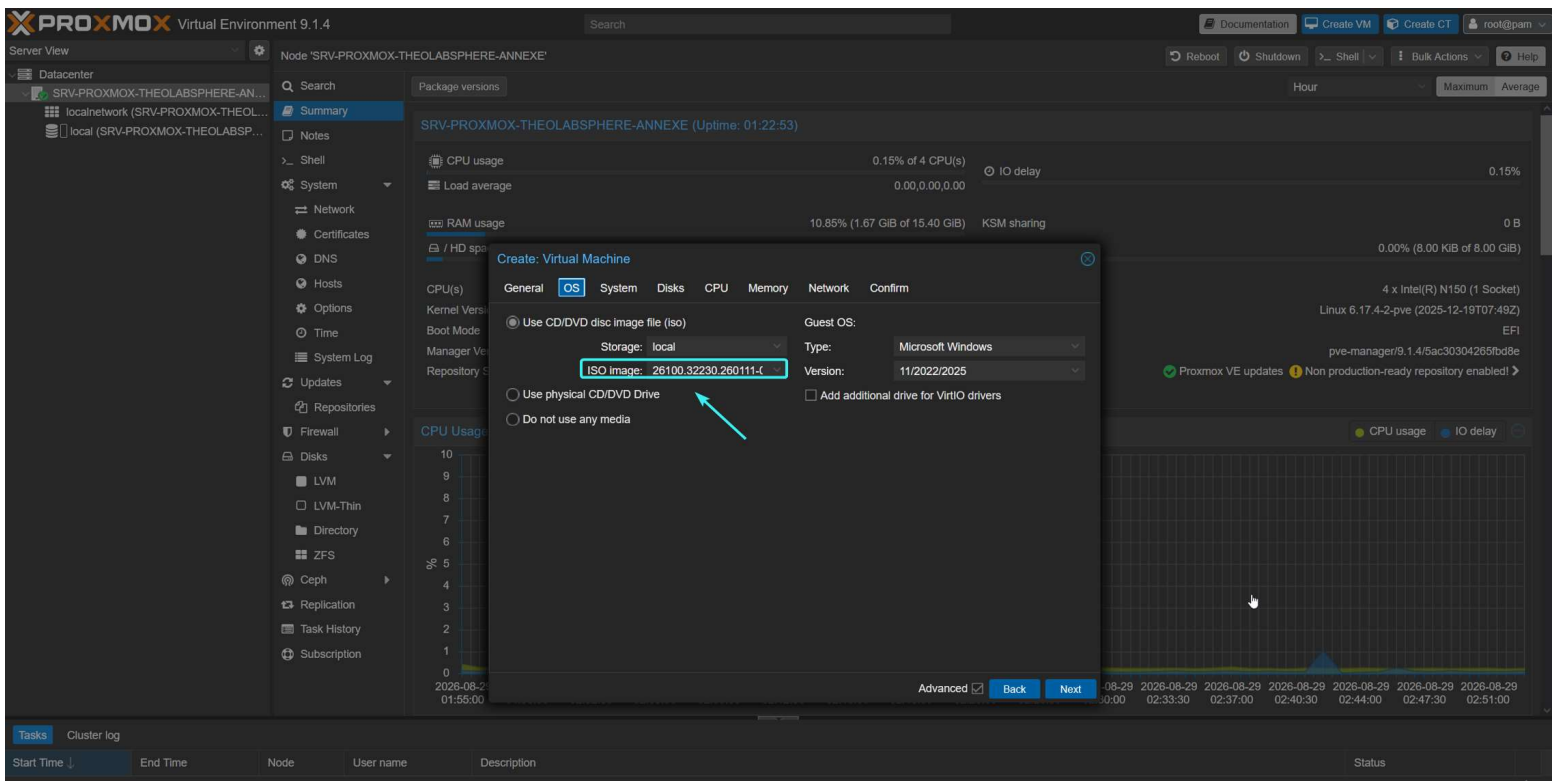
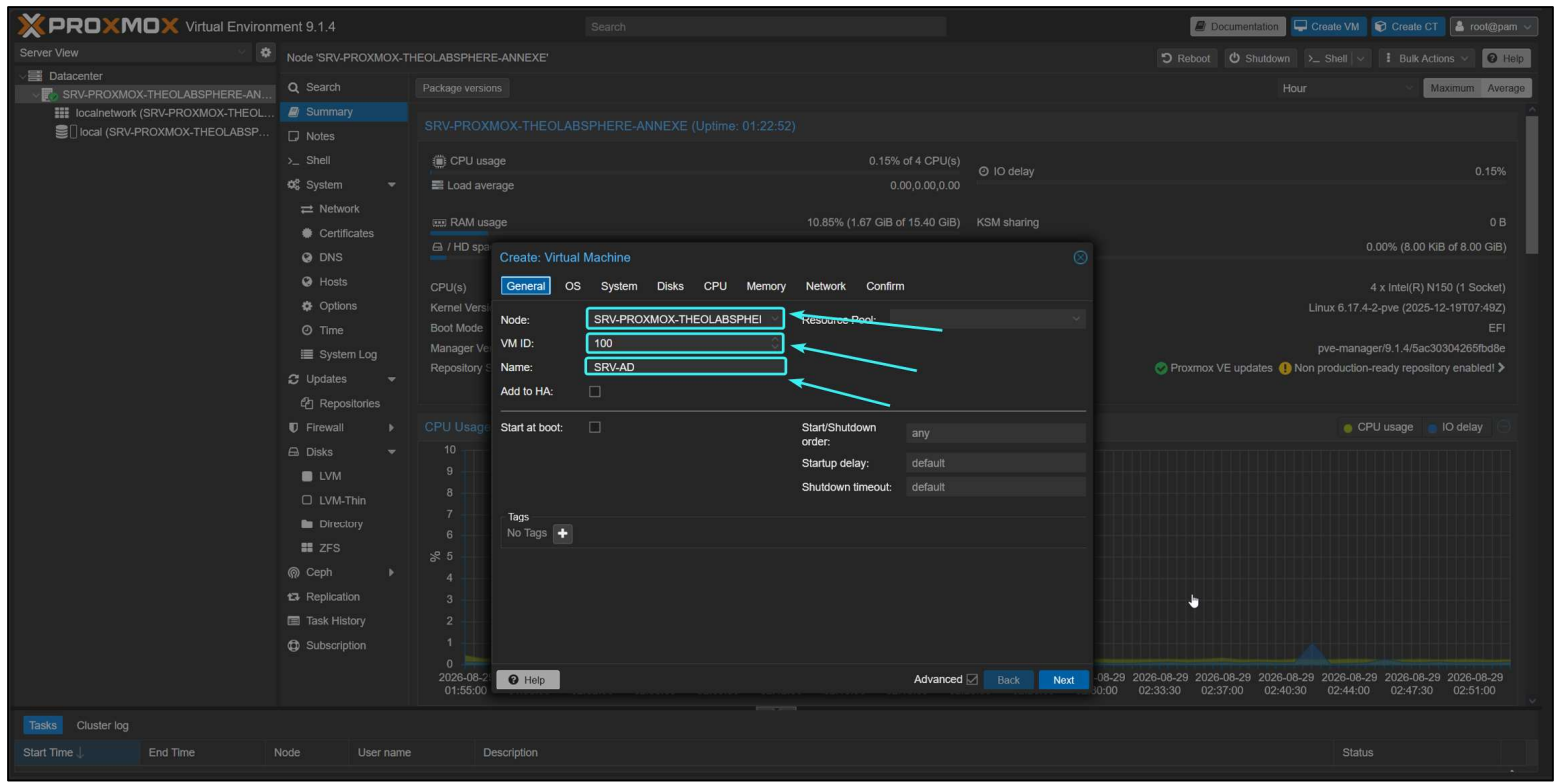
Etape 1 : Création du VLAN 20 - AD :

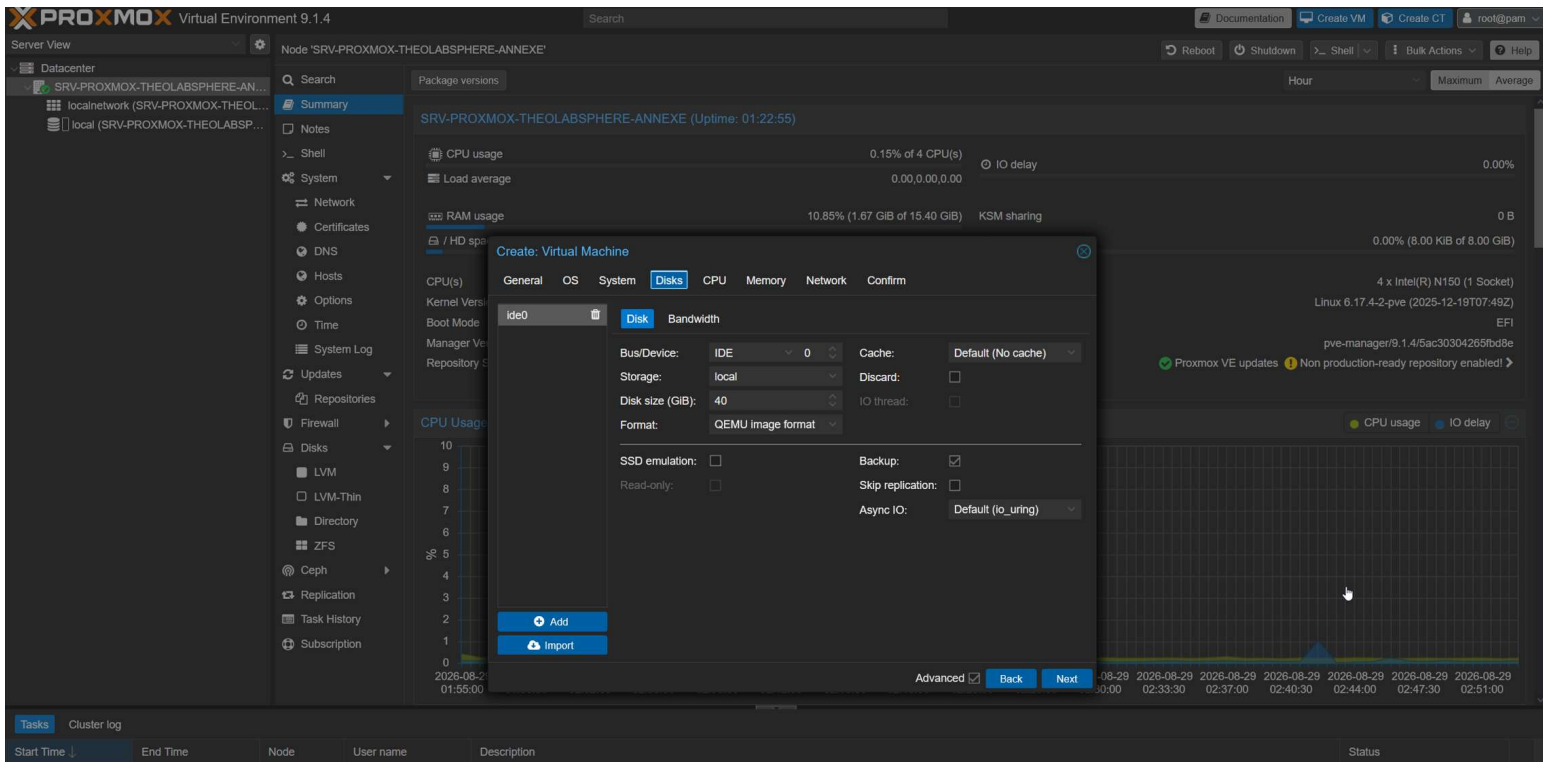
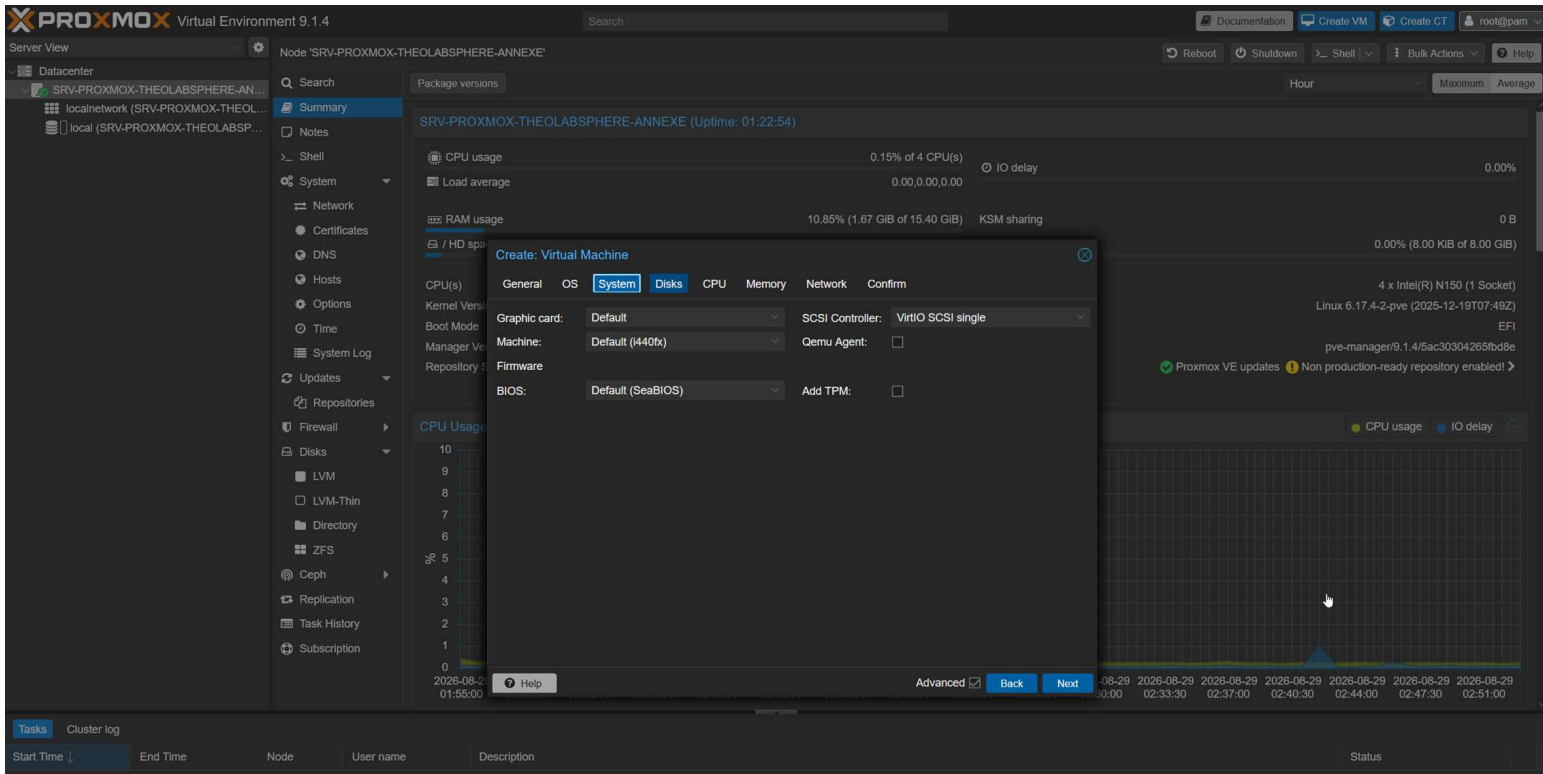
```
SW-HOMELAB_THEO(config)#vlan 20
SW-HOMELAB_THEO(config-vlan)#name Reseau_AD
SW-HOMELAB_THEO(config-vlan)#exit
SW-HOMELAB_THEO(config)#
SW-HOMELAB_THEO(config)#
```

Etape 2 : Création de la sous interface sur le Fortigate :



Etape 3 : Création de la Machine Virtuelle :





PROXMOX Virtual Environment 9.1.4

Server View

Node 'SRV-PROXMOX-THEOLABSPHERE-ANNEXE'

Summary

SRV-PROXMOX-THEOLABSPHERE-ANNEXE (Uptime: 01:22:57)

CPU usage: 0.59% of 4 CPU(s)

Load average: 0.00,0.00,0.00

RAM usage: 10.85% (1.67 GiB of 15.40 GiB)

IO delay: 0.07%

4 x Intel(R) N150 (1 Socket)

Linux 6.17.4-2-pve (2025-12-19T07:49Z)

pve-manager/9.1.4/5ac30304265fbd8e

Proxmox VE updates Non production-ready repository enabled!

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Sockets: 1 Type: x86-64-v2-AES

Cores: 4 Total cores: 4

VCPUs: 4 CPU units: 100

CPU limit: unlimited Enable NUMA: ☐

CPU Affinity: All Cores

Extra CPU Flags:

Default nested-virt Controls nested virtualization, namely 'svm' for AMD CPUs and 'vmx' for Intel CPUs. Live migration still only works if it's the same flag on both sides. Use a CPU model similar to the host, with the same vendor, not x86-64-vx!

Default md-clear Required to let the guest OS know if MDS is mitigated correctly.

Default pcid Meltdown fix cost reduction on Westmere, Sandy-, and IvyBridge Intel CPUs.

Default spec-ctrl Allows improved Spectre mitigation with Intel CPUs.

Default ssbd Protection for 'Speculative Store Bypass' for Intel models.

Advanced ☒ Back Next

PROXMOX Virtual Environment 9.1.4

Server View

Node 'SRV-PROXMOX-THEOLABSPHERE-ANNEXE'

Summary

SRV-PROXMOX-THEOLABSPHERE-ANNEXE (Uptime: 01:23:00)

CPU usage: 0.59% of 4 CPU(s)

Load average: 0.00,0.00,0.00

RAM usage: 10.85% (1.67 GiB of 15.40 GiB)

IO delay: 0.07%

4 x Intel(R) N150 (1 Socket)

Linux 6.17.4-2-pve (2025-12-19T07:49Z)

pve-manager/9.1.4/5ac30304265fbd8e

Proxmox VE updates Non production-ready repository enabled!

Create: Virtual Machine

General OS System Disks CPU Memory Network Confirm

Memory (MiB): 4096

Minimum memory (MiB): 4096

Shares: Default (1000)

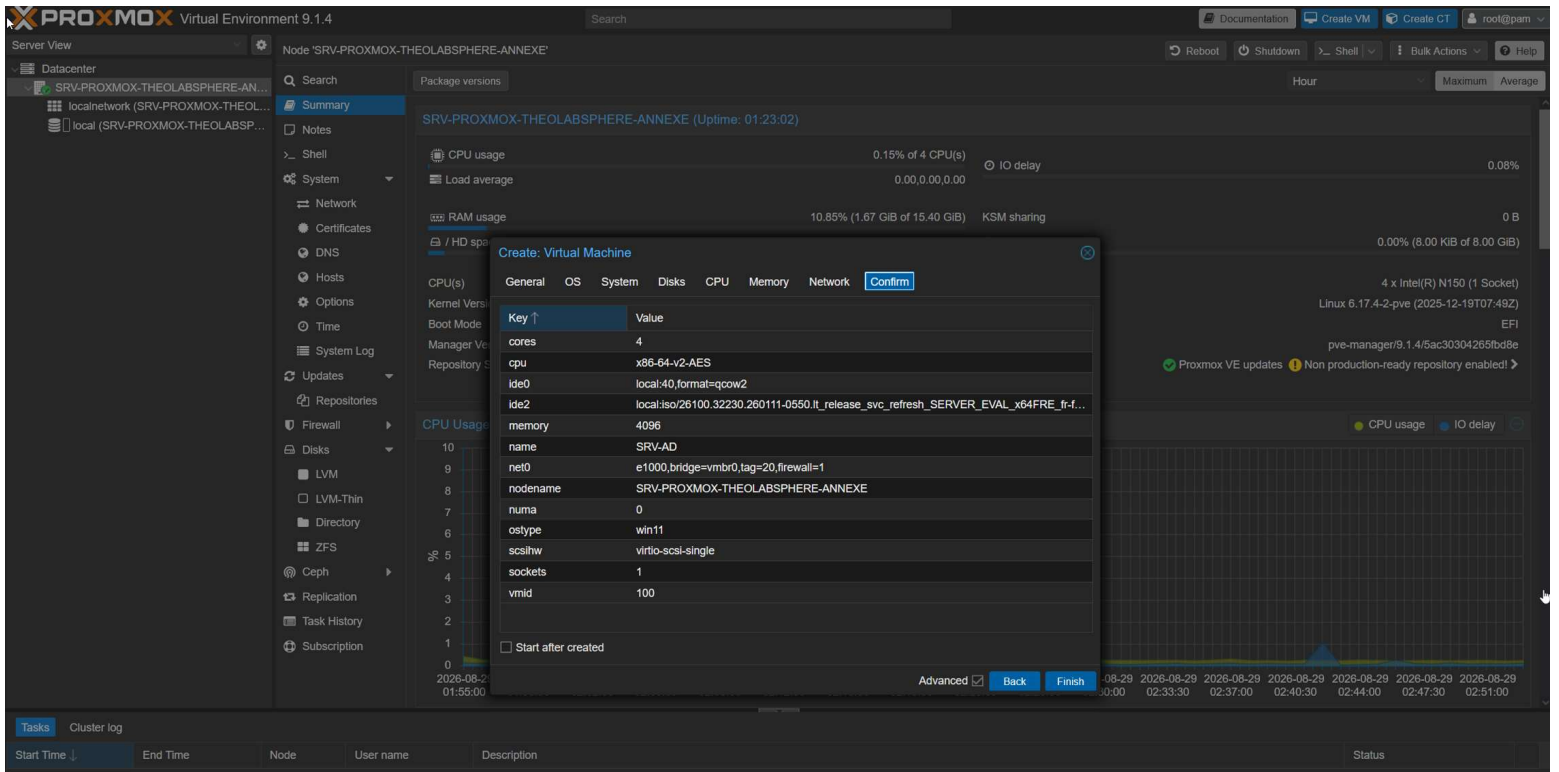
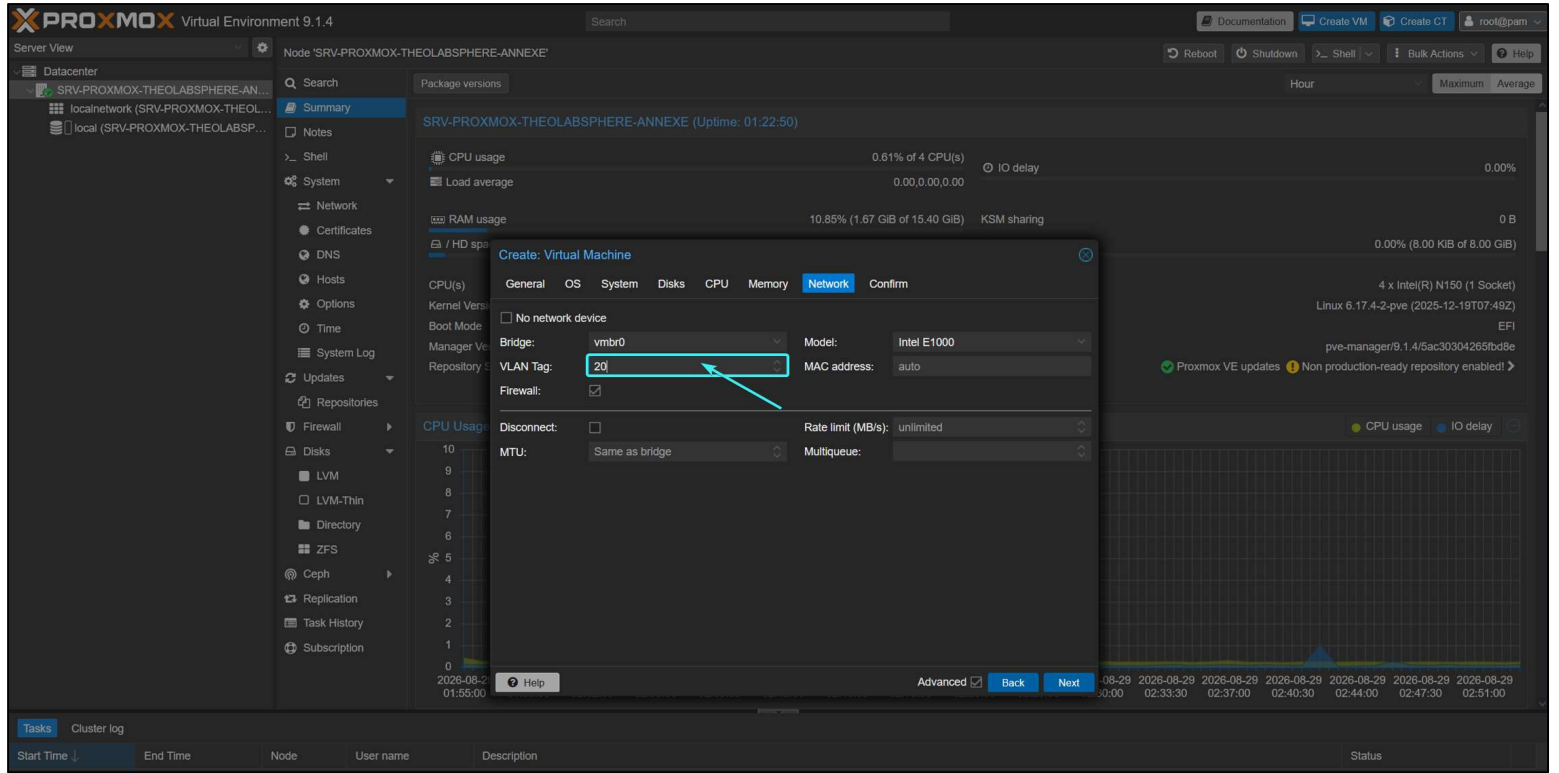
Ballooning Device: ☒

Allow KSM: ☒

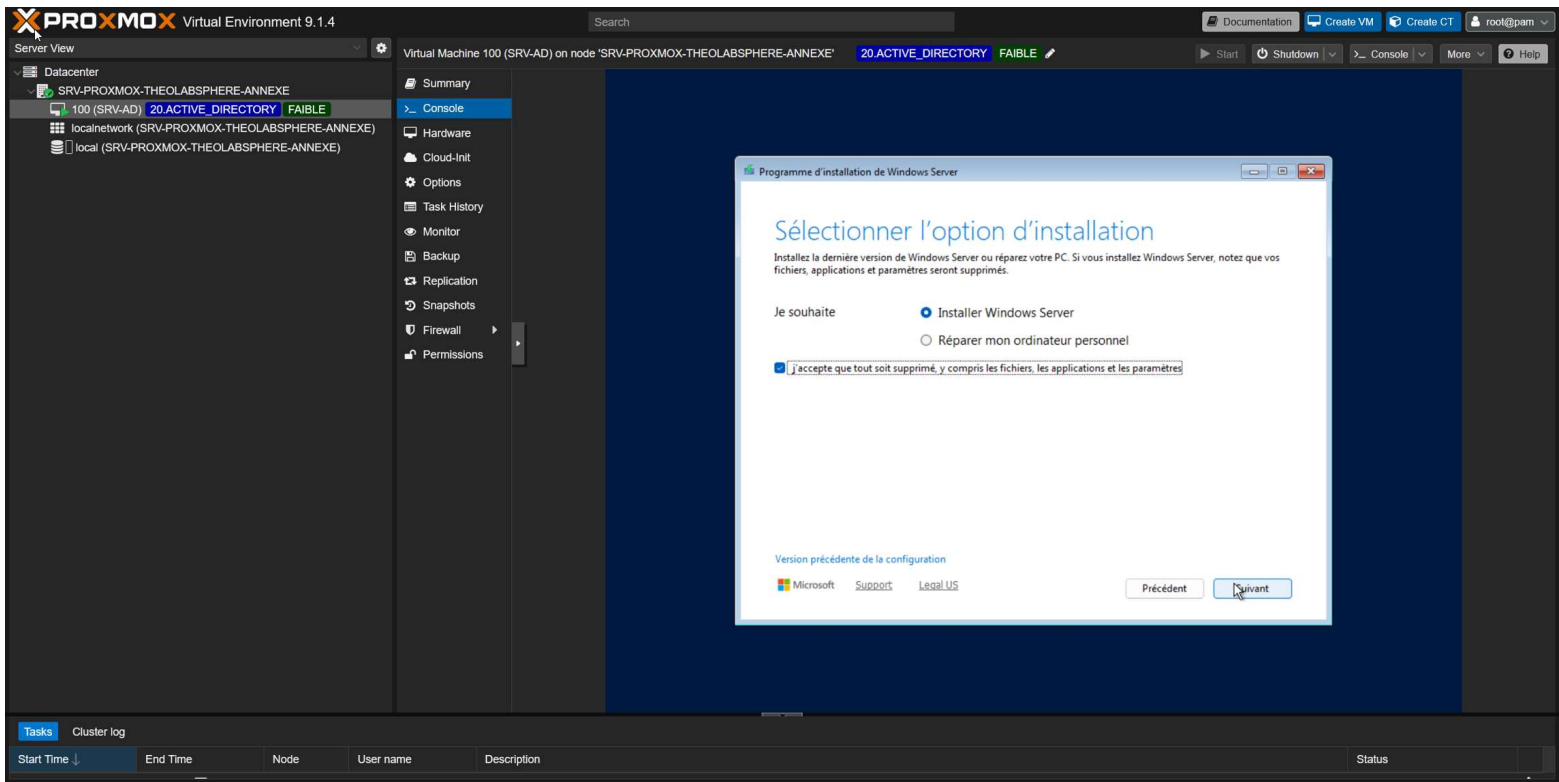
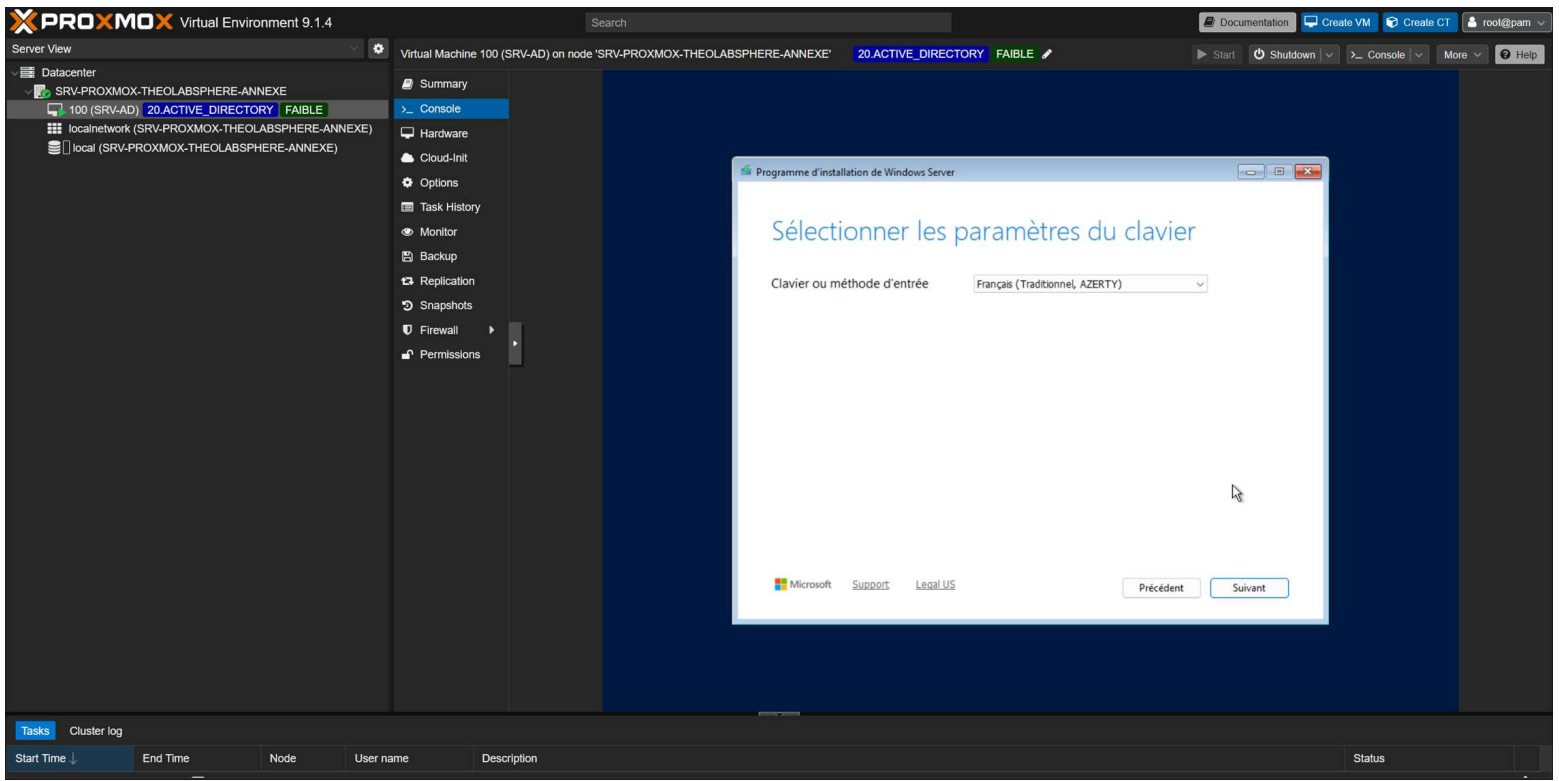
Advanced ☒ Back Next

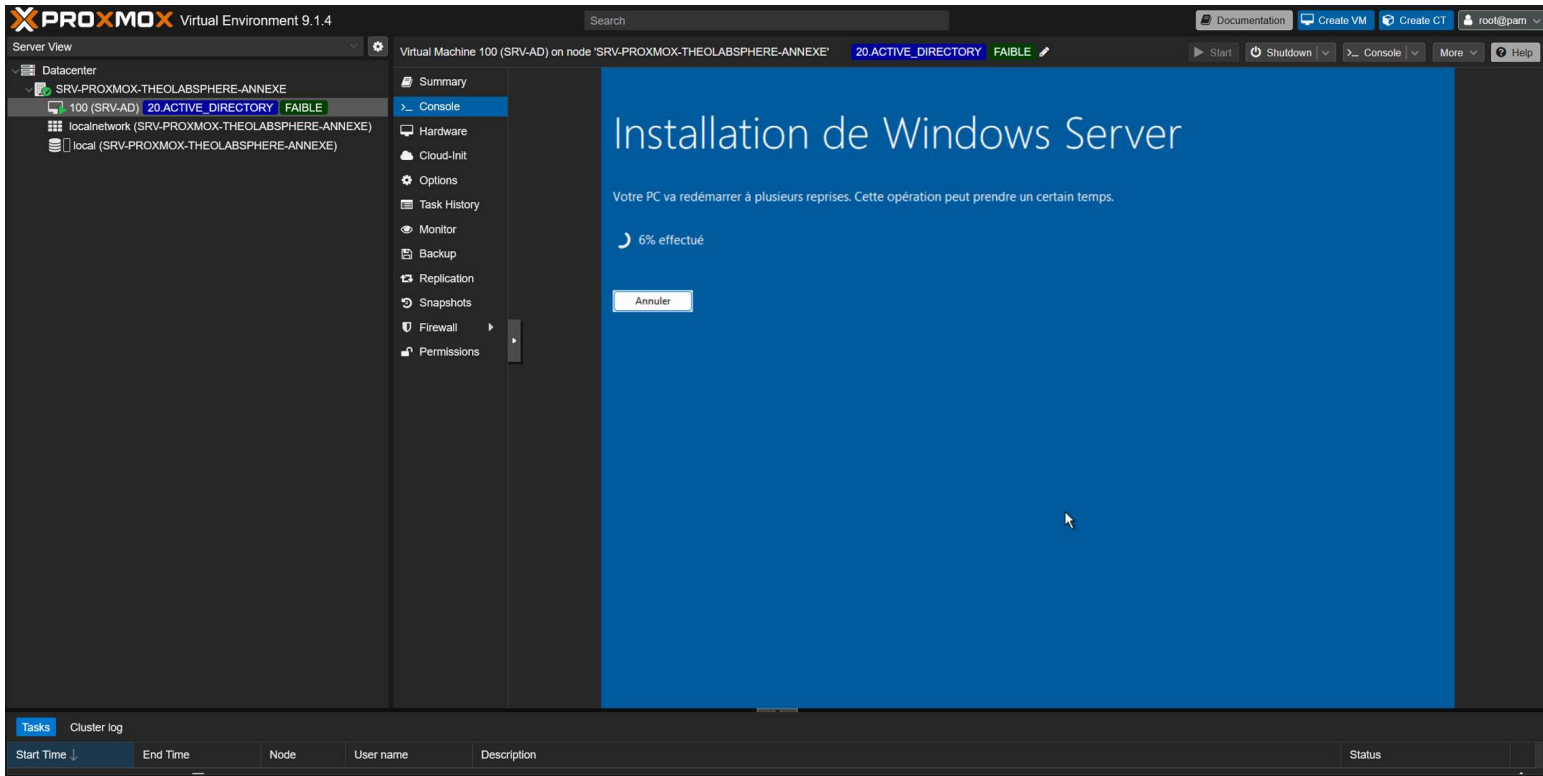
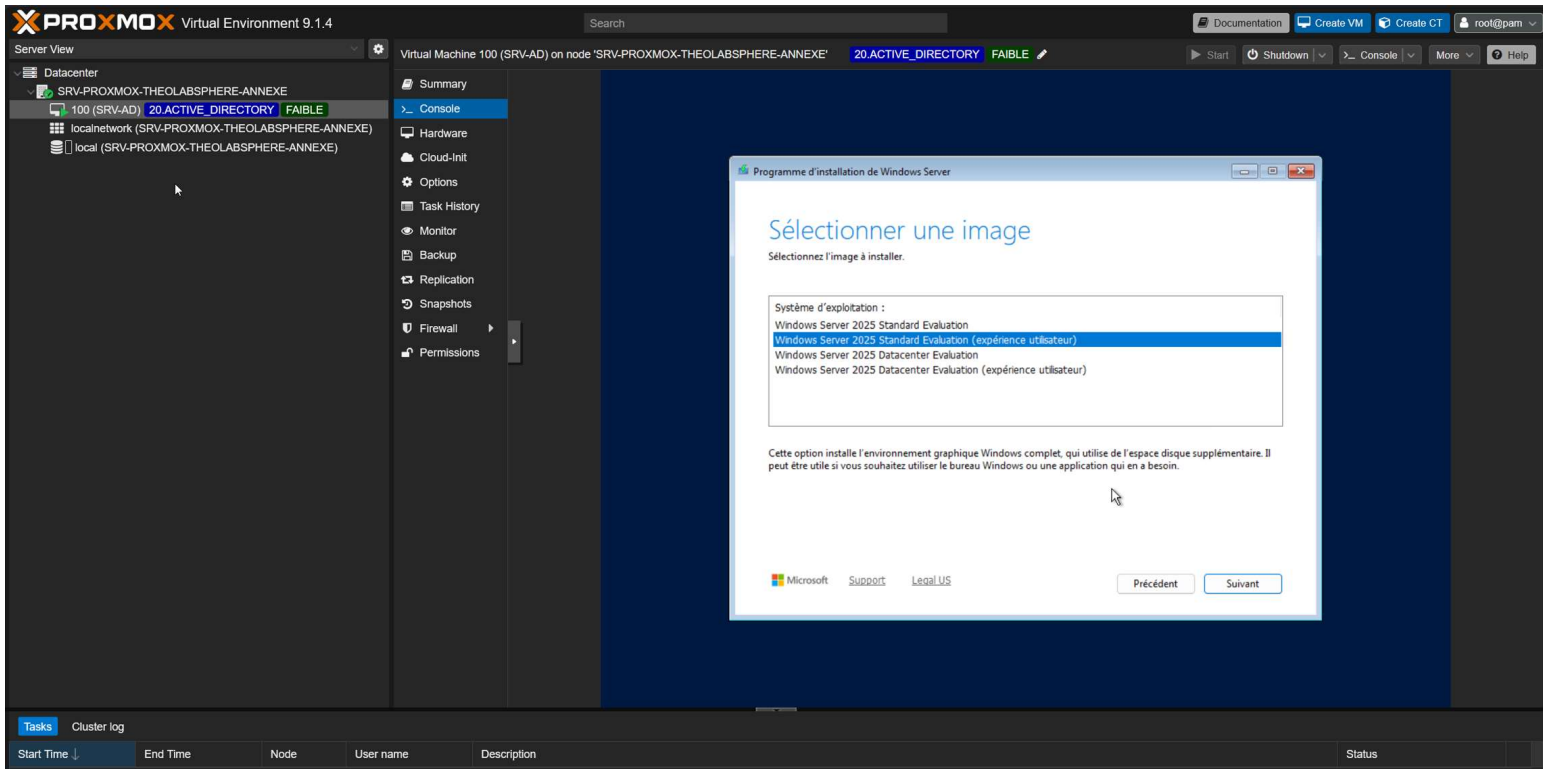


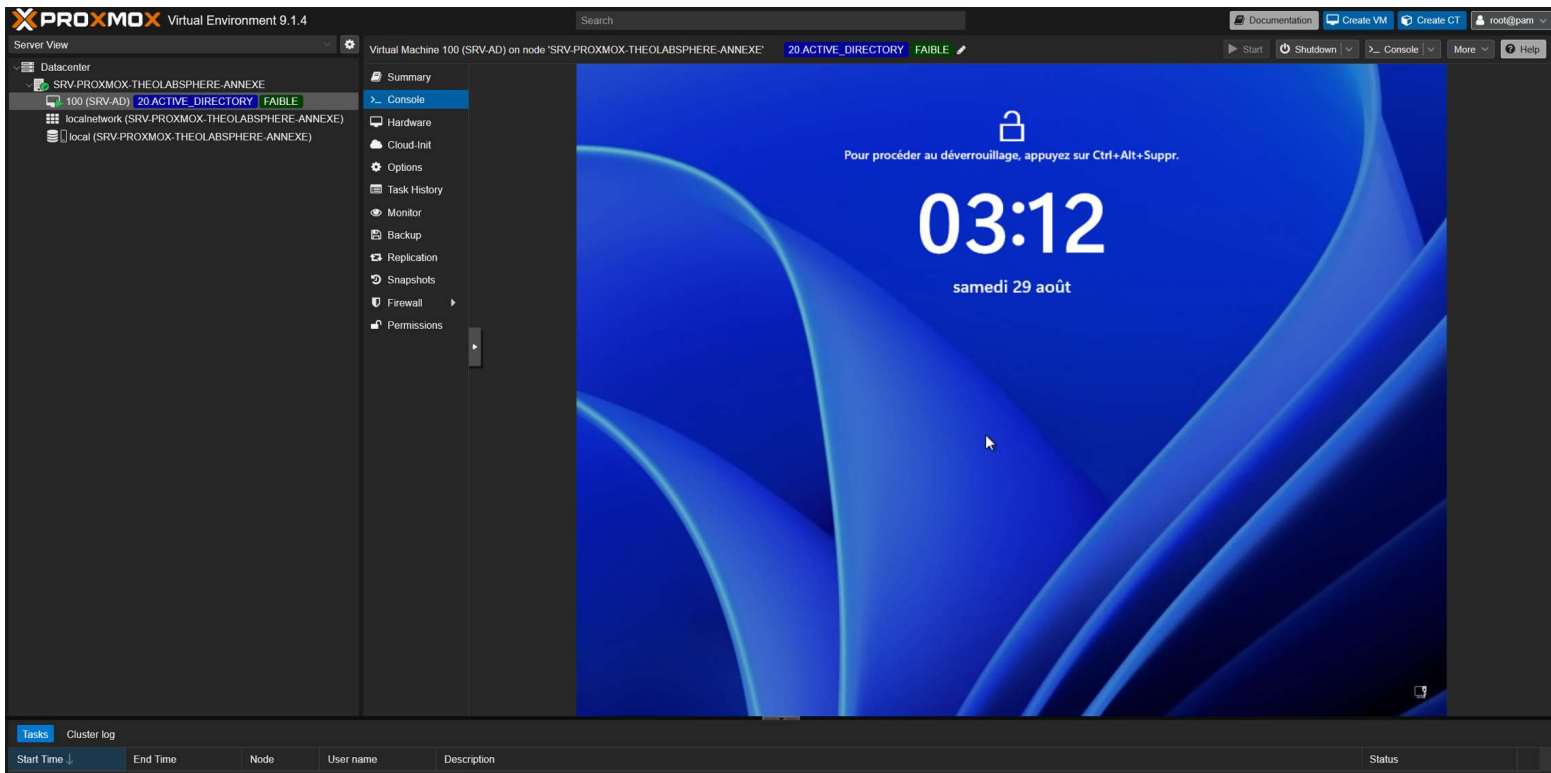
Affecter la VM au VLAN 20 :



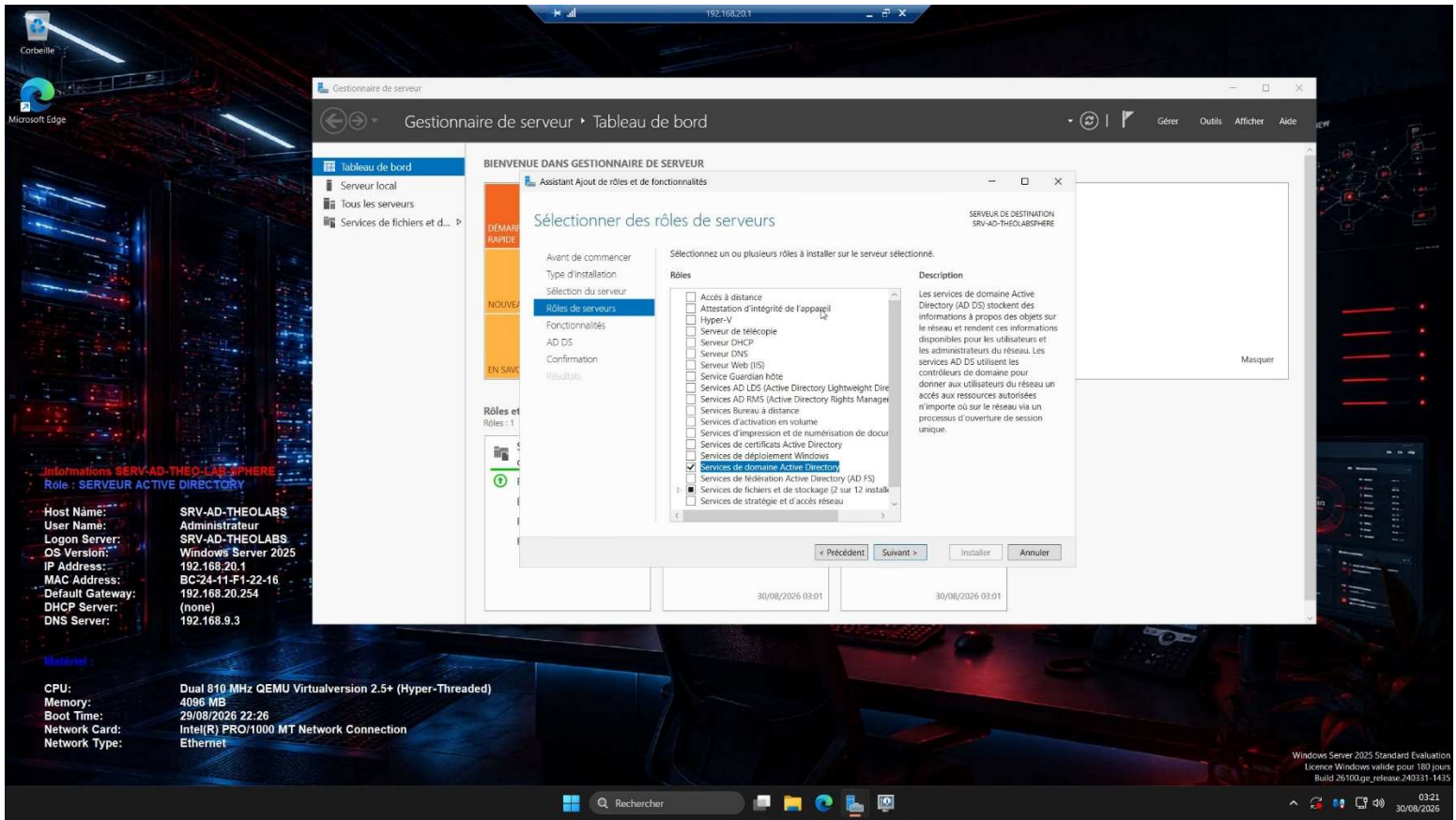
Etape 4 : Installation de Windows Server

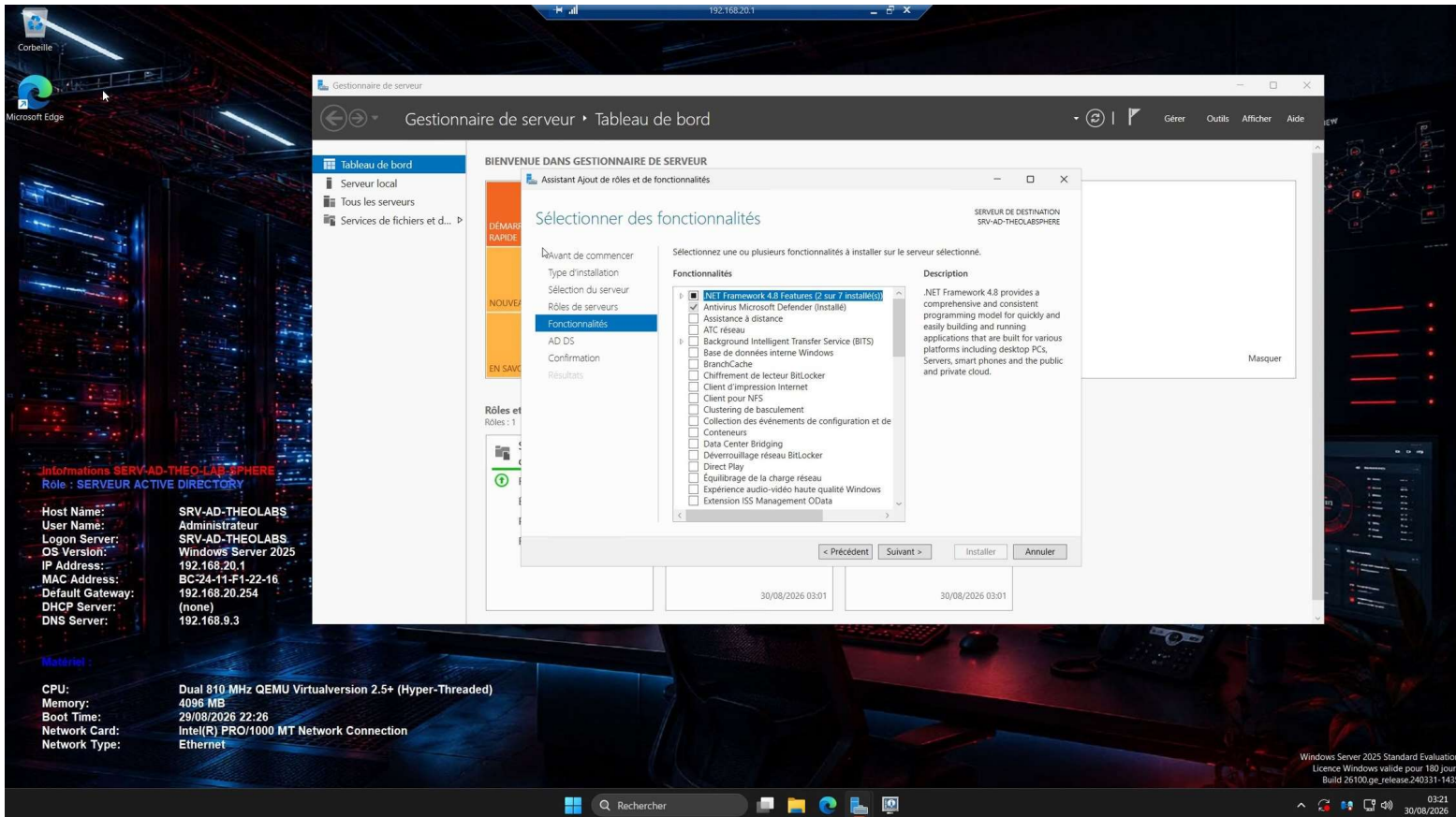
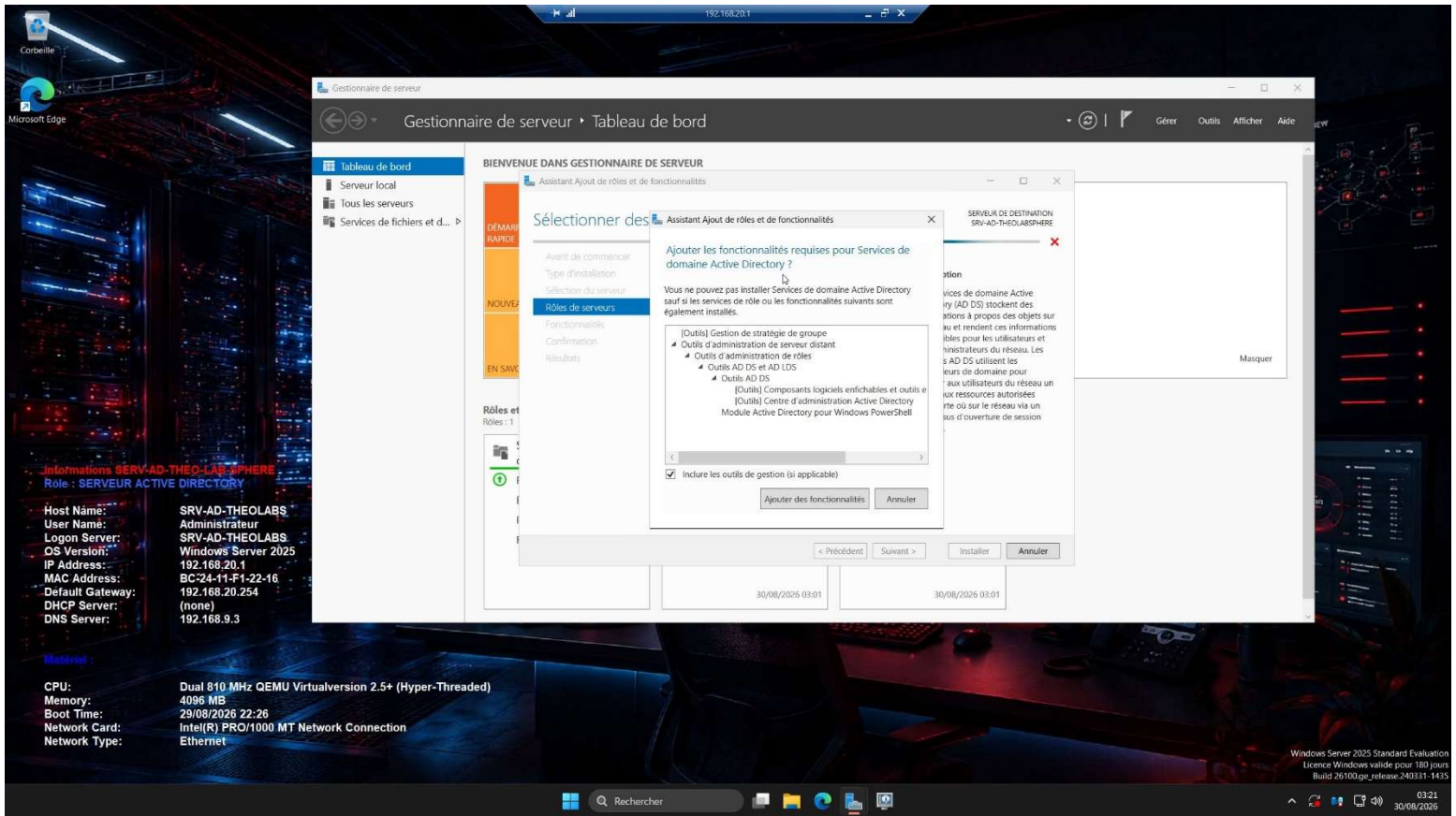


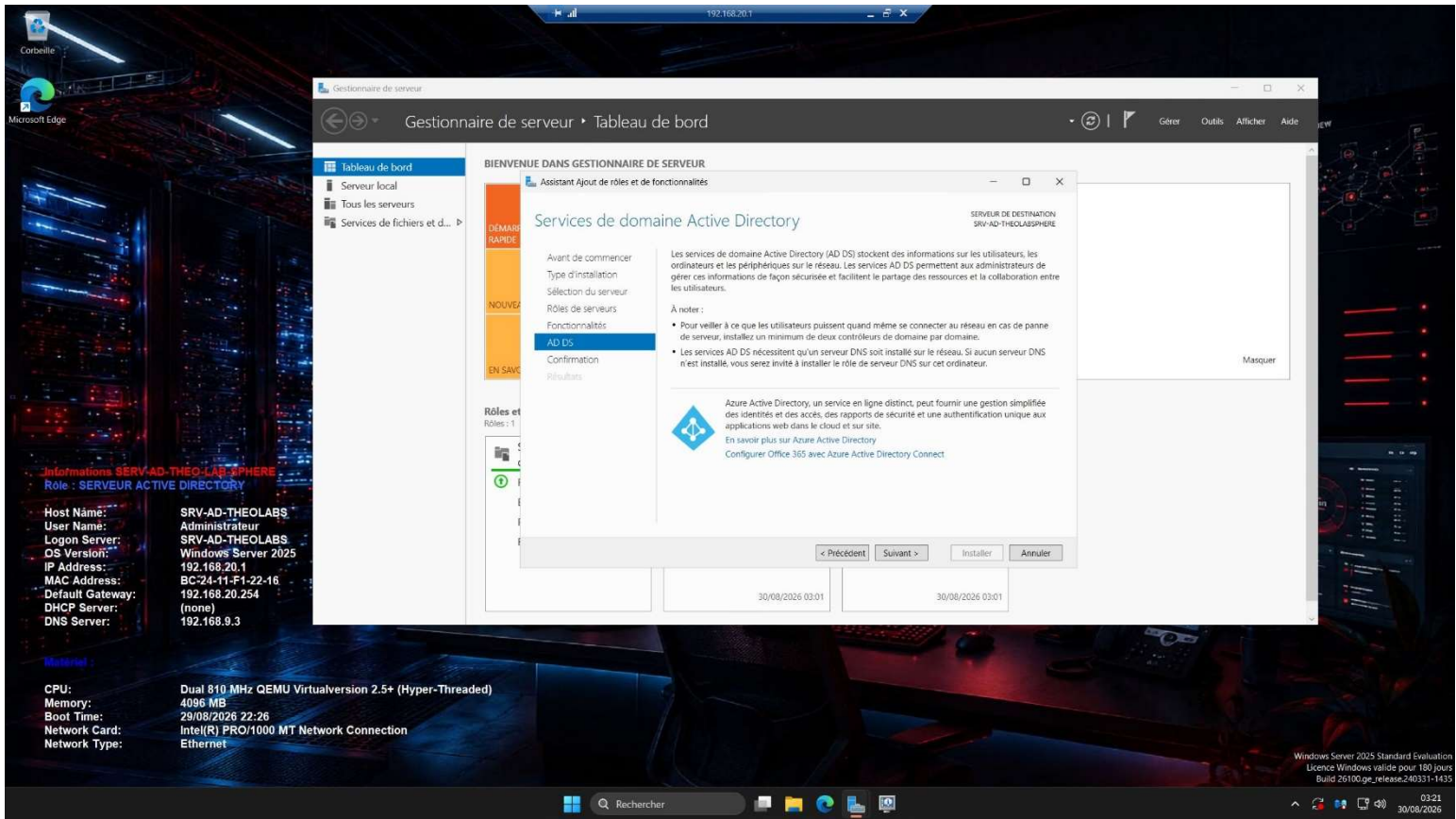


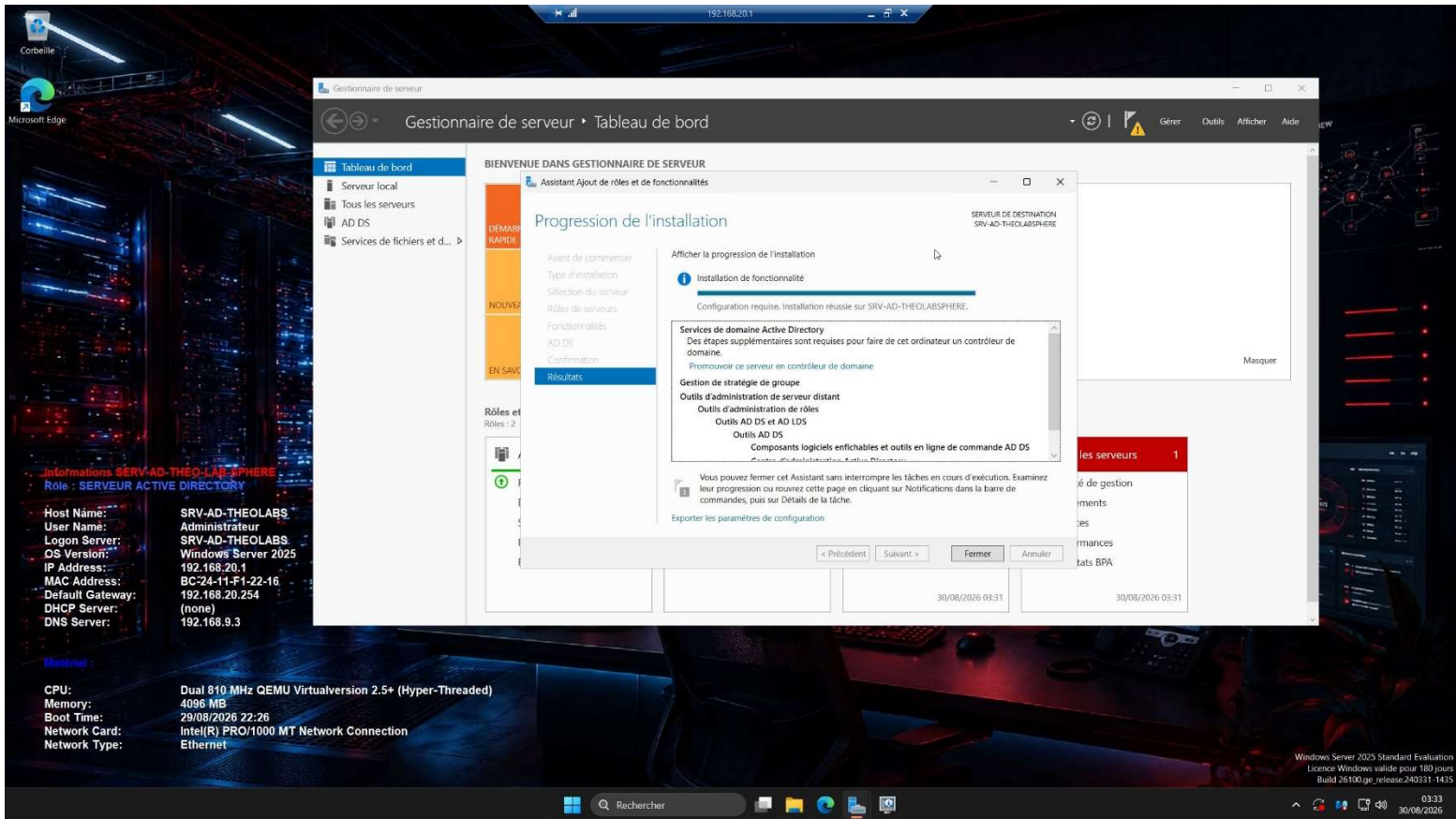


Etape 5 : Ajout du rôle Active Directory :

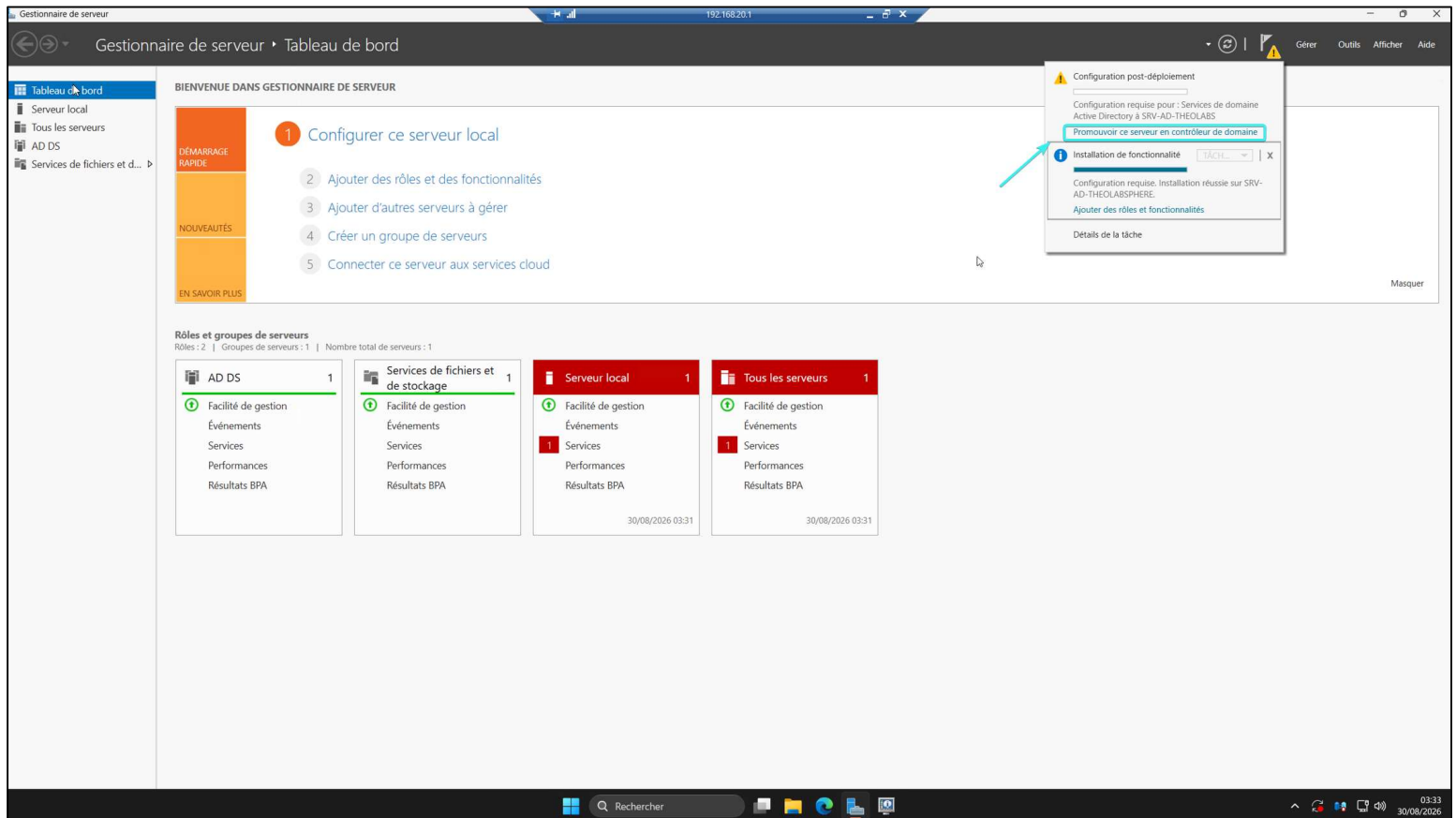


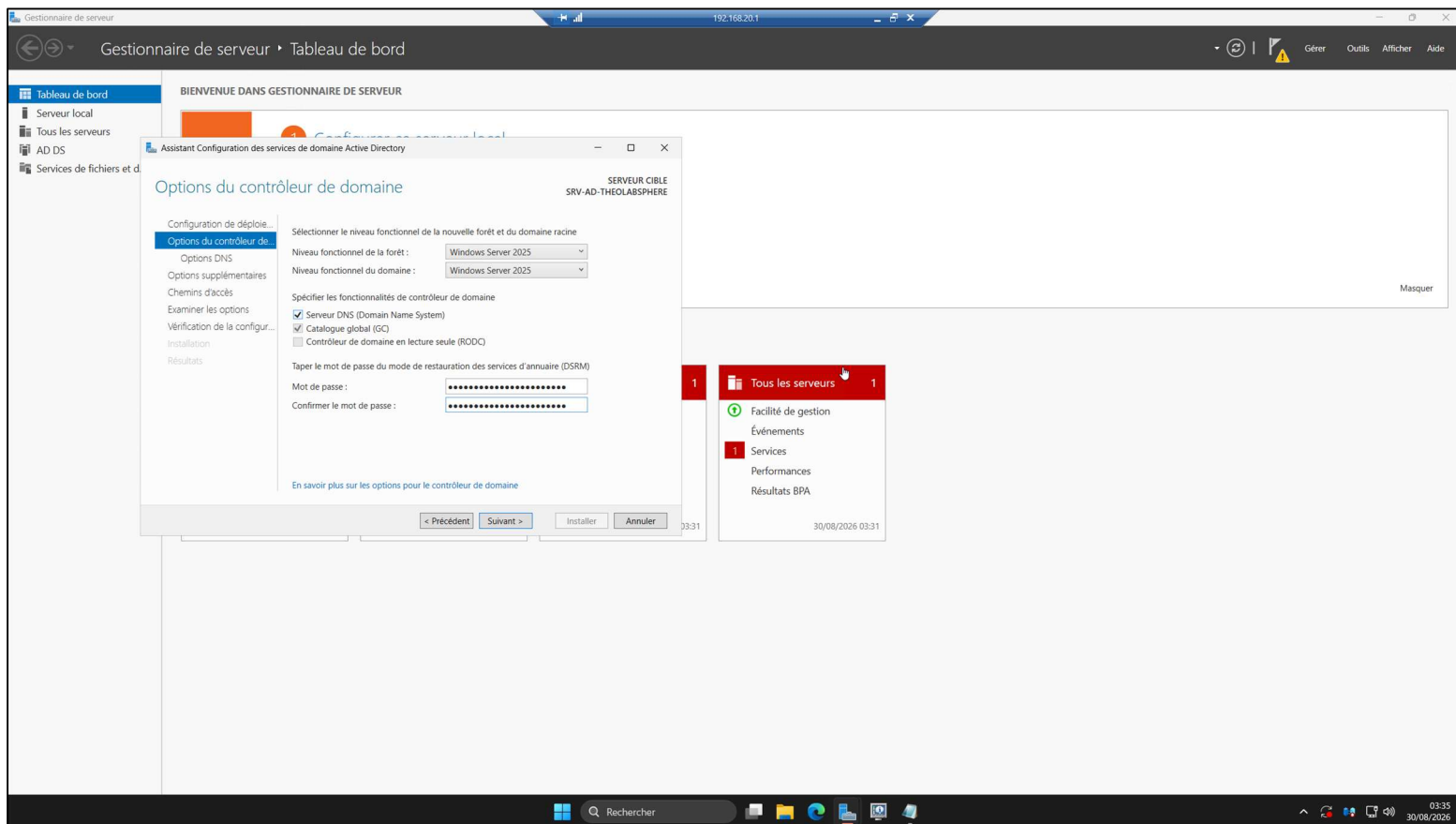
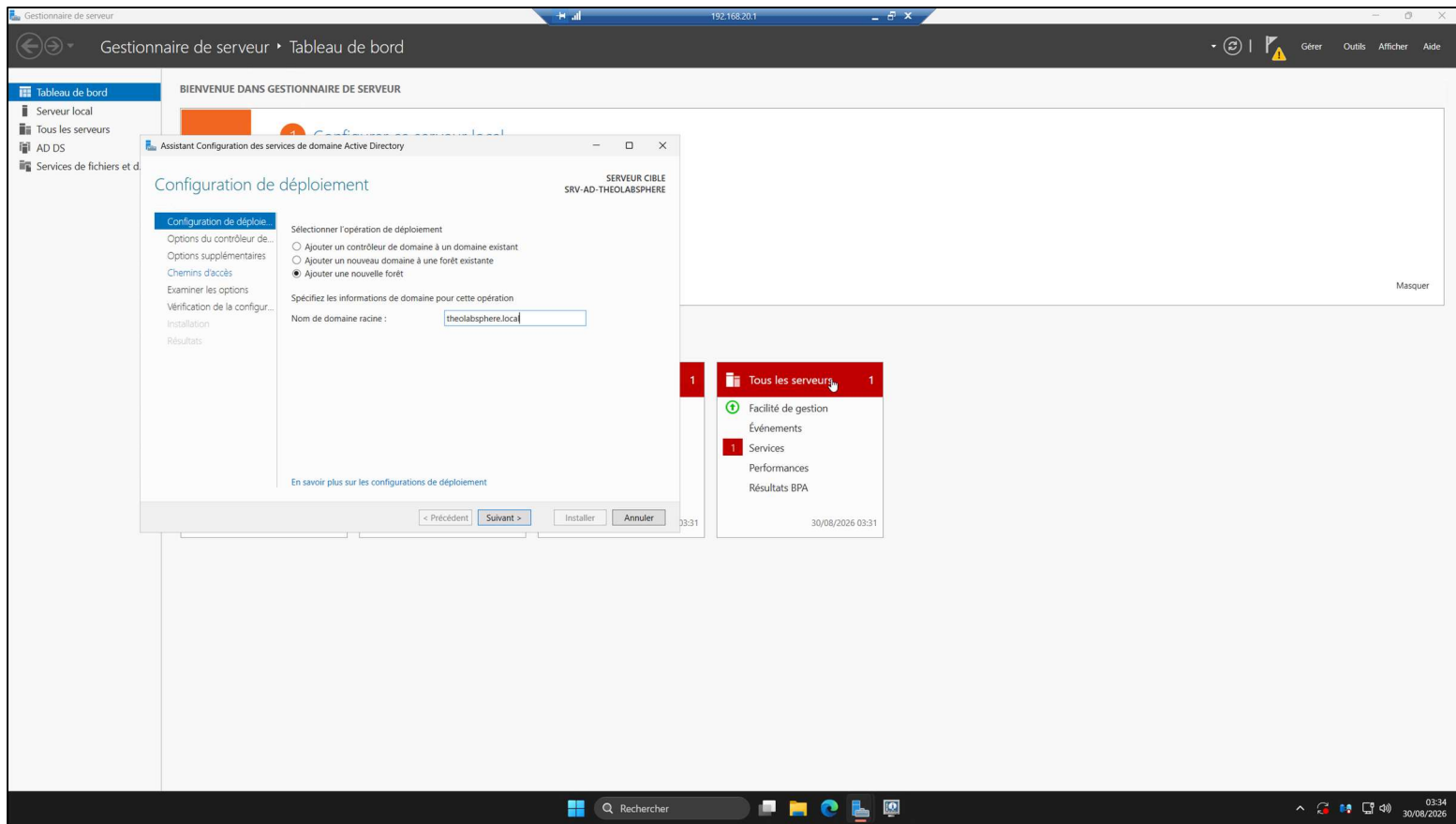


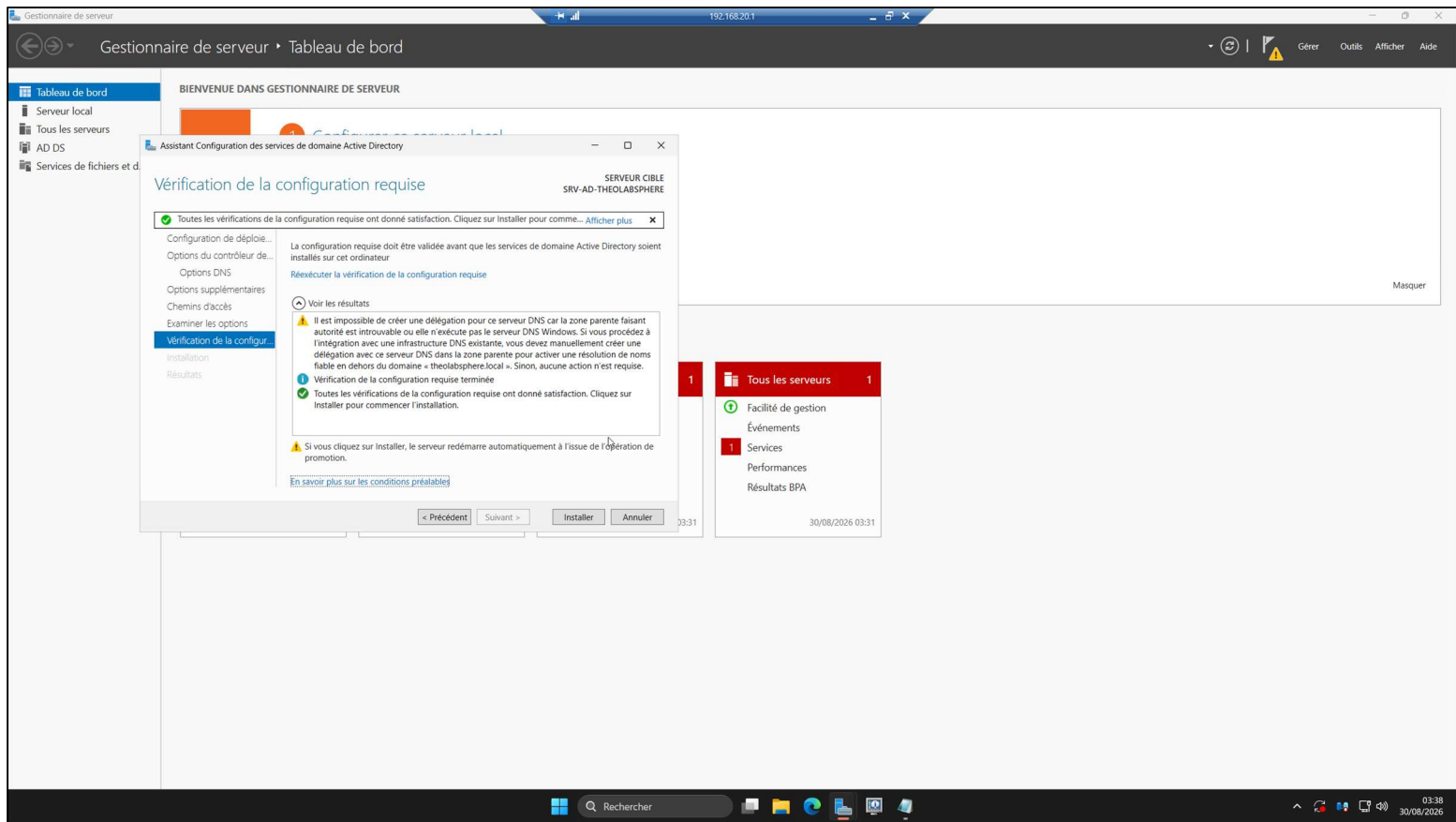




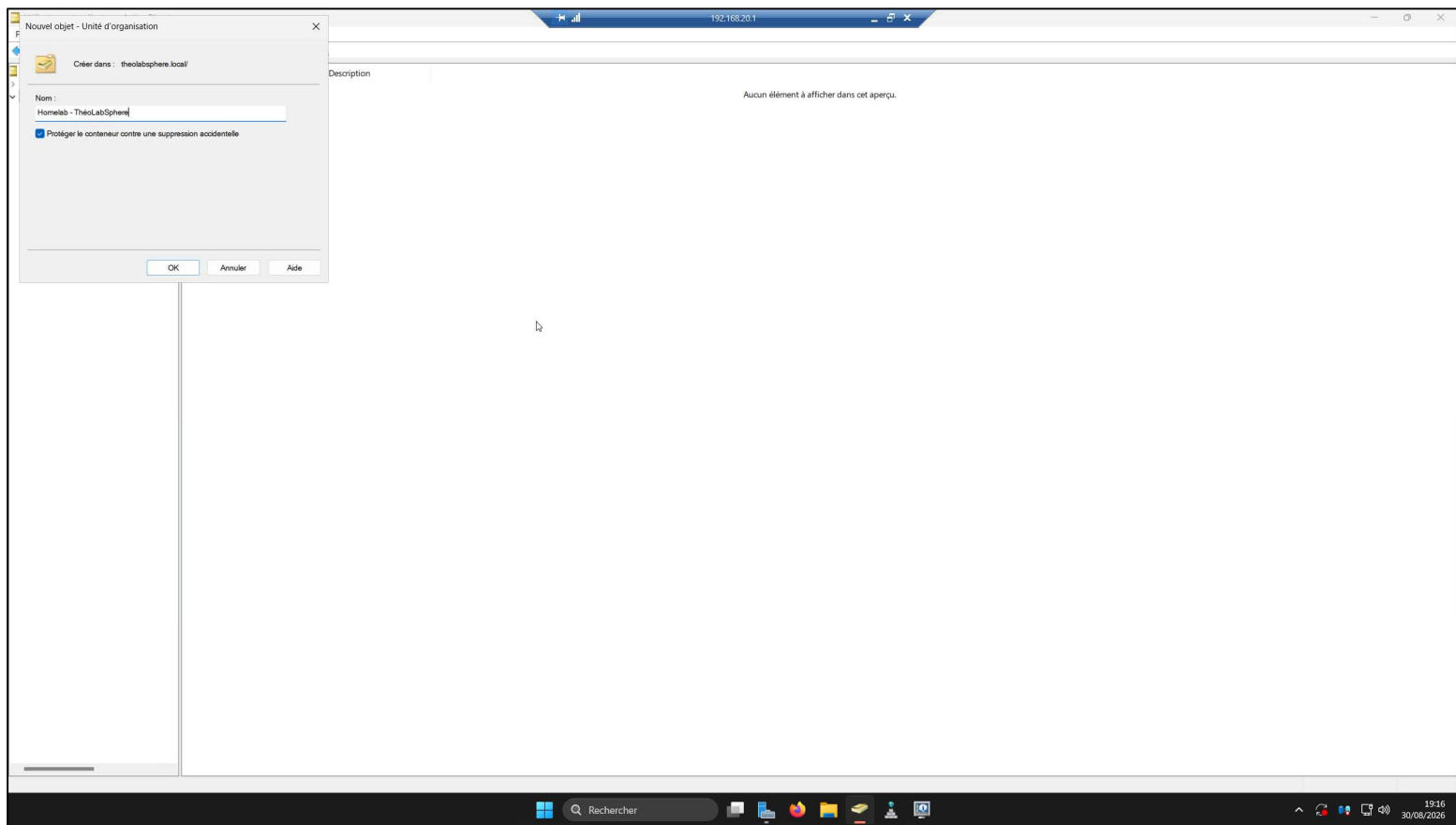
Etape 6 : Promouvoir le contrôleur de domaine :



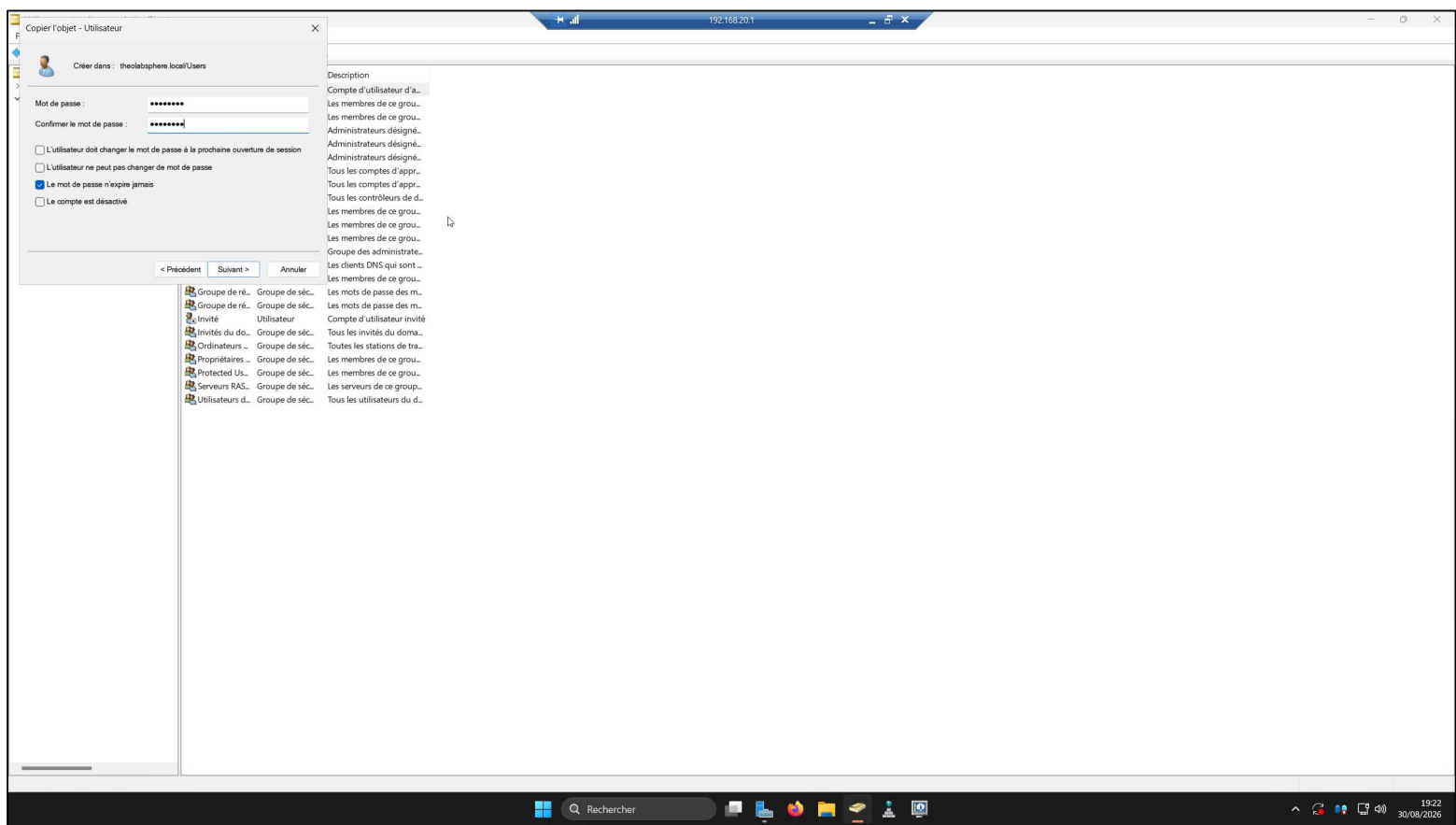
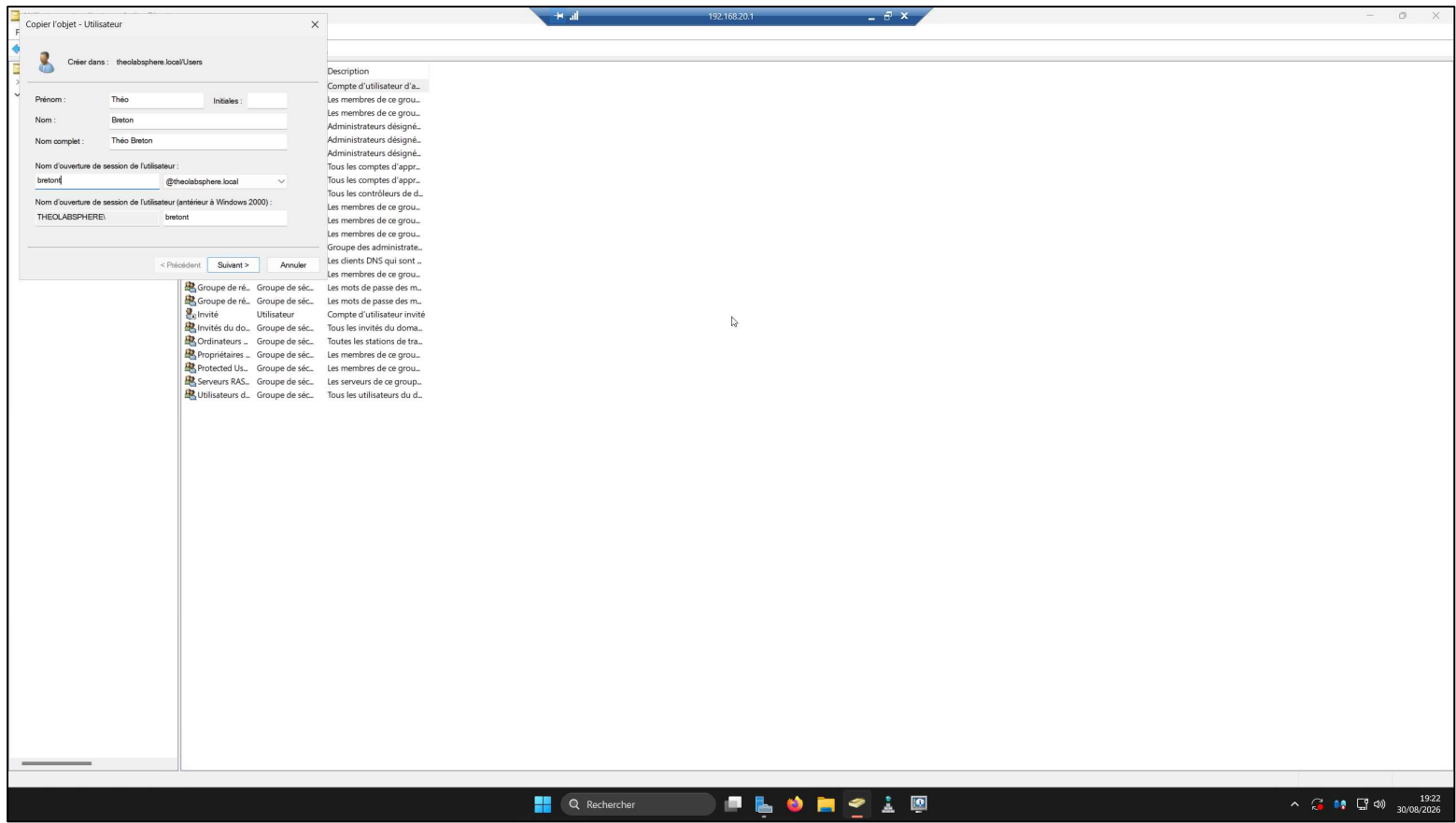




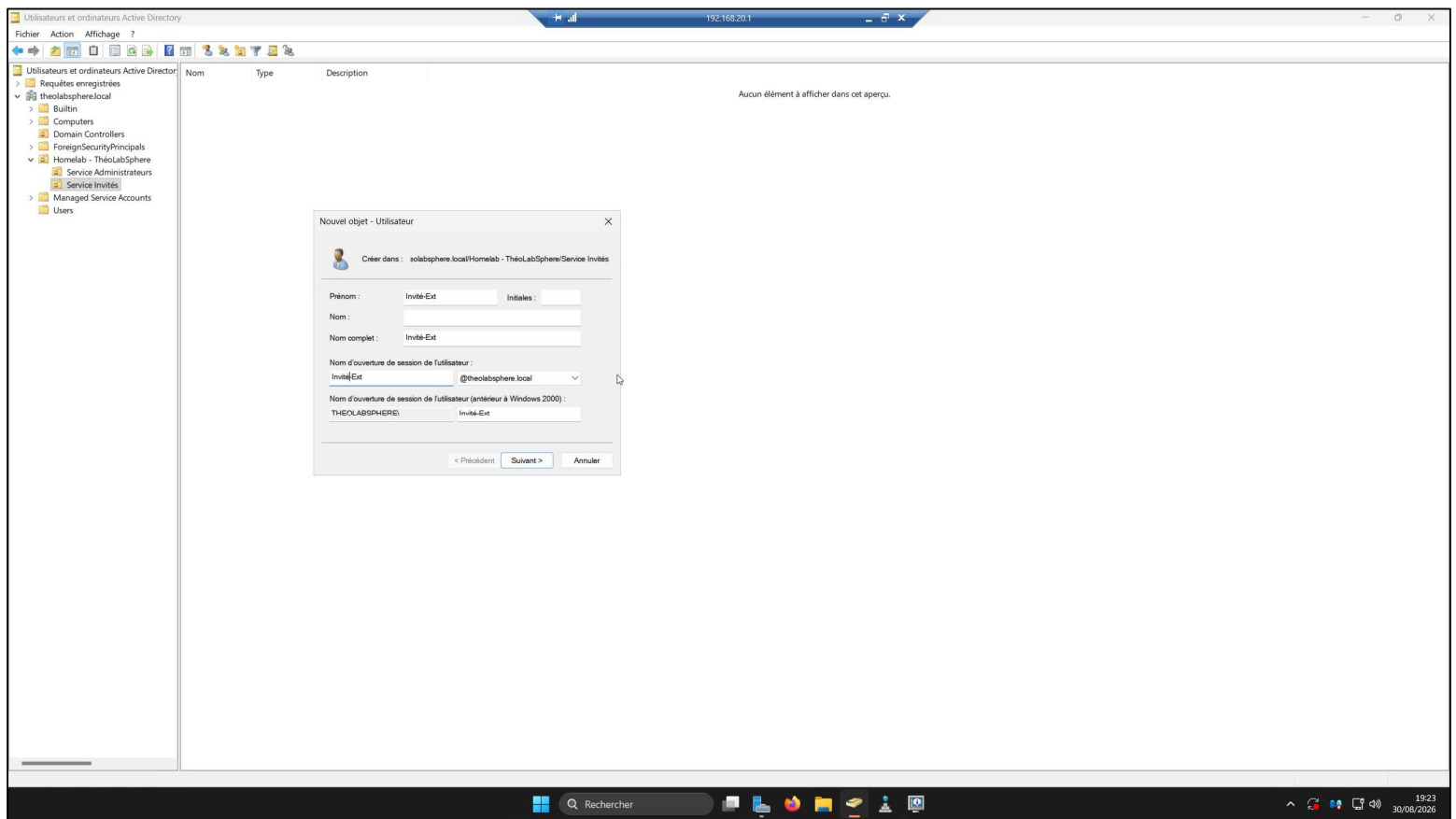
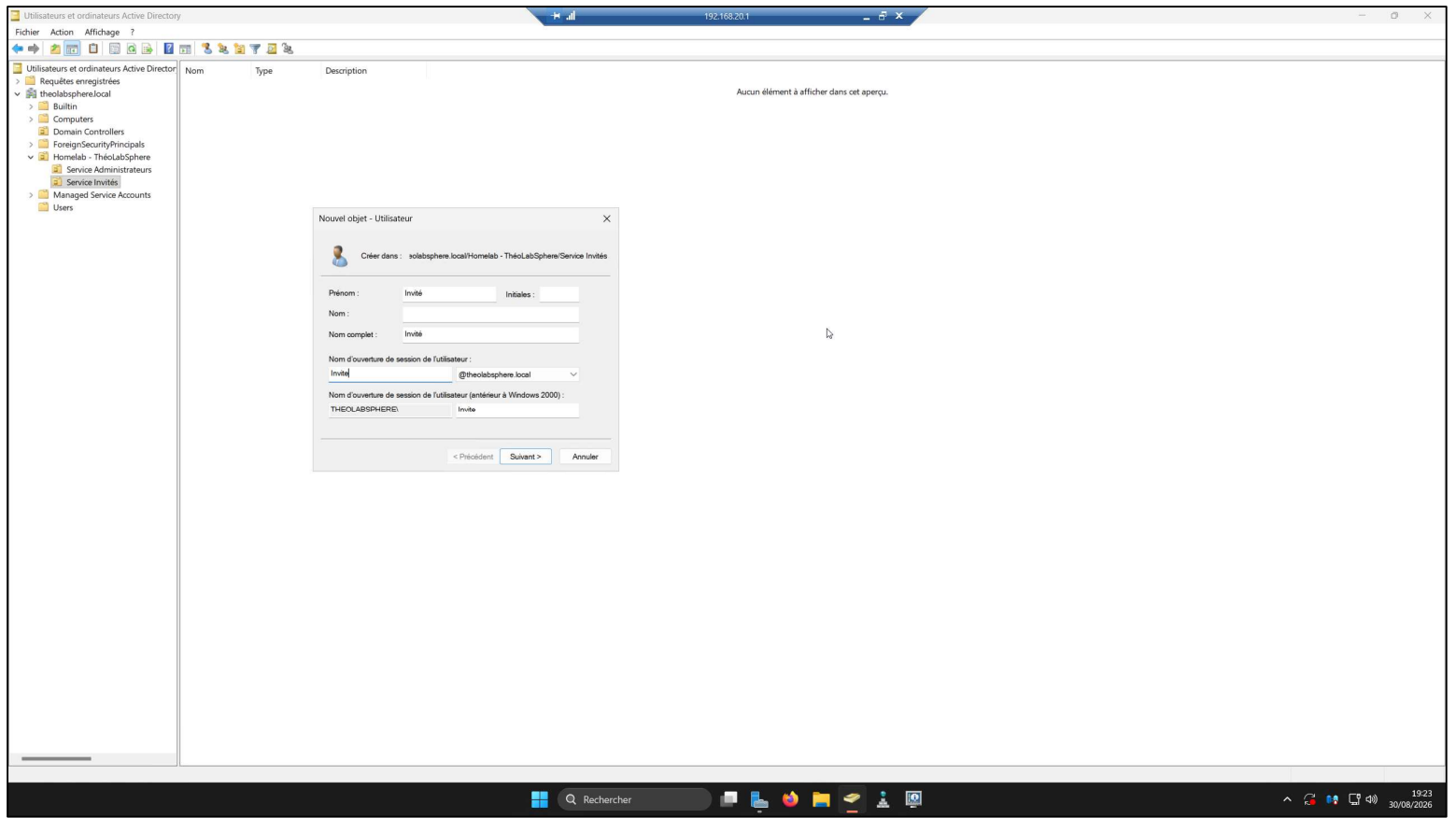
Etape 7 : Création de mes Unités d'Organisations :

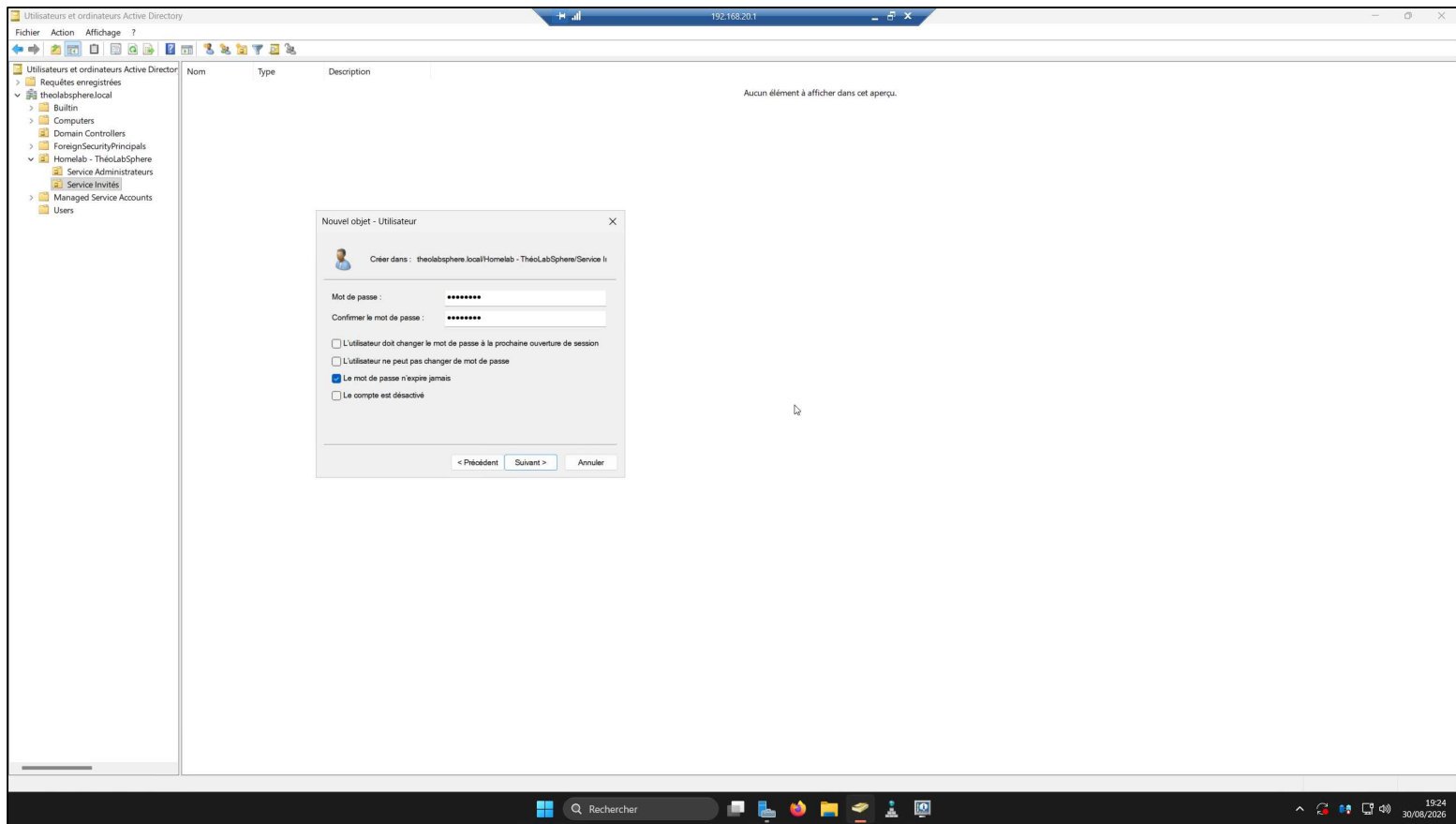


Création d'un compte Administration dans le service Administrateur :

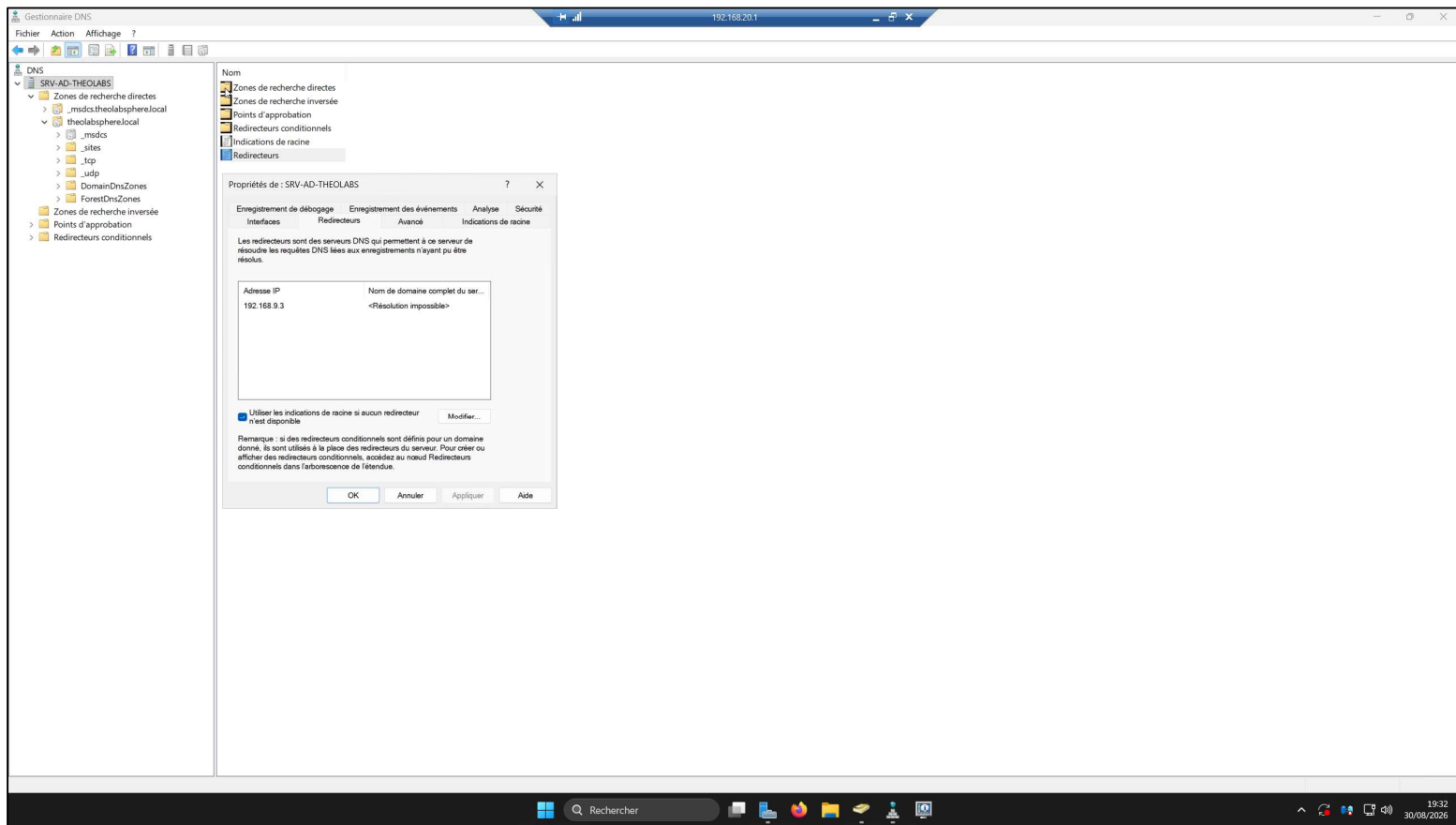


Création d'un compte Invité-Ext dans le service Administrateur :





Etape 7 : Configuration / Vérification résolution DNS :



Administrateur : Windows Po

PS C:\Users\Administrateur> Test-NetConnection 192.168.9.3 -Port 53

ComputerName : 192.168.9.3
RemoteAddress : 192.168.9.3
RemotePort : 53
InterfaceAlias : Ethernet
SourceAddress : 192.168.20.1
TcpTestSucceeded : True

PS C:\Users\Administrateur> Resolve-DnsName google.com -Server 192.168.9.3

Name	Type	TTL	Section	IPAddress
google.com	AAAA	162	Answer	2a00:1450:4007:811::200e
google.com	A	227	Answer	172.217.16.238

PS C:\Users\Administrateur> Resolve-DnsName google.com -Server 192.168.20.1

Name	Type	TTL	Section	IPAddress
google.com	AAAA	129	Answer	2a00:1450:4007:811::200e
google.com	A	194	Answer	172.217.16.238

PS C:\Users\Administrateur> |

Le serveur arrive à joindre le serveur DNS du Homelab et à résoudre le nom de google.com .

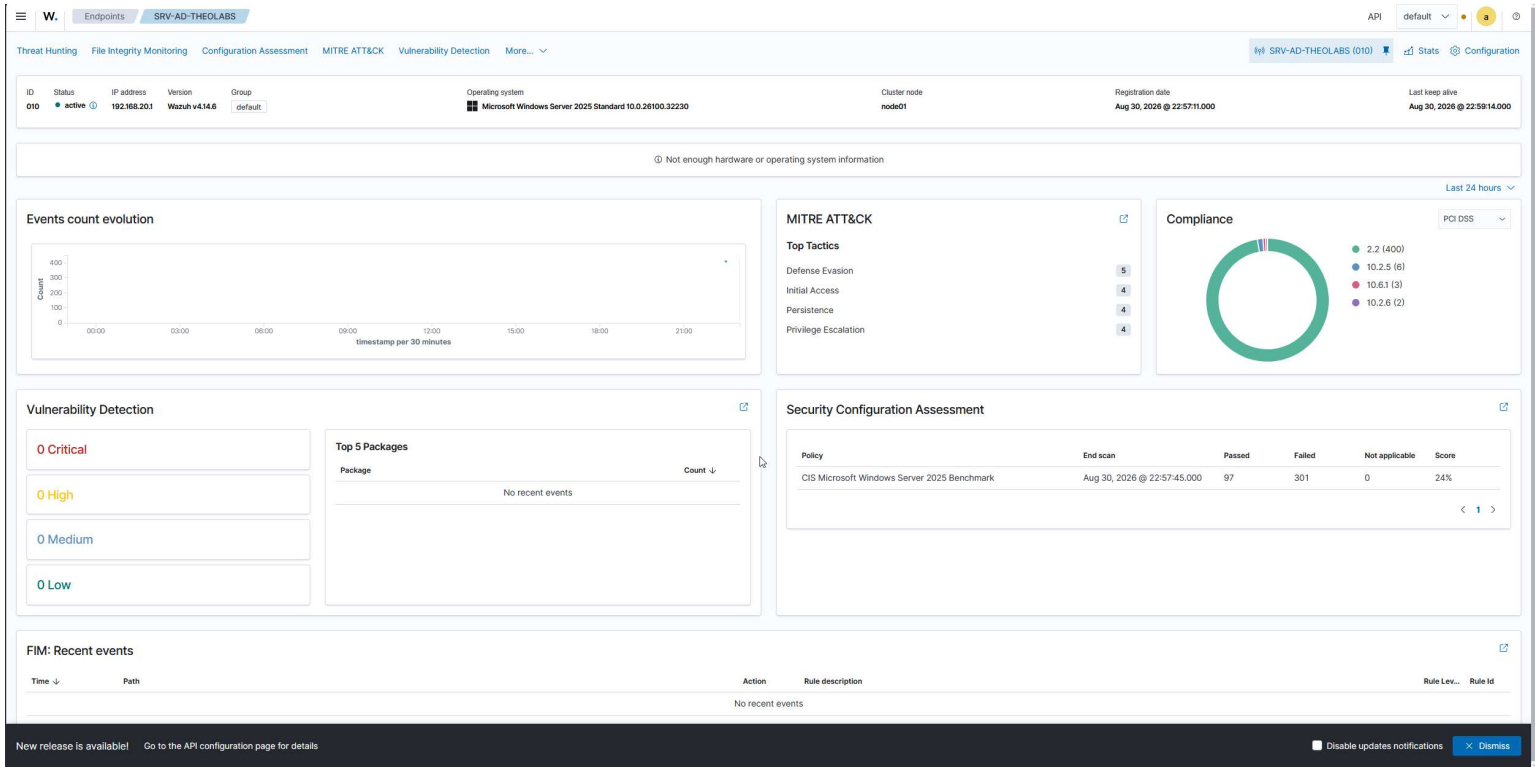
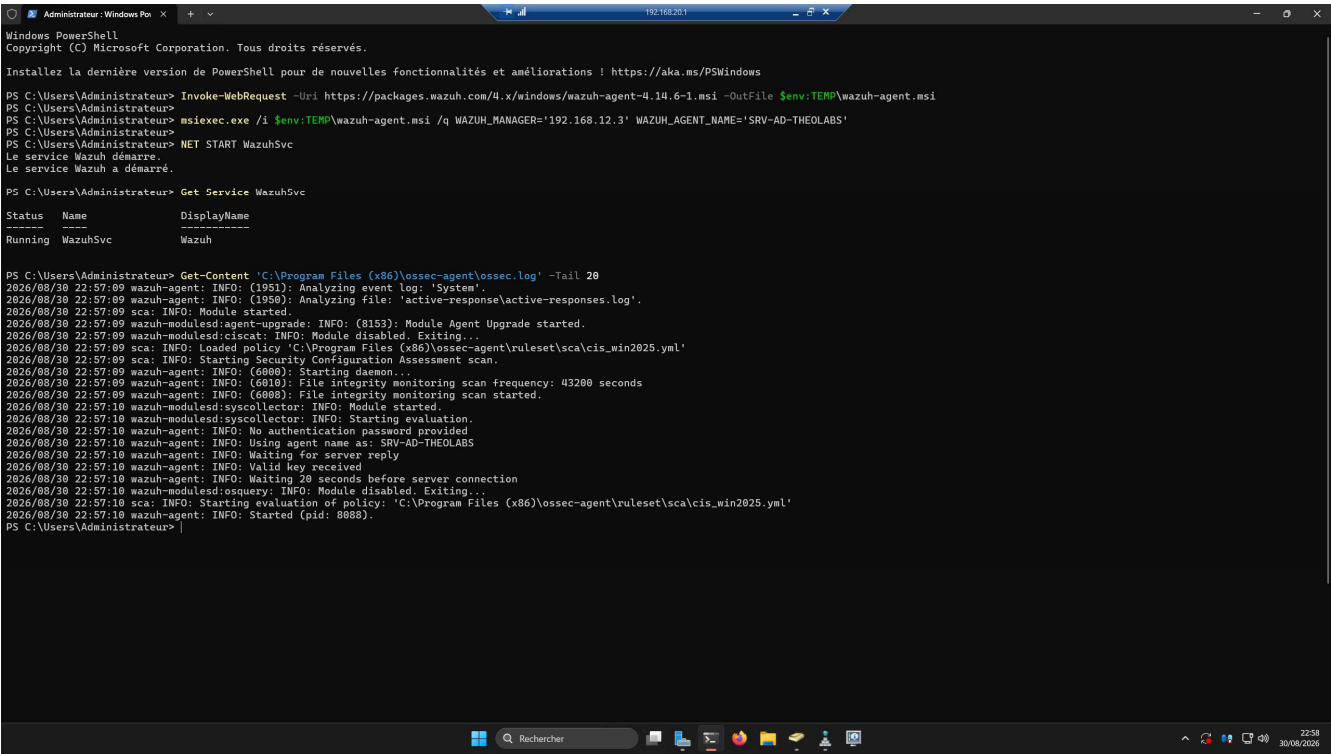


Etape 8 : Ajout du serveur AD dans Wazuh

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.14.6-1.msi -OutFile $env:TEMP\wazuh-agent.msi

msiexec.exe /i $env:TEMP\wazuh-agent.msi /q WAZUH_MANAGER='192.168.12.3' WAZUH_AGENT_NAME='SRV-AD-THEOLABS'

NET START WazuhSvc
```



Etape 9 : Ajout du serveur AD su ZABBIX

ZABBIX

ZABBIX-THEO

Tableaux de bord

Surveillance

Services

Inventaire

Rapports

Collecte de données

Alertes

Utilisateurs

Administration

Support

Intégrations

Aide

Paramètres utilisateur

Déconnexion

Hôtes

Hôte

IPMI

Tags

Macros

Inventaire

Chiffrement

Table de correspondance

Nom de l'hôte

SRV-AD

Nom visible

SRV-AD

Modèles

Windows by Zabbix agent

Supprimer lien

Supprimer lien et nettoyer

Groupes d'hôtes

SRV-THEO

Interfaces

Agent

192.168.20.1

Nom DNS

Connexion à

IP

DNS

Port

10050

Supprimer

Description

Surveillé par

Serveur

Proxy

Groupe de proxy

Activé

Actualiser

Clone

Supprimer

Annuler

192.168.11.37 Ubuntu

class: os

target: linux

Active

Dernières données 75

Problèmes

Graphiques

Tableaux de bord

Web

127.0.0.1 Zabbix server

class: os

class: software

target: linux

Activé

Dernières données 153

Problèmes

Graphiques

Tableaux de bord

Web

Affichage de 20 sur 20 trouvés

Zabbix 7.0.27 © 2001–2026 Zabbix SIA

ZABBIX

ZABBIX-THEO

Tableaux de bord

Surveillance

Services

Inventaire

Rapports

Collecte de données

Alertes

Utilisateurs

Administration

Support

Intégrations

Aide

Paramètres utilisateur

Déconnexion

Current problems

Temps

Info

Hôte

Problème • Sévérité

Durée

Actualiser

Actions

Tags

15:13:35

Ubuntu-Docker

Linux: FS [/]: Space is low (used > 80%, total 53.8GB)

7h 47m 16s

Actualiser

class: os

component: storage

filesystem: /

15:00

TC79

ICMP Ping: Unavailable by ICMP ping

22h 7m 46s

Actualiser

class: network

component: health

component: network

29/08/2026 23:19:10

PC-THEO

Windows: FS [C:]: Space is critically low (used > 90%, total 930.8GB)

23h 41m 41s

Actualiser

class: os

component: storage

filesystem: C:

29/08/2026 23:19:09

PC-

Windows: "GoogleUpdaterService152.0.7933.0" (Service de mise à jour Google

23h 41m 42s

Actualiser

class: os

component: system

Carte

HOMELAB - THEOLABSHERE

RESEAU LAN



PARTIE 2 : OPERATIONS SUR MICROSOFT AZURE

Étape 11 : Création du groupe de ressources

Création d'un groupe de ressources **gr-homelab-hybrid** qui regroupera l'ensemble des éléments du projet.

Groupe de ressources (gr-homelab-hybrid) : C'est un conteneur logique qui regroupe toutes le ressources Azure du projet — facilite la gestion, la facturation et la suppression en bloc.

Microsoft Azure

Accueil > Gestionnaire des ressources | Groupes de ressources

Rechercher dans les ressources, services et documents (Ctrl+J)

Copilot

theo.breton@cam.ac.uk
GEC DU HAYS DE VERNON (GEC)

Créer un groupe de ressources

Informations de base Balises Vérifier + créer

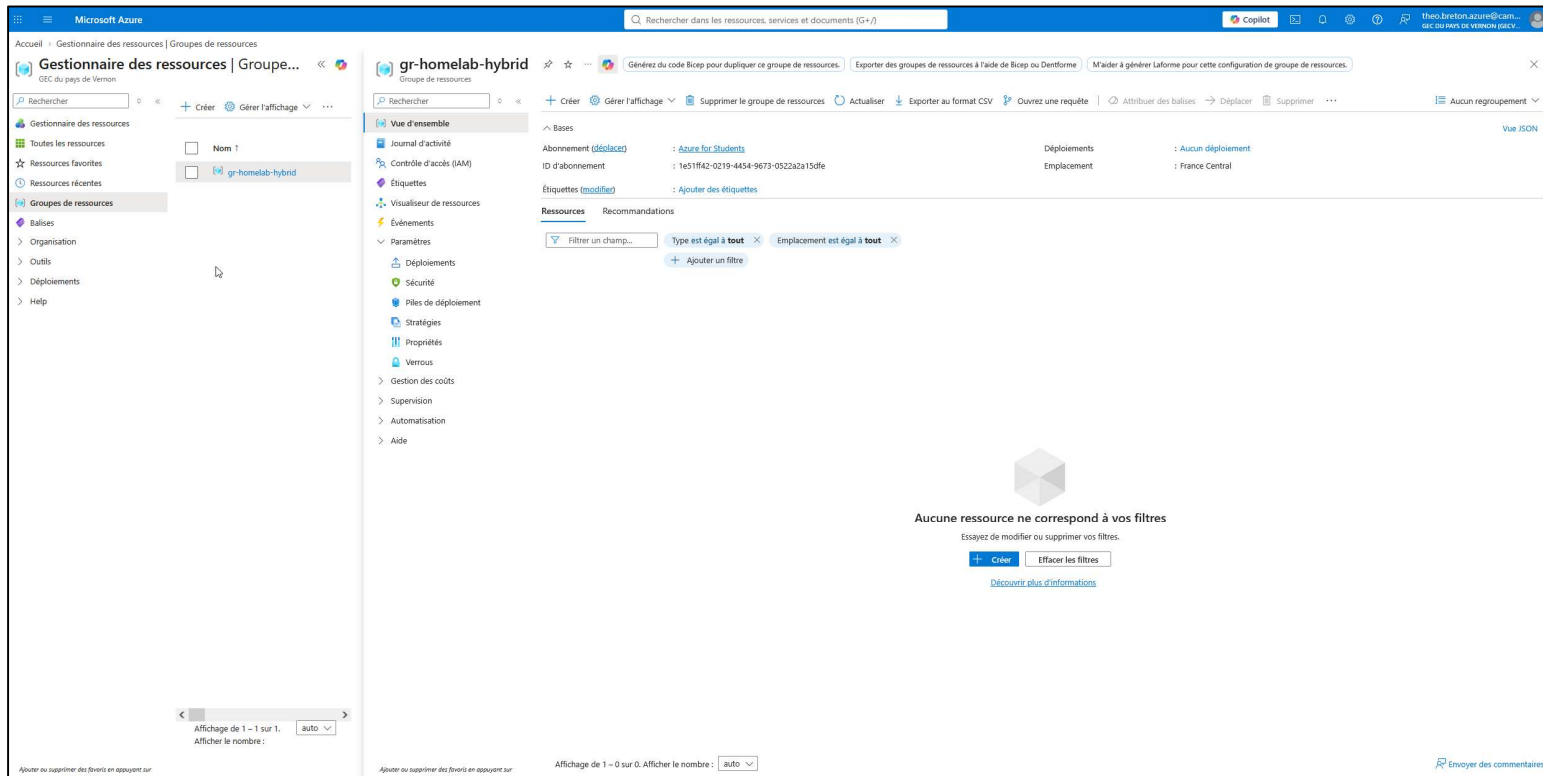
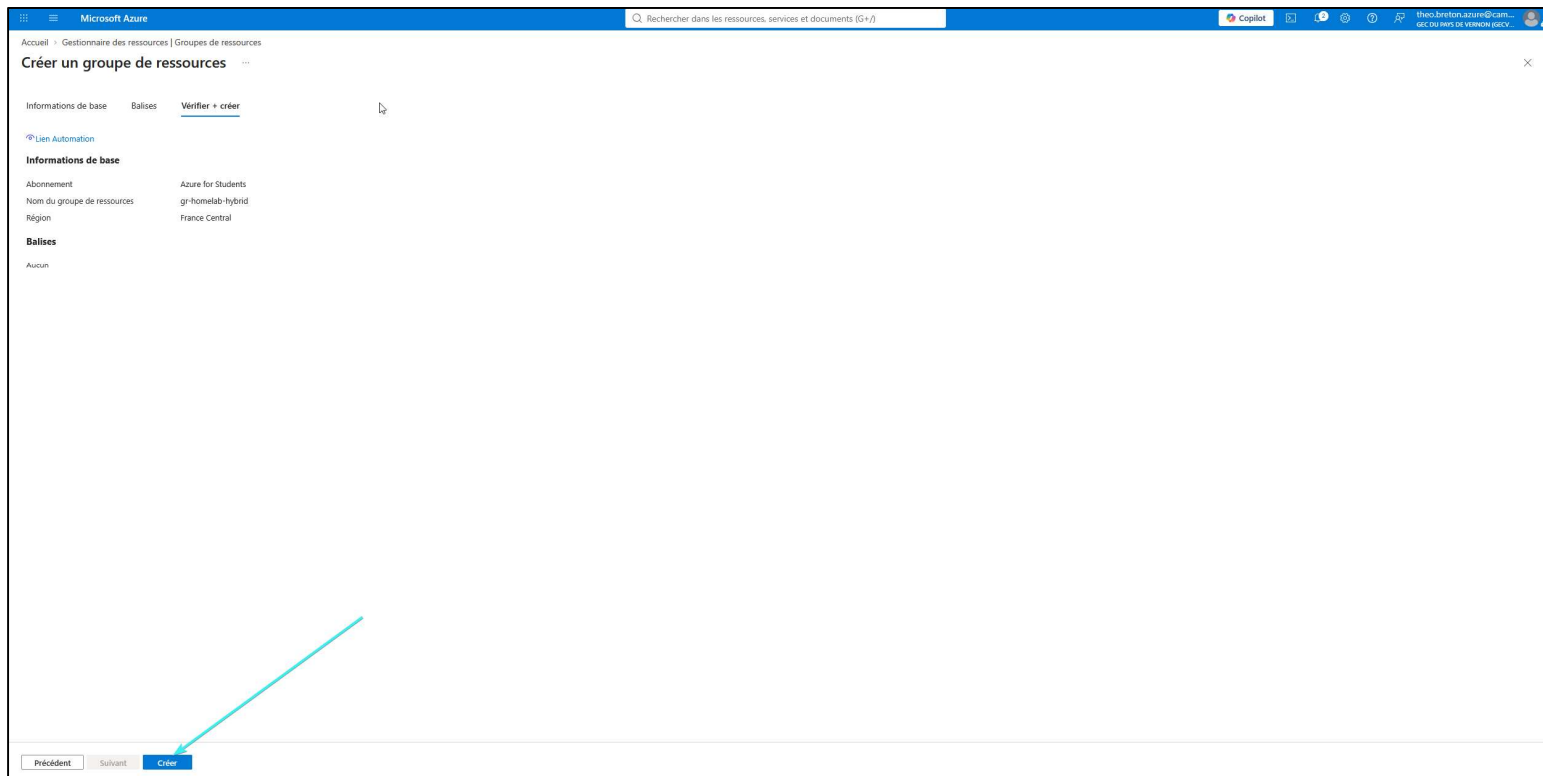
Groupe de ressources - Conteneur qui contient les ressources associées à une solution Azure. Le groupe de ressources peut inclure toutes les ressources de la solution, ou uniquement les ressources que vous voulez gérer en tant que groupe. Vous choisissez la façon dont vous voulez allouer des ressources aux groupes de ressources en fonction de ce qui est le plus adapté à votre organisation. [En savoir plus](#)

Abonnement *

Nom du groupe de ressources *

Région *

Précédent Suivant Vérifier + créer



Étape 12 : Création du réseau virtuel

Créer le VNet avec le plan d'adressage 10.100.0.0/24, distinct de celui de mon Homelab.

VNet (vnet-homelab-hybrid, 10.100.0.0/24) : Mon réseau privé virtuel dans Azure — l'équivalent de mon réseau physique au homelab mais côté cloud. Les VMs et services Azure communiquent à travers lui.

Microsoft Azure

Région : France Central

Région : France Central

Accueil > Base du réseau > Réseaux virtuels

Créer un réseau virtuel

Informations de baseSécuritéEspace d'adressageBalisesVérifier > créer

Réseau virtuel Azure (VNet) est le composant fondamental de votre réseau privé dans Azure. VNet permet à de nombreux types de ressources Azure, notamment des machines virtuelles Azure, de communiquer de manière sécurisée entre elles, avec Internet et sur les réseaux locaux. VNet est similaire à un réseau traditionnel que vous opérez dans votre propre centre de données, avec en plus les avantages de l'infrastructure Azure comme la mise à l'échelle, la disponibilité et l'isolation.

[En savoir plus...](#)

Détails du projet

Sélectionnez l'abonnement pour gérer les ressources déployées et les coûts. Utilisez des groupes de ressources comme des dossiers pour organiser et gérer toutes vos ressources.

Abonnement *

Azure for Students

Groupe de ressources *

gr-homelab-hybrid

Créer nouveau

Détails de l'instance

Nom du réseau virtuel *

vnet-homelab-hybrid

Région *

(Europe) France Central

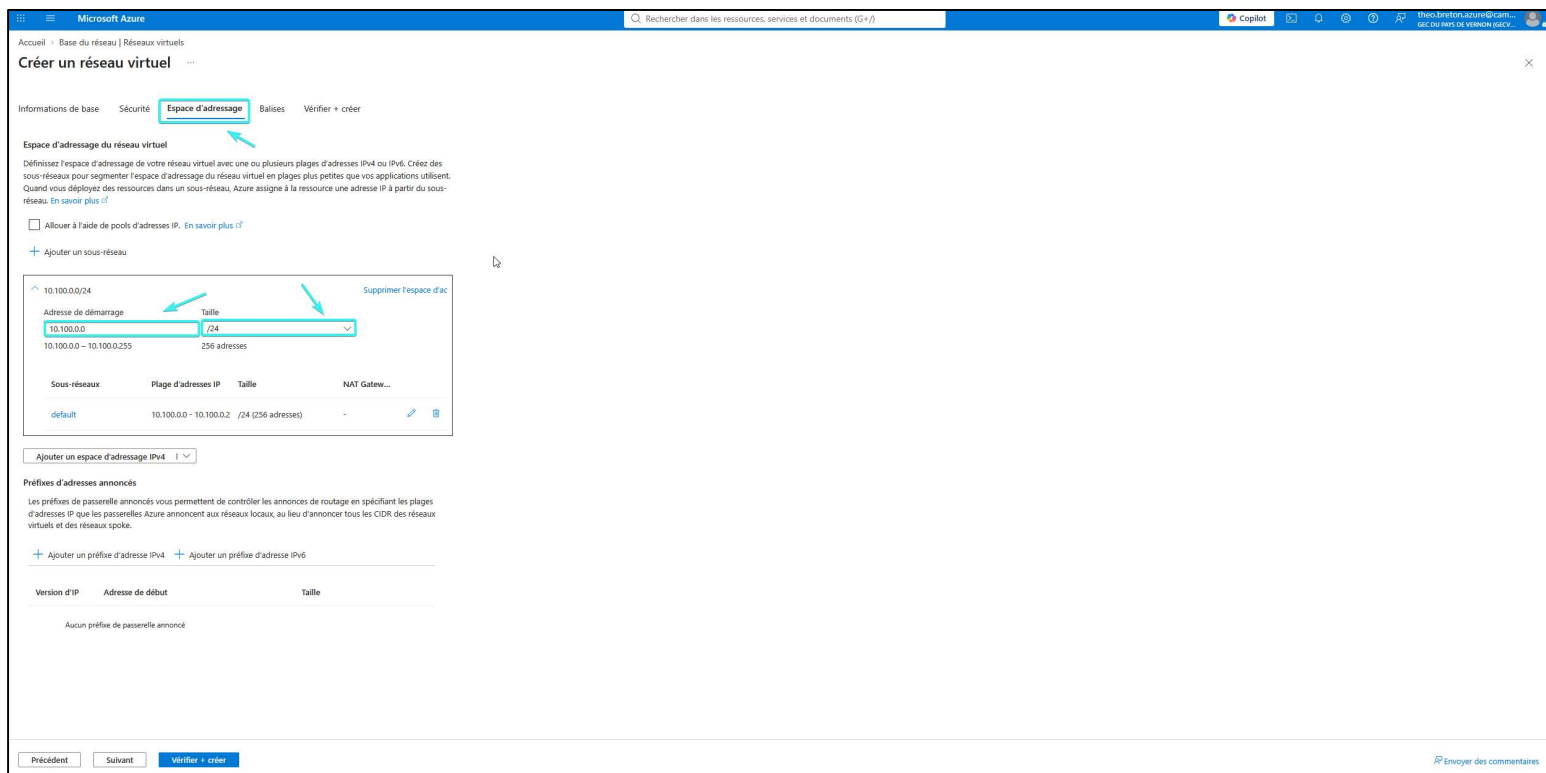
[Déployer sur une zone étendue Azure](#)

Précédent

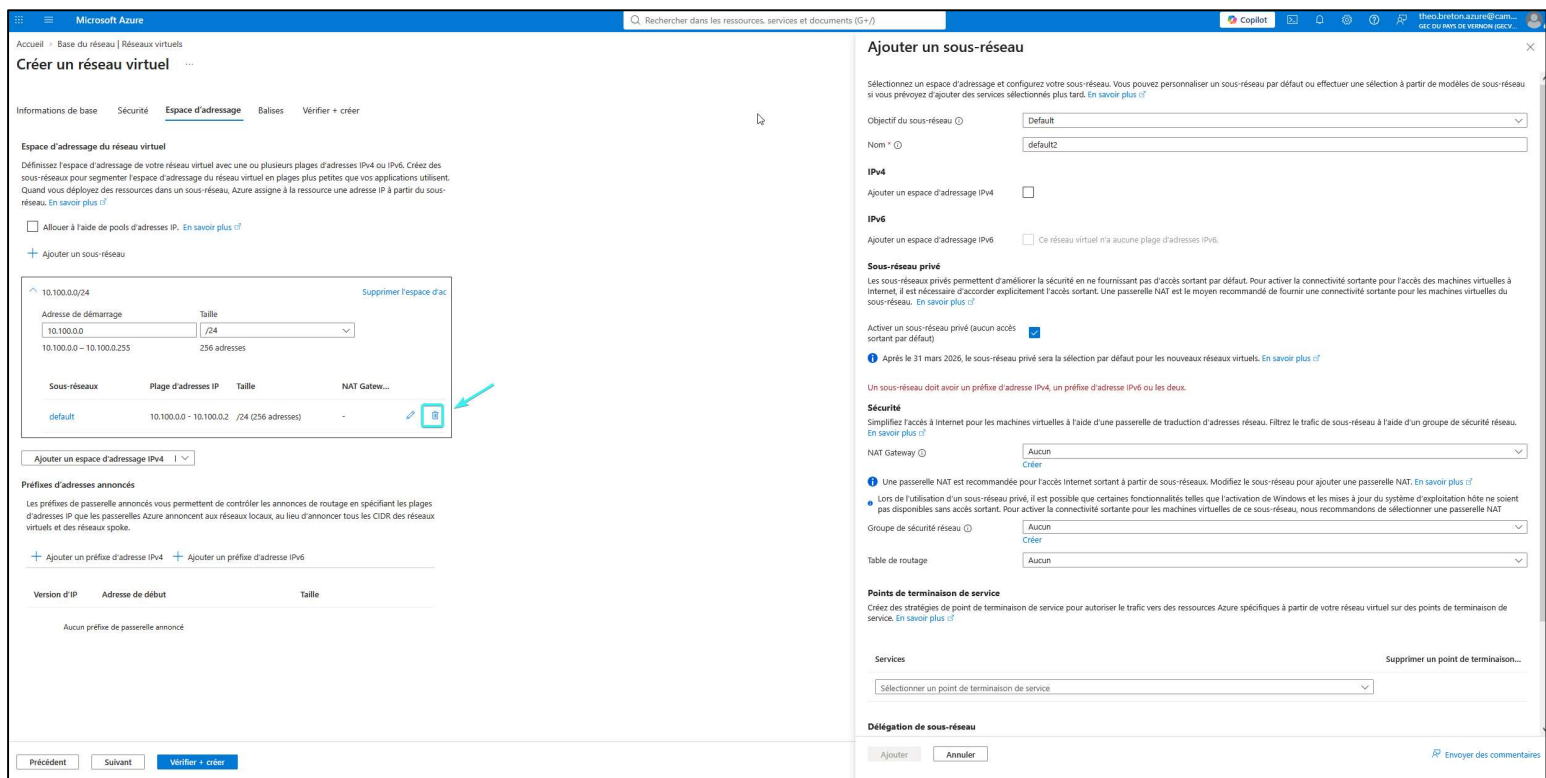
Suivant

Vérifier > créer

Envoyer des commentaires



Suppression du sous réseau créer par défaut.



Étape 13 : Création des sous-réseaux

Créer GatewaySubnet en 10.100.0.0/27 et Subnet-App en 10.100.0.32/27.

GatewaySubnet (10.100.0.0/27) : sous-réseau réservé exclusivement à la passerelle VPN Azure. C'est obligatoire et le nom ne peut pas être changé — Azure y déploie les instances qui gèrent le tunnel IPsec vers mon FortiGate.

Subnet-App (10.100.0.32/27) : sous-réseau pour tes machines virtuelles et ressources applicatives (ma future VM Windows Server qui rejoindra le domaine AD). C'est l'équivalent de mes VLANs côté homelab.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton@com...
SEC DU INFOS DE MONTON (GRCV)

Accueil > Base du réseau | Réseaux virtuels

Créer un réseau virtuel

Informations de baseSécuritéEspace d'adressageBalisesVérifier + créer

Espace d'adressage du réseau virtuel

Définissez l'espace d'adressage de votre réseau virtuel avec une ou plusieurs plages d'adresses IPv4 ou IPv6. Créez des sous-réseaux pour segmenter l'espace d'adressage du réseau virtuel en plages plus petites que vos applications utilisent. Quand vous déployez des ressources dans un sous-réseau, Azure assigne à la ressource une adresse IP à partir du sous-réseau. [En savoir plus](#)

☐ Allouer à l'aide de pools d'adresses IP. [En savoir plus](#)

+ Ajouter un sous-réseau

10.100.0.0/24

Supprimer l'espace d'ac

Adresse de démarrage

Taille

10.100.0.0

/24

10.100.0.0 – 10.100.0.255

256 adresses

Sous-réseau

Plage d'adresses IP

Taille

NAT Gatew...

Ajouter un espace d'adressage IPv4

Préfixes d'adresses annoncés

Les préfixes de passerelle annoncés vous permettent de contrôler les annonces de routage en spécifiant les plages d'adresses IP que les passerelles Azure annoncent aux réseaux locaux, au lieu d'annoncer tous les CIDR des réseaux virtuels et des réseaux spoke.

+ Ajouter une préfixe d'adresse IPv4

+ Ajouter une préfixe d'adresse IPv6

Version d'IP

Adresse de début

Taille

Aucun préfixe de passerelle annoncé

Précédent

Suivant

Vérifier + créer

Ajouter un sous-réseau

Sélectionnez un espace d'adressage et configurez votre sous-réseau. Vous pouvez personnaliser un sous-réseau par défaut ou effectuer une sélection à partir de modèles de sous-réseau si vous prévoyez d'ajouter des services sélectionnés plus tard. [En savoir plus](#)

Objectif du sous-réseau

Virtual Network Gateway

Nom

GatewaySubnet

IPv4

Ajouter un espace d'adressage IPv4

Plage d'adresses IPv4

10.100.0.0/24

10.100.0.0 – 10.100.0.255

Adresse de début

10.100.0.0

Taille

/27 (32 adresses)

Plage d'adresses de sous-réseau

10.100.0.0 – 10.100.0.31

IPv6

Ajouter un espace d'adressage IPv6

☐ Ce réseau virtuel n'a aucune plage d'adresses IPv6.

Sous-réseau privé

Les sous-réseaux privés permettent d'améliorer la sécurité en ne fournissant pas d'accès sortant par défaut. Pour activer la connectivité sortante pour l'accès des machines virtuelles à Internet, il est nécessaire d'accorder explicitement l'accès sortant. Une passerelle NAT est le moyen recommandé de fournir une connectivité sortante pour les machines virtuelles du sous-réseau. [En savoir plus](#)

Activer un sous-réseau privé (aucun accès sortant par défaut)

☒

Après le 31 mars 2026, le sous-réseau privé sera la sélection par défaut pour les nouveaux réseaux virtuels. [En savoir plus](#)

Sécurité

Simplifiez l'accès à Internet pour les machines virtuelles à l'aide d'une passerelle de traduction d'adresses réseau. Filtrage du trafic de sous-réseau à l'aide d'un groupe de sécurité réseau. [En savoir plus](#)

NAT Gateway

Aucun

Créer

Une passerelle NAT est recommandée pour l'accès Internet sortant à partir de sous-réseaux. Modifiez le sous-réseau pour ajouter une passerelle NAT. [En savoir plus](#)

Lors de l'utilisation d'un sous-réseau privé, il est possible que certaines fonctionnalités telles que l'activation de Windows et les mises à jour du système d'exploitation hôte ne soient pas disponibles sans accès sortant. Pour activer la connectivité sortante pour les machines virtuelles de ce sous-réseau, nous recommandons de sélectionner une passerelle NAT

Groupe de sécurité réseau

Aucun

Créer

Table de routage

Aucun

Points de terminaison de service

Créez des stratégies de point de terminaison de service pour autoriser le trafic vers des ressources Azure spécifiques à partir de votre réseau virtuel sur des points de terminaison de service. [En savoir plus](#)

Ajouter

Annuler

Envoyer des commentaires

PROJET PERSONNEL – Théo BRETON

PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

28

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cent...
GEC DU PAYS DE VERNON (GECV...)

Accueil > Base du réseau > Réseaux virtuels

Créer un réseau virtuel

Informations de baseSécuritéEspace d'adressageBalisesVérifier + créer

Espace d'adressage du réseau virtuel

Définissez l'espace d'adressage de votre réseau virtuel avec une ou plusieurs plages d'adresses IPv4 ou IPv6. Créez des sous-réseaux pour segmenter l'espace d'adressage du réseau virtuel en plages plus petites que vos applications utilisent. Quand vous déployez des ressources dans un sous-réseau, Azure assigne à la ressource une adresse IP à partir du sous-réseau. En savoir plus

Alouer à l'aide de pools d'adresses IP. En savoir plus

+ Ajouter un sous-réseau

10.100.0.0/24

Supprimer l'espace d'ad...

Adresse de démarrage10.100.0.0Taille/24256 adresses

10.100.0.0 – 10.100.0.255

Sous-réseauxPlage d'adresses IPTailleNAT Gatew...

GatewaySubnet10.100.0.0 – 10.100.0.3 /27 (32 adresses)

Ajouter un espace d'adressage IPv4

Préfixes d'adresses annoncés

Les préfixes de passerelle annoncés vous permettent de contrôler les annonces de routage en spécifiant les plages d'adresses IP que les passerelles Azure annoncent aux réseaux locaux, au lieu d'annoncer tous les CIDR des réseaux virtuels et des réseaux spoke.

+ Ajouter un préfixe d'adresse IPv4

+ Ajouter un préfixe d'adresse IPv6

Version d'IP

Adresse de début

Taille

Aucun préfixe de passerelle annoncé

Précédent

Suivant

Vérifier + créer

Ajouter un sous-réseau

Sélectionnez un espace d'adressage et configurez votre sous-réseau. Vous pouvez personnaliser un sous-réseau par défaut ou effectuer une sélection à partir de modèles de sous-réseau à vous prévoyez d'ajouter des services sélectionnés plus tard. En savoir plus

Objectif du sous-réseau

1

Default

Nom

2

Subnet-App

IPv4

Ajouter un espace d'adressage IPv4

Plage d'adresses IPv4

3

10.100.0.0/24

10.100.0.0 – 10.100.0.255

Adresse de début

4

10.100.0.32

Taille

5

/27 (32 adresses)

Plage d'adresses de sous-réseau

10.100.0.32 – 10.100.0.63

IPv6

Ajouter un espace d'adressage IPv6

Ce réseau virtuel n'a aucune plage d'adresses IPv6.

Sous-réseau privé

Les sous-réseaux privés permettent d'améliorer la sécurité en ne fournissant pas d'accès sortant par défaut. Pour activer la connectivité sortante pour l'accès des machines virtuelles à Internet, il est nécessaire d'accorder explicitement l'accès sortant. Une passerelle NAT est le moyen recommandé de fournir une connectivité sortante pour les machines virtuelles du sous-réseau. En savoir plus

Activer un sous-réseau privé (aucun accès sortant par défaut)

Après le 31 mars 2026, le sous-réseau privé sera la sélection par défaut pour les nouveaux réseaux virtuels. En savoir plus

Sécurité

Simplifiez l'accès à Internet pour les machines virtuelles à l'aide d'une passerelle de traduction d'adresses réseau. Filtrez le trafic de sous-réseau à l'aide d'un groupe de sécurité réseau. En savoir plus

NAT Gateway

Aucun

Créer

Une passerelle NAT est recommandée pour l'accès Internet sortant à partir de sous-réseaux. Modifiez le sous-réseau pour ajouter une passerelle NAT. En savoir plus

Lors de l'utilisation d'un sous-réseau privé, il est possible que certaines fonctionnalités telles que l'activation de Windows et les mises à jour du système d'exploitation hôte ne soient pas disponibles sans accès sortant. Pour activer la connectivité sortante pour les machines virtuelles de ce sous-réseau, nous recommandons de sélectionner une passerelle NAT

Groupe de sécurité réseau

Aucun

Créer

Table de routage

Aucun

Points de terminaison de service

Créez des stratégies de point de terminaison de service pour autoriser le trafic vers des ressources Azure spécifiques à partir de votre réseau virtuel sur des points de terminaison de service. En savoir plus

6

Ajouter

Annuler

Envoyer des commentaires

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cent...
GEC DU PAYS DE VERNON (GECV...)

Accueil > Base du réseau > Réseaux virtuels

Créer un réseau virtuel

Informations de baseSécuritéEspace d'adressageBalisesVérifier + créer

Validation réussie

Voir le modèle d'automatisation

Informations de base

AbonnementAzure for Students

Groupe de ressourcesgr-homelab-hybrid

Nomvnet-homelab-hybrid

RégionFrance Central

Sécurité

Azure BastionDésactivé

Pare-feu AzureDésactivé

Protection réseau Azure DDoSDésactivé

Espace d'adressage

Espace d'adressage10.100.0.0/24 (256 adresses)

Sous-réseauGatewaySubnet (10.100.0.0/27) (32 adresses)

Sous-réseau privéActivé

Sous-réseauSubnet-App (10.100.0.32/27) (32 adresses)

Sous-réseau privéActivé

Balises

Précédent

Suivant

Créer

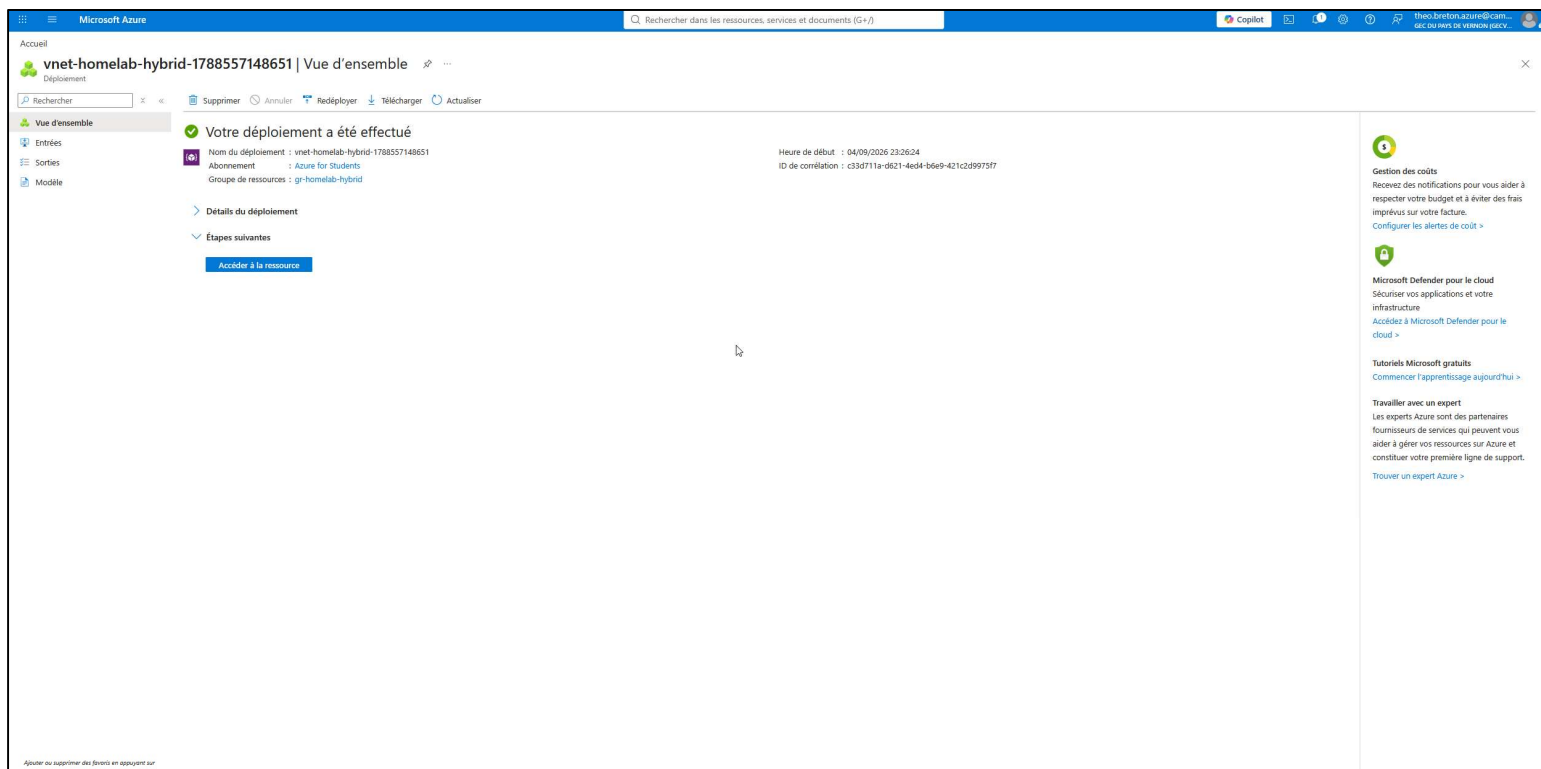
Télécharger un modèle pour automatisation

Envoyer des commentaires

PROJET PERSONNEL – Théo BRETON

PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

29



Étape 14 : Création de l'adresse IP publique

Création d'une adresse IP publique statique, SKU Standard, destinée à la passerelle VPN.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Accueil > Base du réseau > Adresses IP publiques

Créer une adresse IP publique

Informations de base Protection DDoS Balises Vérifiez + créez

Créez une adresse IP publique. Associez-la à une machine virtuelle ou à d'autres ressources Azure. Les ressources Internet communiquent avec les ressources Azure par le biais d'une adresse IP publique. Découvrez plus d'informations.

Détails du projet

Sélectionnez l'abonnement pour gérer les ressources déployées et les coûts. Utilisez des groupes de ressources comme des dossiers pour organiser et gérer toutes vos ressources.

Abonnement * Azure for Students

Groupe de ressources * gr-homelab-hybrid

Détails de l'instance

Région * (Europe) France Central

Détails de la configuration

Nom * publique-ip-vpn-gw-homelab

Version d'IP * IPv4

Référence SKU * Standard

Zone de disponibilité * Zone-redondant

Niveau * Regional

Précédent Suivant Vérifier + créer

Envoyer des commentaires

Cette IP sera l'adresse publique de ta passerelle VPN Azure — c'est elle que tu configureras côté FortiGate comme "remote gateway".

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/J)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VENNON (J&CV...)

Accueil > Base du réseau | Adresses IP publiques

Créer une adresse IP publique

Validation réussie

Informations de baseProtection DDoSBalisesVérifiez + créez

Informations de base

Abonnement

Groupe de ressources

Région

Nom

Version d'IP

Référence SKU

Niveau

Zone de disponibilité

Attribution d'adresse IP

Préférence de routage

Délai d'inactivité (minutes)

Étiquette du nom DNS

Étendue de l'étiquette du nom de domaine (préversion)

Azure for Students

gr-homelab-hybrid

francecentral

publique-ip-vpn-gw-homelab

IPv4

Standard

Regional

Zone-redundant

Static

MicrosoftNetwork

4

-

Protection DDoS

Type de protection

Réseau

Balises

Précédent

Suivant

Créer

Télécharger un modèle pour automation

Envoyer des commentaires

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/J)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VENNON (J&CV...)

Accueil

PublicIPAddress-ARM | Vue d'ensemble

Déploiement

Rechercher

SupprimerAnnulerRedéploierTéléchargerActualiser

Vue d'ensemble

Entrées

Sorties

Modèle

Votre déploiement a été effectué

Nom du déploiement : PublicIPAddress-ARM

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 04/09/2026 23:36:43

ID de corrélation : 25060648-90b2-437e-855f-ee948b9654f7

Détails du déploiement

Ressource	Type	Statut	Détails de l'opération
publique-ip-vpn-gw-homelab	Adresse IP publique	OK	Détails de l'opération

Étapes suivantes

Accéder à la ressource

Gestion des coûts

Recevez des notifications pour vous aider à respecter votre budget et à éviter des frais imprévus sur votre facture.

Configurer les alertes de coût >

Microsoft Defender pour le cloud

Securiser vos applications et votre infrastructure

Accédez à Microsoft Defender pour le cloud >

Tutoriels Microsoft gratuits

Commencer l'apprentissage aujourd'hui >

Travailler avec un expert

Les experts Azure sont des partenaires fournisseurs de services qui peuvent vous aider à gérer vos ressources sur Azure et constituer votre première ligne de support.

Trouver un expert Azure >

Ajouter ou supprimer des favoris en appuyant sur CTRL+SHIFT+F



Microsoft Azure

Accueil > PublicIPAddress-ARM | Vue d'ensemble

publique-ip-vpn-gw-homelab
Adresse IP publique

Rechercher

Associer Dissocier Supprimer Déplacer Actualiser Ouvrir sur un appareil mobile Envoyer des commentaires

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Visualiseur de ressources

Paramètres

Supervision

Automatisation

Aide

Essentials

Groupe de ressources (déplacer) : gr-homelab-hybrid

Emplacement (déplacer) : France Central

Abonnement (déplacer) : Azure for Students

ID d'abonnement : 1e51f842-0219-4454-9673-0522a2a15dfe

Référence SKU : Standard

Niveau : Regional

Adresse IP : 51.11.238.14

Nom DNS : -

Associé à : -

Machine virtuelle : -

Balises (modifier) : Ajouter des balises

Afficher plus

Démarrer Propriétés Didacticiels

Utiliser des adresses IP publiques pour les connexions publiques à des ressources Azure

Associer et configurer des adresses IP publiques à différentes ressources Azure [Découvrez plus d'informations](#)

Associer à une ressource
Associez votre adresse IP publique à une ressource Azure telle qu'un Azure Load Balancer ou une interface réseau.
[Associer des IP](#)

Configurer une adresse IP publique
Configurez une durée d'inactivité DNS, un nom et un enregistrement d'alias pour votre adresse IP publique.
[Configurer](#)

Protéger une adresse IP
Choisissez le niveau de protection DDoS approprié pour votre adresse IP.
[Protéger](#)

Ajouter ou supprimer des favoris en appuyant sur **Ctrl+Shift+F**

Étape 15 : Déploiement de la passerelle VPN

Déployer la Virtual Network Gateway : type VPN, SKU VpnGw1, mode route-based. Compter 30 à 45 minutes de déploiement.

Se rendre dans : portal.azure.com/#create/Microsoft.VirtualNetworkGateway

Microsoft Azure

Accueil

Créer une passerelle de réseau virtuel

De base Étiquettes Vérifier + créer

Azure a fourni un guide de planification et de conception pour vous aider à configurer les différentes options de passerelle VPN. [En savoir plus](#)

Détails du projet
Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * : Azure for Students

Groupe de ressources : gr-homelab-hybrid (dérivé du groupe de ressources du réseau virtuel)

Détails de l'instance

Nom * : vpn-gw-homelab

Région * : France Central
Déployer sur une zone étendue Azure

Configuration de la passerelle

Type de passerelle * : ☒ VPN ☐ ExpressRoute

RÉFÉRENCE (SKU) * : VpnGw1AZ

Activation la connectivité avancée : ☐ Activé ☒ Désactivé

Réseau virtuel * : vnet-homelab-hybrid
Créer un réseau virtuel

Sous-réseau : GatewaySubnet (10.100.0.0/27)

Seuls les réseaux virtuels dans l'abonnement et la région sélectionnés sont listés.

Adresse IP publique

Adresse IP publique * : ☐ Créer ☒ Utiliser l'existante

[Vérifier + créer](#) [Précédent](#) [Suivant : Étiquettes >](#) [Télécharger un modèle pour automation](#)

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

theo.breton.azure@cam...
DEC DU PAYS DE VERNON (GECV...

Accueil

Créer une passerelle de réseau virtuel

Détails de l'instance

Nom *vpn-gw-homelab

Région *France Central
Déployer sur une zone étendue Azure

Configuration de la passerelle

Type de passerelle *VPN

RÉFÉRENCE (SKU) *VpnGw1AZ

Activation la connectivité avancée *Désactivé

Réseau virtuel *vnet-homelab-hybrid
Créer un réseau virtuel

Sous-réseau *GatewaySubnet (10.100.0.0/27)

Seuls les réseaux virtuels dans l'abonnement et la région sélectionnés sont listés.

Adresse IP publique

Adresse IP publique *Utiliser l'existante

Choisir une adresse IP publique *publique-ip-vpn-gw-homelab (51.11.238.14)

Activer le mode actif/passif *Désactivé

Configurer BGP *Désactivé

Informations d'authentification

Autoriser l'accès Key Vault *Désactivé

Azure recommande d'utiliser un appareil VPN validé avec votre passerelle de réseau virtuel. Pour voir la liste des appareils validés et les instructions de configuration, consultez l'article documentation d'Azure concernant les appareils VPN validés.

Vérifier + créer

Précédent

Suivant : Étiquettes >

Télécharger un modèle pour automation

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

theo.breton.azure@cam...
DEC DU PAYS DE VERNON (GECV...

Accueil

Créer une passerelle de réseau virtuel

Validation réussie

De baseÉtiquettesVérifier + créer

De base

Abonnement	Azure for Students
Groupe de ressources	gr-homelab-hybrid
Nom	vpn-gw-homelab
Région	France Central
RÉFÉRENCE (SKU)	VpnGw1AZ
Réseau virtuel	vnet-homelab-hybrid
Sous-réseau	GatewaySubnet (10.100.0.0/27)
Type de passerelle	Vpn
Type de VPN	RouteBased
Activer le mode actif/passif	Désactivé
Activation la connectivité avancée	Désactivé
Configurer BGP	Désactivé
Adresse IP publique	publique-ip-vpn-gw-homelab

Étiquettes

Aucun

Créer

Précédent

Suivant

Télécharger un modèle pour automation



Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...)

Accueil

Microsoft.VirtualNetworkGateway-20260904235626 | Vue d'ensemble

Deploiement

Rechercher

Supprimer Annuler Redeployer Télécharger Actualiser

Vue d'ensemble

Entrées

Sorties

Modèle

Le déploiement est en cours

Nom du déploiement : Microsoft.VirtualNetworkGateway-20260904235626

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 04/09/2026 23:59:31

ID de corrélation : af25244c-8b1f-41df-b493-d1db8c062907

Détails du déploiement

Ressource	Type	Statut	Détails de l'opération
Il n'y a aucune source à afficher.			

Envoyer des commentaires

Partagez votre expérience avec le déploiement

Microsoft Defender pour le cloud

Sécuriser vos applications et votre infrastructure

Accédez à Microsoft Defender pour le cloud >

Tutoriels Microsoft gratuits

Commencer l'apprentissage aujourd'hui >

Travailler avec un expert

Les experts Azure sont des partenaires fournisseurs de services qui peuvent vous aider à gérer vos ressources sur Azure et constituer votre première ligne de support.

Trouver un expert Azure >

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...)

Accueil

Microsoft.VirtualNetworkGateway-20260904235626 | Vue d'ensemble

Deploiement

Rechercher

Supprimer Annuler Redeployer Télécharger Actualiser

Vue d'ensemble

Entrées

Sorties

Modèle

✓ Votre déploiement a été effectué

Nom du déploiement : Microsoft.VirtualNetworkGateway-20260904235626

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 04/09/2026 23:59:32

ID de corrélation : af25244c-8b1f-41df-b493-d1db8c062907

Détails du déploiement

Étapes suivantes

Accéder à la ressource

Envoyer des commentaires

Partagez votre expérience avec le déploiement

Gestion des coûts

Recevez des notifications pour vous aider à respecter votre budget et à éviter des frais imprévus sur votre facture.

Configurer les alertes de coût >

Microsoft Defender pour le cloud

Sécuriser vos applications et votre infrastructure

Accédez à Microsoft Defender pour le cloud >

Tutoriels Microsoft gratuits

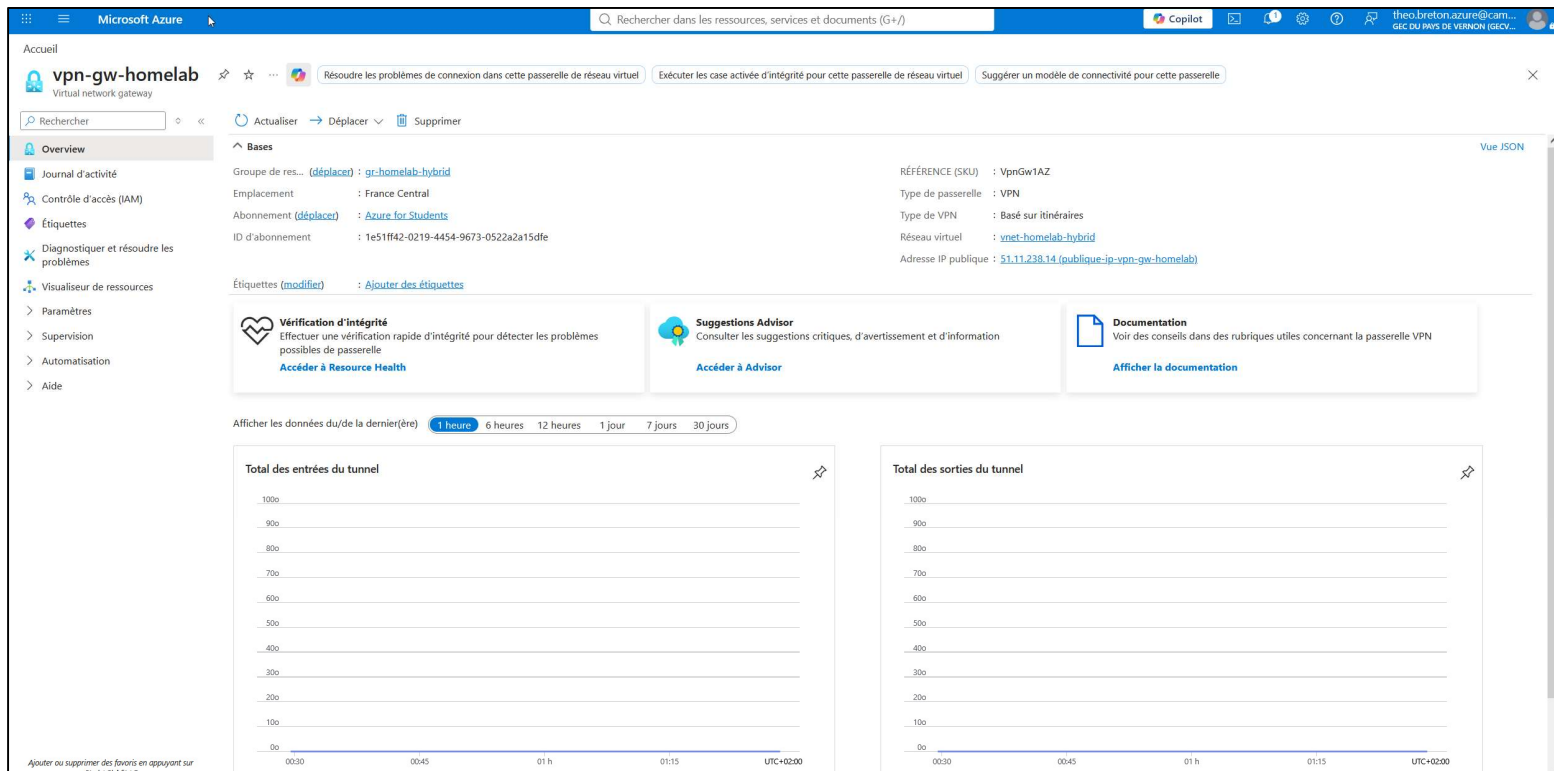
Commencer l'apprentissage aujourd'hui >

Travailler avec un expert

Les experts Azure sont des partenaires fournisseurs de services qui peuvent vous aider à gérer vos ressources sur Azure et constituer votre première ligne de support.

Trouver un expert Azure >





Étape 16 : Création de la Local Network Gateway

Déclarer le FortiGate côté Azure : IP publique de la Freebox et plage 192.168.20.0/24.

The screenshot shows the 'Créer une passerelle de réseau local' (Create a local network gateway) wizard in the Azure portal. The wizard is in the 'De base' (Basic) step, and the user is configuring the gateway details. The configuration includes selecting the subscription, resource group, region, name, and IP address. The IP address is set to 192.168.20.0/24. The wizard also shows a 'Vérifier + créer' button at the bottom. The configuration details are as follows:

- Abonnement: Azure for Students
- Groupe de ressources: gr-homelab-hybrid
- Région: France Central
- Nom: lgw-fortigate-homelab
- Point de terminaison: Adresse IP (FQDN)
- Adresse IP: 88
- Espaces d'adressage: 192.168.20.0/24

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

theo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...

Accueil > Hybrid connectivity | Local network gateways

Créer une passerelle de réseau local

Validation réussie

De base Avancé Vérifier + créer

Récapitulatif

Nom
Abonnement
Groupe de ressources
Région
Point de terminaison
Adresse IP
Espaces d'adressage

lgw-fortigate-homelab
Azure for Students
gr-homelab-hybrid
France Central
Adresse IP
88. ...
192.168.20.0/24

Créer Précédent Suivant

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

theo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...

Accueil > LocalNetworkGatewayCreate-20260905012454 | Vue d'ensemble

lgw-fortigate-homelab

Local network gateway

Y a-t-il des pannes qui impactent cette ressource

Diagnostiquer les problèmes liés à cette ressource

Interroger les dépendances pour cette ressource

Rechercher

Déplacer Supprimer

Overview

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Visualiseur de ressources

Paramètres

Automatisation

Aide

Bases

Groupe de res... (déplacer) : g Copier dans le Presse-papiers

Adresse IP : 88. ...

Espaces d'adressage : 192.168.20.0/24

Emplacement : France Central

Abonnement (déplacer) : Azure for Students

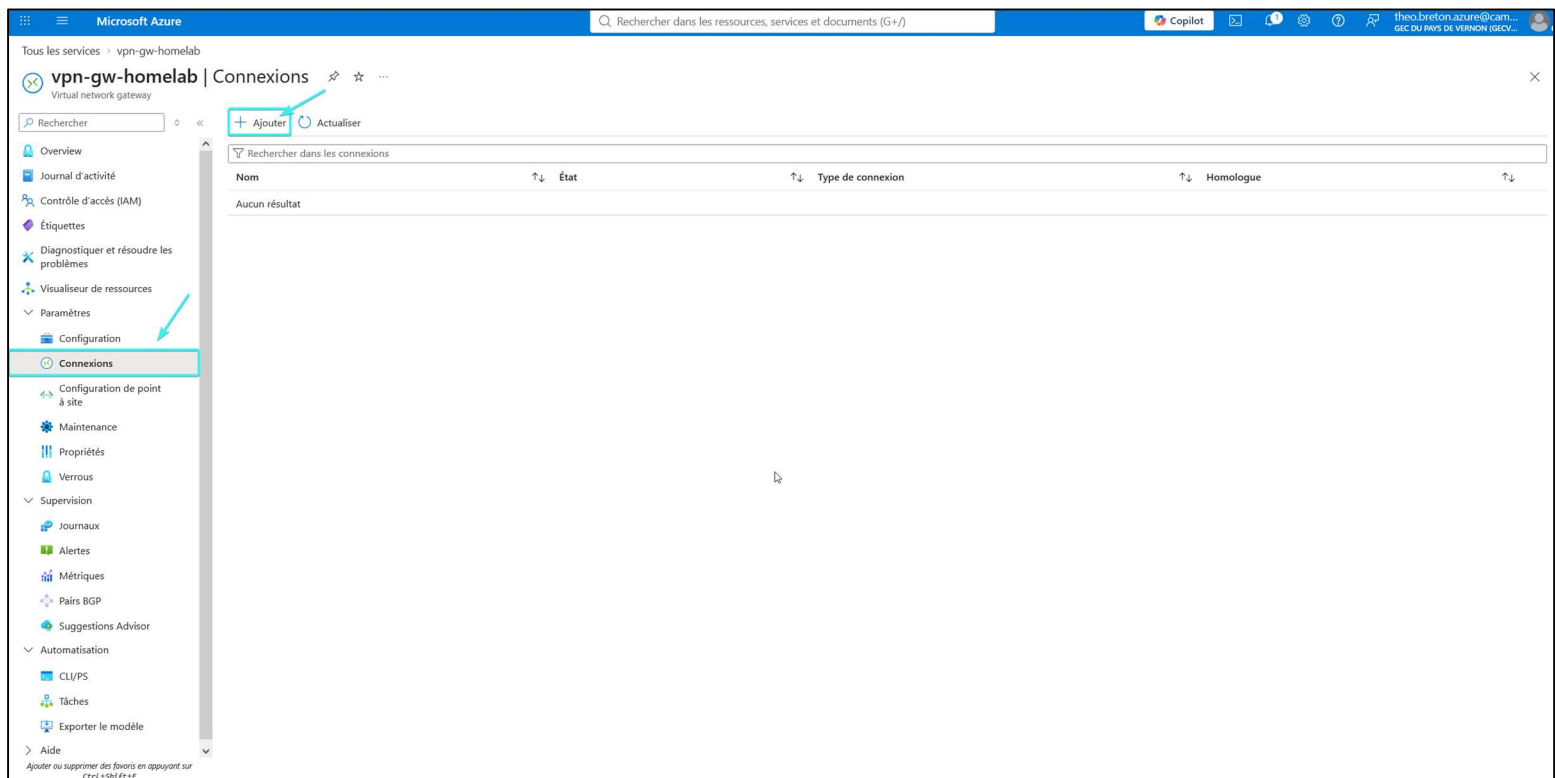
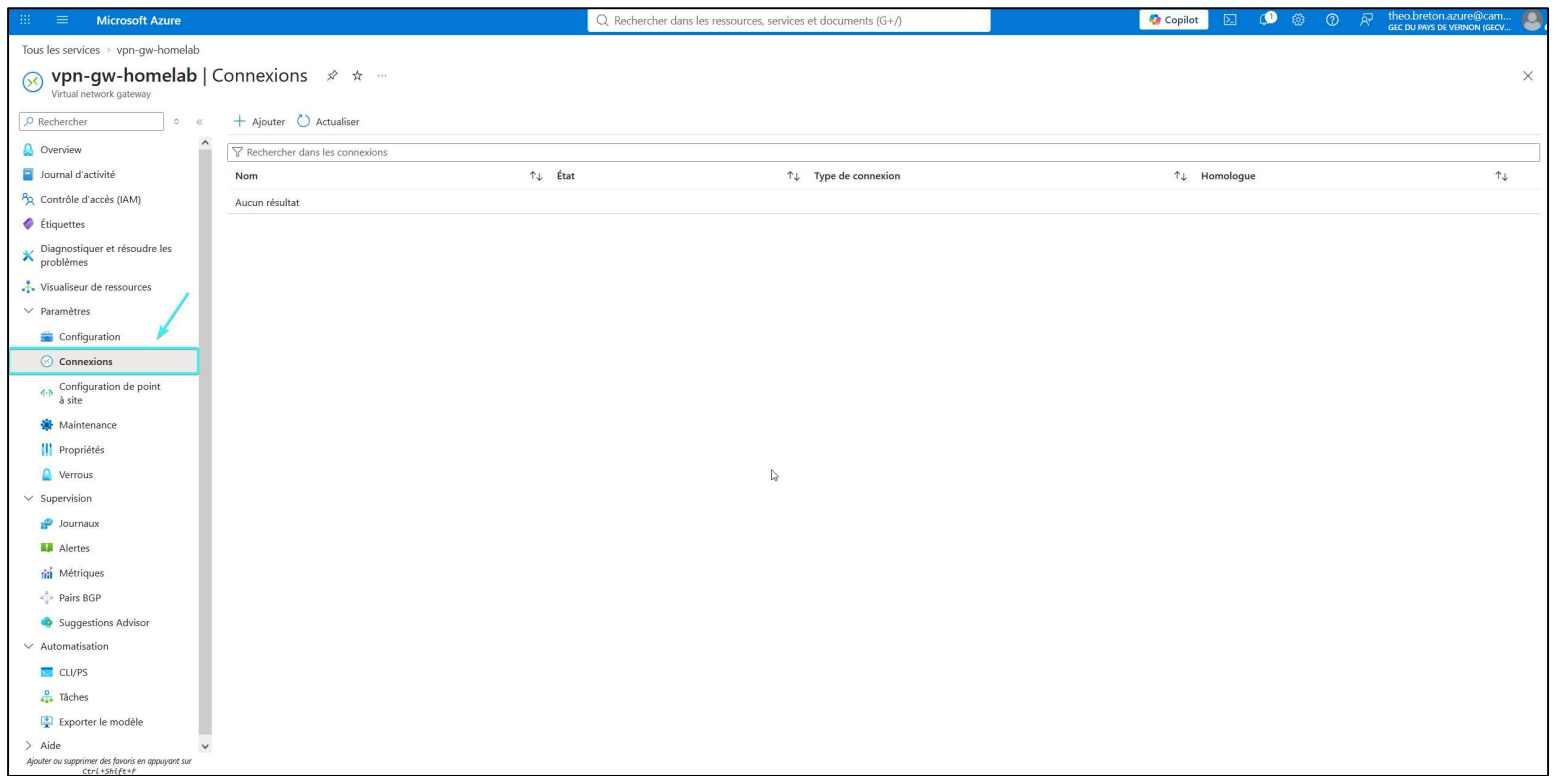
ID d'abonnement : 1e51ff42-0219-4454-9673-0522a2a15dfe

Étiquettes (modifier) : Ajouter des étiquettes

Ajouter ou supprimer des favoris en appuyant sur Ctrl+Shift+F

Étape 17 : Création de la connexion Site-to-Site

Créer la connexion en IKEv2 et définir la clé pré-partagée (PSK), à réutiliser côté FortiGate.



Microsoft Azure

Tous les services > vpn-gw-homelab | Connexions

Créer une connexion

1 De base 2 Paramètres 3 Monitoring 4 Étiquettes 5 Vérifier + créer

Créez une connexion sécurisée à votre réseau virtuel en utilisant VPN Gateway ou ExpressRoute.
En savoir plus sur VPN Gateway
En savoir plus sur ExpressRoute

Détails du projet

Abonnement * Azure for Students

Groupe de ressources * gr-homelab-hybrid

Détails de l'instance

Type de connexion * Site à site (IPsec)

Nom * connexion-homelab-avec-azure

Région * France Central

Précédent Suivant : Paramètres >

Microsoft Azure

Tous les services > vpn-gw-homelab | Connexions

Créer une connexion

✓ De base 1 Paramètres 2 Monitoring 3 Étiquettes 4 Vérifier + créer

Passerelle de réseau virtuel

Pour pouvoir utiliser un réseau virtuel avec une connexion, le réseau doit être associé à une passerelle de réseau virtuel.

Passerelle de réseau virtuel * vpn-gw-homelab

Passerelle de réseau local * lgw-fortigate-homelab

Méthode d'authentification Clé partagée (PSK) Certificat X

Clé partagée (PSK) *

Protocole IKE IKEv1 IKEv2

Utiliser l'adresse IP privée Azure

Activer BGP

Stratégie IPsec/IKE Par défaut Personnalisée

Lors de l'utilisation de stratégies IPsec/IKE personnalisées, veuillez vérifier que les paramètres personnalisés sont correctement configurés sur l'appareil local pour l'établissement initial du tunnel et la récréation de clé.

IKE Phase 1 Chiffrement * Intégrité/PRF * Groupe DH * AES256 SHA256 DHGroup14

IKE Phase 2 (IPsec) Chiffrement IPsec * Intégrité IPsec * Groupe PFS * AES256 SHA256 PFS2048

Durée de vie de l'association de sécurité IPsec en kilo-octets * 28800

Durée de vie de l'association de sécurité IPsec en secondes * 3600

Utiliser le sélecteur de trafic basé sur une stratégie Activer Désactiver

Délai d'expiration de DPD en secondes * 45

Mode de connexion Default InitiatorOnly ResponderOnly

Précédent Suivant : Monitoring >

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
SEC DU PAYS DE VERMOREL (S&CV)

Tous les services > vpn-gw-homelab | Connexions

Créer une connexion

Validation réussie

✓ De base

✓ Paramètres

✓ Monitoring

✓ Étiquettes

✓ Vérifier + créer

Informations de base

Abonnement

Groupe de ressources

Région

Type de connexion

Nom de la connexion

Azure for Students

gr-homelab-hybrid

France Central

Site à site (IPsec)

connexion-homelab-avec-azure

Paramètres

Passerelle de réseau virtuel

Passerelle de réseau local

Protocole IKE

Stratégie IPsec/IKE

IKE Phase 1

IKE Phase 2 (IPsec)

vpn-gw-homelab

lgw-fortigate-homelab

IKEv2

Personnalisée

Chiffrement: AES256, Intégrité: PRF, SHA256, Groupe DH: DHGroup14

Chiffrement IPsec: AES256, Intégrité IPsec: SHA256, Groupe DH: PFS2048, Durée de vie de l'association de sécurité IPsec en kilo-octets: 28800, Durée de vie de l'association de sécurité IPsec en secondes: 3600

Désactiver

Utiliser le sélecteur de trafic basé sur une stratégie

Délai d'expiration de DPD en secondes

Mode de connexion

Cle partage (PSK)

45

Default

utk1TuRm4hA37uQrQzqv

Étiquettes

Aucun

Créer

Précédent

Suivant

Télécharger un modèle pour automation

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
SEC DU PAYS DE VERMOREL (S&CV)

Tous les services

CreateConnection-20260905013202 | Vue d'ensemble

Déploiement

Rechercher

Supprimer

Annuler

Redéployer

Télécharger

Actualiser

Vue d'ensemble

Entrées

Sorties

Modèle

Le déploiement est en cours

Nom du déploiement : CreateConnection-20260905013202

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 05/09/2026 01:42:30

ID de corrélation : 19a9e156-b40c-42a9-8f7b-ed1e19407162

Détails du déploiement

Ressource	Type	Statut	Détails de l'opération
connexion-homelab-avec-azure	Connection	Created	Détails de l'opération

Microsoft Defender pour le cloud

Sécuriser vos applications et votre infrastructure

Accédez à Microsoft Defender pour le cloud >

Tutoriels Microsoft gratuits

Commencer l'apprentissage aujourd'hui >

Travailler avec un expert

Les experts Azure sont des partenaires fournisseurs de services qui peuvent vous aider à gérer vos ressources sur Azure et constituer votre première ligne de support.

Trouver un expert Azure >



Tous les services

CreateConnection-20260905013202 | Vue d'ensemble

SupprimerAnnulerRedéployerTéléchargerActualiser

Vue d'ensemble

Entrées

Sorties

Modèle

✓

Votre déploiement a été effectué

Nom du déploiement : CreateConnection-20260905013202

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 05/09/2026 01:42:35

ID de corrélation : 19aee166-b40c-42a9-87fb-ed1e19407162

Détails du déploiement

Étapes suivantes

Accéder à la ressource

Gestion des coûts

Recevez des notifications pour vous aider à respecter votre budget et à éviter des frais imprévus sur votre facture.

Configurer les alertes de coût >

Microsoft Defender pour le cloud

Sécuriser vos applications et votre infrastructure

Accédez à Microsoft Defender pour le cloud >

Tutoriels Microsoft gratuits

Commencer l'apprentissage aujourd'hui >

Travailler avec un expert

Les experts Azure sont des partenaires fournisseurs de services qui peuvent vous aider à gérer vos ressources sur Azure et constituer votre première ligne de support.

Trouver un expert Azure >

Ajouter ou supprimer des favoris en appuyant sur 

Tous les services > CreateConnection-20260905013202 | Vue d'ensemble

gr-homelab-hybrid

Rechercher

+ CréerGérer l'affichageSupprimer le groupe de ressourcesActualiserExporter au format CSVOuvrez une requêteAttribuer des balisesDéplacerSupprimerExporter un modèleOuvrir sur un appareil mobileAccéder au groupe de services

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Visualiseur de ressources

Événements

Paramètres

Gestion des coûts

Supervision

Automatisation

Aide

Bas

Abonnement (déplacer) : Azure for Students

ID d'abonnement : 1e51ff42-0219-4454-9673-0522a2a15dfe

Étiquettes (modifier) : Ajouter des étiquettes

Déploiements : 5 Réussite

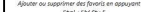
Emplacement : France Central

RessourcesRecommandations

Filter un champ...Type est égal à toutEmplacement est égal à toutAjouter un filtre

Nom ?	Type	Emplacement
connexion-homelab-avec-azure	...	France Central
lgw-fortigate-homelab	Local network gateway	France Central
publique-ip-vpn-gw-homelab	Adresse IP publique	France Central
vnet-homelab-hybrid	Réseau virtuel	France Central
vpn-gw-homelab	Virtual network gateway	France Central

Affichage de 1 – 5 sur 5. Afficher le nombre: auto

Ajouter ou supprimer des favoris en appuyant sur 

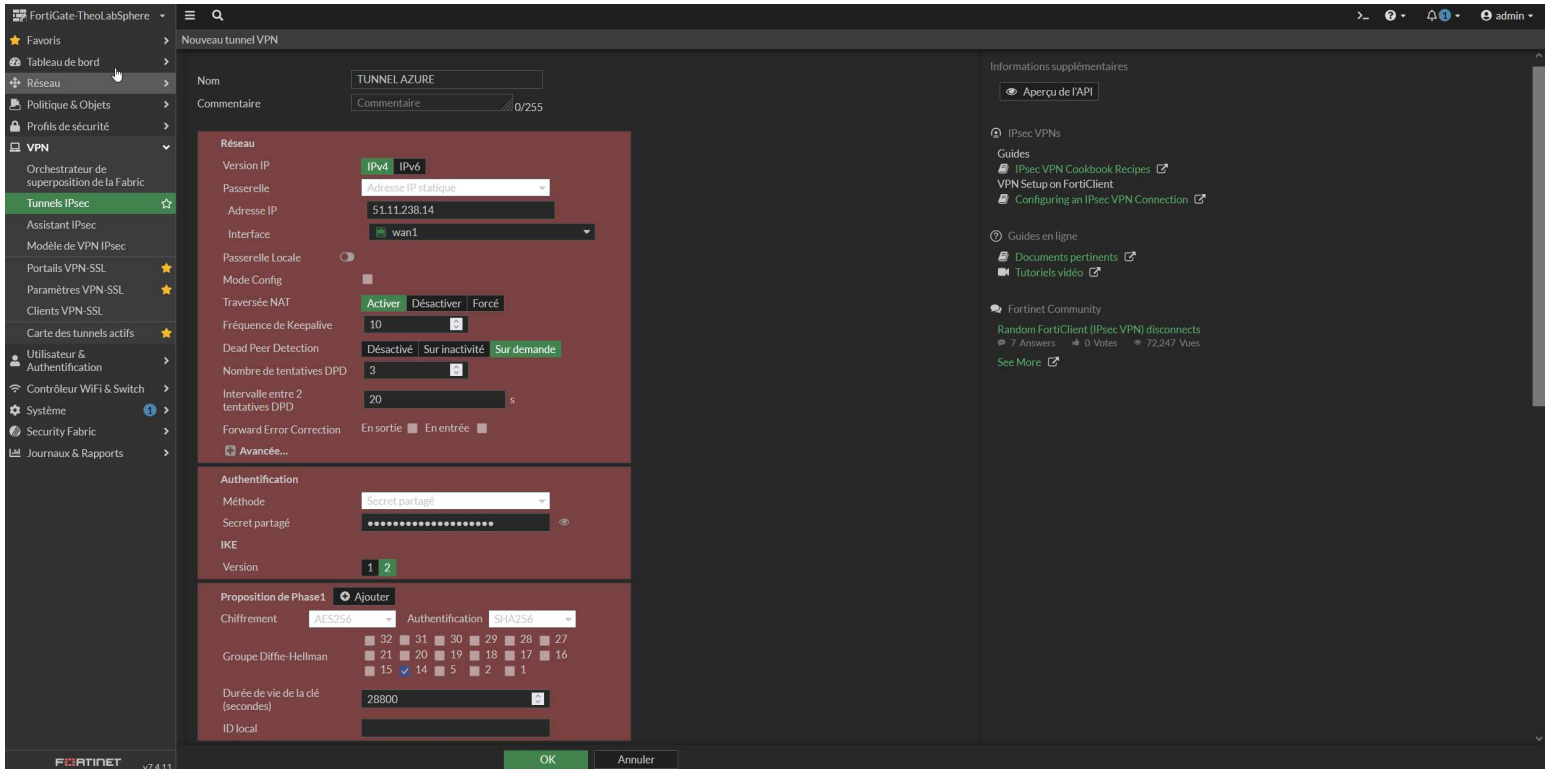
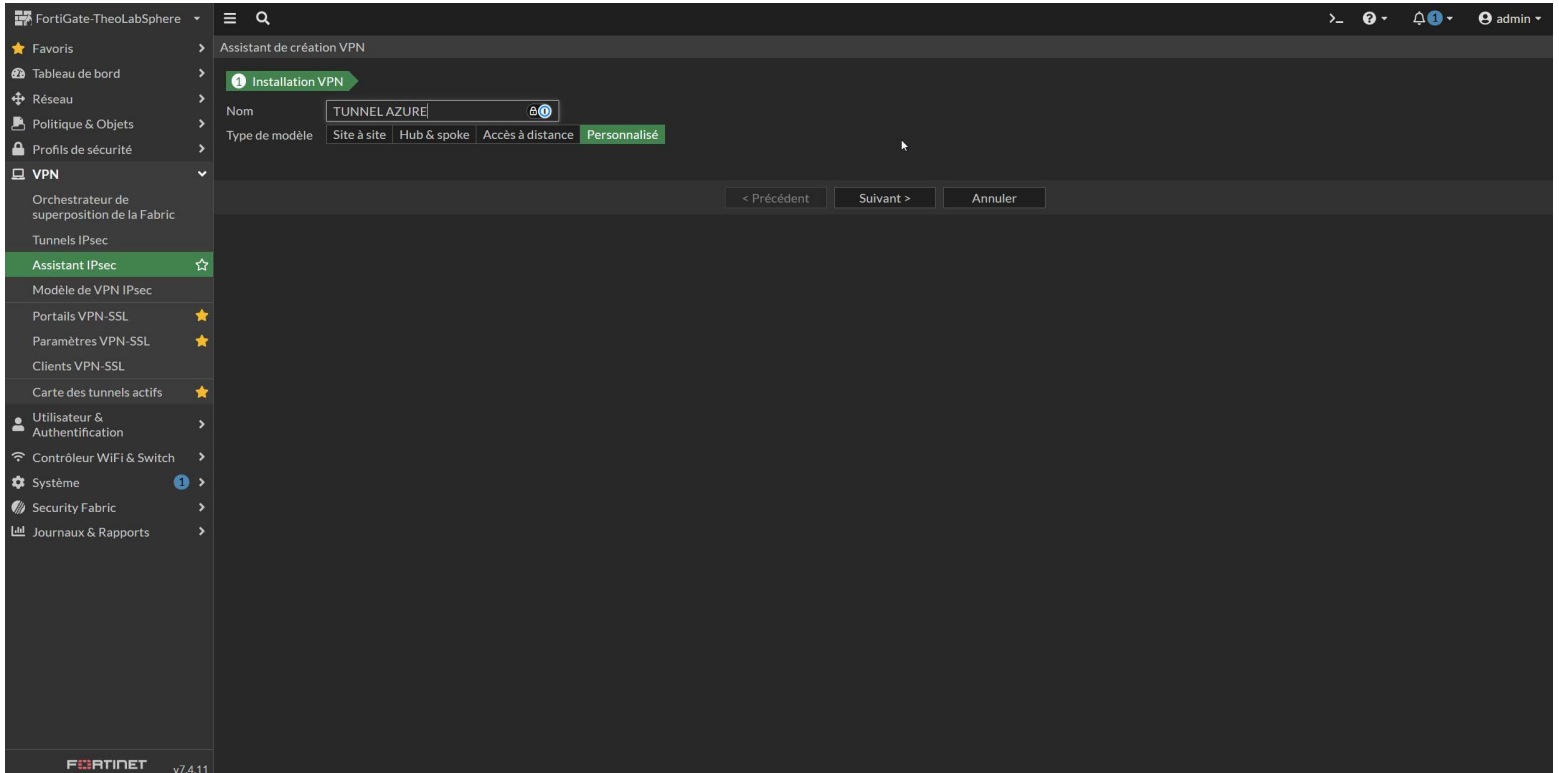
Envoyer des commentaires

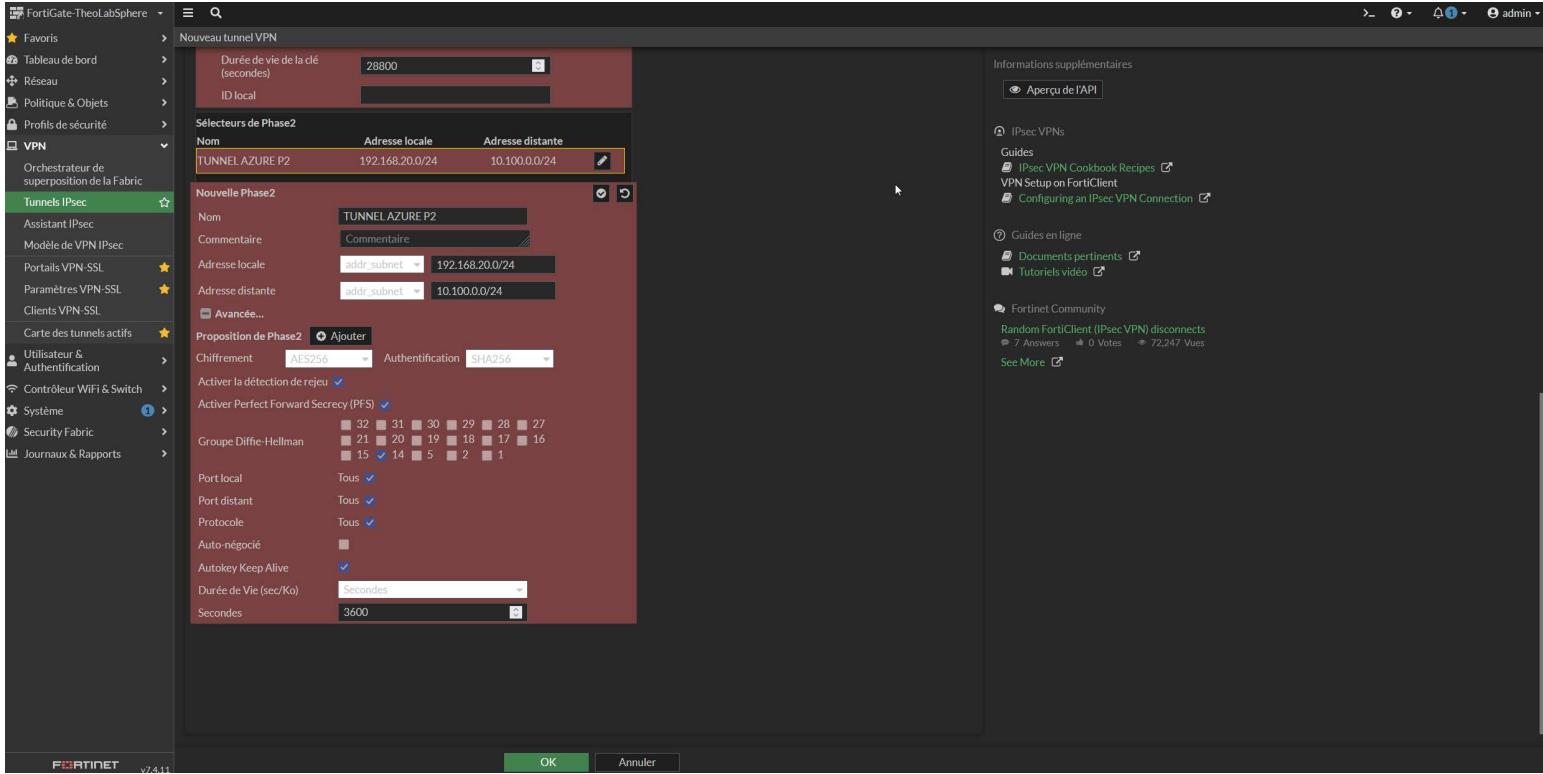
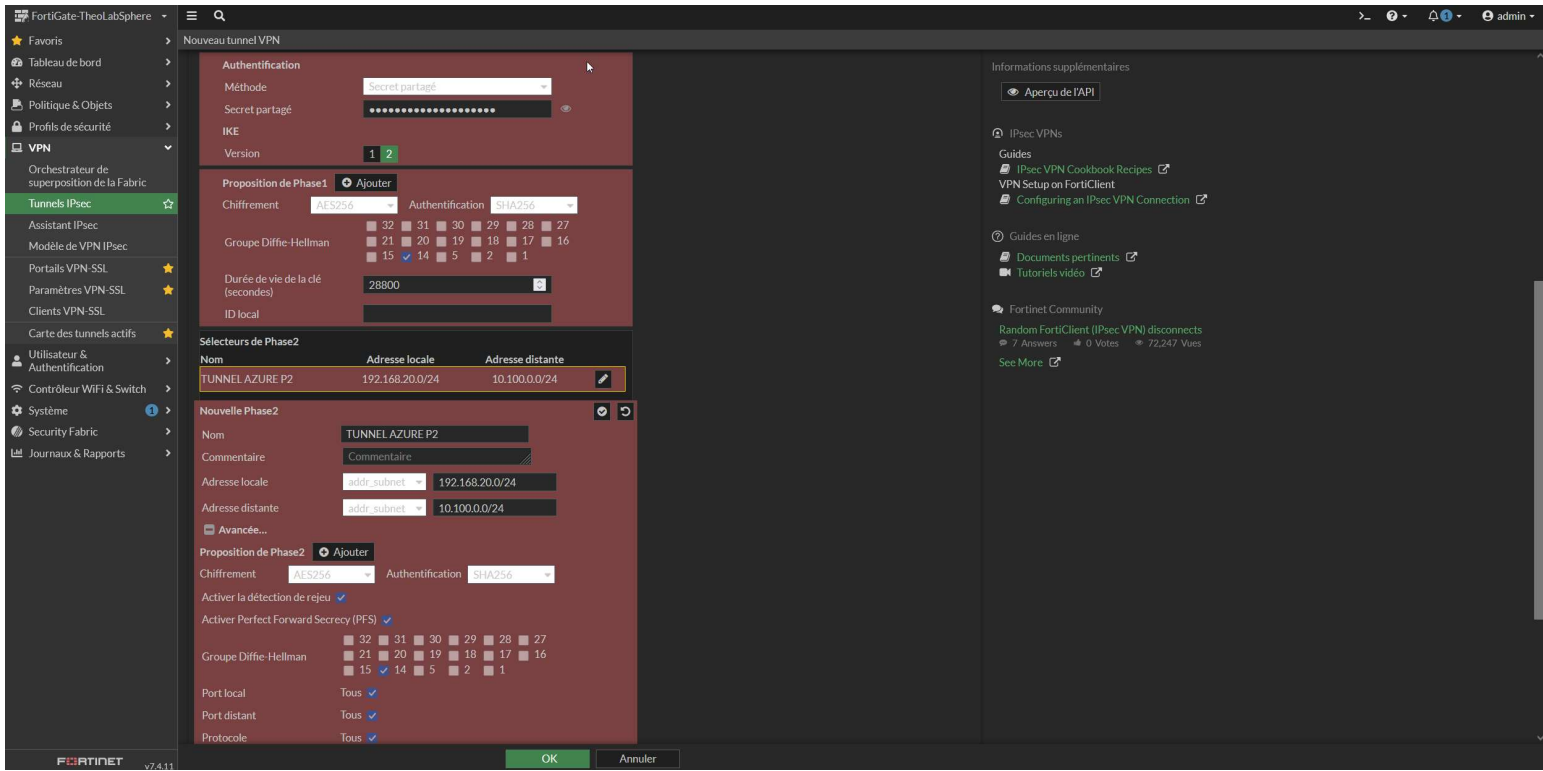


PARTIE 3 : RETOUR SUR LE HOMELAB — LE TUNNEL

Étape 18 : Création du tunnel IPsec route-based

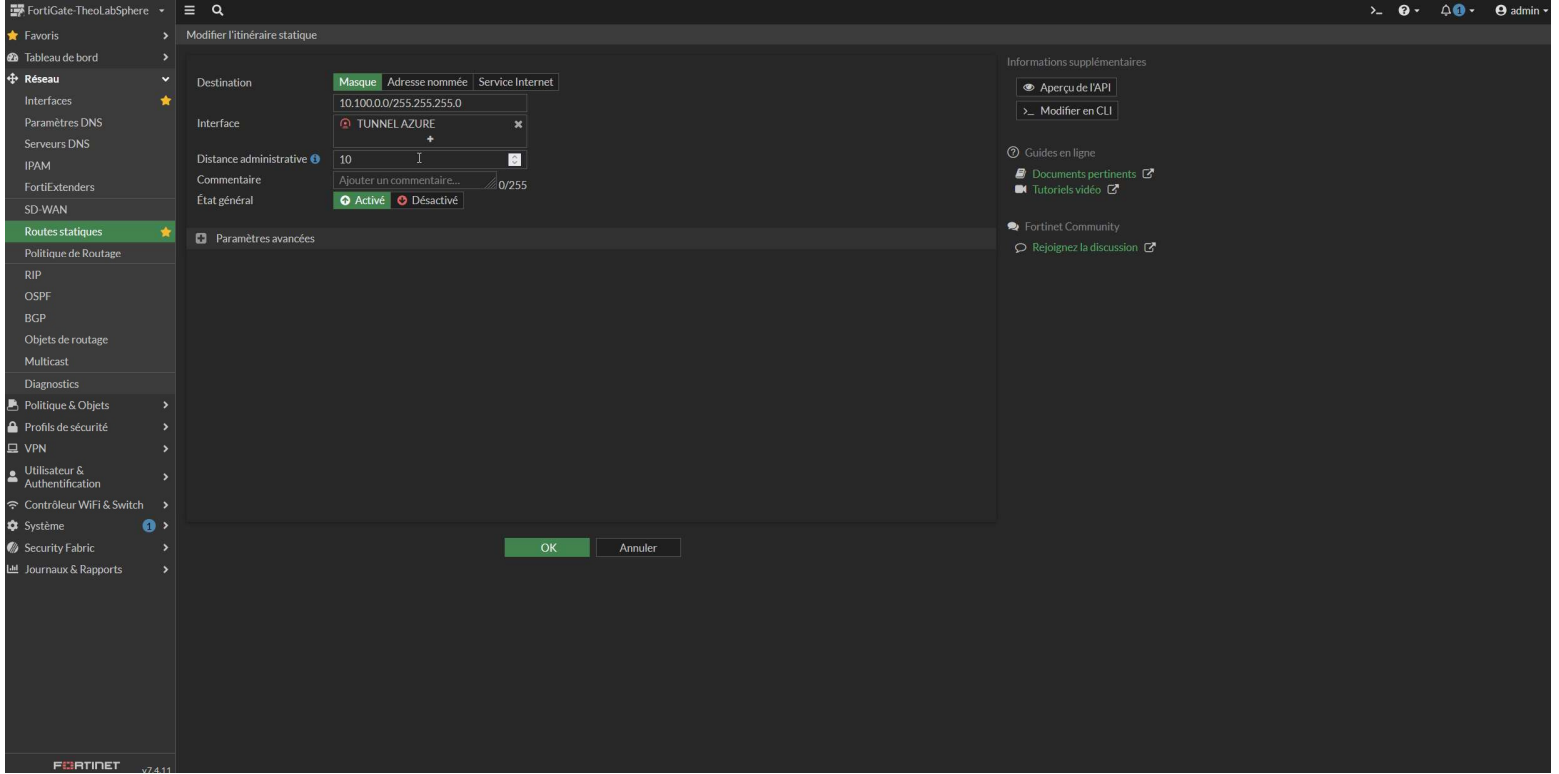
Phase 1 : IKEv2, AES256, SHA256, DH Group 14, passerelle distante = IP publique de la gateway Azure, PSK identique à l'étape 17. Phase 2 : mêmes algorithmes, PFS activé, sélecteurs 192.168.20.0/24 ↔ 10.100.0.0/24. L'interface VTI est créée automatiquement par le FortiGate.





Étape 19 : Routage statique vers le VNet Azure

Ajouter une route statique vers 10.100.0.0/24 via l'interface du tunnel.



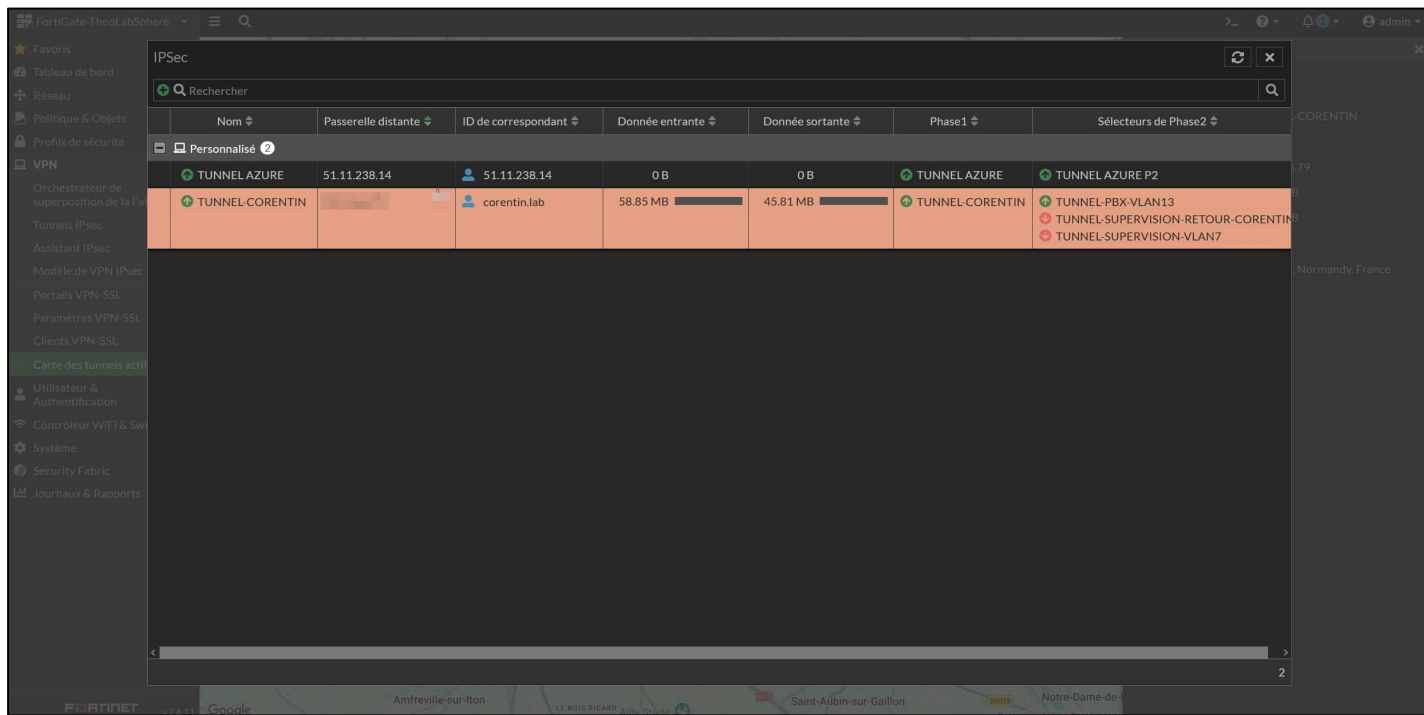
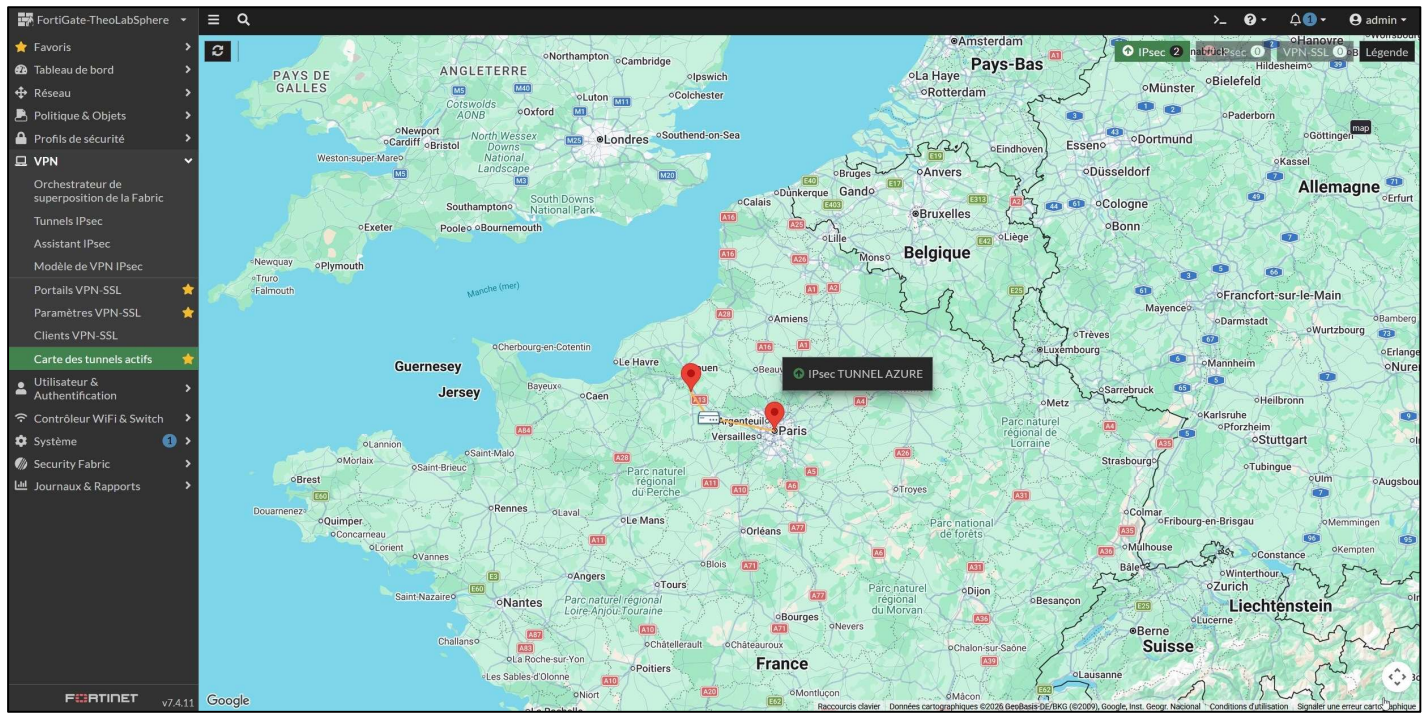
Étape 20 : Création des règles de filtrage

Création de la règles VLAN 20 ↔ VNet, **NAT décoché**, restreintes aux ports AD (DNS 53, Kerberos 88, LDAP 389/636, SMB 445, RPC 135 + plage dynamique) plus ICMP pour les tests.

PARTIE 4 : VALIDATION DE LA CHAÎNE

Étape 21 : Vérification du tunnel

Contrôler l'état « Connected » dans le portail Azure et le tunnel *up* sur le FortiGate, puis tester le ping dans les deux sens. En cas d'échec, utiliser Network Watcher → Résolution des problèmes de connexion.



J'ai rencontré un soucis au moment de la création de la VM j'ai dû changer de zone géographique pour aller au Danemark. Par conséquent j'ai dû changer certain réglage :

Pour permettre de créer la VM dans la zone du Danemark, j'ai créé un nouveau sous réseau avec une nouvelle passerelle.

Commande 1 — Crée le VNet Denmark East :

- Un réseau virtuel **vnet-azure-denmark** à Denmark East avec l'espace d'adressage 10.101.0.0/24
- Avec un sous-réseau **Subnet-App** en 10.101.0.32/27 (pour les VM)

```
az network vnet create --resource-group gr-homelab-hybrid --name vnet-azure-denmark --location denmarkeast --address-prefixes 10.101.0.0/24 --subnet-name Subnet-App --subnet-prefixes 10.101.0.32/27
```

Commande 2 — Peering France Central → Denmark :

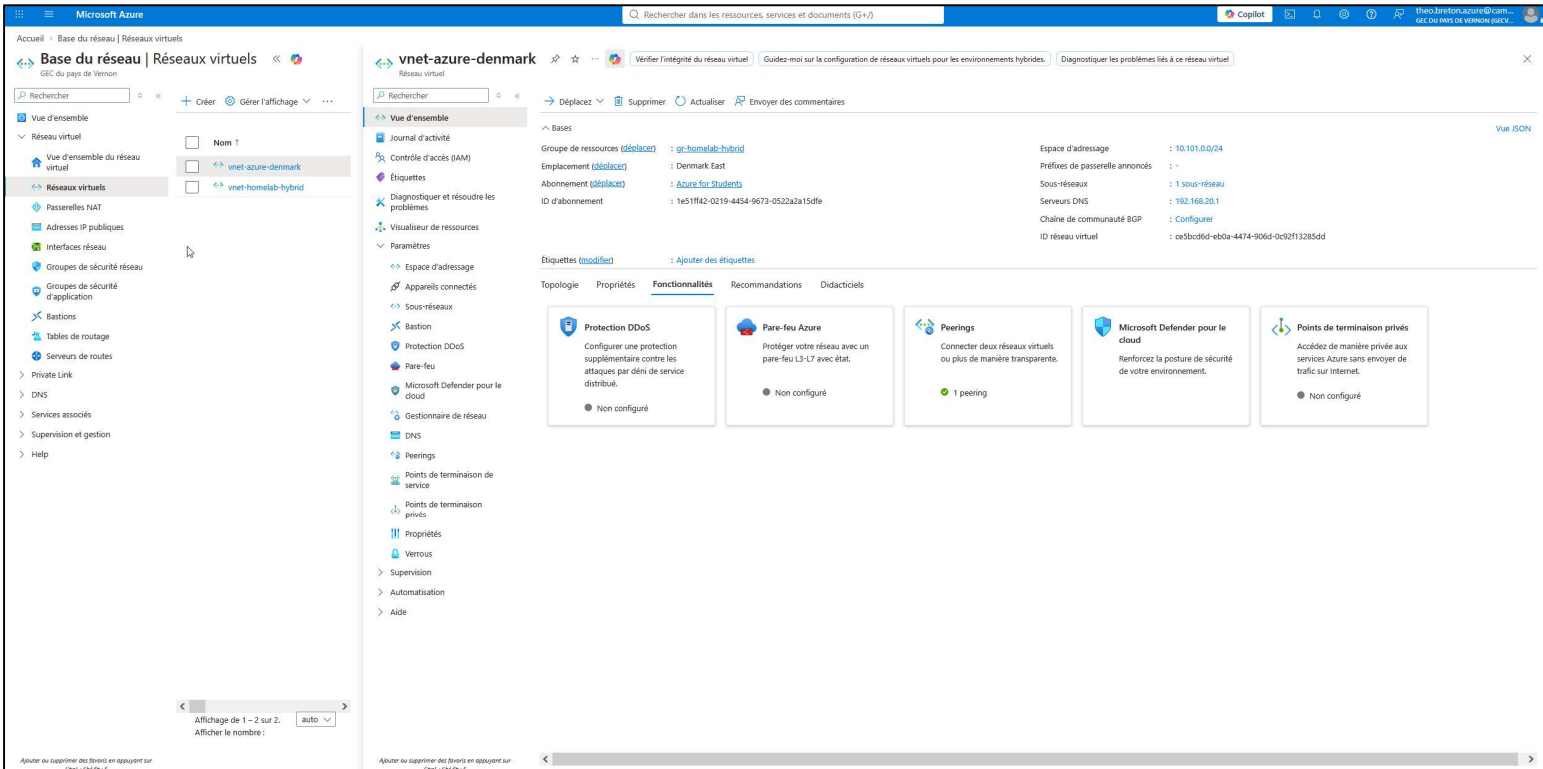
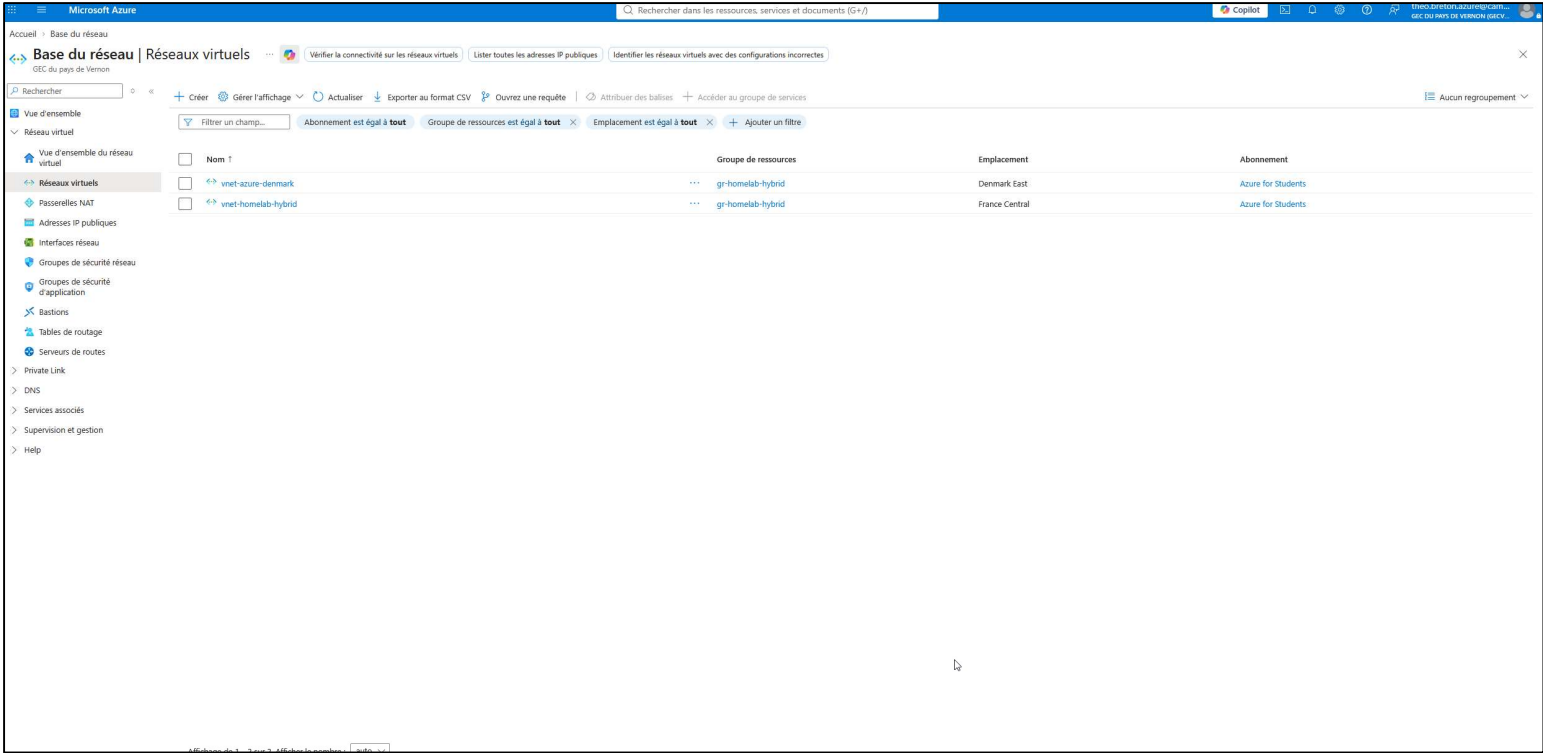
- Relie le VNet France Central vers le VNet Denmark
- --allow-gateway-transit : autorise le VNet Denmark à utiliser la passerelle VPN de France Central (c'est ce qui permet à ta VM en Denmark de passer par le tunnel VPN sans avoir sa propre passerelle)

```
az network vnet peering create --resource-group gr-homelab-hybrid --name peering-fc-to-denmark --vnet-name vnet-homelab-hybrid --remote-vnet vnet-azure-denmark --allow-vnet-access --allow-forwarded-traffic --allow-gateway-transit
```

Commande 3 — Peering Denmark → France Central :

- Le peering dans l'autre sens (il faut toujours les deux)
- --use-remote-gateways : dit au VNet Denmark "utilise la passerelle VPN de France Central comme si c'était la tienne"

```
az network vnet peering create --resource-group gr-homelab-hybrid --name peering-denmark-to-fc --vnet-name vnet-azure-denmark --remote-vnet vnet-homelab-hybrid --allow-vnet-access --allow-forwarded-traffic --use-remote-gateways
```



Microsoft Azure

Accueil > Base du réseau > Réseaux virtuels > vnet-homelab-hybrid > Peerings

peering-fc-to-denmark

vnet-homelab-hybrid

L'appariage de réseaux virtuels vous permet de connecter de manière transparente au moins deux réseaux virtuels dans Azure. Cela permettra aux ressources du réseau virtuel de se connecter et de communiquer directement avec des ressources du réseau virtuel apparié. Vous pouvez utiliser le peering de sous-réseaux pour connecter uniquement les sous-réseaux spécifiques que vous choisissez entre réseaux virtuels.

Résumé du réseau virtuel distant

Type de peering: ☒ Réseau virtuel ☐ Sous-réseau

ID de réseau virtuel distant: lab-hybrid/providers/Microsoft.Network/virtualNetworks/vnet-azure-denmark

Espace d'adressage IP: 10.101.0.0/24

Activer le peering IPv6 uniquement: ☐

Le réseau virtuel « vnet-homelab-hybrid » ne dispose d'aucun sous-réseau IPv6 disponible à jumeler avec

Résumé du réseau virtuel local

Nom du lien de peering: peering-fc-to-denmark

État de l'appariage: Connected

Paramètres de l'appariage de réseaux virtuels local

Autoriser 'vnet-homelab-hybrid' à accéder à 'vnet-azure-denmark': ☒

Autoriser 'vnet-homelab-hybrid' à recevoir le trafic transféré de 'vnet-azure-denmark': ☒

Autoriser une passerelle ou un serveur de routes dans 'vnet-homelab-hybrid' à transférer le trafic vers 'vnet-azure-denmark': ☒

Activer 'vnet-homelab-hybrid' pour utiliser une passerelle distante ou un serveur de routes de 'vnet-azure-denmark': ☐

Enregistrez Annuler

Envoyer des commentaires

La partie du peering **Denmark → France Central** (peering-fc-to-denmark).

Les 3 options cochées (flèches bleues) :

"Autoriser vnet-azure-denmark à accéder à vnet-homelab-hybrid" — J'autorise les ressources de mon VNet Denmark (ma VM azure-01) à communiquer avec les ressources de mon VNet France Central. Sans cette option, mes deux VNets seraient isolés même s'ils sont peerés.

"Autoriser vnet-azure-denmark à recevoir le trafic transféré de vnet-homelab-hybrid" — J'accepte le trafic qui ne provient pas directement de mon VNet France Central mais qui transite par lui. Dans mon cas, c'est le trafic de mon homelab (192.168.20.0/24) qui arrive par le tunnel VPN dans France Central et qui est ensuite transféré vers Denmark. Sans cette option, seul le trafic originaire de France Central passerait, pas celui venant de mon homelab.

"Activer vnet-azure-denmark pour utiliser une passerelle distante de vnet-homelab-hybrid" — C'est l'option la plus importante. J'indique à mon VNet Denmark qu'il n'a pas sa propre passerelle VPN, mais qu'il doit utiliser celle de France Central. C'est grâce à cette option que ma VM azure-01 peut atteindre mon homelab via le tunnel VPN sans que j'aie à déployer et payer une deuxième passerelle VPN au Denmark. L'option décochée ("Autoriser une passerelle... à transférer le trafic")

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

Théo BRETON

Accueil > vnet-azure-denmark | Peerings

peering-denmark-to-fc

vnet-azure-denmark

L'appariage de réseaux virtuels vous permet de connecter de manière transparente au moins deux réseaux virtuels dans Azure. Cela permettra aux ressources du réseau virtuel de se connecter et de communiquer directement avec des ressources du réseau virtuel apparié. Vous pouvez utiliser le peering de sous-réseaux pour connecter uniquement les sous-réseaux spécifiques que vous choisissez entre réseaux virtuels.

Résumé du réseau virtuel distant

Type de peering

☒ Réseau virtuel

☐ Sous-réseau

ID de réseau virtuel distant

/subscriptions/1e51ff42-0219-4454-9673-0522a2a15dfe/resourceGroups/gr... [🔗](#)

Espace d'adressage IP10.100.0.0/24

Activer le peering IPv6 uniquement [?](#)

☐

Le réseau virtuel « vnet-azure-denmark » ne dispose d'aucun sous-réseau IPv6 disponible à jumeler avec.

Résumé du réseau virtuel local

Nom du lien de peering *peering-denmark-to-fc

État de l'appariage

Connected

Paramètres de l'appariage de réseaux virtuels local

Autoriser « vnet-azure-denmark » à accéder à « vnet-homelab-hybrid » [?](#)☒

Autoriser « vnet-azure-denmark » à recevoir le trafic transféré de « vnet-homelab-hybrid » [?](#)☒

Autoriser une passerelle ou un serveur de routes dans « vnet-azure-denmark » à transférer le trafic vers « vnet-homelab-hybrid » [?](#)☐

Activer « vnet-azure-denmark » pour utiliser une passerelle distante ou un serveur de routes de « vnet-homelab-hybrid » [?](#)☒

Enregistrer

Annuler

[Envoyer des commentaires](#)

La partie du peering **France Central → Denmark** (peering-fc-to-denmark), l'autre sens. Les 3 options cochées :

"Autoriser vnet-homelab-hybrid à accéder à vnet-azure-denmark" — J'autorise les ressources de mon VNet France Central à communiquer avec celles de mon VNet Denmark. C'est le pendant de l'option côté Denmark : le peering doit être autorisé dans les deux sens.

"Autoriser vnet-homelab-hybrid à recevoir le trafic transféré de vnet-azure-denmark" — J'accepte que mon VNet France Central reçoive du trafic transféré depuis Denmark. Cela permet les réponses retour de ma VM azure-01 vers mon homelab via le tunnel VPN.

"Autoriser une passerelle dans vnet-homelab-hybrid à transférer le trafic vers vnet-azure-denmark" — C'est l'option clé de ce côté. J'autorise ma passerelle VPN (située dans France Central) à relayer le trafic de mon homelab vers le VNet Denmark. Sans cette option, la passerelle VPN garderait le trafic on-prem pour elle-même et ne le transmettrait pas au VNet peeré. C'est le complément du "Utiliser une passerelle distante" coché côté Denmark.

Étape 22 : Déploiement de la VM Azure

Déployer une VM Windows Server dans le Subnet-App, sans rôle particulier.

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

theo.breton.azure@cam...
acc ou pers de version jscv...

Créer une machine virtuelle

Informations de base Disques Mise en réseau Gestion Surveillance Avancé Balises Vérifier et créer

utilisez votre propre image personnalisée. Renseignez l'onglet Informations de base, puis Vérifier + créez pour provisionner une machine virtuelle avec les paramètres par défaut ou passez en revue chaque onglet pour une personnalisation complète. [En savoir plus](#)

Détails du projet

Sélectionnez l'abonnement pour gérer les ressources déployées et les coûts. Utilisez des groupes de ressources comme des dossiers pour organiser et gérer toutes vos ressources.

Abonnement *  Azure for Students 

Groupe de ressources *  gr-homelab-hybrid  [Créer nouveau](#)

Détails de l'instance

Nom de machine virtuelle *  azure-01  

Région *  (Europe) Denmark East  [Déployer sur une zone étendue Azure](#)

Options de disponibilité  Aucune redondance d'infrastructure requise 

Type de sécurité  Standard 

Image *  Windows Server 2022 Datacenter - x64 Gen2  [See all images](#) [Configurer la génération de machine virtuelle](#)

VM architecture *  ☐ ARM64 ☒ x64 

Taille *  Standard D2s - 2 vcpus, 4 GB memory (60.88 \$US/month)  [Voir toutes les tailles](#) [Personnaliser les cœurs](#)

Exécuter avec la remise Azure Spot 

Compte administrateur

Nom d'utilisateur(-trice) *  azureuser 

Mot de passe *  

Confirmez le mot de passe *  

Précédent **Suivant** Vérifier + créer

[Envoyer vos commentaires](#)

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/)

Copilot

theo.breton.azure@cam...
acc ou pers de version jscv...

Créer une machine virtuelle

Informations de base **Disques** Mise en réseau Gestion Surveillance Avancé Balises Vérifier et créer

 Il s'agit d'une préversion de nouvelle expérience de création de machine virtuelle. Les fonctionnalités sont limitées dans cette expérience et l'ensemble des commentaires sont les bienvenus. [Cliquez ici pour accéder à l'expérience précédente.](#)

Les machines virtuelles Azure ont un disque de système d'exploitation et un disque temporaire pour le stockage à court terme. Vous pouvez attacher des disques de données supplémentaires. La taille de la machine virtuelle détermine le type de stockage que vous pouvez utiliser et le nombre de disques de données autorisés. [En savoir plus](#)

 Les ressources de stockage sous-jacentes consommées par votre machine virtuelle sont facturées. [En savoir plus](#)

 La configuration de cette ressource machine virtuelle et de ses disques attachés risque de ne pas permettre aux disques d'utiliser leurs performances débit complètes. La taille actuelle de machine virtuelle prend en charge jusqu'à 23 Mbit/s. Le nombre total de disques attachés à machine virtuelle « azure-01 » est de 100 Mbit/s. Vous pouvez modifier la taille de la ressource machine virtuelle pour prendre en charge des disques supplémentaires débit. [En savoir plus](#)

Chiffrement de disque de machine virtuelle

Le chiffrement de Stockage sur disque Azure chiffre automatiquement vos données stockées sur des disques managés Azure (disques de système d'exploitation et de données) au repos par défaut lors de leur conservation dans le cloud.

Chiffrement sur l'hôte   Le chiffrement sur l'hôte n'est pas inscrit pour l'abonnement sélectionné. [En savoir plus](#)

Disque de système d'exploitation

Taille du disque du système d'exploitation  Image par défaut (127 GiB) 

Type de disque de système d'exploitation  SSD Standard   La taille de machine virtuelle sélectionnée prend en charge les disques Premium. Nous vous recommandons d'utiliser des disques SSD Premium pour les charges de travail avec des taux IOPS élevés. Les machines virtuelles équipées de disques SSD Premium remplissent les conditions de connectivité à 99,9 % du contrat SLA.

☒ Supprimer avec la machine virtuelle 

Activer la compatibilité avec les disques Ultra   Le disque Ultra n'est pas pris en charge dans Denmark East.

Gestion des clés  Clé gérée par la plateforme

Disques de données

Vous pouvez ajouter et configurer des disques de données supplémentaires pour votre machine virtuelle ou attacher des disques existants. Cette machine virtuelle est également fournie avec un disque temporaire.

Nu...	Nom	Taille (Go...	Type de disque	Mise en cache de l'hôte	Supprimer avec la
-------	-----	---------------	----------------	-------------------------	-------------------

Précédent **Suivant** Vérifier + créer

[Envoyer vos commentaires](#)

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

théo.breton.azure@cam...
SEC DU BREV DE VERNON (SECY...

Accueil

Créer une machine virtuelle

Informations de baseDisquesMise en réseauGestionSurveillanceAvancéBalisesVérifier et créer

Il s'agit d'une préversion de nouvelle expérience de création de machine virtuelle. Les fonctionnalités sont limitées dans cette expérience et l'ensemble des commentaires sont les bienvenus.
[Cliquez ici pour accéder à l'expérience précédente.](#)

Définissez la connectivité réseau de votre machine virtuelle en configurant les paramètres de la carte d'interface réseau. Vous pouvez contrôler les ports et la connectivité entrante/sortante avec des règles de groupe de sécurité, ou placer derrière une solution d'équilibrage de charge existante. [En savoir plus >](#)

Réseau virtuel

Le réseau virtuel Azure permet à de nombreux types de ressources Azure de communiquer de manière sécurisée les uns avec les autres, Internet et les réseaux locaux. [En savoir plus sur les réseaux virtuels >](#)

Virtual network *

vnet-azure-denmark

Subnet *

Subnet-App - 10.101.0.32/27

Interface réseau

Une interface réseau permet à une machine virtuelle Azure de communiquer avec Internet, Azure et les ressources locales. Une machine virtuelle peut avoir une ou plusieurs interfaces réseau.

Adresse IP publique

Aucun

Groupe de sécurité réseau de la carte réseau

Aucune

Essentiel

Avancé

Ports entrants publics *

Aucune

Autoriser les ports sélectionnés

Sélectionner des ports d'entrée

Sélectionner un ou plusieurs ports

Tout le trafic en provenance d'Internet sera bloqué par défaut. Vous pouvez changer les règles de port d'entrée dans la page Machine virtuelle > Mise en réseau.

Supprimer la carte réseau lors de la suppression de la machine virtuelle

☒

Activer les performances réseau accélérées

☐

Précédent

Suivant

Vérifier + créer

Envoyer vos commentaires

Accueil

Créer une machine virtuelle

Informations de baseDisquesMise en réseauGestionSurveillanceAvancéBalisesVérifier et créer

Voir le modèle d'automatisation

Prix

1 X Standard B2s par Microsoft

Des crédits d'abonnement s'appliquent

0,0566USD/h

CONDITIONS

En cliquant sur « Create », (a) j'accepte les conditions légales et les déclarations de confidentialité associées aux offres de la Place de marché indiquées ci-dessus. (b) j'autorise Microsoft à facturer selon mon mode de paiement actuel les frais associés aux offres, à la même fréquence de facturation que mon abonnement Azure et (c) j'accepte que Microsoft puisse partager mes informations de contact et relatives à mon utilisation et à mes transactions avec les fournisseurs des offres concernant le support, la facturation et les autres activités liées aux transactions. Microsoft ne fournit pas de droits pour les offres de tiers. Consultez les [Conditions de la Place de marché Azure](#) pour plus d'informations.

Informations de base

Abonnement

Azure for Students

Groupe de ressources

gr-homelab-hybrid

Nom de machine virtuelle

azure-01

Région

Denmark East

Options de disponibilité

Aucune redondance d'infrastructure requise

Type de sécurité

Standard

Image

Windows Server 2022 Datacenter

Taille

Standard B2s

Architecture de machine virtuelle

x64

Nom d'utilisateur

azureuser

Ports entrants publics

Aucune

Vous avez déjà une licence Windows ?

Non

Azure Spot

Non

Disques

Taille du disque du système d'exploitation

Image par défaut

Type de disque de système d'exploitation

StandardSSD_LRS

Utiliser des disques managés

Oui

Supprimer le disque de système d'exploitation avec la machine virtuelle

Oui

Disque de système d'exploitation éphémère

Aucune

Mise en réseau

Réseau virtuel

vnet-azure-denmark

Sous-réseau

Subnet-App

IP publique

Aucun

Groupe de sécurité réseau de la carte

Aucun

Précédent

Suivant

Créer

Envoyer vos commentaires

PROJET PERSONNEL – Théo BRETON

PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

50

Accueil

CreateVirtualMachine-azure-01 | Vue d'ensemble

Déploiement

Rechercher

Supprimer Annuler Redéployer Télécharger Actualiser

Vue d'ensemble

Entrées

Sorties

Modèle

✓

Votre déploiement a été effectué

Nom du déploiement : CreateVirtualMachine-azure-01

Abonnement : Azure for Students

Groupe de ressources : gr-homelab-hybrid

Heure de début : 05/09/2026 20:12:34

ID de corrélation : 3219aa33-61f2-4974-8fb0-2db88a8a3e2c

Détails du déploiement

Ressource	Type	Statut	Détails de l'opération
azure-01	Microsoft.Compute/virtualMach	OK	Détails de l'opération
azure-0134	Microsoft.Network/networkInter	Created	Détails de l'opération
azure-01-nsg	Groupe de sécurité réseau	OK	Détails de l'opération

Étapes suivantes

Configurez l'arrêt automatique Recommandé

Monitorisez les dépendances réseau, les performances et l'intégrité des machines virtuelles Recommandé

Exécuter un script à l'intérieur de la machine virtuelle Recommandé

Accédez à la ressource

Créez une autre machine virtuelle

Effectuez un scale-out de votre machine virtuelle

1

Gestion des coûts

Recevez des notifications pour vous aider à respecter votre budget et à éviter des frais imprévus sur votre facture.

Configurer les alertes de coût >

Alaport ou supprimer des données en appuyant sur Ctrl+Shift+F

Nom	Abonnement	Groupe de ressources	Emplacement	État	Système d'exploitation	Taille	Adresse IP publique	Disques	Mettre à jour l'état
azure-01	Azure for Students	gr-homelab-hybrid	Denmark East	Exécution	Windows	Standard_B2s	-	1	Activer l'évaluation périodique...

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copier

Théo.Breton@cam...

Accueil

CreateVirtualMachine-azure-01 | Vue d'ensemble

Machine virtuelle

Rechercher

Connecter Démarrer Redémarrer Arrêter Mise en veille prolongée Capturer Supprimer Actualiser Échelle Ouvrir sur l'appareil mobile Commentaires CLUPs

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Diagnostiquer et résoudre les problèmes

Monitorer

Visualiseur de ressources

Se connecter

Mise en réseau

Paramètres

Disponibilité + mise à l'échelle

Sécurité

Sauvegarde + récupération d'urgence

Opérations

Supervision

Automatisation

Aide

Bases

Groupe de res... : gr-homelab-hybrid

Statut : En cours d'exécution

Emplacement : Denmark East

Abonnement : Azure for Students

ID d'abonnement : fe51ff42-0219-4454-9673-0522a2a15dfe

Étiquettes (modifier) : ajouter des étiquettes

Propriétés

Supervision

Fonctionnalités (8)

Recommandations

Tutoriels

Machine virtuelle

Nom de l'ordinateur : azure-01

Système d'exploitation : Windows (Windows Server 2022 Datacenter)

Génération de machine virtuelle : V2

Architecture de machine virtuelle : x64

État de l'agent : Ready

Version de l'agent : 2.7.41491.1216

Mise en veille prolongée : Désactivé

Groupe hôte : -

Hôte : -

Groupe de placement de proximité : -

État de colocation : N/A

Groupe de réservations de capacité : -

Type de contrôleur de disque : SCSI

Spot Azure

Spot Azure : -

Stratégie d'éviction Azure Spot : -

Disponibilité - mise à l'échelle

Zone de disponibilité (modifier) : -

Zone développée : -

Groupe à haute disponibilité : -

Ensemble d'échelle (attacher) : -

Sécurité

Arrêt automatique

Mettre à jour cette machine virtuelle avec Azure CU

M'aidier à copier cette machine virtuelle dans n'importe quelle région

Gérer cette machine virtuelle avec Azure CU

Système d'exploitation : Windows (Windows Server 2022 Datacenter)

Taille : Standard B2s (2 processeurs virtuels, 4 Gio de mémoire)

Adresse IP publique de la... : -

Réseau/sous-réseau virtuel : vnet-azure-denmark/Subnet-App

Nom DNS : -

État d'intégrité : -

Heure de création : 05/09/2026 18:12 UTC

Mise en réseau

Adresse IP publique : -

Adresse IP publique (IPv6) : -

Adresse IP privée : 10.10.10.10

Adresse IP privée (IPv6) : -

Réseau/sous-réseau virtuel : vnet-azure-denmark/Subnet-App

Nom DNS : -

Taille

Taille : Standard B2s

Processeurs virtuels : 2

RAM : 4 Gio

Threads par cœur : 1

Détails d'image source

Éditeur d'image source : microsoftwindowsserver

Offre d'image source : windowsserver2022

Plan d'image source : 2022-datacenter-g2

Disque

Disque du système d'exploitation : azure-01_OsDisk_1_2f86f84b5676403a6284215bd09998c

Chiffrement sur l'hôte : Désactivé

Azure Disk Encryption : Non activé

Disque de système d'exploitation éphémère : N/A

Disques de données : 0

Alaport ou supprimer des données en appuyant sur Ctrl+Shift+F



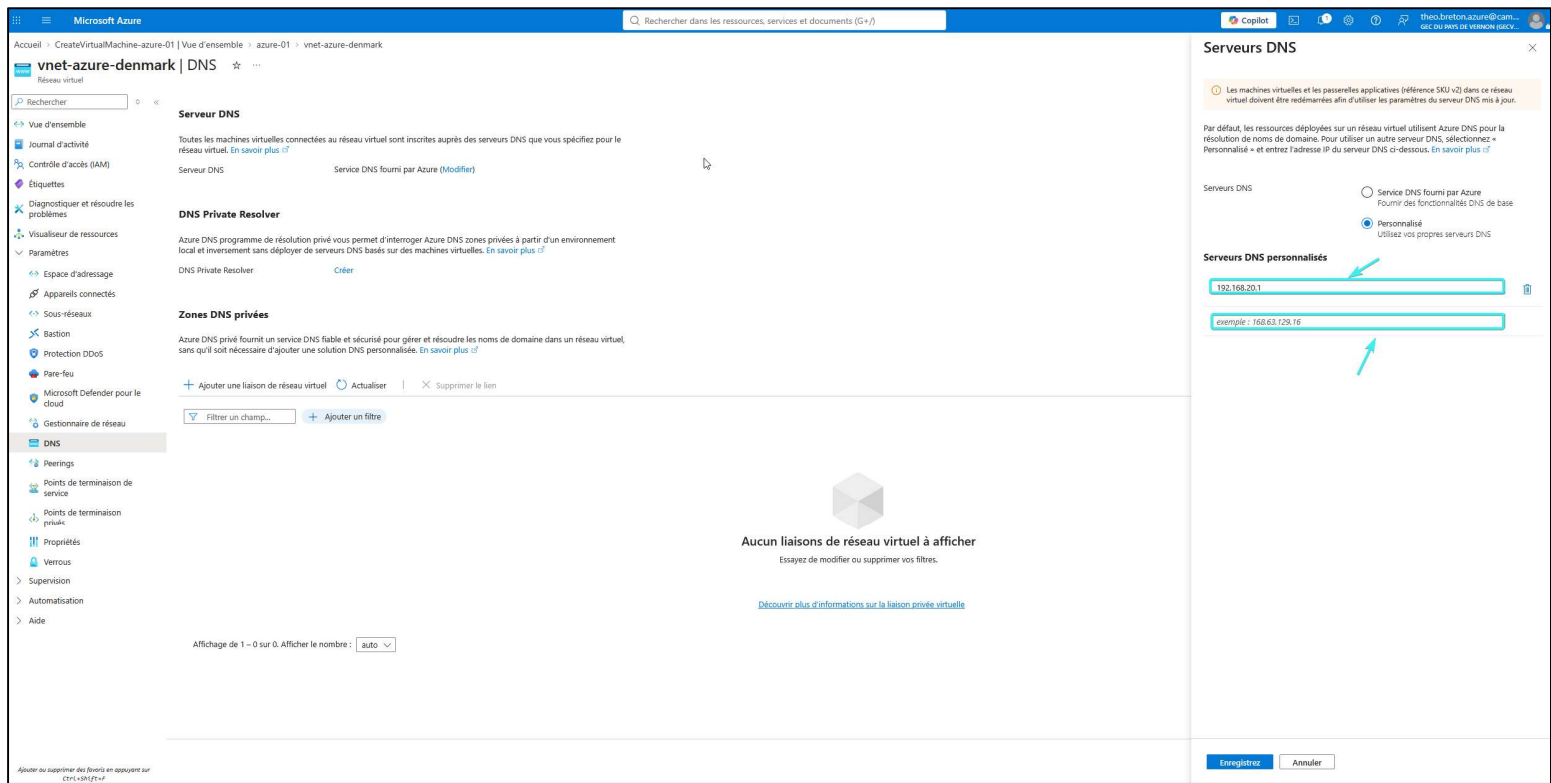
PROJET PERSONNEL – Théo BRETON

PROJET N°14 : MISE EN PLACE D'UNE INFRASTRUCTURE HYBRIDE ENTRE UN HOMELAB MON MICROSOFT AZURE

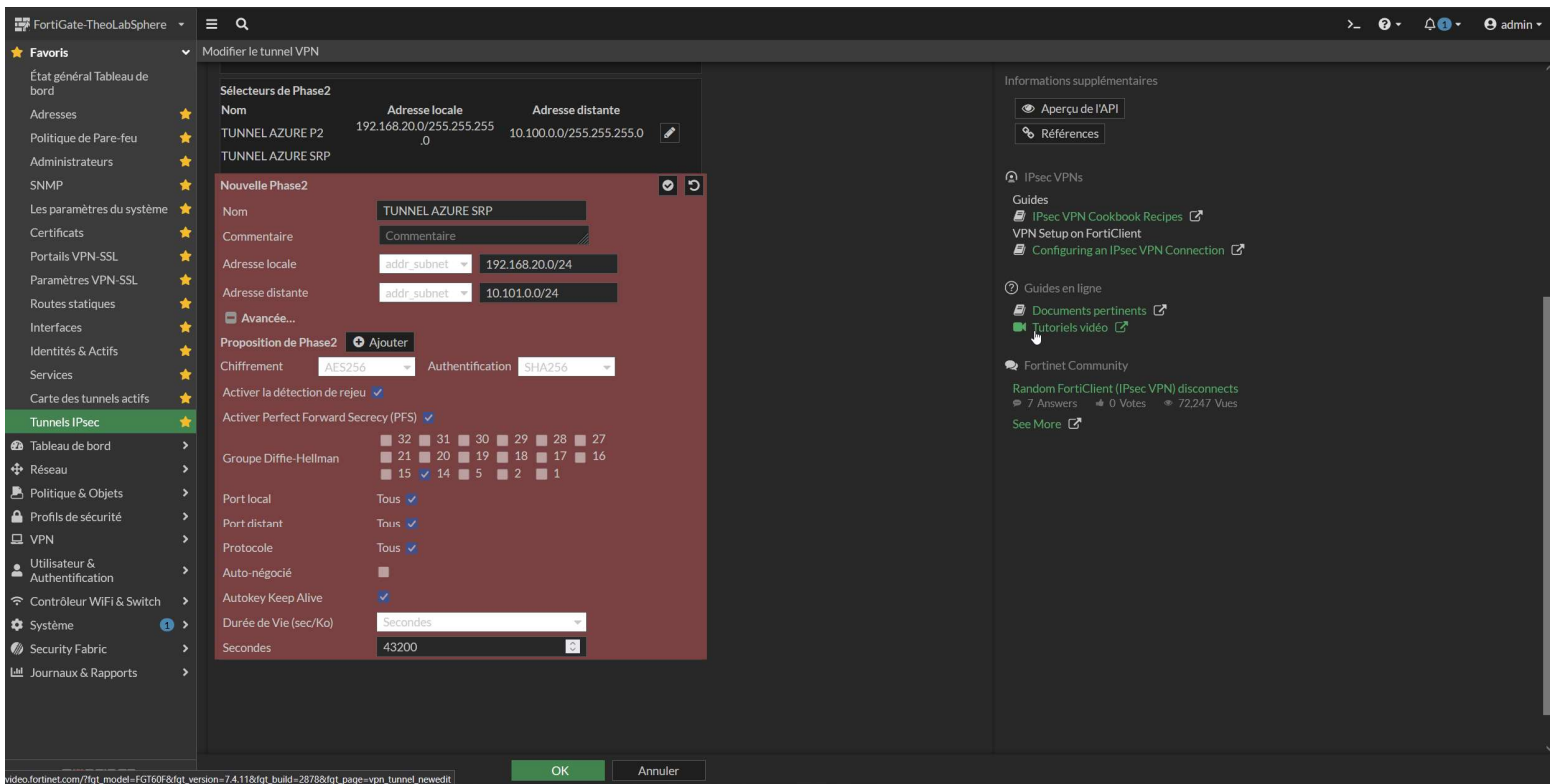
51

Étape 23 : Configuration du DNS du VNet

Faire pointer le DNS du VNet vers 192.168.20.1, le contrôleur de domaine de mon Homelab.



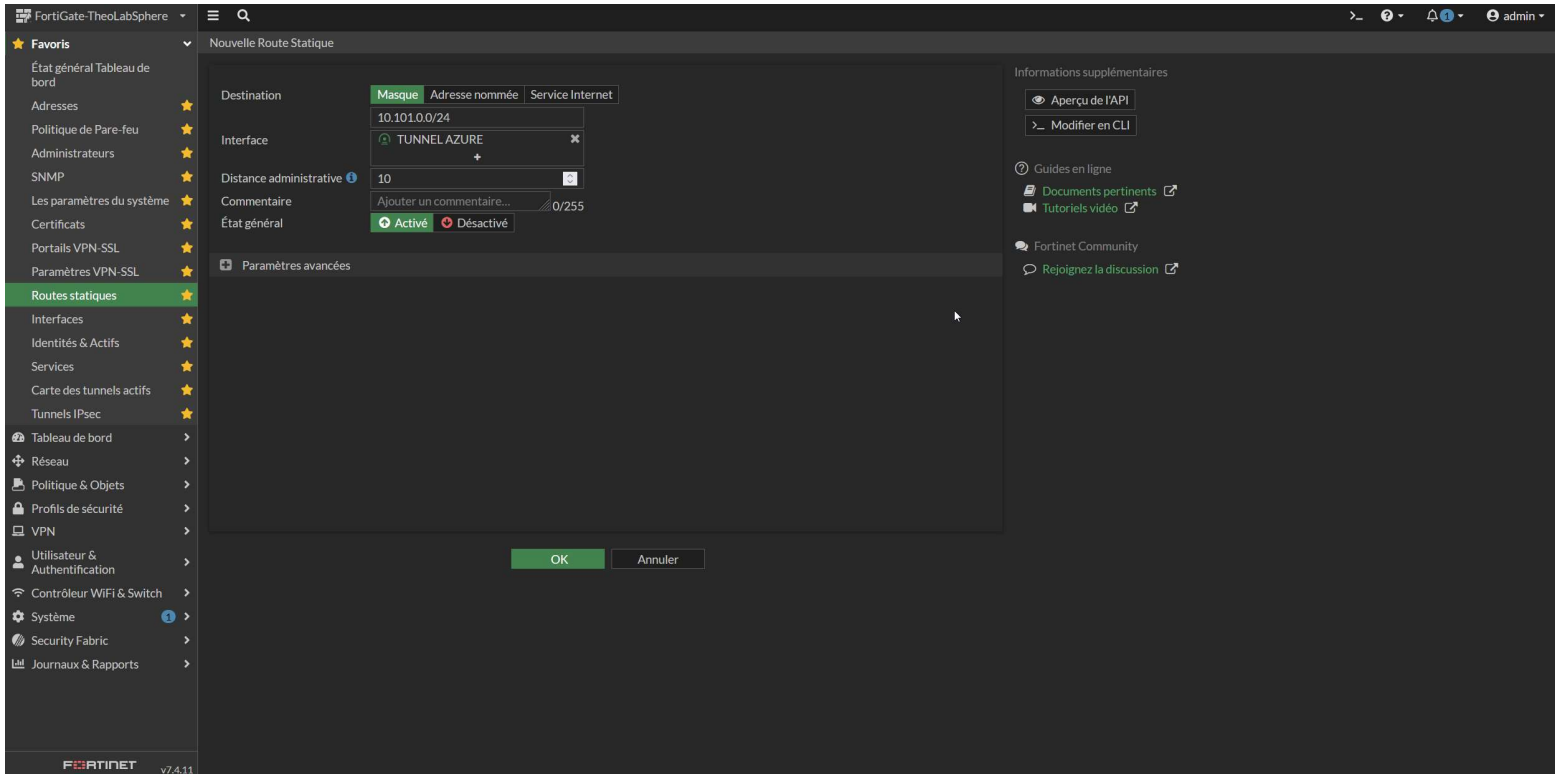
Étape 24 : Ajout du nouveau sous réseau du Danemark au Fortigate :



TUNNEL AZURE	51.11.238.14	51.11.238.14	0B	0B	TUNNEL AZURE	TUNNEL AZURE P2	TUNNEL AZURE SRP
--------------	--------------	--------------	----	----	--------------	-----------------	------------------



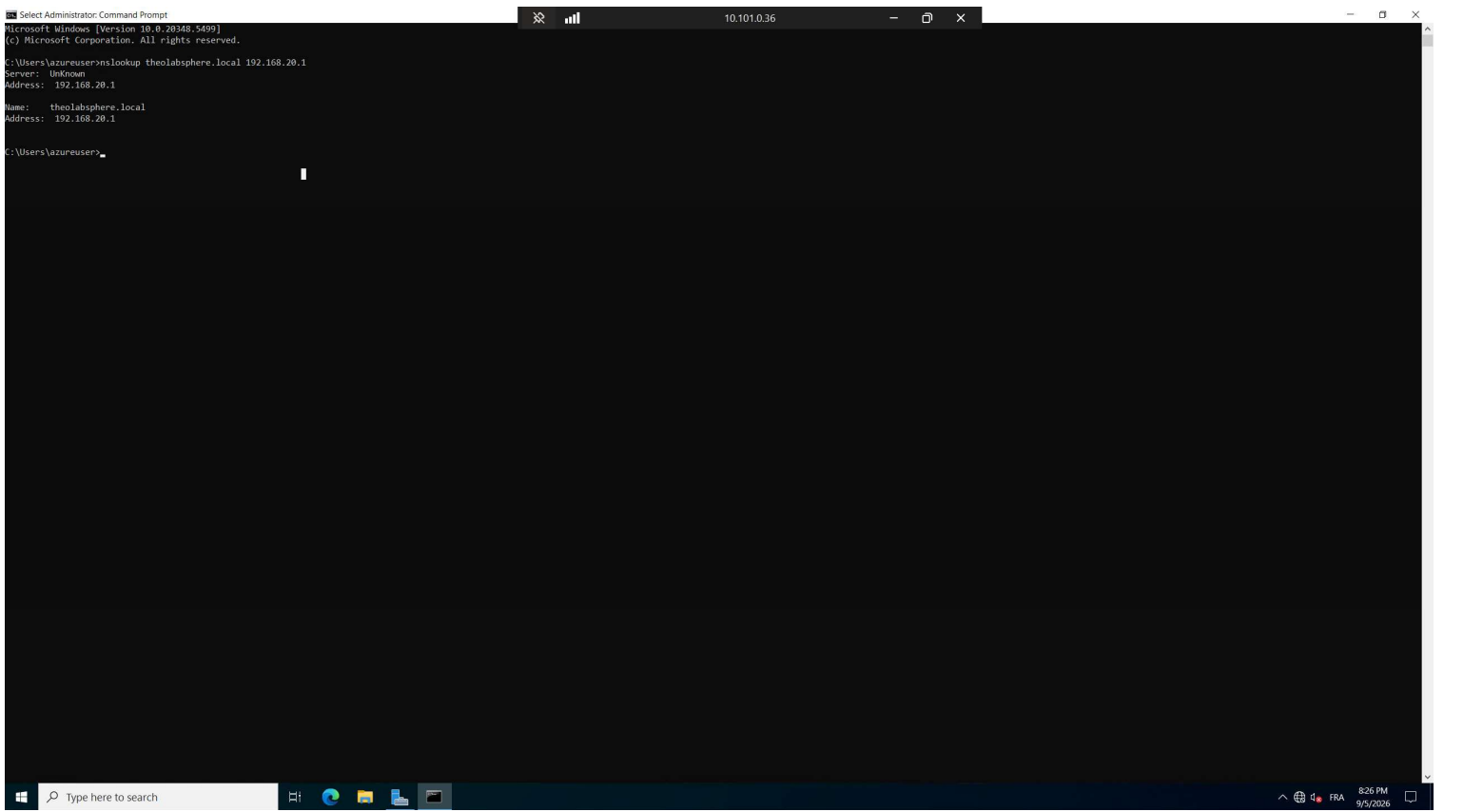
Étape 25 : Ajout de route statique vers le nouveau sous réseau sur le Fortigate



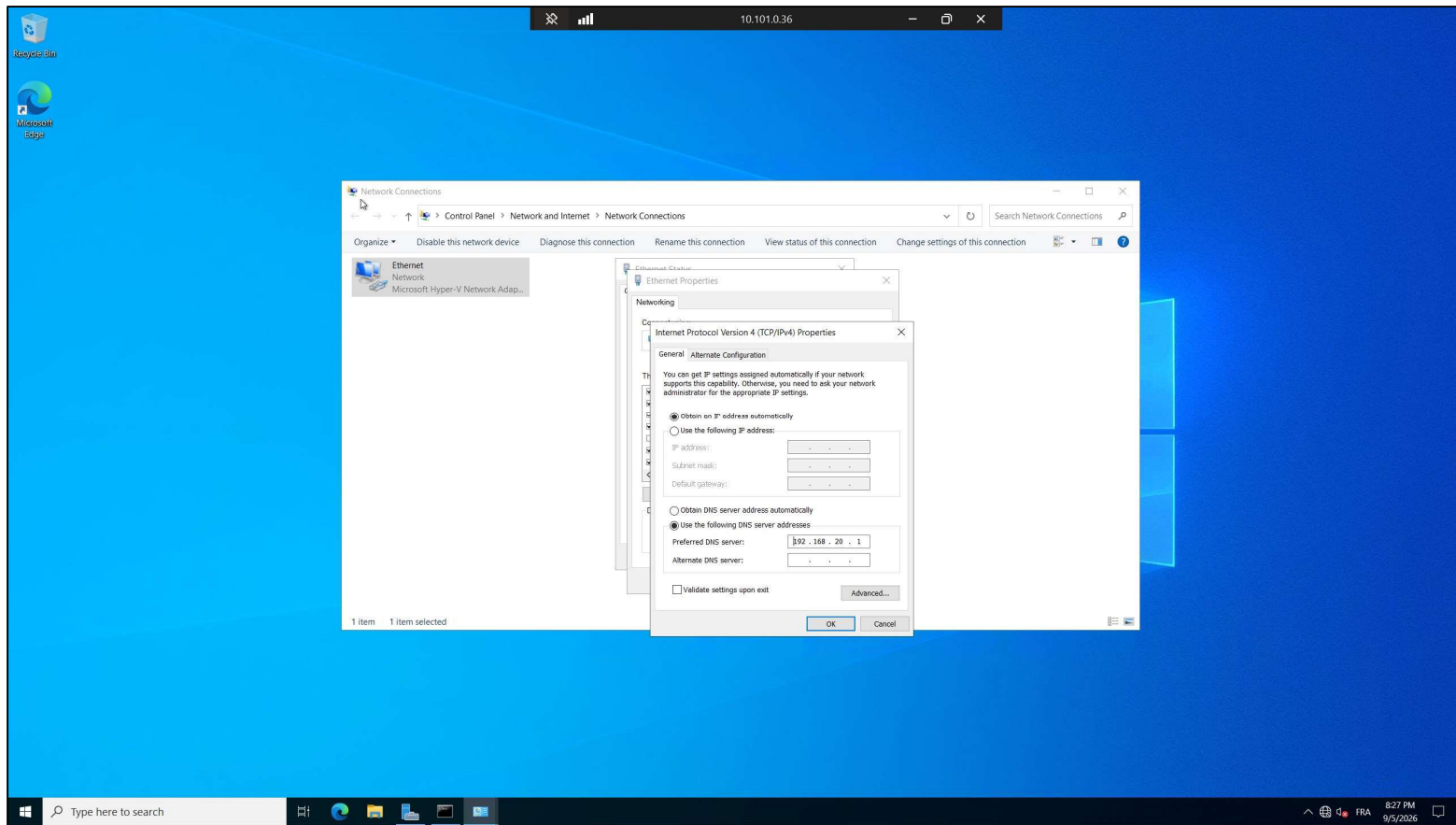
Étape 26 : Jonction de la VM au domaine

Joindre la VM Azure au domaine theolabsphere.local. Cette étape valide l'ensemble de la chaîne technique.

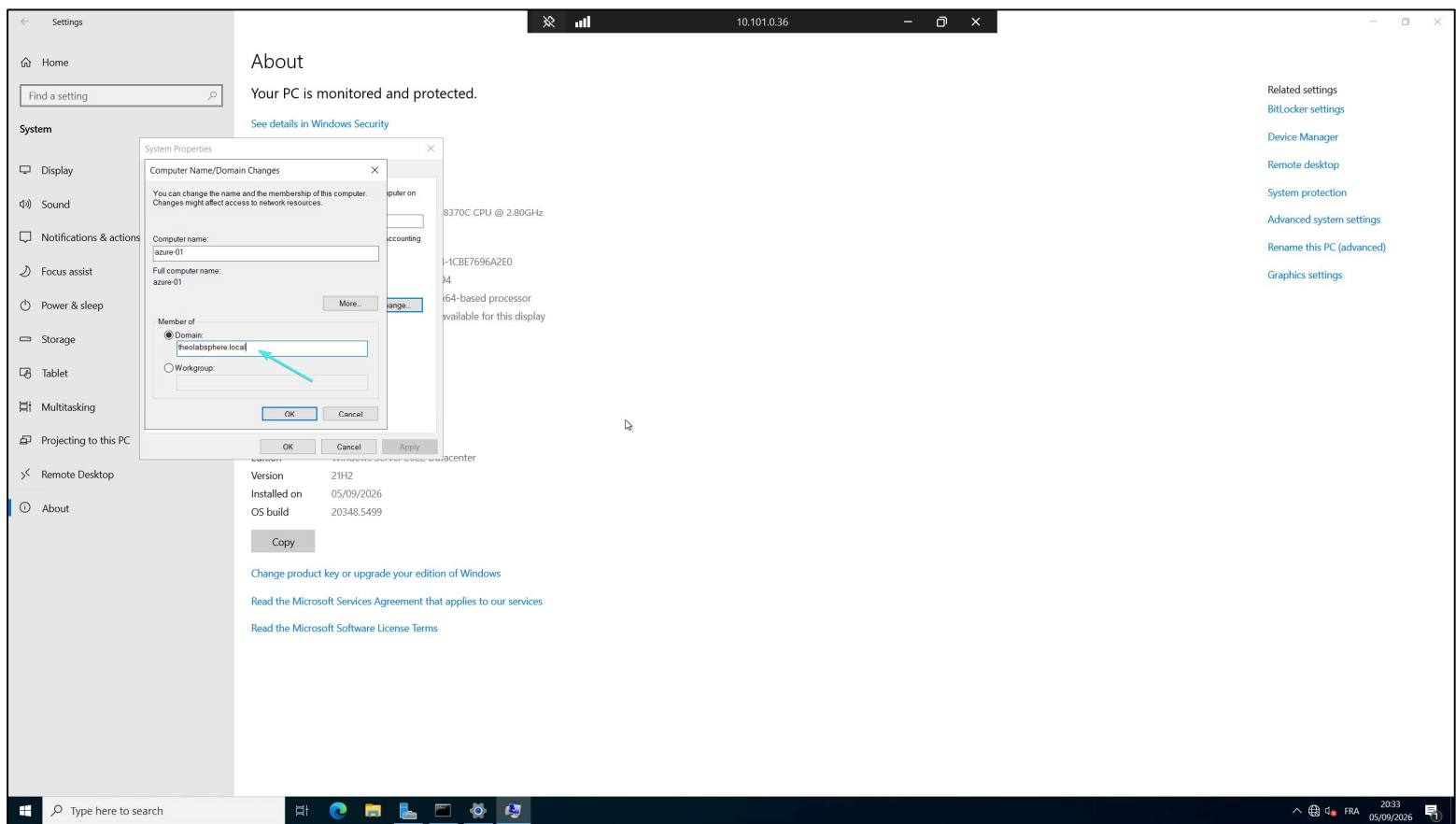
Test de résolution du nom de domaine :



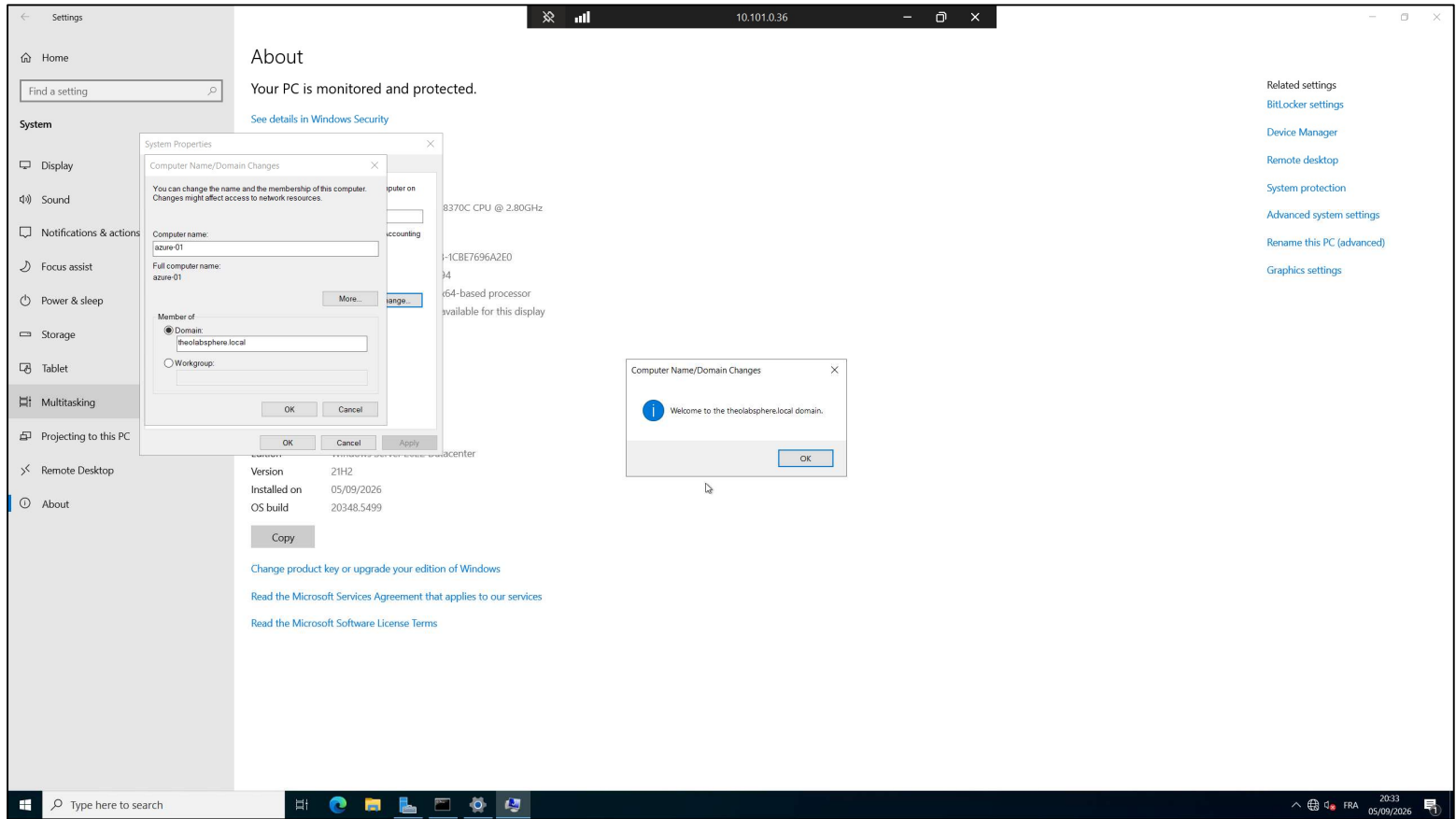
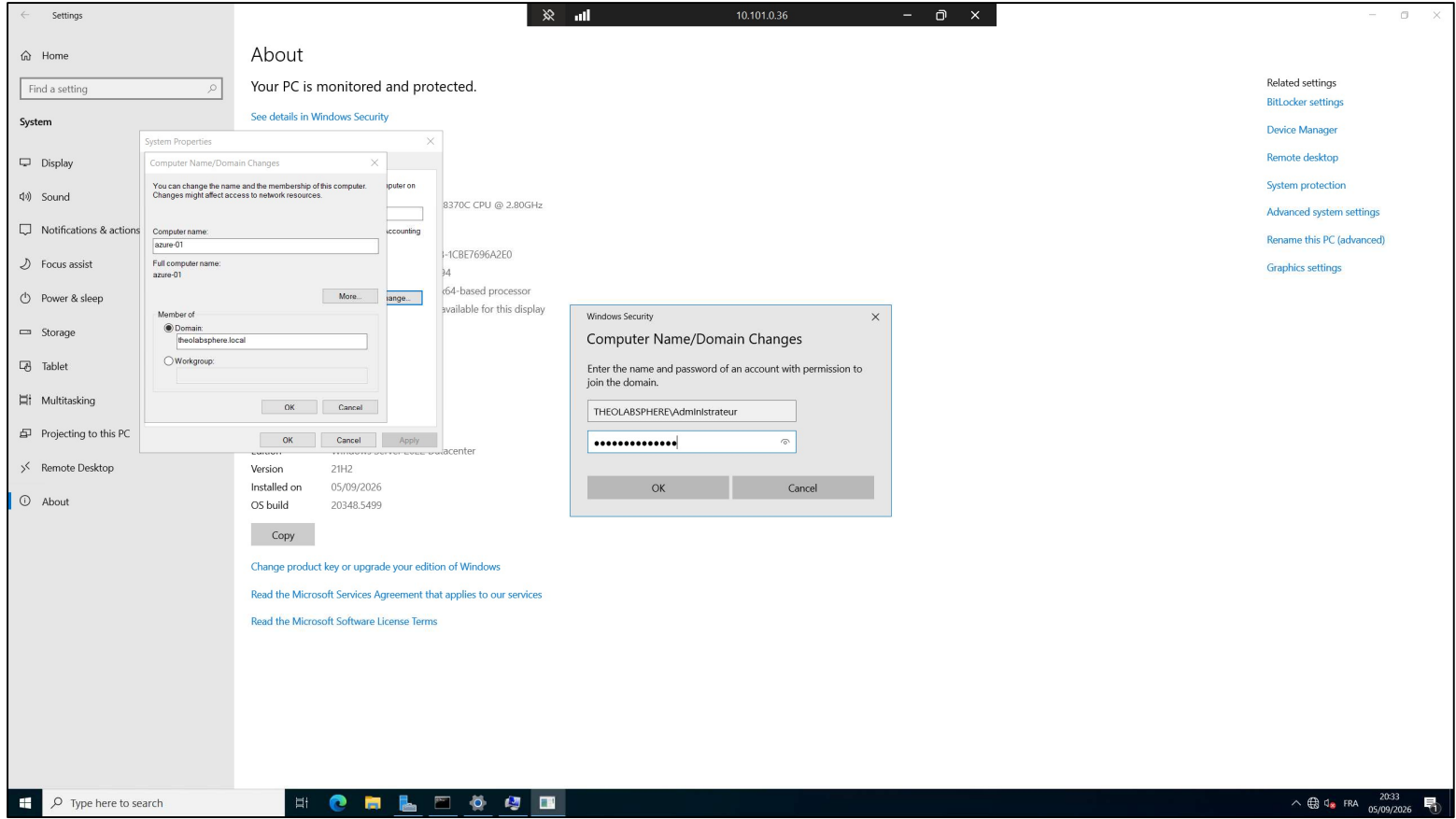
Configuration statique du DNS sur le Serveur Azure :



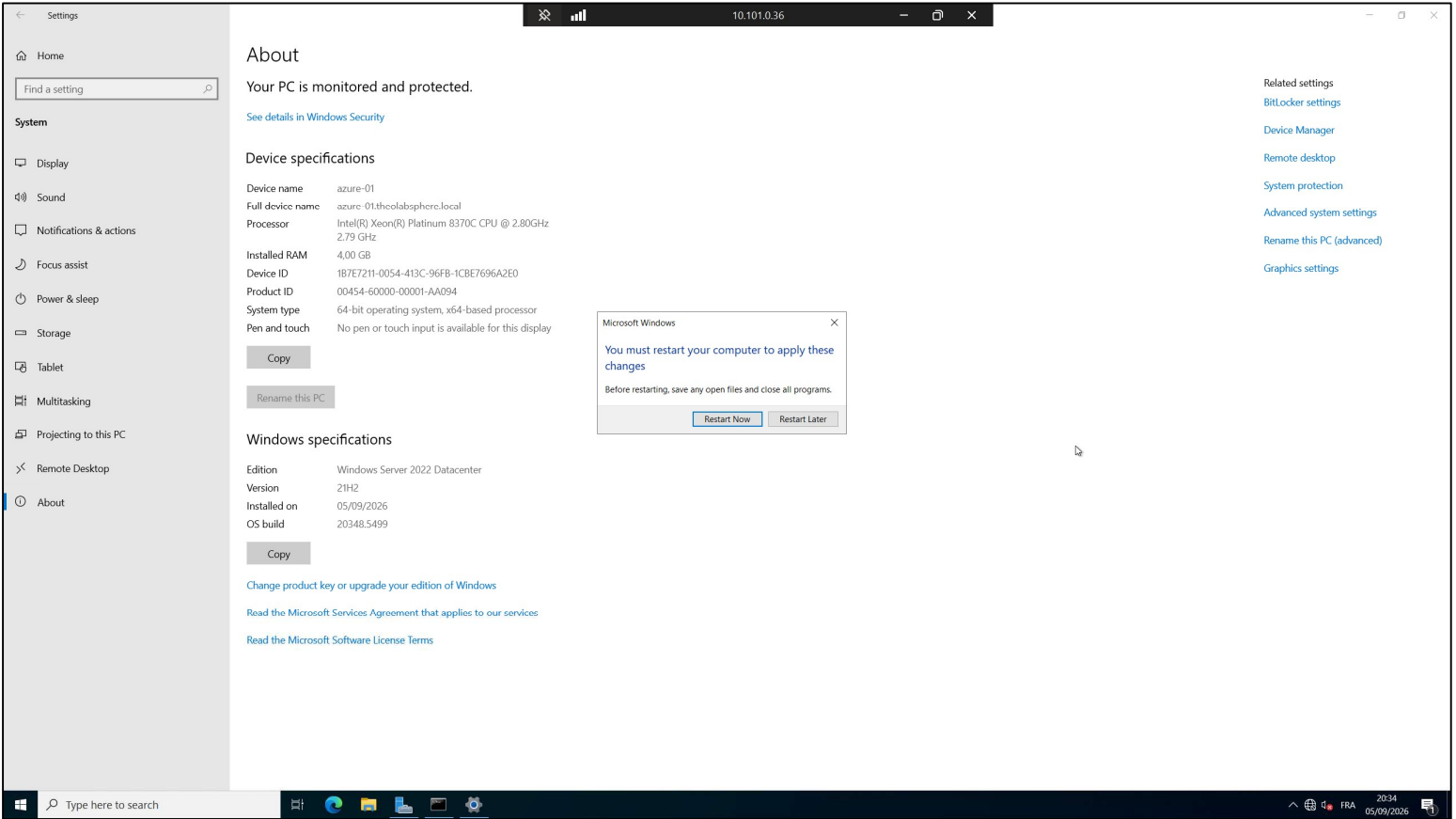
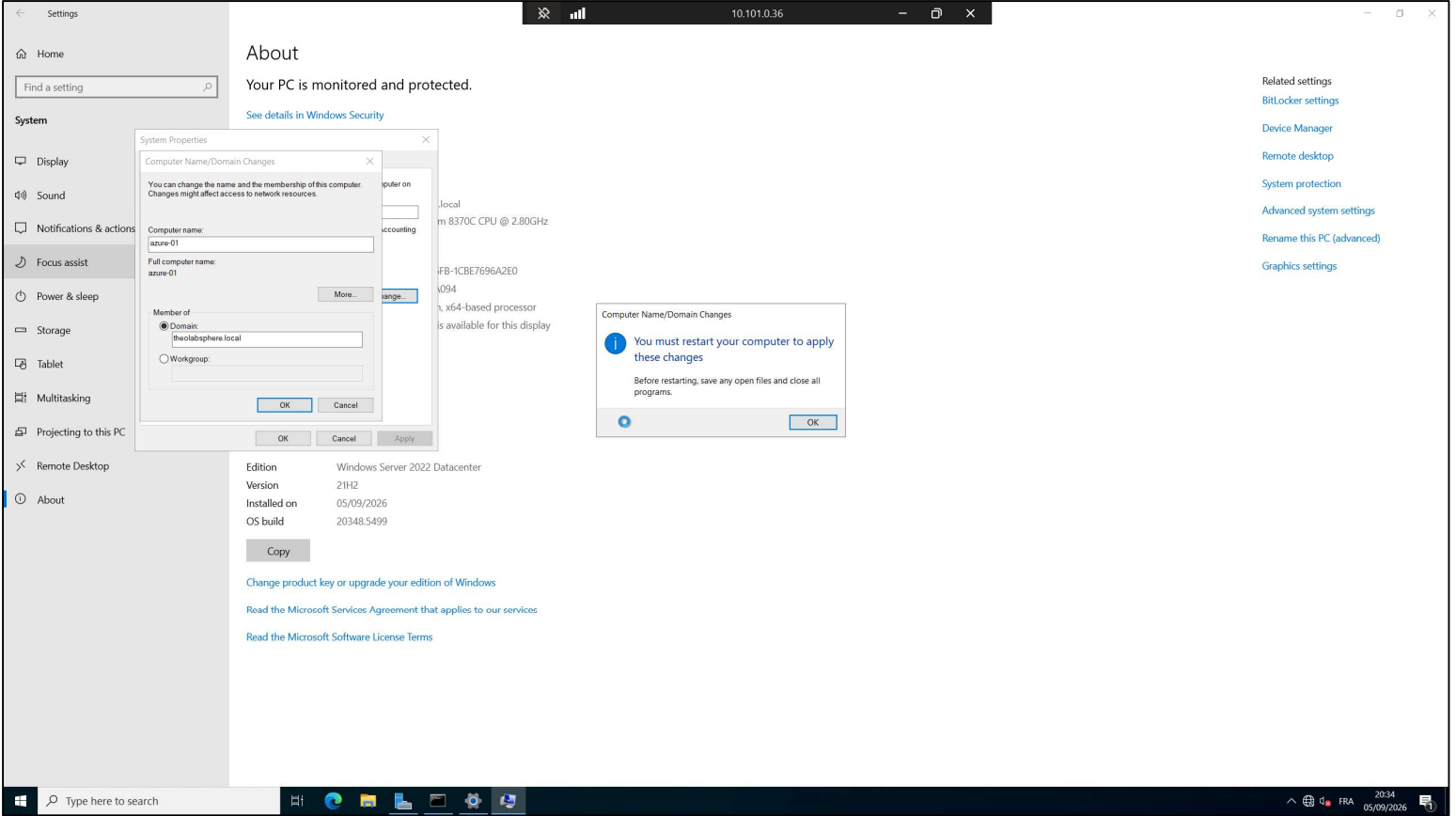
Configuration du domaine sur le serveur :



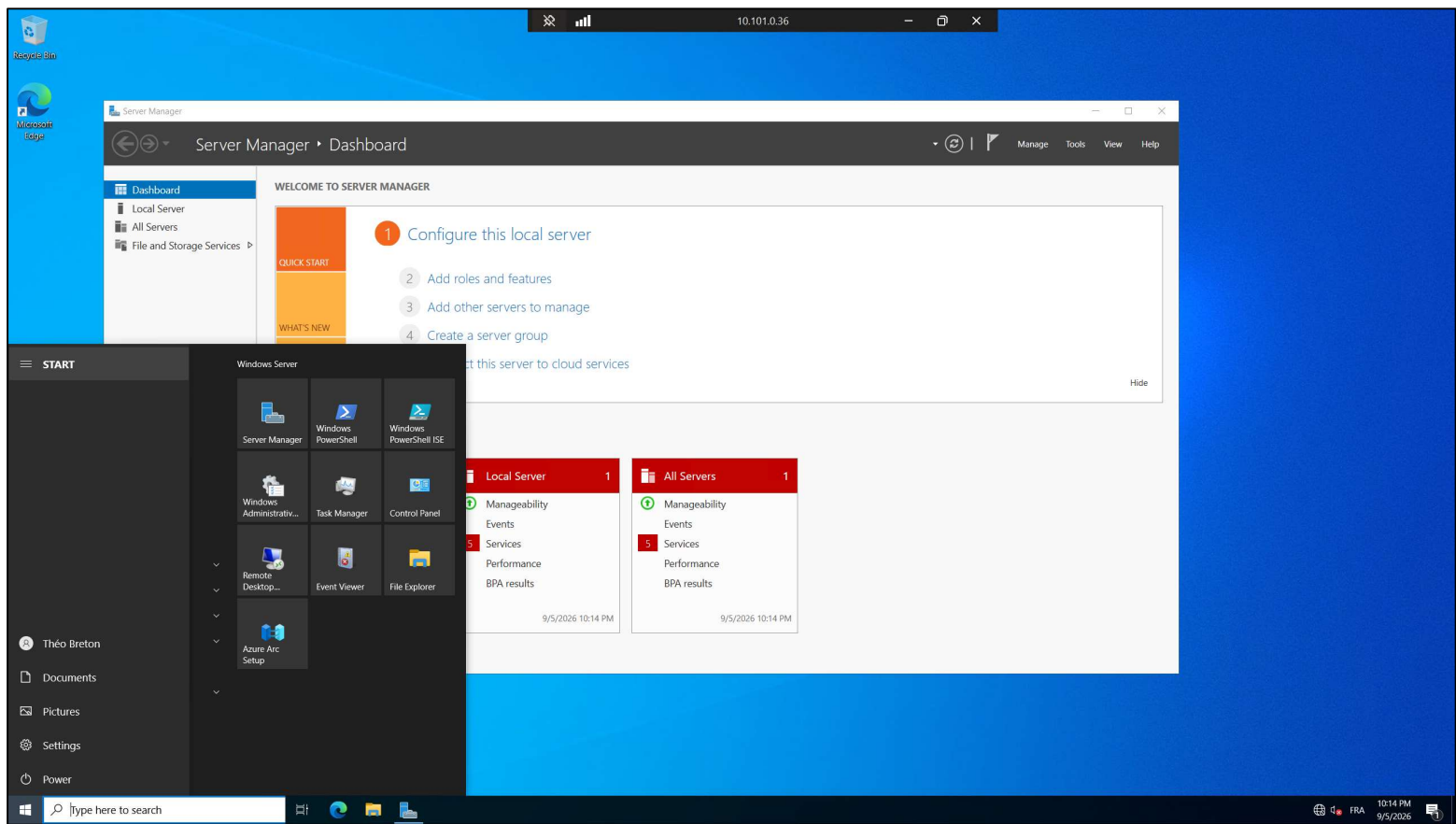
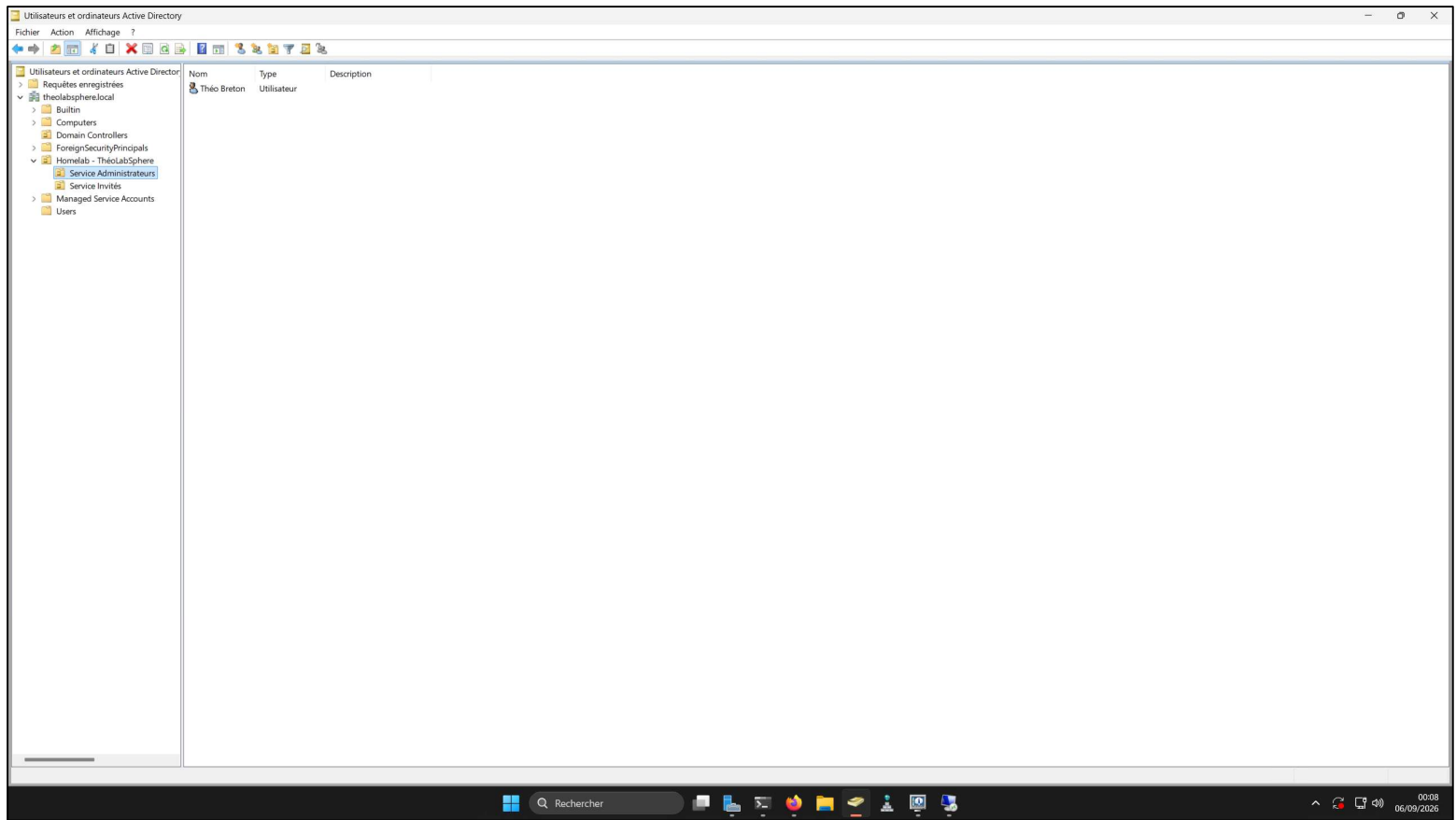
Connexion avec le compte Administrateur du domaine :



Redémarrage de la VM pour appliquer les configuration réalisées :



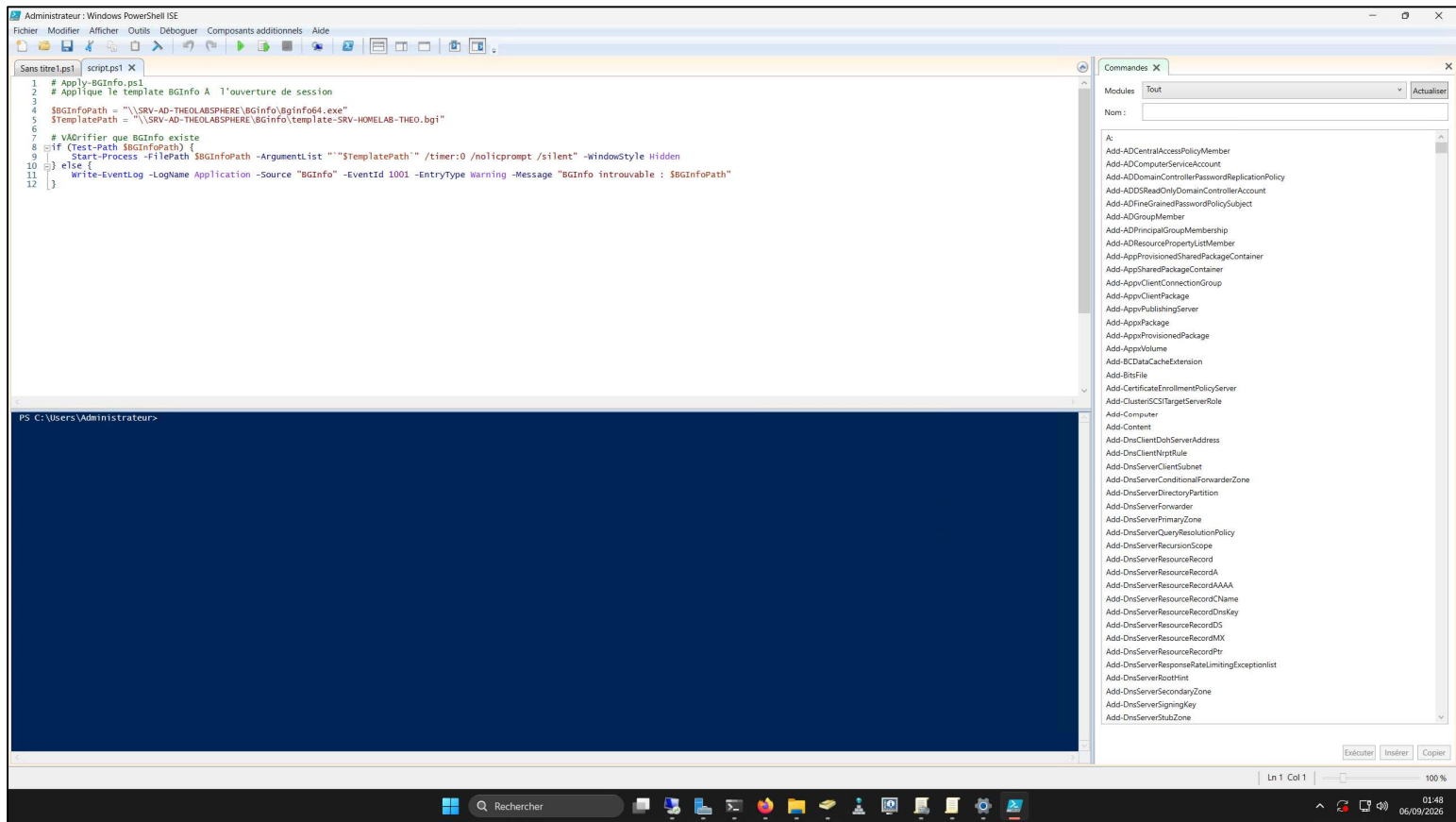
Connexion avec un utilisateur du domaine :



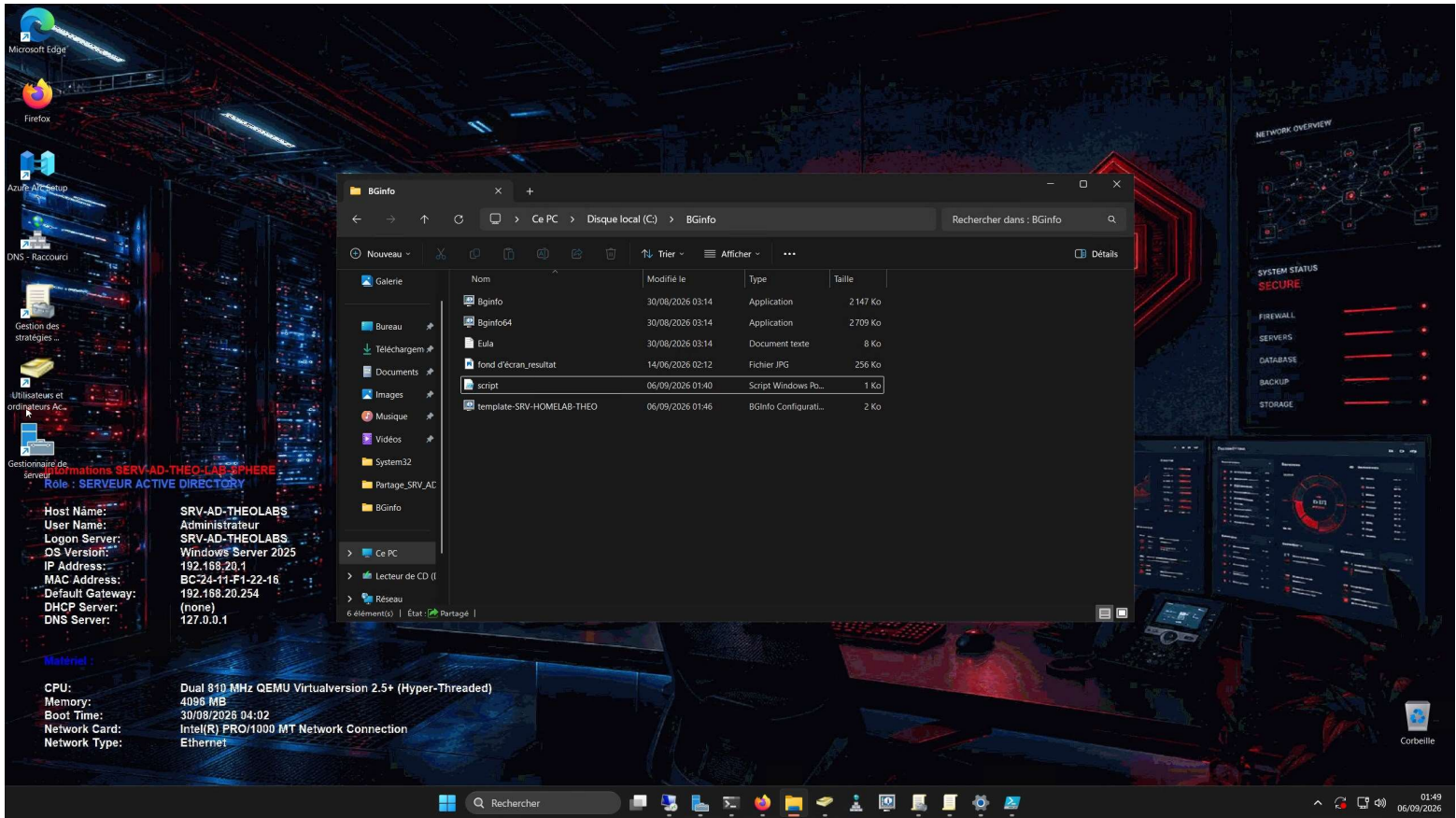
PARTIE 5 : ÉVOLUTIONS

Étape 27 : Appliquer une GPO pour déployer la template BGInfo du Homelab :

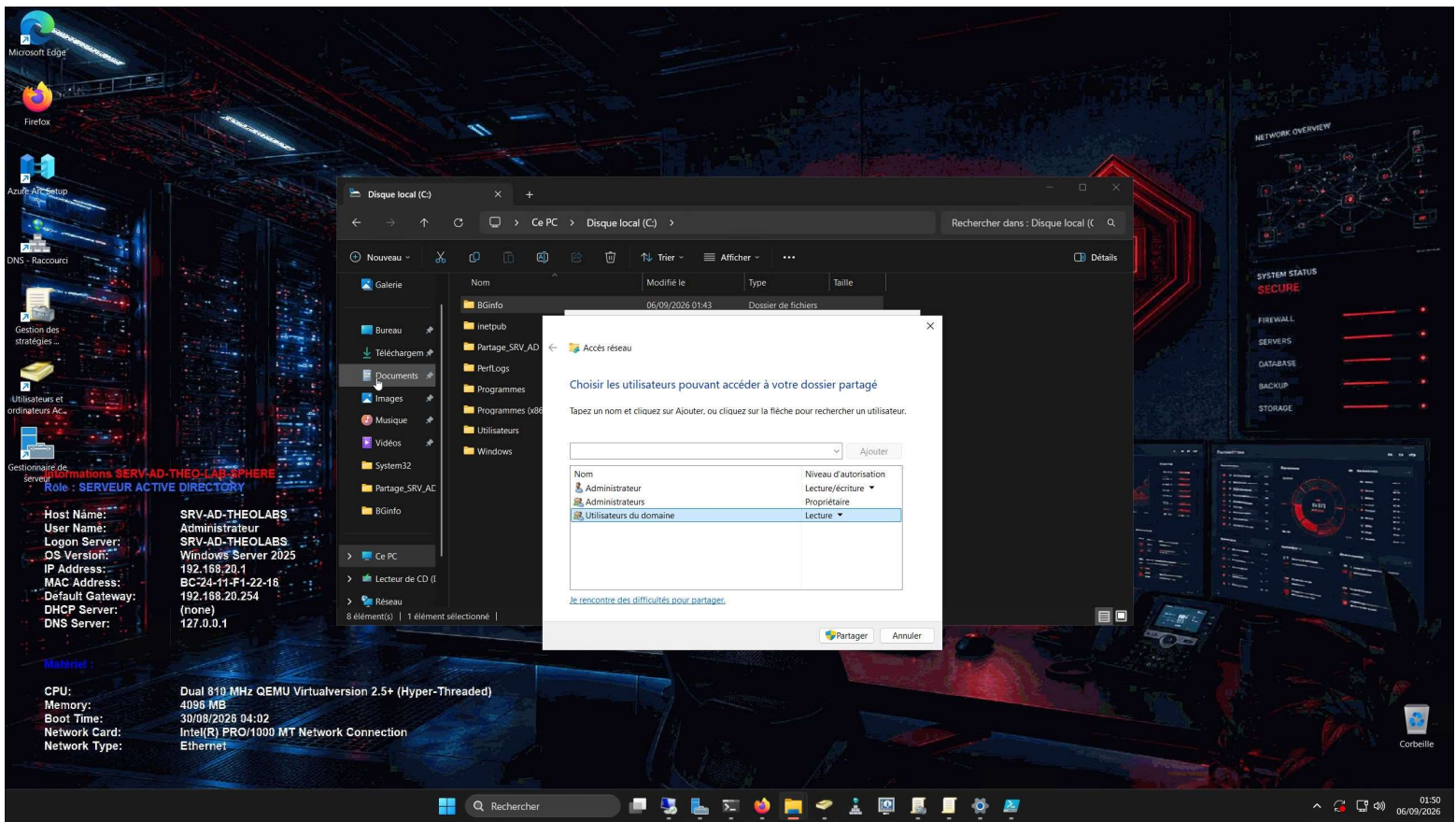
Etablissement du script :



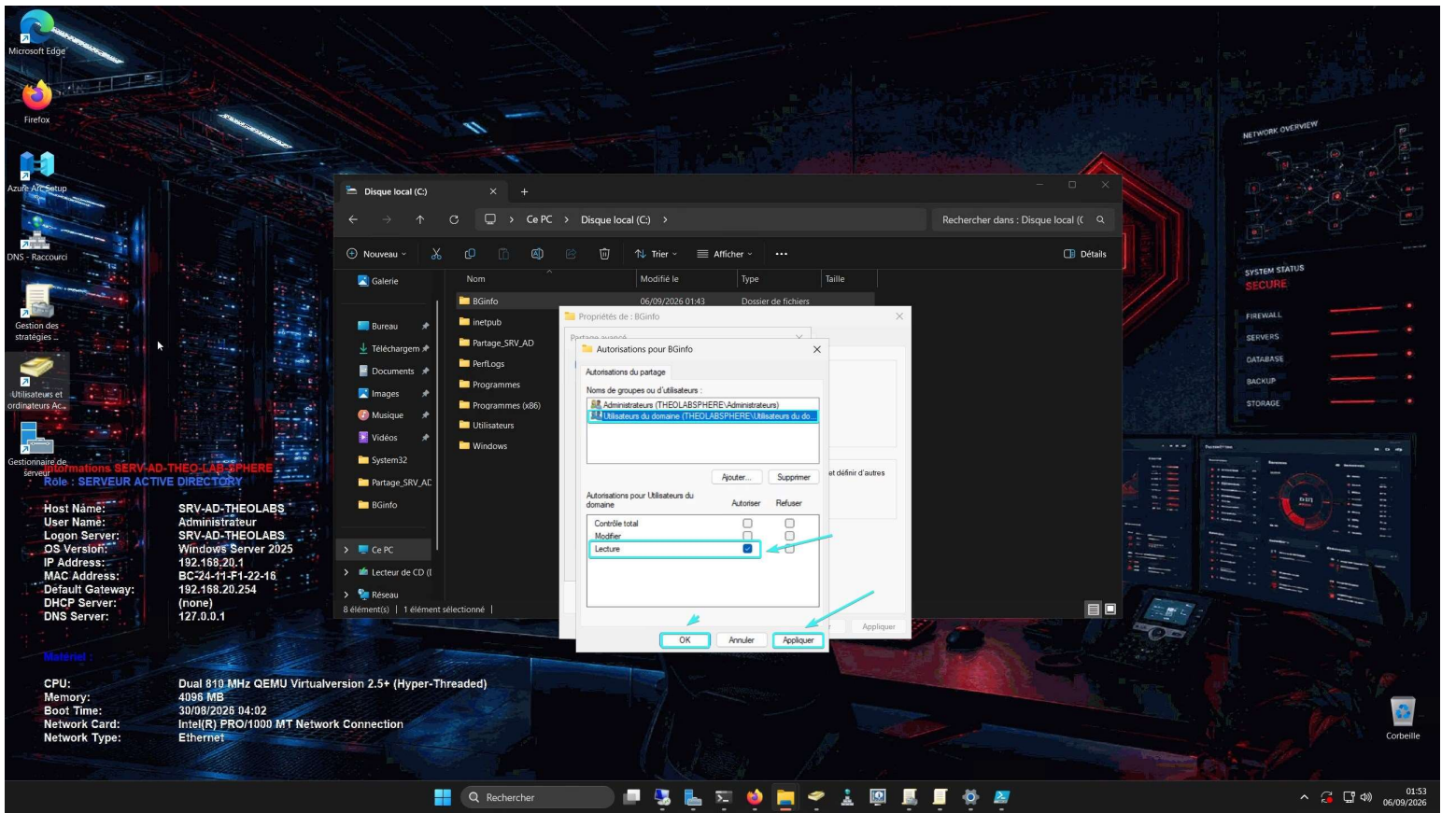
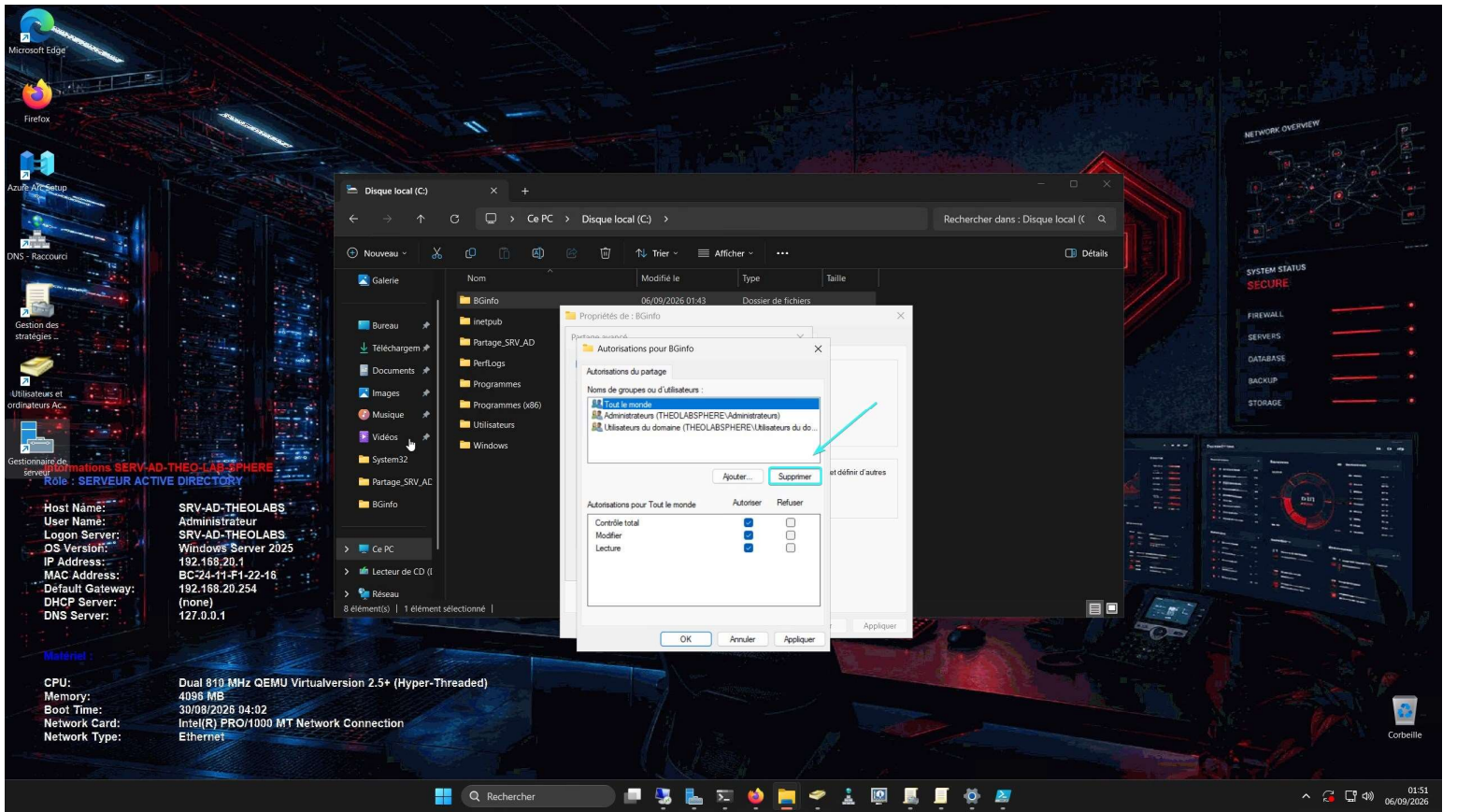
Mettre le logiciel BGInfo et la template dans un dossier partagé :



Avec les utilisateur du domaine en lecture :

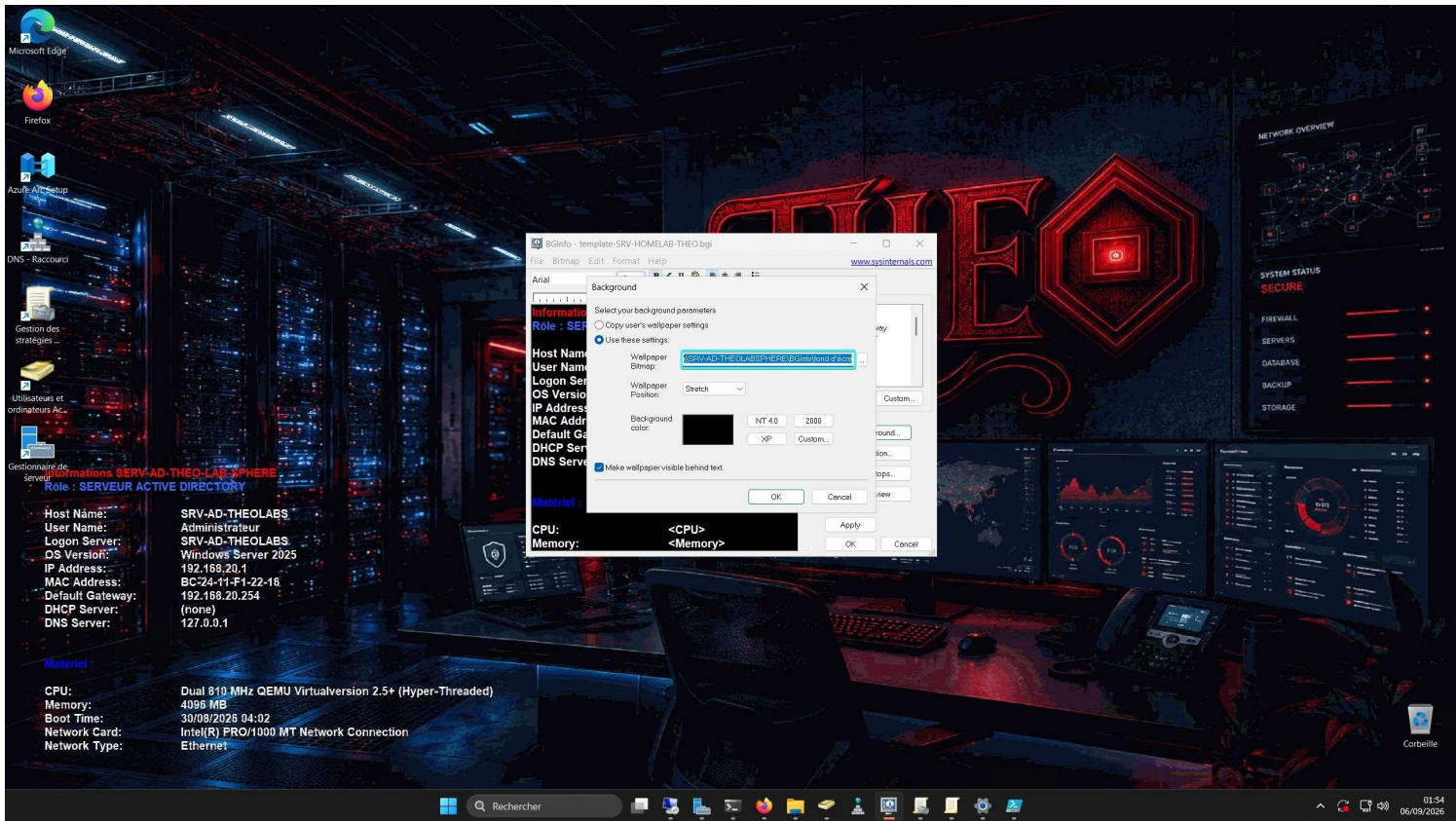


Dans les partages avancée on retire le groupe « Tout le monde » et on ajoute les utilisateurs du domaine toujours en lecture.

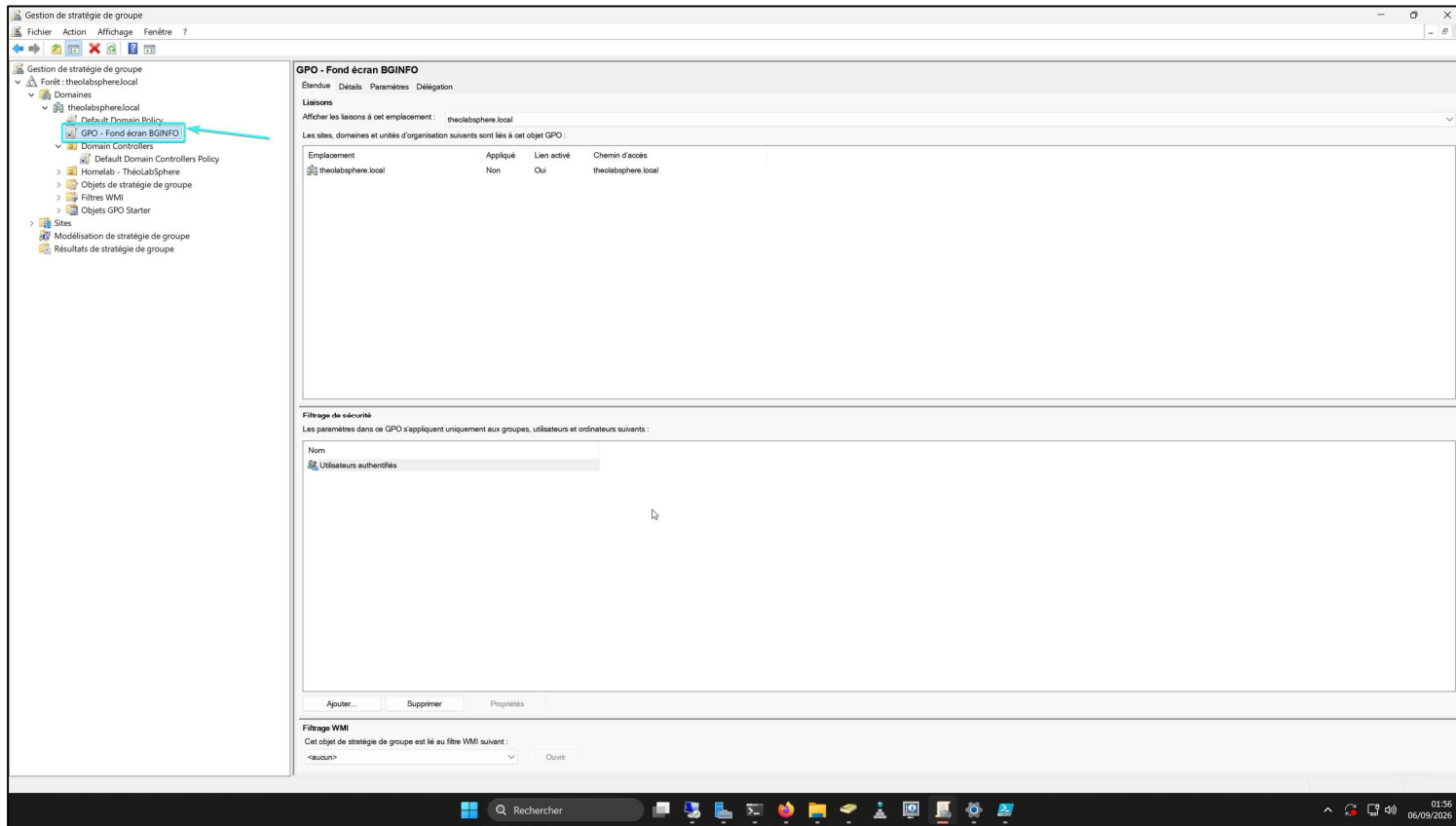


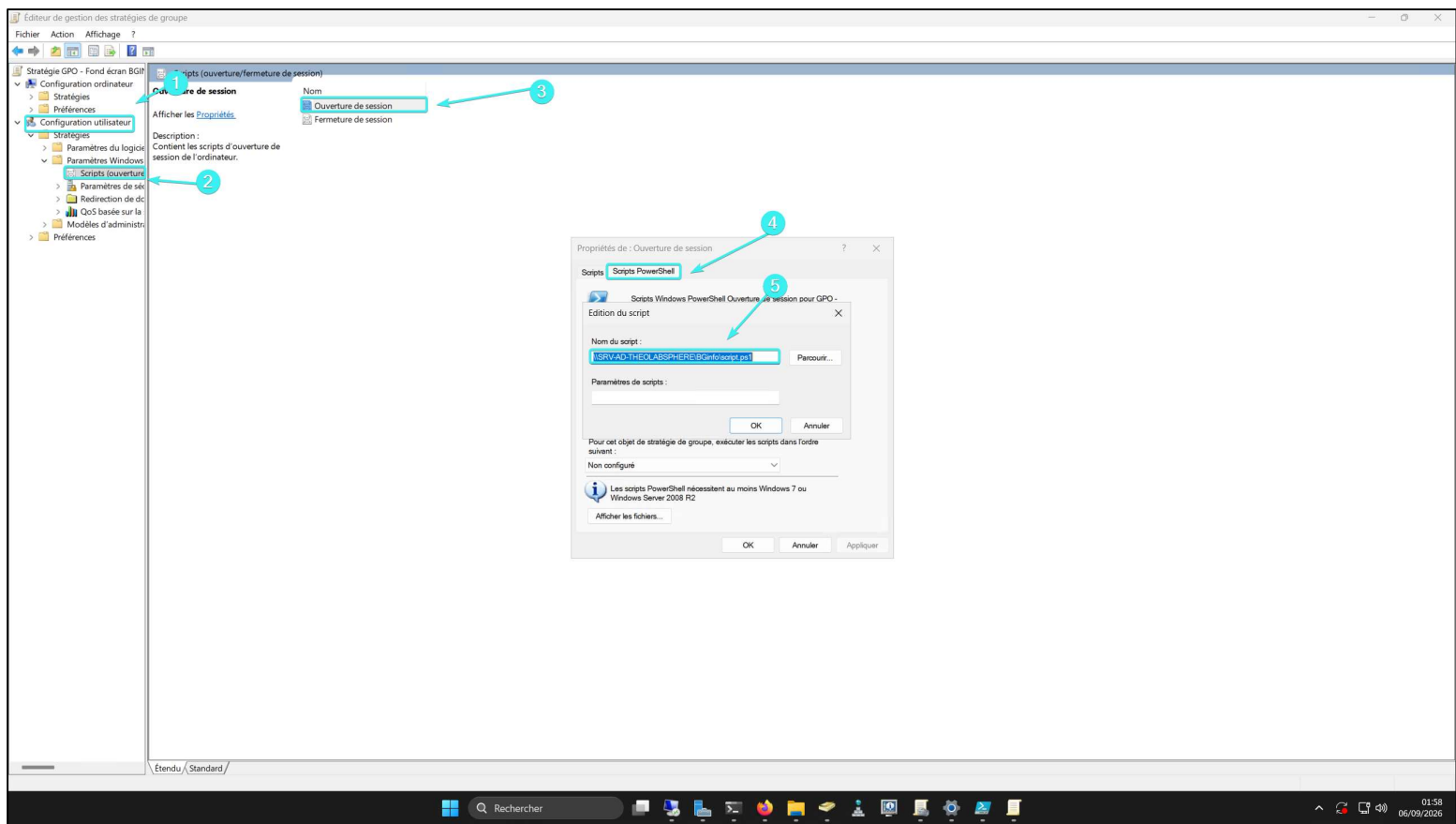
Dans BGInfo on configure le nom du serveur suivi du chemin pour exécuté le fond écran :

\\SRV-AD-THEOLABSPHERE\BGinfo\fond d'écran_resultat.jpg

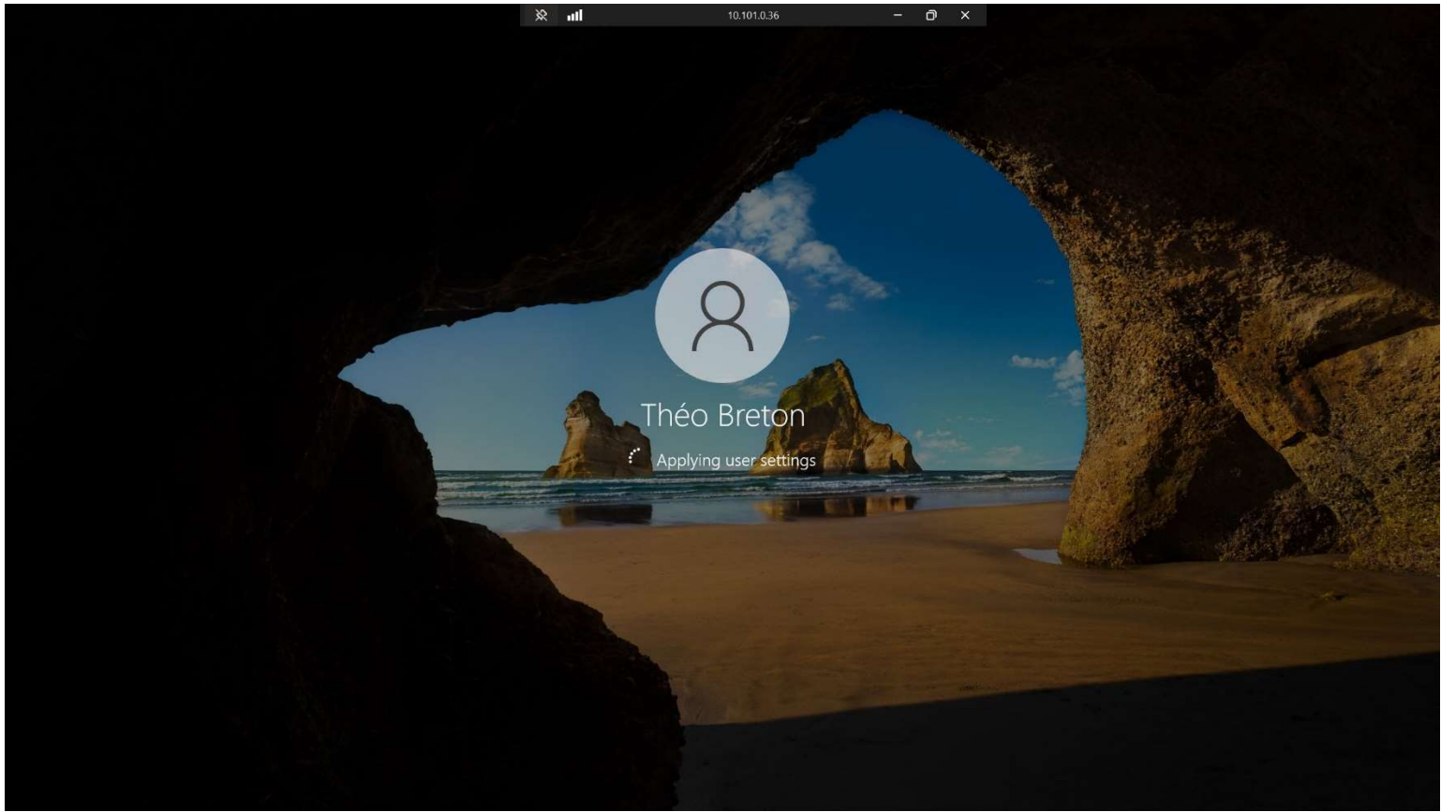


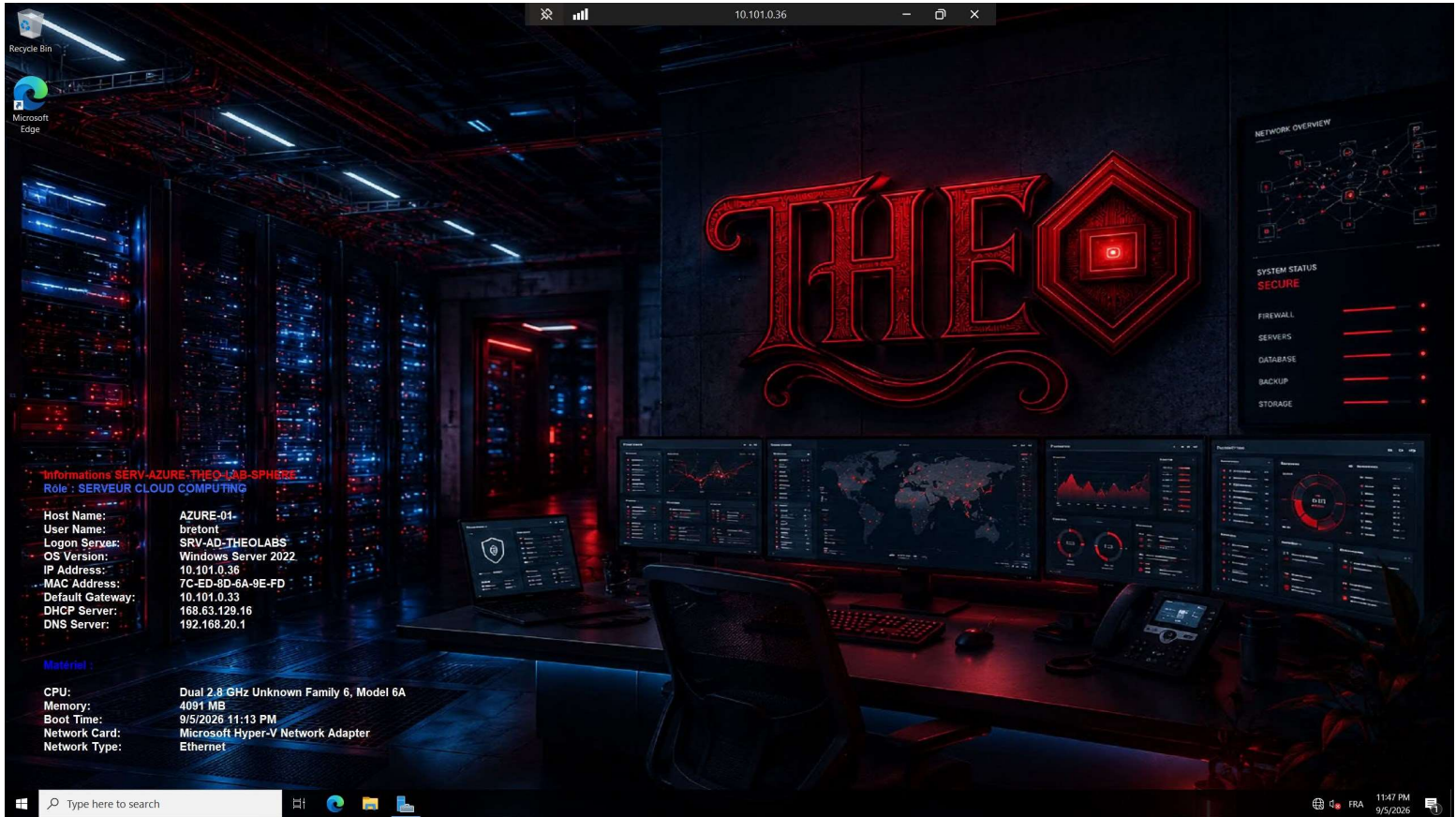
Ensuite on créer un GPO fond d'écran pour les Utilisateurs du domaine :





Test avec un utilisateur du domaine :

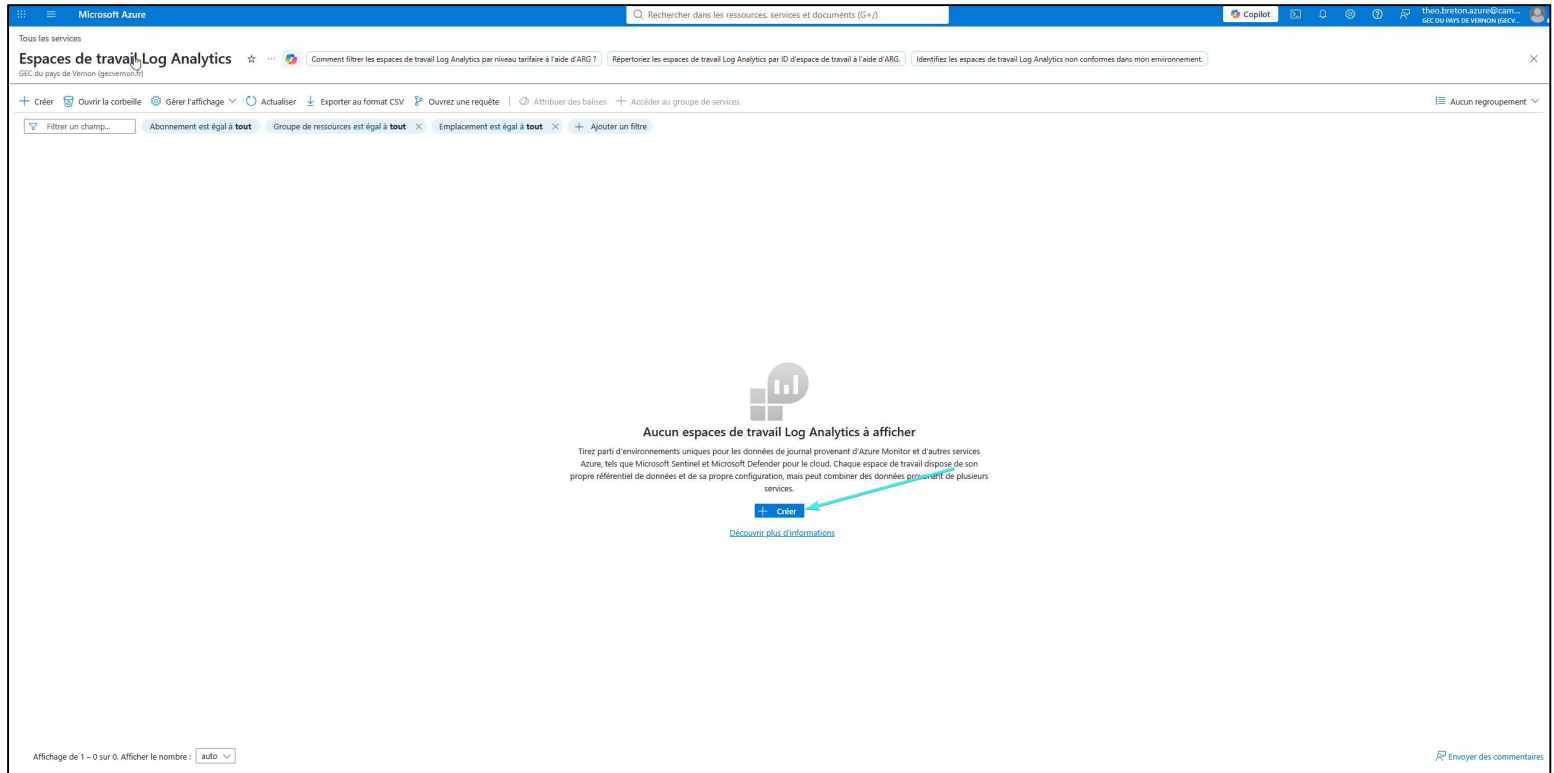




Étape 28 : Ajouter un nouveau poste client dans le homelab à l'AD

Étape 29 : Supervision de sécurité Cloud

Créer un Log Analytics Workspace



Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

Théo.BRETON@univ-brest.fr

Tous les services>Espaces de travail Log Analytics

Créer un espace de travail Log Analytics

Informations de baseBalisesVérifier + créer

L'espace de travail Log Analytics est l'unité de gestion de base des journaux Azure Monitor. Voici certains points à prendre en compte quand vous créez un espace de travail Log Analytics. En savoir plus

Grâce aux journaux Azure Monitor, vous pouvez facilement stocker, conserver et interroger les données collectées à partir de vos ressources supervisées dans Azure et d'autres environnements pour obtenir des insights intéressants. Un espace de travail Log Analytics est l'unité de stockage logique où vos données de journal sont collectées et stockées.

Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement *

Azure for Students

Groupe de ressources *

gr-homelab-hybrid

Détails de l'instance

Nom *

log-theolabsphere

Région *

France Central

Vérifier + créerPrécédentSuivant : Balises >

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

Théo.BRETON@univ-brest.fr

Tous les services>Espaces de travail Log Analytics

Créer un espace de travail Log Analytics

Informations de baseBalisesVérifier + créer

Espace de travail Log Analytics

par Microsoft Corporation

Informations de base

Abonnement

Azure for Students

Groupe de ressources

gr-homelab-hybrid

Nom

log-theolabsphere

Région

France Central

Tarifs

Niveau tarifaire

Paiement à l'utilisation (par Go 2018)

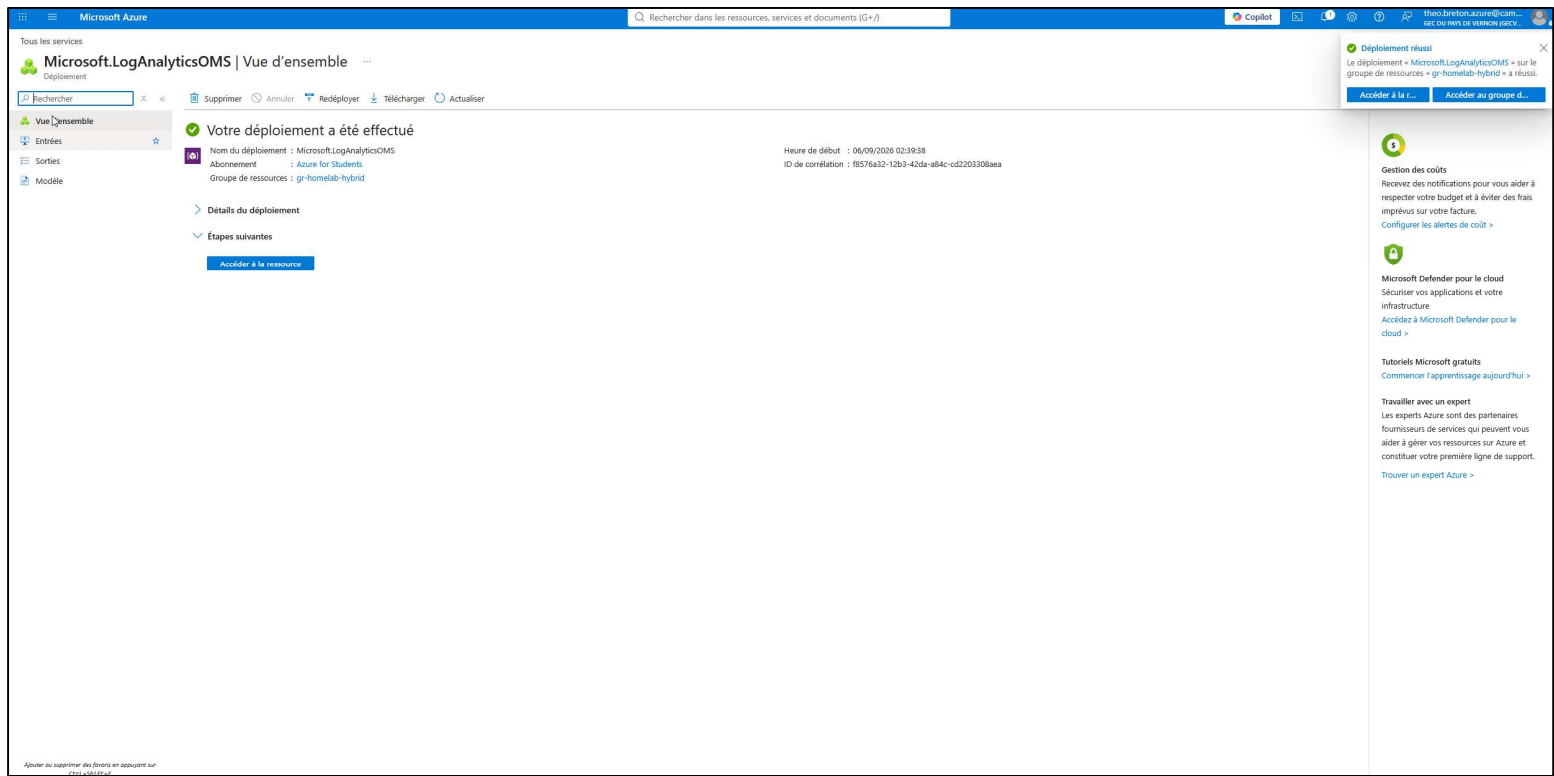
Le coût de votre espace de travail dépend du volume de données ingérées et de leur durée de conservation. Les détails de la tarification régionale sont disponibles sur le site page de tarification Azure Monitor. Vous pouvez passer à un niveau tarifaire différent après la création de l'espace de travail. En savoir plus sur les modèles tarifaires Log Analytics.

Balises

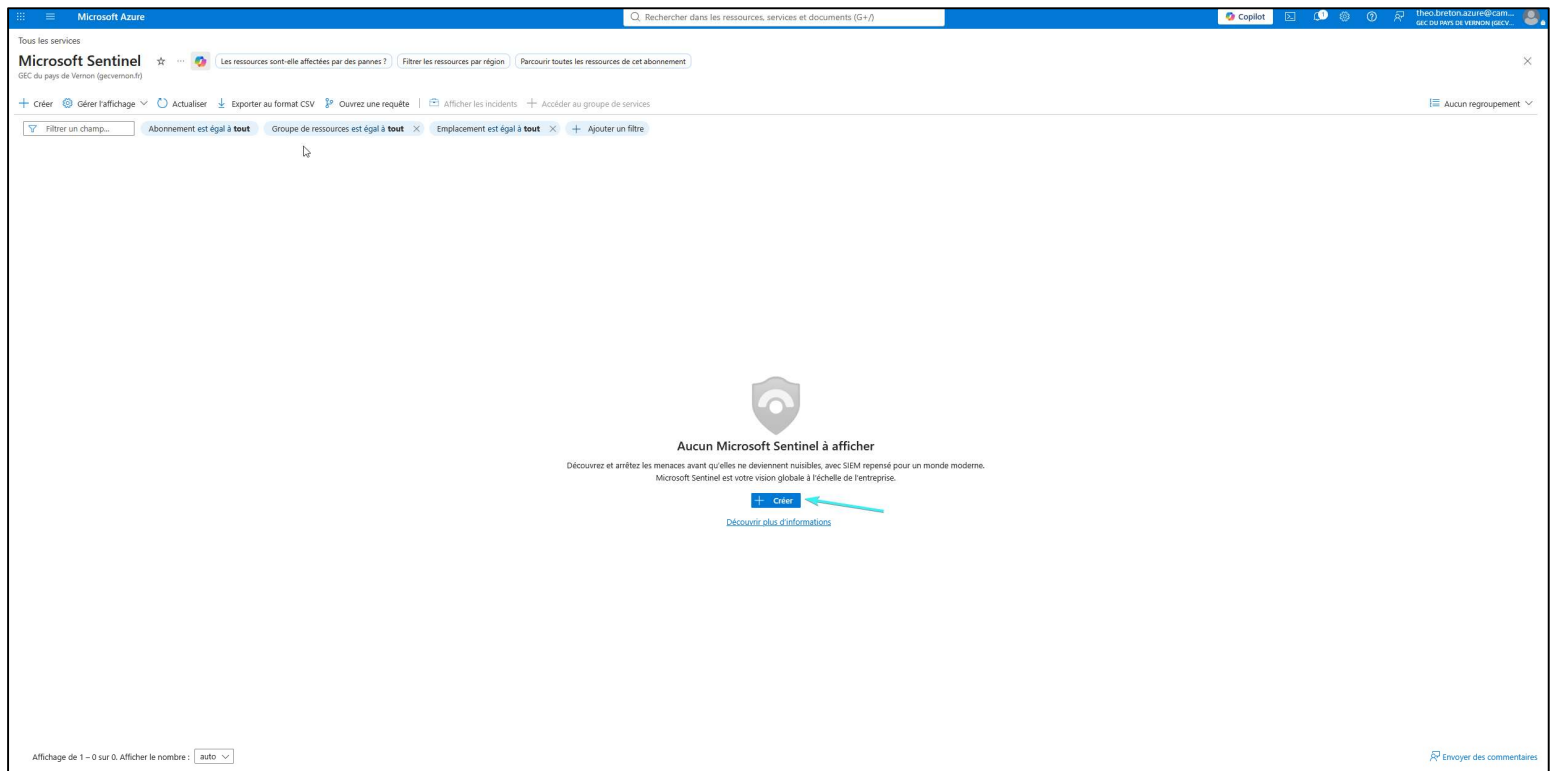
Aucun

CréerPrécédentTélécharger un modèle pour automation





Activer Microsoft Sentinel



Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

theo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...)

Tous les services > Microsoft Sentinel

Ajouter Microsoft Sentinel à un espace de travail ...

+ Créer un espace de travail

Actualiser

Microsoft Sentinel offre un essai gratuit de 31 jours. Pour plus d'informations, consultez le [tarification Microsoft Sentinel](#).

Les nouveaux espaces de travail Microsoft Sentinel créés par des utilisateurs autorisés sont automatiquement intégrés et redirigés vers le portail Defender. [Découvrez plus d'informations](#)

Filterer par nom...

Espace de travail ↑↓	Emplacement ↑↓	ResourceGroup ↑↓	Abonnement ↑↓	Annuaire ↑↓
log-theolabsphere	francecentral	gr-homelab-hybrid	Azure for Students	GEC du pays de Vernon

Ajouter

Annuler

Microsoft Azure

Rechercher dans les ressources, services et documents (G+/I)

Copilot

theo.breton.azure@cam...
GEC DU PAYS DE VERNON (GECV...)

Tous les services > Microsoft Sentinel

Ajouter Microsoft Sentinel à un espace de travail ...

+ Créer un espace de travail

Actualiser

Microsoft Sentinel offre un essai gratuit de 31 jours. Pour plus d'informations, consultez le [tarification Microsoft Sentinel](#).

Les nouveaux espaces de travail Microsoft Sentinel créés par des utilisateurs autorisés sont automatiquement intégrés et redirigés vers le portail Defender. [Découvrez plus d'informations](#)

Filterer par nom...

Espace de travail ↑↓	Emplacement ↑↓	ResourceGroup ↑↓	Abonnement ↑↓	Annuaire ↑↓
log-theolabsphere	francecentral	gr-homelab-hybrid	Azure for Students	GEC du pays de Vernon

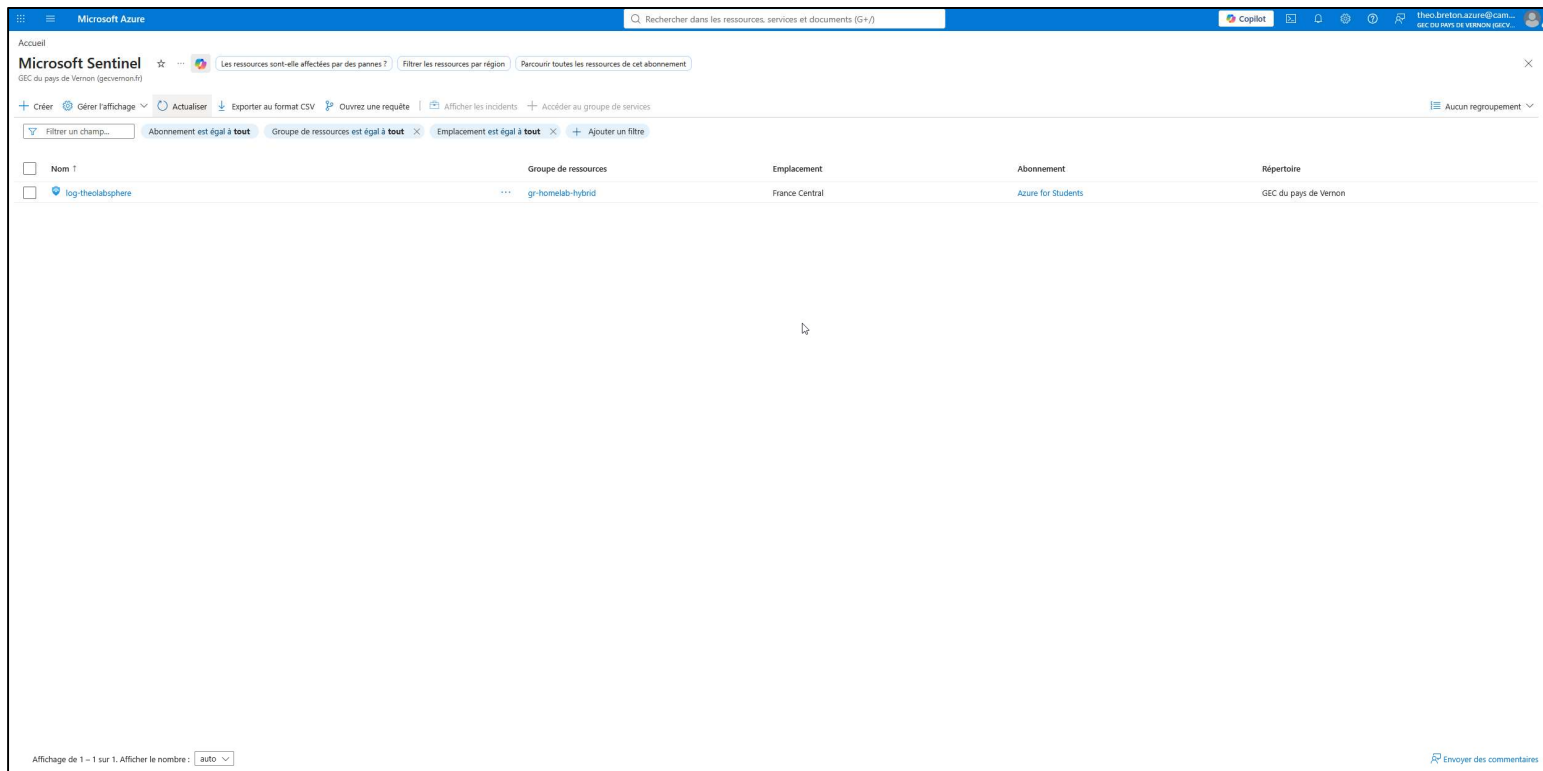
Ajouter

Annuler

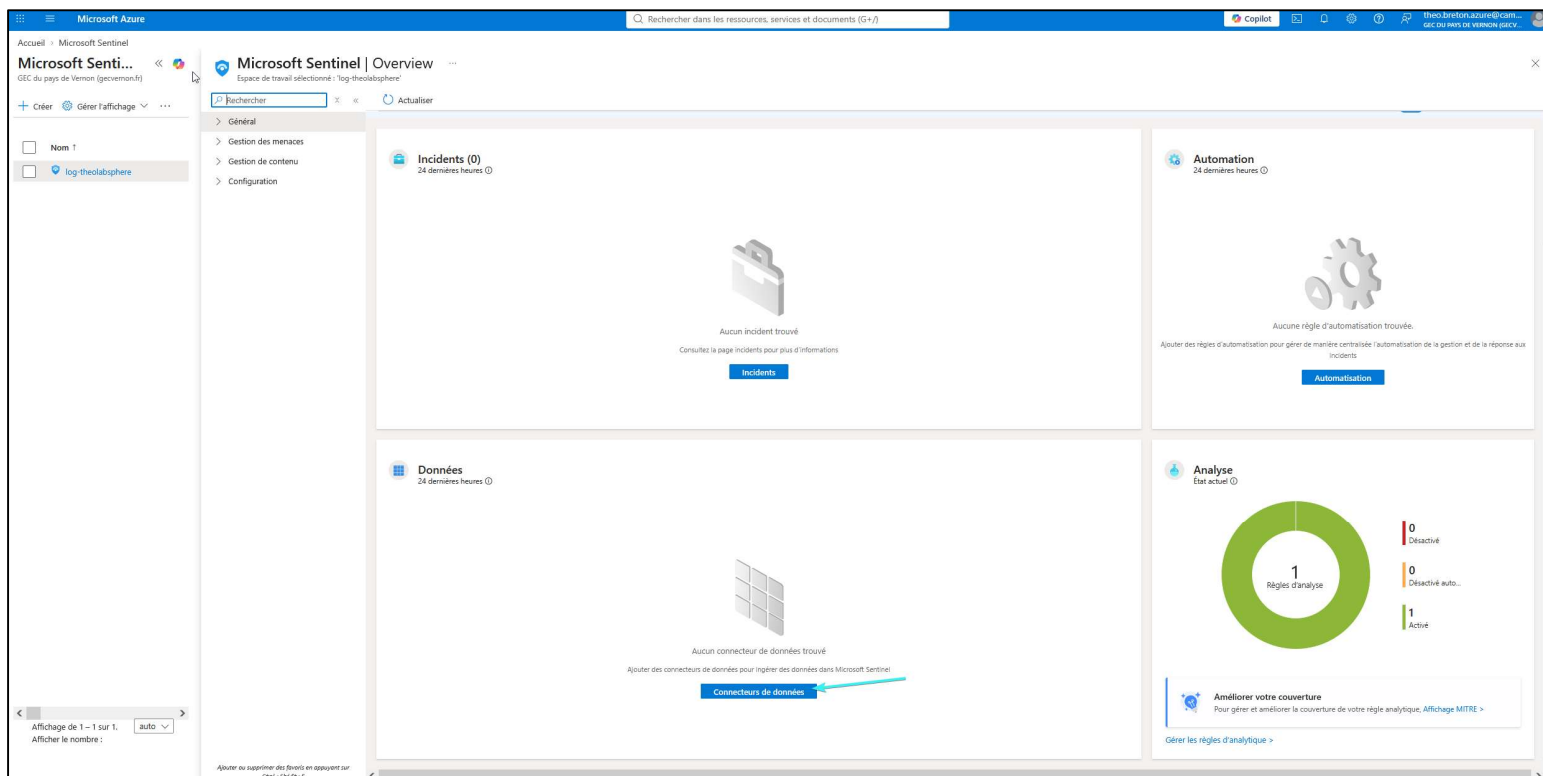
... Ajout de Microsoft Sentinel

Ajout de Microsoft Sentinel à l'espace de travail 'log-theolabsphere'





Connecter les logs Windows



Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

Théo.BRETON@univ-lyon1.fr

Microsoft Sentinel | Connecteurs de données

Espace de travail sélectionné : Top-theodolophere

Unité Windows via AMA

Refresh

Guides et commentaires

Device specific AMA connectors have been deprecated. Learn more.

In anticipation of the End of Support of the HTTP Data Collector API, Azure Function-based data connectors using legacy API will not be supported after September 14, 2026. Please update to CCF-based data connectors. Learn more.

0 Connectors

0 Connected

More content at Content Hub

Search by name or provider

Providers

Data Types

Status

Data connectors

What is it?

Microsoft Sentinel comes with several data connectors for Microsoft and non-Microsoft products to help get your data onboarded. These data connectors are available out of the box and provide real-time integration with products including Microsoft Defender XDR, Microsoft Defender for Identity, Microsoft 365 sources, Azure AD, Microsoft Defender for Cloud Apps, and more. In addition, there are built-in connectors to the broader security ecosystem for non-Microsoft products.

Getting started

Featured data connectors

These are the top data connectors for your data ingestion and onboarding needs.

Get these data connectors

More data connectors

Explore all connectors in content hub. Install on demand.

Go to content hub

No Connector selected

Select a Connector to view more details

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

Théo.BRETON@univ-lyon1.fr

Microsoft Sentinel | Connecteurs de données

Hub de contenu

Actualiser

Installer/mettre à jour

Supprimer

Migration SIEM

Guides et commentaires

505 Solutions

382 Contenu autonome

0 Installé

0 Mises à jour

Vous ne trouvez pas ce que vous cherchez ? Nous affichons un ensemble limité de résultats. Essayez d'affiner votre recherche pour obtenir des résultats plus spécifiques. En savoir plus

Windows Security Events

État : Tout

Type de contenu : Connecteur de données (473)

Support : Tout

Fournisseur : Tout

Catégorie : Tout

Sources de contenu : Tout

	Titre du contenu	État	Source de contenu	Fournisseur	Support	Catégorie	Type de contenu
☐	Windows Security Events	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Règle analytique (21) Connecteur de données (2) +2 ...
	Windows Security Events via AMA	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Connecteur de données
	Security Events via Legacy Agent	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Connecteur de données
☐	Windows Forwarded Events	☐ Non installé	Solution	Microsoft	Microsoft	Opérations informatiques	Règle analytique (6) Connecteur de données ...
	Windows Forwarded Events	☐ Non installé	Solution	Microsoft	Microsoft	Opérations informatiques	Connecteur de données
☐	Windows Server DNS	☐ Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Règle analytique (5) Connecteur de données (2) +2 ...
	Windows DNS Events via AMA	☐ Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Connecteur de données
	DNS	☐ Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Connecteur de données
☐	Windows Firewall	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données (2) Classeur ...
	Windows Firewall Events via AMA	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données
	Windows Firewall	☐ Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données
☐	Microsoft Exchange Security for Exchange On-Premises	☐ Non installé	Solution	Microsoft	Community	Application	Règle analytique (2) Connecteur de données (8) +3 ...
	Microsoft Exchange Logs and Events	☐ Non installé	Solution	Microsoft	Community	Application	Connecteur de données
☐	Cynerio Medical Device Security Sentinel Connector	☐ Non installé	Solution	Cynerio	Cynerio	Sécurité - Gestion des vulnérabilités, Sécurité - Réseau	Règle analytique (5) Connecteur de données +2 ...
	Cynerio Security Events	☐ Non installé	Solution	Cynerio	Cynerio	Sécurité - Gestion des vulnérabilités, Sécurité - Réseau	Connecteur de données
☐	Uniqkey Security Events	☐ Non installé	Solution	Uniqkey	Uniqkey	Identité, Sécurité - Autres	Règle analytique (9) Connecteur de données +1 ...
	Uniqkey Security Events	☐ Non installé	Solution	Uniqkey	Uniqkey	Identité, Sécurité - Autres	Connecteur de données

< Précédent

Page 1 sur 1

Suivant >

Affichage des résultats 1 à 19 sur 19.

Microsoft Azure

Accueil > Microsoft Sentinel > Connecteurs de données

Hub de contenu

Actualiser Installer/mettre à jour Supprimer Migration SIEM Guides et commentaires

505 Solutions 382 Contenu autonome 1 Installé 0 Mises à jour

Vous ne trouvez pas ce que vous cherchez ? Nous affichons un ensemble limité de résultats. Essayez d'affiner votre recherche pour obtenir des résultats plus spécifiques. [En savoir plus](#)

Windows Security Events

État : Tout Type de contenu : Connecteur de données (473) Support : Tout Fournisseur : Tout Catégorie : Tout Sources de contenu : Tout

Titre du contenu	État	Source de contenu	Fournisseur	Support	Catégorie	Type de contenu
Windows Security Events	Installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Règle analytique (21) Connecteur de données (2)
Windows Security Events via AMA	Installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Connecteur de données
Security Events via Legacy Agent	Installé	Solution	Microsoft	Microsoft	Sécurité - Protection contre les menaces	Connecteur de données
Windows Forwarded Events	Non installé	Solution	Microsoft	Microsoft	Opérations informatiques	Règle analytique (4) Connecteur de données
Windows Forwarded Events	Non installé	Solution	Microsoft	Microsoft	Opérations informatiques	Connecteur de données
Windows Server DNS	Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Règle analytique (5) Connecteur de données (2)
Windows DNS Events via AMA	Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Connecteur de données
DNS	Non installé	Solution	Microsoft	Microsoft	Mise en réseau	Connecteur de données
Windows Firewall	Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données (2) Classeur
Windows Firewall Events via AMA	Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données
Windows Firewall	Non installé	Solution	Microsoft	Microsoft	Sécurité - Réseau	Connecteur de données
Microsoft Exchange Security for Exchange On-Premises	Non installé	Solution	Microsoft	Community	Application	Règle analytique (2) Connecteur de données (3)
Microsoft Exchange Logs and Events	Non installé	Solution	Microsoft	Community	Application	Connecteur de données
Cynerio Medical Device Security Sentinel Connector	Non installé	Solution	Cynerio	Cynerio	Sécurité - Gestion des vulnérabilités, Sécurité -	Règle analytique (5) Connecteur de données (+2)
Cynerio Security Events	Non installé	Solution	Cynerio	Cynerio	Sécurité - Gestion des vulnérabilités, Sécurité - Réseau	Connecteur de données
Uniqkey Security Events	Non installé	Solution	Uniqkey	Uniqkey	Identité, Sécurité - Autres	Règle analytique (9) Connecteur de données (+1)

< Précédent Page 1 sur 1 Suivant > Affichage des résultats 1 à 19 sur 19.

Windows Security Events

Microsoft Fournisseur Microsoft Support 3.0.13 Version

Description

Note: Please refer to the following before installing the solution:

- Review the solution [Release Notes](#)
- There may be known [issues](#) pertaining to this Solution, please refer to them before installing.

The Windows Security Events solution for Microsoft Sentinel allows you to ingest Security events from your Windows machines using the Windows Agent into Microsoft Sentinel. This solution includes two (2) data connectors to help ingest the logs.

- Windows Security Events via AMA** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the new Azure Monitor Agent. Learn more about ingesting using the new Azure Monitor Agent [here](#). **Microsoft recommends using this Data Connector.**
- Security Events via Legacy Agent** - This data connector helps in ingesting Security Events logs into your Log Analytics Workspace using the legacy Log Analytics agent.

Data Connectors: 2. Workbooks: 2. Analytic Rules: 21. Hunting Queries: 50

[Learn more about Microsoft Sentinel](#) | [Learn more about Solutions](#)

Type de contenu

21 Règle analytique 2 Connecteur de données 30 Requête de repérage

2 Classeur

Catégorie

Sécurité - Protection contre les menaces

Tarification

Gratuit

Gérer Actions Afficher les détails

Microsoft Azure

Accueil > Microsoft Sentinel

Microsoft Sentinel | Connecteurs de données

Espace de travail sélectionné : log-theodabsphere

Rechercher Refresh Guides et commentaires

Général Gestion des menaces Gestion de contenu Configuration Gestionnaire d'espaces de travail (préversion)

Connecteurs de données

2 Connectors 0 Connected

Search by name or provider Providers: Microsoft Data Types: SecurityEvents Status: Not connected (2)

Status Connector name 1

[DEPRECATED] Security Events via Legacy Agent Microsoft

Windows Security Events via AMA Microsoft

Updates

Deprecated

Windows Security Events via AMA

Disconnected Status Provider Microsoft Last Log Received --

Content source: Windows Security Events Version: 1.0.0

Author: Microsoft Supported by: Microsoft Corporation | Email

Related content

0 Workbooks 1 Queries 20 Analytics rules templates

Data received

Go to log analytics

4 3 2 1 0

30 août 31 août 1 septembre 3 septembre 3 septembre

SecurityEvents

0

Data types

SecurityEvents --

Open connector page

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VERMOREL 04/07/2024

Accueil > Microsoft Sentinel | Connecteurs de données

Windows Security Events via AMA

Delete

Windows Security Events via AMA

Disconnected
Status

Microsoft
Provider

Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](#).

Last data received

--

Content source

Version

Windows Security Events

1.0.0

Author

Supported by

Microsoft

Microsoft Corporation | Email

Related content

0
Workbooks

1
Queries

20
Analytics rules templates

Data received

Go to log analytics

4

3

2

1

0

30 août

31 août

1 septembre

3 septembre

5 septembre

SecurityEvents

0

Data types

SecurityEvents --

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

Workspace data sources: read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. [Learn more](#)

Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Refresh

Rule name

Created by

Filter name

No results

+ Create data collection rule

Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Copilot

théo.breton.azure@cam...
GEC DU PAYS DE VERMOREL 04/07/2024

Accueil > Microsoft Sentinel | Connecteurs de données

Windows Security Events via AMA

Delete

Windows Security Events via AMA

Disconnected
Status

Microsoft
Provider

Last Log Received

Description

You can stream all security events from the Windows machines connected to your Microsoft Sentinel workspace using the Windows agent. This connection enables you to view dashboards, create custom alerts, and improve investigation. This gives you more insight into your organization's network and improves your security operation capabilities. For more information, see the [Microsoft Sentinel documentation](#).

Last data received

--

Content source

Version

Windows Security Events

1.0.0

Author

Supported by

Microsoft

Microsoft Corporation | Email

Related content

0
Workbooks

1
Queries

20
Analytics rules templates

Data received

Go to log analytics

4

3

2

1

0

30 août

31 août

1 septembre

3 septembre

5 septembre

SecurityEvents

0

Data types

SecurityEvents --

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

Workspace data sources: read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. [Learn more](#)

Configuration

Enable data collection rule

Security Events logs are collected only from **Windows** agents.

Refresh

Rule name

Created by

Filter name

No results

+ Create data collection rule

Create Data Collection Rule

Data collection rule management

Basic Resources Collect Review + create

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all of your resources.

Rule details

Rule name*

Subscription?

Resource group*

Next Resources >



Microsoft Azure

Rechercher dans les ressources, services et documents (0-7)

Capital

théo.bretton@univ-lille.fr

Accueil > Microsoft Sentinel | Connecteurs de données

Windows Security Events via AMA

Delete

Windows Security Events via AMA

Disconnected Status Microsoft Provider Last Log Received

Description

Last data received

Content source Version Windows Security Events 1.0.0

Author Supported by Microsoft Microsoft Corporation | Email

Related content

0 Workbooks 1 Queries 20 Analytics rules templates

Data received

Go to log analytics

0 SecurityEvents

Data types

SecurityEvents

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

Workspace data sources: read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

Configuration

Enable data collection rule

Security Events logs are collected only from Windows agents.

Refresh

Rule name Created by Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Choose a set of machines to collect data from. This set of machines will replace any previous selection, make sure to re-select any you'd like to keep. The Azure Monitor Agent will automatically be installed.

This will also enable System Assigned Managed Identity on these machines. In addition to existing User Assigned identities (if any). Note: Unless specified in the request, the machine will default to using System Assigned identity for all other applications. Learn more

Subscriptions Resource Groups Resource Types Locations

Selected: All Selected: All Selected: All Selected: All

Search to filter items...

Show Selected

Scope Resource Type Location

Azure for Students

gr-home-lab-hybrid

azure-01 microsoft.compute/virtualmachines Denmark East

Previous Next Collect

Microsoft Azure

Rechercher dans les ressources, services et documents (0-7)

Capital

théo.bretton@univ-lille.fr

Accueil > Microsoft Sentinel | Connecteurs de données

Windows Security Events via AMA

Delete

Windows Security Events via AMA

Disconnected Status Microsoft Provider Last Log Received

Description

Last data received

Content source Version Windows Security Events 1.0.0

Author Supported by Microsoft Microsoft Corporation | Email

Related content

0 Workbooks 1 Queries 20 Analytics rules templates

Data received

Go to log analytics

0 SecurityEvents

Data types

SecurityEvents

Prerequisites

To integrate with Windows Security Events via AMA make sure you have:

Workspace data sources: read and write permissions.

To collect data from non-Azure VMs, they must have Azure Arc installed and enabled. Learn more

Configuration

Enable data collection rule

Security Events logs are collected only from Windows agents.

Refresh

Rule name Created by Filter name

No results

+Create data collection rule

Create Data Collection Rule

Data collection rule management

Validation passed

Basic Resources Collect Review + create

Basic

Data rule name azure01

Subscription Azure for Students

Resource Group gr-home-lab-hybrid

Selected resources

Name Type

azure-01 microsoft.compute/virtualmachines

Selected events

All events

Previous Create



Microsoft Azure

Rechercher dans les ressources, services et documents (G+)

Accueil > Microsoft Sentinel

Microsoft Sentinel | Overview

Espace de travail sélectionné : log-theolabsphere

Créer Gérer l'affichage

Nom 1

log-theolabsphere

Général

Gestion des menaces

Gestion de contenu

Configuration

Incidents (0)

24 dernières heures

Aucun incident trouvé

Consultez la page incidents pour plus d'informations

Incidents

Données

24 dernières heures

Aucun connecteur de données trouvé

Ajouter des connecteurs de données pour intégrer des données dans Microsoft Sentinel

Connecteurs de données

Automation

24 dernières heures

Aucune règle d'automatisation trouvée

Ajouter des règles d'automatisation pour gérer de manière centralisée l'automatisation de la gestion et de la réponse aux incidents

Automatisation

Analyse

État actuel

1 Règles d'analyse

0 Désactivé

0 Désactivé auto...

1 Actif

Améliorer votre couverture

Pour gérer et améliorer la couverture de votre règle analytique, Affichez MITRE >

Gérer les règles d'analytique >

Ajouter ou supprimer des favoris en appuyant sur Ctrl+Shift+F