



Google Cloud Platform



easy Former



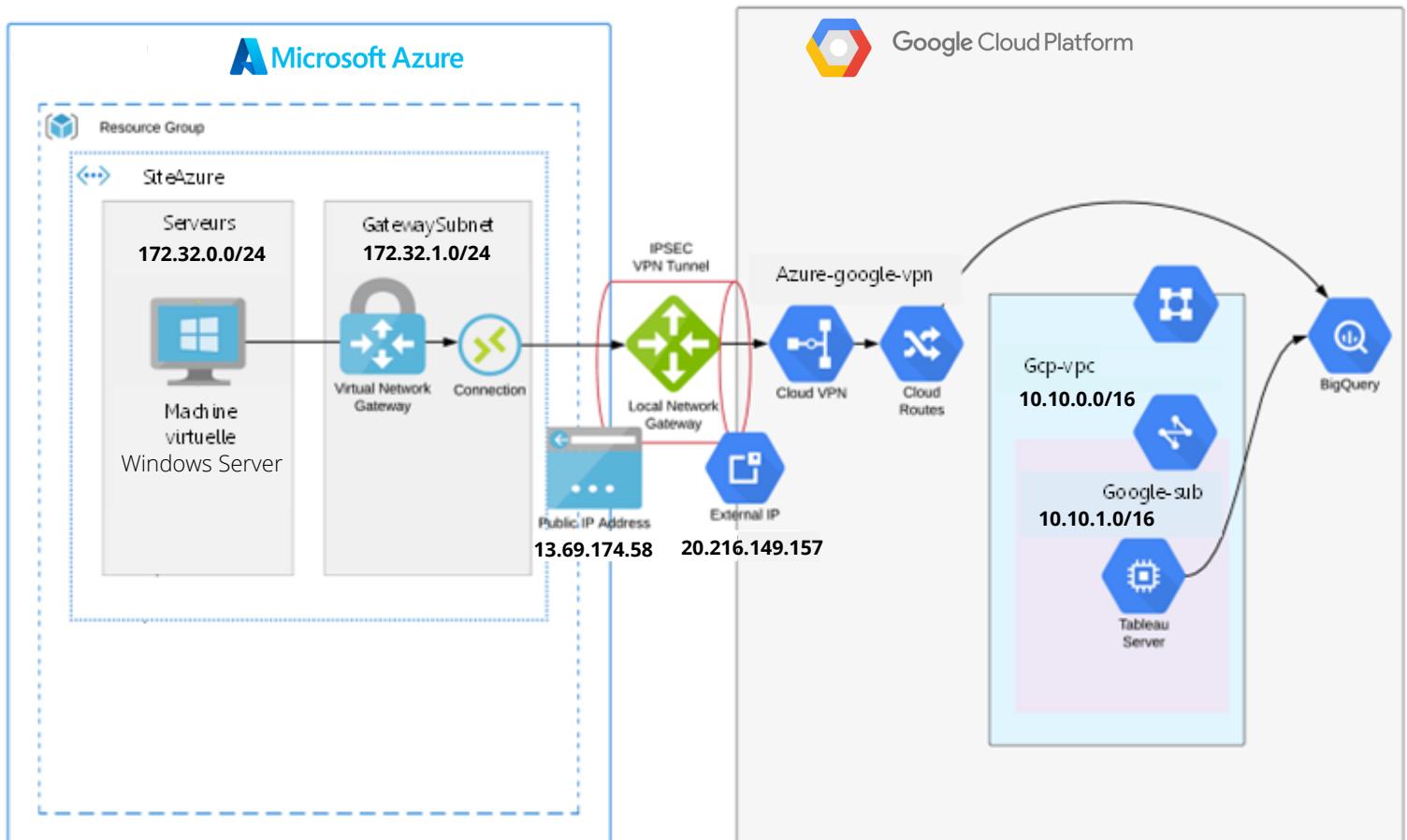
Connexion VPN inter site Azure GCP Implémentation d'un Azure AD DS

EL HASSAN MOUMD
IBRAHIM OUAALI

TABLE DES MATIÈRES

- 1** → Schéma du TP
- 2** → Introduction du TP
- 3** → Site Azure 1ère partie
 - 1. Création d'un groupe de ressources
 - 2. Création du réseau virtuel
 - 3. Ajout d'un sous-réseau dans le réseau virtuel
 - 4. Création de la machine virtuelle
 - 4.1. Ouverture des ports dans la machine virtuelle
 - 5. Création de la passerelle de réseau virtuel (VPN)
- 4** → Site Google
 - 1. Création d'un réseau VPC
 - 2. Création d'une connectivité hybride (VPN)
 - 3. Création de la machine virtuelle
 - 4. Ouverture des ports pour le RDP et l'ICMP
- 5** → Site Azure 2^e partie
 - 1. Création de la passerelle de réseau local
 - 2. Crédit de la connexion (Tunnel)
 - 3. Vérifications de communication
- 6** → Azure AD DS
 - 1. Création d'utilisateur
 - 2. Ajout d'un Windows Serveur dans le domaine Azure

SCHÉMA DU TP



INFORMATIONS MISE EN PLACE DU VPN

Site Azure :

Espace d'adressage du réseau Azure (Vnet) : 172.32.0.0/16

Espace d'adressage des sous-réseaux d'Azure :

- Serveurs : 172.32.0.0/24
- GatewaySub : 172.32.1.0/24

Machine virtuelle : WindowsServer

OS Windows (Windows Server 2019 Datacenter)

Taille A2 standard v2 (2 processeurs virtuels, 4 Gio de mémoire)

Adresse IP Publique pour accès en RDP : 13.69.174.58

Site Google :

Espace d'adressage du réseau Google (VPC) : 10.10.0.0/16

Adresse IP de la passerelle : 10.10.0.1

Machine virtuelle : googlevms

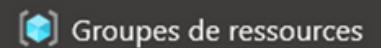
Adresse IP Publique pour accès en RDP : 34.77.207.246



I. SITE AZURE

1. CRÉATION D'UN GROUPE DE RESSOURCES

Sur le portail Azure se rendre sur groupe de ressources :



Puis ajouter un nouveau nommé SiteAzure :

Accueil > Groupes de ressources >

Créer un groupe de ressources

De base • Étiquettes Vérifier + créer

Groupe de ressources- Un 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](#)

Détails du projet

Abonnement * ⓘ

Azure pour les étudiants



Groupe de ressources * ⓘ

SiteAzure

✖ Un groupe de ressources avec le même nom existe déjà dans l'abonnement sélectionné Azure pour les étudiants.

Détails de la ressource

Région * ⓘ

(Europe) France-Centre



2. CRÉATION DU RÉSEAU VIRTUEL

Lorsque le groupe de ressources est créé, l'ouvrir et aller sur ajouter afin de créer un réseau virtuel. (Mise en réseau > réseau virtuel)

- Intégration
- Internet des objets
- Outils de gestion
- Média
- Migration
- Mixed Reality
- Monitoring & Diagnostics
- Mise en réseau**
- Sécurité

Quest
APERÇU



Foglight Evolve (aperçu)
[En savoir plus](#)

f5
APERÇU

F5 Advanced WAF for Azure (PAYG)
(aperçu)
[En savoir plus](#)

HashiCorp Consul Service on Azure
APERÇU

HashiCorp Consul Service on Azure
(aperçu)
[En savoir plus](#)

[Accueil](#) > [Groupes de ressources](#) > [SiteAzure](#) >

Nouveau

[Place de marché Azure](#) [Tout afficher](#)

- Démarrer
- Création récente
- IA + Machine Learning
- Analyse
- Blockchain

[Proposé](#) [Tout afficher](#)

 [Réseau virtuel](#)
[Démarrages rapides + tutoriels](#)

 APERÇU

VMware NSX Advanced Load Balancer (Avi Networks) (aperçu)
[En savoir plus](#)

Pour le nom on met SiteAzure :

[Accueil](#) > [Groupes de ressources](#) > [SiteAzure](#) > [Nouveau](#) >

Créer un réseau virtuel

[De base](#) [Adresses IP](#) [Sécurité](#) [Étiquettes](#) [Vérifier + 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 sur le réseau virtuel](#)

Détails du projet

Abonnement * 

Azure pour les étudiants

Groupe de ressources * 

SiteAzure

[Créer nouveau](#)

Détails de l'instance

Nom *

SiteAzure

 Il existe déjà une ressource ayant le même nom et le même type dans le groupe de ressources actuel.

Région *

(Europe) France-Centre

Créer un réseau virtuel

[De base](#) [Adresses IP](#) **Sécurité** [Étiquettes](#) [Vérifier + créer](#)

Espace d'adressage du réseau virtuel, spécifié sous la forme d'un ou plusieurs préfixes d'adresse en notation CIDR (par exemple, 192.168.1.0/24).

Espace d'adressage IPv4

172.32.0.0/16



⚠ L'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) » chevauche l'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) » du réseau virtuel « SiteAzure ». Les réseaux virtuels avec des espaces d'adressage qui se chevauchent ne peuvent pas être appariés. Si vous voulez appairer ces réseaux virtuels, changez l'espace d'adressage « 172.32.0.0/16 (172.32.0.0 - 172.32.255.255) ». [En savoir plus](#)

Ajouter un espace d'adressage IPv6 (i)

Plage d'adresses du sous-réseau en notation CIDR (par exemple, 192.168.1.0/24). Elle doit faire partie de l'espace d'adressage du réseau virtuel.

+ Ajouter un sous-réseau

Supprimer le sous-réseau

Nom de sous-réseau

Espace d'adressage de sous-réseau

Ce réseau virtuel n'a pas de sous-réseaux.

Ajouter un sous-ré... X

On indique l'espace d'adressage IPv4 : 172.32.0.0/16 puis on créer un sous-réseau nommé serveurs avec comme espace d'adressage : 172.32.0.0/24.

On vérifie et on crée :

Vérifier + créer

Nom de sous-réseau *

Serveurs



Espace d'adressage de sous-réseau * (i)

172.32.0.0/24



172.32.0.0 - 172.32.0.255 (251 + 5 adresses réservées Azure)

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](#)

Services (i)

0 sélectionné



3. CRÉATION DE SOUS-RÉSEAU DE PASSERELLE

Ensuite, on va dans notre groupe de ressources > SiteAzure > Sous-réseaux > Sous-réseau de passerelle et on indique la plage 172.32.1.0/24 : validation.

4. CRÉATION DE LA MACHINE VIRTUELLE

Dans le menu, sélectionner :  Machines virtuelles

Puis les paramètres seront les suivants :

Créer une machine virtuelle

Abonnement *	<input type="text" value="Azure pour les étudiants"/>
Groupe de ressources *	<input type="text" value="SiteAzure"/> Créer nouveau
Détails de l'instance	
Nom de la machine virtuelle *	<input type="text" value="2K19SRV-DC01"/>
Région *	<input type="text" value="(Europe) France-Centre"/>
Options de disponibilité	<input type="text" value="Aucune redondance d'infrastructure requise"/>
Image *	<input type="text" value="Windows Server 2019 Datacenter - Génération 1"/> Parcourir toutes les images publiques et privées
Instance Azure Spot	<input type="radio"/> Oui <input checked="" type="radio"/> Non
Taille *	<input type="text" value="Standard_A2_v2 - (97,88 €/mois)"/> Sélectionner la taille
Compte d'administrateur	
Nom d'utilisateur *	<input type="text" value="Administrateur"/>
Mot de passe *	<input type="text" value="*****"/>
Confirmer le mot de passe *	<input type="text" value="*****"/>
Règles des ports d'entrée	
Sélectionnez les ports réseau de machine virtuelle accessibles publiquement à partir d'Internet. Vous pouvez spécifier un accès réseau plus limité ou granulaire sous l'onglet Mise en réseau.	
Ports d'entrée publics *	<input type="radio"/> Aucun <input checked="" type="radio"/> Autoriser les ports sélectionnés
Sélectionner des ports d'entrée *	<input type="text" value="HTTP (80), HTTPS (443), SSH (22), RDP (3389)"/>

Dans la partie réseau : je spécifie le réseau dont le serveur va appartenir.

Interface réseau

Quand vous créez une machine virtuelle, une interface réseau est créée pour vous.

Réseau virtuel *	<input type="text" value="SiteAzure"/> 
	Créer
Sous-réseau *	<input type="text" value="Serveurs (172.32.0.0/24)"/> 
	Gérer la configuration du sous-réseau
Adresse IP publique	<input type="text" value="Aucun"/> 
	Créer
Groupe de sécurité réseau de la carte réseau	<input checked="" type="radio"/> Aucun <input type="radio"/> De base <input type="radio"/> Paramètres avancés
Mise en réseau accélérée	<input type="radio"/> Activé <input checked="" type="radio"/> Désactivé
	<small>La taille de machine virtuelle sélectionnée ne prend pas en charge la mise en réseau accélérée.</small>

Équilibrage de charge

Vous pouvez placer cette machine virtuelle dans le pool de back-ends d'une solution d'équilibrage de charge Azure existante.
[En savoir plus](#)

Placer cette machine virtuelle derrière une Oui Non solution d'équilibrage de charge existante ?

4.1. OUVERTURE DES PORTS DANS LA MACHINE VIRTUELLE

Se rendre dans SiteAzure puis dans le groupe de sécurité et y ajouter les règles pour l'ICMP et le RDP :

Groupe de res... (modifier) : SiteAzure		Règles de sécurité perso... : 5 trafic entrant, 0 trafic sortant	
Emplacement : France-Centre		Associé à : 0 sous-réseaux, 1 interfaces réseau	
Abonnement (modifier) : Azure pour les étudiants 			
ID d'abonnement : 16bab315-18f1-4963-9aff-df3e7519826c			
Étiquettes (modifier) : Cliquez ici pour ajouter des étiquettes			
Règles de sécurité de trafic entrant			
Priorité	Nom	Port	Protocole
300	 RDP	3389	TCP
320	 SSH	22	TCP
340	HTTPS	443	TCP
360	HTTP	80	TCP
370	 ICMP	N'importe lequel	ICMP
Règles de sécurité de trafic sortant			
Priorité	Nom	Port	Protocole
300	 RDP	3389	TCP
320	 SSH	22	TCP
340	HTTPS	443	TCP
360	HTTP	80	TCP
370	 ICMP	N'importe lequel	ICMP

5. CRÉATION DE LA PASSERELLE DE RÉSEAU VIRTUEL (VPN)

On crée la passerelle virtuelle (Attention, ici l'IP publique a déjà été créée, il faut donc sélectionner créer et lui indiquer un nom)

Abonnement ▾

Azure pour les étudiants

Groupe de ressources ⓘ

SiteAzure (dérivé du groupe de ressources du réseau virtuel)

Détails de l'instance

Nom *

VPN

Région *

France-Centre

Type de passerelle * ⓘ

VPN ExpressRoute

Type de VPN * ⓘ

Basé sur itinéraires Basé sur des stratégies

RÉFÉRENCE (SKU) * ⓘ

VpnGw1

Génération ⓘ

Generation1

Réseau virtuel * ⓘ

SiteAzure

[Créer un réseau virtuel](#)

Sous-réseau ⓘ

GatewaySubnet (172.32.1.0/24)

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

Adresse IP publique

Adresse IP publique * ⓘ

Crée Utiliser l'existante

Choisir une adresse IP publique *

SiteAzure (51.103.54.99)

Activer le mode actif/passif * ⓘ

Activé Désactivé

Configurer l'ASN BGP * ⓘ

Activé Désactivé



II. SITE GOOGLE



Une fois connecté sur la plateforme GCP, on crée un réseau VPC avec ces paramètres :

Réseau VPC

[Créer un réseau VPC](#)

Réseaux VPC

Nom * Utilisez que des lettres minuscules, des chiffres et des traits d'union

Description

Sous-réseaux

Les sous-réseaux vous permettent de créer votre topologie cloud privée dans Google Cloud. Cliquez sur "Automatique" pour créer un sous-réseau dans chaque région ou sur "Personnalisé" pour définir manuellement les sous-réseaux. [En savoir plus](#)

Mode de création du sous-réseau

Personnalisées

Automatique

Nouveau sous-réseau

Nom * Utilisez que des lettres minuscules, des chiffres et des traits d'union

Ajouter une description

Région *

Plage d'adresses IP *

Réseaux VPC

CRÉER UNE PLAQUE D'ADRESSES IP SECONDAIRE

Accès privé à Google ?

Activé

Désactivé

Journaux de flux

L'activation des journaux de flux VPC n'affecte pas les performances, mais certains systèmes génèrent un grand nombre de journaux, et, par conséquent, peuvent entraîner une augmentation des coûts dans Stackdriver. [En savoir plus](#)

Activé

Désactivé

ANNULER OK

AJOUTER UN SOUS-RÉSEAU

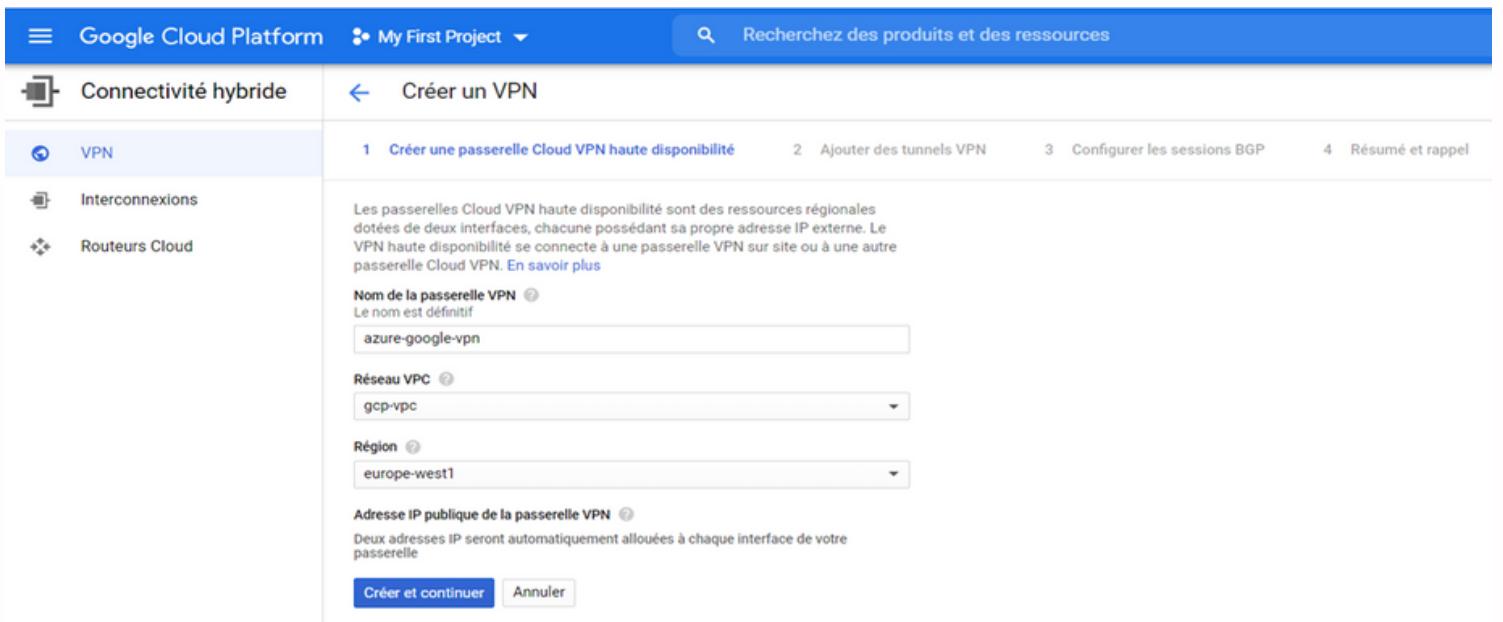
Mode de routage dynamique ?

Régional
Les routeurs cloud n'apprennent que les routes de la région dans laquelle ils ont été créés

Mondial
Le routage mondial vous permet d'apprendre de manière dynamique les routes vers et depuis l'ensemble des régions, à l'aide d'un seul VPN ou d'une interconnexion et de Cloud Router

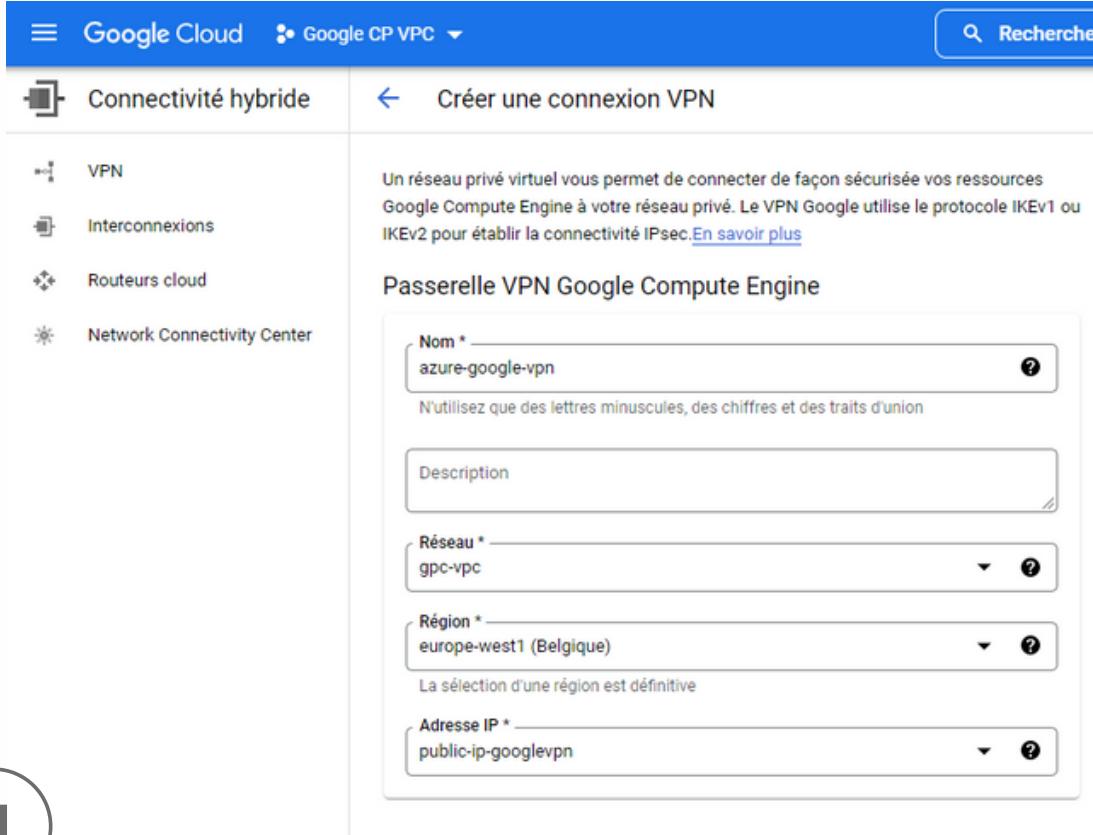
2. CRÉATION D'UNE CONNECTIVITÉ HYBRIDE (VPN)

On se rend dans l'onglet connectivité hybride puis on sélectionne VPN, ensuite on sélectionne le VPN standard et ensuite :



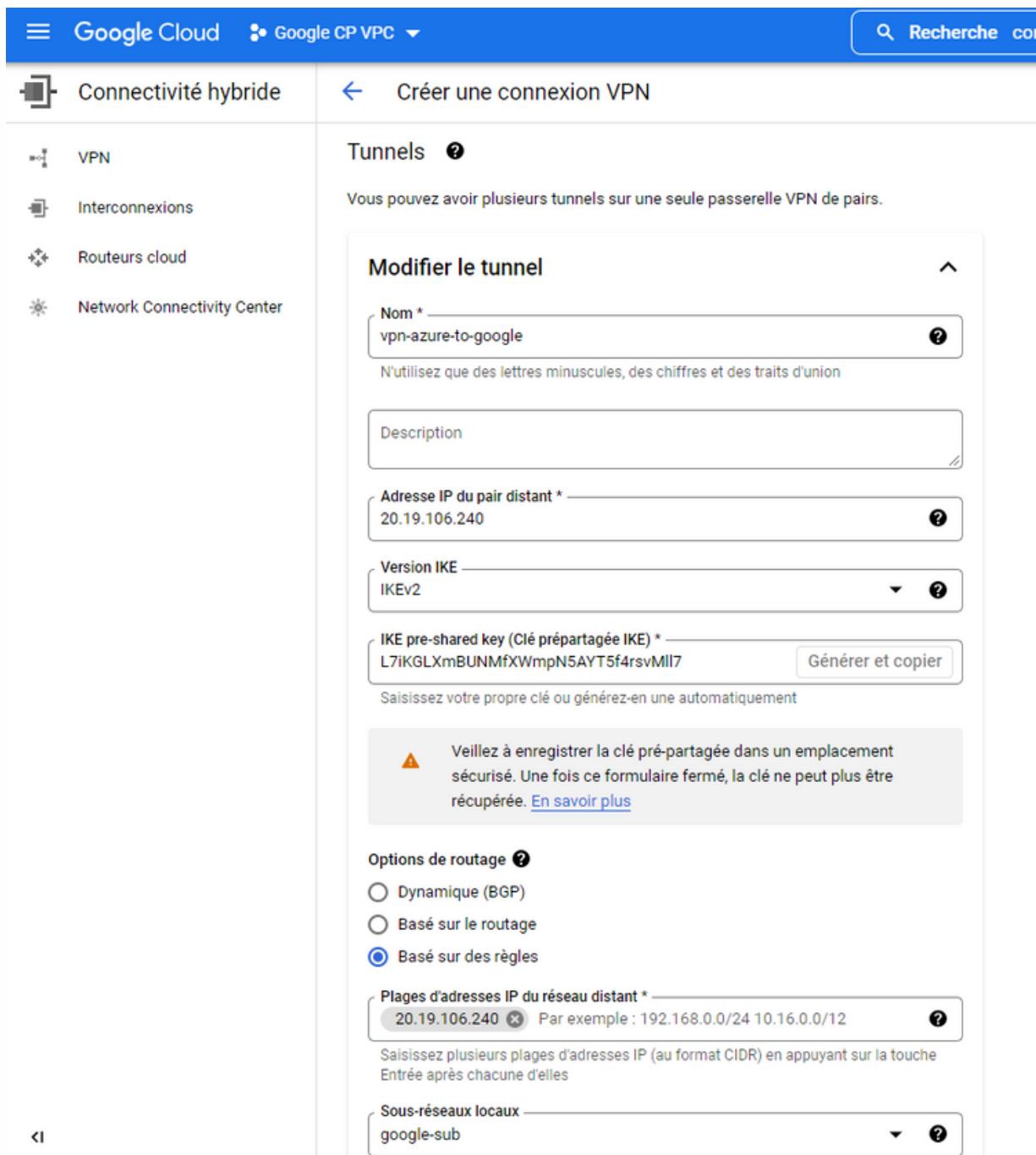
The screenshot shows the Google Cloud Platform interface for creating a Cloud VPN gateway. The left sidebar has 'Connectivité hybride' selected under 'VPN'. The main panel title is 'Créer un VPN'. It includes steps: 1. Crée une passerelle Cloud VPN haute disponibilité, 2. Ajouter des tunnels VPN, 3. Configurer les sessions BGP, 4. Résumé et rappel. The 'Nom de la passerelle VPN' field contains 'azure-google-vpn', 'Réseau VPC' is set to 'gcp-vpc', and 'Région' is 'europe-west1'. A note says two public IP addresses will be assigned to each interface. Buttons at the bottom are 'Créer et continuer' and 'Annuler'.

On crée une adresse IP Publique :



The screenshot shows the Google Cloud Platform interface for creating a VPN connection using Google Compute Engine. The left sidebar has 'Connectivité hybride' selected under 'VPN'. The main panel title is 'Créer une connexion VPN'. It includes a note about using a virtual private network to connect Google Compute Engine resources. The 'Passerelle VPN Google Compute Engine' section shows fields for 'Nom' (set to 'azure-google-vpn'), 'Description', 'Réseau' (set to 'gpc-vpc'), 'Région' (set to 'europe-west1 (Belgique)'), and 'Adresse IP' (set to 'public-ip-googlevpn').

Et dans le paramètre du tunnel :



The screenshot shows the Google Cloud Platform interface for creating a VPN connection. The left sidebar lists 'Connectivité hybride' under 'VPN'. The main page title is 'Créer une connexion VPN'. A sub-section titled 'Tunnels' is shown, with a note: 'Vous pouvez avoir plusieurs tunnels sur une seule passerelle VPN de pairs.' Below this is a 'Modifier le tunnel' form:

- Nom ***: vpn-azure-to-google
- Description**: (empty)
- Adresse IP du pair distant ***: 20.19.106.240
- Version IKE**: IKEv2
- IKE pre-shared key (Clé prépartagée IKE) ***: L7IKGLXmBUNMfXWmpN5AYT5f4rsvMII7 (with a 'Générer et copier' button)
- Avertissement**: 'Veillez à enregistrer la clé pré-partagée dans un emplacement sécurisé. Une fois ce formulaire fermé, la clé ne peut plus être récupérée.' (with a 'En savoir plus' link)
- Options de routage**: Radio buttons for 'Dynamique (BGP)', 'Basé sur le routage', and 'Basé sur des règles'. The last one is selected.
- Plages d'adresses IP du réseau distant ***: 20.19.106.240 (with a 'Par exemple' placeholder: 192.168.0.0/24 10.16.0.0/12)
- Sous-réseaux locaux**: google-sub

On prend soin de bien noter la clé partagée IKE et on note l'adresse IP publique du VPN Azure (créeée juste avant).

Puis finalement, on crée ce VPN.

Google Cloud Google CP VPC

Recherche connectivité

Connectivité hybride

Créer une connexion VPN

Version IKE
IKEv2

IKE pre-shared key (Clé prépartagée IKE) *
L7iKGLXmBUNMfXWmpN5AYT5f4rsvMII7

Générer et copier

Saisissez votre propre clé ou générez-en une automatiquement

A Veillez à enregistrer la clé pré-partagée dans un emplacement sécurisé. Une fois ce formulaire fermé, la clé ne peut plus être récupérée. [En savoir plus](#)

Options de routage ?

- Dynamique (BGP)
- Basé sur le routage
- Basé sur des règles

Plages d'adresses IP du réseau distant *
20.19.106.240

Par exemple : 192.168.0.0/24 10.16.0.0/12

Saisissez plusieurs plages d'adresses IP (au format CIDR) en appuyant sur la touche Entrée après chacune d'elles

Sous-réseaux locaux
google-sub

Plages d'adresses IP locales *
10.10.0.0/16

Par exemple : 192.168.0.0/24 10.0.0.0/12

OK

AJOUTER UN TUNNEL

CRÉER ANNULER

LIGNE DE COMMANDE ÉQUIVALENTE

Créer le VPN



3. CRÉATION DE LA MACHINE VIRTUELLE GOOGLE

On crée une nouvelle instance de VM nommée googlevm, avec les paramètres suivants pour la VM .

[Créer une instance](#)

Pour créer une instance de VM, sélectionnez l'une de ces options :

- Nouvelle instance de VM
Créer entièrement une instance de VM unique
- Nouvelle instance de VM à partir d'un modèle
Créer une instance de VM unique à partir d'un modèle existant
- Nouvelle instance de VM à partir d'une image système
Créer une instance de VM unique à partir d'une image système existante
- Marketplace
Déployer une solution prête à l'emploi sur une instance de VM

Nom *

Libellés [?](#)
[+ AJOUTER DES LIBELLÉS](#)

Région * Zone *
La sélection d'une région est définitive La zone est définitive

Configuration de la machine

Famille de machines

USAGE GÉNÉRAL	OPTIMISÉ POUR LE CALCUL	MÉMOIRE OPTIMISÉE	GPU
---------------	-------------------------	-------------------	-----

Types de machines pour les charges de travail courantes permettant d'optimiser les coûts et la flexibilité

Série Sélection de la plate-forme de processeur en fonction de la disponibilité

Type de machine

	vCPU 1 à 2 vCPU (1 cœur partagé)	Memory 4 Go
---	-------------------------------------	----------------

Plate-forme du processeur

GPU

Le nombre de GPU associés affecte la quantité maximale de mémoire et le nombre maximal de processeurs de la VM. [En savoir plus](#)

[+ AJOUTER UN GPU](#)

[▲ PLATE-FORME DU CPU ET GPU](#)

Appareil d'affichage

Activer pour utiliser les outils de capture d'écran et d'enregistrement.

Activer l'appareil d'affichage

Service Confidential VMs [?](#)

L'informatique confidentielle est désactivée sur cette instance de VM.

[ACTIVER](#)

Conteneur [?](#)

Déployez une image de conteneur dans cette instance de VM.

[DEPLOY CONTAINER](#)

Disque de démarrage [?](#)

Nom	googlevm
Type	Nouveau disque persistant avec équilibrage
Taille	10 Go
Type de licence ?	Gratuit
Image	 Debian GNU/Linux 11 (bullseye)

[MODIFIER](#)

Identité et accès à l'API ?

Comptes de service ?

Compte de service

Compute Engine default service account

Vous devez définir le rôle "Utilisateur du compte de service" (roles/iam.serviceAccountUser) pour les utilisateurs qui souhaitent accéder aux VM avec ce compte de service. [En savoir plus](#)

Niveaux d'accès ?

Autoriser l'accès par défaut

Autoriser l'accès complet à l'ensemble des APIs Cloud

Définir l'accès pour chaque API

Pare-feu ?

Ajouter des tags et des règles de pare-feu pour autoriser un trafic réseau spécifique provenant d'Internet

Autoriser le trafic HTTP

Autoriser le trafic HTTPS

Options avancées

Mise en réseau

Nom d'hôte et interfaces réseau

Tags réseau
azureetgoogle ?

Nom d'hôte

Définissez un nom d'hôte personnalisé pour cette instance ou laissez-le par défaut. Ce choix est définitif.

Transfert IP ?

Activer

Configuration des performances du réseau

Carte d'interface réseau

-

Nom de domaine PTR

OK

[AJOUTER UNE INTERFACE RÉSEAU](#)

Disques

Disques supplémentaires

Nouveau disk-1, Image: windows-server-1809-dc-core-v20200609, 32 GB
disque

[+ AJOUTER UN DISQUE](#)

[+ ASSOCIER UN DISQUE EXISTANT](#)

[+ AJOUTER UN DISQUE SSD LOCAL](#)

Sécurité

VM protégées et clés SSH

Gestion

Règles de description, de protection contre la suppression, de réservation, d'automatisation et de disponibilité

Location unique

Libellés d'affinité de noeuds et sursollicitation des processeurs

Votre crédit d'essai gratuit sera utilisé pour cette instance de VM. [Version gratuite de Google Cloud](#)

[CRÉER](#)

[ANNULER](#)

LIGNE DE COMMANDE ÉQUIVALENTE

Bandes passantes réseau

Augmenter la bande passante de sortie totale

Bandes passantes réseau sortante maximale : 2 Gbit/s

Interfaces réseau ?

L'interface réseau est définitive

Modifier l'interface réseau

Réseau * ?

gpc-vpc

Sous-réseau * ?

google-sub IPv4 (10.10.0.0/16)

? Pour utiliser IPv6, vous avez besoin d'une plage de sous-réseau IPv6. [EN SAVOIR PLUS](#)

Type de pile d'adresses IP

IPv4 (pile unique)

IPv4 et IPv6 (double pile)

Adresse IP interne principale
Éphémère (automatique)

Plages d'adresses IP d'alias

[+ AJOUTER UNE PLAGE D'ADRESSES IP](#)

Adresse IPv4 externe
Éphémère

Niveau de service réseau

Premium ?

Standard (europe-west1) ?

Nom de domaine PTR

OK

AJOUTER UNE INTERFACE RÉSEAU

Disques

Disques supplémentaires

Nouveau disk-1, Image: windows-server-1809-dc-core-v20200609, 32 GB
disque

[+ AJOUTER UN DISQUE](#)

[+ ASSOCIER UN DISQUE EXISTANT](#)

[+ AJOUTER UN DISQUE SSD LOCAL](#)

Sécurité

VM protégées et clés SSH

Gestion

Règles de description, de protection contre la suppression, de réservation, d'automatisation et de disponibilité

Location unique

Libellés d'affinité de noeuds et sursollicitation des processeurs

Votre crédit d'essai gratuit sera utilisé pour cette instance de VM. [Version gratuite de Google Cloud](#)

[CRÉER](#)

[ANNULER](#)

LIGNE DE COMMANDE ÉQUIVALENTE

On la crée puis on vérifie :



Instances de ... CRÉER UNE INSTANCE IMPORTER LA VM ACTUALISER DÉMARRER/REPRENDRE ARRÊTER OPÉRATIONS

INSTANCES PLANIFICATIONS D'INSTANCES

Les instances de VM sont des machines virtuelles hautement configurables permettant d'exécuter des charges de travail sur l'infrastructure Google. [En savoir plus](#)

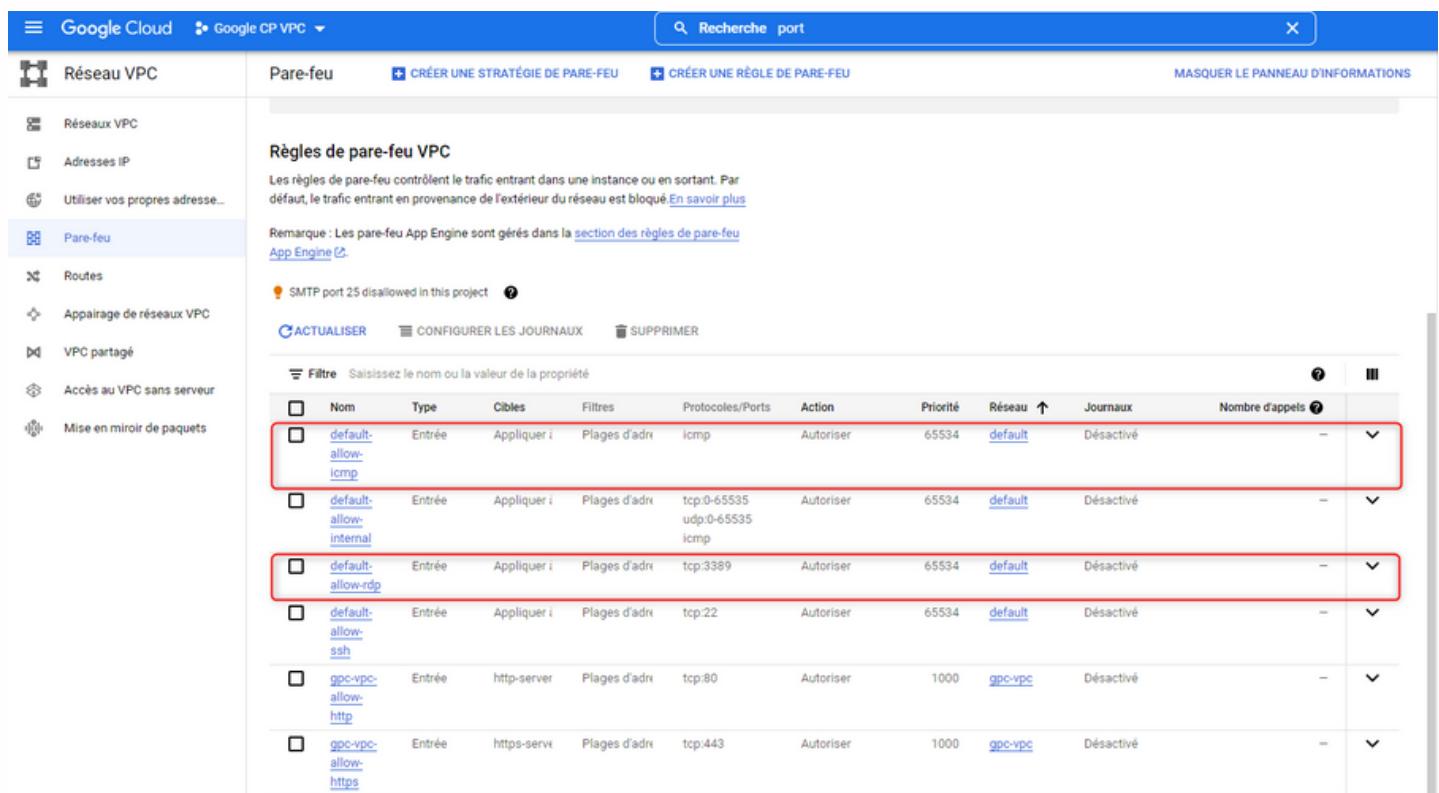
Filtre Saisissez le nom ou la valeur de la propriété

Etat	Nom	Zone	Recommandations	Utilisé par	Adresse IP interne	Adresse IP externe	Connecter
<input type="checkbox"/>	<input checked="" type="checkbox"/> googlevm	europe-west1-b			10.10.0.2 (nic0)	35.210.76.161 (nic0)	SSH

Actions associées HIDE

4. OUVERTURE DES PORTS POUR LE RDP ET L'ICMP

Veiller à bien ouvrir ces ports :



Google Cloud Google CP VPC Recherche port

Réseau VPC Pare-feu CRÉER UNE STRATÉGIE DE PARE-FEU CRÉER UNE RÈGLE DE PARE-FEU MASQUER LE PANNEAU D'INFORMATIONS

Règles de pare-feu VPC

Les règles de pare-feu contrôlent le trafic entrant dans une instance ou en sortant. Par défaut, le trafic entrant en provenance de l'extérieur du réseau est bloqué. [En savoir plus](#)

Remarque : Les pare-feu App Engine sont gérés dans la [section des règles de pare-feu App Engine](#).

SMTP port 25 disallowed in this project.

ACTUALISER CONFIGURER LES JOURNAUX SUPPRIMER

Filtre Saisissez le nom ou la valeur de la propriété

Nom	Type	Cibles	Filtres	Protocoles/Ports	Action	Priorité	Réseau	Journaux	Nombre d'appels
default-allow-icmp	Entrée	Appliquer i	Plages d'adr	icmp	Autoriser	65534	default	Désactivé	-
default-allow-internal	Entrée	Appliquer i	Plages d'adr	tcp:0-65535 udp:0-65535 icmp	Autoriser	65534	default	Désactivé	-
default-allow-rdp	Entrée	Appliquer i	Plages d'adr	tcp:3389	Autoriser	65534	default	Désactivé	-
default-allow-ssh	Entrée	Appliquer i	Plages d'adr	tcp:22	Autoriser	65534	default	Désactivé	-
gpc-vpc-allow-http	Entrée	http-server	Plages d'adr	tcp:80	Autoriser	1000	gpc-vpc	Désactivé	-
gpc-vpc-allow-https	Entrée	https-servr	Plages d'adr	tcp:443	Autoriser	1000	gpc-vpc	Désactivé	-



III. SITE AZURE DEUXIÈME PARTIE



1. CRÉATION DE LA PASSERELLE DE RÉSEAU LOCAL

Lorsque l'on vient créer la passerelle, on spécifie l'adresse IP publique de Google que l'on a récupéré avant ainsi que le réseau local de Google.

Accueil > Passerelles de réseau local >

Créer une passerelle de réseau local

[De base](#) [Avancé](#) [Vérifier + créer](#)

Une passerelle de réseau local est un objet spécifique qui représente un emplacement local (le site) à des fins de routage. [En savoir plus.](#)

Détails du projet

Abonnement *	Azure for Students
Groupe de ressources *	SiteAzure
	Créer nouveau

Détails de l'instance

Région *	France Central
Nom *	LocalGW
Point de terminaison ⓘ	Adresse IP FQDN
Adresse IP *	34.77.207.246
Espaces d'adressage ⓘ	10.10.0.0/16
	Ajouter une autre plage d'adresses

l'adresse IP publique de google

Le réseau local de Google

2. CRÉATION DE LA CONNEXION (TUNNEL)

On va dans tous les services > Connexions > Créer une connexion

Créer une connexion

[De base](#) [Paramètres](#) [Étiquettes](#) [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 *	SiteAzure
	Créer nouveau

Détails de l'instance

Type de connexion *	Site à site (IPsec)
Nom *	VPN_AZURE
Région *	France Central

On valide et ensuite on sélectionne :
 La passerelle de réseau virtuel et local
 On y insère la clé partagée créée par Google juste avant

Accueil > Connexions >

Créer une connexion ...

De base Paramètres Étiquettes 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

Passerelle de réseau local * ⓘ

LocalGW

Clé partagée (PSK) * ⓘ

L7iKGLXmBUNMfXWmpN5AYT5f4rsvMll7



la clé partagée créée par Google juste avant

Protocole IKE ⓘ

IKEv1 IKEv2

Utiliser l'adresse IP privée Azure ⓘ

Activer BGP ⓘ

Stratégie IPsec/IKE ⓘ

Par défaut Personnalisé

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

Associations de règles NAT

Associez les règles NAT qui ont déjà été configurées sur la ou les passerelles réseau virtuel connectées.

Règles NAT entrantes

0 sélectionné

Règles NAT sortantes

0 sélectionné

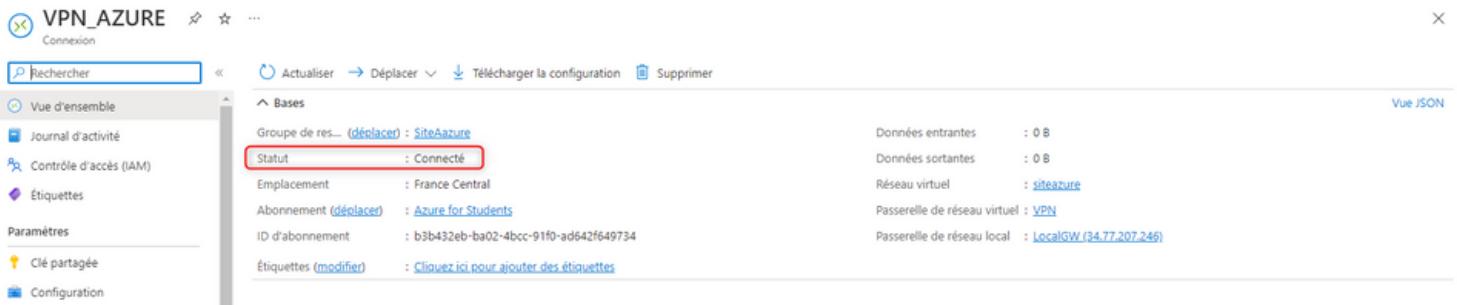
Vérifier + créer

Précédent

Suivant : Étiquettes >

Télécharger un modèle pour automation

On vérifie la connexion :

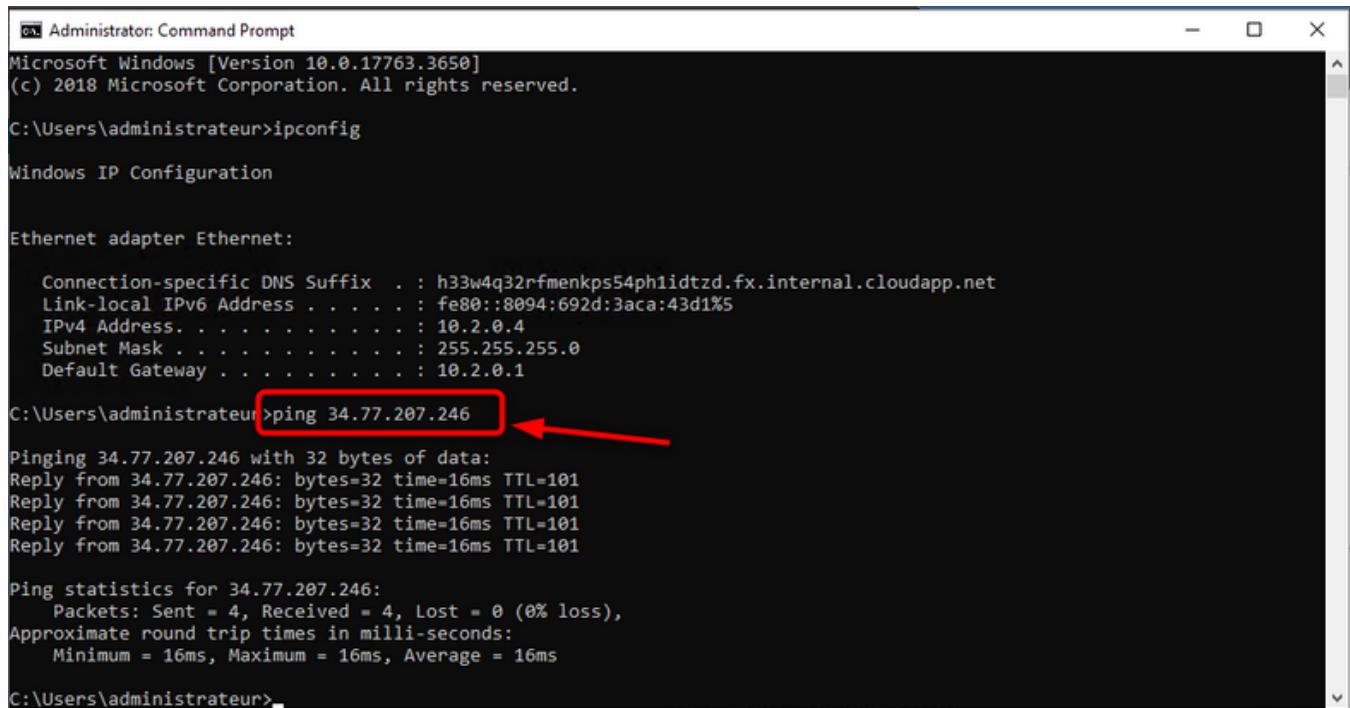


The screenshot shows the Azure portal interface for a VPN connection named "VPN_AZURE". The status is listed as "Connecté". Other details include:

- Groupe de ressources (déplacé) : SiteAzure
- Emplacement : France Central
- Abonnement (déplacé) : Azure for Students
- ID d'abonnement : b3b432eb-ba02-4bcc-91f0-ad642f649734
- Étiquettes (modifier) : Cliquez ici pour ajouter des étiquettes
- Données entrantes : 0 B
- Données sortantes : 0 B
- Réseau virtuel : siteazure
- Passerelle de réseau virtuel : VPN
- Passerelle de réseau local : LocalGW (34.77.207.246)

3. VÉRIFICATIONS DE COMMUNICATION

On peut maintenant tester le ping d'une machine à l'autre :



```

Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.3650]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\administateur>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : h33w4q32rfmenkps54ph1idtzd.fx.internal.cloudapp.net
Link-local IPv6 Address . . . . . : fe80::8094:692d:3aca:43d1%5
IPv4 Address . . . . . : 10.2.0.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 10.2.0.1

C:\Users\administateur>ping 34.77.207.246
Pinging 34.77.207.246 with 32 bytes of data:
Reply from 34.77.207.246: bytes=32 time=16ms TTL=101

Ping statistics for 34.77.207.246:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 16ms, Average = 16ms

C:\Users\administateur>

```



IV. AZURE DS



créer un Azure AD Domain Services :

Accueil > Azure AD Domain Services >

Créer Azure AD Domain Services ...

* De base * Mise en réseau Administration Synchronisation Paramètres de sécurité Étiquettes Vérifier + créer

Azure AD Domain Services fournit des services de domaine managé comme la jonction de domaine, la stratégie de groupe, LDAP et l'authentification Kerberos/NTLM. Vous pouvez utiliser Azure AD Domain Services sans avoir besoin de gérer, de corriger ou de dépanner les contrôleurs de domaine dans le cloud. Pour simplifier, les valeurs par défaut ont été spécifiées pour fournir un déploiement en un clic. [En savoir plus](#)

Détails du projet

Quand vous choisissez les informations de base nécessaires à Azure AD Domain Services, n'oubliez pas que l'abonnement, le groupe de ressources, le nom de domaine DNS et l'emplacement ne peuvent pas être modifiés après la création.

Abonnement *	Azure subscription 1
Groupe de ressources *	<input type="text" value="azuresite"/> Créer nouveau

[M'aider à choisir l'abonnement et le groupe de ressources](#)

Nom de domaine DNS *	<input type="text" value="hassanmoumd.onmicrosoft.com"/>
----------------------	--

[M'aider à choisir le nom DNS](#)

Région *	France Central
----------	----------------

Référence *	Enterprise
-------------	------------

[M'aider à choisir une référence SKU](#)

Type de forêt *	<input checked="" type="radio"/> Utilisateur <input type="radio"/> Ressource
-----------------	--

[M'aider à choisir un type de forêt](#)

[Vérifier + créer](#)

[Précédent](#)

[Suivant](#)

La création de ce ADDS nécessite un réseau en : 10.0.0.0/8
Par défaut, il nous le propose, ce qui aurait pu être le point de départ du réseau virtuel de notre TP.

Accueil > Azure AD Domain Services >

Créer Azure AD Domain Services

* De base *** Mise en réseau** Administration Synchronisation Paramètres de sécurité Étiquettes Vérifier + créer

Azure AD Domain Services utilise un sous-réseau dédié à l'intérieur d'un réseau virtuel pour contenir toutes ses ressources. Si vous utilisez un réseau existant, assurez-vous que la configuration réseau ne bloque pas les ports nécessaires à l'exécution d'Azure AD Domain Services. [En savoir plus](#)

Réseau virtuel * ⓘ

(nouveau) ADDS

Créer


[M'aider à choisir le réseau virtuel et l'adresse](#)

Sous-réseau * ⓘ

(nouveau) ADDSSubnet (10.0.0.0/16)


[M'aider à choisir le sous-réseau et le NSG](#)

i Un groupe de sécurité réseau sera automatiquement créé et associé au sous-réseau pour protéger les services de domaine AAD. Le groupe de sécurité réseau sera configuré en fonction de [instructions de configuration des NSG](#).

Créer Azure AD Domain Services

* De base * Mise en réseau Administration Synchronisation Paramètres de sécurité Étiquettes **Vérifier + créer**

De base

Nom	hassanmoumd.onmicrosoft.com
Abonnement	Azure subscription 1
Groupe de ressources	azuresite
Région	France Central
Référence	Enterprise
Type de forêt	Utilisateur

Réseau

Réseau virtuel	(nouveau) ADDS
Sous-réseau	(nouveau) ADDSSubnet
Adresse de sous-réseau	10.0.0.0/16
Groupe de sécurité réseau	(nouveau) aadds-nsg

Groupe des administrateurs

Groupe des administrateurs	AAD DC Administrators
Type d'appartenance	Affecté(s)

Notifications

Notifier les administrateurs généraux	Oui
Notifier le groupe d'administrateurs DC AAD	Oui

Synchronisation

Étendue de la synchronisation

Tout



Créer

Précédent

Suivant

Télécharger un modèle pour automation

On peut vérifier et valider

Créer Azure AD Domain Services ...

You devez savoir...

Les choix suivants sont définitifs et ne peuvent pas être modifiés après la création.

- Nom DNS
- Abonnement
- Groupe de ressources
- Réseau virtuel
- Sous-réseau
- Type de forêt

Cliquez sur OK pour continuer à créer Azure AD Domain Services.



Le déploiement de cet ADDS met un peu de temps.

Une fois fini, on met à jour le DNS afin de permettre aux VMs d'utiliser ce domaine

Required configuration steps



Update DNS server settings for your virtual network

Update the DNS server settings for your virtual network to point to the IP addresses (10.0.1.5 and 10.0.1.4) where Azure AD Domain Services is available.

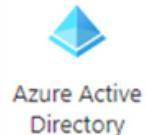
[More information](#)

A blue rectangular button with the word "Configure" in white text, enclosed in a red rectangular border.

1. CRÉATION D'UTILISATEUR

Créer un utilisateur et se connecter à son compte.

La première étape est de le créer en se rendant sur :



Ensuite, dans utilisateurs aller sur nouvel utilisateur et spécifier les propriétés de cet utilisateur en y indiquant éventuellement ses groupes, rôles etc...

Nouvel utilisateur

Répertoire par défaut

 Des commentaires ?

 L'invitation et la création en bloc se trouvent désormais sous l'élément de menu « Opérations en bloc » dans la vue « Tous les utilisateurs ». [Afficher tous les utilisateurs](#)

Sélectionner un modèle

Crée un utilisateur

Créez un utilisateur dans votre organisation.

Inviter un utilisateur

Invitez un nouvel utilisateur invité à collaborer avec votre organisation. L'utilisateur reçoit par e-mail une invitation qu'il peut accepter

[Aidez-moi à choisir](#)

Identité

Nom d'utilisateur * 

hassan.moumd  @ hassanmoumd1@gmail.on... 

Le nom de domaine dont j'ai besoin n'est pas affiché ici

Nom * 

Moumd 

Prénom

Hassan 

Nom de famille

Mot de passe

Générer automatiquement le mot de passe

Me permettre de créer le mot de passe

Mot de passe initial * 

***** 

Créer

Le mot de passe initial sera changé lors de la toute première connexion de l'utilisateur. Lorsqu'une connexion est établie par l'utilisateur, nous avons à disposition un journal de connexions :

Utilisateurs ...

Nouvel utilisateur | Télécharger les utilisateurs | Opérations en bloc | Actualiser | Gérer l'affichage | Supprimer | MFA par utilisateur | Fonctionnalités d'évaluation | Des commentaires ?

Tous les utilisateurs (préversion)

Vous souhaitez revenir à l'expérience de liste des utilisateurs hérités ? Cliquez ici pour quitter l'aperçu.

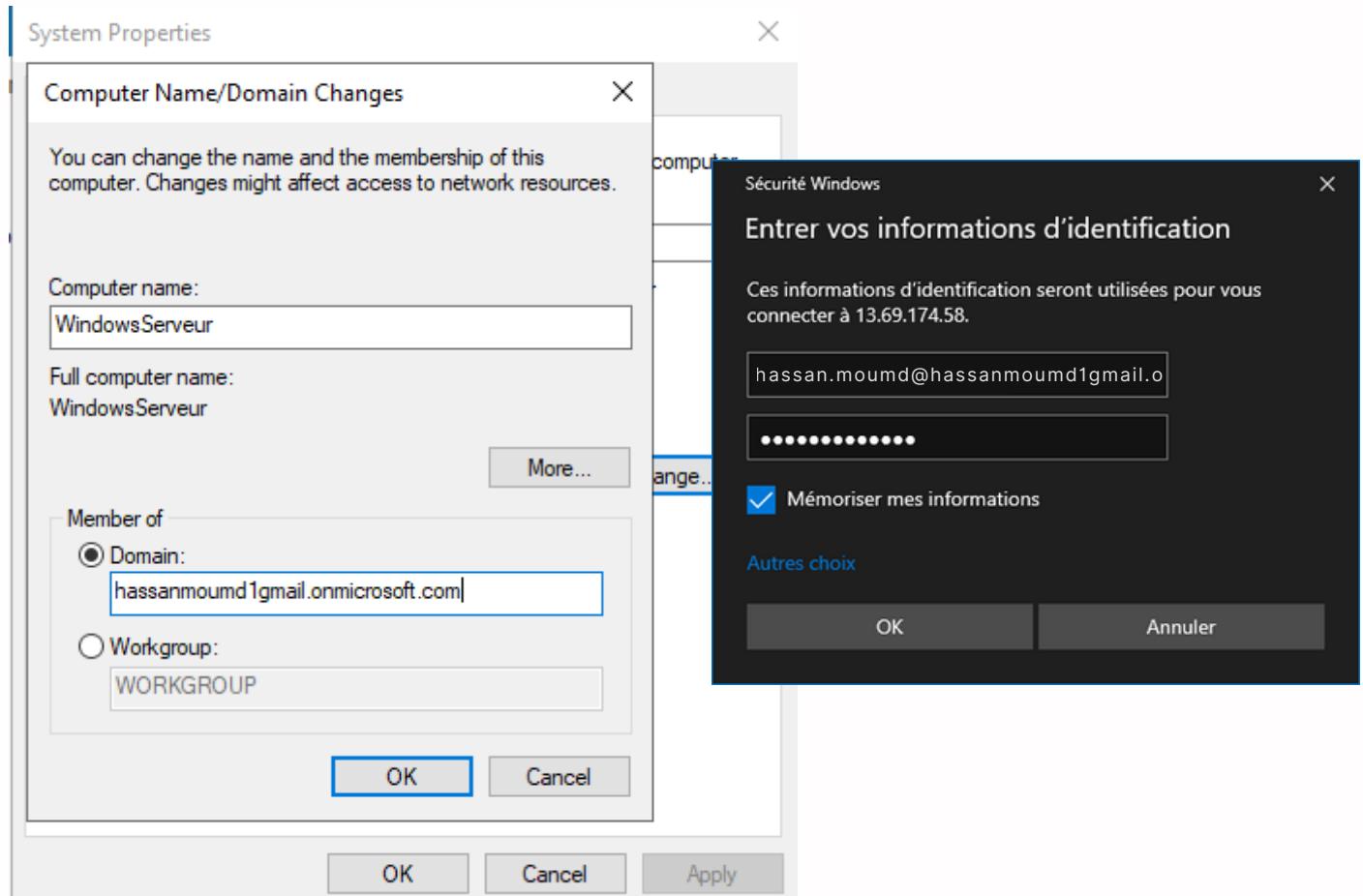
Rechercher	Ajouter un filtre					
2 utilisateurs trouvés						
<input type="checkbox"/> Nom d'affichage : HAS SAN	Nom d'utilisateur principal hassanmoumd1_gmail.co...	Type d'utilisateur Membre	Synchronisatio...	Identités MicrosoftAccount	Nom de l'entreprise	Type de création
<input type="checkbox"/> MO Moumd	hassan.moumd@hassanm...	Membre	Non	hassanmoumd1gmail.onmicrosoft		

Gérer

- Journaux d'audit
- Journaux de connexion
- Diagnostiquer et résoudre les problèmes
- Utilisateurs supprimés (préversion)
- Réinitialisation du mot de passe
- Paramètres utilisateur
- Résultats de l'opération en bloc

2. AJOUT D'UN WINDOWS SERVEUR DANS LE DOMAINE AZURE

Pour cela, on prend n'importe quelle machine virtuelle dans le sous réseau de l'AD (même via VPN), on s'y connecte en RDP ou Bastion pour ajouter de la sécurité, puis on l'ajoute au domaine simplement :



On y rentre un compte admin du domaine, ici, on utilise l'adresse mail : hassanmoumd1@gmail.onmicrosoft.com avec le mot de passe qui va avec.