



RAPPORT DE STAGE

Diplôme BTS – Services Informatiques aux Organisations option SLAM
session 2023

ARTHUR Félix-Vincent

Du 30 mai 2022 au 24 juin 2022

Tuteur de stage : MONTIGNAC Robin

Description de l'entreprise :

AG2R La Mondiale est une société de groupe d'assurance mutuelle, de protection sociale et patrimoniale, à but non lucratif. Sa gouvernance repose sur le paritarisme et le mutualisme.

Établissement/Formation

Lycée Fulbert
BTS – Services Informatiques
aux Organisations option
SLAM

Entreprise d'accueil :

AG2R La Mondiale
12 Rue Edmond Poillot,
28000, Chartres
Tel: 09.74.50.12.34

SOMMAIRE

Table des matières

I – Introduction :	3
1.1 – Résumé :	3
1.2 – Présentation de l’entreprise :	3
1.3 – Objectifs du stage :	4
1.4 – Outils et technologies utilisés	4
II – Analyse du domaine de l’étude & Enjeux stratégiques :	5
III – Les missions :	6
1.1 – Découverte et appropriation de Microsoft Azure :	6
1.2 – Création et utilisation d’un groupe de ressource :	6
1.3 – Création d’une machine virtuelle	7
1.4 – Création d’une API pour Terraform :	7
1.5 – Création de mon premier script Terraform :	7
1.6 – Déploiement d’une infrastructure sur Microsoft Azure à la main :	8
1.7 – Déploiement d’une infrastructure sur Microsoft Azure grâce à Terraform :	9
1.8 – Les tickets d’incidents sur CASSIUS	11
IV – Présentation et justification de la méthodologie de travail suivie : ..	12
V – Synthèse des compétences métiers développées lors du stage :	13
VI - Bilan professionnel et personnel quant à l'expérience vécue en guise de conclusion :	13
VII - Glossaire	14
VIII – Annexes :	16
ANNEXE 1 : Création d’un groupe de ressource sur Microsoft Azure .	16
ANNEXE 2 : Fonctionnement de Terraform	16
ANNEXE 3 : Microsoft Azure Active Directory	17
ANNEXE 4 : API Terraform	17
ANNEXE 5 : Les fichiers Terraform	17
ANNEXE 6 : Script Terraform pour créer un groupe de ressource	18
ANNEXE 7 : Plan réseau	18
ANNEXE 8 : Peerings sur Microsoft Azure	19
ANNEXE 9 : Le protocole RDP	19

ANNEXE 10 : Règles de pare-feu	19
ANNEXE 11 : Script Terraform vnet.....	20
ANNEXE 12 : Script Terraform subnet	20
ANNEXE 13 : Script Terraform peering	21
ANNEXE 14 : Script Terraform machine virtuelle	21
ANNEXE 15 : Script Terraform interface réseau	22
ANNEXE 16 : Les règles de pare-feu.....	22

I – Introduction :

1.1 – Résumé :

Dans le cadre de mes études informatiques (BTS Services Informatiques aux Organisations) au Lycée Fulbert, je dois effectuer un stage en entreprise d'une durée d'un mois (30 mai au 24 juin).

Ce stage me permettra de mettre en œuvre les compétences ainsi que les connaissances acquises durant la première année de ma formation. Faire un stage dans une entreprise comme AG2R LA MONDIALE me permet, également d'apprendre et de découvrir de nouvelles choses.

1.2 – Présentation de l'entreprise :

J'ai effectué mon stage dans l'entreprise AG2R LA MONDIALE. AG2R LA MONDALE est un organisme spécialisé dans la protection sociale et patrimoniale. C'est un groupe paritaire et mutualiste. L'entreprise assure les personnes pour les protéger face aux aléas de la vie.

Depuis 115 ans, l'entreprise assure plus de 15 millions de clients particuliers et plus de 500 entreprises pour préparer leur retraite, préserver leur santé et celle de leurs proches. AG2R LA MONDIALE est spécialisé dans plusieurs domaines comme par exemple :

- La retraite complémentaire
- La retraite supplémentaire
- La prévoyance
- La santé
- L'assurance-vie

Avec ses 12 000 collaborateurs dont plus de 1000 personnes dans le SI, le groupe s'est installé sur l'ensemble du territoire français comme à Tours, Chartres, Paris etc...

Le but de l'entreprise c'est de répondre à tous les besoins de protections pour une personne ou une entreprise.

AG2R LA MONDIALE de Chartres dispose d'un datacenter pour ses applications et ses traitements, mais le principal datacenter se trouve à Aubert-Villiers qui gère les stockages, héberge les sites internet etc...

1.3 – Objectifs du stage :

Mon stage chez AG2R LA MONDIALE avait pour objectif de me faire découvrir dans un premier temps le Cloud Computing par le biais de Microsoft Azure. Ensuite, de concevoir et de déployer une infrastructure réseau dans le Cloud manuellement avec le portail Microsoft Azure et ensuite l'automatiser grâce à un outil développé par HashiCorp qui est Terraform.

Mon tuteur de stage voulait me faire travailler sur Terraform pour montrer aux autres collaborateurs que Terraform est un outil simple d'utilisation. Il voulait montrer en à peine 1 mois, il est possible de faire des grosses infrastructures automatisées.

Dans l'entreprise, personne ne s'est lancé pour faire du Terraform. Donc, mon maître de stage en a profité que je sois là pour m'en faire faire et inciter les autres collaborateurs de l'entreprise à faire du Terraform.

Pour finir, mon tuteur de stage et moi avons résolu quelques tickets d'incidents via CASSIUS. CASSIUS est un outil qui permet d'ouvrir, gérer, traiter les tickets d'incidents.

1.4 – Outils et technologies utilisés

Tout au long de mon stage j'ai utilisé les outils suivants :

- Microsoft Teams
- Office 365
- Remote Desktop Manager
- Le serveur Bastion de l'entreprise CYBERARK
- Terraform v1.2.4

II – Analyse du domaine de l'étude & Enjeux stratégiques :

La direction de l'organisation et des systèmes d'information d'AG2R LA MONDIALE à Chartres est organisée en six groupes. Les deux premiers groupes contrôlent les systèmes d'information et recherchent s'il y a des anomalies etc... C'est à cet endroit qu'on effectue des simulations et des tests de sécurité (SECURITE & CONTINUITE DU SI et PILOTAGE & PERFORMANCE).

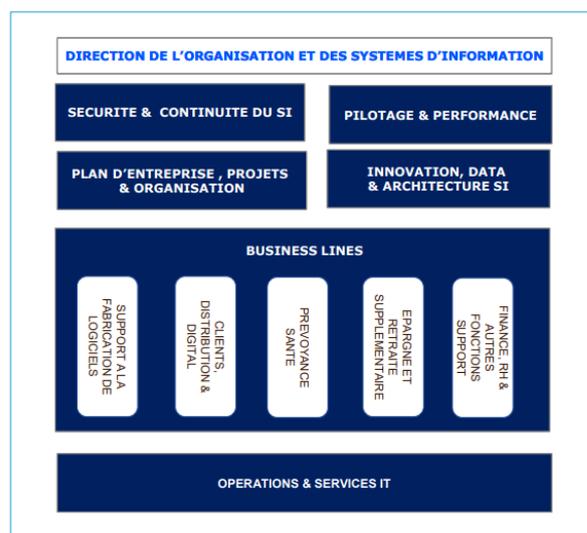
Le troisième et le quatrième groupe s'occupent de la gestion des projets, de l'organisation et des plans d'entreprises, mais également des données de l'entreprise et de l'architecture du système d'information (PLAN D'ENTREPRISE, PROJETS & ORGANISATION et INNOVATION, DATA & ARCHITECTURE SI).

Le cinquième groupe, c'est le cœur de l'entreprise, c'est les « Business Lines ». Les services proposés par l'entreprise sont traités ici.

Pour finir le dernier groupe s'occupe du développement, du traitement des solutions IT. Il y a deux services dans ce groupe : Service Windows Annuaires et Service Linux (OPERATIONS & SERVICES IT) c'est là que se trouve mon maître de stage.

L'entreprise AG2R LA MONDIALE à Chartres est le site qui contient le PRA : Plan de Relance d'Activité. S'il y a un événement qui impacte un site, le site qui a des dommages peut reprendre son activité à 70 % grâce au datacenter qui se trouve au sous-sol. Toutefois, le plus gros datacenter d'AG2R LA MONDIALE se situe à Aubert-Villiers.

Schéma représentant la direction de l'organisation et des systèmes d'information au sein de l'entreprise AG2R LA MONDIALE :



III – Les missions :

1.1 – Découverte et appropriation de Microsoft Azure :

Les premiers jours de stage, j'avais pour but de découvrir Azure et les outils qui sont sur mon poste de travail. Mon maître de stage m'a créé un compte sur Microsoft Azure pour découvrir ce dernier.

Microsoft Azure permet aux entreprises de regrouper l'ensemble de ses services dans le cloud. L'avantage de ce dernier c'est qu'il permet aux entreprises, aux organisations d'accéder aux ressources informatiques sans investir dans les Datacenter ou à gérer les serveurs, cela signifie qu'ils n'y ont quasiment plus de serveurs physiques gérés par l'entreprise.

De plus, l'entreprise paye Azure qu'à la consommation des ressources sur Azure

Tout comme Microsoft Azure, il y a d'autres concurrents sur le marché du Cloud Computing, on y trouve en particulier : Amazon Web Services (AWS), Alibaba, Google Cloud Platform et récemment le groupe OVH qui s'est lancé dans ce domaine.

Amazon le leader incontesté dans ce domaine. Microsoft Azure le rattrape peu à peu grâce à ses fonctionnalités et ses services.

1.2 – Création et utilisation d'un groupe de ressource :

Pour ma première mission mon maitre de stage m'a demandé de regarder la documentation de Microsoft Azure et de créer un groupe de ressource ([ANNEXE 1](#)).

Le groupe de ressource, inclut les ressources que l'entreprise veut gérer comme groupe.

J'ai appelé mon groupe de ressource : **rg-win-np-fr-001** en suivant une nomenclature.

rg: Resource group **win**: Windows **np**: Non-Production **fr**: France

001 : instance

Par exemple, l'entreprise peut décider de mettre dans un groupe de ressource, un ensemble des machines virtuelles pour mettre à disposition pour une partie du système d'information et ainsi de suite.

1.3 – Création d'une machine virtuelle

Après avoir créé un groupe de ressource, j'ai déployé un Windows Server 2019 Datacenter directement depuis le portail Azure pour comprendre et apprendre à déployer des ressources manuellement avant d'automatiser cela avec Terraform ([ANNEXE 2](#)).

La création d'une machine virtuelle est assez simple sur Microsoft Azure puisque tout se fait en ligne sur le portail avec un navigateur.

Je me suis ensuite connecté à la machine que je venais de créer avec un outil qui utilise le protocole RDP port 3389.

1.4 – Création d'une API pour Terraform :

Après avoir installé Terraform sur mon poste de travail grâce à la documentation de Terraform, mon maitre de stage m'a demandé de chercher sur internet « comment Terraform peut-il déployer des services sur le cloud ? ».

Après avoir cherché quelques minutes, j'ai fini par trouver la documentation Terraform qui demande de créer une API pour permettre à Terraform de déployer sur Microsoft Azure.

J'ai créé mon API sous la rubrique Azure Active Directory. En effet, pour mettre à une application à effectuer des opérations sur le Cloud, il lui faut des droits spécifiques. On attribue des droits grâce à des groupes déjà créés par l'entreprise par des administrateurs réseaux. ([ANNEXE 3](#)) De plus, pour que l'API puisse ajouter des ressources il faut lui donner quelques informations concernant Microsoft Azure.

J'ai nommé mon Api : API_Azure_Terraform

Grâce à mon API, je peux maintenant utiliser Terraform pour pouvoir automatiser le déploiement de ressources. ([ANNEXE 4](#)).

1.5 – Création de mon premier script Terraform :

Pour mon premier script, mon maitre de stage m'a demandé de créer un groupe de ressource avec Terraform. Terraform est un outil très puissant

notamment grâce aux possibilités qu'il offre mais également par sa facilité de compréhension et d'utilisation.

Avant d'écrire mon code, j'ai cherché comment écrire mon code et comment le structurer.

Dans un premier temps, je suis allé sur les documentations de Terraform pour voir comment créer un code pour pouvoir déployer des composants sur Microsoft Azure.

Pour faire un script Terraform, il faut obligatoirement un fichier qu'on va appeler main.tf et il est vivement conseillé d'utiliser un deuxième fichier variables.tf qui permet de déclarer les variables et de leur attribuer les valeurs pour créer les ressources que l'on souhaite.

Si l'on souhaite externaliser les valeurs dans un autre fichier au lieu de les mélanger avec le fichier de variables.tf, il est tout à fait possible de faire un autre fichier qui va contenir les valeurs : nom_du_fichier.tfvars ([ANNEXE 5](#))

Ensuite, je suis passé à la pratique. J'ai créé un script Terraform permettant de créer un groupe de ressource sur Azure ([ANNEXE 6](#)).

1.6 – Déploiement d'une infrastructure sur Microsoft Azure à la main :

Mon maitre de stage m'a demandé de créer et de déployer entièrement une infrastructure réseau sur le cloud dans le domaine « préproduction » c'est-à-dire dans le domaine de test pour éviter de toucher le domaine de production.

Avant de faire les machines virtuelles, j'ai fait un schéma avec l'outil en ligne draw.io pour représenter l'infrastructure finale pour voir à quoi ça va ressembler ([ANNEXE 7](#)).

Mon maitre de stage m'a demandé de faire une DMZ qui va contenir une machine linux serveur WEB (Apache). Ensuite, un serveur bastion pour pouvoir accéder et administrer les serveurs qui se situe dans la DMZ et dans le LAN. Ces machines étaient regroupées dans différents vnet Il y a donc au total 3 vnet ([ANNEXE 7](#)).

- vnet LAN
- vnet DMZ
- vnet Bastion

Pour que les machines puissent communiquer, nous avons fait les peerings. Les peerings ce sont de liens qu'il faut appliquer pour que les

machines puissent communiquer dans le réseau et en dehors du réseau AG2R pour se connecter à Microsoft Azure. Sans les peerings, il est impossible de joindre les machines ([ANNEXE 8](#)).

Pour communiquer en toute sécurité, nous avons mis en place des règles de pare-feu pour bloquer certains protocoles. Par défaut, tous les ports sont bloqués. Pour administrer les serveurs linux, j'ai utilisé les clés SSH. On a utilisé le protocole SSH (port 22) pour administrer les serveurs linux. Pour ce qui est des serveurs Windows, on les a administrés par le protocole RDP avec des noms d'utilisateur et des mots passes. ([ANNEXE 9](#))

On a installé les serveurs WEB sur les serveurs linux qui se situent dans la DMZ, LAN et un IIS sur le serveur Windows qui se situe également dans la DMZ pour apprendre à utiliser différents services.

Pour le serveur Windows dans la DMZ, j'ai installé un IIS, mon maitre de stage m'a demandé de le faire à distance pour que ce soit plus intéressant avec un script PowerShell au lieu de le faire sur la machine directement. Le script PowerShell est :

Ligne de commande PowerShell :

```
Invoke-Command -ComputerName wtstagedmz -FilePath script.ps1
```

script.ps1 :

```
Install-WindowsFeature -name Web-Server IncludeManagementTools
```

Ensuite, j'ai ouvert le port 80 qui correspond au protocole http sur le pare-feu de chaque machine après l'installation d'apache ([ANNEXE 10](#))

Pour finir, après le déploiement sur Microsoft Azure, j'ai testé le fonctionnement des règles de pare-feu.

- On a utilisé les clés SSH pour se connecter sur les machines linux.
- Tester les règles de pare-feu sur chaque machine
- Tester les connexions entre les réseaux virtuels

1.7 – Déploiement d'une infrastructure sur Microsoft Azure grâce à Terraform :

Mon maitre de stage m'a demandé de faire l'infrastructure à la main pour comprendre et surtout prendre conscience du temps qu'il faut pour le faire depuis le portail Azure en effet, j'ai fait à la main :

- Le découpage réseau

- La configuration des machines
- Créer les vnet
- Créer les interfaces réseaux
- Créer les groupes de ressources
- Mettre en place les règles de pare-feu.

Après avoir testé l'infrastructure, mon maitre de stage m'a demandé de le refaire mais cette fois-ci avec Terraform. Comme j'ai compris le fonctionnement de Terraform, je me suis lancé sur la création de mon script qui est basé sur 2 fichiers : main.tf et variables.tf

Pour m'organiser dans mon code j'ai fait des ressources et des modules pour chaque ressource de l'infrastructure.

Dans mon fichier principal main.tf, j'ai commencé par créer mon groupe de ressource dans lequel, je vais mettre les 3 vnet et les subnets (sous-réseau) pour chaque domaine du réseau : DMZ, LAN, BASTION.

Ensuite j'ai créé les autres ressources pour faire mon infrastructure :

- Groupe de ressource ([ANNEXE 6](#))
- Les vnets ([ANNEXE 11](#))
- Les subnets ([ANNEXE 12](#))
- Les peerings ([ANNEXE 13](#))
- Les machines virtuels ([ANNEXE 14](#))
- Les interfaces réseaux ([ANNEXE 15](#))
- Les règles de pare-feu ([ANNEXE 16](#))

Pour exécuter mon script Terraform, il faut ouvrir une invite de commande ou PowerShell pour ensuite taper les commandes qui permettent d'exécuter le code.

Terraform est simple d'utilisation en effet les commandes principales sur Terraform sont :

- terraform init (permet d'initialiser et de télécharger les plugins nécessaires)
- terraform plan (permet d'afficher à l'utilisateur ce que le script va faire création/modification/suppression)
- terraform apply (va appliquer les opérations indiquées sur terraform plan)
- terraform destroy (permet de détruire/supprimer ce que l'on a fait)

J'ai rencontré quelques problèmes lors du déploiement avec Terraform.

1. Le premier c'est qu'il faut lier l'id du subnet dans la configuration de l'interface réseau. Cette liaison permet à la machine d'intégrer un réseau et dans un subnet précis.
2. Le deuxième problème c'est pour faire les peerings en effet, par exemple s'il on prend 2 réseau virtuel, il faut faire 2 peerings sur le réseau virtuel soit 4 peerings pour 2 réseau virtuel. Pour automatiser cela, j'ai fait une boucle for avec une liste d'information pour éviter de répéter un même code plusieurs fois mon fichier principal.

1.8 – Les tickets d'incidents sur CASSIUS

Pour ma dernière mission, j'ai fait quelques tickets d'incidents avec mon maître de stage. AG2R LA MONDIALE a un logiciel de gestion de tickets d'incident qui a été développé en interne. Le nom du logiciel est CASSIUS. Voilà à quoi ressemble CASSIUS :

The screenshot shows the CASSIUS interface with a list of incidents. The table below represents the data visible in the screenshot:

Numéro	Demandeur	Ouvert	Ouvert par	État	Description courte	Priorité	Groupe d'affectation
INC1329957	FAUCON DAVID	23/06/2022 11:00:04	(vide)	Ouvert	MICROSOFT TEAMS -- Fichier partagés plus présent sur TEAMS	P4	DOSIT IC SERVEURS WINDOWS RUN
INC1329870	POLLET SEBASTIEN	23/06/2022 10:10:43	(vide)	Ouvert	[TEST PSI] : INCIDENT - Application A0784	P4	DOSIT IC SERVEURS WINDOWS RUN
INC1328427	ALLAM KAMEL	21/06/2022 13:53:51	(vide)	Ouvert	QUESTION CONCERNANT LA FICHE DE CORRESPONDANCE VOIR PIECE JOINTE	P4	DOSIT IC SERVEURS WINDOWS RUN
INC1327300	COBAR IBRAHIMA	20/06/2022 10:20:43	(vide)	Ouvert	OUTLOOK -- Mails ne s'envoient pas	P1	DOSIT IC SERVEURS WINDOWS RUN
INC1327232	TOUMI LESLIE	20/06/2022 09:51:53	(vide)	Ouvert	[A2] MICROSOFT SHAREPOINT-affichage	P4	DOSIT IC SERVEURS WINDOWS RUN
		17/06/2022			Détection de multiples		DOSIT IC

The screenshot shows the detailed view of an incident (INC1327901) in the CASSIUS system. The form contains the following information:

- Numéro:** INC1327901
- Demandeur:** LIROCHON THIBAUD
- Bénéficiaire:** LIROCHON THIBAUD
- Site d'intervention:** CHARTRES-POILLOT
- Emplacement:** Sur site
- Poste:** (empty)
- Poste non trouvé:**
- Environnement EC:** Production
- Famille d'EC:** TECHNOLOGIES ET INFRASTRUCTU
- EC en cause:** NEWTEST
- Type de contact:** Supervision
- Si métier:** -- Aucun --
- État:** En cours
- Groupe d'affectation:** DOSIT IC INFRASTRUCTURES EXI
- Mauvaise Qualification:**
- Affecté à:** MONTIGNAC ROBIN
- Impact:** Faible
- Urgence:** Basse
- Priorité:** P4
- Non imputable DSI:**
- Communication:** (empty)

Ce logiciel permet d'ouvrir, de gérer et de traiter des tickets d'incidents. J'ai résolu quelques tickets d'incident, par exemple un utilisateur a bloqué son compte interne après plusieurs tentatives. Il a donc ouvert un ticket. Le ticket avait la même structure que la capture d'écran ci-dessus. J'ai donc récupéré son nom d'utilisateur et je lui ai renvoyé un mail pour déverrouiller son compte qui s'est bloqué par sécurité.

Les tickets d'incidents sont classés en fonction de l'impact et de l'urgence. Un compte bloqué n'a pas d'impact fort et d'urgence haute par exemple mais plutôt impact = Faible ; Urgence = Moyen

L'utilisation de ce logiciel m'a permis de revoir les notions ITIL et la gestion des tickets mais également de comprendre les processus de gestion des incidents jusqu'à la garantie de continuité des services informatiques.

IV – Présentation et justification de la méthodologie de travail suivie :

Pour pouvoir faire les missions que mon tuteur m'attribue, je commence par comprendre la mission en elle-même notamment l'objectif de ce dernier. Dans un premier temps, j'essaye de le faire sans aide pour voir si je peux faire la mission sans aide. Si je n'y arrive pas, je passe quelques minutes à regarder la documentation en ligne ou sinon des exemples sur internet.

Pour continuer, après mes recherches, je passe aux tests pour remplir les missions qu'on m'a attribuées. Si je ne réussis pas même avec de l'aide des documentations, je demande à mon maître de stage des pistes de recherches sans pour autant lui demander la réponse.

Très souvent j'arrive à me débrouiller pour finir ma mission, mais lorsque c'est très difficile, je passe voir la documentation.

Durant ces 4 semaines des stages, il m'est arrivé plusieurs fois de rester sur une ou plusieurs erreurs pendant plusieurs jours comme par exemple Terraform. Pour déboguer ces problèmes, je peux passer plusieurs heures pour comprendre les erreurs mais quand j'ai vraiment beaucoup de mal je demande de l'aide à mon tuteur de stage ainsi qu'à ses autres collègues.

Je trouve que ma méthode de travail permet d'apprendre plein de choses tout en continuant les missions qu'on m'a conseillées. Lorsque j'ai des problèmes, je peux compter sur les documentations en ligne ou de l'aide des personnes dans l'entreprise même s'ils sont dans un autre domaine.

V – Synthèse des compétences métiers développées lors du stage :

Tout au long de mon stage, j'ai mobilisé mes connaissances pour chaque mission. J'ai également développé et découvert de nouvelles choses. J'ai recensé, identifié des ressources informatiques que ce soit physique ou numérique et vérifié les niveaux d'habilitations des utilisateurs sur différents services sur Microsoft Azure. Pour continuer, j'ai collecté, suivi, et traité des tickets d'incidents des clients avec CASSIUS. Ensuite, j'ai participé à des réunions sur Microsoft Teams et à des projets en groupe. De plus, j'ai mis à disposition des ressources informatiques pour plusieurs groupes de personnes du système d'information dans le cloud. Pour finir, j'ai mis en place mon environnement de travail, mettre en place un calendrier pour faire mes missions, un gestionnaire de version GitLab avec mon maître de stage pour créer, modifier mon code Terraform.

VI - Bilan professionnel et personnel quant à l'expérience vécue en guise de conclusion :

Pour conclure, ce stage en entreprise fût une expérience très enrichissante, à la fois d'un point de vue personnel et professionnel. Mon intégration dans l'équipe Windows Annuaire, c'est très bien passé, il y a même une personne qui a fait le BTS SIO à Fulbert.

Tout au long de mon stage, j'ai remarqué que l'informatique est certes très importante, mais ce qui est le plus important, c'est la communication et les informations qu'on partage avec d'autres personnes pour le bon avancement des mission/projet en effet, j'étais amené à travailler avec différentes personnes qui sont issues de différents corps de métiers.

J'ai eu l'occasion de travailler en équipe avec d'autres personnes dans l'entreprise notamment dans le service Linux. Ce stage m'a permis de développer mes compétences de Devops pour le futur.

D'un point de vue professionnel, pouvoir travailler en toute autonomie m'a beaucoup aidé en effet, lorsque j'avais des problèmes, je devais me débrouiller tout seul, ce qui m'a permis d'être plus autonome.

D'un point de vue personnel, ce stage m'a permis de consolider mes connaissances en réseau et du cloud.

Mon maître de stage ainsi que ses autres collègues ont été surpris de voir un élève de BTS SIO de première année avoir des connaissances en réseau ainsi qu'en développement. Les compétences acquises durant ma

première année m'ont beaucoup servi dans ce stage et me serviront dans le futur.

Pour finir, ce stage m'a permis d'améliorer mes méthodes de travail et m'a poussé à travailler en équipe avec des personnes que je ne connais pas. Je suis satisfait des missions qu'on m'a confiées.

VII - Glossaire

A

API

Une API, ou interface de programmation d'application, est un ensemble de définitions et de protocoles qui facilite la création et l'intégration de logiciels d'applications., **2, 7, 17**

B

Bastion

un bastion informatique vise à protéger un réseau ou une partie d'un réseau de menaces extérieures, **8, 18**

C

Cloud Computing

Le Cloud Computing est la pratique consistant à fournir des services informatiques à distance, en les hébergeant dans un ou plusieurs centres de données externes plutôt que sur des serveurs dédiés sur place, **4**

D

DMZ

En informatique, une zone démilitarisée (ou DMZ) fait référence à un sous-réseau qui héberge les services exposés et accessibles de l'extérieur d'une entreprise. Elle agit comme une zone tampon avec les réseaux non sécurisés tels qu'Internet., **8, 9, 10, 18**

G

groupe de ressource

Un groupe de ressources est un conteneur réunissant les ressources associées d'une solution Azure. Le groupe de ressources peut inclure toutes les ressources d'une solution., **2, 6, 7, 8, 10, 16, 18**

I

IIS

Internet Information Services, communément appelé IIS, est un serveur Web des différents systèmes d'exploitation Windows NT, **9**

L

LAN

Le LAN ou Local Area Network est un réseau informatique physique et/ou virtuel. Il permet d'interconnecter par Wi-Fi ou câbles Ethernet des terminaux entre eux. Le LAN peut aussi se connecter à l'extérieur grâce à un accès Internet., **8, 9, 10, 18, 20, 21**

M

Microsoft Azure

Microsoft Azure est une plateforme cloud. Elle regroupe les services du Cloud Computing. On peut y trouver des solutions open-sources, les applications propriétaires Microsoft et même nos propres applications., **4, 6, 7, 8, 9, 16, 17, 18**

P

peerings

Le peering est l'interconnexion qui existe entre un réseau et le réseau mondial de Microsoft, à des fins d'échange de trafic Internet entre les services en ligne Microsoft et les services Microsoft Azure., **8, 10**

R

RDP

Remote Desktop Protocol (RDP) est un protocole qui permet à un utilisateur de se connecter sur un serveur exécutant Microsoft Terminal Services., **2, 7, 9, 19**

ressources

Une ressource ou un module est une entité d'un service (cloud ou pas). De multiples ressources forment ainsi une infrastructure. Chaque type de ressource est fournie par un provider, qui est en fait un plugin Terraform. Quant aux modules, le module peut faire appel à plusieurs ressources., **6, 7, 8, 9, 10**

S

SSH

SSH signifie Secure SHell. C'est un protocole qui permet de faire des connexions sécurisées (i.e. cryptées) entre un serveur et un client SSH, **8, 9**

subnet

Un subnet ou en français un sous-réseau, est un réseau à l'intérieur d'un réseau. Les sous-réseaux rendent les réseaux plus efficaces. Grâce au subnetting, le trafic réseau peut parcourir une distance plus courte sans passer par des routeurs inutiles pour arriver à destination., **3, 10, 20**

T

Terraform

Terraform est un outil qui permet de déployer des ressources sur le cloud. Il permet de créer des composants dans le cloud à partir du code c'est ce que l'on appelle l'infra-as-code., **4, 7, 8, 9, 10, 12, 16, 17, 18, 20, 21**

V

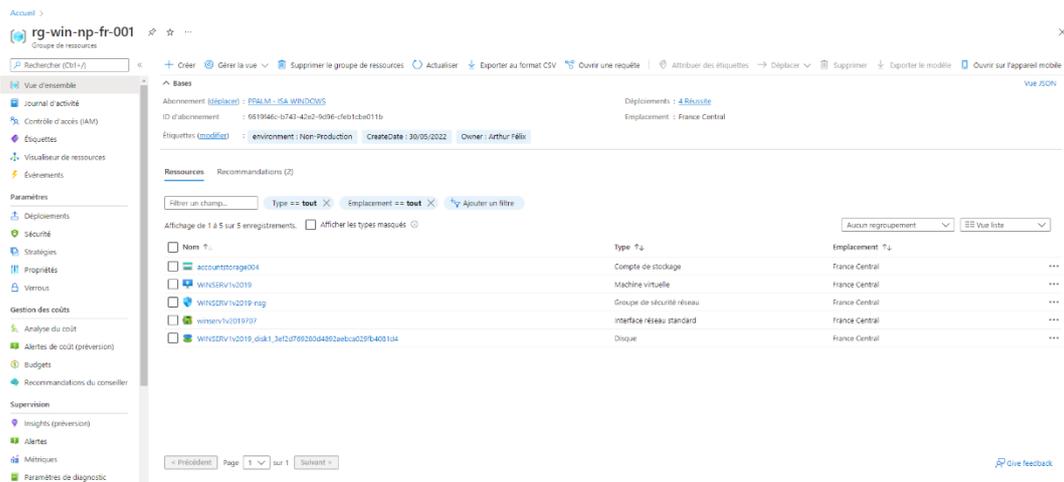
vnet

Le réseau virtuel est similaire à un réseau traditionnel et permet à de nombreux types

de ressources Azure, telles que les machines virtuelles (VM) Azure, de communiquer de manière sécurisée entre elles, avec Internet et avec les réseaux locaux., **8, 9, 10, 20**

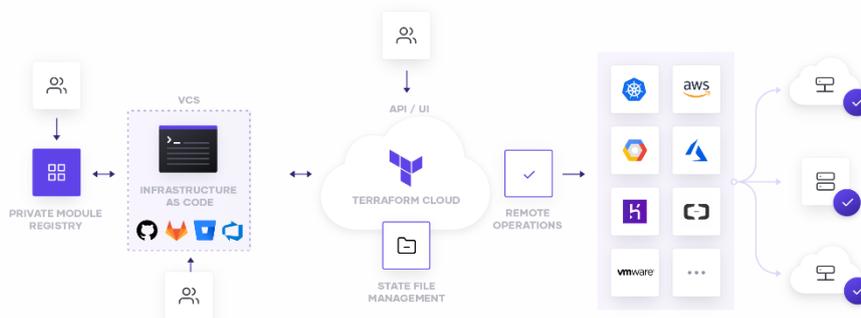
VIII – Annexes :

ANNEXE 1 : Création d'un groupe de ressource sur Microsoft Azure



Légende : Capture montrant le contenu d'un groupe de ressource

ANNEXE 2 : Fonctionnement de Terraform



Légende : Image montrant le fonctionnement de Terraform et ses options avec différents providers

ANNEXE 3 : Microsoft Azure Active Directory

The screenshot shows the 'Utilisateurs' (Users) page in the Microsoft Azure portal. A table lists 457 users with columns for Name, User Principal Name, User Type, Password Synchronized, Account Active, Issuer of Identity, Organization Name, and Creation Type. A blue box highlights a portion of the table.

Nom	Nom d'utilisateur prin...	Type d'utilisateur	Annuaire synchronisé	Compte actif	Emetteur d'identité	Nom de l'entreprise	Type de création
ADMSTR01		Membre	Oui	Non	psa@psa.microsoft.com		
ADMSTR02		Membre	Oui	Non	psa@psa.microsoft.com	GIE LA MONDIALE GROU...	
ADMSTR03		Membre	Oui	Non	psa@psa.microsoft.com	GIE LA MONDIALE GROU...	
ADMSTR04		Membre	Oui	Non	psa@psa.microsoft.com	GIE AZR	
ADMSTR05		Membre	Oui	Non	psa@psa.microsoft.com	GIE AZR	
ADMSTR06		Membre	Oui	Non	psa@psa.microsoft.com	GIE LA MONDIALE GROU...	
ADMSTR07		Membre	Oui	Non	psa@psa.microsoft.com	SYSTAJANS	
ADMSTR08		Membre	Oui	Non	psa@psa.microsoft.com		
ADMSTR09		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR10		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR11		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR12		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR13		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR14		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR15		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR16		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR17		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR18		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR19		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR20		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR21		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR22		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR23		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR24		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR25		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR26		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR27		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR28		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR29		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR30		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR31		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR32		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR33		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR34		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR35		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR36		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR37		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR38		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR39		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR40		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR41		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR42		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR43		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR44		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR45		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR46		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR47		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR48		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR49		Membre	Non	Oui	psa@psa.microsoft.com		
ADMSTR50		Membre	Non	Oui	psa@psa.microsoft.com		

Légende : Capture montrant l'accueil de l'Active Directory de Microsoft Azure avec la liste des utilisateurs et le type de compte de la préproduction.

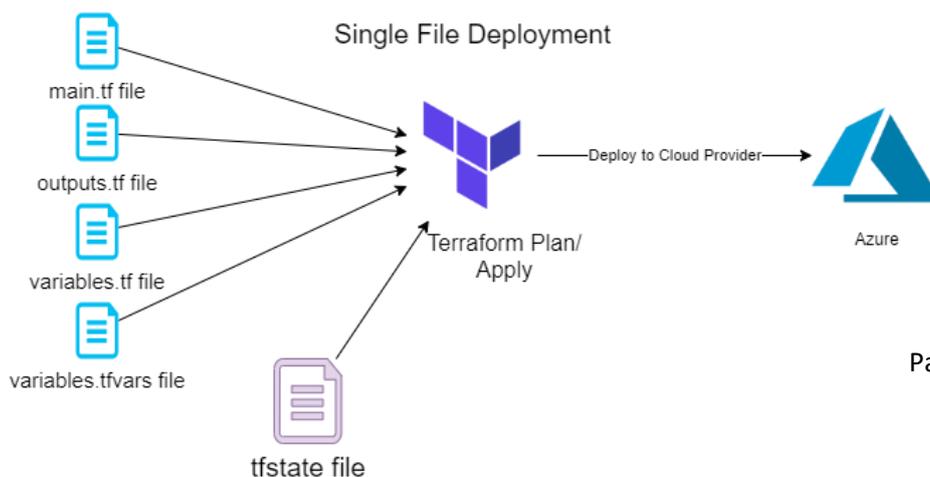
ANNEXE 4 : API Terraform

The screenshot shows the 'Certificats & secrets' page for an API in the Microsoft Azure portal. It displays a table of secrets with columns for Description, Date d'expiration, Valeur, and ID de secret.

Description	Date d'expiration	Valeur	ID de secret
Password uploaded on Tue May 31 2022	01/12/2022	msU*****	2e9d273b-4ab1-40f9-b23a-b2d0d92b7f
Password uploaded on Tue May 31 2022	01/12/2022	WFRQ-a1_FyhndRyYKpRQSiR_6d9M...	f2e41082-b63d-4336-92c9-2c0f1282a768

Légende : API permettant à Terraform de pouvoir déployer des services sur Azure grâce à l'authentification par clé.

ANNEXE 5 : Les fichiers Terraform



Légende : Schéma représentant les fichiers requis pour créer un script Terraform :

Le fichier main.tf est obligatoire. Par contre les fichiers output.tf, variables.tf, variables.tfvars sont facultatif.

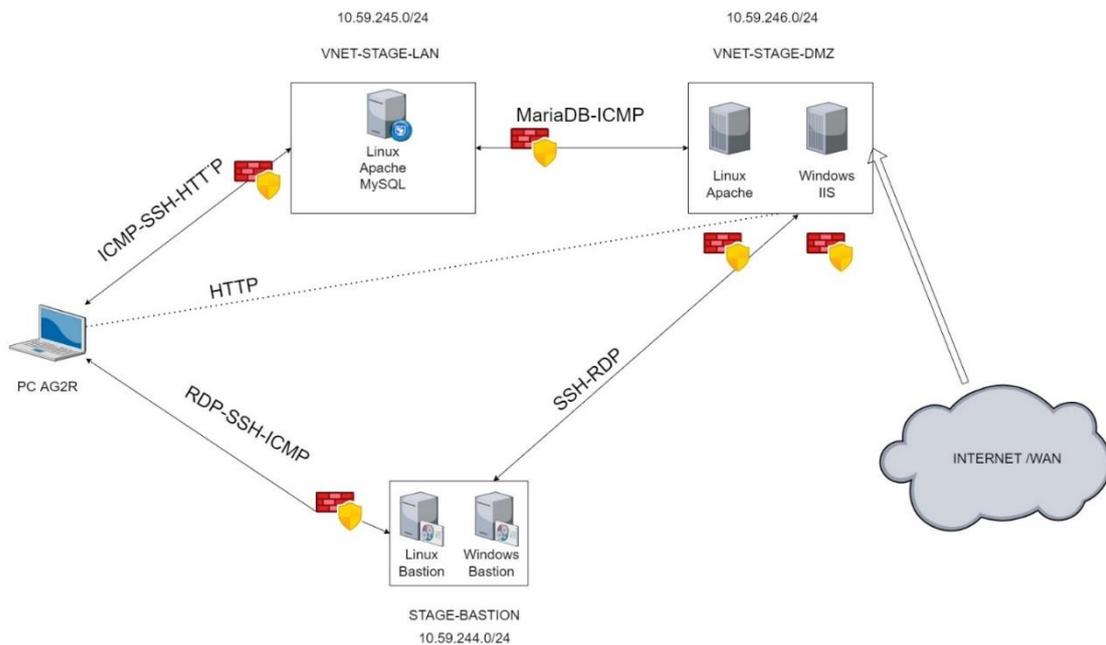
Pour tfstate, le fichier sera généré automatiquement lors de l'exécution de la commande terraform init

ANNEXE 6 : Script Terraform pour créer un groupe de ressource

```
resource "azurerm_resource_group" "grp_resource" {  
  name = "rg-win-np-fr-002"  
  location = "francecentral"  
}
```

Légende : Capture d'un script qui va créer un groupe de ressource sur Microsoft Azure.

ANNEXE 7 : Plan réseau



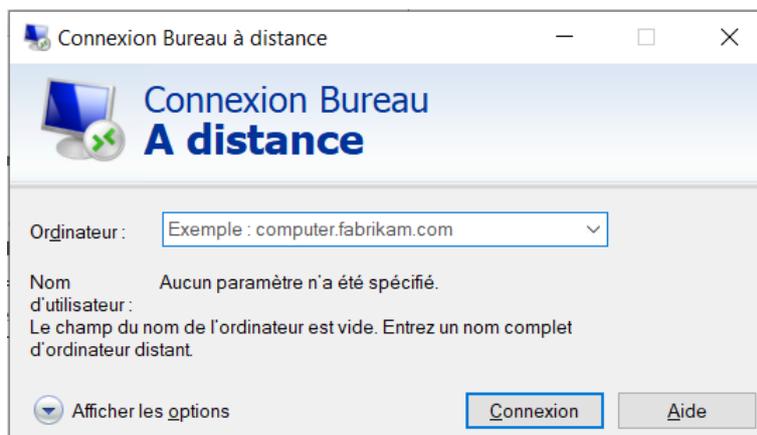
Légende : Schéma représentant la DMZ, le LAN et le Bastion.

ANNEXE 8 : Peerings sur Microsoft Azure



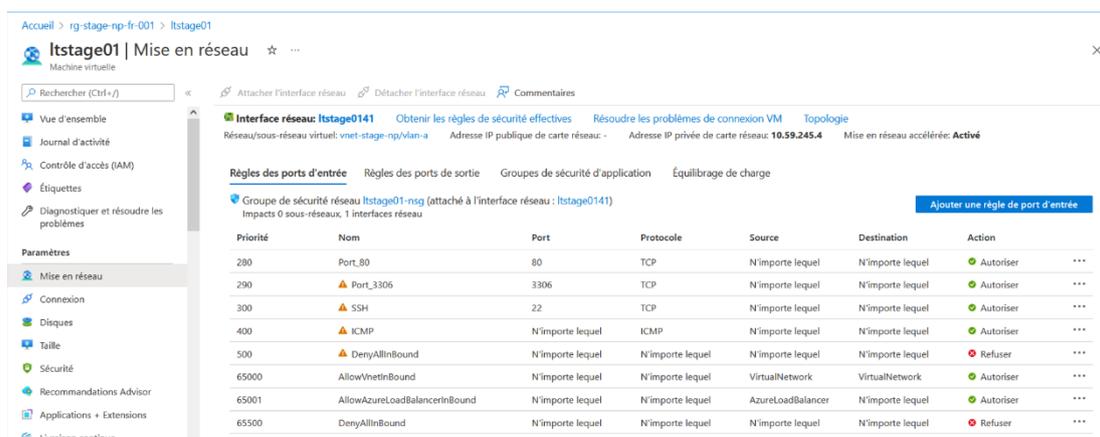
Légende : Capture du portail Microsoft Azure rubrique peering.

ANNEXE 9 : Le protocole RDP



Légende : Capture d'écran d'un outil permettant d'administrer une machine à distance grâce au protocole RDP.

ANNEXE 10 : Règles de pare-feu



Légende : Capture de l'interface de pare-feu.

ANNEXE 11 : Script Terraform vnet

```
resource "azurerm_virtual_network" "lan" {  
  name           = var.vnet.lan.name  
  location       = var.vnet.lan.location  
  resource_group_name = var.vnet.lan.resource_group_name  
  address_space  = var.vnet.lan.address_space  
}
```

```
variable "vnet" {  
  type = map(any)  
  default = {  
    lan = {  
      name           = "vnet-terraform-lan"  
      location       = "francecentral"  
      resource_group_name = "rg-terraform-np-001"  
      address_space  = ["10.59.240.0/24"]  
      subnet_name    = "vlan-LAN"  
      address_prefix = "10.59.240.0/24"  
    }  
  }  
}
```

Légende : Capture d'un script Terraform pour déployer le vnet LAN.

ANNEXE 12 : Script Terraform subnet

```
resource "azurerm_subnet" "subnet_lan" {  
  name           = "vnet-terraform-lan"  
  resource_group_name = azurerm_virtual_network.lan.resource_group_name  
  virtual_network_name = azurerm_virtual_network.lan.name  
  address_prefixes   = ["10.59.240.0/24"]  
}
```

```
variable "subnet_lan" {  
  default = {  
    name           = "internal"  
    resource_group_name = "rg-terraform-np-001"  
    virtual_network_name = "vnet-terraform-lan"  
    address_prefixes   = ["10.59.240.0/24"]  
  }  
}
```

Légende : Capture d'un script Terraform pour déployer un subnet dans le vnet LAN.

ANNEXE 13 : Script Terraform peering

```
module "peering-sharedtolan" {
  source          = "aztfm/virtual-network-peering/azurerms"
  version        = ">=1.0.0"
  resource_group_name = "Groupe_RESEAU_ADMIN"
  virtual_network_name = "PP_VNET_SHARED"
  peerings = [
    {
      name              = var.peering.lanshared.name
      remote_virtual_network_id = azurerms_virtual_network.lan.id
      allow_gateway_transit = true
    }
  ]
}
```

```
variable "peering" {
  type = map(any)
  default = {
    sharedlan = {
      name              = "PP_PEERING_PP_VNET_SHARED_TO_vnet-terraform-lan"
      location          = "francecentral"
      resource_group_name = "rg-terraform-np-001"
      virtual_network_name = "vnet-terraform-lan"
      #remote_virtual_network_id = "70fae88f-6736-42af-bbe6-480d55978f2b"
      allow_gateway_transit = true
    }
  }
}
```

Légende : Capture d'un script Terraform pour déployer un peering SHARED (Azure) vers LAN (réseau local du réseau virtuel)

ANNEXE 14 : Script Terraform machine virtuelle

```
resource "azurerms_virtual_machine" "machine_linux_lan" { //MACHINE LINUX LAN
  name              = "lt-terraform-lan"
  resource_group_name = var.machine_linux_lan.resource_group_name
  location          = var.machine_linux_lan.location
  size              = var.machine_linux_lan.size
  admin_username    = "azureuser"
  network_interface_ids = [azurerms_network_interface.interface_reseau_lan.id]

  admin_ssh_key {
    username = "azureuser"
    public_key = tls_private_key.example_ssh.public_key_openssh
  }

  os_disk {
    caching              = var.machine_linux_lan.os_disk.caching
    storage_account_type = var.machine_linux_lan.os_disk.storage_account_type
  }

  source_image_reference {
    publisher = var.machine_linux_lan.source_image_reference.publisher
    offer     = var.machine_linux_lan.source_image_reference.offer
    sku      = var.machine_linux_lan.source_image_reference.sku
    version  = var.machine_linux_lan.source_image_reference.version
  }
  tags = {
    environment = "Non-Production"
    owner       = "Terraform"
    SHT         = "06H20H5J"
    STA         = "06H20H5J"
  }
}
```

```
variable "machine_linux_lan" {
  default = {
    resource_group_name = "rg-terraform-np-001"
    location            = "francecentral"
    size                = "Standard_DS1_v2"
    admin_username      = "azureuser"
    computer_name       = "lt-terraform-lan"
    disable_password_authentication = true
    #network_interface_ids = [
    # interface_reseau_lan.id
    #]

    admin_ssh_key = {
      username = "admin-terraform-stage"
    }

    os_disk = {
      caching              = "ReadWrite"
      storage_account_type = "Standard_LRS"
    }

    source_image_reference = {
      publisher = "Canonical"
      offer     = "UbuntuServer"
      sku      = "18.04-LTS"
      version  = "latest"
    }
  }
}
```

Légende : Capture d'un script Terraform pour déployer une machine virtuelle Linux dans le LAN.

ANNEXE 15 : Script Terraform interface réseau

```
resource "azurerms_network_interface" "interface_reseau_lan" {
  name           = var.interface_reseau_lan.name
  location       = var.interface_reseau_lan.location
  resource_group_name = var.machine_linux_lan.resource_group_name

  ip_configuration {
    name           = var.interface_reseau_lan.ip_configuration.name
    subnet_id      = azurerms_subnet.subnet_lan.id
    private_ip_address_allocation = var.interface_reseau_lan.ip_configuration.private_ip_address_allocation
  }
}
```

```
variable "interface_reseau_lan" {
  default = {
    name           = "lt-terraform-lan-interface"
    location       = "francecentral"
    resource_group_name = "rg-terraform-np-001"

    ip_configuration = {
      name = "internal"
      #subnet_id      = azurerms_subnet.subnet_lan.id
      private_ip_address_allocation = "Dynamic"
    }
  }
}
```

Légende : Capture d'un script Terraform pour déployer une interface réseau pour la machine linux.

ANNEXE 16 : Les règles de pare-feu

```
resource "azurerms_network_security_rule" "testrules" {
  for_each      = local.nsgrules
  name         = each.key
  direction    = each.value.direction
  access       = each.value.access
  priority     = each.value.priority
  protocol     = each.value.protocol
  source_port_range = each.value.source_port_range
  destination_port_range = each.value.destination_port_range
  source_address_prefix = each.value.source_address_prefix
  destination_address_prefix = each.value.destination_address_prefix
  resource_group_name = azurerms_resource_group.groupe_ressource.name
  network_security_group_name = azurerms_network_security_group.nsg_lan.name
}

locals {
  nsgrules = [
    http = {
      name           = "http"
      priority       = 201
      direction     = "Inbound"
      access         = "Allow"
      protocol       = "Tcp"
      source_port_range = "*"
      destination_port_range = "80"
      source_address_prefix = "*"
      destination_address_prefix = "*"
    }
  ]
}
```

Légende : Capture d'un script Terraform pour ouvrir le port 80 pour une machine