Mise en place d'une infrastructure sécurisé

Dans le cadre de la création d'une entreprise il vous est demandé de mettre en place une infrastructure IT.

Il est nécessaire de mettre l'accent sur la sécurité de cette infrastructure, limiter les flux sur les réseaux.

Auteurs

Roblot Jean-Philippe - jroblot.simplon@proton.me
Drula Kevin - kdrula.simplon@proton.me
Jarousse Quentin - qjarousse.simplon@proton.me
Mathurin Florent - fmathurin.simplon@proton.me

Version

15/05/2024 - V1R0

Stack technique

Powered by https://shields.io

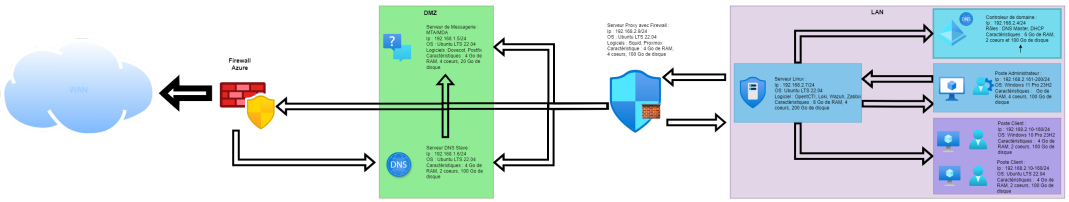
Contexte

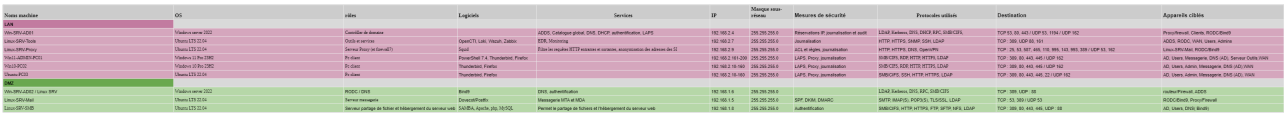
Il vous faudra mettre en place les machines suivantes :

- 1 poste d'administration Win11 (6Go de RAM, 4 cœurs, 100Go de disque) ;
- 1 poste utilisateur Win10 (4Go de RAM, 2 cœurs, 100Go de disque) ;
- 1 poste utilisateur Linux Ubuntu (4Go de RAM, 2 cœurs, 100Go de disque) ;
- 1 contrôleur de domaine Win2022 en LAN (6Go de RAM, 2 cœurs, 100Go de disque) ;
- 1 pare-feu « appliance virtuelle », type pfsense
- 1 Serveur DNS, bind9
- 1 serveur Linux « proxy » (4Go de RAM, 4 cœurs, 100Go de disque) ;
- 1 serveur Linux de messagerie MTA/MDA (4Go de RAM, 4 cœurs, 20Go de disque) (Postfix/Dovecot);

Les interconnexions / flux seront a mettre en place par vos soins, pour se faire il vous faut :

- Créer un DAT
- Créer une matrice de Flux





La mise en place, le deploiement, sera a consigner dans une procédure.

Procédure de déploiement

Afin d'effectuer un déploiement sécurisé, il est nécessaire de mettre en place un Pare-feu Azure pour sécuriser le déploiement le temps que les éléments de sécurité intrinsèques soient en place.

Raisonnement global

On cherche ici à déployer une infrastructure virtuelle dans Azure de façon sécurisée. La réflexion porte donc sur comment déployer une machine centrale dans l'infrastructure en veillant à ne pas l'exposer.

Dans cette optique, on va d'abord chercher à maitriser et filtrer les flux réseau. La première étape est la mise en place d'un firewal azure devant le réseau. Par défaut le firewall à toutes ses interfaces d'entrées de fermées. Par la suite, nous déployons un serveur de test Windows 2022, puis nous créons les règles pour ouvrir le port 53 (DNS) le 3389 (rdp). Une fois les tests de fonctionnement effectué avec le serveur de test, on va pouvoir commencer l'installation et la configuration de l'Active directory, dns master et dhcp.

Nous procéderons ensuite à l'installation de notre serveur tools linux qui embarquera nos outils de supervision. A ce stade, les machines essentielles de notre réseau LAN sont en place, et l'on va chercher à mettre en place une DMZ pour nos usages externes.

Un second firewall (pfSense) peut-être installé entre la dmz et le lan, et paramétré selon la matrice des flux. Le port 80 et 443 du premier firewall peut être ouvert afin de permettre les différents téléchargements de mise à jour.

Une fois notre ADDS et notre serveur tools à jour (ainsi que le téléchargement et les mises à jour des solutions embarquées), nous allons pouvoir commencer à provisionner la DMZ.

Nous commençons par un DNS esclave (Linux - Bind9), puis un serveur de messagerie. En vue de l'installation des machines utilisateur dans le LAN, nous mettons en place un serveur Proxy (Squid).

Une fois paramétré, nous provisionnons nos trois machines clients (1 poste administrateur et 2 postes utilisateurs).

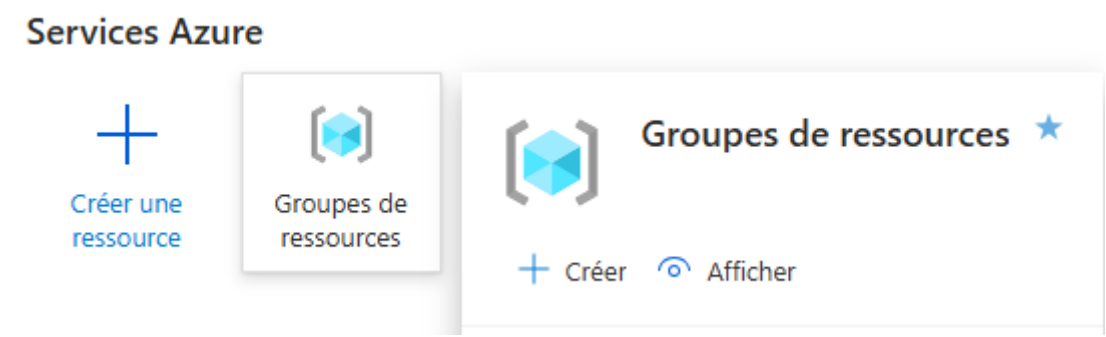
Azure Firewall

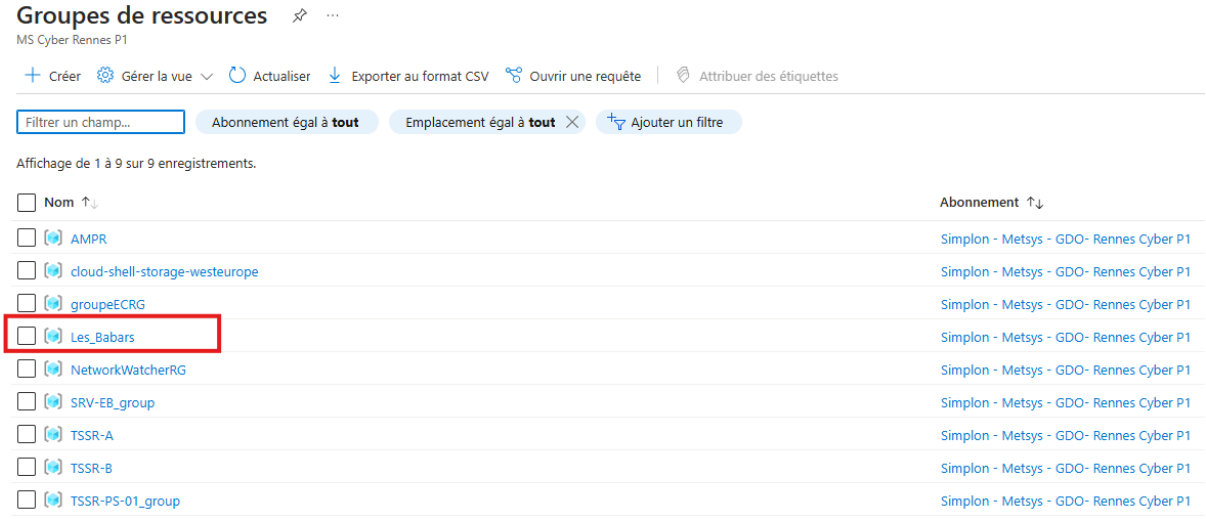
Le trafic réseau est soumis aux règles de pare-feu configurées lorsque vous routez votre trafic réseau vers le pare-feu en tant que sous-réseau de passerelle par défaut.

Dans un premier temps, il faudra ici créer un réseau virtuel avec deux sous-réseaux afin de faciliter le déploiement. L'objectif est d'avoir :

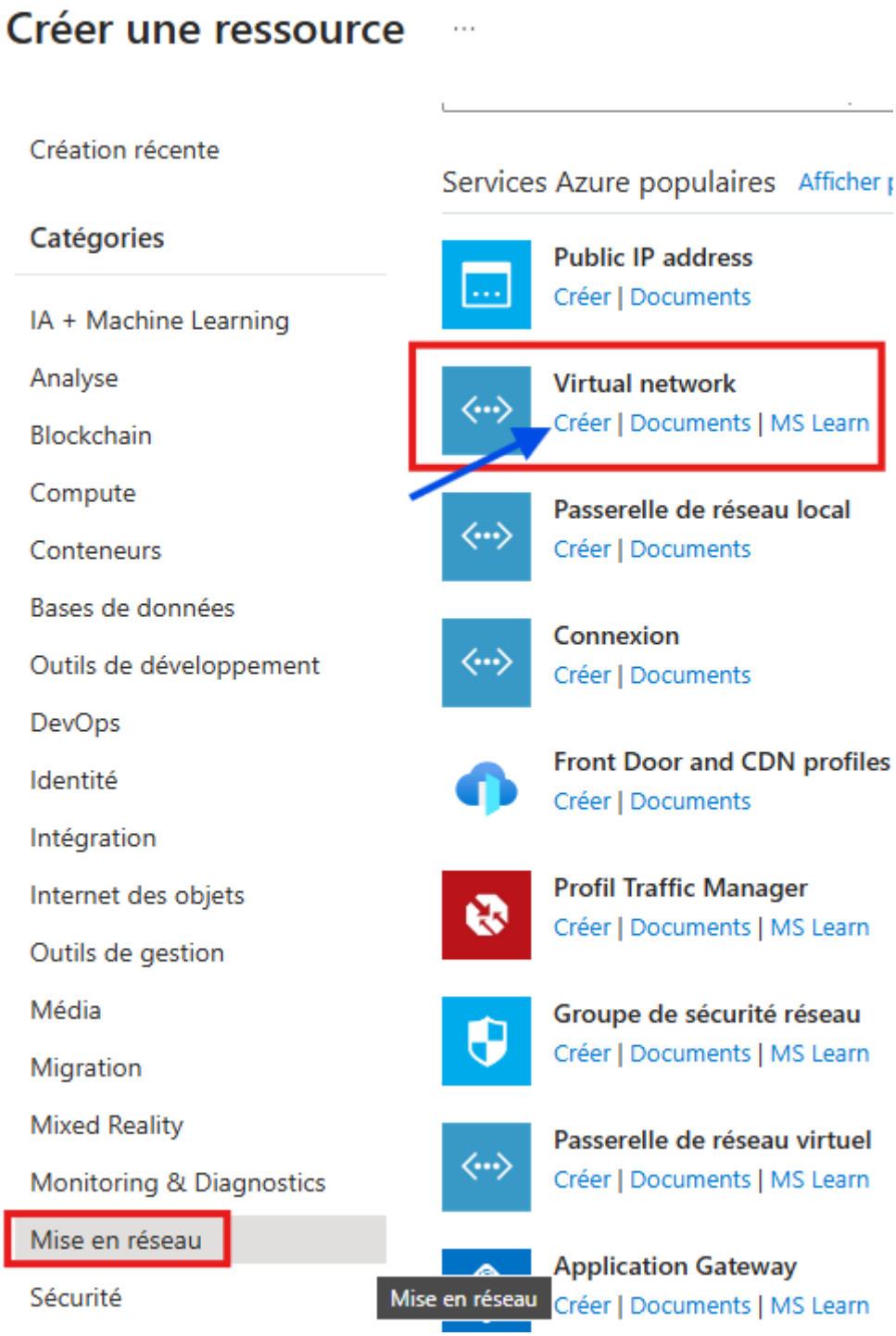
- un sous-réseau AzureFirewallSubnet : le pare-feu est dans ce sous-réseau.
- un sous-réseau infrasecureLAN-SN, qui correspond au réseau LAN interne de notre entreprise Infrasecure Inc. Le traffic de ce sous réseau est filtré par le Firewall.

    1. Créer un groupe de ressources via l'acceuil du portail Azure (Les_Babars dans notre exemple) qui contiendra toute les ressources nécessaire à notre infrastructure


Services Azure
Créer une ressource
Groupes de ressources
Groupes de ressources
Créer
Afficher


Groupes de ressources
MS Cyber Rennes P1
Créer
Gérer la vue
Actualiser
Exporter au format CSV
Ouvrir une requête
Attribuer des étiquettes
Filtrer un champ...
Abonnement égal à tout
Emplacement égal à tout
Ajouter un filtre
Affichage de 1 à 9 sur 9 enregistrements.
Nom
Abonnement
AMPR
cloud-shell-storage-westeurope
groupeECRG
Les_Babars
NetworkWatcherRG
SRV-EB_group
TSSR-A
TSSR-B
TSSR-PS-01_group
Simplon - Metsys - GDO- Rennes Cyber P1

2. Créer un réseau virtuel et suivre l'assistant pour renseigner les informations nécessaires



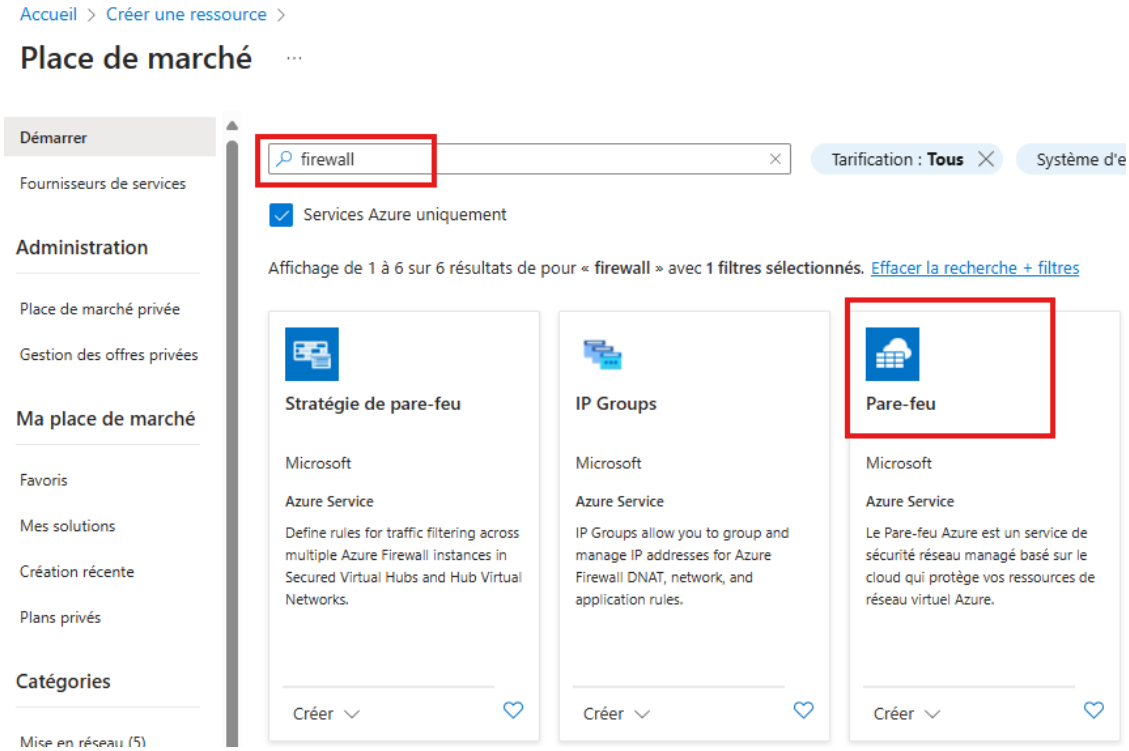
- Le nommer Les-Babars-VN
- Pour l'IPv4, les valeurs sont à adapter à votre plan d'adressage, dans notre cas : 192.168.0.0/24
- créer un premier sous-réseau, le nommer AzureFirewallSubnet. Le pare-feu se trouvera dans ce sous-réseau et le nom du sous-réseau doit être AzureFirewallSubnet. Son adressage IP sera 192.168.1.0/24
- ajouter le deuxième sous-réseau infrasecureLAN-SN avec la plage IP 192.168.2.0/24

3. Créer un serveur virtuel de test dans le sous-réseau infrasecureLAN-SN. Il n'est pas nécessaire pour le déploiement du Firewall, mais il nous permettra de tester son bon fonctionnement au terme de son déploiement.

- Créer une ressource
- Sélectionner Windows Server 2022 Datacenter
- Groupe de ressource : Les-Babars > Nom de la machine : Srv-Test > Nom d'utilisateur / Mot de passe
- Règles des ports d'entrée > Ports d'entrée publics : aucune
- Mise en réseau : s'assurer que le réseau virtuel choisi est bien Les-Babars-VN et le sous-réseau InfrasecureLAN-SN
- IP publique : aucune
- Vérifier + créer > Créer
- Noter l'IP privée de la machine une fois son déploiement terminé.

4. Déployer le firewall et la stratégie :

- Créer le pare-feu (faire une recherche dans la création de ressource)



- Nom : Temp-FW
- Gestion de pare-feu : Utiliser une stratégie de pare-feu pour gérer ce pare-feu.
- Stratégie de pare-feu : Ajouter un nouveau, puis entrez fw-temp-pol. Sélectionnez la même région que celle utilisée précédemment.
- Choisir le réseau virtuel Les-Babars-VN
- IP publique : Ajouter nouveau, puis entrez fw-pip pour le nom.
- Vérifier + créer > créer
- Une fois le déploiement terminé, accéder au groupe de ressources Les-Babars, puis sélectionner le pare-feu Temp-FW.
- Noter les adresses IP privée et publique du pare-feu.

5. Créer un itinéraire par défaut

Pour le sous-réseau InfrasecureLAN-SN, configurez l'itinéraire sortant par défaut pour qu'il traverse le pare-feu.

- Mise en réseau, sélectionner Tables d'itinéraires.

- Sélectionner "Créer",puis entrez les valeurs nécessaires comme vu précédemment
- Revoir + créer > Créer Une fois le déploiement terminé, sélectionner Accéder à la ressource
    1. Sur la page de Firewall-route, sélectionner Sous-réseaux, puis sélectionner Associer.
    2. Sélectionner Réseau virtuel > Les-Babars-VN.
    3. Pour Sous-réseau, sélectionner InfrasecureLAN-SN. Veiller à ne sélectionner que le sous-réseau InfrasecureLAN-SN pour cette route, sinon le pare-feu ne fonctionnera pas correctement.
    4. Sélectionner OK.
    5. Sélectionner Itinéraires, puis Ajouter.
    6. Pour Nom de l'itinéraire, entrer fw-dg.
    7. Pour Préfixe d'adresse, entrer 0.0.0.0/0.
    8. Pour Type de tronçon suivant, sélectionner Appliance virtuelle. Le Pare-feu Arure est en réalité un service managé, mais l'appliance virtuelle fonctionne dans ce cas.
    9. Pour Adresse du tronçon suivant, entrer l'adresse IP privée du pare-feu que vous aver notée précédemment.
    10. Sélectionner OK.

6. Configurer une règle d'application

   Pour cet exemple, un accès sortant à www.google.com va être autoriser.

    1. Ouvrir le groupe de ressources Test-FW-RG, puis sélectionner la stratégie de pare-feu fw-test-pol.
    2. Sélectionner Règles d'application.
    3. Sélectionner Ajouter une collection de règles.
    4. Pour nom, entrer App-Coll01.
    5. Pour Priorité, entrer 200.
    6. Pour Action de collection de règles, sélectionner Autoriser.
    7. Sous Règles, dans Nom, entrer Allow-Google.
    8. Pour Type de source, sélectionner Adresse IP.
    9. Pour Source, entrer 192.168.2.0/24.
    10. Pour Protocol:port, entrer http, https.
    11. Pour Type de destination, sélectionner FQDN.
    12. Pour Destination, entrer www.google.com
    13. Sélectionner Ajouter.

7. Configurer une règle de réseau

   Il s'agit ici de la règle de réseau qui autorise un accès sortant à deux adresses IP sur le port 53 (DNS).

    1. Sélectionnez Règles de réseau.
    2. Sélectionnez Ajouter une collection de règles.
    3. Pour Priorité, entrez 200.
    4. Pour nom, entrez Net-Coll01.
    5. Pour Action de collection de règles, sélectionnez Autoriser.
    6. Pour Groupe de collection de règles, sélectionnez DefaultNetworkRuleCollectionGroup.

7. Sous Règles, dans Nom, entrez Allow-DNS.
8. Pour Type de source, sélectionnez Adresse IP.
9. Pour Source, entrez 192.168.2.0/24.
10. Pour Protocole, sélectionnez UDP.
11. Pour Ports de destination, entrez 53.
12. Pour Type de destination, sélectionnez Adresse IP.
13. Pour Destination, entrez 192.168.2.4, 8.8.8.8.
14. Sélectionnez Ajouter.

8. Configurer une règle DNAT

   Cette règle vous permet de connecter un bureau à distance à la machine virtuelle Srv-Test par le biais du pare-feu.

   1. Sélectionner les règles DNAT.
   2. Sélectionner Ajouter une collection de règles.
   3. Pour Nom, entrer rdp.
   4. Pour Priorité, entrer 200.
   5. Pour Groupe de collection de règles, sélectionner DefaultDnatRuleCollectionGroup.
   6. Sous Règles, dans Nom, entrer rdp-nat.
   7. Pour Type de source, sélectionner Adresse IP.
   8. Pour Source, entrer *.
   9. Pour Protocole, sélectionner TCP.
   10. Pour Ports de destination, entrer 3389.
   11. Pour Type de destination, sélectionner Adresse IP.
   12. Pour Destination, entrer l'adresse IP publique du pare-feu.
   13. Pour Adresse traduite, entrer l'adresse IP privée de Srv-Test.
   14. Pour Port traduit, entrer 3389.
   15. Sélectionner Ajouter.

9. Modifier les adresses DNS principales et secondaires de l'interface réseau Srv-Work
   À des fins de test, il faut configurer les adresses DNS principales et secondaires du serveur.

   1. Dans le menu du Portail Azure, sélectionner Groupes de ressources ou rechercher et sélectionner Groupes de ressources dans n'importe quelle page.
   2. Sélectionner le groupe de ressources Les-Babars.
   3. Sélectionner l'interface réseau de la machine virtuelle Srv-Test.
   4. SousParamètres, sélectionner Serveurs DNS.
   5. Sous Serveurs DNS, sélectionner Personnalisé.
   6. Saisisser 192.168.2.4 dans la zone de texte Ajouter un serveur DNS, et 8.8.8.8 dans la zone de texte suivante.
   7. Sélectionner Enregistrer.
   8. Redémarrer la machine virtuelle Srv-Test.

10. Tester le pare-feu

    1. Connectez un Bureau à distance à l'adresse IP publique du pare-feu et connectez-vous à la machine virtuelle Srv-Work. Ouvrez Internet Explorer et accédez à https://www.google.com.

2. Sélectionnez OK>Fermer sur les alertes de sécurité d'Internet Explorer.
3. La page d'accueil Google doit s'afficher.
4. Accédez à https://www.microsoft.com.
5. Vous devriez être bloqué par le pare-feu.

Maintenant que vous avez vérifié que les règles de pare-feu fonctionnent :

- Vous pouvez accéder au nom de domaine complet autorisé, mais pas à d'autres.
- Vous pouvez résoudre les noms DNS à l'aide du serveur DNS externe configuré.

Domain Controler

Pour créer une machine virtuelle dans Azure à partir du portail d'administration, il faut suivre les étapes suivantes :

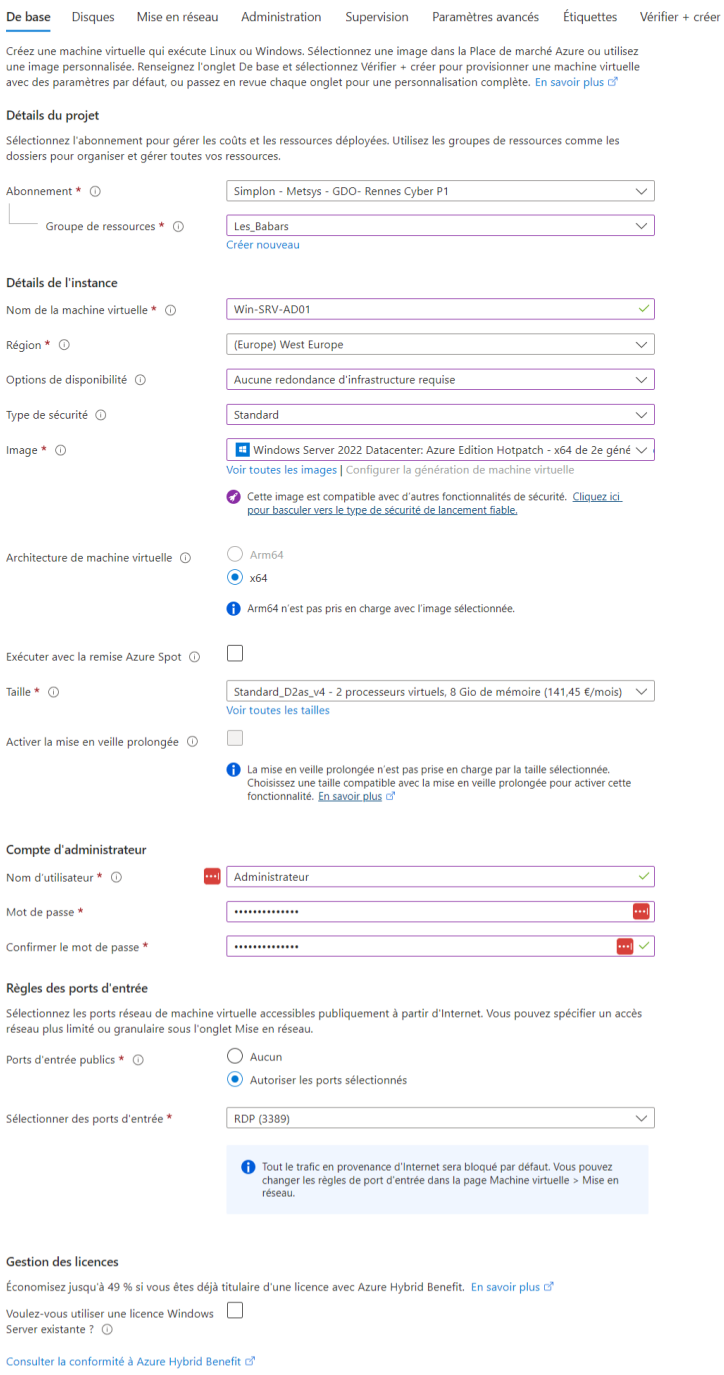
Accédez au portail d'Azure.

1. Sélectionnez "Créer"
2. "Machine virtuelle Azure".
   L'assistant de création d'une nouvelle VM va démarrer, avec les différentes étapes habituelles : options de base, disques, réseau, etc.

Étape 1 : Options de Base

Dans le premier onglet nommé "De base", plusieurs informations essentielles doivent être renseignées :

1. Abonnement : Sélectionner la souscription Azure à utiliser.
2. Groupe de ressources : Créer un nouveau groupe de ressources pour cette machine virtuelle ou utiliser un groupe de ressources existant.
3. Nom de la machine virtuelle : Donner un nom au serveur, utilisé au niveau du système et dans la console Azure.
4. Région : Choisir la région Azure dans laquelle déployer la VM. Cela correspond à l'emplacement géographique des ressources.
5. Options de disponibilité : Configurer la redondance de la VM dans d'autres régions Azure afin d'assurer une haute disponibilité en cas de crash du datacenter. Cette option est particulièrement utile pour les environnements de production.
6. Type de sécurité : Choisir "Lancer des machines virtuelles approuvées" pour activer le vTPM, le Secure Boot et la surveillance de l'intégrité.
7. Image : Sélectionner le type de système d'exploitation. Par exemple, "Windows Server 2022 Datacenter: Azure Edition - Génération 2".
8. Architecture : L'architecture doit être x64 pour ce système.
9. Taille : Choisir le type de machine virtuelle. La VM "Standard_B2s" est basique, mais suffisante pour ce type d'usage.



Reseau

Pour la partie réseau, il est possible de créer un nouveau réseau virtuel s'il s'agit d'un nouvel environnement.

Dans ce cas, il peut être rattaché à un réseau virtuel existant, comme "Les-Babars-VN-192.168.0.0/24", qui contient un sous-réseau. Cette étape est essentielle pour configurer le "réseau local" Azure.

Proxy / firewall

L'installation d'un proxy firewall commence par l'installation de pfsense, qui jouera la partie firewall. L'installation se fera sur une machine de 4 Gb de RAm, 4 coeurs et 100 Go d'espace disque. Dans un premier temps, il va falloir créer une VM sur hyper-V, pour pouvoir installer l'os de pfsense puis importer le template dans une VM Azure dans un conteneur.

Étape 1 : Création de la machine virtuelle Ubuntu server

Retournez au portail Azure. Cliquez sur "Machines virtuelles" puis sur "+ Ajouter" et "Machine virtuelle".

Configuration de base : Abonnement : Sélectionnez votre abonnement. Groupe de ressources : Choisir les Babars.

Nom de la machine virtuelle : Linux-SRV-Tools. Région : La même région que le réseau virtuel. Image : Choisir Ubuntu Server.

Taille : Sélectionnez la taille appropriée pour votre besoin (ex: Standard_B1ms).

Configuration de l’authentification : Nom d'utilisateur : Par exemple, Administrateur. Méthode d’authentification : Clé SSH (générer une nouvelle clé SSH ou utiliser une clé existante). (pour le test j'ai choisi mot de passe : Jesaispasmoi@)

Réseau : Réseau virtuel : Sélectionnez le réseau virtuel que vous avez créé (Les-Babars-VN-192.168.0.0/24).

Sous-réseau : Sélectionnez le sous-réseau (Subnet-1).

Adresse IP publique : Si nécessaire, choisissez "aucune" pour une machine interne ou configurez selon vos besoins.

Cliquez sur "Revoir + créer" puis sur "Créer" pour déployer la machine virtuelle.

Étape 3 : Configuration du groupe de sécurité réseau (NSG)

Allez dans "Groupes de sécurité réseau" dans le menu de gauche et cliquez sur "+ Ajouter".

Configuration du NSG : Nom : Par exemple, NSG-UbuntuVM.

Groupe de ressources : Utilisez le même groupe de ressources que votre VM. Cliquez sur "Créer".

Après la création, allez dans le NSG et ajoutez des règles de sécurité entrante/sortante selon vos besoins (par exemple, pour autoriser SSH).