23/12/2023

Evaluation 3ème année

Azure

Nicolas WARLOP et Selim AKALAN

ASI SR

SOMMAIRE

Evaluation 3ème année : Réalisation d'une infrastructure multiple sur le Cloud Azure	20/12/2023

WARLOP Nicolas
AKALAN Selim

Contexte :

Vous faites partie de l'équipe d'ingénieurs Cloud de "NovaTech Solutions", une entreprise innovante spécialisée dans les solutions technologiques cloud et les infrastructures informatiques avancées. Votre équipe est réputée pour son expertise dans la mise en œuvre de projets complexes sur Azure.

Votre équipe a été sélectionnée pour un projet crucial : la conception et la mise en place d'une infrastructure multiple sur le **Cloud Azure** pour un client important, "**EcoEnergy Corp**", qui souhaite moderniser sa gestion des données et ses applications.

Livraison et Évaluation :

Chaque groupe de deux doit soumettre un **rapport d'intervention détaillé**, démontrant les étapes suivies, les configurations réalisées, et les preuves de réussite des tâches assignées.

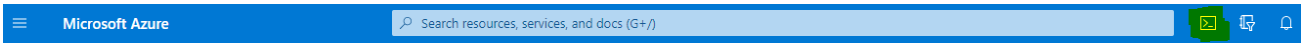
Tâches à réaliser - Objectifs du Projet :

Création d'une Infrastructure Cloud : Utilisez Azure CLI pour créer un groupe de ressources, un réseau virtuel (VNET) et un sous-réseau (SUBNET).
Mise en Place d'une VM : Configurez une VM Windows Server 2019.
Intégration et Sécurité : Employez le Vnet Peering pour connecter votre VNET/Subnet avec celui d'un autre groupe.
Solutions de Sauvegarde : Mettez en place une solution de sauvegarde pour assurer la sécurité et la récupération des données.
Synchronisation et Partage de Fichiers : Implémentez Azure File Sync pour gérer la synchronisation et le partage de données.
Déploiement d'Application Web : Déployer une application Web vers Azure App Service en utilisant Git localement
Création d'une VM Golden Image Windows 11 : Personnalisez une VM Windows 11 avec des logiciels spécifiques, effectuez la préparation système ("sysprep") et hébergez l'image dans votre Azure Shared Image Gallery. Cette image servira de référence à l'autre élève pour déployer une VM Windows 11.

Création d'une Infrastructure Cloud : Utilisez Azure CLI pour créer un groupe de ressources, un réseau virtuel (VNET) et un sous-réseau (SUBNET).

Azure CLI : Créez un groupe de ressource rg-VOTRENOM

Pour créer un groupe de ressource, il faut accéder au CLI de Azure en cliquant sur le bouton suivant :



Ensuite entrez la commande : az group create --name MonGroupeDeRessources --location eastus

Remplacez *MonGroupeDeRessources* par le nom de votre groupe de ressource, et *eastus* par la région Azure où tu veux créer ton groupe de ressources.

Exemple pour mon groupe de ressource :

```
nicolas [ ~ ]$ az group create --name rg-warlop --location westeurope
```

Mon groupe de ressource s'appelle donc rg-warlop, et sa localisation est l'Europe de l'Ouest.

Azure CLI : Créez un VNET 10.X.0.0/16 nommé VNET-01-VOTRENOM

Pour créer un VNET via le CLI d'Azure, tapez la commande suivante :

```
az network vnet create \
 --resource-group NomGroupeDeRessources \
--name NomVNET \
 --address-prefixes "10.0.0.0/16"
```

Remplacez:

- NomGroupeDeRessources par le nom du groupe de ressources dans lequel vous souhaitez créer le VNET.
- NomVNET par le nom que vous voulez donner au VNET
- Spécifiez votre plage d'adresses IP pour le VNET dans la commande –address-prefixes

Dans mon cas, voici ma commande :

```
nicolas [ ~ ]$ az network vnet create \
> --resource-group rg-warlop \
> --name VNET-01-WARLOP \
> --address-prefixes "10.18.0.0/16"
```

```
{
  "newVNet": {
    "addressSpace": {
      "addressPrefixes": [
        "10.18.0.0/16"
      ]
    },
    "enableDdosProtection": false,
    "etag": "W/\"33668cc7-5fa5-4f55-afed-287316ab5be8\"",
    "id": "/subscriptions/b24e0928-ccb5-49f8-b6fb-1bdf361cc65e/resourceGroups/rg-warlop/providers/Micr
osoft.Network/virtualNetworks/VNET-01-WARLOP",
    "location": "westeurope",
    "name": "VNET-01-WARLOP",
    "provisioningState": "Succeeded",
    "resourceGroup": "rg-warlop",
    "resourceGuid": "80d2a238-486b-482d-9c5f-95b8474a309a",
    "subnets": [],
    "type": "Microsoft.Network/virtualNetworks",
    "virtualNetworkPeerings": []
  }
}
```


Azure CLI : Créez un SUBNET 10.X.X.0/24 nommé SUBNET-01-BL

```
az network vnet subnet create \
 --resource-group NomGroupeDeRessources \
--vnet-name NomVNET \
--name NomSousReseau \
--address-prefix "10.X.X.0/24"
```

--resource-group NomGroupeDeRessources: Remplace "NomGroupeDeRessources" par le nom du groupe de ressources où se trouve le VNET.

--vnet-name NomVNET: Remplace "NomVNET" par le nom du VNET dans lequel tu veux créer le sous-réseau.

--name NomSousReseau: Remplace "NomSousReseau" par le nom que tu veux donner au sous-réseau.

--address-prefix "10.X.X.0/24": Spécifie la plage d'adresses IP pour le sous-réseau.

La commande que je rentre est la suivante :

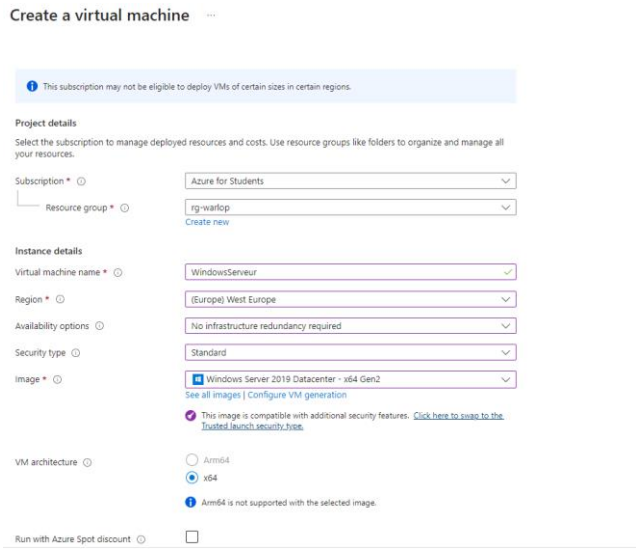
az network vnet subnet create –resource-group rg-warlop –vnet-name VNET-01-WARLOP –name SUBNET-01-BL –address-prefix « 10.18.18.0/24 »

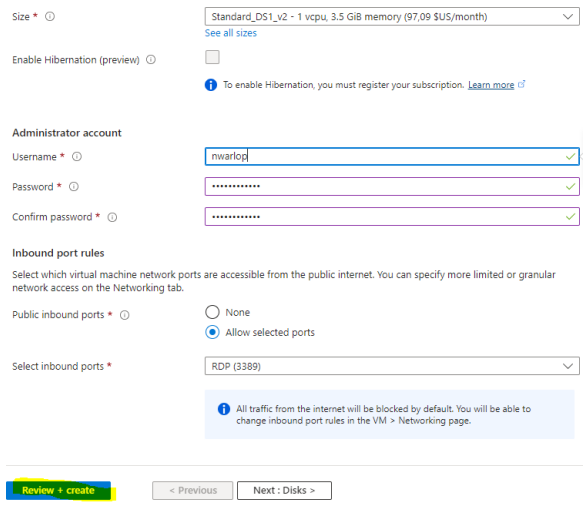
```
nicolas [ ~ ]$ az network vnet subnet create --resource-group rg-warlop --vnet-name VNET-01-WARLOP --name SUBNET-01-BL --address-prefix "10.18.18.0/24"
{
  "addressPrefix": "10.18.18.0/24",
  "delegations": [],
  "etag": "W/\"c4eb3a7b-342b-4792-8ce2-dd7d6eda6527\"",
  "id": "/subscriptions/b24e0928-ccb5-49f8-b6fb-1bdf361cc65e/resourceGroups/rg-warlop/providers/Microsoft.Network/virtualNetworks/VNET-01-WARLOP/subnets/SUBNET-01-BL",
  "name": "SUBNET-01-BL",
  "privateEndpointNetworkPolicies": "Disabled",
  "privateLinkServiceNetworkPolicies": "Enabled",
  "provisioningState": "Succeeded",
  "resourceGroup": "rg-warlop",
  "type": "Microsoft.Network/virtualNetworks/subnets"
}
```

Mise en Place d'une VM : Configurez une VM Windows Server 2019.

Portal : Créez une VM Windows Server 2019 VM (B2ms ou D2s v3)

Je créé ma VM avec les options suivantes :

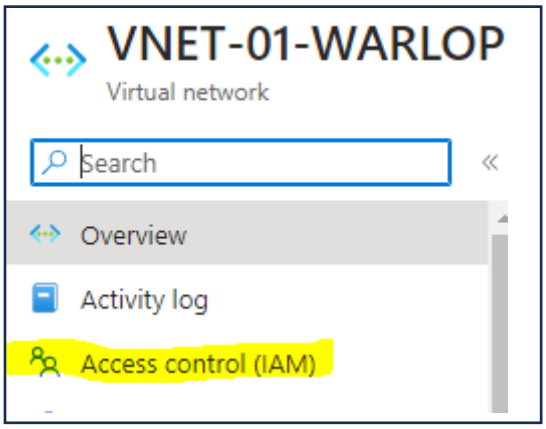




Intégration et Sécurité : Employez le Vnet Peering pour connecter votre VNET/Subnet avec celui d'un autre groupe.

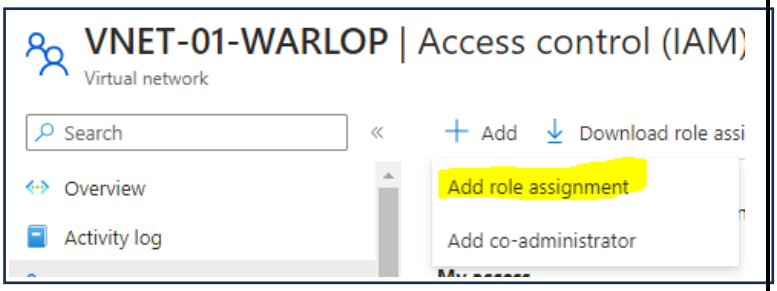
Portal : Vnet Peering : Vous utiliserai le vnet peering afin d'interconnecter votre VNET/Subnet avec celui de votre voisin (peering A to B).

Pour commencer cette étape, nous allons créer un rôle dans notre VNET :

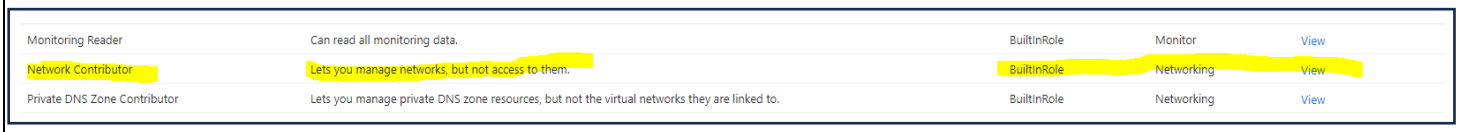


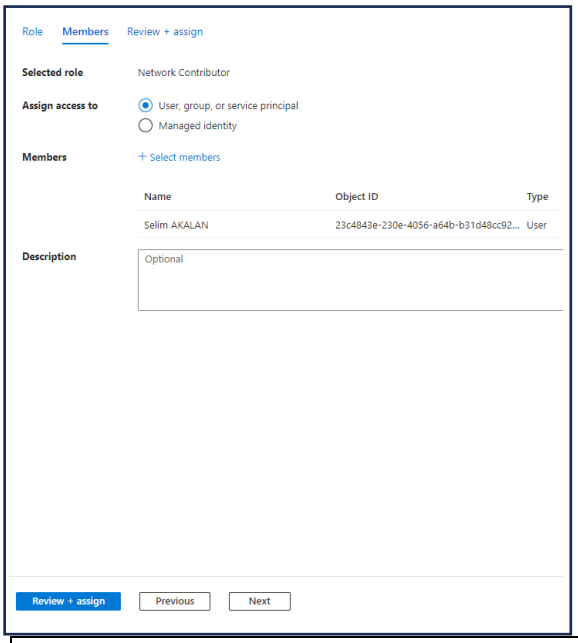
Dans votre VNET, cliquez sur « Access control (IAM) »

Cliquez sur Add, puis « Add rôle assignment » :

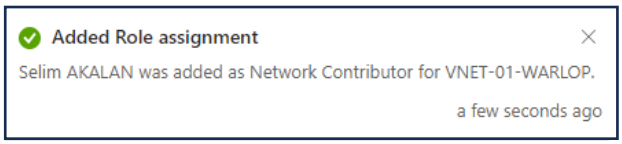


Trouvez et sélectionnez le rôle Network Contributor :

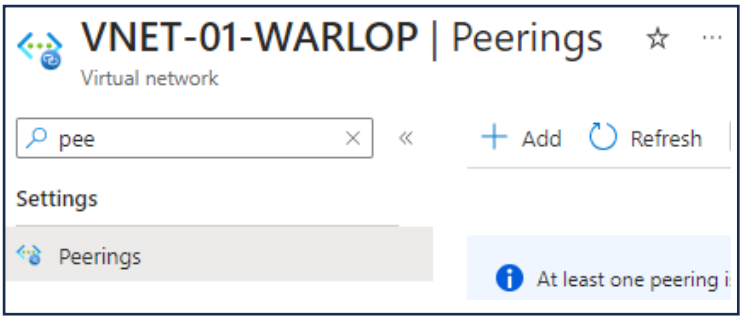




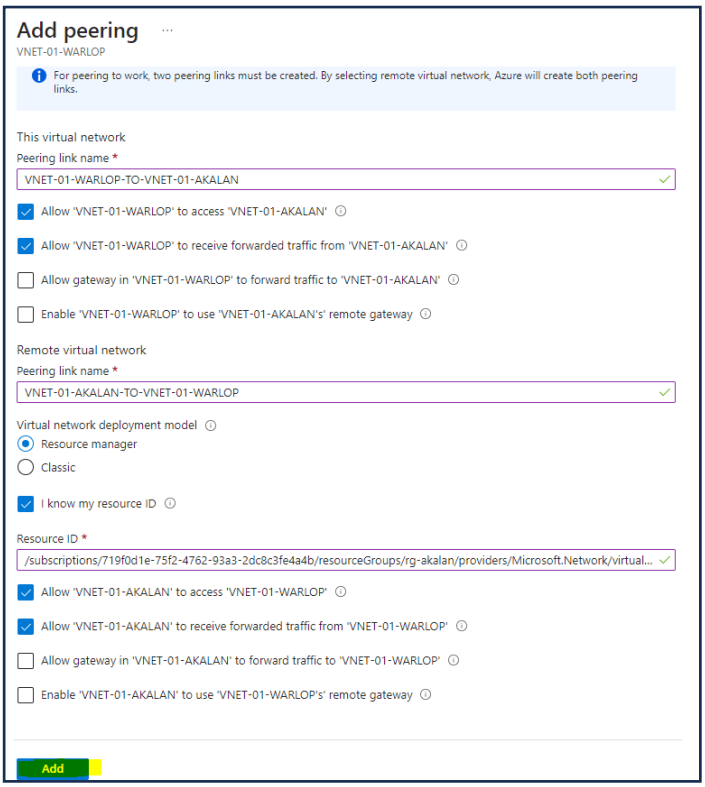
Ensuite, j'ajoute mon binôme, et je l'assigne.



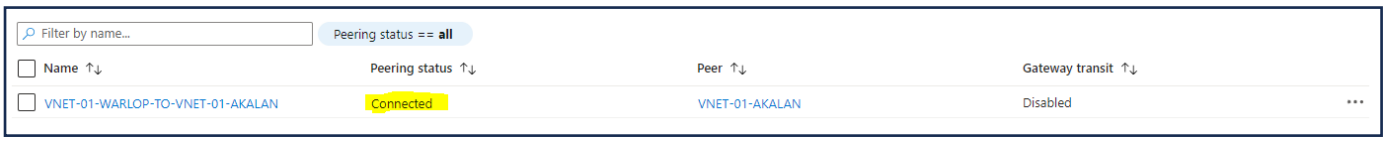
Allez dans peerings, et cliquez sur +Add :



Je rentre les informations suivantes pour mon peering :

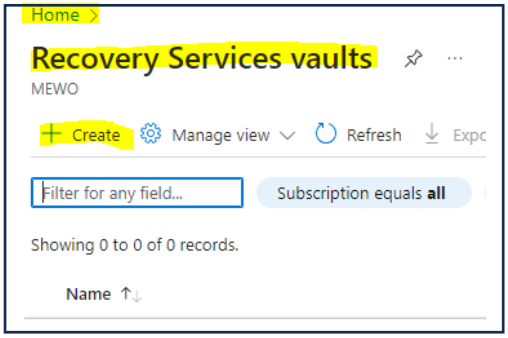


La connexion fonctionne correctement :



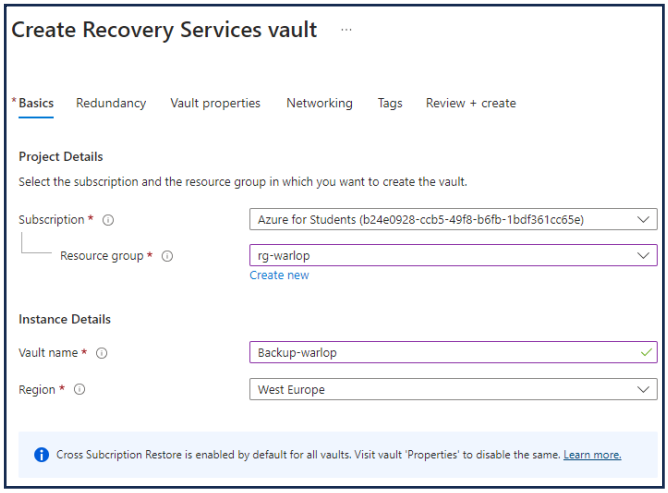
Solutions de Sauvegarde : Mettez en place une solution de sauvegarde pour assurer la sécurité et la récupération des données.

Portal : Créer une solution de Backup pour Backuper votre VM-01

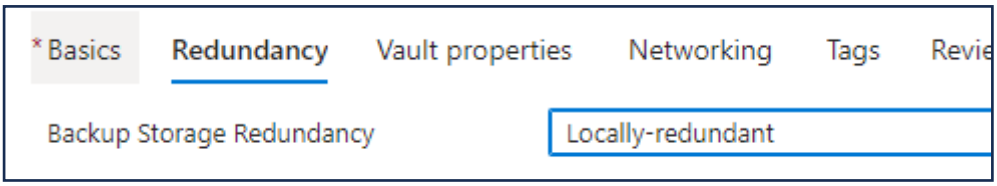


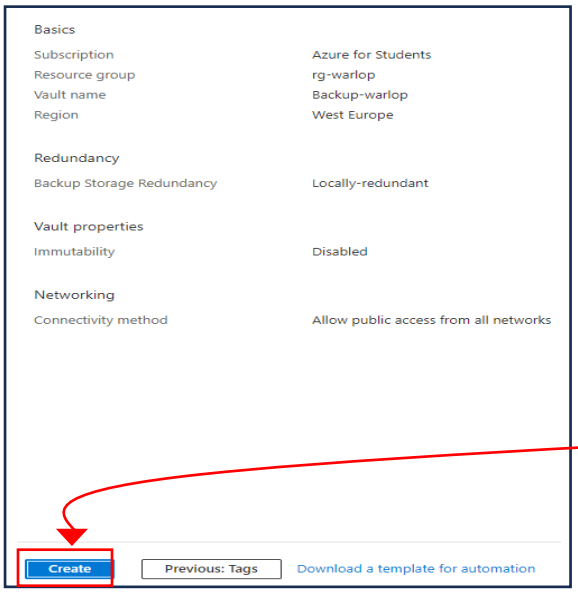
Rendez-vous dans « Recovery Services vaults » depuis home, et sur « create »

Entrez les valeurs suivantes vous concernant et cliquez sur « Vérifier et créer » :

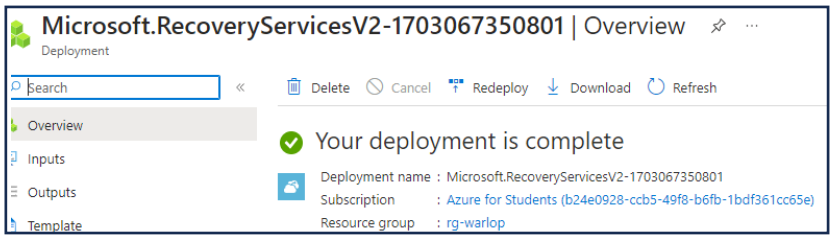


Séléctionnez l'option « Locally-redundant » dans l'onglet « Redundancy » :

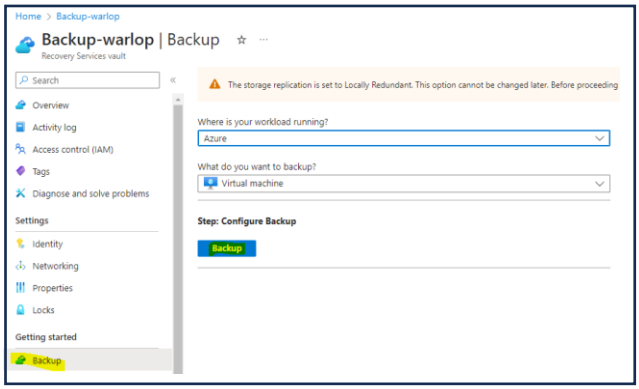


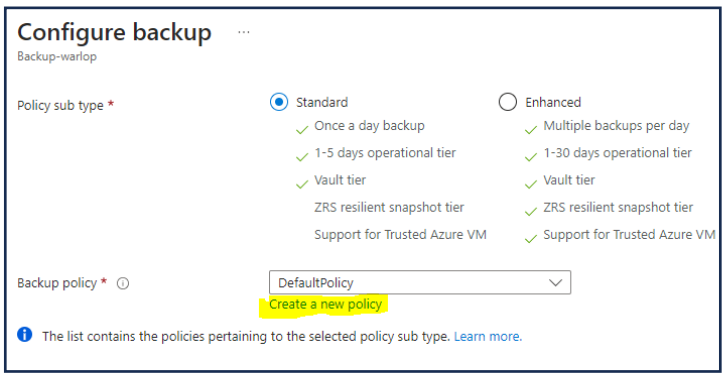


Les informations générales sont résumées ici, si tout est correct, cliquez sur « Create »



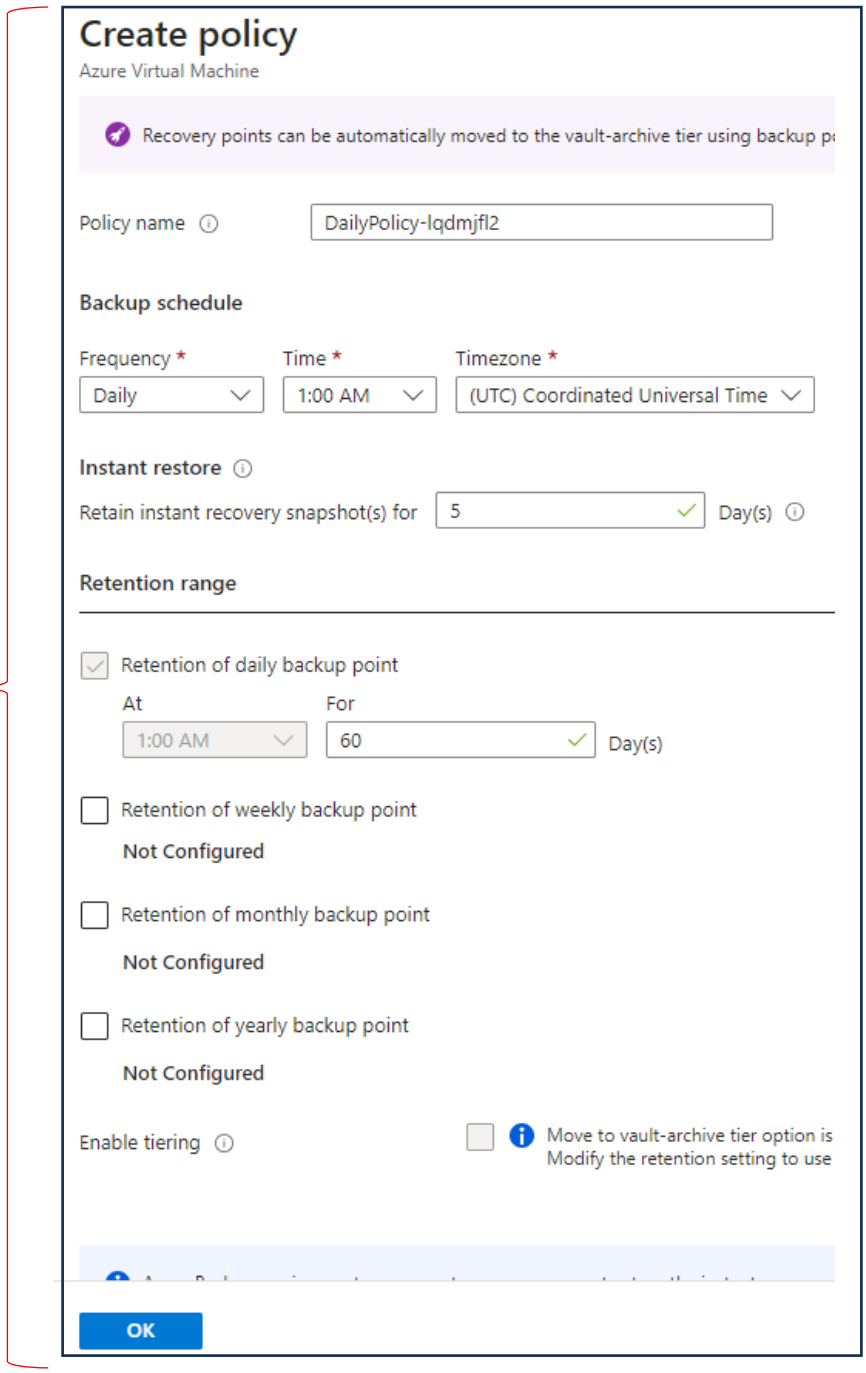
Ensuite rendez-vous dans votre coffre fraichement créé, et entrez les options suivantes :

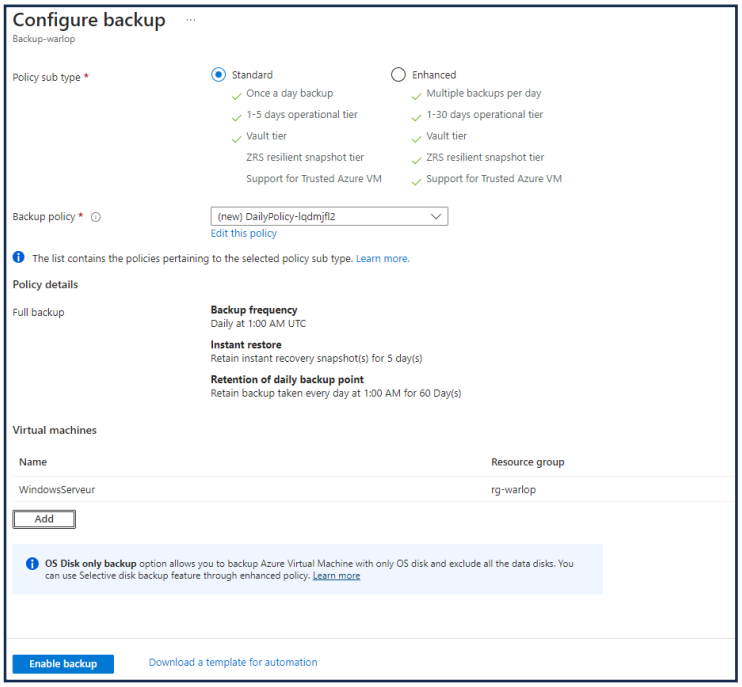




Ensuite nous allons créer une politique de backup, cliquez sur « Create a new policy ».

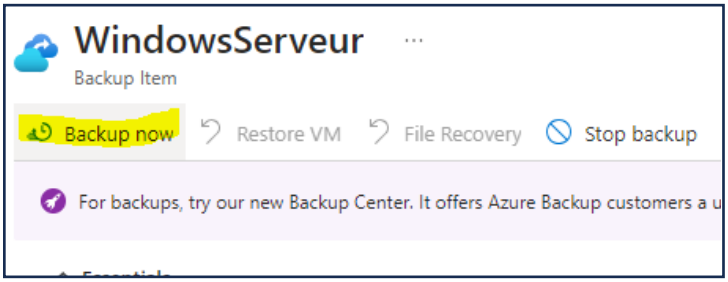
Voici les options qui nous intéresse :



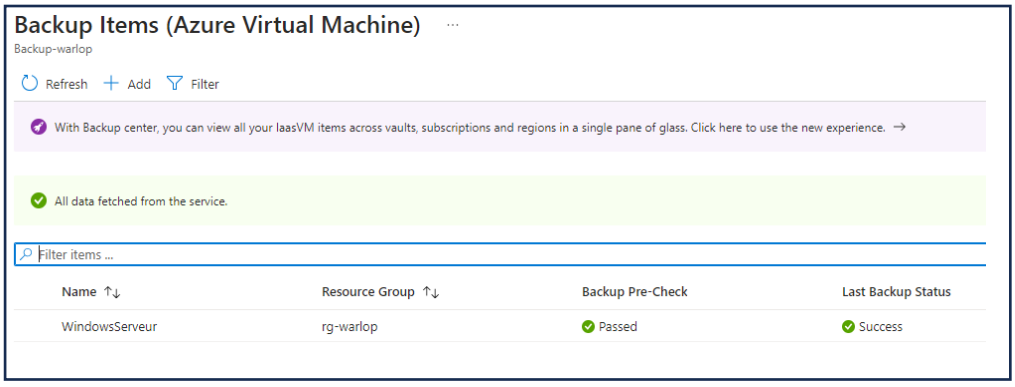


Dans la configuration du backup, sélectionnez l'option Standard, votre politique créer auparavant, puis cliquez sur Enable backup.

Ensuite, rendez-vous sur la VM que vous souhaitez sauvegarder, et cliquez sur « Backup now » :

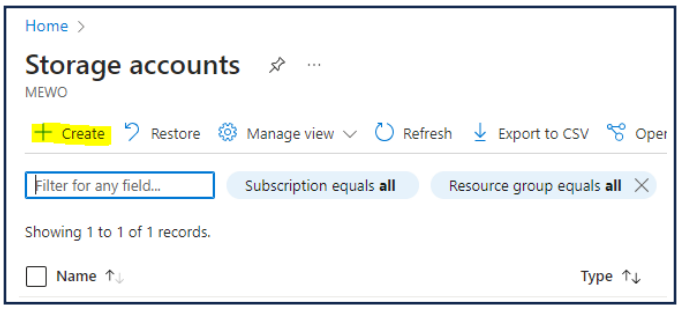


Votre VM se retrouve donc dans vos éléments sauvegarder, ci-dessous ma VM windows serveur :



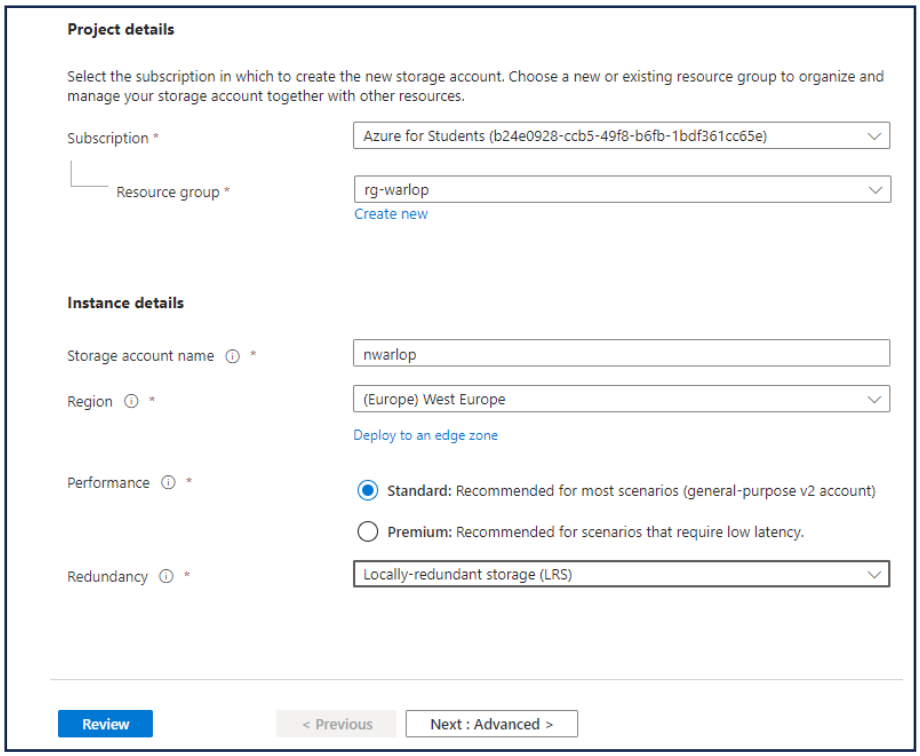
Synchronisation et Partage de Fichiers : Implémentez Azure File Sync pour gérer la synchronisation et le partage de données.

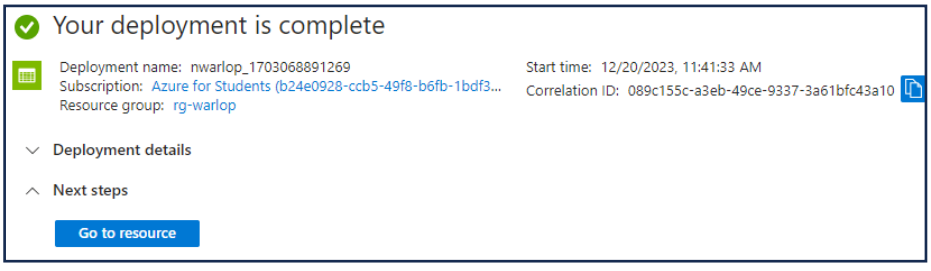
Portal : Azure File Sync : Elève A ou B créera un Azure File Share(Cloud Endpoint) et Eleve A possèdera un server endpoint et Eleve B possèdera un server endpoint, vous fournirez la preuve que la synchro s'effectue entre les trois endpoints.



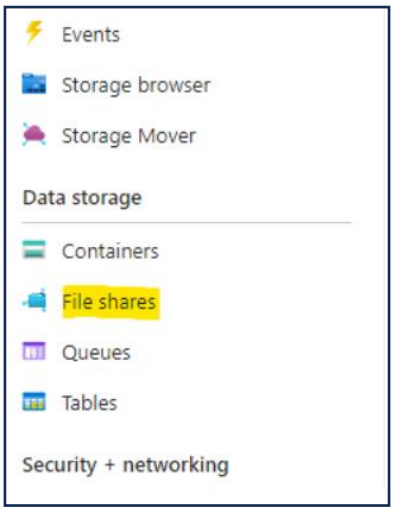
Premièrement, nous devons créer un storage account, pour se faire rendez-vous sur Storage account, puis cliquez sur le bouton « Create »

Entrez les informations requises telles que votre groupe de ressource, le nom de compte de votre storage, la région, la performance que vos souhaitez attribuer, et la redondance, les miennes s'y dessous :



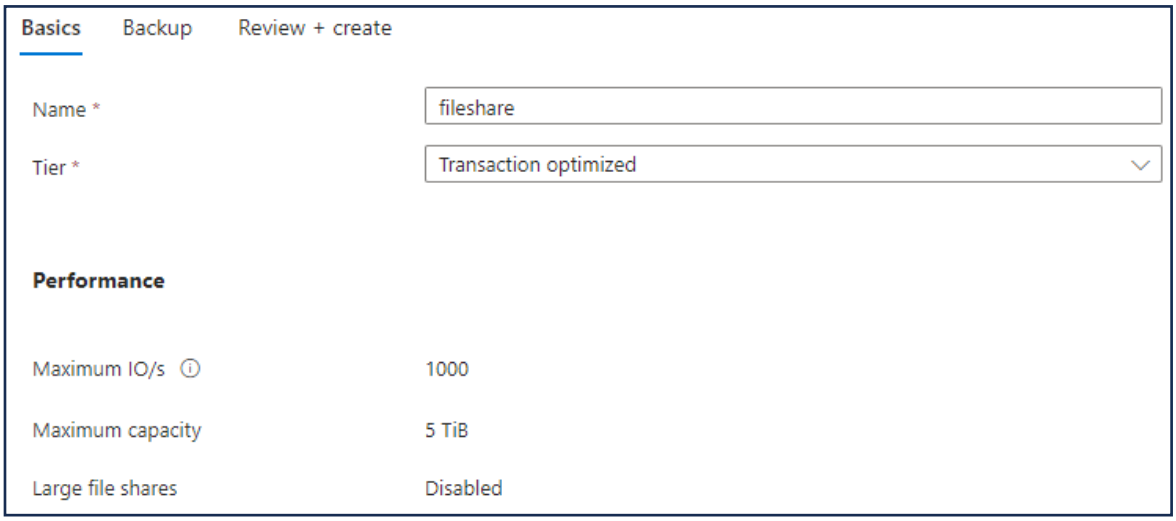


Une fois créé, rendez-vous dans votre storage account, et cliquez sur « file share » dans l'onglet « Data storage » :

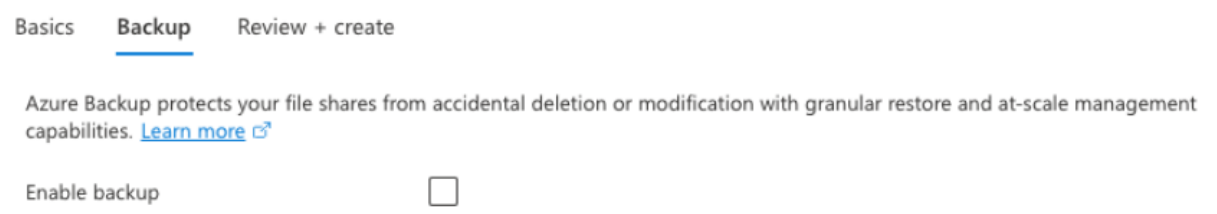


Créer un partage de fichiers en cliquant sur le bouton « + File Share » :

Dans la page suivante, entrez les informations suivantes, puis cliquez sur Next / Sauvegarde :

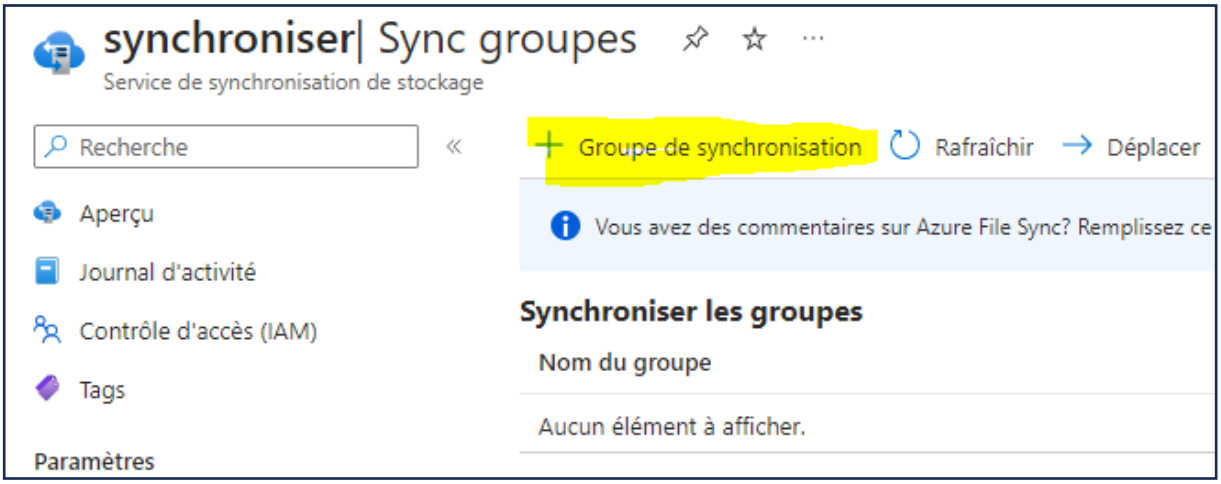


Décochez la case Enable Backup, puis vous pouvez cliquer sur Review + Create :

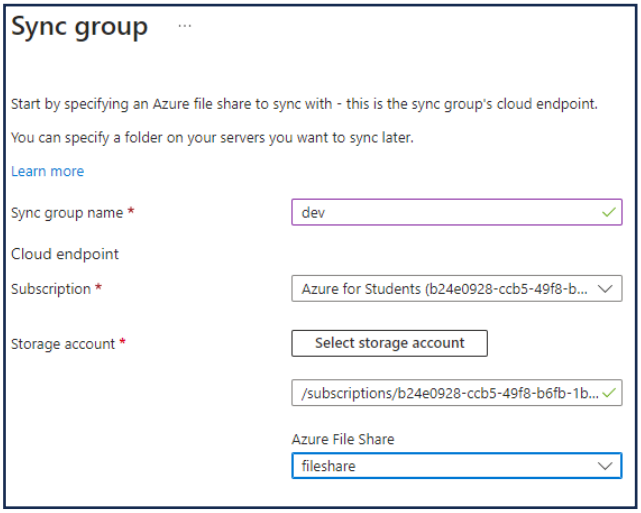


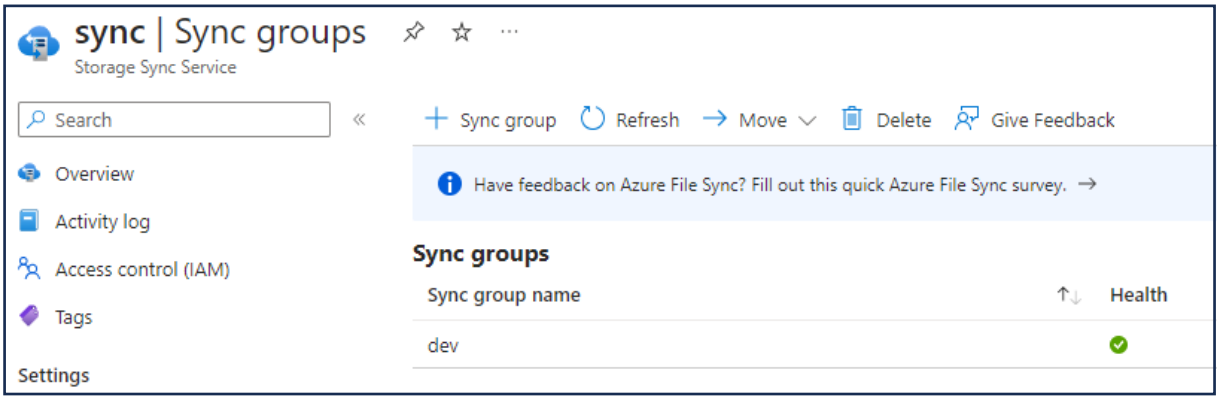
Ensuite recherchez le service de synchronisation de stockage en entrant dans la barre de recherche « Storage Sync Services » :

Puis cliquez sur le bon bouton « + Sync group »/ « +Groupe de synchronisation » afin d'ajouter un groupe :



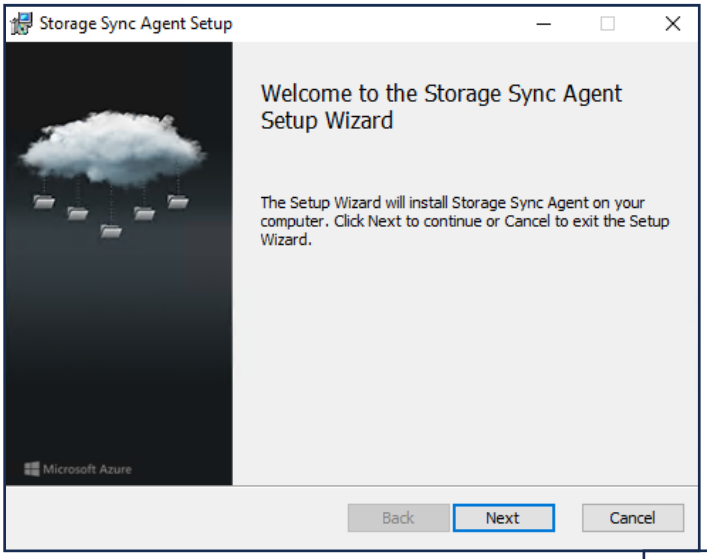
Dans cette page, nommez votre groupe Sync « dev », puis cliquez sur Select Storage Account et sélectionnez votre compte de stockage précédemment créé :





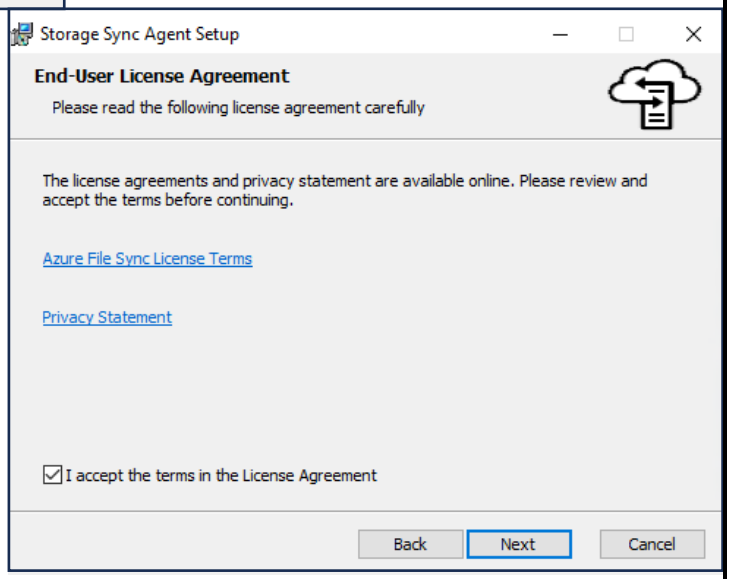
Connectez-vous en RDP à votre VM Windows Serveur.

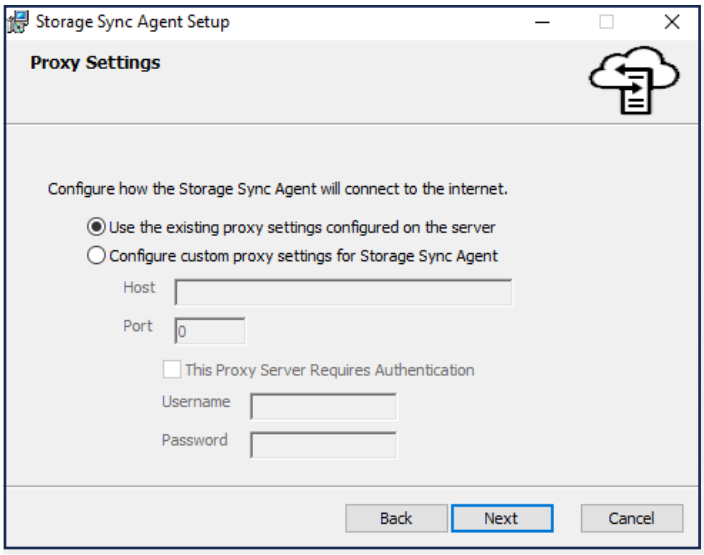
Une fois connecté, installez l'agent via le lien suivant : https://www.microsoft.com/en-us/download/details.aspx?id=57159



Cliquez sur Next

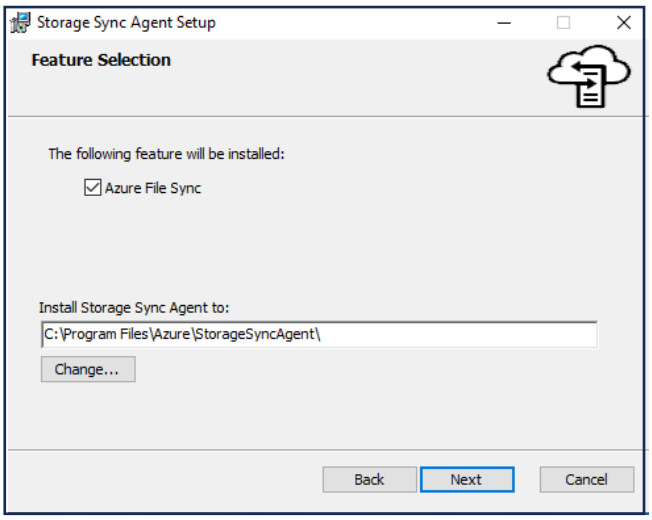
Acceptez les termes et cliquez sur Next

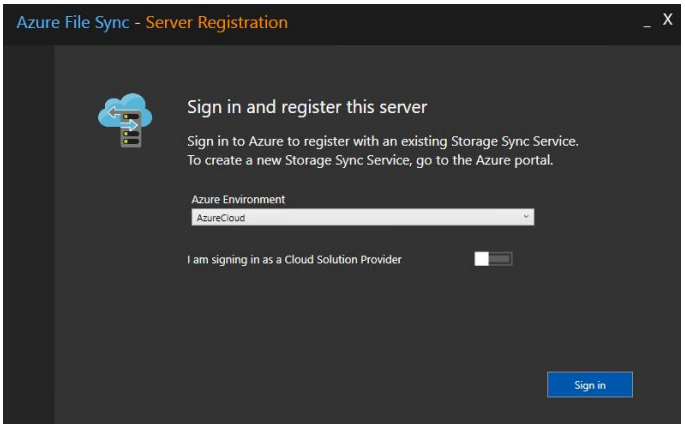




Laissez la première case cochée et cliquez sur Next

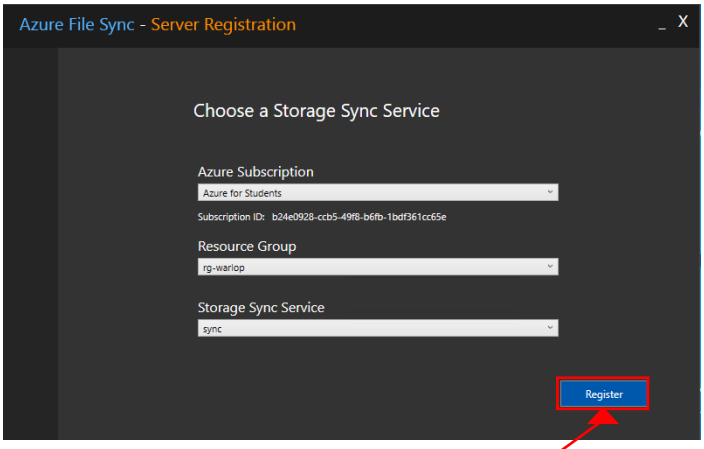
Concernant le chemin de stockage de votre agent, je vous conseille de le laisser par défaut et de cliquer ensuite sur Next

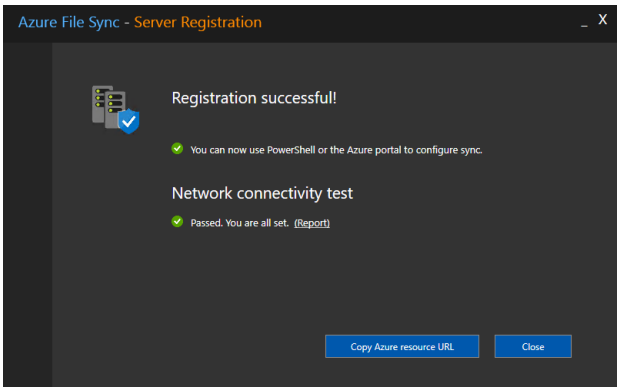




Nous sommes désormais sur l'agent, entrez « AzureCloud » pour l'environnement Azure.

Dans la page d'après, entrez les seules informations possibles pour chaque lignes et cliquez sur Register :

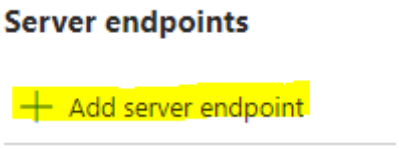




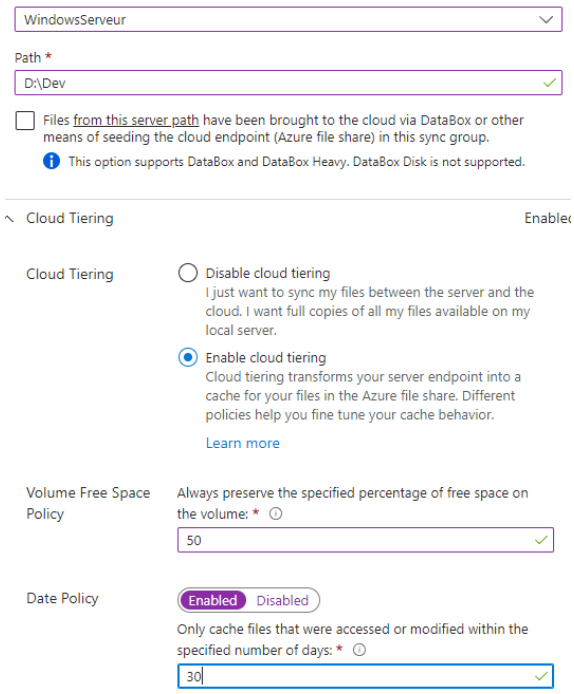
La connexion s'établit correctement.

Dans le portail Azure, recherchez lab-sync.

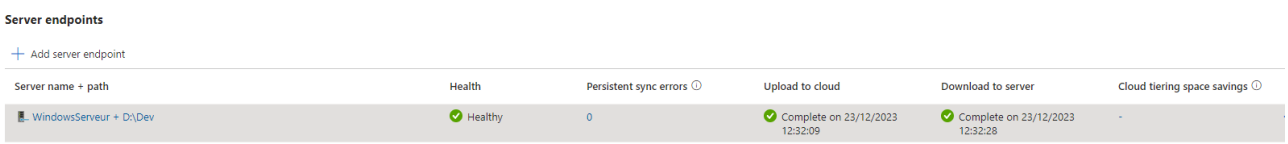
Cliquez ensuite sur Dev, vous allez créer un serveur Endpoint en cliquant sur le bouton « Add Server Endpoint » :



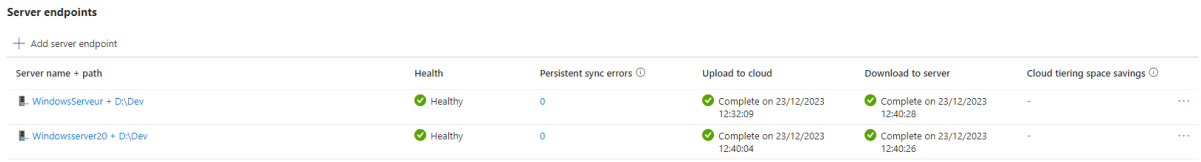
Entrez les informations suivantes puis cliquer sur créer :



Après environ deux minutes, le point de terminaison du serveur Windows serveur recevra une coche verte dans sa colonne HEALTH :

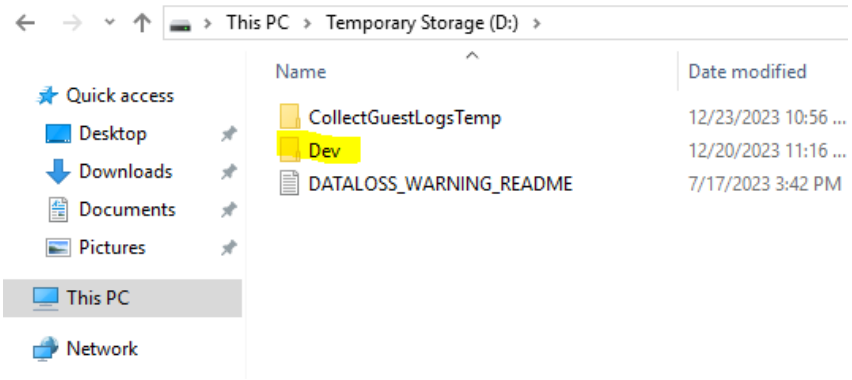


Mon collègue a ajouté sa VM, qui se met également en health au bout de quelques minutes



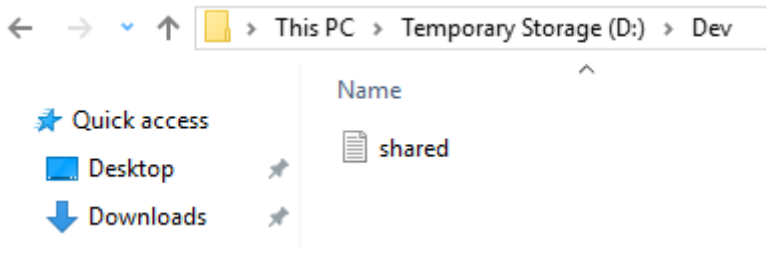
Afin de tester la capacité de base d'Azure File Sync à synchroniser les fichiers entre le point de terminaison du serveur et le point de terminaison du nuage je vais créer un fichier dans mon fichier Dev.

Je me rends sur mon windows serveur, puis dans mon disque D:\



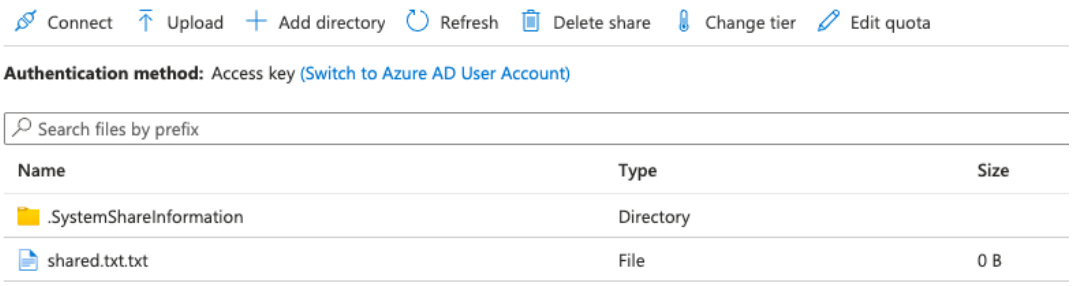
Mon dossier Dev apparait, le point d'accès au serveur fonctionne donc correctement.

Je vais un nouveau fichier texte que je vais appeler shared par exemple :



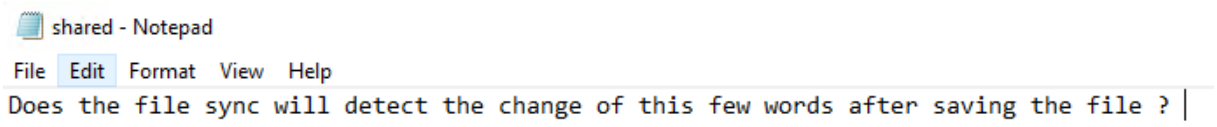
Le fichier s'est également créé sur le poste de mon collègue, la synchronisation fonctionne !

Dans le partage de fichiers de synchronisation du portail Azure, sous Parcourir, cliquez sur Actualiser et observez le fichier shared.txt qui est créé :

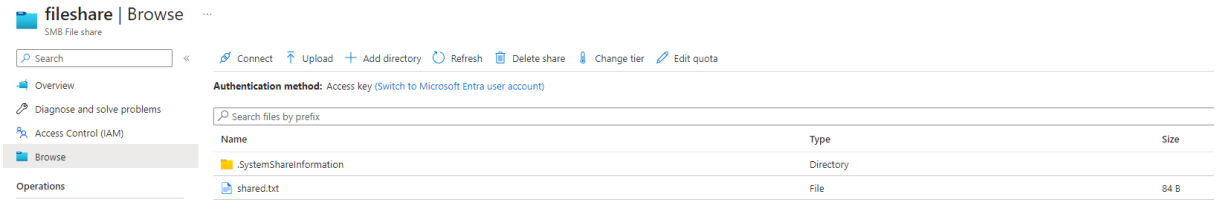


Le fichier est actuellement de zéro octet (0 B) car il s'agit d'un fichier vide. Le fichier. SystemShareInformation est utilisé par le partage de fichiers et est automatiquement ignoré par la synchronisation des fichiers.

Nous allons désormais tester s'il prend la modification de taille en compte, pour se faire nous allons écrire quelques mots dans notre fichier :

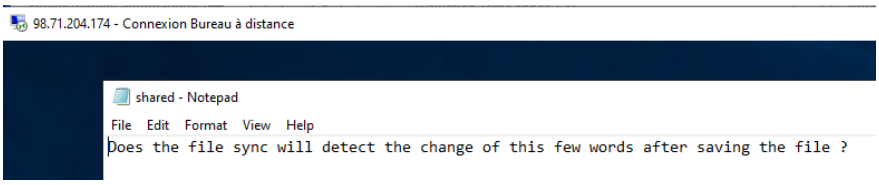


Je le sauvegarde et je vérifie dans la même page que tout à l'heure si la taille de mon fichier a changé :

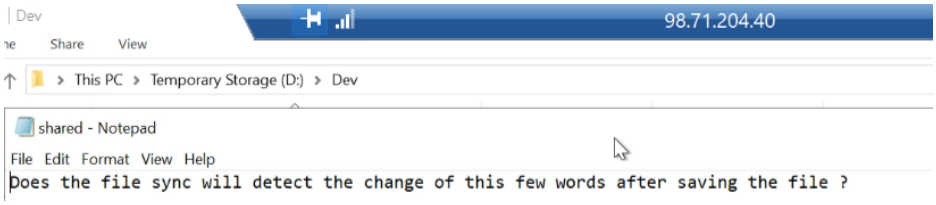


La taille du fichier a changé, il détecte donc les modifications et met à jour le fichier dans un délai d'environ 10 secondes, environ 10 secondes pour le mettre à jour sur le poste de mon collègue également.

Screenshot de ma VM depuis mon serveur Endpoint :



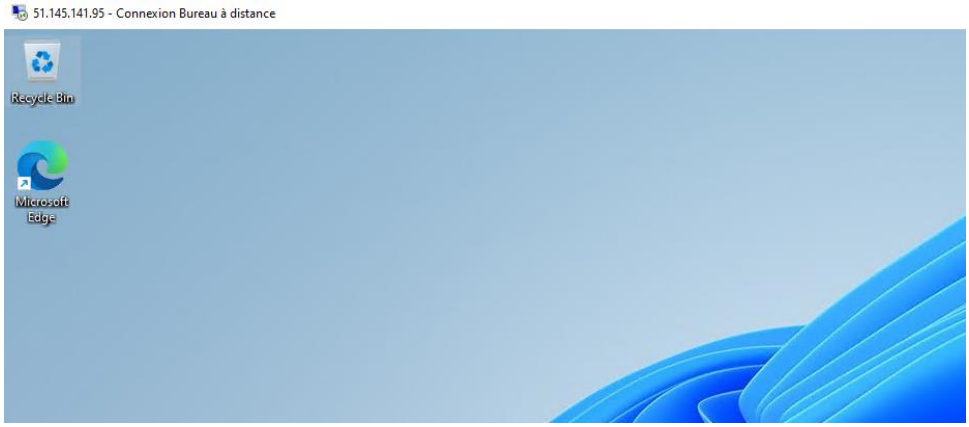
Screenshot de mon collègue depuis son serveur Endpoint :



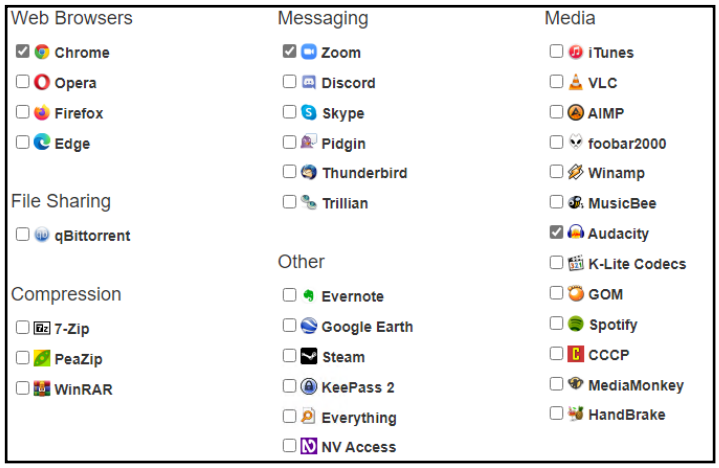
Création d'une VM Golden Image Windows 11 : Personnalisez une VM Windows 11 avec des logiciels spécifiques, effectuez la préparation système ("sysprep") et hébergez l'image dans votre Azure Shared Image Gallery. Cette image servira de référence à l'autre élève pour déployer une VM Windows 11.

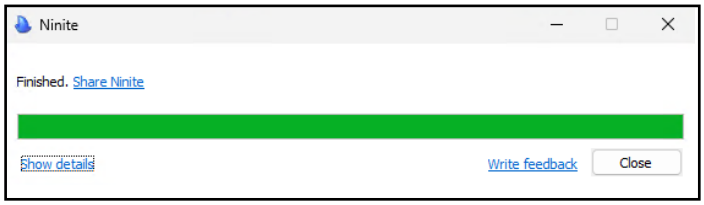
Vous déploierez une VM W11 basé sur l'image de votre voisin

Premièrement, je me créer simplement une VM Windows 11 et je m'y connecte en RDP :



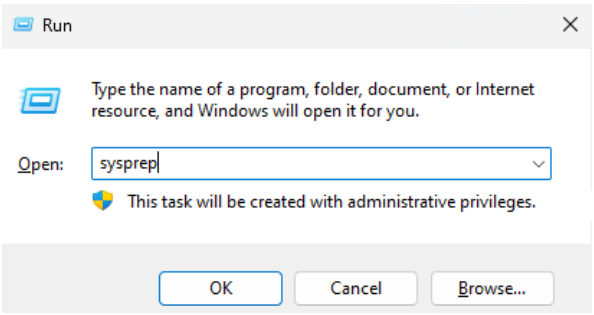
Ensuite, j'installe quelques applications (chrome, Zoom, Audacity) avec l'utilitaire Ninite :



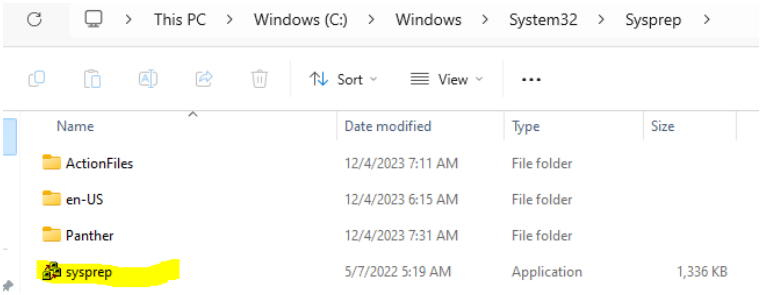


Je vais maintenant utiliser Sysprep pour généraliser la VM. Cela éliminera les informations spécifiques à la machine, la rendant prête à être déployée sur d'autres machines.

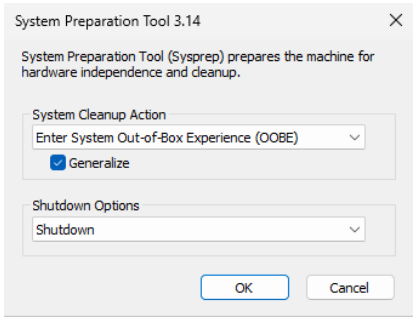
Pour se faire, je fais la combinaison win+r sur mon clavier et j'écris sysprep :



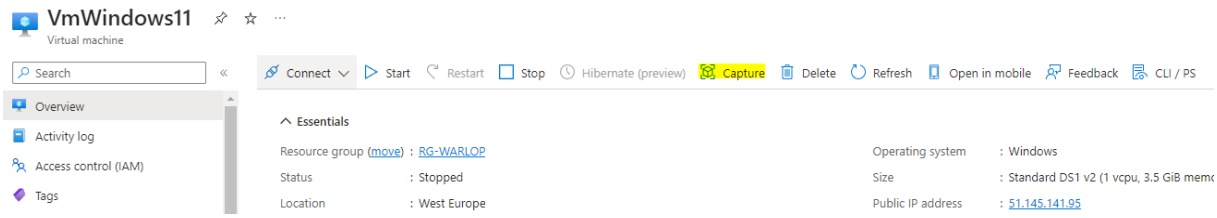
Cliquez sur l'application sysprep :



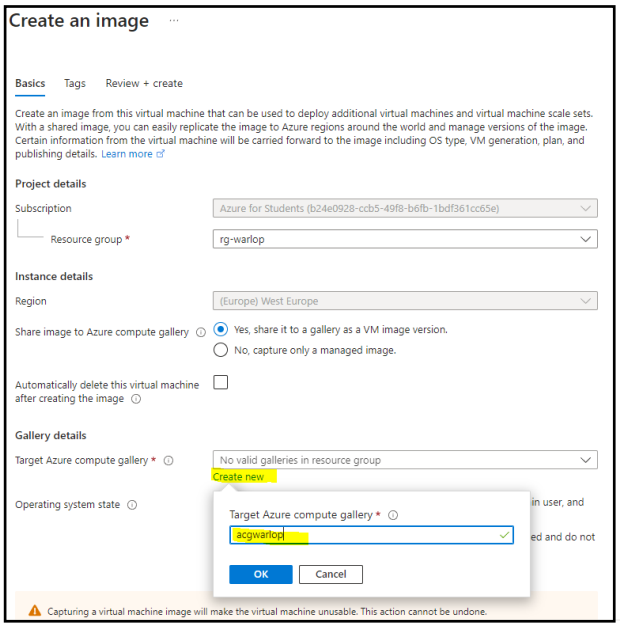
Dans la page suivante, cochez la case « Generalize » puis sélectionnez Shutdown pour l'option de fermeture :

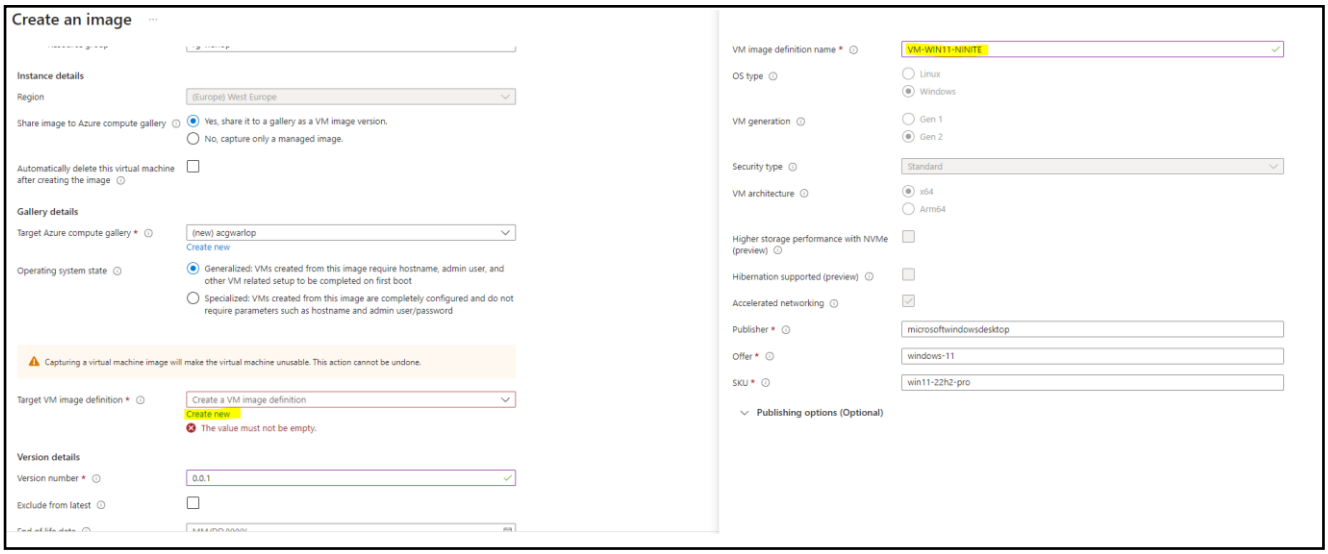


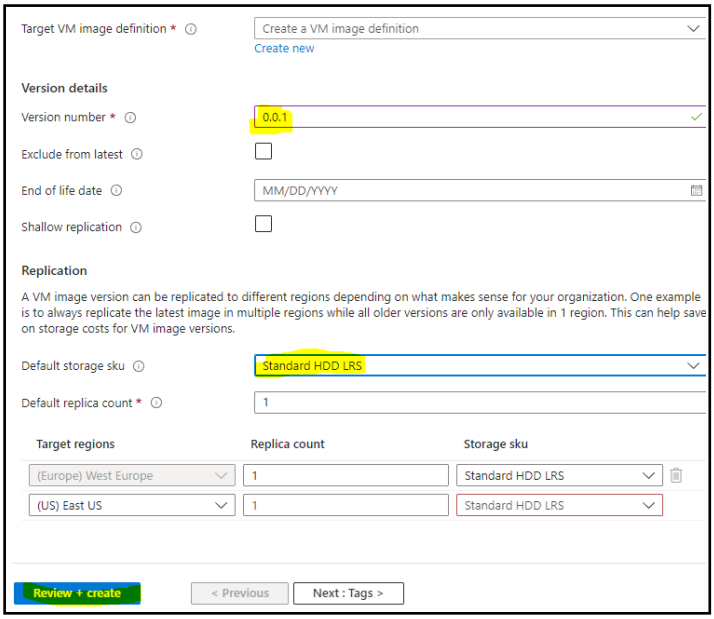
Depuis le portail Azure, accède à la VM, cliquez sur "Capture" et suivez les instructions pour créer une image personnalisée :

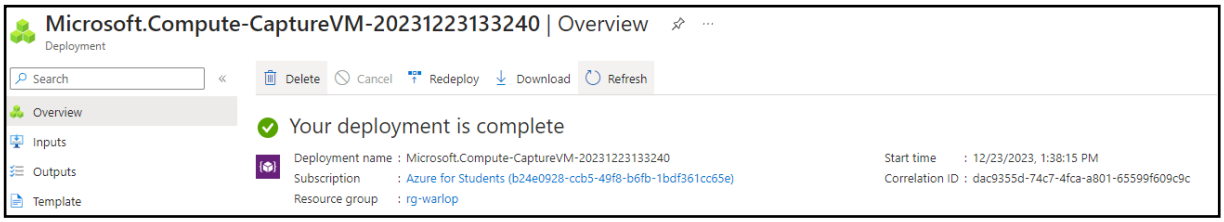


Ci-dessous, les informations à entrer dans l'image :



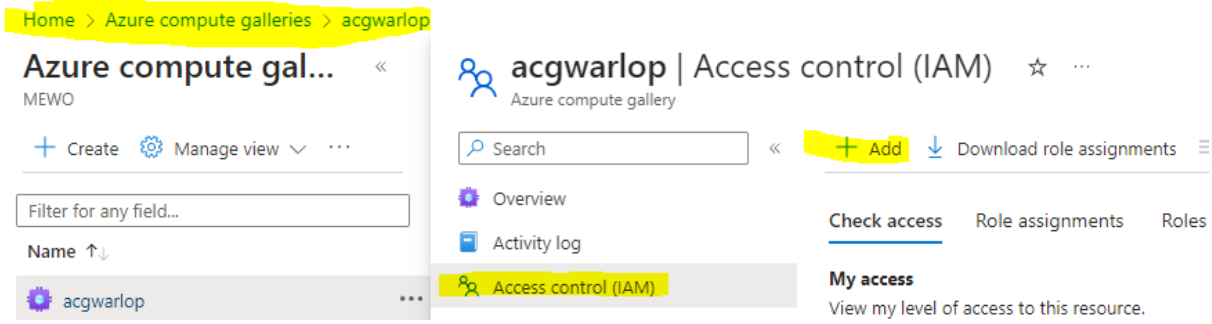




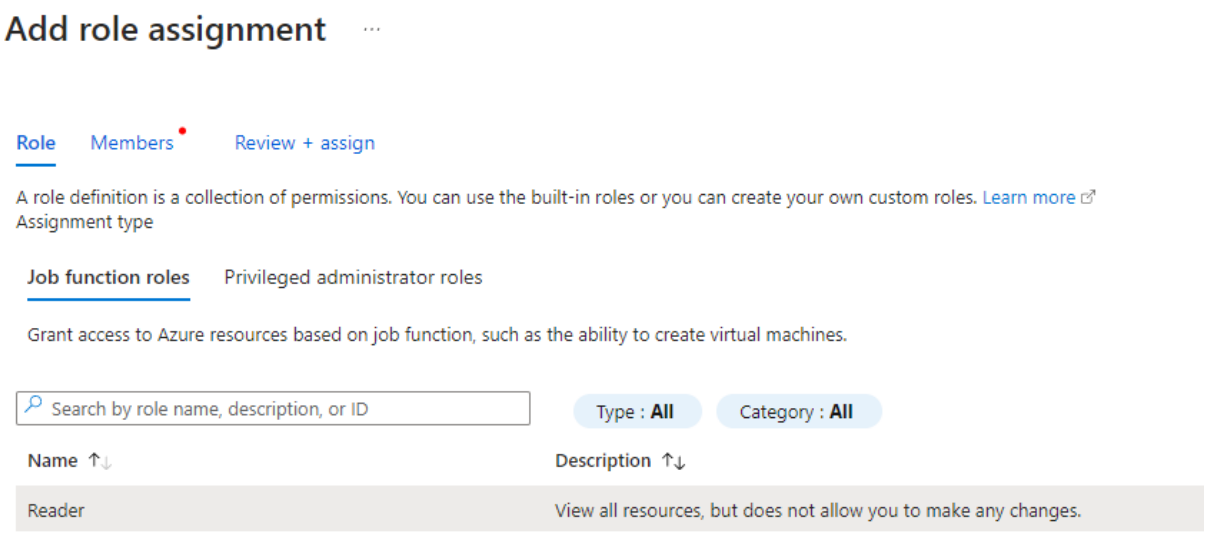


Je vais maintenant me rendre dans mon Azure compute gallery créé précédemment (acgwarlop).

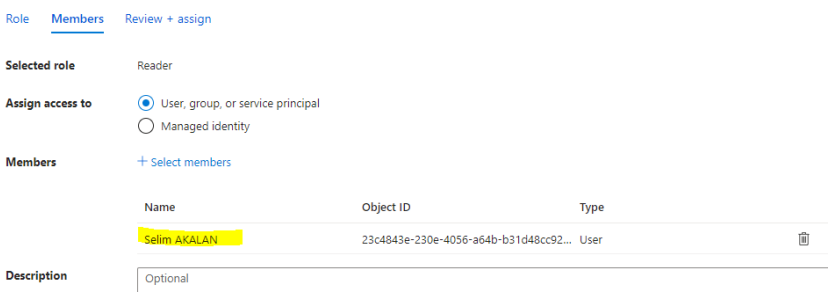
Et je vais ajouter un rôle dans mes IAM :



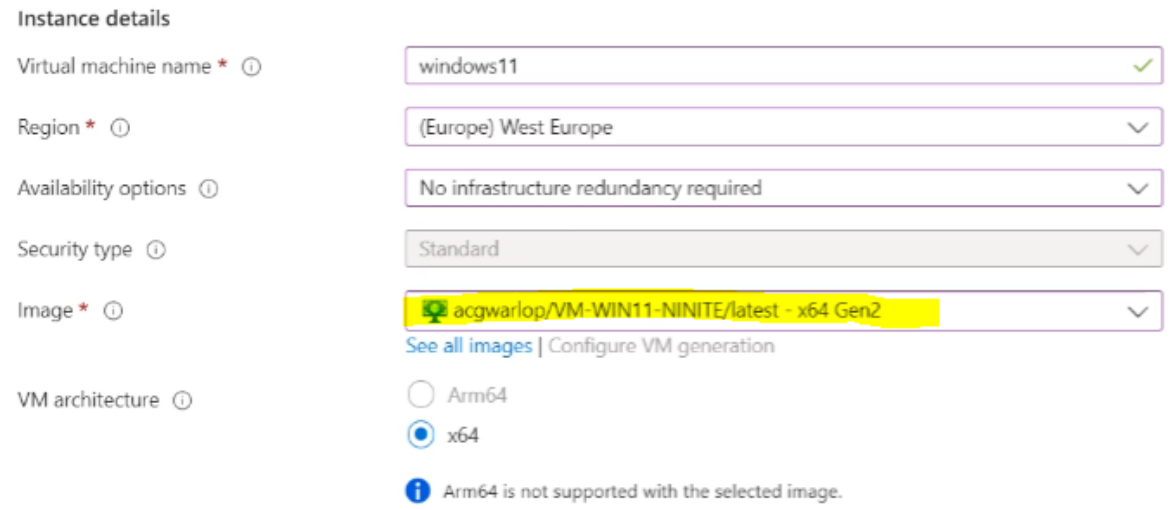
Je sélectionne Reader et je clique sur next :



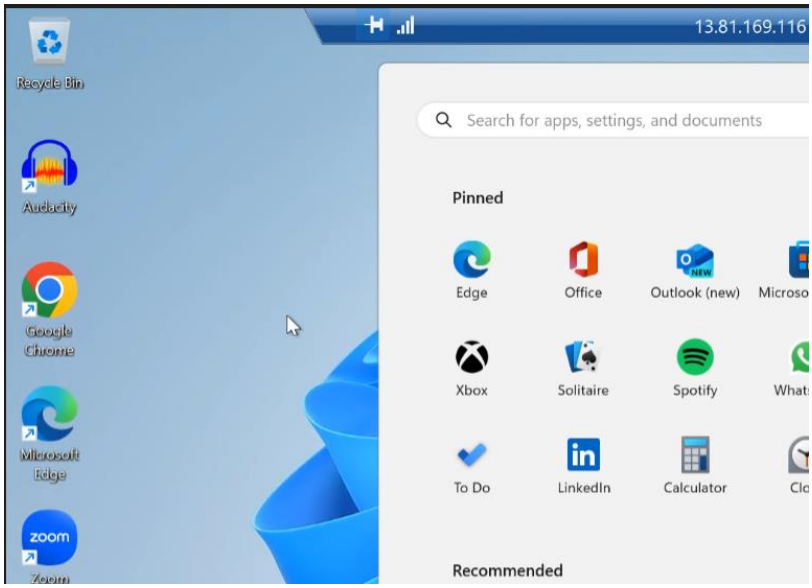
J'ajoute mon collègue concerné et je clique sur Review + Assign :



Désormais, mon collègue va tenter de créer une VM avec l'image que je viens de créer :



Il trouve bien mon image dans les images disponible, il va donc créer sa VM en utilisant mon image, et nous allons vérifier qu'il obtient bien une « copie » de ma VM :

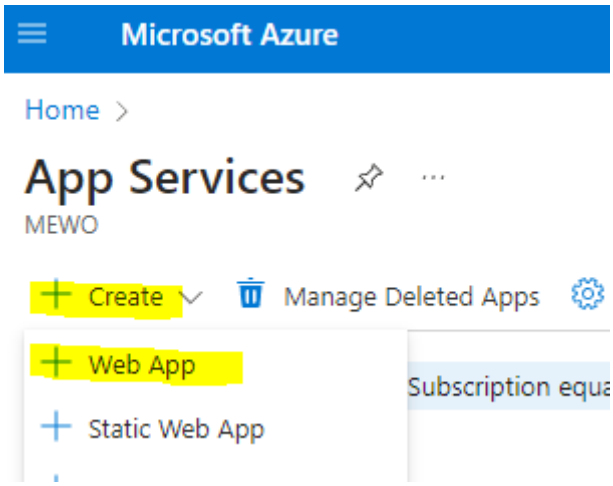


Après avoir allumé et s'être connecté à la VM, il retrouve les logiciels que j'avais préinstallé sur mon image principale. La procédure à donc fonctionnée correctement.

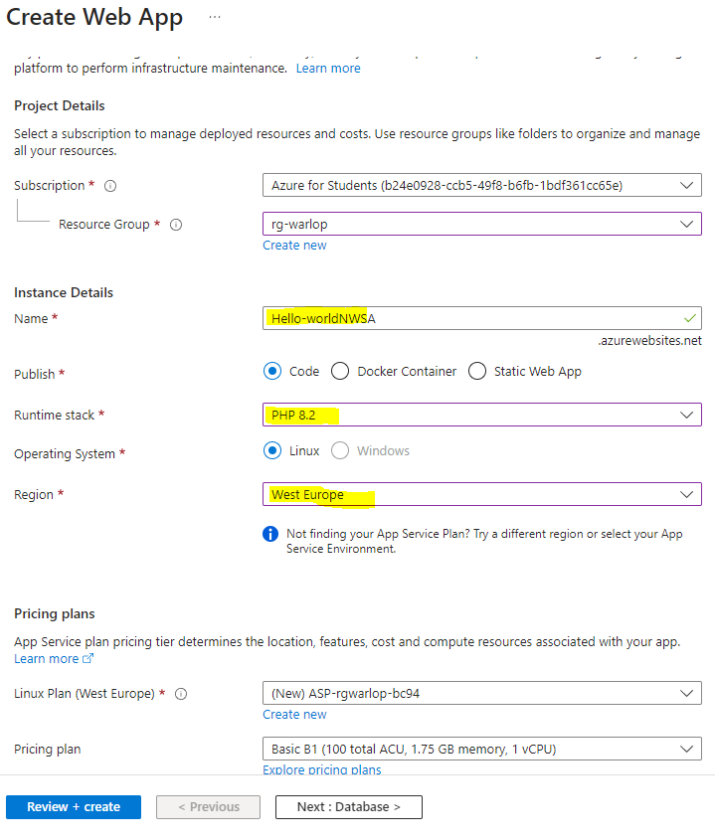
Déploiement d'Application Web : Déployer une application Web vers Azure App Service en utilisant Git localement.

Portal : Vous déploierez une Application Web (Hello-world) sur Azure App Service en utilisant Git en local.

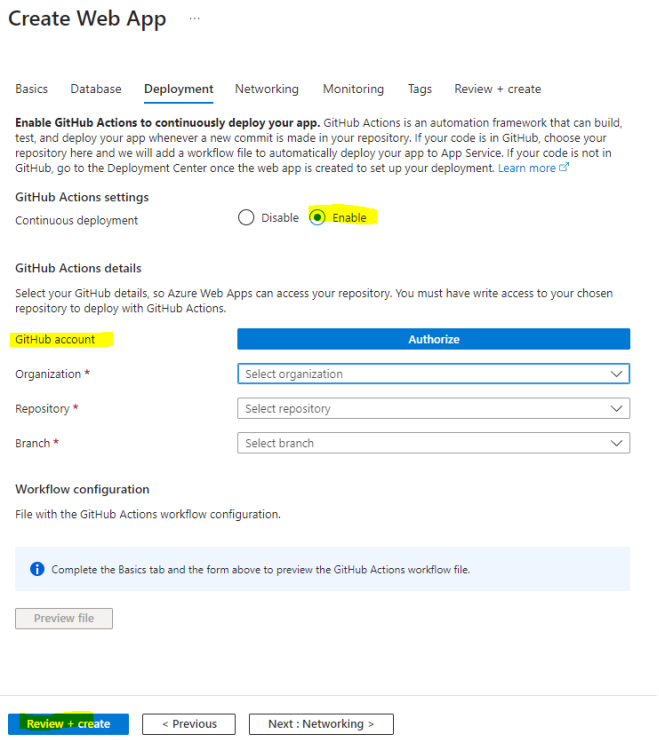
Pour commencer, rendez-vous sur Azure App Service, et ajouter une Web-App :



Je rentre personnellement les informations suivantes, le nom correspond à Nicolas warlop et Selim Akalan :



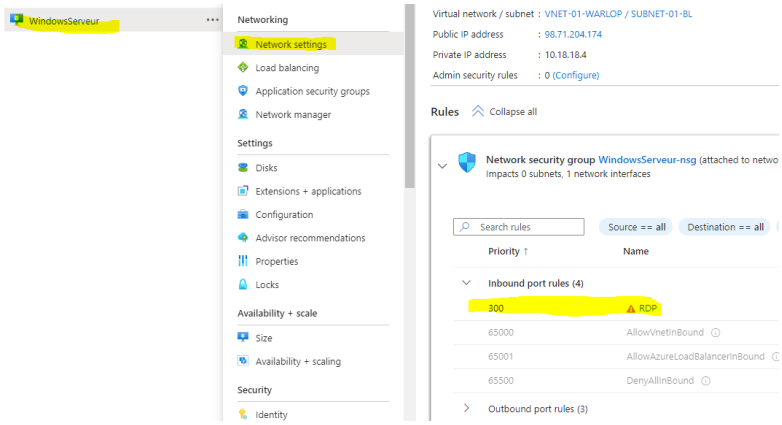
Dans la page Deployment, selectionnez Enable pour Github, puis entrez les informations de votre compte, et cliquez sur Review+Create :



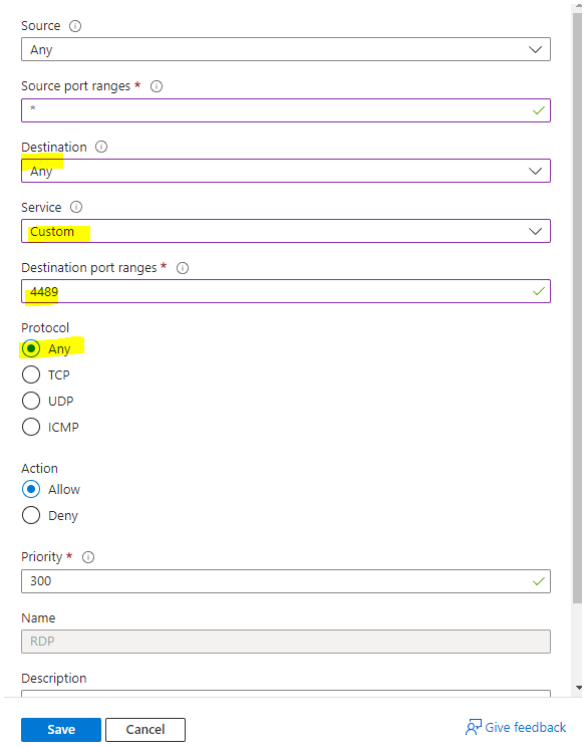
Changer le port RDP d'une VM en 4489.

Pour changer le port RDP d'une VM :

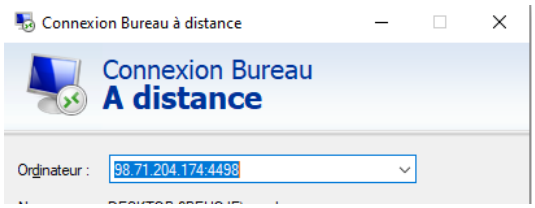
Rendez-vous sur les paramètres de la VM dans Azure, puis dans Network settings, et cliquez sur le port RDP afin de le modifier :



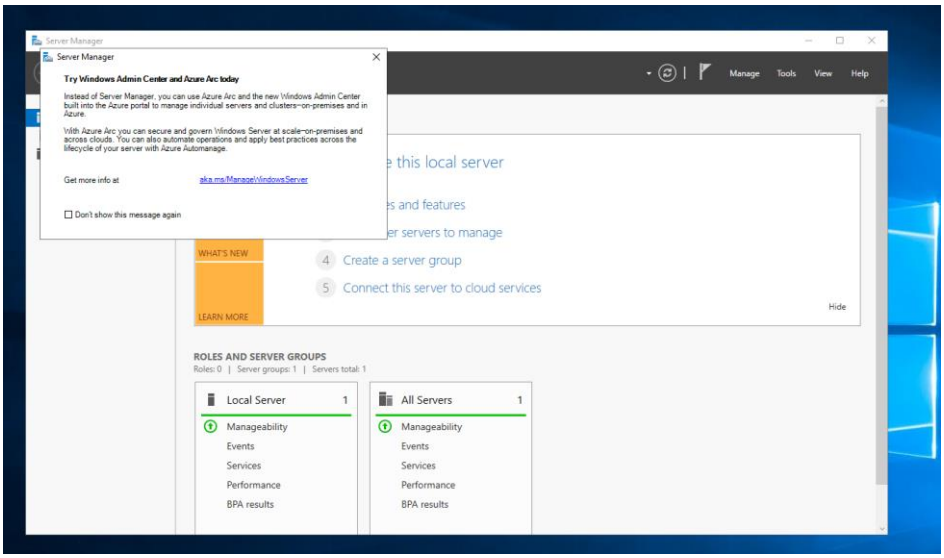
Puis entrez les informations suivantes, et cliquez sur Save :



Ensuite allumez la page RDP de votre poste, entrez l'adresse IP publique de votre VM suivie de « :4489 » et connectez-vous :



Je m'y connecte correctement !



Ps : Si cela ne marche pas, reconnectez-vous sur votre VM en RDP 3389 et entrez les commandes suivantes dans powershell :

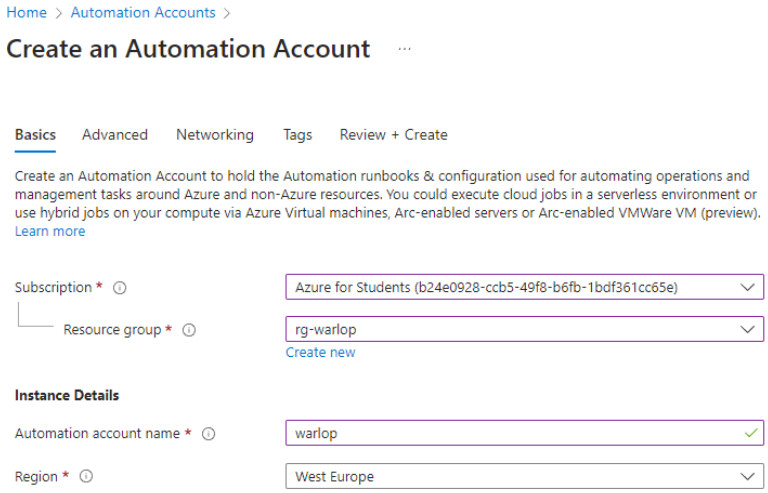
```
PS C:\Users\admina> $portvalue = 4489
>>
>> Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "PortNumber" -Value $portvalue
>>
>> New-NetFirewallRule -DisplayName 'RDPPORTLatest-TCP-In' -Profile 'Public' -Direction Inbound -Action Allow -Protocol TCP -LocalPort $portvalue
>> New-NetFirewallRule -DisplayName 'RDPPORTLatest-UDP-In' -Profile 'Public' -Direction Inbound -Action Allow -Protocol UDP -LocalPort $portvalue
```

Commande pour vérifier le port :

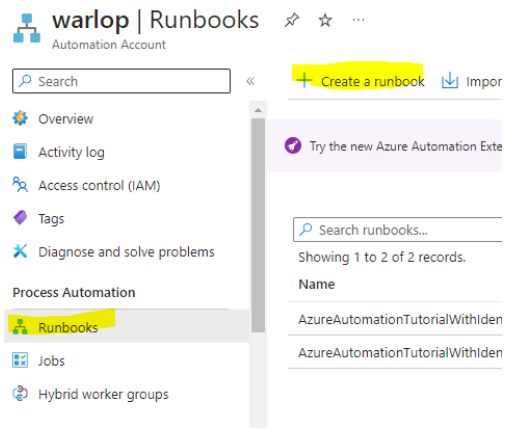
```
PS C:\Users\admina> Get-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "PortNumber"


PortNumber    : 4489
PSPath        : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp
PSParentPath  : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations
PSChildName   : RDP-Tcp
PSDrive       : HKLM
PSProvider    : Microsoft.PowerShell.Core\Registry
```

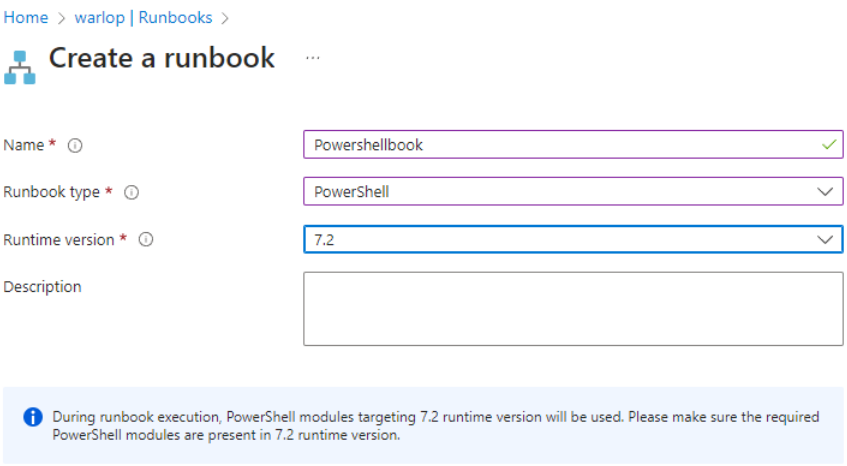
Eteindre automatiquement une VM à 22h et la redémarrer à 6h00.

Pour se faire, commencez par vous rendre dans Automation, et cliquez sur Enable on existing machine :

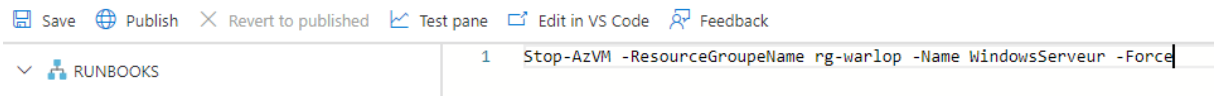


Après vous être connecté à votre compte, cliquez sur l'onglet Runbooks, puis « create a runbook » :

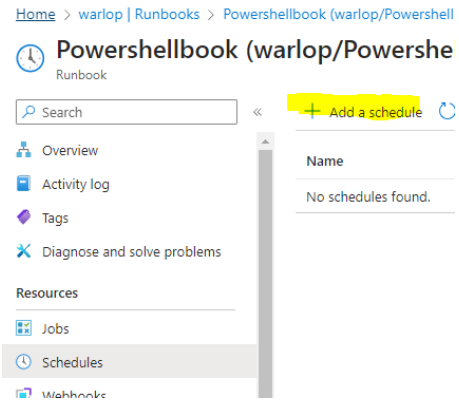




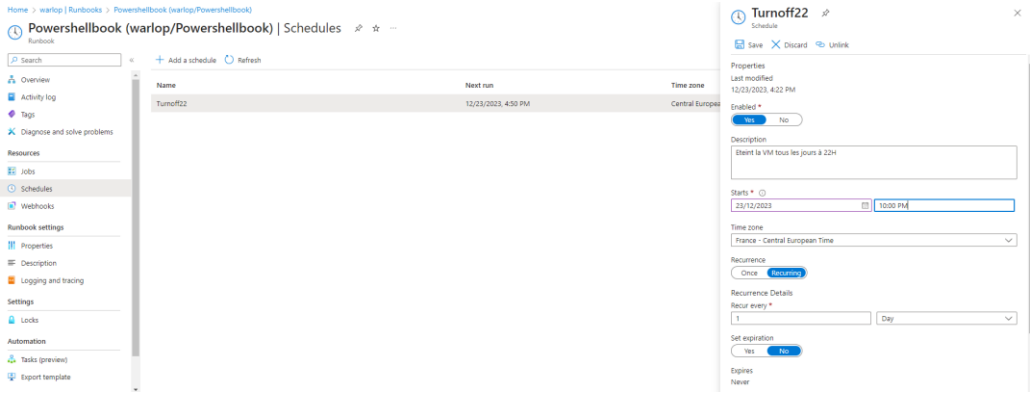
Une fois dans votre Runbook, nous allons utiliser un script PowerShell pour arrêter la VM :



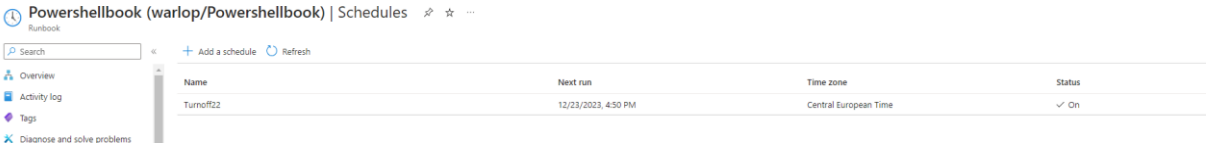
Ensuite publiez votre runbook, et allez dans la section planification pour la configurer afin que le runbook s'exécute tous les jours à 22h :



Vous allez surement avoir besoin de créer un calendrier afin de le lier à ce runbook, je créé donc mon calendrier qui à pour but d'éteindre ma VM à 22h tous les jours :

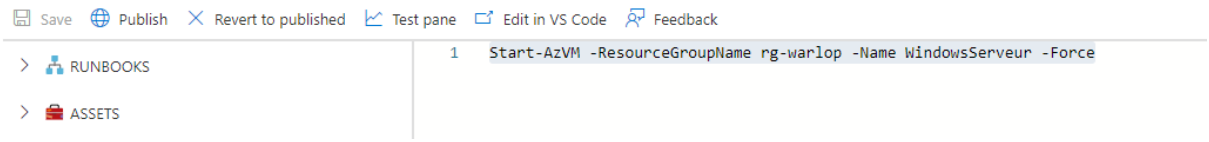


Une fois mon calendrier créé, retournez dans votre Runbook et lier le à votre calendrier :

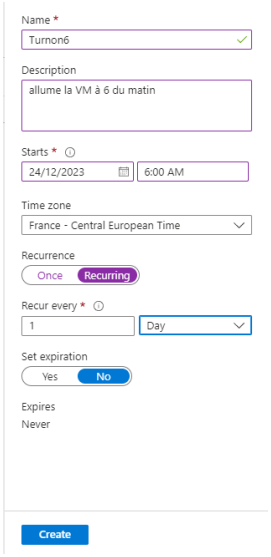


Nous savons maintenant que notre VM s'éteint à 22h tous les jours, nous devons maintenant créer la règle qui allume la VM tous les jours à 6h du matin.

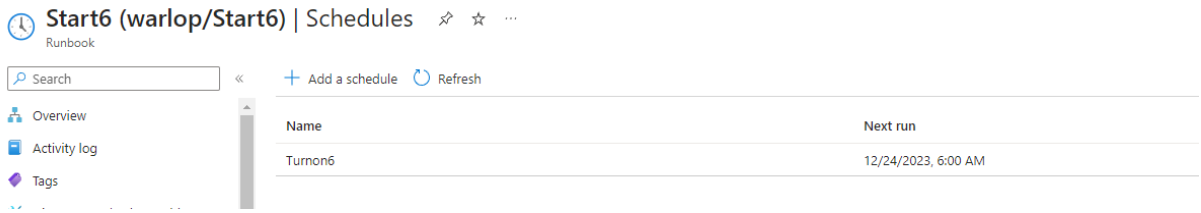
Pour se faire, créez un autre Runbook avec qui portera la commande suivante :



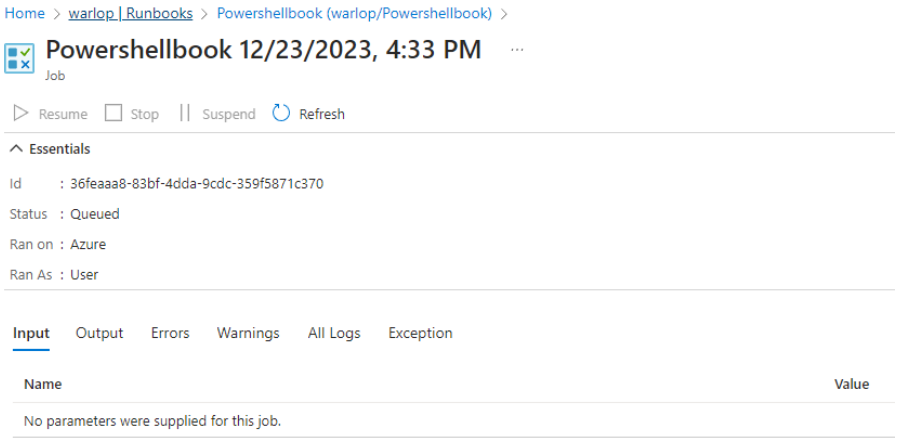
Et créez également un nouveau calendrier avec les options suivantes :



Liez le runbook avec le nouveau calendrier :



Pensez à bien start vos runbook :



Et voilà, plus qu'à attendre 22H pour vérifier que cela fonctionne !