Objectifs du TP :

- Comprendre les rôles intégrés et leur attribution dans Azure.
- Apprendre à contrôler les accès par niveaux (souscription, groupe de ressources, ressource).
- Mettre en place des rôles préconfigurés pour des machines virtuelles Azure.
- Appliquer les principes d'héritage des droits et gestion via des groupes/utilisateurs.

Prérequis :

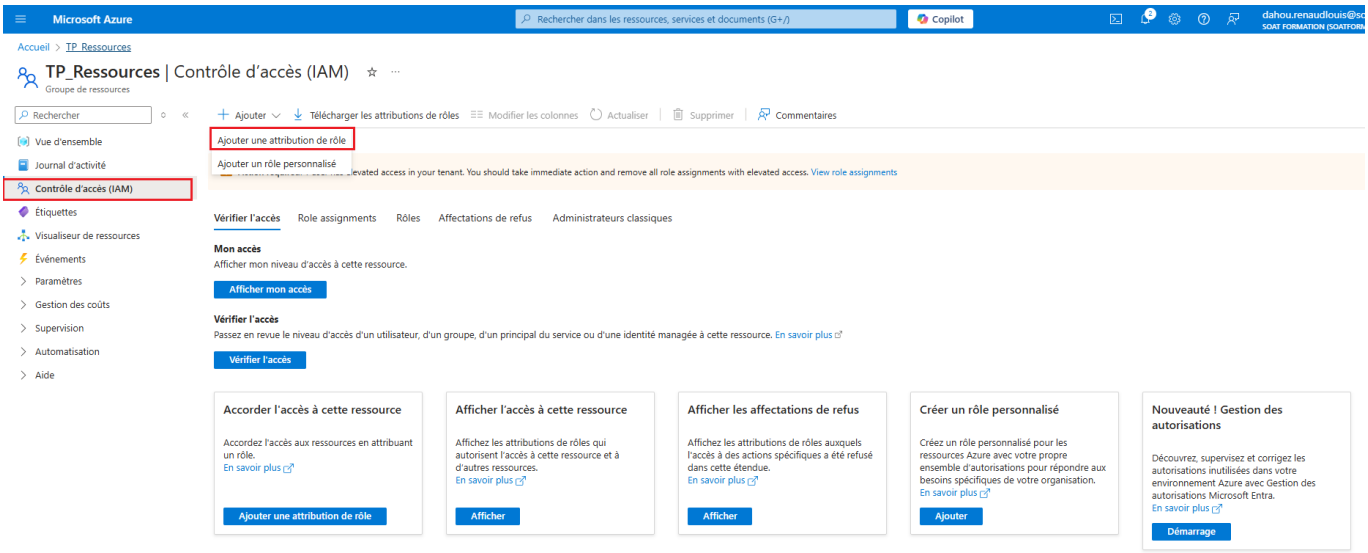
- Un abonnement Azure actif.
- Une machine virtuelle Azure.
- Accès au portail Azure (Azure Portal).
- Connaissances de base sur les concepts de contrôle des accès (IAM - Identity and Access Management).

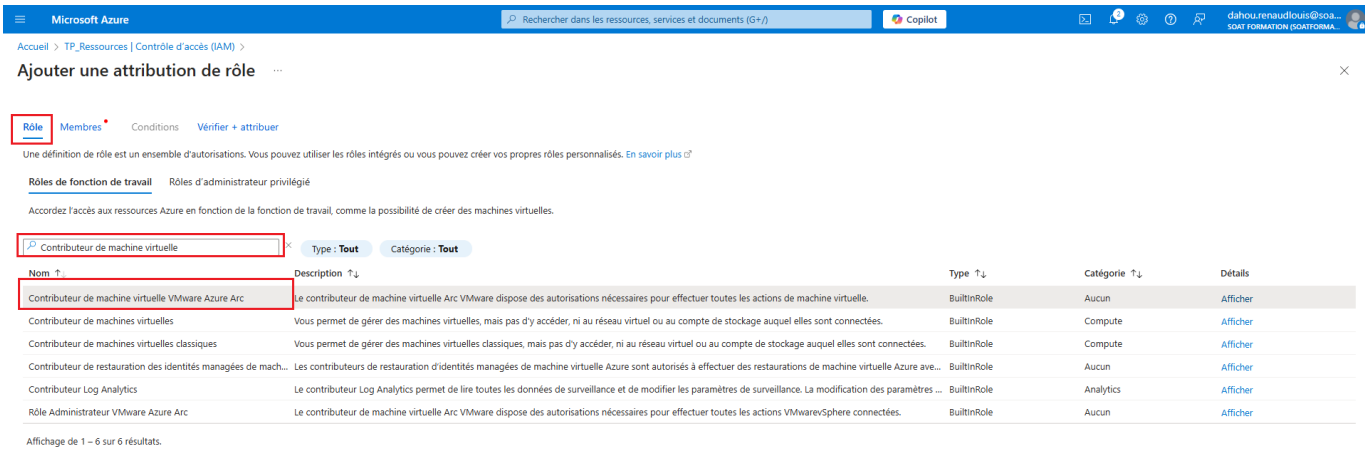
Créer un groupe de ressources :

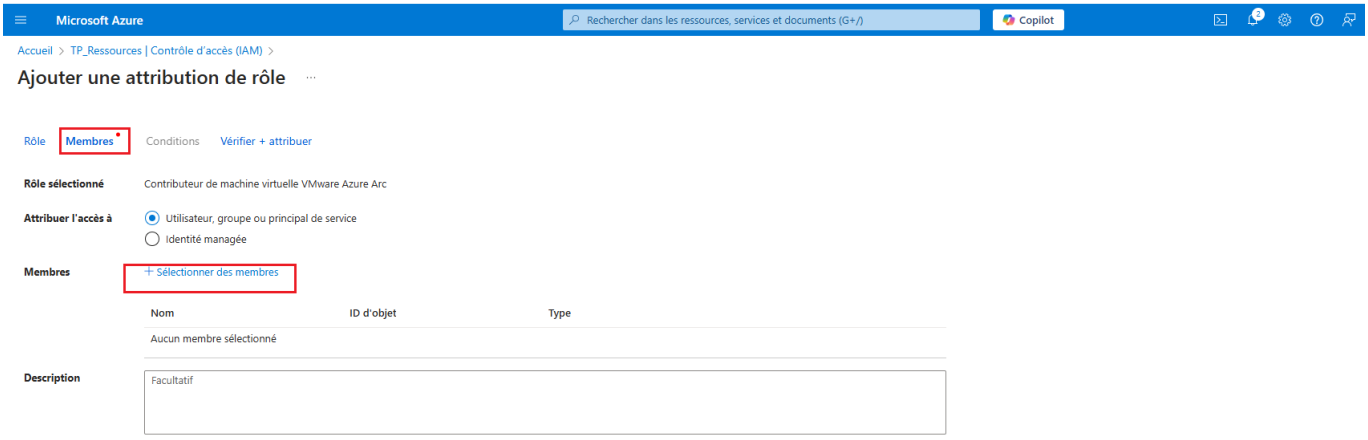
- Allez dans **"Groupes de ressources"** et créez un groupe de ressources, par exemple "TP_Ressources".

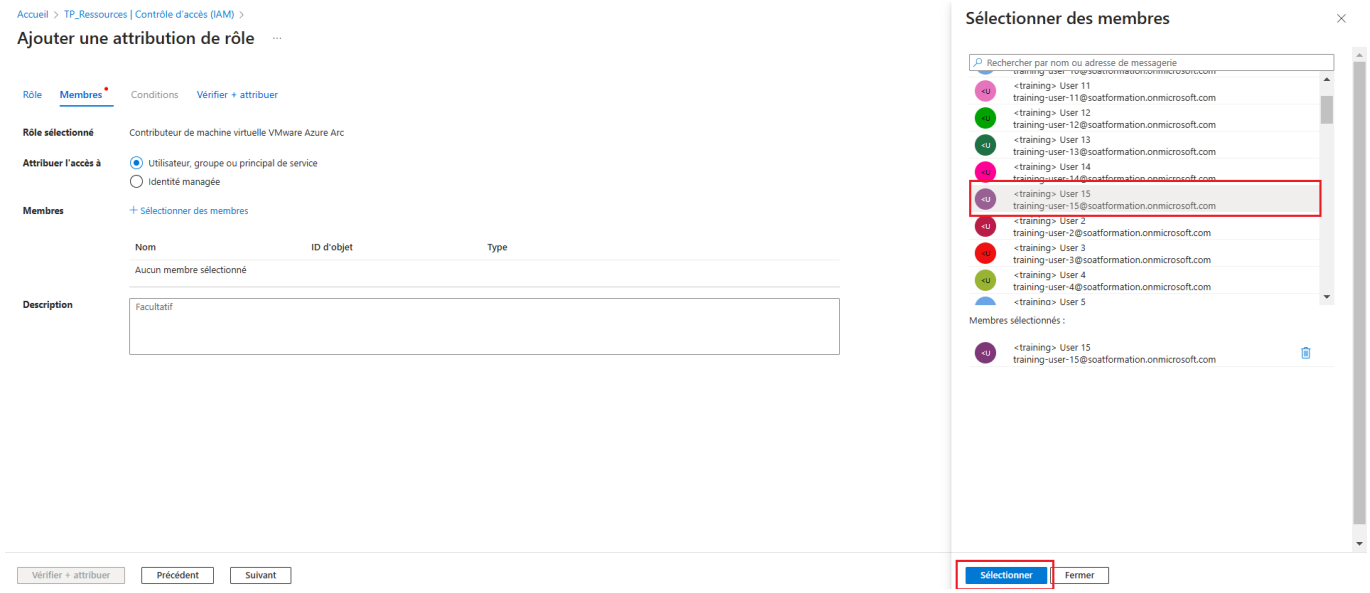
Attribuer des rôles aux utilisateurs :

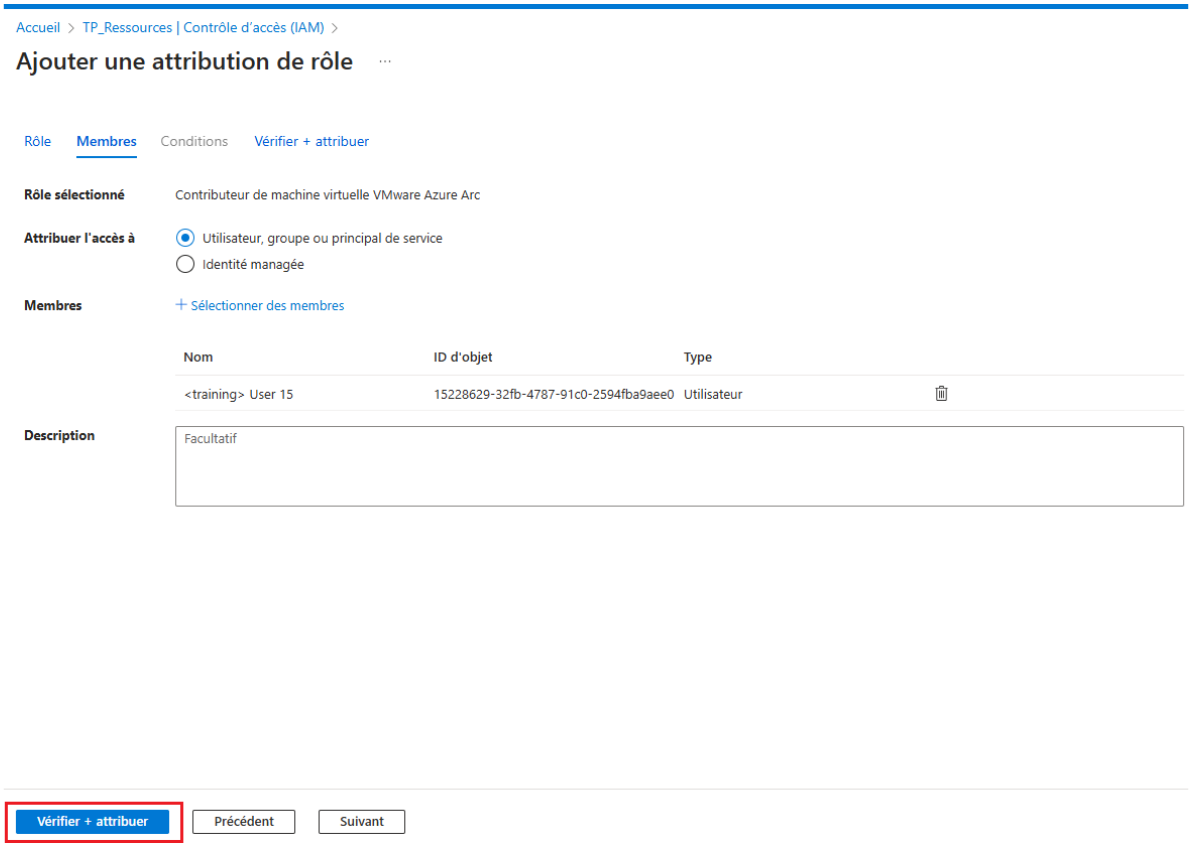
- Allez dans le groupe de ressources créé et sélectionnez **"Contrôle d'accès (IAM)"**.
- Cliquez sur **"Ajouter un rôle"**.
- Sélectionnez le rôle approprié (par exemple, "Contributeur de machine virtuelle VMware Azure Arc").
- Assignez ce rôle à un utilisateur spécifique ou à un groupe d'utilisateurs.

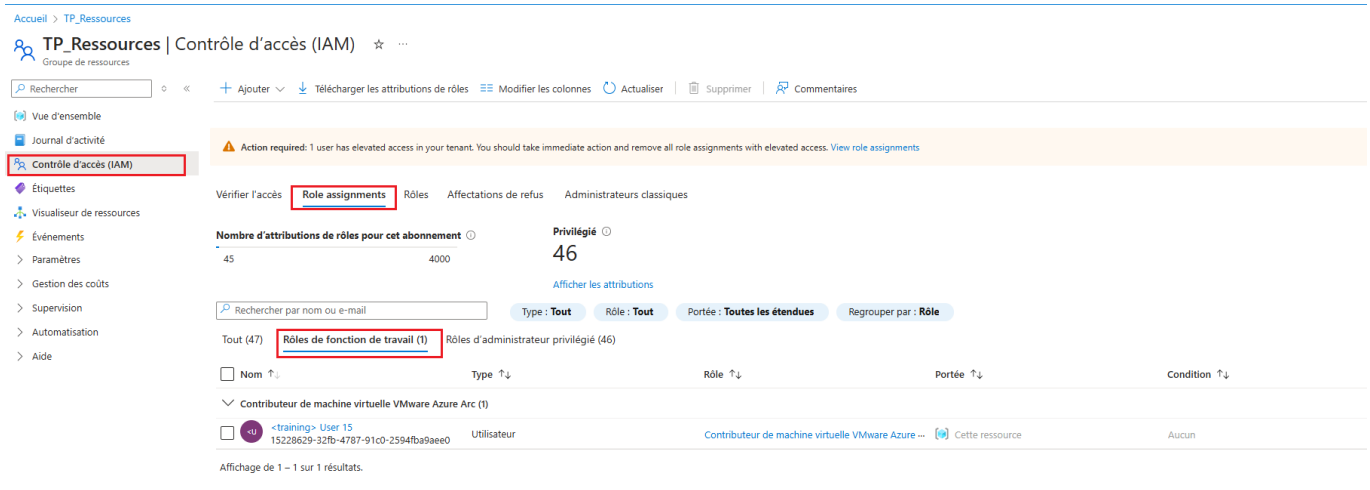

Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
Accueil > TP_Ressources
TP_Ressources | Contrôle d'accès (IAM)
Groupe de ressources
Rechercher
Vue d'ensemble
Journal d'activité
Contrôle d'accès (IAM)
Étiquettes
Visualiseur de ressources
Événements
Paramètres
Gestion des coûts
Supervision
Automatisation
Aide
Ajouter
Télécharger les attributions de rôles
Modifier les colonnes
Actualiser
Supprimer
Commentaires
Ajouter une attribution de rôle
Ajouter un rôle personnalisé
Vérifier l'accès
Role assignments
Rôles
Affectations de refus
Administrateurs classiques
Mon accès
Afficher mon niveau d'accès à cette ressource.
Afficher mon accès
Vérifier l'accès
Passez en revue le niveau d'accès d'un utilisateur, d'un groupe, d'un principal du service ou d'une identité managée à cette ressource. En savoir plus
Vérifier l'accès
Accorder l'accès à cette ressource
Accordez l'accès aux ressources en attribuant un rôle.
En savoir plus
Ajouter une attribution de rôle
Afficher l'accès à cette ressource
Affichez les attributions de rôles qui autorisent l'accès à cette ressource et à d'autres ressources.
En savoir plus
Afficher
Afficher les affectations de refus
Affichez les attributions de rôles auxquels l'accès à des actions spécifiques a été refusé dans cette étendue.
En savoir plus
Afficher
Créer un rôle personnalisé
Créez un rôle personnalisé pour les ressources Azure avec votre propre ensemble d'autorisations pour répondre aux besoins spécifiques de votre organisation.
En savoir plus
Ajouter
Nouveauté ! Gestion des autorisations
Découvrez, supervisez et corrigez les autorisations inutilisées dans votre environnement Azure avec Gestion des autorisations Microsoft Entra.
En savoir plus
Démarrage


Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
Accueil > TP_Ressources | Contrôle d'accès (IAM) >
Ajouter une attribution de rôle
Rôle
Membres
Conditions
Vérifier + attribuer
Une définition de rôle est un ensemble d'autorisations. Vous pouvez utiliser les rôles intégrés ou vous pouvez créer vos propres rôles personnalisés. En savoir plus
Rôles de fonction de travail
Rôles d'administrateur privilégié
Accordez l'accès aux ressources Azure en fonction de la fonction de travail, comme la possibilité de créer des machines virtuelles.
Contributeur de machine virtuelle
Type : Tout
Catégorie : Tout
Nom
Description
Type
Catégorie
Détails
Contributeur de machine virtuelle VMware Azure Arc
Le contributeur de machine virtuelle Arc VMware dispose des autorisations nécessaires pour effectuer toutes les actions de machine virtuelle.
BuiltInRole
Aucun
Afficher
Contributeur de machines virtuelles
Vous permet de gérer des machines virtuelles, mais pas d'y accéder, ni au réseau virtuel ou au compte de stockage auquel elles sont connectées.
BuiltInRole
Compute
Afficher
Contributeur de machines virtuelles classiques
Vous permet de gérer des machines virtuelles classiques, mais pas d'y accéder, ni au réseau virtuel ou au compte de stockage auquel elles sont connectées.
BuiltInRole
Compute
Afficher
Contributeur de restauration des identités managées de mach...
Les contributeurs de restauration d'identités managées de machine virtuelle Azure sont autorisés à effectuer des restaurations de machine virtuelle Azure ave...
BuiltInRole
Aucun
Afficher
Contributeur Log Analytics
Le contributeur Log Analytics permet de lire toutes les données de surveillance et de modifier les paramètres de surveillance. La modification des paramètres ...
BuiltInRole
Analytics
Afficher
Rôle Administrateur VMware Azure Arc
Le contributeur de machine virtuelle Arc VMware dispose des autorisations nécessaires pour effectuer toutes les actions VMwarevSphere connectées.
BuiltInRole
Aucun
Afficher
Affichage de 1 – 6 sur 6 résultats.


Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
Accueil > TP_Ressources | Contrôle d'accès (IAM) >
Ajouter une attribution de rôle
Rôle
Membres
Conditions
Vérifier + attribuer
Rôle sélectionné
Contributeur de machine virtuelle VMware Azure Arc
Attribuer l'accès à
Utilisateur, groupe ou principal de service
Identité managée
Membres
+ Sélectionner des membres
Nom
ID d'objet
Type
Aucun membre sélectionné
Description
Facultatif







Via Azure CLI

```
###Attribuer un rôle à un utilisateur :
az role assignment create --assignee "john.doe@votreentreprise.onmicrosoft.com" --
role "Contributeur de machine virtuelle" --scope /subscriptions/{subscription-
id}/resourceGroups/{resource-group-name}

###Attribuer un rôle à un groupe :
az role assignment create --assignee "AdminsVM" --role "Contributeur de machine
virtuelle" --scope /subscriptions/{subscription-id}/resourceGroups/{resource-
group-name}
```

Contributeur de machine virtuelle

Création d'une VM pour tester les permissions de l'utilisateur

```
az vm create --resource-group TP_Ressources --name MyVM --image Ubuntu2204 --
admin-username azureuser --ssh-key-values "ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQCXhkjJATVZ4gwS+cfk3UuUO3sY1J3NDuDOElTDicaAgAA6STmOIy
hYMzjP0Cp0W7zhaXo9xHsCPJBGRSMH0I1ZtaqrGFQV43J7eOsrZ2bdzqCsbj8qstxxMigfaZ4ds9DSE8Od
/KflNx/SWlgPCps8gJAfDtzvrmnbUB88h25ZboVHODkpeb3BhqeoNrG+qZ4bypgVqv8A/FpUqM/Tse43Tt
743kY2KdF2HBHbXGfpHshtfTOI09qY77O6Ua3ew/ZyhoVUtBstQuhZZj67gqOt4aZS7iiqaxvFvpr7PWnq
c7iHZfUGsh5HrBepwobod3ONneieLZypLBE6V6xTq7pHqa8eFVCZZtxCBk8tHIPd9WBxxvbsope1SOl5vb
Sjr2+iB6lL4We+PRUyuvyYZZIfpu+JECbYYOoef4uDgvpTnKRBTm4FsUwsFsArSnvdSuMxTUz7V3bVTYJx
JuDRf0qxxeJI541yCMFjUWUpwY/uu8n9qFBUEeytzSXDI/fvyi0= generated-by-azure" --size
Standard_DS1_v2
```

Modification de permission

Le but ici est de réduire les permissions

```
az role assignment list --assignee training-user-15@soatformation.onmicrosoft.com
--all --output table
Principal                                       Role
Scope
----------------------------------------------  ------------------------------  -
-------------------------------------------------------------------------------
training-user-15@soatformation.onmicrosoft.com  Azure Arc VMware VM Contributor
/subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8/resourceGroups/TP_Ressources



az role assignment delete --assignee training-user-
15@soatformation.onmicrosoft.com --role "Azure Arc VMware VM Contributor" --scope
/subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8/resourceGroups/TP_Ressources
```

```
az role assignment create --assignee training-user-
15@soatformation.onmicrosoft.com --role "Virtual Machine Contributor" --scope
/subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8/resourceGroups/TP_Ressources
```

```
Attention:  Si l'utilisateur fait partir d'un group d'utilisateur qui a déja des
permission élevé ça fonctionnera pas

etant donné qu'il apartient au groupe "Training Users" qui a un role "Owner" nous
allons retiré cela d'abord



az ad user get-member-groups --id training-user-15@soatformation.onmicrosoft.com -
-output table

az ad group show --group "Training Users" --query "id" --output table

az role assignment list --assignee <Object-ID-du-groupe> --all --output table

az role assignment list --assignee c8492b57-07e1-4034-9dd0-577d65c8b6f2 --all --
output table

az role assignment delete --assignee c8492b57-07e1-4034-9dd0-577d65c8b6f2 --role
"Owner" --scope /subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8

az role assignment create --assignee training-user-
15@soatformation.onmicrosoft.com --role "Virtual Machine Contributor" --scope
/subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8/resourceGroups/TP_Ressources
```

🔷 Étape 3 : Tester les permissions de l'utilisateur

1️⃣ Tester l'accès au portail Azure

📌 **Connectez-vous avec l'utilisateur de test** :

1. Ouvrez une session avec l'utilisateur (ex. `training-user-15@soatformation.onmicrosoft.com`).
2. Accédez au portail Azure.
3. Naviguez vers **Groupes de ressources** → Sélectionnez le groupe contenant la VM.
4. **Vérifiez que l'utilisateur peut :** ✅ Démarrer / arrêter la machine virtuelle.
   ✅ Modifier ses paramètres (ex. taille, étiquettes, extensions).
   ✅ Supprimer la VM.
   ❌ Ne peut pas supprimer VNet
