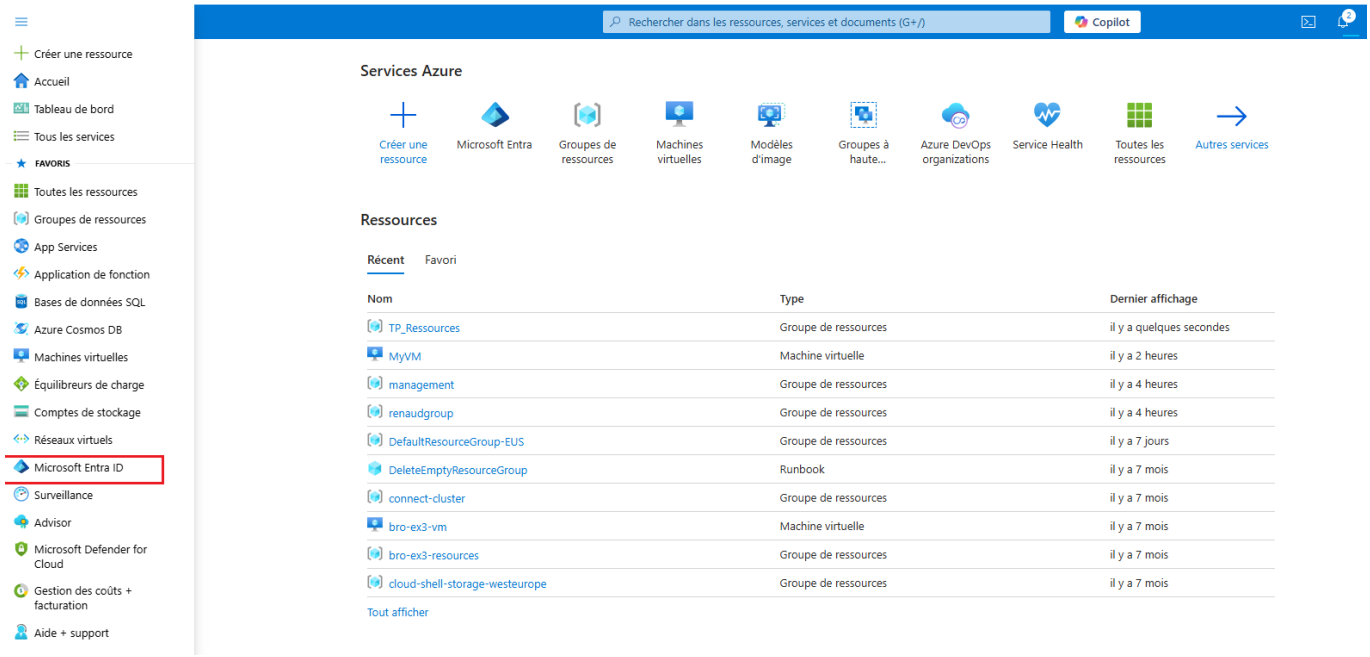
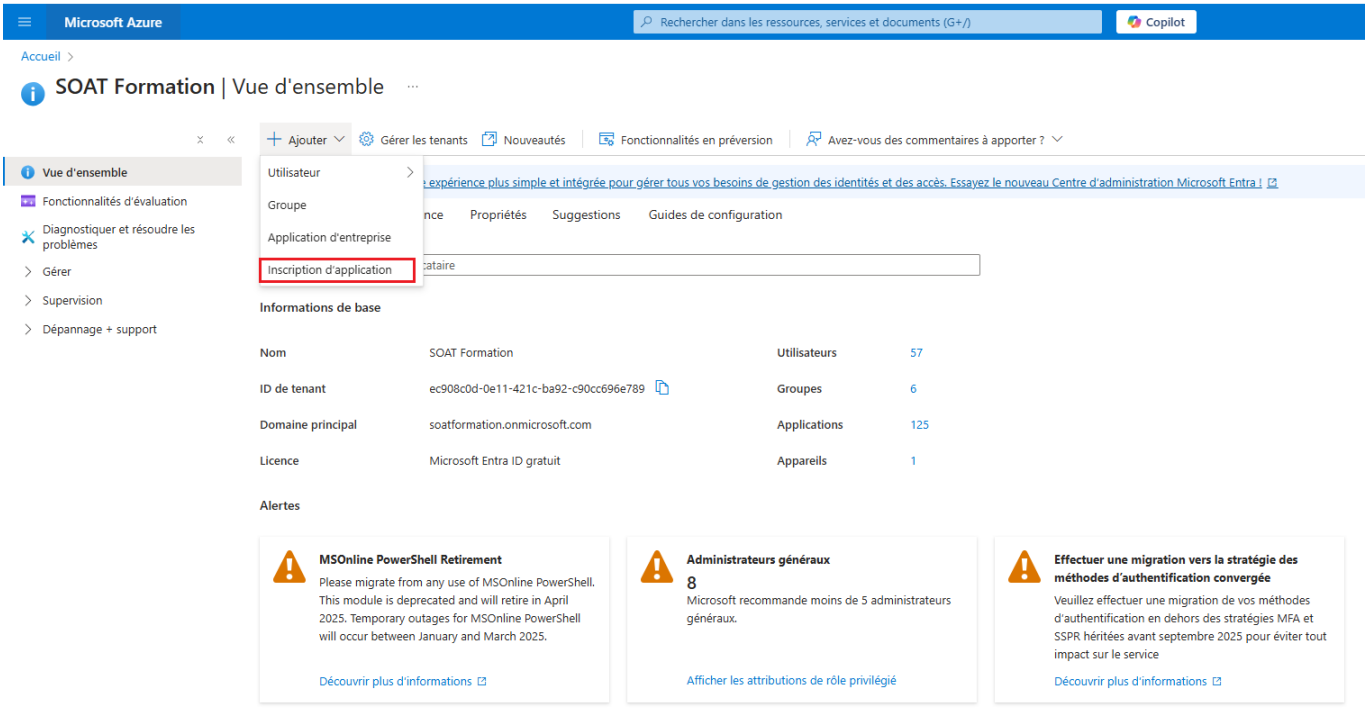
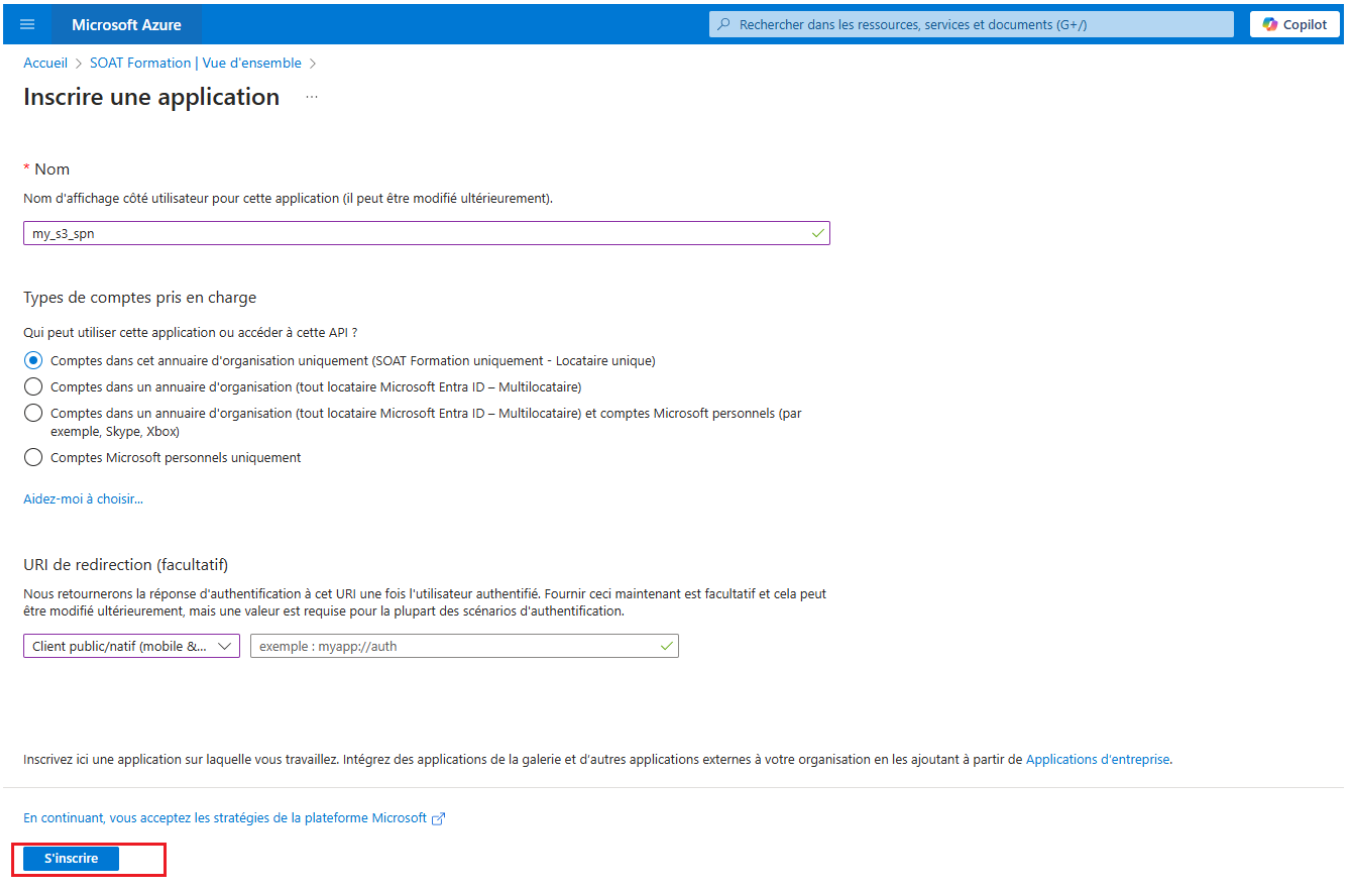
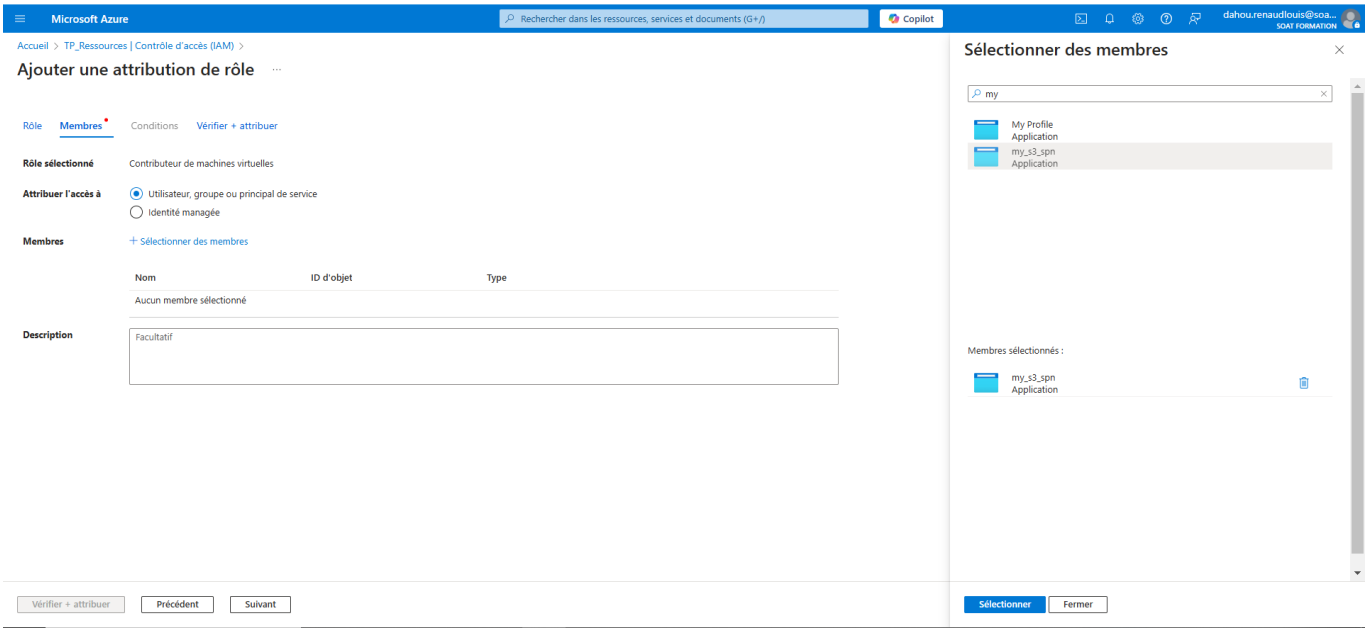
Attribution des rôles via un Service Principal (SPN) et Azure Active Directory (AAD)

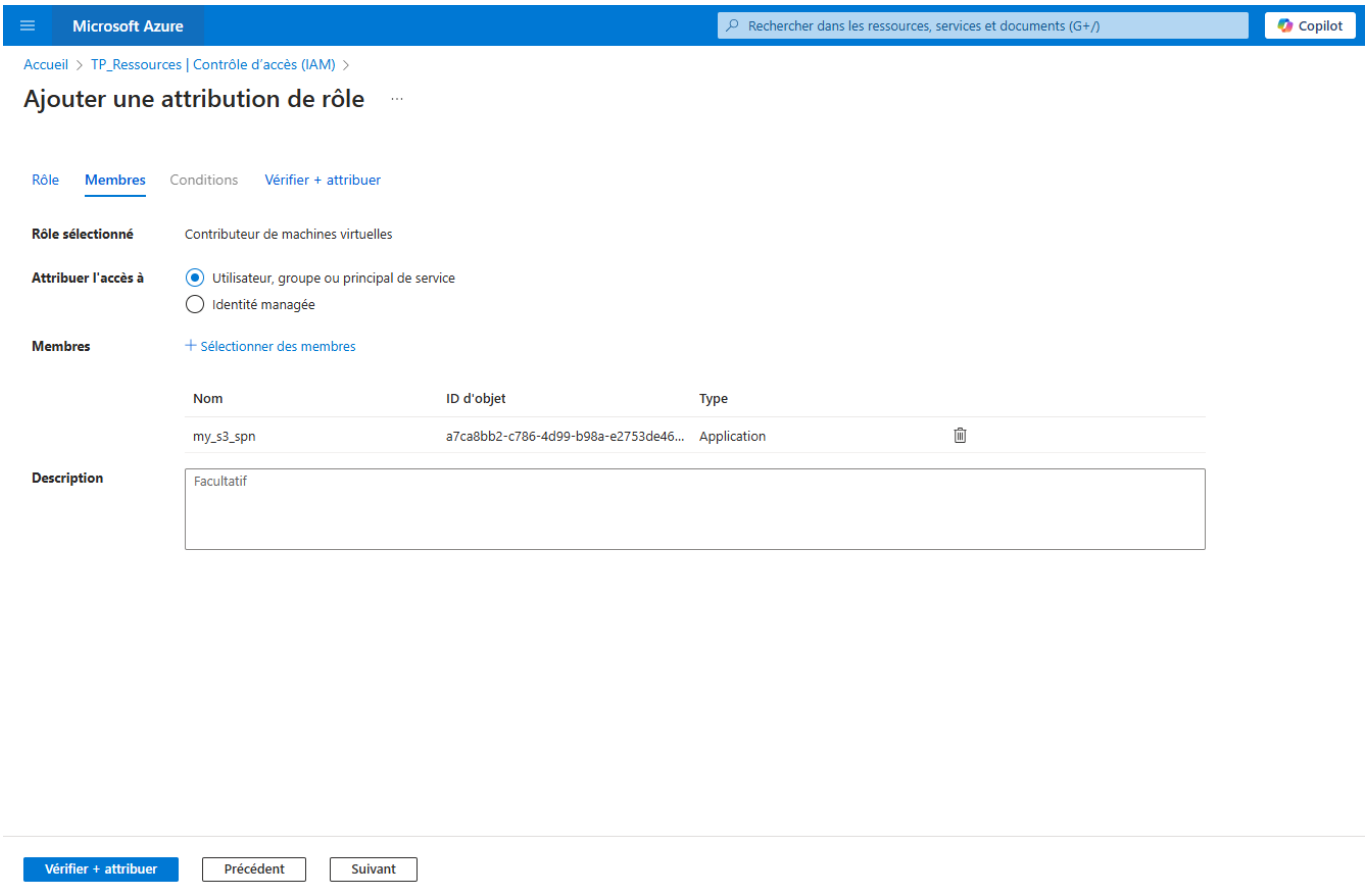
1. **Création d'un Service Principal (SPN)** :
    - Allez dans **Azure Active Directory** et créez un Service Principal (SPN) pour représenter une application ou un service.
2. **Attribuer des rôles via le Service Principal** :
    - Allez dans **Contrôle d'accès (IAM)** et attribuez un rôle spécifique au SPN. Par exemple, attribuer le rôle "Contributeur de machine virtuelle" à un SPN pour qu'il puisse gérer les ressources.
3. **Test d'attribution des rôles via AAD** :
    - Utilisez le SPN pour exécuter une tâche nécessitant un rôle spécifique (par exemple, déployer une machine virtuelle) et vérifiez les permissions.

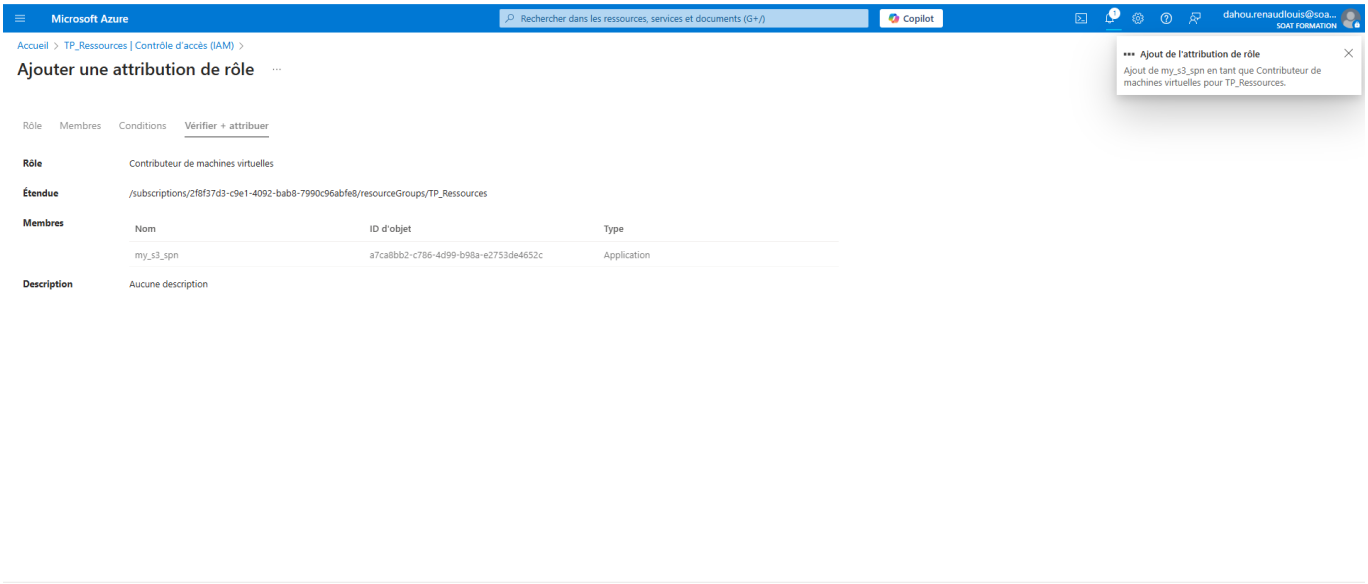


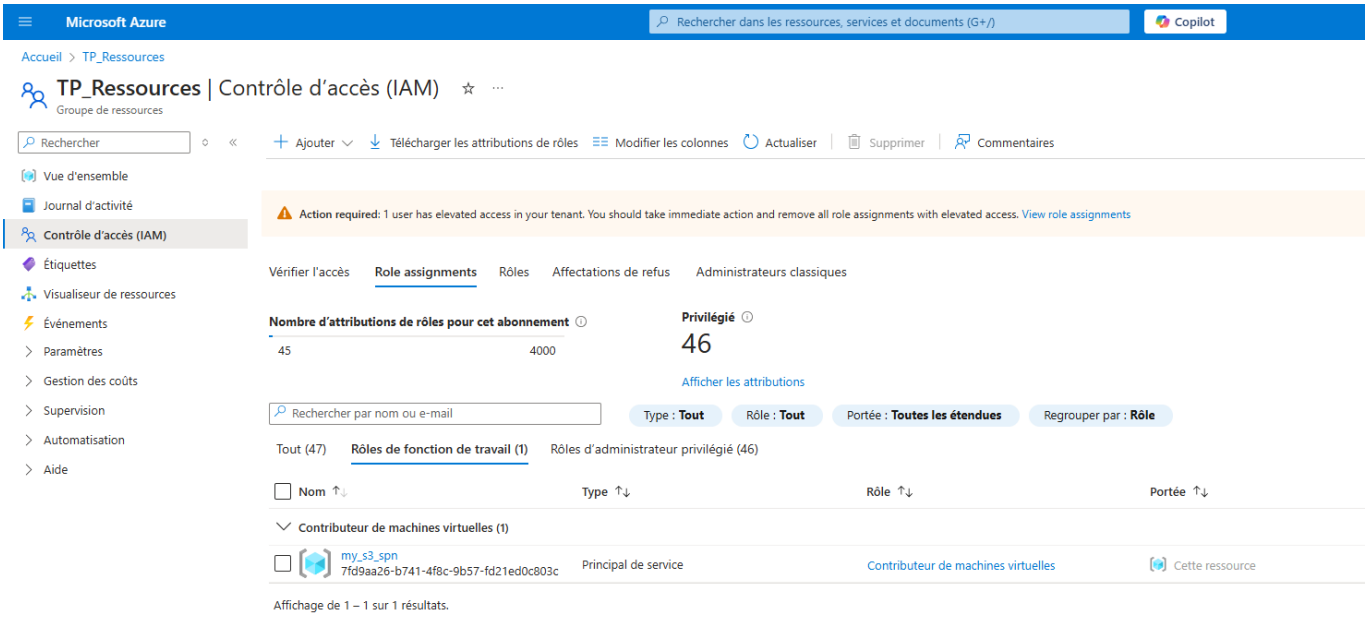

Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
Accueil
SOAT Formation | Vue d'ensemble
Ajouter
Gérer les tenants
Nouveautés
Fonctionnalités en préversion
Avez-vous des commentaires à apporter ?
Vue d'ensemble
Fonctionnalités d'évaluation
Diagnostiquer et résoudre les problèmes
Gérer
Supervision
Dépannage + support
Utilisateur
Groupe
Application d'entreprise
Inscription d'application
Propriétés
Suggestions
Guides de configuration
Informations de base
Nom
SOAT Formation
ID de tenant
ec908c0d-0e11-421c-ba92-c90cc696e789
Domaine principal
soatformation.onmicrosoft.com
Licence
Microsoft Entra ID gratuit
Utilisateurs
57
Groupes
6
Applications
125
Appareils
1
Alertes
MSOnline PowerShell Retirement
Please migrate from any use of MSOnline PowerShell. This module is deprecated and will retire in April 2025. Temporary outages for MSOnline PowerShell will occur between January and March 2025.
Découvrir plus d'informations
Administrateurs généraux
8
Microsoft recommande moins de 5 administrateurs généraux.
Afficher les attributions de rôle privilégié
Effectuer une migration vers la stratégie des méthodes d'authentification convergée
Veuillez effectuer une migration de vos méthodes d'authentification en dehors des stratégies MFA et SSPR héritées avant septembre 2025 pour éviter tout impact sur le service
Découvrir plus d'informations


Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
Accueil
SOAT Formation | Vue d'ensemble
Inscrire une application
* Nom
Nom d'affichage côté utilisateur pour cette application (il peut être modifié ultérieurement).
my_s3_spn
Types de comptes pris en charge
Qui peut utiliser cette application ou accéder à cette API ?
Comptes dans cet annuaire d'organisation uniquement (SOAT Formation uniquement - Locataire unique)
Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – Multilocataire)
Comptes dans un annuaire d'organisation (tout locataire Microsoft Entra ID – Multilocataire) et comptes Microsoft personnels (par exemple, Skype, Xbox)
Comptes Microsoft personnels uniquement
Aidez-moi à choisir...
URI de redirection (facultatif)
Nous retournerons la réponse d'authentification à cet URI une fois l'utilisateur authentifié. Fournir ceci maintenant est facultatif et cela peut être modifié ultérieurement, mais une valeur est requise pour la plupart des scénarios d'authentification.
Client public/natif (mobile &...
exemple : myapp://auth
Inscrivez ici une application sur laquelle vous travaillez. Intégrez des applications de la galerie et d'autres applications externes à votre organisation en les ajoutant à partir de Applications d'entreprise.
En continuant, vous acceptez les stratégies de la plateforme Microsoft
S'inscrire


Microsoft Azure
Rechercher dans les ressources, services et documents (G+/)
Copilot
dahou.renaudlouis@soa...
SOAT FORMATION
Accueil > TP_Ressources | Contrôle d'accès (IAM) >
Ajouter une attribution de rôle
Rôle
Membres
Conditions
Vérifier + attribuer
Rôle sélectionné
Contributeur de machines virtuelles
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
Vérifier + attribuer
Précédent
Suivant
Sélectionner des membres
my
My Profile
Application
my_s3_spn
Application
Membres sélectionnés :
my_s3_spn
Application
Sélectionner
Fermer


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 machines virtuelles
Attribuer l'accès à
Utilisateur, groupe ou principal de service
Identité managée
Membres
+ Sélectionner des membres
Nom
ID d'objet
Type
my_s3_spn
a7ca8bb2-c786-4d99-b98a-e2753de46...
Application
Description
Facultatif
Vérifier + attribuer
Précédent
Suivant





AZ CLI

Commande pour créer un Service Principal (SPN) et lui attribuer un rôle:

```
az ad sp create-for-rbac --name <AppName> --role "Contributeur de machine virtuelle" --scopes /subscriptions/{subscription-id}/resourceGroups/{resource-group-name}
```

```
az ad sp create-for-rbac --name my_s3_spn --role "Virtual machine contributor" --scopes /subscriptions/2f8f37d3-c9e1-4092-bab8-7990c96abfe8/resourceGroups/TP_Ressources
```

```
{
  "appId": "0d54935c-f91c-4ce1-bd62-5af0ea3c881e",
  "displayName": "my_s3_spn",
  "password": "_Xb8Q~clT6~0jRiNiA7VTsxhbkS2RXZs3TtiDchV",
```

```
  "tenant": "ec908c0d-0e11-421c-ba92-c90cc696e789"
}
```

Cela permet à des applications ou services de s'authentifier et d'opérer avec des privilèges définis par les rôles dans Azure Active Directory.

```
az login --service-principal -u <appId> -p <password> --tenant <tenant>
```

```
pip install azure-identity azure-mgmt-resource

from azure.identity import ClientSecretCredential
from azure.mgmt.resource import SubscriptionClient

# Remplissez les informations depuis votre JSON
tenant_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
client_id = "xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx"
client_secret = "xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx"

# Authentification via Service Principal
credential = ClientSecretCredential(
    tenant_id=tenant_id,
    client_id=client_id,
    client_secret=client_secret
)

# Créer un client pour interagir avec les ressources Azure (exemple :
SubscriptionClient)
subscription_client = SubscriptionClient(credential)

# Exemple : Liste des abonnements Azure
subscriptions = subscription_client.subscriptions.list()

for subscription in subscriptions:
    print(subscription.subscription_id)
```