Définition et Utilisation de la Notion de Compte "Hybride" sur Azure Entra

InnovateCorp, une entreprise de conseil en technologie, se développait rapidement et cherchait à moderniser ses systèmes de gestion des identités pour supporter sa croissance. Avec de nombreux consultants travaillant à distance et des partenariats stratégiques avec d'autres entreprises, InnovateCorp avait besoin de sécuriser et de simplifier la gestion des accès externes et hybrides.

Auteurs

Roblot Jean-Philippe - jroblot.simplon@proton.me

Version

15/05/2024 - V1R0

Stack technique

Powered by https://shields.io

Contexte

Sophie, la directrice informatique d'InnovateCorp, observait des défis croissants dans la gestion des identités et des accès.

Les consultants et partenaires de l'entreprise devaient souvent accéder à des ressources internes et cloud de manière sécurisée, mais le processus de provisionnement et de gestion des comptes externes était complexe et inefficace.

Pour résoudre ces problèmes, Sophie proposa l'adoption d'Azure Entra, une solution permettant de gérer les identités hybrides et externes de manière centralisée.

La direction approuva le projet, et une équipe dédiée fut constituée pour mener cette transformation.

Dans une optique de securisation maximal, Sophie souhaite de changer la gestion des droits des administrateurs en utilisant RBAC.

Mettre en place sur l'infrastructure des administrateurs avec :

- Accés total au domaine en lecture seul
- Accés total au domaine en Lecture/Ecriture La mise en place de RBAC pourra se faire directement au niveau de votre ADDS.

Il vous faudra mettre en place des dossiers partager par services :

- Administratif
- Support

- IT
- Direction Au sein de votre AD vous aurez par service un utilisateur et un manager.

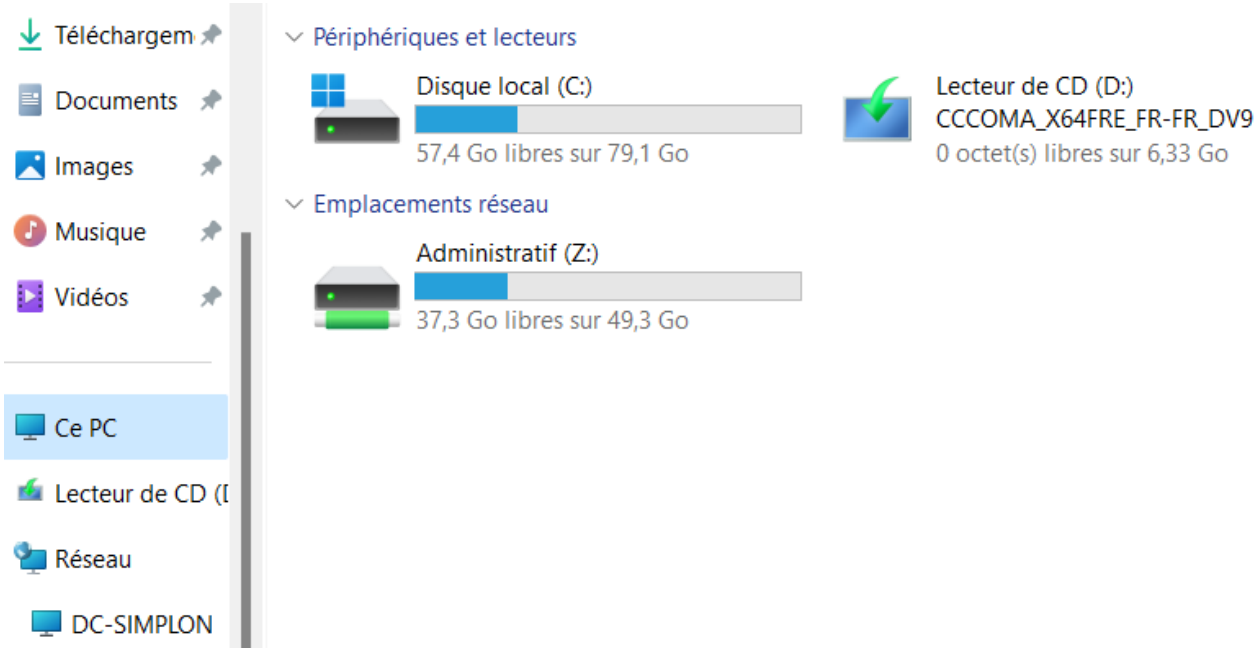
Chaque utilisateur aura le droit d'accés aux ressources de son service.

Chaque manager pourra aussi avoir accés aux ressources Administratif.

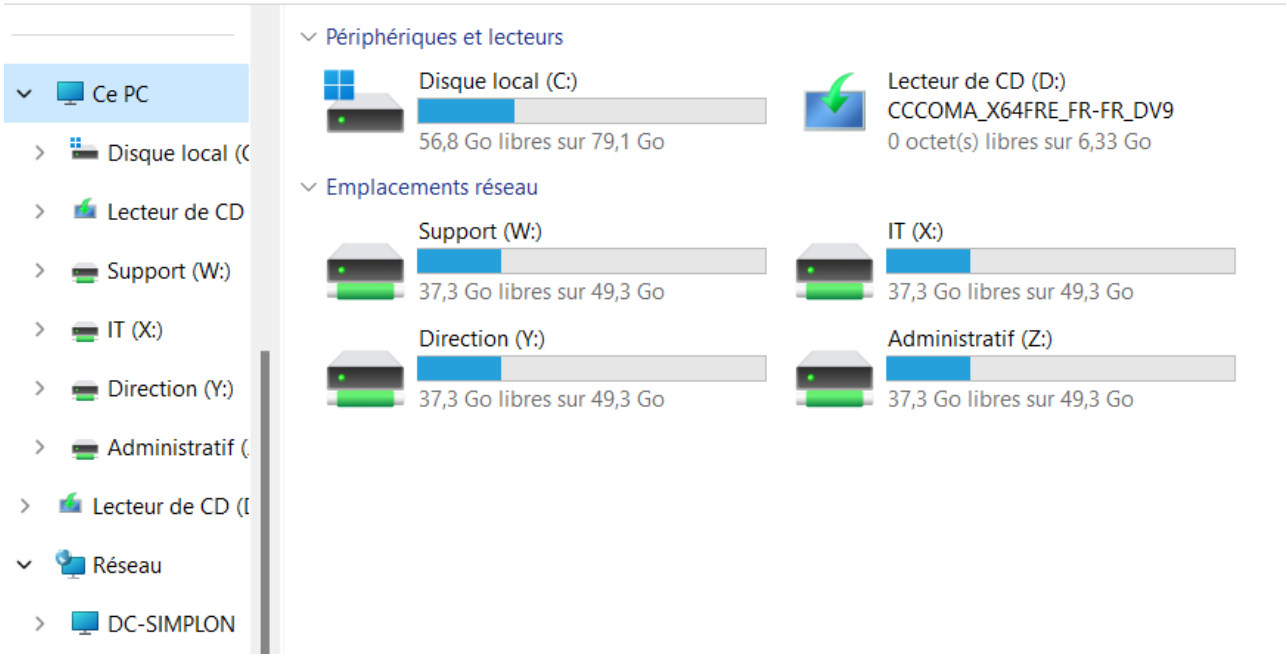
Les personnes de la direction pourrons quand a eux avoir accés aux partages spécifique de chacun des services.

Vous pourrez vérifer le bon fonctionnement en mettant en place les GPO de disque partagé et en testant la connexion pour chacun des utilisateurs (vérification par captures d'écran des disques monté par les utilisateurs.).

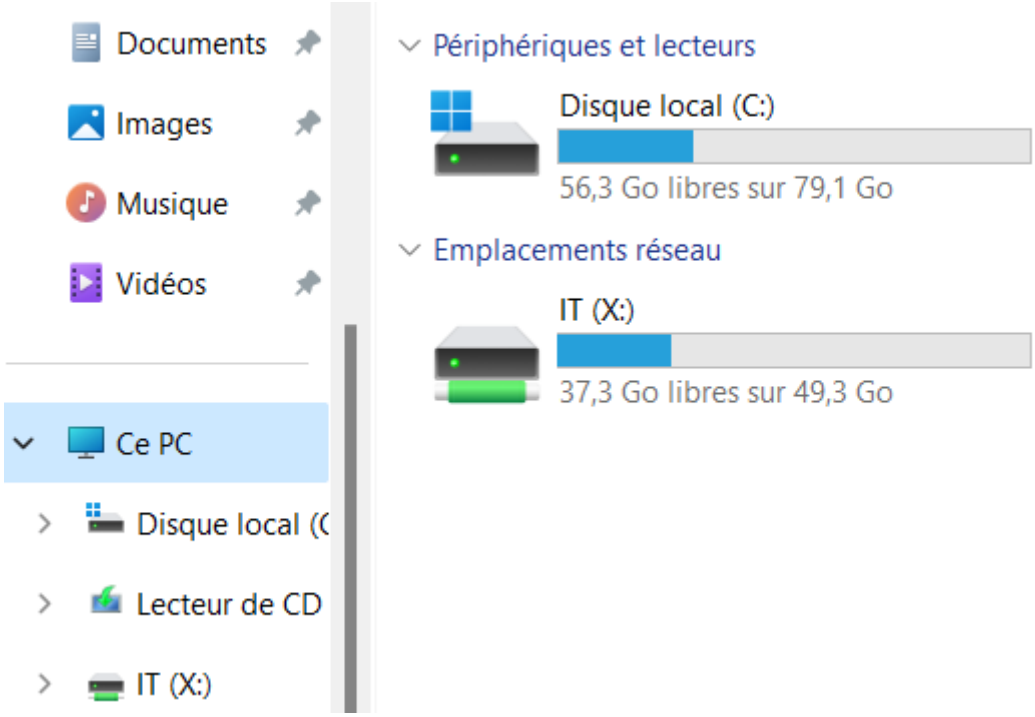
- Pierre Vazquez, Manager administratif :



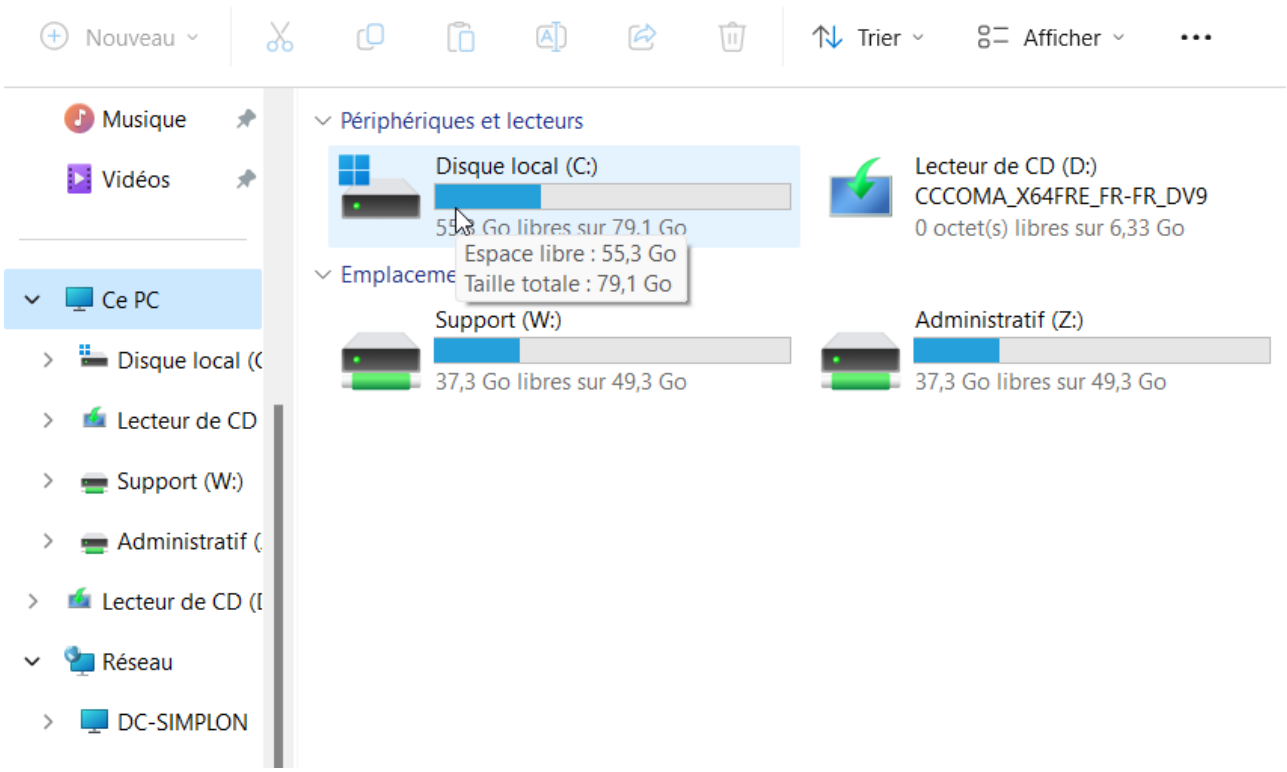
- Kevin Drula, Direction :



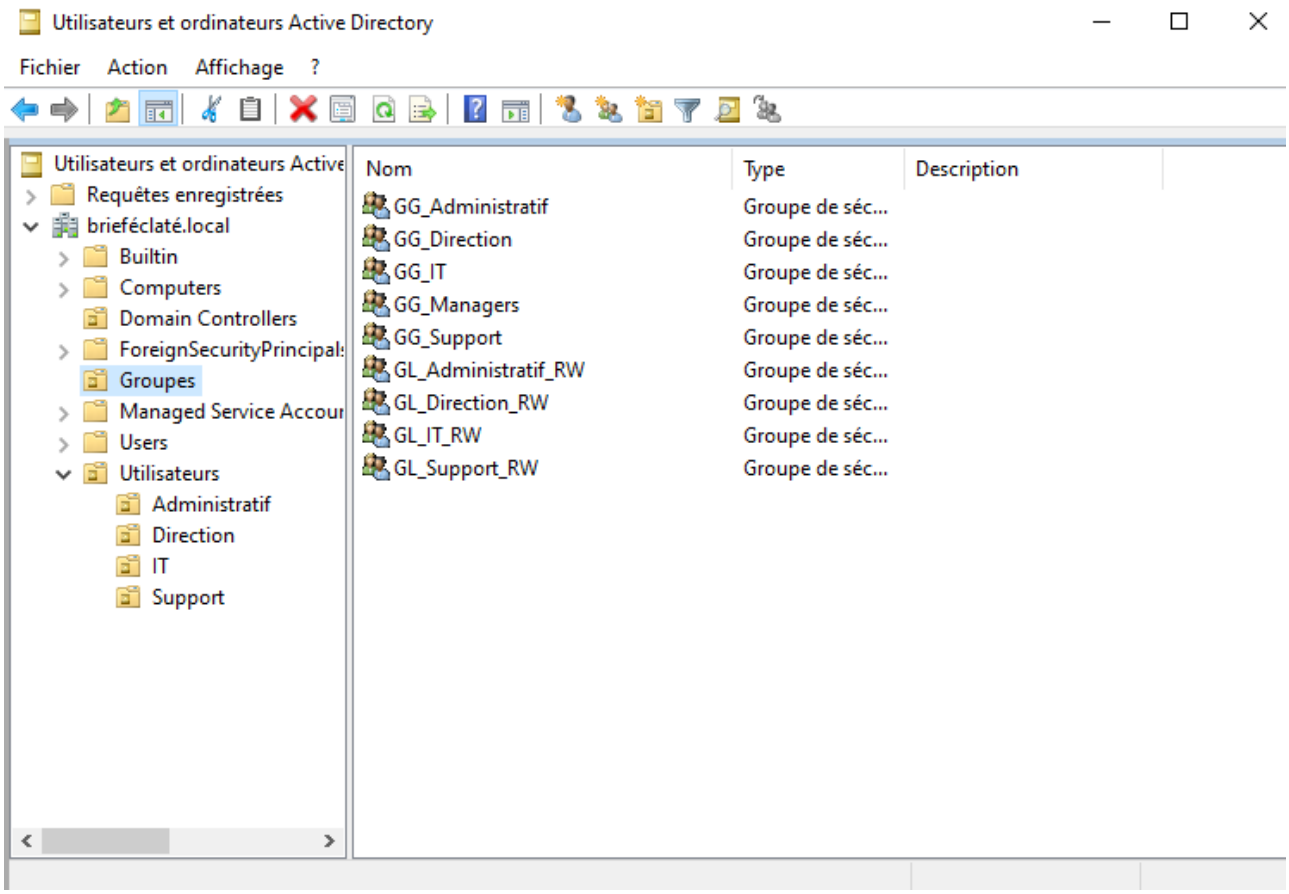
- Erwan Lejolly, utilisateur IT

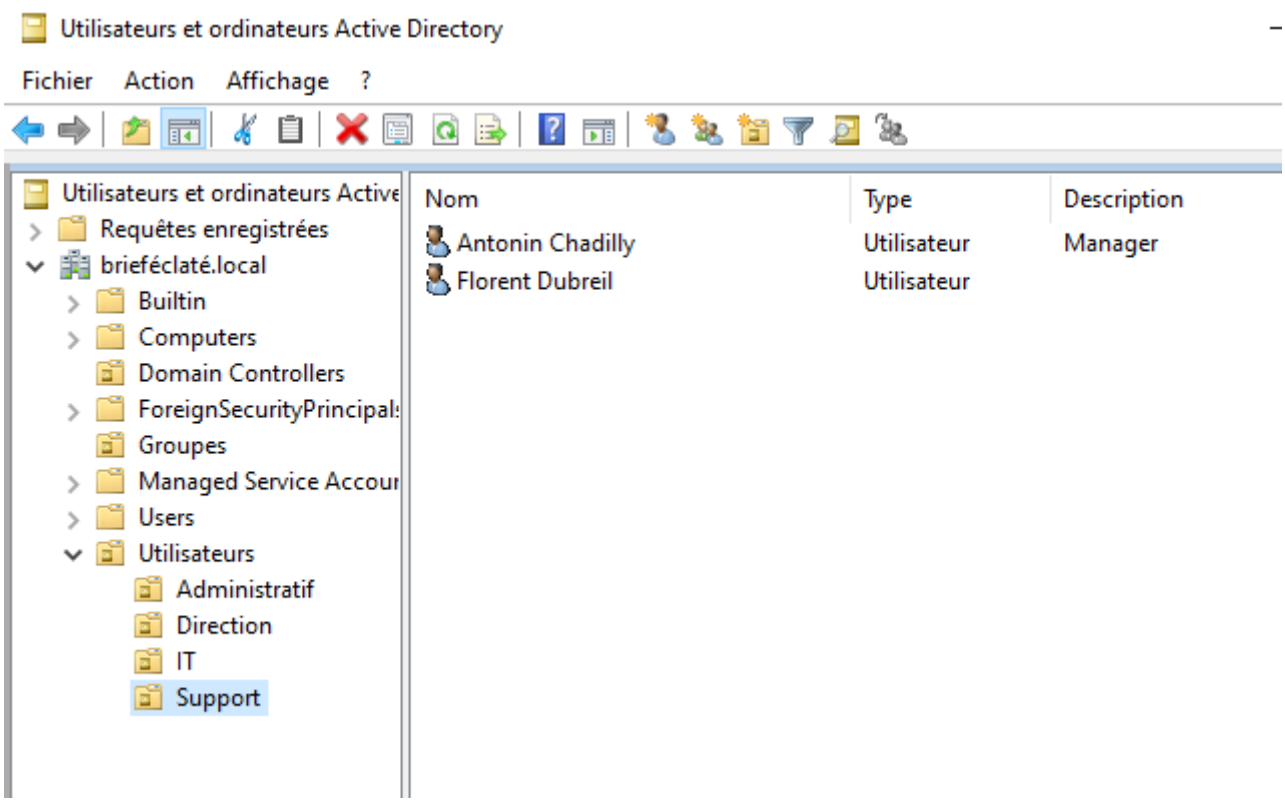


- Antonin Chadilly, Manager Support



- Arborescence AD





Questions

1- Qu'est-ce qu'un compte hybride dans le contexte d'Azure Entra et comment est-il généralement utilisé dans une organisation ?

Un compte hybride Azure Entra se réfère à l'identité d'utilisateur unique qui permet l'authentification et l'autorisation d'accès à toutes les ressources, qu'elles soient situées sur site ou dans le cloud. Cette identité hybride est obtenue par le biais de l'approvisionnement et de la synchronisation entre l'Acitve Directory on premise et Entra ID.

2- Quels sont les principaux avantages de la synchronisation des identités entre un annuaire local et Azure AD ?

la synchronisation des identités facilite la gestion, renforce la sécurité et offre une expérience utilisateur fluide entre les environnements locaux et Azure AD. Elle offre en autre les options suivantes :

- Authentification unique (SSO)
- Gestion centralisée des comptes
- Intégration avec Office 365

3- Quelles sont les différentes options d'authentification disponibles pour les comptes hybrides avec Azure AD Connect ?

Différents options sont accessible selon que l'on s'authentifie dans le cloud ou en local. Voici les méthodes principales proposées :

1. Authentification dans le cloud
    - Synchronisation du hachage de mot de passe Microsoft Entra, permet aux utilisateurs d'utiliser le même nom d'utilisateur et mot de passe que dans Active Directory
    - Authentification basée sur les certificats
2. Authentification locale
    - Authentification par hachage de mot de passe, le hachage est alors synchronisé avec Entra ID.
    - Authentification unique (SSO), l'utilisateur se connecte via l'annuaire local, sans stockage du hash dans le cloud
    - Authentification par fédération, via fournisseur d'identités tiers comme AD FS.

4- Qu'est-ce qu'une identité externe sur Azure Entra et pourquoi est-elle importante pour les organisations ?

L'identité externe est utiliser pour utilisateurs qui ne font pas pertie de l'organisation, mais on cependant besoin d'accéder à des application et/ou ressources.Qu'est-ce qu'une identité externe sur Azure Entra et pourquoi est-elle importante pour les organisations ?le permet de collaborer avec des partenaires et des client de façon sécurisée via invitation ou inscription en libre-service.
Elle permet aussi de gérer l'authentification et la gestion des identités dans un tenant distinct pour des applications grand public.

5- Quels outils et technologies sont utilisés pour inviter et gérer des utilisateurs externes dans Azure AD ?

Avec Entra External ID, plusieurs fonctionnalités parmettent d'inviter et gérer des utilisateurs externes :

- B2B Collaboration : permet aux employés d'une organisation de collaborer avec des utilisateurs externes qui s'authentifient auprès de leur organisation ou fournisseur d'identité.
- Connexion directe B2B : vous créez des relations d'approbations bidirectionnelles avec d'autres organisations Microsoft Entra en utilisant des canaux partagés Microsoft Teams

- Microsoft Entra External ID pour les clients : solution est destinée aux entreprises qui souhaitent mettre des applications à la disposition de leurs clients en utilisant la plateforme Microsoft Entra pour les identités et les accès.
- Organisation multilocataire Microsoft Entra : Les organisations multilocataires (qui possède plusieurs instances Entra ID) utilisent un service de synchronisation unidirectionnelle dans Microsoft Entra ID, appelé synchronisation interlocataires.

6- Comment Azure AD Connect facilite-t-il la synchronisation des identités entre ADDS et Azure AD ?

Pour effectuer le provisionnement et la synchronisation inter-annuaires, Entra ID utilise Microsoft Entra Cloud Sync, basé sur la spécification SCIM (System for Cross-domain Identity Management), un standard utilisé pour automatiser l'échange d'informations d'identité d'utilisateur ou de groupe entre des domaines d'identité, qui est en passe de devenir le standard pour le provisionnement.
Pour ce faire, elle utilise l'agent de provisionnement cloud Microsoft Entra. L'agent fournit une expérience de provisionnement inter-annuaires légère qui sert de passerelle entre Microsoft Entra ID et Active Directory.

7- Quels sont les principaux défis de sécurité associés à la gestion des identités dans une infrastructure distribuée ?

- Identité universelle et authentification : Assurer l'authentification sécurisée des applications et des données dans un environnement hétérogène (bord, plusieurs clouds et points de présence réseau) est complexe. Il faut gérer les identités de manière cohérente sans compromettre la sécurité.
- Gestion des secrets : Stocker et distribuer des secrets (comme les clés d'API, les certificats) sans compromettre un coffre-fort central est un défi. Les solutions traditionnelles ne sont pas toujours adaptées à cette distribution sécurisée.
- Gestion des clés distribuées : Sécuriser les données au repos nécessite une gestion efficace des clés. Cela devient plus difficile dans un environnement distribué

8- Quelles politiques de sécurité peuvent être appliquées aux utilisateurs externes pour garantir la sécurité des ressources ?

Plusieurs politiques de sécurité sont applicables au sein d'Entra ID :

- Contrôle d'accès basé sur les rôles (RBAC) : Utilisez RBAC pour attribuer des rôles spécifiques aux utilisateurs externes.
- Conditions d'accès conditionnel : Créez des stratégies d'accès conditionnel pour imposer des règles spécifiques en fonction du contexte.
- Protection des identités : Utilisez les fonctionnalités de protection des identités, telles que la détection des risques et l'authentification multifacteur.

9- Quels sont les pré-requis pour installer et configurer Azure AD Connect dans une infrastructure existante ?

Les pré-requis pour intégrer Entra ID dans une infrastructure existante sont les suivants :

- Locataire Microsoft Entra : Vous devez disposer d'un locataire Microsoft Entra. Vous pouvez en obtenir un via un essai gratuit Azure. Assurez-vous d'avoir vérifié et ajouté le domaine que vous prévoyez d'utiliser dans Microsoft Entra ID.
- Préparation des données locales : Utilisez l'outil IdFix pour identifier les erreurs dans votre répertoire local avant la synchronisation avec Microsoft Entra ID et Microsoft 365.
- Active Directory local :

    - La version de schéma Active Directory et le niveau fonctionnel de forêt doivent être Windows Server 2003 ou ultérieur.
    - Le contrôleur de domaine utilisé par Microsoft Entra ID doit être accessible en écriture (l'utilisation d'un contrôleur de domaine en lecture seule n'est pas prise en charge).
    - Évitez d'utiliser des noms NetBIOS avec un point (par exemple, contoso.com) pour vos forêts ou domaines locaux

10- Comment les outils de gestion de la configuration et de l'orchestration aident-ils à administrer une infrastructure distribuée ?

Différents outils permettent d'automatiser, surveiller et maintenir l'infrastructure distribuée :

- Gestion de la configuration
    - Ansible, Chef, Puppet, SaltStack : Ces outils permettent de définir, surveiller et maintenir la configuration de manière automatisée et cohérente
- Orchestration des conteneurs
    - L'orchestration des conteneurs automatise et gère le cycle de vie des conteneurs et des services. Des outils tels que Kubernetes, Docker Swarm et Amazon ECS facilitent la gestion de plusieurs conteneurs et architectures de microservices à grande échelle

11- Qu'est ce que le RBAC ?

Le Role Based Access Control (RBAC), est une méthode de gestion des autorisations qui attribue des permissions aux utilisateurs en fonction de leur rôle au sein de votre organisation. Plutôt que d'attribuer des autorisations individuelles à chaque utilisateur, le RBAC assigne des rôles spécifiques et accorde des permissions différentes à chaque rôle.

12- Quels sont les différences de gestion des utilisateurs avec RBAC ?

- Attribution des rôles :
    - Administrateur : Accès complet à toutes les ressources et capacités de gestion.
    - Contributeur : Peut créer et gérer des ressources, mais sans accès administratif.
    - Lecteur : Peut afficher les ressources, mais sans possibilité de modification.
- Granularité des autorisations :
    - RBAC permet des autorisations granulaires, adaptées aux responsabilités spécifiques de chaque utilisateur.
- Simplicité de gestion :
    - Plutôt que d'attribuer des autorisations individuelles, vous affectez simplement des rôles, simplifiant la gestion des accès.