Abdessamed
ZIANI SiO2

VEILLE AZURE AD

SOMMAIRE :

DÉFINITION DE L’ACTIVE DIRECTORY

Qu’est-ce que le Cloud Computing ?

Le Cloud Computing est un environnement où l'on externalise des processus tels que le stockage/traitement de données, d’informations, services ou applications, au sein de serveurs distants (Data Center) privés et payants, appartenant à des hébergeurs tels que OVH, Netflix ou encore Microsoft.
La délocalisation de ses données ou ressources évolutives se fait de plus en plus aujourd’hui, que ce soit par les entreprises ou les particuliers.

Qu’est-ce que l’Active Directory ?

L’ Active Directory (AD) est une base de données et un ensemble de services qui permettent de mettre en lien les utilisateurs avec les ressources présentes sur le réseau afin de mener à bien leurs missions.

Les caractéristiques de l’AD :

- Gestion centralisée des utilisateurs et des droits d’accès, mais aussi des configurations des ordinateurs et des utilisateurs (GPO)

- Stratégie A.A.A (la plus utiliser) :
  Authentification (ID+MDP), Autorisation (Ressources), Audit (Logs)

- Mutualisation des ressources, les données sont stockées dans un espace de stockage central ou elles peuvent être partagées avec d’autres utilisateurs pour faciliter la collaboration .

- Surveillance, l’Active Directory nous permet de vérifier l’état de nos machines, si elles sont conformes ou pas, leurs activités, si elles sont infectées etc…

Qu’est-ce que l’Azure AD ?

Habituellement en entreprise le service Active Directory est mise en place sur un Windows Server lui-même installé et configuré par la société elle-même.

Içi l'Azure AD qui est une solution, un produit du Cloud Microsoft Azure nous permettant d'externaliser ce service chez Microsoft, donc en payant la licence pour chaque administrateur de notre AD.

Azure Active Directory est disponible en 4 éditions :

- Gratuite incluse dans un abonnement à un service Microsoft, Azure, Dynamics 365, Intune et Power Platform
- Applications Office 365
- Prenium 1
- Prenium 2

https://azure.microsoft.com/fr-fr/pricing/details/active-directory/

Méthode d'achat	Azure Premium P1	Azure Premium P2
Commercial Microsoft	Inclus avec Microsoft 365	Inclus avec Microsoft 365
En ligne	5,535 € utilisateur/mois*	8,303 € utilisateur/mois*

Les versions prenium 1 et 2 sont les plus utilisées en entreprise aujourd'hui

Le service étant constamment mis à jour et amélioré par Microsoft, nous sommes à l'abri des attaques type que peuvent subir les anciennes versions de Windows Server.

Pourquoi virtualiser le service AD ?

Les avantages d'utilisation d'une machine virtuelle (Cloud) sont nombreux :

- Le matériel n'a pas besoin d'être maintenue
- Indépendant de tout matériel physique
- Accès depuis n'importe ou dans le monde
- Plus facile d'utilisation (Pour avoir utiliser les 2)
- Certes cela coûte un certain prix, par exemple en entreprise on avait 6 licences P1, donc 6X5X12 = 360€ par an pour le service AD, mais cela compense les coûts d'électricité, de matériel et de maintenance si le service était hébergé chez nous.

LA VEILLE

Ma veille à été réalisée sur 11 mois de mai 2022 à mars 2023.

En mai 2022, Microsoft a annoncé la mise à disposition générale de l'authentification unique (SSO) pour les applications natives dans Azure AD. Cette fonctionnalité permet aux utilisateurs d'authentifier une seule fois pour accéder à plusieurs applications natives dans Azure AD.

Comment fonctionne Active Directory SSO ?

Cette section détaille l'explication du fonctionnement de la solution WatchGuard SSO. Pour consulter une brève synthèse de la procédure de configuration de SSO pour un domaine Active Directory unique, consultez :

- Démarrage Rapide — Configurer Single Sign-On (SSO) avec Active Directory
- Tutoriel vidéo Commencer avec SSO (9 minutes)

La solution WatchGuard SSO

La solution WatchGuard SSO pour Active Directory comprend ces composants :

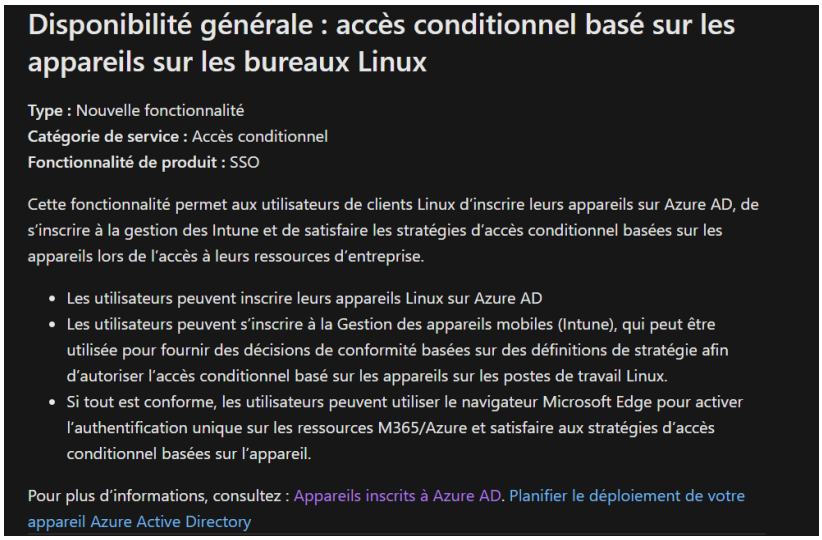
- *SSO Agent* — Requis
- *SSO Client* — Facultatif
- *Event Log Monitor* — Facultatif
- *Exchange Monitor* — Facultatif

SSO Agent collecte les informations de connexion des utilisateurs auprès de SSO Client, Event Log Monitor ou Exchange Monitor.

Vous pouvez configurer plus d'une méthode SSO. Par exemple, vous pouvez configurer le SSO Client comme votre méthode SSO principale et configurer Event Log Monitor ou Exchange Monitor comme méthodes SSO de secours.

https://www.watchguard.com/help/docs/help-center/fr-FR/Content/en-US/Fireware/authentication/sso_about_c.html

En août 2022, l'inscription d'appareils Linux à été permise sur Azure Active Directory



Disponibilité générale : accès conditionnel basé sur les appareils sur les bureaux Linux

Type : Nouvelle fonctionnalité
Catégorie de service : Accès conditionnel
Fonctionnalité de produit : SSO

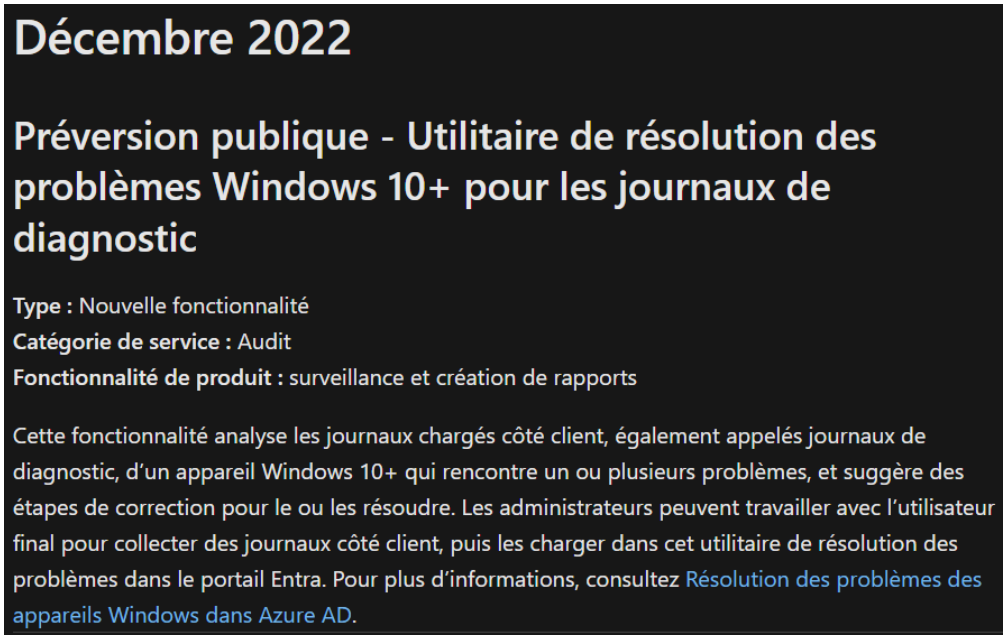
Cette fonctionnalité permet aux utilisateurs de clients Linux d'inscrire leurs appareils sur Azure AD, de s'inscrire à la gestion des Intune et de satisfaire les stratégies d'accès conditionnel basées sur les appareils lors de l'accès à leurs ressources d'entreprise.

- Les utilisateurs peuvent inscrire leurs appareils Linux sur Azure AD
- Les utilisateurs peuvent s'inscrire à la Gestion des appareils mobiles (Intune), qui peut être utilisée pour fournir des décisions de conformité basées sur des définitions de stratégie afin d'autoriser l'accès conditionnel basé sur les appareils sur les postes de travail Linux.
- Si tout est conforme, les utilisateurs peuvent utiliser le navigateur Microsoft Edge pour activer l'authentification unique sur les ressources M365/Azure et satisfaire aux stratégies d'accès conditionnel basées sur l'appareil.

Pour plus d'informations, consultez : Appareils inscrits à Azure AD. Planifier le déploiement de votre appareil Azure Active Directory

https://learn.microsoft.com/fr-fr/azure/active-directory/fundamentals/whats-new#october-2022

En décembre 2022, Microsoft met à disposition des administrateurs de l'AD une nouvelle fonctionnalité, qui suggère des étapes de correction en analysant les logs du client afin de lui résoudre son problème.



https://learn.microsoft.com/fr-fr/azure/active-directory/fundamentals/whats-new#january-2023

En mars 2023, Microsoft permet la synchronisation des mots de passe avec l'authentification “Pass-Through” pour Azure AD.
Cette fonctionnalité permet aux utilisateurs de se connecter aux applications à l'aide de leur mot de passe local sans que celui-ci soit stocké ou synchronisé sur Azure AD.

https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-pta-quick-start