# GESTION DE L'ACCES DES UTILISATEURS A **MICROSOFT 365 ET AUX APPLICATIONS CLOUD** A L'AIDE DE **WINDOWS SERVER ACTIVE DIRECTORY**

Windows Server Active Directory (AD) est la pierre angulaire de la gestion des identités depuis plus de 20 ans. Mais alors que les entreprises sont confrontées à de nouveaux défis pour fournir des services aux travailleurs distants pendant une pandémie de santé mondiale, l'accès aux applications métier et aux données stockées dans le cloud public est passé au rang des priorités.

Dans ce livre blanc, nous examinerons les différentes options permettant d'étendre Windows Server Active Directory sur site à Microsoft Azure et Microsoft 365. Les organisations peuvent sécuriser l'accès aux applications cloud sans changer la façon dont elles gèrent les identités des utilisateurs avec Windows Server Active Directory aujourd'hui.

Nous explorerons également une option alternative, UserLock, qui continue d'utiliser Active Directory local comme répertoire d'utilisateurs. Combiné à l'authentification multifacteur, UserLock fournit un accès en un clic aux ressources hébergées sur le réseau et dans Microsoft 365 et d'autres applications cloud.

# Qu'est-ce-qu'Azure Active Directory?

Azure Active Directory est la plateforme de gestion des identités de Microsoft pour le cloud. Lorsque les utilisateurs se connectent à des applications cloud, comme Microsoft 365, Azure AD authentifie les identités des utilisateurs avant d'accorder l'accès. Azure AD fonctionne également avec des plates-formes cloud SaaS tierces, telles que Salesforce et ServiceNow, et avec des applications cloud développées en interne.

Azure Active Directory n'est pas seulement Windows Server Active Directory «levé et déplacé» vers le cloud. Azure AD a été conçu dès le départ pour servir les applications cloud. Il ne prend pas en charge les protocoles et services Windows Server tels que l'authentification Kerberos / NTLM, la stratégie de groupe, LDAP et la jonction de domaine. Azure Active Directory Domain Services, un service géré facultatif qui déploie des contrôleurs de domaine Windows Server dans Azure, ajoute la prise en charge des services et protocoles hérités pour les organisations qui souhaitent lever et déplacer les applications héritées, comme les services Internet (IIS) et les applications développées en interne, dans le cloud.

Azure AD utilise des protocoles de gestion des identités fédérées conçus pour les applications cloud, comme OAuth 2.0, SAML et OpenID. L'accès conditionnel Azure AD et Azure Identity Protection sécurisent davantage l'accès à vos applications et données cloud. Microsoft ajoute régulièrement de nouvelles fonctionnalités de sécurité à Azure AD, dont certaines peuvent être utilisées avec Windows Server AD dans une configuration hybride.

# Choix d'une méthode d'authentification unique et d'une topologie hybride pour étendre Windows Server Active Directory à Azure

En raison de l'investissement important dans Windows Server AD sur site, les entreprises souhaitent continuer à l'utiliser pour gérer l'authentification aux applications cloud sans gêner les utilisateurs ou interrompre des opérations informatiques. Pour résoudre ce problème, Microsoft Azure AD Connect active les fonctionnalités d'authentification unique (SSO) pour les utilisateurs de Windows Server AD qui travaillent également avec des applications cloud.

## Azure AD Connect

Azure AD Connect est une application gratuite qui synchronise les comptes d'utilisateurs Windows Server AD avec Azure AD. Vous pouvez choisir de synchroniser les hachages de mot de passe Windows Server AD des utilisateurs avec Azure AD ou de laisser Windows Server AD authentifier les utilisateurs tout en conservant leurs mots de passe sur site.

Les deux méthodes offrent aux utilisateurs un moyen sécurisé de se connecter aux services cloud avec une authentification unique.

- ***Synchronisation du hachage de mot de passe***

  Microsoft recommande la synchronisation de hachage de mot de passe pour la plupart des environnements AD hybrides, car elle est simple à déployer, sécurisée et prend en charge la plus large gamme de fonctionnalités Azure AD. Pour améliorer la sécurité, un hachage du hachage du mot de passe de l'utilisateur est synchronisé avec le cloud.

- ***Authentification Pass-through***

  Pour les organisations qui ne souhaitent pas synchroniser les hachages de mots de passe avec le cloud ou qui souhaitent appliquer les stratégies de sécurité et de mot de passe de Windows Server AD, l'authentification pass-through (PTA) est une alternative à la synchronisation de hachage de mot de passe.

  Azure AD envoie des demandes de validation de mot de passe à Windows Server AD. Un ou plusieurs agents PTA sont déployés sur site pour faciliter cela. S'il est utilisé sans synchronisation de hachage de mot de passe, PTA ne fonctionne pas avec les services de domaine Azure AD, Azure AD Connect Health ou la fonctionnalité de fuite d'informations d'identification dans Azure Identity Protection.

## Azure AD Connect vs. Active Directory Federation Services (ADFS)

Les services ADFS (Active Directory Federation Services) sont une solution d'identité fédérée autonome qui fait partie de Windows Server AD. Il peut être utilisé pour fournir des fonctionnalités d'authentification unique Microsoft 365 aux utilisateurs de Windows Server AD, mais il est complexe à déployer et à gérer. ADFS nécessite des certificats, SQL Server, Windows Server et le clustering de basculement pour une haute disponibilité.

Dans la plupart des cas, ADFS ne fournit aucun avantage par rapport à la synchronisation de hachage de mot de passe Azure AD Connect ou PTA. Microsoft ne recommande plus ADFS mais Azure AD Connect peut vous aider à installer et à configurer ADFS si vous choisissez de l'utiliser.

## Topologies AD hybrides

La topologie Azure AD Connect la plus courante synchronise une forêt unique avec un seul locataire Azure AD. Il est facile de déployer avec la synchronisation de hachage de mot de passe à l'aide de l'option d'installation express dans Azure AD Connect.

Si vous disposez de plusieurs forêts AD locales, vous pouvez toutes les synchroniser à l'aide d'un seul serveur de synchronisation Azure AD Connect. Azure AD Connect essaiera de consolider les utilisateurs locaux afin qu'ils ne soient représentés qu'une seule fois dans Azure AD. Si vous avez plusieurs forêts AD déconnectées, les agents *d'approvisionnement* cloud Azure AD Connect peuvent agir comme un pont.

# Gestion de la synchronisation entre Windows Server AD et Azure AD

Une fois qu'Azure AD Connect est configuré à l'aide de la méthode d'authentification et de la topologie que vous avez choisies, il s'exécute en arrière-plan pour synchroniser les utilisateurs AD locaux avec Azure AD. Par défaut, seuls certains attributs sont synchronisés. Vous pouvez choisir les attributs de compte d'utilisateur AD qu'Azure AD Connect synchronise avec Azure AD. Par exemple, vous souhaiterez peut-être empêcher les attributs qui contiennent des informations sensibles, comme des informations personnellement identifiables, de se synchroniser avec Azure AD.

## Intégration des fonctionnalités d'Azure Active Directory à Windows Server Active Directory

Le processus de synchronisation est unidirectionnel, mais il est possible d'activer la « réécriture » sur certains attributs, de sorte qu'une fois mis à jour dans le cloud, ils sont synchronisés à nouveau sur AD sur site. L'exemple le plus courant est la réécriture de mot de passe.

La fonctionnalité de réinitialisation de mot de passe en libre-service dans Azure AD nécessite que les mots de passe des utilisateurs soient réécrits dans Windows Server AD pour les déploiements hybrides. La réécriture de groupe vous permet de provisionner des groupes Microsoft 365 dans votre Active Directory local si vous disposez également d'Exchange Server local.

## Azure AD Connect Health et haute disponibilité

Azure AD Connect Health utilise un agent sur site pour envoyer des informations au cloud. Le service informatique peut ensuite surveiller l'infrastructure d'identité locale à l'aide d'un portail en ligne pour maintenir une connexion fiable à Azure. Mais si vous choisissez l'authentification pass-through, Azure AD Connect Health n'est pas en mesure de surveiller les agents PTA, ce qui peut entraîner des problèmes de fiabilité.

Microsoft ne prend pas en charge le déploiement de plusieurs serveurs de synchronisation Azure AD Connect pour un seul locataire Azure AD. Si vous avez besoin d'une haute disponibilité pour la synchronisation, vous pouvez déployer Azure AD Connect en mode intermédiaire et basculer vers le serveur en mode intermédiaire en cas de défaillance du serveur de synchronisation principal. Le basculement est géré à l'aide de l'assistant Azure AD Connect.

# Gestion des utilisateurs au quotidien

Les utilisateurs peuvent être gérés avec les outils dont vous disposez actuellement pour Active Directory, tels que la console Utilisateurs et ordinateurs Active Directory (ADUC), le centre d'administration Active Directory (ADAC) et PowerShell. Lorsque vous créez un nouvel utilisateur AD local, Azure AD Connect crée automatiquement un objet utilisateur dans Azure AD pour représenter le compte Windows Server AD.

L'utilisateur peut ensuite accéder à votre domaine local et aux applications cloud sans aucune autre intervention du service informatique. Azure AD Connect synchronise également automatiquement les modifications que vous apportez aux comptes d'utilisateurs Windows Server AD existants, à condition que les attributs modifiés soient activés dans les options de synchronisation.

Dans les environnements Exchange Server hybrides, le centre d'administration Exchange (EAC) prend en charge la création de nouveaux comptes cloud hybrides et le provisionnement automatique de boîtes aux lettres pour les nouveaux utilisateurs dans le cloud. Il n'est donc pas nécessaire de créer manuellement des boîtes aux lettres dans Exchange Online.

# L'intégration de Windows Server AD à Azure simplifiée

Microsoft vous a facilité l'intégration de vos forêts AD locales avec Azure AD. Azure AD Connect est simple à configurer si vous optez pour la méthode d'authentification recommandée par Microsoft, qui est la synchronisation de hachage de mot de passe. L'option d'installation express fait tout le travail si vous n'avez pas besoin de personnaliser les paramètres. PTA est plus complexe à configurer et vous devez déployer au moins trois agents PTA pour une haute disponibilité. Et tandis qu'Azure AD Connect peut aider à simplifier le déploiement d'ADFS, vous devez envisager d'utiliser PTA si possible.

Mais la meilleure partie est qu'Azure AD Connect étend les capacités de Windows Server AD pour fournir une authentification unique transparente aux applications cloud pour les utilisateurs de domaine. Et le service informatique peut continuer à gérer les identités des utilisateurs avec des outils familiers tout en apportant une valeur supplémentaire à l'organisation.

# Authentification unique à l'aide d'identités Active Directory sur site

Pour les organisations qui souhaitent continuer à utiliser Active Directory sur site comme répertoire d'utilisateurs, UserLock propose une solution. Installé en quelques minutes sur un serveur Windows standard, il prend en charge les protocoles SAML 2.0 et OIDC pour permettre l'authentification fédérée de Microsoft 365 et d'autres applications cloud de premier plan. Combiné à l'authentification multifacteur, UserLock peut faciliter l'offre d'un accès sans friction et sécurisé aux applications cloud et aux ressources réseau de l'entreprise.

Téléchargez la version d'essai gratuite entièrement fonctionnelle et constatez par vous-même à quel point UserLock peut vous aider à sécuriser l'accès au réseau.

ESSAI GRATUIT