Éviter les écarts de données causés par l'utilisation d'Azure AD Connect dans le cadre de votre stratégie Cloud de reprise d'activité

Vos objets et attributs Cloud ne sont pas pris en compte par votre plan local de sauvegarde et de restauration.

INTRODUCTION

Si votre entreprise a mis en place un environnement Active Directory (AD) hybride, ou si elle envisage de le faire, sachez que c'est le cas de la plupart des entreprises. En effet, d'après Microsoft, 75 % de ses entreprises clientes comptant 500 utilisateurs ou plus, disposent d'un environnement AD hybride : leur instance locale d'AD reste leur principale source d'authentification et d'autorisation, et elles la synchronisent avec Azure AD à l'aide d'Azure AD Connect.[1]. Les informations d'identification locales sont utilisées pour authentifier les utilisateurs dans les applications Cloud, et la solution locale de sauvegarde et de restauration protège l'ensemble de l'environnement. Que demander de plus ?

Justement, il existe une ombre au tableau, et pas des moindres : votre solution locale ne sauvegarde pas et ne récupère pas l'intégralité de vos données. Il est pour ainsi dire impossible d'utiliser la suite Office 365 ou les services Azure sans créer des objets Cloud. Puisque dans la plupart des cas, la synchronisation AD Connect ne s'effectue que dans un sens, c'est-à-dire de l'instance locale d'Active Directory vers Azure AD, ces objets Cloud ne sont pas pris en compte par vos outils de sauvegarde et de restauration locaux. De plus, l'option native qui consiste à restaurer les objets Cloud qui se trouvent dans la Corbeille est très limitée. Votre entreprise se retrouve donc avec une stratégie de restauration des données incomplète.

Ce livre blanc explore ce problème et propose une solution. Nous allons aborder le fonctionnement des environnements AD hybrides, expliquer le rôle de chaque type d'objet et d'attribut Cloud, et voir les limites des outils natifs permettant de récupérer ces derniers. Ensuite, nous verrons comment obtenir une sauvegarde, une restauration et une reprise d'activité complètes qui répondent aux besoins de votre environnement AD hybride à l'aide des solutions Quest®.

1 Simons, Alex, « Best way to connect to Office 365 and Azure AD (latest data) + Azure AD Connect Momentum », blog Microsoft Enterprise Mobility + Security (en anglais), janvier 2016, https://cloudblogs.microsoft.com/enterprisemobility/2016/01/05/best-way-to-connect-to-office-365-and-azure-ad-latest-data-azure-ad-connect-momentum/

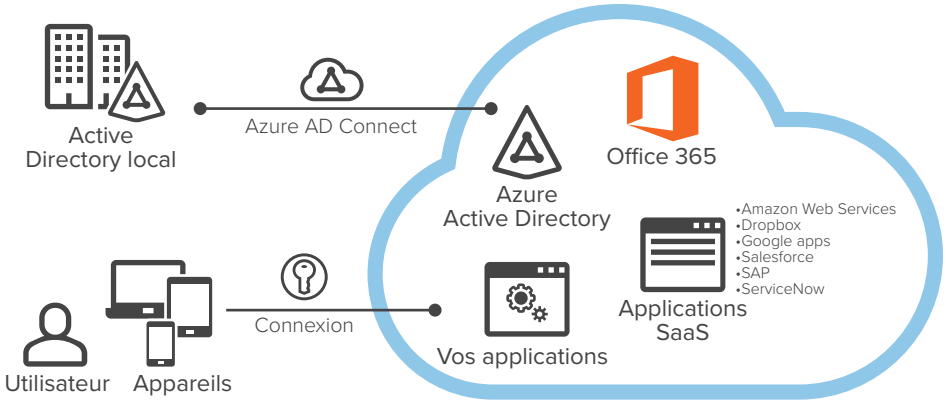

Figure 1. De nombreuses entreprises utilisent Azure AD Connect pour lier leur environnement Active Directory local au Cloud Microsoft Azure.

Lorsque nous demandons à nos clients le nombre d'objets et d'attributs Cloud dont ils disposent, il est fréquent qu'ils ne le sachent pas.

STRUCTURE D'UN ENVIRONNEMENT ACTIVE DIRECTORY HYBRIDE

Dans la plupart des entreprises qui disposent d'un environnement AD hybride, l'instance locale d'AD constitue la principale source d'authentification et d'autorisation, et celle-ci est synchronisée avec Azure AD à l'aide d'Azure AD Connect. Les informations d'identification locales sont utilisées pour authentifier les utilisateurs dans Office 365, dans les applications Cloud personnalisées, ainsi que dans les applications SaaS courantes telles que Dropbox, Google Apps et Amazon Web Services (AWS), comme illustré dans la Figure 1.

CE QUI N'EST PAS PRIS EN COMPTE PAR LA SYNCHRONISATION AZURE AD CONNECT

Cependant, pour la plupart des clients, la synchronisation n'est effectuée que dans un sens, c'est-à-dire de l'instance locale d'AD vers Azure AD. Les objets et les attributs qui sont créés dans le Cloud ne sont généralement pas synchronisés vers l'instance locale d'AD. Ils ne sont donc pas pris en compte par les solutions locales de sauvegarde et de restauration. Pire encore, lorsque les entreprises activent la fonctionnalité de réécriture pour la synchronisation bidirectionnelle, elles prennent le risque d'augmenter le nombre d'objets Azure AD non pris en compte par le plan de sauvegarde et de restauration.

Lorsque nous demandons à nos clients le nombre d'objets et d'attributs Cloud dont ils disposent, il est fréquent qu'ils ne le sachent pas. Nous venons donc de voir les types d'élements Cloud les plus courants, qui sont invisibles pour les solutions locales de sauvegarde et de restauration, ainsi que les défis que constitue leur restauration dans le Cloud à l'aide d'outils natifs.

Attributs Cloud

Même si la plupart des objets Azure AD sont synchronisés à partir d'une instance locale d'AD, ceux-ci possèdent souvent des attributs supplémentaires qui ne sont présents que dans le Cloud. Ces solutions incluent :

- **Type de licence Office 365 :** chaque utilisateur Azure AD possède un type de licence Office 365 qui détermine les fonctionnalités auxquelles il a accès.
- **Attributs d'extension :** Azure AD permet également de créer des attributs pour les utilisateurs, les groupes et certains autres objets. Par exemple, les fournisseurs de services financiers peuvent développer des applications de trading dans Azure, et créer un attribut d'extension qui contrôle l'accès à ces applications.

Si vous supprimez un objet utilisateur ayant un ou plusieurs attributs Cloud, vous pouvez récupérer l'objet utilisateur de l'instance locale d'AD et utiliser Azure AD Connect pour le resynchroniser vers Azure AD. Le problème ici est que les attributs Cloud auront disparu et que l'utilisateur n'aura donc plus accès à l'objet. Cela signifie que si un utilisateur est restauré sans l'attribut de type de licence, il ne pourra plus accéder aux applications Office 365. Vous devrez donc vous dépêcher de restaurer l'attribut avant qu'un autre utilisateur ne revendique la licence.

Par conséquent, au lieu d'utiliser Azure AD Connect, vous devez restaurer l'objet utilisateur à partir de la Corbeille Azure AD. Cela peut sembler relativement simple.

Notez, toutefois, que cette procédure comporte des limites :

- Il est difficile de déterminer ce qui doit être restauré. En effet, il n'existe aucun journal des modifications ni aucun rapport de comparaison natifs qui pourraient vous aider à déterminer les objets Azure AD qui ont été modifiés ou supprimés. Comment donc savoir ce qui doit être restauré ?
- Vous pouvez uniquement récupérer les objets qui ont été supprimés récemment. En effet, la Corbeille Azure AD ne conserve les éléments supprimés que pendant 30 jours. Si l'utilisateur a été supprimé depuis plus longtemps, vous ne pourrez pas le restaurer.
- Certains objets ne peuvent jamais être restaurés. Un objet supprimé de manière définitive ne passe pas par la Corbeille. Il est donc impossible de le restaurer à l'aide des outils natifs, même s'il a été supprimé récemment.
- Vous ne pouvez pas effectuer de restauration en bloc sans PowerShell. Les pirates extérieurs, les scripts errants et les utilisateurs internes malveillants peuvent modifier ou supprimer un très grand nombre de données dans Azure AD. Toutefois, il n'existe aucun outil local qui vous permette de restaurer plusieurs utilisateurs en même temps sans utiliser PowerShell.

De plus, il arrive que l'objet ne soit pas réellement supprimé, mais que ce soit le type de licence Office 365 de l'objet ou son attribut d'extension qui ait été modifié ou supprimé. Si c'est votre cas, les choses vont se compliquer sérieusement. Étant donné que les attributs Cloud ne sont jamais enregistrés sur l'instance locale d'AD, ni Azure AD Connect ni les outils natifs ne pourront vous aider à les restaurer.

Pour finir, vous ne pouvez pas restaurer certains attributs qui ont été modifiés dans un objet utilisateur.

Groupes Office 365

Les utilisateurs créent souvent des groupes Office 365 dans le but de regrouper les utilisateurs avec lesquels ils veulent collaborer. Ils créent également des groupes de ressources à partager avec ces utilisateurs, telles qu'une boîte aux lettres et un calendrier dans Exchange Online, des sites d'équipes dans SharePoint Online ou des blocs-notes dans OneNote.

Si l'un de ces groupes est supprimé par erreur, les utilisateurs concernés voudront que la situation soit rétablie rapidement. Vous ne pouvez pas restaurer ce groupe à l'aide d'Azure AD Connect, puisqu'il n'a jamais existé sur l'instance locale d'AD. La Corbeille Azure AD stocke les groupes supprimés pendant 30 jours. Cependant, la restauration d'un groupe Office 365 est un processus compliqué. Vous pouvez utiliser PowerShell ou le centre d'administration Exchange pour restaurer les groupes, mais vous ne pouvez pas restaurer les attributs et les groupes un par un.

De même, si un utilisateur malveillant supprime l'appartenance puis le groupe, vous ne pouvez restaurer le groupe qu'au moment de la suppression, sans pouvoir récupérer l'appartenance de manière native. Pour cela, vous devez identifier les utilisateurs qui ont été supprimés, mais là encore, il n'existe pas de journal des modifications ou de rapport de comparaison pour vous aider à identifier les objets Azure AD qui ont été modifiés ou supprimés.

Groupes Azure AD et appartenance

Les entreprises créent également des groupes Azure AD pour gérer l'accès aux ressources efficacement, tout en respectant les bonnes pratiques. Malheureusement, si un groupe Azure AD ou son appartenance sont supprimés, vous devrez les recréer intégralement. Les groupes Azure AD et l'appartenance aux groupes ne sont pas déplacés dans la Corbeille après suppression et ne peuvent donc pas être restaurés à l'aide d'outils natifs.

Comptes Azure AD B2B et B2C

Azure AD propose deux types de comptes d'utilisateurs qui peuvent aider à la prise en charge de vos clients et partenaires externes : les comptes B2B et les comptes B2C. Les entreprises possèdent souvent des milliers, voire des millions de comptes de ce type. Toutefois, les comptes B2B et B2C ne sont pas des comptes Microsoft Azure Enterprise. Ils ne peuvent donc pas être inclus dans la synchronisation Azure AD Connect. Ces comptes ont une finalité différente :

- Les entreprises utilisent des comptes B2B pour authentifier les utilisateurs appartenant aux entreprises partenaires. Supposons, par exemple, que la branche États-Unis d'une entreprise multinationale soit passée à un environnement AD hybride, mais que ce ne soit pas le cas de la branche canadienne. Pour permettre aux salariés canadiens d'accéder aux applications Cloud et aux documents de l'entreprise, la branche États-Unis va leur fournir des comptes Azure B2B.
- Les comptes B2C vous permettent d'inviter les utilisateurs de vos applications mobiles et Web dans Azure AD à l'aide d'une identité sociale prise en charge avec fédération directe, telle que leurs comptes Facebook, Microsoft ou Google+. Les comptes B2C sont déjà très populaires dans un grand nombre de secteurs, comme la finance, la santé,

Un objet supprimé de manière définitive ne passe pas par la Corbeille. Il est donc impossible de le restaurer à l'aide des outils natifs, même s'il a été supprimé récemment.

les assurances ou la vente. Par exemple, une entreprise peut permettre à ses clients d'utiliser leurs informations d'identification LinkedIn pour se connecter à leur environnement Azure AD. L'entreprise crée un compte B2C pour ses clients, afin de leur permettre d'accéder à certaines applications ou données.

Si un compte B2B ou B2C est supprimé, l'utilisateur ne pourra plus accéder aux ressources et aux données dont il a besoin. Vous ne pouvez pas restaurer ce compte à l'aide de votre solution locale, puisqu'il n'a jamais existé sur l'instance locale d'AD. Vous devez donc le restaurer à partir de la Corbeille Azure AD, si la situation le permet (comme évoqué plus haut).

Si un compte B2B ou B2C est supprimé, l'utilisateur ne pourra plus accéder aux ressources et aux données dont il a besoin. Vous ne pouvez pas restaurer ce compte à l'aide de votre solution locale, puisqu'il n'a jamais existé sur l'instance locale d'AD. Vous devez donc le restaurer à partir de la Corbeille Azure AD, si la situation le permet (comme évoqué plus haut).

Autres comptes d'utilisateurs Cloud

En plus de synchroniser les objets utilisateurs d'une instance locale d'AD à l'aide d'Azure AD Connect, certaines entreprises créent des comptes Azure AD en utilisant soit un annuaire externe, tel qu'un annuaire virtuel, soit une solution de gestion des identités. Il arrive également qu'elles créent des objets utilisateurs Cloud qui permettent aux salariés de se connecter aux applications SaaS, telles que Concur ou Salesforce, via Azure AD. Cependant, la sauvegarde et la restauration locales ne prennent en compte ni ces comptes d'utilisateurs ni leurs propriétés.

Objets synchronisés à partir de sources autres qu'une instance locale d'AD

Certaines applications, en particulier celles créées en interne, ne fonctionnent pas nativement avec AD, en raison de leur conception ou de leur fonction. Elles écrivent directement les données dans Azure AD en dehors du processus de synchronisation natif. Il peut s'agir, par exemple, de logiciels pour l'authentification multifacteur qui écrivent des données dans Azure AD afin de permettre aux utilisateurs d'y accéder, ou d'applications qui écrivent des données dans un environnement Azure AD étendu dans le but de valider les utilisateurs.

Si la synchronisation à partir d'Azure AD n'est pas effectuée, ces objets ne sont pas pris en compte par la sauvegarde et la restauration locales.

MIGRATION LOCATAIRE À LOCATAIRE

Un autre cas d'utilisation auquel on pense peu est celui de la migration locataire à locataire, lorsque l'entreprise ou les rôles viennent à changer dans le cadre d'un regroupement, d'une fusion, d'une acquisition ou d'une cession. Certaines entreprises se tournent alors vers Azure AD pour leur stratégie de sauvegarde et de restauration.

Prenons, par exemple, une société faisant l'objet d'un regroupement. Elle compte plusieurs dizaines de locataires et doit remplacer les utilisateurs de ces locataires en raison des futurs changements de rôles et de hiérarchie. Elle a également conscience qu'il pourra lui être utile de garder une certaine marge de manœuvre pendant le regroupement, en vue de répondre aux situations imprévues, par exemple, en restaurant le niveau d'accès aux applications de certains utilisateurs ou en fournissant plusieurs niveaux d'accès temporaires à certains utilisateurs. Nous pourrions également prendre l'exemple d'une société procédant à la cession de l'une de ses lignes de produits et qui doit supprimer un locataire comptant plusieurs centaines ou milliers de comptes d'utilisateurs. Dans ce cas, il serait prudent de conserver une sauvegarde finale de ces comptes.

Certaines entreprises comptent des dizaines, voire des centaines, de locataires Azure AD pour leurs différentes branches qui sont gérées par différentes équipes administratives. Si elles se reposent sur Azure AD comme sur un système de sécurité pour les migrations, et qu'une erreur se produit au cours de la migration locataire à locataire ou du regroupement, elles se rendront compte que les outils natifs ne sont pas bien adaptés à la reprise d'activité.

SAUVEGARDE ET RESTAURATION POUR LES ENTREPRISES DISPOSANT D'UN ENVIRONNEMENT HYBRIDE

Pour assurer la sécurité, la conformité et la continuité de l'activité, il est indispensable de disposer d'un système de sauvegarde et de restauration fiable, à la fois pour les instances locales d'AD et pour Azure AD. Comme nous l'avons vu, le fait de disposer d'une solution locale robuste ne suffit pas, car il est quasiment impossible d'utiliser Office 365 ou Azure sans créer des utilisateurs, des groupes et des attributs Cloud. La Corbeille Azure AD est pratique pour restaurer certains objets récemment supprimés, cependant, elle n'a pas été conçue pour constituer une solution de sauvegarde et de restauration pour l'entreprise.

Les solutions Quest vous permettent de protéger vos environnements hybrides dans leur intégralité. Recovery Manager for Active Directory s'intègre désormais à Quest On Demand Recovery for Azure

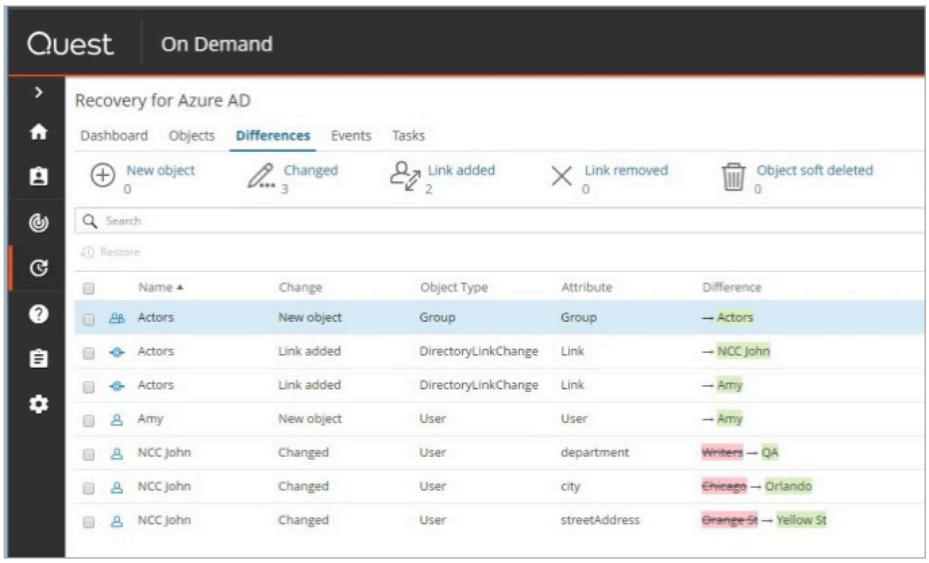

Figure 2. Les rapports de comparaison entre les sauvegardes et les instances Azure AD actives permettent de déterminer aisément les modifications apportées, et de sélectionner puis de restaurer précisément les changements souhaités.

Active Directory, afin d'offrir une solution de restauration hybride et complète et vous garantir une tranquillité d'esprit.

Recovery Manager for AD permet à plus de 1 600 entreprises de se protéger contre la modification malveillante ou involontaire de leurs données Active Directory. Sans nécessiter la mise hors ligne d'Active Directory, il prend également en compte les objets des instances locales que vous avez synchronisés dans le Cloud à l'aide d'Azure AD Connect. Vous pouvez automatiser les sauvegardes, repérer les modifications en comparant la configuration actuelle d'Active Directory à celle d'une sauvegarde, et récupérer rapidement des sections entières d'annuaire, ou de certains objets ou attributs.

Quest On Demand Recovery s'occupe du reste, notamment des objets qui n'ont pas été synchronisés par Azure AD Connect.

En associant ces deux solutions, vous obtenez un tableau de bord de restauration, à la fois pour les objets Cloud et les objets hybrides, qui comprend des informations détaillées que les outils natifs ne fournissent pas, telles que le type des objets. Vous pouvez générer des rapports de comparaison afin de déterminer les éléments qui doivent être récupérés, et restaurer les modifications effectuées localement ou dans Azure AD, directement dans le rapport (voir Figure 2).

Avec Quest On Demand Recovery, vous pouvez surveiller la progression de la synchronisation des objets effectuée par Azure AD Connect.

Vous pouvez également identifier les objets et les attributs Cloud qui n'ont pas été synchronisés, et éviter ainsi les restaurations incomplètes.

CONCLUSION

De nombreuses entreprises utilisent Azure AD Connect pour synchroniser les données de leurs instances locales d'AD avec Azure AD. Toutefois, ce genre de synchronisation unidirectionnelle les expose à des écarts de données lors d'une reprise d'activité, car les objets et les attributs Cloud ne sont pas pris en compte par les outils locaux de sauvegarde et de restauration.

En adoptant des solutions hybrides, les entreprises utilisent de plus en plus d'attributs Cloud, de groupes Office 365, de groupes Azure AD, de comptes B2B/B2C et autres fonctionnalités des environnements AD hybrides, en vue d'améliorer l'expérience utilisateur. Il devient donc de plus en plus urgent de remédier aux écarts de données résultant de stratégies de reprise d'activité incomplètes.

L'intégration de Quest Recovery Manager for AD à Quest On Demand permet de bénéficier d'un tableau de bord de restauration, qui aide à éviter de tels écarts. Les entreprises peuvent utiliser la solution Quest pour différencier les objets hybrides des objets Cloud, pour générer des rapports de comparaison entre les sauvegardes de production et les sauvegardes en temps réel, et pour restaurer les modifications localement et dans Azure AD.

Avec Quest On Demand Recovery, vous pouvez surveiller la progression de la synchronisation des objets effectuée par Azure AD Connect. Vous pouvez également identifier les objets et les attributs Cloud qui n'ont pas été synchronisés, et éviter ainsi les restaurations incomplètes.

PROFIL DE QUEST

L'objectif de Quest est de résoudre des problèmes complexes avec des solutions simples. Nous y parvenons en appliquant une philosophie qui repose sur l'excellence de nos produits, un service de qualité et un objectif global de simplicité dans nos interactions. Notre vision est de proposer une technologie qui apporte à la fois efficacité et résultats concrets, afin que votre entreprise consacre moins de temps à la gestion informatique et plus de temps à l'innovation.

En cas de questions sur l'utilisation de ce document, nous vous invitons à contacter :

Quest Software Inc.
Attn: LEGAL Dept

Veuillez vous rendre sur notre site Web (www.quest.com/fr) pour obtenir nos coordonnées locales et internationales.