Chapitre 4
Gestion des identités sous Windows 10

1. Gestion des identités

La gestion des identités et de l'identité d'un utilisateur est différente en environnement d'entreprise par rapport à un environnement privé.

En effet, en environnement privé, les utilisateurs auront tendance à utiliser une authentification basée sur leur compte Microsoft et les informations qu'ils auront fournis, alors qu'en entreprise, les utilisateurs exploiteront un compte Active Directory et un jeu d'informations constituant celui-ci. Ces informations étant basées sur diverses sources, l'agrégation de celles-ci composera l'identité de l'utilisateur.

1.1 Qu'est-ce qu'une identité ?

La protection des informations et la gestion des utilisateurs passent par la constitution d'une identité par utilisateur.

Cette identité doit être fiable donc construite à partir de sources elles-mêmes fiables telles qu'un annuaire d'entreprise, une base de données des Ressources Humaines ou toute autre source maîtrisée et dont la structure est connue.

L'identité est donc un jeu de données permettant de décrire de façon unique une personne et possiblement les liens entretenus avec d'autres personnes.

Dans un environnement Microsoft, l'objet utilisateur Active Directory représente l'identité de la personne et se voit complété d'informations techniques telles qu'un identifiant unique afin de permettre à cet objet de prendre part aux processus d'authentification et d'autorisation.

2. Authentification

Avant d'utiliser un poste de travail Windows, les utilisateurs doivent ouvrir une session sur celui-ci. Ce processus d'ouverture de session exploite ainsi le processus d'authentification. L'authentification est un processus de vérification de l'identité de la personne ou du service qui tente d'accéder à une ressource.

Sous Windows 8, l'authentification se base sur de nombreux critères tels qu'un nom d'utilisateur et un mot de passe mais également une image et des clics particuliers sur celle-ci.

Les ressources sur lesquelles il est possible de s'authentifier sont multiples : imprimantes, partages de fichiers, messagerie…

Dans ce chapitre, nous allons décrire les principes fondamentaux de l'authentification utilisateur.

2.1 Authentification et autorisation

L'authentification est un processus permettant de vérifier l'identité de l'utilisateur.

Dans la plupart des cas, l'utilisateur fournit des informations d'identification basées sur deux critères tels qu'un nom d'utilisateur et un mot de passe supposés être individuels et secrets.

Ces données fournies au système et validées par celui-ci permettent alors à l'utilisateur d'être authentifié.

2.1.1 Types d'authentification

Il existe deux types d'authentification :

– l'authentification locale (ou ouverture de session interactive), lorsque l'utilisateur ouvre une session directement sur le système d'exploitation.
– l'authentification à distance (ou authentification réseau), lorsque l'utilisateur est connecté sur une machine et accède à une ressource distante telle qu'un partage de fichiers ou une infrastructure de messagerie.

2.1.2 Processus d'autorisation

L'autorisation est un processus qui suit l'authentification. Il permet ou non l'accès à une ressource et ce, en fonction de règles d'accès définies sur celle-ci.

Une demande d'autorisation est effectuée par le système sur lequel l'utilisateur est authentifié. Cette demande s'effectue au travers d'un jeton d'authentification ou *Security Token*, ce jeton représente l'utilisateur et lui est fourni par l'autorité locale de sécurité (LSA : *Local Security Authority*).

Le jeton d'authentification contient entre autres le SID (identifiant de sécurité) de l'utilisateur et des groupes dont il est membre. Le SID est une suite de caractères alphanumériques qui identifient de façon unique l'utilisateur authentifié.

Le jeton d'authentification représente également les privilèges octroyés à l'utilisateur sur le système sur lequel il est authentifié.

Il est important de noter que :

– un jeton d'accès est généré et conservé sur le système sur lequel l'utilisateur possède une session interactive ;
– un jeton n'est jamais transmis au travers du réseau ;
– le LSA d'une machine n'accepte pas les jetons générés par une autre machine.

Lorsqu'un utilisateur souhaite accéder à une ressource distante, le serveur authentifie l'utilisateur et génère un jeton localement. Le jeton d'authentification ainsi généré sur le serveur est différent du jeton présent sur le poste client. Ce jeton côté serveur est utilisé pour définir les autorisations octroyées à l'utilisateur sur la ressource.

2.2 Les différentes formes d'authentification

Les comptes de type Microsoft ID, Hotmail ou Xbox Live sont rassemblés sous la dénomination Comptes Microsoft (Microsoft Account). Si un utilisateur possède un compte Microsoft, il est en mesure d'ouvrir une session sur un poste Windows 8.

Windows 8 est maintenant capable d'exploiter ces comptes afin de proposer une expérience avancée aux utilisateurs :

- authentification sur le Windows Store pour télécharger et installer des applications,
- authentification sur les services tels que OneDrive pour le stockage de données en ligne,
- synchronisation des mots de passe et divers paramètres sur les postes Windows 8 de l'utilisateur,
- …

En complément de cette nouvelle possibilité d'authentification, l'utilisateur peut également utiliser un compte local ou de domaine pour toute ouverture de session interactive.

2.2.1 Authentification multifactorielle via Azure MFA

Azure Multi Factor Authentication, permet de s'appuyer sur les services Azure afin de renforcer l'authentification de l'utilisateur.

L'authentification multifactorielle se base sur l'utilisation de plusieurs méthodes d'identification de l'utilisateur.

Ces méthodes sont multiples :

– applications installées sur un téléphone mobile
– envoi de SMS ou appel
– nom d'utilisateur et mot de passe
– carte à puce et code PIN
– biométrie

Ces facteurs d'authentification sont plus ou moins évolués. L'utilisation de carte à puce pour ce processus peut par exemple être étendue et permettre le chiffrement des données.

L'authentification multifactorielle permet d'authentifier l'utilisateur en se basant sur :

– quelque chose qu'il possède : une carte à puce, un nom d'utilisateur.

et

– quelque chose qu'il connaît : un code PIN, un mot de passe, un dessin.

2.2.2 Cartes à puce virtuelles

Les cartes à puce virtuelles sont un nouveau moyen d'authentification disponible avec Windows 8 et Windows Server 2012.

Les cartes puce virtuelles (*ou virtual smart cards*) émulent des cartes à puces physiques. En lieu et place d'une carte à puce physique, c'est une carte virtuelle qui est générée et sauvegardée au sein de la puce TPM (*Trusted Platform Module*) de la machine physique.

Ce type de puce est présent dans la plupart des machines récentes et est également utilisé lors du chiffrement de disques avec BitLocker.

L'utilisateur peut exploiter ce moyen d'authentification virtuel comme il le fait avec une carte physique, celle-ci est affichée et exploitable de la même façon.

Si l'utilisateur se connecte à plusieurs machines (équipées de puces TPM), une nouvelle carte à puce virtuelle sera générée et stockée localement sur chacune des machines. De même, si un utilisateur requiert plusieurs cartes à puces virtuelles sur la même machine, ces cartes seront générées localement et stockées dans la puce TPM locale.

Cette solution d'authentification est généralement moins onéreuse que la distribution de carte physique car elle ne nécessite pas d'achat de lecteurs et de cartes à puce.

2.2.3 Authentification biométrique

L'authentification biométrique se base sur des critères physiques authentifiant de façon unique une personne. Ces critères sont multiples, les plus communs sont :

– les empreintes digitales ;

– la voix ;

– les vaisseaux sanguins situés au fond de l'œil ;

– l'iris ;

– …

2.2.4 Images mots de passe

Windows 8 propose une nouvelle méthode d'authentification basée sur des images cliquables utilisées comme des mots de passe.

Cette solution permet de répondre à la demande croissante d'authentification basée sur des mots de passe toujours plus complexes tout en répondant au problème lié à l'erreur et au temps consacré à la saisie de ceux-ci.

L'authentification basée sur des images mots de passe consiste pour l'utilisateur en une série de clics sur des zones prédéfinies de l'image. La position et l'ordre des clics permettront de confirmer l'identité de l'utilisateur : il sera ainsi authentifié.