

Glossaire des termes de gestion d'accès privilégiés (PAM) fréquemment utilisés



PARLES-TU LE PAM?

Il n'y a pas si longtemps, quand j'ai commencé à travailler chez Devolutions (ça fait cinq ans – le temps passe vite quand on s'amuse!), j'évaluais mes compétences linguistiques comme étant « assez bonnes ». Je parle quand même couramment l'anglais et le français, et j'ai une bonne maîtrise de l'hébreu (מולש!) et de l'espagnol (holà!).

Un jour, un de mes collègues m'a demandé: « Parles-tu le PAM? »

Je n'avais aucune idée de quoi il parlait. À l'époque, je pensais que c'était probablement une langue fictive, un peu comme le [Shyriiwook](#).

Et bien, devinez quoi? Parler « PAM », c'est encore plus utile que parler Shyriiwook (mes excuses à tous les Wookiees de ce monde). En fait, à peu près tout le monde parle le « PAM » ces temps-ci.

Beaucoup d'entre vous sont des techniciens qui connaissent probablement tout sur le sujet. À un point tel que, si vous participiez au quiz Jeopardy! et que la catégorie de questions était « Gestion des accès privilégiés », vous auriez probablement toutes les bonnes réponses et forceriez vos concurrents à [quitter la scène dans une honte absolue](#).

Sauf que plusieurs personnes qui visitent notre blogue sont des utilisateurs professionnels et non des utilisateurs techniques. Même pour les plus ultra-geeks d'entre nous, c'est toujours utile de se rafraîchir la mémoire. J'ai donc pensé qu'il serait intéressant de vous concocter un petit glossaire des termes de gestion d'accès privilégiés fréquemment utilisés :

Compte de moindre privilège : compte utilisateur comprenant un nombre minimal de privilèges nécessaires pour effectuer des opérations quotidiennes.

Compte utilisateur : compte standard qui représente un utilisateur humain avec des privilèges standards (généralement lié à un profil Active Directory).

Compte d'urgence : se dit d'un compte créé pour faciliter l'accès d'urgence à un système sécurisé. Les comptes Firecall (comptes administrateurs) sont parfois accédés par les utilisateurs sans comptes privilégiés pour accéder aux systèmes clés quand arrivent des problèmes (**voir Scénarios d'urgence « Break-the-Glass »**).

Compte de services : permet des interactions à distance (de logiciel à logiciel) avec d'autres systèmes ou d'exécuter des services spécifiques.

Compte partagé : compte partagé entre plusieurs utilisateurs à des fins de maintenance et d'installation de logiciels. Comprend fréquemment des comptes d'urgence (Firecall ou Break-the-Glass), qui fournissent un accès temporaire à un système d'information sécurisé en cas d'erreur critique ou de situation d'urgence (**voir Scénario d'urgence « Break-the-Glass »**).

Compte privilégié : compte qui possède des privilèges supérieurs. Il peut être partagé entre plusieurs utilisateurs et représente une application, un système, un service ou un administrateur. Il existe plusieurs types de comptes privilégiés (**voir Compte système, Compte partagé et Compte de services**).

Compte système : compte intégré utilisé par les administrateurs afin d'accéder aux applications et aux systèmes, comme le compte racine (root) des systèmes Unix / Linux ou Administrateur sur les systèmes Windows.

Injection des identifiants : l'action qui initie un lancement de session par un protocole connu (SSH, RDP, VNC, X11, etc.) et qui injecte les informations d'identification au même moment. Les informations d'identification sont

insérées dans le back-end, ce qui signifie que les utilisateurs finaux ne voient jamais les mots de passe, mais ils peuvent toujours accéder aux comptes nécessaires pour effectuer leur travail quotidien.

Privilège : droit d'apporter des modifications administratives ou de niveau supérieur à un réseau ou à un ordinateur et de consulter des informations sensibles.

Scénarios d'urgence « Break-the-Glass » : se dit de toute méthode établie pour fournir un accès d'urgence à un système d'information sécurisé. En cas d'erreur critique ou de fin anormale, les utilisateurs qui n'ont pas d'accès privilégié peuvent accéder aux systèmes clés et corriger le problème.

Utilisateur informatique privilégié : utilisateur ayant accès à l'infrastructure informatique de l'entreprise.

Utilisateur privilégié : utilisateur qui bénéficie d'un accès privilégié. Il existe plusieurs types d'utilisateurs privilégiés (voir **Utilisateur professionnel privilégié** et **Utilisateur informatique privilégié**).

Utilisateur professionnel privilégié : utilisateur ayant accès à des données et des informations sensibles, comme les dossiers RH, les fiches de paie, les informations financières, la propriété intellectuelle de l'entreprise, etc.

Et voilà! Vous parlez maintenant couramment le PAM. Partagez ce glossaire avec vos collègues et clients plus ou moins geek pour que vous puissiez enfin parler le même langage. Vous verrez, ça peut faire une réelle différence sur l'efficacité et la sécurité! Comme dirait Chewbacca dans un élégant et poétique Shyriiwook : oooaowhrrrcraaohuanraaoahoowhthhhhhggg!

