

Cloud : AWS muscle l'authentification sur son bureau virtuel

AWS, l'entité Cloud d'Amazon, supporte désormais l'authentification multi-facteurs sur son service de bureau virtuel [Workspaces, lancé en mars dernier](#). Le mécanisme repose sur un serveur Radius on-premise Un ajout attendu par les entreprises et qui permet de **mieux intégrer le service Cloud à la politique d'authentification** des utilisateurs. En effet, comme l'indique AWS, les utilisateurs Workspaces peuvent maintenant « *s'authentifier en utilisant les mêmes mécanismes que ceux utilisés pour d'autres formes d'accès distants aux ressources de l'entreprise* ». Autrement dit, ils se connecteront « *en entrant leur nom d'utilisateur et mot de passe Active Directory suivi d'un mot de passe éphémère (OTP – One Time Password) fourni par un système de token matériel ou logiciel* ». AWS précise que le système fonctionne avec tous les fournisseurs d'authentification au protocole Radius (avec support de PAP, CHAP, MS-CHAP1, MS-CHAP2 ainsi que de proxy Radius).

Le leader du Cloud public indique également qu'il prévoit de **supporter d'autres formes d'authentification comme des cartes à puce** ou des certificats.

Amazon WorkSpaces permet de disposer d'un poste de travail en mode Cloud, accessible depuis un large ensemble de terminaux : des ordinateurs classiques fonctionnant sous Windows ou OS X, mais également des tablettes tournant sous Android ou iOS. Bien évidemment, les tablettes Kindle Fire d'Amazon sont compatibles avec cette offre.

D'autres bénéfices du Cloud rendent ce service intéressant pour les entreprises : définition de machines virtuelles sur mesure ; **administration centralisée** du parc de machines virtuelles ; paiement des ressources à l'usage ; **mises à jour automatiques** ; sauvegardes chiffrées sur Amazon S3 ; pré-installation possible de certaines applications clés, comme Microsoft Office...

A lire aussi :

[Dossier : comment garantir la sécurité du Cloud public](#)