

L'Etat français (ANSSI) va certifier les Cloud de confiance

	L'Etat français (ANSSI) va certifier les Cloud de confiance
-----------------------------------------------------------------------------------	-------------------------------------------------------------

L'Agence nationale pour la sécurité des systèmes d'information (Anssi) s'apprête à certifier les Cloud de quelques prestataires. Deux niveaux de labellisation sont attendus.



L'Agence nationale pour la sécurité des systèmes d'information (Anssi), dépendant du Premier ministre, est engagée dans un processus qui aboutira à la qualification des fournisseurs de Cloud. Les prestataires présentant le niveau de sécurité requis recevront donc un label de l'Agence, qui permettra aux entreprises et administrations de recourir à leurs services en se basant sur les garanties fournies par l'Etat français. « *Huit prestataires se sont lancés dans ce processus de qualification* », assure Guillaume Poupard, le directeur général de l'Anssi, qui a appelé les grands acteurs du Cloud américains à rejoindre le mouvement. « *La qualification n'est pas un outil de protectionnisme* », reprend Guillaume Poupard. Selon lui, les AWS et autre Microsoft (pour Azure) sont en train d'étudier une éventuelle qualification. Façon de dire aussi qu'il n'est pas acquis qu'ils se soumettent un jour aux exigences de l'Anssi.

Notons que, sur ce dossier, l'Anssi travaille en coordination avec ses homologues allemands du BSI (l'Office fédéral de la sécurité des technologies de l'information) : un prestataire homologué outre-Rhin recevra automatiquement son label dans l'Hexagone et vice-versa.

Deux niveaux : Cloud Secure et Cloud Secure +

Ce label étatique fait suite à une démarche entamée dès la mi-2014. A cette époque, l'Anssi avait publié un premier référentiel et appelé les entreprises à le commenter. Un grand nombre de commentaires, parfois critiques, avaient été remontés à l'Agence. Depuis, cette dernière a réuni un comité restreint pour travailler à une seconde version du référentiel, largement inspiré de la norme ISO 27 001.



Guillaume Poupard, directeur général de l'Anssi.

En réalité, la démarche doit accoucher de deux niveaux de qualification : Cloud Secure et Cloud Secure +. Dans la première, selon des déclarations publiques d'un membre de l'Anssi en octobre dernier, on retrouve des bonnes pratiques assez classiques : contrôles d'accès physiques, authentification forte avec mots de passe hachés et salés, chiffrement logiciel et hébergement des données en Europe. Le niveau le plus élevé ira plus loin, imposant une authentification multi-facteurs, un chiffrement matériel (via HSM) ou encore un hébergement en France. Parmi les acteurs figurant dans la liste des premiers prestataires certifiés, on devrait retrouver Thales, Orange ou Oodrive, qui se présentait en octobre dernier comme l'acteur pilote de la qualification Secure Cloud +. Notons qu'à l'époque, l'Anssi indiquait que les OIV – les quelque 250 organisations identifiées comme essentielles au fonctionnement de la nation – pourraient se voir imposer le recours à des prestataires certifiés Secure Cloud +. Les premiers arrêtés encadrant les politiques de sécurité des OIV n'y font toutefois pas référence à ce jour.

Cloud Secure + : les Américains out ?

« *Nous nous sommes engagés à nous conformer à cette norme auprès de certains clients* », explique Laurent Seror, le président d'Outscale, le fournisseur de IaaS né sous l'impulsion de Dassault Systèmes. « *Etant donné que nous sommes déjà certifiés ISO 27 001, je considère que nous sommes prêts. Ne pas être certifié juste au moment de la sortie du référentiel ne sera pas pénalisant compte tenu de la longueur des cycles de décision* », ajoute Laurent Seror. Ce dernier relève toutefois que, par construction, le niveau Cloud Secure + restera difficile à atteindre pour les grands prestataires américains. D'abord parce qu'ils ne possèdent pas, à ce jour, de datacenter en France (à l'exception de Salesforce). Mais, au-delà de ce seul élément, d'autres questions se posent. Selon lui, chez AWS, un administrateur américain, donc soumis au Patriot Act, peut accéder à toutes les machines virtuelles, quelle que soit la zone où ces dernières sont hébergées. « *On en est sûr à 99% en raison de la nature d'une fonction qu'ils proposent pour la migration entre deux régions géographiques. Celle-ci suppose l'existence d'un réseau à plat entre toutes les plates-formes.* »

La question de la localisation des données reste un élément central de la politique de certains pays européens souhaitant reconquérir leur souveraineté dans le Cloud. Lors du débat au Sénat sur le projet de loi pour une République numérique (porté par Axelle Lemaire), un amendement, déposé par les sénateurs du groupe communiste et prévoyant d'obliger les entreprises à stocker les données personnelles des citoyens français sur le territoire européen, a été voté. « *Cet amendement n'était pas téléguilé, assure aujourd'hui Guillaume Poupard. Je l'ai découvert au moment des débats.* » Le 29 juin, une commission mixte paritaire doit harmoniser les versions de ce projet de loi sorties respectivement des débats à l'Assemblée et au Sénat. Rien ne permet d'affirmer que ledit amendement, absent de la version votée par le Palais Bourbon, soit présent dans la mouture finale du texte de loi.

Article original de Reynald Fléchaux



Réagissez à cet article

Original de l'article mis en page : L'Etat français va certifier les Cloud de confiance