Pack d'intégration Cloud

Créez et contrôlez les clés de chiffrement au sein de votre HSM certifié FIPS 140-2, pour ensuite les exporter en toute sécurité dans le cloud

CARACTÉRISTIQUES

Fournit aux utilisateurs des services de cloud public la possibilité de générer des clés de chiffrement au sein de leur propre environnement et de garder le contrôle de ces clés tout en les rendant disponibles, selon les besoins, pour une utilisation dans le cloud de leur choix.

- Contrôle de vos clés de chiffrement permettant une stratégie multicloud ou hybride
- Sécurisation de la génération de clés grâce à une source à forte entropie
- Protection des clés à long terme grâce aux HSM certifiés FIPS et Critères Communs (CC)
- Prend en charge Amazon Web Services, Google Compute Engine, Microsoft Azure

Protège vos clés dans le cloud avec le plus haut niveau de sécurité possible

Garantit la protection de votre marque et de vos données

Certifiés conformes à des normes de sécurité parmi les plus rigoureuses telles que les FIPS 140-2 et les Critères communs, les HSM nShield de Entrust sont capables de protéger vos données même dans les conditions de sécurité les plus difficiles et les plus exigeantes, que ce soit sur site ou dans le Cloud.

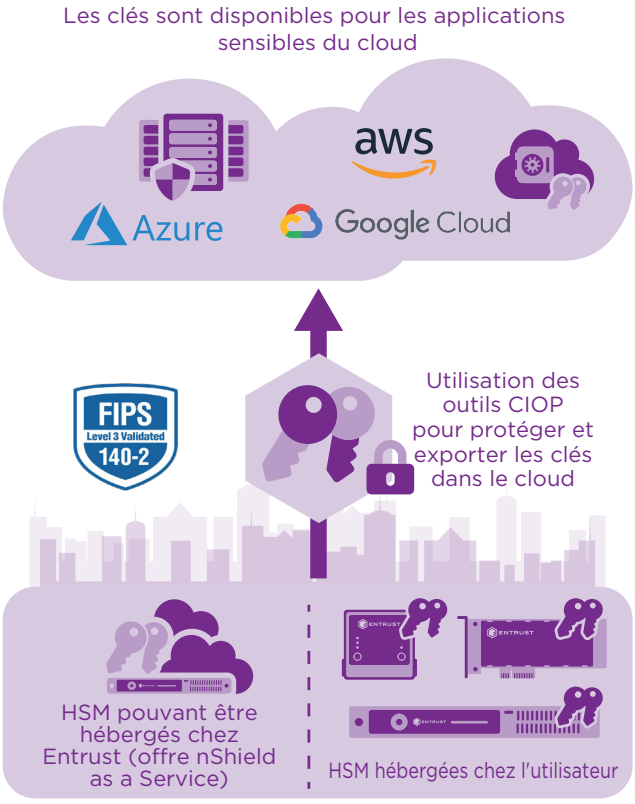

Schéma 1. Les clés de chiffrement sont générées dans un HSM nShield, puis protégés et exportés sur le cloud

DÉCOUVREZ-EN PLUS SUR ENTRUST.COM/FR/HSM

Pack d'options d'intégration cloud

Fournisseurs de services cloud pris en charge :

Le pack d'options d'intégration dans le cloud (CIOP) vous fournit les outils vous permettant de générer vos clés de chiffrement à l'aide d'un HSM nShield, puis de les protéger et de les exporter vers les fournisseurs de services de cloud suivants :

- Services Web Amazon (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (en utilisant le mécanisme Azure BYOK)

Pour les utilisateurs qui recherchent un niveau de protection élevé, Microsoft propose la solution nCipher BYOK. La méthode nCipher BYOK permet de garantir que les autorisations des clés créées au moment de leur génération soient conservées pendant le transfert vers Microsoft Azure Key Vault. En outre, Microsoft utilise l'architecture Entrust nShield Security World pour limiter l'utilisation des clés dans un certain périmètre dans Azure. Cette méthode ne nécessite pasl'achat de CIOP. Consultez la page **Import HSM-protected keys for Key Vault (nCipher)** pour plus d'informations.

Contrôle des clés dans les environnements hybrides et multicloud

Le pack d'options d'intégration dans le cloud procure aux utilisateurs le niveau de contrôle et de sécurité dont ils ont besoin, que ce soit pour déployer une stratégie de cloud hybride, une stratégie de cloud unique ou une stratégie multicloud. En apportant vos clés de chiffrement au fournisseur de services cloud, vous évitez les problèmes de réversibilité liés à l'enfermement propriétaire qui peuvent les problèmes de réversibilité rendre difficile la migration d'un fournisseur de services cloud à un autre.

Configurations prises en charge

- Nécessite le logiciel nShield Security World v12.60 et le micrologiciel v12.60 ou plus récent pour Azure BYOK
- Nécessite le logiciel nShield Security World v12.40 pour AWS et Google Compute Engine
- La compatibilité de cette version a été testée sur plusieurs environnements, dont :
  - Microsoft Windows Server 2019 x64 et 2016 x64
  - Microsoft Windows 10 x64 et 7 x64
  - Red Hat Enterprise Linux 7 x64 et AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 et 11 x64
  - Oracle Enterprise Linux 7.6 x64 et 6.10 x64
- HSM pris en charge
  - Compatible avec tous les modèles de la gamme nShield

En savoir plus

Pour en savoir plus sur les HSM nShield de Entrust, rendez-vous sur **entrust.com/fr/hsm**. Pour en savoir plus sur les solutions de protection numérique de Entrust pour les identités, l'accès, les communications et les données, rendez-vous sur **entrust.com/fr**

Découvrez-en plus sur
entrust.com/HSM

ENTRUST

Nous contacter :
HSMinfo@entrust.com