Cloud Integration Option Pack

Crie e controle chaves criptográficas em seu HSM com certificação FIPS 140-2 e exporte-as com segurança para a nuvem

DESTAQUES

Fornece aos usuários de serviços de nuvem pública a capacidade de gerar chaves criptográficas em seu próprio ambiente e manter o controle dessas chaves, ao mesmo tempo que as disponibiliza, conforme necessário, para uso na nuvem de sua escolha.

- Controle de suas chaves criptográficas com suporte a uma estratégia de nuvem múltipla ou híbrida
- Geração de chave segura usando uma fonte de entropia forte
- Proteção de chave de longo prazo usando um HSM certificado por FIPS
- Suporte para Amazon Web Services, Google Compute Engine, Microsoft Azure

Proteja suas chaves na nuvem com o mais alto nível de garantia

Proteja sua marca e seus dados

Validados pelos mais altos padrões de segurança, como FIPS 140-2 e Common Criteria, os HSMs Entrust nShield estão prontos para proteger seus dados mesmo nas situações de segurança mais desafiadoras e exigentes, seja no local ou na nuvem.

Figura 1. As chaves de criptografia são geradas em um HSM nShield, agrupadas e exportadas com segurança para a nuvem

SAIBA MAIS EM ENTRUST.COM/HSM

Cloud Integration Option Pack

Provedores de nuvem suportados:

O Cloud Integration Option Pack (CIOP) fornece as ferramentas para permitir que você crie suas chaves criptográficas usando um HSM nShield e, em seguida, encapsule-as e exporte-as com segurança para os seguintes provedores de serviços de nuvem:

- Amazon Web Services (AWS)
- Google Compute Engine
- Microsoft Azure Key Vault (usando o mecanismo Azure BYOK)

Para clientes que buscam um nível mais alto de garantia, a Microsoft oferece o nCipher BYOK. O método nCipher BYOK fornece garantias adicionais de que as permissões de chave criadas no momento da geração são preservadas durante a transferência para o Microsoft Azure Key Vault. Além disso, a Microsoft usa o Entrust nShield Security World para restringir o uso de chaves a uma região específica do Azure. Este método não requer a compra do CIOP. Consulte **Importar chaves protegidas por HSM para Key Vault (nCipher)** para obter mais informações.

Controle de chaves em ambientes híbridos e com várias nuvens

O Cloud Integration Option Pack oferece aos clientes o controle e a garantia de que precisam, seja implementando uma estratégia de nuvem híbrida um único provedor de serviços de nuvem ou uma estratégia de várias nuvens. Ao trazer suas chaves criptográficas para o provedor de serviços de nuvem, você evita as dificuldades associadas à fidelização a um fornecedor, o que pode dificultar a migração de um provedor de serviços de nuvem para outro.

Configurações suportadas

- Requer nShield Security World Software v12.60 e firmware v12.60 ou posterior para Azure BYOK
- Requer o software nShield Security World v12.40 para AWS e Google Compute Engine
- Esta versão foi testada para compatibilidade em uma variedade de plataformas, incluindo:
  - Microsoft Windows Server 2019 x64 e 2016 x64
  - Microsoft Windows 10 x64 e 7 x64
  - Red Hat Enterprise Linux 7 x64 e AS/ES 6 x86/x64
  - SUSE Enterprise Linux 12 x64 e 11 x64
  - Oracle Enterprise Linux 7.6 x64 e 6.10 x64
- HSMs suportados
  - Compatível com todos os modelos nShield

Saiba mais

Para saber mais sobre os HSMs Entrust nShield, visite **entrust.com/HSM**. Para saber mais sobre as soluções digitais da Entrust para identidades, acesso, comunicações e dados, visite **entrust.com**

Saiba mais em
entrust.com/HSM

ENTRUST

Entre em contato conosco:
HSMinfo@entrust.com