nShield Database Security Option Pack

Integración impecable de bases de datos de servidor Microsoft SQL con módulos de seguridad de hardware de nShield de alta garantía

CARACTERÍSTICAS PRINCIPALES

Raíz sólida de confianza para las implementaciones de base de datos del servidor Microsoft SQL

- Protege las claves criptográficas de la base de datos en los módulos de seguridad de hardware (HSM) con certificaciones de mejores prácticas FIPS y Common Criteria
- Asegura tanto la encriptación a nivel celular y de datos transparentes (TDE)
- Protege los datos fundamentales de una organización ante fallas de seguridad

Las bases de datos son un depósito significativo de información confidencial en la mayoría de las organizaciones. Las bases de datos corporativas contienen datos de tarjetas de crédito de clientes, información competitiva confidencial y propiedad intelectual. La pérdida o robo de datos suponen un riesgo significativo de daños de imagen y reputación para las organizaciones, así como graves multas. Al proteger los datos fundamentales ante amenazas internas y externas, las organizaciones mitigan el riesgo de fallas de datos y cumplen las obligaciones normativas y legislativas, incluido la normativa de seguridad de datos industriales de tarjetas de pago (PCI DSS). De hecho, la sección 3.6 de la última normativa PCI DSS (v3.2.1) especifica que "las claves cifradas deben ser almacenadas de forma segura...dentro de un dispositivo criptográfico seguro como un HSM." Además, la sección 3.6 destaca las buenas prácticas de gestión de claves proporcionadas como una función de un HSM como el control dual.

Proteja su base de datos con los niveles de seguridad más altos

Cifrar los datos de su base de datos protege los datos, pero también hay que proteger las claves de cifrado que desbloquean dichos datos. El uso de los módulos de seguridad de hardware (HSM) protege las claves cifradas al almacenar las claves de forma separada de los datos en una plataforma segura y de confianza. Los HSM nShield aplican su política de seguridad interna al solicitar la autorización según la función y separar la seguridad y la administración de base de datos, facilitando demostrar el cumplimiento a los auditores.

Disponible como una tarjeta PCIe exclusiva para un servidor único o un dispositivo de red compartida para los entornos virtualizados.

nShield Database Security Option Pack (para Servidor Microsoft SQL) también conocido como el proveedor SQLEKM es la API de gestión de claves extensibles (EKM) proporcionada para el servidor Microsoft SQL.

nShield Database Security Option Pack

El servidor Microsoft SQL se lanza con dos prestaciones de cifrado integradas para proteger sus datos: TDE y cifrado de nivel celular. Estas funciones le permiten proteger toda la base de datos o proteger solo los campos de la base de datos confidenciales, y pueden ser activadas sin alterar sus aplicaciones actuales, estructuras de base de datos y procesos.

Proteja su marca y sus datos

Validados con algunos de los estándares de seguridad más altos, como las certificaciones FIPS y Common Criteria, los HSM nShield de Entrust están listos para proteger sus datos incluso en las situaciones más complicadas y exigentes. Los controles de acceso detallados de los HSM nShield le permiten gestionar las claves cifradas para Microsoft SQL Server. Para aplicar sus políticas, las capacidades de seguridad están separadas de funciones administrativas.

Los HSM nShield de Entrust ofrecen:

- **Protección de claves de hardware** – Almacena claves cifradas de base de datos en un entorno seguro y resistente a falsificaciones para evitar las copias o peligros
- **Aplicación de usuarios y funciones** – Proporciona un control más sólido para el acceso de datos cifrados en Microsoft SQL Server
- **Estrecho control de las claves** – Utiliza la autenticación de la tarjeta inteligente por parte de los administradores para proporcionar un control sólido para las claves cifradas de la base de datos
- **Separación de funciones** – Divide la responsabilidad para tareas y procedimientos importantes entre múltiples administradores
- **Configuración e integración fácil** – Los HSM nShield de Entrust se integran de forma impecable con Microsoft SQL Server para proporcionar:
  - Los TDE y los modos cifrados de nivel celular con la protección de las claves cifradas aplicables

Ajustándolos para cubrir sus necesidades cambiantes, los HSM nShield se integran de forma innovadora con otras aplicaciones empresariales líderes, incluidos los servidores web y de aplicaciones e infraestructuras de claves públicas (PKI).

Los HSM nShield Connect basados en la red pueden compartirse entre diferentes servidores proporcionando:

- **Apoyo para entornos virtualizados** – Almacenamiento de claves basadas de hardware para servidores virtualizados, incluidos Hyper-V y VMware
- **Apoyo para fallo de cluster** incluido el grupo de disponibilidad AlwaysOn
- **Administración simplificada** – Gestiona las claves cifradas para muchas bases de datos así como las claves utilizadas por otras aplicaciones
- **Capacidad de fallo** – Cuando es esencial una alta disponibilidad, los usuarios tienen la opción para cambiar de forma automática a otro HSM cuando otro HSM no está disponible
- **Recuperación en caso de desastre** – Procesos sencillos y seguros para archivar y recuperar las claves
- **Recurso económico** – El uso compartido del módulo entre diferentes servidores reduce los costes de hardware, licencias y operativos

nShield Database Security Option Pack

ESPECIFICACIONES TÉCNICAS

Configuraciones soportadas

- Requiere nShield Security World Software v12.40.2 o v12.60.x o mayor.
- Versión Microsoft SQL server (edición empresa) 2019 x64, 2017 x64
- Apoyo para el sistema operativo del servidor Windows 2019 R2 x64, 2016 R2 x64
- HSM admitidos
  - Compatibles con todos los modelos de HSM nShield Solo y Connect

Algoritmos criptográficos soportados

- Asimétricos - incluidas longitudes de claves de RSA 2048, 3072 y 4096 bits
- Simétricos - incluidos longitudes de claves de AES 128, 192 y 256 bits

FUNCIONALIDAD NSHIELD QUE APOYA

Accede a la siguiente funcionalidad cuando integra un HSM nShield con el servidor Microsoft SQL:

Funcionalidad	Apoyo
1 de N conjunto de tarjetas	Sí
K de N conjunto de tarjetas	No
Tarjetas de software	Sí
Clave única de módulo	No
Recuperación de claves	Sí
Importación de claves	Parcial [1]
Equilibrado de carga	Sí
Fallo	Sí
Soporte estricto FIPS (FIPS 140-2 de nivel 3)	Sí [2]

1. La importación de claves es soportada solo para claves nCore. La API nCore es la interfaz nativa de programación de la aplicación para módulos nShield
2. Consulte los comunicados de prensa y la guía de usuario para más detalles.

Más información

Para saber más sobre los HSM nShield de Entrust visite **entrust.com/HSM**. Para saber más sobre las soluciones de seguridad digital de Entrust para identidades, acceso, comunicaciones y datos, visite **entrust.com**

Para saber más sobre los HSM nShield de Entrust

HSMinfo@entrust.com
entrust.com/HSM

SOBRE ENTRUST CORPORATION

Entrust ayuda a que el mundo se mueva de forma segura al permitir la protección fiable de identidades, pagos y datos. Ahora más que nunca, la gente necesita experiencias seguras impecables, mientras cruzan fronteras, realizan compras, acceden digitalmente a servicios del gobierno o inician sesión en redes corporativas. Entrust ofrece una variedad incomparable de soluciones de seguridad digital y emisión de credenciales en el núcleo de todas estas interacciones. Con más de 2500 colegas, una red de socios globales y clientes de más de 150 países, no es una sorpresa que la mayoría de organizaciones autorizadas del mundo confíen en nosotros.

Más información
entrust.com/HSM

ENTRUST

Contáctenos:
HSMinfo@entrust.com