Oracle Advanced Security

Talleres Oracle

Formación Online

Objetivo

Actualmente las empresas requieren cumplir con determinados estándares de seguridad en cumplimiento de regulaciones vigentes e implementar estrictos controles de acceso a información sensible.

Los niveles de seguridad exigidos en estos entornos; no son solucionados con solo la gestión de usuarios, roles y privilegios. Sino requieren activar funcionalidades avanzadas de seguridad tanto en el acceso a la base de datos; como control sobre las tramas de sentencias SQL que se desplazan en la red.

En el taller de Seguridad Avanzada, aprenderás a implementar funcionalidades de seguridad en Oracle utilizando herramientas como el cifrado de datos, enmascaramiento, ofuscamiento, auditoría, bloqueo en la red entre otros.

Características

- √ Online en vivo con instructor desarrollando el Taller.
- √ Comunicación fluida de preguntas y respuestas.
- √ Disponibilidad de vídeos después de clases.
- √ Plataforma de recursos por curso disponible.

Certificación

Se emite certificado al entregar el Proyecto de Servidor configurado con la aplicación de los temas tratados.

Requerimiento de Equipo

En el Taller se requiere equipo con las siguientes características:

Espacio en disco : 100 Gb (recomendable SSD)
Procesador : Core i5 (mínimo) recomendado i7
Memoria mínima en equipo : 16 Gb RAM

Taller : Advanced Security

1. Implementación de Transparent Data Encryption (TDE)

El cifrado transparente de datos (TDE) es una opción de la Seguridad Avanzada de Oracle que protege los datos confidenciales tales como números de tarjetas de crédito almacenados en tablas y espacios de tabla (información en reposo) e información en tránsito (red, copias de seguridad).

Beneficios:

- Cumple con los estándares de seguridad establecidos por las reglamentaciones de entidades competentes.
- En caso de sustracción de medios la información está protegidos por el cifrado de datos.

2. Implementación de Data Redaction

Oracle Data Redaction enmascara datos confidenciales justo antes de que los resultados de la consulta SQL se devuelvan a la aplicación que emitió la consulta. Limita la visualización de datos sensibles, mostrándolos parcialmente, aleatoriamente o impidiendo totalmente su exposición.

Los datos almacenados en la base de datos *NO* se modifican de ninguna manera.

3. Implementación de Oracle Database Vault

Activación de control de acceso para usuarios privilegiados mediante Oracle Database Vault, bloqueando el acceso no autorizado a datos confidenciales creando entornos de aplicaciones restringidos dentro de Oracle Database.

Los controles de seguridad de Oracle Database Vault ayudan a las organizaciones a abordar la conformidad de las leyes y normas de privacidad de datos, como el Estándar de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS) y muchas otras regulaciones que requieren estrictos controles internos sobre el acceso a la información confidencial.

4. Oracle Audit Vault and Database Firewall -AVDF

Para las bases de datos de Oracle, Oracle Audit Vault y Database Firewall permiten a un auditor establecer políticas de auditoría y aprovisionarlas desde la consola de Audit Vault. Para las bases de datos, proporciona un firewall de base de datos que puede monitorear y/o bloquear declaraciones SQL en la red según una política de firewall diseñada por el auditor.

5. Oracle Data Masking

Revisión de enmascaramiento de entornos no-productivos mediante Data Masking