VIDEO 4: Seguridad y Alta Disponibilidad en SAP HANA

Curso: Modelado en SAP HANA
Fuente: YouTube - Seguridad y alta disponibilidad
Duración: 30:30 minutos

---

1. INTRODUCCIÓN

Esta video aborda los conceptos fundamentales de alta disponibilidad y sistemas de seguridad en SAP HANA, completando el módulo con aspectos críticos para la administración y gestión de la base de datos.

---

2. ALTA DISPONIBILIDAD

2.1 Definición y Objetivos

La alta disponibilidad busca que en el sistema puedan acceder un gran número de usuarios de forma simultánea sin bloqueos mutuos, garantizando el acceso a la información requerida. Además, incluye tolerancia a desastres del sistema.

Ejemplo práctico: Si el servidor de la empresa se cae, inmediatamente se levanta un sistema de reserva para que los usuarios puedan continuar trabajando. Es similar a un generador de emergencia en un hospital.

2.2 Enfoques de Implementación

2.2.1 Un Solo Data Center (Scale Out)

- Múltiples servidores con almacenamiento compartido
- Servidores en espera que toman el lugar del servidor que falla
- Configuración: n servidores activos + x servidores en espera
- Capa de persistencia común a todos los servidores

Proceso de failover:

1. Sistema normal: Base de datos HANA conectada a tres servidores activos + un servidor en espera
2. Fallo del servidor: Por pico de tensión, reinicio o avería de hardware
3. Activación automática: El servidor en espera toma inmediatamente el lugar del servidor fallido
4. Continuidad: Tiempo de caída mínimo para los usuarios

2.2.2 Múltiples Data Centers

- Servidores distribuidos geográficamente (España, Estados Unidos, Inglaterra)
- Tolerancia a desastres mejorada
- Capacidad de desvío de tráfico entre centros

2.3 Sistema Distribuido

En un sistema distribuido, todos los servidores (activos e inactivos) incluyen:

- **Servidor de nombres:** Traduce IPs a nombres reconocibles
- **Servidor de índices:** Se conecta a la capa de persistencia (base de datos)

Características del failover:

- El servidor en standby mantiene el servidor de índices en standby
- Al activarse, toma la misma ubicación del servidor caído
- Todo el proceso es gestionado automáticamente por el servidor de nombres

2.4 Configuración de Nodos Maestros

- Se pueden definir hasta **tres servidores de nodos maestros**
- Durante el inicio, un servidor es elegido como **nodo maestro activo**
- El nodo maestro activo asigna volúmenes para cada servidor de índices
- Los servidores en espera no reciben volumen inicialmente

2.5 Gestión de Errores

Error en Servidor de Nombres Maestro

- Otro servidor maestro restante toma automáticamente su lugar

Error en Servidor de Índices

- El servidor de nombres maestro detecta el fallo
- Ejecuta el cambio por error (failover)
- Asigna el volumen del servidor fallido al servidor en espera

2.6 Replicación y Rendimiento

- **Duplicación:** Se ofrece a nivel del sistema de almacenamiento
- **Impacto en rendimiento:** Esperado cuando el reflejo síncrono está activado
- **Factores externos que afectan:** Distancia, conexión entre centros de datos
- **Punto crítico:** Escritura sincrónica del registro

2.7 Proceso de Recuperación ante Desastres

En caso de emergencia:

1. Centro de datos principal no disponible
2. Se inicia proceso de adquisición (manual o automatizado)
3. El proceso finaliza oficialmente el reflejo
4. Se montan discos al software
5. Se ponen en marcha las instancias HANA instaladas

Condiciones ideales:

- Nombres de host e instancia idénticos en ambos lados del clúster
- No se requieren pasos adicionales con HDB
- Posibilidad de ejecutar instancias de desarrollo/calidad en hardware secundario

---

3. CARACTERÍSTICAS DE SEGURIDAD

SAP HANA proporciona características cruciales para garantizar la seguridad de:

- La base de datos

- Aplicaciones del motor XS (clásica y avanzada)
- Objetos de desarrollo en repositorios de tiempo de diseño

3.1 Autenticación

Definición: Proceso de verificación de permisos para conectarse a la base de datos HANA.

Métodos de Autenticación

Sistema básico:

- Usuario y contraseña
- Verificación simple de credenciales

Sistema avanzado - Kerberos:

- Protocolo de autenticación creado por MIT
- Permite demostración mutua de identidad en redes inseguras
- Modelo cliente-servidor con autenticación mutua
- Protección contra eavesdropping y ataques de replay

Componentes de Kerberos:

- **KDC (Key Distribution Center):** Centro de distribución de claves
  - **AS (Authentication Server):** Servidor de autenticación
  - **TGS (Ticket Granting Server):** Servidor emisor de tickets
- **Base de datos de claves secretas**
- **Tickets para verificación de identidad**
- **Claves de sesión para cifrar comunicaciones**

Funcionamiento de Kerberos:

1. Cliente se autentica contra Authentication Server
2. Demuestra al Ticket Granting Server que está autorizado
3. Recibe ticket de servicio
4. Demuestra al Service Server que ha sido aprobado

3.2 Usuarios y Roles

Gestión de Privilegios

Usuarios individuales:

- Asignación directa de privilegios específicos
- Acceso de lectura/escritura a tablas
- Permisos de ejecución sobre procedimientos

Sistema de Roles:

- **Definición:** Conjunto de privilegios agrupados
- **Ventaja:** Evita asignación manual repetitiva
- **Flexibilidad:** Permite personalización adicional por usuario

Metodología de Asignación

Proceso recomendado:

1. **Crear roles por perfil:** Desarrollador, Modelador, Usuario normal
2. **Asignar rol base:** Cubre necesidades comunes del perfil
3. **Añadir privilegios específicos:** Necesidades particulares del usuario

Ejemplos de perfiles:

- **Desarrollador:** Acceso a tablas + permisos de ejecución + creación de objetos
- **Modelador:** Permisos de creación en esquemas + consulta + permisos específicos

Filosofía de Seguridad

Principio de menor privilegio:

- Dar al usuario **los mínimos privilegios necesarios**
- Preferible privilegios insuficientes que excesivos
- Solicitud progresiva de privilegios adicionales

Ventajas del enfoque restrictivo:

- **Seguridad:** Previene accesos no autorizados
- **Control de daños:** Limita impacto de errores o malicia
- **Gestión ordenada:** Proceso controlado de expansión de privilegios

3.3 Autorización

Diferencia clave: No confundir con autenticación

- **Autenticación:** Credenciales de usuario
- **Autorización:** Privilegios analíticos sobre objetos

Privilegios Analíticos

Funcionalidad:

- Objetos aplicables sobre tablas o vistas
- **Filtrado dinámico** según privilegios del usuario
- **Resultado variable:** Diferentes usuarios ven diferentes datos de la misma tabla

Aplicación práctica:

- Sistema de filtrado inteligente
- Acceso contextual a la información
- Seguridad a nivel de datos

3.4 Cifrado (Criptografía)

Objetivo Principal

Mantener la información segura asegurando que solo usuarios autorizados y correctamente logueados puedan leer la información del sistema.

Evolución Histórica

Antecedente histórico - Máquina Enigma:

- Utilizada en la Segunda Guerra Mundial
- Cambio de posición de letras
- Necesidad de clave para descifrar mensajes
- Base de la encriptación moderna

Aplicación Moderna

Características actuales:

- **Complejidad superior:** Extremos muy superiores a métodos históricos
- **Resistencia:** Prácticamente indescifrable a corto plazo
- **Protección ante secuestros de datos:** Información inutilizable sin claves

Limitaciones teóricas:

- Con suficiente potencia computacional y tiempo, todo es descifrable
- Tiempos de descifrado no manejables prácticamente

3.5 Audit Logging (Registros de Auditoría)

Definición

Sistema de trazabilidad completa que registra todas las actividades del sistema.

Capacidades de Seguimiento

Accesos monitorizados:

- Recursos de datos
- Funciones y procedimientos
- Administración de usuarios y roles
- Parámetros de seguridad
- Reglas del sistema

Resultado:

- **Registro completo:** Traza detallada de todas las actividades
- **Auditoría integral:** Seguimiento de cambios y accesos
- **Cumplimiento:** Soporte para requisitos de auditoría

---

4. HERRAMIENTAS DE ADMINISTRACIÓN

4.1 SAP HANA 1.0

- **HANA Studio:** Interfaz única para todas las tareas
- **Funcionalidades integradas:** Desarrollo, modelado, administración
- **Ventaja:** Todo centralizado en una herramienta

4.2 SAP HANA 2.0

Opciones Disponibles

- **Cockpit:** Entorno web principal
- **HANA Studio:** Mantenido para ciertas tareas específicas

Evolución y Recomendaciones

- **Transición gradual:** Algunas tareas inicialmente solo en HANA Studio
- **Recomendación SAP:** Usar Cockpit siempre que sea posible
- **Futuro:** Cockpit como único enfoque de administración esperado

---

5. CONCLUSIONES

Esta unidad proporciona las bases teóricas fundamentales para la gestión de SAP HANA. A partir del siguiente módulo, el curso se enfocará en aspectos más prácticos, manteniendo la teoría necesaria para la comprensión de conceptos pero incorporando ejercicios prácticos en cada unidad.

Puntos Clave para Recordar

1. **Alta disponibilidad** es crítica para sistemas empresariales
2. **Seguridad multicapa** protege datos y accesos
3. **Gestión de privilegios** debe seguir el principio de menor acceso
4. **Herramientas modernas** evolucionan hacia interfaces web
5. **Teoría y práctica** se combinan para dominio completo de la tecnología

---

Fin del Video 4 - Seguridad y Alta Disponibilidad en SAP HANA