

ADMINISTRACION DE BASE DE DATOS

6. Monitoreo y auditoria

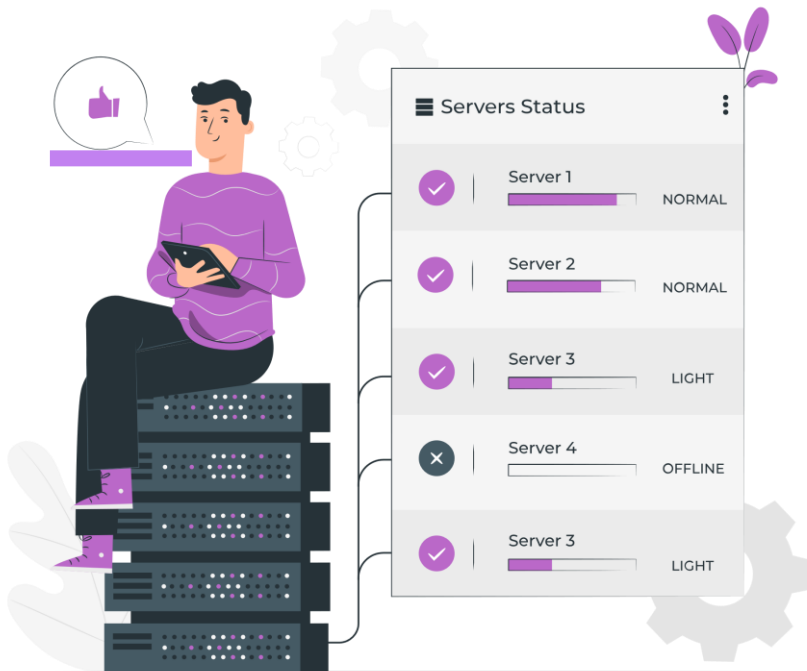
6. Monitoreo y auditoria

TEMAS

- 6.1 Monitoreo
- 6.2 Auditoría

Competnecia

- Implementa la auditoría de base de datos para controlar la seguridad de la información.
- Implementa el monitoreo del rendimiento de un SGBD para verificar su funcionamiento.



6.1 Monitoreo

El monitoreo de la actividad en bases de datos está evolucionando hacia la auditoría y la protección de bases de datos

6.1 Monitoreo

Monitoreo general de un DBMS

- Monitoreo de espacio en disco.
- Monitoreo de logs.
- Monitoreo de Memoria compartida
- Monitoreo de Base de Datos
- Monitoreo de modos de operación.
- Monitoreo de espacios espejados.

El monitoreo de la actividad en bases de datos está evolucionando hacia la auditoría y la protección de bases de datos

6.1 Monitoreo

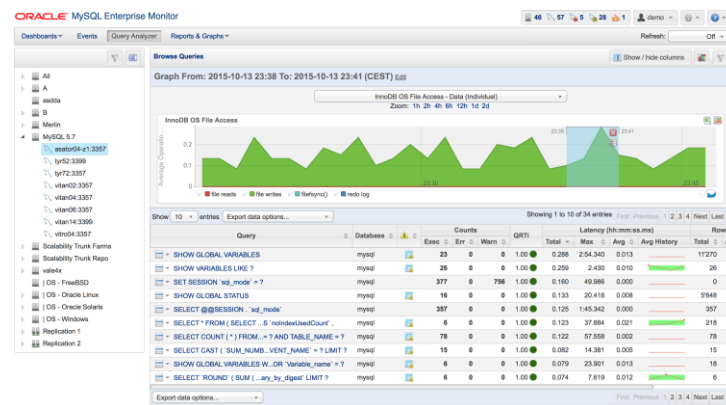
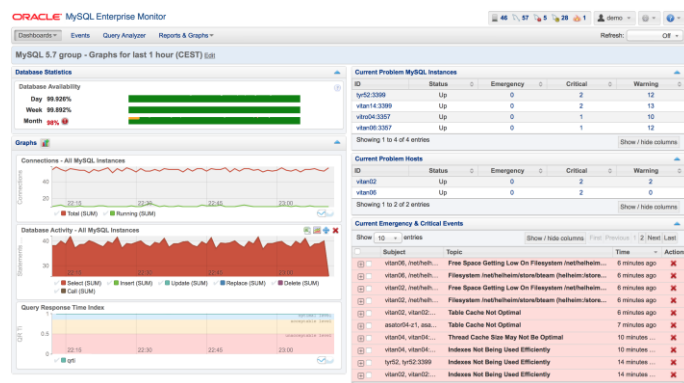
La teoría de la planificación del desarrollo define el seguimiento o monitoreo como un ejercicio destinado a identificar de manera sistemática la calidad del desempeño de un sistema, subsistema o proceso a efecto de introducir los ajustes o cambios pertinentes y oportunos para el logro de sus resultados y efectos en el entorno.



6.1 Monitoreo

El MySQL Enterprise Monitor

El MySQL Enterprise Monitor descubre la topología de replicación de MySQL y le da visibilidad sobre el rendimiento, la disponibilidad y la salud de todos los Maestros de MySQL y de esclavos. La nueva replicación del tablero de instrumentos muestra la instrumentación disponible dentro de MySQL 5.7 y la vista de topología muestra la configuración actual de los grupos de replicación, lo que le permite ver rápidamente el estado de cada nodo y cada subsistema de replicación. Tanto si utiliza una jerarquía de una sola fuente de árbol, la replicación circular, o un complejo de varios niveles, la jerarquía de múltiples fuentes, la vista de topología muestra cómo su grupo de replicación está replicando actualmente.



6.1 Monitoreo

Monitor automático de diagnóstico de base de datos (ADDM)

Es una de las herramientas más interesantes que presenta Oracle con respecto al rendimiento de la base de datos. El ADDM realiza un análisis del sistema, identifica los posibles problemas y sus causas potenciales, y por último plantea recomendaciones para solucionarlos.

La información que analiza el ADDM es:

- Cuellos de botella en la CPU
- Gestión ineficiente de conexiones
- Bloqueos
- Operaciones de entrada/salida
- Tamaño de las estructuras de memoria
- Carga de sentencias sql.
- Tiempo de ejecución de procedimientos PL/SQL y Java

Es muy fácil de generar. Tan solo tendremos que seleccionar el botón “ejecutar ADDM ahora” de la pestaña “Rendimiento”.



6.1 Monitoreo

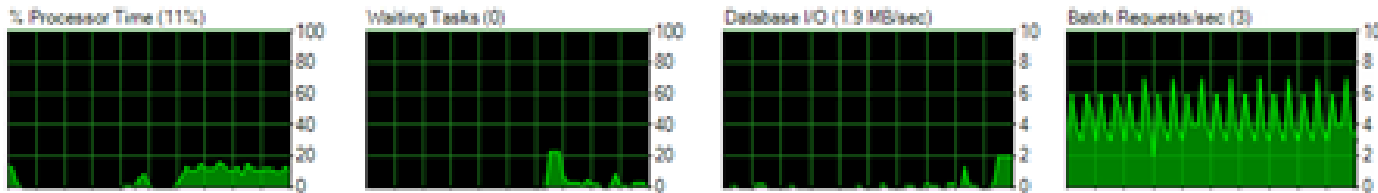
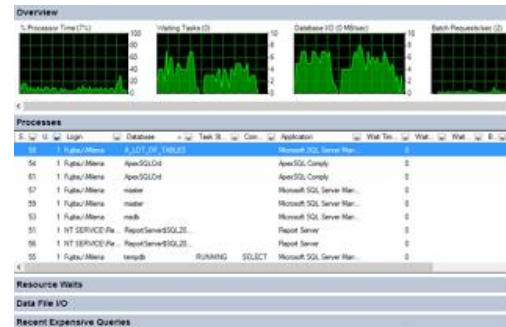
SQL Server provee dos características integradas de monitoreo: Activity Monitor y Data Collector.

Activity Monitor

Activity Monitor rastrea solo las métricas de SQL Server más importantes. Para obtenerlas, ejecuta consultas contra su instancia SQL Server anfitrión cada 10 segundos. EL desempeño es monitoreado sólo mientras Activity Monitor está abierto, lo que lo hace una solución ligera con casi ningún costo extra.

Las métricas son mostradas en 5 paneles colapsables: **Overview**, **Processes**, **Resource Waits**, **Data File I/O**, y **Recent Expensive Queries**.

El panel **Overview** muestra el porcentaje de tiempo del procesador, número de tareas en espera, operaciones I/O en la base de datos en MB/seg, y el número de requerimientos batch.



6.1 Monitoreo

Data Collector

Data Collector es otra característica de monitoreo y optimización integrada en SQL Server Management Studio. Colecta métricas de desempeño de instancias SQL Server, las guarda en un repositorio local de tal manera que puedan ser usadas para un análisis posterior. Usa Data Warehousing, SQL Server Agent e Integration Services.







A diferencia de Activity Monitor, Data Collector le permite especificar las métricas que monitoreará. Ofrece tres conjuntos integrados de métricas (colectores de datos) con las métricas de monitoreo de desempeño más importantes y comunes. Para monitorear métricas de desempeño adicionales, colectores de datos personalizados pueden ser creados vía código T-SQL o API.

Disk Usage Collection Set

on FUJITSU\SQL2014 at 5/11/2014 12:38:06 PM



This report provides an overview of the disk space used for all databases on the server and growth trends for the data file and the log file for each database for the last 3 collection points between 5/11/2014 12:30:37 PM and 5/11/2014 12:37:16 PM.

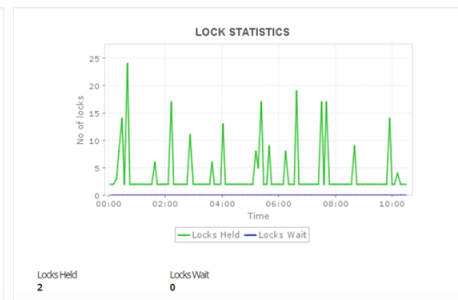
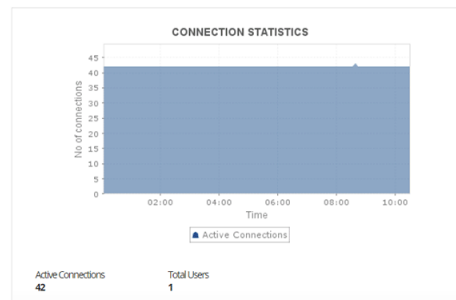
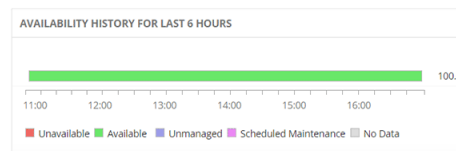
Database Name	Database				Log			
	Start Size (MB)	Trend	Current Size (MB)	Average Growth (MB/Day)	Start Size (MB)	Trend	Current Size (MB)	Average Growth (MB/Day)
A LOT OF TABLES	18.19		18.19	0	0.81		0.81	0
AdventureWorks2014	205.00		205.00	0	1.00		1.00	0
ApexSQLMonitor	111.19		112.19	1	24.13		24.13	0
master	4.00		4.00	0	2.00		2.00	0
MDW_Host	100.00		100.00	0	10.00		10.00	0

6.1 Monitoreo

El monitoreo de PostgreSQL también necesita rastrear cómo la base de datos usa la CPU, el espacio de disco, la memoria, el ancho de banda y otros recursos del sistema comunes para asegurar que puede responder a consultas de lectura y escritura de manera eficiente.

El monitoreo de Applications Manager PostgreSQL rastrea algunos parámetros clave de rendimiento, tales como:

- Estadísticas de conexión
- Estadísticas de bloqueo
- Estadísticas de búfer
- Detalles de uso del disco
- Detalles de escaneo de índice
- Estadísticas de consulta
- Detalles de la transacción
- Detalles del escaneo de la tabla





6.2 Auditoria

6.2 Auditoría

La auditoría de base de datos, es un proceso implementado por los auditores de sistemas con el fin de auditar los accesos a los datos, por lo general siguiendo bien una metodología basada en un checklist que contempla los puntos que se quieren comprobar o mediante la evaluación de riesgos potenciales.

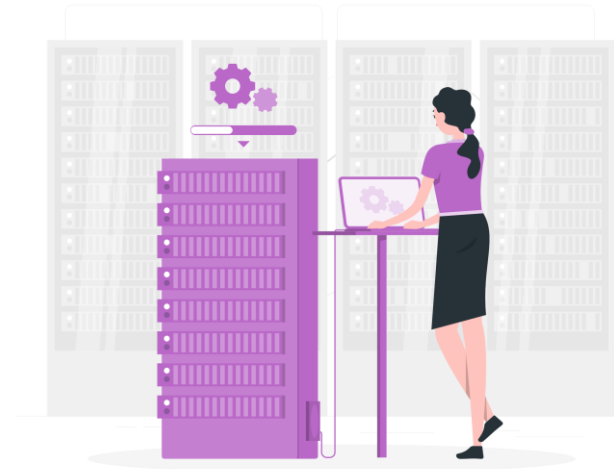
En concreto, se realiza un examen de los accesos a los datos almacenados en las bases de datos con el fin de poder medir, monitorear y tener constancia de los accesos a la información almacenada en las mismas. Si bien el objetivo puede variar en función de la casuística, en todos los casos el fin último persigue, de uno u otro modo, la seguridad corporativa.

Una auditoría de base de datos, por lo tanto, facilita herramientas eficaces para conocer de forma exacta cuál es la relación de los usuarios a la hora de acceder a las bases de datos, incluyendo las actuaciones que deriven en una generación, modificación o eliminación de datos.

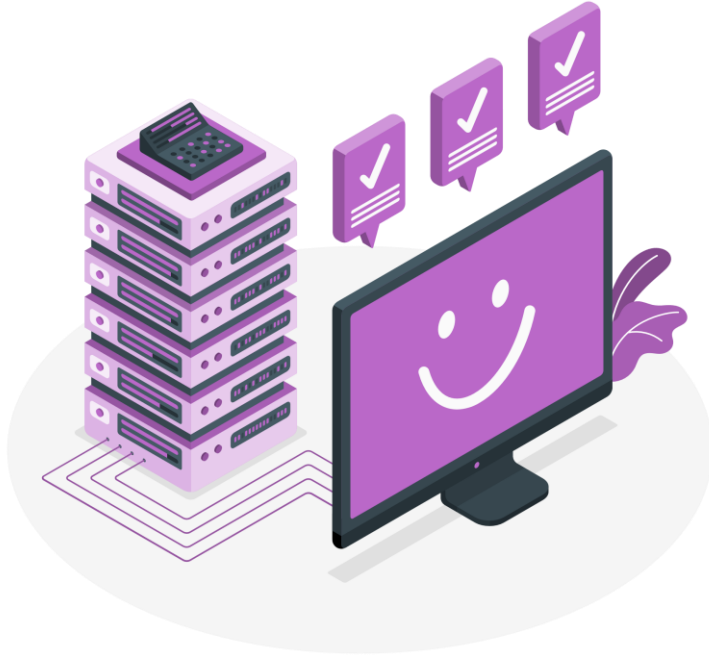
6.2 Auditoría

Los tópicos que se incluyen tienen que ver con la exactitud, consistencia y confiabilidad de la información y con la privacidad y confidencialidad de los datos. Las Bases de Datos tienen dentro de sus características elementos que pueden ser utilizados para garantizar la calidad de la información almacenada y procesada:

- ✓ Claves primarias;
- ✓ Dominios de los atributos;
- ✓ Reglas de integridad;
- ✓ Vistas;
- ✓ Perfiles de usuario y acceso a la BD;
- ✓ Auditoría;
- ✓ Criptografía;
- ✓ Disparadores o triggers.



6.2 Auditoría



OBJETIVOS DE LA AUDITORIA

- Investigar actividades dudosas sobre la BD
- Recopilar información acerca de actividades específicas de la BD
- Recopilar estadísticas sobre qué tablas se están actualizando, cuantas E/S lógicas se realizan y cuántos usuarios se conectan de forma simultánea en las horas de máxima actividad La auditoría se puede realizar por sesión ó por acceso

6.2 Auditoría

GESTIONAR LA AUDITORIA

Se debe definir lo que se desea auditar:

- ✓ Usuarios, sentencias u objetos
- ✓ Ejecuciones de sentencias correctas, ejecuciones de sentencias incorrectas ó ambas Se debe gestionar los registros de la auditoría:
 - Controlar el aumento de los registros de la auditoría
 - Proteger los registros de auditoría de un acceso no autorizado

6.2 Auditoría

En esencia, un registro de auditoría es un archivo o base de datos especial en el que el sistema lleva automáticamente la cuenta de todas las operaciones realizadas por los usuarios sobre los datos normales. En algunos sistemas el registro de auditoría puede estar integrado físicamente con la bitácora de recuperación mientras que en otros, los dos pueden ser distintos pero los usuarios deben —de cualquier forma— tener la posibilidad de consultar el registro de auditoría usando su lenguaje de consulta normal (por supuesto, siempre y cuando tengan autorización). Un registro de auditoría típico podría contener la siguiente información:

- Petición (texto de origen)
- Terminal desde la que se llamó a la operación
- Usuario que llamó a la operación
- Fecha y hora de la operación
- Valores, tuplas, atributos afectados
- Valores antiguos Valores nuevos