Supervisión del rendimiento del sistema (Implantación de sistemas operativos)

Herramientas de monitorización en tiempo real

Para no tener que recurrir a la restauración de copias de seguridad o reparación del sistema operativo, hay que detectar los problemas antes de que ocurran.

Las herramientas de monitorización en tiempo real son sistemas diseñados para recopilar, analizar y presentar datos operativos y de rendimiento de sistemas, redes y aplicaciones en tiempo real. Estas herramientas permiten a los administradores de sistemas y equipos de operaciones supervisar el estado y el rendimiento de los activos de TI de manera continua y proactiva, lo que facilita la detección temprana de problemas y la toma de medidas correctivas antes de que afecten negativamente a los usuarios finales. Las herramientas de monitorización en tiempo real pueden incluir una variedad de características y funcionalidades, como:

1. **Recopilación de datos**: Las herramientas de monitorización recopilan datos operativos y de rendimiento de una amplia gama de fuentes, incluyendo sistemas informáticos, dispositivos de red, bases de datos, aplicaciones y servicios en la nube. Estos datos pueden incluir información sobre el uso del sistema, la utilización de recursos, el tráfico de red, la latencia, los errores y las alertas generadas por los sistemas y aplicaciones.
2. **Análisis y procesamiento de datos**: Una vez recopilados,

los datos son analizados y procesados para identificar patrones, tendencias y anomalías significativas. Esto puede implicar el uso de algoritmos de análisis avanzados para detectar problemas potenciales o comportamientos anómalos, así como la aplicación de reglas y umbrales predefinidos para generar alertas cuando se detectan condiciones fuera de lo normal.

3. **Presentación de datos**: Los resultados del análisis se presentan en forma de paneles de control, gráficos, informes y alertas visuales que permiten a los usuarios visualizar y comprender fácilmente el estado y el rendimiento de los sistemas y aplicaciones en tiempo real. Esto facilita la identificación rápida de problemas y la toma de decisiones informadas sobre las acciones correctivas necesarias.
4. **Notificaciones y alertas**: Las herramientas de monitorización en tiempo real pueden generar notificaciones y alertas automáticas cuando se detectan problemas o condiciones anómalas que requieren atención inmediata. Estas alertas pueden enviarse por correo electrónico, mensajes de texto, mensajes instantáneos u otros canales de comunicación, y pueden dirigirse a usuarios específicos o grupos de trabajo según sea necesario.
5. **Integración con otros sistemas**: Las herramientas de monitorización en tiempo real suelen ser compatibles con una variedad de sistemas y tecnologías, lo que permite su integración con otros sistemas de gestión de TI, herramientas de ticketing, sistemas de automatización y orquestación, y otros sistemas empresariales. Esto facilita la colaboración entre equipos y la automatización de procesos de respuesta a incidentes.

Herramientas de monitorización continuada

La monitorización continua es el proceso formal de revisión y evaluación de la efectividad del mecanismos de rendimiento que hay en un sistema operativo.

Las herramientas de monitorización continuada son sistemas diseñados para supervisar y analizar de manera constante el estado y el rendimiento de los sistemas, redes y aplicaciones de una organización. A diferencia de las herramientas de monitorización en tiempo real, que se centran en proporcionar visibilidad inmediata sobre el estado actual de los activos de TI, las herramientas de monitorización continuada están diseñadas para realizar un seguimiento a largo plazo y recopilar datos históricos para análisis retrospectivos y tendenciales. Aquí se detallan algunas características y funcionalidades clave de estas herramientas:

1. **Recopilación y almacenamiento de datos históricos**: Las herramientas de monitorización continuada recopilan datos operativos y de rendimiento de forma continua a lo largo del tiempo y los almacenan en bases de datos o repositorios de datos históricos. Esto permite a los administradores de sistemas y analistas acceder a datos históricos para realizar análisis retrospectivos y tendenciales.
2. **Análisis retrospectivo**: Los datos recopilados por las herramientas de monitorización continuada pueden ser analizados retrospectivamente para identificar patrones, tendencias y problemas recurrentes que puedan haber pasado desapercibidos en el pasado. Esto puede ayudar a detectar problemas crónicos o de larga duración que puedan requerir atención o resolución.
3. **Generación de informes históricos**: Las herramientas de monitorización continuada pueden generar informes

históricos que resumen el rendimiento y la disponibilidad de los sistemas y aplicaciones a lo largo del tiempo. Estos informes pueden ser útiles para la evaluación del rendimiento, la planificación de la capacidad, la evaluación del cumplimiento de los SLA (acuerdos de nivel de servicio) y la identificación de áreas de mejora.
4. **Análisis de tendencias**: Las herramientas de monitorización continuada pueden identificar tendencias a lo largo del tiempo, lo que puede ayudar a prever problemas potenciales antes de que ocurran. Por ejemplo, un aumento gradual en el uso del CPU o en el tráfico de red puede indicar la necesidad de realizar mejoras en la infraestructura o en la capacidad de los recursos.
5. **Alertas basadas en tendencias**: Además de generar alertas en tiempo real, algunas herramientas de monitorización continuada pueden generar alertas basadas en tendencias, que se activan cuando se detectan cambios significativos en el rendimiento o el comportamiento de los sistemas y aplicaciones con el tiempo. Estas alertas pueden ayudar a los equipos de operaciones a anticipar y mitigar problemas potenciales antes de que afecten negativamente a los usuarios finales.

Herramientas de análisis del rendimiento

Los sistemas operativos ofrecen herramientas para analizar el rendimiento del sistema operativo.

En PowerShell se puede gestionar el rendimiento mediante el Monitor de rendimiento, que analiza el rendimiento del sistema operativo. Tiene control de la CPU, el disco, la red y la memoria. Se puede monitorizar el rendimiento en tiempo real o de forma continuada.

En Linux también existen herramientas para realizar la monitorización del sistema.

Registros de sucesos

El control de lo que ocurre en el sistema operativo se lleva a cabo mediante los Eventos del sistema, que son acontecimientos que ocurren en el sistema operativo.

Ejemplos

Almacenar información en un fichero (prueba de concepto)

- https://www.jesusninoc.com/05/05/ejercicios-de-powershell-crear-una-funcion-que-valide-un-usuario-leyendo-el-nombre-y-el-password-en-hash-correcto-de-un-fichero-en-el-caso-de-que-el-login-sea-correcto-se-almacena-la-palabra-cor/

List event log

- https://www.jesusninoc.com/2018/03/27/list-event-log

Escribir y ver un evento en el registro de eventos de aplicación

- https://www.jesusninoc.com/2018/05/04/escribir-y-ver-un-evento-en-el-registro-de-eventos-de-aplicacion/

Almacenar información convertida a byte en un evento en el registro de eventos de aplicación

- https://www.jesusninoc.com/2018/05/05/almacenar-informacion-convertida-a-byte-en-un-evento-en-el-registro-de-eventos-de-aplicacion/

Ejecutar la información que se encuentra en un evento en el registro de eventos de aplicación

- https://www.jesusninoc.com/2018/05/06/ejecutar-la-informacion-que-se-encuentra-en-un-evento-en-el-registro-de-eventos-de-aplicacion/

Monitorización de sucesos

El visor de eventos en Windows permite ver y examinar eventos que ocurren en el equipo. Windows tiene definidos tres tipos de registros de eventos o sucesos:

- De las aplicaciones. Son sucesos relacionados con la actividad de una determinada aplicación, los programadores pueden definir estos sucesos para recoger información acerca de la dinámica de las aplicaciones (errores, avisos, etc.).
- De seguridad. Son sucesos de auditoría definidos y activados previamente, para ello hay que activar las directivas de auditoría en la utilidad de Configuración de seguridad local.
- De sistema. Son sucesos relacionados con la actividad del sistema operativo.

En Linux también hay registros en donde se muestra información sobre el funcionamiento del sistema operativo o de las aplicaciones.

Gestión de aplicaciones, procesos y

subprocesos

La gestión de aplicaciones, procesos y subprocesos es una parte fundamental de la administración de sistemas y la optimización del rendimiento en entornos de TI. Aquí hay algunos aspectos clave de este tema:

1. **Gestión de Aplicaciones**: Consiste en supervisar, mantener y optimizar el funcionamiento de las aplicaciones informáticas utilizadas en una organización. Esto incluye la instalación, actualización, configuración y eliminación de aplicaciones según sea necesario. La gestión de aplicaciones también implica garantizar que las aplicaciones funcionen correctamente y cumplan con los requisitos de rendimiento y seguridad de la organización.
2. **Gestión de Procesos**: Se refiere al control y la administración de los procesos en ejecución en un sistema operativo. Esto incluye la asignación de recursos, la priorización de procesos, el monitoreo del rendimiento y la resolución de problemas relacionados con la ejecución de procesos. La gestión de procesos garantiza que los recursos del sistema se utilicen de manera eficiente y que los procesos críticos se ejecuten sin problemas.
3. **Gestión de Subprocesos**: Los subprocesos son unidades más pequeñas de ejecución dentro de un proceso más grande. La gestión de subprocesos implica controlar la creación, finalización y sincronización de subprocesos para garantizar un funcionamiento coherente y eficiente del proceso principal. Esto incluye la asignación de recursos, la gestión de la concurrencia y la prevención de condiciones de carrera y bloqueo.
4. **Monitorización y Optimización**: La monitorización continua del rendimiento de las aplicaciones, procesos y

subprocesos es esencial para identificar cuellos de botella, problemas de rendimiento y posibles mejoras. Esto puede implicar el uso de herramientas de monitorización en tiempo real y continuada para recopilar datos sobre el uso de recursos, la actividad del sistema y el comportamiento de las aplicaciones.
5. **Automatización de Tareas**: La automatización de tareas relacionadas con la gestión de aplicaciones, procesos y subprocesos puede ayudar a mejorar la eficiencia operativa y reducir la carga de trabajo manual. Esto puede incluir la implementación de políticas de gestión automatizada, la configuración de reglas de alerta y la creación de scripts y flujos de trabajo automatizados para tareas comunes de administración y mantenimiento.

Más información

- https://www.jesusninoc.com/07/07/7-gestion-de-procesos-en-powershell/

Monitorización de aplicaciones y procesos

La monitorización de aplicaciones y procesos es una práctica esencial en la gestión de sistemas de TI, que permite supervisar y optimizar el rendimiento de las aplicaciones y los procesos en ejecución en un entorno informático. Aquí se destacan algunos aspectos clave de esta práctica:

1. **Supervisión del rendimiento**: La monitorización de

aplicaciones y procesos implica recopilar datos sobre el rendimiento de las aplicaciones y los procesos en ejecución. Esto incluye métricas como el uso de CPU, memoria, almacenamiento, redes y otros recursos del sistema.

2. **Detección de problemas**: La monitorización permite detectar problemas potenciales en las aplicaciones y los procesos, como cuellos de botella, tiempos de respuesta lentos, errores de aplicación y problemas de rendimiento. Identificar estos problemas de manera temprana es crucial para minimizar el impacto en el usuario final y resolverlos antes de que afecten negativamente a la operación del sistema.
3. **Generación de alertas**: Las herramientas de monitorización pueden configurarse para generar alertas cuando se detecten problemas o condiciones anómalas en las aplicaciones y procesos. Estas alertas pueden enviarse a los administradores del sistema o a equipos de operaciones para que tomen medidas correctivas de manera oportuna.
4. **Análisis de tendencias**: La monitorización de aplicaciones y procesos también permite realizar un análisis de tendencias a lo largo del tiempo. Al recopilar datos históricos sobre el rendimiento de las aplicaciones y los procesos, es posible identificar patrones y tendencias que pueden indicar cambios en el comportamiento o la demanda de recursos del sistema.
5. **Optimización del rendimiento**: Utilizando los datos recopilados a través de la monitorización, los administradores de sistemas pueden identificar áreas de mejora en el rendimiento de las aplicaciones y los procesos. Esto puede implicar la optimización de la configuración, la asignación de recursos adicionales o la implementación de ajustes de software para mejorar la eficiencia y la capacidad de respuesta del sistema.
6. **Planificación de capacidad**: La monitorización de aplicaciones y procesos proporciona información valiosa

para la planificación de la capacidad de los sistemas de TI. Al analizar las tendencias de uso de recursos y el crecimiento de la carga de trabajo, los administradores pueden anticipar las necesidades futuras de recursos y tomar decisiones informadas sobre la escalabilidad y el dimensionamiento de los sistemas.

Más información

- https://www.jesusninoc.com/07/07/7-gestion-de-procesos-en-powershell/
