**Diagnóstico y Resolución del Incidente ("High swap space usage")**

La alerta "Windows: High swap space usage (less than 20% free)" indica que el sistema operativo está haciendo un uso intensivo del archivo de paginación (Pagefile.sys), lo cual ocurre cuando la memoria RAM física disponible es insuficiente para la carga de trabajo. Esto degrada drásticamente el rendimiento del servidor.

**Pasos para el Diagnóstico:**

1. **Confirmación y Evaluación del Impacto:**
   * **Verificar en el Sistema de Monitoreo:** Confirmar que la alerta es persistente y ver la tendencia del uso de swap. ¿Es un pico puntual o un consumo sostenido y creciente?
   * **Estado del Servidor:** Intentar conectarse al servidor vía RDP o consola. ¿Está el servidor lento, no responde o está casi colgado? Esto indicará la severidad del problema.
   * **Impacto en la Aplicación:** Verificar si los usuarios están reportando lentitud, errores o indisponibilidad de la aplicación/servicios alojados en el servidor.
2. **Identificación del Consumidor de Memoria (en el servidor Windows):**
   * **Administrador de Tareas (Task Manager):**
     + Abrir el Administrador de Tareas (Ctrl+Shift+Esc o Ctrl+Alt+Del -> Administrador de Tareas).
     + Ir a la pestaña **"Rendimiento" (Performance)**, y luego a **"Memoria"**. Aquí se puede ver el uso de la memoria RAM y el "Tamaño del archivo de paginación" (Page file).
     + Ir a la pestaña **"Procesos" (Processes)** o **"Detalles" (Details)**. Ordenar por la columna **"Memoria (conjunto de trabajo)" (Memory (working set))** o **"Memoria (conjunto de trabajo privado)" (Memory (Private Working Set))**. Esto revelará qué proceso(s) están consumiendo la mayor cantidad de memoria RAM.
     + Identificar el proceso principal (ej., w3wp.exe para IIS Application Pools, sqlservr.exe para SQL Server, un ejecutable de tu aplicación, etc.).
   * **Monitor de Recursos (Resource Monitor):**
     + Acceder desde el Administrador de Tareas (pestaña "Rendimiento" -> "Abrir Monitor de Recursos").
     + Ir a la pestaña **"Memoria"**. Ofrece una vista más detallada del uso de memoria física, los procesos con errores de página (Hard Faults/sec), y la cantidad de memoria usada por el Pagefile. Esto ayuda a confirmar si el problema es la falta de RAM física.
   * **Monitor de Rendimiento (Performance Monitor - perfmon.msc):**
     + Permite agregar contadores para monitorear métricas específicas a lo largo del tiempo.
     + **Contadores clave:**
       - \Memory\Pages/sec: Indica la tasa de paginación de datos de memoria hacia y desde el disco. Un valor alto y sostenido es un claro signo de agotamiento de RAM.
       - \Paging File(\*)\% Usage: Muestra el porcentaje de uso de cada archivo de paginación.
       - \Process(<nombre\_proceso>)\Working Set: Muestra el uso actual de memoria RAM por un proceso específico.
       - \Process(<nombre\_proceso>)\Private Bytes: Muestra la memoria privada asignada a un proceso que no puede ser compartida con otros procesos.
   * **Visor de Eventos (Event Viewer):**
     + Revisar los logs de "Sistema" y "Aplicación" en busca de errores o advertencias que precedan el aumento del uso de swap, como fallos de aplicaciones, errores de servicios, o advertencias de memoria insuficiente.
3. **Identificación de la Causa Raíz (Análisis):**
   * **Fuga de Memoria (Memory Leak):** La causa más común. Una aplicación o servicio no libera la memoria que ya no necesita, lo que lleva a un consumo creciente con el tiempo.
   * **Configuración Insuficiente de RAM:** El servidor simplemente no tiene suficiente RAM para la carga de trabajo actual o esperada (ej., durante picos de tráfico).
   * **Aplicación Ineficiente:** La aplicación está diseñada para consumir mucha memoria debido a consultas de base de datos ineficientes, manipulación de grandes conjuntos de datos en memoria, o algoritmos poco optimizados.
   * **Configuración de IIS/SQL Server:** Parámetros de configuración de IIS (ej., límites de reciclaje de Application Pool) o SQL Server (ej., max server memory) que no están optimizados o son demasiado permisivos.
   * **Malware/Procesos No Deseados:** Un proceso desconocido o malicioso que está consumiendo recursos de forma anómala.

**Pasos para la Resolución Inmediata (Mitigación):**

1. **Reiniciar el Proceso Ofensor:** Si un proceso específico (ej., un Pool de Aplicaciones de IIS, un servicio de la aplicación) se identifica como el principal consumidor, reiniciarlo puede liberar la memoria y aliviar la presión sobre el swap.
   * Desde PowerShell: Restart-WebAppPool -Name "MiAppPool" o Restart-Service -Name "MiServicio".
2. **Reiniciar el Servidor (Último Recurso):** Si el servidor está extremadamente lento o no responde, un reinicio completo puede ser necesario para liberar toda la memoria y el swap. Esto causará una interrupción del servicio, por lo que debe hacerse con precaución y en un momento de bajo impacto si es posible.
3. **Aumentar Temporalmente el Tamaño del Archivo de Paginación:** Si hay espacio en disco, se podría aumentar manualmente el tamaño del archivo de paginación como una medida temporal para evitar fallos completos del sistema, pero esto no resuelve la causa raíz de la escasez de RAM.

**8.2. Herramientas y Acciones para Mitigar y Prevenir la Recurrencia**

* **Herramientas para Mitigación (ya cubiertas en el diagnóstico):**
  1. Administrador de Tareas (Task Manager).
  2. Monitor de Recursos (Resource Monitor).
  3. Monitor de Rendimiento (Performance Monitor).
  4. Visor de Eventos (Event Viewer).
  5. Comandos PowerShell (Get-Process, Restart-Service, Restart-WebAppPool).
* **Acciones para Prevenir la Recurrencia (Soluciones a Largo Plazo):**
  1. **Optimización de Recursos (Escalabilidad):**
     + **Escalado Vertical (Aumentar RAM):** Si la carga de trabajo ha crecido o la aplicación tiene una necesidad legítima de más memoria, la solución más efectiva es aumentar la cantidad de RAM física en la VM.
     + **Escalado Horizontal (Añadir Servidores):** Si la aplicación lo permite (es stateless o puede distribuirse), añadir más instancias del servicio web en VMs separadas detrás de un balanceador de carga. Esto distribuye la carga de memoria entre varios servidores.
     + **Optimización de la Aplicación:** Colaborar con el equipo de desarrollo para:
       - Identificar y resolver **fugas de memoria** en el código.
       - Optimizar el uso de memoria de la aplicación, como la gestión de cachés, el tamaño de los pools de conexiones a base de datos, o el manejo de objetos grandes en memoria.
       - Mejorar la eficiencia de las consultas a la base de datos o el procesamiento de datos.
     + **Configuración de IIS Application Pools:**
       - Configurar el reciclaje programado del Application Pool (ej., cada 24 horas o después de un cierto umbral de solicitudes/memoria) para liberar memoria periódicamente y prevenir el crecimiento incontrolado.
       - Establecer límites de memoria suaves o duros para los Application Pools para evitar que consuman todos los recursos del servidor.
  2. **Monitoreo Proactivo y Alertas Mejoradas:**
     + **Métricas Granulares:** Monitorear métricas de memoria más detalladas a través de tu sistema de monitoreo (Zabbix, Prometheus con windows\_exporter, Dynatrace, New Relic) para detectar el aumento del consumo de RAM y el crecimiento del "Private Bytes" de procesos clave.
     + **Umbrales de Alerta Más Bajos:** Configurar alertas para el uso de RAM (ej., cuando supera el 70-80%) *antes* de que el sistema empiece a usar el swap de forma crítica.
     + **Alertas de Paginación:** Monitorear el contador \Memory\Pages/sec y generar alertas si supera un umbral sostenido, indicando paginación excesiva.
  3. **Configuración Óptima del Archivo de Paginación:**
     + **Tamaño Fijo:** Establecer el tamaño del archivo de paginación a un valor fijo y recomendado (ej., 1.5x a 2x la RAM física, o un valor específico basado en la carga de trabajo y las recomendaciones de Microsoft para SQL Server/Exchange si están presentes). Evitar que Windows lo gestione automáticamente si hay problemas de rendimiento.
     + **Ubicación:** Si es posible, colocar el archivo de paginación en un volumen de disco separado y rápido (ej., un disco SSD dedicado), diferente del disco del sistema operativo y de los discos de datos/logs de las aplicaciones, para evitar contención de I/O.
  4. **Análisis de Logs Centralizado:**
     + Centralizar los Event Logs de Windows y los logs de la aplicación en una solución de gestión de logs (ELK Stack, Splunk). Esto permite una búsqueda y correlación de eventos más eficiente para identificar patrones o errores que contribuyen al consumo de memoria.
  5. **Revisiones de Capacidad:**
     + Realizar revisiones periódicas de la capacidad del servidor y la aplicación para anticipar futuras necesidades de recursos antes de que se conviertan en incidentes.