**Diagnóstico y mitigación durante pico de tráfico con alta CPU y lentitud en Windows Server**

**Paso a Paso para Diagnóstico:**

**A. Verificación del sistema operativo (nivel de host):**

* **Administrador de tareas (Ctrl + Shift + Esc)**:
  + Revisar uso de CPU, memoria, disco y red.
  + Ver qué procesos están consumiendo más recursos.
* **Monitor de rendimiento (Performance Monitor - perfmon)**:
  + Agregar contadores: % Processor Time, Available MBytes, Disk Queue Length.
* **Visor de eventos (eventvwr.msc)**:
  + Verificar errores críticos o advertencias bajo **Registros de Windows > Sistema** o **Aplicación**.
* **PowerShell**:

**Get-Process | Sort-Object CPU -Descending | Select-Object -First 10**

* + Ver carga de CPU:

**Get-Counter '\Processor(\_Total)\% Processor Time'**

* **resmon** (Monitor de recursos): Visualización detallada de uso de CPU, memoria, disco y red.

**B. Verificación de red:**

* **ping nombre\_equipo\_o\_IP**: Conectividad básica.
* **tracert nombre\_equipo\_o\_IP**: Ruta a destino.
* **netstat -anob**: Ver puertos abiertos, procesos asociados y conexiones activas.
* **Get-NetTCPConnection** (PowerShell): Alternativa moderna a netstat.
* **Test-NetConnection -Port**:

**Test-NetConnection -ComputerName localhost -Port 8080**

**C. Verificación del servicio/aplicación:**

* **services.msc**: Verifica si el servicio de la aplicación está corriendo.
* **sc query nombre\_del\_servicio**: Estado desde línea de comandos.
* **Get-Service nombre\_del\_servicio**: Estado desde PowerShell.
* **iisreset /status** (si corre en IIS): Verifica el estado del servicio web.

**Mitigación Inmediata (si es crítico):**

1. **Reiniciar servicio** desde PowerShell:

**Restart-Service -Name "NombreDelServicio"**

1. **Reciclado del pool de aplicaciones** si es IIS:
   * IIS Manager → App Pools → Seleccionar → Reciclar.
2. **Limitar conexiones con reglas de firewall o modificar límites en IIS**.
3. **Aumentar recursos (vCPU, RAM)** si se trata de una máquina virtual.

**Causas raíz comunes en Windows Server:**

* Cuellos de botella en el Application Pool de IIS.
* Base de datos no optimizada o saturada.
* Log de eventos con errores frecuentes (OOM, falta de recursos).
* Servicio mal configurado o con memory leaks.

**Herramientas o comandos para validar el estado del servicio**

**Nivel de Red:**

* ping, tracert
* Test-NetConnection, netstat -anob
* **PowerShell**:

**Test-NetConnection -ComputerName localhost -Port 443**

**Nivel de Sistema Operativo:**

* taskmgr (Administrador de tareas)
* resmon (Monitor de recursos)
* perfmon (Monitor de rendimiento)
* eventvwr.msc (Visor de eventos)
* Get-Process, Get-Service, Get-Counter (PowerShell)

**Nivel de Aplicación:**

* Revisión de logs propios de la app (en carpetas tipo C:\ProgramData\..., o C:\inetpub\logs si es IIS).
* Pruebas con curl o navegadores hacia http://localhost o puerto específico.
* Validación de Application Pools en IIS.
* Revisar errores .NET (si aplica) desde el Visor de eventos → Aplicación.