SEQRITE EPP HEALTH MONITORING

Troubleshooting Resource Spikes on Windows Systems

Audience: EPP Customers

Applies to: Windows 10, Windows 11, Windows Server 2019, Windows Server 2022

Alert threshold: Resource utilization sustained above 70% triggers an EPP Health Monitoring alert

Overview

The Serqrite EPP Health Monitoring Service monitors CPU, memory, and disk utilization on managed Windows EPP Server. When utilization exceeds 70% for a sustained period, the service generates an alert. Prolonged resource spikes degrade application responsiveness, slow system performance, and can cause instability.

Use this guide to identify the source of a resource spike, apply targeted remediation, and put precautionary measures in place to prevent recurrence. All procedures use built-in Windows tools—no additional software downloads are required.

> ⚠ **Important** If you are unsure about any step, contact your IT support team or EPP administrator before proceeding.

1 High CPU Utilization

High CPU utilization (sustained above 70%) often results from resource-intensive processes, outdated drivers, or misconfigured applications.

1.1 Identify the Source

Task Manager

1. Press Ctrl+Shift+Esc to open Task Manager.
2. **Processes tab:** Select the CPU column header to sort processes from highest to lowest. Note any process consistently using more than 10–20% CPU (for example, chrome.exe).

Resource Monitor

3. **Open Resource Monitor:** Press Windows key+R, type `resmon`, and then press Enter.
4. On the CPU tab, expand the CPU section to view thread-level activity and associated services. Sort by Average CPU to identify top consumers.

Event Viewer

5. **Open Event Viewer:** Press Windows key+R, type `eventvwr.msc`, and then press Enter.
6. Go to Windows Logs > System.
7. In the Actions pane, select Filter Current Log, check Error and Warning, and then select OK.
8. Search for CPU-related entries in the Details pane.

1.2 Run PowerShell Diagnostics

Open PowerShell as administrator: right-click Start, and then select Windows PowerShell (Admin). Run the following commands one at a time.

List the top five CPU-consuming processes

PowerShell

```powershell
Get-Process | Sort-Object CPU -Descending | Select-Object Name, CPU, Id -First 5
```

This command returns process names, cumulative CPU time in seconds, and process IDs. A high CPU value indicates a long-running or intensive task.

Sample CPU utilization over time

PowerShell

```powershell
Get-Counter '\Processor(_Total)\% Processor Time' -SampleInterval 1 -MaxSamples 10
```

This command samples total processor utilization once per second for 10 samples. Averages consistently above 70% confirm the alert.

Identify services linked to high CPU

```powershell
Get-Service | Where-Object {$_.Status -eq 'Running'} |
  ForEach-Object { Get-Process -Name $_.Name -ErrorAction SilentlyContinue } |
  Sort-Object CPU -Descending |
  Select-Object ProcessName, CPU -First 5
```

This command maps running services to their associated processes and sorts by CPU impact.

1.3 Troubleshooting Steps

9. **End a non-essential process:** In Task Manager, on the Processes tab, right-click a high-usage, non-system process (avoid svchost.exe), and then select End Task. Confirm whether CPU usage decreases on the Performance tab.
10. **Update drivers and software:** Open Device Manager (Windows key+X > Device Manager). Right-click any device that shows a yellow exclamation mark, select Update driver > Search automatically. For Windows updates, go to Settings > Update & Security > Windows Update > Check for updates, and then install all available updates.
11. **Review startup items:** In Task Manager, select the Startup tab. Right-click unnecessary startup items and select Disable. Restart the computer to apply changes.

1.4 Remediation Actions

Issue	Action	Expected Outcome
Outdated software or drivers	Install updates via Windows Update or Device Manager. Restart after installation.	Prevents recurring spikes. Monitor for 24 hours in Resource Monitor.
Resource-intensive app (for example, browser with many tabs)	Close excess browser tabs; limit to 5–10. Restart the app if needed.	Reduces baseline CPU by 10–30%. Verify in Task Manager > Processes.
Windows Services overload	Open Services (services.msc). Right-click non-critical services (for example, Print Spooler if unused) > Properties > set Startup type to Manual > Apply > OK.	Frees 5–15% CPU during idle periods. Verify with Get-Service in PowerShell.

1.5 Precautionary Measures

- Enable automatic Windows updates: Settings > Update & Security > Windows Update > Advanced options > Receive updates for other Microsoft products.
- Lower process priority: In Task Manager > Details tab, right-click a non-critical process > Set priority > Below Normal.
- Monitor continuously: Run Get-Counter '\Processor(*)\% Processor Time' -Continuous in PowerShell (press Ctrl+C to stop).
- Reduce background throttling (advanced): In Registry Editor (regedit), navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Power\PowerThrottling. Create a DWORD value named PowerThrottlingOff and set it to 1. Restart the computer. Back up the registry before editing.

ⓘ **Note** Use the PowerThrottlingOff registry value with caution. Always export a registry backup (File > Export) before making changes.

2 High Memory (RAM) Utilization

Memory utilization sustained above 70% typically results from memory leaks, too many concurrent applications, or insufficient virtual memory configuration. When physical RAM is exhausted, Windows uses the pagefile (virtual memory), which significantly degrades performance.

2.1 Identify the Source

Task Manager

12. Press Ctrl+Shift+Esc to open Task Manager.
13. On the Processes tab, select the Memory column header to sort from highest to lowest. Note apps using more than 500 MB (for example, web browsers).

Resource Monitor

14. **Open Resource Monitor:** Press Windows key+R, type `resmon`, and then press Enter.
15. On the Memory tab, review the Committed, Working Set, and Standby lists. Sort by Working Set. A steadily increasing Private Bytes value indicates a potential memory leak.

Event Viewer

16. **Open Event Viewer:** Press Windows key+R, type `eventvwr.msc`, and then press Enter.
17. Go to Windows Logs > System. Filter for Error and Warning events. Search for the terms memory or pagefile in the Details pane.

2.2 Run PowerShell Diagnostics

Open PowerShell as administrator. Run the following commands.

List the top five memory-consuming processes

PowerShell

```PowerShell
Get-Process | Sort-Object WorkingSet -Descending | Select-Object Name, WorkingSet, Id -
First 5
```

WorkingSet values are in bytes. Divide by 1,048,576 to convert to MB.

Check total committed memory

PowerShell

```PowerShell
Get-Counter '\Memory\% Committed Bytes In Use'
```

A value above 70% confirms the alert condition.

Monitor a process for memory leaks

PowerShell

```
while($true) {
  Get-Process chrome | Select-Object Name, WorkingSet;
  Start-Sleep -Seconds 30
}
```

Replace chrome with the suspect process name. Press Ctrl+C to stop. A WorkingSet value that increases steadily over time indicates a memory leak.

2.3 Troubleshooting Steps

18. **Close unused applications:** In Task Manager, right-click high-memory processes and select End Task. Monitor the Performance > Memory graph for relief.
19. **Investigate for memory leaks:** Run the PowerShell loop above against the suspect process for 5–10 minutes.
20. **Verify virtual memory settings:** Right-click This PC > Properties > Advanced system settings > Performance > Settings > Advanced > Virtual memory > Change. Select Automatically manage paging file size for all drives. Select OK, and then restart the computer.
21. **Repair system files:** Open Command Prompt as administrator. Run `sfc /scannow`. The scan can take 10–20 minutes. Restart if repairs are found.

2.4 Remediation Actions

Issue	Action	Expected Outcome
Memory leak in an application	Close and restart the app. If the leak persists, update the app. Monitor with the PowerShell loop for one hour.	Recovers 1–2 GB; prevents gradual memory buildup.
Insufficient physical RAM	Close background apps via Task Manager. Consider a hardware upgrade (consult your IT team). Current RAM is visible in Task Manager > Performance > Memory.	Eliminates excessive pagefile swapping. 16 GB or more is recommended for modern workloads.
Browser or tab overload	Close excess browser tabs manually. Restart the browser.	Reduces memory usage by 30–50%. Verify in Resource Monitor.

Issue	Action	Expected Outcome
System file or cache issue	Run sfc /scannow. Also run DISM /Online /Cleanup-Image /RestoreHealth in an elevated Command Prompt.	Frees temporary memory allocations. Restart and verify in Task Manager.

2.5 Precautionary Measures

- Let Windows manage the paging file size automatically (see step 3 in the troubleshooting section above).
- Disable unnecessary startup programs: Task Manager > Startup > right-click items > Disable. Restart to apply.
- Monitor available memory continuously: Run Get-Counter '\Memory\Available Bytes' -Continuous in PowerShell (Ctrl+C to stop).
- Limit concurrent Remote Desktop sessions (Windows Pro and Server editions): Open Group Policy Editor (gpedit.msc). Go to Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Remote Desktop Session Host > Connections. Enable Restrict Remote Desktop Services users to a single Remote Desktop Services session.

3 High Disk Utilization

Disk utilization sustained above 70% is often caused by disk fragmentation, hardware issues, or I/O-intensive background tasks such as indexing, backups, or antivirus scans.

3.1 Identify the Source

Task Manager

22. Press Ctrl+Shift+Esc to open Task Manager.
23. On the Processes tab, select the Disk column header to sort from highest to lowest. Note processes such as searchindexer.exe.

Resource Monitor

24. **Open Resource Monitor:** Press Windows key+R, type `resmon`, and then press Enter.
25. On the Disk tab, review read/write rates and file paths. Sort by Total (B/sec) to identify top consumers.

Event Viewer

26. **Open Event Viewer:** Press Windows key+R, type `eventvwr.msc`, and then press Enter.
27. Go to Windows Logs > System. Filter for Error and Warning events. Search for the term disk in the Details pane.

3.2 Run PowerShell Diagnostics

Open PowerShell as administrator. Run the following commands.

Check drive health

```PowerShell
Get-PhysicalDisk | Select-Object OperationalStatus, HealthStatus, MediaType, Size
```

All drives should report an OperationalStatus of OK and a HealthStatus of Healthy. Note the MediaType to determine whether the drive is an SSD or HDD.

Sample disk activity over time

```PowerShell
Get-Counter '\PhysicalDisk(_Total)\% Disk Time' -SampleInterval 1 -MaxSamples 10
```

Values consistently above 70% confirm the alert condition.

3.3 Troubleshooting Steps

28. **Run Disk Cleanup:** Press the Windows key, type Disk Cleanup, and then press Enter. Select the system drive (C:), select Temporary files, select Clean up system files, and then select OK > Delete Files.
29. **Check the drive for errors:** Open Command Prompt as administrator. Run `chkdsk C: /f /r` (replace C: with the appropriate drive letter). Type Y to schedule the check on the next restart, and then restart the computer.
30. **Review scheduled tasks:** Press Windows key+R, type `taskschd.msc`, and then press Enter. In Task Scheduler Library, review EPP or backup tasks. Select the Triggers tab in each task's Properties to check timing and overlap.
31. **Defragment the drive:** Press the Windows key, type Defragment and Optimize Drives, and then press Enter. Select the drive and select Optimize. For SSDs, this operation runs TRIM automatically.

3.4 Remediation Actions

Issue	Action	Expected Outcome
Disk fragmentation (HDDs)	Run Optimize Drives weekly. Select Change settings to create a recurring schedule.	Improves I/O performance by 20–40%. Verify in Resource Monitor after optimization.
Excessive indexing activity	Open Services (services.msc). Find Windows Search, right-click, and select Stop. To exclude specific folders from indexing, right-click the folder in File Explorer > Properties > Advanced, and clear Allow files in this folder to have contents indexed.	Reduces spikes during file access. Restart the service when exclusions are set.
Failing drive	Run chkdsk as described above. If errors persist, back up all data immediately and contact your IT team for hardware replacement.	Prevents data loss. Monitor drive health with Get-PhysicalDisk in PowerShell.
Background backups or EPP scans	In Task Scheduler, right-click the relevant task > Properties > Triggers > Edit. Reschedule tasks to off-peak hours (for example, 2:00 AM).	Distributes disk load across the day. Verify there are no scheduling conflicts in Task Scheduler.

3.5 Precautionary Measures

- Enable Storage Sense: Settings > System > Storage > turn on Storage Sense. Configure it to run on a weekly schedule.
- Benchmark baseline disk performance: In an elevated Command Prompt, run winsat disk. Review the output for read and write speeds.
- Schedule EPP scans during off-peak hours: In EPP settings (accessible from the system tray or Start menu), adjust scan schedules to avoid peak business hours.
- Confirm drive type: Run Get-PhysicalDisk in PowerShell and check the MediaType column. SSDs provide significantly better I/O performance than HDDs.

4 General Best Practices

4.1 Holistic Monitoring

After applying any remediation, run the following PowerShell command every hour to track improvement:

PowerShell

```
Get-Process | Sort-Object CPU -Descending | Select-Object -First 5
```

Adapt the Sort-Object property to WorkingSet for memory or use Get-Counter for disk monitoring. Continue observing EPP alerts for 24–48 hours to confirm stability.

4.2 When to Escalate

Escalate to EPP support if resource spikes continue after remediation. To collect diagnostic data for escalation:

32. Open Event Viewer.
33. In the Actions pane, select Save All Events As.
34. Save the file in .evtx format and share it with EPP support.

> **Note** If needed, the EPP alert threshold can be adjusted in server settings (for example, to 80% for server workloads). Contact your EPP administrator for this change.

4.3 Additional Resources

For additional guidance, search Microsoft Learn (learn.microsoft.com) in Microsoft Edge, or contact EPP support directly.

Quick Reference: Key Tools and Commands

Tool	How to open	Use for
Task Manager	`Ctrl+Shift+Esc`	CPU, memory, disk, and startup process overview
Resource Monitor	`Windows key+R, then type resmon`	Detailed thread, memory, and disk I/O analysis
Event Viewer	`Windows key+R, then type eventvwr.msc`	System error and warning logs
Services	`Windows key+R, then type services.msc`	Start, stop, or configure Windows services
Task Scheduler	`Windows key+R, then type taskschd.msc`	Review and reschedule background tasks
Disk Cleanup	`Windows key, then type Disk Cleanup`	Remove temporary files and free disk space
Optimize Drives	`Windows key, then type Defragment and Optimize Drives`	Defragment HDDs; run TRIM on SSDs
Group Policy Editor	`Windows key+R, then type gpedit.msc (Pro editions)`	Configure session and system policies
PowerShell (Admin)	`Right-click Start > Windows PowerShell (Admin)`	Run diagnostic and monitoring commands