

Why Watch Task Scheduler Instances?

Windows Task Scheduler 2.0 saw a major overhaul with Window Server 2008/Vista. As a result the Windows OS now uses tasks much more extensively than previously -- there are over 30 tasks installed on every Windows Server 2008 machine! See list below. Unfortunately there still is no native alerting system for tasks, nor any easy way to see what they are all doing.

In addition:

- Many 3rd party software packages use Task Scheduler as their native scheduler and create tasks behind the scenes, unbeknownst to the user. These tasks kick off jobs such as antivirus, defrag, backups, etc. that can compete for resources on the server and impact performance just like SQL Agent jobs.
- A common practice used by hackers for years has been to create temporary tasks using the AT command to carry out malicious tasks (copy files, delete files, etc.), then auto-delete leaving no trace.

As long as you are watching a Task Scheduler instance with SQL Sentry Event Manager, if software or a user creates a task on the machine, you'll receive an email alert about it, and you'll see the tasks on the Event Manager calendar alongside all other events.

Bottom line, it's more important than ever to watch all Task Scheduler instances, otherwise you'll end up with a gap in visibility regarding everything that's happening on a server.

Name	Description
\\Microsoft\\Windows\\CertificateServicesClient\\SystemTask	Certificate Services Client automatically manages digital identities such as Certificates, Keys and Credentials for the users and the machine, enabling enrollment, roaming and other services.
\\Microsoft\\Windows\\Power Efficiency Diagnostics\\AnalyzeSystem	This job analyzes the system looking for conditions that may cause high energy use.
\\Microsoft\\Windows\\Customer Experience Improvement Program\\Consolidator	If the user has consented to participate in the Windows Customer Experience Improvement Program, this job collects and sends usage data to Microsoft.
\\Microsoft\\Windows\\Application Experience\\AitAgent	Aggregates and uploads Application Telemetry information if opted-in to the Microsoft Customer Experience Improvement Program.
\\Microsoft\\Windows\\Application Experience\\ProgramDataUpdater	Collects program telemetry information if opted-in to the Microsoft Customer Experience Improvement Program
\\Microsoft\\Windows\\Customer Experience Improvement Program\\Server\\ServerCeipAssistant	This task is part of the Windows Server Customer Experience Improvement Program. Please do not manually delete this task. Please see http://go.microsoft.com/fwlink/?linkid=52095 for more information.
\\Microsoft\\Windows\\Customer Experience Improvement Program\\Server\\ServerRoleUsageCollector	This task is part of the Windows Server Customer Experience Improvement Program. Please do not manually delete this task. Please see http://go.microsoft.com/fwlink/?linkid=52095 for more information.
\\Microsoft\\Windows\\Customer Experience Improvement Program\\UsbCeip	The USB CEIP (Customer Experience Improvement Program) task collects Universal Serial Bus related statistics and information about your machine and sends it to the Windows Device Connectivity engineering group at Microsoft. The information received is used to help improve the reliability, stability, and overall functionality of USB in Windows. If the user has not consented to participate in Windows CEIP, this task does not do anything.
\\Microsoft\\Windows\\MUI\\LPRemove	Launch language cleanup tool
\\Microsoft\\Windows\\Autochk\\Proxy	This task collects and uploads autochk SQM data if opted-in to the Microsoft Customer Experience Improvement Program.
\\Microsoft\\Windows\\CertificateServicesClient\\UserTask	Certificate Services Client automatically manages digital identities such as Certificates, Keys and Credentials for the users and the machine, enabling enrollment, roaming and other services.

\Microsoft\Windows\Time Synchronization\SynchronizeTime	Maintains date and time synchronization on all clients and servers in the network. If this service is stopped, date and time synchronization will be unavailable. If this service is disabled, any services that explicitly depend on it will fail to start.
\Microsoft\Windows\Registry\RegIdleBackup	Registry Idle Backup Task
\Microsoft\Windows\Customer Experience Improvement Program\KernelCeipTask	The Kernel CEIP (Customer Experience Improvement Program) task collects additional information about the system and sends this data to Microsoft. If the user has not consented to participate in Windows CEIP, this task does nothing.
\Microsoft\Windows\Customer Experience Improvement Program\Server\ServerRoleCollector	This task is part of the Windows Server Customer Experience Improvement Program. Please do not manually delete this task. Please see http://go.microsoft.com/fwlink/?linkid=52095 for more information.
\Microsoft\Windows\Windows Error Reporting\QueueReporting	Windows Error Reporting task to process queued reports.
\Microsoft\Windows\TextServicesFramework\MsCtfMonitor	TextServicesFramework monitor task
\Microsoft\Windows\Server Manager\ServerManager	Task for launching Initial Configuration Tasks or Server Manager at logon.
\Microsoft\Windows\WindowsColorSystem\Calibration Loader	This task applies color calibration settings.
\Microsoft\Windows\Windows Filtering Platform\BfeOnServiceStart\TypeChange	This task adjusts the start type for firewall-triggered services when the start type of the Base Filtering Engine (BFE) is disabled.
\Microsoft\Windows\WDI\ResolutionHost	The Windows Diagnostic Infrastructure Resolution host enables interactive resolutions for system problems detected by the Diagnostic Policy Service. It is triggered when necessary by the Diagnostic Policy Service in the appropriate user session. If the Diagnostic Policy Service is not running, the task will not run
\Microsoft\Windows\User Profile Service\HiveUploadTask	This task will automatically upload a roaming user profile's registry hive to its network location.
\Microsoft\Windows\UPnP\UPnPHostConfig	Set UPnPHost service to Auto-Start
\Microsoft\Windows\Tcpip\IpAddressConflict2	This event is triggered when an IP address conflict is detected.
\Microsoft\Windows\Tcpip\IpAddressConflict1	This event is triggered when an IP address conflict is detected.
\Microsoft\Windows\Task Manager\Interactive	Runs a task as the interactive user.
\Microsoft\Windows\SoftwareProtectionPlatform\SvcRestartTask	This task restarts the Software Protection Platform service at the specified time
\Microsoft\Windows\Ras\MobilityManager	Provides support for the switching of mobility enabled VPN connections if their underlying interface goes down.
\Microsoft\Windows\RAC\RacTask	Microsoft Reliability Analysis task to process system reliability data.
\Microsoft\Windows\NetTrace\GatherNetworkInfo	Network information collector
\Microsoft\Windows\Multimedia\SystemSoundsService	System Sounds User Mode Agent
\Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector	Task for launching the Memory Diagnostic
\Microsoft\Windows\MemoryDiagnostic\CorruptionDetector	Task for launching the Memory Diagnostic
\Microsoft\Windows\Defrag\ScheduledDefrag	This task defragments the computers hard disk drives.
\Microsoft\Windows\CertificateServicesClient\UserTask-Roam	Certificate Services Client automatically manages digital identities such as Certificates, Keys and Credentials for the users and the machine, enabling enrollment, roaming and other services.
\Microsoft\Windows\AppID\VerifiedPublisherCertStoreCheck	Inspects the AppID certificate cache for invalid or revoked certificates.
\Microsoft\Windows\AppID\PolicyConverter	Converts the software restriction policies policy from XML into binary format.
\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Manual)	Updates the AD RMS rights policy templates for the user. This job provides a credential prompt if authentication to the template distribution web service on the server fails.
\Microsoft\Windows\Active Directory Rights Management Services Client\AD RMS Rights Policy Template Management (Automated)	Updates the AD RMS rights policy templates for the user. This job does not provide a credential prompt if authentication to the template distribution web service on the server fails. In this case, it fails silently.