

PCS File System Monitor v1.1

Dateizugriffe überwachen und protokollieren

Überwachen Sie den Zugriff (z.B. Lesen, Schreiben, Löschen) von Dateien in ihrem Datenspeicher. Der **PCS File System Monitor** gibt die Antwort auf die Frage, wann eine Datei erstellt, gelesen, verändert oder gelöscht hat. Überwachen Sie die komplette Festplatte, oder nur ausgewählte Verzeichnisse / Unterverzeichnisse oder bestimmte Dateitypen.

Systemvoraussetzungen

Voraussetzungen für den Betrieb vom **PCS File System Monitor**:

- Microsoft Windows XP 32bit
- Microsoft Windows Server 2003 32bit
- NTFS-Dateisystem
- Microsoft .Net Framework 2.0

Überwachung durch den File System Monitor

Aufbau der Protokolldatei

Die Protokolldatei ist wie folgt aufgebaut:

■ Benutzeraccount

Gibt den Benutzer in Form DOMAIN\USER an, der den Vorgang durchgeführt hat

■ Datum und Zeit

Gibt Datum und Zeit des durchgeführten Vorgangs an (Systemzeit)

■ Process ID

Gibt die Windows PID an

■ Process Name

Gibt den Process Namen an (z.B. explorer.exe) der auf die Datei zugegriffen hat

■ Zugriffsart

Typ des Zugriffes (z.B. READ,WRITE, DELETED)

■ Zugriffene Datei

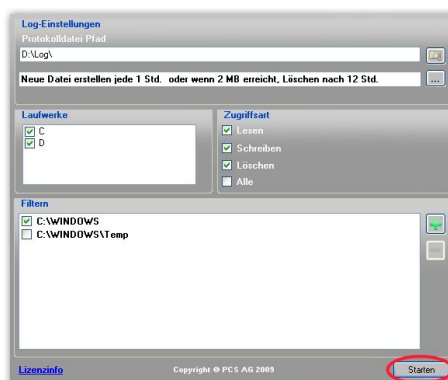
Gibt die Datei an, auf die zugegriffen wurde

■ Info Offset Length

Bereich der Datei, in der zugegriffen wurde

Starten oder Anhalten

Durch Klicken des Button Start wird die Überwachung gestartet. Bitte beachten Sie, dass mindestens ein Ordner für die Überwachung ausgewählt sein muss. Durch erneutes Klicken wird die Überwachung beendet.



Pfad der Protokolldatei

Wählen Sie in den Log-Einstellungen der FSM Console den gewünschten Speicherort der Protokolldateien aus. Klicken Sie dazu auf den Ordner-Button und wählen einen Ordner aus. Der ausgewählte Ordner wird nun in der Console angezeigt. Der voreingestellte Standardpfad .\Trace befindet sich im Hauptordner der Programminstallation.

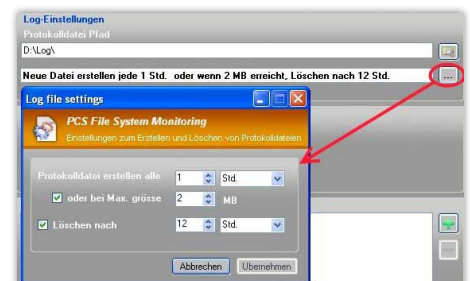


Einstellungen der Protokolldatei

Definieren Sie das Intervall, in dem neue Protokolldateien erstellt werden. Die Standardeinstellung beträgt 1 Stunde.

Ebenso können Sie durch Aktivieren der Checkbox oder bei max. Größe festlegen, ob die Protokolldateien nach Überschreitung einer bestimmten Dateigröße automatisch erstellt werden.

Aktivieren Sie die Checkbox Löschen nach, wenn Sie die Protokolldateien nach einer definierten Zeit automatisch löschen wollen. Eine Zusammenfassung der gewählten Einstellungen wird in der FSM Console angezeigt.



Filtern

Bevor die Überwachung gestartet werden kann, muss mindestens ein Ordner ausgewählt sein, der vom FSM überwacht werden soll.

PCS File System Monitor v1.1

Klicken Sie auf den "+" Button und wählen Sie einen Ordner aus (z.B. C:\Windows). Es werden automatisch alle Unterordner in die Überwachung miteinbezogen.

Um einen Unterordner auszuschliessen, gehen Sie wie folgt vor: Klicken Sie erneut auf den "+" Button und wählen den Unterordner aus, der ausgeschlossen werden soll (z.B. C:\Windows\Temp). Deaktivieren Sie nun die Checkbox des entsprechenden Unterordners, um diesen von der Überwachung auszuschliessen.

Um Ordner wieder aus der Überwachung zu löschen, selektieren Sie diesen und drücken den "-" Button. Der Ordner wird aus der Auswahlliste gelöscht.



Um nur bestimmte Dateitypen zu überwachen, ändern Sie in der Filterliste den Pfad (z.B. C:\Windows\Temp*.exe). Drücken Sie dazu die F2-Taste oder klicken Sie doppelt auf den Pfad und geben Sie die Änderungen manuell ein. Es werden nun nur exe-Dateien überwacht. Deaktivieren Sie die Checkbox in der Filterliste, um Dateitypen explizit auszuschliessen.

Laufwerke

Wählen Sie die Laufwerke ihres Computers aus, die von FSM überwacht werden sollen. Es werden alle lokalen Partitionen angezeigt.



Zugriffsart

Wählen Sie aus, welche Aktivitäten FSM im Dateisystem überwachen soll. Die Optionen gliedern sich wie folgt:

- „Lesen“: Protokolliert den lesenden Zugriff im Dateisystem
- „Schreiben“: Protokolliert den schreibenden Zugriff im Dateisystem

■ „Löschen“: Protokolliert Löschvorgänge im Dateisystem

- „Alle“: Protokolliert lesenden und schreibenden Zugriff im Dateisystem, sowie folgende Zugriffsarten: CREATE, PNP, POWER, FLUSH_BUFFERS, QUERY_INFORMATION, SET_INFORMATION, DEVICE_CONTROL, INTERNAL_DEVICE_CONTROL, SYSTEM_CONTROL, CLEANUP, CLOSE, SHUTDOWN



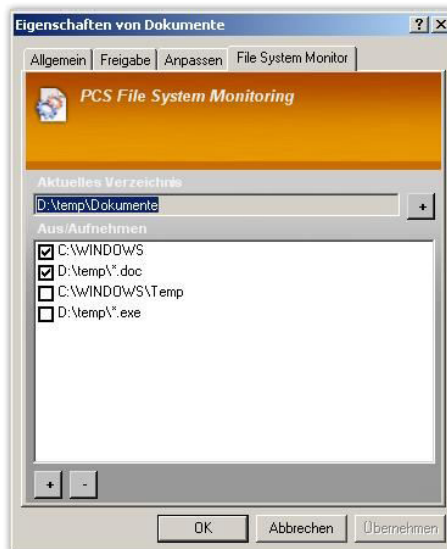
Eine detaillierte Beschreibung der einzelnen Zugriffsarten ist zu finden unter:

<http://msdn.microsoft.com/de-de/library/ff550710.aspx>

Hinweis: Wir empfehlen die Zugriffsart „Alle“ nur bei Bedarf zu aktivieren, da die Logdateien im Zugriffsmodus „Alle“ sehr schnell anwachsen können und mit einer erhöhten Systemlast zu rechnen ist.

Explorer Integration

Der File System Monitor verfügt über eine Explorer Integration. Wählen Sie dazu über den Explorer das Eigenschaftenfenster des Ordners aus und navigieren Sie in den File System Monitor Tab. Sie können nun den ausgewählten Ordner direkt zu den zu überwachenden Ordnern hinzufügen.



Lizenzinfo

Diese Software ist 14 Tage kostenlos nutzbar. Wird sie darüber hinaus genutzt, ist ein Lizenzkey notwendig. Senden Sie eine Anfrage für diesen mit Ihrem Freischaltsschlüssel an info@pcs-ag.de

Geplante Features für die kommenden Versionen:

- Support für MS Vista / Server 2008 x86/x64
- automatisches Benachrichtigungssystem