Event Controller
Produktbeschreibung

Datum 13. Sep 2010

Die Ausgangssituation

In jedem Unternehmen laufen unterschiedliche Dienste und Applikationen und viele dieser können Fehler melden.

Bei interaktiven Programmen werden Fehlermeldungen sofort direkt auf dem Bildschirm ausgegeben, allerdings gibt es auch Programme, die im Hintergrund laufen und ihre Arbeit ohne permanente Überwachung erledigen.

Dabei gibt es die unterschiedlichsten Hintergrund-Programme wie beispielsweise

- Tagesabschluss von Rechnungsdaten, Auswertungsläufe
- Datenaustausch mit Kunden oder Partnern, Übertragung von Daten zu Internet-Portalen
- Technische Programme wie E-Mail und Web-Server
- Auch das Betriebssystem oder Peripheriegeräte wie Router können Fehlermeldungen senden

Treten nun Fehler auf, so werden sie entweder gar nicht dokumentiert oder in Log-Dateien geschrieben und nicht weiter beachtet.

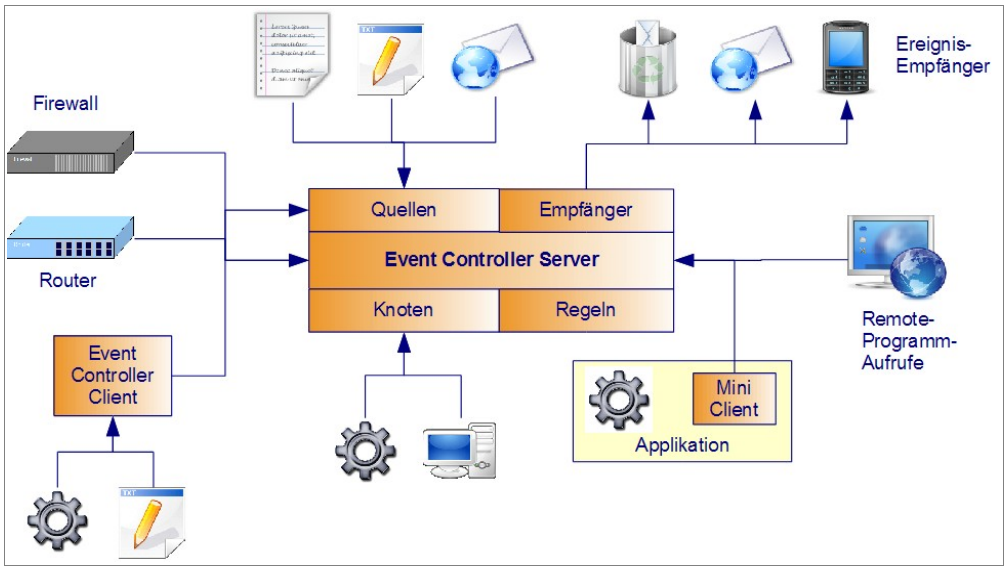
Einige Systeme sind auch in der Lage, im Fehlerfall E-Mails zu senden, doch sind diese dann nicht qualifiziert. Dabei besteht zudem das Problem, dass es zu massenhaften Meldungen (Fehlerschleife) kommen kann oder das auch »uninteressante« Fehler gemeldet werden. Vor allem nicht relevante Fehlermeldungen sorgen dafür, dass die Gefahr besteht, dass alle Meldungen unbeachtet bleiben.

Zudem wird ebenfalls die Verfügbarkeit von Servern wie beispielsweise Web- oder FTP-Server nicht überwacht, so dass ein Ausfall erst dann bemerkt wird, wenn sich Kunden, Partner oder Mitarbeiter melden.

Treten dann einmal erhebliche Störungen oder Probleme auf, werden einzelne Insellösungen entwickelt, um beim nächsten Auftreten gewarnt zu sein. Hier kann es dann wiederum zu irrelevanten Fehlern oder Massenmeldungen kommen.

Die Lösung

Hier setzt der Event Controller an: Er scannt Log-Dateien auf Fehlermeldungen hin, überwacht Netzverbindungen oder kann periodisch Systembefehle zur Systemüberwachung absetzen und das Resultat analysieren.



Über Quellen werden Log-Dateien oder Verzeichnisse permanent überwacht und neue Einträge gelesen und ausgewertet. E-Mails können entgegengenommen und ausgewertet werden.

Mit Knoten wird die Verfügbarkeit von Systemen oder Diensten geprüft und es können Systembefehle ausgeführt und deren Ergebnis analysiert werden.

Mittels Log-Server können Meldungen von Fremdsystemen, Routern oder anderen Peripheriegeräten entgegengenommen werden.

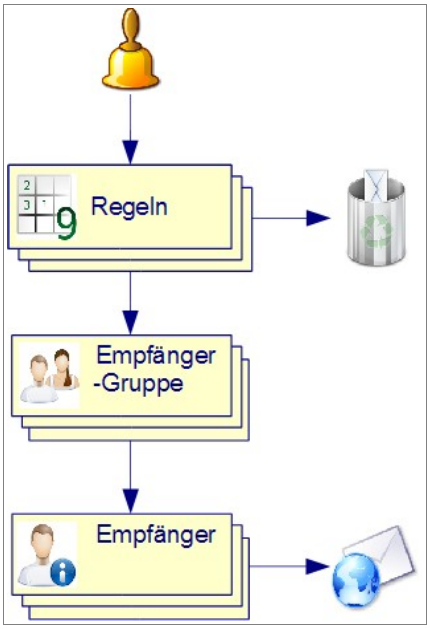
Event Controller Clients lesen die Windows Ereignisse, überwachen die Festplatte, Speicher oder laufende Prozesse und lesen Log-Dateien. Kritische Ergebnisse reichen sie über das Netzwerk an den Event Controller Server weiter. Dadurch lassen sich effektiv mehrere Systeme gleichzeitig überwachen.

Über Mini-Clients lassen sich beispielsweise auch einzelne Fehlermeldungen aus Anwendungen heraus direkt an den Event Controller senden.

Die entscheidenden Meldungen werden dann über vorher definierte Regeln qualifiziert an einzelne Empfänger übermittelt. Dadurch werden die Empfänger aktiv informiert so dass die Fehler jetzt entsprechend wahrgenommen werden können.

Über Regeln lassen sich beliebige Eskalationsstufen definieren, wodurch rechtzeitig entsprechende Gegenmaßnahmen ergriffen werden können.

Verarbeitung von Ereignissen



Meldungen durchlaufen einen vorher definierten Satz an Regeln. Diese entscheiden, ob eine Meldung verworfen oder gesendet werden soll. Dabei kann eingestellt werden, was im Wiederholungsfall geschehen soll.

Es können eine oder mehrere Regeln greifen. Hierdurch lässt sich qualifiziert festlegen, wann eine Meldung wohin gesendet werden soll (Eskalationsstufen).

Zu jeder Regel lassen sich Informationen hinterlegen, die Hinweise für die Beseitigung von Fehlern geben. Diese werden mit der Meldung an den oder die entsprechenden Empfänger übermittelt.

Greift eine Regel, wird anhand der dort hinterlegten Empfängergruppe überprüft, an welche Empfänger diese gesendet werden soll.

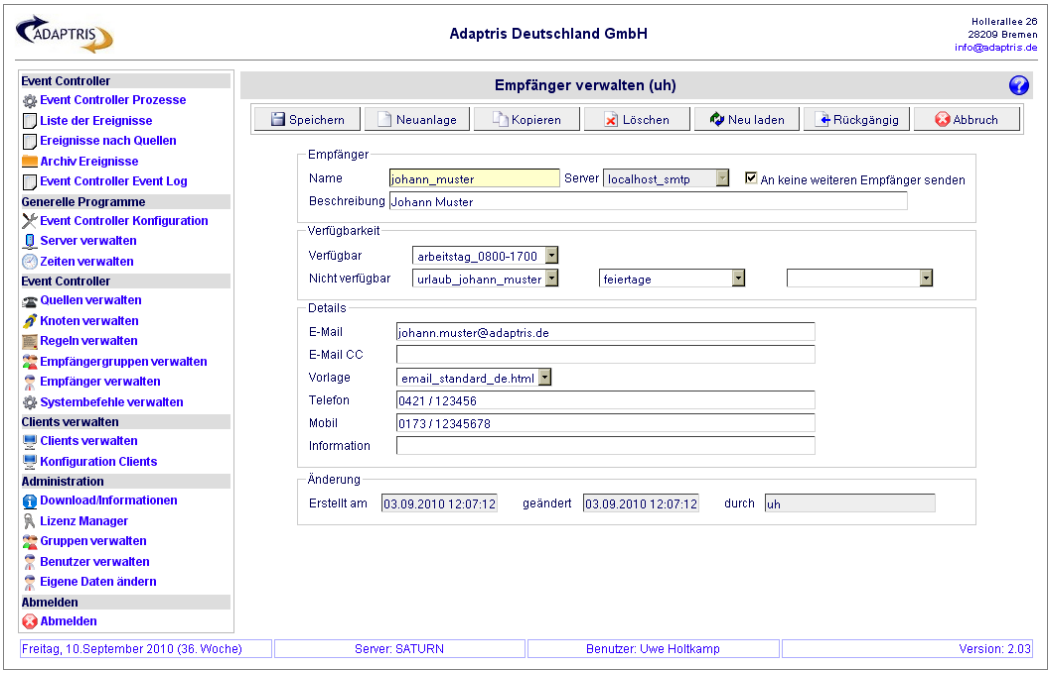
Bei den einzelnen Empfängern kann ein Zeitprofil hinterlegt werden. So ist es beispielsweise möglich, Nachrichten nach Dienstschluss an einen anderen Empfänger oder auf ein Mobiltelefon zu senden.

Empfänger müssen nicht zwingend E-Mail-Empfänger sein. Es können beispielsweise auch Meldungen in Dateien oder eine Datenbank-Tabelle geschrieben werden. Dies kann zur Unterstützung eines Nachrichten- oder Support-Systems notwendig sein.

Zudem lassen sich die Meldungen parallel in eine Event-Verwaltung schreiben, in der sie dann mit einem Bearbeitungsstatus und Kommentaren versehen werden können. Dadurch kann die Bearbeitung von Meldungen dokumentiert werden.

Administration

Die Konfiguration erfolgt über einen Web-Browser (wie Firefox, Internet-Explorer), so dass zur Administration keine weitere Software installiert werden muss.



Bei der Gestaltung der Oberfläche wurde darauf geachtet, sie so einfach und intuitiv wie möglich zu halten.

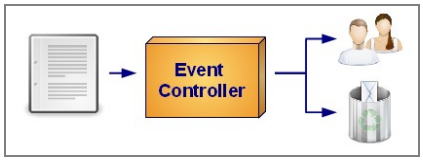
Zum Zugriff auf die Oberfläche ist eine Benutzeranmeldung notwendig, die über Benutzergruppen reglementiert werden kann.

Die Oberfläche ist multilingual (gemäß Browser-Einstellung). Zudem lassen sich viele Einstellungen individuell anpassen.

Einsatzmöglichkeiten (Beispiele)

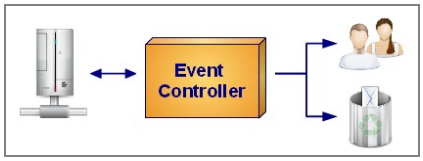
Fehlermeldungen aus Dateien / E-Mails

Die grundlegende Möglichkeit ist die Überwachung von Log- oder Fehler-Dateien. Hier können Fehlermeldungen aus Dateien gescannt oder Fehlermeldungen in Dateien per FTP oder E-Mail entgegengenommen und entsprechend der Regeln verteilt werden.



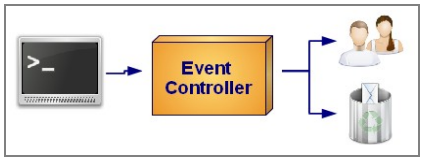
Periodische Überwachung von Systemen

Es können Server periodisch überprüft werden, indem eine Verbindung mit ihnen aufgenommen wird. So wird festgestellt, ob sie erreichbar sind oder der gewünschte Dienst noch zur Verfügung steht.

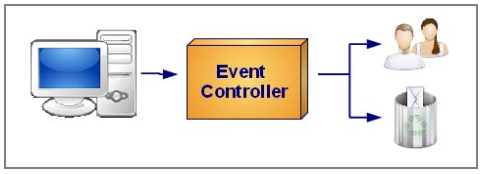


Weiterhin lassen sich periodisch oder zu bestimmten Zeitpunkten System-Befehle ausführen, deren Ausgabe weitergereicht werden kann. So können Programme oder Skripte ausgeführt werden, die Tests oder periodisch wiederkehrende Aufgaben durchführen.

Anbindung von Clients



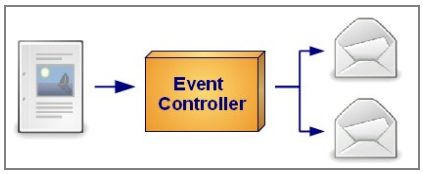
Auf Fremdsystemen können Clients installiert werden, die dort das System überwachen (Plattenplatz, laufende Prozesse, Prozessorlast), Dateien scannen oder periodisch Programme ausführen. Diese sind vom Server aus konfigurierbar und senden im Ausnahmefall ihre Ergebnisse an den Server weiter.



Zudem können mittels Clients Meldungen direkt an den Server gesendet werden (beispielsweise aus Skripten oder Programmen heraus).

Der Event Controller kann auch als Syslog-Server fungieren und Nachrichten von anderen Systemen oder Peripheriegeräten empfangen.

Verteilung von Dokumenten



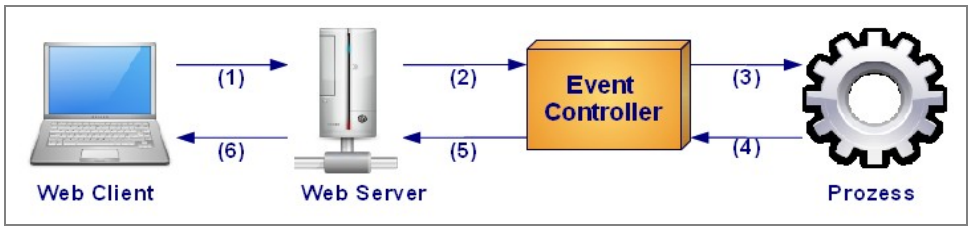
Werden von einer Applikationen Dokumente erzeugt, so können diese vom Event Controller aufgenommen und verteilt werden.

Hier wäre es beispielsweise denkbar, dass Dokumente aus einem Berichtswesen an bestimmte Empfänger verteilt werden sollen.

Externe Befehle

Der Event Controller kann wie eine Befehlsverwaltung verwendet werden, die dann von Clients remote gestartet werden können. Dies ist vergleichbar mit Web Services oder Remote Procedure Calls, nur dass es sich einfacher gestalten lässt und beliebige Befehle verwendet werden können.

Beispielsweise könnte durch ein Klick auf einer Webseite von dort aus die Generierung eines Dokuments gestartet werden, die dann wieder an den Web-Client übertragen wird.



Beispiel:

Der Benutzer klickt auf einen Link (1), wodurch ein Befehl an den Event Controller gesendet wird (2). Dieser führt das entsprechende Programm aus (3), welches ein Dokument generiert (4) welches dann vom Event Controller über den Webserver (5) an den Benutzer gesendet wird. Hierbei können dem auszuführenden Programm Informationen aus der Webseite mitgegeben werden, die der Benutzer vorher erfasst hat.

Leistungsmerkmale

- Geringe Systemanforderungen
- Einfach zu installieren und anzuwenden, geringer Lernaufwand
- System- und Applikationsunabhängigkeit
- Konfiguration via Web-Browser (keine Installation von Verwaltungssoftware notwendig)
- Mehrsprachig (automatisch, gemäß Einstellung im Web-Browser)

- Benutzermanagement (Benutzer und Gruppen)
- Beliebig viele Applikationen und Systeme können überwacht werden
- Verfügbarkeitsüberwachung von Servern, Netzwerkgeräten und Diensten
- Scannen von Log-Dateien, Protokollen und Verzeichnissen
- Überwachen von Plattenplatz, laufende Programme, Prozessorlast
- Scannen von Windows Ereignissen (Windows Ereignisanzeige)
- Syslog Server zum Empfangen von Meldungen von UNIX-Systemen und Peripheriegeräten
- Verteilung von Dokumenten (beispielsweise automatisch generierte Auswertungen)
- Regelmäßiges Ausführen und Analysieren von Systembefehlen und Skripten
- Meldungen senden aus Skripten oder Programmen direkt an den Server
- Regelsätze und Regeln, nach denen die Meldungen erfolgen, können individuell definiert werden
- Informationen zur Fehlerbehebung können bei den einzelnen Regeln hinterlegt werden
- Irrelevante, vereinzelte und wiederholte Meldungen können ignoriert werden
- Mehrere Regeln können zu einem Ereignis definiert werden (Eskalationsstufen)
- Benachrichtigungen können an einen oder mehrere Empfänger gesendet werden
- Versendung von Benachrichtigungen kann via E-Mail erfolgen
- Empfängern kann eine zeitliche Verfügbarkeit zugeordnet werden (Vertretungen definieren)
- Zur Dokumentation und Analyse können die akzeptierten Fehlermeldungen in eine Event-Verwaltung geschrieben werden
- Verwaltung von Ereignissen (Status, Kommentare), Antwort via E-Mail möglich
- Archivieren von Ereignissen