# Die Administration der Administration

**Sven Mendler**
**WEDACO.de**
**D-99625 Beichlingen**

**Schlüsselworte:**

Administration, Logdatei, Logfile, Analyse, Auswertung, Logging

## Einleitung

Der Betrieb von Anwendungen und das Bereitstellen von Services stellen einen hohen administrativen Aufwand dar. Jede Komponente bringt eigene Administrationswerkzeuge mit und erzeugt diverse Logdateien. Komponenten aller Anwendungsschichten, wie zum Beispiel Applikationen, Middleware, Datenbank- und Betriebssysteme sowie deren automatisierte Aktionen wie z.B. Backups, Datentransfer oder Wartungsarbeiten, müssen zusätzlich überwacht werden. Darüber hinaus fallen auch bei Hardware- und Infrastrukturkomponenten diverse Logdateien an.

## Das Dilemma des Administrators

Zu den Aufgaben eines Administrators gehört es, immer zu wissen, ob eine Anwendung oder ein Service stabil läuft bzw. den Status aller geplanten Tasks zu kennen. Auftretende Fehler oder Warnungen hat dieser sofort zu analysieren.
Unangenehm ist es, wenn ein verantwortlicher Administrator durch Anwender auf Probleme, Fehler oder Ausfälle hingewiesen wird. Um dies zu vermeiden, müsste man mehrere Admin-Tools ständig im Auge behalten und zusätzlich noch Email-Warnungen sowie einzelne Logdateien beachten.
Jeder Administrator kennt das: Tag für Tag ellenlange Logdateien auswerten ist eine harte Geduldsprobe.

## Wo liegt denn das eigentliche Problem?

Die zu administrierende Systemumgebung in mittelständischen Unternehmen umfasst meist eine Serverlandschaft mit heterogenen Betriebssystemen, diversen Anwendungen, Datenbanksystemen und automatisierten Aktionen. Viele dieser Komponenten benutzen eine Logdatei. Andere Komponenten - wie zum Beispiel Oracle Datenbanken, Clustermechanismen oder Applikationsserver - stellen deutlich mehr essentielle Log- und Tracedateien zur Verfügung.

Ein Administrator wird von zwei Gattungen von Fragestellungen konfrontiert – Fragen, die sich jeder Administrator selbst stellt und Fragen, die ihm regelmäßig gestellt werden. Beispielhaft dafür wären:
„Läuft alles so, wie es soll?“ und „Waren alle automatisierten Aktionen erfolgreich?“.
Um diese Fragen immer qualifiziert beantworten zu können, muss ein Administrator erheblichen Aufwand betreiben. Die benötigten Informationen sind in den entsprechenden Logdateien der Komponenten und ggf. weiterer Log- und Tracedateien zu finden.
In Systemumgebungen mittelständischer Unternehmen fallen täglich durchschnittlich zwischen 70 und 100 Logdateien an, deren Informationen wichtige Hinweise für die kontinuierliche Administration, vorhandenes Optimierungspotential und notwendige Problembehebungen geben.

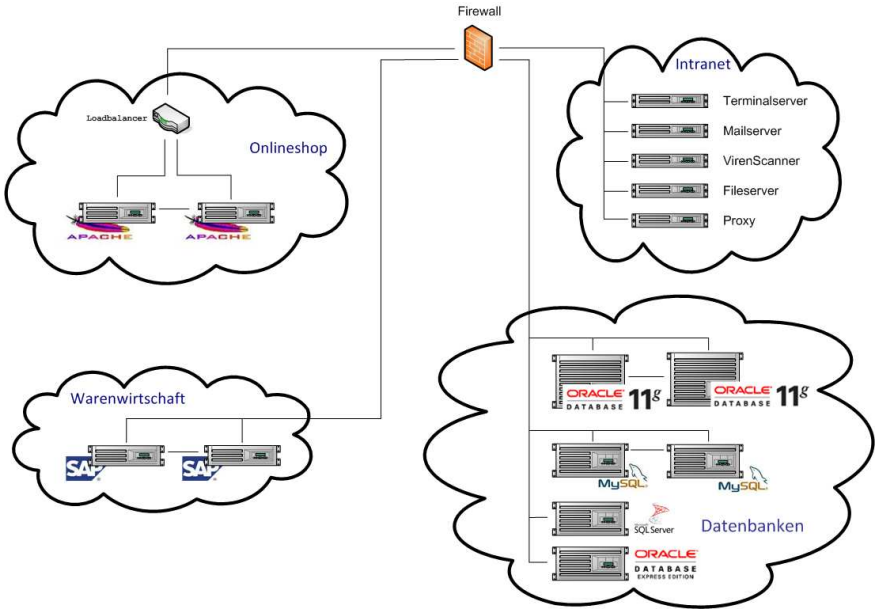


*Abb. 1: Systemumgebung am Beispiel eines mittelständischen Unternehmens*

**„Omnes viae Romam ferunt“ – „Alle Wege führen nach Rom"**

Alle traditionellen Methoden, um diese Aussagen effizient und verlässlich treffen zu können, haben ihre Berechtigung. Sei es, dass man die Administrations-Tools jeder Komponente benutzt, um deren Status zu ermitteln, sich regelmäßig via Email Bericht erstatten lässt oder gar manuell in den Tiefen der Logdateien verschwindet, um Statusmeldungen zu finden. Jeder Weg führt letztlich zum Ziel. Dabei entscheidet jeder verantwortliche Administrator für sich selbst, wie viel Energie er dafür bereit ist, aufzubringen.

Die mitgelieferten grafischen Administrations-Tools jeder Komponente, werten essentielle Logdateien aus und bereiten die Log-Informationen grafisch auf. Anhand dieser Diagramme kann man den aktuellen Status der Komponente interpretieren. Diese Tools bedienen sich dabei vordefinierter Meldungen, die einen bestimmten Status beschreiben.
Eine Berichterstattung per Email wird häufig eingesetzt, um Fehler, die während automatisierter Aktionen, wie zum Beispiel Backup oder Datenreplikationen, auftraten, zu melden. Diese Methode hat den Charme, dass man nur im Fehlerfall mit Informationen belästigt wird. Befürworter der Email-Notification arbeiten oft nach folgender philosophischer These: „Kommt keine Email an, lief alles erfolgreich!“.
Ist das so? Was, wenn der Server gar nicht läuft oder keine Email verschicken kann? Was, wenn der Email-Service im Unternehmen ausfällt? Was, wenn der zuständige Administrator - in dessen Postfach diese wichtigen Nachrichten landen - nicht verfügbar ist? …
Um essentielle Informationen in den entsprechenden Logdateien durch manuelles Suchen zu finden, muss man einen erheblichen Aufwand betreiben. Neben den Zugangsberechtigungen für alle Systeme, benötigt man detaillierte Informationen über die einzelnen Systeme (zum Beispiel Log-Verzeichnisse und Logdateinamen).
Betrachtet man die unterschiedlichen Möglichkeiten, Log-Informationen zu analysieren, so kann man feststellen, dass jede Methode entscheidende Vorteile hat.
Eine Kombination dieser einzelnen Vorzüge würde den Arbeitsalltag eines Administrators merklich vereinfachen.

Einige Wunschanforderungen an eine effiziente Analyse ALLER Logdateien im Unternehmen könnte wie folgt aussehen:

- schneller Zugriff auf alle Log-Informationen,
- kumulierter Status aller Logdateien,
- bedarfsweises Abfragen dieser Informationen,
- sofortiges Finden der Fehlermeldung,
- gleiche Zugriffswege für alle Administratoren,
- Übersicht über alle wichtigen Log-Aktionen im Unternehmen,
- Vertretung von Administratoren einfach realisierbar,
- Historisierung der Logdateien,
- Einhaltung von Sicherheitsstandards beim Umgang mit Logdateien

… und das Alles ohne regelmäßigen großen Aufwand.

**Der LOGFILE MONITOR**

Die schlanke Webanwendung „LOGFILE MONITOR“ bietet eine effiziente Analyse ALLER textbasierten Logdateien eines Rechenzentrums. Dabei werden alle Logdateien zentral vorgehalten und nach automatischer Analyse grafisch in einer Oberfläche aufbereitet.
Der Status einer Logdatei wird anhand frei definierbarer Meldungen automatisch durch einen Hintergrundprozess des LOGFILE MONITOR festgestellt. Diese Meta-Informationen werden in einer Datenbank gespeichert.

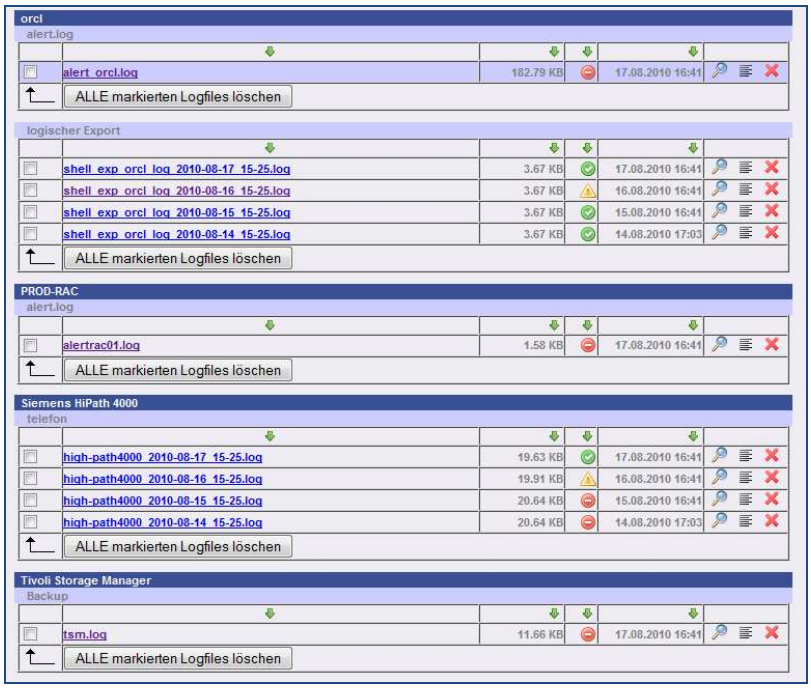

*Abb. 2: Anzeige der aktuell analysierten Logdateien mit Darstellung des Status und weiterer Dateiinformationen*

Bei Bedarf kann die Logdatei direkt geöffnet werden. Dabei wird sofort die Zeile der Logdatei angezeigt, die die festgestellte Meldung beinhaltet. Wird in der Logdatei auf weitere Log- oder Tracedateien verwiesen, können diese direkt im Browser geöffnet werden.

```
Thread 1 advanced to log sequence 353
  Current log# 2 seq# 353 mem# 0: /oradata/orcl/orcl/redo02.log
Mon Jan 11 00:00:46 2010
Thread 1 advanced to log sequence 354
  Current log# 3 seq# 354 mem# 0: /oradata/orcl/orcl/redo03.log
Mon Jan 11 01:13:37 2010
Errors in file /opt/oracle/product/10.2.0/admin/orcl/bdump/orcl_mmnl_11590.trc:
ORA-07445: Exception aufgetreten: CORE Dump [082BADFC] [SIGSEGV] [Address not mapped to object] [0x0] [] []
Mon Jan 11 01:14:30 2010
Restarting dead background process MMNL
MMNL started with pid=12, OS id=21784
Wed Jan 13 20:47:24 2010
MMNL absent for 239618 secs; Foregrounds taking over
```

*Abb. 3: möglicher Zugriff auf weitere Log- und Tracedateien, die detailliertere Informationen enthalten*

Für die Speicherung der Logdatei-Metadaten, basiert die Anwendung wahlweise auf einer Oracle- oder einer MySQL Datenbank. Um vorhandene Ressourcen im Unternehmen effizient zu nutzen, ist es möglich, die Webanwendung des LOGFILE MONITORs auf einem bereits eingesetzten Apache Webserver zu betreiben. Die Datenbasis kann ebenfalls eine bestehende MySQL Datenbank oder ein zusätzliches Schema einer bestehenden Oracle Datenbank nutzen. Alternativ dazu, kann der LOGFILE MONITOR natürlich auch auf dedizierter Hardware und diversen Betriebssystemen installiert werden.

Ein Rollen- und Rechtesystem steuert den Zugriff auf die einzelnen Logdateien. Ein „Manager View“ (Nur gucken – nicht anfassen) kann bei Bedarf einen lesenden Zugriff auf Logdateien für einzelne Benutzer gewähren.
Durch das einfache Hinzufügen des Zugriffsrechtes auf eine Logdatei, kann die Vertretung eines Administrators leicht realisiert werden. Für die Zeit der Abwesenheit hat ein anderer Administrator Zugriff auf die entsprechenden Logdateien.

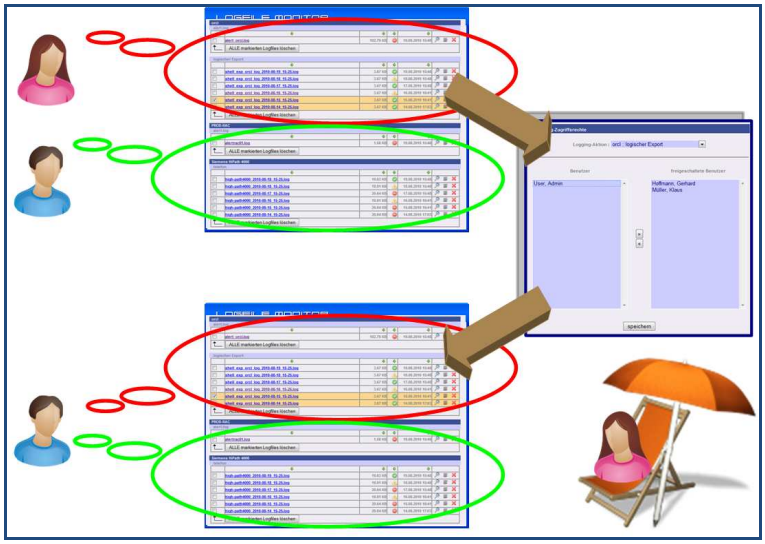

*Abb. 4: einfache Einrichtung der Vertretung eines Administrators durch Zugriffsänderung auf die Logdateien*

**Historisierung von Log-Informationen**

Der Bedarf der Administratoren und Anwendungsbetreuer, unternehmensinterne Festlegungen oder gesetzliche Vorgaben gem. BSI (Bundesamt für Sicherheit in der Informationstechnik) bieten die Grundlage für die Aufbewahrung von Log-Informationen.
Durch die zentrale Bereitstellung aller Logdateien im LOGFILE MONITOR ist es sehr einfach, diese zentral zu sichern oder zu archivieren. Die Sicherung/Archivierung eines Dateisystems ist ausreichend, um ALLE essentiellen Logdateien entsprechend zu behandeln.

**Sicherheit im Rechenzentrum**

Bei einigen Systemen sind unterschiedliche Administratoren, Anwendungsbetreuer und ggf. Anwender auf Log-Informationen angewiesen. Dieser Zugriff auf einzelne Logdateien stellt ein erhebliches Sicherheitsrisiko dar, da diverse Personen Zugriffsberechtigungen auf die (Betriebs-) Systeme haben. Ist ein solcher Zugriff nicht gewünscht, stellt die Bereitstellung dieser Log-Informationen einen erheblichen Aufwand dar.
Durch den Einsatz des LOGFILE MONITOR kann der Zugriff auf alle benötigten Logdateien leicht eingerichtet werden. Dabei werden weder Zugriffsberechtigungen, noch detaillierte Kenntnisse der entsprechenden Systeme benötigt. Ein Zugriff in sicherheitsempfindliche produktive DMZ kann wirkungsvoll verhindert oder vermieden werden.

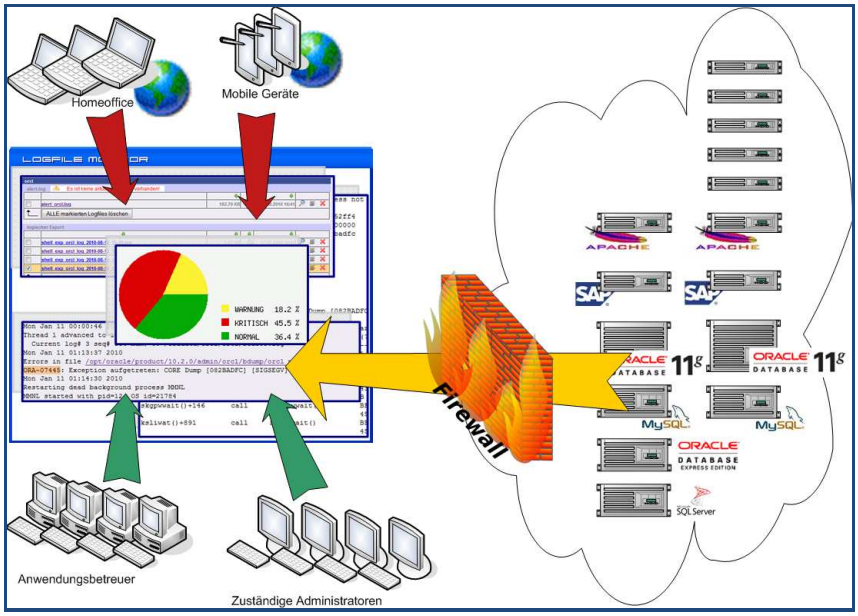

*Abb. 5: Logdateien analysieren, ohne Zugriff auf die entsprechenden Systeme*

Für die Fernüberwachung wichtiger Systeme während der Rufbereitschaft, Dienstreisen oder sonstiger Abwesenheit der zuständigen Administratoren, ist der Remotezugriff auf NUR EINE Anwendung (günstigenfalls in eine separate DMZ) erforderlich.

**Kontaktadresse:**

**Sven Mendler**
WEDACO.de
Am Kirschberg 168-169
D-99625 Beichlingen

Telefon: +49 (0) 171-7915167
Fax: +49 (0) 3635-602978
E-Mail: Sven.Mendler@WEDACO.de
Internet: www.WEDACO.de