LU12b - Logdateien

In Logdateien werden Ereignisse, Zustände und Aktivitäten eines Systems aufgezeichnet. Sie dienen als Basis für die Überwachung und Fehlersuche .

Insgesamt ist das Logging in verteilten Systemen ein wesentlicher Bestandteil der Betriebsführung und Fehlerbehandlung. Durch effektives Logging können Entwickler und Administratoren die Integrität, Leistung und Sicherheit des Systems gewährleisten und potenzielle Probleme frühzeitig erkennen und beheben.

Aspekte beim Erstellen von Logdateien

Ereignisprotokollierung

Jedes Ereignis oder jede Aktivität in einem verteilten System, sei es eine Anforderung, eine Fehlermeldung, eine Transaktion oder eine Systemwarnung, wird protokolliert. Diese Protokolle dienen als Aufzeichnung für spätere Analysen und diagnostische Zwecke.

Zentralisierte und verteilte Protokollierung

In verteilten Systemen können Protokolle zentralisiert oder dezentralisiert sein. Bei einer zentralisierten Protokollierung werden alle Protokolle an einem zentralen Ort gesammelt und gespeichert, während bei einer verteilten Protokollierung Protokolle an verschiedenen Standorten oder Knoten im System gesammelt werden.

Protokollformate und Strukturen

Protokolle können in verschiedenen Formaten und Strukturen vorliegen, einschliesslich Textdateien, JSON, XML oder Binärdateien. Die Wahl des Formats hängt von den Anforderungen an die Lesbarkeit, Speicherung und Analyse der Protokolle ab.

Protokollierungsstufen und -niveaus

Protokolle können verschiedene Stufen oder Niveaus von Informationen enthalten, die den Schweregrad und die Bedeutung der Ereignisse widerspiegeln. Typische Stufen umfassen Debugging, Information, Warnung, Fehler und kritische Fehler.

Protokollrotation und -verwaltung

Da Protokolldateien im Laufe der Zeit wachsen können, ist eine effektive Protokollrotation und -verwaltung wichtig. Dies umfasst das regelmäßige Rotieren oder Löschen alter Protokolldateien sowie die Implementierung von Mechanismen zur Sicherstellung, dass Protokolle nicht die verfügbaren Speicherressourcen übermäßig beanspruchen.

Sicherheit und Datenschutz

Bei der Protokollierung in verteilten Systemen ist auch die Sicherheit und der Datenschutz zu beachten. Dies beinhaltet die Verschlüsselung von Protokollen, die Beschränkung des Zugriffs auf sensible Protokolldaten und die Einhaltung von Datenschutzbestimmungen und -vorschriften.

Analyse und Monitoring

Gesammelte Protokolle werden oft analysiert und überwacht, um Leistungsprobleme, Fehler oder Anomalien zu erkennen. Dies kann manuell durch Inspektion der Protokolle oder automatisiert mithilfe von Überwachungstools und Analysesystemen erfolgen.

Beispiel: Apache HTTP Server

access.log

Im `access.log` werden alle Zugriffe auf den Server protokolliert. Mit Hilfe dieser Datei können wir Fehler, Engpässe aber auch Angriffe auf unseren Server erkennen.

```
***.***.***.*** - - [08/Apr/2024:00:00:47 +0200] "GET
/wikiV2/modul/m426/projektideen/start?ns=modul/m231/learningunits/lu03&tab_f
iles=files&do=media HTTP/1.1" 200 12368
"https://www.it.bzz.ch/wikiV2/modul/m426/projektideen/start?ns=modul/m231/le
arningunits&tab_files=files&do=media" "Mozilla/5.0 (Linux; Android 7.0;)
AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible;
PetalBot;+https://webmaster.petalsearch.com/site/petalbot)"
***.***.***.*** - - [08/Apr/2024:00:00:56 +0200] "GET
/wikiV2/howto/aws/start HTTP/1.1" 200 12824 "-" "Mozilla/5.0
AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0;
+http://www.bing.com/bingbot.htm) Chrome/116.0.1938.76 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:01:46 +0200] "GET
/wikiV2/modul/m321/learningunits/start?tab_files=upload&do=media&ns=modul/m1
83 HTTP/1.1" 200 11788
"https://cloud.it.bzz.ch/wikiV2/modul/m321/learningunits/start?ns=modul/m183
&tab_files=files&do=media" "Mozilla/5.0 (Linux; Android 7.0;)
AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible;
PetalBot;+https://webmaster.petalsearch.com/site/petalbot)"
***.***.***.*** - - [08/Apr/2024:00:02:26 +0200] "GET
```

```
/wikiV2/modul/m323/learningunits/lu06/loesungen/blueprints HTTP/1.1" 200
14548
"https://casa.it.bzz.ch/wikiV2/doku.php?id=modul%3Am323%3Alearningunits%3Alu
06%3Aloesungen%3Ablueprints&rev=1696511304" "Mozilla/5.0 (Linux; Android
7.0;) AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36
(compatible; PetalBot;+https://webmaster.petalsearch.com/site/petalbot)"
***.***.***.*** - - [08/Apr/2024:00:02:52 +0200] "GET
/wikiV2/modul/m122/javascript?ns=modul/m293/learningunits/lu02/aufgaben&tab_
files=files&do=media HTTP/1.1" 200 11849
"https://casa.it.bzz.ch/wikiV2/modul/m122/javascript?ns=modul/m293/learningu
nits/lu02&tab_files=files&do=media" "Mozilla/5.0 (Linux; Android 7.0;)
AppleWebKit/537.36 (KHTML, like Gecko) Mobile Safari/537.36 (compatible;
PetalBot;+https://webmaster.petalsearch.com/site/petalbot)"
***.***.***.*** - - [08/Apr/2024:00:03:33 +0200] "GET
/wikiV2/lib/exe/css.php?t=bootstrap3&tseed=5f67e5457e0b7591a8355ccbcc27cda5
HTTP/1.1" 200 214697 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
Chrome/100.0.4896.127 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:03:34 +0200] "GET
/wikiV2/lib/tpl/bootstrap3/css.php?f=bootstrap.css HTTP/1.1" 200 3784 "-"
"Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; bingbot/2.0;
+http://www.bing.com/bingbot.htm) Chrome/100.0.4896.127 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:03:35 +0200] "GET
/wikiV2/lib/tpl/bootstrap3/assets/bootstrap/default/bootstrap.min.css
HTTP/1.1" 200 125343 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
Chrome/100.0.4896.127 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:03:37 +0200] "GET
/wikiV2/lib/tpl/bootstrap3/iconify.php?prefix=mdi&icons=magnify,wrench,accou
nt,toolbox,file-document-outline,home,share-
variant,twitter,linkedin,facebook,pinterest,telegram,whatsapp,yammer,reddit,
microsoft-teams,calendar,chevron-up,folder-open,folder,chevron-down
HTTP/1.1" 200 12813 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
Chrome/100.0.4896.127 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:07:38 +0200] "GET
/wikiV2/lib/tpl/bootstrap3/iconify.php?prefix=mdi&icons=magnify,wrench,accou
nt,toolbox,file-document-outline,home,share-
variant,twitter,linkedin,facebook,pinterest,telegram,whatsapp,yammer,reddit,
microsoft-teams,calendar,chevron-up,folder-open,folder,chevron-down
HTTP/1.1" 200 12813 "-" "Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko;
compatible; bingbot/2.0; +http://www.bing.com/bingbot.htm)
Chrome/100.0.4896.127 Safari/537.36"
***.***.***.*** - - [08/Apr/2024:00:07:50 +0200] "GET
/wikiV2/_media/modul/m320/learningunits/lu05/aufgaben/lu03-aufg8-
schulverwaltung-1.png?h=90&tok=ce481d&w=90 HTTP/1.1" 200 90209 "-"
"Mozilla/5.0 (Linux; Android 5.0) AppleWebKit/537.36 (KHTML, like Gecko)
Mobile Safari/537.36 (compatible; Bytespider; spider-
feedback@bytedance.com)"
***.***.***.*** - - [08/Apr/2024:00:10:24 +0200] "GET
/wikiV2/_media/howto/virtualmachine/fontsize02.png?w=400&tok=679db4
```

```
HTTP/1.1" 200 63044 "-" "Googlebot-Image/1.0"
```

Aus Datenschutzgründen wurden die IP-Adressen des Clients durch Sterne ersetzt.

error.log

Im Error-Log werden verschiedene Arten von Fehlern protokolliert. Dabei ist es abhängig von der Konfiguration, ob auch Warnungen und Informationen aufgezeichnet werden. Neben Fehlern in den Applikationen kann das Error-Log auch auf mögliche Angriffe durchsucht werden.

```
[Sun Apr 07 02:24:01.838719 2024] [php7:error] [pid 1980703] [client
***.***.***.***:48480] script '/var/www/it.bzz.ch/wp-login.php' not found or
unable to stat
[Sun Apr 07 06:29:58.968286 2024] [access_compat:error] [pid 1982505]
[client ***.***.***.***:50430] AH01797: client denied by server
configuration: /var/www/it.bzz.ch/vendor
[Sun Apr 07 06:29:59.357233 2024] [php7:error] [pid 1981328] [client
***.***.***.***:50482] script '/var/www/it.bzz.ch/phpinfo.php' not found or
unable to stat
[Sun Apr 07 06:29:59.506455 2024] [php7:error] [pid 1982498] [client
***.***.***.***:50502] script '/var/www/it.bzz.ch/info.php' not found or
unable to stat
[Sun Apr 07 06:29:59.751310 2024] [access_compat:error] [pid 1982324]
[client ***.***.***.***:50532] AH01797: client denied by server
configuration: /var/www/it.bzz.ch/vendor
[Sun Apr 07 06:30:01.022539 2024] [access_compat:error] [pid 1982603]
[client ***.***.***.***:50694] AH01797: client denied by server
configuration: /var/www/it.bzz.ch/data
[Sun Apr 07 06:30:08.751906 2024] [php7:error] [pid 1982324] [client
***.***.***.***:39722] script '/var/www/it.bzz.ch/phpinfo.php' not found or
unable to stat
[Sun Apr 07 15:33:21.705306 2024] [php7:warn] [pid 1985319] [client
***.***.***.***:58265] PHP Warning:  call_user_func_array() expects
parameter 1 to be a valid callback, class 'Doku_Renderer_metadata' does not
have a method 'table_align' in /var/www/it.bzz.ch/wikiV2/inc/parserutils.php
on line 535, referer: https://moodle.bzz.ch/
[Sun Apr 07 15:41:38.115651 2024] [php7:error] [pid 1985320] [client
***.***.***.***:51200] script '/var/www/it.bzz.ch/wp-login.php' not found or
unable to stat
[Sun Apr 07 19:42:12.761806 2024] [php7:error] [pid 1986230] [client
***.***.***.***:36316] script '/var/www/it.bzz.ch/wp-login.php' not found or
unable to stat
```

M321-LU12