Understanding Barracuda Message Archiver Syslog Data

https://campus.barracuda.com/doc/42047885/

This article refers to the Barracuda Message Archiver firmware version 5.0 or higher.

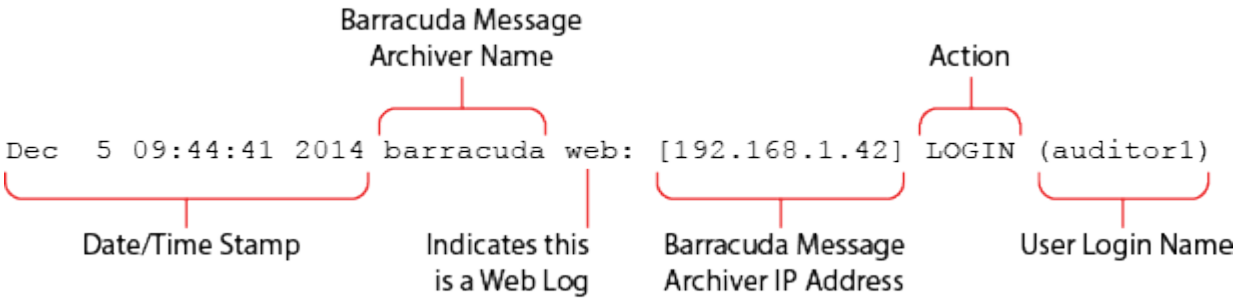
If remote logging servers are configured, you can designate a Syslog server to which to send Barracuda Message Archiver web interface and mail syslog data on the **Advanced > Syslog** page in the web interface.

Click **Monitor Syslog** in the web interface to open a new browser window and view data as it is generated.

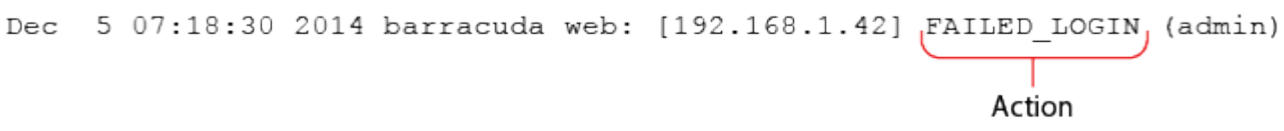
Web Interface Syslog

The Web Interface Syslog includes information related to configuration changes made from the web interface, as well as any user login activities. The data appears on the local facility with login information at the info priority level, and configuration changes at the debug priority level on the specified Syslog server.

Example 1. User Login.



Example 2. Failed Login Attempt.



Example 3. Virus Scanning Disabled by Admin.

```
Dec  5 09:28:53 2014 barracuda web: [192.168.1.42] global[] CHANGE scana_filter_virus_check (No) [admin]
```

Action

Mail Syslog

The Mail Syslog includes mail-related data such as timestamp, mail type, unique message identifier, message size, envelope 'From' and 'To' addresses, and any additional information related to the message (for example, the uncompressed message size and size occupied on disk). The data appears on the mail facility at the debug priority level on the specified mail server.

Example 1. New Message from jae.black@enron.com to david.forster@enron.com and larry.valderrama@enron.com with Timestamp 1411416561.

```
Sep 22 16:09:21 2014 barracuda [worker] - new_mail: fc49e66f5889785eb723c634f4061b88 1411416561 <jae.black@enron.com> david.forster@enron.com 0 inbound 10581 4096
Sep 22 16:09:21 2014 barracuda [worker] - new_mail: fc49e66f5889785eb723c634f4061b88 1411416561 <jae.black@enron.com> larry.valderrama@enron.com 0 inbound 10581 4096
```

Reserved
Uncompressed Message Size
Size Occupied on Disk

Example 2. Two Separate New Messages from lynn.blair@enron.com.

In this example, the IDs after `new_mail` are different, showing that these are different messages.

```
Sep 22 16:09:17 2014 barracuda [worker] - new_mail: afdd42d518ab9b0ec4929ce35bee9a58 1411416557 lynn.blair@enron.com rick.dietz@enron.com 0 inbound 4038 4096
Sep 22 16:09:17 2014 barracuda [worker] - new_mail: 709771f3fd82a6204eefa0dd425b6276 1411416557 lynn.blair@enron.com center.ets@enron.com 0 inbound 3568 4096
```

Figures

1. user_login.png
2. failed_login.png
3. scan_disable.png
4. example1.png
5. example2.png