Centralized Event Logging Support

Ubersmith can log system events to a syslog daemon, which can then be forwarded along to a centralized logging service. This is an important capability for PCI-DSS compliance as well as for security purposes.

By default, Ubersmith is not configured to log system events out to the main host's syslog daemon, so some configuration updates are required. This documentation assumes that your installation is in the default location of `/usr/local/ubersmith`.

On this page:

On this page:

Implementation

In Ubersmith's `/usr/local/ubersmith/docker-compose.yml` file, there is an `rsyslog` service defined, which is normally unused. When started, this service creates a socket in:

`/usr/local/ubersmith/logs/rsyslog/`

```
root@billing:/usr/local/ubersmith/logs/rsyslog# ls -l
total 0
srw-rw-rw- 1 root root 0 Nov 20 12:17 log
root@billing:/usr/local/ubersmith/logs/rsyslog# file log
log: socket
```

The `php` service, which executes Ubersmith's code, then mounts this socket as a volume and Ubersmith's code is able to send log messages to the syslog daemon.

Configuration

It is possible that upon the initial configuration of this feature, there will be unwanted contents in `/usr/local/ubersmith/logs/rsyslog`, which should be deleted. After deleting the contents of that directory, execute the following commands in your Ubersmith root:

The following commands will cause a brief interruption of service as the `php` container will not be online to process requests.

```
docker-compose rm -sf php rsyslog
docker-compose up -d rsyslog
docker-compose up -d php
```

This will create the socket in `/usr/local/ubersmith/logs/rsyslog/` and allow the `php` container to mount it.

These logs will then appear on the main system, at `/var/log/ubersmith/ubersmith/docker.log`. The logs will use the syslog tag `ubersmith/ubersmith`.

If `/var/log/ubersmith` is empty, try restarting the rsyslog daemon. This is typically achieved with the command:

`service rsyslog restart`

The main system's rsyslog configuration can be updated to forward logs on to a centralized logging system. It is possible to filter the logs forwarded based on syslog tags, but that is outside the scope of this documentation.

It may be necessary to edit the Ubersmith startup script `ubersmith_start.sh` to include the `rsyslog` service in the "`docker-compose up`" command. This will ensure the service is started when this script is executed.

Related Topics