Remote logging

Version: 3581

Table of Contents

Remote logging

Overview

Remote logging uses the built-in syslog subsystem to send syslog messages to a remote log host.
Messages are sent using the standard
No additional packages are required for use of Remote logging

Requirements

A remote server configured to receive syslog messages.
A valid DNS server configured if the remote server is specified by DNS name.

Configuration

Configuration of remote logging can be done by simply using the menu system.
To access this menu option follow the Main Menu ---> #1. Configuration menu ---> #2. Global Configuration ---> #3. Configure Event Logging ---> #1. Configure remote event logging.
This will activate a configuration script that will require two parameters; the ip address or Dns Name of the remote logging server and the logging facility. Only advanced users will need to set the logging facility. The default is blank.
Once the user inputs both parameters the logging system will restart and messages will be sent via UDP port 514 to the remote logging server.

Example of user Configuration

Follow the menu system: Main Menu ---> #1. Configuration menu ---> #2. Global Configuration ---> #3. Configure Event Logging ---> #1. Configure remote event logging.
After using the Menu system the customer below entered 10.30.0.52 as the remote logging server(Dns Names are valid). And they leaving the facility disabled by just hitting enter. Below is the output that you see when configuring this service.

```
Remember that you must configure your remote syslog server to accept syslog data from
remote systems.  Most syslog implementations use '-r' to enable this function.  Consult
your server documentation or man pages.

Enter name or IP address of machine to log to, or leave blank to disable remote logging: 10.30.0.
Do you want to log message to a specific local facility?
Enter the facility (i.e. 'local6' without quotes) or leave blank to disable facility logging:

Now rebuilding /etc/syslog.conf...done.
done.
```

After configuring this remote logging you can see the router sending the syslog messages to the remote server.

```
sa-gateway:/usr/local/sand# tcpdump -i eth0.1030 port 514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0.1030, link-type EN10MB (Ethernet), capture size 65535 bytes
15:59:53.760642 IP 10.30.0.1.syslog > 10.30.0.52.syslog: SYSLOG daemon.notice, length: 77
15:59:53.760658 IP 10.30.0.1.syslog > 10.30.0.52.syslog: SYSLOG daemon.notice, length: 117
15:59:53.763547 IP 10.30.0.1.syslog > 10.30.0.52.syslog: SYSLOG daemon.notice, length: 85
15:59:54.048002 IP 10.30.0.1.syslog > 10.30.0.52.syslog: SYSLOG auth.info, length: 75
4 packets captured
7 packets received by filter
0 packets dropped by kernel
```