DISCLAIMER! This document is nothing more than the musings of the author as he attempts to perform the stated tasks. Conclusions and approaches may very well be incorrect, inefficient, or otherwise outside of professionally accepted best practices. Use this document at your own risk! In this document, screen outputs will be presented in **green**. Where keyboard input is required, the prompt will be in bolded red. **#** means you should be at the super user prompt, **$** means you should be at an unprivileged user prompt. Do not include these prompts in your input! The command to be typed will be shown in **blue**.

# ls -al

means you type ls -al at the super user prompt. We have a few systems in our network. Having to review log files on each system is a serious effort in time. A better approach would be to send all of the log files to a centralized server, so we can monitor them from a single system. This section will explain how to do this on a Solaris 10 box.

The first thing you need to do is to define a loghost in your /etc/hosts (or dns which is not covered in this documentation since we don't use dns).

Your host file entry should be like this...

```
192.168.10.15   10ADM 10ADM.wwwpages.com  loghost
```

In this scenario, the box 10ADM is going to be a loghost. Notice we added entries on the host file line with the FQDN (fully qualified doman name) of the server.

The next step is to let 10ADM know it is going to act as a loghost.

```
# svccfg -s system-log setprop config/log_from_remote=true
```

You may have to update the legacy service as well, so edit the /etc/default/syslogd file and uncomment the line stating

```
LOG_FROM_REMOTE=YES
```

Now we tell our client system (in this case, 11ADM) that 10ADM is the loghost. To do this, modify the host file entry on 11ADM for 10ADM as shown above. Make sure that 11ADM's host file doesn't include any other loghost entries.

Now on both 10ADM and 11ADM, restart the syslog service

```
# svcadm restart system-log:default
```

I was having problems getting it to work, until I ran the following command on 10ADM

```
# syslogd -d
```

and noticed the output was giving me a lot of errors about my config file. I remembered that **syslog.conf HATES spaces**. Sure enough, when I copied and pasted, the tabs were converted to spaces. A few minutes of editing and all was working fine!

```
 #ident  "@(#)syslog.conf        1.5     98/12/14 SMI"   /* SunOS 5.0 */
#
# Copyright (c) 1991-1998 by Sun Microsystems, Inc.
# All rights reserved.
#
# syslog configuration file.
#
# This file is processed by m4 so be careful to quote (`') names
# that match m4 reserved words.  Also, within ifdef's, arguments
# containing commas must be quoted.
#
*.err;kern.notice;auth.notice                   /dev/sysmsg
*.err;kern.debug;daemon.notice;mail.crit        ifdef(`LOGHOST', /var/adm/messages, @loghost)
*.alert;kern.err;daemon.err                     operator
*.alert                                         root
*.emerg                                         *
# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
auth.debug                      ifdef(`LOGHOST', /var/log/authlog, @loghost)
mail.debug                      ifdef(`LOGHOST', /var/log/maillog, @loghost)
#
# non-loghost machines will use the following lines to cause "user"
# log messages to be logged locally.
#
ifdef(`LOGHOST', ,
user.err                          /dev/sysmsg
user.err                          /var/adm/messages
user.alert                        `root, operator'
user.emerg                           *
)
```

Notice that I have a maillog file. I created that, so my mail related stuff would show up here, and not in syslog. In order to get this to work, I had to do the following:

# touch /var/log/maillog

# chmod 644 /var/log/maillog

# logadm -w /var/log/maillog -s 20m

The later rotates the log when it gets to 20mb.

All that remains to be done is to install the same syslog.conf on each box I wish to use, update the host file to show 10ADM as the loghost, then restart the system-log service (**# svcadm restart system-log**
)

<< end of document >>