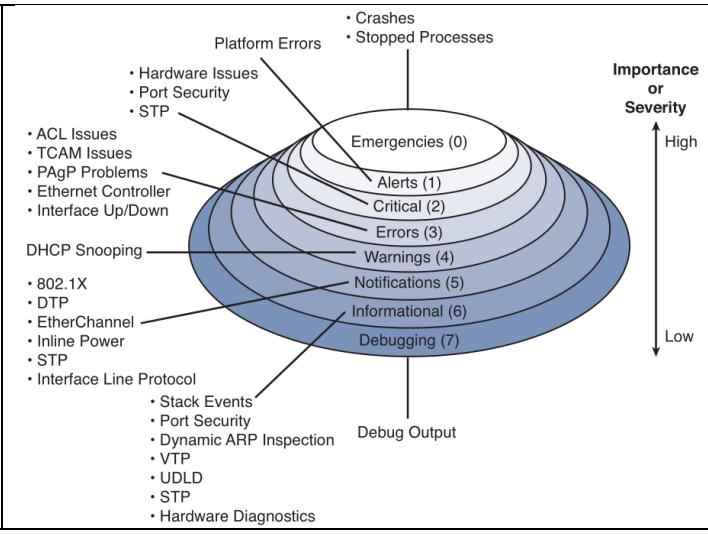
SYSLOG (LOGGING) cloudkod.com

Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unstable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG



Destination	Location	Enabled by default
Buffer	Local buffer	yes
Console	Local console	yes
Monitor	VTY lines	no
Host	Remote syslog	no

Logging Message Format

Element	Format	Purpose	Enabled	Command
Sequence #	xxxxxx	Simple incrementing number	no	service sequence-numbers
Timestamp	HH:MM:SS M D HH:MM:SS	Device uptime using internal clock Actual time using internal clock or NTP	yes no	service timestamps log uptime service timestamps log datetime
Facility	%	Categorizes the function or module that generated the message Default is Local7	yes	
Severity	0-7	Syslog severity level	yes	
MNEMONIC	CONFIG_I	Text string that uniquely describes the message	yes	
Description	…	Text string containing detailed information about the event	yes	

Default Config;

root@R3# show system syslog |display set
set system syslog user * any emergency → * means all users will get emergency alerts on terminals
set system syslog file messages any any → log all messages into a file called 'messages'.
set system syslog file messages authorization info → logging SSH/HTTPS access
set system syslog file interactive-commands interactive-commands any → This shows all the commands (show/edit..etc) enter'd.
show log messages | last |no-more
file show /var/log/messages |last |no-more
show log interactive-commands |last |no-more

Send all Authorization syslog messages to a file; # set system syslog file **AUTH** authorization any

```
root@Core1> file show /var/log/AUTH
Feb 21 05:12:02  Core1 login: Login attempt for user root from host [unknown]
Feb 21 05:12:05  Core1 login: creating file /var/run/10305.env
Feb 21 05:12:05  Core1 login[10305]: (pam_sm_authenticate): DEBUG: PAM_USER: root
Feb 21 05:12:05  Core1 login[10305]: (pam_sm_authenticate): DEBUG: Updating lock-attempts of user: root  attempts: 1
Feb 21 05:12:05  Core1 login[10305]: (pam_sm_acct_mgmt): DEBUG: PAM_USER: root
Feb 21 05:12:05  Core1 login[10305]: LOGIN_INFORMATION: User root logged in from host [unknown] on device ttyu0
Feb 21 05:12:05  Core1 login[10305]: LOGIN_ROOT: User root logged in as root from host [unknown] on device ttyu0
```

Send all commands to file COMMANDS and display logs with severity level:

set system syslog file **COMMANDS** explicit-priority interactive-commands any

```
root@Core1> show log COMMANDS
Feb 21 05:20:32  Core1 mgd[10311]: %INTERACT-6-UI_CMDLINE_READ_LINE: User 'root', command 'show log COMMANDS '
```

Severity level = 6 → informational syslog messages

CONSOLE LOGGING:

Log all messages to console (not telnet/ssh session) using: # **set system syslog console any any**

You can log specific info, instead logging everything using;

root@Core1# **set system syslog console ?**

Possible completions:

any	All facilities
authorization	Authorization system
change-log	Configuration change log
ntp	NTP process
user	User processes

To login and view on console terminal, all the commands enter'd by a specific user using any severity level;

 # set system syslog user root interactive-commands any

Log everything to remote syslog server **# set system syslog host 10.10.10.125 any any**

Syslog Configuration

Ensure that all the devices have following Syslog configuration:

4) All "emergency" messages regardless of facility are displayed on terminals of all currently logged users.
5) All messages regardless of facility with the severity level of "info" and higher are sent to the default syslog file.
6) A file named "interactive-commands" for command audit tracking receives records about the users and commands they execute.
7) A separate file named "authorization-file" is used for authorization messages with the severity "info" and higher.
8) All messages with severity level "warning" and higher regardless of facility are sent to the S1 syslog server. Additionally use explicit priority tag and prefix message "JNCIE-ENT".
9) The archive size is set to 3 files with 100K size each.

Use the example below as a reference for this task configuration.

```
[edit system syslog]
lab@Mercury# show
archive size 100k files 3;
user * {
    any emergency;
}
host 10.10.10.1 {
    any warning;
    log-prefix JNCIE-ENT;
    explicit-priority;
}
file messages {
    any info;
}
file interactive-commands {
    interactive-commands info;
}
file authorization-file {
    authorization info;
}
```