Cheatography

Syslog Cheat Sheet

by Awfki via cheatography.com/35829/cs/11368/

Severity

Value	Severity	Keyword
0	Emergency	emerg
1	Alert	alert
2	Critical	crit
3	Error	err
4	Warning	warning
5	Notice	notice
6	Informational	info
7	Debug	debug

Our Local Facilities

local0	Internet Edge
local1	Internet Firewalls
local2	VPN Firewalls
local3	Core - Agg - DMZ/Outside
local4	Distribution
local5	Mgmt Network
local6	AAA
local7	

Our Syslog Ports

Cisco	514
Palo Alto	1514
SecureAuth	11514
ISE	2514
Extrahop	3514

We use different ports so that Logstash can filter the different log formats.

Facility

Facility Code	Keyword	Description
0	kern	kernel messages
1	user	user-level msgs
2	mail	mail system
3	daemon	system daemons
4	auth	security/auth msgs
5	syslog	mgs gen'd by syslogd
6	lpr	line printer msgs
7	news	network news msgs
8	uucp	UUCP
9		clock daemon
10	authpriv	security/auth msgs
11	ftp	ftpd
12		NTP subsystem
13		log audit
14		log alert
15	cron	scheduling daemon
16	local0	local use
17	local1	local use
18	local2	local use
19	local3	local use
20	local4	local use
21	local5	local use
22	local6	local use
23	local7	local use