

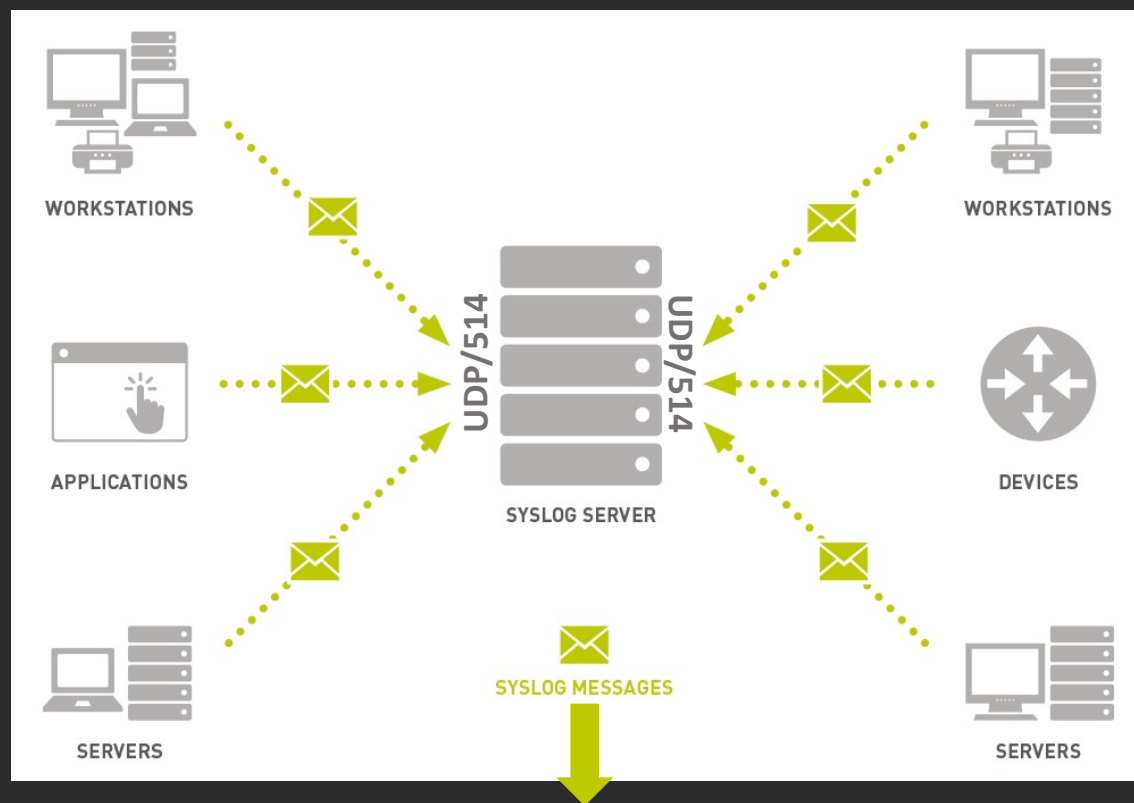
Lesson 8: Administering the System

Objectives covered

- *107.1 Manage user and group accounts and related system files (weight: 5)*
- *108.2 System logging (weight: 4)*
- *108.1 Maintain system time (weight: 3)*
- *108.3 Mail Transfer Agent (MTA) basics (weight: 3)*

System logging

Syslog protocol



<165>1 2019-08-01T15:30:54.001Z ubuntu-box apache 200 20031 - " The Apache Server encountered an error"

PRI **HEADER** **MSG**

PRI = facility value*8 + serverity value

HEADER = Timestamp + Hostname/IP

MSG = process name + PID + MsgID + Content

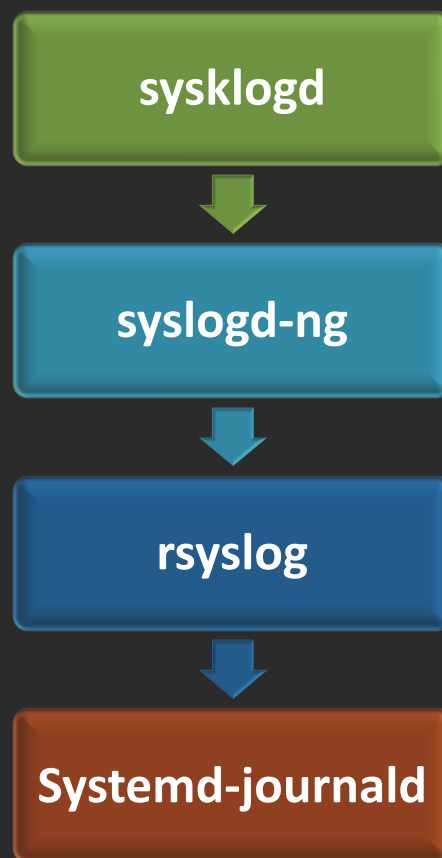
Syslog protocol – facility values

Code	Keyword	Description
0	kern	Messages generated by the system kernel
1	user	Messages generated by user events
2	mail	Messages from a mail application
3	daemon	Messages from system applications running in background
4	auth	Security or authentication messages
5	syslog	Messages generated by the logging application itself
6	lpr	Printer messages
7	news	Messages from the news application
8	uucp	Messages from the Unix-to-Unix copy program
9	cron	Messages generated from the cron job scheduler
10	authpriv	Security or authentication messages
11	ftp	File Transfer Protocol application messages
12	ntp	Network Time Protocol application messages
13	security	Log audit messages
14	console	Log alert messages
15	solaris-cron	Another scheduling daemon message type
16-23	local0-local7	Locally defined messages

Syslog protocol – severity values

Code	Keyword	Description
0	emerg	The event causes the system to be unusable
1	alert	An event that requires immediate attention
2	crit	An event that is critical but doesn't require immediate attention
3	err	An error condition that allows the system or application to continue
4	warning	A non-normal warning condition in the system or application
5	notice	A normal but significant condition message
6	info	An informational message from the system
7	debug	Debugging messages for developers

Linux logging applications




rsyslog configuration

/etc/rsyslogd.conf




facility.serverity action



```
auth,authpriv.*      /var/log/auth.log
*.*;auth,authpriv.none -/var/log/syslog
kern.*                -/var/log/kern.log
mail.*                -/var/log/mail.log
mail.err              /var/log/mail.err
*.emerg                :omusrmsg:*
```

Ubuntu



```
*.info;mail.none;authpriv.none;cron.none /var/log/messages
authpriv.*                               /var/log/secure
mail.*                                   -/var/log/maillog
cron.*                                  /var/log/cron
*.emerg                                 :omusrmsg:*
uucp,news.crit                           /var/log/spooler
local7.*                                 /var/log/boot.log
```

CentOS

rsyslog send logs to syslog server

/etc/rsyslogd.conf



***facility.serverity* TCP | UDP[(z#)]HOST:[PORT#]**

- *TCP/UDP*: You can select either the TCP or UDP protocols (covered in Chapter 8) to transport your log messages to the central log server. UDP can lose data, so you should select TCP if your log messages are important. Use a single at sign (@) to select UDP and double at signs (@@) to choose TCP.
- [(z#)]: The brackets indicate this syntax is optional. The z selects zlib to compress the data prior to traversing the network, and the # picks the compression level, which can be any number between 1 (lowest compression) and 9 (highest compression). Note that you must enclose the z and the number between parentheses, such as (z5).
- HOST: This syntax designates the central logging server either by a fully qualified domain name (FQDN), such as example.com, or an IP address. If you use an IPv6 address, it must be encased in brackets.
- [PORT#]: The brackets indicate that this syntax is optional. This designates the port on the remote central logging host where the log service is listening for incoming traffic.

```
*.* @@(z9)loghost.ivytech.edu:6514
```

Rotating logs

Directive	Description
hourly	Log file is rotated hourly. If this setting is employed, the schedule for the logrotate cron job typically needs modification.
daily	Log file is rotated daily.
weekly <i>n</i>	Log file is rotated weekly on the <i>n</i> day of the week, where 0 is equal to Sunday, 1 is equal to Monday, 2 is equal to Tuesday, and so on to 6 for Saturday. 7 is a special number that indicates the log file is rotated every 7 days, regardless of the current day of the week.
monthly	Log file is rotated the first time logrotate is run within the current month.
size <i>n</i>	Rotates log file based on size and not time, where <i>n</i> indicates the file's size that triggers a rotation (<i>n</i> followed by nothing or k assumes kilobytes, M indicates megabytes, and G denotes gigabytes).
rotate <i>n</i>	Log files rotated more than <i>n</i> times are either deleted or mailed, depending on other directives. If <i>n</i> equals 0, rotated files are deleted, instead of rotated.
dateformat <i>format-string</i>	Modify the dateext setting's date string using the <i>format-string</i> specification.
missingok	If log file is missing, do not issue an error message and continue on to the next log file.
notifempty	If the log file is empty, do not rotate this log file, and continue on to the next log file.

```
$ cat /etc/logrotate.conf
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# use date as a suffix of the rotated file
dateext

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp and btmp -- we'll rotate them here
/var/log/wtmp {
    monthly
    create 0664 root utmp
    minsize 1M
    rotate 1
}

/var/log/btmp {
    missingok
    monthly
    create 0600 root utmp
    rotate 1
}

# system-specific logs may be also be configured here.
$
```

Log your own application

logger [-isd] [-f file] [-p priority] [-t tag] [-u socket] [message]

```
$ logger This is a test message from rich
$ tail /var/log/syslog
...
Feb  8 20:21:02 myhost rich: This is a test message from rich
```

systemd-journald

/etc/systemd/journald.conf

Directive	Description
Storage=	Set to auto, persistent, volatile, or none. Determines how systemd-journald stores event messages. (Default is auto.)
Compress=	Set to yes or no. If yes, journal files are compressed. (Default is yes.)
ForwardToSyslog=	Set to yes or no. If yes, any received messages are forwarded to a separate syslog program, such as rsyslogd, running on the system. (Default is yes.)
ForwardToWall=	Set to yes or no. If yes, any received messages are forwarded as wall messages to all users currently logged into the system. (Default is yes.)
MaxFileSec=	Set to a number followed by a time unit (such as month, week, or day) that sets the amount of time before a journal file is rotated (archived). Typically this is not needed if a size limitation is employed. To turn this feature off, set the number to 0 with no time unit. (Default is 1month.)
RuntimeKeepFree=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald must keep free for other disk usages when employing volatile storage. (Default is 15% of current space.)
RuntimeMaxFileSize=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald journal files can consume if it is volatile.
RuntimeMaxUse=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald can consume when employing volatile storage. (Default is 10% of current space.)
SystemKeepFree=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald must keep free for other disk usages when employing persistent storage. (Default is 15% of current space.)
SystemMaxFileSize=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald journal files can consume if it is persistent.
SystemMaxUse=	Set to a number followed by a unit (such as K, M, or G) that sets the amount of disk space systemd-journald can consume when employing persistent storage. (Default is 10% of current space.)

Journal files

```
$ ls /var/log/journal/e9af6ca5a8fb4a70b2ddec4b1894014d/
system@220262350f2a468c87bb85484e9ad813-0000000000000001-0005897bfdead50c.journal
system@220262350f2a468c87bb85484e9ad813-000000000000197b0-000589f47e451cdc.journal
system@80103f1d22df49c7beee5c818e58f96f-0000000000000001-000587c56d17a0fd.journal
[...]
system.journal
user-1000@be988ab4869e43239d9cfdebd38c7e72-00000000000000451-000571ee64814f08.journal
user-1000@be988ab4869e43239d9cfdebd38c7e72-000000000000004e25-000584a03f80097a.journal
[...]
user-1000.journal
user-1001@e19748f488ce450b94e17fed79ee9669-000000000000028c7-000572dfa721935c.journal
[...]
user-1001.journal
[...]
```

Systemd-journald and syslog working together

Journal Client Method

- `$ grep ModLoad /etc/rsyslog.conf | grep -E "imjournal | imuxsock"`
\$ModLoad imuxsock # provides support for local system logging [...]
\$ModLoad imjournal # provides access to the systemd journal

Forward to Syslog Method

- To use this method, you need to modify the journal configuration file, `/etc/systemd/journald.conf`, and set the `ForwardToSyslog` directive to `yes`
- This method employs the file `/run/systemd/journal/syslog`

Viewing journals

journalctl [OPTIONS...] [MATCHES...]

Options

Short option	Long option	Description
-a	--all	Display all data fields, including unprintable characters.
-e	--pager-end	Jump to the end of the journal and display the entries.
-k	--dmesg	Display only kernel entries.
-n <i>number</i>	--lines= <i>number</i>	Show the most recent <i>number</i> journal entries.
-r	--reverse	Reverse the order of the journal entries in the output.
-S <i>date</i>	--since= <i>date</i>	Show journal entries starting at <i>date</i> , where <i>date</i> is formatted as YYYY-MM-DD:HH:MM:SS. If time specification is left off of <i>date</i> , then 00:00:00 is assumed. Keywords such as yesterday, today, tomorrow, and now can all replace <i>date</i> .
-U <i>date</i>	--until= <i>date</i>	Show journal entries until <i>date</i> is reached in the entries. <i>date</i> formatting is the same as it is for the -S option.
-u <i>unit</i> or <i>pattern</i>	--unit= <i>unit</i> or <i>pattern</i>	Show only journal entries for the systemd <i>unit</i> or systemd units that match <i>pattern</i> .

Matches

Match	Description
<i>field</i>	Match the specific <i>field</i> in the journal. Can enter multiple occurrences of <i>field</i> on same line but must be separated with a space. You can separate multiple <i>field</i> specifications with a plus sign (+) to use a <i>logical or</i> between them.
OBJECT_PID= <i>pid</i>	Match only entries made by the specified application <i>pid</i> .
PRIORITY= <i>value</i>	Match only entries with the specified priority value. The value can be set to one of the following numbers or keywords: emerg (0), alert (1), crit (2), err (3), warning (4), notice (5), info (6), debug (7).
_HOSTNAME= <i>host</i>	Match only entries from the specified <i>host</i> .
_SYSTEMD_UNIT= <i>unit.type</i>	Match only entries made by the specified systemd <i>unit.type</i> .
_TRANSPORT= <i>transport</i>	Match only entries received by the specified <i>transport</i> method.
_UDEV_SYSNAME= <i>dev</i>	Match only entries received from the specified device.
_UID= <i>userid</i>	Match only entries made by the specified user ID.

```
$ sudo journalctl --since=today _SYSTEMD_UNIT=ssh.service
-- Logs begin at Wed 2018-07-25 12:02:39 EDT, end at Wed 2019-05-29 [...]
May 29 14:10:50 Ubuntu1804 sshd[772]: Server listening on 0.0.0.0 port 22.
May 29 14:10:50 Ubuntu1804 sshd[772]: Server listening on :: port 22.
May 29 14:10:55 Ubuntu1804 sshd[772]: Received SIGHUP; restarting.
[...]
```

Managing journals

Cleanup archived journals

Option	Description
<code>--disk-usage</code>	Show total disk usage of all journal files
<code>--vacuum-size=BYTES</code>	Reduce disk usage below specified size
<code>--vacuum-time=TIME</code>	Remove journal files older than specified time

```
$ journalctl --disk-usage
Archived and active journals take up 344.0M in the file system.
$
$ sudo journalctl --vacuum-size=300M
Deleted archived journal
[...]
Vacuuming done, freed 24.0M of archived journals from /var/log/journal/
e9af6ca5a8fb4a70b2ddec4b1894014d.
$
$ journalctl --disk-usage
Archived and active journals take up 320.0M in the file system.
```

Viewing other journals other than active ones

Option	Description
<code>-D --directory=PATH</code>	Show journal files from directory
<code>--file=PATH</code>	Show journal file

Making journal entries

```
$ echo "Test of systemd-cat" | systemd-cat
$
$ journalctl --no-pager | grep systemd-cat
May 30 17:43:46 Ubuntu1804 cat[2599]: Test of systemd-cat
$
```

```
$ logger "Test of logger"
$
$ journalctl -r
-- Logs begin at Thu 2018-07-26 18:19:45 EDT, end at Thu 2019-05-30 [...]
[...]
May 30 17:45:29 Ubuntu1804 Christine[2606]: Test of logger
[...]
May 30 17:43:46 Ubuntu1804 cat[2599]: Test of systemd-cat
[...]
$
```

Question... ■