Configuring Remote Logging using rsyslog in CentOS/RHEL

By admin

Remote logging

Standard system log management configuration rotates log files every week and retains them for four rotations. It is often desirable to maintain logs longer than the four-week default, especially when establishing system performance trends related to tasks, such as month-end financial closings, which are executed just once a month. By sending log messages to a remote log host with dedicated mass storage, administrators can maintain large archives of system logs for their systems without changing the default log rotation configuration, which is intended to keep logs from overconsuming disk storage.

Central collection of system log messages can also be very useful for monitoring the state of systems and for quickly identifying problems. It also provides a backup location for log messages in case a system suffers a catastrophic hard drive failure or other problems, which cause the local logs to no longer be available. In these situations, the copy of the log messages which reside on the central log host can be used to help diagnose the issue that caused the problem.

Standardized system logging is implemented in Red Hat Enterprise Linux 7 by the **rsyslog** service. System programs can send syslog messages to the local **rsyslogd** service, which will then redirect those messages to files in **/var/log**, remote log servers, or other databases based on the settings in its configuration file, **/etc/rsyslog.conf**.

Log messages have two characteristics that are used to categorize them. The facility of a log message indicates the type of message it is. The priority, on the other hand, indicates the importance of the event logged in the message.

Syslog Priority Levels

Priority	Meaning
emerg	System is unusable
alert	Immediate action required
crit	Critical condition
err	Error condition
warning	Warning condition
notice	Normal but significant condition
info	Informational messages
debug	Debugging messages

Configuring a central log host

The implementation of a central log host requires the configuration of the rsyslog service on two types of systems: the remote systems where the log messages originate from and the central log host receiving the messages. On the central log host, the rsyslog service needs to be configured so that log messages from remote hosts are accepted.

To configure the rsyslog service on the central log host to accept remote logs, uncomment either the TCP or UDP reception lines in the modules section in the **/etc/rsyslog.conf** file.

For UDP reception:

```
# Provides UDP syslog reception
$ModLoad imudp.so
$UDPServerRun 514
```

for TCP reception:

```
# Provides TCP syslog reception
$ModLoad imtcp.so
$InputTCPServerRun 514
```

TCP provides more reliable delivery of remote log messages, but UDP is supported by a wider variety of operating systems and networking devices.

> **Note**: Plain TCP transport of syslog messages is fairly widely implemented but not yet standardized. Most implementations currently use port 514/TCP, which is the legacy rshd port. If the system has the rsh-server package installed and is using the old insecure rshd service, it will conflict with using port 514/TCP for plain TCP syslog reception. Configure the log server to use a different port by changing the setting for $InputTCPServerRun.

The rules contained in /etc/rsyslog.conf are configured by default to accommodate the logging of messages on a single host. Therefore, it sorts and bundles messages by the facility. For example, mail messages are funneled into /var/log/maillog while messages generated by
the crond daemon are consolidated into /var/log/cron to facilitate locating each type of message.

While sorting of messages by the facility is ideal on a single host, it produces an undesirable result on a central log host since it causes messages from different remote hosts to be mixed with each other. On a central log host, it is usually more optimal for log messages from remote systems to remain separate from each other. This separation can be achieved by defining dynamic log file names using the template function of rsyslog.

Templates are defined in /etc/rsyslog.conf and can be used to generate rules with dynamic log file names. A template definition consists of the **$template** directive, followed by a template name, and then a string representing the template text. The template text can be made dynamic by making use of values substituted from the properties of a log message. For example, to direct cron syslog messages from different systems to different files on a central log host, use the following template to generate dynamic log file names based on the **HOSTNAME** property of each message:

```
$template DynamicFile,"/var/log/loghost/%HOSTNAME%/cron.log"
```

The dynamic file name created using the template definition can then be referenced by the template name in a rule as follows:

```
cron.*    ?DynamicFile
```

On systems performing extremely verbose logging, it may be desirable to turn off syncing of the log file after each writes operation in order to improve performance. The syncing of a log file after every logging can be omitted by prefixing the log file name with the minus (-) sign in a logging rule. However, the trade-off of improved performance does create the possibility of log data loss if the system crashes immediately after a write attempt.

The following is another example of the use of templates to generate dynamic log file names. In this example, remote log messages will be sorted by their host name and facility values by referencing the **HOSTNAME** and **syslogfacility-test** properties. Log messages will be written to the dynamically generated log file names and no syncing will be performed after the write operation.

```
$template DynamicFile,"/var/log/loghost/%HOSTNAME%/%syslogfacility-text%.log"
*.*    -?DynamicFile
```

> **Note**: A full list of the syslog messages properties made available by rsyslog can be found in the Available Properties section of the rsyslog.conf(5) man page.

Once syslog reception has been activated and the desired rules for log separation by host has been created, restart the rsyslog service for the configuration changes to take effect. In addition, add the necessary UDP and/or TCP firewall rules to allow incoming syslog traffic and then reload **firewalld**.

```
# systemctl restart rsyslog
# firewall-cmd --add-port=514/udp --permanent
# firewall-cmd --add-port=514/tcp --permanent
# firewall-cmd --reload
```

When new log files are created, they may not be included by the log host's existing log rotation schedule. This should be remedied to ensure that the new log files do not grow to unmanageable sizes. For instance, to include the new log files from the previous examples in log rotation, add the following entry to the list of log files in the **/etc/logrotate.d/syslog** configuration file.

```
/var/log/loghost/*/*.log
```

Redirecting logging to central log host

Once the central log host is configured to accept remote logging, the rsyslog service can be configured on remote systems to send logs to the central log host. To configure a machine to send logs to a remote rsyslog server, add a line to the rules section in the /etc/rsyslog.conf file. In place of the file name, use the IP address of the remote rsyslog server. To use UDP, prefix the IP address with a single @ sign. To use TCP, prefix it with two @ signs (@@).

For instance, to have all messages with info or higher priority sent to loghost.example.com via UDP, use the following line:

```
*.info @loghost.example.com
```

To have all messages sent to loghost.example.com via TCP, use the following line:

```
*.*     @@loghost.example.com
```

Optionally, the log hostname can be appended with **:PORT**, where PORT is the port that the remote rsyslog server is using. If no port is given, it assumes the default port **514**.

After adding the rule(s), restart the rsyslog service and send a test message using the logger command:

```
[root@logclient ~]# logger "Test from logclient"
```

Check the logs on the remote server to ensure the message was received.