Reliable Logging Enhancements in Red Hat Enterprise Linux 6

Rich Jerrido - RHCA, RHCVA – Solutions Architect

Logging, why should you care?

- **Troubleshooting**
- **Compliance (PCI, SOX, HIPPA, etc)**
- **Security**
- **Auditing**
- **Because my Red Hat Solutions Architect ™ said so**

Rsyslog

- **Introduced as optional drop-in replacement for sysklogd in RHEL5.2**
- **Default syslog daemon in RHEL6 (version 4.x)**
- **Designed to be a modern replacement to sysklogd adding features & capabilities**

Rsyslog Features

- **Rsyslog Features**
- **Multi-threaded syslog daemon**
- **TCP, SSL, TLS, RELP**
- **MySQL, PostgreSQL**
- **ISO 8601 timestamp support (millisecond granularity and timezone information)**
- **On-disk queuing**
- **Componentized design (load only the modules you need)**
- **Filter any part of syslog message**
- **Fully configurable output format**

RELP

- **Reliable Event Logging Protocol**
- **Not just for syslog**
- **Similar in purpose to AMQP (Advanced Message Queuing Protocol) - line-level protocol**
- **Designed to address deficiencies of TCP, mainly that TCP provides reliability at the connection level. RELP provides reliability at the application level. RELP usage implies TCP usage.**
- **Provided via the rsyslog-relp package.**

Security

- **GNUTLS**
  - Provided via the rsyslog-gnutls package
  - Provides SSL
  - Currently mutually-exclusive with RELP
- **Stunnel**
  - Provides SSL layer encryption of syslog traffic
  - Use with rsyslog-relp for best effect (secure + reliable)
  - Provides a slew of other features (non-repudiation, mutual authentication)

What about?

- **RHEL5 (rsyslog v3) - No RELP, deploy with TCP and Stunnel**

- **RHEL3/RHEL4 - No RELP, no TCP, deploy with UDP syslog**

- **RHEL2 – (These still exist?) same as RHEL3/RHEL4**

Security & Reporting

- **Log to a database (MySQL, Postgres)**
- **Native OS tools (grep/awk/sed)**
- **Logwatch**
- **3rd party tools**
  - "Australian grep"
  - Internal Security Incident Management tool
- **Syslog Relay Chains (feed other syslog servers with your data)**

Best Practices

- **Consider deploying syslog server on RHEL6**
- **Deploy with SSL & RELP where possible.**
- **Queue where possible (separate log delivery from database insertion)**
- **Consider logging to a database (for reporting)**
- **Use high-precision (ISO 8601) timestamps, especially if you have systems in multiple time zones**

So let's build

- **Just two lines in /etc/rsyslog.conf on the Server.**

```
$ModLoad imrelp.so #Load the RELP Input Module
$InputRELPServerRun 60001
```

- **Just two lines in /etc/rsyslog.conf on the Client**

```
$ModLoad omrelp.so #Load the RELP Output Module
*.*:omrelp:1.2.3.4:60001;RSYSLOG_ForwardFormat
```

And now let's integrate

- **Apache**

```
 CustomLog "|/usr/bin/logger -p local7.info -t 'Apache'" combined

 ErrorLog "|/usr/bin/logger -p local7.info -t 'Apache'"
```

- **Iptables**

```
 iptables -A INPUT -j LOG --log-prefix "firewall-DENY: " --log-level debug
```

And now let's integrate (cont'd)

- **Rsyslog supports expression based filtering of log messages**
- **Example:**

```
  if $msg startswith 'firewall-DENY' then
/var/log/iptables.log
```

- **Example:**

```
if $msg contains 'Apache' then /var/log/apache.log
```

- **Expressions give the ability to adapt to business requirements**

References

- **RELP - http://www.librelp.com/relp.html**
- **Rsyslog - http://www.rsyslog.com/**
- **Log Analyzer - http://loganalyzer.adiscon.com/**
- **Red Hat Customer Portal: http://access.redhat.com**

Questions?