Solaris Rsyslog Onboarding for New Relic Log Management

Gulab Sidhwani
New Relic Data Labs

Topics

Getting Started

The **system/rsyslog** service is newly available in the Solaris 11.1 release. To send and receive messages over TCP, the rsyslog pkg must be installed on the sending Solaris system (the source system) .

The rsyslog package is not installed by default in Solaris 11.1 and later, and may need to be added. On the source Solaris systems here are the steps:

Installation

Step 1: Please verify , if the *rsyslog* package is already installed.

Unset

```
# pkg info system/rsyslog
pkg: info: no packages matching the following patterns you specified
are
installed on the system.  Try specifying -r to query remotely:
        system/rsyslog
```

If the *rsyslog* package is not installed, it can be installed with:

Unset

```
pkg install system/rsyslog
```

Step 2: Confirm the *rsyslog* instance.

Unset

```
# svcs -a | grep "system-log"
disabled       18:27:16 svc:/system/system-log:rsyslog
online         18:27:21 svc:/system/system-log:default
```

This output confirms that the *rsyslog* instance exists, though it is disabled.

Step 3: Switch to the *rsyslog* service.

Unset

```
# svcadm disable svc:/system/system-log:default
# svcadm enable svc:/system/system-log:rsyslog
# svcs -a | grep "system-log"
disabled       Dec_23   svc:/system/system-log:default
online         Dec_23   svc:/system/system-log:rsyslog
```

Step 4: After a successful installation, install the following packages to allow *rsyslog* to send logs over an encrypted connection:

Unset

```
pkg install  ca-certificates
```

Configuration

Step 5 : After a successful installation, restart the `ca-certificates` service

Unset

```
svcadm restart ca-certificates
```

Step 6 : Ensure CA Certificate service is running and there are no errors reported in log file:

Unset

```
# svcs -x ca-certificates
svc:/system/ca-certificates:default (CA Certificates Service)
 State: online since Fri Dec 23 12:35:41 2022
   See: x509v3_config(5openssl)
   See: /var/svc/log/system-ca-certificates:default.log
Impact: None.
```

Step 6 : Next, create a text file in /etc/rsyslog.d/ called newrelic.conf. Add the following to your newly created text file, making sure to replace YOUR_NR_INSERT_KEY with your New Relic Insights API Insert key.

Unset

```
#Define New Relic syslog format

$template NRLogFormat,"YOUR_NR_INSERT_KEY <%pri%>%protocol-version%
%timestamp:::date-rfc3339% %hostname% %app-name% %procid% %msgid%
%structured-data% %msg%\n"
```

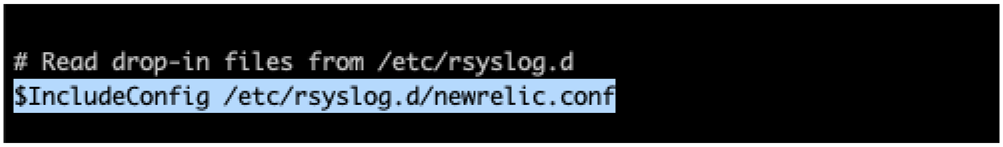
```
# Configure TLS and log forwarding to New Relic

$DefaultNetstreamDriverCAFile /etc/certs/ca-certificates.crt

$DefaultNetstreamDriver gtls

$ActionSendStreamDriverMode 1

$ActionSendStreamDriverAuthMode x509/name
$ActionSendStreamDriverPermittedPeer *.syslog.nr-data.net
*.* @@newrelic.syslog.nr-data.net:6514;NRLogFormat
```

Step 7 : Restart the *rsyslog* service

Unset

```
svcadm restart rsyslog
```

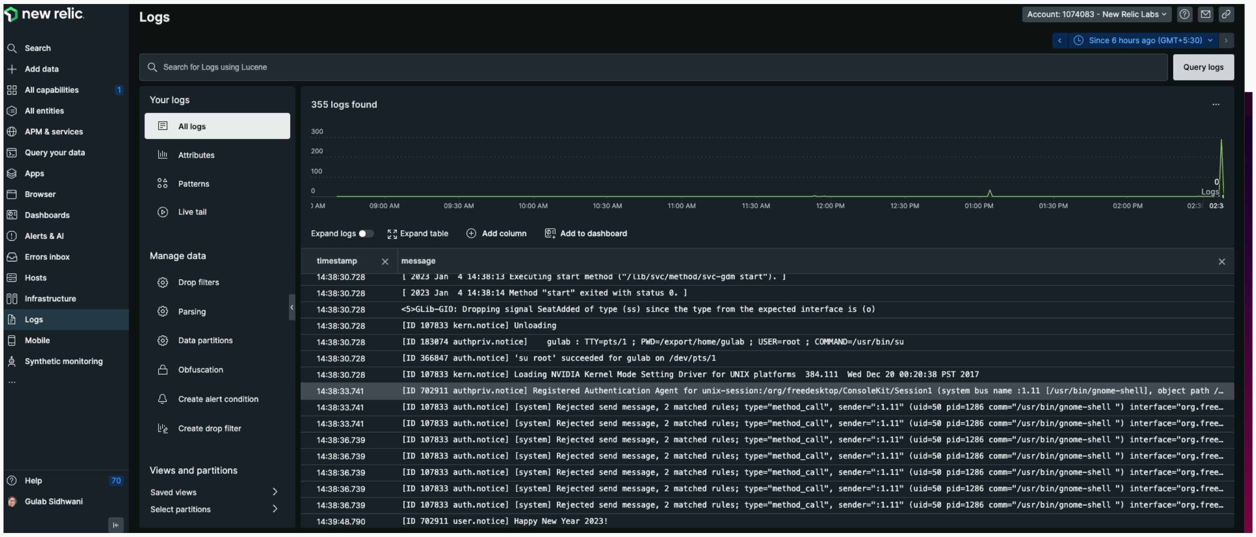
Note : In case newrelic.conf changes are not reflected after the restart, try to configure the exact path in **/etc/rsyslog.conf** and then restart the rsyslog service.



```
# Read drop-in files from /etc/rsyslog.d
$IncludeConfig /etc/rsyslog.d/newrelic.conf
```

Step 8 : Verify that /var/adm/messages, system logs (refer to the log configuration in **/etc/rsyslog.conf)** and the sample message below are being sent to [new relic platform]

```
Unset
logger "Happy New Year 2023!"
```



```
14:38:30.728   [ 2023 Jan  4 14:38:13 Executing start method ("/lib/svc/method/svc-gdm start"). ]
14:38:30.728   [ 2023 Jan  4 14:38:14 Method "start" exited with status 0. ]
14:38:30.728   <5>GLib-GIO: Dropping signal SeatAdded of type (ss) since the type from the expected interface is (o)
14:38:30.728   [ID 107833 kern.notice] Unloading
14:38:30.728   [ID 183074 authpriv.notice]    gulab : TTY=pts/1 ; PWD=/export/home/gulab ; USER=root ; COMMAND=/usr/bin/su
14:38:30.728   [ID 366847 auth.notice] 'su root' succeeded for gulab on /dev/pts/1
14:38:30.728   [ID 107833 kern.notice] Loading NVIDIA Kernel Mode Setting Driver for UNIX platforms  384.111  Wed Dec 20 00:20:38 PST 2017
14:38:33.741   [ID 702911 authpriv.notice] Registered Authentication Agent for unix-session:/org/freedesktop/ConsoleKit/Session1 (system bus name :1.11 [/usr/bin/gnome-shell], object path /…
14:38:33.741   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:33.741   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:36.739   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:36.739   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:36.739   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:36.739   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:38:36.739   [ID 107833 auth.notice] [system] Rejected send message, 2 matched rules; type="method_call", sender=":1.11" (uid=50 pid=1286 comm="/usr/bin/gnome-shell ") interface="org.free…
14:39:48.790   [ID 702911 user.notice] Happy New Year 2023!
```

Additional Steps for EU Region

To configure a rsyslog server in the EU region via the **/etc/rsyslog.d/newrelic.conf** file, please see the example below:

$ActionSendStreamDriverPermittedPeer *.syslog.eu.nr-data.net
. @@newrelic.syslog.eu.nr-data.net:6514;NRLogFormat

You may see a TLS error with the above configuration when you connect to the EU region's syslog server.

```
rsyslogd: not permitted to talk to peer, certificate invalid: GnuTLS returned no specific
reason [v8.15.0]
Jan 10 17:59:50 gulab rsyslogd: invalid cert info: peer provided 3 certificate(s). Certificate 1
info: certificate valid from Fri Dec 30 13:16:17 2022 to Thu Mar 30 13:16:16 2023;
Certificate public key: RSA; DN: CN=*.syslog.eu.nr-data.net; Issuer DN: C=US,O=Let's
Encrypt,CN=R3; SAN:DNSname: *.syslog.eu.nr-data.net;  [v8.15.0]
```

You may also reproduce the error message with openssl.

```
#openssl s_client -showcerts -servername server -connect
newrelic.syslog.eu.nr-data.net:6514 > /dev/null
depth=3 O = Digital Signature Trust Co., CN = DST Root CA X3
verify error:num=10:certificate has expired
notAfter=Sep 30 14:01:15 2021 GMT
```

Why do we have this TLS problem for an EU-based rsyslog server ?

newrelic.syslog.nr-data.net uses TLS certificates from Amazon certificates.
newrelic.syslog.eu.nr-data.net uses TLS Let’s encrypt certificates.

The latest Trusted Certificates from Let’s encrypt may not be available in Source’s Certificate Store to verify the identity of newrelic.syslog.eu.nr-data.net. Because of this, it is necessary to update the Certificate Trust Store manually. See the update steps below:

Here are the steps required to connect the EU region’s server.

Step 1 : Update Certificate Store

Download

https://letsencrypt.org/certs/isrg-root-x2.pem https://letsencrypt.org/certs/lets-encrypt-r3.pem

Unset

```
cd  /etc/certs/CA
curl https://letsencrypt.org/certs/isrg-root-x2.pem -k >
isrg-root-x2.pem
curl https://letsencrypt.org/certs/lets-encrypt-r3.pem -k >
lets-encrypt-r3.pem
```

Move or Delete DST_Root_CA_X3.pem from this folder `(/etc/certs/CA)` as it will conflict with the above set of new certificate files. As to why, the intermediary CA Authority for this certificate has expired and will no longer be renewed so it will fail to verify the identity of newrelic.syslog.eu.nr-data.net .

After successfully performing the steps, restart the `ca-certificates` service

Unset

```
svcadm restart ca-certificates
```

The command above will generate a new **/etc/certs/ca-certificate.crt** certificate. Please validate if all new certificate entries are captured/updated.

Ensure CA Certificate service is running and there are no errors reported in log file:

Unset

```
# svcs -x ca-certificates
svc:/system/ca-certificates:default (CA Certificates Service)
 State: online since Fri Dec 23 12:35:41 2022
   See: x509v3_config(5openssl)
   See: /var/svc/log/system-ca-certificates:default.log
Impact: None.
```

Verify Connection :

```
# openssl s_client -showcerts -servername server -connect
newrelic.syslog.eu.nr-data.net:6514 > /dev/null
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R3
verify return:1
depth=0 CN = *.syslog.eu.nr-data.net
verify return:1
```

So, at this point our Certificate Store is healthy .

Step 2: Update GNUtls package for Solaris

Unset

```
pkgadd -d http://get.opencsw.org/now
/opt/csw/bin/pkgutil -U
/opt/csw/bin/pkgutil -y -i gnutls
/usr/sbin/pkgchk -L CSWgnutls # list files
```

After a successful package installation restart the *rsyslog* service

Unset

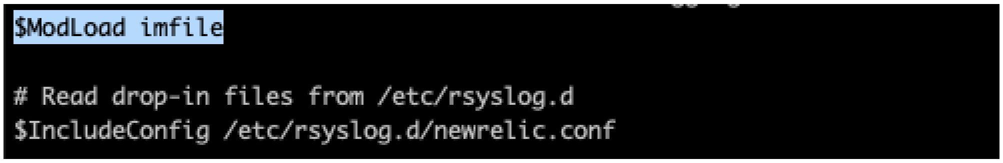
```
svcadm restart rsyslog
```

If needed, reboot the machine to make the changes permanent. You should be able to see logs are transferred to the New Relic Log Management System when the machine comes up back online.

Configuration for specific logs

The steps above provide a simple configuration that will forward to New Relic any logs collected by rsyslog. Let’s step through how to configure tailing specific log files.

Step 1. Enable the imfile module to allow rsyslog to tail files. Add the following to the Modules section of your **/etc/rsyslog.conf** if it isn't already present:



```
$ModLoad imfile

# Read drop-in files from /etc/rsyslog.d
$IncludeConfig /etc/rsyslog.d/newrelic.conf
```

Step 2. Define the file(s) that rsyslog should tail by adding the following to the top of the newrelic.conf file that you created in the previous section:

Note: Depending on your version of rsyslog, wildcards are supported when defining $InputFileName.

Unset

```
$InputFileName
/var/svc/log/application-graphical-login-gdm:default.log

$InputFileTag  session_access

$InputFileStateFile  apache_state

$InputFileSeverity info

$InputRunFileMonitor
```

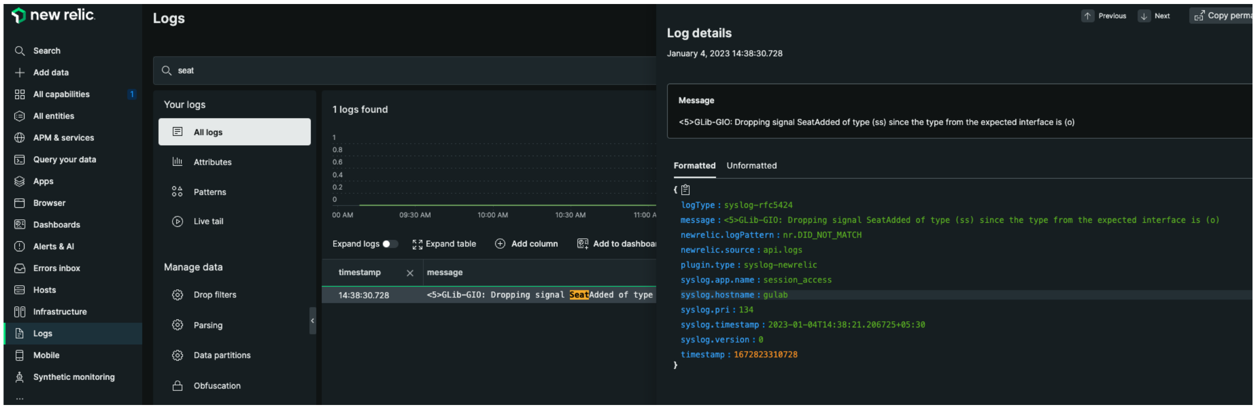
Note: You may add as many as files you want.

Step 3. Restart rsyslog and check your New Relic account for logs:

Unset

```
svcadm restart rsyslog
```

Step 4 : Verify that specific file message are being sent to new relic platform by querying for a specific *keyword.*



seat

1 logs found

timestamp	message
14:38:30.728	`<5>GLib-GIO: Dropping signal SeatAdded of type`

Log details

January 4, 2023 14:38:30.728

Message

<5>GLib-GIO: Dropping signal SeatAdded of type (ss) since the type from the expected interface is (o)

```
{
  logType : syslog-rfc5424
  message : <5>GLib-GIO: Dropping signal SeatAdded of type (ss) since the type from the expected interface is (o)
  newrelic.logPattern : nr.DID_NOT_MATCH
  newrelic.source : api.logs
  plugin.type : syslog-newrelic
  syslog.app.name : session_access
  syslog.hostname : gulab
  syslog.pri : 134
  syslog.timestamp : 2023-01-04T14:38:21.206725+05:30
  syslog.version : 0
  timestamp : 1672823310728
}
```