Solaris Rsyslog Onboarding for New Relic Log Management

Gulab Sidhwani

New Relic Data Labs

**Topics**

[**Getting Started**](#_57yh16o74i1w) **2**

[**Installation**](#_w5qqhifmbcds) **2**

[**Configuration**](#_fe6kix57e71f) **4**

[**Additional Steps for EU Region**](#_bub0xmo73s1k) **6**

[**Configuration for specific logs**](#_izz3fnlqytiz) **9**

# 

# 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.

# 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:

pkg install system/rsyslog



### Step 2: Confirm the *rsyslog* instance.

****# 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.

# 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:

pkg install ca-certificates



# Configuration

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

svcadm restart ca-certificates



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

# 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](https://docs.newrelic.com/docs/telemetry-data-platform/ingest-manage-data/ingest-apis/use-event-api-report-custom-events#register).

#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

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.

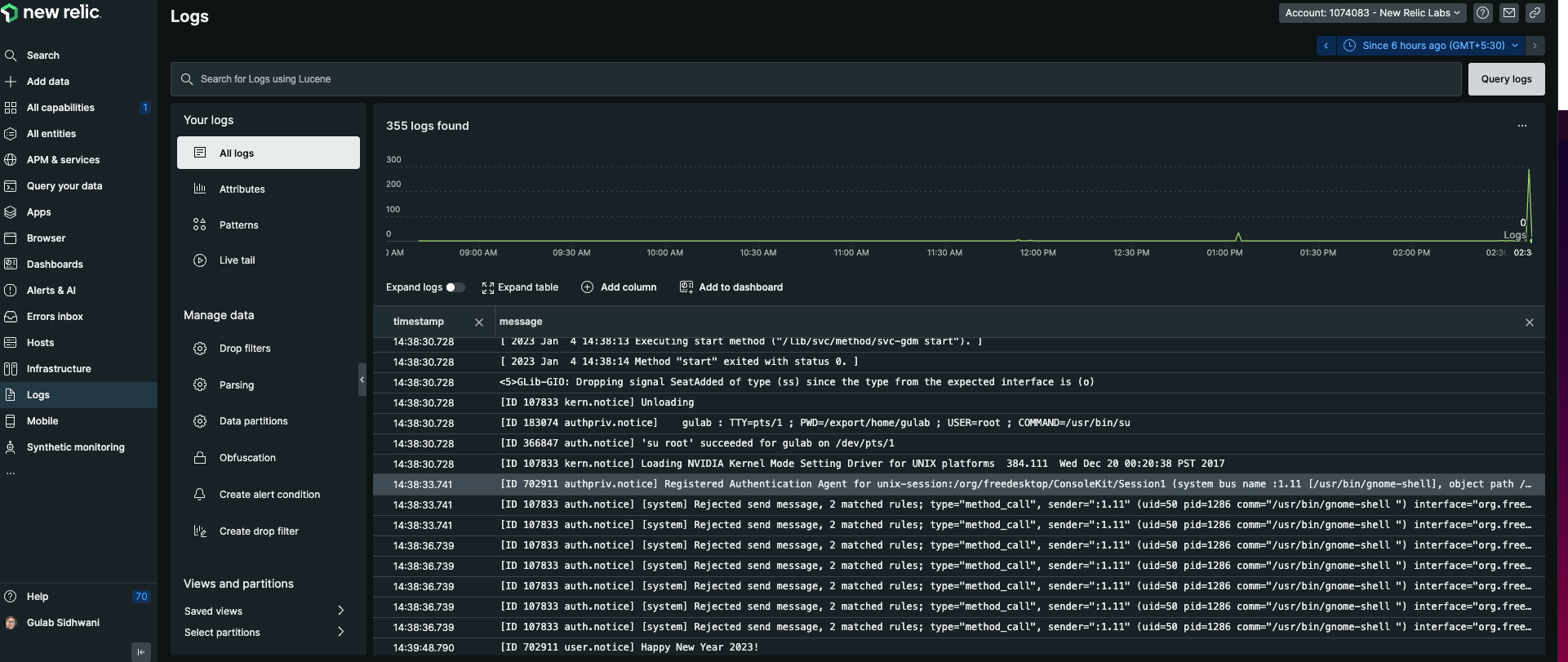


### 

### 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](https://one.newrelic.com/)

logger "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](http://syslog.eu.nr-data.net/); Issuer DN: C=US,O=Let's Encrypt,CN=R3; SAN:DNSname: \*.[syslog.eu.nr-data.net](http://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](http://newrelic.syslog.nr-data.net/) uses TLS certificates from Amazon certificates.

[newrelic.syslog.eu.nr-data.net](http://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](http://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>

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](http://newrelic.syslog.eu.nr-data.net/) .

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

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:

# 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](http://syslog.eu.nr-data.net/)

verify return:1

So, at this point our Certificate Store is healthy .

## Step 2: Update GNUtls package for Solaris

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

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](https://www.rsyslog.com/doc/v8-stable/configuration/modules/imfile.html) 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:



**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](https://www.rsyslog.com/doc/v8-stable/configuration/modules/imfile.html#wildcards) are supported when defining $InputFileName.

$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:

svcadm restart rsyslog

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

## 