Solaris Rsyslog Onboarding for New Relic Log Management

# 

# 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 both the source Solaris systems .

# 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.

Step3: 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 successful installation , Install the following packages to allow *rsyslog* to send logs over an encrypted connection:

pkg install ca-certificates



# Configuration

Step 5 : After successful installation , copy the certificate file to new directory (/etc/ssl/certs) for the new relic platform integration

cp /etc/certs/ca-certificates.crt /etc/ssl/certs/ca-certificates.crt



Step 6 : Ensure CA Certificate service is running :

# 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/ssl/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



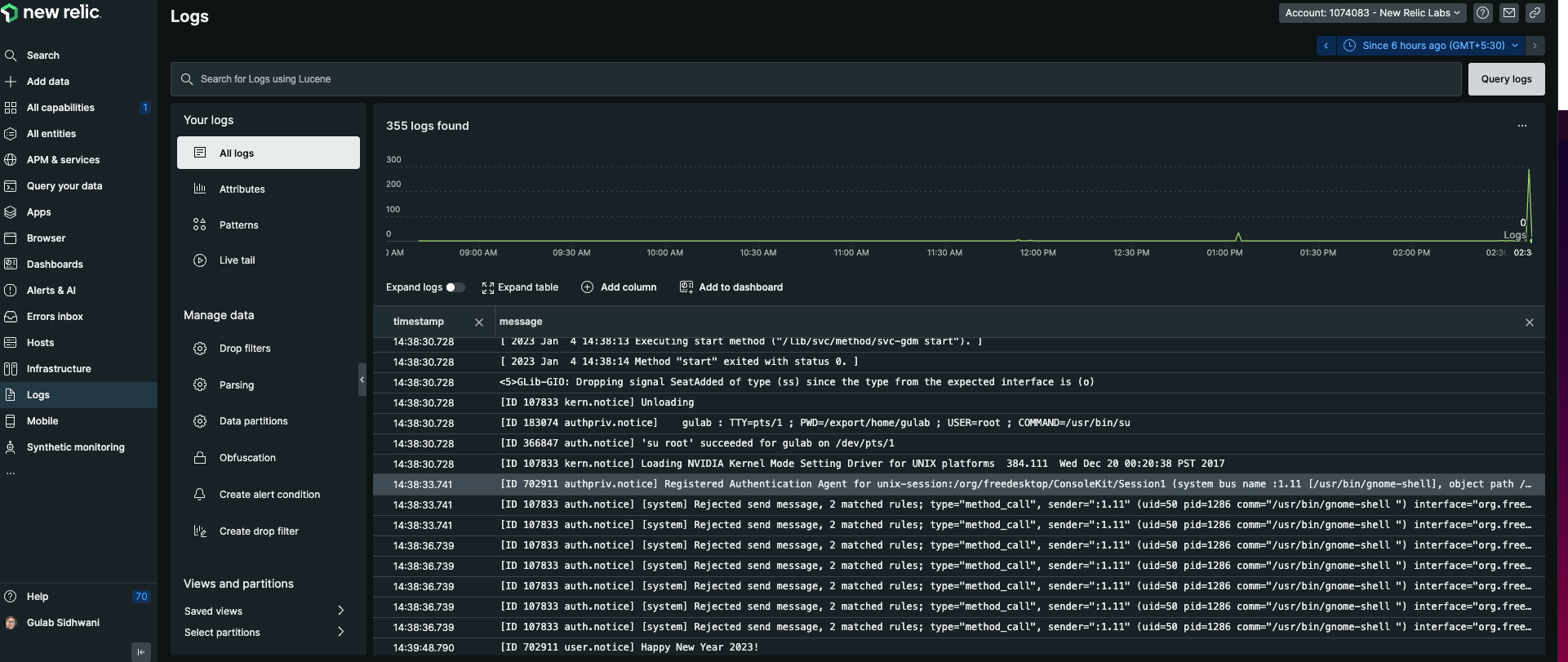
**Note** : In case newrelic.conf changes are not reflected after the restart then try to configure the exact path in **/etc/rsyslog.conf** and then restart the service.



Step 8 : verify that /var/adm/messages, system logs ( refer 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!"





# 

# Configuration for specific logs

## The steps above provide a simple configuration that will forward any logs that rsyslog currently collects to New Relic. 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 a specific *keyword*

## 