RSA NetWitness Platform

Event Source Log Configuration Guide

Sun Solaris

Last Modified: Thursday, October 11, 2018

Event Source Product Information:

Vendor: Sun
Event Source: Solaris
Versions: 8, 9, 10, 11.x

Note: RSA is qualifying support for the major version. In case of any configuration changes or logs not parsing in a minor version, please open a case and we will add support for it.

RSA Product Information:

Supported On: NetWitness Platform 10.0 and later
Event Source Log Parser: solaris
Collection Method: Syslog
Event Source Class.Subclass: Host.UNIX

To configure Syslog collection for the Sun Solaris you must:

I. Configure Syslog Output on Sun Solaris:
   - Configure Syslog Output on Sun Solaris Version 10 or 11.x
   - Configure Syslog Output on Sun Solaris Versions 7, 8, or 9

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output on Sun Solaris

See the section that corresponds to your Solaris version:

- Configure Syslog Output on Sun Solaris Version 10 or 11.x, or
- Configure Syslog Output on Sun Solaris Versions 8 or 9

Configure Syslog Output on Sun Solaris Version 10 or 11.x

The following procedure describes how to configure Sun Solaris version 10 or 11.x.

To configure Sun Solaris version 10 or 11:

1. Configure the Solaris syslog service to log all messages of debug level and higher to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
   a. Open the **/etc/syslog.conf** file with a file editor.
   b. Add the following line, where ***xxx.xxx.xxx.xxx*** is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector:

      ```
      *.debug     @xxx.xxx.xxx.xxx
      ```

   c. Save the file.
   d. Force the syslogd service to read the configuration file by sending it the **SIGHUP** signal.
2. Allow information from the wtmp/wtmpx database files to be logged (This allows the system to report on user logins and logouts, connection duration times, and login method, such as Telnet, FTP, rlogin, and so forth.):
   a. Create the nilogger.sh file (with execute permissions set) and add the following lines:

      ```
      mv /tmp/Last10 /tmp/Last10old
      last -10 > /tmp/Last10
      diff /tmp/Last10old /tmp/Last10 | grep '>' | logger -p auth.notice -t
      LAST10
      ```

   b. Create a cron job to run the nilogger.sh script every 10 minutes.

3. Enable tracing of all TCP connections for **inetd** supported services:
   a. Become superuser or assume a role that includes the Service Management rights profile.
   b. Change the default value of the **inetd** tcp_trace property to true:

```
# inetadm -M tcp_trace=true
```

   c. Verify that the change has been made:

```
# inetadm -p
NAME=VALUE
bind_addr=""
bind_fail_max=-1
bind_fail_interval=-1
max_con_rate=-1
max_copies=-1
con_rate_offline=-1
failrate_cnt=40
failrate_interval=60
inherit_env=TRUE
tcp_trace=TRUE
tcp_wrappers=FALSE
```

4. Enable connection logging for FTP sessions:
   a. Become superuser or assume a role that includes the Service Management rights profile.
   b. Add –l to the exec property of the FTP service:

```
# inetadm -m svc:/network/ftp:default exec="/usr/sbin/in.ftpd -a -l"
```

   c. Verify that the property has changed:

```
# inetadm -l svc:/network/ftp:default
SCOPE    NAME=VALUE

      name="ftp"
      endpoint_type="stream"
      proto="tcp6"
      isrpc=FALSE
      wait=FALSE
      exec="/usr/sbin/in.ftpd -a -l"
      user="root"

default bind_addr=""
default bind_fail_max=-1

      default bind_fail_interval=-1
      default max_con_rate=-1
      default max_copies=-1
      default con_rate_offline=-1
      default failrate_cnt=40
```

```
default failrate_interval=60
default inherit_env=TRUE
default tcp_trace=TRUE
default tcp_wrappers=FALSE
```

Configure Syslog Output on Sun Solaris Versions 8 or 9

The following procedure describes how to configure Sun Solaris versions 8 and 9.

To configure Syslog output on Sun Solaris version 8 or 9:

1. Configure the Solaris syslog service to log all messages of debug level and higher to the IP address of the RSA NetWitness Log Decoder or Remote Log Collector:
   a. Open the **/etc/syslog.conf** file with a file editor.
   b. Add the following line, where xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector:

      ```
      *.debug    @xxx.xxx.xxx.xxx
      ```

   c. Save the file.
   d. Force the syslogd service to read the configuration file by sending it the SIGHUP signal.
2. Allow information from the **wtmp/wtmpx** database files to be logged. (This allows the system to report on user logins and logouts, connection duration times, and login method, such as Telnet, FTP, rlogin, and so forth.):
   a. Create the **nilogger.sh** file (with **execute** permissions set) and add the following lines:

      ```
      mv /tmp/Last10 /tmp/Last10old
      last -10 > /tmp/Last10
      diff /tmp/Last10old /tmp/Last10 | grep '>' | logger -p auth.notice -t
      LAST10
      ```

   b. Create a cron job to run the **nilogger.sh** script every 10 minutes.
3. Enable tracing of all TCP connections for inetd supported services:
   a. Open the **/etc/init.d/inetsvc** file in a file editor.
   b. Add **-t** to the **inetd** line:

      ```
      /usr/sbin/inetd -s -t &
      ```

   c. Save the file.
   d. Reboot the system to restart the inetd service cleanly.

4. Enable connection logging for FTP sessions:
   a. Open the /etc/inet/inetd.conf in a file editor.
   b. Add -d -l to the in.ftpd line:
      ftp stream tcp6 nowait root /usr/sbin/in.ftpd in.ftpd -d -l
   c. Save the file.
   d. Force the **inetd** service to read the config file by sending it a **SIGHUP** signal.

Configure RSA NetWitness Platform

Perform the following steps in RSA NetWitness Platform:

- Ensure the required parser is enabled
- Configure Syslog Collection

Ensure the Required Parser is Enabled

If you do not see your parser in the list while performing this procedure, you need to download it in RSA NetWitness Platform Live.

Ensure that the parser for your event source is enabled:

1. In the **NetWitness** menu, select **ADMIN** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **Config**.
3. In the Service Parsers Configuration panel, search for your event source, and ensure that the **Config Value** field for your event source is selected.

Note: The required parser is **solaris**.

Configure Syslog Collection

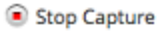
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

You should configure either the Log Decoder or the Remote Log Collector for Syslog. You do not need to configure both.

To configure the Log Decoder for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Log Decoder, and from the Actions menu, choose **View** > **System**.
3. Depending on the icon you see, do one of the following:

- If you see 

, click the icon to start capturing Syslog.
- If you see 

, you do not need to do anything; this Log Decoder is already capturing Syslog.

To configure the Remote Log Collector for Syslog collection:

1. In the **NetWitness** menu, select **Administration** > **Services**.
2. In the Services grid, select a Remote Log Collector, and from the Actions menu, choose **View** > **Config** > **Event Sources**.
3. Select **Syslog/Config** from the drop-down menu.

   The Event Categories panel displays the Syslog event sources that are configured, if any.
4. In the Event Categories panel toolbar, click +.

   The Available Event Source Types dialog is displayed.
5. Select either **syslog-tcp** or **syslog-udp**. You can set up either or both, depending on the needs of your organization.
6. Select the new type in the Event Categories panel and click + in the Sources panel toolbar.

   The Add Source dialog is displayed.
7. Enter **514** for the port, and select **Enabled**. Optionally, configure any of the Advanced parameters as necessary.

   Click **OK** to accept your changes and close the dialog box.

Once you configure one or both syslog types, the Log Decoder or Remote Log Collector collects those types of messages from all available event sources. So, you can continue to add Syslog event sources to your system without needing to do any further configuration in NetWitness.

Trademarks

For a list of RSA trademarks, go to www.emc.com/legal/emc-corporation-trademarks.htm#rsa.