RSA NetWitness Platform

Event Source Log Configuration Guide

Bind DNS

Last Modified: Monday, October 15, 2018

Event Source Product Information:

Vendor: Bind
Event Source: Bind DNS Logs
Versions:

- Bind DNS: 9.x, 11
- Red Hat Enterprise Linux 3.x, 4.x, 5.x, 6.0, 7.0
- Solaris 8, 9, 10, 11.x

RSA Product Information:

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

To configure the Bind DNS event source, you must:

I. Configure Syslog Output for Bind DNS

II. Configure RSA NetWitness Platform for Syslog Collection

Configure Syslog Output for Bind DNS

To configure your OS to send logs to RSA NetWitness Platform, depending on your version, do one of the following:

- Configure **Solaris** to send logs, or
- Configure **other Linux** versions, ***and*** turn on Bind DNS Logging

Configure Solaris to Send Logs

To configure Solaris, perform the following procedure.

To configure Solaris to send logs to the RSA NetWitness Platform:

1. On the Solaris appliance, open the `/etc/syslog.conf` file in a text editor.
2. To configure the event source to log all messages to the syslog server, add the following line:

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

   where xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.
3. Save the file, and close the text editor.
4. To restart the syslog service, run the following command:

   ```
   sudo svcadm restart system-log
   ```

Configure Linux to Send Logs

To configure versions of Linux other than Solaris, perform the following procedure.

To configure Linux to send logs to the RSA NetWitness Platform:

1. On the Linux appliance, open the `/etc/syslog.conf` file in a text editor. If you are using Redhat Linux 6.0, open `/etc/rsyslog.conf`.
2. To configure the event source to log all messages to the syslog server, add the following line:

   `*.* @@xxx.xxx.xxx.xxx:514`

   where xxx.xxx.xxx.xxx is the IP address of the RSA NetWitness Log Decoder or Remote Log Collector.

3. Save the file, and close the text editor.
4. To restart the syslog service, depending on your version of Linux, run the following command:
   - For Redhat Linux 6.0:

     ```
     service rsyslog restart
     ```
   - For other version of Linux:

     ```
     service syslog restart
     ```

Turn on Bind DNS Logging

Note: This step is not required on Solaris.

To turn on Bind DNS server logging, run the following command from your Linux event source:

```
# rndc querylog
```

Note the following:

- This command toggles query logging. If you run it again, it turns off query logging.
- You must run this command as root (or have sudo privileges).

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 parsers are **solaris** (if you are running a Solaris platform), or **rhlinux** (if you are running any other Linux platform).

Configure Syslog Collection

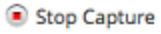
Note: You only need to configure Syslog collection the first time that you set up an event source that uses Syslog to send its output to NetWitness.

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.