RSA NetWitness Logs

Event Source Log Configuration Guide

UnboundID Identity Data Store

Last Modified: Monday, July 24, 2017

Event Source Product Information:

Vendor: UnboundID
Event Source: Identity Data Store
Versions: 4.5.1.1

RSA Product Information:

Supported On: NetWitness Suite 10.0 and later
Event Source Log Parser: unboundidids
Collection Method: Syslog
Event Source Class.Subclass: Security. Access Control

Configure UnboundID Identity Data Store

To configure UnboundID Identity Data Store, you must complete these tasks:

I. Configure UnboundID Identity Data Store to generate logs

II. Configure NetWitness Suite for Syslog

Configure the UnboundID Event Source to Generate Logs

You configure UnboundID Identity Data Store to work with RSA NetWitness Suite by running an interactive program in a command line screen in your Linux OS.

> **Note:** RSA supports collection of access and error logs only from the UnboundID Identity Data Store.

To configure UnboundID Identity Data Store access logs:

1. Log onto the UnboundID event source with administrative credentials.
2. Run the following command:

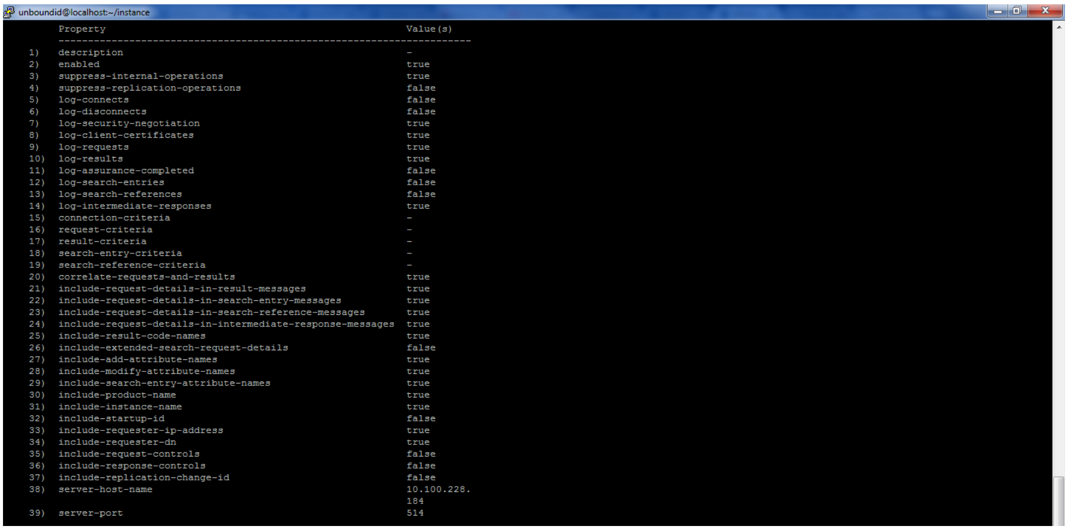
   ```
   bin/dsconfig
   ```

3. From the displayed list of options, enter the number for **Log Publisher**.
4. At the **What would you like to do prompt**, select the following:

   ```
   2) Create a new Log Publisher
   ```

5. At the **How** prompt, you can choose either to use an existing Log **Publisher** template, or to create your own.
6. You need to edit two parameters:
   - Set `server-host-name` to the IP address of your NetWitness Suite Log Decoder or Remote Log Collector.
   - Set `enabled` to **true**.
7. Enter **f**, then **q** to complete the steps.

Please set the properties as shown in the configuration parameter screen shown here:



```
          Property                                                   Value(s)
          -------------------------------------------------------------------
     1)   description                                                -
     2)   enabled                                                    true
     3)   suppress-internal-operations                               true
     4)   suppress-replication-operations                            false
     5)   log-connects                                               false
     6)   log-disconnects                                            false
     7)   log-security-negotiation                                   true
     8)   log-client-certificates                                    true
     9)   log-requests                                               true
     10)  log-results                                                true
     11)  log-assurance-completed                                    false
     12)  log-search-entries                                         false
     13)  log-search-references                                      false
     14)  log-intermediate-responses                                 true
     15)  connection-criteria                                        -
     16)  request-criteria                                           -
     17)  result-criteria                                            -
     18)  search-entry-criteria                                      -
     19)  search-reference-criteria                                  -
     20)  correlate-requests-and-results                             true
     21)  include-request-details-in-result-messages                 true
     22)  include-request-details-in-search-entry-messages           true
     23)  include-request-details-in-search-reference-messages       true
     24)  include-request-details-in-intermediate-response-messages  true
     25)  include-result-code-names                                  true
     26)  include-extended-search-request-details                    false
     27)  include-add-attribute-names                                true
     28)  include-modify-attribute-names                             true
     29)  include-search-entry-attribute-names                       true
     30)  include-product-name                                       true
     31)  include-instance-name                                      true
     32)  include-startup-id                                         false
     33)  include-requester-ip-address                               true
     34)  include-requester-dn                                       true
     35)  include-request-controls                                   false
     36)  include-response-controls                                  false
     37)  include-replication-change-id                              false
     38)  server-host-name                                           10.100.228.
                                                                     184
     39)  server-port                                                514
```

To configure UnboundID Identity Data Store error logs:

1. Log onto the UnboundID event source with administrative credentials.
2. Run the following command:

   `bin/dsconfig`

3. From the displayed list of options, enter the number for **ErrorLogPub**.
4. At the **How** prompt, you can choose either to use an existing template, or to create your own.
5. You need to edit two parameters:
   - Set `server-host-name` to the IP address of your NetWitness Suite Log Decoder or Remote Log Collector.
   - Set `enabled` to **true**.
6. Enter **f**, then **q** to complete the steps.

Configure NetWitness Suite for Syslog

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 ▶ Start Capture, click the icon to start capturing Syslog.
   - If you see ■ Stop Capture, 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