

RSA NetWitness Platform

Event Source Log Configuration Guide



Citrix XenApp

Last Modified: Tuesday, June 18, 2019

Event Source Product Information:

Vendor: [Citrix](#)

Event Source: XenApp

Versions: 5 (for Windows Server 2003), 6, 6.5, 7.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: citrixxa

Collection Method: ODBC

Event Source Class.Subclass: Host.Virtualization

Configure Citrix XenApp Farm to Log to the Database

To configure Citrix XenApp Farm to log to the database:

1. Log on to the Citrix Delivery Services Console.
2. Right-click on **Server Farm**, and select **Farm Properties**.
3. Under the **Farm-wide** drop-down list, select **Configuration Logging**.
4. In the **Database Type** field, click **Configure Database**.
5. In the Configuration Logging Database window, complete the fields as follows:
 - a. In the **Select a connection type** field, select **SQL Server**.
 - b. In the **Select a server name** field, type the SQL server name that you want to store the configuration logging.
 - c. In the **Select an authentication mode** field, select the authentication mode based on your environment.
 - d. In the **Enter credentials** field, enter the credentials based on what you selected in the authentication mode field.

Note: Ensure this user has a Database role membership of db_owner.

- e. Click **Next**.
 - f. In the **Specify the Database** field, enter the name of the database that you created for configuration logging.
 - g. Click **Next**.
 - h. In the **Connection Options** and the **Connection Pooling** fields, select the settings based on your environment.
 - i. Click **Next**.
 - j. Click **Test Database Connection**, and click **OK**.
6. Click **Finish**.

Configure NetWitness Platform for ODBC Collection

To configure ODBC collection in RSA NetWitness Platform, perform the following procedures:

- I. Ensure the required parser is enabled
- II. Configure a DSN
- III. Add the Event Source Type

For table reference, see [Reference Tables](#) below.

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 **citrixxa**.

Configure a DSN

Configure a DSN (Data Source Name):

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
5. The **DSNs** panel is displayed with the existing **DSNs**, if any.
6. Click **+** to open the **Add DSN** dialog.


Note: If you need to add a DSN template, see the "Configure DSNs" topic in the *Log Collection Configuration Guide*, available in [RSA Link](#).

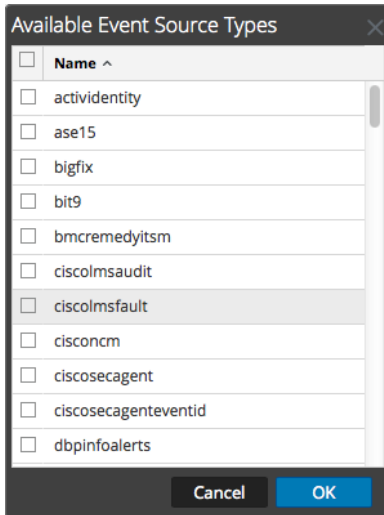
7. Choose a DSN Template from the drop down menu and enter a name for the DSN. (You use the name when you set up the ODBC event source type.)
8. Fill in the parameters and click **Save**.

Field	Description
DSN Template	Choose the correct template from the available choices.
DSN Name	Enter a descriptive name for the DSN
Parameters section	
Database	Specify the database used by Citrix XenApp
PortNumber	Specify the Port Number. The default port number is 1433
HostName	Specify the hostname or IP Address of Citrix XenApp
Driver	Depending on your NetWitness Log Collector version: <ul style="list-style-type: none">• For 10.6.2 and newer, use /opt/netwitness/odbc/lib/R3sqls27.so• For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3sqls26.so

Add the Event Source Type

Add the ODBC Event Source Type:

1. In the **NetWitness** menu, select **ADMIN > Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click  under **Actions** and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/Config** from the drop-down menu.
The Event Categories panel is displayed with the existing sources, if any.
5. Click **+** to open the **Available Event Source Types** dialog.

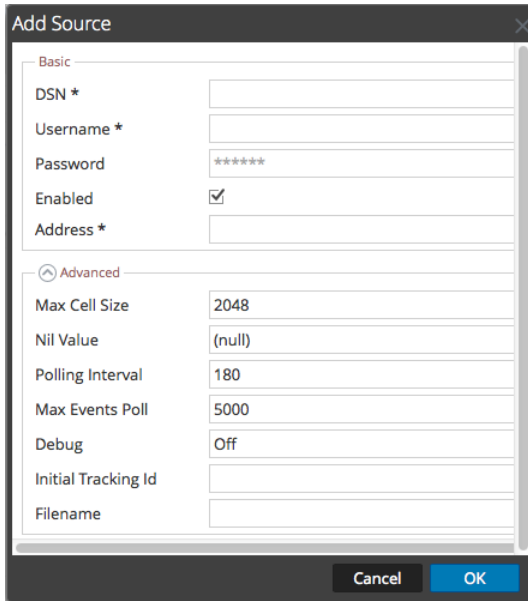


6. Choose the log collector configuration type for your event source type and click **OK**.

For the Event Source Type, select one of the following, based on your version of Citrix XenApp:

- For version 7.x, select **xenapp7configdb**
- For earlier versions, do one of the following:
 - To specify the Config Database, select **xenappconfigdb**
 - To specify the Summary Database, select **xenappdb**

7. In the **Event Categories** panel, select the event source type that you just added.
8. In the **Sources** panel, click **+** to open the **Add Source** dialog.



9. Enter the DSN you configured during the **Configure a DSN** procedure.
10. For the other parameters, see the "ODBC Event Source Configuration Parameters" topic in the *RSA NetWitness Platform Log Collection Guide*.

Reference Tables

This event source collects data from the following tables, using the indicated typespec files.

- The **ConfigLoggingSchema.LowLevelOperationStart** table uses the **xenapp7configdb.xml** typespec file.
- The following tables use the **xenappconfigdb.xml** typespec file:
 - CTXLOG_ADMINTASK_LOGENTRY
 - CTXLOG_ADMINTASK_OBJECT
 - CTXLOG_ADMINTASK_REFERENCCELIST
- The following tables use the **xenappdb.xml** typespec file:
 - LU_APPNAME
 - SDB_SESSION
 - LU_USER
 - LU_SERVERNAME
 - LU_SERVER

-
- LU_CLIENT
 - LU_SERVERINF
 - LU_NETDOMAIN
 - LU_FARMNAME
 - SDB_APPHISTORY

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved.

Trademarks

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

