

NetWitness® Platform XDR

Sybase Adaptive Server Enterprise Event Source Log Configuration Guide

Sybase Adaptive Server Enterprise

Event Source Product Information:

Vendor: [Sybase](#)

Event Source: Sybase Adaptive Server Enterprise

Versions: 15.x

Note: NetWitness 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.

Platforms: Microsoft Windows 2003, Red Hat Enterprise Linux 3, Solaris 2.10

RSA Product Information:

Supported On: NetWitness Platform 11.7 and later

Event Source Log Parser: sybasease

Collection Method: ODBC

Event Source Class.Subclass: Storage.Database

Contact Information

NetWitness Community at <https://community.netwitness.com> contains a knowledge base that answers common questions and provides solutions to known problems, product documentation, community discussions, and case management.

Trademarks

RSA and other trademarks are trademarks of RSA Security LLC or its affiliates ("RSA"). For a list of RSA trademarks, go to <https://www.rsa.com/en-us/company/rsa-trademarks>. Other trademarks are trademarks of their respective owners.

License Agreement

This software and the associated documentation are proprietary and confidential to RSA Security LLC or its affiliates and are furnished under license, and may be used and copied only in accordance with the terms of such license and with the inclusion of the copyright notice below. This software and the documentation, and any copies thereof, may not be provided or otherwise made available to any other person.

No title to or ownership of the software or documentation or any intellectual property rights thereto is hereby transferred. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

This software is subject to change without notice and should not be construed as a commitment by RSA.

Third-Party Licenses

This product may include software developed by parties other than RSA. The text of the license agreements applicable to third-party software in this product may be viewed on the product documentation page on NetWitness Community. By using this product, a user of this product agrees to be fully bound by terms of the license agreements.

Note on Encryption Technologies

This product may contain encryption technology. Many countries prohibit or restrict the use, import, or export of encryption technologies, and current use, import, and export regulations should be followed when using, importing or exporting this product.

Distribution

Use, copying, and distribution of any RSA Security LLC or its affiliates ("RSA") software described in this publication requires an applicable software license.

RSA believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." RSA MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Miscellaneous

This product, this software, the associated documentations as well as the contents are subject to NetWitness' standard Terms and Conditions in effect as of the issuance date of this documentation and which can be found at <https://www.netwitness.com/standard-form-agreements/>.

© 2023 RSA Security LLC or its affiliates. All Rights Reserved.

September, 2022

Contents

- Enable Auditing on Sybase ASE 5**
- Configure NetWitness Platform for ODBC Collection 8**
 - Ensure the Required Parser is Enabled 8
 - Configure a DSN 8
 - Add the Event Source Type 9
- Getting Help with NetWitness Platform 11**
 - Self-Help Resources11
 - Contact NetWitness Support 11
 - Feedback on Product Documentation 12

Enable Auditing on Sybase ASE

Adaptive Server stores audit trail logs in system tables, named `sysaudits_01` through `sysaudits_08`. You have the option to create and specify up to eight system tables for storing audit trails. NetWitness log collection file queries and collects data from all eight audit tables.

Note: You occasionally need to purge the Sybase audit table.

To enable auditing on the Sybase ASE event source:

1. Open a command prompt.
2. Go to the root of the Sybase directory.
If you are in a Linux or UNIX environment, use **SYBASE.csh** or **SYBASE.sh** file if you have not setup the Sybase environment variables.
3. Start the **isql** program as user **sa**:
`isql -Usa -Ppassword -Sserver_name`
4. Determine the next available device number to use for the auditing devices and use `disk init` to create the auditing devices

- For the auditing database:

```
declare @devno int
select @devno = max(low/16777216)+111111 from sysdevices
disk init
name = "auditdev1",
physname = "/opt/sybase/data/sybaud1.dat",
vdevno = @devno,
size = 5120
go

declare @devno int
select @devno = max(low/16777216)+111112 from sysdevices
disk init name = "auditdev2",
physname = "/opt/sybase/data/sybaud2.dat",
vdevno = @devno,
size = 5120
go

declare @devno int
select @devno = max(low/16777216)+111113 from sysdevices
disk init name = "auditdev3",
physname = "/opt/sybase/data/sybaud3.dat",
vdevno = @devno,
size = 5120
go
```

- For the auditing database log:

```
declare @devno int
select @devno = max(low/16777216)+222222 from sysdevices
disk init
name = "auditlogdev",
physname = " C:\sybase\data\sybaudlg.dat",
vdevno = @devno,
size = 5120
go
```

Note: You can tailor auditing devices' sizes to customers' environments.

5. Create the auditing database:

```
create database sybsecurity on auditdev1
log on auditlogdev
go
alter database sybsecurity on auditdev2
go
alter database sybsecurity on auditdev3
go
```

6. Exit the isql program:

```
exit
```

7. Change to the ASE scripts directory and set the DSQUERY environment variable:

```
set DSQUERY = server_name
```

8. Start the **isql** program as user **sa** with the install security script as the input file:

- Windows: `isql -Usa -Ppassword -Sserver_name -iinstsecu`
- Linux or UNIX: `isql -Usa -Ppassword -Sserver_name -iinstallsecurity`

9. Exit the **isql** program and restart the Adaptive Server.

10. Start the **isql** program as user **sa**:

```
isql -Usa -Ppassword -Sserver_name
```

11. Add the additional audit tables:

```
sp_addaudittable auditdev2
go
sp_addaudittable auditdev3
go
```

Note: To create additional auditing devices and audit tables, follow the instructions provided in steps 4 thru 11 above.

12. Enable auditing:

```
sp_configure "auditing",1
```

13. Display the current settings of all the auditing options:

```
sp_displayaudit
go
```

14. Enable auditing options:

```

sp_audit "security","all","all","on"
go
sp_audit "all","sa_role","all","on"
go
sp_audit "all","sso_role","all","on"
go
sp_audit "all","oper_role","all","on"
go
sp_audit "login","all","all","on"
go
sp_audit "logout","all","all","on"
go

```

Note: Refer to Chapter 18 of the *Sybase ASE System Administration Guide: Volume 1* for more information about auditing options.

15. Create a threshold action to periodically clear the audit log:

```

create procedure audit_thresh
as
declare @audit_table_number int
/*
** Select the value of the current audit table
*/
select @audit_table_number = scc.value
from master.dbo.syscurconfigs scc, master.dbo.sysconfigures sc
where sc.config=scc.config and sc.name = "current audit table"
/*
** Set the next audit table to be current.
** When the next audit table is specified as 0,
** the value is automatically set to the next one.
*/
exec sp_configure "current audit table", 0, "with truncate"
return(0)

```

16. Attach the threshold action to the audit log:

```

use sybsecurity
go
sp_addthreshold sybsecurity, aud_seg_01, 100, audit_thresh
go
sp_addthreshold sybsecurity, aud_seg_02, 100, audit_thresh
go
sp_addthreshold sybsecurity, aud_seg_03, 100, audit_thresh
go

```

17. Confirm the threshold action is attached to the audit log:

```

sp_helpthreshold aud_seg_01
go

```

Note: Refer to Chapter 15 of the *Sybase ASE System Administration Guide: Volume 2* for more information about threshold options.

Configure NetWitness Platform for ODBC Collection



To configure Sybase ASE for ODBC collection in NetWitness Platform, perform the following procedures:

- I. [Ensure the Required Parser is Enabled](#)
- II. [Configure a DSN](#)
- III. [Add the Event Source Type](#)

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 NetWitness Platform Live.



Ensure that the parser for your event source is available:

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 `sybasease`.

Configure a DSN

Configure a DSN (Data Source Name):



1. From the NetWitness Platform menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click **Actions** () menu and select **View > Config**.
4. In the Log Collector **Event Sources** tab, select **ODBC/DSNs** from the drop-down menu.
The DSNs panel is displayed with the existing DSNs, if any.
5. Click **+** to open the **Add DSN** dialog.
6. Fill in the DSN Name with a unique and identifiable name.

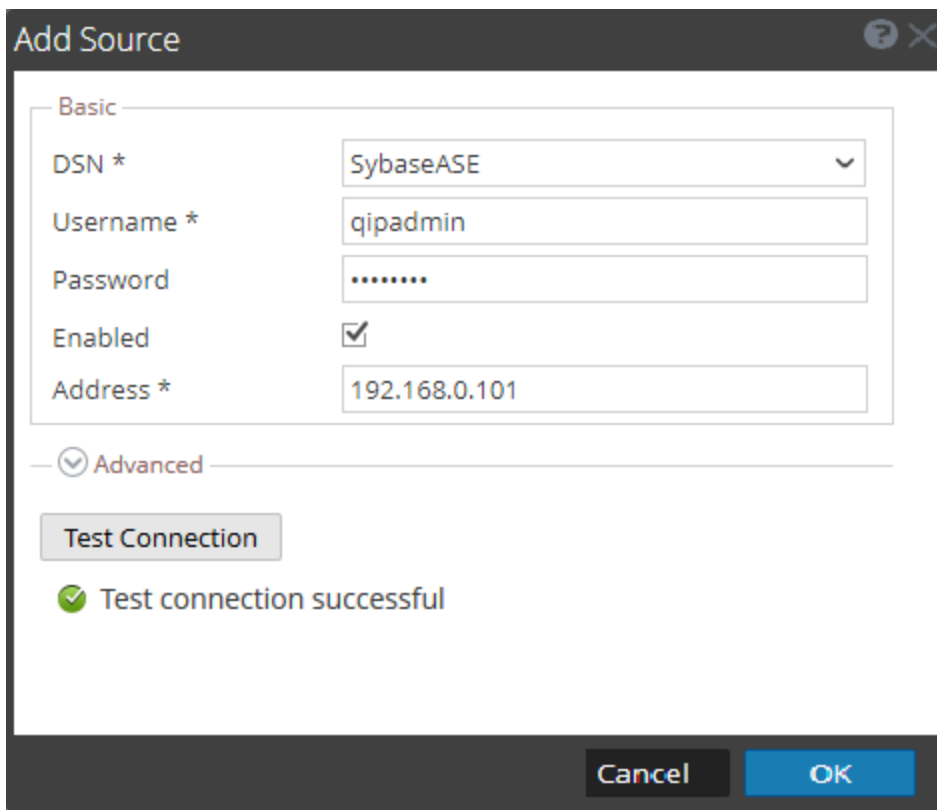
7. Fill in the parameters as follows.

Field	Description
Database	Enter the database name.
NetworkAddress	Enter the IP or Hostname of the Sybase Server, followed by a comma, and then the Port Number to use. For example: 192.168.0.101,5000
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/R3ase27.so • For 10.6.1 and older, use /opt/netwitness/odbc/lib/R3ase26r.so

8. Click **Save** to save the DSN.

Add the Event Source Type

1. From the NetWitness Platform menu, select  (Admin) > **Services**.
2. In the **Services** grid, select a **Log Collector** service.
3. Click **Actions** () menu 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. Select **ase15** from the **Available Event Source Types** dialog and click **OK**.
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, and fill in the values as follows:
 - **DSN**: select the DSN you created earlier
 - **Username**: enter the username used to log in to the Sybase server
 - **Password**: enter the password used to log in to the Sybase server
 - **Address**: enter the IP or hostname of the Sybase server
9. Click the test connection button to verify that the settings are correct.



10. Click **OK** to save your settings.

Getting Help with NetWitness Platform

Self-Help Resources

There are several options that provide you with help as you need it for installing and using NetWitness:

- See the documentation for all aspects of NetWitness here: <https://community.netwitness.com/t5/netwitness-platform/ct-p/netwitness-documentation>.
- Use the **Search** and **Create a Post** fields in NetWitness Community portal to find specific information here: <https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions>.
- See the NetWitness Knowledge Base: <https://community.netwitness.com/t5/netwitness-knowledge-base/tkb-p/netwitness-knowledge-base>.
- See the documentation for Logstash JDBC input plugin here: <https://www.elastic.co/guide/en/logstash/current/plugins-inputs-jdbc.html>.
- See Troubleshooting section in the guides.
- See also [NetWitness® Platform Blog Posts](#).
- If you need further assistance, [Contact NetWitness Support](#).

Contact NetWitness Support

When you contact NetWitness Support, please provide the following information:

- The version number of the NetWitness Platform or application you are using.
- Logs information, even source version, and collection method.
- If you have problem with an event source, enable **Debug** parameter (set this parameter to **On** or **Verbose**) and collect the debug logs to share with the NetWitness Support team.

Use the following contact information if you have any questions or need assistance.

NetWitness Community Portal	https://community.netwitness.com In the main menu, click Support > Case Portal > View My Cases .
International Contacts (How to Contact NetWitness Support)	https://community.netwitness.com/t5/support/ct-p/support
Community	https://community.netwitness.com/t5/netwitness-discussions/bd-p/netwitness-discussions

Feedback on Product Documentation

You can send an email to nwdocsfeedback@netwitness.com to provide feedback on NetWitness Platform documentation.