Integrating NetApp Data ONTAP

EventTracker

Publication Date: Mar 4, 2014

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This guide provides instructions to configure NetApp Data ONTAP to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, and NetApp Data ONTAP 8.1.1 operating in 7- mode and later.

Audience

NetApp Data ONTAP users, who wish to forward CIFS auditing events to EventTracker manager.

Contents

Pre-requisites

Before you begin

- EventTracker must be installed
- NetApp Data ONTAP 8.1.1 operating in 7-mode (or later) must be installed

Configurations

Before you begin

Following are the prerequisites for CIFS auditing:

- CIFS must be licensed and enabled on the storage system before enabling auditing.
- The file or directory to be audited must be in a mixed or NTFS volume or qtree. You cannot audit CIFS events for a file or directory in a UNIX volume or qtree unless Storage-Level Access Guard is enabled.
- Access auditing for individual files and directories must be activated.
- You must specify access events to record.
- IPv4 or IPv6 network connectivity must be configured.

Enable CIFS auditing

When you enable or disable CIFS auditing, auditing of policy change events is enabled. There is no separate CIFS option to enable policy change events at this time.

To turn auditing options on or off, perform one of the following actions as mentioned in the table below.

If you want to turn auditing on or off…	Enter the command…..
File access events	options cifs.audit.file_access_events.enable {on | off}
Logon and Logoff events	options cifs.audit.logon_events.enable {on | off}
Local account management	options cifs.audit.account_mgmt_events.enable {on | off}

events	**NOTE:** You can use MMC Event Viewer to view changes to the account management
All events	cifs audit {start | stop} Alternatively, you can start and stop CIFS auditing using the cifs.audit.enable option. For example, entering the following command is the equivalent the cifs audit start command: options cifs.audit.enable {on | off} Use onto start CIFS auditing or off to stop auditing **NOTE:** CIFS auditing is disabled by default

Specify the maximum size of the cifsaudit.alf file

You can use the cifs.audit.logsize option to specify the maximum size of the cifsaudit.alf file.

Enter the following command:

options cifs.audit.logsize *size*

size is the number of bytes. If you enter an invalid number, a message displays the range of acceptable values.

NOTE:

Data ONTAP overwrites the oldest data after the cifsaudit.alf file reaches the maximum size. To prevent loss of event data, you should save the cifsaudit.alf file before it is filled. By default, when the file is 75 percent full, a warning message is issued. Additional warning messages are sent when the file is nearly full and data is about to be overwritten, and also when data has already been overwritten.

Specify the external event log location

If you prefer to store event logs in a different location, you can use the cifs.audit.saveas option to specify the location.

To specify where Data ONTAP logs audit event information, enter the following command:

options cifs.audit.saveas *filename*

filename is the complete path name of the file to which Data ONTAP logs audit event information. You must use '.evt' as the file extension. You must use quotes around path names that contain a space.

Examples

options cifs.audit.saveas /etc/log/mylog.evt

Specify counter extensions

If you select 'counter' for automatic file naming, the extension is a number value.

Enter the following command:

options cifs.audit.autosave.file.extension counter

Specify maximum number of automatically saved files

You can use the cifs.audit.autosave.file.limit option to specify the maximum number of event files that can be saved automatically.

Enter the following command:

options cifs.audit.autosave.file.limit *value*

value is a number from 0 to 999.
If you set this value to 0, there is no limit for the number of event files that is stored in the storage system automatically. If you set this value to anything other than 0, the oldest event file is always overwritten after the storage system auto save file limit is reached.

NOTE:

If you set this value to 0, you should regularly monitor the /etc/log directory and clear out unnecessary log files. Too many log files in this directory can cause system performance degradation.

Verify the audit log file

Now audit log file will be created under /etc/log/ folder.

NOTE:

Log folder on NetApp server should be shared. EventTracker user should have appropriate access in EventTracker configuration and should be given Read/Write access including on this share.

Configure NetApp Filer Logging

This section describes the configuration to be done on NetApp Filer for enabling different logging formats.

Configure NetApp Filer Message Logs

The NetApp Filer needs to be configured to send the message log events over Syslog to the EventTracker.

To configure NetApp Filer to send message log events over syslog:

1. Log in to NetApp Filer with root privileges.

   The ONTAP> command prompt is displayed.

2. Run the following command to enter advanced mode:

   ONTAP>**priv -level advanced**

3. In advanced mode, edit the /etc/syslog.conf file and add the IP address for the EventTracker.

   . @*IP_address_of_Event_Tracker*

4. To save the file, press **Escape** key and then enter **:wq**.

5. Restart the Syslog daemon for the changes to take effect.

Configure NetApp Filer CIFS audit logs to forward .evt files to EventTracker

Import logs into EventTracker Locally (DLA)

1. Login to EventTracker Enterprise.
2. Click **Admin** dropdown, and then click **Manager**.

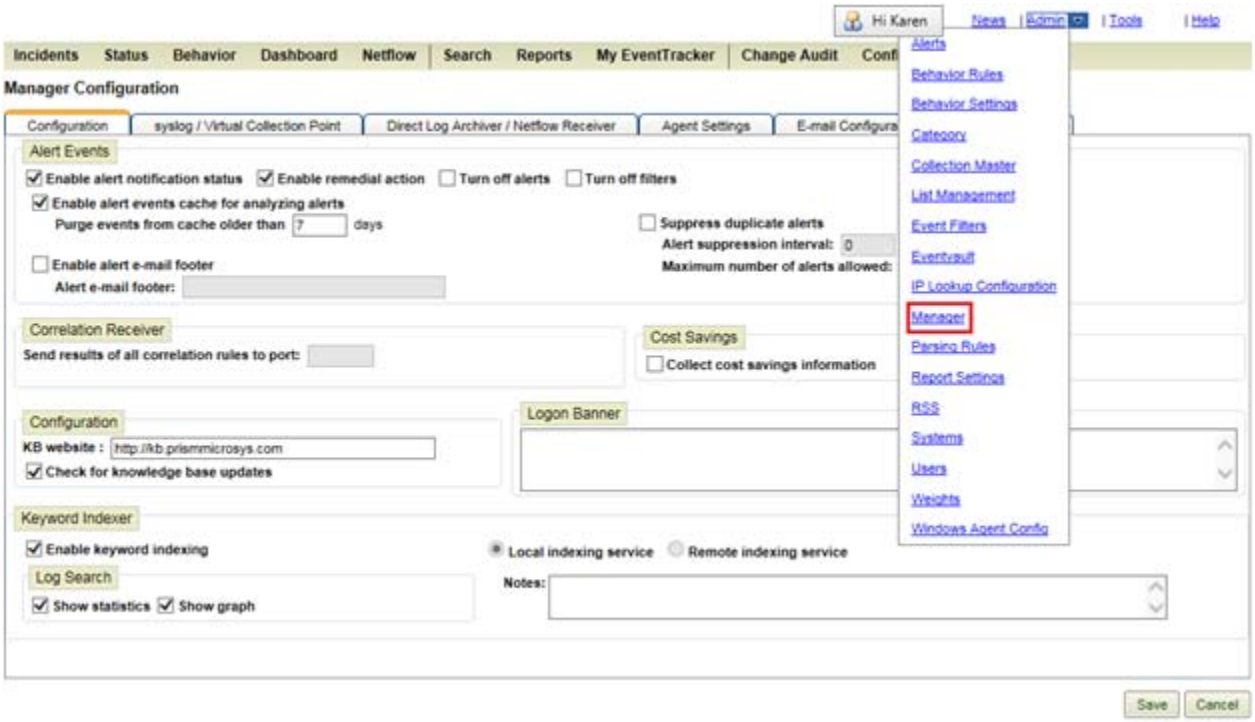

Figure 1

3. Click **Direct Log Archiver /NetFlow Receiver** tab.
4. Click **Direct log file archiving from external sources** option.

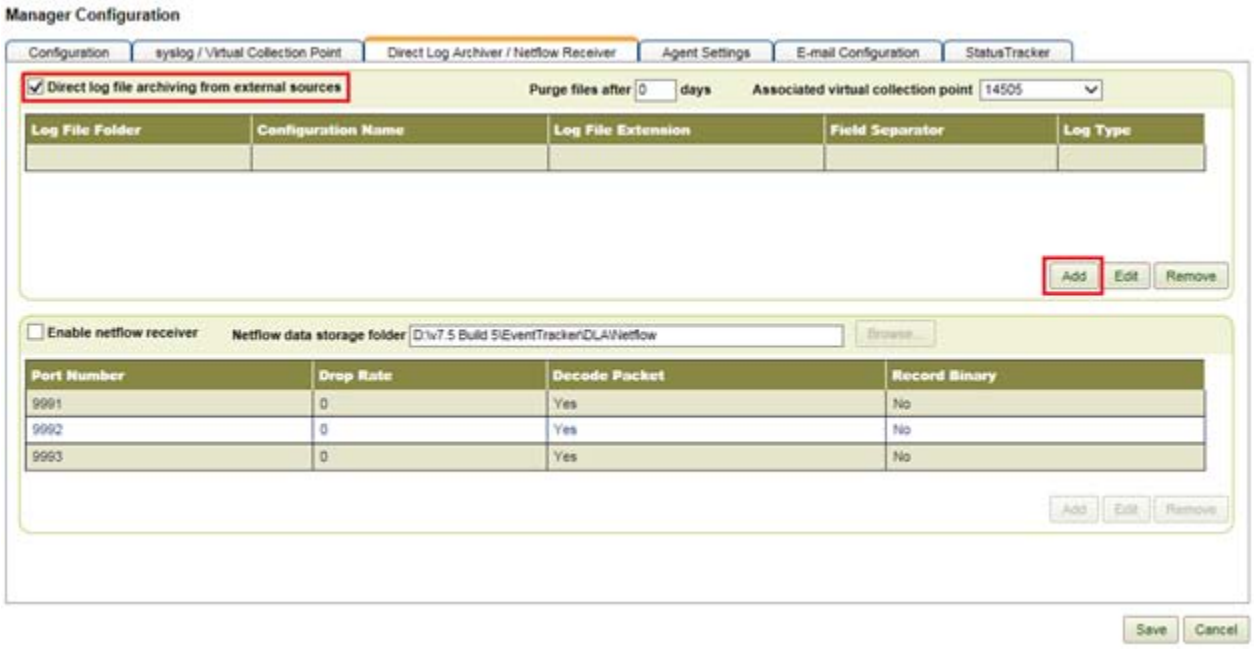

Figure 2

5. Click the **Add** button.

   EventTracker displays Direct Archiver Configuration window.

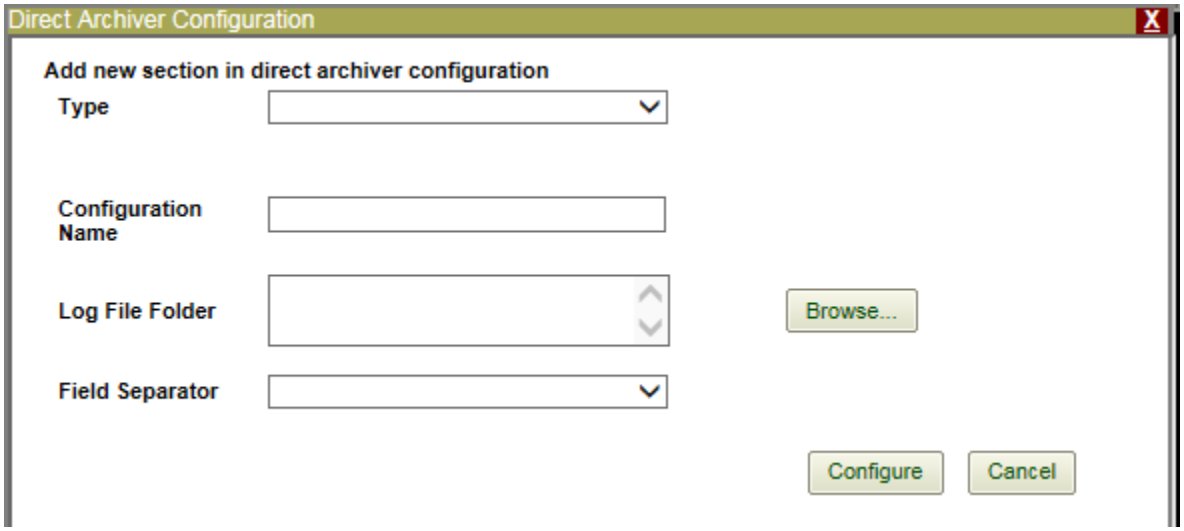

Figure 3

6. In **Type** dropdown, select the type as **EVT** (DLA-Extension).
7. In **Event Log Type** dropdown, select the log type as **Security**.
8. Click the **Browse** button to select the **Log File Folder** path.

(OR)

Type the **Log File Folder** path in the text box.

9. Click the **Configure** button.

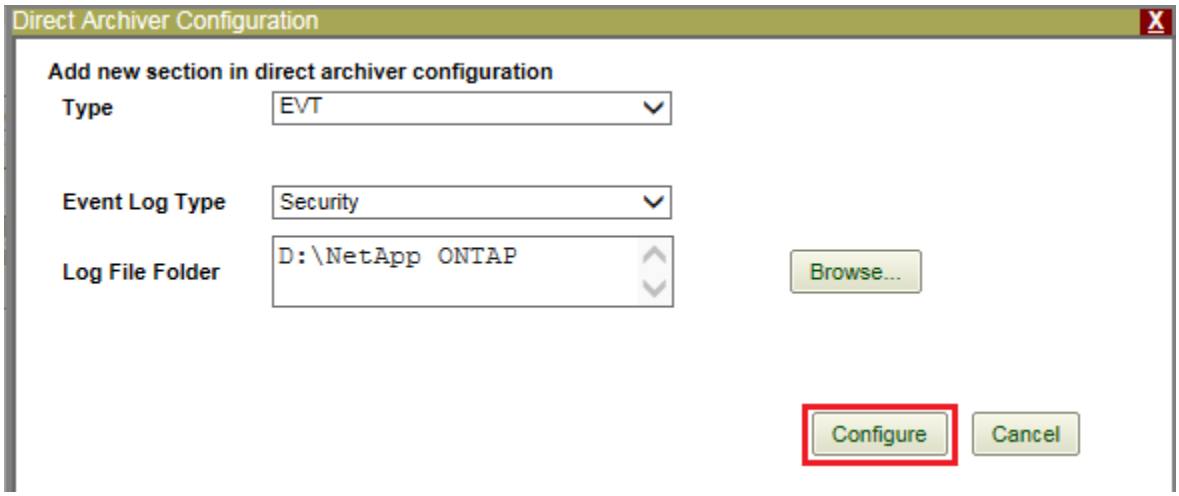

Figure 4

The relevant folder is configured in the DLA folder.

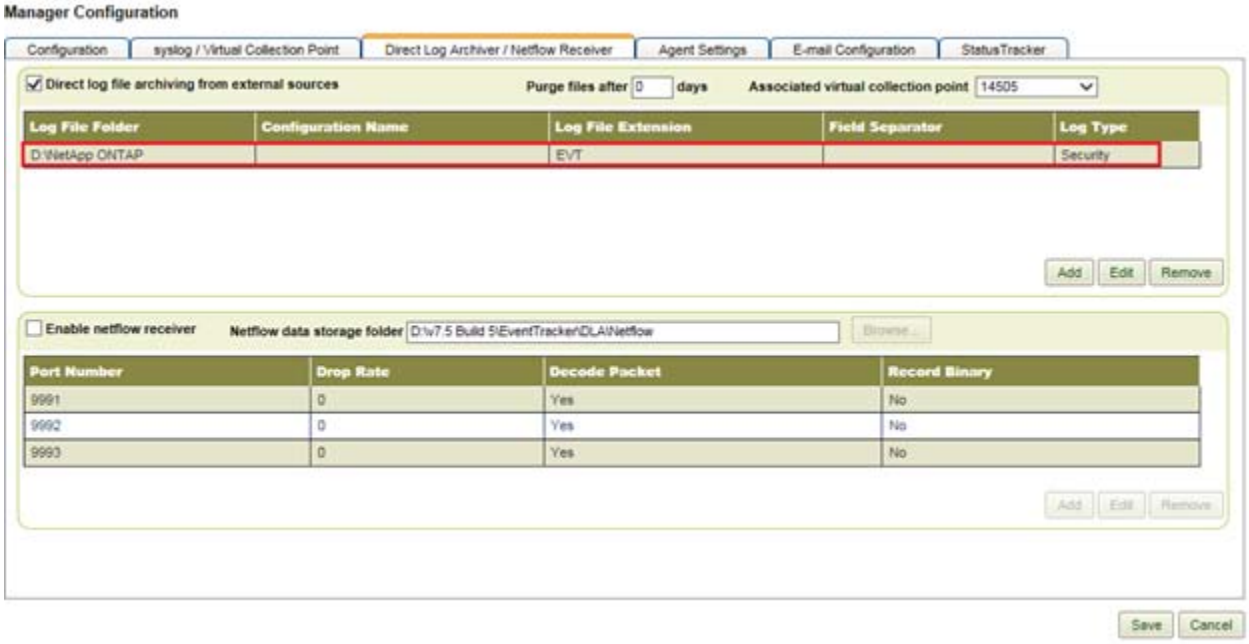

Figure 5

10. Click the **Save** button.

    Now Direct Log Archiver (DLA) has been created successfully. Check the logs in search option of EventTracker.

11. Once DLA is configured and configurations are saved, edit Parser.ini file in notepad and look for NetApp configuration section.

    Parser.ini file is available in **\\InstallDIR\EventTracker**

12. Change log file path to UNC path i.e. shared path of NetApp log file folder (*.evt)).

13. Change EventTracker Scheduler service account to the user used for EventTracker configuration i.e.

    a. Click **Start**, and then click the **Run** button.

    b. Enter **services.msc** and then click the **OK** button.

    c. Right-click **EventTracker Scheduler**, and then select **Properties.**

    d. Select **Log On** tab, and then select **This account:** option**.**

    e. Enter the correct domain name and credentials.

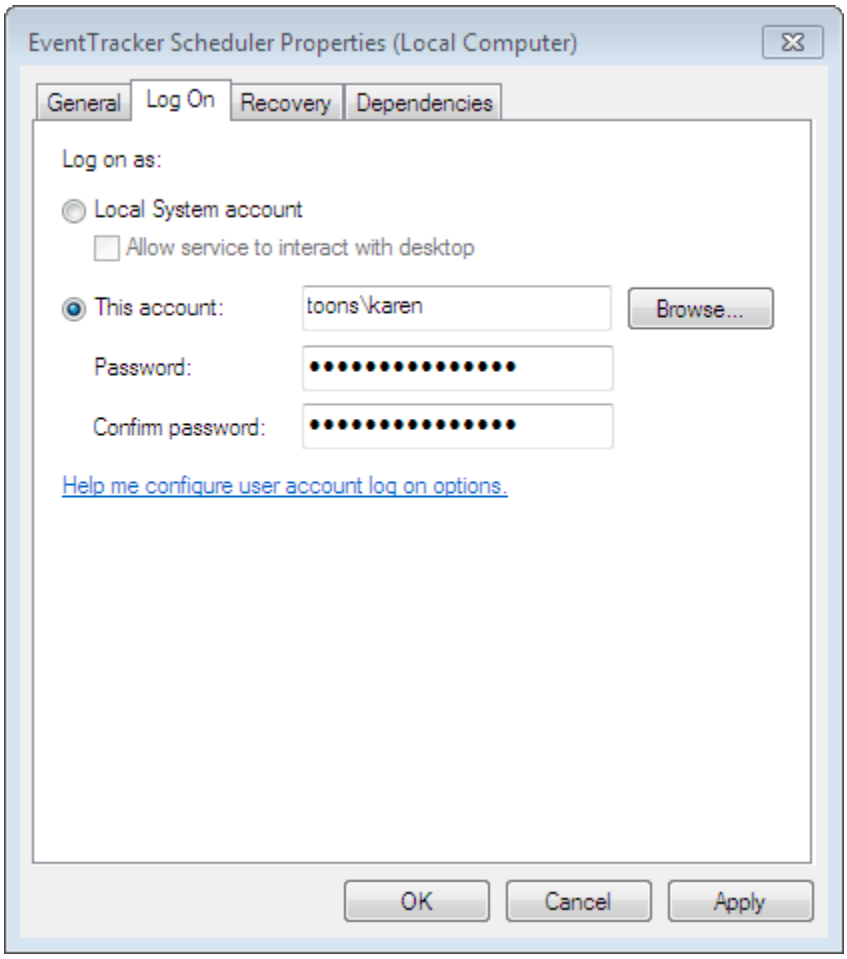

Figure 6

f. Click **Apply** and then click the **OK** button.

g. Click **Restart the Service** for EventTracker Scheduler.