

Configure auditing

The Content Platform Engine, which is the main component of IBM FileNet P8 Platform, provides auditing capabilities for tracking additions, changes, and deletes to the object store content. In this section, you will learn how to configure auditing.

What is auditing?

Auditing is the automatic logging of actions that are performed on a FileNet P8 object or a class.

- You can audit custom or system events that occur for objects so that you can track critical activities.
- Most events on FileNet P8 classes can be audited including the events for security, content management, and business transactions.
- The automatic logging of an event creates an audit entry in the audit log (in the database Event table).
- Audit entries can be programmatically created by custom applications.

For example, you can configure an audit definition for a document class to automatically log audit entries whenever documents of that class are checked in. Checking in a document is the initiating action that causes the CheckinEvent event to fire, which in turn causes an audit entry to be logged.

The following representation shows the sequence of cause and effect:

Initiating action (Checking in) => Event fired on source object (CheckinEvent) => audit entry created in the audit log

Reasons for auditing

You configure auditing to gain information about objects:

- How often was this document accessed?
- When did this property value change?
- Which user made the change?
- Who deleted that document?

With auditing, you can record every time a document is opened, any changes to this document, and every time something was filed in a folder. You can also monitor if a user tries to open a document while lacking read access (denial of access).

About Audit Definitions

An audit definition describes how to audit an event. It includes the event to audit and the following options:

- Record the modified post-event object and the original pre-event object in the audit record.
- Apply a filter expression to the source object of the event.
The filter expression determines whether the event is audited. For example, a filter expression can test if a property on the source object is changed; if not, the event is not audited.
- Name an audit definition to associate it with a particular audit processing client or client function.
- Disable an audit definition.

For a complete list of auditable events, please refer to FileNet P8 Platform V5.5.x Knowledge Center:

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc197.htm

Audit entries

When an audit event occurs, audit entries are created in an audit log that is stored in the Event table of the object store database. Audit entries are instances of one of the subclasses of the Event class. For example, CheckinEvent is an Event subclass.

They can be searched for, viewed, and exported for reporting purposes.

Audit entries contain the following information or properties:

- Event, method, or action that occurred and any applicable parameters
- Name of the user who performed the action
- Date and time of the event
- Class and ID of the associated object
- Success or failure of the event
- Names of any changed properties, depending on the object state recording level
- Text of the query (for queries)
- Statement that the permissions were modified (for security updates)
- Ownership of the audit entry

Audit history and audit log

You can view the audit entries for an object by viewing the object properties (audit history) or by querying the audit log.

You can query the audit log with an object store search. You search for objects that belong to the Event class and its subclasses (Example: object change event). You can enter criteria to further limit the search results returned.

Pruning audit entries

Each event object that is created by auditing is stored as a row in the Event table in the object store database. You can delete audit entries that you no longer need by using manual or automatic pruning to control the size of audit log.

- The *audit subsystem* controls the pruning of audit events from the audit log. You can specify a schedule and configure parameters that control how the audit pruning process is run.
- An *audit disposition policy* specifies the criteria for identifying audit entries for disposition. You can define one or more audit disposition policies at the object store level.
- In *automatic pruning*, audit entries in the audit log are pruned in accordance with audit disposition policies.
- The audit entries for a deleted object are not automatically deleted from the audit log.
- In *manual pruning*, you can manage the size of the audit log by using a query to retrieve and delete audit entries.

If an audit disposition policy is enabled for an audit log, do not manage the size of the log manually.

Audit processing bookmarks

When you manage audit logs with automatic pruning, your custom audit processing applications can partly control the pruning of audit events by setting bookmarks. Bookmarks prevent the subsystem task from deleting those audit events that are still needed.

- A bookmark is a leave-off point in the audit log, which indicates the last record that is processed by the audit processing client.
- When an audit processing client ends a session, it sets its bookmark with an audit sequence number; when it later starts a new session, it retrieves its bookmark and resumes processing at the next audit sequence number.
- There can be multiple bookmarks, each reflecting a different audit processing client.
- The audit disposition subsystem does not delete any records that have audit sequence numbers greater than the lowest-valued bookmark, with the intention of deleting only audited events that were previously processed by clients.
- Applications can use the Content Engine API to set bookmarks.
- You can edit or delete audit disposition bookmarks by using the Administration Console for Content Platform Engine.

Activity: Create audit definitions

In this activity, you enable auditing for an object store and create an audit definition to a custom document class. You update a document and then observe the audit history. You must be the administrator for the object store with full control access to configure items for auditing.



In this activity, you will accomplish the following:

- Enable auditing on the Sales object store.
- Create audit definitions.
- Create audit entries.
- View the audit history.
- Create more audit entries.
- Query the audit log.

Enable auditing on the Sales object store.

You can enable and disable auditing at the object store level. Auditing is disabled by default.

- Ensure that the IBM FileNet P8 Platform components are started.
If you have not started them earlier, start the components by using the earlier activity: *Prepare your system - Start IBM FileNet P8 Platform*.
- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the **Sales** tab > **General** subtab, scroll down and then select **Yes** from the list for the **Enable auditing** field (third row from the bottom of the page).

Compress database tables and indexes : 	No
* Enable auditing :	Yes
* Default checkout type : 	Exclusive
Advanced storage deletion delay : 	600

- Click **Save** and then click **Refresh**.

Create audit definitions.

In this task, you create audit definitions on the Order document subclass. The Order class has two subclasses. These are custom classes that are created for this course on the student system.

- On the left pane for the **Sales** object store tab, navigate to **Data Design > Classes > Document** and select **Order**.

- From the **Order** tab on the right pane, select the **Audit Definitions** subtab.

Use the down arrow on the right to select the subtab from the list. You can also use the forward and backward arrows to scroll to find the subtab.

If the contents of the tab is not displayed, click *Refresh* or click the tab and the content will be refreshed.

- On the **Audit Definitions** subtab, click **New**.
- On the **New Audit Definition** page, type or select the following values for the fields listed below:
 - Display name: **Audit Updates**
 - Event: **Update Event**
 - Object state recording level: **Modified object only**
 - Audit type: **Success**
 - Apply to subclasses: **Selected**
 - Is Enabled: **Selected**

Leave the default for the other fields that are not mentioned here.

The completed page contains the values you entered:

The screenshot shows the 'New Audit Definition' dialog box. It has a title bar 'New Audit Definition' and a subtitle 'Audit definitions represent information that describes how to audit an event. Learn more...'. The dialog is divided into two main sections. The left section contains labels for 'Display name', 'Event', 'Object state recording level', 'Audit type', 'Filter expression', 'Filter property name', and 'Options', each followed by an information icon. The right section contains the corresponding input fields: a text field for 'Display name' with the value 'Audit Updates', a dropdown menu for 'Event' with 'Update Event' selected, a dropdown menu for 'Object state recording level' with 'Modified object only' selected, a group box for 'Audit type' containing two radio buttons ('Success' is selected, 'Failure' is unselected), a text area for 'Filter expression', a text field for 'Filter property name', and a group box for 'Options' containing two checked checkboxes ('Apply to subclasses' and 'Is Enabled'). At the bottom right are 'OK' and 'Cancel' buttons.

Field	Value
Display name	Audit Updates
Event	Update Event
Object state recording level	Modified object only
Audit type	Success
Apply to subclasses	Selected
Is Enabled	Selected

- Click **OK** to create the Audit Definition.
- Verify that your Audit Definition is listed on the **Audit Definitions** subtab of the **Order** tab and then click **Save** to save your work.
- Use the following values and repeat the steps to create another audit definition.
 - Display name: **Audit Deletions**
 - Event: **Deletion Event**
 - Object State Recording Level: **None**
 - Audit type: **Success**
 - Apply to subclasses: **Selected**
 - Is Enabled: **Selected**
- Click **Save** to save the changes to the **Order** class definition and then click **Refresh**.

Verify that your audit definitions are listed on the **Audit Definitions** subtab of the **Order** tab with the values that you selected.

Preprocessor Definitions Subscriptions Audit Definitions Replication Class Mappings							
<input type="button" value="New"/> <input type="button" value="Delete"/> <input type="checkbox"/> Show Inherited							
<input type="checkbox"/>	Display Name	Event	Is Enabled	Apply To Subclasses	Success Audit Type	Failure Audit Type	Object State Recording
<input type="checkbox"/>	Audit Updates	Update Event	True	True	True	False	Modified object only
<input type="checkbox"/>	Audit Deletions	Deletion Event	True	True	True	False	None

- Log out of the administration console and close the browser.

Create audit entries.

In this task, you create audit entries by updating values for properties of the Order document class.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

The Content Navigator Desktop opens with the Browse view as indicated on the upper left of the page.

- From the upper right, click the down arrow next to **LoanProcess** and select **Sales** from the list.
- On the left pane, from the **Sales** object store, click the **Orders** folder.
- On the right pane, right-click a document (Example: **Order Basic A**), and then select **Properties**.
- In the **Properties** tab, change the value (Example: **100**) for the **Amount_due** property and then click **Save**.
- Log out of IBM Content Navigator and then close the browser.

View the audit history.

When auditing is enabled, you can view the audit history of an object to check which audited events took place. The audit log entries include when the change was made, and the user that made the change.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the left pane of the **Sales** tab, expand **Browse > Root Folder** and then click **Orders**.
- Click the link to open the document that you changed in the previous task (Example: **Order Basic A**).
- From the **Order Basic A** tab, open the **Audit History** subtab.
Use the down arrow on the right and select the tab name from the list.
- Click **Refresh** and then verify that there is at least one audit log entry.

Document: Order Basic A, Version: 1.0, Status: Released					
on	Lifecycle Policy	Parents	Children	Tasks	Subscriptions
View the audit entries for an object by viewing the object properties or by querying the audit log.					
Audit history					
	Event	Date Created	Event Status	Creator	Id
	Update	February 2, 2019 at 8:32:57 AM GMT-05:00	Succeeded	p8admin	{8069AE68-0000-C92C-A9BC-78B5AC5A7C53}

- To examine the information that is provided in the audit entry, click the **Update** link.
- From the **Update** tab, under the **General** subtab, examine the values in the fields.

Modified properties :	LastModifier = p8admin amount_due = 100.0 DateLastModified = February 2, 2019 at 8:32:57 AM GMT-05:00
-----------------------	---

The properties that you modified are shown.

- Click **Close** on the **Update** tab, log out of the administration console, and then close the browser.

Create more audit entries.

In this task, you use IBM Content Navigator to check out and download a document to save a local copy. Then you delete the same document from the object store.

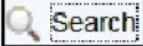
- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the upper right, click the down arrow next to **LoanProcess** and select **Sales** from the list.
- On the left pane, from the **Sales** object store, click the **Orders** folder.
- On the right pane, right-click a document (Example: **PO 3411.tif**) and then select **Check Out > Check Out and Download**.
- In the **Opening ...** dialog box, select **Save File** and then click **OK**.

The file is saved in the Downloads folder.

- Right-click the same document and select **Cancel Check Out**.
- Right-click the same document, select **Delete** and then confirm the Delete.
- Log out of the IBM Content Navigator desktop and then close the browser.

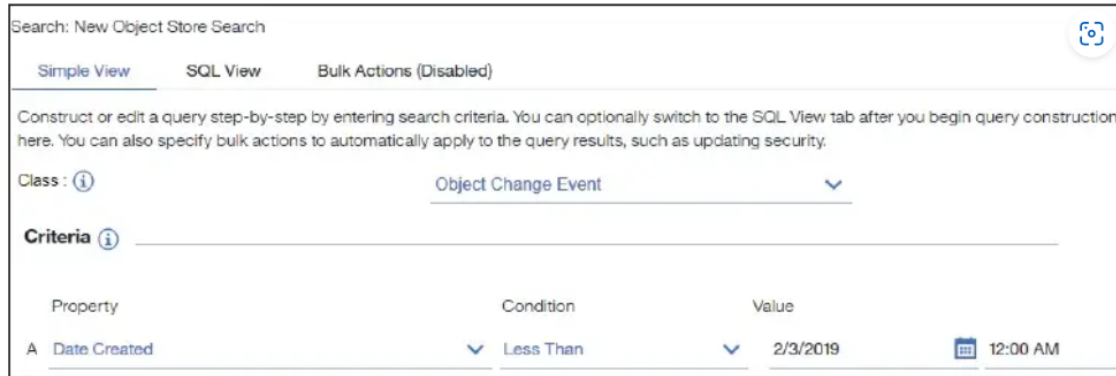
Query the audit log.

In this task, you use the administration console Search page to find audit log entries.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the left pane for the **Sales** object store tab, click the **Search**  icon.
- From the **Saved Searches** tab on the right pane, click **New Object Store Search** to create a new search.

- In the **New Object Store Search** tab > **Simple View** subtab, select the values for the following fields:
 - Class: **Object Change Event**
 - Column A: **Date Created**
 - Condition: **Less than**
 - Value: **Tomorrow's date and any time**



The Completed New Object Store Search contains the class and date that you entered.







Search: New Object Store Search

Simple View SQL View Bulk Actions (Disabled)

Construct or edit a query step-by-step by entering search criteria. You can optionally switch to the SQL View tab after you begin query construction here. You can also specify bulk actions to automatically apply to the query results, such as updating security.

Class:  Object Change Event 



Criteria 

Property	Condition	Value
A Date Created	 Less Than	 2/3/2019  12:00 AM

You can also search for the *Event* parent class (instead of *Object Change Event*) which will return more results.

- Scroll down and in the **Search Result Display** section, select **Audit Sequence** for the **Order By** field.



Order by:  Audit Sequence  ☒ Ascending ☐ Descending

- Click **Run** on the toolbar to execute the search.

- In the **Search Results** tab, review the results and verify that there are two types of audit entries: **Update Event** and **Deletion Event**.

Simple View SQL View Bulk Actions (Disabled) Search Results x			
Actions v			
Search Result Count : 4			
<input type="checkbox"/> ID	Class Description	Audit Sequence	
<input type="checkbox"/> {8069AE68-0000-C92C-A9BC-78B5AC5A7C53}	Update Event	2	
<input type="checkbox"/> {507BAE68-0000-C96E-9522-6C2645CD6DFC}	Update Event	3	
<input type="checkbox"/> {207CAE68-0000-CC54-81B6-F82E4B830DEF}	Deletion Event	4	
<input type="checkbox"/> {507CAE68-0000-CC58-84D2-205BAA1E4248}	Deletion Event	5	

- Click **Save As** on the toolbar to save the Search.
- In the **Save Query** window, type **Object Change Event Query** for the **Document Title** field, and click **OK**.
Note that what name you provide is not critical.
- Click **Close** the new search tab and click **Yes** in the message window to save the changes.
- In the **Saved Searches** tab, click **Refresh**.
Your saved search is listed and can be used for future use.
- Log out of the administration console and close the browser window.

Activity: Prune audit entries

Audit logs can grow quickly and use up storage space. You can export the audit entries to a file (for example, XML) to cut down the storage space used. Then, you can prune the audit logs manually by using a search template, or automatically by using an audit disposition policy. In this activity, you create an audit disposition policy.

In this activity, you will accomplish the following:

- Create an audit disposition policy.
- Configure the audit subsystem.
- Verify that the audit logs are deleted.
- Configure an audit disposition schedule.
- Create some audit entries.
- Disable auditing on the Sales object store.

Create an audit disposition policy.

In this task, you create an audit disposition policy that deletes audit entries that are older than 10 minutes.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the left pane for the **Sales** object store tab, expand the **Administrative > Audit Disposition** node and then click **Audit Disposition Policies**.
- From the **Audit Disposition Policies** tab on the right pane, click **New**.
- Use the following data to complete the wizard and click **Next** to move to the next page of the wizard:
 - Name: **Prune Audit Logs**
 - Disposition rule: **DateCreated < Now () - TimeSpan(10, 'Minutes')**
 - Duration between completed sweeps: **300 seconds**
 - Enable audit disposition policy: **Selected**

Disposition rule includes an expression to identify the audited records to delete from the Event table and it must be a fragment of an SQL WHERE-clause expression. If the expression evaluates to true, the audited event is deleted.

With the value you provided, the audit disposition policy will delete the audit logs that are older than 10 minutes.

Sales Audit Dispo... New Audit D... *

< Back Next > Finish Cancel

Set the Audit Disposition Policy parameters

* Disposition rule : ⓘ DateCreated < Now () - TimeSpan(10, 'Minutes')

* Duration between completed sweeps : ⓘ 300 seconds

☒ Enable audit disposition policy ⓘ

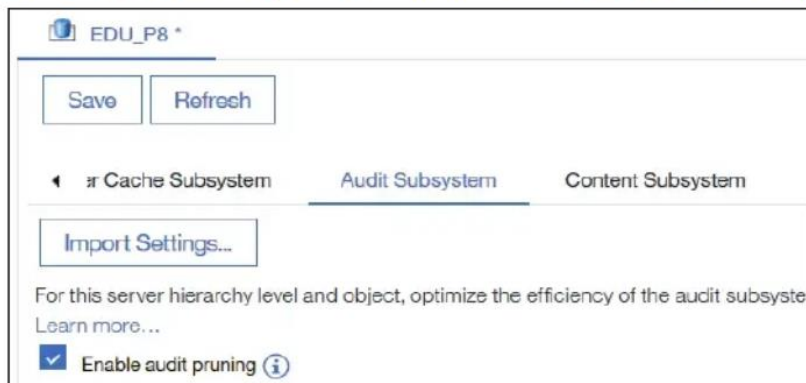
- On the **Summary** page, verify the values that you entered, click **Finish**, and then on the **Success** page, click **Close**.

- In the **Audit Disposition Policies** tab, click **Refresh**.
Verify that your new audit disposition policy is listed.
- Close the **Audit Disposition Policies** and **Sales** tabs and leave the administration console open for the next task.

Configure the audit subsystem.

The audit subsystem controls the pruning of the audit entries from the audit log. In this task, you enable the audit subsystem so that the auto disposition policy that you defined in the previous task can run.

- In **ACCE**, from the **EDU_P8** tab, select the **Audit Subsystem** subtab on the right pane.
Use the down arrow on the right to select the tab.
- Click **Refresh** if the content on the tab is not displayed.
- On the **Audit Subsystem** subtab, select the **Enable audit pruning** option.



- Click **Save** and then click **Refresh**.

Verify that the audit logs are deleted.

In the previous tasks, you enabled the audit subsystem and configured the audit disposition policy to delete audit logs that are older than 10 minutes. In this task, you verify that the audit entries are deleted from the audit log.

- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the left pane for the **Sales** object store tab, click the **Search** icon.
- From the **Saved Searches** tab, click the **Object Change Event Query** link (the search that you saved earlier).
- In the **Object Change Event Query** tab, click **Run**.
- Verify that the search returns zero results this time.

Search: Object Change Event Query, Version: 1.0, Status: Released

Description :

Simple View SQL View Bulk Actions (Disabled) Search Results ✕

Actions ▼

Search Result Count : 0

Query returned no object

Recall that in the previous activity, the same search returned results. Since you deleted the audit entries by using an audit disposition policy, the search returns zero results.

- Close the **Object Change Event Query**, **Saved Searches**, and **Sales** tabs.
- In **Windows Explorer**, navigate to the folder that contains the Content Platform Engine server logs: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**
- Open the **p8_server_error.log** file in **Notepad++**, scroll to the end of the file, and then verify that a full audit disposition sweep was completed.

```
75 2019-02-02T09:35:38.038 FC1BB8AA AUDT FNRCE0000I - INFO
A full audit disposition sweep has completed; 5 records deleted, 0 failure(s).
```

Note: A single line on the log file is shown in two screen captures.

- Close the file, minimize the **Notepad++** and the **Windows Explorer** windows.

Configure an audit disposition schedule.

In this task, you create a schedule for the audit subsystem so that the audit disposition policy runs every 5 minutes, one day a week.

- In the **ACCE**, from the **EDU_P8** tab, select the **Audit Subsystem** subtab.
- On the **Audit Subsystem** subtab, scroll down to the **Schedule** area and click **New**.
- Use the following values for the fields to configure on the **New Time Period** dialog box:
 - Day of week: **Today's day of the week**
 - Start time: **Current system time plus 5 minutes**
 - Duration: **0 hours 15 minutes**

For the Start time field, select closest time slot that is listed, then edit the value.

New Time Period

A time period determines when the subsystem processing begins and ends.

* Day of week : Monday ▼

* Start time : 9:45 AM ▼

* Duration : 0 hours 15 minutes

OK
Cancel

- Click **OK** on the dialog box and then click **Save** on the **EDU_P8** tab.
- Log out of the administration console and close the browsers.

Create some audit entries.

In this task, you use IBM Content Navigator to update property values for documents.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the upper right, click the down arrow next to **LoanProcess** and select **Sales** from the list.
- On the left pane, from the **Sales** object store, click the **Orders** folder.
- On the right pane, right-click a document (Example: **Order Basic A**) and then select **Properties**.
- On the **Properties** tab, change the value (Example: **150**) for the **Amount_due** property and then click **Save**.
- Repeat the previous steps in this task to change the value for the **Amount_due** property on a couple of the documents.

If any of the documents do not have a value for this property, type a value.

- Log out of IBM Content Navigator and close the browser.

- Log out of IBM Content Navigator and close the browser.
- In **Windows Explorer**, navigate to the folder that contains the Content Platform Engine server logs: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**
- Open the **p8_server_error.log** file in **Notepad++**, scroll to the end of the file, and then verify that there are a series of delay entries, one for each object store.

```
2019-02-02T09:59:01.978 9C2645FB ENG FNRCE0000I - INFO ScheduledPoolExecutor: AuditDisposition:
2019-02-02T09:59:01.978 9C2645FB ENG FNRCE0000I - INFO ScheduledPoolExecutor: AuditDisposition:
2019-02-02T09:59:01.978 9C2645FB ENG FNRCE0000I - INFO ScheduledPoolExecutor: AuditDisposition:
2019-02-02T09:59:01.978 9C2645FB ENG FNRCE0000I - INFO ScheduledPoolExecutor: AuditDisposition:
```

```
AuditDisposition:LoanProcessQA serial=27 added to the delay queue true size of the delay queue 48
AuditDisposition:SalesQA serial=47 added to the delay queue true size of the delay queue 48
AuditDisposition:Sales serial=37 added to the delay queue true size of the delay queue 48
AuditDisposition:LoanProcess serial=17 added to the delay queue true size of the delay queue 48
```

Lengthy lines on the log file are shown in two screen captures.

The Audit Disposition subsystem is delaying until the time that you scheduled as the start time. If the start time is reached, there will not be any delay queues, instead there will be an entry with a full audit disposition sweep that is completed.

- Check the **p8_server_error.log** again after **5 minutes** and then keep checking the log until after the **15-minute** duration time expires.
- In **Notepad++**, right-click the tab with file name and select reload to refresh the entries in the file.

Notice that after the duration time expires, there are no more entries that are logged for a full audit disposition sweep. The next audit disposition sweep will run one week from today, starting with the scheduled start time.

One of the entries should show a number of records that are deleted, corresponding to the number of documents that you updated.

```
ScheduledPoolExecutor: AuditDisposition:Sales serial=37 added to the delay queue
ScheduledPoolExecutor: AuditDisposition:SalesQA serial=47 added to the delay que
A full audit disposition sweep has completed; 0 records deleted, 0 failure(s).
A full audit disposition sweep has completed; 0 records deleted, 0 failure(s).
A full audit disposition sweep has completed; 5 records deleted, 0 failure(s).
```

If the entries are not shown at the expected time, close the file and reopen.

- Close the **p8_server_error.log** file and then minimize the **Notepad++** window.

Disable auditing on the Sales object store.

Since the audit logs can grow quickly and use up storage space, you will disable auditing for the object store that you enabled earlier.

- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or type the following URL: **http://vclassbase:9080/acce**
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- On the left pane of the **EDU_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.
- On the **Sales** tab > **General** subtab, scroll down and select **No** from the list for the **Enable auditing** field (third row from the bottom of the page).
- Click **Save** and then click **Refresh**.
- Log out of the administration console and then close the browser window.