

Work with audit logs

Why is this lesson important to you?

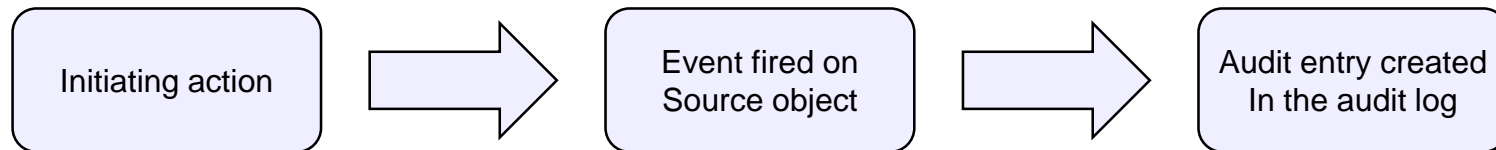
- As a system administrator, you are asked to help determine when event actions are successful and when they fail. You must know how to configure auditing to log these event actions, search for the audit events, and manage the audit log size.

Unit objectives

- Create audit definitions
- View audit entries
- Prune audit entries

What is auditing?

- Auditing is the automatic logging of actions that are performed on an object or class.
 - Applications can create custom audit classes.



Example:

Configure an audit definition for a document class to automatically log audit entries when:

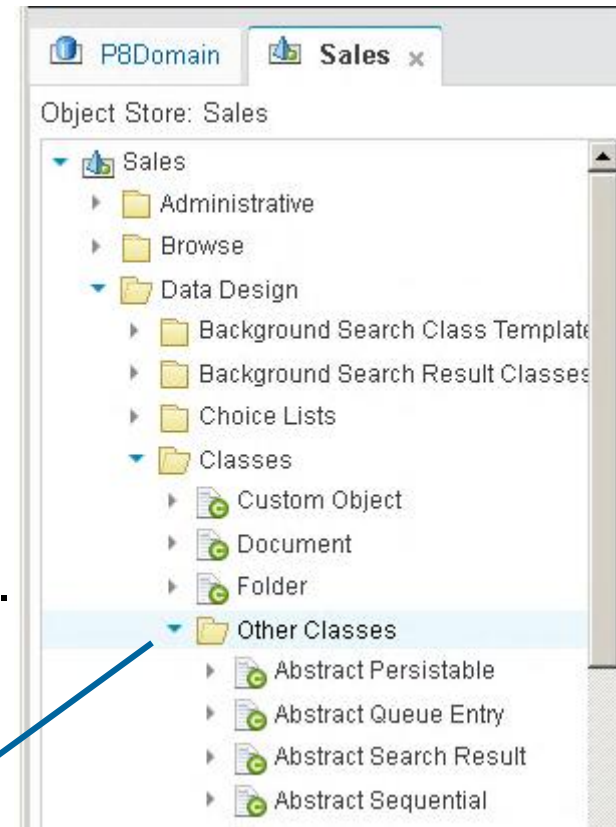
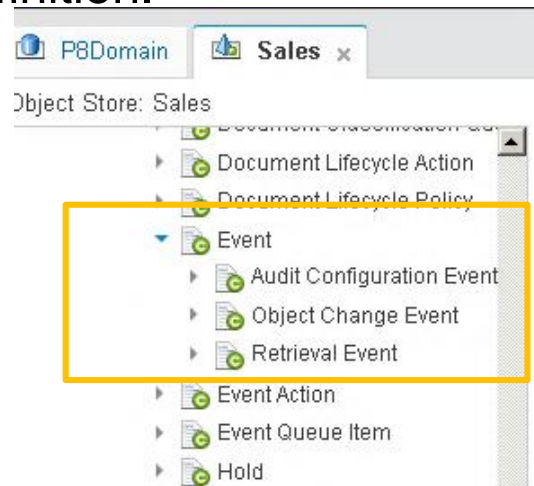
- Documents of that class are checked in.

Why audit?

- You configure auditing to gain information about objects.
- For example:
 - How often was this document accessed?
 - When did this property value change?
 - User made the change.
 - Who deleted that document?
- More examples of other data that you can record:
 - Everything that ever changed on this document.
 - Every time something was filed in a folder.
 - When a user tries to open a document while lacking read access.
 - Every time a document is opened.

Audit Definitions

- An audit definition describes how to audit an event.
- An audit definition 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.
 - Name an audit definition to associate it with a particular audit processing client or client function.
 - Disable an audit definition.



Create an audit definition

Object Store: Sales

- Data Design
 - Background Search Class Template
 - Background Search Result Classes
 - Choice Lists
 - Classes
 - Custom Object
 - Document
 - Book
 - Code Module
 - Email
 - Entry Template
 - Order

Audit Dispo... x New Audit D... * x Order x

Save Refresh Actions Close

Class Definition: Order

finitions Subscriptions **Audit Definitions** Replication Class Ma

New Delete Show Inherited

Display Name Event

New Audit Definition

Audit definitions represent information that describes how to audit an event. [Learn more...](#)

Display name: ?

* Event: ? Deletion Event

* Object state recording level: ? None

* Audit type: ?
☐ Success
☐ Failure

Filter expression: ?

Filter property name: ?

Options: ?
☐ Apply to subclasses
☐ Is Enabled

Object operations that you can audit

The screenshot shows a configuration window for auditing object operations. On the left, there are several fields with question mark icons for help:

- * Event: ?
- * Object state recording level: ?
- * Audit type: ?
- Filter expression: ?
- Filter property name: ?
- Options: ?

A dropdown menu is open on the right, displaying a list of auditable events. The first item, "Deletion Event", is highlighted. The list includes:





- Deletion Event
- Cancel Checkout Event
- Change Class Event
- Change State Event
- Checkin Event
- Checkout Event
- Classify Complete Event
- Creation Event
- Deletion Event
- Demote Version Event
- Freeze Event
- Get Content Event
- Get Object Event
- Lock Event
- Move Content Event
- Promote Version Event
- Query Event
- Unlock Event
- Update Event
- Update Security Event

Audit entries

- Audit entries are stored in the Event table of the object store database.
 - Can be searched for, viewed, and exported for reporting purposes.
- Each entry is a subclass of the Event class.
 - CheckinEvent is an Event subclass.
- Audit entries contain the following information or properties:
 - The event, method, or action that occurred and any applicable parameters.
 - The date and time of the event.
 - The class and ID Of the associated object.
 - The event was a success or failure.
 - The names of any changed properties, depending on the object state recording level.
 - For queries, the text of the query.
 - For security updates, a statement that the permissions were modified.
- Audit entries have an ownership property.

View audit entries

- View the Audit History of an object by using Administration Console for Content Platform Engine.
 - Find the Audit History tab of the object.

Audit history					
	Event	Date Created	Event Status	Creator	Id
	Update	September 15, 2016 at 5:10:37 PM Eastern Standard Time	Succeeded	P8Admin	{9FB0B3B8-4700-435B-BD10-3CFC308CD4D7}
	Update	September 15, 2016 at 5:10:22 PM Eastern Standard Time	Succeeded	P8Admin	{63EC7E73-FA39-4632-A230-462D6ED13B4E}
	Creation	September 15, 2016 at 5:10:22 PM Eastern Standard Time	Succeeded	P8Admin	{5F7A1C7D-65C5-4BF8-B1CF-6D7A2B50869C}


- Create a search for audited events:
 - Specify class: Event, Object Change Event, Deletion Event, and so on.
 - Specify limiting criteria, such as Date Created.


Search: Query audit log, Version: 1.0, Status: Released



Description:

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. bulk actions to automatically apply to the query results, such as updating security.

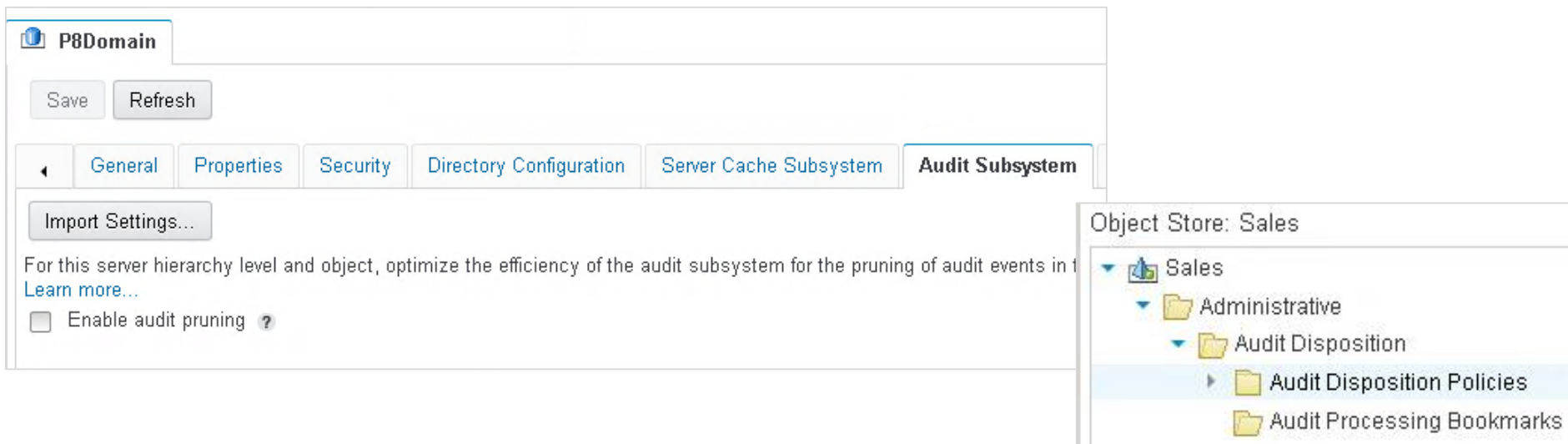
Class: 

Criteria 

Column	Condition	Value
A <input type="text" value="Date Created"/>	<input type="text" value="Less Than"/>	<input type="text" value="9/30/2016 12:00 AM"/>  

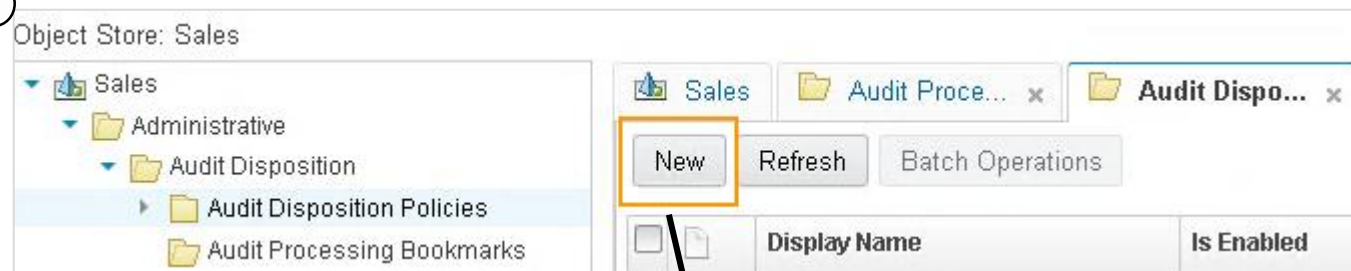
Pruning audit entries

- Audit disposition subsystem
 - Controls the pruning of audit events from the audit log.
 - Can schedule to control when the audit pruning process runs.
- Audit disposition policy:
 - Automate the deletion of audit entries that you no longer need.
 - Useful for controlling the size of the audit log.
- Audit disposition bookmarks
 - Prevent deleting audit events that are still needed.
- Manual pruning – use search templates with bulk actions



Create an audit disposition policy

①



②

Name the Audit Disposition Policy

A disposition policy specifies the criteria for selecting audit records for deletion. [Learn more...](#)

* Name:

Prune audit entries older than 90 days

Existing names:

Prune audit logs

Prune Managers

③

Set the Audit Disposition Policy parameters

* Disposition rule: ?

DateCreated < Now () - TimeSpan(90, 'Days')

* Duration between completed sweeps: ?

86400 seconds

☒ Enable audit disposition policy ?

Audit disposition schedule

History Configuration | Server Cache Subsystem | **Audit Subsystem** | Content Subsystem | Content Cache Sub

Import Settings...

For this server hierarchy level and object, optimize the efficiency of the audit subsystem for the pruning of audit events in the audit log. [Learn more...](#)

☒ Enable audit pruning ?

* Deletion batch size: ?

* Deletion query size: ?

* Wait interval: ? sec

* Maximum lease interval: ? sec

Schedule ?

The schedule is the designated time periods of the week during which the dispatcher prunes audit entries. If you do not define any time periods, the dispatcher can run at any time.

<input checked="" type="checkbox"/>	Start Day	Start Time	Duration
<input type="checkbox"/>	Tuesday	10:15 AM	13mins

New Time Period

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

* Day of week:

* Start time:

* Duration: hours minutes

Unit summary

- Create audit definitions
- View audit entries
- Prune audit entries

Exercise: Work with audit logs

Exercise introduction

- Create audit definitions
- Prune audit entries

