Course Guide

IBM FileNet Content Manager 5.2.1: Auditing and Logging

Course code F287 ERC 1.0

IBM Training

October 2016 edition

Notices

This information was developed for products and services offered in the US.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml.

Contents

Trademarks

The reader should recognize that the following terms, which appear in the content of this training document, are official trademarks of IBM or other companies:

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

FileNet® WebSphere®

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Windows is a trademark of Microsoft Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

Course description

IBM FileNet Content Manager 5.2.1: Auditing and Logging

Duration: 2 hours

Purpose

This course is for administrators that maintain IBM FileNet Content Manager environments, and need to learn: How to monitor the system logs and enable trace logging to troubleshoot issues. How to use auditing to trace object activity.

Audience

This course is intended for system administrators who maintain IBM FileNet Content Manager environments.

Prerequisites

- Skills:
- Experience with P8 terminology, including: Content Platform Engine, IBM Content Navigator, object stores, objects.
- Ability to add, checkout, and delete documents, using IBM Content Navigator.
- Experience with the Administration Console for Content Platform Engine.
- Experience creating document and folder classes, property templates, and so on.
- Recommended prerequisite courses to teach required skills:
- F270 – IBM Content Navigator 2.0.3.6: Introduction, or equivalent knowledge
- F280 - IBM FileNet Content Manager 5.2.1: Introduction, or equivalent knowledge
- F282 - IBM FileNet Content Manager 5.2.1: Work with object metadata, or equivalent knowledge
- F283 - IBM FileNet Content Manager 5.2.1: Security, or equivalent knowledge

Objectives

- Monitor system logs.
- Enable/disable trace logging for troubleshooting.
- Configure a content migration policy.
- Create an audit definition.
- View audit entries.

- Prune audit entries.

Contents

- Content Platform Engine system logs
- Web Application server logs
- Log locations
- Trace logs
- Trace subsystem - domain level configuration
- Trace subsystem - site level configuration
- Guidelines: Monitor log files
- What is auditing?
- Why audit?
- Audit definitions
- Create an audit definition
- Object operations that you can audit
- Audit entries
- View audit entries
- Pruning audit entries
- Create and audit disposition policyAudit disposition schedule

Curriculum relationship

To learn about related courses, visit the IBM training and skills website: http://www.ibm.com/services/learning

Agenda

Note

The following unit and exercise durations are estimates, and might not reflect every class experience.

Day 1

(00:15) Course introduction
(00:20) Unit 1. Work with system logs
(00:30) Exercise 1. Work with system logs
(00:30) Unit 2. Work with audit logs
(00:40) Exercise 2. Work with audit logs

Unit 1. Work with system logs

Estimated time

00:35

Overview

In this unit, you learn how to monitor the system logs and configure trace logging for troubleshooting.

How you will check your progress

Successfully complete the unit exercises.

References

IBM Knowledge Center for FileNet P8 Platform 5.2.1

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8toc.doc/welcome_p8.htm

IBM Training

Why is this lesson important to you?

- As the system administrator, you must be familiar with:
  - The logs available to monitor IBM FileNet Content Manager environments.
  - How to monitor the content and size of the logs.
  - How to archive log files.
  - How to enable/disable trace logging for troubleshooting.

Figure 1-1. Why is this lesson important to you?

IBM Training

Unit objectives

- Monitor system logs
- Enable/disable trace logging for troubleshooting

Figure 1-2. Unit objectives

IBM Training

Content Platform Engine System Logs

- Content Platform Engine produces several log files during normal operation.
  - Primary troubleshooting tool for the administrator:
    - p8_server_error.log
    - pesvr_system.log
    - p8_server_trace.log
- You must monitor these log files to do the following tasks:
  - Become familiar with normal log entries.
  - Observe changes in behavior that might indicate a problem.
  - Ensure that log files have enough space for growth.

Figure 1-3. Content Platform Engine System Logs

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Viewing the FileNet P8 log files

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.common.admin.doc/logs/logs_reference.htm

The Content Platform Engine, which is the main engine of IBM FileNet Content Manager, provides logging capabilities for issue tracking, error tracking, troubleshooting, and auditing or process tracking.

Information

If the organization uses the document approval workflows, there are more tools available to monitor the workflow system:

- vwtool
- vwmsg
- PElog
- vwverify

The IBM Case Foundation administration courses will help you use these tools effectively.

IBM Training

Location of logs

- Default location:
  - WebSphere Application Server:
    - install_root/profiles/profile_name/FileNet/server_instance_name
    - Example:
      C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1
  - WebLogic Server:
    - bea/user_projects/domains/domain_name/FileNet/AdminServer
  - JBoss Application Server:
    - jboss_install/jboss-as/bin/FileNet/server_instance_name
- File location can be configured.
- System log location is shown in the CE Ping page.
- In a clustered environment, the Content Platform Engine log files exist on each server.
  - Located in the *server_instance_name* under the current working directory of the deployed application.

Figure 1-4. Location of logs

By default the Content Platform Engine logs are stored in the web application servers' profile or instance folder.

You can change the location where the files are stored.

The Content Engine Startup Content page (CE Ping page) shows the path configured for the log files.

In a clustered environment, each server will contain its own log files.

IBM Training

Web application server logs

- Each web application server generates its own logs.
- WebSphere
  - Location: *install_root*/profiles/*profile_name*/logs/*server_name*
  - Logs:
    - SystemOut.log
    - SystemErr.log
    - startServer.log
    - stopServer.log
- WebLogic
  - Location:
    - *oracle_home*/admin/*domain_name*/aserver/servers/AdminServer/logs
  - Logs:
    - AdminServer.log
    - access.log
    - Base_domain.log
- JBoss
  - Location: *install_root*/server/*server_name*/log
    - Server.log

Figure 1-5. Web application server logs

You might also need to monitor the web application server logs. When troubleshooting IBM FileNet Content Manager issues, you will need to collect the logs for the Content Platform Engine and the web application server. IBM Content Navigator, which provides the user interface for IBM FileNet Content Manager, logs errors and entries in the web application server's logs.

This slide lists the three web application servers supported, the default path for the log files and the log files in order of importance.

WebSphere

Examples of log locations:

WebSphere (Windows): C:\Program Files\IBM\WebSphere\AppServer\profiles\default\logs\server1

WebSphere (Linux): /opt/ibm/WebSphere/AppServer/profiles/AppSrv01/logs/server1

WebLogic

Example of log location:

WebLogic: C:\bea\user_projects\domains\base_domain\servers\AdminServer\logs

To change the name and location of server logs, refer to the BEA documentation.

IBM Training

Trace logs

- Trace logs are used for troubleshooting particular problems.
- Often requested by a support representative.
- Content Platform Engine trace logging:
  - Use Administration Console for Content Platform Engine to configure trace logging
  - Configure at Domain level or site level
- Web application server trace logging
  - Configure level of detail
- Disable trace logging when you no longer need it.
  - Trace logs can grow quickly and impact system performance and disk space.

Figure 1-6. Trace logs

Help paths

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Troubleshooting>Creating a trace log

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc070.htm

MustGather technote: http://www.ibm.com/support/docview.wss?uid=swg21308231

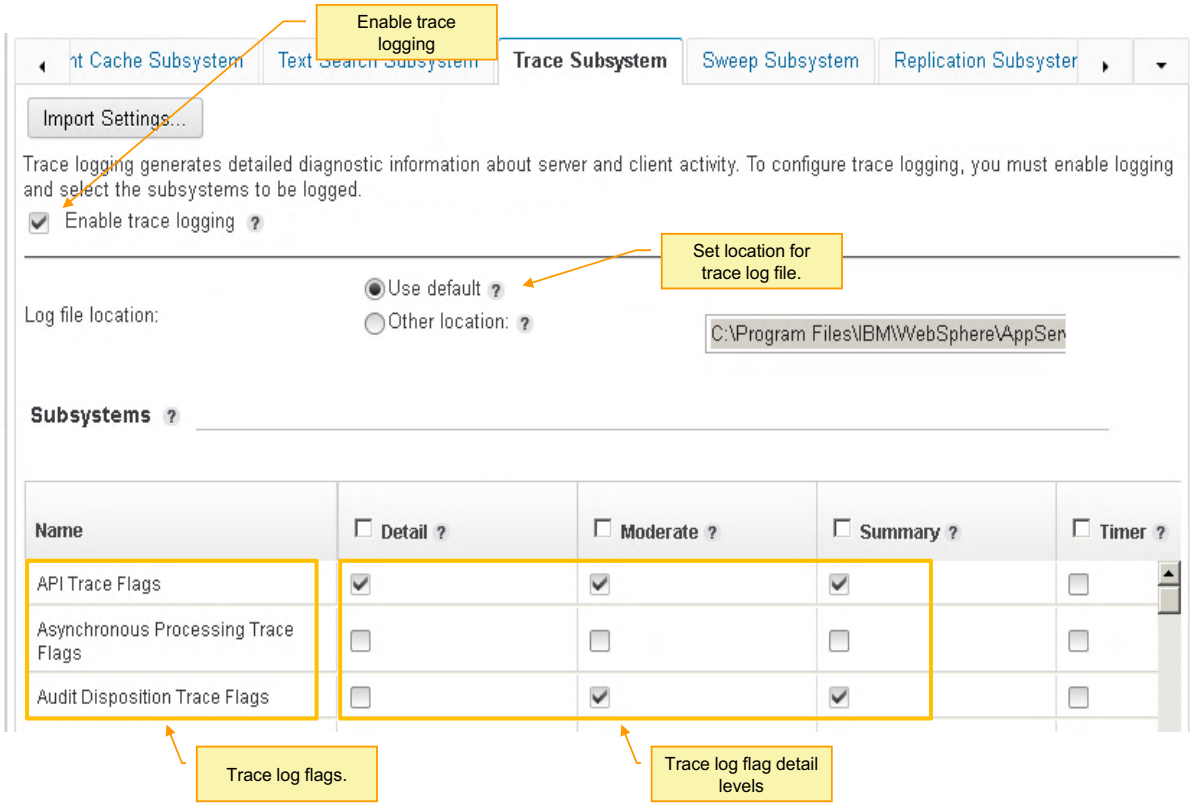
As an administrator you need to know how to configure trace logging.

Trace logs are used to troubleshoot specific issues. If you open a support call, the representative might request that you enable trace logging and reproduce the issue. In that situation, the representative will recommend which subsystem flags to enable and what level of detail to collect. The Must Gather technote, included in the help paths, provides guidelines for what data and logs to collect when reporting an issue with support. If your organization has a dedicated web application server administrator, you will need to collaborate to capture the web application server trace logs.

You can configure trace logging at the domain level or the site level. The site-level configuration takes precedence over the domain level. Site level configuration is used in organizations that have multiple sites.

IBM Training

Trace subsystem – domain level configuration



Work with system logs

Figure 1-7. Trace subsystem – domain level configuration

Help paths

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Troubleshooting>Creating a trace log>Subsystems that support trace logging

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.dev.ce.doc/logging_concepts.htm#supported_subsystems

Configuration:

Enable trace logging on the domain or site object

Specify the subsystems and their flags.

For each flag, specify the level of detail.

The graphic shows the Trace Subsystem tab in the Administration Console for Content Platform Engine at the domain level. The call-outs show:

- How to enable trace logging.
- How to set the log file location.
- How select trace logging flags.
- How to set the level of detail to collect.

The trace logging subsystem can be configured at the domain level, the site level, or both. If the settings are configured at the site level, then those settings override the domain level settings.

You must first enable trace logging to be able to select any other settings.

Important: When you configure trace logging, make sure that you check the domain and site settings. Site settings override domain settings.

The server configures trace logging for a particular subsystem by setting the value of the corresponding trace logging configuration property.

Trace flag detail levels

- **Summary** (value 2) Enables minimal high level logging by providing summary information for all operations. This setting should not significantly affect system performance.
- **Moderate** (value 4) Enables more detailed high level logging than the SUMMARY option for all operations (includes all SUMMARY level information). This setting has some impact on system performance.
- **Detail** (value 8) Enables the most detailed logging by providing detailed information for all operations. This setting is primarily used to aid in debugging (includes all SUMMARY and MODERATE level information). This setting significantly affects system performance, and in some cases, can have a severe impact.
- **Timer** (value 1) Provides the length of time (in milliseconds) that Content Platform Engine takes to complete an operation, such as uploading a file. This setting should not significantly impact system performance. Be aware that if detail or moderate logging levels are selected, the timing will be affected.

IBM Training

Trace Subsystem – site level configuration

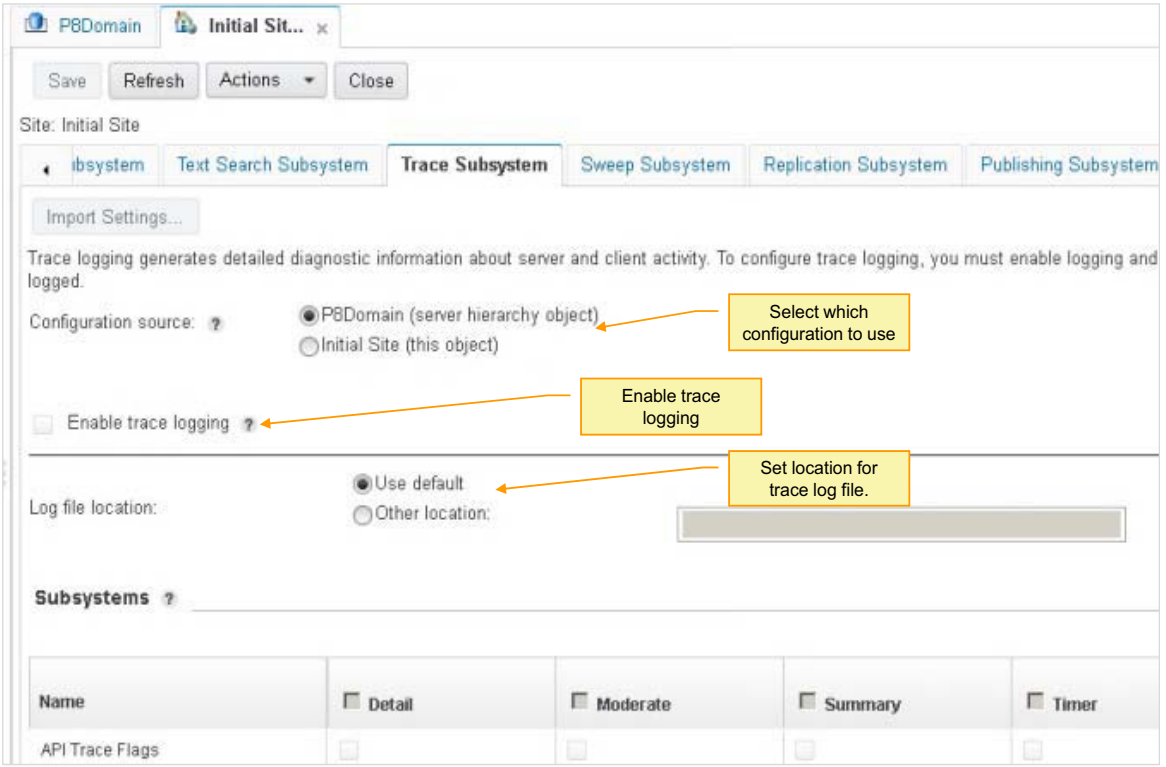


Figure 1-8. Trace Subsystem – site level configuration

The graphic shows the Trace Subsystem tab in the Administration Console for Content Platform Engine at the site level. The call-outs show:

- How to select whether to use domain level trace subsystem configuration or site level. For example, if Initial Site (this object) is selected, then the Trace Subsystem configuration defined for the P8Domain is ignored and the configuration defined for the Initial Site is used.
- How to enable trace logging.
- How to set the log file location.

How you select the trace flags and the level of detail to include, is configured the same way at the site level as it is configured at the domain level.

IBM Training

Guidelines: Monitor log files

- Establish a baseline: Know what to expect.
  - Observe normal log activity so that you can identify changes.
- Monitor logs regularly (daily).
  - Watch for new error messages.
  - Watch for any change in error log size.
    - Example: 1 log file is normally 64 KB, and on one day it is 100 KB.
- Increase monitoring after any system changes.
  - Example: Patches applied
- Keep records of normal comparison logs.
  - Keep representative usage time intervals for each month.
  - After a year, keep representative time intervals for each year.

Figure 1-9. Guidelines: Monitor log files

Part of detecting problems is being aware of what normal activity looks like. If you establish a baseline of activity and you are familiar with the normal error messages that your system generates, you can better detect anomalies, such as new or more frequent error messages.

Log level sizes can be a clue that something is wrong. For instance, a single error might produce a new log entry every 5 minutes. This new log entry causes the log file to grow much more quickly, which you first detect by observing the change in the log file size. If you keep a week of logs each month, you have comparison information to use in case of a change. If you keep more than that, you might be using more space than you need. If no major changes have changed the log behavior after a year or so, you might decide that you need only a representative week for the whole year. It is important to have a baseline to compare your system logs to, so that you can observe changes. When you call customer support for help with a problem, the customer support technician does not know your system baseline log behavior. You can provide information about changes only if you are tracking the logs. This information can help the customer support technician isolate the problem and provide a quicker solution.

IBM Training

Unit summary

- Monitor system logs
- Enable/disable trace logging for troubleshooting

Figure 1-10. Unit summary

IBM Training

Exercise: Work with system logs

Work with system logs

Figure 1-11. Exercise: Work with system logs

IBM Training

Exercise introduction

- Archive and view system logs
- Configure trace logging

Figure 1-12. Exercise introduction

Unit 2. Work with audit logs

Estimated time

00:30

Overview

In this unit, you learn how to configure audit definitions to track object activity.

How you will check your progress

Successfully complete the unit exercises.

References

IBM Knowledge Center for FileNet P8 Platform 5.2.1

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8toc.doc/welcome_p8.htm

IBM Training

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.

Figure 2-1. Why is this lesson important to you?

IBM Training

Unit objectives

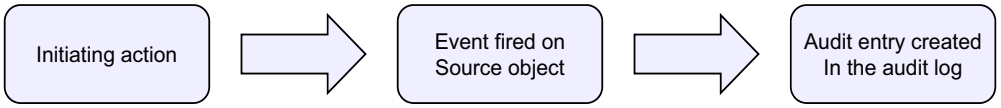
- Create audit definitions
- View audit entries
- Prune audit entries

Figure 2-2. Unit objectives

IBM Training

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.

Figure 2-3. What is auditing?

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc004.htm

Auditing is the logging of 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 those events that pertain to security, content management, and business transactions. The automatic logging of an event creates an audit entry in the audit log (the database Event table). Audit entries can also be programatically created by custom applications.

The diagram shows the sequence of cause and effect.

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.

Why audit?

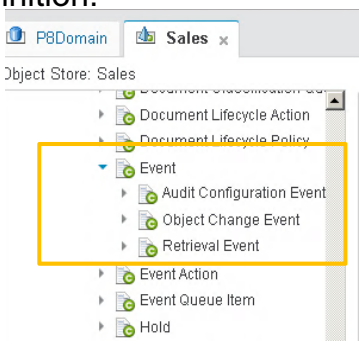
- You configure auditing to gain information about objects.
- For example:
  - How often was this document accessed?
  - When did this property value change?
  - User made the change.
  - Who deleted that document?
- More examples of other data that you can record:
  - Everything that ever changed on 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.

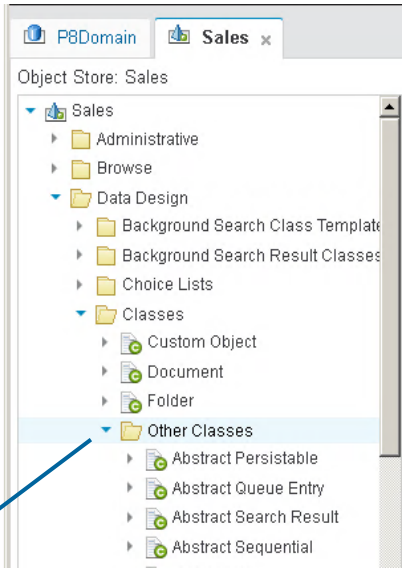
Figure 2-4. Why audit?

IBM Training

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.





Work with audit logs

Figure 2-5. Audit Definitions

Help path

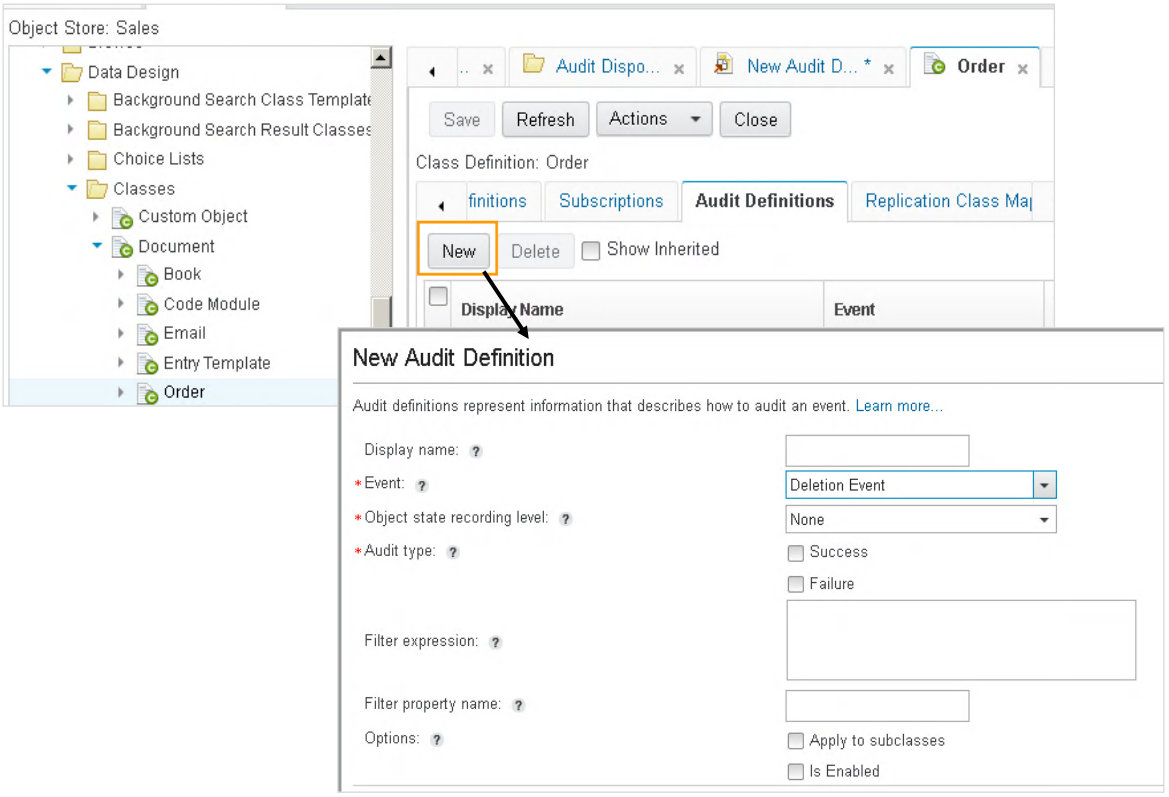
FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Enabling audit logging>Configuring a class to log events>Audit definitions

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc005.htm

You can find the event classes for an object store under Data Design > Classes > Other Classes > Event. The screen capture, on the right, shows the object store, Sales, in the Administration Console for Content Platform Engine. Data Design > Classes > Other Classes > Event > Other Classes. Scroll down the list of other classes until you see Event. If you expand the class, Event, you see the list of Event subclasses (screen capture on the left).

IBM Training

Create an audit definition



Work with audit logs

Figure 2-6. Create an audit definition

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Developing FileNet P8 applications> Content Engine Development> Content Engine Java and .NET Developer's Guide> Reference>SQL Syntax Reference>Relational Queries

http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.ce.dev.ce.doc/query_sql_syntax_rel_queries.htm

To create an audit definition, you use the Administration Console for Content Platform Engine to create an audit definition. Open the object you want to audit and go to the Audit Definitions tab. For example, the upper screen capture show the document class, Order with the Audit Definitions tab selected. When you click New, to create a new audit definition, the New Audition Definition page is displayed (lower screen capture).

Display name: The name of the audit definition.

Event: The type of event to audit. In this example: Deletion Events are being audited. You can specify multiple audit definitions on a single class.

Object state recording level:

- None

- Modified object only – save only the modified object.
- Original and modified objects – save the original object and the modified object.

Information

The objects are stored as binary objects in the Event table, not easily read.

Filter expression: The filter expression determines whether the event is audited. If the value of the expression evaluates to true, the event is audited; otherwise, the event is not audited. For example, a filter expression can test if a property on the source object changed; if not, the event is not audited. Filter expressions are applied only for successful operations. Functionality equivalent to subscription filtering.

> For example, Audit update events when AccountBalance < 1000. Set Filter Expression to: “AccountBalance < 1000.0”. Filter expression is an optional field. The IBM Knowledge Center topic, listed in the Help path, is a reference that will assist in creating filter expressions.

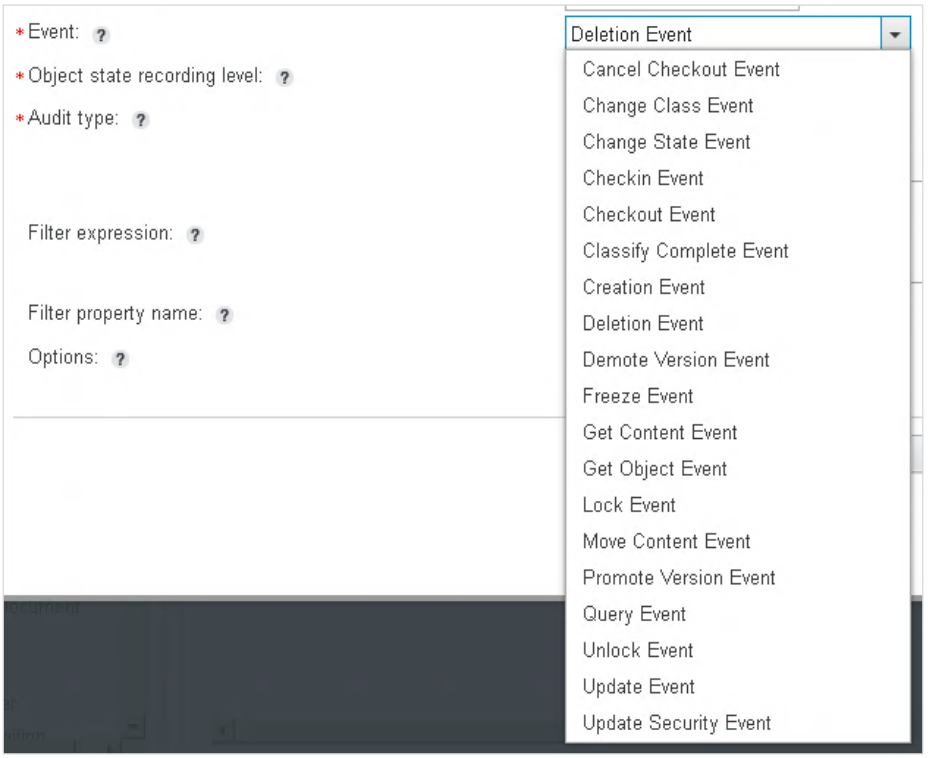
Filter property name: the symbolic name of the object-valued property that is defined on the source object for use in the evaluation by the filter expression.

Options:

- **Apply to subclasses:** Whether or not to apply the audit definition to the current class and all its subclasses or just the current class.
- **Is Enabled:** Whether or not to enable the audit definition. If the option is not selected, the audit definition is inactive. You can start or stop auditing for a specific event and class without having to re-create an audit definition.

IBM Training

Object operations that you can audit



Work with audit logs

Figure 2-7. Object operations that you can audit

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Subscribable and auditable events

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc197.htm

You can subscribe to or audit many Content Platform Engine events. The IBM Knowledge Center topic, provides a table that lists:

- The events in alphabetical older, that you can audit.
- The actions that fire the events and the classes on which the actions apply.
- Additional event-related information.

Note

An action on an object can generate multiple events. For example, when you create a document, a Creation event is generated, an Update event is generated when the content is set to the document, and another Update event is generated when the system properties (for example Creator, Date Created) are set. A Checkin event is generated when you check in a document and also when you create a document. When you delete a document that has multiple versions, multiple Deletion events are generated, one for each document version.

IBM Training

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.

Figure 2-8. Audit entries

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Viewing audit entries>Audit entries

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc006.htm

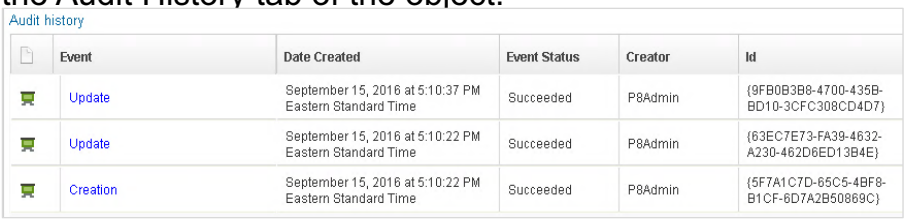
FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Viewing audit entries>Audit entry security

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc037.htm

When an audit event occurs, the Content Platform Engine creates *audit entries* 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.

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.



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

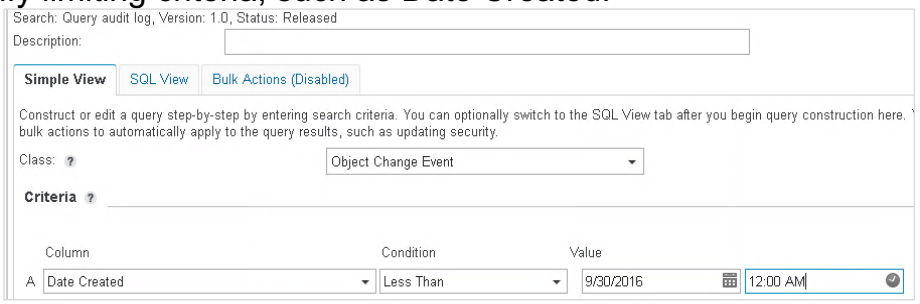


Figure 2-9. View audit entries

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Viewing audit entries

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc025.htm

Audit history:

You can view the audit entries in the audit history of the specific object. The upper screen capture, shows the audit history of a document of a specific document class, that is auditing for creation and update events.

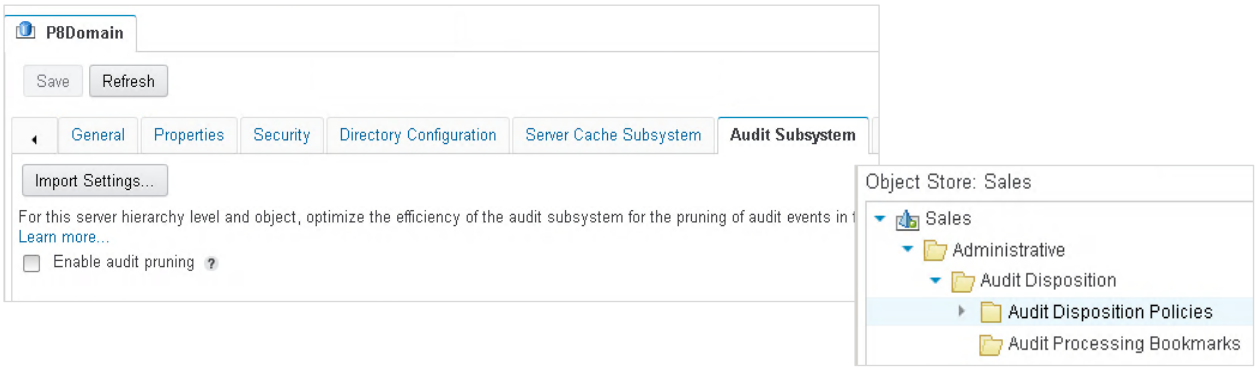
Audit log:

You can query the audit log with an object store search. You specify the class to search for as the class, event, object change event, which includes several of the events, or a specific event. For example, Deletion Event. You can enter criteria to further limit the search results returned. The lower screen capture, shows an object store search that will return audit entries for creation, checkout/checkin, deletion, update, and so on, where the date created is less then September 30, 2016 at midnight.

IBM Training

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



Work with audit logs

Figure 2-10. Pruning audit entries

Help path

FileNet P8 Platform>FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Managing objects>Tracking object activity>Pruning audit entries

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/p8pcc024.htm

Audit disposition subsystem:

The audit disposition subsystem controls the pruning of audit event in the audit log. You enable the audit pruning from the Audit Subsystem tab of the P8 domain, using the Administration Console for Content Platform Engine (screen capture on the lower left). In the Audit Subsystem tab you can also schedule when you want the pruning process to run.

Audit disposition policy:

At the object store level, you can define audit disposition policies, (screen capture on the lower right). The audit disposition policy defines exactly what to delete. For example, delete Update Events that are older than 90 days.

Audit disposition bookmarks:

Audit disposition bookmarks are set to audit sequence numbers. The audit disposition subsystem does not delete any audit events that have audit sequence numbers greater than the lowest-valued bookmark. Applications can use the Content Engine API to set bookmarks so that audit events are not deleted before audit entries are processed. You can edit or delete audit disposition bookmarks using the Administration Console for Content Platform Engine.

Manual pruning:

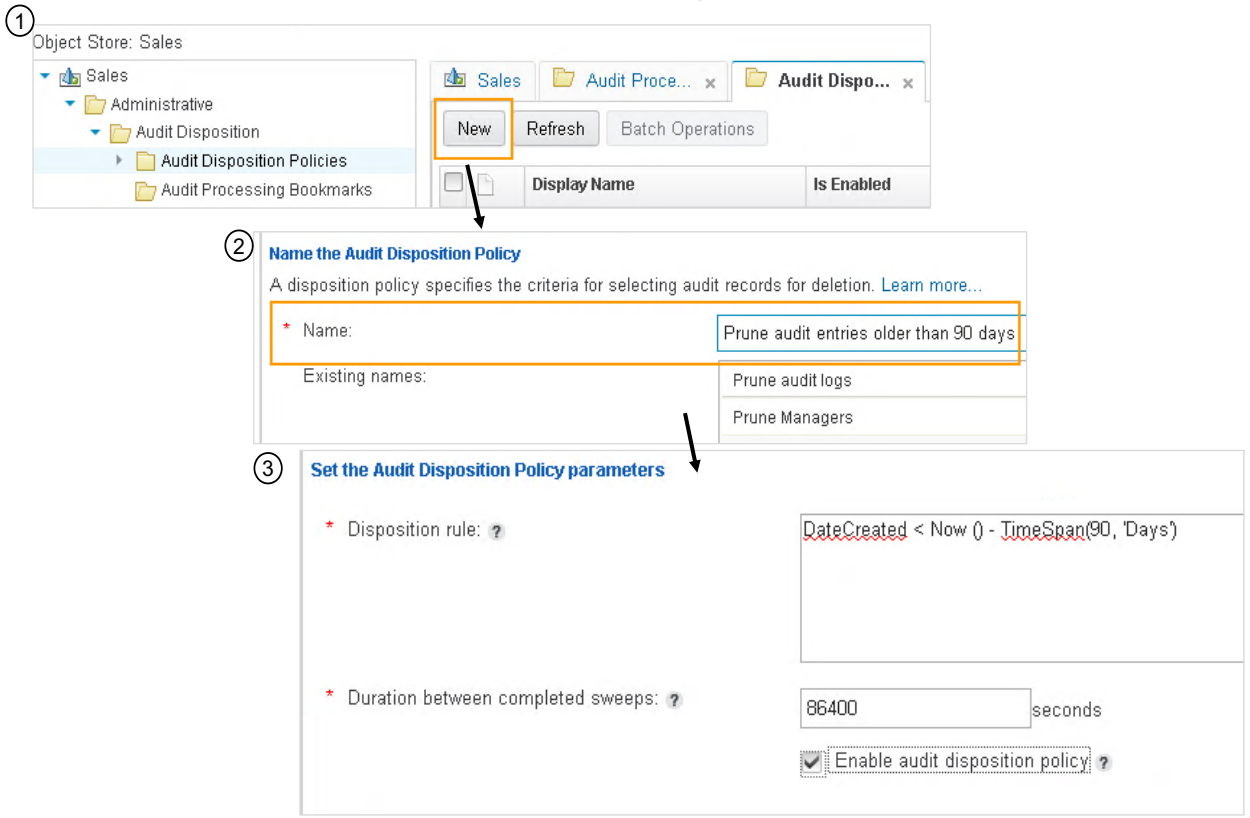
Audit entries for deleted objects are not automatically deleted. You can manually manage the size of the audit log by using a query to retrieve and delete audit entries. For example, you can use a query to delete the audit entries that were created on a particular day or by a particular user.

Important

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

IBM Training

Create an audit disposition policy



Work with audit logs

Figure 2-11. Create an audit disposition policy

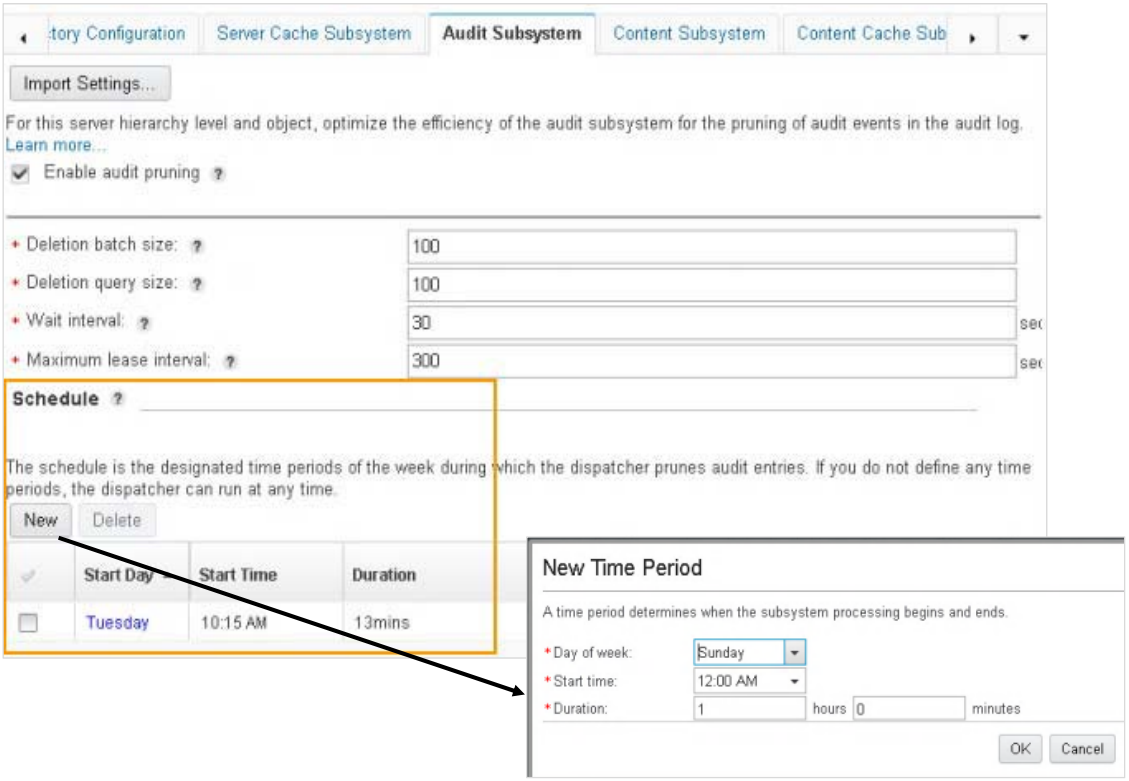
To create an audit disposition policy:

1. Open object store in the Administration Console for Content Platform Engine, and go to Administrative > Audit Disposition > Audit Disposition Policies. Then click New (upper screen capture).
2. Type a name for the audit disposition policy. If audit disposition policies already exist, they are displayed under Existing names.
3. Set the Audit Disposition Policy parameters:
   - Disposition rule: Similar to the filter expression used to define the audited events.
   - Duration between completed sweeps: The number of seconds that the system waits before running the disposition policy again. By default the value is 84,600 seconds or 24 hours.
   - Enable audit disposition policy flag: If set the disposition policy is enabled to run.

   The lower screen capture shows a disposition rule that will delete audit entries that are older than 90 days. The disposition policy will run once every 24 hours and it is enabled.

IBM Training

Audit disposition schedule



Work with audit logs

Figure 2-12. Audit disposition schedule

You can control when the deposition policy runs by configuring time periods in the schedule section of the audit subsystem.

The graphic shows the Audit Subsystem tab, at the domain level. The orange rectangle shows a time period scheduled to start on Tuesday at 10:15 AM that runs for 13 minutes. When the duration of 13 minutes expires, the audit subsystem will be suspended until the following Tuesday at 10:15 AM.

You can create multiple time periods to control when audit pruning runs. You click New, to create a new time period. The arrow points to the new time period wizard.

Scheduled time periods:

- Can be defined at the domain level and the site level.
- Control when audit definitions run as well.

IBM Training

Unit summary

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

Figure 2-13. Unit summary

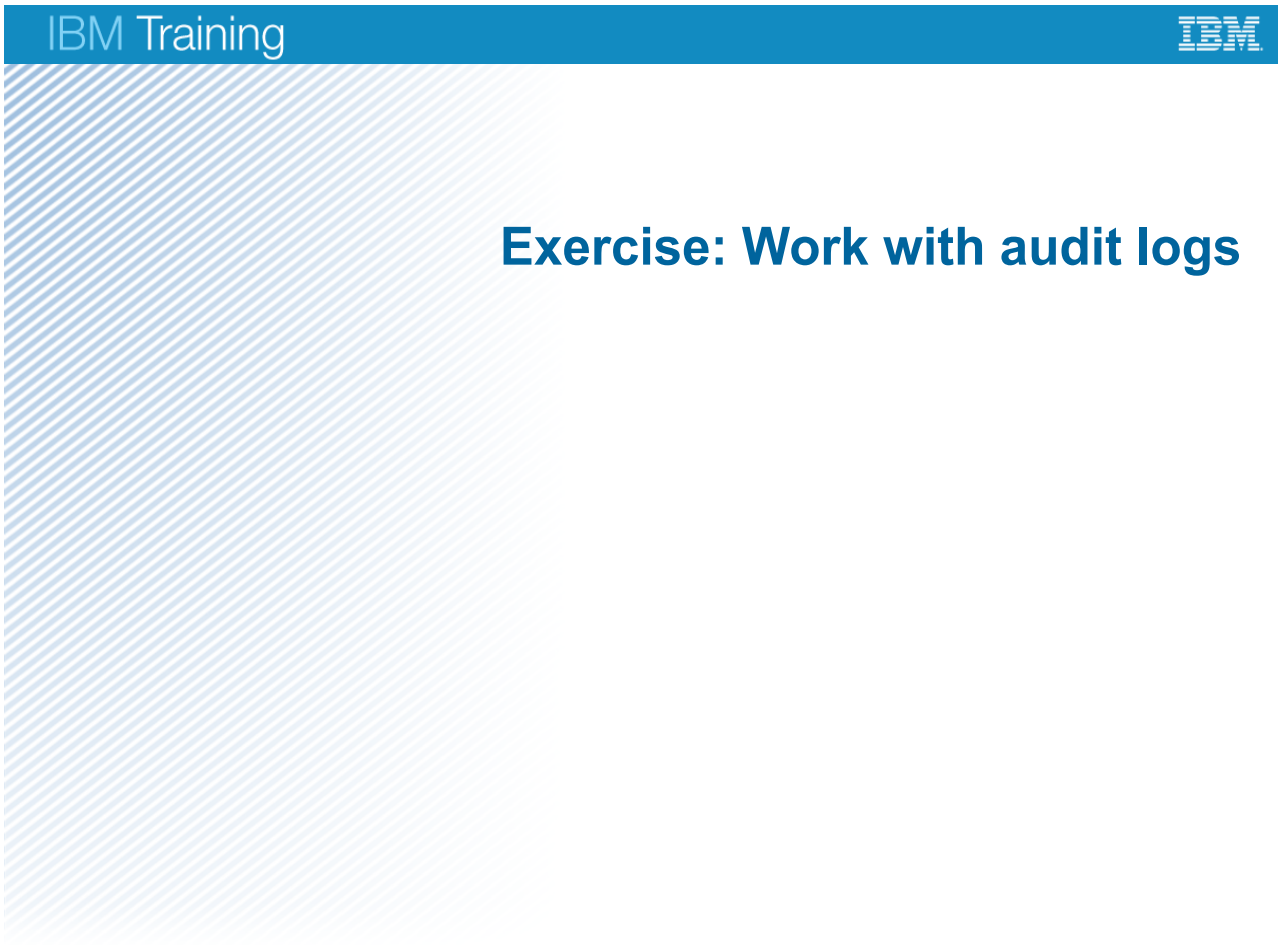


Figure 2-14. Exercise: Work with audit logs

IBM Training

Exercise introduction

- Create audit definitions
- Prune audit entries

Figure 2-15. Exercise introduction

IBM Training