

## Course Guide

# **IBM FileNet P8 Platform Essentials (V5.5.x)**

Course Code: F2800G ERC 1.0

Revision Date: April 2019



# April 2019

## NOTICES

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

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*

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:  
**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 states 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 supply 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 the names and addresses used by an actual business enterprise 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](http://www.ibm.com/legal/copytrade.shtml).

Adobe, and the Adobe logo, are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

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

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

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Notepad++ is a registered trademark.

**© Copyright International Business Machines Corporation 2019.**

**This document may not be reproduced in whole or in part without the prior written permission of IBM.**

US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

## ACCESSIBILITY

Accessibility features assist users who have a disability, such as restricted mobility or limited vision, to use information technology content successfully. Many IBM products include accessibility features for navigating the user interface, and for authoring reports so that they're accessible for yourself or others. Please consult the product documentation for an overview of accessible product features. Online product documentation can be accessed at the IBM Knowledge Center (<http://www.ibm.com/support/knowledgecenter/>).

---

# Course information

---

## Course overview

This course introduces you to the key concepts of IBM FileNet P8 Platform such as architecture, P8 domain structures, organizing the content across the enterprise, and security. Includes information to manage logging, auditing, and storage areas.

## Intended audience

This course is for administrators and users who are responsible for administrating and configuring IBM FileNet P8 Platform.

## Course prerequisites

Participants should have:

- Familiarity with enterprise content management concepts.

## Course outline

- Introduction to IBM FileNet P8 Platform
- Architecture and domain structures
- Configure logging
- Configure auditing
- Introduction to IBM FileNet P8 Platform security
- Manage storage areas
- Introduction to IBM FileNet P8 content services containers
- Organize content across the enterprise

---

## Additional training resources

---

Visit the [IBM Skills Gateway](http://www.ibm.com/training/) (<http://www.ibm.com/training/>) for details on:

- Instructor-led training in a classroom or online
- Self-paced training that fits your needs and schedule
- Comprehensive curricula, skills validation with the IBM Open Badge program, and learning journeys that help you identify the courses that are right for you
- For other resources that will enhance your success, bookmark the [IBM Analytics Skills Gateway](https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=C067650S63836C42) (<https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=C067650S63836C42>)
- IBM Knowledge Center: IBM FileNet P8 Platform V5.5.x documentation ([https://www.ibm.com/support/knowledgecenter/en/SSNW2F\\_5.5.0/com.ibm.p8toc.doc/welcome\\_p8.htm](https://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.5.0/com.ibm.p8toc.doc/welcome_p8.htm))

# Introduction to IBM FileNet P8 Platform

In this section, you will learn about the Enterprise Content Management (ECM) concepts, IBM FileNet P8 Platform features, integration options, and components.

## What is Enterprise Content Management?

An ECM system captures, stores, and manages business-related digital assets. ECM is also about:

- Supporting business applications
- Providing users with access to the right information in the context of their application
- Governing information and ensuring you meet business or industry regulations
- Enabling businesses to support a wide-range of document-centric use cases

Enterprise Content Management software provides the following set of core capabilities:

- User interfaces for working with the content
- Metadata management to enable searching and categorizing
- Security to ensure that only people with the correct access can view, edit, or delete documents
- API and programming model for the development of custom solutions
- Event management to automate actions based on events, such as document or metadata creation or updates
- Workflow management to automate document approval
- Records and retention management to govern information and ensure that you can meet business and industry regulations
- Logging and reporting to provide required audit trails
- Tools with which to administer the ECM environment

## IBM FileNet P8 Platform features

IBM FileNet Content Manager is an Enterprise Content Management offering. IBM FileNet Content Manager is also included in other product offerings and is referred to as IBM FileNet P8 Platform. Content Platform Engine (CPE) is the core component of the IBM FileNet P8 Platform. This course uses both IBM FileNet P8 Platform and IBM FileNet Content Manager interchangeably.

IBM FileNet P8 Platform provides the enterprise-level capabilities that are required for solving critical business requirements. The platform contains the following features:

- **Content Management**

Repository services for capturing, managing, and storing your business-related digital assets form the core of the platform. Multiple repositories, called object stores, can be created and managed within a single system to serve your business requirements.

Object stores can be configured to store content in a database, a file system, cloud storage, or a fixed content device, or a combination of these options.

- **Business user environment**

IBM Content Navigator (ICN) is a web client that provides users with a console for working with content from multiple content servers, including content that is stored on Content Platform Engine object stores. ICN can be used with IBM Content Manager (CM8), IBM Content Manager OnDemand (CMOD), any CMIS-compliant repository, and Box.

- **Application environment**

IBM FileNet P8 Platform provides a rich set of APIs that enable you to build custom applications, as well as tailor the out of the box interface ICN.

- **System management**

It provides a complete set of system administration tools.

- **Workflow management**

You can create, modify, and manage business processes, or workflows in the IBM FileNet P8 Platform.

## IBM FileNet P8 Platform integration options

The IBM FileNet P8 Platform provides the baseline components, for enterprise content management (ECM) solutions, that address ECM and business process management requirements.

IBM FileNet P8 Platform is included in other product offerings.

The following components can be added to a system to enable additional capabilities:

- **IBM Datacap**

A data capture product that scans, classifies, recognizes, validates, verifies, and exports data and document images quickly, accurately and cost effectively.

Datacap can be used to automate the import of captured data and scanned documents from Datacap into the IBM FileNet P8 Platform repositories for storage and use in other business applications.

Datacap Navigator is integrated with IBM Content Navigator to give business users a consistent user interface in which to work.

- **IBM Enterprise Records**

IBM Enterprise Records creates and maintains accurate, secure, and reliable records for both electronic and physical information. These records help to place the documents under corporate control and to meet government regulations.

The IBM Enterprise Records administrative interface is integrated with IBM Content Navigator, and while the processing of documents as records can be automated, business users can also declare documents as records using the IBM Content Navigator interface.

- **IBM Business Automation Workflow**

IBM Business Automation Workflow (BAW) provides a platform to create workflow applications to improve productivity.

BAW provides:

- Tools that simplify designing and deploying business solutions
- A ready-to-use interface that is flexible and customizable
- An active-content infrastructure that manages the persisted case object model
- Rich analytics that provide several methods to track and measure workflow business performance
- Ability to identify and incorporate both structured and unstructured content into workflows

- **IBM FileNet Content Federation Services**

IBM FileNet Content Federation Services federate documents from multiple repositories. The documents remain in the source repository; but can be viewed as if they were native FileNet P8 documents.

Examples of supported source repositories include IBM Content Manager and Image Services.

For a complete list of supported repositories, refer to the IBM FileNet P8 Platform Knowledge Center.

## **IBM FileNet P8 Platform components**

The IBM FileNet P8 Platform includes the following components.

- **Content Platform Engine (CPE)**

CPE is the core component of IBM FileNet P8 Platform that provides both content and process services.

- **IBM Content Navigator (ICN)**

ICN is the primary web interface for business users to work with content. Users can browse or search for content in the repositories, access their work items, and set up special team rooms to coordinate and collaborate on content-related activities. ICN is highly customizable. Both IBM Datacap and IBM Enterprise Records can be used through the ICN interface.

IBM Content Navigator also provides:

- A sync service to synchronize content on a business user's desktop and the CPE repository
- An edit service that enables business users to open content directly in the appropriate authoring application
- Role-based redaction to ensure sensitive information in a document is seen only by the appropriate users
- An integration with Microsoft Office that enables users to access, add, and update content in the CPE repository from the Microsoft Office suite of products
- An integration with Microsoft SharePoint that enables SharePoint users to access content in the CPE repository and to automatically save content added to SharePoint in the CPE repository

- **Content Search Services (CSS)**

CSS provides full content indexing so that text searches can be performed on both document content and metadata.

- **System Dashboard**

The system dashboard can be used to monitor the performance of the servers hosting IBM FileNet P8 Platform components. It also provides a tool for tracking license usage.

## **IBM FileNet P8 Platform solutions**

IBM FileNet P8 Platform provides tools for building solutions and applications that address business needs and challenges in various industries such as banking, academia, and government agencies.

Usually, a solution includes the following elements:

- **Metadata**

Metadata is information about objects, whether they are documents or other kinds of business objects. The metadata classifies the information so that users can find objects, and so that appropriate automated actions can be taken as metadata values are updated.

- **Content storage**

The content of documents needs to be stored securely. The rules around where content should be stored, whether the content should be encrypted, and how long the content should be kept for can be configured easily. Tools are also provided that enable you to move content to different types of storage as part of managing the lifecycle of the document.

- **Searches**

Searches can have a considerable effect on system performance. When designing a solution, a solution builder needs to predict the kinds of searches that are going to be used and create searches to efficiently use the system resources.

- **Security**

There are two primary aspects to securing your system: authentication and authorization.

Authentication determines who has access to the system, while authorization determines what the user can do once they have accessed the system.

- **User interface options**

IBM Content Navigator (ICN) can be used as the start point for your user experience. ICN can be customized and extended by using plug-ins. You can also embed ICN within your own completely custom user interfaces.

- **Automation**

Take advantage of the capabilities within the platform to automate repetitive processes that do not need user interaction. Automation can also be used to trigger processes based on adding or updating content or metadata.

- **Integration**

The IBM FileNet P8 environment can be integrated with other business processes and applications.

## Review Questions

**Question 1:** How would you define an IBM FileNet P8 Platform solution? (Select one)

- A. An object store that contains folders and files
- B. A set of workflows
- C. A solution that addresses a business need
- D. A set of stored searches

**Answer 1:** C

IBM FileNet P8 Platform provides tools for building a solution or application that addresses a business need.

**Question 2:** IBM FileNet P8 Platform is commonly used by which industry? (Select one)

- A. Banking
- B. Academia
- C. Government agencies
- D. All of the above

**Answer 2:** D

IBM FileNet P8 Platform is used by many industries.

**Question 3:** What are the capabilities of an Enterprise Content Management system? (Select all that apply)

- A. Providing users with access to the right information
- B. Metadata management to enable searching
- C. Logging and reporting to provide required audit trail
- D. Document viewing

**Answer 3:** A, B, C, and D

An Enterprise Content Management system provides user access & metadata management, logging, auditing, and document viewing.

**Question 4:** Which IBM FileNet P8 Platform component provides the default client interface for business users to work with content? (Select one)

- A. IBM Content Navigator
- B. Content Search Services
- C. Content Platform Engine
- D. System Dashboard

**Answer 4:** A

IBM Content Navigator is the primary web interface for business users to work with content and it can connect to the IBM FileNet Content Manager repositories.

**Question 5:** IBM FileNet P8 Platform integrates with which of the following systems? (Select one)

- A. IBM Datacap
- B. IBM Enterprise Records
- C. IBM Business Automation Workflow
- D. IBM FileNet Content Federation Services

**Answer 5:** A, B, C, and D

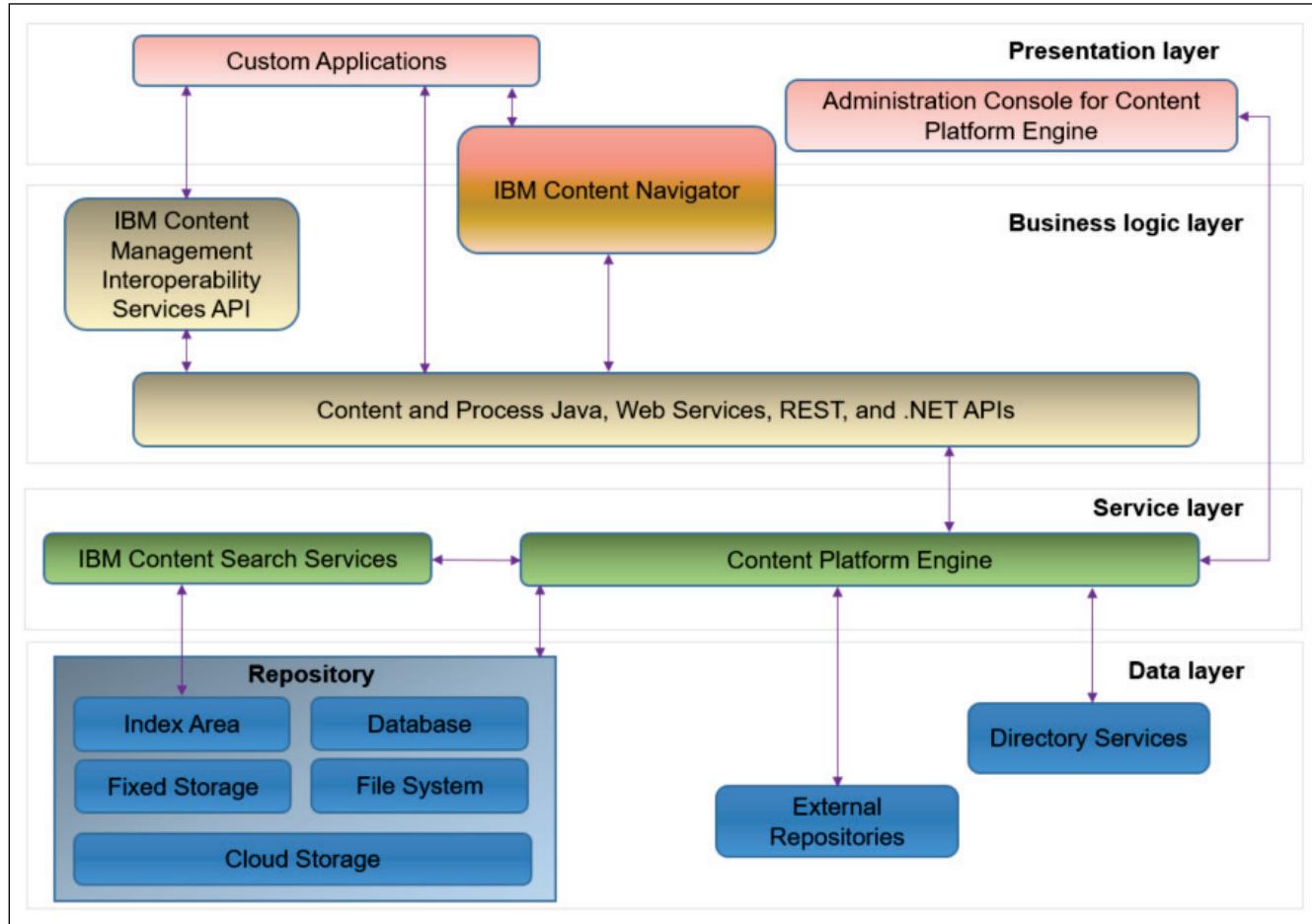
IBM FileNet P8 Platform integrates with IBM Datacap, IBM Enterprise Records, IBM Business Automation Workflow, and IBM FileNet Content Federation Services.

# Architecture and domain structures

In this section, you will learn about the IBM FileNet P8 Platform architecture, P8 domain, and objects present within the domain.

## IBM FileNet P8 Platform Architecture

The IBM FileNet P8 Platform includes back-end services, development tools, and applications that address enterprise content and process management requirements.



- The presentation layer and business logic layer, on the top, focus on the clients that connect to Content Platform Engine.  
IBM Content Navigator (ICN) is the primary web client to manage the content. You can customize and extend ICN and also create custom applications.  
Administration Console for Content Platform Engine is the web client to configure and administer Content Platform Engine.  
The business logic layer includes Content and Process Java, Web Services, REST, and .NET APIs.

- The services layer in the middle includes the core components that make up IBM FileNet P8 Platform.

The Content Platform Engine is the core engine providing both content and process services.

This layer also includes IBM Content Search Services.

- The data layer, which is the lowest layer, includes LDAP directory services, databases, and content storage.

## **Content Platform Engine architecture**

Content Platform Engine is an IBM FileNet P8 Platform component that manages enterprise-wide objects and documents by offering powerful and administration tools. Using these tools, an administrator can create and manage the classes, properties, storage, and metadata that form the foundation of an enterprise content management system.

The Content Platform Engine architecture includes the following aspects:

- **Object-oriented, extensible metadata model**

This model enables Content Platform Engine to provide complex and flexible data representation.

The model includes a rich event framework that provides the means to trigger actions in response to activities performed against Content Platform Engine objects.

- **Content Engine Application programming interfaces (APIs)**

The APIs provide an extensible platform for development.

A Java-based API provides a rich set of Java classes that maps to object store objects, such as Document, Folder, or Property Description.

A Web Service API enables users to author applications in a platform and language-independent manner that expose the object model in a few generic methods suitable for deployment in a web environment.

A Microsoft .NET framework-based API, functionally equivalent to the Java-based API, provides for development of applications that use the .NET framework.

- **Process Engine Application programming interfaces (APIs)**

A Java-based API provides a rich set of Java classes to customize the way that the application interfaces with user, data, and workflow services.

A Web Service API enables users to author applications in a platform and language-independent manner.

The REST Service enables lightweight client applications to access workflow system resources over HTTP and perform the fundamental workflow system operations.

- **Java EE-compliant application server**

Java Platform, Enterprise Edition (Java EE) offers reliability, scalability, and high availability features, and support for a wide range of operating system platforms, application servers, and database technologies.

The Content Platform Engine can be deployed to suit the demands of the enterprise. As the enterprise's needs change, you can reconfigure the system by replacing, adding, or removing servers or applications without bringing the system down. You can add members to web server clusters and Content Platform Engine server clusters at any time.

- **Directory server**

Each P8 domain is associated with one or more LDAP directory servers. The LDAP users and groups are used to define authentication and authorization rights.

- **Database server**

Each environment needs one or more database servers to host the tables that are used to define the P8 domain, the object stores, and workflow systems, as well as the configuration database used by IBM Content Navigator.

- **Content services**

These services are responsible for adding, retrieving, and deleting content and objects from an object store. In addition to servicing requests from enterprise content management (ECM) applications, the content services host various background tasks that maintain all the resources that are associated with each object store.

- **Process services**

These services manage all aspects of business processes (also called workflows).

## Content Platform Engine resources (P8 Domain)

The FileNet P8 domain represents a logical grouping of Content Platform Engine physical resources (such as object stores) and the Content Platform Engine servers that provide access to those resources.

Each resource and server belong to only one domain. A server can access any resource in the domain, but cannot access any resource that lies outside of the domain.

Each FileNet P8 Domain contains:

- A Global Configuration Database (GCD) that contains domain level configuration and properties.
- One or more object stores.

An object store is a repository for storing objects (such as documents, folders, and business objects) and the metadata that defines those objects.

Each object store contains:

- Business Objects  
Documents, Folders, and custom business objects used by applications
  - Metadata  
Customizable definitions of business object classes and their properties
  - Full Text Indexes  
Indexes that allow rapidly searching across document content
  - One or more storage areas.  
A storage area is a container for content storage.
- Optional workflow system - A workflow system contains the queues, rosters, and event logs that are necessary to create and process workflows.

## Content Platform Engine tools

The Content Platform Engine provides the following tools to help with administration and maintenance:

- **Administration Console for Content Platform Engine (ACCE)**

ACCE is a web tool that is used to administer and configure a FileNet P8 Domain, as well as to define and manage object stores and workflow systems.

- **FileNet Configuration Manager**

FileNet Configuration Manager is a graphical user interface to configure and deploy Content Platform Engine instances on an application server. It is generally used during initial installation or when applying software upgrades.

- **FileNet Deployment Manager (FDM)**

FDM is a desktop tool used to move data from one object store to another. FDM is often used to move data from one environment to another. For example, from development to Quality Assurance, and then to Production.

FDM can also be used to move workflow and Content Navigator-related information, as well as to reassign object stores to different P8 domains.

- **IBM Content Engine Bulk Import Tool**

Bulk Import Tool is a command-line tool that you can use to import large volumes of documents into a Content Platform Engine object store.

## Sites

A site is created to organize Content Platform Engine resources based on network topology. A site represents a geographical location where resources are connected through a local area network (LAN). Object stores, storage areas, content cache areas, index areas, and virtual servers are all associated with an individual site.

After you create a domain, the domain node contains one site that is named as Initial Site. This site is set as the default site for the domain. The default site contains the associated resources such as virtual servers, index areas, and object stores.

Resources that are added to the domain are associated with the default site, unless otherwise specified.

You can create a new site and set it as the default site. You can have multiple sites in a single FileNet P8 domain but each site name must be unique within the domain.

## FileNet P8 component relationships

The components in a FileNet P8 environment are interdependent. Although most components do not require other components to be running to start successfully, the absence of some components can affect processing.

Generally, start the components and related servers in the following order. Reverse the order to shut down.

- Directory services
- Database servers
- Content Platform Engine servers
  - Content Platform Engine runs as an application within a Java EE application server.
- IBM Content Search Services servers
- IBM Content Navigator
  - IBM Content Navigator runs as application within a Java EE application server
- Other FileNet P8 components

# Activity: Prepare your system - Start IBM FileNet P8 Platform.

The environment that is provided with this course requires that you start the IBM WebSphere Application Server that hosts the IBM FileNet P8 Platform components. The WebSphere Admin folder on the desktop includes the scripts that you need to run to start the components.

For this course, you will use a Windows Server 2012 R2 operating system, and the server name is VCLASSBASE.edu.ibm.com.

Complete the following tasks to ensure that your environment is ready and the services are running before working on other activities in the course.

## Log in to the system.

If the system is powered off, power the system on.

- Log in to the operating system by using the following credentials:
  - User: **p8admin**
  - Password: **FileNet1**

## Start the WebSphere Application Server deployment manager and node agent.

- Start the services by clicking the **Services**  shortcut on the taskbar.
- If the **IBM WebSphere Application Server V9.0 - Dmgr01** service does not have the Running status, then start it by right-clicking the service and selecting **Start**.
- If the **IBM WebSphere Application Server V9.0 - Node01** service does not have the Running status, then start it by repeating the previous step.

## Start the WebSphere Application Server application servers.

Two application servers are needed: The *server1* application server runs Content Platform Engine (CPE) and the *ICNserver* application server runs IBM Content Navigator (ICN). Because ICN must be deployed in its own application server instance (deployed into a single JVM). Running ICN and CPE in the same JVM is not supported. CPE uses the port number 9080 and ICN uses 9081.

In this task, you will start *server1* first and then *ICNserver*. *Server1* usually starts in a couple of minutes and *ICNserver* can take longer.

- On the **Windows desktop**, open the **WebSphere Admin** folder.
- Right-click **\_1 Start server1.bat**, and then select **Run as administrator**.

- Click **Yes** if prompted to allow the program to make changes.  
Wait for the command window to close.
- Right-click **\_2 Start ICNserver.bat**, and then select **Run as administrator**.
- Click **Yes** if prompted to allow the program to make changes.  
Wait for the command window to close.

## Troubleshooting.

- If any of the clients are not coming up, verify that the following two services are running:
    - IBM WebSphere Application Server V9.0 - Dmgr01
    - IBM WebSphere Application Server V9.0 - Node01
  - Stop and start the components  
In the WebSphere Admin folder, stop the two application servers and restart them.
    - Right-click **\_3 Stop ICNserver.bat** and then select **Run as administrator**.  
Wait for the command window to close.
    - Right-click **\_4 Stop server1.bat** and then select **Run as administrator**.  
Wait for the command window to close.
    - Right-click **\_1 Start server1.bat** and then select **Run as administrator**.  
Wait for the command window to close.
    - Right-click **\_2 Start ICNserver.bat** and then select **Run as administrator**.  
Wait for the command window to close.
- Do not start the next script until the command window closes for the previous script.

# Activity: Explore the core IBM FileNet P8 Platform applications

In this activity, you use the WebSphere Integrated Solutions console to explore the core IBM FileNet P8 Platform applications in WebSphere Application Server.

In this activity, you will accomplish the following:

- Check the FileNet P8 system components are running.
- Examine the IBM FileNet P8 Platform applications.
- Explore the interdependencies between IBM Content Navigator and Content Platform Engine.

## Check the IBM FileNet P8 components are running.

In this activity, you will verify that all the components that are used in this course for the IBM FileNet P8 system are running. The IBM FileNet P8 system includes Content Platform Engine with two primary services (content and process) and the IBM Content Navigator client application. Because these two applications rely on more software, testing the two applications also ensures that the underlying software is also functioning properly within your system.

- Ensure that the IBM FileNet P8 Platform components are started.  
If you have not started them, start the components by using the earlier activity:  
*Prepare your system - Start IBM FileNet P8 Platform*
- In the **Mozilla Firefox** browser, click the **Bookmarks** menu and then select **System Health > CE Ping**  
You can also enter the following URL for the ping page:  
<http://vclassbase:9080/FileNet/Engine>
- Verify that the **Content Engine Startup Context (Ping Page)** is displayed to indicate that Content Platform Engine content services are functioning properly.

 Content Engine Startup Context (Ping Page)	
Key	Value
Local Host	VCLASSBASE
Start Time	Mon Mar 11 16:33:30 EDT 2019
Product Name	P8 Content Platform Engine - 5.5.2.0

This page contains information about the FileNet P8 system including the product name and version, and log files location.

- In the **Mozilla Firefox** browser, open a new tab, click the **Bookmarks** menu and then select **System Health > PE Ping**  
You can also enter the following URL for the ping page:  
<http://vclassbase:9080/peengine/IOR/ping>
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **OK**.
- Verify that the **Process Engine Server Information (Ping Page)** is displayed to indicate that Content Platform Engine process services are functioning properly.  
This page contains information about the FileNet P8 system including the product name and version, and log files location.
- In the **Mozilla Firefox** browser, open a new tab, click the **Bookmarks** menu and then select **System Health > FileNet P8 System Health**  
You can also enter the following URL: <http://vclassbase:9080/P8CE/Health>
- Verify that the **IBM FileNet Content Manager - CE System Health** page is displayed.  
This page includes information about P8 Domain, Site, and other resources. Each item has a link to see more details. The green circle shows these resources are available.
- Close the browser, reopen, click the **Bookmarks** menu and then select **System Health > ICN Ping**  
You can also enter the following URL for the ping page:  
<http://vclassbase:9081/navigator/ping.jsp>
- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **OK**.
- Verify that the **IBM Content Navigator Ping Page** is displayed to indicate that IBM Content Navigator application is functioning properly.  
This page contains information about Content Navigator including the product name and version.  
The new protected ping page (ping.jsp) can only be accessed by administrators and requires login.
- In the **Mozilla Firefox** browser, open a new tab, click the **Sample Desktop** bookmark.  
You can also enter the following URL: <http://vclassbase:9081/navigator/>
- If prompted to login, type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

- Verify that the Content Navigator Desktop (called **Sample Desktop**) opens with the **Browse** view (indicated on the upper left).
- In this view, you browse to folders, view documents, and manage the content. If you get the Browse page, it indicates that the following components are running and communicating within your student system:
  - A database system.
 Your student system uses the IBM DB2 database software. Every time a user logs in to the desktop, the desktop configuration is loaded from the DB2 database. This desktop is configured to browse the LoanProcess object store by default, which demonstrates that the database used by the Content Platform Engine is functional.
- An LDAP directory service to handle user authentication. Your system uses Active Directory.
- Logout of the ICN desktop and close the browser.

## **Examine the IBM FileNet P8 Platform applications.**

In this task, you will open the WebSphere Integrated Solutions Console and observe the IBM FileNet P8 Platform applications.

- In the **Mozilla Firefox** browser, click the **WAS** bookmark or enter the following URL: <https://vclassbase:9043/ibm/console/logon.jsp>
- Type the following values and then click **Log in**:
  - User ID: **wasadmin**
  - Password: **FileNet1**
- The console opens.
- On the left pane, expand the **Applications > Application Types** node and then click **WebSphere enterprise applications**.
- On the right pane, verify that the **Application Status** column shows a green arrow to indicate that the following two applications are running.
  - FileNetEngine (Content Platform Engine)
  - navigator (IBM Content Navigator)

Select	Name	Application Status
You can administer the following resources:		
<input type="checkbox"/>	<a href="#">DefaultApplication</a>	
<input type="checkbox"/>	<a href="#">FileNetEngine</a>	
<input type="checkbox"/>	<a href="#">navigator</a>	

These two key applications are required for IBM FileNet P8 Platform. You will not be using the DefaultApplication and starting it is not required.

- Click **FileNetEngine** to open it.  
If it does not open immediately, right-click FileNetEngine and select Open Link in New Tab.
- Under the **Modules** section, click **Manage Modules**.  
A list of modules are shown that make up the *FileNetEngine* application.  
The *acce* application is the Administration Console for Content Platform Engine.
- If you opened the **FileNetEngine** application in a separate tab, close the tab.

## **Explore the interdependencies between IBM Content Navigator and Content Platform Engine.**

In this task, you will stop the FileNetEngine application (Content Platform Engine) and open an IBM Content Navigator (ICN) desktop. ICN is the primary web client for business users to work with content and workflow tasks. ICN connects to the IBM FileNet Content Manager repositories.

- On the left pane, click the **Applications > Application Types > WebSphere enterprise applications** node.
- On the right pane, select the box next to **FileNetEngine** and click **Stop**.
- Wait until a **red X** is shown to the right of **FileNetEngine** on the **Application Status** column.
- Log out of the **WebSphere Integrated Solutions Console** and close the browser.
- 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 Sample desktop of IBM Content Navigator (ICN) opens.

You get an error with the message that the repository is not available. ICN attempts to load the desktop. It cannot load the desktop because FileNetEngine is not running and ICN cannot connect to the repository.

- Close the browser and reopen to log in to the **WebSphere Integrated Solutions Console (WAS)** again with the same user ID and password as above (**wasadmin/FileNet1**).

- On the left pane, expand the **Applications > Application Types** node and then click **WebSphere enterprise applications**.
- On the right pane, select the box next to **FileNetEngine** and click **Start**.
- Wait until a green check mark is shown to the right of FileNetEngine on the **Application Status** column.
- Log out of the **WebSphere Integrated Solutions Console** and close the browser.
- 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**.
- This time, the desktop opens without any errors and the **LoanProcess** Repository is listed in the **Browse** mode.

The screenshot shows the 'Sample Desktop' interface. On the left, there's a sidebar with a 'Browse' dropdown menu. Under 'LoanProcess', several sub-folders are listed: CodeModules, Loan Entry Template, Loan Types, Loans, and Real Estate. On the right, there's a main content area with three buttons at the top: Refresh, Add Document, and New Folder. Below these buttons is a section titled 'LoanProcess' with a 'Name' field. Underneath the 'Name' field, there are two entries: CodeModules and Loan Entry Templates.

- Click the **head and shoulder icon** on the banner, select **Log Out** to log out of **IBM Content Navigator** and then close the browser.

The screenshot shows the user profile banner with the name 'p8admin'. Below the banner, there are two options: 'Change Language and Locale Settings' and 'Log Out'.

# Activity: Locate P8 domain structures

In this activity, you will use Administration Console for Content Platform Engine to locate P8 domain structures.

In this activity, you will accomplish the following:

- Log in to Administration Console for Content Platform Engine (ACCE)
- Explore the domain level properties.
- Locate the Global Configuration folder structure.
- Locate the Object Stores folder structure.
- Find specific objects in a FileNet P8 Domain (Optional)

## Log in to Administration Console for Content Platform Engine (ACCE).

Throughout this course, Administration Console for Content Platform Engine (ACCE) is also referred to as ACCE or administration console.

- 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**.

This account has administrative rights on the FileNet P8 Domain.

Administration Console for Content Platform Engine (ACCE) opens.

On the right pane, there are a series of subtabs, with the General subtab selected.

## Explore the domain level properties.

In this task, you use ACCE to explore the domain level properties.

- On the right pane of ACCE, under the **General** subtab, notice the general properties that are listed.

The screenshot shows the IBM Administative Console for Content Platform Engine interface. On the left, there's a navigation tree with 'EDU\_P8' selected. The main pane shows the 'General' subtab of the 'EDU\_P8' domain configuration. The properties listed are:

- Name: EDU\_P8
- Id: {1B6358E8-3B59-480C-BC26-F9F7AA7AA}
- Domain type: Standalone

Buttons for 'Save' and 'Refresh' are visible at the top of the configuration pane.

Name, ID, and Domain type of the EDU\_P8 domain are shown. The domain for the student system is named EDU\_P8.

- Select the **Properties** subtab, click the **Property Name** cell to sort the list alphabetically and then review the properties that are listed.  
The Default Site property has Initial Site as the value.
- Scroll down to the **Subsystem Configurations** property, and then click the blue down arrow to the right of that property.

The screenshot shows the 'Properties' subtab for the EDU\_P8 domain. The 'Subsystem Configurations' property is selected, and its dropdown menu is open, displaying a list of subsystem configurations:

- 10) Text Search Configuration
- 11) Auditing Configuration
- 12) Thread Pool Configuration
- 13) Sweep Configuration

Observe that a list of different subsystem configurations displays. When you select a subsystem, it opens as a separate tab and the configuration can be updated.

- If you opened any subsystem tabs, you can close them.

- In the **EDU\_P8** main tab, click the **Security** subtab.  
In the security tab is where you grant access to the entire domain.

The screenshot shows the 'EDU\_P8' main tab with the 'Security' subtab selected. At the top, there are 'Save' and 'Refresh' buttons. Below them are tabs: General, Properties, Security (which is underlined), Directory Configuration, and Server Cache Subsyst. A note says 'customize a predefined permission as needed. Learn more...'. Under 'Access Permissions', there are buttons for 'Add Permissions...', 'Edit...', and 'Remove'. It shows 2 total entries:

<input type="checkbox"/>		Name	Source	Permission Type	Permission Group	Apply To
<input type="checkbox"/>		#AUTHENTICATED-USERS	Direct	Allow	Custom	This object and children
<input type="checkbox"/>		p8admin	Direct	Allow	Full Control	This object and

In this domain (EDU\_P8), the p8admin user has full control on the domain and all its children. The default #AUTHENTICATED-USERS group has custom permission access for the domain and its immediate children.

- Click the **Directory Configuration** subtab.  
Notice that EDU\_AD is defined for the P8 domain. A FileNet P8 Domain can be configured to use multiple directory configurations.
- Click the **EDU\_AD** link in the **Name** column.  
The EDU\_AD tab opens.
- In the **EDU\_AD** tab, examine the properties that are displayed, such as **Directory Server Type** and then close the tab.  
The directory configuration is generally configured with the FileNet Configuration Manager. ACCE can be used to update the settings or just to view them.
- Click the **Server Cache Subsystem** tab and then review the properties.  
You optimize the efficiency of the server cache for improving the system performance.
- Optionally, click each of the subsequent tabs to review the properties.  
Click the forward arrow to access more tabs.

- Click the down arrow at the top right and select **SMTP Subsystem** tab.  
Click the SMTP Subsystem tab, if the content is not displayed. In this tab, you can configure an SMTP mail server to set up email notifications. Mail services are not enabled on this domain for the student system.
- Click the **Workflow Subsystem** tab.  
In this tab, you enable Workflow and Case Analyzer and adjust tuning parameters.

## Explore the Global Configuration folder structure.

In this task, you explore the properties and objects that are located in the Global Configuration folder.

- On the left pane of the **EDU\_P8** tab, expand **Global Configuration > Administration > Sites > Initial Site (Default)**.  
This is the site that is created when you create a P8 domain. This site is set as the default site for the domain.  
You can create a new site and set it as the default site. You can have multiple sites in a single FileNet P8 domain.
- Observe that there are several nodes listed under the **Initial Site (Default)** node.  
The default site contains the associated resources such as virtual servers, index areas, and object stores.  
Any resources that are added to the domain are associated with the default site, unless otherwise specified.
- Select the **Initial Site (Default)** node and then on the right pane, explore the subtabs that are available for the **Initial Site (Default)** tab.
- On the left pane of the **EDU\_P8** tab, expand **Global Configuration > Administration > Database Connections** and select **FNOSDS**.  
The FNOSDS tab opens.
- On the right pane, click the **Properties** subtab of the **FNOSDS** tab and then examine the data source properties and the database type.
- Click the **Object Stores** tab.  
The object stores that use this database connection are listed.
- Click the **Sales** object store.  
A new tab opens for the Sales object store. You will explore the object store in the next task.

- Close the **Sales** tab by clicking the **X** on the tab, and then close the **FNOSDS** tab by clicking **Close**.
- From the **EDU\_P8** tab, on the left pane, collapse the **Administration** folder, expand the **Global Configuration > Data Design** and click the **Add-ons** folder.

On the right pane, object store add-ons are listed. When you create a new object store, you choose from this list of Add-ons. Each Add-on provides predefined metadata that extends the basic operation of IBM FileNet P8 Platform. For example, Thumbnail Extensions are required if your object store needs to support thumbnails.

- Close the **Add-ons** tab.
- On the left pane, notice the **Data Design > Marking Sets** folder.

Marking Sets are primarily used for records management. No Marking Sets are defined in this domain.

## **Explore the Object Stores folder structure.**

In this task, you explore the objects and properties that are located in the Object stores folder.

- On the left pane of the **EDU\_P8** tab, collapse the **Global Configuration** folder and expand the **Object Stores** folder.

A list of object stores that exist in the **EDU\_P8** domain are shown.

- Click the **Sales** object store.

The Sales tab opens.

- On the left pane, expand the **Administrative > Workflow system** and observe that there are nodes for **Connection Points** and **Isolated Regions**.

To learn more about how to configure a workflow system, refer to the *F231G: IBM Case Foundation 5.2.1 - Configure the workflow system* course.

- On the left pane, collapse **Administrative**, expand the **Browse** folder and then verify that there are two main nodes: **Root Folder** and **Unfiled Documents**.
- Expand **Root Folder** to view all the top-level folders that exist in this object store and then click **Orders** folder to open it.
- From the **Orders** tab > **Contents** subtab on the right, notice a list of documents that are filed in this folder.
- Open a document by clicking the link in the **Containment Name** column.

The document opens in a separate tab with the document name. You can access the properties and settings of the document.

- On the left pane, collapse the **Root Folder** and then click the **Unfiled Documents** node.  
If any documents are added to this object store but not filed in a folder, they will be listed under this node.
- Close all open tabs on the right pane.
- On the left pane, collapse the **Browse** folder and expand the **Data Design** node.  
Under this node, are objects that are used to define metadata such as property templates, classes, and choice lists.
- Expand **Classes > Document** to view all the document subclasses.
- Expand the **Order** subclass and notice that there are sub-classes that are called **ProductOrder** and **ServiceOrder**.
- Click **Order** to open the Order tab on the right pane.
- From the **Order** tab, click the **Property Definitions** subtab to access the property definitions that are defined for the **Order** class.  
You will explore these property definitions in the following steps.
- Collapse **Classes**, expand the **Property Templates** folder and then scroll down to **customer\_name**.  
You can type the name in the filter field to find it quickly.  
This is one of the property definitions that you saw for the Order class in the prior step.
- Click **customer\_name** to open it and explore the subtabs under the **customer\_name** tab.
- Close all open tabs on the right.

## **Find specific objects in a FileNet P8 Domain (Optional).**

In this task, you will use Administration Console for Content Platform Engine (ACCE) to find specific objects in the FileNet P8 Domain. For more details, refer to the previous tasks.

- In **ACCE**, open the **Sales** object store, if it is not already opened.
- How many property definitions are defined for the **PriceQuote** document class?
- What are the names of the two workflows in the **Workflows** folder?
- Verify your answers:

The PriceQuote class has three property definitions: customer\_name, Description, and price.

The screenshot shows the 'Data Design' section on the left with a tree view of various templates and classes. The 'PriceQuote' class is selected. On the right, the 'Class Definition: PriceQuote' panel is open, showing the 'Property Definitions' tab. This tab includes buttons for 'Add', 'Remove', and 'Propagate'. There are also checkboxes for 'Display inherited properties' and 'Display system properties'. A table lists the properties with their data types and names:

Property	Data Type	Is Name
customer_name	String	
Description	String	
price	Float	

The names of the two workflows are: Sample Workflow, and Test Subscription Workflow.

The screenshot shows the 'Browse' section on the left with a tree view of various folders. The 'Workflows' folder is selected. On the right, the 'Folder: Workflows' panel is open, showing the 'Contents' tab. It includes buttons for 'Save', 'Refresh', 'Actions', and 'Close'. A table lists the workflows:

Containment Name	Document Name
<input type="checkbox"/> Sample Workflow	Sample Workflow
<input type="checkbox"/> Test Subscription Workflow	Test Subscription Workflow

- Click the Head and Shoulder icon on the banner and select **Log out** to log out of the Administration Console for Content Platform Engine.
- Close the browser.

# Activity: Use IBM Content Navigator

IBM Content Navigator (ICN) is the primary web client for business users to work with content and workflow tasks. ICN client can be configured to connect to the IBM FileNet Content Manager repositories. Users can browse or search for content in the repositories, access their work items, and do many more content-related activities. In this activity, you will use the IBM Content Navigator Sample Desktop that is configured for the student system and explore a very simplified view of the application.

In this activity, you will accomplish the following:

- Log in to IBM Content Navigator desktop.
- Explore the repositories, folders, and documents.
- Add a folder and a document.

## Log in to IBM Content Navigator desktop.

- 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.

- Notice that the default page opened is **Browse**, as indicated in the upper left and the default repository opened is **LoanProcess**.
- From the upper left, click the down arrow next to **Browse** and notice that the following features are listed: **Home**, **Browse**, **Search**, **Entry Template Manager**, **Work**, and **Administration**

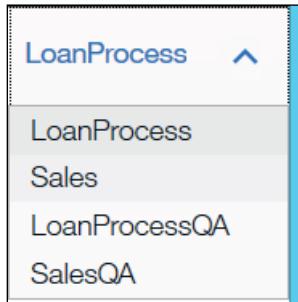
Each feature in an ICN desktop open as a page that contains a set of functionality and actions. For example, on the **Browse** feature page, you can browse the folders and documents, and you can perform actions associated with documents and folders.

Leave the **Browse** page in Content Navigator open for the next task.

## Explore the repositories, folders, and documents.

P8admin user has access to multiple repositories. The LoanProcess repository opens by default. In this task, you will access other repositories and check the folders, documents, and the details for the documents.

- To open a different repository, click the down arrow next to **LoanProcess** on the upper right and select any of the available repositories from the list to access the content of that repository.



All the repositories that are configured for this desktop are shown in the list.

- Select the **Sales** repository.

This the repository that you explored in the Administration Console for Content Platform Engine (ACCE) tool in a previous activity.

On the left pane, under the Sales repository, a list of top-level folders, to which the user has access is shown.

- Click **Workflows** and then observe that there are two documents filed in this folder.

This the folder that you explored in the ACCE tool in a previous activity.

The documents in the selected folder are shown on the right pane. If there are any subfolders, they will also displayed.

- On the left pane, click the **Orders** folder, select a document (for example, **PO 3411.tif**) by clicking the document title.

Single-click the document to view the properties on the lower right pane. A double-click opens the document in the Viewer (for the document mime types that are configured for this desktop).

Content Navigator provides a thumbnail view of the document on the upper right pane.

- Review the information that is shown in the **Properties** section on the right pane.

The document class is ProductOrder.

It includes many custom properties that are specific to product order documents, such as customer\_id, customer\_name, po\_number, and product\_ids.

- Double-click the **PO 3411.tif** document title.

The document opens in the Viewer.

Notice that there are controls to magnify, rotate, and invert at the top. There are more controls on the left to add annotations to the image.

- Close the Viewer and leave Content Navigator open for the next task.

## Add a folder and a document.

In this task, you create a folder and a document in an object store using the IBM Content Navigator (ICN) desktop.

- From the Browse page, click the down arrow next to **Sales** on the upper right and select the **LoanProcess** repository.

You can also add folders and documents in any of the other repositories.

- Click **New Folder** from the toolbar.
- In the **New Folder** page, type **SampleFolder** for the **Folder Name** field.

Leave the default values for all the other fields. Observe the Folder class and security that is assigned to this folder.

- Click **Add**.
- Back on the **Browse** page, double-click **SampleFolder** to open the new folder, and then click **Add Document** from the toolbar.
- In the **Add Document** page, type **SampleDoc** for the **Document Title** field.
- For the **What do you want to save?** field, click **Browse**.
- On the **File Upload** page, select any file from the **C:\Training\F2800G\SampleDocs** folder and then click **Open**.

Back on the Add Document page, leave the default for all the other fields. Observe the Document class and security that is assigned to this document.

- Click **Add**, back on the **Browse** page, verify that the new document is listed.
- Click the **head and shoulder icon** in the banner, select **Log Out** to log out of IBM Content Navigator and then close the browser.

Throughout this course, you will be using IBM Content Navigator desktop to add content and modify properties.

IBM Content Navigator (ICN) courses provide details on ICN administration and on using ICN to manage the IBM FileNet Content Manager repository content.

# Configure logging

The Content Platform Engine, which is the main component of IBM FileNet P8 Platform, provides logging capabilities for tracking functional issues and troubleshooting. In this section, you will learn how to monitor the system logs and configure trace logging for troubleshooting.

## Content Platform Engine System Logs

Content Platform Engine produces several log files during normal operation. Following are the primary troubleshooting tools for the administrator:

- p8\_server\_error.log
- pesvr\_system.log
- p8\_server\_trace.log

You must become familiar with normal log entries and monitor these log files to do the following tasks:

- Observe changes in behavior that might indicate a problem.
- Ensure that log files are managed.  
Keep the files to a reasonable size, roll over to new files and deleting old ones (when you no longer need them).

If the organization uses workflows, the following tools are available to monitor the workflow system:

- vwtool
- vwmsg
- pelog
- peverify

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

## Default location of logs

By default the Content Platform Engine logs are stored in the following locations:

- 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

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 Content Platform Engine log files. They are located in the server\_instance\_name under the current working directory of the deployed application.

## Web application server logs

When troubleshooting IBM FileNet P8 Platform, you will need to collect the logs from the Content Platform Engine as well as the logs from the web application server. IBM Content Navigator, which provides the user interface for IBM FileNet P8 Platform, logs errors and entries in the web application server's logs.

Each web application server generates its own logs.

The following list contains supported web application servers, default path for the log files, and the name of the log files in the order of importance.

## WebSphere

- Location: install\_root/profiles/profile\_name/logs/server\_name
- Examples of log locations:
  - WebSphere (Windows): C:\Program Files\IBM\WebSphere\AppServer\profiles\ AppSrv01\logs\server1
  - WebSphere (Linux):
    - /opt/ibm/WebSphere/AppServer/profiles/AppSrv01/logs/server1
- Log files:
  - SystemOut.log
  - SystemErr.log
  - startServer.log
  - stopServer.log

## WebLogic

- Location:
  - oracle\_home/admin/domain\_name/aserver/servers/AdminServer/logs
- Examples of log location:
  - C:\bea\user\_projects\domains\base\_domain\servers\AdminServer\logs
- Log files:
  - AdminServer.log
  - access.log
  - Base\_domain.log

Note that the MustGather technote

(<https://www.ibm.com/support/docview.wss?uid=swg21308231>) provides suggestions 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 requested web application server logs.

## Trace logs

Trace logs are used to troubleshoot specific issues. Trace logging is typically implemented to collect and record information about application failures in test or production environments. If you open a support call, the representative might request that you enable trace logging and reproduce the issue. In that situation, the representative recommends which subsystem flags to enable and what level of detail to collect.

You can configure trace logging at the domain level or the site level. The site-level configuration takes precedence over any domain level settings. Site level configuration is used in organizations that have servers and users in more than one geographical location. For details about Domain and Site, see the *Architecture and domain structures* section in this course.

Use Administration Console for Content Platform Engine to configure trace logging, including configuring the level of detail for server trace logging and setting the location of the trace log file. The configuration is done on the Trace Subsystem tab of the domain properties. The default file name is p8\_server\_trace.log.

Disable trace logging when you no longer need it. Trace logs can grow quickly and impact system performance and disk space.

## Guidelines for monitoring log files

- Establish a baseline and know what to expect.

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.

- Monitor logs regularly.

Watch for new error messages and any change in error log size.

Example: If the size of a log file is normally 64 KB, and on one day it shows 100 KB

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.

Tools such as ECM System Monitor can be used to generate alerts when unusual activity occurs.

- Increase monitoring after any system changes.

Example: Patches applied

- Keep records of normal logs for comparison purposes.

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 there no major changes to the log behavior after a year or so, you might decide to keep a week of logs for the whole year.

# Activity: View and archive system logs

In this activity, you locate the Content Platform Engine logs and the WebSphere Application Server logs. You shut down the web application server to archive the logs. You restart the web application server and examine the new logs created.

In this activity, you will accomplish the following:

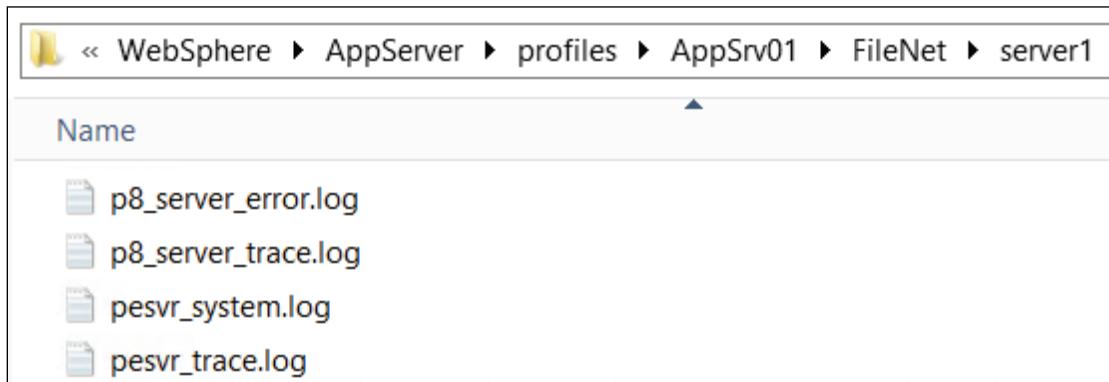
- Locate the Content Platform Engine logs.
- Locate the WebSphere Application Server logs.
- Disable WebSphere Application Server trace logging.
- Archive old log files.
- Examine the new log files.

## Locate the Content Platform Engine logs.

- 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, open the **Content Engine Startup Context (Ping Page)**.
  - Use the bookmark in the **Bookmarks** menu > **System Health > CE Ping** or enter the following URL: <http://vclassbase:9080/FileNet/Engine>
- In the Ping page, scroll down and note down the value for the **Log File Location** key.

Log File Location	C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1
-------------------	--

- In a **Windows Explorer** window, navigate to that folder path: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1** and notice that there are four log files:
  - p8\_server\_error.log**
  - p8\_server\_trace.log**
  - pesvr\_system.log**
  - pesvr\_trace.log**



- Minimize the Windows Explorer window.

## Locate the WebSphere Application Server logs.

- In a **Windows Explorer** window, navigate to the **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder and notice that there many log files:
  - SystemOut.log**
  - SystemErr.log**

These two files are most often referenced.

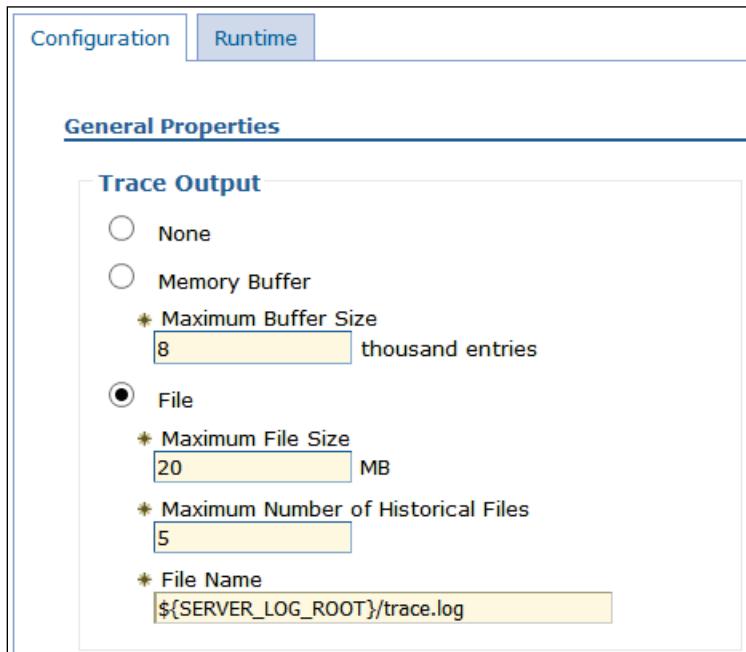
## Disable WebSphere Application Server trace logging.

In this task, you disable trace output for the WebSphere Application Server. The student system is configured with the trace output enabled.

- In the **Mozilla Firefox** browser, click the **WAS** bookmark or enter the following URL: <https://localhost:9043/ibm/console/>
- Type the following values for user ID and password and click **Log in**.
  - User name: **wasadmin**
  - Password: **FileNet1**

- On the left navigation pane, expand **Troubleshooting** and then click **Logs and trace**.
- On the right pane, click the **server1** link in the **Server** column.
- Click **Diagnostic Trace** under **General Properties** section.

On the Configuration tab of the Diagnostic trace service page, notice that you can control the Maximum File Size, Maximum Number of Historical Files to keep before overwriting, File Name, and location of the trace log.



- On the **Configuration** tab, select **None** to disable the trace output and then click **OK** at the end of the page.
- In the **Messages** section, click **Save** to save the configuration.
- Log out of the **WebSphere Integrated Solutions Console** and close the browser.

The change does not take effect until WebSphere Application Server is restarted. You restart WebSphere Application Server in the next task.

## Archive old log files.

In this task, you stop the server and archive the WebSphere Application Server and Content Platform Engine logs.

- Open the **WebSphere Admin** folder on the desktop, right-click the **\_4 Stop server1.bat** file, and then select **Run as administrator** from the list.

- Click **Yes** when you are prompted with the **User Account Control** dialog box to allow the program to run.  
Wait for the operation to complete (the command window closes).
- Minimize the **WebSphere Admin** folder window.
- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Create a folder that is called **Archived\_CPE\_Logs** (this name is not critical) in this directory to store the archived Content Platform Engine logs and move all the four **\*.log** files to the new folder.
- Select the **Do this for all current items** option and then click **Continue** when you are prompted with the **File Access Denied** dialog box to move the files.
- Minimize the **Windows Explorer** window.  
Maximize the Windows Explorer window where you viewed the WebSphere Application Server log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder.
- Create a folder that is called **Archived\_WAS\_Logs** (this name is not critical) in this directory to store the archived WebSphere Application Server logs and move the **SystemOut.log**, **startServer.log**, and **SystemErr.log** files to the new folder.
- Select the **Do this for all current items** option and then click **Continue** when you are prompted with the **File Access Denied** dialog box to move the files.
- Minimize the **Windows Explorer** window.
- Open the **WebSphere Admin** folder on the desktop, right-click the **\_1 Start server1.bat** file, and then select **Run as administrator** from the list.
- Click **Yes** when you are prompted with the **User Account Control** dialog box to allow the program to run.  
Wait for the operation to complete (the command window disappears).
- Minimize the **WebSphere Admin** folder window.

## Examine the new log files

If no log files exist, the Content Platform Engine and the WebSphere Application Server create new logs at startup.

- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.

- Notice the four log files that are created with the current date and time.
- Right-click the **p8\_server\_error.log** file, select **Edit with Notepad++**, and examine the log entries that are created during startup.  
Cancel any prompts to update to the Notepad++ version.
- Maximize the **Windows Explorer** window where you viewed the WebSphere Application Server log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1** folder.
- Notice that the log files (that were archived) are created with the current date and time.
- Open **SystemOut.log** with **Notepad++** and examine the log entries that are created during startup.
- Scroll down the log file to the text **P8 Content Platform Engine Startup: 5.5.2.0** as shown in the following screen capture.

You can also search for the text: P8 Content Platform Engine Startup

```
o [Perf Log] No interval found. Auditor disabled.
o =====
o P8 Content Platform Engine Startup: 5.5.2.0 dap552.1260 Copyright IBM Corp. 2003, 2018 All rights reserved
o =====
```

This text indicates the Content Platform Engine startup.

Errors are logged as Java stack traces. There are a couple of errors such as the following one:

"ResourceMgrIm E WSR0017E: Error encountered binding the J2EE resource, CNMailSession, as mail/CNMailSession"

These errors can be ignored because the components are not being used. However, it is important that you monitor your organization's log files regularly and learn to recognize errors that might indicate a serious issue.

- Close the **SystemOut.log** file, open **SystemErr.log** with **Notepad++** and then examine the log entries that are created during startup.  
Notice that this log file does not have as many entries as the SystemOut.log.
- Open **startServer.log** with **Notepad++** and examine the log entries.  
Notice the last entry that includes the text: *Server server 1 open for e-business*.  
This log entry indicates that the WebSphere Application Server started successfully.
- When you are done examining the log files, click **File > Close All** and then exit **Notepad++**.
- Minimize the Windows Explorer windows.

# Activity: Configure trace logging

Trace logging options can be set on the domain or at the site level. If the settings are configured on the site, they override the settings on the domain.

In this activity, you configure trace logging on the Content Platform Engine at the domain level and site level. You log in to an IBM Content Navigator desktop to create security entries in the trace log and then examine the entries in the trace log.

In this activity, you will accomplish the following:

- View and configure initial trace configuration.
- Configure trace logging on the domain.
- Configure trace logging at the site level.
- Inspect the trace log files.
- Create trace log entries.
- Disable trace logging.

## Configure trace logging on the domain.

In this task, you will first view the trace log file before enabling the trace logging. You will configure trace logging at the domain level, and then configure the site to inherit these settings.

- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Right-click the **p8\_server\_trace.log** file, select **Edit with Notepad++**, and examine the initial log entries.

Since the trace logging is not yet enabled, there is not a lot of information.

- Close the **p8\_server\_trace.log** file.
- In the **Mozilla Firefox** browser, click the **ACCE** bookmark or enter 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 right pane, from the **EDU\_P8** tab, select the **Trace Subsystem** subtab. Use the forward arrow on the right to scroll to find the tab. You can also use the down arrow to select the subtab from the list.  
If the contents of the tab is displayed, click the tab and the content will be refreshed.
- On the **Trace Subsystem** subtab, select the **Enable trace logging** option.
- For the **Log file location** field, select the **Use default** option.  
The trace log is saved in the same folder as the Content Platform Engine log files.

Trace logging generates detailed diagnostic information about server and client activity, and select the subsystems to be logged.

Enable trace logging [\(i\)](#)

Log file location :  Use default [\(i\)](#)  Other location: [\(i\)](#)

- Scroll down to the **Subsystems** section and select the **Detail** level trace options for the following subsystems:
  - Error Trace Flags**
  - Search Trace Flags**

Moderate and Summary levels are automatically selected.

Name	<input type="checkbox"/> Detail <a href="#">(i)</a>	<input type="checkbox"/> Moderate <a href="#">(i)</a>	<input type="checkbox"/> Summary <a href="#">(i)</a>
Error Trace Flags	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Search Trace Flags	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Log files at the Detail level grow quickly. Enable only the subsystems that you need. Remember to disable trace logging when you no longer need it.

- Click **Save** to save the **EDU\_P8** domain configuration and then click **Refresh**.
- On the left navigation pane, expand the **Global Configuration > Administration > Sites** folder and select **Initial Site (Default)**.
- From the **Initial Site** tab on the right, select the **Trace Subsystem** subtab and verify that **EDU\_P8 (server hierarchy object)** as the **Configuration source**.

- If it is not already selected, select the option, click **Save**, and then click **Refresh**. Ensure that Enable trace logging is selected.
- Log out of the administration console and close the browser.
- Maximize the **Windows Explorer** window where you viewed the Content Platform Engine log files earlier: **C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1**.
- Open the **p8\_server\_trace.log** file in **Notepad++** and then verify that the file contains a couple of **DEBUG** level entries at the end of the file.

The Debug value is on the Sev column of the log file.

```
2019-03-05T05:23:29.359 7BB6685F SRCH FNRCE0000D - DEBUG Search for: "SELECT * FROM CmSweep WITH
2019-03-05T05:23:29.374 B89708D5 SRCH FNRCE0000D - DEBUG Search for: "SELECT * FROM CmSweep WITH
2019-03-05T05:23:29.374 B6C44D59 SRCH FNRCE0000D - DEBUG Search for: "SELECT * FROM CmSweep WITH
2019-03-05T05:23:29.374 92B9B375 SRCH FNRCE0000D - DEBUG Search for: "SELECT * FROM CmSweep WITH
2019-03-05T05:23:29.374 7BB6685F SRCH FNRCE0000D - DEBUG Server query time = 5.378 milliseconds f
```

- Close the trace log file and minimize the Notepad++ window.

## Configure trace logging at the site level.

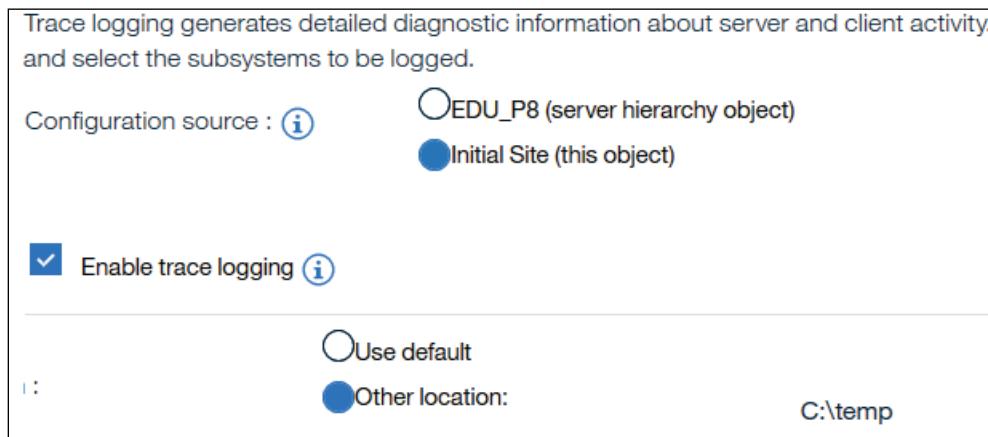
In the previous task, you enabled trace logging at the domain level. In this task, you configure the trace logging at the site level and it will override the domain settings.

- 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**.
- In the **ACCE**, on the left navigation pane, expand the **Global Configuration > Administration > Sites** folder and click **Initial Site (Default)**.
- From the **Initial Site** tab on the right, select the **Trace Subsystem** subtab and then select **Initial Site (this object)** for the **Configuration source** field.
- When you are prompted with a dialog box **Selecting this option means...**, click **OK** and then verify that **Enable trace logging** is selected.

The parent (domain) configuration values that apply to child objects will not apply to this node (site). Since the settings are configured on the site, it will override the settings on the domain, and so domain configurations values will not apply.

- For the **Log file location** field, select the **Other location** option and then type **C:\temp**.

The trace log will be saved to this new folder.



- Click **Save** and then click **Refresh**.
- From the **Initial Site** tab, scroll down to the **Subsystems** section, select the **Detail** level trace options for the **Security trace flags** subsystem.

If you are unable to select, log out of the administration console to clear the cache and log back in.

The Error Trace Flags and Search Trace Flags entries are already selected because of the previous configuration.

- Click **Save**, click **Refresh**, and then click **Close** to close the **Initial Site** tab.
- Log out of the administration console and close the browser.
- In **Windows Explorer**, navigate to the new folder location (**C:\temp**) that you specified for the trace log and verify that the **p8\_server\_trace.log** file generated. Refresh the display and notice that the file size.
- Open the file in **Notepad++** and verify that the file contains **DEBUG** level entries.
- Close the file.

## Create trace log entries.

You enabled security trace logging. You will log in to IBM Content Navigator as Olivia and then check the trace log file for this entry.

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

- Maximize the **Notepad++** window with the **p8\_server\_trace.log** file opened and if prompted, click **Yes** to reload the file.
- In **Windows Explorer**, navigate to the **C:\temp** folder and open the **p8\_server\_trace.log** file again.
- Search for the word **Olivia** and review the log entry.  
Some log entries show Olivia's login event.
- Close the trace log file and then exit **Notepad++**.
- Log out of the **IBM Content Navigator desktop** and close the browser.

## **Disable trace logging.**

Trace logging affects system performance and uses disk space. It is a good practice not to leave trace logging enabled for long periods of time.

- 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 **EDU\_P8** tab, open the **Trace Subsystem** subtab.
- Clear the **Enable trace logging** option, click **Save**, and then click **Refresh**.  
Even if you configured trace logging at the Site level and those settings override any global (domain) settings, you still have to disable trace at the domain level.
- On the left navigation pane, expand the **Global Configuration > Administration > Sites** folder and click **Initial Site (Default)**.
- From the **Initial Site** tab on the right, select the **Trace Subsystem** subtab and then clear the **Enable trace logging** option.
- Click **Save**, and then click **Refresh**.
- Log out of the administration console and close the browser.  
Optionally, you can repeat the earlier Create trace log entries task with a different user (Oscar, FileNet1) and check the trace log file. You will not find any entries for Oscar since you disabled the trace logging.
- Close all the open Windows Explorer windows.

# 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 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 Knowledge Center:

[https://www.ibm.com/support/knowledgecenter/SSNW2F\\_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc197.htm](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 object store administrator 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**.  
The Administration Console for Content Platform Engine (ACCE) opens.
- On the left pane of the **EDU\_P8** tab, expand the **Object Stores** folder and then click the **Sales** object store.  
The Sales tab opens.

- On the **Sales** tab > **General** subtab, scroll down and 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, 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:

New Audit Definition

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

Display name : <a href="#">i</a>	Audit Updates	
* Event : <a href="#">i</a>	Update Event <a href="#">▼</a>	
* Object state recording level : <a href="#">i</a>	Modified object only <a href="#">▼</a>	
* Audit type : <a href="#">i</a>	<input checked="" type="checkbox"/> Success <input type="checkbox"/> Failure	
Filter expression : <a href="#">i</a>		
Filter property name : <a href="#">i</a>		
Options : <a href="#">i</a>	<input checked="" type="checkbox"/> Apply to subclasses <input checked="" type="checkbox"/> Is Enabled	

[OK](#) [Cancel](#)

- Click **OK** to create the Audit Definition.
- Verify that your Audit Definition is listed on the **Audit Definitions** subtab of the **Order** tab and 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.

	Display Name	Event	Is Enabled	Apply To Subclasses	Success Audit Type	Failure Audit Type	Object State Recording Level
	Audit Updates	Update Event	True	True	True	False	Modified object only
	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**).
- In the **Order Basic A** tab, open the **Audit History** tab.  
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	<a href="#">Audit History</a>
View the audit entries for an object by viewing the object properties or by querying the audit log.						
<a href="#">Audit history</a>						
Event	Date Created	Event Status		Creator	Id	
<a href="#">Update</a>	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.
- In 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 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, 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** [▼](#)

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-F82E4B880DEF}	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 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.

The screenshot shows a configuration interface for an audit disposition policy. At the top, there are tabs for 'Sales' and 'Audit Dispo...', and a title bar 'New Audit D... \*'. Below the title bar are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'. The main area is titled 'Set the Audit Disposition Policy parameters'. It contains three fields: 1) 'Disposition rule' with the value 'DateCreated < Now () - TimeSpan(10, 'Minutes')'. 2) 'Duration between completed sweeps' with the value '300 seconds'. 3) A checked checkbox labeled '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, select the **Audit Subsystem** subtab from the **EDU\_P8** tab 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.

The screenshot shows the 'Audit Subsystem' configuration page. At the top, there are 'Save' and 'Refresh' buttons. Below them, three tabs are visible: 'Server Cache Subsystem', 'Audit Subsystem' (which is selected), and 'Content Subsystem'. Under the 'Audit Subsystem' tab, there is a button labeled 'Import Settings...'. A note below the tabs states: 'For this server hierarchy level and object, optimize the efficiency of the audit subsystem' with a link 'Learn more...'. At the bottom of the page, there is a checked checkbox labeled 'Enable audit pruning' with an information icon.

- 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.
- In 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.

The screenshot shows the 'Object Change Event Query' search results page. At the top, it displays 'Search: Object Change Event Query, Version: 1.0, Status: Released'. Below that is a 'Description' field with a blank line. The main area has tabs: 'Simple View', 'SQL View', 'Bulk Actions (Disabled)', and 'Search Results' (which is selected). Underneath these tabs, there is a dropdown menu labeled 'Actions'. Below the tabs, it says 'Search Result Count : 0' and 'Query returned no object'.

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**, select the **Audit Subsystem** subtab from the **EDU\_P8** tab on the right pane.
- 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.
- 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.

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.

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.

# Introduction to IBM FileNet P8 Platform security

You will learn about basic concepts on the IBM FileNet P8 Platform security in this section. Another course will provide more details on security.

## What is authentication?

Authentication is the act of verifying a user identity based on credentials (user name and password) that the user presents (who is the user?).

Authentication of individuals or of the roles that an individual has, through the external authentication mechanism, is key to the security features in IBM FileNet P8 Platform.

The two main authentication standards that are used by IBM FileNet P8 Platform are:

- Java Authentication and Authorization Service (JAAS)

The JAAS standard forms the framework for security interoperability in the Java EE world.

- Web Services Security

The Web Services Security standard forms the framework for security interoperability in the heterogeneous world of clients and servers that communicate through web services interfaces.

## Example of an authentication error

A user tries to log into IBM Content Navigator and receives a login error.

- Error message: *The user ID or password is not valid for the server.*

Causes: User is not a member in the LDAP directory or the LDAP directory service is not reachable.

Solution: Ensure that LDAP is running and reachable by the Content Platform Engine and check the LDAP directory to verify that the user exists.

## Authentication providers

An authentication provider is a supported LDAP-compliant directory service that provides authentication for the FileNet P8 domain. The authentication provider is identified during FileNet P8 installation through the JAAS configuration.

Supported directory service providers include IBM Security Directory Server, CA Directory, NetIQ eDirectory, Oracle Internet Directory Server, and Microsoft Active Directory.

For a complete list of authentication providers, refer to the Software Product Compatibility Report (SPCR) for IBM FileNet Content Manager that can be generated on the following site:  
<https://www.ibm.com/software/reports/compatibility/clarity/softwareReqsForProduct.html>

## What is authorization?

Authorization is the act of allowing a user to complete actions on the object based on the user and group memberships (What can the user do?).

Authorization requires prior authentication and uses the security token that is generated during authentication.

When an authenticated security principal attempts to access FileNet P8 objects such as an object store, a folder, or a document, Content Platform Engine checks that principal's user and group memberships from the directory service provider against the permissions assigned to the object. If successful, the user is authorized to carry out actions on the object as described by the access rights.

## Example of an authorization error

A user tries to log in to IBM Content Navigator and receives a login error. This user is a verified member in the LDAP directory.

- Error message: *You do not have the appropriate permissions to access the following repository: <repository name>*

Cause: User is not authorized to view the object store that is defined for Authentication on the IBM Content Navigator desktop.

Solution: Ensure that the user is authorized to access the object store.

## User roles

Different user roles provide varying level of access to the objects. For example, administrators, solution builders, authors, and users might have different access rights to the same objects.

Even administrators with access to Administration Console for Content Platform Engine can have different levels of access to objects. For example, one administrator might have permission to modify document classes, properties and templates that another administrator has no access to.

## FileNet P8 object security terms

Object access rights (which are also called permissions) determine which users can view the objects and what those users can do.

Following are the key terms used in the FileNet P8 security:

- **Access Control List (ACL)**

Each securable Content Platform Engine object has an associated security descriptor, part of which is the Access Control List (ACL). An ACL is a collection of all the Access Control Entries (ACEs) on an object.

- **Access Control Entry (ACE)**

An ACL consists of a set of Access Control Entries (ACEs) which are also called permissions. ACEs define who can do what.

- **Security Identifier (SID)**

Each ACE consists of a globally unique Security Identifier (SID). It uniquely identifies a security principle which is a user or group that Content Platform Engine grants or denies access to.

Each permission specifies one security principal (user or group) through a SID, and an access mask for that SID. The access mask defines the specific operations that the grantee identified by the SID is allowed to perform. Each bit in the mask corresponds to a specific operation. If the bit is set, the security principal is authorized to perform that operation.

## **Security sources of ACE**

Every ACE has a source either Default Security, Direct Instance Security, Security Inheritance or Security Template. You can view the source types of ACE in the security editor of Administration Console for Content Platform Engine (ACCE).

- **Direct Instance Security**

These permissions are directly added to an object and the ACEs are directly editable. You can view the access control entries (ACE) for a document in its Security tab in ACCE. All the ACEs in the list make up the ACL of that document.

- **Default Security**

Default permissions are placed on an object (Example: document or folder) by the default instance security ACL of its class (Example: Document class or Folder class) as well as permissions placed on a subclass by its parent class.

Default ACEs are directly editable, but if you edit an ACE, then its source type becomes Direct. You can view the ACL for a Document class in its Default Instance Security tab in ACCE. ACL on this tab will show up in the security tab of the documents that belong to this class.

- **Security Inheritance**

In this scenario, permissions are passed from a parent object to a child object. For example, a folder could be a parent of a subfolder or a document. Because of the security inheritance, an administrator can apply security permissions to many objects in one operation by setting the permissions at the parent level.

- **Security Template**

Template permissions are assigned to the objects by a security policy. Security policies along with document versioning states allow an administrator to configure the system to automatically modify ACLs on documents when their versioning state changes.

For example, the administrator can configure a system to automatically grant access to a document to a wide audience when it is released.

## **Order in which security source permissions are granted**

Each ACE has one access type either allow or deny. When evaluating the access granted by a particular ACL, the current system applies ACEs in the following order:

ACE source and type are listed on each bullet.

- Direct/Default - Deny
- Direct/Default - Allow
- Template - Deny
- Template - Allow
- Inherit - Deny
- Inherit - Allow

Higher on the list takes precedence over the lower. Deny takes precedence over allow within each category. For example, if you explicitly deny an access right to a group and explicitly allow it to a member of that group, the access right will be denied to the member.

## **#AUTENTICATED-USERS group**

This special group represents all users in the LDAP domain who are defined for IBM FileNet P8 Platform and who have been authenticated by the application server. You use this group if you want to grant access to a document to all users of IBM FileNet P8 Platform.

## Object ownership

Most objects have an owner who is typically the user who created the object.

IBM FileNet P8 Platform automatically applies an internal special user account called the #Creator-Owner and grants full control access on that object. System administrators can take ownership when necessary to change the object's security.

## Add a new security user or group to an existing object store?

There are situations where you want to add a new security user, group, or admin to an existing object store. The best practice is to setup user groups (instead of individual users) to define security on the object store when it is created. In this way, if you want to add a new admin, you just need to add the administrator user to the LDAP group, there is no change required on the FileNet Platform.

If individual users are used in the initial setup, and now if you want to add a new admin, you need to use the ACCE Security Script wizard. If you add the new user to an existing object store or domain directly (without the wizard), the user will have permissions only on those objects that are created after the addition of that user. In order for any new users to have default permissions to all existing objects requires the use the ACCE Security Script wizard. The wizard updates the security of an existing object store with users and groups as if those users and groups had been added when the object store was originally created.

## Independent and dependent security

Most objects have Access Control Lists (ACLs) that can be independently set. These objects are called independently securable.

Dependently securable objects depend on their parent object for their access rights. They are secured through the parent object.

Examples of dependently securable objects:

- Content elements, which have the same security as the associated document object
- A property that is assigned to a securable object, which has the same security as that object
- The individual choices in a choice list, which have the same security as the object that the choice list is assigned to
- A lifecycle state in a lifecycle policy

Security is more than securing documents and folders. The security of the system design determines which objects are securable by which users. For example, administrators might be responsible for securing the domain root and the object stores. Application builders might be responsible for securing classes, instances like stored searches and entry templates, and property templates. Authors might be responsible for securing folders and documents.

## **IBM Content Navigator Desktop security**

A desktop is configured to authenticate users against a specific repository in your environment. Users who want to access this desktop must be defined as having access to that repository. Also, you can limit access to the desktop to a specific set of users and groups in your repository.

A user can log in to Administration Console for Content Platform Engine but be unable to log in to the IBM Content Navigator Desktop if that user is not authorized to access that specific object store.

# Activity: Identify access issues

IBM Content Navigator (ICN) is the primary client through which users access the contents of the IBM FileNet Content Manager repositories. In this activity, you will log in to ICN as different users and identify a few scenarios where a login failure happens or access is denied.

In this activity, you will accomplish the following:

- Examine the authentication login error.
- Log in as an unauthorized user.
- Observe object store access.
- Check the security in the ICN admin desktop.

## Examine the authentication login error.

In this activity, you will attempt to log in to IBM Content Navigator as a user who is not a member of the LDAP directory and examine the error when authentication fails.

- 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 **Sample Desktop** bookmark or enter the following URL: <http://vclassbase:9081/navigator>
- Type **Jayda** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Notice that you get the following error: *The user ID or password is not valid for the server.*

- Verify that the **Content Engine Startup Context (Ping Page)** is running by entering the following URL in a browser: <http://ecmedu01:9080/FileNet/Engine>  
You can also use the bookmark (Bookmarks menu > System Health > CE Ping).

When the ping page is displayed, you have verified that the Content Platform Engine is running.

Optionally, you can open the active directory and verify that this user (Jayda) does not exist.

Similar errors can also occur if the LDAP directory service is not reachable. In a scenario where the user exists in the LDAP directory and you still get this error, you must look at the error logs to check if the LDAP service is reachable.

## Log in as an unauthorized user.

A user, in addition to being a member of the LDAP directory, must have permission (authorization) on the object store (that is used for authentication) in order to log in to an IBM Content Navigator client. The student system already has a user called Scott who is a verified member in LDAP but does not have permission to access the object store that is used for authentication. In this task, you will attempt to log in as this user and examine the error when authorization fails.

Note that if an object store is configured to provide access to the #AUTHENTICATED USERS group, then anyone who can log in to the domain can have access to that object store. The student system does not have this configuration, so only users who have explicit permission can access the object store.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: <http://vclassbase:9081/navigator>.
- Type **Scott** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that you cannot log in and get the following error: *You do not have the appropriate permissions to access the following repository: <repository name>*  
Notice that this time, the error message is different from the one that you got in the previous task. It provides a clue about the underlying cause of the login failure.  
Scott does not have access to the object store that is defined for authentication for this ICN desktop. A user must have access to the object store that IBM Content Navigator uses for authentication to log in. In some cases, an authorization problem might appear to be an authentication problem.
- Close the browser.

## Check the security in ICN admin desktop.

A desktop is configured to authenticate users against a specific repository in your environment. Users who want to access this desktop must be defined in the repository. In this task, you will log in to the ICN admin desktop and check some of the security features that control access to FileNet P8 assets.

- In the **Mozilla Firefox** browser, click the **ICN Admin** bookmark or enter the following URL: <http://vclassbase:9081/navigator/?desktop=admin>

- Type **p8admin** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.

The ICN admin desktop opens.

On the **Desktops** tab, the available desktops for this ICN instance are listed. From this admin client, you can configure all the ICN features for your desktops.

- Click **Repositories** from the left navigation pane.
- From the **Repositories** tab on the right pane, notice the list of repositories.

The Server Type column shows that all these repositories are of IBM FileNet Content Manager type. You can also configure other type of repositories. You must configure a FileNet P8 object store in this tab by using the Server URL to be able to access the content for that object store.

- Close the **Repositories** tab.
- On the **Desktops** tab, select **Sample** and click **Edit**.

This is the Sample Desktop that you were using for the earlier activities.

- On the **Sample** tab > **General** subtab, verify that **LoanProcess** repository is listed under the **Authentication** section.

When users log in to Sample desktop, ICN authenticates the users against the LoanProcess object store. If the user does not have access to this object store, the access to the ICN desktop is denied.

- On the **Sample** tab, select the **Repositories** subtab and observe the list of repositories.

Recall that these repositories were displayed on the Sample desktop in the previous tasks and authorized users were able to access content.

You can learn more on configuring repositories and desktops in the IBM Content Navigator courses.

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

## **Observe object store access.**

Object stores are usually secured by using group memberships. Users who have access to object stores can log in and use the object stores. Each user, depending on their role, has access to some but not necessarily all the object stores in an IBM Content Navigator (ICN) desktop. In this task, you will sign in as Mary and verify that Mary is able to access the LoanProcess object store but not the other object stores that are available in the ICN desktop.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: **http://vclassbase:9081/navigator**.
- Type **Mary** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- Verify that Mary is able to access the folders and documents in the **LoanProcess** object store.
- Double-click the folders in the right pane to open them.  
You can also click the folders from the left navigation pane.
- To open another repository, click the down arrow next to **LoanProcess** on the upper right.  
All the repositories that are available for this desktop are shown in the list:  
**LoanProcess, Sales, LoanProcessQA, and SalesQA**
- Attempt to open each of the object stores in the list by clicking it and verify that Mary is denied access to the other repositories.
- Log out of IBM Content Navigator and then close the browser.

# Activity: Explore the security settings in ACCE

In this activity, you will explore some of the security concepts that you learned earlier in this course. You will log in as the user P8Admin who has been given full access to the objects in the IBM FileNet Content Manager repositories. This user has already been created and configured on the student system to complete these activities.

In this activity, you will accomplish the following:

- Check the security settings.

## Check the security settings.

In this activity, you will log in to Administration Console for Content Platform Engine (ACCE) and check the security settings.

- 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 **LoanProcess** object store.
- From the **LoanProcess** tab, on the left pane, expand the **LoanProcess > Browse > Root Folder** node and then click **Loans**.
- From the **Loans** tab on the right pane, click any document (Example: **J Jones' Loan**)
- From the **J Jones' Loan** tab, select the **Security** subtab.

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

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

In the Security subtab, under the Access Permissions section, each row with a security user or group name is an Access Control Entry (ACE). All the rows collectively form the Access Control List (ACL) for the document.

Notice that the ACEs are editable. If you select a row in the list, the Edit and Delete buttons are enabled.

Observe that each row has the value Direct for the Source column. It indicates that the security source is Direct Instance Security.

- From the **J Jones' Loan** tab, select the **General** subtab, scroll down, and observe the **Inherit Security from folder** field.

If a value is assigned to this field, it indicates the folder object (security parent) from which this document inherits security.

You can learn about security inheritance and other security concepts in another course.
- Close the **J Jones' Loan** tab and the **Loans** tab.
- From the **LoanProcess** tab, on the left pane, collapse the **Browse** node, expand the **Data Design > Classes** node and click the **Document** class.
- From the **Document** tab on the right pane, select the **Default Instance Security** subtab.

In the Default Instance Security subtab, the ACL list that is under the Access Permissions section, will become the default security for the documents that belong to this Document class.
- Log out of the administration client and close the browser.

# Activity: Change direct security of an object

When you first create an object, typically, it acquires the default security settings that is defined for the class. These settings identify which users and groups can access the object. The default security for an object can also be determined by other sources such as an entry template, a security policy, folder inheritance, and so on.

In IBM Content Navigator, you can specify security on a document by using the following predefined security roles: Owner, Author, Reader, and No access. Each of these groups has a predefined set of access rights.

In this activity, you will create a document and observe its default instance security. You will then modify its security directly for the group access, access level, and ownership in IBM Content Navigator.

In this activity, you will accomplish the following:

- Add a folder and a document.
- Verify access to the document by a different user.
- Remove group access to the document.
- Verify that access is removed.
- Change access level.
- Change ownership.
- Verify the change in ownership.
- Examine the ownership.

## Add a folder and a document.

Mary and Matt are the members of the Loan Managers group. In this task, you will log in as the user Mary, create a folder and a document, and check who has access to the newly created items.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: <http://vclassbase:9081/navigator>.
- Type **Mary** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, click **New Folder** from the toolbar.
- On the **New Folder** page, type **SecurityTest** for the **Folder Name** field, observe the default security for the folder, and then click **Add**.
- Back on the **Browse** page, double-click **SecurityTest** to open the folder and then click **Add Document** from the toolbar.

- On the **Add Document** page, type **AccessLoan** for the **Document Title** field.
- For the **What do you want to save?** field, click **Browse**.
- On the **File Upload** page, navigate to the **C:\Training\F2800G\SampleDocs** folder, select any file (Example: **MarketingPlan5.pdf**), and then click **Open**.
- In the **Add Document** page, leave the default for all the other fields and observe the security that is assigned to this document.

The Owner group has the following members: P8Admin, P8Admins, and Mary

The Readers group has the following members: Loan managers, Loan officers, Loan processors, and Loan underwriters

- Click **Add** and then, on the **Browse** page, verify that the new document is listed.
- Click the **head and shoulder icon** in the banner, click **Log Out** to log out of **IBM Content Navigator** and then close the browser.

For all the following tasks, when you log out as one user and before signing in as another user, close the browser to avoid any caching issue.

## **Verify access to the document by a different user.**

Since Matt is a member of the Loan managers group which is authorized to view the document created in the previous task, Matt should be able to access the document that Mary created. In this task, you will verify the access by logging in as Matt.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: <http://vclassbase:9081/navigator>.
- Type **Matt** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, double-click the **SecurityTest** folder to open it and then verify that you can access the **AccessLoan** document.
- Right-click the document and then verify that user **Matt** has access to open, preview, or download the document (these actions are enabled) but he cannot delete this document (action is grayed out) since he is not the owner of this document.

Matt also cannot check out the document because the Loan managers have only Reader access. In a later task, you will change Matt to be the owner of the document.

- Log out of **IBM Content Navigator**.

## Remove group access to the document.

In your business scenario, you determine that the Loan processors group no longer needs access to your document. In this task, you will verify that Peter who is a member of the Loan processors group is able to view the document. You will then remove the Loan processors group access to the document and verify that Peter can no longer access the document.

- In the **Mozilla Firefox** browser, click the **Sample Desktop** bookmark or enter the following URL: <http://vclassbase:9081/navigator>.
- Type **Peter** for the **User name** field, **FileNet1** for the **Password** field, and then click **Log In**.
- From the **LoanProcess** repository, open the **SecurityTest** folder and then verify that the **AccessLoan** document is displayed.
- Log out of **Sample Desktop** and close the browser.
- Log in as **Mary** (Password: **FileNet1**).
- Open the **SecurityTest** folder, right-click the **AccessLoan** document and then select **Properties**.
- On the **Properties** page, open the **Security** tab.
- Remove the permission for **Loan processors** to read the document by clicking the **X** on the group and then click **Save**.
- Log out of IBM Content Navigator and close the browser.

## Verify that access is removed.

User Mary has removed access to the document for Loan processors. You will log in as Peter and verify that he is not able to access the document.

- Log in to **IBM Content Navigator Sample Desktop** as **Peter**:
  - **Sample Desktop** bookmark or URL: <http://vclassbase:9081/navigator>
  - User name: **Peter**
  - Password: **FileNet1**
- From the **LoanProcess** repository, open the **SecurityTest** folder and then verify that the folder is empty.

This security configuration is an example of an implicit denial. When a user has no permissions (not listed in the ACL), the document is not displayed.

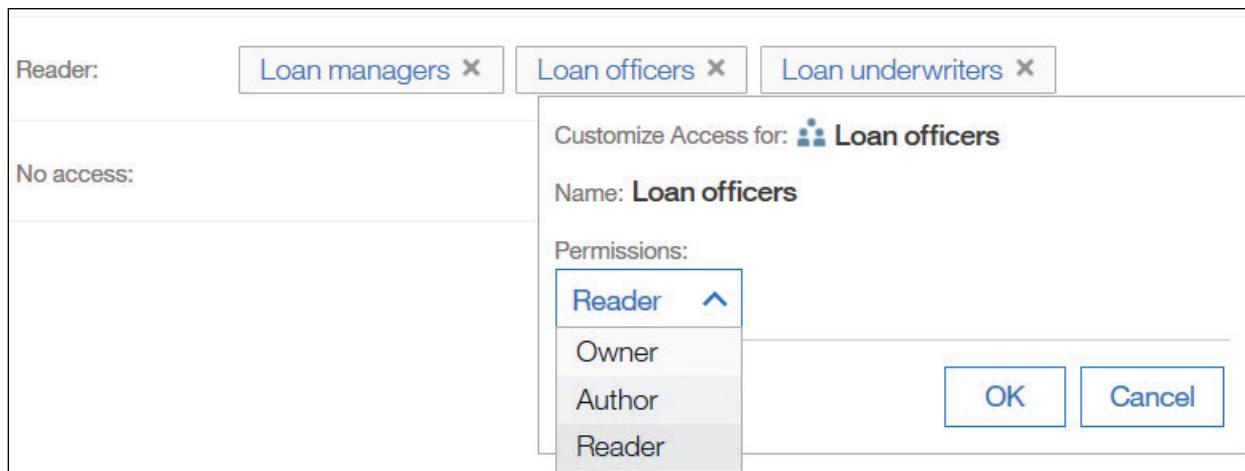
- Log out of **IBM Content Navigator** and close the browser.

## Change access level.

The members of the Loan officers group have Reader access to the document, by default. You want to grant Loan officers with Authors access for this document. As an owner of this document, Mary can change the access levels.

In this task, you will check the Reader access for Olivia who is a member of the Loan officers group. You will grant her group Author access and then check her access again.

- Log in to **IBM Content Navigator Sample Desktop** as **Olivia**:
  - **Sample Desktop** bookmark or URL: <http://vclassbase:9081/navigator>
  - User name: **Olivia**
  - Password: **FileNet1**
- From the **LoanProcess** repository, open the **SecurityTest** folder.
- Right-click the **AccessLoan** document, and then verify that user Olivia has access to open, preview, and download the document (these actions are enabled) but she cannot check out the document (this action is grayed out) because the Loan officers have only Reader access.
- Log out of **Sample Desktop**, close the browser, and then log in as **Mary** (Password: **FileNet1**).
- Open the **SecurityTest** folder, and then open the **Properties** page for the **AccessLoan** document.
- On the **Properties** page, open the **Security** tab.
- Click the **Loan officers** link and then select **Author** from the **Permissions** list.



- Click **OK**, verify that **Loan officers** are now in the **Authors** group, and then click **Save**.

- Log out of **Sample Desktop**, close the browser, and then log in as **Olivia** (Password: **FileNet1**).
- Open the **SecurityTest** folder, right-click the **AccessLoan** document, and then verify that Olivia now has access to check out the document (this action is enabled) because the Loan officers have been given Author access.
- Log out of **IBM Content Navigator Sample Desktop** and close the browser.

## Change ownership.

The user Mary is the owner of the document that you created in the earlier task and this user has full access to the document. Mary will no longer be working on this document and she wants to change the ownership to Matt who is also a member of the Loan managers group. You have already checked that Matt does not have checkout or delete access to this document. In this task, you will make Matt the owner of the document, and then recheck his access.

- Log in to **IBM Content Navigator Sample Desktop** as **Mary** (Password: **FileNet1**).
- Open the **SecurityTest** folder and then open the **Properties** page for the **AccessLoan** document.
- On the document's **Properties** page, click the **Security** tab and then for the **Share with** field, click **Select** next to the **Specific users and groups**.
- On the **Add Permissions** page, for the **Search for** field, verify that **Users** is selected, type **Matt**, and then click the Search  icon.
- Select **Matt** from the **Available** pane and move it to the **Selected** pane by using the forward arrow.
- At the end of the page, make sure **Owner** is selected for the **Permissions** field and then click **Add**.
- Back on the **Properties** page, verify that **Matt** is added to the list of Owners, and then click the **X** on **Mary** to remove the user from the Owners list, and then click **Save**.
- On the **Browse** page, right-click the **AccessLoan** document, and then verify that Mary no longer has Owner access.

Delete, checkout and a few other actions are now disabled. Since she is part of the Loan managers group, she continues to have Reader access through that membership and can open or download the document.

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

## Verify the change in ownership.

You changed the ownership of the document to Matt. In this task, you will verify that Matt has full access to the document (including delete).

- Log in to **IBM Content Navigator Sample Desktop** as **Matt** (Password: **FileNet1**)
- Open the **SecurityTest** folder, right-click the **AccessLoan** document, and then verify that Matt can now check out, delete, and other actions (these action are enabled now).
- Log out of IBM Content Navigator and close the browser.

## Examine the ownership.

The security that is set on a document in the IBM Content Navigator (ICN) client is executed as configured in ICN. Even though you changed the ownership of the document to Matt, Mary remains the owner when you examine the ownership in Administration Console for Content Platform Engine (ACCE). This is because how ICN maps its security groups (For example, Owner, Author, or Reader) Mary will be able to take owner actions on this document in ACCE even after she is removed as the owner in ICN. An administrator must reset the ownership in ACCE to complete the process. In this task, you will examine this and change the ownership to Matt.

- 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**.
- From the **EDU\_P8** tab, expand the **Object Stores** folder on the left pane and then click the **LoanProcess** object store.
- From the **LoanProcess** tab, expand the **LoanProcess > Browse > Root Folder** node on the left pane and then click **SecurityTest**.
- From the **SecurityTest** tab on the right, click the **AccessLoan** document link.
- Scroll the tabs to the right and then click the **Security** tab to open it.
- To verify that **Mary** is still the owner of the document, scroll down the page to the **Owner/Active Markings** section and then confirm that the **Owner** is **mary@edu.ibm.com**.
- Click **Change Owner**.
- On the **Change Owner** page, select the **Change owner to** option, and then click **Find**.

- On the **Add Users and Groups** page, search for **Matt** (by **Short name**).

The screenshot shows a search interface with the following fields:

- Search by : dropdown set to "Short name".
- Starts with dropdown.
- Search input field containing "Matt".
- Search button.

- Select **Matt** from the **Available Users and Groups** pane and then move Matt to the **Selected Users and Groups** pane by clicking the forward arrow.
- Scroll down, click **OK**, and then verify that Matt (**matt@edu.ibm.com**) is now the owner on the **AccessLoan** tab.
- Click **Save**, click **Refresh**, and then click **Close** to close the **AccessLoan** tab.
- Close the **SecurityTest** tab.
- From the **LoanProcess** tab, click **Refresh**.  
This completes the change of ownership at all levels.
- Log out of **Administration Console for Content Platform Engine**, and then close the browser.

# Activity: Customize security access

In Administration Console for Content Platform Engine, you can specify security by using the following predefined Permission groups: Full Control, Minor versioning, Major versioning, Modify properties, View content, View properties, Publish, and Custom.

In this activity, you will use Permission groups for common security scenarios, and specify custom permissions for fine-grained security configurations.

In this activity, you will accomplish the following:

- Add typical document permissions.
- Edit security settings.

## Add typical document permissions.

In this task, you will create a folder and a document. You set security by using the predefined Permission Groups.

- 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**.
- From the **EDU\_P8** tab on the left pane, expand the **Object Stores** folder and click the **LoanProcess** object store.
- From the **LoanProcess** tab, expand the **LoanProcess > Browse** node on the left pane, right-click **Root Folder**, and then select **New Folder**.
- Type **AT Folder** for the **Folder name** field, click **Next** two times, and on the **Summary** page, click **Finish**.
- Click **Close** on the **Success** page.
- Expand the **LoanProcess > Browse > Root Folder** node on the left pane and then click **AT Folder** to open the new folder.
- On the **AT Folder** tab, click **Actions > New Document** from the top toolbar.
- On the **New Document** tab, type **Access Test** for the **Document title** field, verify that the **With content** option is selected and then click **Next**.
- Click **Add** to add a content element, and then click **Browse** to select a document.
- On the **File Upload** page, navigate to the **C:\Training\F2800G\SampleDocs** folder, select a document (For example, **SampleTextDoc1.txt**) and then click **Open**.

- On the **Add Content Element** window, click **Add Content**.
- Click **Next** several times, leave the default values, and then click **Finish** on the **Summary** page.
- Click **Close** on the **Success** page.
- On the **AT Folder** tab, click **Refresh**, verify that the new document is listed, and then click the **Access Test** link.
- On the **Access Test** tab, scroll to the **Security** subtab.
- On the **Security** subtab, click **Add Permissions > Add User/Group Permission**.
- In the **Add User and Groups** page, type **Case** on the **Search by** field and then click **Search**.
- Select the **Case workers** from the **Available Users and Groups** pane and then move to **Selected Users and groups** by clicking the forward arrow.

Search by : Short name Starts with Case Search

**Search Results**

Available Users and Groups	Selected Users and Groups
#AUTHENTICATED-USERS	Case workers
#CREATOR-OWNER	
#REALM-USERS(EDU_AD)	

- Scroll down to the **Permissions** section, select **Major versioning** from the **Permission group** list.

**Permissions**

Permission type :	Allow
Apply to :	This object only
Permission group :	Full Control
	Full Control
	Minor versioning
	Major versioning

Verify that the following individual permissions are automatically selected: View all properties, View content, Change state, Major versioning, Read permissions, Unlink document, Modify all properties, Link a document / Annotate, Create instance, and Minor versioning.

- Click **OK** and back on the **Access Test** tab, click **Save**.

## Edit security settings.

For this scenario, the Major versioning Permission group grant access to more actions than what you want to grant to the Case workers group. You can control the security at a more granular level by setting custom permissions. In this task, you will modify the permissions to a custom level.

You are already logged on to Administration Console for Content Platform Engine as p8admin. You are viewing the Access Test document security tab.

- On the **Access Test** tab > **Security** subtab, select the **Case workers** row under **Access Permissions** section and then click **Edit**.
- In the **Edit Permissions** page, under the **Permission group** section, clear the **Unlink document** permission.
- Confirm that the value for the **Permission group** field changes to **Custom**.

Users and Groups :	Case workers
Permission type :	Allow
Apply to :	This object only
Permission group :	Custom
<input checked="" type="checkbox"/> View all properties <input checked="" type="checkbox"/> Modify all properties	

- Click **OK** to close the page.
- On the **Access Test** tab > **Security** subtab, click **Save**.
- Log out of **Administration Console for Content Platform Engine** and close the browser.

# Manage storage areas

## What is a storage area?

A storage area is a container where Content Platform Engine (CPE) stores content. CPE can be configured for file storage, fixed storage, database storage, or advanced storage. These storage options can be used individually or together.

When you create an object store, the wizard prompts you to specify the default content storage and the selection determines which content store serves as your default store when you add documents to the object store.

## Types of storage areas

- **Database storage area**

This is the database that is used for the object store. Content Platform Engine stores both the objects and the content for those objects in the same database. Database storage areas are used for a smaller number and size of documents. For larger number of documents, other storage options are preferred.

- **File storage area**

This is a storage area that contains document content in a directory tree (a hierarchy of folders) on a local or shared network drive. The disk drive can be a Windows NTFS volume, a UNIX file system, or an IBM General Parallel File System (GPFS). You cannot create a file storage area on an encrypted NTFS volume.

Content Platform Engine server must have full access to the folders and the shared network drive that is used for storage.

A many-to-many relationship exists between Content Platform Engine servers and file storage areas. Many servers can manage one file storage area and a single server can manage multiple file storage areas.

File storage area contains the following directory structure:

Base directory - It is the user-named parent directory for one or more file storage areas.

Root directory - It is the user-named top-level directory for a specific file storage area. Contains a stakefile which is a system file.

Content directory tree –The directories at the lowest level of the content directory tree store the committed content element files. The Storage Area wizard creates the tree.

- **Fixed storage area**

This file storage area is an external (non-FileNet P8) fixed content system that provides more storage and data retention. It consists of a file storage staging area on the FileNet P8 system and a separate content device.

- **Advanced storage areas**

An advanced storage area supports heterogeneous storage devices. OpenStack cloud storage and file system storage, as well as IBM Cloud Object Storage (ICOS). Amazon S3, and Dell Elastic Cloud Storage can be used as advanced storage areas. Advanced storage areas provide high availability content storage and disaster recovery through the use of replication and replica repair.

If you use advanced storage areas for your object stores, you need to choose a replication model that best suits your storage requirements. Replicas are storage area devices with identical content. Advanced storage areas are designed to be flexible enough to support a wide variety of replication models. An advanced storage area replicates synchronously to a designated number of storage devices in a designated priority order. You can set up both synchronous and asynchronous replication.

## **Support for S3 advanced storage devices**

The Content Platform Engine S3 connector provides the ability to store and retrieve documents to and from an S3-compatible object storage solution that is deployed either on premise or in a private or public cloud. The connector uses the Content Platform Engine Advanced Storage Area interface that is specially designed for object and cloud connectivity.

You can use the connector with a number of devices, including:

- IBM Cloud Object Storage device
- Amazon Simple Storage Service (S3) storage device
- Dell Elastic Cloud Storage

Content Platform Engine integrates with the S3 REST API and supports basic object operations such as adding, retrieving, and deleting objects in an S3 storage repository.

For more details on the supported storage solutions, review the Software Product Compatibility report for IBM FileNet Content Manager. The information is provided on the Hardware tab of the report. Reports can be generated here:  
<http://www.ibm.com/software/reports/compatibility/clarity/index.html>

FileNet fix pack compatibility matrices are available here:

<http://www.ibm.com/support/docview.wss?rs=3278&uid=swg27014734>

## Storage area options

Content Platform Engine offers the following options to store the content:

- **Encryption**

Content Platform Engine encrypts and decrypts content by using AES in Counter mode, a Federal Information Processing Standard (FIPS) 140-compliant algorithm.

Encryption:

- protects the confidentiality of content that you add to a storage area.
- incurs a performance cost for content upload and retrieval.

The retrieval of encrypted content relies upon information that is stored in the object store database. If that information is lost, the content cannot be retrieved. To avoid such problems, regularly back up the object store database.

- **Duplication suppression**

The suppression of duplicate content potentially reduces the storage space that is required to store content. Content Platform Engine checks the existing content before adding new content to the storage area. If identical content exists, the new content is not stored separately from the existing content.

Content duplication suppression:

- incurs a performance cost for uploading content.
- does not apply to fixed content storage areas.

- **Compression**

Content that is uploaded to a storage area is compressed if content compression is enabled and if the content can be compressed below the content compression threshold.

Content compression:

- reduces storage space that is required for content storage.
- can affect overall performance.

If both compression and encryption are enabled, compression is applied before encryption. Each compressed block is encrypted independently.

- **Content Caching options**

Content caching provides faster access to content across sites by temporarily storing remote content locally.

- To reduce network traffic, content can be cached on the file system that is local to the Content Platform Engine server.
- A content cache area is an area that contains frequently accessed document content that is duplicated from the original content in storage areas.
- The following content caching options are available:
  - Not Allowed: Storage area content caching is disabled.
  - Cross-site Only: Caching of storage area content is available only when the storage area does not belong to the same site as the server that accesses the content.
  - Allowed: Storage area content can be cached to any cache area.

Note that if encryption is enabled, the content will be encrypted in the content cache as well as in the storage area.

- **Storage level hold for Hitachi devices**

Support has been added for implementing storage level holds on content stored on Hitachi HCL storage devices.

This is an aligned mode feature:

Both the Content Platform Engine software and the Hitachi storage hardware set the storage hold. The storage hold is controlled by Content Platform Engine (CPE) and CPE determines when to set and clear the storage hold on the Hitachi storage device. When a storage hold is set, content cannot be deleted until the storage hold is removed.

The storage hold capability is enabled through the Administration Console for Content Platform Engine. When enabled, all new content that is stored on Hitachi storage has a hold placed on it. When the content is to be deleted, Content Platform Engine removes the hold prior to deleting the content on Hitachi storage.

Storage level hold applies to content that is ingested after the capability is enabled. You cannot apply storage holds to existing content.

Storage level holds can be applied whether the Hitachi storage device is configured in aligned or unaligned mode.

## Resource statuses of File Storage Area

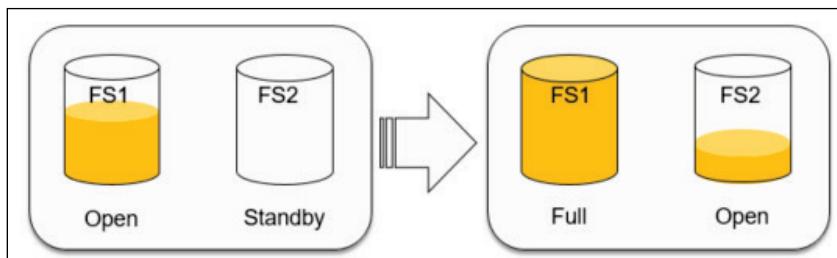
A resource status is a status associated with a storage area that determines, in combination with the storage area configuration, the permissible content operations for that storage area.

You can configure a storage area to disable the following content operations:

- Create content and Append content
- Delete content

Resource status changes occur in the following ways.

- **Automatically:** Content Platform Engine sets the resource status to Open for newly created storage areas, and also for storage areas with a status of Standby (in some circumstances). Content Platform Engine changes the resource status from Open to some other status when detecting a particular storage area condition. For example, as shown in the following diagram, if FS1 reaches the maximum size and FS2 is on Standby, then FS1 switches from Open to Full, while FS2 switches from Standby to Open.



- **Indirectly:** You indirectly change the resource status when you set a storage area to be online or offline. For example, enabling the storage area to be online causes the resource status to be Open, and disabling the storage area causes the resource status to be Closed.
- **Directly:** You can directly change the resource status for a storage area.

## What is storage policy?

A storage policy provides mapping to specific physical storage areas and is used to specify where content is stored for a class or object with content (for example, a document). Each storage policy can have one or more storage areas as its assigned content storage target.

## Storage area farms

A storage area farm is a group of storage areas (a subset of the available storage areas) acting as a single logical target for content storage. Through this farming, Content Platform Engine provides load-balancing capabilities for content storage by transparently spreading the content elements across multiple storage areas.

The storage policy functions as both the mechanism for defining the membership of a storage area farm, and the means for assigning documents to that farm.

You can specify a single default content storage location for a document class. If you want to use storage farm capabilities, you need to use storage policies to manage the content delivery to the different storage areas.

For more information on storage management and best practices, refer to the article:  
<https://www.ibm.com/developerworks/data/library/techarticle/dm-1003filenetstoragemanagement/index.html>

# Activity: Create a file storage area

In this activity, you create a file storage area, set it as the default storage area for the Document class, and then test it by adding a document.

In this activity, you will accomplish the following:

- Examine the default storage area.
- Examine an existing storage directory.
- Create a subdirectory for the file storage area.
- Create a file storage area.
- Verify the storage area directory structure.
- Set default storage for the content of Document class.
- Edit your storage area.
- Add a document to verify the configuration.

## Examine the default storage area.

In this task, you will add a document to an object store to check its default storage option for the Document class. You will also verify the default storage area statistics before and after adding a document.

- 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 **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left pane, navigate to **LoanProcessQA > Administrative > Storage > Storage Areas** and select **Default Database Storage Area**.
- From the **Default Database Storage Area** tab on the right, open the **Statistics** subtab and then click **Refresh**.

- Verify that the value for the **Total files** field is **0** (zero) and then close the tab.

The screenshot shows a software window titled "LoanProcess...". At the top, there are tabs for "Save", "Refresh", "Actions", and "Close". Below the tabs, the title bar says "Database Storage Area: Default Database Storage Area". There are five tabs at the top of the main area: "General", "Properties", "Configuration", "Statistics" (which is highlighted in blue), and "Storage Policies". A sub-header below the tabs reads: "Set parameters to define the capacity of the storage area. You can also view when the storage area is full or near full." Under the "Statistics" tab, there are two entries: "Total files : 0" and "Total file size : 0".

- On the left pane, collapse the **Administrative** node and then expand **Browse**.
- Right-click **Root Folder** and then select **New Folder** to create a folder.
- From the **New Folder** tab on the right pane, type **Test** for the **Folder name** field and then click **Next**.
- Leave the defaults, click **Next** one more time, and then on the **Summary** page, click **Finish**.
- Click **Close** on the **Success** page and then click **Refresh** on the **LoanProcessQA** tab.
- On the left pane, expand **Browse > Root Folder**, right-click the **Test** folder, and click **New Document** to add a document.
- From the **New Document** tab on the right pane, type **TestDoc** for the **Document title** field, select the **With content** option, and then click **Next**.
- On the **Document Content Source** page, under the **Content Elements** section click **Add**.
- On the **Add Content Element** dialog box, click **Browse**.
- On the **File Upload** window, select a document (Example: **SampleDoc1.docx**) from the **C:\Training\F2800G\SampleDocs** folder and then click **Open**.
- On the **Add Content Element** dialog box, click **Add Content**.
- Click **Next** four more times (On the **Document Content Source**, **Object Properties**, **Document Content and Version**, **Specify Settings for Retaining Objects** pages).

- On the **Advanced Features** page, verify that **Default Database Storage Policy** is selected and then click **Next**.

The screenshot shows a software interface titled 'LoanProcess...' with a sub-tab 'New Document... \*'. Below the tabs are buttons: '< Back', 'Next >', 'Finish', and 'Cancel'. The main content area is titled 'Advanced Features' with the sub-instruction: 'Specify additional options that you can assign to the document you are adding to the object store.' Two options are listed: 'Storage area : (i)' and 'Storage policy : (i)'. A blue box highlights the 'Storage policy' row, with the text 'Default Database Storage Policy' appearing below it.

This default policy is associated with the default storage area. After you add this document, there will be a change in the total number of files for the default storage area.

You will work with Storage policy in the following activity.

- On the **Summary** page, click **Finish** and then click **Close** on the **Success** page.
- View the default storage area statistics again:
- On the left pane, navigate to **Administrative > Storage > Storage Areas** and click **Default Database Storage Area**.
- From the **Default Database Storage Area** tab on the right, open the **Statistics** subtab and click **Refresh**.
- Verify that the **Total files** field now has a value: **1 (one)**.

The screenshot shows a table with tabs: 'General', 'Properties', 'Configuration', 'Statistics' (which is underlined), and 'Storage Policies'. The 'Statistics' tab displays the message: 'Set parameters to define the capacity of the storage area. You can also view when the storage'. Below this are two rows: 'Total files : (i)' with the value '1' and 'Total file size : (i)' with the value '0'.

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

## **Examine an existing storage directory.**

In this task, you will view the existing file storage directories.

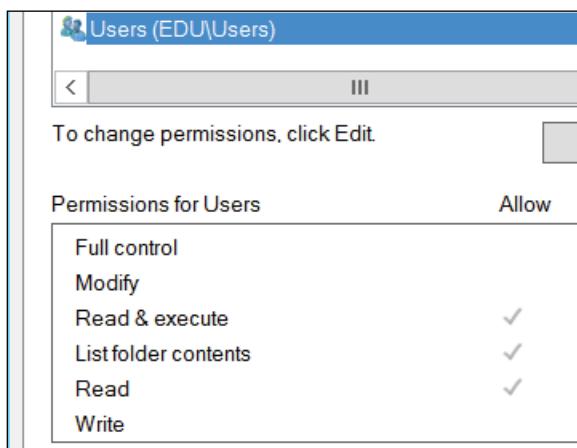
- In **Windows Explorer**, navigate to **C:\filenet**.  
The student system uses this folder as the base directory for file storage.

- Expand the **filenet** folder and observe that there are several folders: **BulkMoveFS**, **file\_stores**, **file\_stores2**, and **PurchaseOrderFS**.  
These folders are the root directories for file storage on the student system.  
You can use any string value for the base and root directory names. You can select any location in your local or distributed file system for the base directory. Content Platform Engine should have full access permission to these folders.
- Open the **file\_stores\content** folder and verify that there are **23** folders that are named **FN0** to **FN22**.  
These directories store the committed content element files. The Storage Area wizard creates these content folders.
- Expand the **FN0** (or any one of the 23 folders) folder and verify that each of them contains a set **23** folders that are named **FN0** to **FN22**.
- Expand the **file\_stores\inbound** folder and verify that there are several folders.  
The inbound folder is the working area for uploading new content.

## **Create a subdirectory for the file storage area.**

In this task, you will create a subfolder to use it as a root directory for the new file storage area.

- In **Windows Explorer**, navigate to the **C:\filenet** folder and then create a folder with a name: **Loan\_filestore**
- Right-click the **Loan\_filestore** folder and select **Properties**.
- In the **Properties** window, click the **Security** tab and then verify that the permission for the non-admin users (Example: **EDU\Users**) is **read-only** to the folder.



Only the system admin user must be able delete and write files in the file store directories.

- Click **Cancel** and then close the **Windows Explorer**.

## Create a file storage area.

In this task, you will create a file storage area in Administration Console for Content Platform Engine (ACCE).

- 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, expand the **Object Stores** folder and then click the **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left pane, navigate to **LoanProcessQA > Administrative > Storage** and click **Storage Areas**.
- From the **Storage Areas** tab on the right pane, click **New**.
- On the **New Storage Area** tab, select **File** for the **Storage area type** field and click **Next**.
- Type **Loan Storage Area** for the **Display name** field, scroll down to verify that **Initial Site** is selected for the **Site** field, and then click **Next**.
- Configure the Storage Area with the following data:
  - Root directory: **C:\filenet\Loan\_filestore**  
This is the directory that you created in the previous task.
  - Directory structure size: **Small**  
Small structure will create two levels with a total of 529 directories. Similar to the one that you inspected in the earlier task.
  - Maximum number of elements: **Unlimited**
  - Maximum size: **Maximum allowed on device**
  - Delete method: **Destroy**
  - Encrypt content: **Disabled**
  - **Options:**
    - **Suppress duplicate content elements:** Cleared (Not selected)
    - **Compress content:** Selected

The completed page contains the values that you entered:

Configure the Storage Area	
* Root directory : <a href="#">i</a>	C:\filenet\Loan_filestore
Directory structure size : <a href="#">i</a>	Small
* Maximum number of elements :	<input checked="" type="radio"/> Unlimited <input type="radio"/> 25000
* Maximum size :	<input checked="" type="radio"/> Maximum allowed on device <input type="radio"/> 5000
Deletion method : <a href="#">i</a>	Destroy
* Encryption method : <a href="#">i</a>	Disabled
Options :	<input type="checkbox"/> Suppress duplicate content elements <a href="#">i</a> <input checked="" type="checkbox"/> Compress content <a href="#">i</a>
Compression threshold (percentage) : <a href="#">i</a>	80
* Standby activation priority : <a href="#">i</a>	0

- For all other fields, leave the defaults and click **Next**.  
Click the information icon next to each field name to get more details about that field.
- For **Select a Storage Policy for this Storage Area**, leave the defaults (not selected) and click **Next**.  
You will create a storage policy in the next activity.
- Click **OK** to close the message about mapping the storage area to a storage policy.
- On the **Summary** page, review the details and click **Finish**.
- On the **Success** page, click **Close** to close the tab.

- On the **Storage Areas** tab, click **Refresh** and then verify that the **Loan Storage Area** is listed.
- Notice that **Loan Storage Area** has the **Type** that you assigned (**File Storage Area**) and the **Total Files** column has zero (**0**) as the value.
- Log out of the administration console and close the browser.

## Verify the storage area directory structure.

- In **Windows Explorer**, navigate to the **C:\filenet\ Loan\_filestore** folder.
- Open the **Loan\_filestore** folder and observe the structure.  
Verify that *content* and *inbound* directories are created. The wizard also creates a folder that is called *system* and an xml file with the name: *fn\_stakefile.xml*
- Expand the **content** folder and verify that there are **23** folders that are named **FN0** to **FN22**.
- Open the **FN0** (or any one of the 23 folders) folder and verify that each of them contains a set of 23 folders that are named **FN0** to **FN22**.
- Open the **C:\filenet\ Loan\_filestore\inbound** folder and verify that there are several folders.
- Close **Windows Explorer**.

## Set default storage for the content of Document class.

In this task, you configure the new file storage area as the default storage container for the Document class.

- 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 **LoanProcessQA** object store.
- From the **LoanProcessQA** object store tab, expand **Data Design > Classes** on the left pane and click **Document**.
- From the **Document** tab > **General** subtab, scroll down and select **Loan Storage Area** from the list for the **Default storage area** field.

- Select <None> from the list for the **Default storage policy** field.

Default storage area :	<a href="#">Loan Storage Area</a>
Default storage policy :	<None>

- Click **Save** on the toolbar and then when prompted, click **Cancel** on the **Propagate Metadata Changes** dialog box.

Depending on the configuration on this page, it affects the subclasses of the Document.

- Close the **Document** tab.
- Click **Refresh** on the **LoanProcessQA** object store tab.

## Edit your storage area.

This task demonstrates how you can edit an existing storage area. You will edit the Loan Storage Area that you created earlier to modify the properties and update the Statistics tab.

- From the **LoanProcessQA** tab, on the left pane, expand **Administrative > Storage > Storage Areas** and then click **Loan Storage Area**.
- From the **Loan Storage Area** tab on the right pane, click the **Configuration** subtab and then edit the following fields.
  - Content Caching: **Not Allowed**
  - Delete method: **Purge**

* Content caching :	<a href="#">Not allowed</a>
* Deletion method :	<a href="#">Purge</a>

- From the **Loan Storage Area** tab, open the **Statistics** subtab.
- In the **Storage Area Maximums** section, change **Maximum Size** to **10 MB**. Click the circle beside the field and change the value.

Maximum size :	<input type="radio"/> Maximum allowed on device
	<input checked="" type="radio"/> 10

- In the **Storage Policies** subtab, observe that the Storage Area is not mapped to any Storage Policies.
- Click **Save** to save your changes to the storage area properties and then click **Close**.
- From the **LoanProcessQA** tab, click **Refresh**.

## Add a document to verify the configuration.

In this task, you will verify that adding a document (of Document class) to the system adds the content to the new file storage area. You will also verify the default storage area statistics before and after adding a document.

- From the **LoanProcessQA** tab, expand **Administrative > Storage > Storage Areas** and click **Loan Storage Area** tab.
- On the **Loan Storage Area** tab, click **Refresh**, open the **Statistics** subtab, and verify that there are zero files.

File Storage Area: Loan Storage Area				
General	Properties	Configuration	<u>Statistics</u>	Storage Policies
Set parameters to define the capacity of the storage area. You can also view when the storage area is full. Total files : <span style="color: blue;">(i)</span> 0 Total file size : <span style="color: blue;">(i)</span> 0				

- Expand **Browse > Root Folder**, right-click the **Test** folder, and then select **New Document**.
- Type the name for the document: **Storage Area Test**
- Confirm that **Document** is selected for the **Class** field and the **With Content** option is selected.
- Click **Next** and then on the **Document Content Source** page, click **Add**.
- On the **Add Content Element** dialog box, click **Browse**.
- On the **File Upload** window, select a document (Example: **SampleTextDoc2.txt**) from the **C:\Training\F2800G\SampleDocs** folder and then click **Open**.
- On the **Add Content Element** dialog box, click **Add Content**.

- Click **Next** four more times (On the **Document Content Source, Object Properties, Document Content and Version, Specify Settings for Retaining Objects** pages).
- On the **Advanced Features** page, confirm that **Loan Storage Area** is selected and then click **Next**.
- On the **Summary** page, click **Finish** and then click **Close** on the **Success** page.
- On the left pane, click the **Test** folder under the **Browse > Root Folder** folder.
- From the **Test** tab on the right pane, click **Refresh**, verify that your new document (**Storage Area Test**) is listed, and then click **Close**.
- On the **Loan Storage Area** tab, click **Refresh**, select the **Statistics** subtab, and then confirm that the Loan Storage area now contains one file.  
The value for the Total files field shows 1 (one).
- Log out of the administration console and close the browser.

# Activity: Create a storage policy

In this activity, you will create two file storage areas to represent a storage area farm. You will also create a storage policy that includes both of these storage areas and assign it to the Document class. The storage policy uses the load-balancing capabilities of the Content Platform Engine to distribute content within a storage area farm. You will then add some documents to the object store and observe the file count information in the storage areas.

In this activity, you will accomplish the following:

- Create storage area farms.
- Configure a new storage policy.
- Assign the storage policy to the Document class.
- Verify that storage area farming is working.

## Create storage area farms.

In this task, you create two subdirectories for storage area farms and then create two storage areas.

- In **Windows Explorer**, navigate to **C:\filenet** folder, create two folders with the following names: **FS\_Farm1** and **FS\_Farm2**, and close the Windows Explorer.
- 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, expand the **Object Stores** folder and then click the **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left tab, expand **Administrative > Storage**, and click the **Storage Areas** node.
- From the **Storage Areas** tab on the right pane, click **New**.
- On the **New Storage Area** tab, configure the Storage Area by using the following data:
  - Storage area type: **File**
  - Display name: **FS1**
  - Site: **Initial Site**
  - Root directory: **C:\filenet\FS\_Farm1**

- Directory structure size: **Small**
- Maximum number of elements: **Unlimited**
- Maximum size: **20 MB**
- Delete method: **Clear**
- Encrypt content: **Disabled**
- Suppress duplicate content elements: **Cleared** (Not selected)
- Compress content: **Selected**
- Select a Storage Policy for this Storage Area page: Leave the defaults (not selected).

For the fields that are not listed here, leave the defaults.

For more step-by-step instructions, refer to the *Create a file storage area* task in the previous activity.

You will create a storage policy in the next task.

- In the **Storage Areas** tab, click **Refresh** and then verify that the **FS1** Storage Area is listed and it has **0** for the **Total Files** field.
- Create a second File Storage area by repeating the above steps and by using the following values:
  - Storage area type: **File**
  - Display name: **FS2**
  - Site: **Initial Site**
  - Root directory: **C:\filenet\FS\_Farm2**
  - Directory structure size: **Small**
  - Maximum number of elements: **Unlimited**
  - Maximum size: **20 MB**
  - Delete method: **Clear**
  - Encrypt content: **Disabled**
  - Suppress duplicate content elements: **Cleared** (Not selected)
  - Compress content: **Selected**
  - Select a Storage Policy for this Storage Area page: Leave the defaults (not selected).

- In the **Storage Areas** tab, click **Refresh** and then verify that the **FS2** Storage Area is listed and it has **0** for the **Total Files**.
- Close the **Storage Areas** tab.

## Configure a new storage policy.

In this task, you create a New Storage Policy and configure it.

- From the **LoanProcessQA** tab, expand **Administrative > Storage** and click **Storage Policies** on the left pane.
- From the **Storage Policies** tab on the right, click **New**.
- On the **New Storage Policy** tab, type **Farm Storage Policy** for the **Display name** field and then click **Next**.
- On the **Select the Content Storage Method** page, choose the **Select the storage Areas from a list** option and then click **Next**.
- For the **Storage areas** field, select **FS1** and **FS2** from the list and then click **Next**.
- On the **Summary** page, review the information, click **Finish**, and then click **Close**.
- On the **Storage Policies** tab, click **Refresh** and then verify that your Storage Policy is listed.

You can add more storage areas to an existing policy from the General tab of that policy.

## Assign the storage policy to the Document class.

In this task, you will remove the previously assigned storage areas and configure the storage policy for the Document class.

- From the **LoanProcessQA** object store tab, expand **Data Design > Classes** on the left pane and then click **Document** class.
- From the **Document** tab on the right pane, under the **General** subtab, scroll down to the **Default storage policy** field and then select **Farm Storage Policy** from the list.
- Select **<None>** for the **Default storage area** field.

Default storage area : 	<b>&lt;None&gt;</b>
Default storage policy : 	<b>Farm Storage Policy</b>

Ensure that <None> is selected for the Default storage area. The Farm Storage policy specifies the FS1 and FS2 storage areas to save the content for the Document class.

If both the Default storage area and the Default storage policy are set, the Default storage area setting takes precedence and the storage policy that you defined is ignored.

- In the **Document** tab, click **Save**.
- When prompted, click **Cancel** on the **Propagate Metadata Changes** dialog box.
- In the **Document** tab, click **Refresh** and then click **Close** to close the Document tab.
- Log out of the administration console and close the browser.

## **Verify that storage area farming is working.**

To verify that the storage area farm functions, you will add some documents to the LoanProcessQA object store and then view the statistics of the FS1 and FS2 storage areas.

- 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 **LoanProcessQA** from the list.
- On the left pane, click the **Test** folder under the **LoanProcessQA** object store.
- In **Windows Explorer**, navigate to **C:\Training\F2800G\SampleDocs**, select and drag all the files, and drop them to the IBM Content Navigator **Test** folder.

Note: Add all of the files, but not the subfolders.

In Content Navigator desktop, the Add Documents page opens.

- In **Content Navigator** desktop, click **Add** to add all the files and wait for the upload to complete.
- Verify that the documents are listed in the **Test** folder and then log out of **Content Navigator** desktop and close the browser.
- 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, expand the **Object Stores** folder and then click the **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left pane, expand **Administrative > Storage**, and then click the **Storage Areas** node.
- In the **Storage Areas** tab, confirm that **FS1** and **FS2** have some documents. Your storage policy used the load-balancing capabilities of the Content Platform Engine to distribute content within the storage area farm. The documents were added to both the file storage areas in the storage area farm.

	Display Name	Type	Status	Total Files	Total File Size
	Default Database Storage Area	Database Storage Area	Open	1	11.1 KB
	Loan Storage Area	File Storage Area	Open	1	0.1 KB
	FS1	File Storage Area	Open	7	892.8 KB
	FS2	File Storage Area	Open	3	201.0 KB

The screen capture that is shown here is a sample. Depending on the number of documents that you added and how they were load-balanced, you might get different numbers for FS1 and FS2.

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

# Activity: Create an advanced storage area

In this activity, you will create an advanced file storage area with two replication devices: ASFD1 and ASFD2. You want to make ASFD1 the primary synchronous device, and ASFD2 the secondary synchronous device. You will then add them to the Farm storage policy.

In this activity, you will accomplish the following:

- Create Advanced Storage Devices.
- Create an Advanced Storage Area.
- Configure the storage devices.
- Edit the storage policy.
- Test the advanced storage area.

## Create Advanced Storage Devices.

You must create an advanced storage device before you can use an advanced storage area.

- In **Windows Explorer**, navigate to **C:\filenet** folder, create two folders with the following names: **ADVS1** and **ADVS2**, and close the Windows Explorer.
- 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, expand the **Object Stores** folder and then click the **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left tab, expand **Administrative > Storage > Advanced Storage > Advanced Storage Devices** and click **File System Storage Devices**.
- From the **File System Storage Devices** tab on the right pane, click **New**.
- On the **New File System Storage Device** tab, type **AFSD1** for the **Display name** field and then click **Next**.
- On the **Configure the File System Device** page, type **C:\filenet\ADVS1** for the **Root directory path** field and then click **Next**.
- On the **Summary** page, verify the details, click **Finish**, and then click **Close** on the **Success** page.

- On the **File System Storage Devices** tab, click **Refresh** and then verify that **AFSD1** is listed.
- Create another File System Storage Device by repeating the above steps and by using the following values.
  - Display name: **AFSD2**
  - Root directory path: **C:\filenet\ADVS2**
- On the **File System Storage Devices** tab, click **Refresh**, verify that **AFSD2** is listed, and then close the tab.
- From the **LoanProcessQA** tab, click **Refresh**.

## **Create an Advanced Storage Area.**

In this task, you will create an advanced storage area by using the two advanced storage devices that you created.

- From the **LoanProcessQA** tab, on the left pane, navigate to **Administrative > Storage > Advanced Storage** and click **Advanced Storage Areas**.
- From the **Advanced Storage Areas** tab, on the right pane, click **New**.
- On the **New Advanced Storage Area** tab, type **ADV\_SA** for the **Display name** field, verify that Initial Site is selected for the **Site** field, and then click **Next**.
- On the **Configure the Advanced Storage Area** page, select **AES Counter Mode with 128-bit key** for the **Encryption method** field and then select the **Compress content** option.

* Encryption method : <a href="#">(i)</a>	AES Counter Mode with 128-bit key
Options :	<input type="checkbox"/> Suppress duplicate content elements <a href="#">(i)</a> <input checked="" type="checkbox"/> Compress content <a href="#">(i)</a>

- Click **Next** and then on the **Associate a Storage Device with this Advanced Storage Area** page, type **2** for the **Required synchronous devices** field.
- For the **Available storage replication devices** field, select the two devices that you created: **AFSD1, AFSD2** and then click **Next**.

The number of required synchronous devices must be greater than zero and equal to or less than the number of available storage replication devices.

- On the **Advanced Storage Area Parameters** page, select **Validate on creation**, verify that **Auto repair on content validation** is already selected, and then click **Next**.

- On the **Select Storage Policies** page, select **Farm Storage Policy** and then click **Next**.
- In the **Summary** page, review the details and click **Finish**.
- In the **Success** page, click **Close** to close the tab.
- In the **Advanced Storage Areas** tab, click **Refresh** and verify that the **ADV\_SA** is listed.

## Configure the storage devices.

In this task, you will change one of the storage devices to be the primary synchronous device. The storage device settings are configured with the defaults. You can change these settings on the Devices tab of the advanced storage area.

- In the **Advanced Storage Areas** tab, click the advanced storage area that you created (**ADV\_SA**).
- In the **ADV\_SA** tab, open the **Devices** subtab.
- For the **AFSD1** row, select **Primary synchronous** from the list and verify that the **AFSD2** row has the value: **Secondary synchronous**.

Device Replica Name	Device Replica Site	Device Replica Type	Deletion Method Supported	Default Synch Type
<input type="checkbox"/> AFSD1	Initial Site	File System Storage Device	Purge	Primary synchronous ▾
<input type="checkbox"/> AFSD2	Initial Site	File System Storage Device	Purge	Secondary synchronous ▾

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

## Edit the storage policy.

The Farm Storage Policy has three storage areas that are associated with it. You associated 2 of them when you created the storage area farms and the third one for the advanced storage area. You will remove the first two file storage areas to test the third one.

- From the **LoanProcessQA** tab, on the left pane, navigate to **Administrative > Storage > Storage Policies** and then click **Farm Storage Policy**.
- From the **Farm Storage Policy** tab on the right pane, scroll down, under the **Associated Storage Areas** section, select **FS1** and **FS2**, and then click **Remove**.
- Click **Save** to save the changes.
- Log out of the administration console and close the browser.

## Test the advanced storage area.

In this task, you will verify that adding a document (of Document class) to the system adds the content to the new file storage area.

- 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 **LoanProcessQA** from the list.
- On the left pane, click the **Test** folder under the **LoanProcessQA** object store.
- In **Windows Explorer**, navigate to **C:\Training\F2800G\SampleDocs**, select and drag all the files, and drop them to the IBM Content Navigator **Test** folder.

Note: Add all of the files, but not the subfolders.

In the Sample Desktop, the Add Documents page opens.

- In **Content Navigator** desktop, click **Add** to add all the files and wait for the upload to complete.
- Verify that the documents are listed in the **Test** folder and then log out of ICN **Sample Desktop** and close the browser.
- 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, expand the **Object Stores** folder and then click the **LoanProcessQA** object store.
- From the **LoanProcessQA** tab, on the left pane, expand **Administrative > Storage > Advanced Storage** node, and then click **Advanced Storage Areas**.
- From the **Advanced Storage Areas** tab, on the right pane, verify that **ADV\_SA** has some documents.

The Total Files column shows the number of documents that you added.

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

# Introduction to IBM FileNet P8 content services Containers

In this section, you will learn about the concepts of containers which provide a way to deploy a full IBM FileNet P8 Platform environment in a fraction of the time required for a standard on-premises installation.

## IBM FileNet P8 content services containers

V5.5.x introduces a new way to deploy an IBM FileNet P8 Platform environment by using Docker containers. You can deploy content services containers on an IBM Cloud Private environment or on a Kubernetes environment with a Docker server.

Containers allow you to package your application with libraries and any dependencies. They are isolated but share operating system (OS), and bins or libraries where applicable. Containers leverage host kernel and libraries to run the services. For example, Virtual Machines do not share OS (requires their own guest OS) or other resources (bins or libraries). Because of these factors, the Docker containers are lightweight. Since there is not much overhead, they startup very quickly.

Containers are:

- open source software development platform
- agnostic to container orchestration platform
- designed to persist data and configuration information outside of the container

This design allows the containers to be updated and upgraded without affecting the data

- packaged with enhanced monitoring components
- security hardened for cloud deployment
- portable, standardized, and faster to deploy
- architected for cloud deployment

They support Content Platform Engine clients by using Content Engine Web Services (CEWS) instead of EJB

- supported by cloud providers such as IBM Cloud, Amazon AWS, Microsoft Azure and Google Cloud
- supported by private cloud providers such as IBM Cloud Private, Pivotal (PKS), and RHEL OpenShift

## Benefits of containers

Deploying IBM FileNet P8 Platform components on a container platform provides the following benefits:

- Rapid deployment of components
- Improved patching and upgrading for components
- Dynamic scalability when running on the Kubernetes container platform
- Improved resiliency for your products

## Available containers for IBM FileNet P8 Platform

The following components are available as a container:

- Content Platform Engine
- Content Search Services
- IBM Content Navigator
- Content Management Interoperability Services (CMIS)

You can configure your Content Platform Engine and IBM Content Navigator container deployments to enable the sharing of content with users that are external to your organization. Configuration for this feature includes deploying an additional container to enable external sharing. Note that this feature is also available in a non-containerized environment.

In addition to these containers, the IBM Business Automation Configuration Container is also offered for deployments on IBM Cloud Private. When deployed, this container provides a configuration tool that offers a more streamlined configuration experience than other container deployment methods.

## Containers on IBM Cloud Private

IBM Cloud Private is an application platform for developing and managing on-premises, containerized applications. It is an integrated environment for managing containers that includes the container orchestrator Kubernetes, a private image registry, a management console, and monitoring frameworks.

## Considerations when choosing containers

Deploying FileNet P8 containers instead of an on-premises installation can be preferable in a number of possible scenarios. But there are also reasons to maintain a standard on-premises installation model.

If you have any of the following requirements, you might want to choose or maintain a standard on-premises installation:

- The platform and software choices that are currently not supported by the container platform
- Custom applications that use the Content Platform Engine EJB transport  
Containers supports Content Platform Engine clients by using Content Engine Web Services (CEWS) instead of EJB
- Applications that are integrated with IBM Content Navigator, such as IBM Enterprise Records, that are not yet available for container deployment.  
(At the time of writing this course, IBM Enterprise Records is not available for container deployment).
- A single IBM Content Navigator instance to connect to Content Manager on Demand (CMOD) and IBM Content Manager in addition to IBM FileNet P8 Platform  
Currently, only the IBM FileNet Content Manager repositories are supported in the container environment.
- Use of Content Platform Engine Virtual Member Manager directory configuration
- Use of the IBM Content Navigator Task Manager features, for example, Teamspace deletion or Box share
- Use of the Hitachi Fixed Content Device and IBM Spectrum Protect fixed content device for Content Platform Engine storage

## **Administering components in a container environment**

In most cases, administering your container environment for content services is the same as administering your on-premises environment. However, some variations exist for container environments.

Examples:

- Product logs are in a different location
- Startup and shutdown tasks are different
- Configuration files are in a different location

## Review Questions

**Question 1:** True or False: You can deploy FileNet P8 content services containers on an IBM Cloud Private environment

**Answer 1:** True

**Question 2:** Deploying the IBM FileNet P8 Platform components on a container platform provides which of the following benefits? (Select all that apply)

- A. Rapid deployment
- B. Improved patching and upgrading
- C. Dynamic scalability
- D. Improved resiliency

**Answer 2:** A, B, C, and D

Deploying the IBM FileNet P8 Platform components on a container platform provides rapid deployment, improved patching and upgrading, dynamic scalability, and improved resiliency

**Question 3:** True or False: FileNet P8 content services containers support Content Platform Engine clients by using Enterprise JavaBeans (EJB) transport

**Answer 3:** False

FileNet P8 content services containers support Content Platform Engine clients by using Content Engine Web Services (CEWS) transport

**Question 4:** In which of the following scenarios can you use container deployment for the IBM FileNet P8 Platform components? (Select one)

- A. You have custom applications that use the Content Platform Engine EJB transport
- B. You need to use IBM Enterprise Records application that is integrated with IBM Content Navigator
- C. You use a single IBM Content Navigator instance to connect to IBM Content Manager on Demand and IBM FileNet P8 Platform
- D. You use a single IBM Content Navigator instance to connect to IBM FileNet P8 Platform

**Answer 4:** D

FileNet P8 content services containers support CEWS transport

At the time of writing this course, IBM Enterprise Records and IBM Content Manager on Demand are not supported for containers.

# Organize content across the enterprise

In this section, you will learn about how content can be organized across the enterprise and isolated in an IBM FileNet P8 Platform system for multitenancy considerations.

## Multitenancy considerations

In a multitenancy scenario, a single instance of a software application serves multiple customers. When deciding on multitenancy for an IBM FileNet P8 Platform system, the following questions need to be addressed:

- Are customers willing to share hardware?
- What level of data isolation is required by the customers to ensure the safety and integrity of their data?
- What are the legal requirements regarding data protection and data location?  
For example, some countries require that personal data must only reside in the country of origin.  
Legal requirements can include retention management, formal records management, and data encryption for the data at rest.
- How similar are the needs of each customer for the following factors?
  - Application functionality
  - Number of users
  - The location and time zones of the users
  - Service level agreements for general system availability and for maintenance windows

## How does IBM FileNet P8 Platform fit with multitenancy needs?

Following are the main capabilities that make IBM FileNet P8 Platform work for multitenancy needs.

- Sizing the IBM FileNet P8 Platform environment
  - IBM FileNet P8 Platform is a modular architecture that can be expanded both vertically and horizontally
  - The environment can be expanded over time by adding additional hardware

- Data isolation
  - IBM FileNet P8 Platform provides flexibility for the physical location of content
  - Content can be stored on different file systems in the same physical location, as well as on different file systems in geographically diverse locations
- Security
  - Access to the IBM FileNet P8 Platform system depends on LDAP authentication
  - Access to the content in the system depends on LDAP authorization
  - Access to the system does not mean that you have access to any particular piece of content or the right to perform a certain task
  - Data that is stored can also be protected through a native data encryption capability
- System availability
  - IBM FileNet P8 Platform can support 24 x 7 availability
  - The system is configured for both high availability and disaster recovery
  - It is recommended to have known formal maintenance windows and to build processes that ensure all maintenance work can be performed in those windows

## **Isolating content in an IBM FileNet P8 Platform system**

Complete data isolation between clients can be achieved at the following levels:

- Highest level: P8 domain level
- Medium level: Object store level
- Lowest level: Within an object store

All environments, irrespective of the level of isolation, can be sized to meet the needs of an organization. There are advantages and disadvantages to all approaches. Higher level of separation reduces the need for some customizations whereas Lower level of separation reduces maintenance overhead. Different models will suit different organizational needs.

## **Isolating content with different P8 domains (Highest level)**

Recall the Content Platform Engine resources (P8 Domain) topic under the Architecture and domain structures heading that was presented earlier in this course.

The FileNet P8 domain represents a logical grouping of physical resources and the Content Platform Engine servers that provide access to those resources. Each resource and server belong to only one domain. A server can access any resource in the domain, but cannot access any resource that lies outside of the domain.

The Java Enterprise Edition security policy domain is used to authenticate users and establish their group memberships. The identity and group membership of the user determine which FileNet P8 domain objects the user can access.

A FileNet P8 domain can act like a closed system and the following components can be isolated:

- LDAP servers
- Database servers
- Application servers
- Storage areas

You can update or change all software levels without affecting any other customers and also set up different administrators for each P8 domain.

The disadvantage to this approach is that the shared resources are very minimal or none.

## **Isolating content with different Object stores (Medium level)**

An object store is a repository for storing objects (such as documents, folders, and business objects) and the metadata defining an object's classes and properties. A single FileNet P8 domain can contain one or many object stores. IBM Content Navigator (which is shipped with the product) is used to access and manage the content.

This level allows sharing of resources.

In a multitenant scenario, each customer:

- is assigned one or more object stores
- can share database servers, application servers, and storage areas
- can access the object store which is controlled through an LDAP group membership
- can use different access points for each object store.

For example, you can use separate Content Navigator servers or separate desktops within a single Content Navigator instance.

- can configure different administrators for each object store, but there is a single group that administers the Global Catalog Database (GCD) which stores the definition of the P8 domain

The disadvantage with this approach is that depending on how the environment is configured, some updates might affect all users. Customization is required to limit the display of users.

## **Isolating content within an object store (Lowest level)**

In a multitenant scenario:

- One or more customers share an object store
- Within an object store, you handle objects security through LDAP group membership
- You can set different access rights on documents, folders, and the structural elements that are used to define the documents and folders
- Each customer can either share the document storage or keep it isolated
- this level allows sharing of resources
- Each customer can have separate access at the Content Navigator level by creating their own unique desktop or Content Navigator instance
- Software updates will take the least amount of effort that is compared to the other configurations discussed in this section.

The disadvantage with this approach is that software updates will affect all customers. Customization is required to limit the display of users.

## Review Questions

**Question 1:** True or False: For IBM FileNet P8 Platform, the content can be stored on different file systems in the same physical location, as well as on different file systems in geographically diverse locations.

**Answer 1:** True

**Question 2:** In a FileNet P8 domain, which of the following components can be isolated? (Select all that apply)

- A. LDAP servers
- B. Database servers
- C. Application servers
- D. Storage areas

**Answer 2:** A, B, C, and D

In a FileNet P8 domain, LDAP servers, Database servers, Application servers, Storage areas can be isolated.

**Question 3:** True or False: If you have access to the IBM FileNet P8 Platform system, you can access any content and perform actions on any objects in the object store.

**Answer 3:** False

Access to the system does not mean that you have access to any particular piece of content or the right to perform a certain task. Access to the IBM FileNet P8 Platform system depends on LDAP authentication and access to the content in the system depends on LDAP authorization.

**Question 4:** Data isolation between clients can be achieved at which of the following levels? (Select two)

- A. P8 domain
- B. Object store
- C. Storage policy
- D. Isolated region

**Answer 4:** A & B

Data isolation between clients can be achieved at P8 domain or object store levels.