Contents

[1. FileNet P8 Architecture 3](#_Toc167190014)

[1.1 What we will cover in this training 4](#_Toc167190015)

[2. Content Platform Engine 4](#_Toc167190016)

[2.1 Walkthrough of Administration Console for Content Platform Engine 4](#_Toc167190017)

[2.1.1 Domain 4](#_Toc167190018)

[2.1.2 Object Store 4](#_Toc167190019)

[2.1.3 Exploring Classes 4](#_Toc167190020)

[2.2 Security 4](#_Toc167190021)

[2.2.1 ACE/ACL (Access Control Entry/Access Control List) 4](#_Toc167190022)

[2.2.3 Role – based access control (RBAC) 5](#_Toc167190023)

[2.2.4 Security Inheritance (Security Proxy) 5](#_Toc167190024)

[2.2.5 Marking Sets 5](#_Toc167190025)

[2.2.6 Security Policies 5](#_Toc167190026)

[2.3 Document Class 5](#_Toc167190027)

[2.3.1 Creation of Property Templates 5](#_Toc167190028)

[2.3.2 Creation of Document Class 5](#_Toc167190029)

[2.3.3 Adding Property Definitions to the Document Class 5](#_Toc167190030)

[2.3.4 Checking the Security 5](#_Toc167190031)

[2.3.5 Creating a Document Instance 5](#_Toc167190032)

[2.3.5 Versioning of Documents 5](#_Toc167190033)

[2.3.6 Implementing Security Proxy 5](#_Toc167190034)

[2.3.7 Implementing Marking Sets 5](#_Toc167190035)

[2.3.8 Implementing RBAC 7](#_Toc167190036)

[2.3.9 Implementing Security Policy 11](#_Toc167190037)

[2.4 Events and Subscriptions 11](#_Toc167190038)

[2.4.1. Introduction 11](#_Toc167190039)

[2.4.2 Creating the Code Module 11](#_Toc167190040)

[2.4.3 Creating the Event Action 11](#_Toc167190041)

[2.4.4 Creating the Subscription 11](#_Toc167190042)

[2.4.5 Testing the Event Action 11](#_Toc167190043)

[2.5 Search Objects in Content Engine 11](#_Toc167190044)

[2.5.1 How to do Object Store Search 11](#_Toc167190045)

[2.5.2 How to do Bulk actions 11](#_Toc167190046)

[2.6 Audit History 11](#_Toc167190047)

[2.6.1 Introduction 11](#_Toc167190048)

[2.6.2 How to Configure and view Audit History in FileNet 11](#_Toc167190049)

[2.7 Sweep Jobs 12](#_Toc167190050)

[2.7.1 Background Search Sweep 12](#_Toc167190051)

[2.8 Content Engine Java API 12](#_Toc167190052)

[2.8.1 Setting up Eclipse 12](#_Toc167190053)

[2.8.2 Creating a FileNet Connection 12](#_Toc167190054)

[2.8.3 Working with Documents 12](#_Toc167190055)

[3. IBM Content Navigator 12](#_Toc167190056)

[3.1 Introduction to Navigator 12](#_Toc167190057)

[3.2 Walkthrough to Navigator Admin desktop 12](#_Toc167190058)

[3.3. Development in Navigator 12](#_Toc167190059)

[3.3.1 Creation of Object Store repositories 12](#_Toc167190060)

[3.3.2 Creation of Desktops 12](#_Toc167190061)

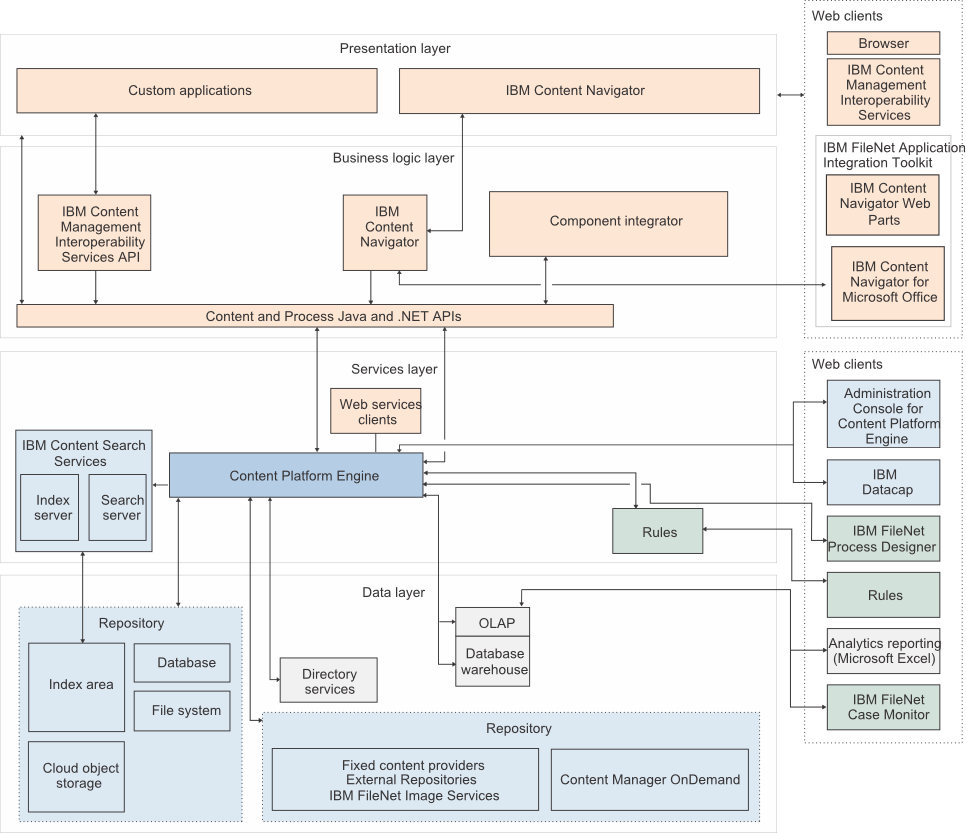
[3.4 Navigator Customizations 12](#_Toc167190062)

[4. IBM Case Manager 12](#_Toc167190063)

IBM FileNet Training

# FileNet P8 Architecture

The FileNet P8 family of products includes back-end services, development tools, and applications that address enterprise content and process management requirements



## What we will cover in this training

The below components we will cover as part of this training

* + 1. **Content Platform Engine (CPE)**
    2. **IBM Navigator**
    3. **IBM Case Manager**

# Content Platform Engine

## 2.1 Walkthrough of Administration Console for Content Platform Engine

### 2.1.1 Domain

### 2.1.2 Object Store

### 2.1.3 Exploring Classes

## 2.2 Security

The Content Engine resides within a Java Platform, Enterprise Edition (Java EE) application server, and uses the Java Authentication and Authorization (JAAS) standard as the basis for authentication. The JAAS programming model is a standard Java framework that manages authentication and authorization.

### 2.2.1 ACE/ACL (Access Control Entry/Access Control List)

**ACE Source:** Every ACE has a source, either Default,Direct, Inherited or Template.

* + 1. **Default:** Permissions are placed on an object by the Default instance security ACL of its class, as well as permissions placed on a sub classs by its parent class. Default ACEs are directly editable. If you do, its source type becomes Direct.
    2. **Direct:** Permissions are added directly to an object. Direct ACEs are directly editable
    3. **Inherited:** Permissions are placed on the object by a security parent or by setting up a relationship with an object-value property whose security proxy type has been set to Inherited. Inherited ACEs are not directly editable.

Example: ***Security Proxy Concept***

* + 1. **Template:** Permissions are placed on the object by a security policy. Template ACEs are not directly editable and do not appear on classes. Rather, a document, folder, or custom object class can have a default security policy which will pass template ACEs to the instances of the class, if all the conditions for the template apply.

Example**:** ***Security Policy Concept***

### 2.2.3 Role – based access control (RBAC)

You can create roles in your object store as another way to grant access to objects. Role-based access depends on three facets of authorization

* What access does the role grant?
* Who, meaning which users or groups, are the members of this role?
* Which objects can be accessed by members of this role

Using roles can simply security in some cases because you can update the role parameters, such a members or what kind of access the role has, without having to update all the objects to which members of the role have access.

### 2.2.4 Security Inheritance (Security Proxy)

### 2.2.5 Marking Sets

### 2.2.6 Security Policies

## 2.3 Document Class

### 2.3.1 Creation of Property Templates

### 2.3.2 Creation of Document Class

### 2.3.3 Adding Property Definitions to the Document Class

### 2.3.4 Checking the Security

### 2.3.5 Creating a Document Instance

### 2.3.5 Versioning of Documents

### 2.3.6 Implementing Security Proxy

### 2.3.7 Implementing Marking Sets

1: WHO Guidelines:

-> Document Title (default property)

-> Country Name -> (India, USA)

-> Severity

india users group

usa users group

-> Default Instance Security :

-> Marking set : can be used with the help of property template only

-> Security Proxy: can be used with the help of property template only

Marking security consists of the Add marking, Remove marking, and Use Marked Objects.

**Add marking and Remove marking**

A user with Add rights to a marking can set the property value associated with the marking, if it has not been set. Only those markings to which the user has Add rights will show in the list of marking values ​​available to be set in a property. A user with Remove rights to a marking can remove the marking value.

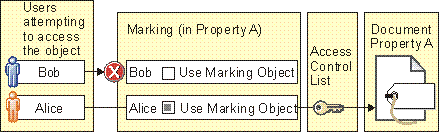
For example:

1. A Document has a property associated with a marking set. No value has been specified for the property.
2. The marking set has markings Red, Blue, and Green.
3. Alice has Use rights to Red; Use and Add rights to Blue and Use, Add and Remove rights to Green.

When Alice views the Document properties, she can set the property value to Blue or Green but not Red. If the property was set to Green, she could alter it to be Blue. If the property was set to Blue, Alice would be unable to alter the property's value.

**Use Marked Objects**

Use right determines whether the presence of the marking on an object constrains access to that object. If the user has Use right to the marking, access to the object will not be constrained.



In this example, Alice has the Use Marked Objects access right which lets her bypass the marking. Her access to the object will be evaluated by the object's ACL. Bob does not have Use Marked Objects and therefore will neither see nor have access to the object, regardless of any permissions the object's ACL might grant him.

Markings and marking sets are Content Platform Engine objects, each with a class description:

* Markings are objects that combine metadata behavior with access control behavior in a way that allows an object's access control to change by changing a property value.
* Marking sets have containers for markings. Marking sets are associated with a Property Template which can then be used to add a property to one or more classes.

Implementation:

Lets assume we have country property on a Covid Guidelines document class, and assume

We have 2 countries

* + 1. India ( intuser1 is the user belongs to india country )
    2. USA ( lucy is the user belongs to USA )

We have one admin user p8 admin:

Scenario: Now whatever Covid Guide lines document created for which country depending on the those country specific users only should be able to see that document.

Lets Achieve this using Marking set

1. Create a Marking Set named “Country Marking”
2. Give two marking india and usa
3. Add the appropriate users to the specific markings and save the marking
4. Create a property template named “Country “ and map the marking set
5. Assign the property template to Covid Guidelines document class
6. Create an instance and test the Marking set security

### 2.3.8 Implementing RBAC

You use the Administration Console for Content Platform Engine to create and assign security roles for you content objects.

When you use role-based access, you create and configure role classes and subclasses, then create instances of the roles. You can associate these role instances with the objects that you want to secure.

Use the following steps to configure role-based access:

1. [**Creating a role class**](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psh028.htm)  
   You use the Administration Console for Content Platform Engine to create role classes.

Roles are created as subclasses under the Role class. You choose whether to create a subclass of the Static Role class or the Dynamic role class:

**Static Role**

In a static role, users and groups are assigned directly to a role. This method is similar to how ACLs are assigned to an object.

**Dynamic Role**

In a dynamic role, external code is used to determine if a user if a member of a role. This method allows for more dynamic role assignments based on application use cases. The external code returns a yes or no response as to whether the specified user is a member of the dynamic role.

**Procedure**

To create a role class:

1. In Administration Console for Content Platform Engine, expand **Data Design** > **Classes** > **Other Classes** > **Role**.
2. Right click the type of role class that you want to create, **Dynamic** or **Static**, and click **New Class**.
   1. Role classes are hierarchical, which means that you can create new roles under existing roles. If you are creating the role class to add to an existing set of roles, choose the appropriate subclass as the parent for your new class.
3. Enter a name and description for the new role.
4. Click **Finish**, then click **Open** to refine your role definition.
   1. Add or remove access definitions by choosing a class and choosing which types of access the role has for that class.
   2. **Tip:** If the tab for defining access definitions does not display, refresh the view.
5. Save your changes.
6. [**Creating a role instance**](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psh029.htm)  
   After you create the role class, you use the Administration Console for Content Platform Engine to create a role instance for the object store.

You use an instance of a security role to grant the access defined by the role to a specific set of users and groups. You can create an instance of your security role in the Data Design section of the Administration Console for Content Platform Engine.

**Procedure**

To create a role instance:

1. In Administration Console for Content Platform Engine, navigate to the object store where you want to create the instance, expand the object store, and click **Roles**.
2. Right click the type of role instance that you want to create, **Dynamic** or **Static**, and click **New Role**.
3. Enter a value for the **Display name**, and choose the role class that is the basis for your new role instance.
4. On the **Role Members** tab, add role members.

You can add users and groups directly, add a realm, or add a nested role.

1. Click **Finish** to save your role instance.

**Results**

The created role instance:

* Includes the users and groups that the role class contains, plus any that were added specifically to the instance
* Grants the permissions to the specified classes (for example, Documents) that you configured on the role class
* Grants additional permissions that you specified for the instance. You can use the **Role Access Definitions** tab to specify additional permissions (access rights). For more information, see topic [About access rights](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psa050.htm).

1. [**Associating a role instance with an object**](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psh030.htm)  
   After you create a role instance, you assign this role instance to an object to secure the object with role-based access control.
2. [**Creating a dynamic role**](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.security.doc/p8psh031.htm)  
   A dynamic role enables custom code to make the determination of whether a given user is to be considered as a member of the role, versus that determination being made solely on the basis of a stored list of members. The custom code might, for example, consult an external database to answer the question of membership.

In this procedure, you create and compile a java class. You can use an editor and your Java SDK to create and compile the class. The rest of the steps for creating the code module, the role membership action, the dynamic role class, and the dynamic role, are completed in the Administration Console for Content Platform Engine.

**Procedure**

1. Create a java file that describes the dynamic role:

package com.sampleclass;

import com.filenet.api.admin.CmRoleMembershipAction;

import com.filenet.api.engine.AuthorizationServices;

import com.filenet.api.engine.RoleMembershipHandler;

import com.filenet.api.security.CmDynamicRole;

import com.filenet.api.security.User;

public class RoleMembershipHandlerImpl implements RoleMembershipHandler {

@Override

public boolean isUserInRole(CmRoleMembershipAction arg0,

CmDynamicRole arg1, User arg2, AuthorizationServices arg3) {

System.out.println("in RoleMembershipHandlerImpl.isUserInRole()");

return false;

}

}

1. Use your Java SDK to compile the file into a Java class, for example, com.sampleclass.RoleMembershipHandlerImpl.class.
2. Save the Java class file to a location that can be accessed by your Content Platform Engine server.
3. In the Administration Console for Content Platform Engine, open the object store where you want to add the Dynamic Role.
4. Navigate to **Browse** > **Root folder**, and right-click **Code Modules**.
5. Click **Actions**, and click **New Document**.
6. On the **Define New Document Object** panel, provide a title, click **Select Class as Code Module**, and click **Next**.
7. Click **Add**, browse to the Java class file that you created, and click **Add Content Element**.
8. Click **Next** to accept the default values in the rest of the wizard, then click **Finish**.
9. In the Object Store view, navigate to and expand **Events, Actions, Processes**, then right-click **Role Membership Actions** and click **New**.
10. On the **New Role Membership Action** screen, click **Class**, and for the **Java class handler value**, enter the name of your newly created Java class, for example, com.sampleclass.RoleMembershipHandlerImpl.class.
11. Click **Configure code module**, then click **Next**.
12. Click **Load Existing**, select the code module that you just created, and click **OK**.
13. Click **Next** and **Finish**.
14. In the Object Store view, navigate to **Data Design** > **Classes** > **Other Classes** > **Role** > **Dynamic Role**.
15. Right-click **Dynamic Role** and click **New**.
16. Provide a name and other details for your new Dynamic Role class.
17. Select the **Role Membership Action** that you just created.
18. Click **Next** and **Finish**.
19. In the Object Store view, navigate to **Roles** > **Dynamic Roles**.
20. Right-click **Dynamic Roles**, click New, and create the dynamic role by using the class that you just created.

### 2.3.9 Implementing Security Policy

## 2.4 Events and Subscriptions

### 2.4.1. Introduction

### 2.4.2 Creating the Code Module

### 2.4.3 Creating the Event Action

### 2.4.4 Creating the Subscription

### 2.4.5 Testing the Event Action

## 2.5 Search Objects in Content Engine

### 2.5.1 How to do Object Store Search

### 2.5.2 How to do Bulk actions

## 2.6 Audit History

### 2.6.1 Introduction

Audit History is used to store the event information of the Document, Folders and objects in FileNet P8. With Audit History, one can view historical changes to documents in a FileNet Content Manager repository.

* In IBM ACCE, Audit history is for all types of items like documents, folders and objects.
* In IBM Content Navigator, Audit history is for document only ( can see the document related audit history )

### 2.6.2 How to Configure and view Audit History in FileNet

**In ACCE:**

1. First, need to make the property “Enable Audit History to Yes on the Object Store

2. Go to the respective document class, where you want to enable the audit history tab and then create an Audit definition by choosing what are all the events you want to audit and save it.

3. Then create a document and trigger the respective events which you have configured and then go that document and go the Audit History tab and see whether it is updated or not

**In IBM Content Navigator:**

1. Go to the respective object store repository and enable the “Document History” setting
2. Do the same in Desktop level as well
3. Then go to respective document in the navigator and open properties and see the history tab

## 2.7 Sweep Jobs

### 2.7.1 Background Search Sweep

To create a background search query, you create a template and a template-based sweep. Multiple sweeps can be created from the same template.

**Before you begin**

If you want the search results of your query to be downloadable as a CSV file, install the Reporting Enablement Extensions add-on for the object store. For information about installing add-ons, see [Installing an add-on feature to an object store](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/featureaddons/fa_install_addon.htm#fa_install_addon). For information about other ways that search results can be exported to a CSV file, see [Search result processing](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc381.htm#p8pcc381).

**About this task**

The template primarily consists of three interrelated elements:

* The search expression
* Parameter properties
* Search result properties

You specify parameter values when the sweep is created from the template. Also, when you create the sweep, you can limit the number of search results for query testing purposes.

**Important:** Some configuration such as creating database indexes might be necessary to prevent your background search queries from running slowly. For more information, see [Tuning Content Platform Engine background searches](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.performance.doc/p8ppt030.htm).

**Procedure**

To create a background search query:

1. Start the New Background Search Class Template wizard in the administration console:
   1. In the domain navigation pane, select the object store.
   2. In the object store navigation pane, select the **Data Design** > **Background Search Class Templates** folder.
   3. On the Background Search Class Templates tab, click **New**.
2. Complete the wizard:
   1. Enter a search expression.
   2. As necessary, edit the attributes of the custom property templates that the wizard creates automatically for parameters and search results.
   3. Optional: Select the **Generate a CSV file** option. The wizard displays this option only if the Reporting Enablement Extensions add-on is installed.
3. [Generating search results with a background search sweep](https://www.ibm.com/docs/en/SSNW2F_5.5.0/com.ibm.p8.ce.admin.tasks.doc/p8pcc382.htm#p8pcc382). Create a template-based sweep.

## 2.8 Content Engine Java API

### 2.8.1 Setting up Eclipse

### 2.8.2 Creating a FileNet Connection

### 2.8.3 Working with Documents

# 3. IBM Content Navigator

## 3.1 Introduction to Navigator

## 3.2 Walkthrough to Navigator Admin desktop

## 3.3. Development in Navigator

### 3.3.1 Creation of Object Store repositories

### 3.3.2 Creation of Desktops

## 3.4 Navigator Customizations

# 4. IBM Case Manager