Course Exercises Guide

IBM FileNet Content Manager 5.2.1: Security

Course code F283 ERC 1.0

IBM Training

August 2016 edition

Notices

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

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

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

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

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

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

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

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

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

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

Trademarks

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

Contents

Trademarks

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

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

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

DB2®
FileNet®
Redbooks®
Tivoli®
WebSphere®

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

VMware and the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks (the "Marks") of VMware, Inc. in the United States and/or other jurisdictions.

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

Exercises description

This course includes the following exercises:

- "Resolve access issues" on page 1-1
- "Modify direct security" on page 2-1
- "Configure object store security" on page 3-1
- "Configure class and property security" on page 4-1
- "Configure security inheritance" on page 5-1

Student system

Exercises in this course require that you have access to a student system on which is installed the software that you are learning.

- If you are taking this course as part of a self-paced online course (SPVC), you must start the student system that is provided by the SPVC provider.
- If you are taking this course as part of an instructor-led training (ILT) program, your instructor can show you how to access your student system.

Conventions used in this course

These guidelines can help you complete the exercises faster.

- Most exercises include required sections which should always be completed. It might be necessary to complete these sections before you can start later exercises. Some exercises might also include optional sections that you might want to complete if you have sufficient time and want an extra challenge.
- `Code font` indicates information that you must type.
- *Italics font* indicates a variable. Substitute a literal value where indicated.
- As you progress through the materials, the lesson instructions become less verbose. You can refer back to earlier examples of procedures if you forget the steps.
- Data tables are used throughout this course. After you learn to perform the steps of a procedure, you can complete the exercise by using the data they provide.
- If a value is not specified in a data table, then the value is already correctly configured by default. Do not change it.

Most exercises include required sections, which should always be completed. It might be necessary to complete these sections before you can start later exercises. If you have sufficient time and want an extra challenge, some exercises might also include optional sections that you can complete.

Exercise 1. Resolve access issues

Objectives

After completing this exercise, you should be able to:

- Resolve logon failure.
- Verify object store access.

Overview

This exercise shows how to resolve typical security access issues.

Estimated time

00:30

Introduction

In this exercise, you simulate a problem with the authentication provider and then observe the results.

Requirements

You must have access to a student system that is configured for these activities. If you are taking this course as a self-paced virtual course (SPVC), ensure that your student system is started.

System start

To start your system:

1. Open the WebSphere Admin folder on your desktop.
2. Double-click Start Server1.bat.
3. Wait for the command window to close.

For more information about starting, stopping, and verifying the system status, refer to Appendix A, "Start and Stop System Components," on page A-1.

Exercise Introduction

Why is this lesson important?

IBM FileNet Content Manager uses an LDAP provider for authentication. Users cannot log in if the LDAP provider service is not running, or the Content Platform Engine cannot connect to the LDAP provider.

Activities

User accounts

Application Name	User ID	Password
Operating System	Administrator	passw0rd
IBM Content Navigator	p8admin	IBMFileNetP8
IBM Content Navigator	carol	filenet

1.1. Resolve login failure

Introduction

In this activity you observe the effects of an LDAP service connection failure.

Scenario

Carol attempts to log on to IBM Content Navigator but receives an error. You track the issue down to the connection with the LDAP provider.

Procedures

Procedure 1, "Stop the authentication provider," on page 1-3

Procedure 2, "Observe logon failure," on page 1-3

Procedure 3, "Observe object store access," on page 1-4

Procedure 4, "Create a user," on page 1-4

Procedure 5, "Log on to IBM Content Navigator as outsider," on page 1-6

Procedure 1: Stop the authentication provider

You stop the service that provides authentication information to the web application server and then observe the effects on the users who attempt to log on.

1. On the desktop of your student system, click Start > Services.
2. Select IBM Tivoli Directory Server Instance V6.3 - dsrdbm01
3. Stop the service.

Procedure 2: Observe logon failure

Carol, a user, complains that she cannot log on to the system. You need to determine the reason. Assume that you have already eliminated the possibility that her account information is wrong.

1. Use Firefox to log on to IBM Content Navigator as carol:
   - http://ecmedu01:9080/navigator
   - User name: carol
   - Password: filenet
2. Verify that you get an error with the logon that indicates the wrong username or password was used.
3. Verify that the Content Platform Engine is running by going to the CE Ping Page.
   - http://ecmedu01:9080/FileNet/Engine

Note

The ping page is up. You have verified that the Content Platform Engine is running. You can check the log files to find out what happened.

4. Copy the location of the log files from the CE Ping page.
5. Using Windows Explorer, open the p8_server_error.log file from this location:
   - C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\FileNet\server1
6. Search the log files for any errors that relate to connectivity to the LDAP provider.
7. Use Windows Services console to restart IBM Tivoli Directory Server Instance V6.3 - dsrdbm01.

Procedure 3: Observe object store access

Object stores are usually secured by using group memberships. Users who have access to object stores can log on and use the object stores. In addition, when a user logs on to IBM Content Navigator, the desktop must have the object store configured as a repository for that desktop.

1. Log on to IBM Content Navigator as carol:
   - http://ecmedu01:9080/navigator
   - User name: `carol`
   - Password: `filenet`
2. Verify that you can see the following object stores in the repository menu:
   - LoanProcess
   - Sales
   - LoanProcessQA
   - SalesQA
3. Attempt to open each of the object stores from the object stores menu.
4. Verify that carol is denied access to LoanProcess.
5. Log out of IBM Content Navigator.

Procedure 4: Create a user

A user must have permission on at least one object store in order to log on to an IBM FileNet Content Manager client. However, if an object store is configured so that #AUTHENTICATED USERS have access, then anyone who can log in to the domain can have access. You are going to create a user for testing system security.

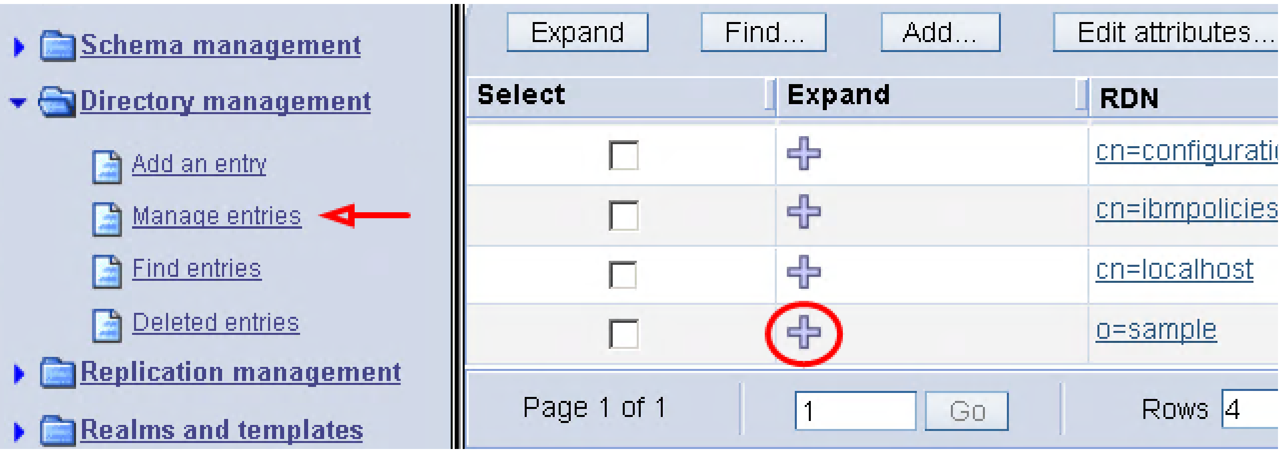
1. Use Internet Explorer to go to the Tivoli Directory Service Web Administration Tool.
   - http://localhost:9080/IDSWebApp/
   - User DN: cn=`root`

- Password: `IBMFileNetP8`

Troubleshooting

If you get a website security certificate error, select the Continue to this website option, then click Yes.

2. In the navigation pane, expand Directory Management > Manage entries.
3. In the details area, expand o=sample by clicking the plus (+) sign.



4. Expand cn=users.
5. Click Add to add a user.
6. In the Select object class window, do the following steps:
   a. Select inetOrgPerson from the Structural object class menu.
   b. Click Next.

Note

You use inetOrgPerson to match the other entries in LDAP.

7. On the Select auxiliary object classes page, click Next.
8. On the Required Attributes page, enter the following information, and then click Next:
   - Relative DN: `cn=outsider`
   - Parent DN: `cn=users,o=sample`
   - cn: `outsider`
   - sn: `outsider`
9. On the Optional Attributes page, do the following steps:
   a. Scroll down to the bottom of the page.

   b. Enter a value for userPassword: `filenet`

   c. Click Finish.

   d. Click No to add a similar entry.

10. Log out of Tivoli Directory Service Web Administration Tool.

Procedure 5: Log on to IBM Content Navigator as outsider

1. Attempt to log on to IBM Content Navigator as outsider:
   - http://ecmedu01:9080/navigator
   - User name: outsider
   - Password: filenet
2. Verify that you cannot log on.

Information

Outsider does not have access to the object stores defined for the default user desktop. A user must have access to the object store that IBM Content Navigator uses for authentication to log on. In some cases, an authorization problem might appear to be an authentication problem.

1.2. Verify object store access

Users have access to different sets of object stores. In this exercise, you log in to IBM Content Navigator with different accounts to see how security affects which object stores you can access.

Procedures

Procedure 1, "Log in as different users," on page 1-7

Procedure 2, "Review object store security," on page 1-7

Procedure 1: Log in as different users

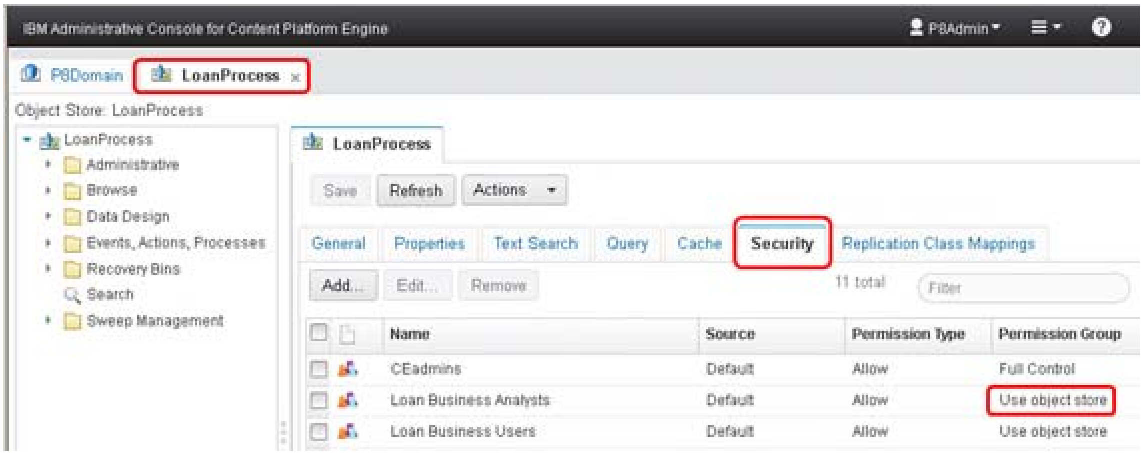
1. Log on to IBM Content Navigator as amy:
   - http://ecmedu01:9080/navigator
   - User name: amy
   - Password: filenet
2. Select each object store.
3. Observe whether the object store is visible or whether an error occurs.
4. Repeat the procedure with the remaining users. The password for each user is filenet.

- allen
- peadmin
- linda

Procedure 2: Review object store security

1. Log on to Administration Console for Content Platform Engine:
   - http://ecmedu01:9080/acce/ (or use the ACCE shortcut)/
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Open the Security tab for each object store.

3. Review the list of users and groups with permission to use the object store.



Name	Source	Permission Type	Permission Group
CEadmins	Default	Allow	Full Control
Loan Business Analysts	Default	Allow	Use object store
Loan Business Users	Default	Allow	Use object store

4. Log out of Administration Console for Content Platform Engine.

5. Close the browser.

End of exercise

Exercise review and wrap-up

In this lesson, you did the following tasks:

- Resolved logon failure from stopped authentication system.
- Observed logon failure from failed object store authorization.
- Observed object store security.

Exercise 2. Modify direct security

Estimated time

00:30

Overview

This exercise covers how to modify direct security on objects.

Objectives

After completing this exercise, you should be able to:

- Change direct security on a document.
- Change ownership of a document.
- Customize document access.

Introduction

In this exercise, you modify direct security on objects in an object store.

Requirements

Your student system is already started.

Exercise Introduction

Why is this lesson important?

Users with sufficient authorization can change the direct security on documents. This is particularly true with the owner of the document. You are going to change security of a document.

Activities

Change direct security of a document, on page 2-3

Customize access, on page 2-9

User accounts

	Type	User ID	Password
	Operating system	Administrator	passw0rd
	P8 Domain	p8admin	IBMFileNetP8
	Finance clerk	Carol	filenet
	Finance clerk	Charles	filenet

Note

Passwords are always case-sensitive.

2.1. Change direct security of a document

Introduction

In this exercise, you create a document as one user in order to observe default instance security. You then modify the security directly and observe the results.

Procedures

Procedure 1: Add a folder and document

You create a document and then change security on it.

1. Log on to IBM Content Navigator as carol:
   - http://ecmedu01:9080/navigator
   - User name: `carol`
   - Password: `filenet`
2. Open the LoanProcessQA object store.
3. Create a folder:
   a. Click New Folder.
   b. Name the folder Loandocs.
   c. Click Add.
4. Open the Loandocs folder.
5. Create a document:
   a. Click Add Document.
   b. For the document content, select any file from Libraries\Documents\sample documents.
   c. Click Add.
6. Log out of IBM Content Navigator.

Procedure 2: Verify access

1. Log on to IBM Content Navigator as charles.
   - User name: `charles`
   - Password: `filenet`
2. Open the LoanProcessQA object store.
3. Open the Loandocs folder.
4. Select the file.
5. Verify that you can see and download the document.
   a. Click Actions > Download > As original.
   b. Open the file.
   c. Close the file.
6. Log out of IBM Content Navigator.

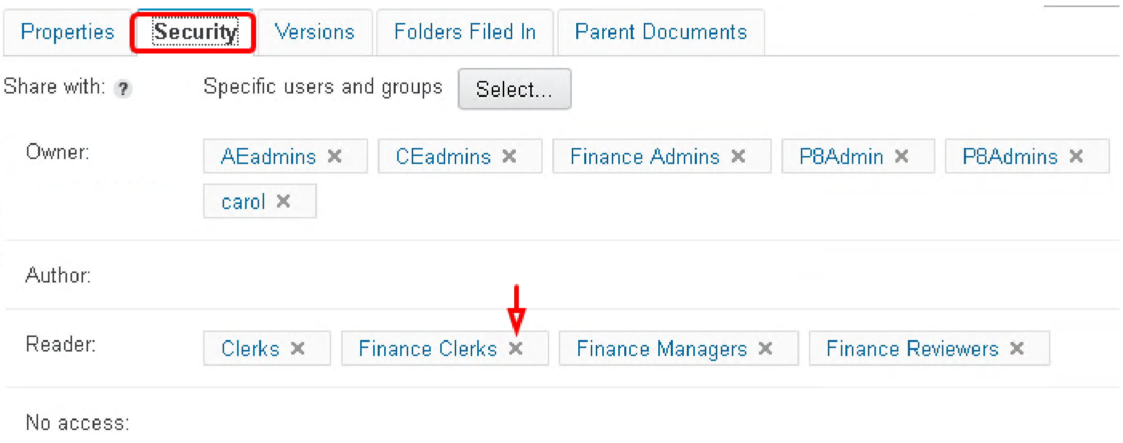
Procedure 3: Remove group access to a document

1. Log on to IBM Content Navigator as carol.
   - User name: `carol`
   - Password: `filenet`
2. Open the LoanProcessQA object store.
3. Open the Loandocs folder.
4. Open the properties of the document by clicking Action > Properties.
5. Open the Security tab.
6. Verify the following settings:

Access group	Members
Owners	AEAdmins CEAdmins Finance Admins P8Admin P8Admins carol
Readers	Clerks Finance Clerks Finance Managers Finance Reviewers

7. Remove the permission for Finance Clerks to read the document.

   a. Click the X on the Finance Clerks group.



Share with: ? Specific users and groups

Owner: AEadmins ✕ CEadmins ✕ Finance Admins ✕ P8Admin ✕ P8Admins ✕ carol ✕

Author:

Reader: Clerks ✕ Finance Clerks ✕ Finance Managers ✕ Finance Reviewers ✕

No access:

   b. Click Save.

8. Log out of IBM Content Navigator.

Procedure 4: Verify that access is removed

Carol has removed access to the document to Finance Clerks. Other Finance clerks, such as Charles, should no longer see the document. However, Carol still has access. You are going to verify these statements.

1. Log on to IBM Content Navigator as Charles.
   - User name: `charles`
   - Password: `filenet`
2. Go to LoanProcessQA > Loandocs.
3. Verify that the folder is empty.

Note

This security configuration is an example of implicit denial. When a user has no permissions, the document is not visible.

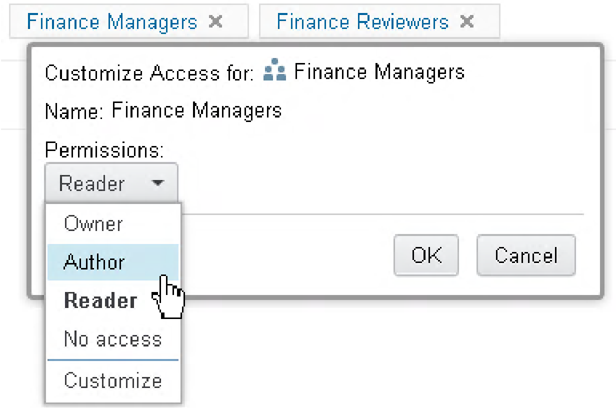
4. Log out of IBM Content Navigator.

Procedure 5: Change access level

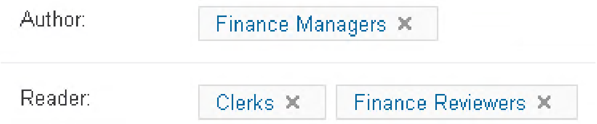
Finance Managers should be authors of the document. As an owner, Carol can change access levels.

1. Log on to IBM Content Navigator as Carol.
   - User name: `carol`
   - Password: `filenet`

2. Go to LoanProcessQA > Loandocs.
3. Open the document Properties page.
4. Open the Security tab.
5. Click Finance Managers.
6. Select Author from the Permissions menu.



7. Click OK.
8. Verify that Finance Managers are now in the Authors group.



9. Click Save.

Procedure 6: Remove ownership

Carol removed Finance Clerks from the document Readers. Other Finance Clerks can no longer access the document. However, Carol can still access the document. To find out what happens when Carol removes herself from the document owners, you remove Carol from the ACL. You are logged on to IBM Content Navigator as Carol. You are in the Loandocs folder of the LoanProcessQA object store.

1. Open the Security tab for the document.
2. Remove carol from the Owners group.
3. Click Save. Verify that you can still see the file.
4. Log out of IBM Content Navigator.

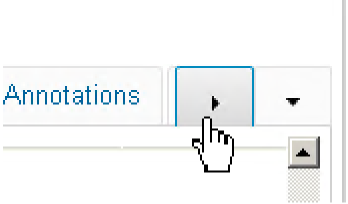
Note

You might think that Carol’s continued access to the file is caused by browser caching or some other glitch. It is not, but you can test this hypothesis if you want. You can clear the browser history and re-open folder. The document is still visible.

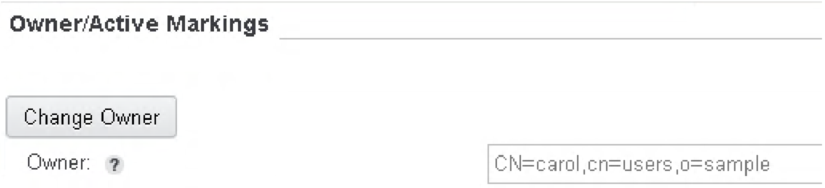
Procedure 7: Change ownership

You removed Finance Clerks and Carol from the document's ACL. However, Carol can still see it. To find out why she can still see it, you must use Administration Console for Content Platform Engine to investigate.

1. Use Firefox to log on to Administration Console for Content Platform Engine:
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Go to LoanProcessQA > Browse > Root Folder > Loandocs.
3. Open the document properties by clicking the document link.
4. Scroll the tabs to the right to open the Security tab.



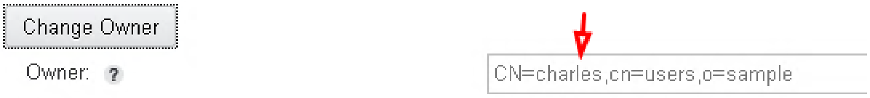
5. Verify that Carol is still the owner.
   a. Scroll down the page to the Owner/Active Markings area.
   b. Confirm that the Owner is CN=carol, cn=users,o=sample.


Owner/Active Markings

Change Owner

Owner: ? CN=carol,cn=users,o=sample

6. Change the owner to Charles:
   a. Click Change Owner.
   b. Select the *Change Owner to* option.
   c. Click Find.
   d. Search for Charles.
   e. Select Charles and click the right-facing arrow.
   f. Click OK.
   g. Verify that Charles is now the owner.


Change Owner

Owner: ? CN=charles,cn=users,o=sample

7. Click Save.
8. Log out of Administration Console for Content Platform Engine.

Information

The Owner of a document is not the same thing as a member of the Owner role in the ACL. The Owner of an object has implicit READ, WRITE_OWNER and WRITE_ACL privileges no matter what is in the object's ACL.

These implicit rights can be lost by marking sets.

Procedure 8: Verify the change in ownership

1. Verify that Charles can see the document:
   a. Log on to IBM Content Navigator as Charles.
   b. Go to LoanProcessQA > Loandocs.
   c. Verify that you can see the document.
   d. Log out of IBM Content Navigator.
2. Verify that Carol cannot see the document:
   a. Log on to IBM Content Navigator as Carol.
   b. Go to LoanProcessQA > Loandocs.
   c. Verify that you cannot see the document.
3. Log out of IBM Content Navigator.

2.2. Customize access

Introduction

In IBM Content Navigator, you can specify security on a document or folder by using predefined security roles, including:

- Owner
- Author
- Reader
- No access

Each of these groups has a predefined set of access rights.

In Administration Console for Content Platform Engine, you can specify security by using predefined Permission Groups. These groups are similar to, but not identical to the roles in IBM Content Navigator. The groups include:

- Full Control
- Minor versioning
- major versioning
- Modify properties
- View content
- View properties
- Publish
- Create subfolder
- Custom

In this exercise, you are going to see how to use Permission Groups for common security scenarios, and specify custom permissions for fine-grained security configurations.

Procedures

Procedure 1, "Add typical document permissions," on page 2-9

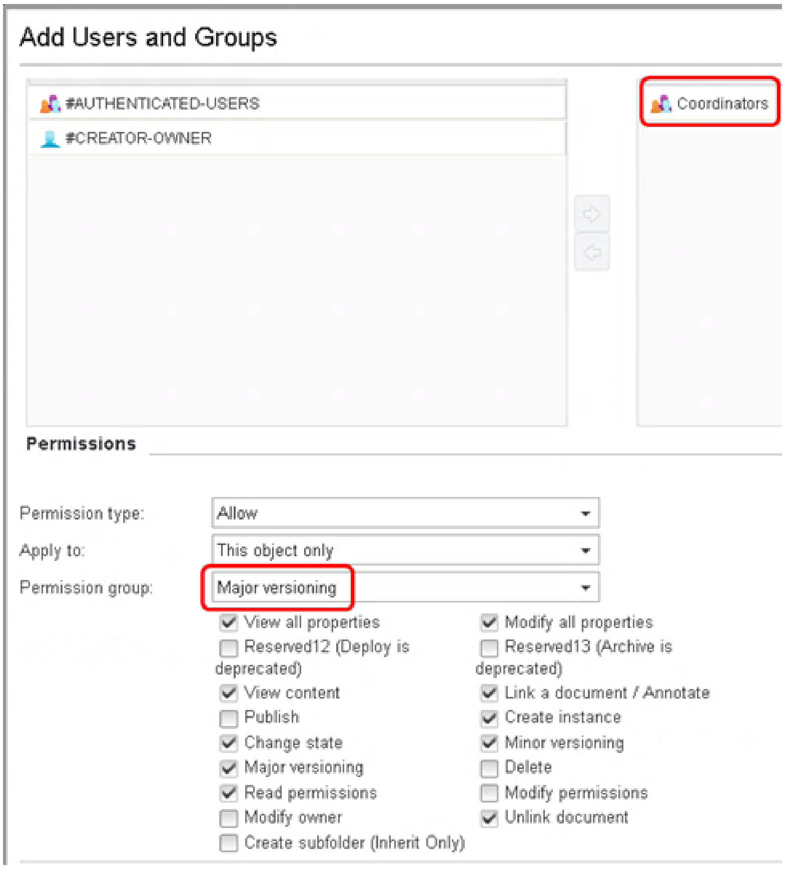
Procedure 2, "Edit security settings," on page 2-11

Procedure 1: Add typical document permissions

You create a document and then modify permissions for different security principals by using the predefined Permission Groups.

1. Log on to Administration Console for Content Platform Engine as p8admin.
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`

2. Open the LoanProcessQA object store.
3. Go to Browse > Root Folder.
4. Use the Actions menu to create a folder that is named `Access Test`.
5. Add a document to this folder, by using one of the files in Libraries\Documents\sample documents as a content element.
   a. Click Actions > New Document.
   b. Name the document anything that you want.
   c. Click Add to add a content element.
   d. Browse to select a document from Libraries\Documents\sample documents.
   e. Complete the wizard by clicking Next and Finish to add the document with default values.
   f. Click Open to open the properties of the document.
6. On the document properties page, open the Security tab.
7. Add Major Versioning permission to Coordinators.
   a. Click Add.
   b. Search for Coordinators.
   c. Add Coordinators to Selected Users and groups.
   d. Select Major Versioning from the Permission group menu.



Add Users and Groups

#AUTHENTICATED-USERS

#CREATOR-OWNER

Coordinators

Permissions

Permission type: Allow

Apply to: This object only

Permission group: Major versioning

☑ View all properties

□ Reserved12 (Deploy is deprecated)

☑ View content

□ Publish

☑ Change state

☑ Major versioning

☑ Read permissions

□ Modify owner

□ Create subfolder (Inherit Only)

☑ Modify all properties

□ Reserved13 (Archive is deprecated)

☑ Link a document / Annotate

☑ Create instance

☑ Minor versioning

□ Delete

□ Modify permissions

☑ Unlink document

Troubleshooting

If all the rights do not show, logout and log back in to retry.

e. Verify that the following individual permissions are selected:

- View all properties
- View content
- Change state
- Major versioning
- Read permissions
- Modify all properties
- Link a document/Annotate
- Create instance
- Minor versioning
- Unlink document

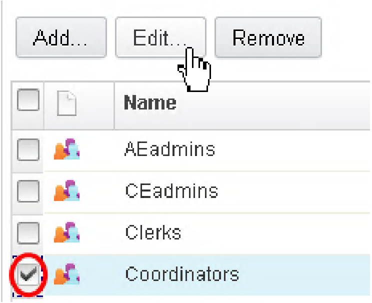
f. Click OK.

8. Click Save.

Procedure 2: Edit security settings

The Major Versioning Permission group has permissions that are not quite what you need. You do not want coordinators to be able to unlink a document. You can specify security more precisely by setting custom permissions. You are logged on to Administration Console for Content Platform Engine as p8admin. You are viewing document properties.

1. Select the Coordinators row.



☐		Name
☐		AEadmins
☐		CEadmins
☐		Clerks
☑		Coordinators

2. Click Edit.

3. Clear the Unlink document permission.

4. Click OK.

5. Click Save.

6. Verify that the Permission group for Coordinators is now Custom.

7. Log out of Administration Console for Content Platform Engine.

End of Exercise

Exercise review and wrap-up

In this lesson, you completed the following tasks:

- Observed the effects of implicit denial.
- Modified direct security on a document.
- Changed the owner of a document.
- Customized user permissions on a document.
- Observed the effects of implicit denial.

Exercise 3. Configure object store security

Estimated time

00:40

Overview

This exercise covers how to configure security on a new object store, how to manage object store access, and how to update the security on an object store by using the Security Script Wizard.

Objectives

After completing this exercise, you should be able to:

- Configure security on a new object store.
- Add an object store to an IBM Content Navigator desktop.
- Use supergroups to manage object store access.
- Use the Security Script wizard to update security on an object store.

Introduction

In this exercise, you create an object store and configure security on it.

Requirements

Your student system is already started. You have completed the previous exercises in this course.

Exercise Introduction

Why is this lesson important?

Your IBM FileNet P8 solution design identifies specific security requirements for the object store that is used in the business solution. A solution builder must implement these security requirements. Document security begins with object store security. Correctly configured object store security can make the difference between a security schema that is effective and flexible and one that must be constantly worked around.

Activities

Configure Initial Object Store Security, on page 3-3

Add groups to an object store by using a supergroup, on page 3-16

Use the Security Script wizard, on page 3-20

User accounts

	Type	User ID	Password
	Operating system	Administrator	passw0rd
	P8 Domain	p8admin	IBMFileNetP8
	Legal user	Larry	filenet
	unauthorized authenticated user	outsider	filenet
	Finance Admin	Adam	filenet
	Finance Admin	Allison	filenet
	Grouptest	Grouptester	filenet
	Scriptest	Scriptester	filenet

Note

Passwords are always case-sensitive.

3.1. Configure Initial Object Store Security

Introduction

In this exercise, you create an object store. You specify security on the object store so that all P8 users (but not all authenticated users) can see it.

This exercise provides a challenge and a walkthrough.

If you are familiar with object store creation, you can skip the walkthrough.

Important

You must complete this exercise to continue the lesson exercises.

Scenario

The Finance department needs an object store for its operations. All P8 users must have default access to the object store. You can further configure security on objects within the object store later.

Procedures

Procedure 1, "Create an object store," on page 3-3

Procedure 2, "Verify the new object store," on page 3-6

Procedure 1: Create an object store

1. In Firefox, sign in to Administration Console as p8admin:
   - http://ecmedu01:9080/acce/ (or use the ACCE bookmark).
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Open the New Object Store wizard.
   a. In the Administration Console, click the P8Domain > Object Stores node on the left pane.
   b. In the Object Stores tab on the right pane, click New.
   c. The New Object Stores tab opens.
3. Name the Object Store.
   a. Enter `Finance` as the value for the Display name field.

      The Symbolic name field is automatically populated with the same name.
   b. Optionally, enter a description to your object store.
   c. Click Next.

4. Define the database:

   a. Select FNOSDS from the list for the database connection field.

   b. Enter Finance for the Schema name field.

   c. Leave the default values (no value) for the other fields.

   d. Click Next.

5. On the Select the Type of Storage Area for Content page, click Next.

6. Grant Administrative Access.

   a. Click Add. The Add Users and Groups window opens.

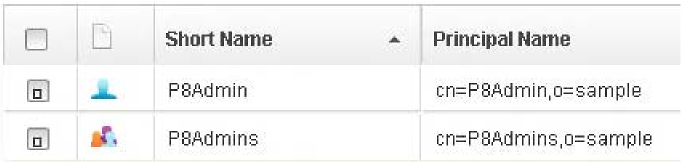
   b. In the Search for field, clear the Search for Users and Search for Special accounts check boxes. Leave Search for Groups selected.

   c. Type P8 in the field that is next to the Starts with field. Click Search.

   d. In the Search Results section > Available Users and Groups column, a list of groups that starts with P8 is listed.

   e. Select and Move P8Admins to the Selected Users and Groups column by clicking the right-facing arrow. Click OK.

   f. Verify your administrators.



□		Short Name ▲	Principal Name
▫		P8Admin	cn=P8Admin,o=sample
▫		P8Admins	cn=P8Admins,o=sample

   g. Click Next.

7. Grant Basic Access.

   a. Click Add on the Grant Basic Access page.

   b. Add the P8Users group.

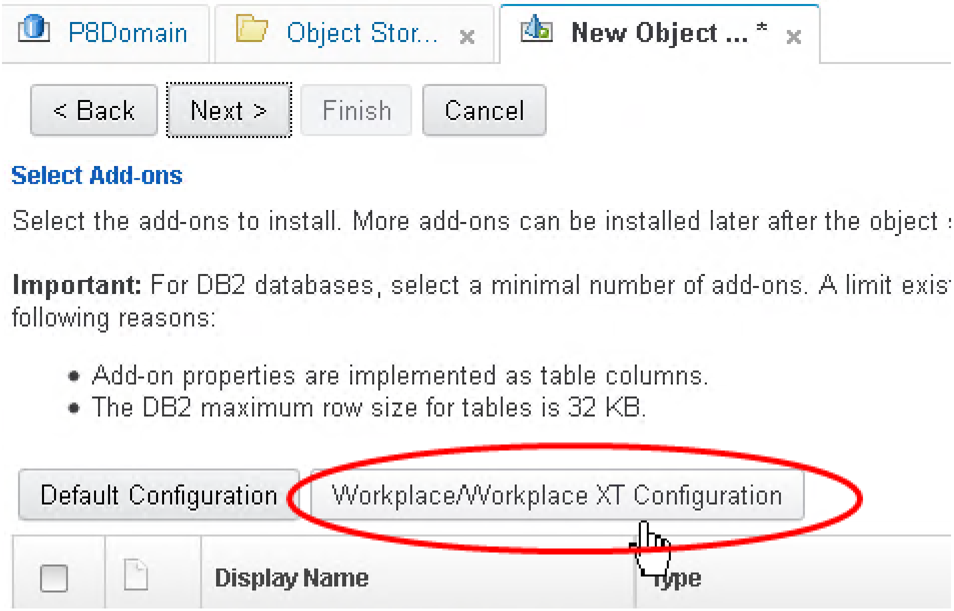
Note

If you specify an empty list, the wizard automatically adds #AUTHENTICATED-USER, which gives all network users in the authentication realm access to the object store. Unless you want anyone who can log in to automatically access this object store, you must specify a group.

   c. Click Next.

8. Select AddOns.

   a. Click the Workplace/WorkplaceXT Configuration button.



Select Add-ons

Select the add-ons to install. More add-ons can be installed later after the object :

Important: For DB2 databases, select a minimal number of add-ons. A limit exis following reasons:

- Add-on properties are implemented as table columns.
- The DB2 maximum row size for tables is 32 KB.

Information

Although FileNet Workplace XT is no longer used, the add-ons are still required for property definitions to be configured properly. The Workplace/Workplace XT Configuration button selects the following add-ons.

- 5.2.1 Base Content Engine Extensions
- 5.2.1 Process Engine Extensions
- 5.2.1 Publshing Extensions
- 5.2.1 Workplace Access Role Extensions
- 5.2.1 Workplace Base Extensions
- 5.2.1 Workplace E-mail Extensions
- 5.2.1 Workplace Forms Extensions
- 5.2.1 Workplace Template Extensions"
- 5.2.1 Workplace XT Extensions

   b. Click Next.

9. Complete the wizard:

   a. In the Summary page, review your selections.

   b. Click Finish to create the object store.

Note

The process might take a few minutes.

If a message states that the script is unresponsive, click OK to continue.

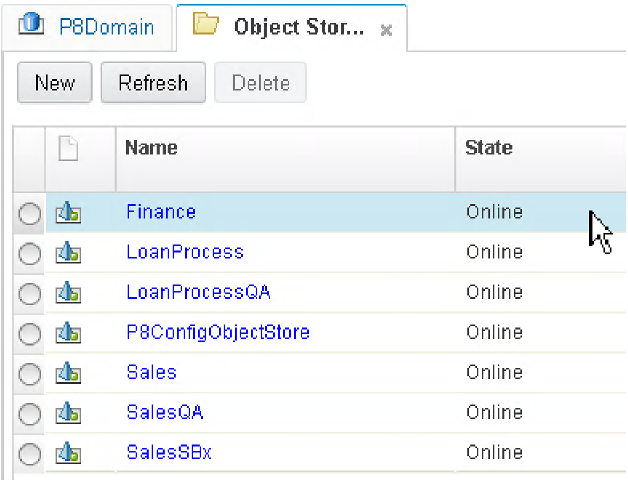
c. In the Success page, click Close.

Procedure 2: Verify the new object store

In this procedure, you verify that the object store has correct security settings.

1. In the Administration Console > Object Stores tab, click Refresh.

   a. Verify that the new object store is listed.



	Name	State
○	Finance	Online
○	LoanProcess	Online
○	LoanProcessQA	Online
○	P8ConfigObjectStore	Online
○	Sales	Online
○	SalesQA	Online
○	SalesSBx	Online

   b. Click to open the Finance object store.

   c. Open the Security tab.

   d. Verify the following access settings:

Name	Permission group
P8Admins	Full Control
P8Users	Use object store
P8Admin	Full Control

2. Log out of Administration Console for Content Platform Engine, and close the browser.

3.2. Modify Root Folder Security

Introduction

The initial security on the object store allows P8users to use the object store. However, you want to restrict who can add folders at the root level. This permission must be given only to Finance Administrators.

Scenario

You created an object store. The object store currently allows all P8 users default permission (Use object store). Any users can currently add documents and folders to the Root folder. In order to restrict the right to organize the top folders, you must remove this access. You must also create the folders in which Finance users can create subfolders.

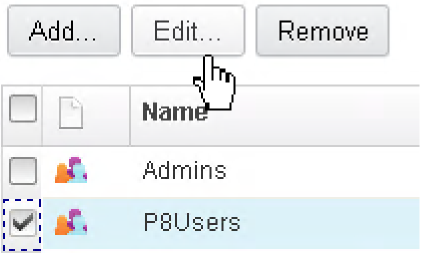
Procedures

Procedure 1: Edit Root Folder security

Restrict general Root Folder permissions but give special permissions to the Finance Admins group.

1. Use Firefox to log on to Administration Console for Content Platform Engine:
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Open the Finance object store.
3. Expand the Browse node.
4. Open the properties page for the Root Folder.
5. Open the Security tab for Root Folder.
6. Edit the P8Users access control entry:
   a. Select the P8users entry.

b. Click Edit.



☐		Name
☐		Admins
☑		P8Users

c. In the Permission group menu, select View Properties.

d. Click OK.

e. Click Save.

7. Provide Finance Admins with Root Folder access:

a. Click Add.

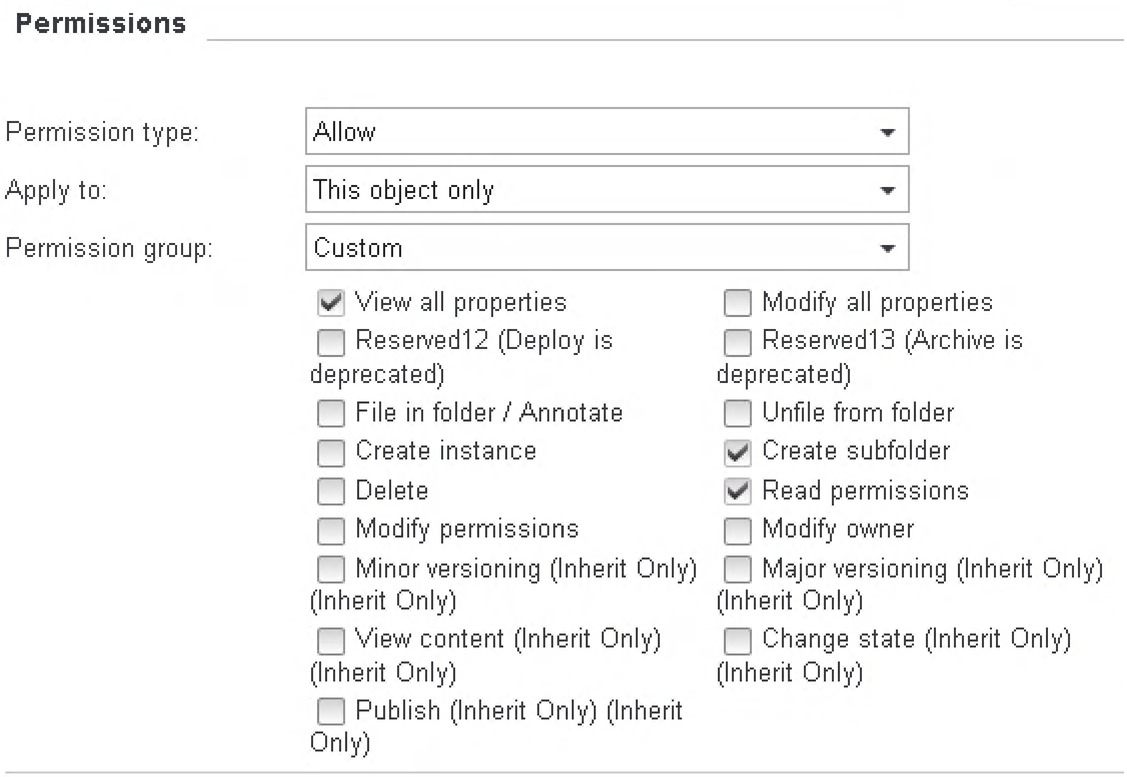
b. Search for Finance Admins.

c. Add Finance Admins group to the Selected Users and Groups.

d. Select *This Object Only* from the *Apply To* field.

e. Select the View Properties Permission group.

f. Add the Create Subfolder custom permission.


Permissions

Permission type: Allow

Apply to: This object only

Permission group: Custom

☑ View all properties	☐ Modify all properties
☐ Reserved12 (Deploy is deprecated)	☐ Reserved13 (Archive is deprecated)
☐ File in folder / Annotate	☐ Unfile from folder
☐ Create instance	☑ Create subfolder
☐ Delete	☑ Read permissions
☐ Modify permissions	☐ Modify owner
☐ Minor versioning (Inherit Only) (Inherit Only)	☐ Major versioning (Inherit Only) (Inherit Only)
☐ View content (Inherit Only) (Inherit Only)	☐ Change state (Inherit Only) (Inherit Only)
☐ Publish (Inherit Only) (Inherit Only)	

g. Click OK.

8. Click Save to save the changes on the Root Folder.

9. Log out of Administration Console for Content Platform Engine.

Information

Finance Admins are now allowed to add subfolders to the Root Folder. Finance Admins can then specify security on the folders that they create.

Procedure 2: Configure your repository

Users access and add content to your object store in IBM Content Navigator.

To access the content in an IBM FileNet P8 repository, you must first configure IBM Content Navigator to connect to that repository.

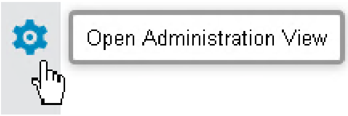
Then, you must associate this repository with a desktop to enable users to access the content.

In this procedure, you configure the repository that recently created.

1. Log in to IBM Content Navigator.

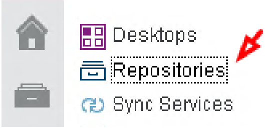
- `http://ecmedu01:9080/navigator/` (or use the Content Navigator shortcut).
- User name: `P8Admin`
- Password: `IBMFileNetP8`

2. On the Content Navigator desktop, click the Open Administration View icon in the leftmost pane.



3. Open the Repositories tab.

   a. In the Administration View page, click Repositories in the left pane.



   b. On the Repositories tab, a list of the repositories that are configured is shown.

4. Create a connection to your repository.

   a. Click New Repository and select FileNet Content Manager from the list.

   b. Enter the values shown in the table.

Table 1.

Property	Value
DIsplay Name	Finance
Server URL	iiop://ecmedu01:2809/FileNet/Engine

Table 1.

Property	Value
Object store symbolic name	Finance
Object store display name	Finance

Information

Your server name is ecmedu01.

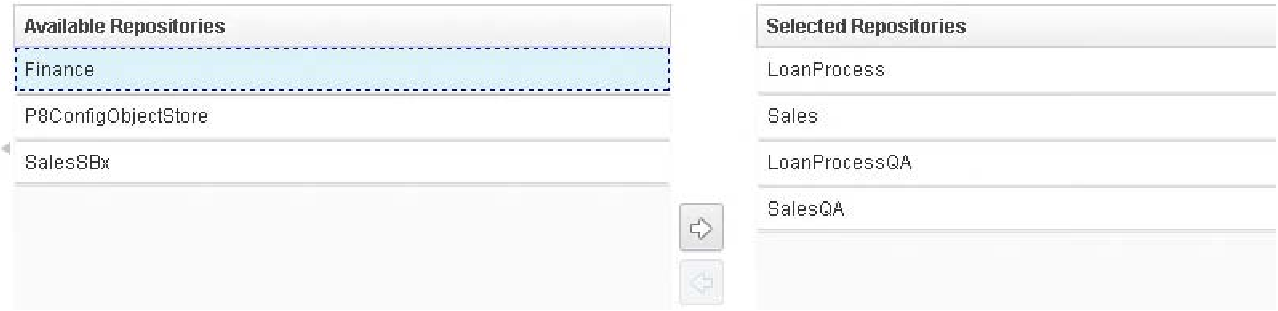
5. Test the connection to the repository.
   a. Click Connect.
   b. In the Log In page, enter the credentials of a user with administrator access to the repository (User: `P8admin`; password: `IBMFileNetP8`).
   c. Click Log In.
6. Save the configuration settings for the new repository.
   a. Click Save and Close to save and close the New Repository tab.
7. Test the new repository.
   a. Verify that the new repository is listed on the Repositories tab. Click Refresh if you do not see it.
   b. This repository is now available to be used in the Content Navigator.
   c. Close the Repositories tab.

Procedure 3: Edit the desktop to add your repository

In this procedure, you associate your repository with a desktop.

1. In the Admin desktop page > Desktops tab, right-click Sample Desktop and click Edit.
   a. In the Sample Desktop tab, click the Repositories subtab.

2. Specify the repository for the desktop.
   a. In the Repositories tab, Select `Finance` repository from the Available Repositories pane and use the right arrow (Add) to move it to the Selected Repositories pane.



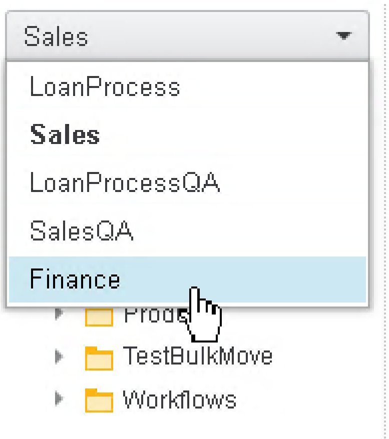
   b. Click Save and Close.
   c. Click OK to close the message to refresh your browser.
3. Log out of IBM Content Navigator.
4. Close Firefox.

Procedure 4: Verify the repository

1. Start Firefox.
2. Sign in to IBM Content Navigator as Adam.

- `http://ecmedu01:9080/navigator/` (or use the Content Navigator shortcut).
- User name: `Adam`
- Password: `filenet`

3. Open the Finance object store.

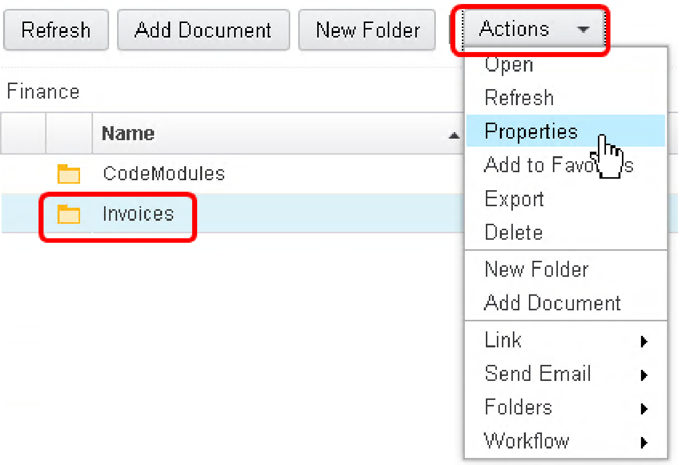


Procedure 5: Add a folder for Finance group

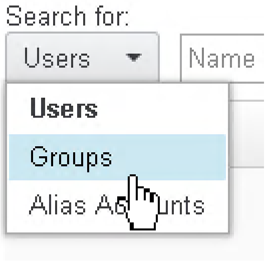
Users in the various Finance groups need to be able to add folders and documents, but they can be allowed to do this only in designated subfolders. As the P8 administrator, you gave the Finance

Admin group permission to add subfolders to the Root Folder. You are logged in to IBM Content Navigator as Adam, a Finance Admin member. The Finance object store is open.

1. Create a subfolder that is named Invoices.
2. Add Finance groups to the folder permissions:
   a. Select the Invoices folder.
   b. Click Actions > Properties.

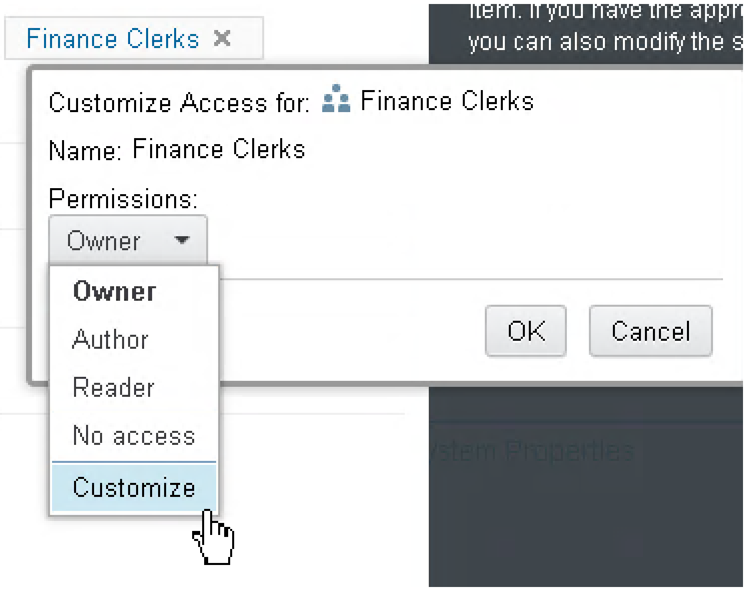


   c. Open the Security tab.
   d. Click Select.
   e. Select Groups from the *Search For* menu.



   f. Search for Finance groups.
   g. Select all Finance groups by holding the shift key and selecting the first and last group.
   h. Select Reader permissions.
   i. Click Add.
3. Edit the permissions for each group:
   a. Click Finance Admins.
   b. Select Owner and then click OK.
   c. Click Finance Clerks.

d. Select Customize from the Permissions menu.



Customize Access for: Finance Clerks

Name: Finance Clerks

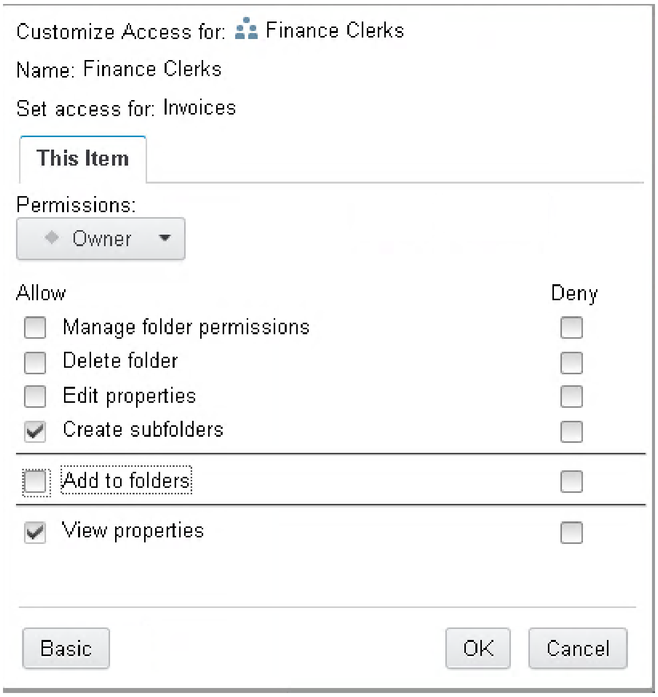
Permissions: Owner

e. Click Advanced.

f. Select Create subfolders.

g. Clear the *Add to folders* permission.

h. Review the Finance Clerk permissions.



Customize Access for: Finance Clerks

Name: Finance Clerks

Set access for: Invoices

This Item

Permissions: Owner

Allow	Deny
□ Manage folder permissions	□
□ Delete folder	□
□ Edit properties	□
☑ Create subfolders	□
□ Add to folders	□
☑ View properties	□

i. Click OK.

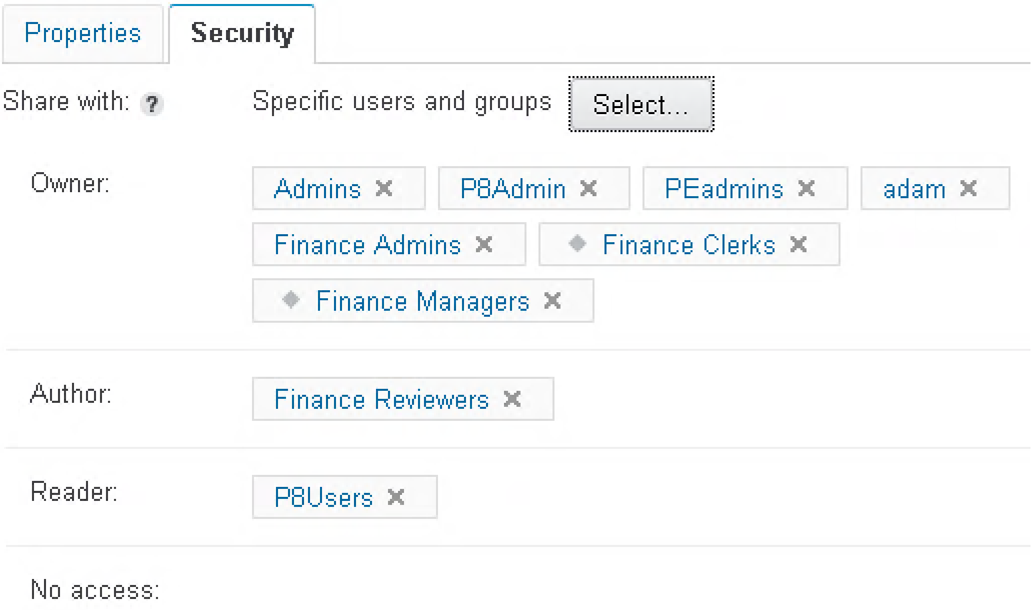
Note

The Owner button has a diamond icon to indicate that it has Advanced permissions.

j. Use this data to configure permissions for the remaining Finance groups:

Group	Permission type	Access Level or permissions
Finance Admins	Basic	Owner
Finance Clerks	Advanced	Create subfolders
Finance Managers	Advanced	Create Subfolders Add to folder
Finance Reviewers	Basic	Author

k. Verify the completed folder permissions:



Share with: ? Specific users and groups

Owner: Admins ✕ P8Admin ✕ PEadmins ✕ adam ✕ Finance Admins ✕ ◆ Finance Clerks ✕ ◆ Finance Managers ✕

Author: Finance Reviewers ✕

Reader: P8Users ✕

No access:

l. Click Save.

4. Log out of IBM Content Navigator.

Procedure 6: Verify folder access

As an administrator, you can check the folder security settings in the Administration Console.

1. Log in to Administration Console:

- http://ecmedu01:9080/acce/ (or use the ACCE bookmark).
- User name: `p8admin`
- Password: `IBMFileNetP8`

2. Open the Finance object store.

3. Expand Browse > Root Folder.

4. Select the Invoices folder.
5. Open the Security tab.
6. Inspect the Finance Admins permissions:
    a. Select security principal by checking the box, then click Edit.
    b. In the Edit Permissions window, inspect the permissions, then click Cancel.
    c. Clear the check box.
7. Inspect the permissions for the other Finance groups to verify that each group has the correct permissions.

Group	Permissions
Finance Admins	View all properties Reserved12 File in folder Create instance Delete Modify permissions Modify all properties Reserved 13 Unfile from folder Create subfolder Read permissions Modify owner Change state
Finance Clerks	View all properties Create subfolder Read permissions
Finance Managers	View all properties File in folder Unfile from folder Create subfolder Read permissions
Finance Reviewers	View all properties File in folder Unfile from folder Read permissions

8. If any group does not have the correct permissions, you can correct them here.
9. Log out of Administration Console.

3.3. Add groups to an object store by using a supergroup

Introduction

You might have to add group access to new groups that did not exist when you first created the object store. When you add groups to the object store when it is created, those groups have default access to all objects on the object store. Users who are added to the object store later do not automatically get the same permissions on existing objects. Therefore new users do not automatically have full access to the object store.

You can add groups to an existing object store in either of two ways:

- By using supergroups.
- By using the security script wizard.

In this lesson, you are going to practice both methods.

Procedures

Procedure 1, "Download the Security Wizard Script files," on page 3-20

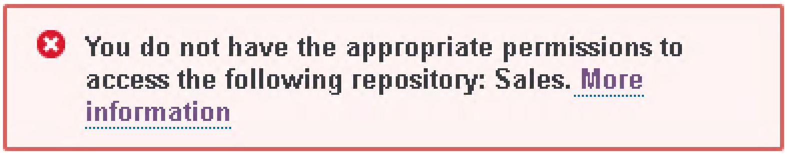
Procedure 2, "Run the Security Script Wizard," on page 3-21

Procedure 3, "Test object store access," on page 3-22

Procedure 1: Test the accounts

Grouptester and Scriptester are two accounts in the LDAP directory. They belong to the Grouptest and Scriptest groups. Although they are authenticated users, they do not have access to any object store.

1. Use Firefox to try to log on to IBM Content Navigator as grouptester.
   - URL: http://ecmedu01:9080/navigator (or use the Content Navigator bookmark).
   - User name: `grouptester`
   - Password: `filenet`
2. Verify that you are not allowed to log on.



You do not have the appropriate permissions to access the following repository: Sales. More information

Note

IBM Content Navigator uses the Sales object store to authenticate, so users who do not have access to Sales receive an error.

3. Test the scriptester account as well. The password is filenet.
4. Log on to Administration Console as grouptester.
   - URL: http://ecmedu01:9080/acce (or use the ACCE bookmark).
   - User name: `grouptester`
   - Password: `filenet`
5. Explore Administration Console for Content Platform Engine.

Information

Although you can log in to the Administration Console, your actions and views are limited. P8ConfigObjectStore and SalesSBx object stores allow access to all authenticated users.

6. Log out of Administration Console for Content Platform Engine.
7. Close the browser.

Optional

You might think that by adding Grouptester to the Sales object store, you can solve your access problems. It is not that simple, however, because basic object store access does not provide any additional permissions on existing objects.

To see for yourself, you can try this experiment to see the results.

1. As P8admin, log into Administration Console.
2. Open the Sales object store.
3. Add Grouptester to the Sales object store with Use Object Store permission group.
4. Attempt to log into IBM Content Navigator as Grouptester.
5. Observe the effects.
6. When you are finished exploring, use the Administration Console to remove Grouptester from the Sales object store.

Procedure 2: Add a group to the P8Users group

The easiest way to add users and groups to an object store is to add them to an existing group that already has access. Several object stores are configured with the P8Users supergroup. By adding a group to the supergroup, you can instantly provide them default access to these object stores.

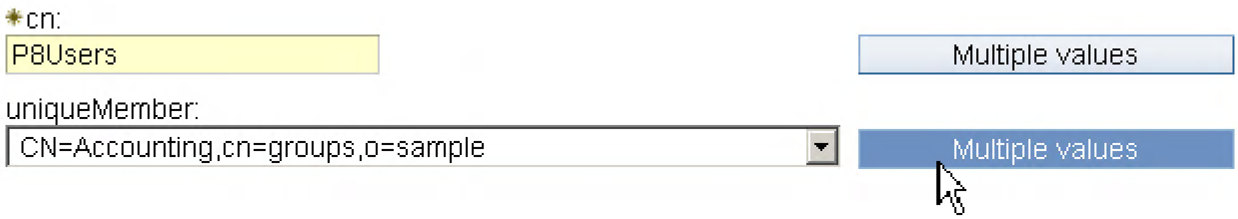
1. In Firefox, go to the Tivoli Directory Service Web Administration Tool.
   - http://localhost:9080/IDSWebApp/
   - User DN: `cn=root`
   - Password: `IBMFileNetP8`

2. In the navigation pane, expand Directory Management > Manage entries.
3. In the details area, expand o=sample by clicking the plus (+) sign.
4. Expand cn=groups.
5. Find the P8Users group.

Hint

To find P8Users, you might need to scroll down and advance to the next page by using the arrows.

6. Click the group title to open it.
7. Add the grouptest group:
   a. Click Multiple Values next to the uniqueMember field.



*cn: P8Users

uniqueMember: CN=Accounting,cn=groups,o=sample

   b. In the uniqueMember field, type: `CN=grouptest,cn=groups,o=sample`

Hint

Entries are case-sensitive.

   c. Click Add.
   d. Click OK at the bottom of the page.
   e. Click Next on the Edit an entry page.
   f. Click Finish.
8. Log out of Tivoli Directory Service Web Administration Tool.

Procedure 3: Retest grouptester

1. Clear the Firefox browser cache.
   a. In the Tools bar, click History > Clear Recent History.
   b. Click Clear Now.
2. Use Firefox to log on to IBM Content Navigator as grouptester.
   - User name: `grouptester`
   - Password: `filenet`

3. Verify that you can see the following object stores:
    - LoanProcess
    - Sales
    - LoanProcessQA
    - SalesQA
    - Finance

Troubleshooting

If you cannot see these object stores, log out, wait about a minute and try again (The User Security Cache TTL needs time to refresh).

4. Log out of IBM Content Navigator.

3.4. Use the Security Script wizard

Introduction

If you need to add a group of users to an object store, and you do not have an established group to add them to, then you can use the Security Script Wizard. The Security Script wizard allows you to assign security roles to user and group accounts in order to create security principals for the objects in an object store. You must run the Security Script Wizard on each object store to which you are adding the accounts.

Important

Be cautious about running the SecurityUpdate script. This script updates an object store's set of administrator groups and regular users. It makes wholesale changes to the Default Instance Permissions settings of many class definitions and also changes the security permissions of all folders. After running it you must remake your Default Instance Permissions changes and possibly redo the security for your folders.

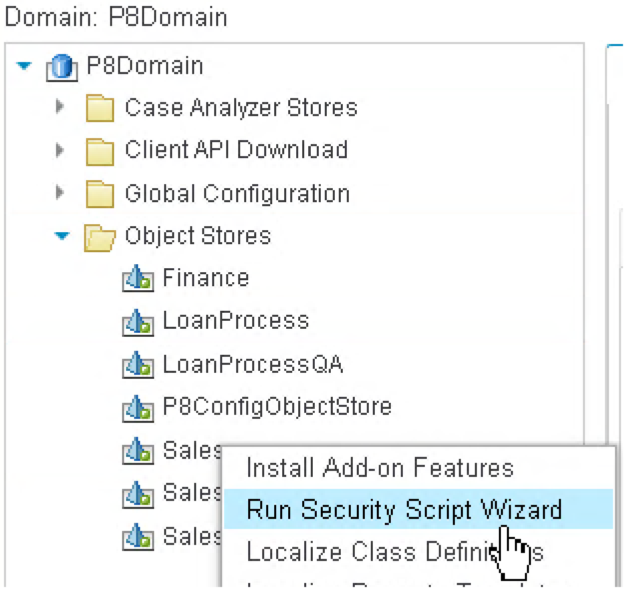
Procedures

Procedure 1: Download the Security Wizard Script files

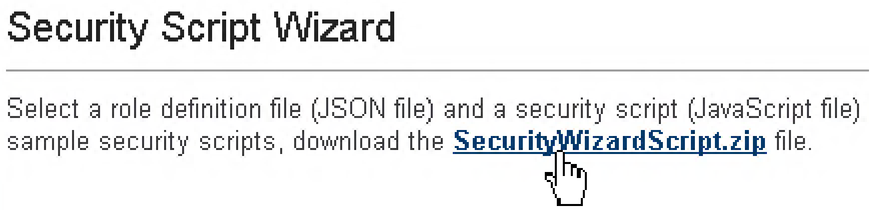
1. Log in to Administration Console:

- http://ecmedu01:9080/acce/ (or use the ACCE bookmark).
- User name: `p8admin`
- Password: `IBMFileNetP8`

2. Right click Sales object store and then select Run Security Script Wizard.



3. Click the SecurityWizardScript.zip file.



Security Script Wizard

Select a role definition file (JSON file) and a security script (JavaScript file) sample security scripts, download the SecurityWizardScript.zip file.

4. Download the file.

Note

If you cannot download the file for any reason, the file is also available on your student system at this location: C:\Labs\FileNet Content Manager 5.2.1 Administration.

5. Cancel the Security Script Wizard.
6. Open the Downloads folder (C:\Users\Administrator\Downloads).
7. Extract the SecurityWizardScript.zip file with the standard Windows archive extraction tool.
8. Verify that you have the necessary files:
   - SecurityScript.js
   - UpdateOSSecurity.json

Procedure 2: Run the Security Script Wizard

Firefox is open. You are logged in to Administration Console as P8Admin.

1. In Firefox, restart the Security Script Wizard on the Sales object store.

2. Select a role definition file:

   a. Browse to and select the UpdateOSSecurity.json file that you recently downloaded.

3. Select a security script file:

   b. Browse to and select the SecurityScript.js file that you recently downloaded.

4. Click Next.

5. Select Role and Role Participants:

   a. Click Add.

   b. Search for group scriptest.

   c. Move scriptest to Selected Users and Groups.

   d. Click OK.

   e. Click Next.

   f. Click OK to close the message about unassigned participants.

6. Click Finish to complete the security script wizard.

7. Wait for the script to complete.

8. Click Close.

9. Log out of Administration Console.

Procedure 3: Test object store access

You ran the Security Script Wizard to provide default object store access to the scriptest group. You are now going to log on to IBM Content Navigator to verify that the security change was successful.

1. Log on to IBM Content Navigator as scriptester.

   - User name: `scriptester`

   - Password: `filenet`

2. Verify that you can see the object stores.

3. Verify that you cannot open any object store except Sales.

4. Log out of IBM Content Navigator.

5. Close the browser.

Information

To provide access to the other object stores, you must run the Security Script Wizard on each one.

Sales was chosen in this exercise because it is the object store that IBM Content Navigator uses for authentication.

End of exercise

Exercise review and wrap-up

In this exercise, you did the following tasks:

- Configured initial security on a new object store.
- Configured the security on the Root Folder of an object store.
- Provided access to an existing object store by adding a group to an established group.
- Provided access to an existing object store by using the Security Script Wizard.

Exercise 4. Configure class and property security

Estimated time

00:30

Overview

This exercise covers how to configure security on classes and properties for certain business use-cases.

Objectives

After completing this exercise, you should be able to:

- Configure default instance security.
- Configure property modification access.

Introduction

In this exercise, you configure default instance security on an object class. Afterward, you configure property modification access on a property definition.

Requirements

Your student system is already started. You have completed the previous exercises in this course.

Exercise Introduction

Why is this lesson important?

Your business solution requires specific group access to certain document classes. You must configure default instance security on those document classes.

A document class has a custom property that you want to make modifiable only by people who have permission to delete the object.

Activities

Configure Default Instance Security, on page 4-3

Configure property modification access, on page 4-6

User accounts

	Type	User ID	Password
	Operating system	Administrator	passw0rd
	P8 Domain	p8admin	IBMFileNetP8
	Finance Clerk	Carol	filenet

Note

Passwords are always case-sensitive.

4.1. Configure Default Instance Security

Introduction

In this activity, you configure default instance security on a document class. Whenever an instance of that class is created, its security is determined by the default instance security.

Procedures

Procedure 1, "Set default instance security on a new document class," on page 4-3

Procedure 2, "Verify default instance security," on page 4-4

Procedure 1: Set default instance security on a new document class

Create a document class that includes one custom property. The procedures for creating classes and properties are covered in the unit: Build an Object Store. You need for Finance Managers to have ownership and Finance Clerks to have Modify Properties permission. You also want the creator of the document to be unauthorized to delete the document after it is created.

1. Use Firefox to log on to Administration Console for Content Platform Engine:
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Create the Invoice number property template:
   a. Go to Finance > Data Design > Property Templates.
   b. Select the Property Templates folder.
   c. Click New to create a property template with the following characteristics.

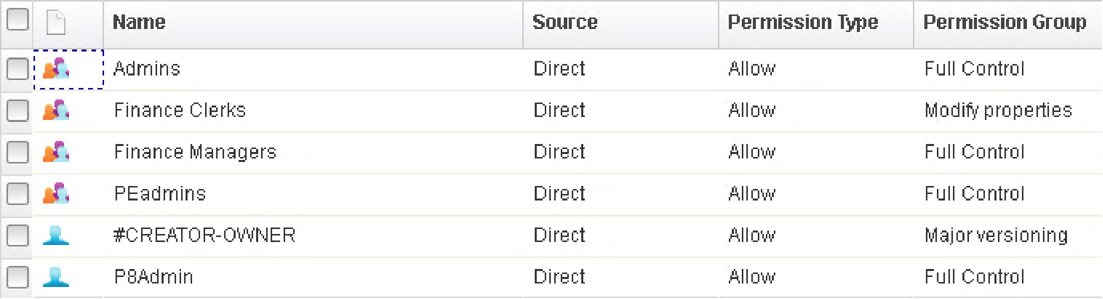
Page	Field	Value
Name and Describe the Property Template	Display name	InvoiceNumber
Select the Data Type	Data type	String
Single or Multi-value	Single or multi-value	Single

3. Create the Invoice document class:
   a. Go to Finance > Data Design > Classes > Document.
   b. Select the Document class.
   c. Click Actions > New Class to create a document subclass named Invoice.
4. Add the InvoiceNumber property to the Invoice document class.
   a. Click Open to edit the class.
   b. Open the Property Definitions tab.
   c. Add the InvoiceNumber property.
   d. Save the change to the Invoice document class.

5. Remove P8Users from default instance security on the class:
   a. Open the Default Instance Security tab.
   b. Select P8Users
   c. Click Remove.
6. Change the permission level of #CREATOR-OWNER to Major versioning.
7. Add the following principals with these Permission groups:

Group	Permission group
Finance Managers	Full Control
Finance Clerks	Modify properties

8. Verify your default instance security settings.



		Name	Source	Permission Type	Permission Group
□		Admins	Direct	Allow	Full Control
□		Finance Clerks	Direct	Allow	Modify properties
□		Finance Managers	Direct	Allow	Full Control
□		PEadmins	Direct	Allow	Full Control
□		#CREATOR-OWNER	Direct	Allow	Major versioning
□		P8Admin	Direct	Allow	Full Control

9. Click Save to save the Invoice class properties.

Hint

You might need to save after each change to ensure that your settings are saved.

10. Log out of Administration Client for Content Platform Engine.
11. Clear the browser cache.

Procedure 2: Verify default instance security

In this procedure, you create an Invoice document and verify the security settings.

1. Log on to IBM Content Navigator as Carol.
   - URL: http://ecmedu01:9080/Navigator
   - User name: `carol`
   - Password: `filenet`
2. Go to Finance > Invoices.
3. Add a subfolder to Invoices. Name the folder `Carol`.

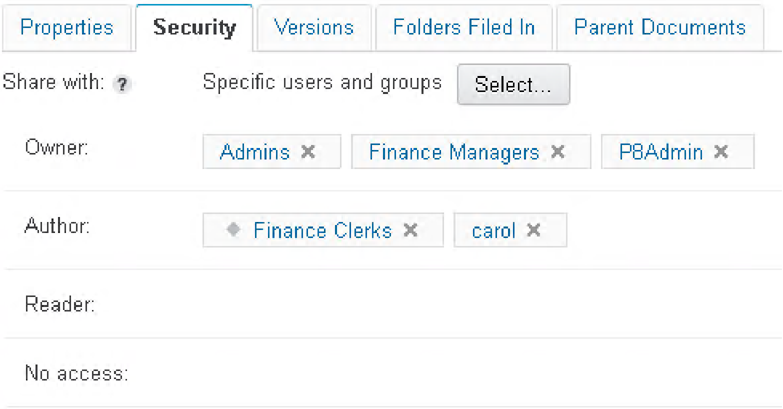
Note

Finance Clerks do not have permission to file documents directly into the Invoices folder, but they can add subfolders.

4. Open the Carol folder.
5. Add a document to the Carol folder:

Property	Value
File	Any file from Documents\sample documents
Class	Invoice
Document Title	Invoice 1
InvoiceNumber	1

6. Open the Security Information page for the new Invoice. Verify the following settings:



Share with: Specific users and groups

Owner: Admins, Finance Managers, P8Admin

Author: Finance Clerks, carol

Reader:

No access:

7. Click Cancel.
8. Log out of IBM Content Navigator.
9. Close the browser.

Troubleshooting

If the security settings are not correct, log in to Administration Console as P8admin and re-apply the default instance security settings.

4.2. Configure property modification access

Introduction

Finance clerks can currently edit the value of the InvoiceNumber property of any Invoice that they create. You want only users who have Full Access to the Invoice documents to be able to change this property. You can customize property modification access to accomplish this goal.

Information

Property modification access behavior is a feature primarily intended for the IBM Enterprise Records application, especially in connection with markings. It is available for use by non-records management applications that need granular control over user ability to modify properties.

Procedures

Procedure 1, "Set property modification access," on page 4-6

Procedure 2, "Verify property modification restriction," on page 4-6

Procedure 1: Set property modification access

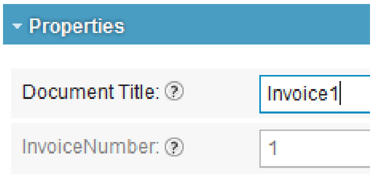
1. Use Firefox to log on to Administration Console for Content Platform Engine:
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Go to Object Stores > Finance > Data Design > Classes > Document > Invoice.
3. Open the Property Definitions tab.
4. Click InvoiceNumber.
5. On the Property Definition page, open the Modification Access tab.
6. Select the Delete option.
7. Click OK.
8. Click Save on the Invoice class definition page.
9. Log out of Administration Console for Content Platform Engine.
10. Clear the browser cache.

Procedure 2: Verify property modification restriction

1. Log on to IBM Content Navigator as Carol.
   - URL: http://ecmedu01:9080/navigator
   - User name: `carol`

- Password: `filenet`

2. Go to Finance > Invoices > Carol.
3. Open the Properties page for the Invoice document that you added.
4. Verify that you cannot edit the value of the InvoiceNumber property, even though you can edit the Document Title.



Properties

Document Title: Invoice1

InvoiceNumber: 1

5. Click Cancel.
6. Log out of IBM Content Navigator.
7. Close the browser.

Note

You changed the InvoiceNumber property definition on the Invoice document class, but you did not change the InvoiceNumber property template. If you create a new class and you use this property template, the property will have normal modification access.

End of exercise

Exercise review and wrap-up

In this lesson, you did the following tasks:

- Configured default instance security on a document class.
- Configured property modification access on a custom property.

Exercise 5. Configure security inheritance

Estimated time

00:40

Overview

This exercise covers how to configure security inheritance by using folders and object-valued properties.

Objectives

After completing this exercise, you should be able to:

- Configure folder inheritance.
- Configure a security parent by using a custom OVP.

Introduction

In this exercise, you configure security to be inherited from other objects. In the first part, you use a folder as the parent object. In the second part, you use a custom object-valued property.

Requirements

Your student system is already started. You have completed the previous exercises in this course.

Exercise introduction

Why is this lesson important?

The design for your business solution calls for some documents to have their security that is determined by the security of a folder or another object. As the solution builder, you must use security inheritance features to implement this functionality.

Activities

Configure folder inheritance, on page 5-3

Configure a security parent using a custom OVP, on page 5-6

User accounts

	Type	User ID	Password
	Operating system	Administrator	passw0rd
	P8 Domain	p8admin	IBMFileNetP8
	Finance Admin	Adam	filenet

Note

Passwords are always case-sensitive.

5.1. Configure folder inheritance

Introduction

In this exercise, you create a folder and use folder inheritance to secure documents.

Procedures

Procedure 1: Preparation: Create a document class

To have security that is completely controlled by inheritance, you must eliminate the default instance permissions. To set up the exercises for this lesson, you are going to create a document class that has no default instance permissions.

1. Use Firefox to log on to Administration Console for Content Platform Engine:
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Create the Receipt document class:
   a. Go to Finance > Data Design > Classes > Document.
   b. Select the Document class.
   c. Click Actions > New Class to create a document subclass named `Receipt`.
   d. Open the document class definition page after you create the class.
3. Remove default instance security on the class:
   a. Open the Default Instance Security tab.
   b. Select all entries except P8Admins.
   c. Click Remove.
   d. Click Save.
   e. Close the Receipt tab.

Procedure 2: Create a parent folder

Create the folder from which receipts inherit permissions.

1. Go to Finance > Browse > Root folder.

2. Click Actions > New Folder.
3. Name the folder: `Receipts`.
4. Accept default values to complete the wizard.
5. Open the Security tab for the folder.
6. Add inheritable security settings:
    a. Click Add.
    b. Search for Finance groups.
    c. Add the Finance Admins and Finance Managers.
    d. From the Apply to menu, select *All children, but not this object*.
    e. From the Permission group menu, select Full Control.
    f. Click OK.
7. Save the changes to the folder.

Procedure 3: Create a receipt

1. On the Receipts tab, click Actions > New Document.
2. Define the new document object:
    a. Name the new document *Test receipt*.
    b. Select the Receipt class.
    c. Click Next.
3. Add document content:
    a. Browse to and add any document from Documents\sample documents.
    b. Click Next.
4. Use default settings to complete the add document wizard.
5. Click Open to open the Test receipt properties page.
6. Open the Security tab.
7. Verify that the only ACE is P8Admins.

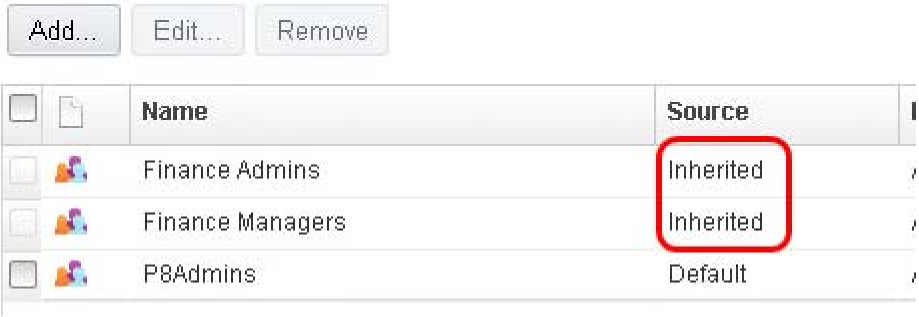
Procedure 4: Configure the document to inherit security

1. Open the General tab for the Test Receipt document.
2. Scroll down.
3. From the Inherit Security from folder, select Receipts.
4. Click Save.

Procedure 5: Verify security change

1. Open the Security tab of the Test receipt.

2. Verify that Finance Admins and Finance Managers have inherited permissions.

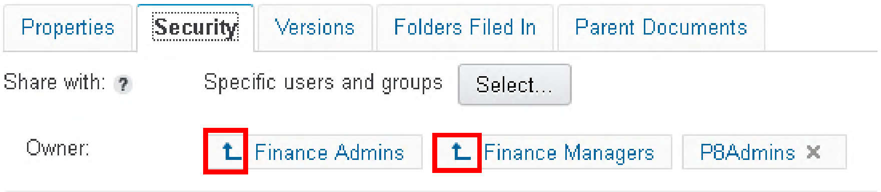


□		Name	Source
□		Finance Admins	Inherited
□		Finance Managers	Inherited
□		P8Admins	Default

3. Verify that the inherited settings are not editable.
4. Log out of Administration Console for Content Platform Engine.

Procedure 6: (Optional) Test security inheritance

1. Use Firefox to log on to IBM Content Navigator as Adam:
   - URL: http://ecmedu01:9080/navigator
   - User name: adam
   - Password: `filenet`
2. Go to Finance > Receipts.
3. Open the properties page for the Test Receipt document.
4. Open the security tab.
5. Confirm the security settings:
   - Finance Manager, Finance Admins, and P8admins are all owners.
   - Finance Admins and Finance Managers permissions have an inheritance indicator.



Share with: ? Specific users and groups

Owner: Finance Admins Finance Managers P8Admins ✕

6. Click Cancel.
7. Delete the Test Receipt document.
   a. Select the document.
   b. Click Actions > Delete.
8. Log out of IBM Content Navigator.

5.2. Configure a security parent using a custom OVP

Introduction

In this procedure, you create an object specifically to be a security parent. Documents that inherit security from this parent will be affected when you change security on the parent.

You use a custom object-valued property (OVP) to designate a security parent. You can set this property's default value on the class definition, so that all new documents of this class are created with the same default security parent.

Procedures

Procedure 1: Create a security parent folder

Create a folder to keep track of security parents.

1. If you are not already logged on to Administration Console for Content Platform Engine, use Firefox to log on as p8admin.
   - URL: http://emcedu01:9080/acce
   - User name: `p8admin`
   - Password: `IBMFileNetP8`
2. Go to Finance > Root Folder.
3. Create a folder named `Security Parents`.
4. Open the folder.

Procedure 2: Create a security parent

1. In the Security Parents folder, create a contentless document:
   a. From the Security Parents folder, click Action > New Document.

b. Name the document `Accounts Payable Access`.

c. Clear the With Content option.

d. Use default values to complete the wizard.

2. Open the Accounts Payable Access document.
3. Click Actions > Copy Object Reference.

Information

You are copying the object reference now, but you do not need to paste it until you edit the property definition for the document class that inherits security from this object. If for any reason your copy buffer gets erased before you edit the property definition, you must come back to this document to copy the object reference.

Procedure 3: Edit security of the security parent

The security parent must have at least one inheritable ACE. You are viewing the Accounts Payable Access document properties page.

1. On the Accounts Payable Access document, open the Security tab.
2. Remove P8users, and the P8admin entries. Do not remove the P8admins entry.
3. Save the changes to the document.
4. Add the following permissions.

Principal	**Permission group**	**Apply To**
Finance Admins	Full Control	All children, but not his object
Finance Managers	Full Control	All children, but not his object
Finance Reviewers	View Content	All children, but not his object
Finance Clerks	Major Versioning	All children, but not his object

5. Verify that the ACL for the Accounts Payable Access document has the correct permissions:

Troubleshooting

If the permissions are not what you expected after you save the document, try editing each ACE separately and saving between.

6. Save the changes to the document.

Procedure 4: Create a custom object valued property template

The custom object valued property assigns the security parent to the document. You must create the property template before you can add it to the document class. You are signed into Administration Console for Content Platform Engine as p8admin.

1. Go to Finance > Data Design > Property Templates.

2. Click New to create a property template.
3. Complete the property template using the following values.

Page	Property	Value
Name and describe the property template	Display name	Security parent OVP
Select the data type	Data type	Object
Single or Multi-value	Single or Multi-value	Single
	Set other attributes	Selected
Additional property template attributes	Security Proxy Type	Inherited

Information

The Security Proxy Type value of Inherited appears as the integer 2 when viewed in the document’s property grid.

4. Use default values to complete the wizard.
5. Click Close.

Procedure 5: Create a document class

The new document class must include the object valued property that you created.

1. Go to Finance > Data Design > Classes > Document.
2. Click Actions > New Class.
3. Name the class Accounts Payable.
4. Complete the document class wizard.
5. Click Open.

Procedure 6: Change default instance security

You want all of the security to be inherited from the security parent. Therefore, you are going to remove the default instance permissions.

1. Open the Default Instance Security tab.
2. Remove all of the ACEs *except* for P8admins.
3. Save the changes to the Accounts Payable class.

Procedure 7: Add the custom OVP to the document class

You now add the custom OVP property to the Accounts Payable class. The Accounts Payable class definition is open.

1. Open the Property Definitions tab.
2. Click Add.

3. Select Security Parent OVP from the Add Properties menu.
4. Click OK.
5. Edit the property definition attributes:
   a. On the Property Definitions tab, click Security Parent OVP.
   b. Open the More tab.
   c. In the Required Class field, select Document.
   d. Click OK.
6. Click Save to save the changes to the class definition.

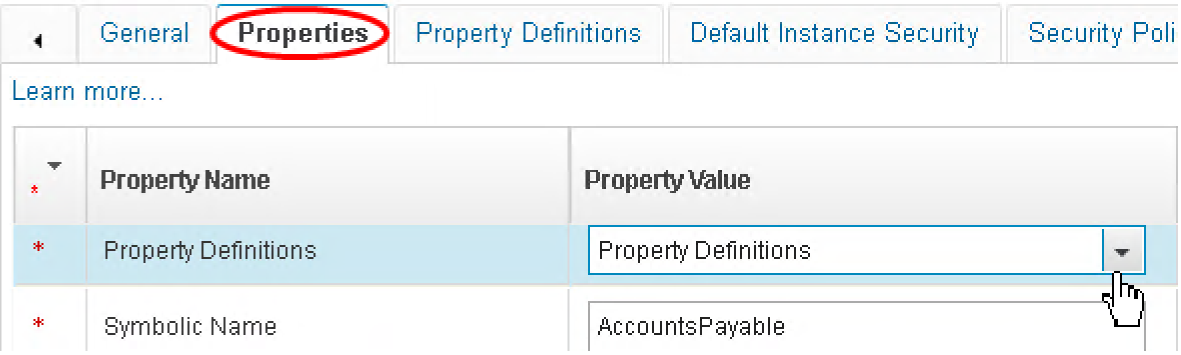
Information

For the Required Class property, you must select the exact class of the parent object.

Procedure 8: Configure the default value for the custom OVP

To save time when users add documents, you can configure the default value of Security Parent OVP property to point to the security parent. All new documents of this class automatically use the Accounts Payable Access document as a security parent by default. The Accounts Payable class definition is open.

1. Open the Properties tab.
2. Open the Property Definitions menu.



*	Property Name	Property Value
*	Property Definitions	Property Definitions
*	Symbolic Name	AccountsPayable

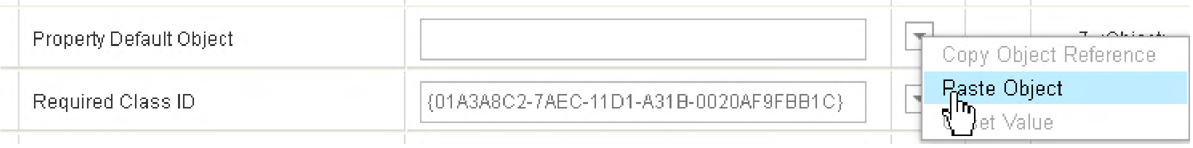
Hint

Be patient: this menu sometimes takes a couple minutes to load. Click the arrow one time and wait. If you are prompted to continue running scripts or stop, select Continue.

Information

The Property Definitions menu on the Properties tab is **not** the same as selecting the Property Definitions tab of the class definition.

3. Select Security Parent OVP from the list. Be sure to select Security Parent OVP, not Security Parent.
4. On the Security Parent OVP Properties page, do the following tasks:
   a. Scroll down to the Property Default Object property.
   b. Click the options arrow to the right of the field, and then select Paste Object.



Property Default Object	
Required Class ID	{01A3A8C2-7AEC-11D1-A31B-0020AF9FBB1C}

Hint

If the Paste Object option is inactive, you need to copy the object reference of the Accounts Payable Access document.

   c. Verify that the Property Default Object Value is now *Accounts Payable Access*.

Note

You cannot save the values on the Security Parent OVP Properties page: you must save the changes to the class definition.

5. Select the Accounts Payable class definition tab.
6. Click Save.

Procedure 9: Create test document

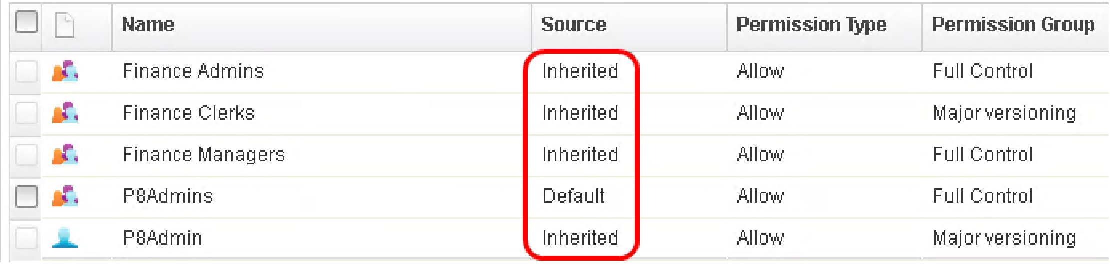
With all the preparations in place, you can create a test instance of an accounts payable document and verify that the inherited security is correct. You are logged on to Administration Console for Content Platform Engine.

1. Create a folder in the Root Folder of Finance. Name the folder `Accounts Payable`.
2. Open the folder.
3. In the Accounts Payable folder, Create a document:
   a. Type a name for the document. The document name is unimportant.
   b. Select the Accounts Payable document class.

c. Use any document from Documents\sample documents for content.

d. Complete the wizard by using default values.

4. Click Open.
5. Select the Security tab.
6. Verify that the document has inherited the security settings from the security parent.



□		Name	Source	Permission Type	Permission Group
□		Finance Admins	Inherited	Allow	Full Control
□		Finance Clerks	Inherited	Allow	Major versioning
□		Finance Managers	Inherited	Allow	Full Control
□		P8Admins	Default	Allow	Full Control
□		P8Admin	Inherited	Allow	Major versioning

Procedure 10:(Optional) Observe inherited security changes

Imagine that you have several thousand documents in the accounts payable class. A change to business practices requires that Finance Reviewers must have Major Versioning access to Accounts Payables. You can change the parent document one time, and the security is changed on all child documents. You are signed in to Administration Console for Content Platform Engine as p8admin.

1. Go to Finance > Browse > Root Folder > Security Parents.
2. Open the Properties page of the Accounts Payable Access document.

Hint

If you do not see the document in this folder, click Refresh.

3. Change the ACL to give Reviewers the Major Versioning permission group. Be sure to apply this setting to all children, but not the current object.
4. Save your changes to the document.
5. Verify the inherited security changes:

   a. Go to Finance > Browse > Root Folder > Accounts Payable.

   b. Open the properties page for the document in this folder.

   c. On the Security tab, verify that Reviewers have Major Versioning permission. You might need to refresh to see the security update.

6. Log out of Administration Console for Content Platform Engine.
7. Close Firefox.

End of exercise

Exercise review and wrap-up

In this exercise, you completed the following tasks:

- Configure folder inheritance.
- Configure a security parent by using a custom OVP.

Appendix A. Start and Stop System Components

Appendix Overview

This image contains three WebSphere Application Server profiles. For this unit, you use the profile for server1, which hosts the following applications:

- Tivoli Directory Server Administration tool
- Content Platform Engine
- IBM Content Navigator
- Administration Console for Content Platform Engine

List of procedures:

- Procedure 1, "Start system components," on page A-1
- Procedure 2, "Check system components," on page A-2
- Procedure 3, "Stop system components," on page A-4

Procedure 1: Start system components

There are start scripts to make starting the WebSphere Application Server profiles easier. The scripts are in the folder WebSphere Admin on the desktop.

Important

If you just started the image, ensure that the Windows 7 Operating System completes starting all the services. Launch the Windows Task Manager and ensure that CPU usage is down to 0-1% CPU usage. It can take several minutes.

1. Open the WebSphere Admin folder on the desktop.
2. Double-click the Start Server1.bat to run the script.
3. Wait for the command window to disappear (Can take several minutes).

Procedure 2: Check system components

An IBM FileNet P8 Workflow system consists of one main engine, the Content Platform Engine, with two primary services, content and process services. In addition to the Content Platform Engine, a client application is required for the users and databases are required to store configuration information and the object stores. The client that you use for these activities is IBM Content Navigator. You work with two IBM Content Navigator desktops that are configured for the workflow administrator and for the workflow author. You need to verify that the Content Platform Engine and the IBM Content Navigator desktops are fully functional before you start your student exercises. 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.

1. Verify that the Content Platform Engine, content services are functioning properly by opening the Content Engine Startup Context (Ping Page).

   a. Open a Mozilla Firefox browser window.
   b. Click the Bookmarks menu and select, System Health > CE ping

      i. URL for Ping Page: `http://ecmedu01:9080/FileNet/Engine`

   Because the Content Engine is running as an application inside the IBM WebSphere Application Server, successfully viewing the Content Platform Engine Ping Page indicates that the web application server is also running on your student system.

2. Verify that the Content Platform Engine process Services are functioning properly.

   a. Open a new browser tab.
   b. Click the Bookmarks menu and select, System Health > PE ping

      i. URL for Ping Page: `http://ecmedu01:9080/peengine/IOR/ping`

   c. If both ping pages display successfully, close the browser and all the tabs.

3. Verify that the P8 Admin console desktop is functioning properly.

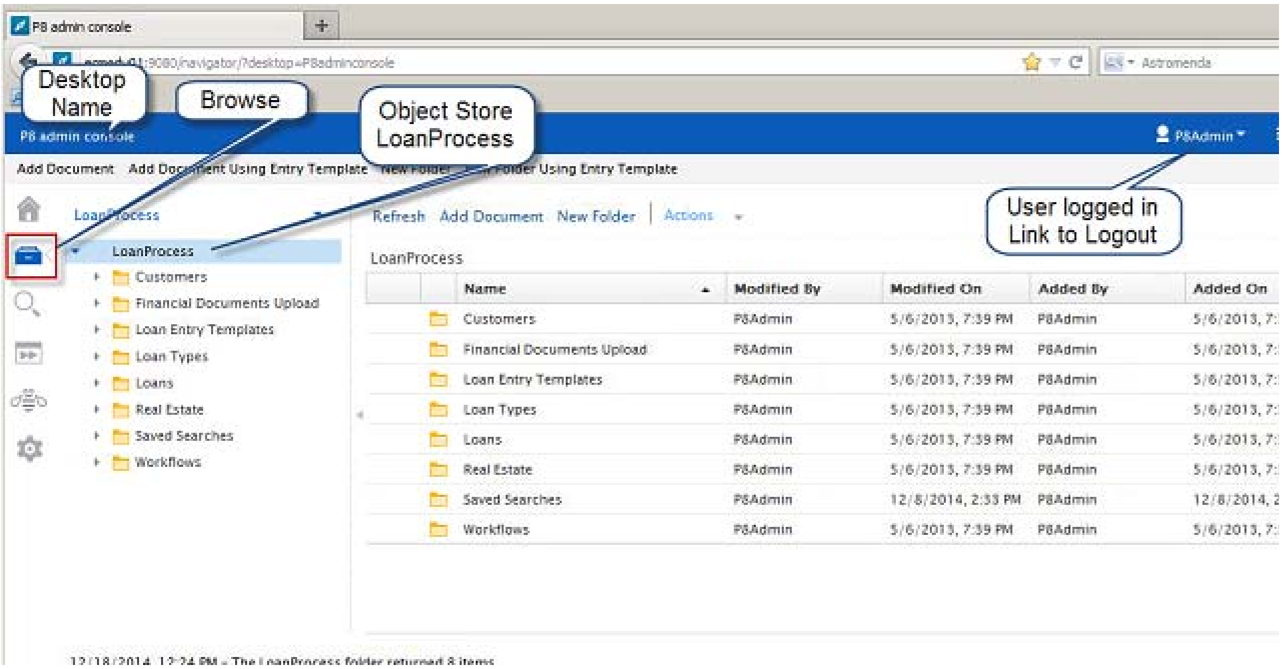
   a. Open a Mozilla Firefox browser window.
   b. Click the Bookmarks menu and select, P8 Admin console

      i. URL for desktop: `http://ecmedu01:9080/navigator/?desktop=P8adminconsole`

   c. Log in as the administrator.

      - Username: `p8admin`
      - Password: `IBMFileNetP8`

A successful login to the P8 Admin console desktop opens to a screen.



LoanProcess

Name	Modified By	Modified On	Added By	Added On
Customers	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Financial Documents Upload	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Loan Entry Templates	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Loan Types	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Loans	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Real Estate	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:
Saved Searches	P8Admin	12/8/2014, 2:33 PM	P8Admin	12/8/2014, 2
Workflows	P8Admin	5/6/2013, 7:39 PM	P8Admin	5/6/2013, 7:

12/18/2014 12:24 PM - The LoanProcess folder returned 8 items

If you get to this screen, it indicates that the following components are running and communicating within your student system:

- A database system. Your system uses the IBM DB2 database software. Every time a user logs in to the P8 Admin console desktop, the desktop configuration is loaded from the IBM Content Navigator 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.
- A directory service to handle user authentication. Your system uses the IBM Tivoli Directory Server.

d. Logout of the P8 Admin console.

i. On the upper right corner of the desktop, click P8Admin and select Log Out.

ii. Click Log Out to confirm.

4. Verify that the Sample desktop is functioning properly.

   a. Open a Mozilla Firefox browser window.

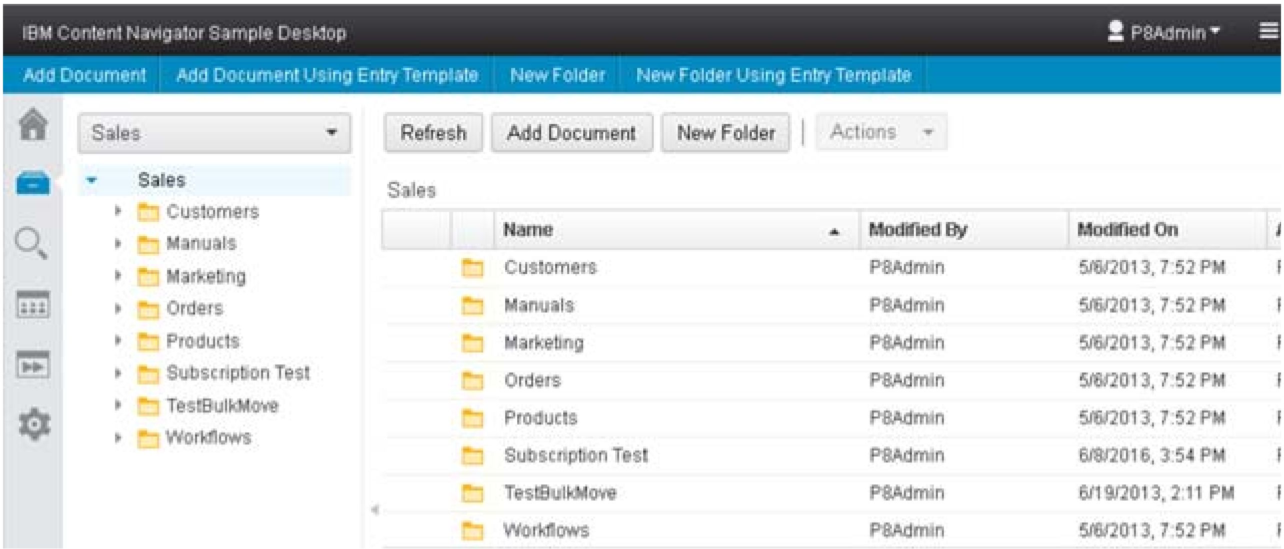
   b. Click the Bookmarks menu and select, Content Navigator.

      i. URL for desktop: `http://ecmedu01:9080/navigator/`

   c. Log in in as an administrator:

      - Username: `p8admin`
      - Password: `IBMFileNetP8`

   d. Confirm that you see the Sample desktop, the Sales object store.



Name	Modified By	Modified On
Customers	P8Admin	5/6/2013, 7:52 PM
Manuals	P8Admin	5/6/2013, 7:52 PM
Marketing	P8Admin	5/6/2013, 7:52 PM
Orders	P8Admin	5/6/2013, 7:52 PM
Products	P8Admin	5/6/2013, 7:52 PM
Subscription Test	P8Admin	6/8/2016, 3:54 PM
TestBulkMove	P8Admin	6/19/2013, 2:11 PM
Workflows	P8Admin	5/6/2013, 7:52 PM

   e. Logout of IBM Content Navigator.

      i. On the upper right corner of the desktop, click P8Admin and select Log Out.

      ii. Click Log Out to confirm.

Procedure 3: Stop system components

1. Open the WebSphere Admin folder on the desktop.
2. Double-click the Stop Server1.bat to run the script.
3. Wait for the command window to disappear (Can take several minutes).

Appendix B. List of users and groups

Users and groups list

This table shows the users and groups defined on your student system.

Group	Members	Object stores
#Authenticated Users	*	P8ConfigObjectStore SalesSBx
Accounting	Allison	
Admins	Finance admins	
	Legal	
AEAdmins	AEadmin	LoanProcessQA
	P8Admin	
Agent	Allen	
	Amy	
Approver	Ana	
BPM Administrator	P8admin	
BPM Designer	P8admin	
BPM User	P8admin	
Case admins	P8admin	
	Sue	
Case initiators	Sue	
	P8admin	
	Cody	
Case workers	Sue	
	Cody	
	Fred	
	Addington	
CEadmins	P8admin	LoanProcess LoanProcessQA
	Ceadmin	
Clerks	Clara	LoanProcessQA
	Clark	
Components	Component	
Coordinators	Connie	
	Conrad	
Customers	Customer	
Finance Admins	Adam	LoanProcessQA
	Allison	
	Steve	
Finance Clerks	Carol	LoanProcessQA
	Charles	

Group	Members	Object stores
Finance Managers	Mark	LoanProcessQA
	May	
Finance reviewers	Richard	LoanProcessQA
	Roberta	
Grouptest	Grouptester	
Legal	Larry	
	Linda	
Loan business analysts	Barb	LoanProcess
	Barry	
Loan business users	Burke	LoanProcess
	Burt	
Loan guests	Gabe	LoanProcess
	Gail	
	loanGuest	
Loan Managers	Mabel	LoanProcess
	Mac	
	Mary	
	Matt	
Loan officers	Olivia	LoanProcess
	Oscar	
Loan operations	Opal	LoanProcess
	Ophelia	
Loan processors	Pat	LoanProcess
	Peter	
Loan system administrators	Sydney	LoanProcess
	Sylvia	
Loan underwriters	Uma	LoanProcess
	Uri	
Managers	Manny	
	Mary	
Operations	Opal	
	Oscar	
P8admins	P8admin	P8ConfigObjectStore LoanProcess LoanProcessQA Sales SalesQA

Group	Members	Object stores
P8users	CaseAdmins	Sales SalesQA
	CaseWorkers	
	CaseInitiators	
	Accounting	
	Agent	
	Approver	
	BPM Administrator	
	BPM Designer	
	BPM User	
	Clerks	
	Components	
	Coordinators	
	Customers	
	Finance Admins	
	Finance Clerks	
	Finance Managers	
	Finance Reviewers	
	Legal	
	Loan Business Analysts	
	Loan Business Users	
	Loan Guests	
	Loan Managers	
	Loan Officers	
	Loan Operations	
	Loan Processors	
	Loan System Admins	
	Loan Underwriters	
	Managers	
	Operations	
	ProductDev	
	QualityAssurance	
	Reviewer	
	Supervisor	
	SysAdmins	
	joe	
	loanGuest	
	p8guest	
PEadmins	P8admin	LoanProcess
	PEadmin	
ProductDev	Pamela	
	Paul	
QualityAssurance	Queenie	
	Quincy	
Reviewer	Mark	

Group	Members	Object stores
Scriptest	Scriptester	
Supervisor	Sue	
Sysadmins	P8admin	
	CEadmin	
	Scott	
	Steve	
	AEadmin	
	PEadmin	

IBM Training