Course 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.

Course description

IBM FileNet Content Manager 5.2.1: Security

Duration: 1 day

Purpose

Learn to administer security on an IBM FileNet Content Manager 5.2.1 system. This comprehensive security course covers directly modifying security, to configuring security on an object store and its objects.

Audience

This course is intended for IBM FileNet Content Manager administrators and solution builders.

Prerequisites

- Basic computer skills: Able to use computers, authenticate using a name and password, follow hyperlinks, and use common user interface elements such as buttons, menus, and tabs.
- Able to use IBM Content Navigator for typical content management tasks, including navigating object stores, downloading and uploading documents, checking in and checking out.
- Able to administer IBM Content Navigator, including configuring desktops.F271 – IBM Content Navigator 2.0.3.6: Administration
- F271 – IBM Content Navigator 2.0.3.6: Administration
- F280 – IBM FileNet Content Manager 5.2.1: Introduction
- F281 – IBM FileNet Content Manager 5.2.1: IBM FileNet Content Manager 5.2.1: Build a FileNet Content Repository
- F282 – IBM FileNet Content Manager 5.2.1: IBM FileNet Content Manager 5.2.1: Work with object metadata

Objectives

- Resolve logon failures
- Verify object store access
- Change security on a document
- Change the owner of a document
- Customize document access
- Configure object store security
- Configure class and property security

- Configure security inheritance

Contents

- Resolve logon failure
- Modify direct security
- Configure object store security
- Configure class and property security
- Configure security inheritance

Curriculum relationship

Visit http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=page&c=Y678448H04759K32 for more information about this and other IBM FileNet Content Manager courses.

Agenda

Note

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

Day 1

(00:15) Course introduction
(00:20) Unit 1. Resolve logon issues
(00:30) Exercise 1. Resolve access issues
(00:30) Unit 2. Modify direct security
(00:30) Exercise 2. Modify direct security
(00:20) Unit 3. Configure object store security
(00:40) Exercise 3. Configure object store security
(00:30) Unit 4. Configure class and property security
(00:30) Exercise 4. Configure class and property security
(00:20) Unit 5. Configure security inheritance
(00:40) Exercise 5. Configure security inheritance

Unit 1. Resolve logon issues

Estimated time

00:20

Overview

This unit describes basic security concepts and includes instruction on how to resolve basic logon and access failures.

How you will check your progress

- Machine exercises

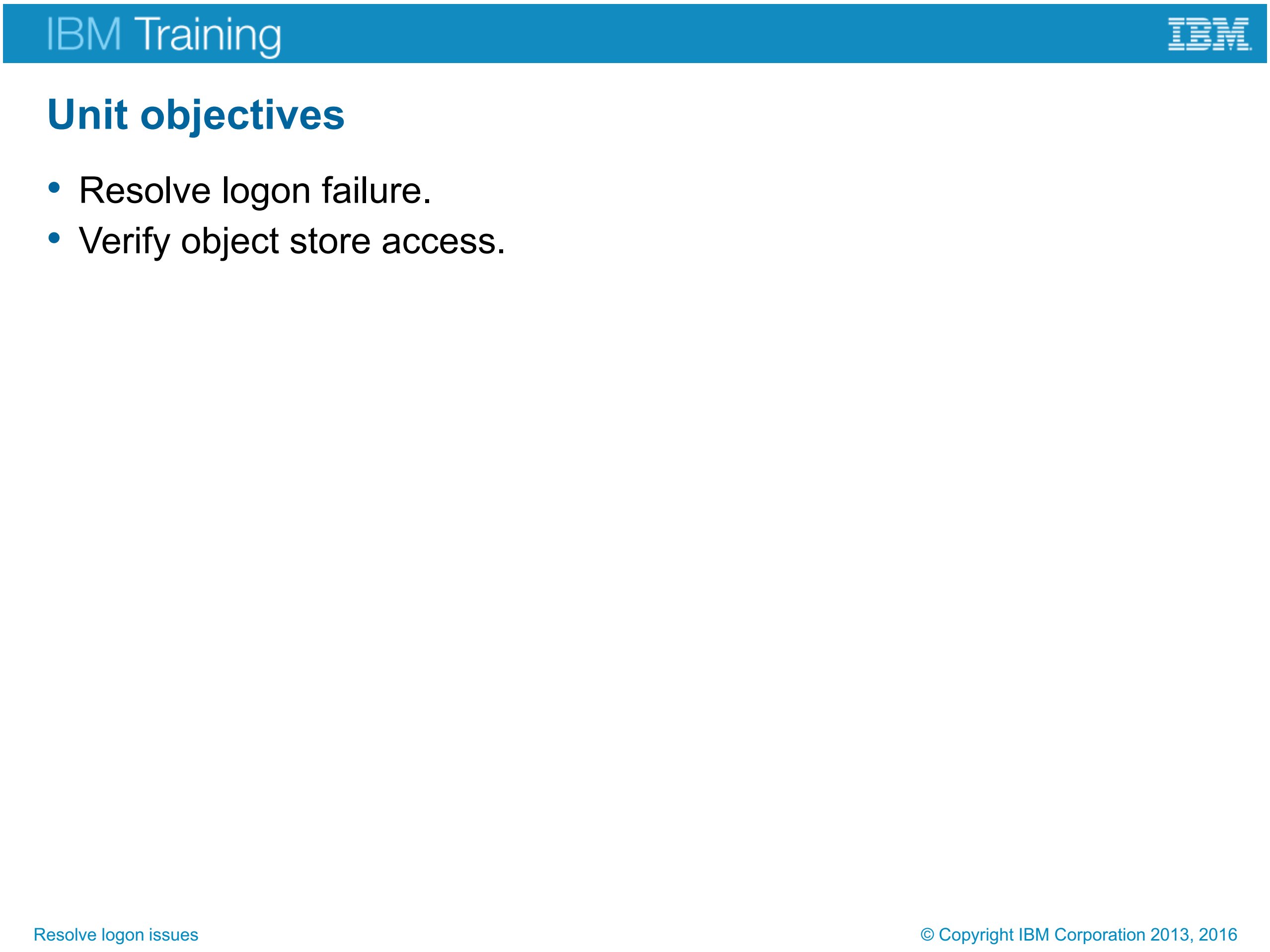
References

IBM Knowledge Center. P8 Platform:

http://www.ibm.com/support/knowledgecenter/SSNW2F

IBM Knowledge Center, Content Navigator:

http://www.ibm.com/support/knowledgecenter/SSEUEX



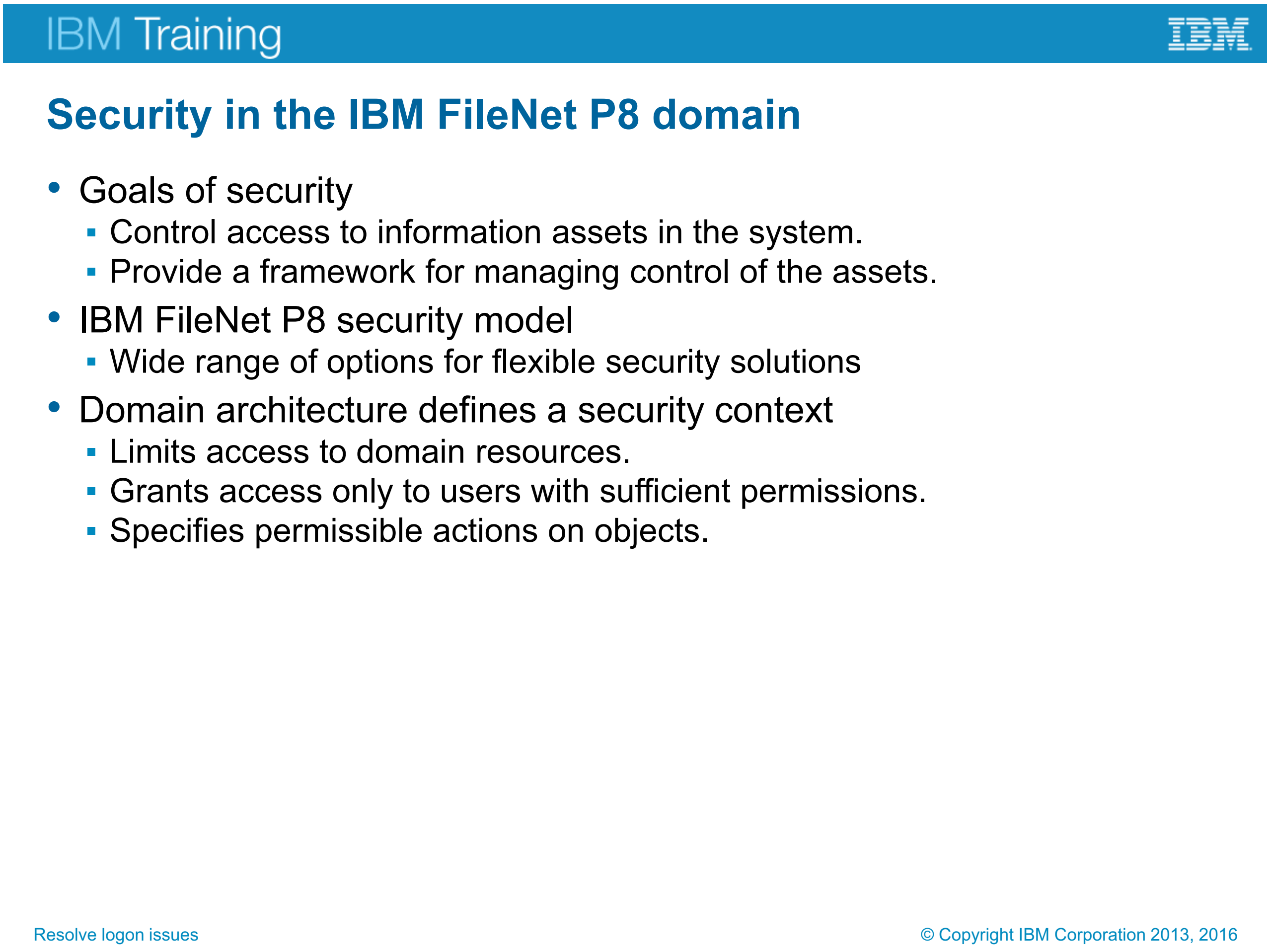
IBM Training

Unit objectives

- Resolve logon failure.
- Verify object store access.

Resolve logon issues

Figure 1-1. Unit objectives



IBM Training

Security in the IBM FileNet P8 domain

- Goals of security
  - Control access to information assets in the system.
  - Provide a framework for managing control of the assets.
- IBM FileNet P8 security model
  - Wide range of options for flexible security solutions
- Domain architecture defines a security context
  - Limits access to domain resources.
  - Grants access only to users with sufficient permissions.
  - Specifies permissible actions on objects.

Resolve logon issues

© Copyright IBM Corporation 2013, 2016

Figure 1-2. Security in the IBM FileNet P8 domain

Help paths

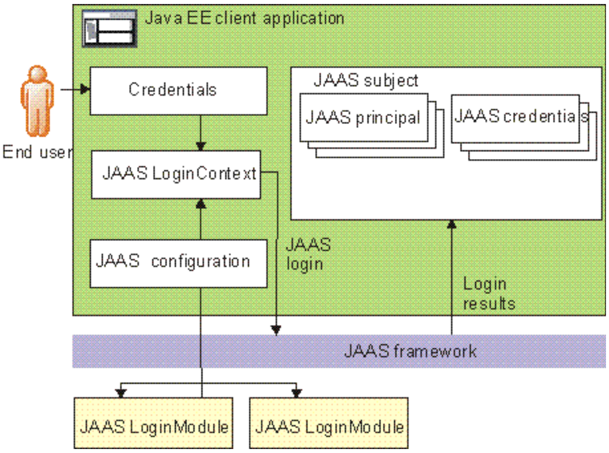
- IBM FileNet P8 Version 5.2.1 Information Center > Security > FileNet P8 security > Security overview
  - http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8pso000.htm
- IBM FileNet P8 Version 5.2.1 Information Center > Security > FileNet P8 security > Security tools and procedures
  - http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8pst017.htm

Because of the wide range of security configuration options available in an IBM FileNet P8 system, effective security design requires an understanding of these options and how they can be used.

IBM Training

Authentication

- Authentication
  - Who you are.
  - Identifies the user who is trying to log on.
  - Requires credentials (a user name and password).
  - Uses an authentication provider
    - LDAP directory service
  - Creates a security token (a data structure that typically persists until the user logs out).
  - Uses JAAS and WS-Security standards.
- FileNet P8 domain
  - Provides the security context for authenticating applications.
  - Is created during IBM FileNet P8 Platform installation.



Resolve logon issues

Figure 1-3. Authentication

Help paths

FileNet P8 Platform 5.2.1>Security>Authentication>Authentication overview>Supported authentication standards

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psn037.htm

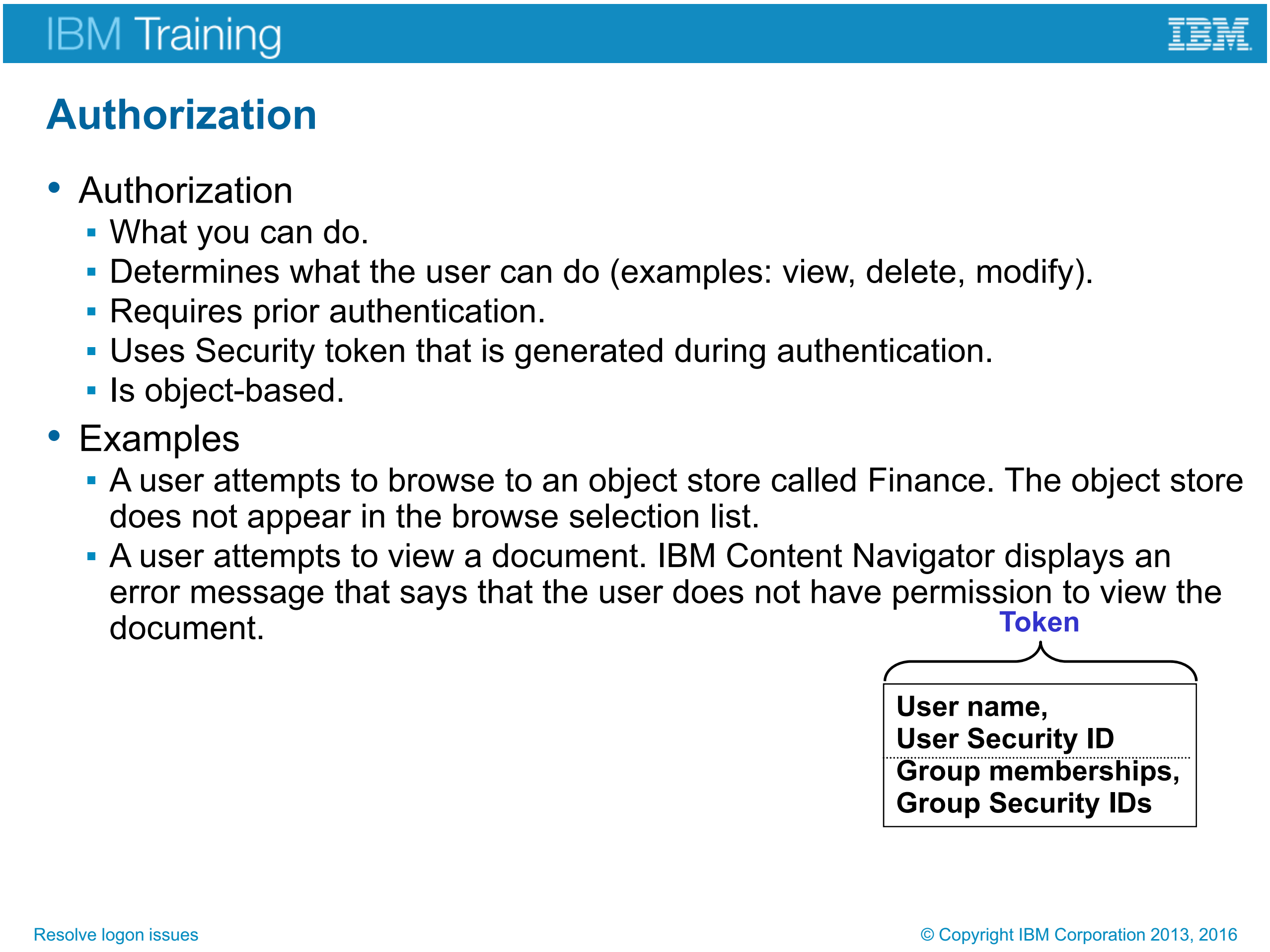
FileNet P8 Platform 5.2.1>Security>Directory service providers

http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psd000.htm

Authentication - Authentication is the act of verifying a user identity based on credentials that the user presents. Authentication of individuals, or ideally of the roles that an individual has, through the external authentication mechanism, is key to the security features in IBM FileNet Content Manager. The two standards at the core of the authentication process in FileNet Content Manager are the Java Authentication and Authorization Service (JAAS) standard and the Web Services Security standard. The JAAS standard forms the framework for security interoperability in the Java EE world. The Web Services Security standard forms the framework for security interoperability in the heterogeneous world of clients and servers that communicate through web services interfaces.

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

Supported directory service providers include IBM Tivoli Directory Server, CA Directory, Novell eDirectory, Sun Java Directory Server, Oracle Directory Server, and Microsoft Active Directory.



IBM Training

Authorization

- Authorization
  - What you can do.
  - Determines what the user can do (examples: view, delete, modify).
  - Requires prior authentication.
  - Uses Security token that is generated during authentication.
  - Is object-based.
- Examples
  - A user attempts to browse to an object store called Finance. The object store does not appear in the browse selection list.
  - A user attempts to view a document. IBM Content Navigator displays an error message that says that the user does not have permission to view the document.

Token

User name,
User Security ID
Group memberships,
Group Security IDs

Resolve logon issues

© Copyright IBM Corporation 2013, 2016

Figure 1-4. Authorization

Help path

FileNet P8 Platform 5.2.1>Security>Authorization

> http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa033.htm

When an authenticated security principal attempts to access FileNet P8 objects, Content Platform Engine attempts to retrieve that principal's user and group memberships from the directory service provider. If successful, the user is authorized to complete actions on the object.

User roles

Different user roles are responsible for securing different types of objects. For example, administrators, solution builders, authors, and users might have different access rights to the same objects.

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

Independent and dependent security

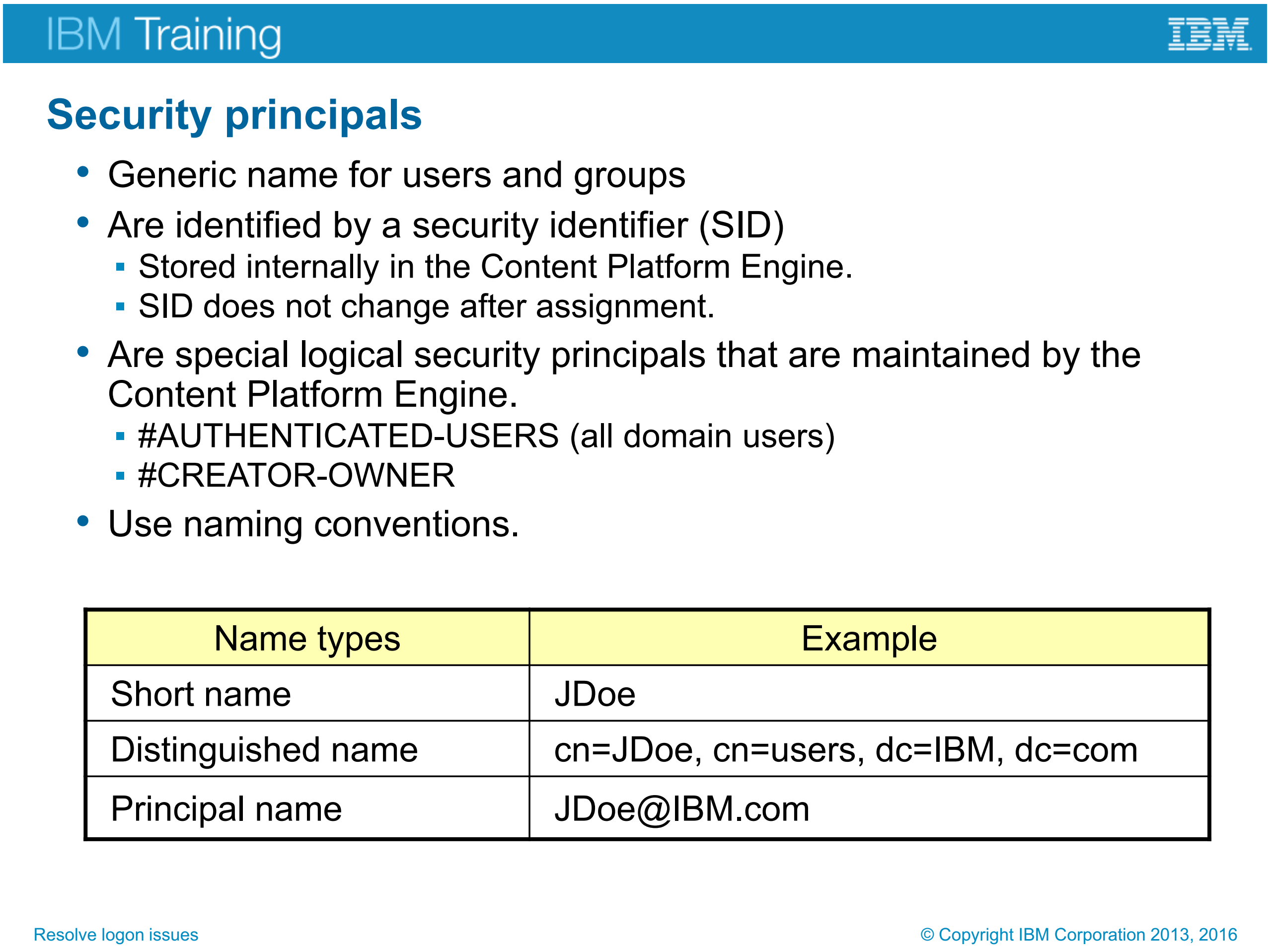
Most objects have Access control Lists (ACLs) that can be independently set. These objects are called independently securable.

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

Examples of dependently securable objects follow:

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

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



IBM Training

Security principals

- Generic name for users and groups
- Are identified by a security identifier (SID)
  - Stored internally in the Content Platform Engine.
  - SID does not change after assignment.
- Are special logical security principals that are maintained by the Content Platform Engine.
  - #AUTHENTICATED-USERS (all domain users)
  - #CREATOR-OWNER
- Use naming conventions.

Name types	Example
Short name	JDoe
Distinguished name	cn=JDoe, cn=users, dc=IBM, dc=com
Principal name	JDoe@IBM.com

Resolve logon issues

Figure 1-5. Security principals

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>About access rights>What are access rights?

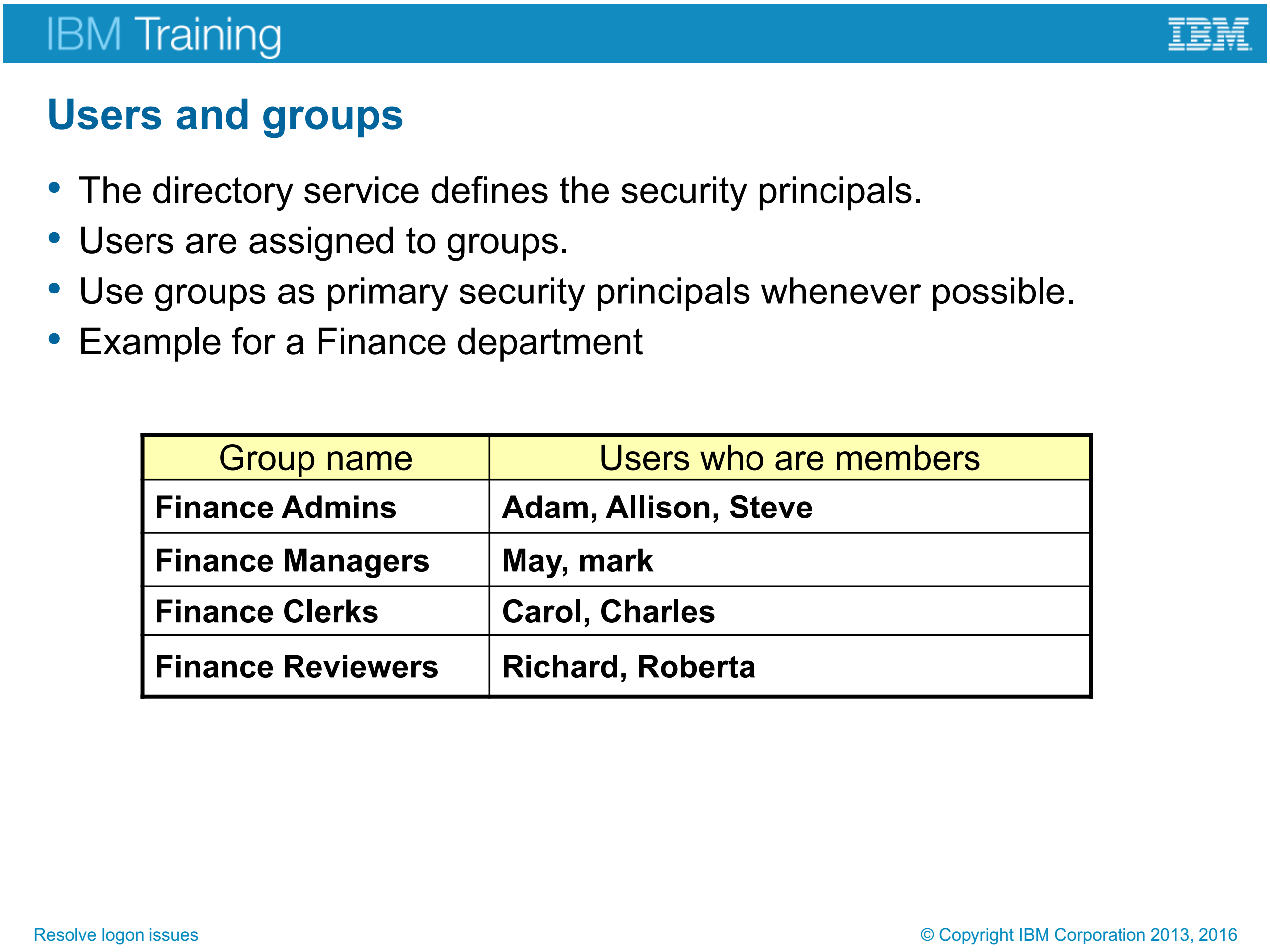
http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa051.htm

The different naming conventions play an important role when you are viewing and configuring security in different contexts. In most of the interfaces that are used for this unit, you see only a short name or a principal name. Security settings that are related to system configuration often use the distinguished name because it is important that the security principal be uniquely identifiable in the security context within which the system is designed to operate.

#AUTHENTICATED-USERS is a group that consists of all domain users.

#CREATOR-OWNER is a role that is assigned to anyone who creates an object. Normally, the #CREATOR-OWNER has ownership of the object by default, but this behavior can be changed for security reasons.

Security principals are also called grantees.



IBM Training

Users and groups

- The directory service defines the security principals.
- Users are assigned to groups.
- Use groups as primary security principals whenever possible.
- Example for a Finance department

Group name	Users who are members
Finance Admins	**Adam, Allison, Steve**
Finance Managers	**May, mark**
Finance Clerks	**Carol, Charles**
Finance Reviewers	**Richard, Roberta**

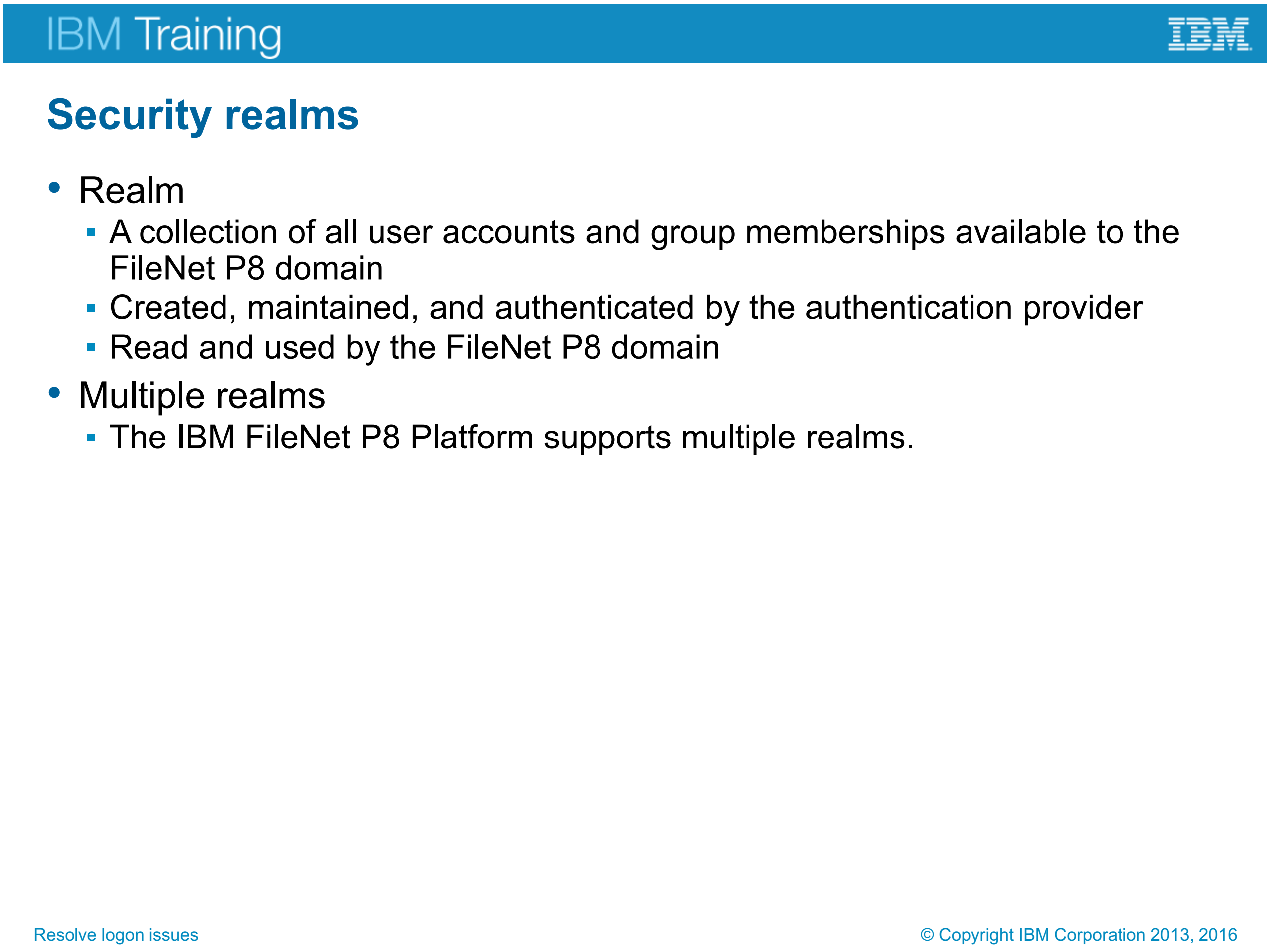
Resolve logon issues

© Copyright IBM Corporation 2013, 2016

Figure 1-6. Users and groups

Personnel changes occur often. When these changes occur, it is much more efficient to change group membership than to reconfigure security.

The directory service is responsible for linking the user to the group so that the solution builder can assign security exclusively to groups.



IBM Training

Security realms

- Realm
  - A collection of all user accounts and group memberships available to the FileNet P8 domain
  - Created, maintained, and authenticated by the authentication provider
  - Read and used by the FileNet P8 domain
- Multiple realms
  - The IBM FileNet P8 Platform supports multiple realms.

Resolve logon issues

© Copyright IBM Corporation 2013, 2016

Figure 1-7. Security realms

Help paths

FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the FileNet P8 infrastructure>FileNet P8 domains

> http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.ce.admin.tasks.doc/aboutem/dom_concepts.htm

FileNet P8 Platform 5.2.1>Security>How to>Configure multiple realms

> http://www.ibm.com/support/knowledgecenter/en/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh011.htm

Multiple realms

You can create multiple authentication realms on your application server. For each authentication realm that you create, you must also create a corresponding directory configuration in Content Platform Engine so that the users and groups in the authentication realm can be authorized. Content Platform Engine requires that all directory services be accessible at run time. If one becomes inaccessible, Content Platform Engine cannot run, even though other directory services are still running. Configure LDAP failover for each directory service to avoid this problem.

Logons from unconfigured LDAP realms

IBM FileNet Content Manager can be configured to allow or disallow log on by users who belong to groups that exist in unconfigured LDAP realms. However, the user must belong to a configured realm.

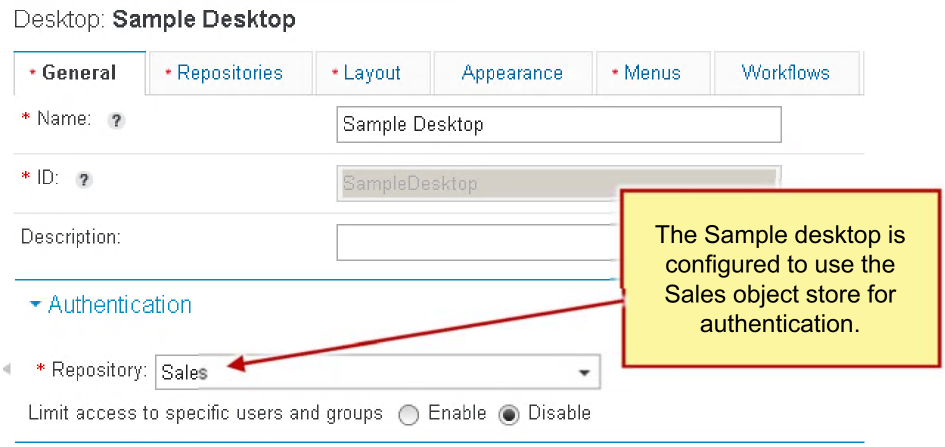
Hidden group logons

FileNet Content Manager can authenticate users who are members of hidden security groups in the LDAP directory.

IBM Training

IBM Content Navigator Desktop

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



* Name: Sample Desktop

* ID: SampleDesktop

Description:

Authentication

* Repository: Sales

Limit access to specific users and groups ○ Enable ● Disable

The Sample desktop is configured to use the Sales object store for authentication.

Resolve logon issues

Figure 1-8. IBM Content Navigator Desktop

Help path

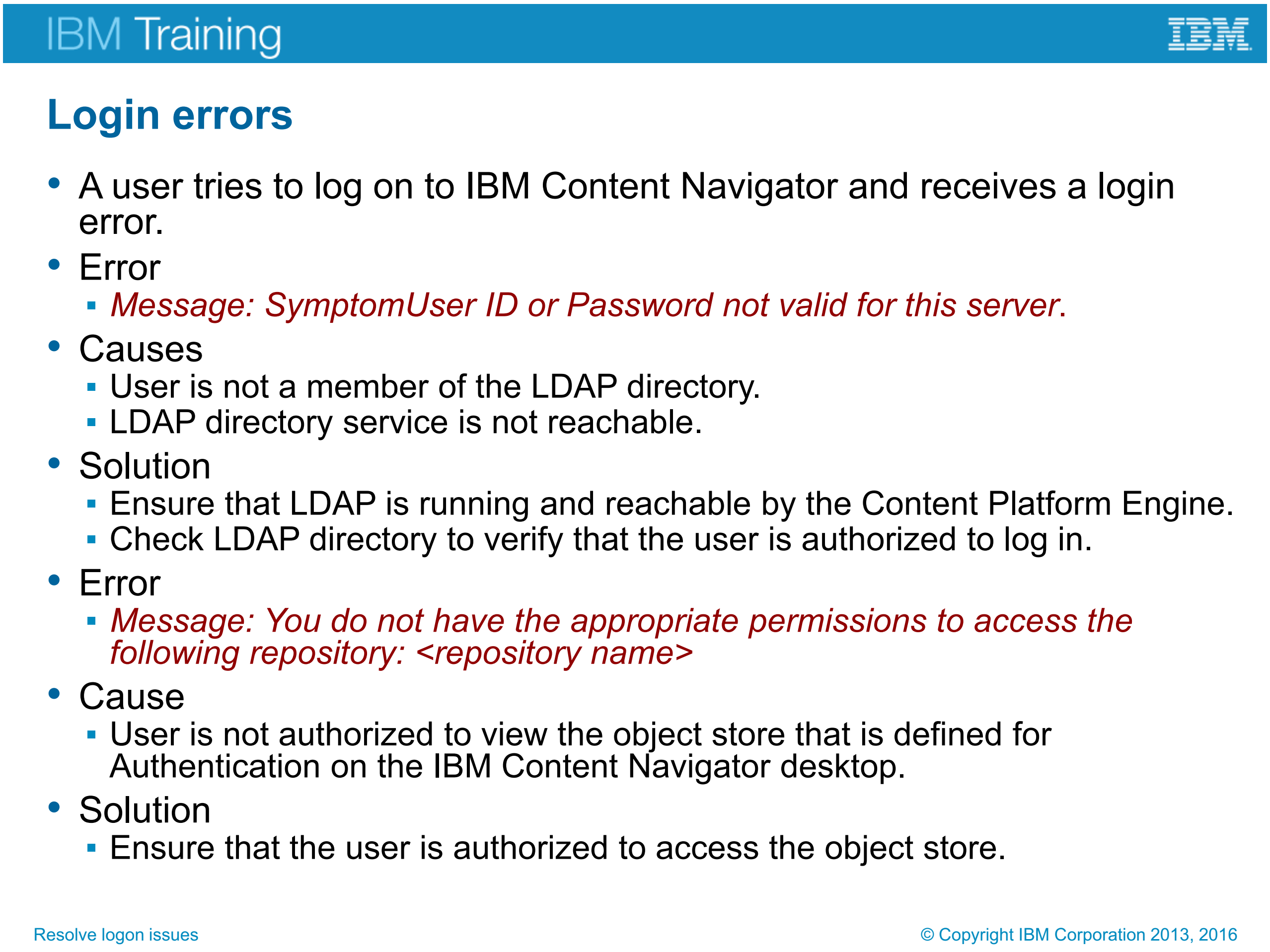
Content Navigator>Content Navigator 2.0.3>Planning, installing, and configuring IBM Content Navigator>Administering IBM Content Navigator components>Configuring the IBM Content Navigator web client>Defining desktops

http://www.ibm.com/support/knowledgecenter/SSEUEX_2.0.3/com.ibm.installingeuc.doc/eucco006.htm

To log in to an IBM Content Navigator Desktop, a user must have access to the object store that is defined for authentication on that desktop. This extra layer of security is beyond what is required by the object store. A user can log in to Administration Console for Content Platform Engine but be unable to log in to the IBM Content Navigator Desktop if that user is not authorized on that object store.

Note

Although a user might be able to log on to Administration Console, that user must also have authorization to change anything.



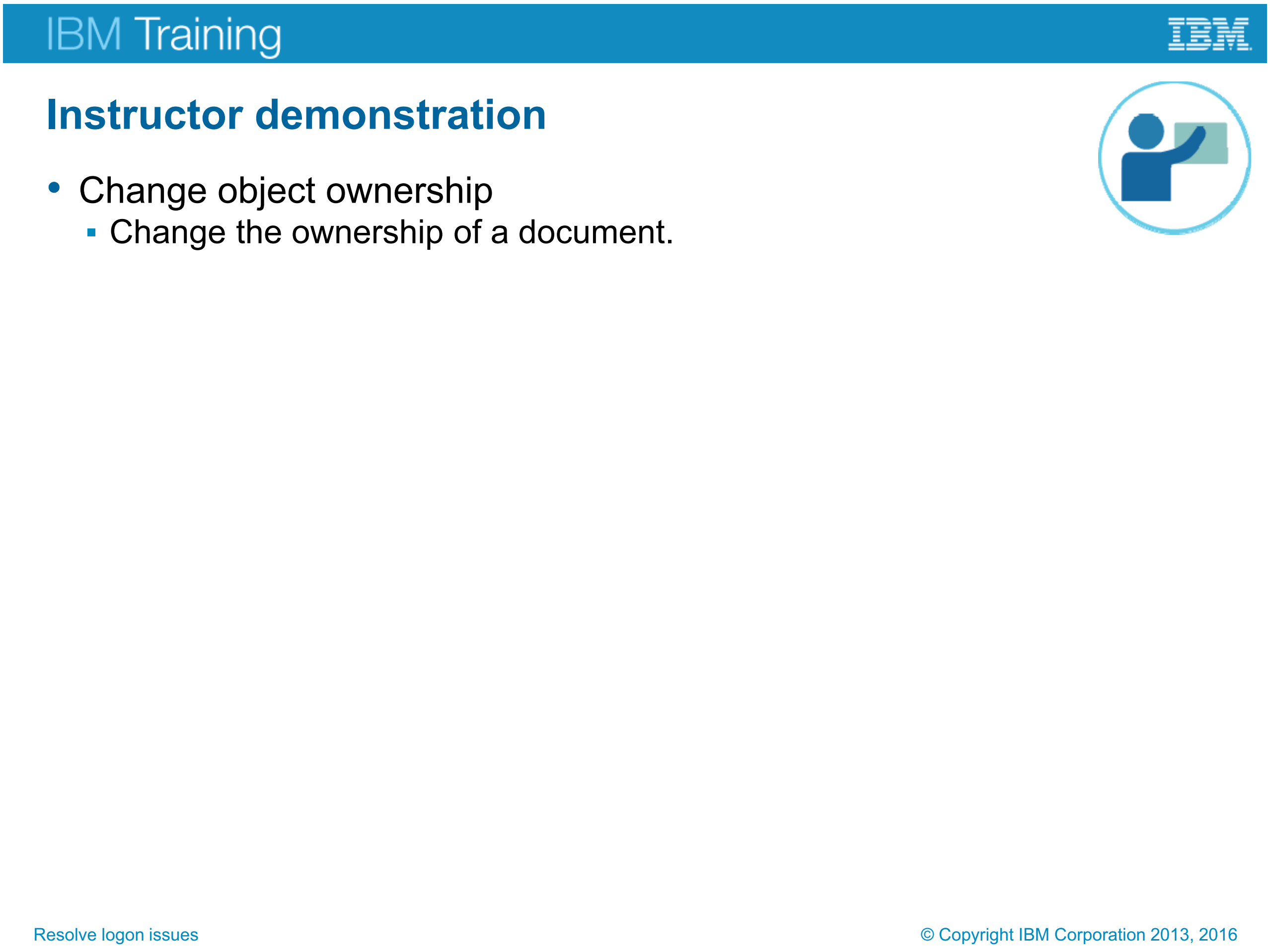
IBM Training

Login errors

- A user tries to log on to IBM Content Navigator and receives a login error.
- Error
  - *Message: SymptomUser ID or Password not valid for this server.*
- Causes
  - User is not a member of the LDAP directory.
  - LDAP directory service is not reachable.
- Solution
  - Ensure that LDAP is running and reachable by the Content Platform Engine.
  - Check LDAP directory to verify that the user is authorized to log in.
- Error
  - *Message: You do not have the appropriate permissions to access the following repository: <repository name>*
- Cause
  - User is not authorized to view the object store that is defined for Authentication on the IBM Content Navigator desktop.
- Solution
  - Ensure that the user is authorized to access the object store.

Resolve logon issues

Figure 1-9. Login errors



IBM Training

IBM

Instructor demonstration

- Change object ownership
  - Change the ownership of a document.

Resolve logon issues

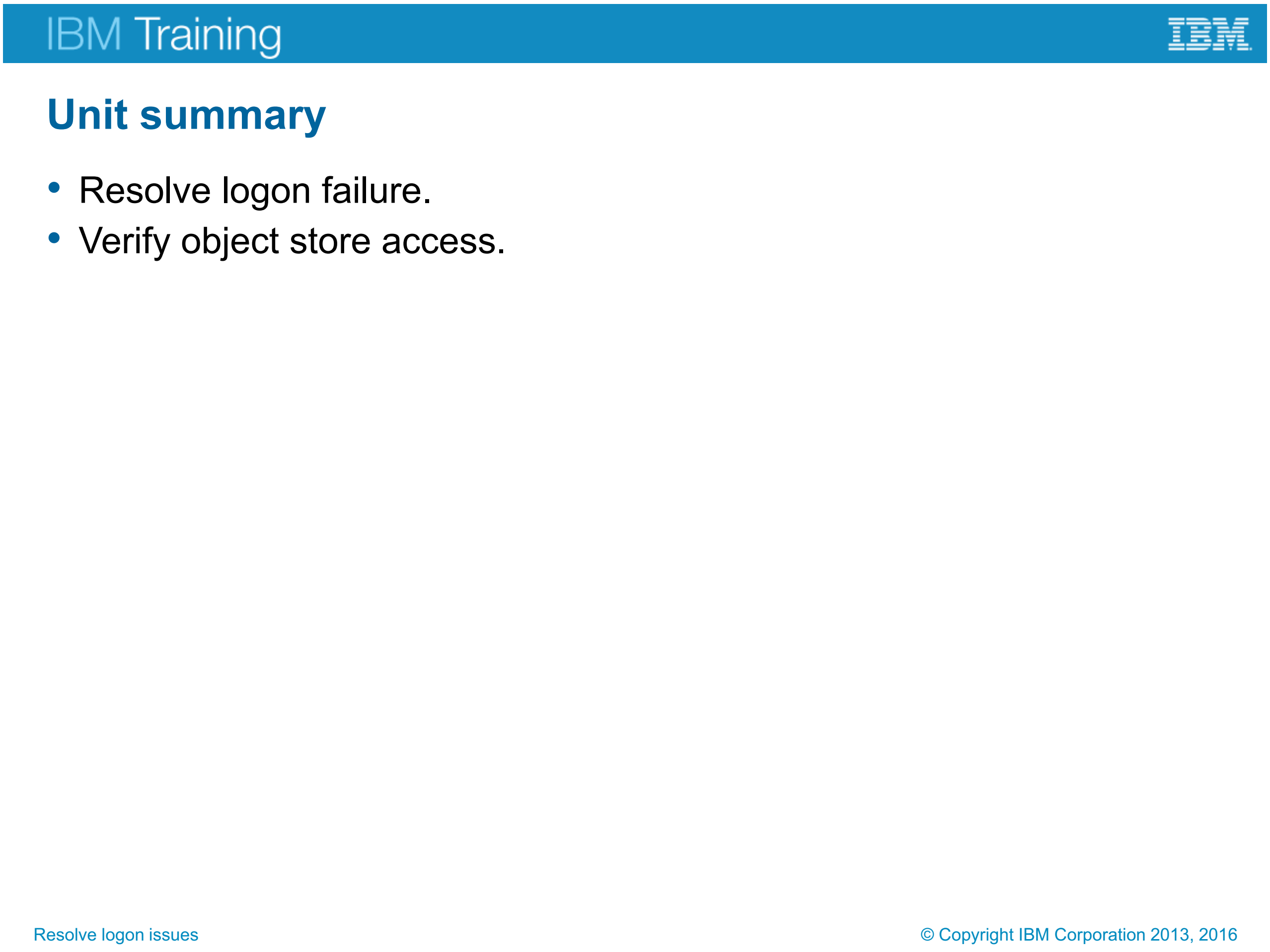
© Copyright IBM Corporation 2013, 2016

Figure 1-10. Instructor demonstration

Add a document as a user, such as Carol.

Log into ACCE as p8admin.

Use ACCE to change the owner of the document to a different user, such as Charles.



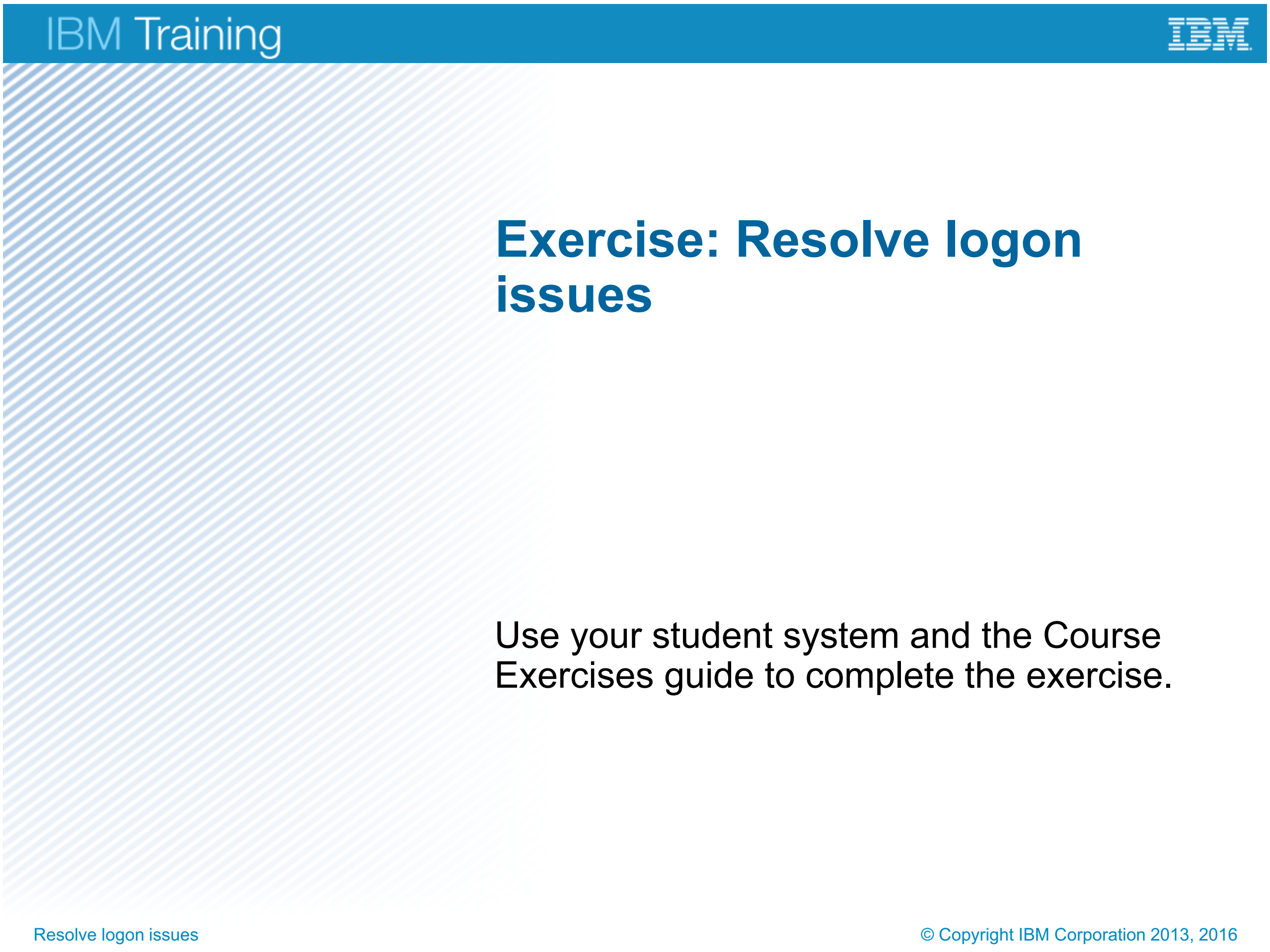
IBM Training

Unit summary

- Resolve logon failure.
- Verify object store access.

Resolve logon issues

Figure 1-11. Unit summary



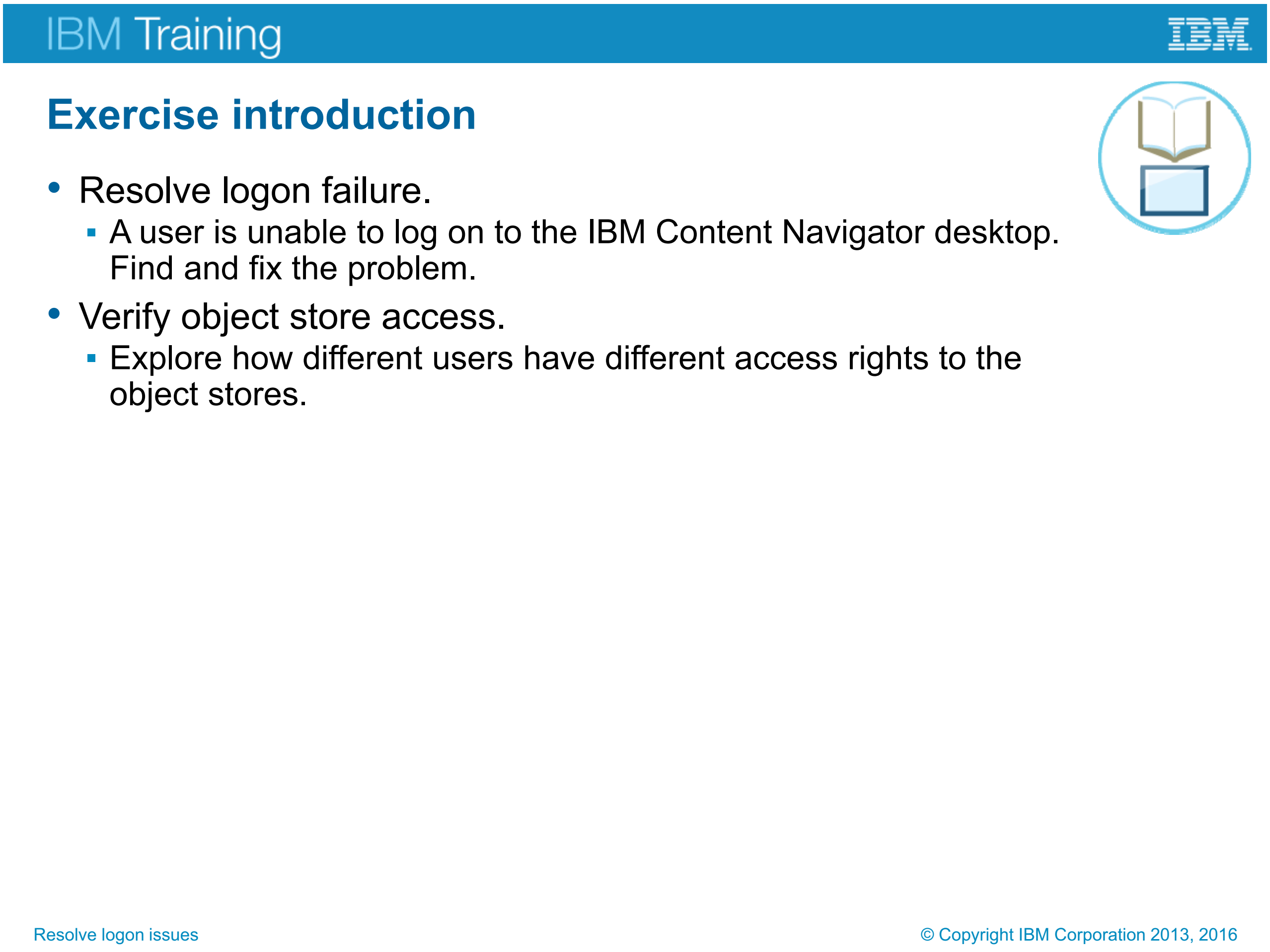
IBM Training

Exercise: Resolve logon issues

Use your student system and the Course Exercises guide to complete the exercise.

Resolve logon issues

Figure 1-12. Exercise: Resolve logon issues



IBM Training

Exercise introduction

- Resolve logon failure.
  - A user is unable to log on to the IBM Content Navigator desktop. Find and fix the problem.
- Verify object store access.
  - Explore how different users have different access rights to the object stores.

Resolve logon issues

Figure 1-13. Exercise introduction

Unit 2. Modify direct security

Estimated time

00:30

Overview

This unit describes how to modify direct security on objects.

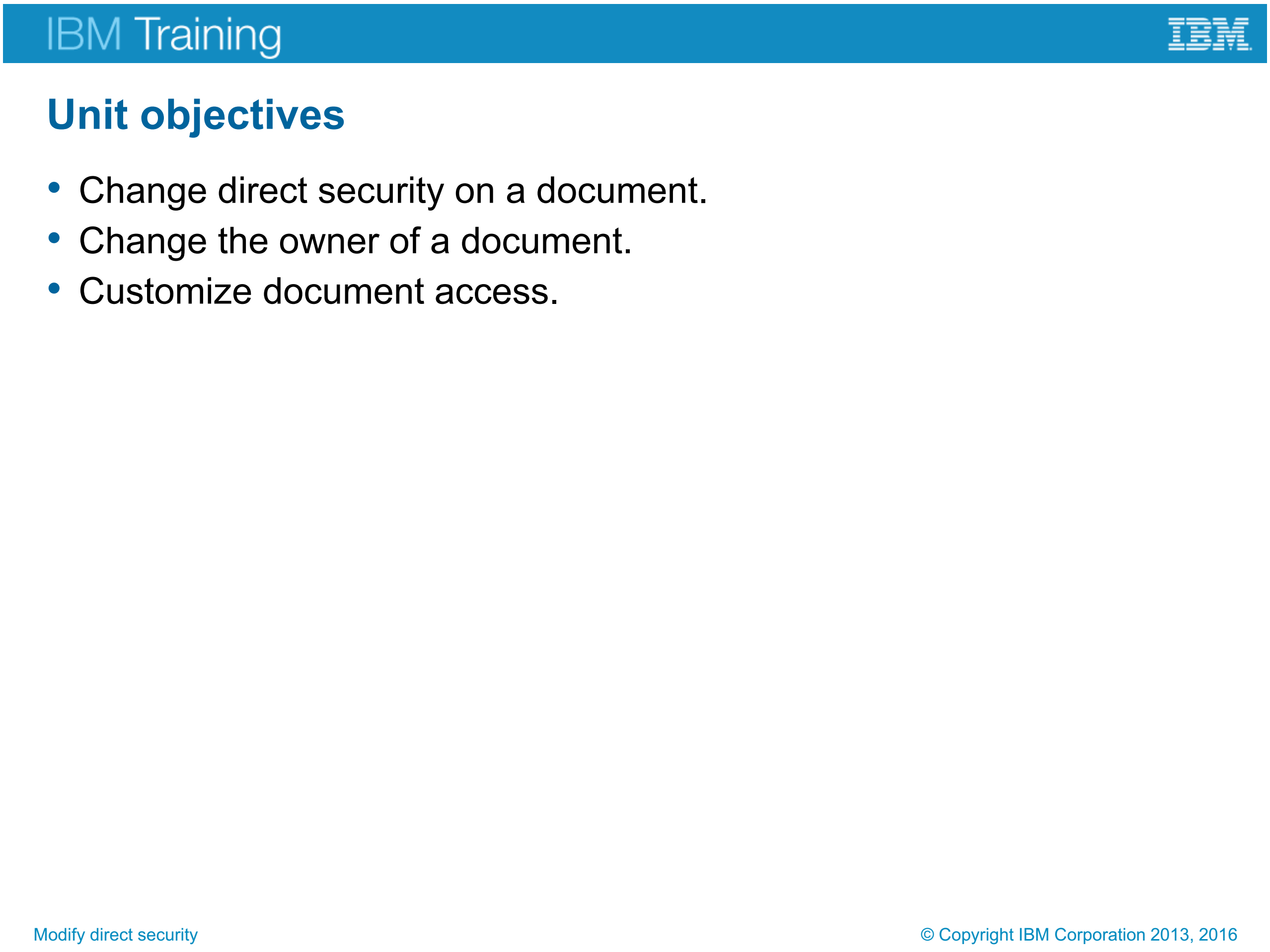
How you will check your progress

- Checkpoint
- Machine exercises

References

IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSNW2F



IBM Training

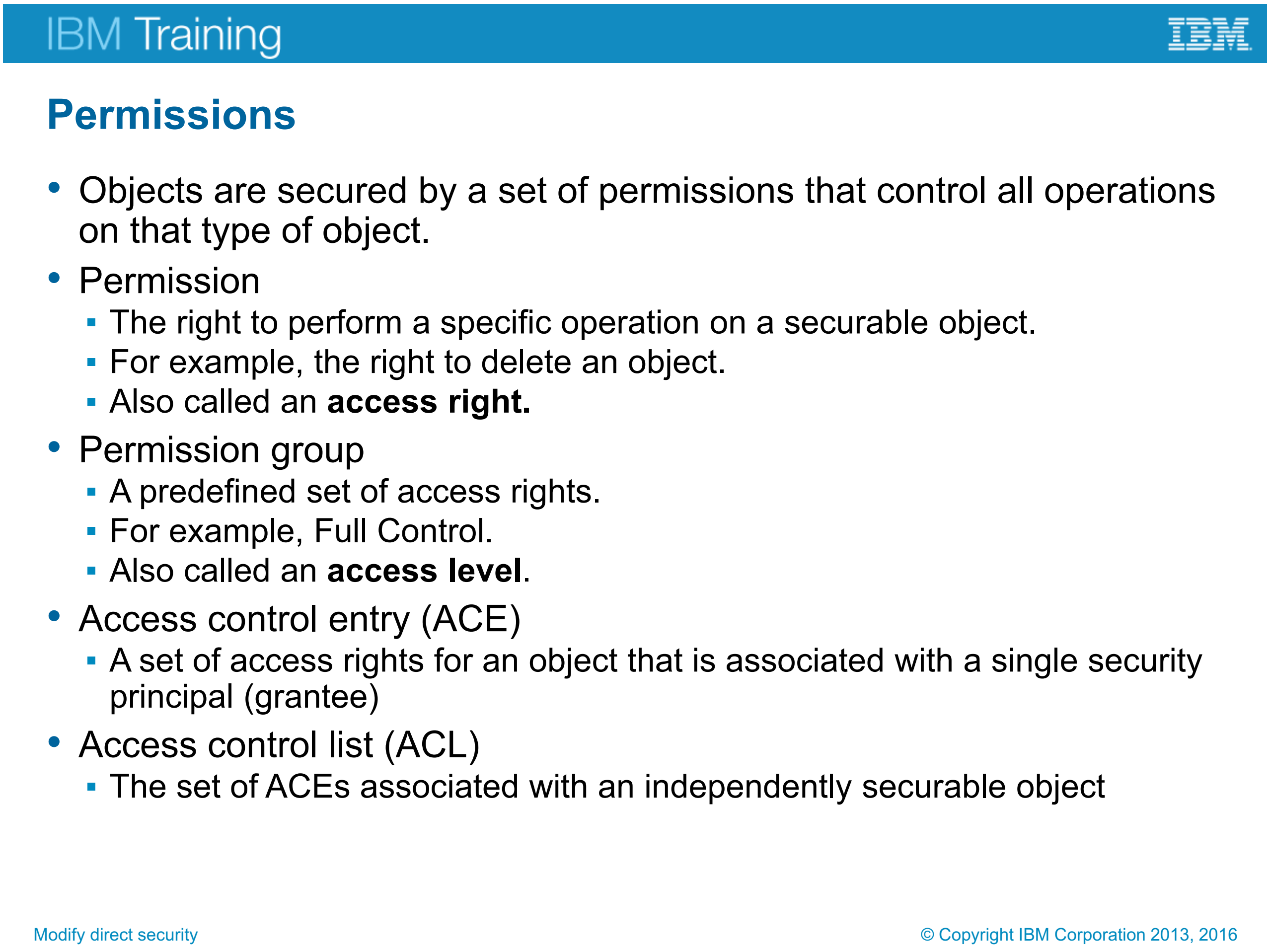
Unit objectives

- Change direct security on a document.
- Change the owner of a document.
- Customize document access.

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-1. Unit objectives



IBM Training

Permissions

- Objects are secured by a set of permissions that control all operations on that type of object.
- Permission
  - The right to perform a specific operation on a securable object.
  - For example, the right to delete an object.
  - Also called an **access right.**
- Permission group
  - A predefined set of access rights.
  - For example, Full Control.
  - Also called an **access level**.
- Access control entry (ACE)
  - A set of access rights for an object that is associated with a single security principal (grantee)
- Access control list (ACL)
  - The set of ACEs associated with an independently securable object

Modify direct security

Figure 2-2. Permissions

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>About access rights

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa050.htm

The examples that follow are securable object store objects:

Object stores

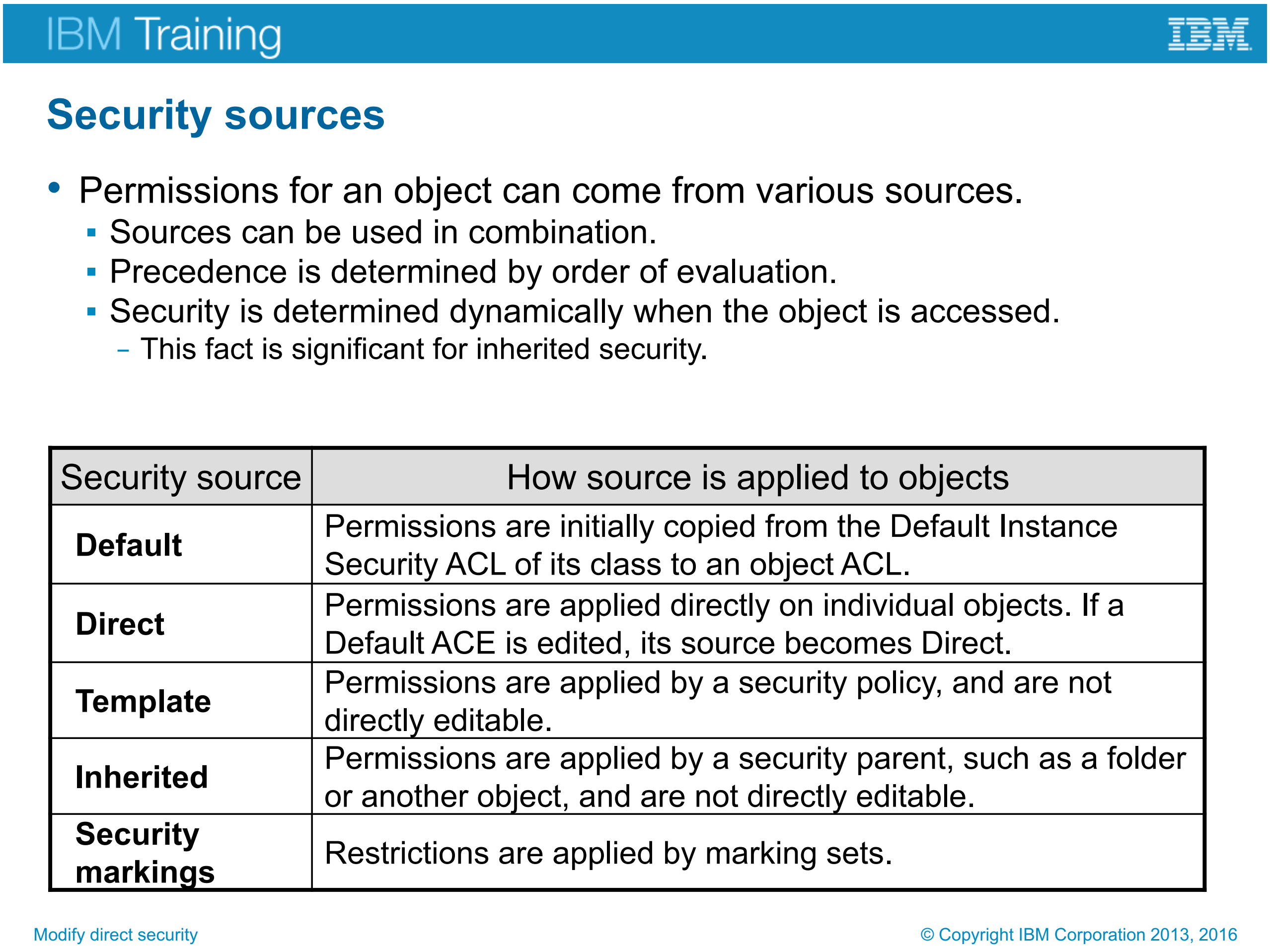
Folders

Documents

Document classes

Property templates

Event actions and subscriptions



IBM Training

Security sources

- Permissions for an object can come from various sources.
  - Sources can be used in combination.
  - Precedence is determined by order of evaluation.
  - Security is determined dynamically when the object is accessed.
    - This fact is significant for inherited security.

Security source	How source is applied to objects
Default	Permissions are initially copied from the Default Instance Security ACL of its class to an object ACL.
Direct	Permissions are applied directly on individual objects. If a Default ACE is edited, its source becomes Direct.
Template	Permissions are applied by a security policy, and are not directly editable.
Inherited	Permissions are applied by a security parent, such as a folder or another object, and are not directly editable.
Security markings	Restrictions are applied by marking sets.

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-3. Security sources

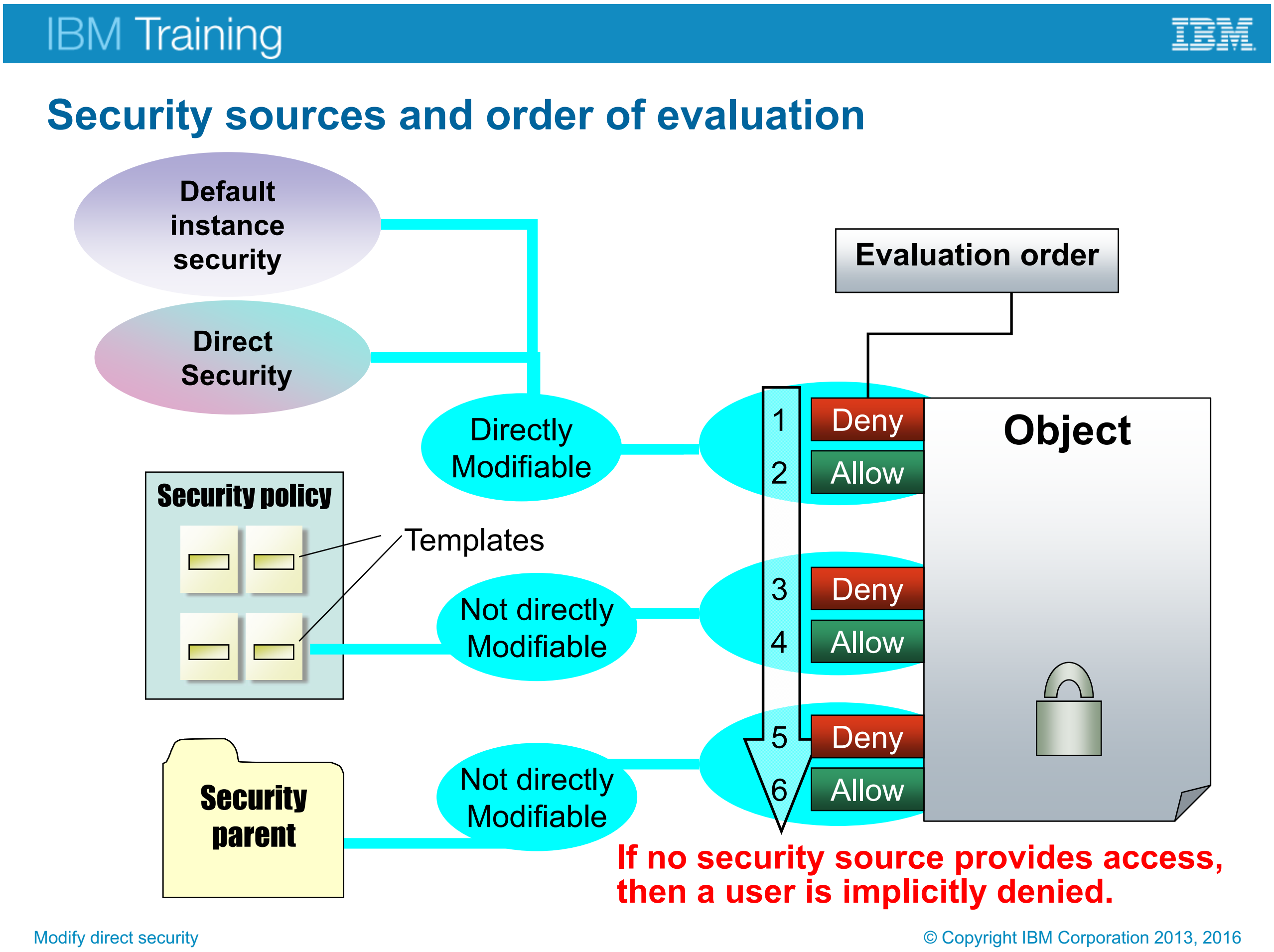
Help paths

FileNet P8 Platform 5.2.1>Security>Authorization>About access rights>ACE source: Default, Direct, Inherited, Template

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa053.htm

Security can be configured in various ways, and you have many complex choices to make as you design a security model.

Security markings are commonly used with records management applications and are beyond the scope of this course.



IBM Training

Security sources and order of evaluation

If no security source provides access, then a user is implicitly denied.

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-4. Security sources and order of evaluation

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>About access rights>Allow or Deny and order of evaluation

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa055.htm

Each security permission can be set to Allow or Deny. If a principal has nothing that is allowed, access is denied. When nothing is allowed, it is implicitly denied. Most security scenarios can function perfectly with Allows only. In a system that uses Allows only, security from multiple sources are summed. The order of evaluation is not important. Example, if Fred is Allowed view properties from Direct security, and he also has Major Versioning from a template, then he has both capabilities.

The order of evaluation is important to understand only if you use Denial. This order determines how security issues are resolved. If someone is allowed access by one security source and denied by another security source, the security is determined by which source comes first in the order of evaluation. For example, if a security policy template allows access and folder inheritance denies access, the user is allowed to view the object because the template security is evaluated before inherited security.

Security policies can be configured not to preserve direct security. Therefore, if a policy is configured to ignore direct security, a user can be granted access to an object even if that user is otherwise denied access by direct security.

If a user is allowed access to a document as an individual user but belongs to a group that is denied access, then that user does **not** have access to the object.

- When objects are added, the default instance security on the class becomes Direct security on the new object.
- Both Direct and Default security can be modified on the object. After either type of security is modified, the source is listed as Direct.

Security markings provide an extra, optional layer of security that is primarily designed for the records management marketplace, but the feature can also be used by non-records management applications.

Implicit denial

On systems that use Allows only, access is granted and where not granted is implicitly denied.

Using Allows exclusively simplifies the security system. Unless explicit denials are required for some reason, it is best to avoid them.

Graphic

The graphic shows the source and priority of security sources:

Default instance security becomes direct security when the object is created, and direct security is directly modifiable on an object.

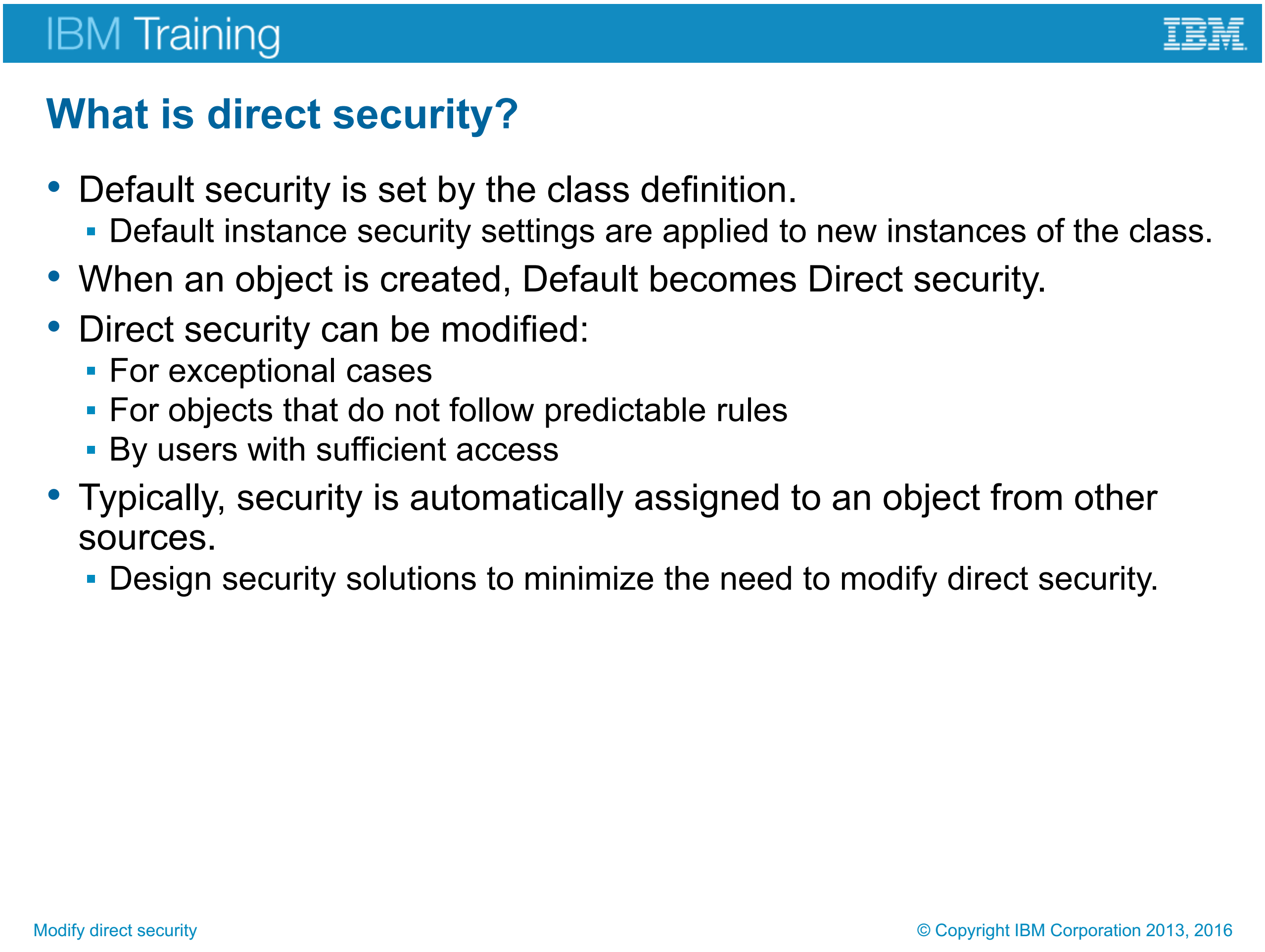
Security policies and security parents can provide security to an object, which is not directly modifiable on the object that uses them.

The evaluation order is presented:

- Default instance and direct security are evaluated first.
- Security policies that provide security are evaluated next.
- Security parents that provide security are evaluated last.

In each case, a Deny access setting takes precedence over an Allow access setting.

If no security source provides access, then a user is implicitly denied access to the object.



IBM Training

What is direct security?

- Default security is set by the class definition.
  - Default instance security settings are applied to new instances of the class.
- When an object is created, Default becomes Direct security.
- Direct security can be modified:
  - For exceptional cases
  - For objects that do not follow predictable rules
  - By users with sufficient access
- Typically, security is automatically assigned to an object from other sources.
  - Design security solutions to minimize the need to modify direct security.

Modify direct security

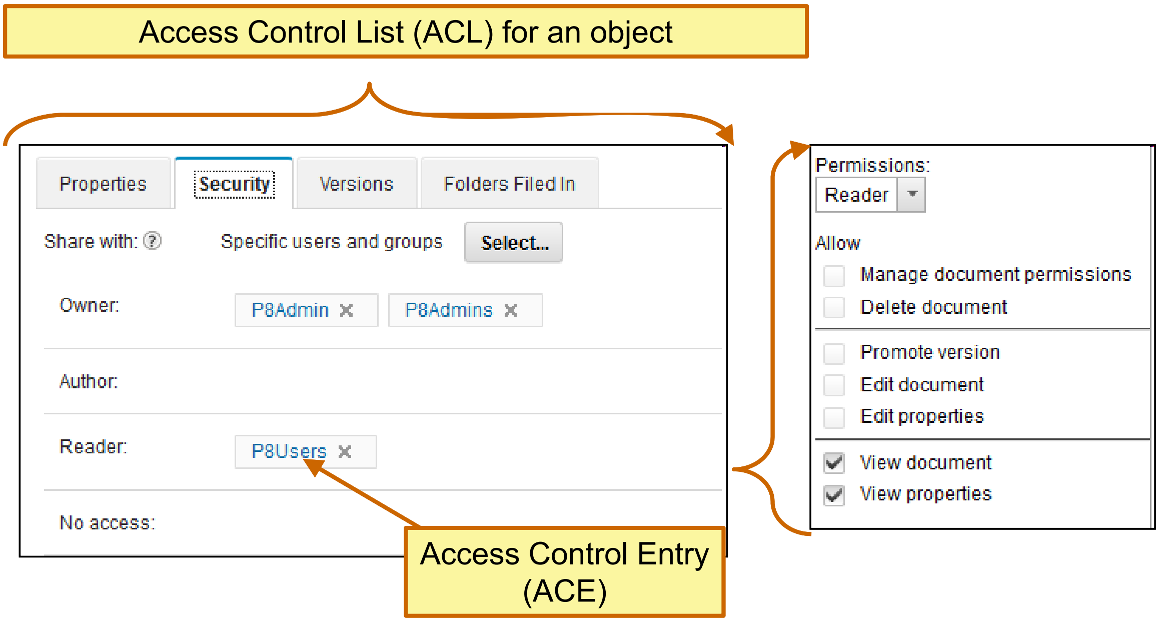
Figure 2-5. What is direct security?

Both Default and Direct security can be modified on an object. After either type of security is modified, the source is listed as Direct.

To modify the security on an object, a user must have the Modify Permissions access right.

IBM Training

Access Control from IBM Content Navigator


Access Control List (ACL) for an object
Access Control Entry (ACE)

Properties | Security | Versions | Folders Filed In

Share with: Specific users and groups Select...

Owner: P8Admin ✕ P8Admins ✕

Author:

Reader: P8Users ✕

No access:

Permissions: Reader

Allow

☐ Manage document permissions
☐ Delete document
☐ Promote version
☐ Edit document
☐ Edit properties
☑ View document
☑ View properties

Modify direct security

Figure 2-6. Access Control from IBM Content Navigator

Help path

Content Navigator>Content Navigator 2.0.3>Getting started with IBM Content Navigator>Content security

> http://www.ibm.com/support/knowledgecenter/SSEUEX_2.0.3/com.ibm.usingeuc.doc/euche014.htm

The graphic shows a typical document ACL in IBM Content Navigator. The expansion on the right shows the permissions for a particular ACE.

You access the ACL in IBM Content Navigator by going to the object's Properties, then opening the Security tab.

The permission level that you specify determines the tasks that the user can perform as follows. You can further limit access to the document by using the advanced options to remove specific tasks from a permission set of the user.

In IBM Content Navigator, access control is displayed by roles.

Owner

A user with owner permissions can do almost anything:

Manage the document security

Delete the document

Promote the document to a major version

Edit the document

Edit the document properties

View the document

View the document properties

Author

A user with author permissions has slightly fewer permissions:

Promote the document to a major version

Edit the document

Edit the document properties

View the document

View the document properties

Reader

A user with reader permissions has limited access:

View the document

View the document properties

No access

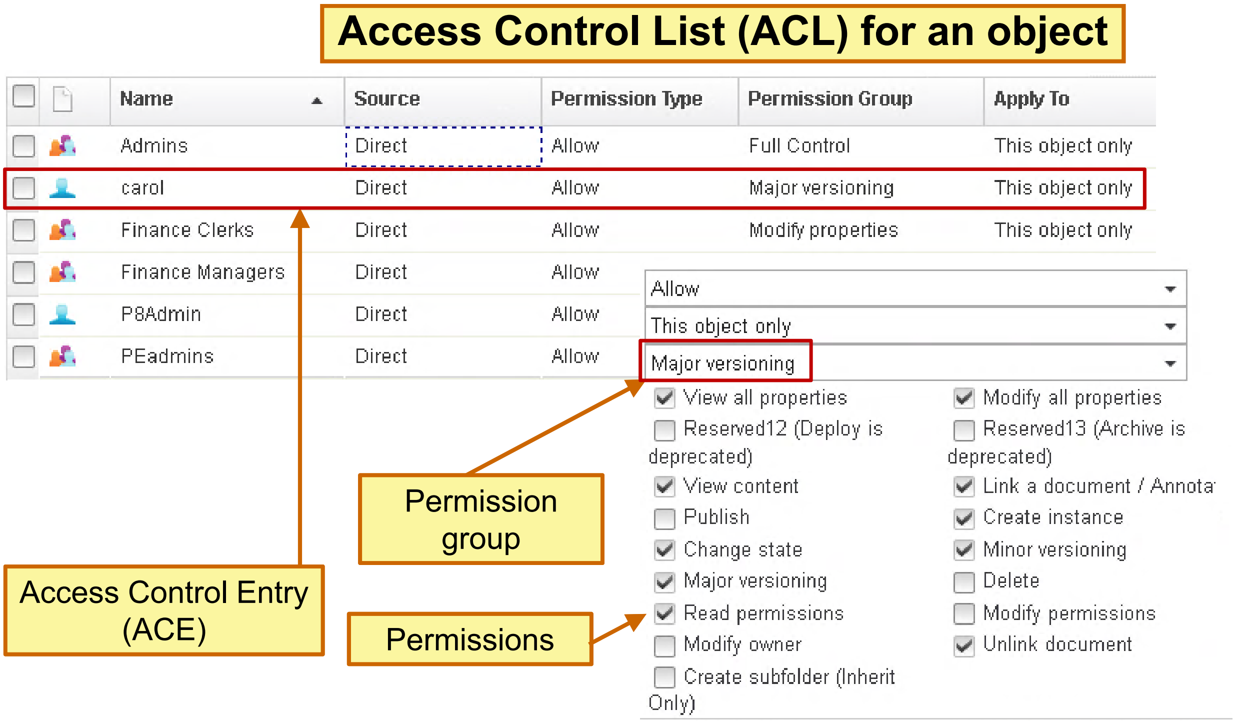
A user with no access is prevented from accessing the document.

Custom

You can customize the permissions for a user with Advanced security in IBM Content Navigator. Principals with custom permissions show a diamond icon to indicate that custom permissions are applied.

IBM Training

Access Control in Administration Console



Access Control List (ACL) for an object

□		Name ▲	Source	Permission Type	Permission Group	Apply To
□		Admins	Direct	Allow	Full Control	This object only
□		carol	Direct	Allow	Major versioning	This object only
□		Finance Clerks	Direct	Allow	Modify properties	This object only
□		Finance Managers	Direct	Allow		
□		P8Admin	Direct	Allow		
□		PEadmins	Direct	Allow		

Allow

This object only

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 / Annota
- ☑ Create instance
- ☑ Minor versioning
- □ Delete
- □ Modify permissions
- ☑ Unlink document

Permission group

Access Control Entry (ACE)

Permissions

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-7. Access Control in Administration Console

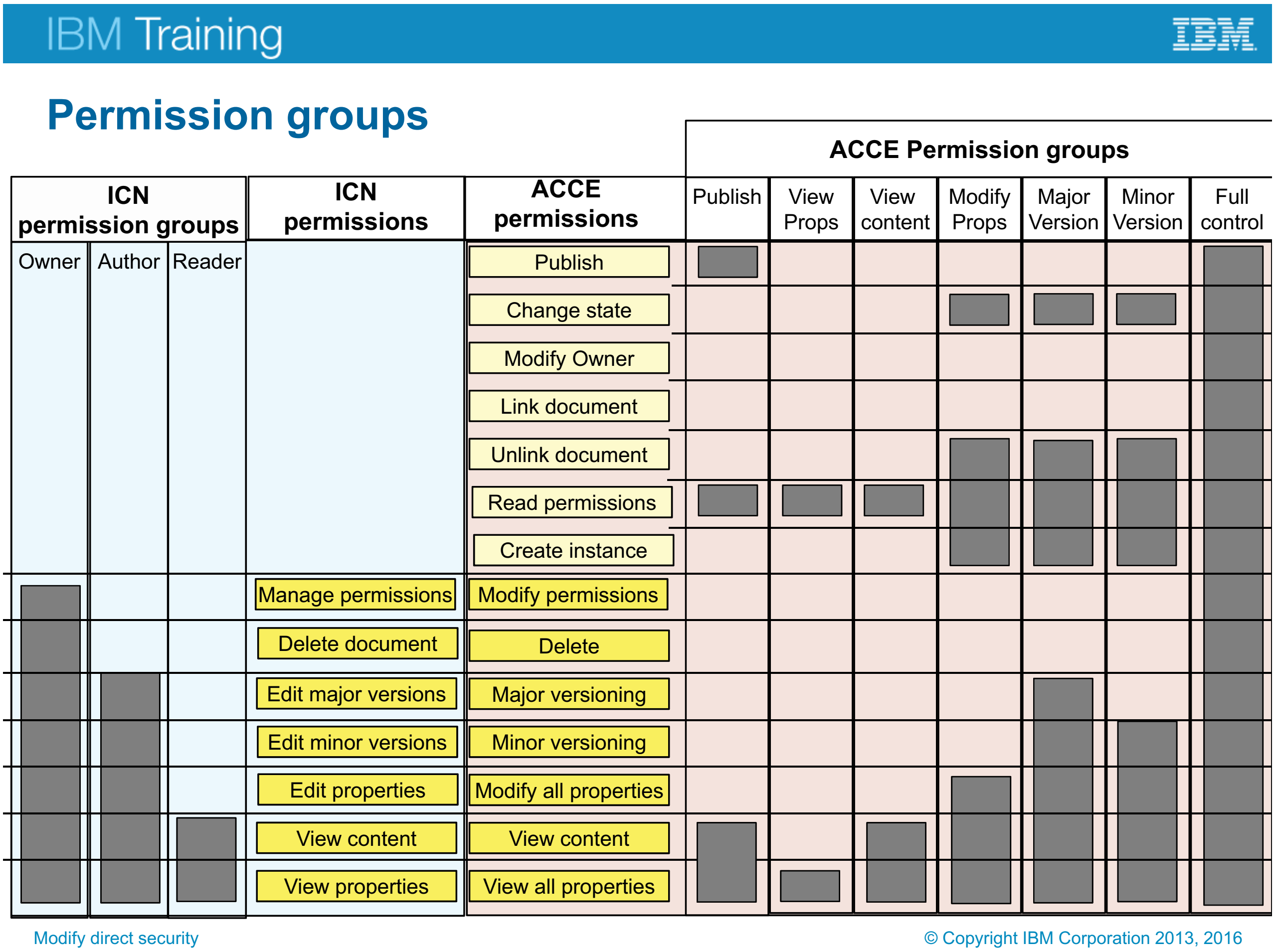
The graphic shows a typical document ACL in Administration Console for Content Platform Engine. The insert shows the individual permissions for one ACE.

In Administration Console for Content Platform Engine, the administrator can specify a permission group, such as Full Control or Major Versioning to select commonly used groups of permissions. You can customize the permissions of the ACE by selecting or clearing individual permissions. The resulting ACE is shown as having Custom permissions.

You can access the ACL for an object on the security tab for that object.

Note

In the diagram, the security source is explicitly labeled in the Source column.



IBM Training

Permission groups

ICN permission groups			ICN permissions	ACCE permissions	ACCE Permission groups						
Owner	Author	Reader			Publish	View Props	View content	Modify Props	Major Version	Minor Version	Full control
				Publish	■						■
				Change state				■	■	■	■
				Modify Owner							■
				Link document							■
				Unlink document				■	■	■	■
				Read permissions	■	■	■	■	■	■	■
				Create instance				■	■	■	■
■			Manage permissions	Modify permissions							■
■			Delete document	Delete							■
■	■		Edit major versions	Major versioning					■		■
■	■		Edit minor versions	Minor versioning					■	■	■
■	■		Edit properties	Modify all properties				■	■	■	■
■	■	■	View content	View content	■		■	■	■	■	■
■	■	■	View properties	View all properties	■	■	■	■	■	■	■

Modify direct security

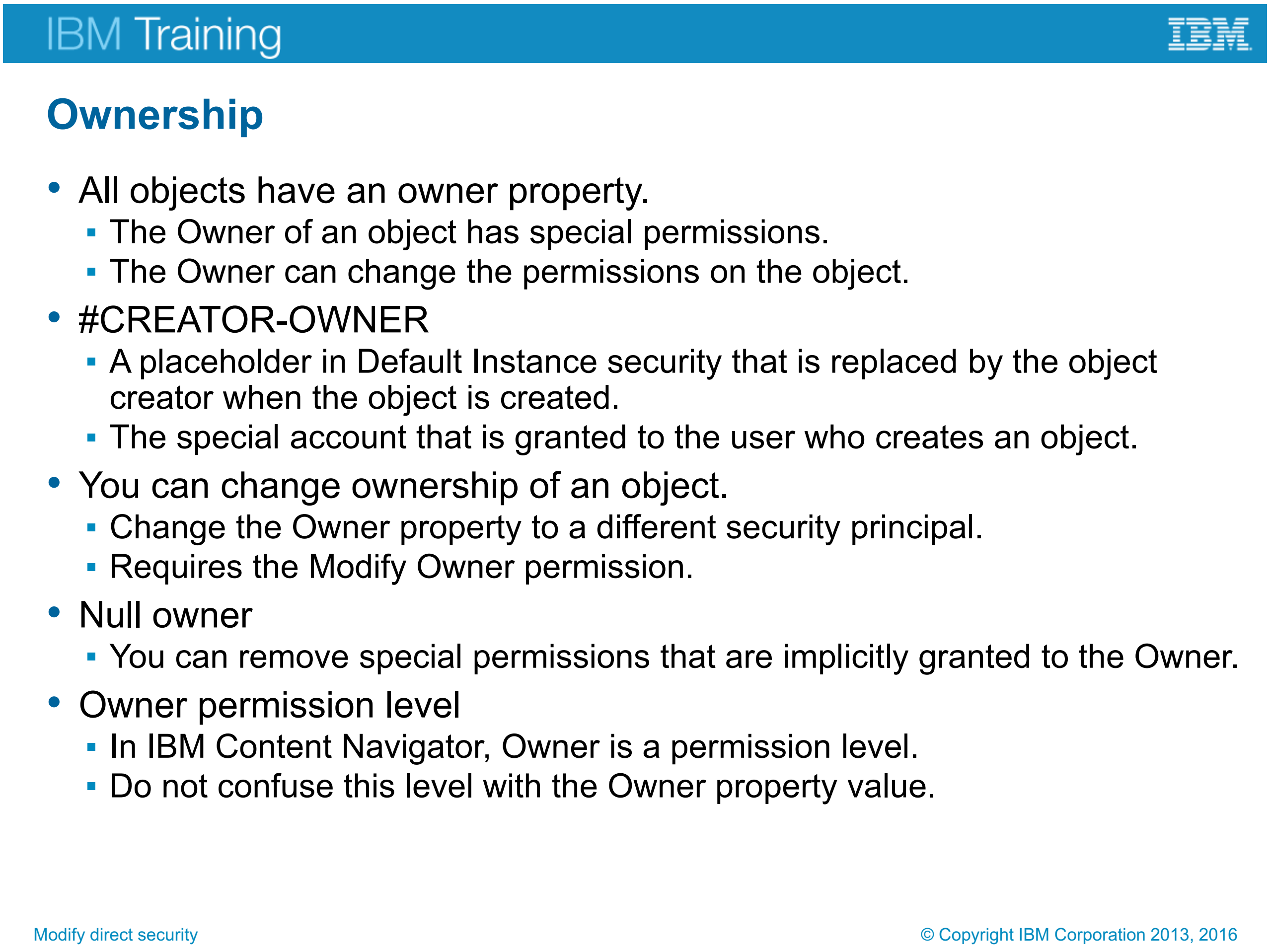
© Copyright IBM Corporation 2013, 2016

Figure 2-8. Permission groups

The graphic shows a graph of permissions for different permission groups and compares the editable permissions in IBM Content Navigator and Administration Console for Content Platform Engine.

Setting permissions on a document in IBM Content Navigator (ICN) and in Administration Console (ACCE) provide different experiences and different levels of granularity. Permissions that are granted in the Administration Console include all of the permissions that can be granted in Content Navigator, plus a few more permissions. Highlighted permissions have different names in each interface, but are functionally equivalent.

IBM Content Navigator provides a simple interface to quickly edit the most commonly used permissions. Use Administration Console for Content Platform Engine if you need to edit other permissions, such as the right to publish or change the state of a document.



IBM Training

Ownership

- All objects have an owner property.
  - The Owner of an object has special permissions.
  - The Owner can change the permissions on the object.
- #CREATOR-OWNER
  - A placeholder in Default Instance security that is replaced by the object creator when the object is created.
  - The special account that is granted to the user who creates an object.
- You can change ownership of an object.
  - Change the Owner property to a different security principal.
  - Requires the Modify Owner permission.
- Null owner
  - You can remove special permissions that are implicitly granted to the Owner.
- Owner permission level
  - In IBM Content Navigator, Owner is a permission level.
  - Do not confuse this level with the Owner property value.

Modify direct security

Figure 2-9. Ownership

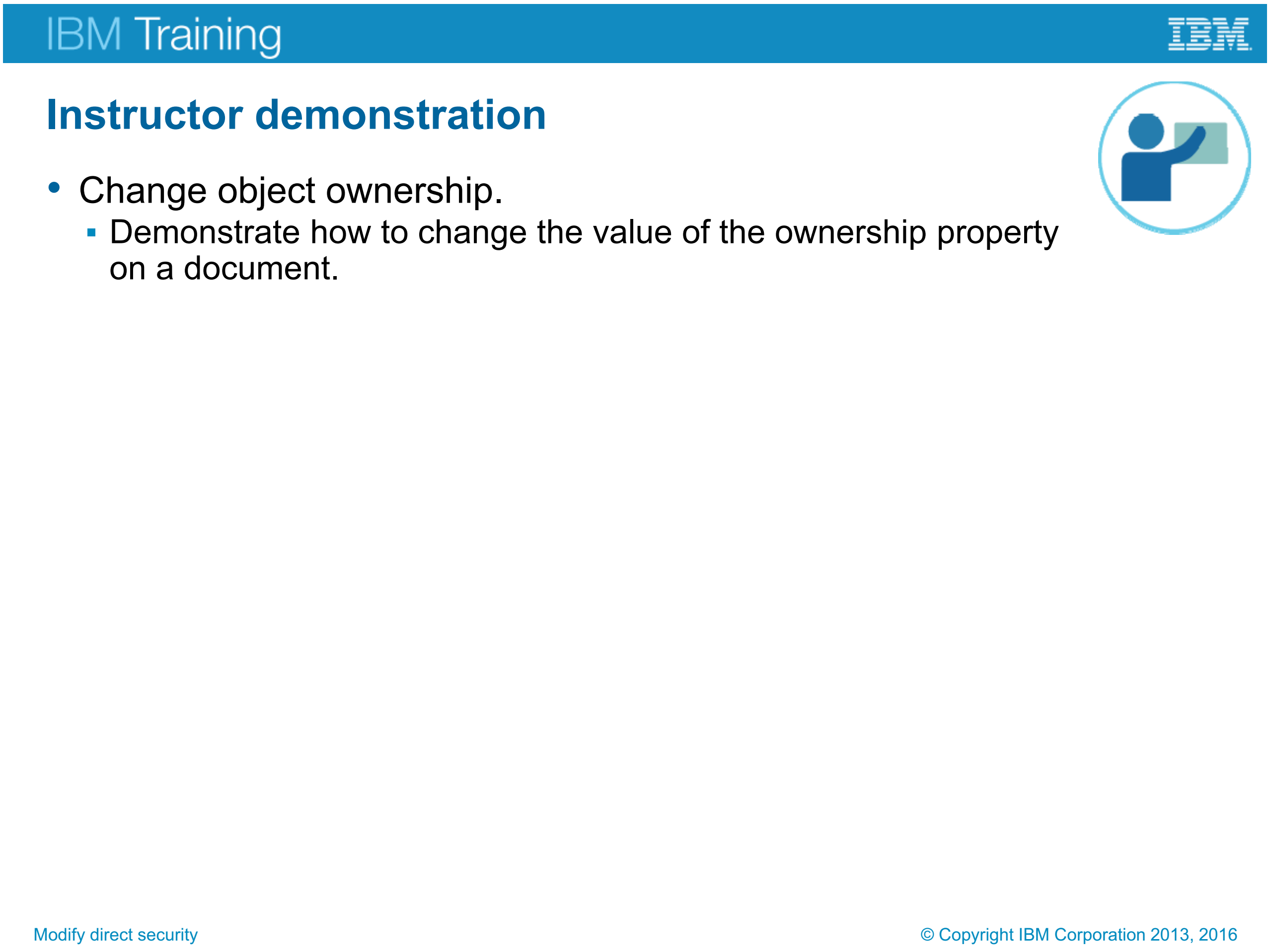
Help path

FileNet P8 Platform 5.2.1>Security>Authorization>Object ownership

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa071.htm

By default, #CREATOR-OWNER appears on the Security and Default Instance Security tabs of all instantiable classes, and is granted Full Control, with an inheritable depth of This object only. This account functions just like a normal user account, and its default permissions can be edited according to normal rules (that is, by users with appropriate permission).

When the ACE is inherited, the permissions that are granted to the #CREATOR-OWNER become the permissions that are granted to the object's current owner. For example, when a user creates a document based on a document class, that user takes on the #CREATOR-OWNER's permissions.



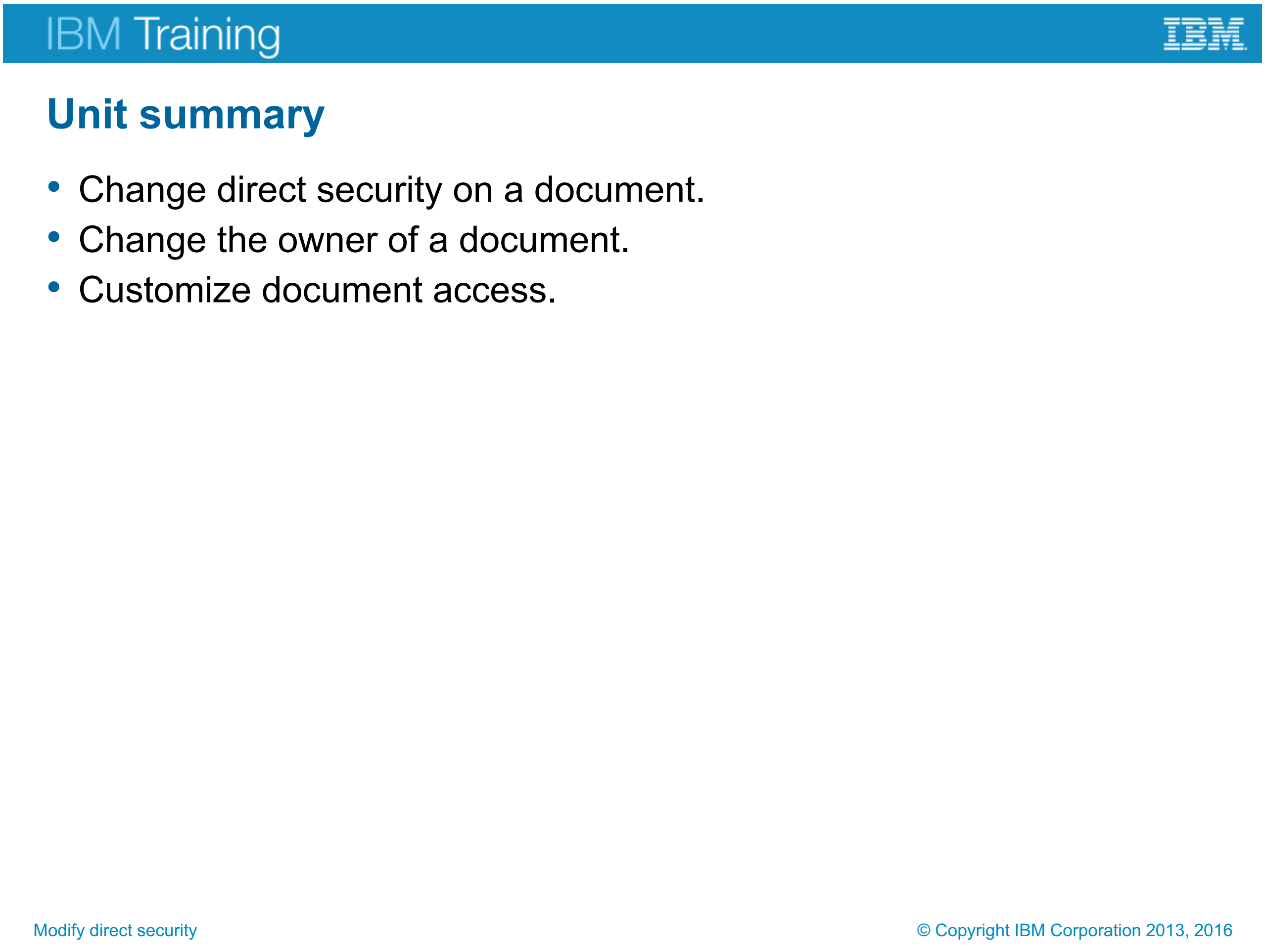
IBM Training

Instructor demonstration

- Change object ownership.
  - Demonstrate how to change the value of the ownership property on a document.

Modify direct security

Figure 2-10. Instructor demonstration



IBM Training

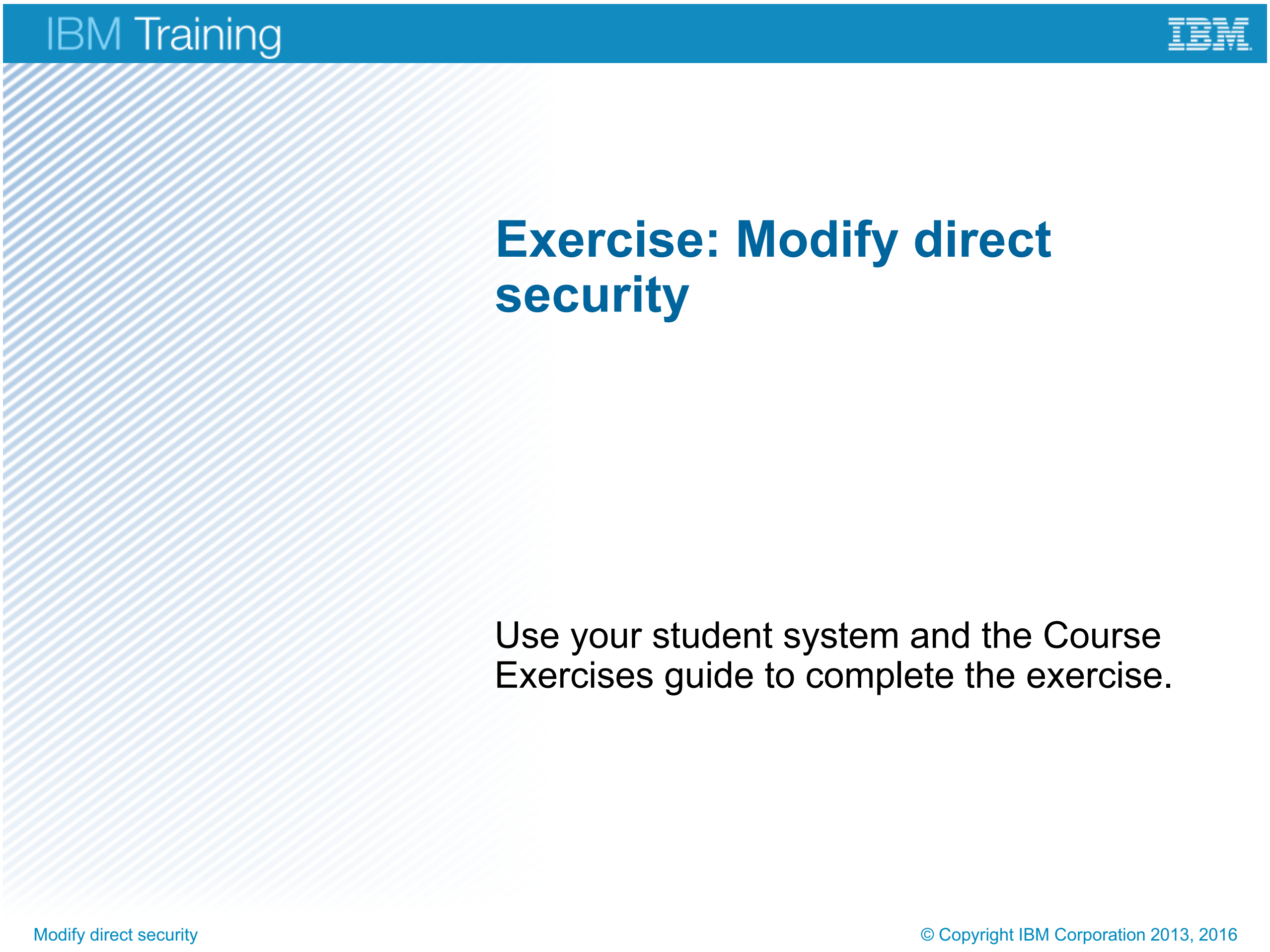
Unit summary

- Change direct security on a document.
- Change the owner of a document.
- Customize document access.

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-11. Unit summary



IBM Training

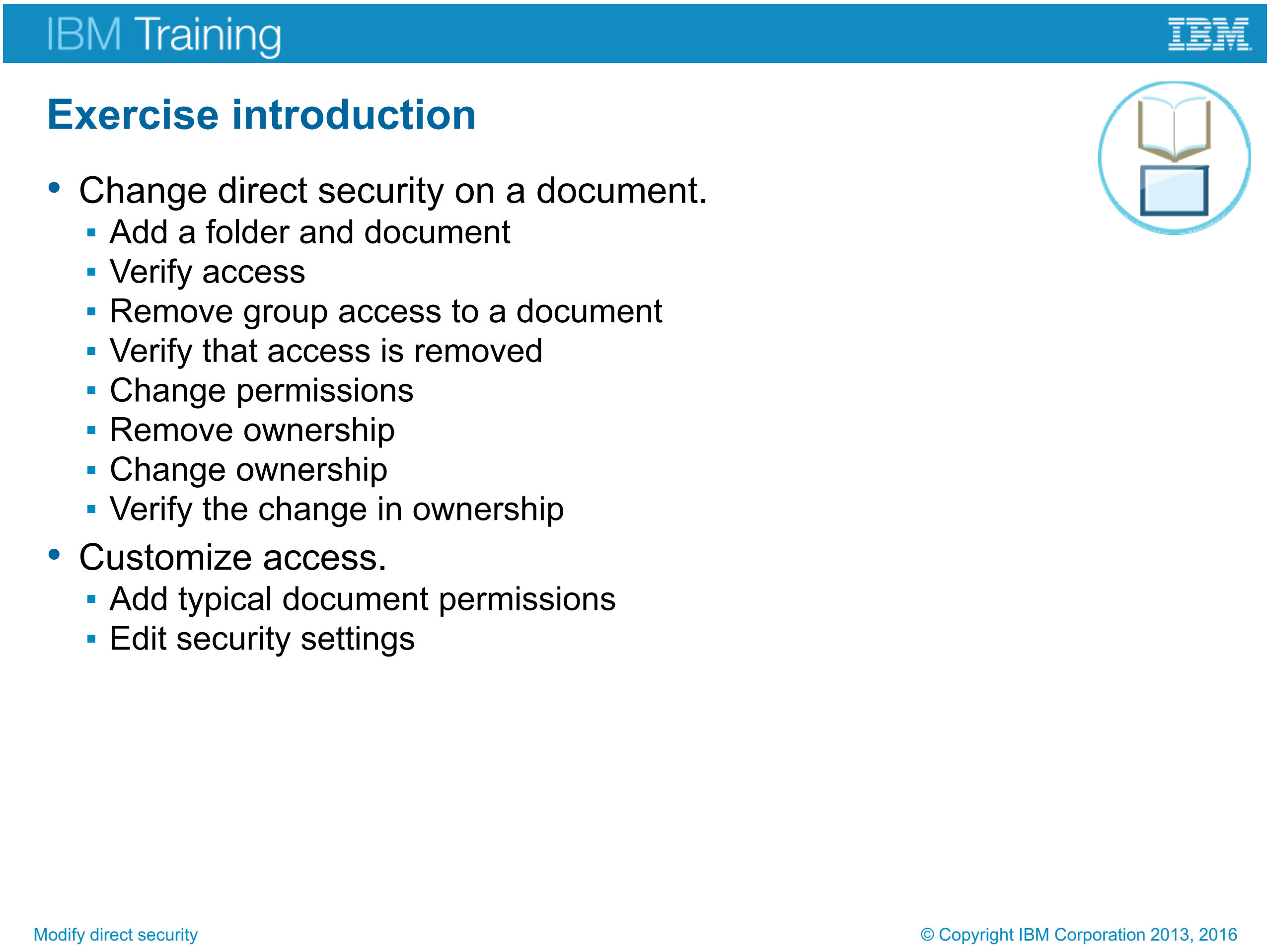
Exercise: Modify direct security

Use your student system and the Course Exercises guide to complete the exercise.

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-12. Exercise: Modify direct security



IBM Training

Exercise introduction

- Change direct security on a document.
  - Add a folder and document
  - Verify access
  - Remove group access to a document
  - Verify that access is removed
  - Change permissions
  - Remove ownership
  - Change ownership
  - Verify the change in ownership
- Customize access.
  - Add typical document permissions
  - Edit security settings

Modify direct security

© Copyright IBM Corporation 2013, 2016

Figure 2-13. Exercise introduction

Unit 3. Configure object store security

Estimated time

00:20

Overview

This unit describes how to configure security on a new object store.

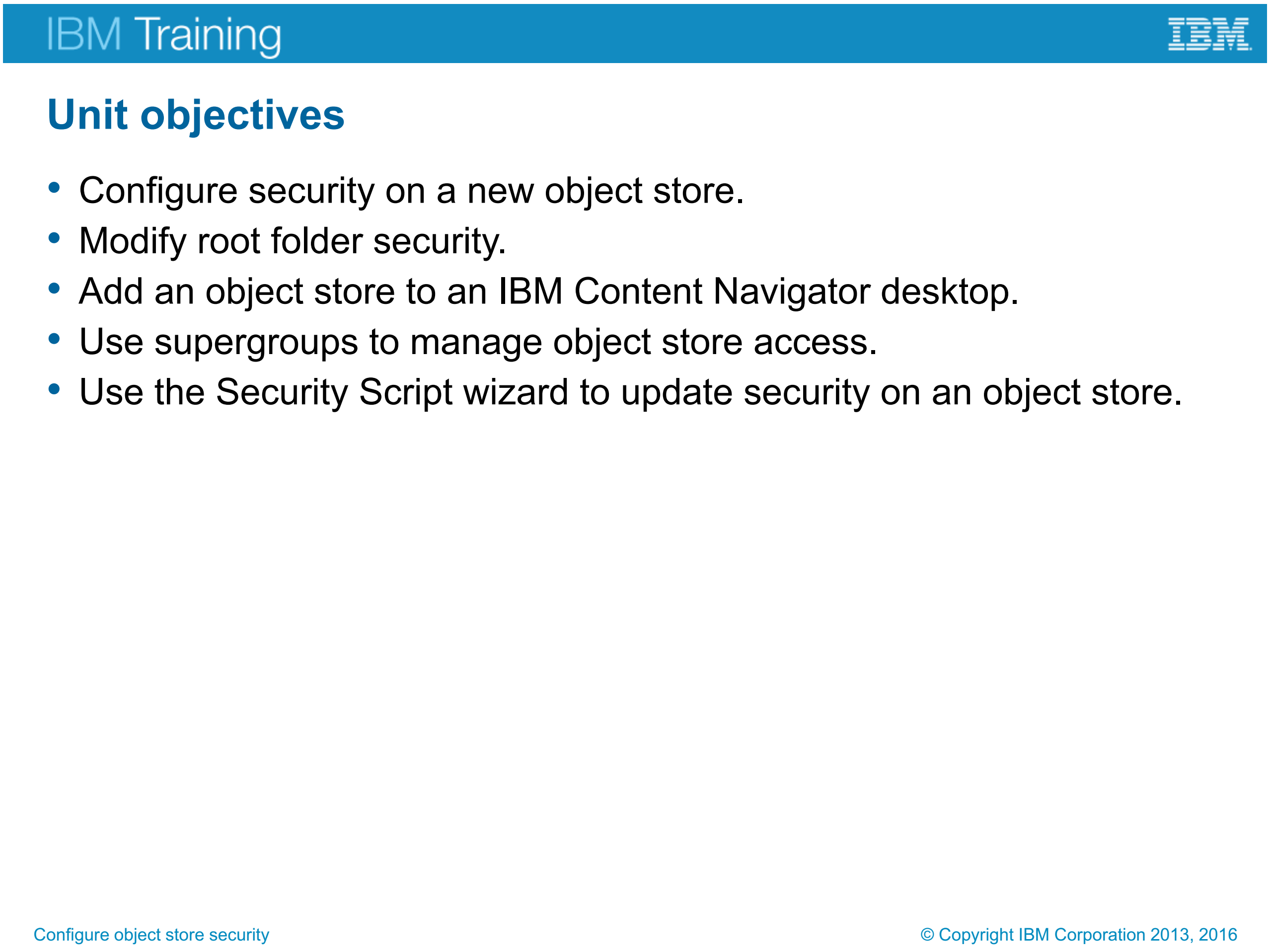
How you will check your progress

- Machine exercises

References

IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSNW2F



IBM Training

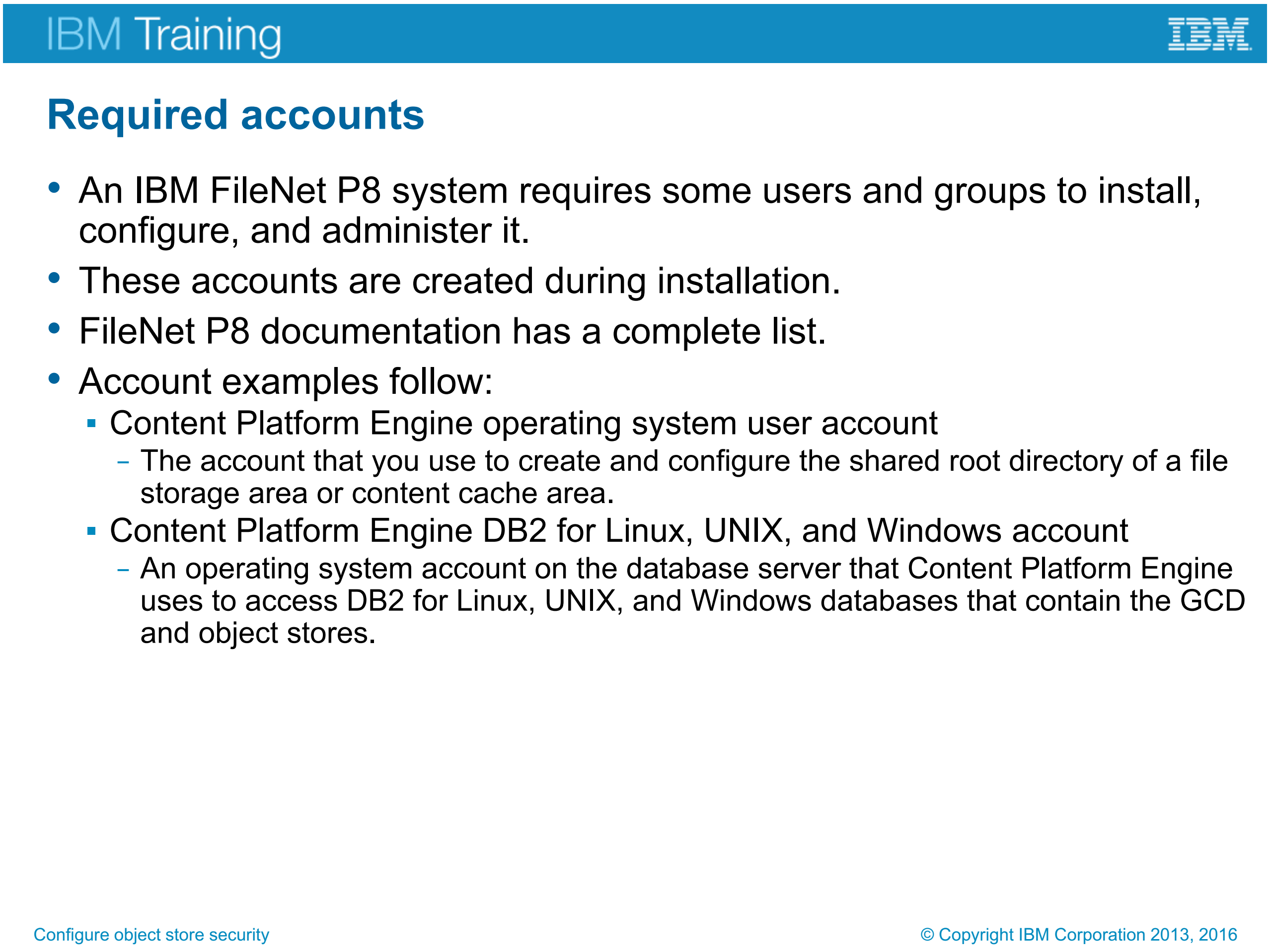
Unit objectives

- Configure security on a new object store.
- Modify root folder security.
- 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.

Configure object store security

© Copyright IBM Corporation 2013, 2016

Figure 3-1. Unit objectives



IBM Training

Required accounts

- An IBM FileNet P8 system requires some users and groups to install, configure, and administer it.
- These accounts are created during installation.
- FileNet P8 documentation has a complete list.
- Account examples follow:
  - Content Platform Engine operating system user account
    - The account that you use to create and configure the shared root directory of a file storage area or content cache area.
  - Content Platform Engine DB2 for Linux, UNIX, and Windows account
    - An operating system account on the database server that Content Platform Engine uses to access DB2 for Linux, UNIX, and Windows databases that contain the GCD and object stores.

Configure object store security

© Copyright IBM Corporation 2013, 2016

Figure 3-2. Required accounts

Help path

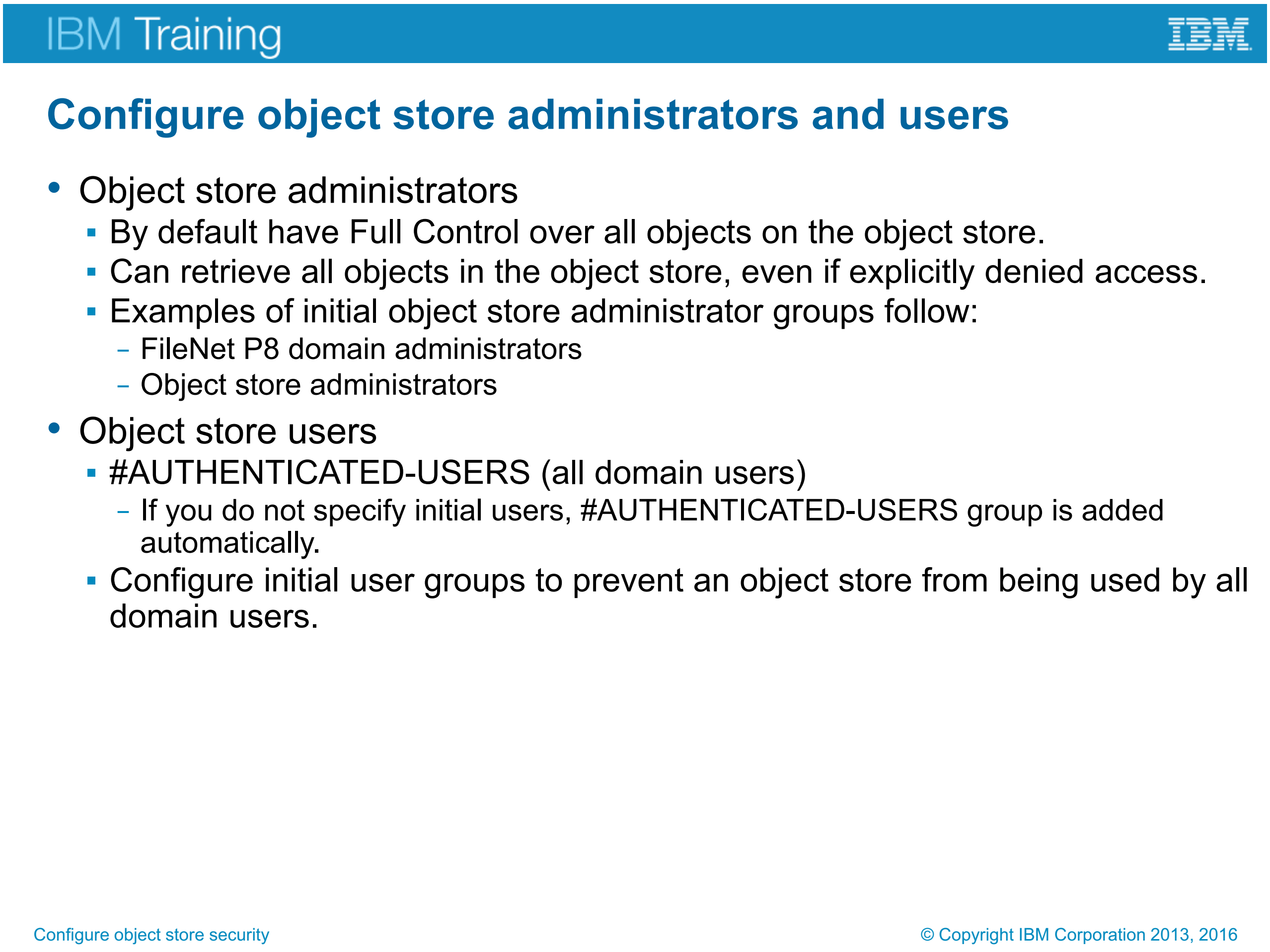
FileNet P8 Platform 5.2.1>Security>Users and groups required by FileNet P8

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psu000.htm

You must be a FileNet P8 domain administrator (the Global Configuration database, or GCD administrator) to create a new object store.

A GCD administrator has full control over the entire FileNet P8 domain object. The GCD administrator is automatically added as an object store administrator.

Object store administrators have full control over the object stores that they are responsible for. Each object store can have its own, unique administrator.



IBM Training

Configure object store administrators and users

- Object store administrators
  - By default have Full Control over all objects on the object store.
  - Can retrieve all objects in the object store, even if explicitly denied access.
  - Examples of initial object store administrator groups follow:
    - FileNet P8 domain administrators
    - Object store administrators
- Object store users
  - #AUTHENTICATED-USERS (all domain users)
    - If you do not specify initial users, #AUTHENTICATED-USERS group is added automatically.
  - Configure initial user groups to prevent an object store from being used by all domain users.

Configure object store security

Figure 3-3. Configure object store administrators and users

Help path

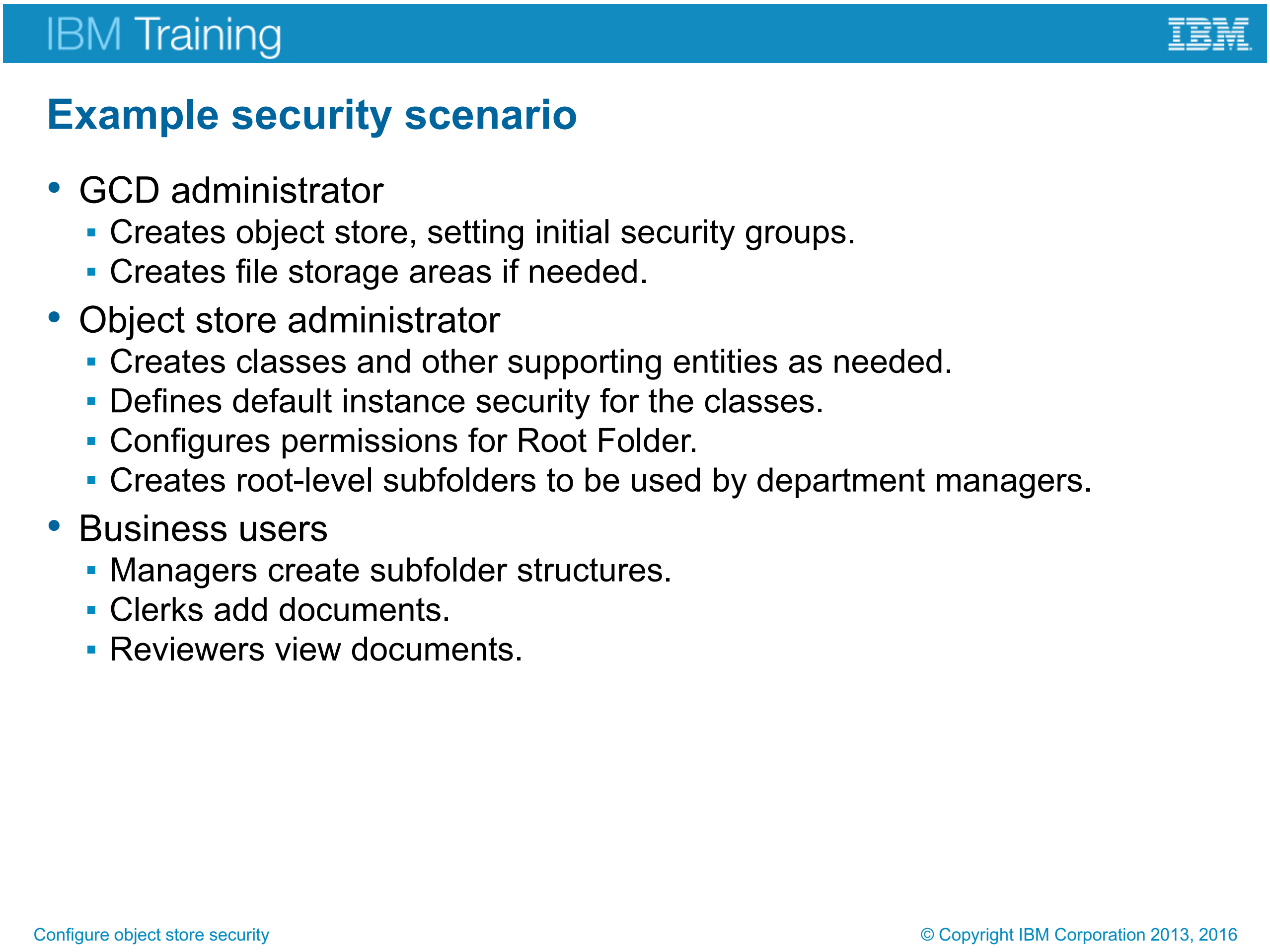
FileNet P8 Platform 5.2.1>Security>Authorization>Default security

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa056.htm

Object store administrators - When you create an object store, you can select groups to become the administrators of that specific object store. Object store administrators have Full Control over all objects on the object store by default. Object store administrators can retrieve all objects (but not necessarily view the content), even if they are removed from the ACL or explicitly denied access. When granted Full Control access level on an object store, these users are given WRITE_OWNER access, an API-level right that allows retrieving all objects.

Object store users - When you create an object store, you select one or more groups to have basic, nonadministrative access rights. If you do not specify any groups at the time of object store creation, the default value, #AUTHENTICATED-USERS, is automatically added. This default access right allows all domain users to have basic access to the object store (as long as they can access the IBM Content Navigator Authentication object store). If you specify a group without including #AUTHENTICATED-USERS, then only that group has basic access. Other domain users are not allowed to use the object store.

If a security principal is removed from an object store ACL, that person or group is denied access to the entire object store.



IBM Training

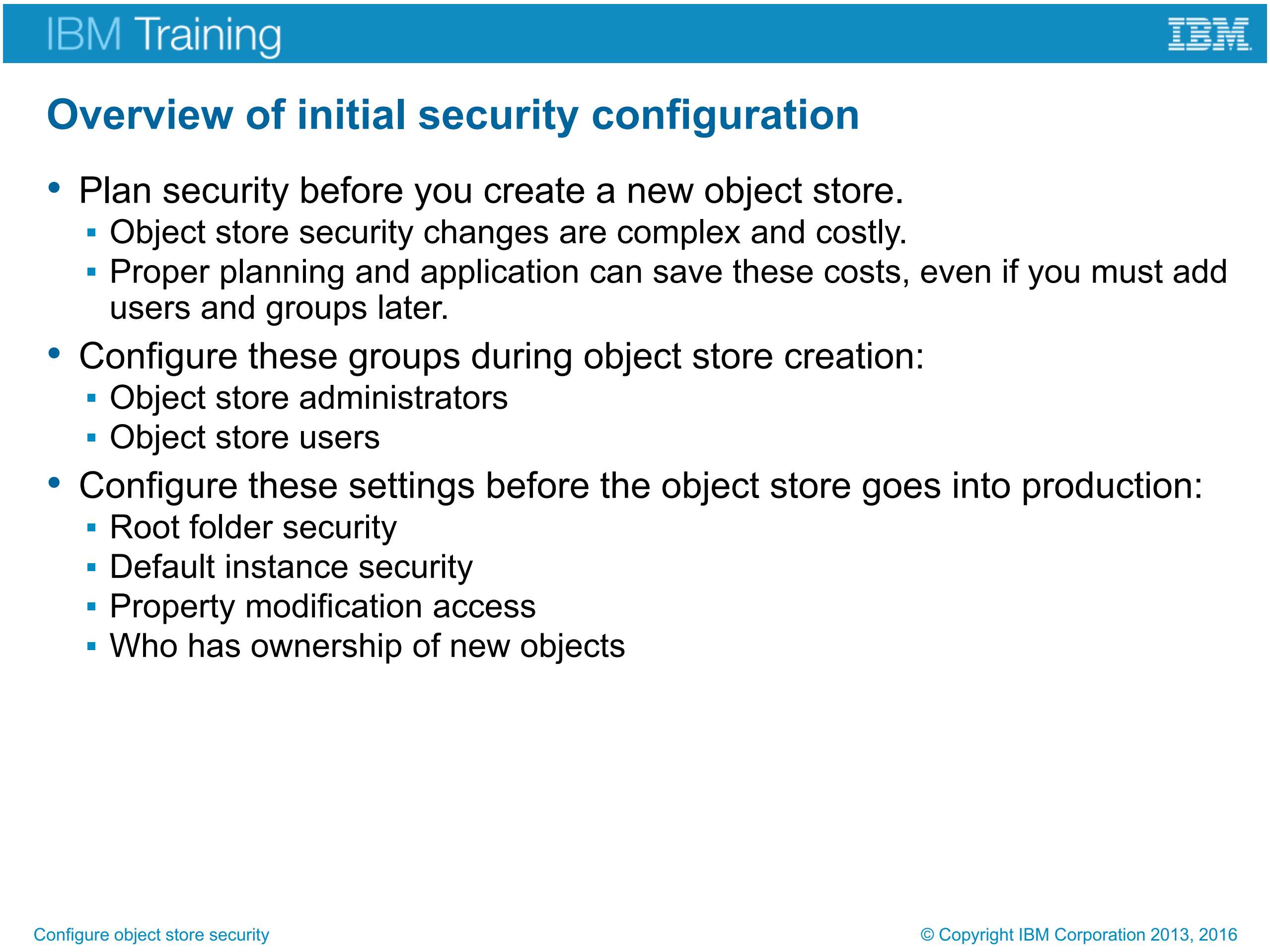
Example security scenario

- GCD administrator
  - Creates object store, setting initial security groups.
  - Creates file storage areas if needed.
- Object store administrator
  - Creates classes and other supporting entities as needed.
  - Defines default instance security for the classes.
  - Configures permissions for Root Folder.
  - Creates root-level subfolders to be used by department managers.
- Business users
  - Managers create subfolder structures.
  - Clerks add documents.
  - Reviewers view documents.

Configure object store security

© Copyright IBM Corporation 2013, 2016

Figure 3-4. Example security scenario



IBM Training

Overview of initial security configuration

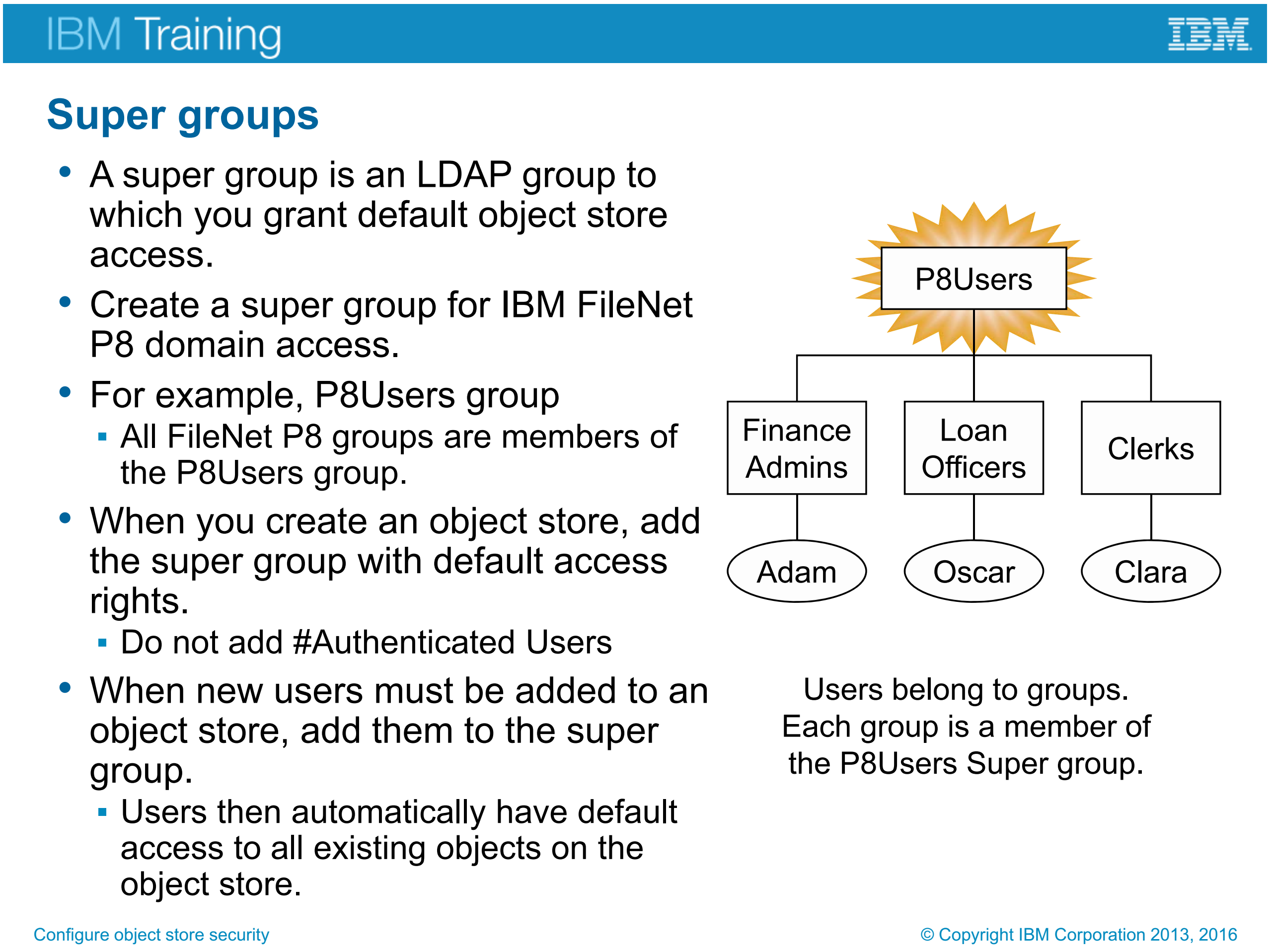
- Plan security before you create a new object store.
  - Object store security changes are complex and costly.
  - Proper planning and application can save these costs, even if you must add users and groups later.
- Configure these groups during object store creation:
  - Object store administrators
  - Object store users
- Configure these settings before the object store goes into production:
  - Root folder security
  - Default instance security
  - Property modification access
  - Who has ownership of new objects

Configure object store security

Figure 3-5. Overview of initial security configuration

Property modification access determines who is allowed to change individual property values for an object class.

Ownership is given by default to the creator of an object and confers special authorization to that object.



IBM Training

Super groups

- A super group is an LDAP group to which you grant default object store access.
- Create a super group for IBM FileNet P8 domain access.
- For example, P8Users group
  - All FileNet P8 groups are members of the P8Users group.
- When you create an object store, add the super group with default access rights.
  - Do not add #Authenticated Users
- When new users must be added to an object store, add them to the super group.
  - Users then automatically have default access to all existing objects on the object store.

P8Users

Finance Admins

Loan Officers

Clerks

Adam

Oscar

Clara

Users belong to groups.
Each group is a member of
the P8Users Super group.

Configure object store security

© Copyright IBM Corporation 2013, 2016

Figure 3-6. Super groups

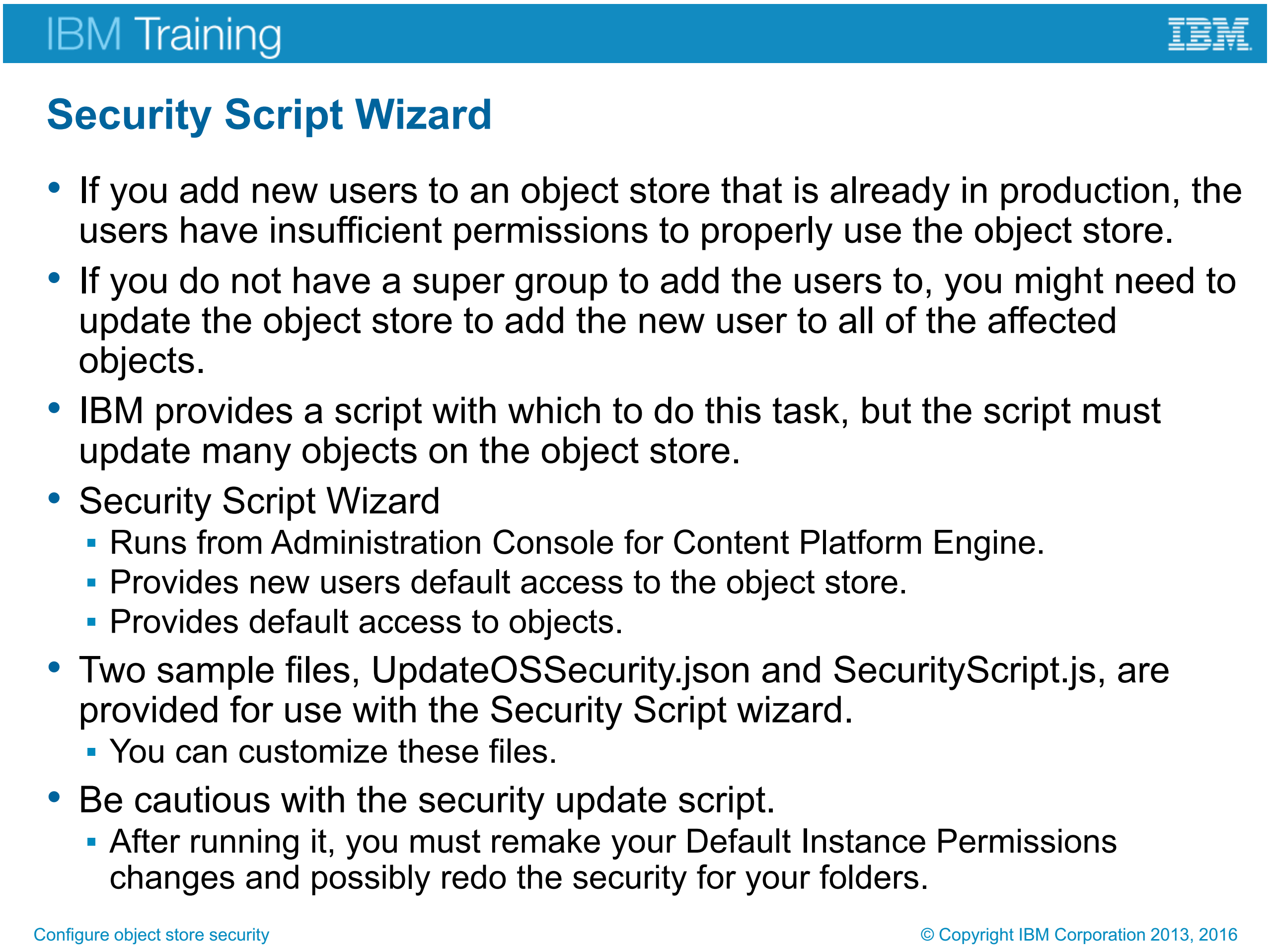
The advantage of using a super group when you create the object store is that it is easy to give new users access to the object store later. An alternative approach, by using the Security Script Wizard, has some drawbacks.

If you use the same super group on multiple object stores, you can grant immediate access to all object stores by adding a user or group to the super group. Otherwise, you can create a separate group for each object store to provide more specific access.

Note

If you use separate groups for each object store, remember to create separate IBM Content Navigator desktops as well. Each desktop might then use a separate object store for authentication.

In some cases, you might need to add a business unit to an object store. If the LDAP directory allows nested groups, you can add the new group to the super group to provide access to the object store.



IBM Training

Security Script Wizard

- If you add new users to an object store that is already in production, the users have insufficient permissions to properly use the object store.
- If you do not have a super group to add the users to, you might need to update the object store to add the new user to all of the affected objects.
- IBM provides a script with which to do this task, but the script must update many objects on the object store.
- Security Script Wizard
  - Runs from Administration Console for Content Platform Engine.
  - Provides new users default access to the object store.
  - Provides default access to objects.
- Two sample files, UpdateOSSecurity.json and SecurityScript.js, are provided for use with the Security Script wizard.
  - You can customize these files.
- Be cautious with the security update script.
  - After running it, you must remake your Default Instance Permissions changes and possibly redo the security for your folders.

Configure object store security

Figure 3-7. Security Script Wizard

Help References

FileNet P8 Platform 5.2.1>Security>How to>Update object store with new users and groups

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh025.htm

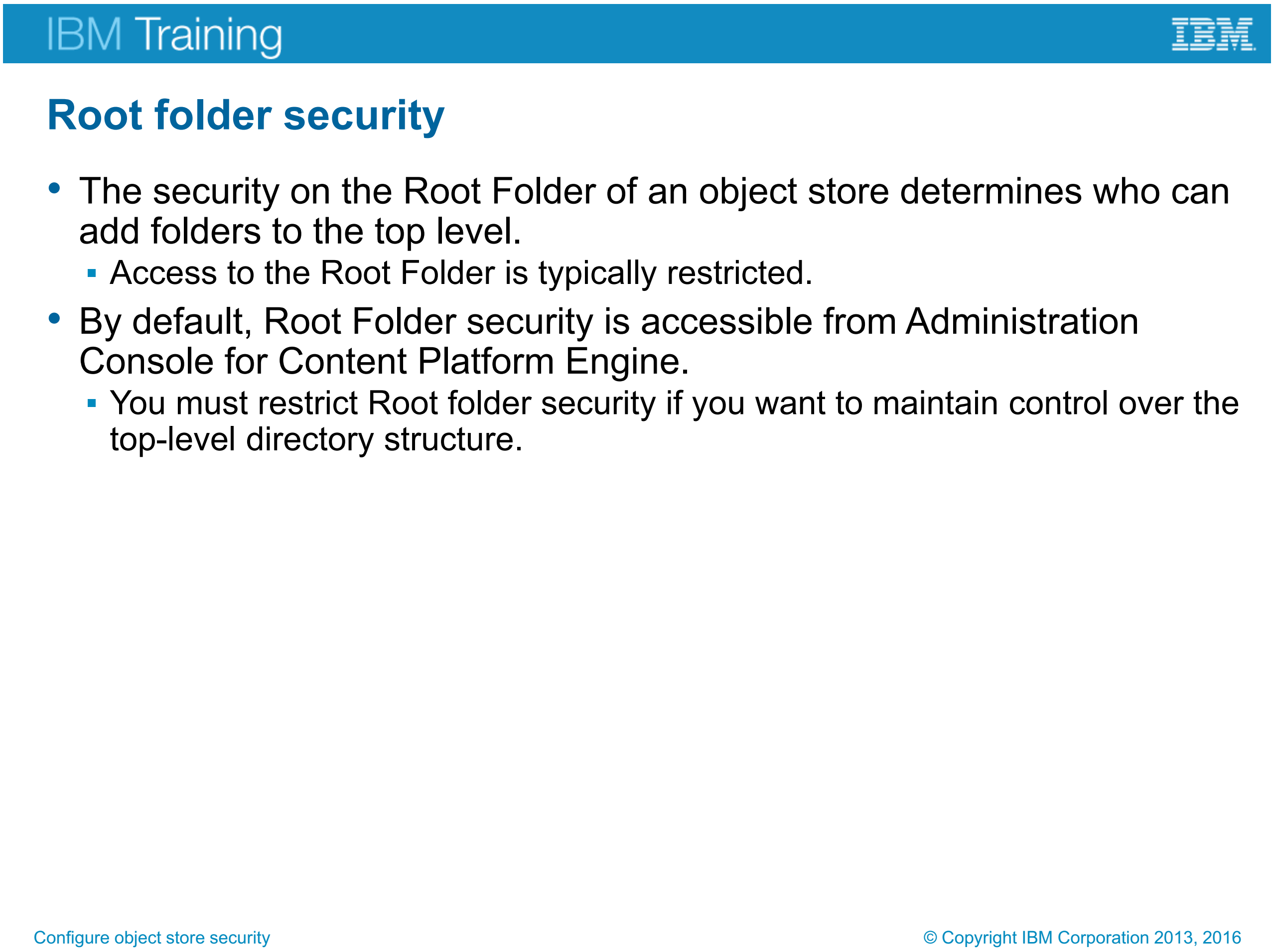
FileNet P8 Platform 5.2.1>Administering>Administering Content Platform Engine>Defining the repository infrastructure>Managing security>The Security Script wizard

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

The Security Script Wizard assigns security roles to user and group accounts to create security principals for the objects in an object store. When you run the Security Script wizard, you select an object store, select a security role, and then add users and groups to that role through a query to your directory service. The Security Script wizard then converts this data to JSON data, appends this data to the JSON role definition file, and merges the combined JSON data structure with the JavaScript security script. The wizard then submits the populated security script to create the security principals for the object store and the objects.

Important

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



IBM Training

Root folder security

- The security on the Root Folder of an object store determines who can add folders to the top level.
  - Access to the Root Folder is typically restricted.
- By default, Root Folder security is accessible from Administration Console for Content Platform Engine.
  - You must restrict Root folder security if you want to maintain control over the top-level directory structure.

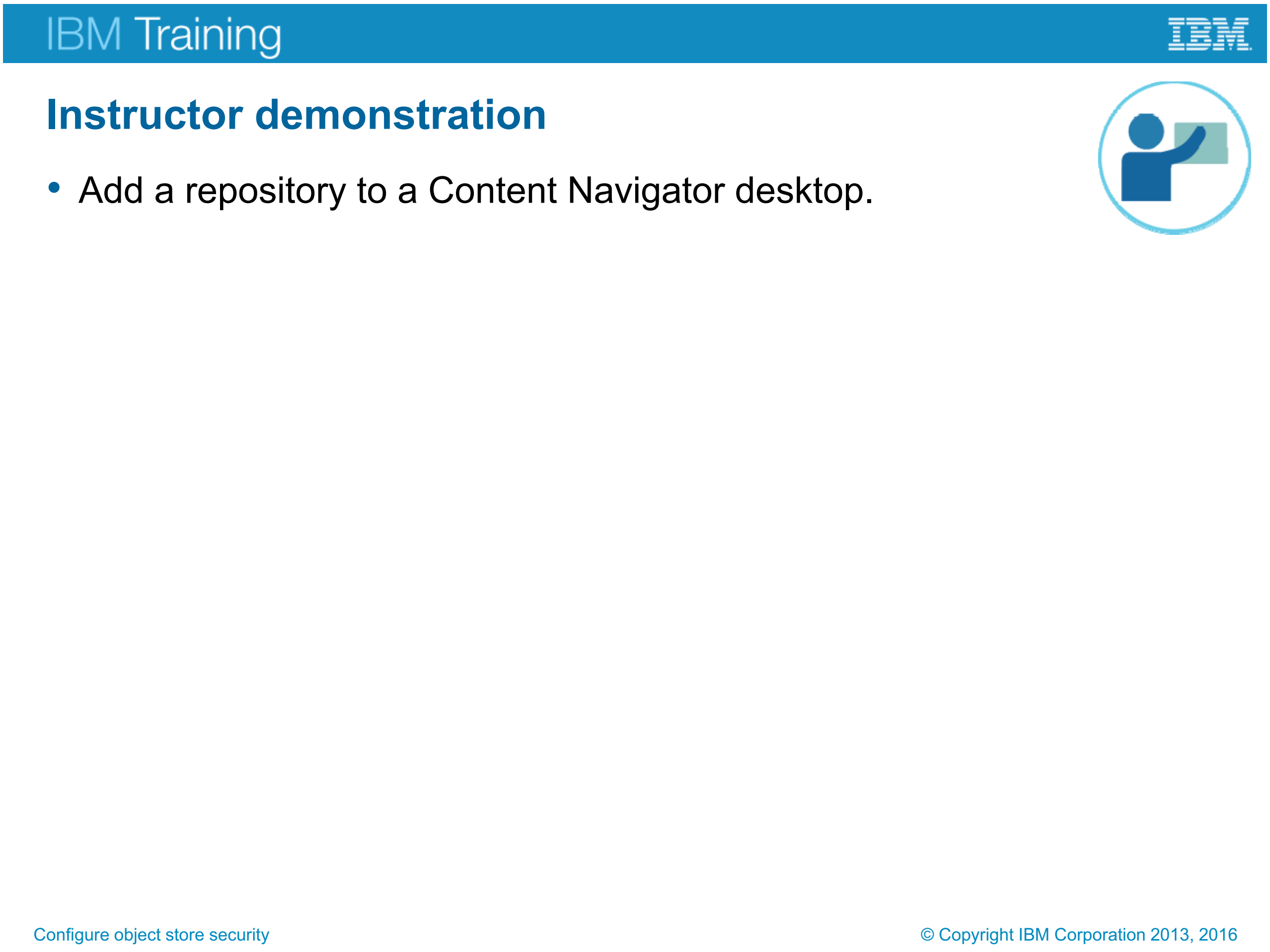
Configure object store security

Figure 3-8. Root folder security

Help path

FileNet P8 Platform 5.2.1>Security>How to>Restrict access to the root folder

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh021.htm



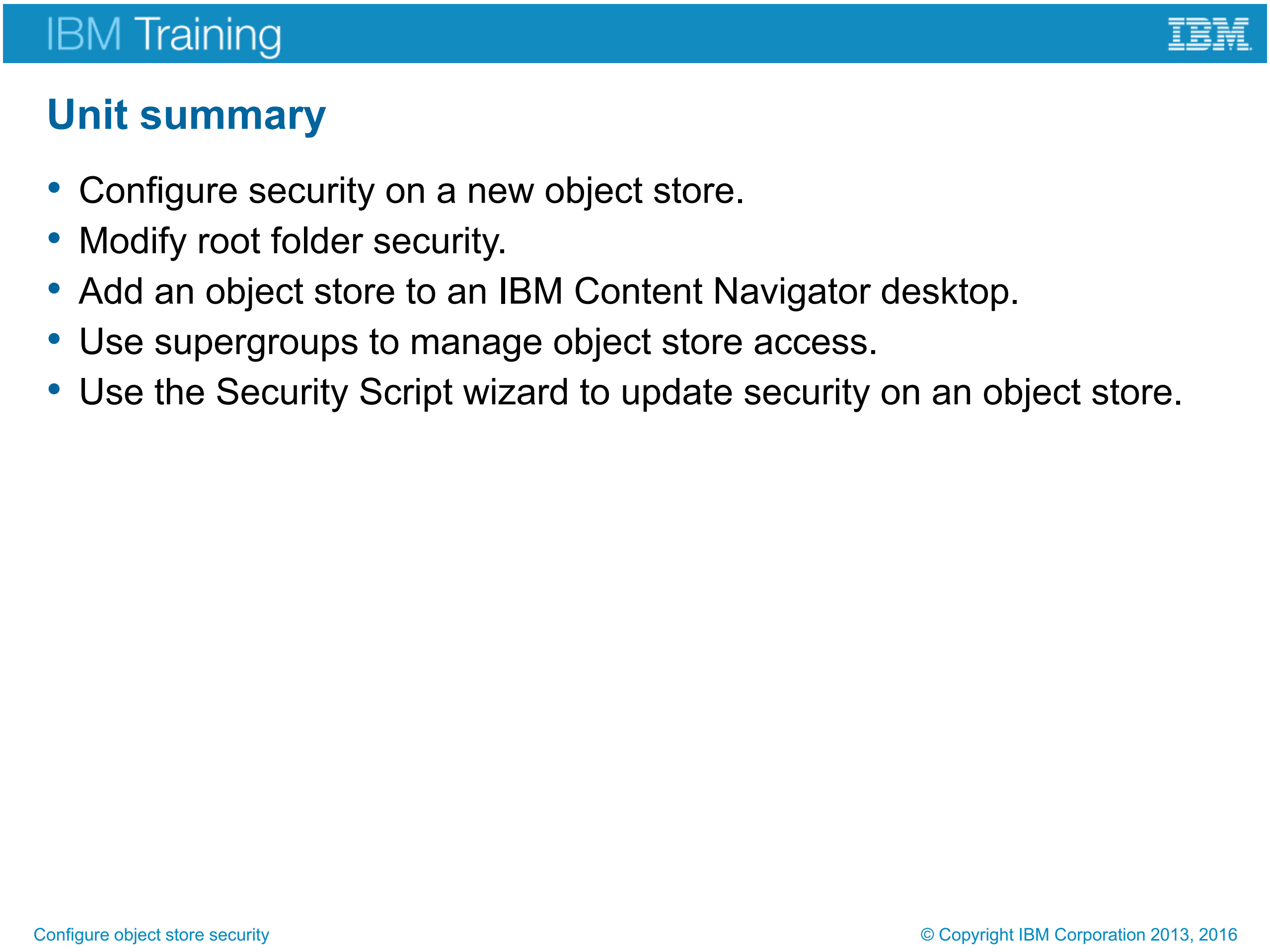
IBM Training

Instructor demonstration

- Add a repository to a Content Navigator desktop.

Configure object store security

Figure 3-9. Instructor demonstration



IBM Training

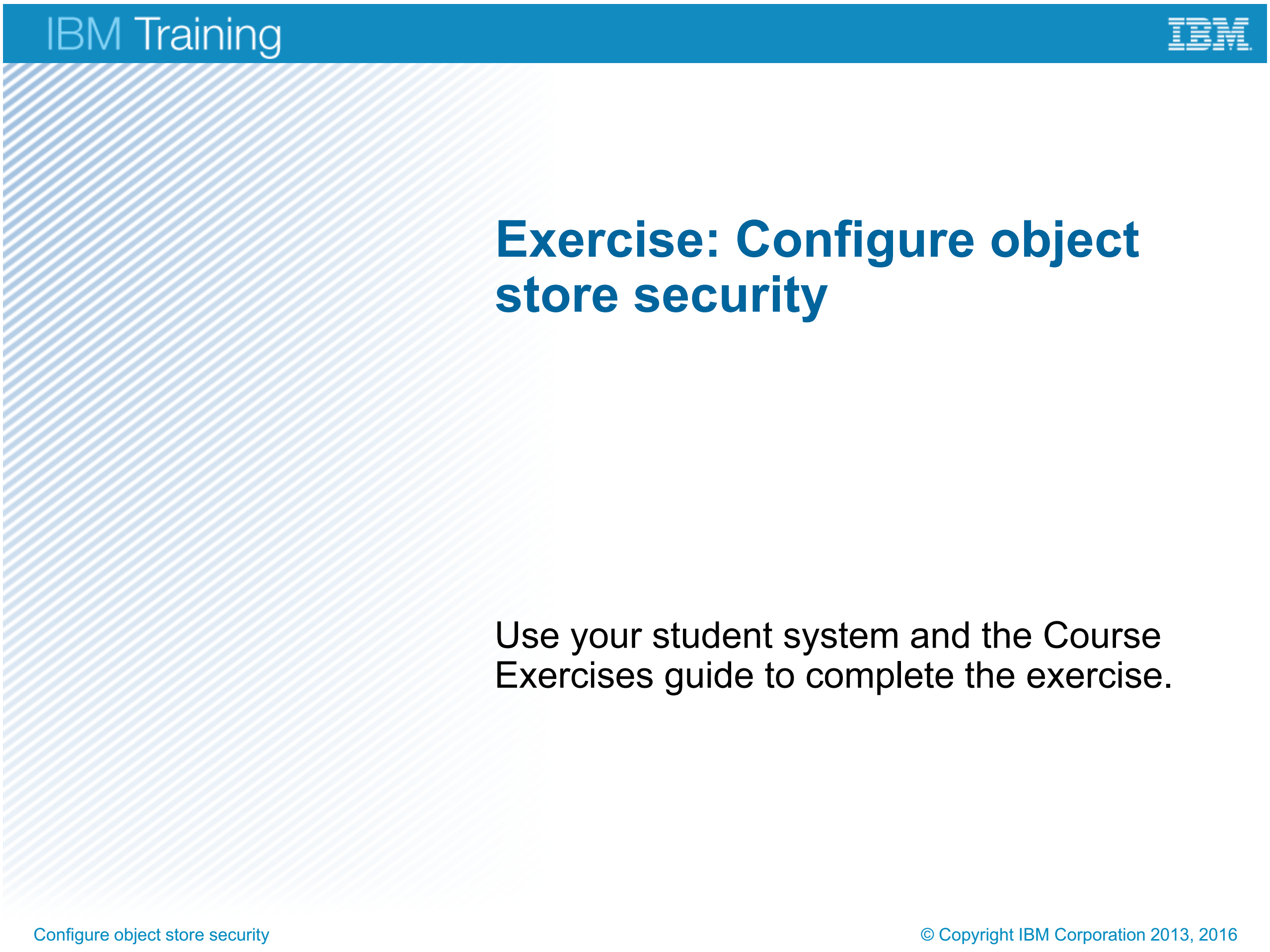
Unit summary

- Configure security on a new object store.
- Modify root folder security.
- 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.

Configure object store security

© Copyright IBM Corporation 2013, 2016

Figure 3-10. Unit summary



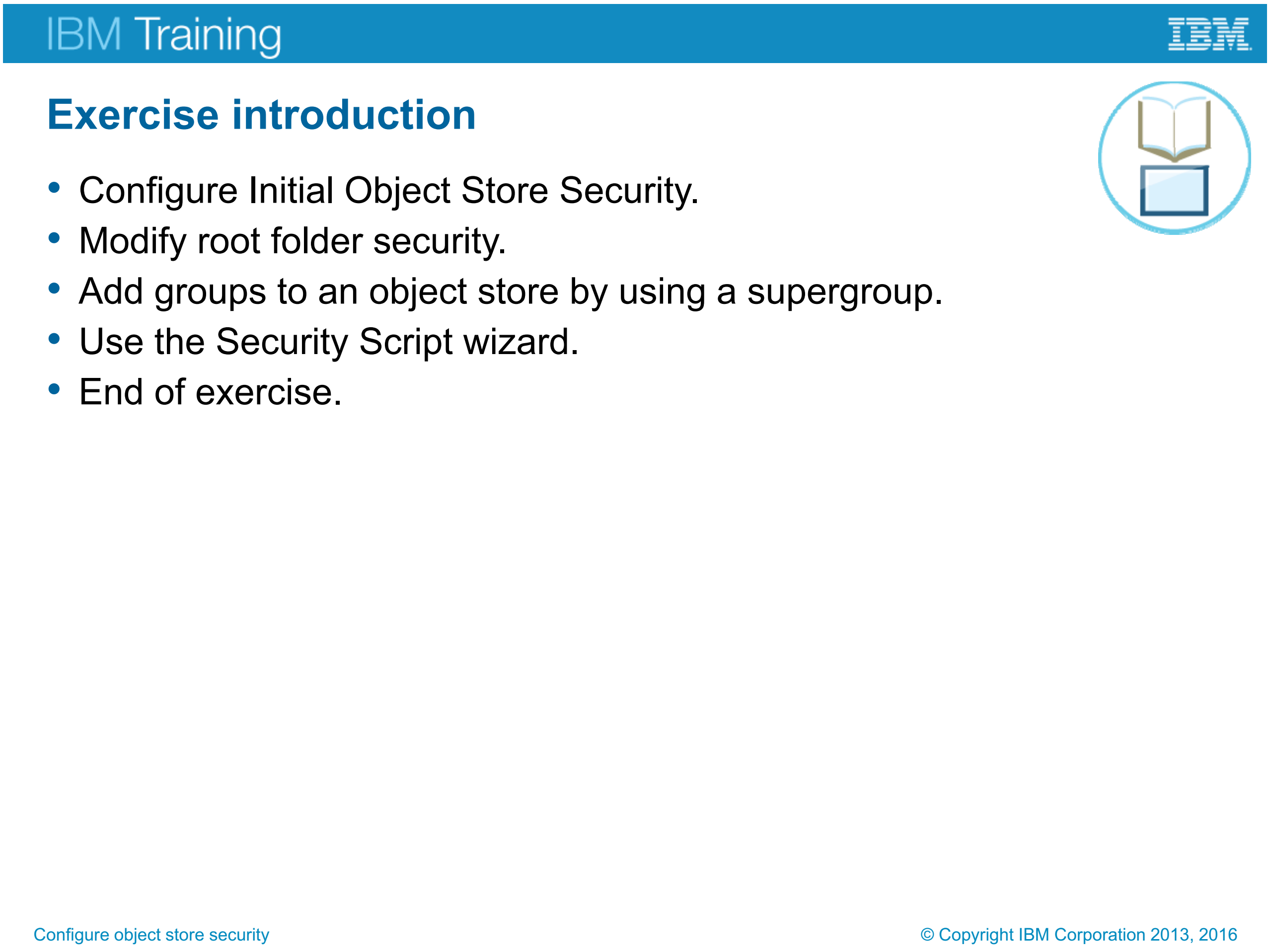
IBM Training

Exercise: Configure object store security

Use your student system and the Course Exercises guide to complete the exercise.

Configure object store security

Figure 3-11. Exercise: Configure object store security



IBM Training

Exercise introduction

- Configure Initial Object Store Security.
- Modify root folder security.
- Add groups to an object store by using a supergroup.
- Use the Security Script wizard.
- End of exercise.

Configure object store security

Figure 3-12. Exercise introduction

Unit 4. Configure class and property security

Estimated time

00:30

Overview

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

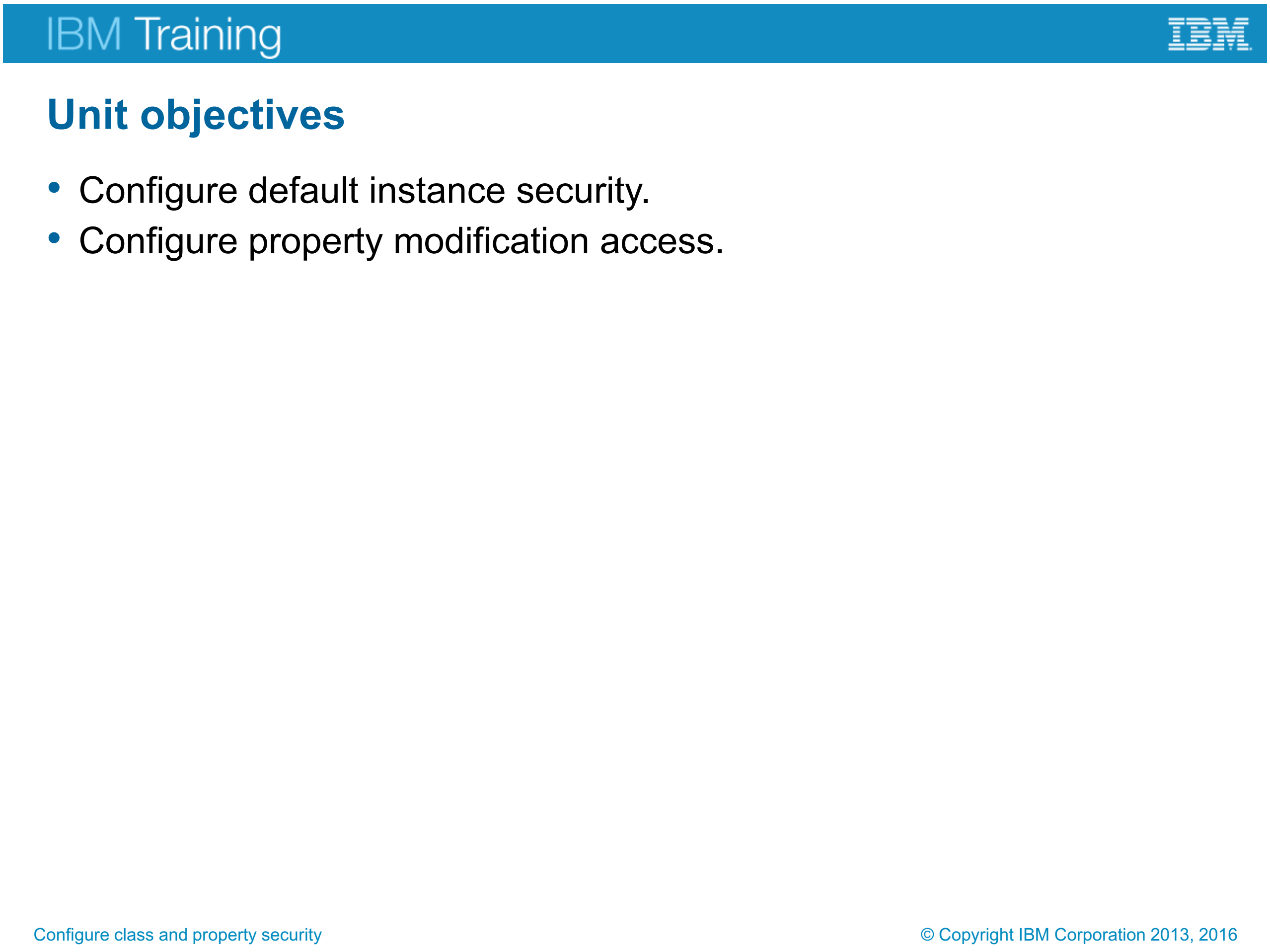
How you will check your progress

- Machine exercises

References

IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSNW2F



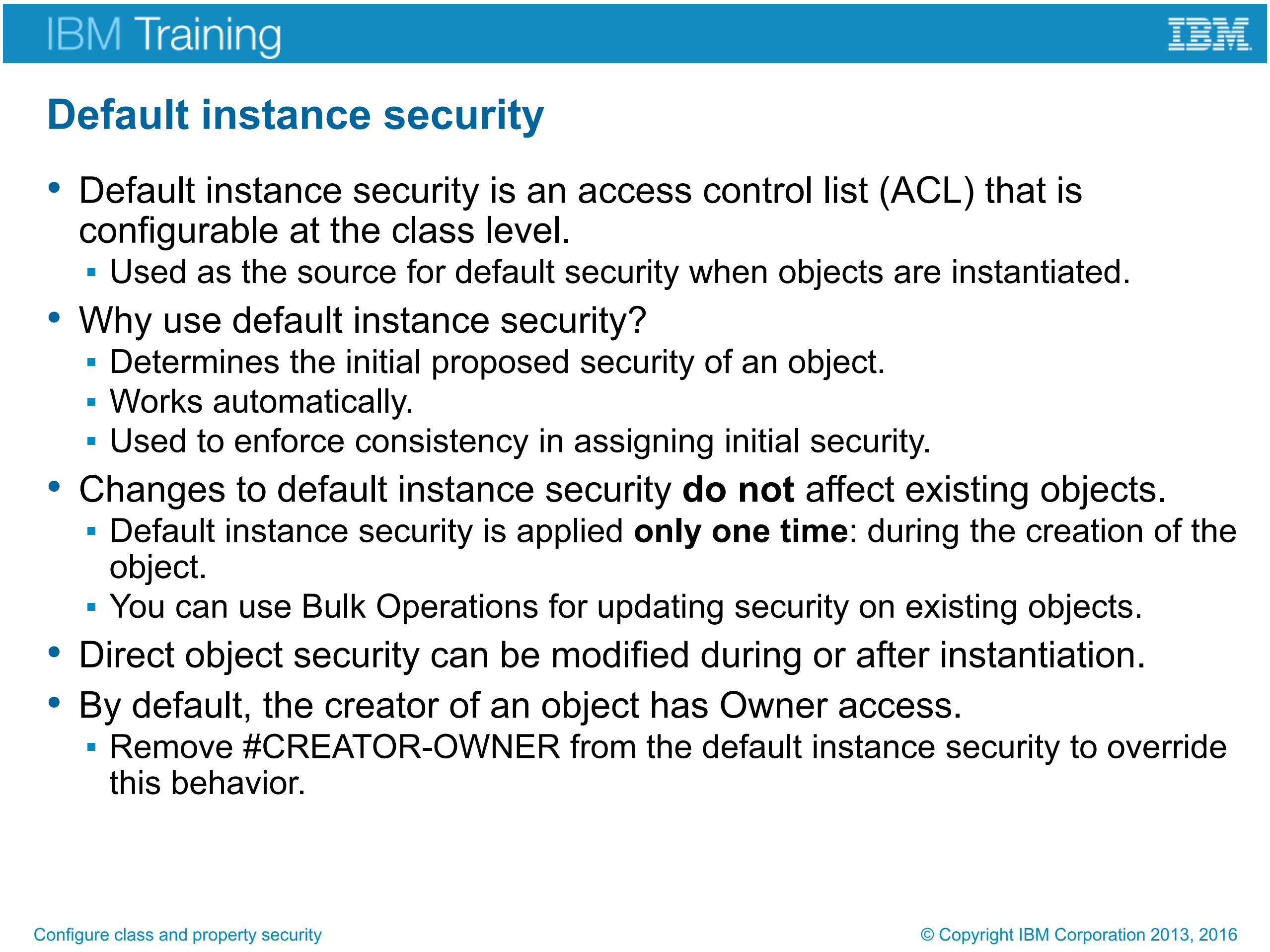
IBM Training

Unit objectives

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

Configure class and property security

Figure 4-1. Unit objectives



IBM Training

Default instance security

- Default instance security is an access control list (ACL) that is configurable at the class level.
  - Used as the source for default security when objects are instantiated.
- Why use default instance security?
  - Determines the initial proposed security of an object.
  - Works automatically.
  - Used to enforce consistency in assigning initial security.
- Changes to default instance security **do not** affect existing objects.
  - Default instance security is applied **only one time**: during the creation of the object.
  - You can use Bulk Operations for updating security on existing objects.
- Direct object security can be modified during or after instantiation.
- By default, the creator of an object has Owner access.
  - Remove #CREATOR-OWNER from the default instance security to override this behavior.

Configure class and property security

© Copyright IBM Corporation 2013, 2016

Figure 4-2. Default instance security

When you create a document, that document automatically gets a set of permissions.

These permissions are preconfigured on the document class. This default set of permissions is called Default instance security.

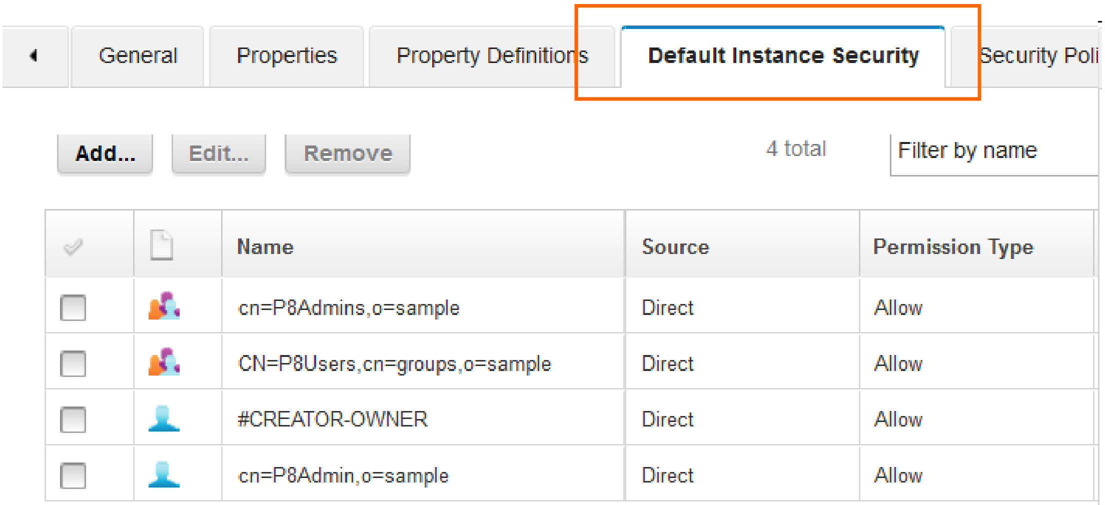
Default instance security is set on the class definition Properties page. When you change default instance security, you can choose to propagate the change to child classes or not.

Do not confuse the default instance security with the security for the class definition itself.

IBM Training

Setting default instance security

- In Administration Console for Content Platform Engine
- [Object store] > Data Design > [object class definition] > Default instance Security tab.



✓		Name	Source	Permission Type
□		cn=P8Admins,o=sample	Direct	Allow
□		CN=P8Users,cn=groups,o=sample	Direct	Allow
□		#CREATOR-OWNER	Direct	Allow
□		cn=P8Admin,o=sample	Direct	Allow

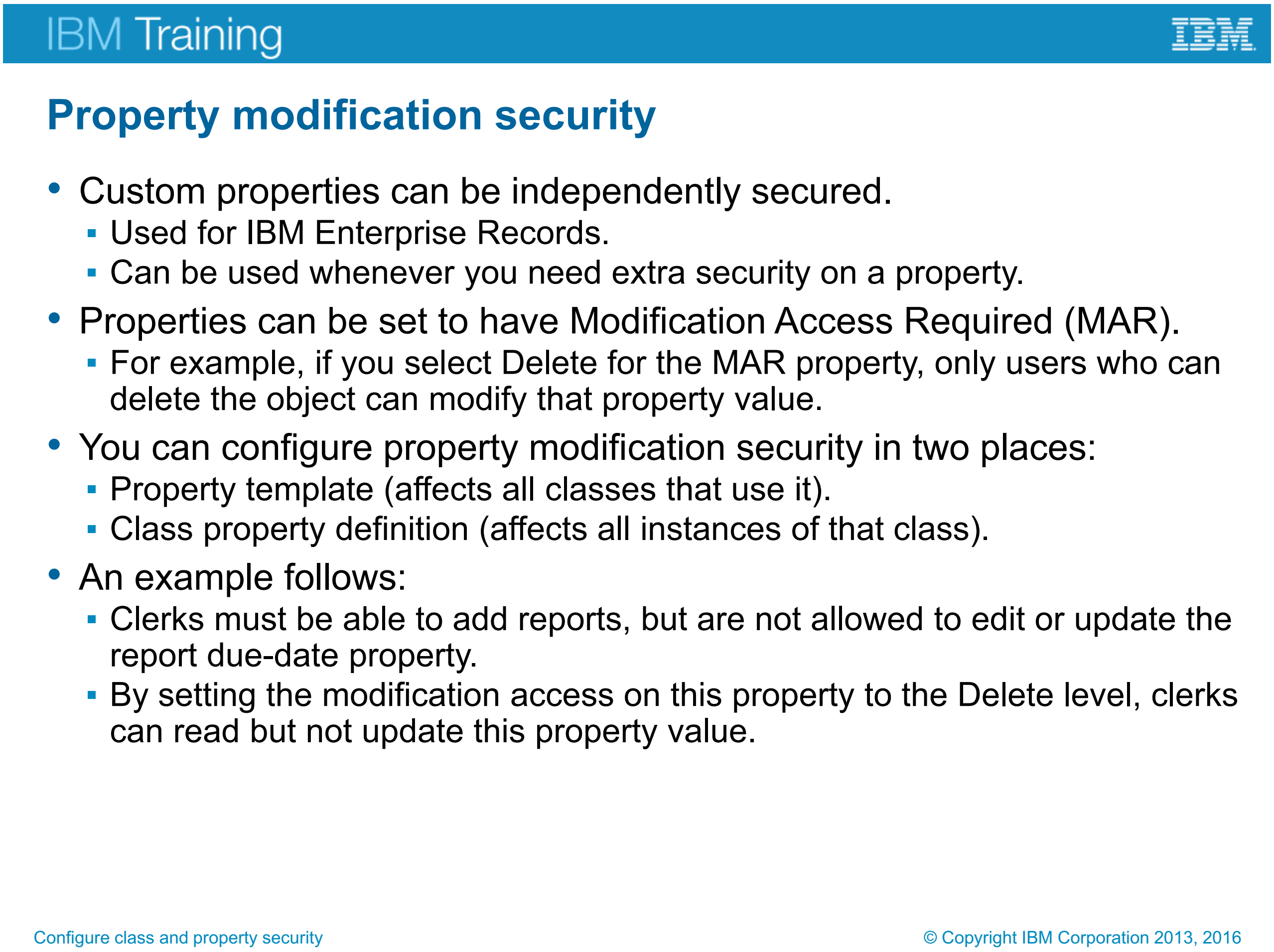
Configure class and property security

Figure 4-3. Setting default instance security

Help path

FileNet P8 Platform 5.2.1>Security>How to>Add users and groups to a class

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh003.htm



IBM Training

Property modification security

- Custom properties can be independently secured.
  - Used for IBM Enterprise Records.
  - Can be used whenever you need extra security on a property.
- Properties can be set to have Modification Access Required (MAR).
  - For example, if you select Delete for the MAR property, only users who can delete the object can modify that property value.
- You can configure property modification security in two places:
  - Property template (affects all classes that use it).
  - Class property definition (affects all instances of that class).
- An example follows:
  - Clerks must be able to add reports, but are not allowed to edit or update the report due-date property.
  - By setting the modification access on this property to the Delete level, clerks can read but not update this property value.

Configure class and property security

© Copyright IBM Corporation 2013, 2016

Figure 4-4. Property modification security

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>Property modification access

> https://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa070.htm

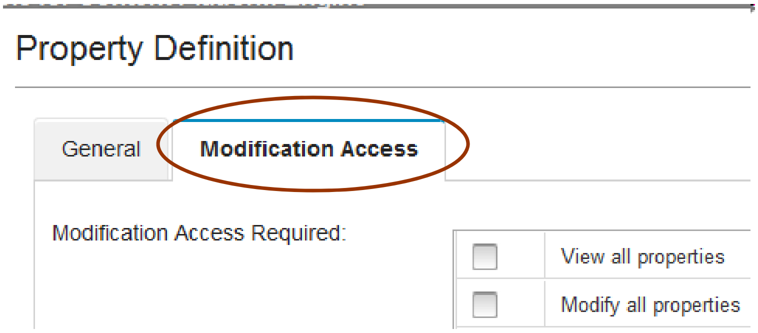
Property modification access is primarily intended for IBM Enterprise Records. It is available for use by non-records management applications that need granular control over user ability to modify properties.

If a property is defined to use this additional security layer, users who add documents are still able to set the values during the addition of the document. However, after the document is added, the property is read-only for them. To ensure that properties are not settable when the document is initially added, use an entry template.

IBM Training

Configure property modification access

1. Edit the property definition (or template) that you want to restrict.
2. Open the Modification Access tab.
3. Select the permissions a user must possess to modify the property value.
4. Save the class definition (or template).



Property Definition

General | Modification Access

Modification Access Required:

□ View all properties

□ Modify all properties

Configure class and property security

Figure 4-5. Configure property modification access

To be able to edit a property, a user generally needs Write access to the property.

The property sheets of all property templates have a Modification Access page that contains a list of access rights. By default, these access rights for all property templates are cleared. If left cleared, then the property template has no modification access behavior and "normal" property security applies. However, if you select one or more access rights, properties based on the property template will have different security than normal.

For example, if you select Delete for the Modification Access Required property, only users who can delete the object can modify that property value.

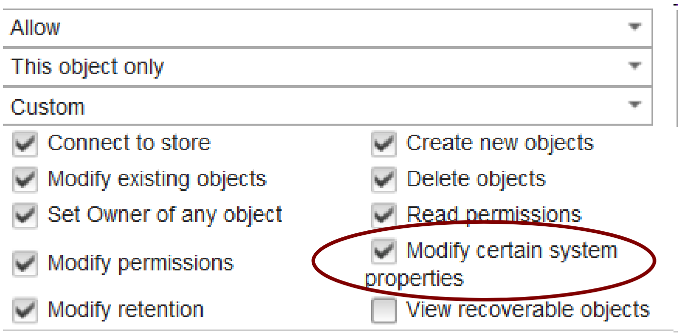
Important

Changes to a property template affect only classes to which you add the template after the change. If you want to change the property modification access on an existing class, you must change the property definition on that class.

IBM Training

System property modification

- Even administrators cannot normally modify certain system properties.
  - For example, Creator, DateCreated, LastModifier. DateLastModified
- To modify these properties, the administrator needs the *Modify certain system properties* permission on the object store.
  - Object store > Security tab.



Allow
This object only
Custom

☑ Connect to store ☑ Create new objects
☑ Modify existing objects ☑ Delete objects
☑ Set Owner of any object ☑ Read permissions
☑ Modify permissions ☑ Modify certain system properties
☑ Modify retention ☐ View recoverable objects

Configure class and property security

© Copyright IBM Corporation 2013, 2016

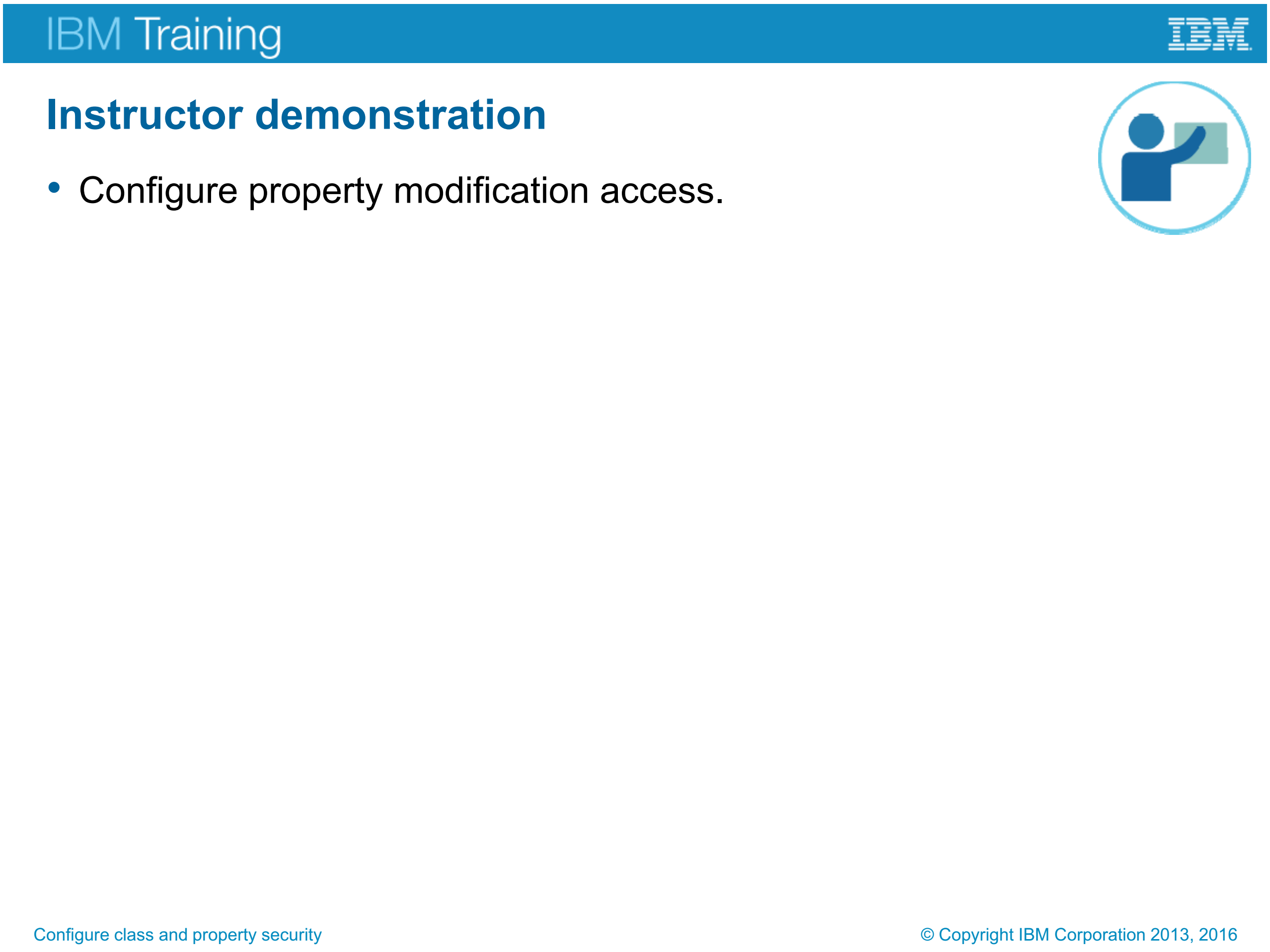
Figure 4-6. System property modification

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>Object access rights and security>Object store access rights

https://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa011.htm

The *Modify certain system properties* permission is typically needed only in specific scenarios: Setting up a change preprocessor, Importing data by using FileNet Deployment Manager, for example.



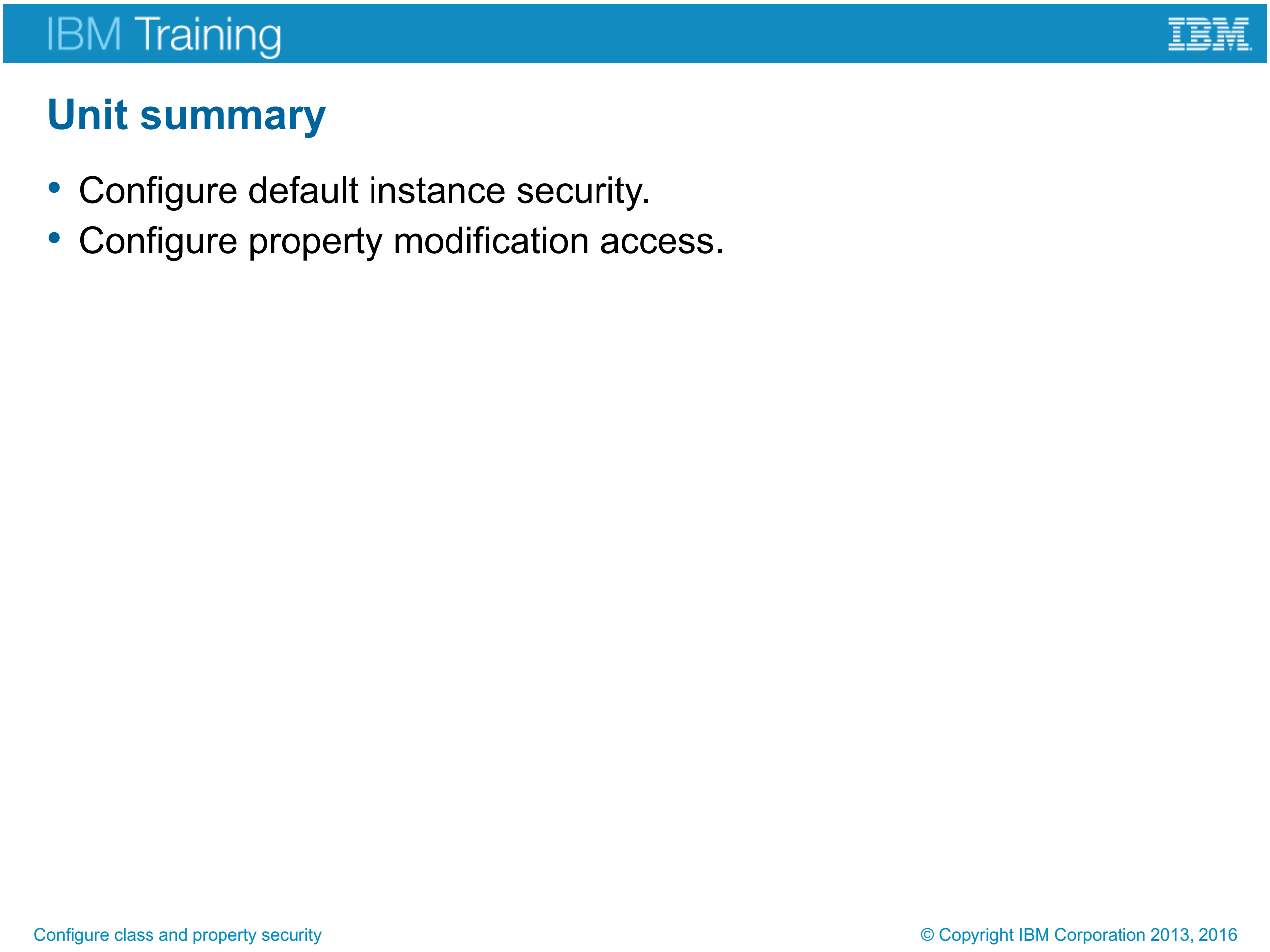
IBM Training

Instructor demonstration

- Configure property modification access.

Configure class and property security

Figure 4-7. Instructor demonstration



IBM Training

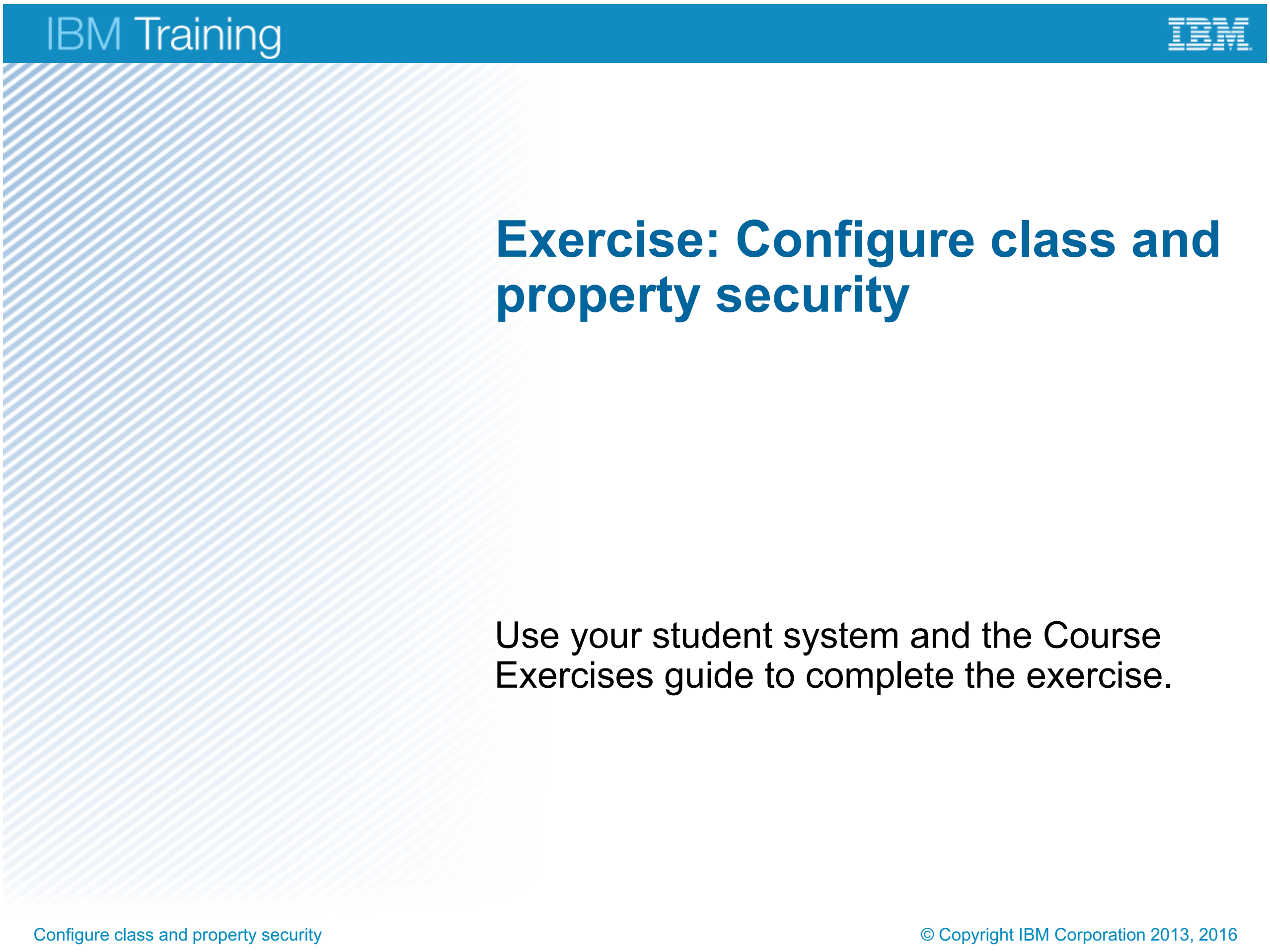
Unit summary

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

Configure class and property security

© Copyright IBM Corporation 2013, 2016

Figure 4-8. Unit summary



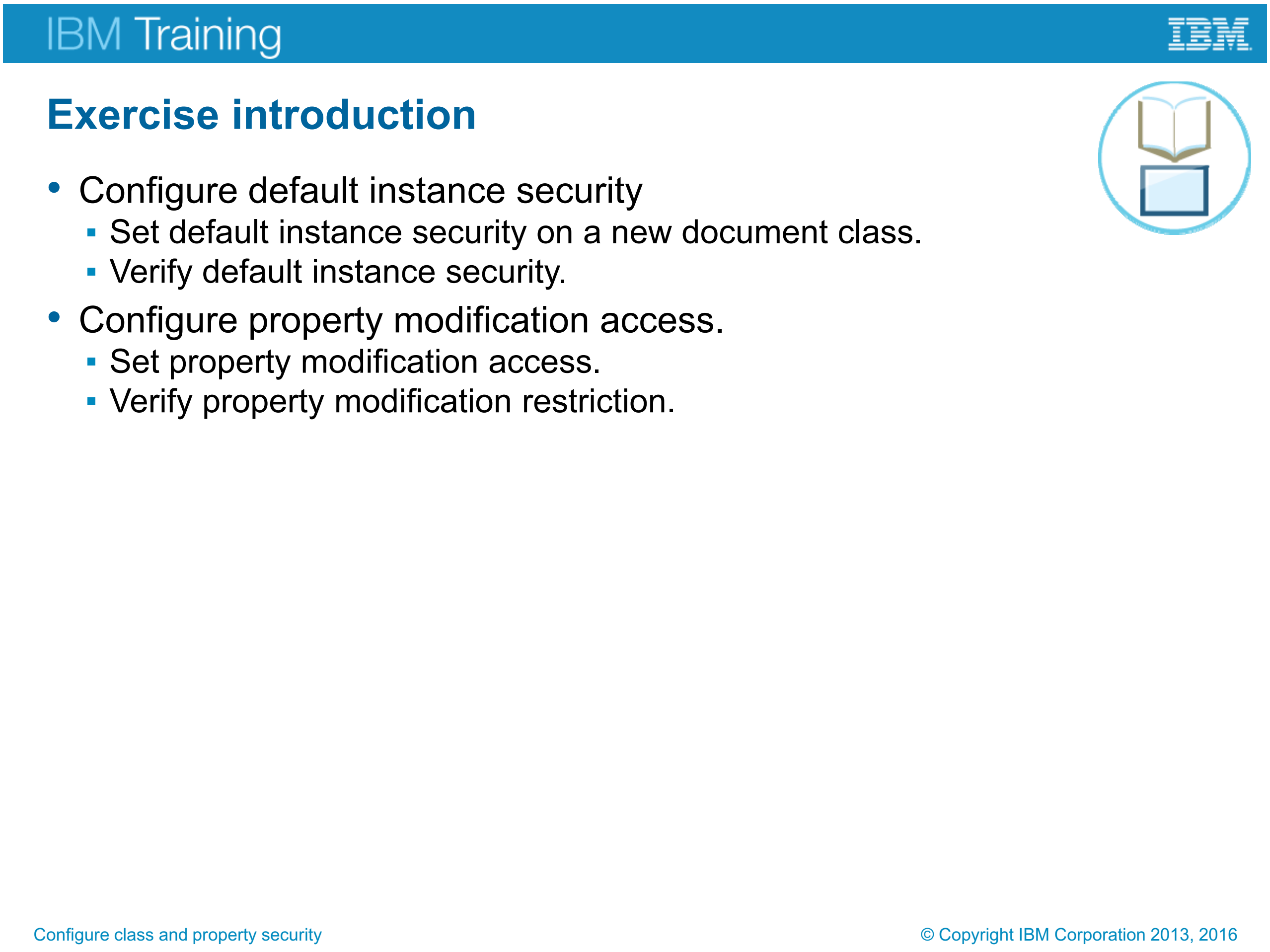
IBM Training

Exercise: Configure class and property security

Use your student system and the Course Exercises guide to complete the exercise.

Configure class and property security

Figure 4-9. Exercise: Configure class and property security



IBM Training

Exercise introduction

- Configure default instance security
  - Set default instance security on a new document class.
  - Verify default instance security.
- Configure property modification access.
  - Set property modification access.
  - Verify property modification restriction.

Configure class and property security

© Copyright IBM Corporation 2013, 2016

Figure 4-10. Exercise introduction

Unit 5. Configure security inheritance

Estimated time

00:20

Overview

This unit describes how to configure security inheritance by using folders and object-valued properties.

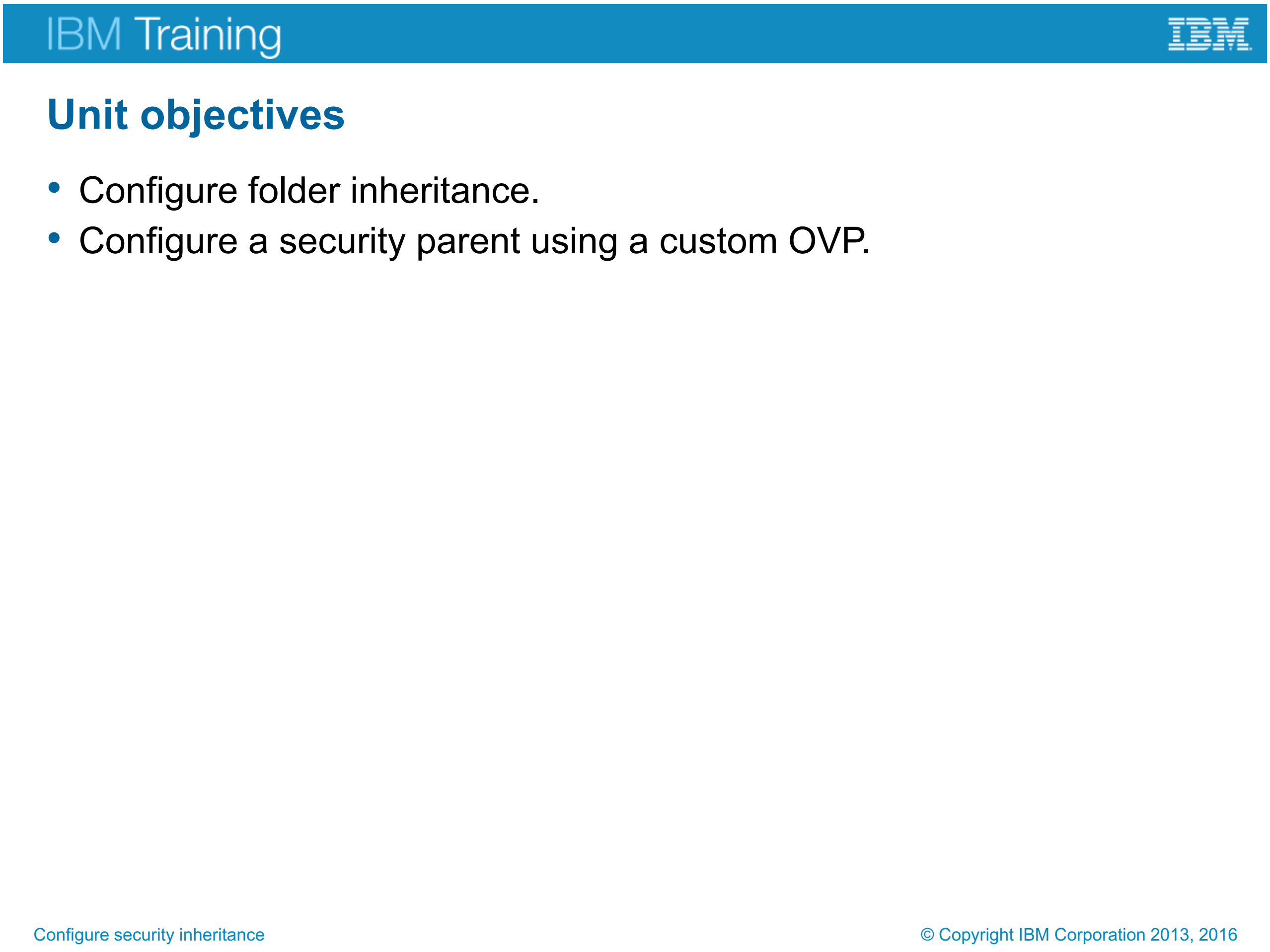
How you will check your progress

- Checkpoint
- Machine exercises

References

IBM Knowledge Center:

http://www.ibm.com/support/knowledgecenter/SSNW2F



IBM Training

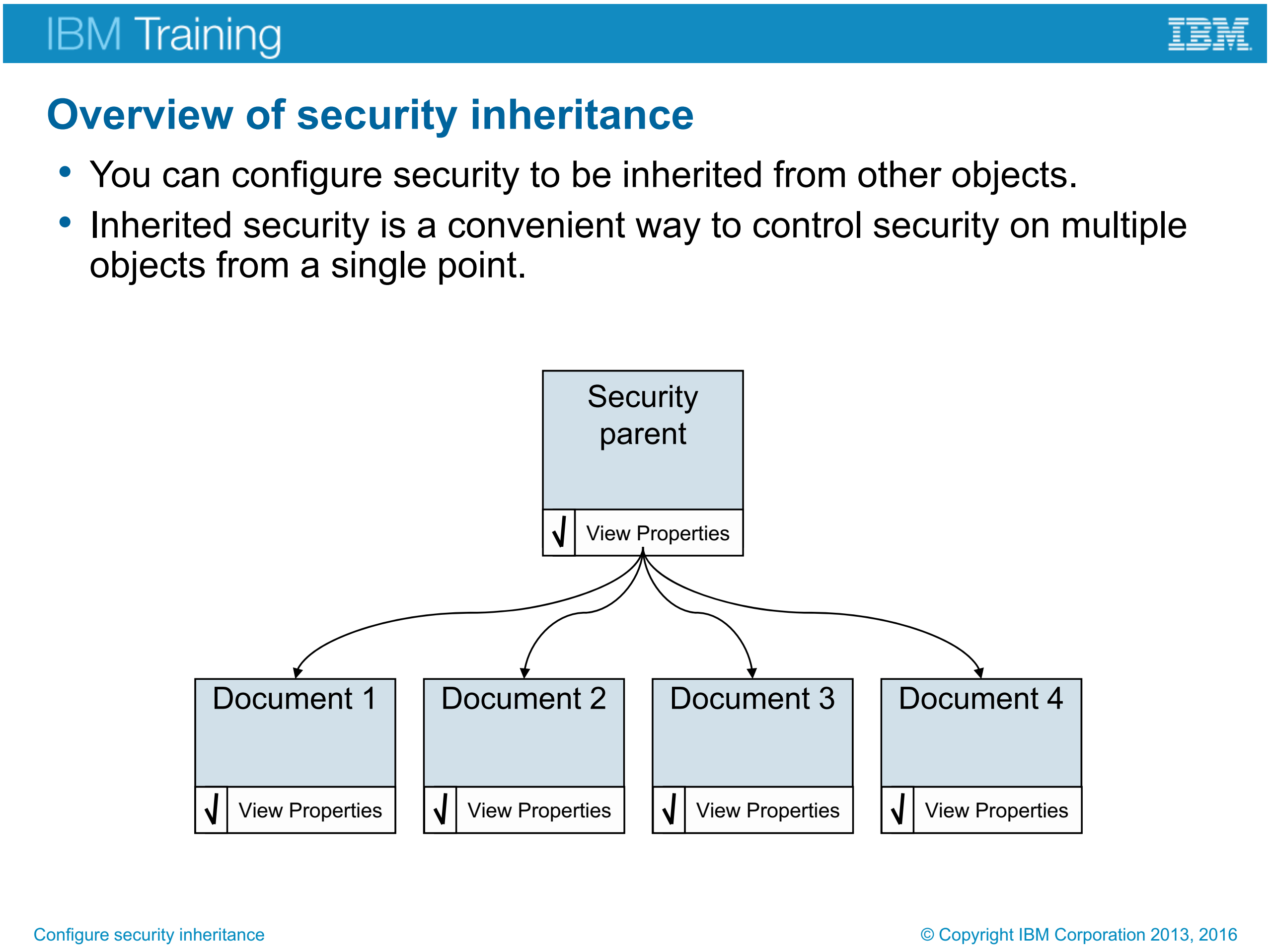
Unit objectives

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

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-1. Unit objectives



IBM Training

Overview of security inheritance

- You can configure security to be inherited from other objects.
- Inherited security is a convenient way to control security on multiple objects from a single point.

Security parent
√ View Properties
Document 1
√ View Properties
Document 2
√ View Properties
Document 3
√ View Properties
Document 4
√ View Properties

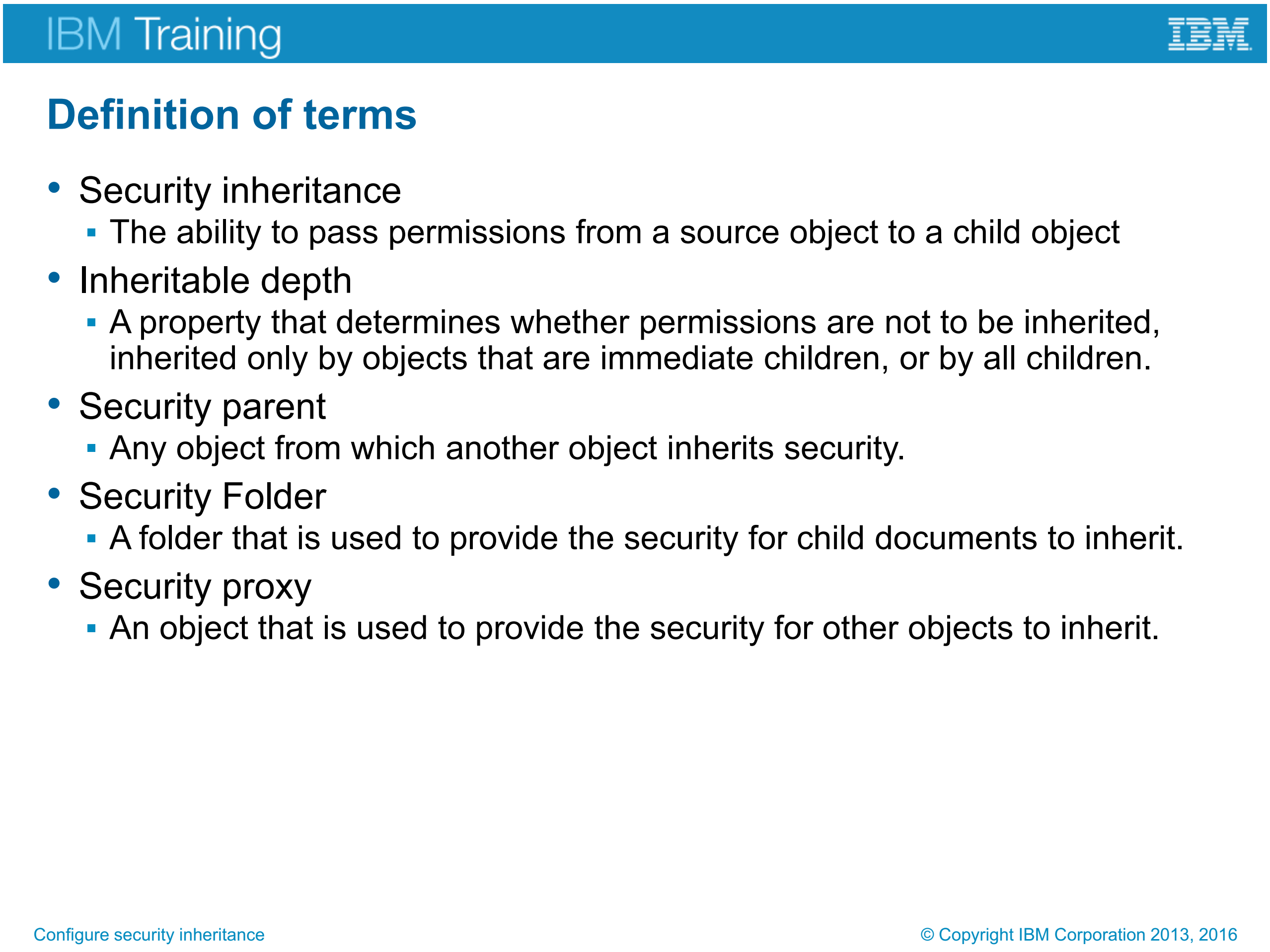
Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-2. Overview of security inheritance

If you specify a security parent for a large group of documents, then you can change permissions on all of these documents by updating the security parent.

In an example scenario, your company has thousands of Invoice documents. A corporate decision mandates that Invoice documents can be viewable by all Finance Clerks. You add Finance Clerks to the security parent for the entire Invoice document class. The new permission is inherited by all Invoice documents. With one change, you gave Finance Clerks access to all Invoice documents.



IBM Training

Definition of terms

- Security inheritance
  - The ability to pass permissions from a source object to a child object
- Inheritable depth
  - A property that determines whether permissions are not to be inherited, inherited only by objects that are immediate children, or by all children.
- Security parent
  - Any object from which another object inherits security.
- Security Folder
  - A folder that is used to provide the security for child documents to inherit.
- Security proxy
  - An object that is used to provide the security for other objects to inherit.

Configure security inheritance

Figure 5-3. Definition of terms

Help path

FileNet P8 Platform 5.2.1>Security>Authorization>Understanding security inheritance

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psa074.htm

Inherited security can be passed on to a child and then on to that child's children, and so on.

Inheritable depth

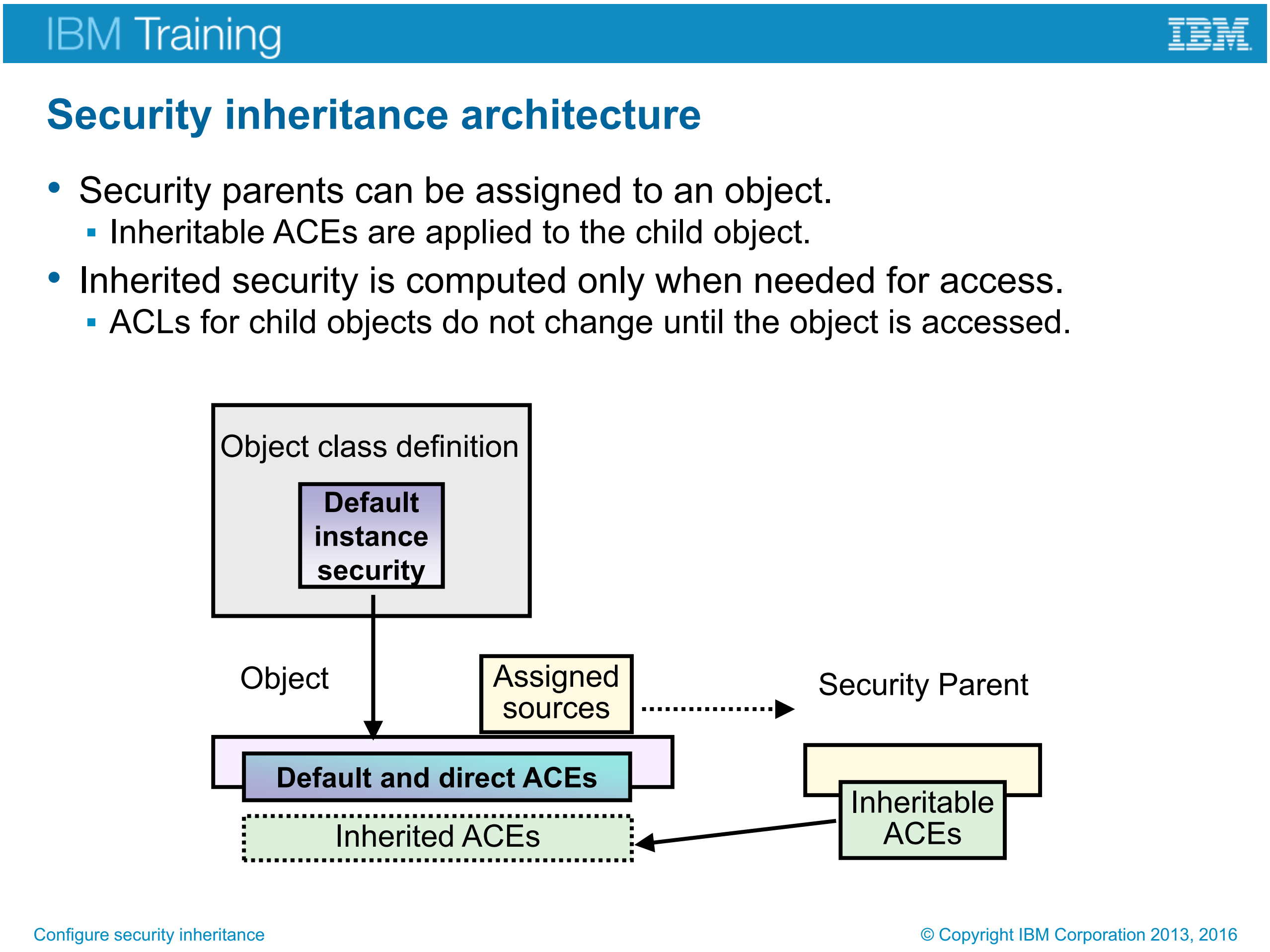
This property is set for each ACE and can be set to one of the following values:

- **This object only**
  - This value is not inherited even if the object is designated as a security parent. This value is the default setting.
- **This object and immediate children**
- This value is inherited by the child of the parent object, but not by the children of the child object. After inheritance takes place, the child ACE has an inheritable depth of *This object only.*
- **This object and all children**

    - This value is inherited by every generation of the child objects of the parent object. After inheritance takes place, the child object ACE has an inheritable depth of *This object and all children*.

- **All children, but not this object**
    - This value is the same as *This object and all children* except the security setting does not apply to the parent object itself
- **Immediate children, but not this object**
    - This value is the same as *This object and immediate children* except the security setting does not apply to the parent object itself.

The previous two settings do not apply to the object itself (for example, a folder), but do apply to objects that inherit the rights (for example, the documents in the folder).



IBM Training

Security inheritance architecture

- Security parents can be assigned to an object.
  - Inheritable ACEs are applied to the child object.
- Inherited security is computed only when needed for access.
  - ACLs for child objects do not change until the object is accessed.

Object class definition

Default instance security

Object

Assigned sources

Security Parent

Default and direct ACEs

Inherited ACEs

Inheritable ACEs

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-4. Security inheritance architecture

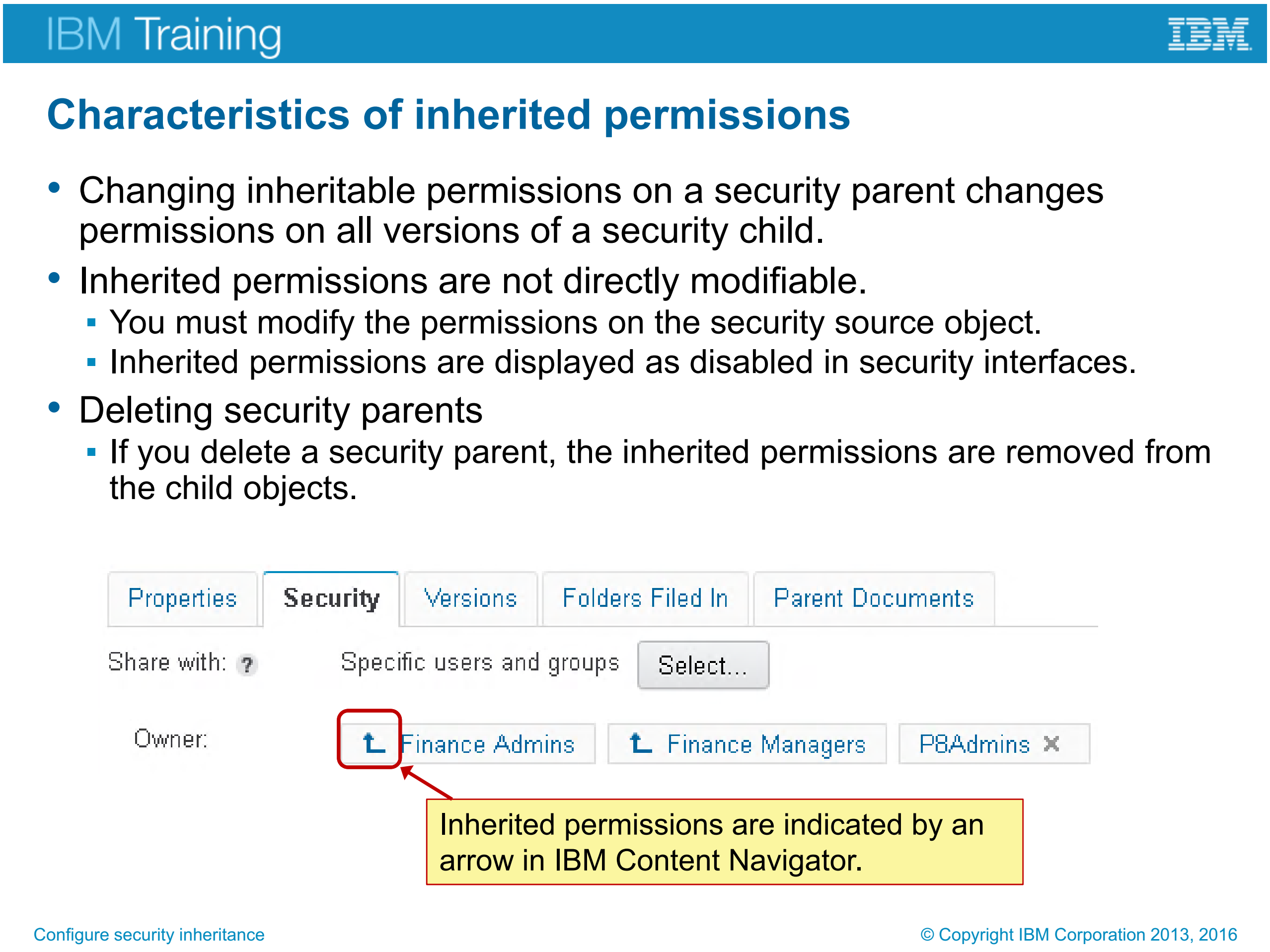
This diagram illustrates how inherited ACEs are applied to an object.

The object class definition has default instance security. When an object of that class is created, the default instance security of the class applies.

In addition to direct ACEs, the object can inherit permissions from a parent object. Inherited permissions are added to existing permissions. If you use Denials, direct permissions are evaluated first, then inherited permissions.

When is inherited security computed?

When security changes on a security parent, the objects that use that object as a security source are not immediately affected (that is, their ACLs do not change) for performance reasons. Inherited security is computed when the object is accessed, and only if Allow or Deny access is not applied directly. Waiting to check the inherited security until the last step in the process is much more efficient than updating all of the security children each time a security parent is updated.



IBM Training

Characteristics of inherited permissions

- Changing inheritable permissions on a security parent changes permissions on all versions of a security child.
- Inherited permissions are not directly modifiable.
  - You must modify the permissions on the security source object.
  - Inherited permissions are displayed as disabled in security interfaces.
- Deleting security parents
  - If you delete a security parent, the inherited permissions are removed from the child objects.

Share with: ? Specific users and groups

Owner: ↑ Finance Admins ↑ Finance Managers P8Admins ✕

Inherited permissions are indicated by an arrow in IBM Content Navigator.

Configure security inheritance

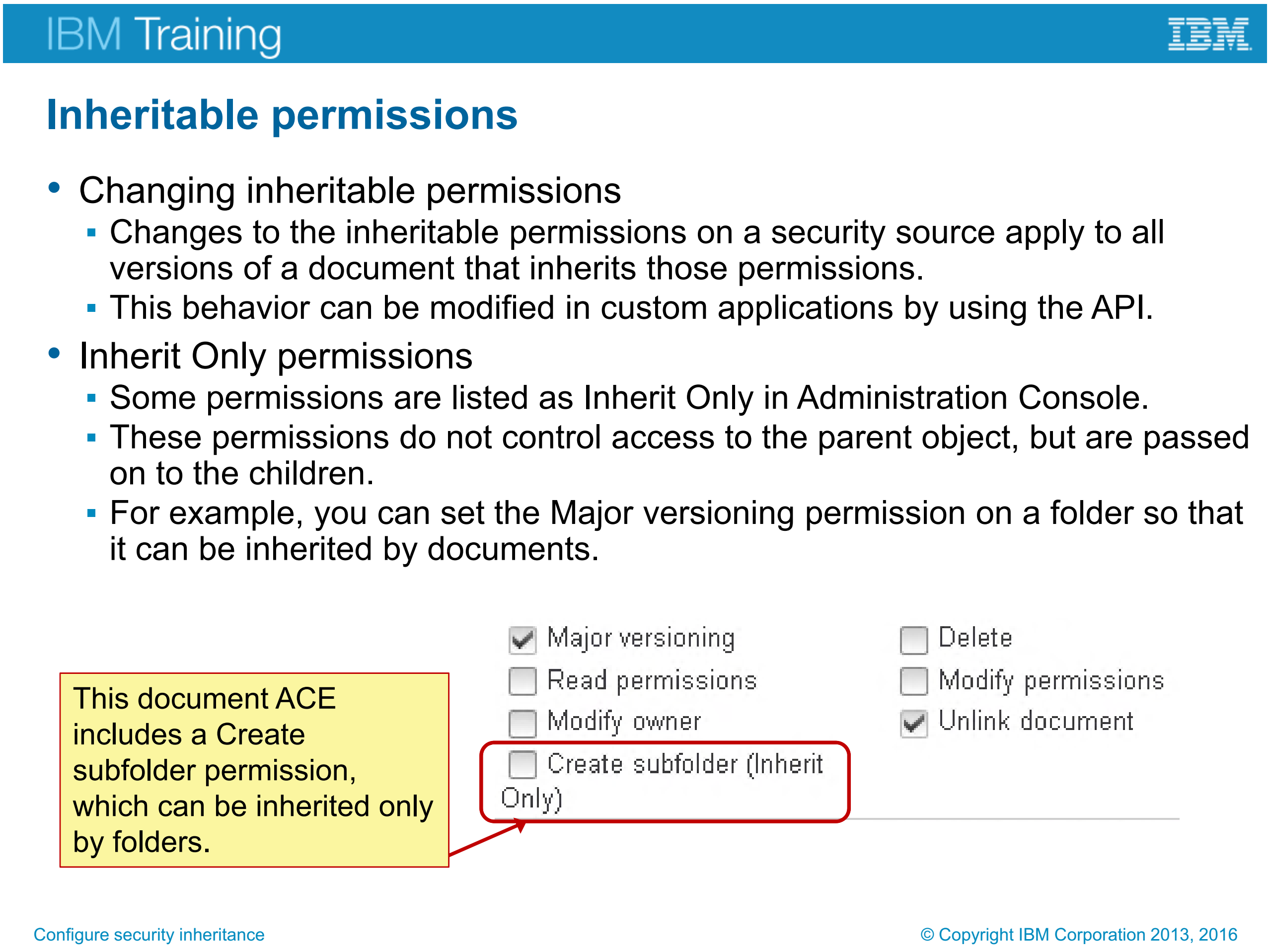
© Copyright IBM Corporation 2013, 2016

Figure 5-5. Characteristics of inherited permissions

By design, inherited security cannot be modified on the child object. It can be modified only on the security source object. Even the owner of a particular object is not able to change the inherited security for that object. You must have permission to change the security of the source to affect the inherited security.

The graphic shows the ACL for a document that includes inherited permissions. The inherited permission is indicated by an arrow. The inherited permission does not include an X because it cannot be deleted. The permission cannot be edited, either.

The reason that you cannot edit or delete inherited permissions on an object is that the inherited permission is not contained on the object. The inherited permission is a pointer to a permission on the parent object.



IBM Training

Inheritable permissions

- Changing inheritable permissions
  - Changes to the inheritable permissions on a security source apply to all versions of a document that inherits those permissions.
  - This behavior can be modified in custom applications by using the API.
- Inherit Only permissions
  - Some permissions are listed as Inherit Only in Administration Console.
  - These permissions do not control access to the parent object, but are passed on to the children.
  - For example, you can set the Major versioning permission on a folder so that it can be inherited by documents.

☑ Major versioning	□ Delete
□ Read permissions	□ Modify permissions
□ Modify owner	☑ Unlink document
□ Create subfolder (Inherit Only)	

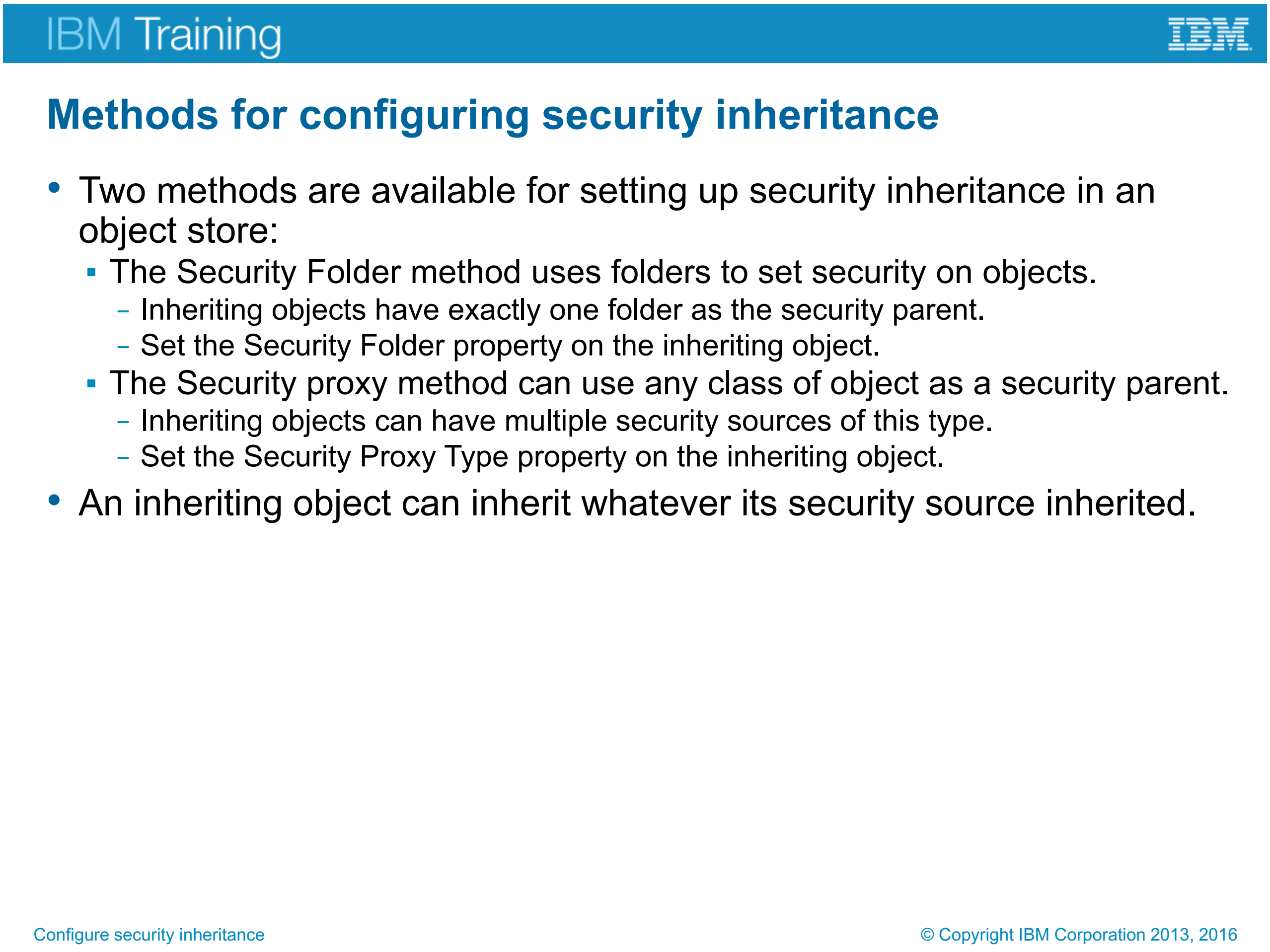
This document ACE includes a Create subfolder permission, which can be inherited only by folders.

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-6. Inheritable permissions

If you are using Administration Console for Content Platform Engine to configure inherited security, use the same type of object for the child and parent security objects. The *Inherit Only* label is not applied in this interface. To ensure that you are configuring permissions that are applicable to the child object class, use the same object class for the parent. For example, use a document as a security parent for other documents.



IBM Training

Methods for configuring security inheritance

- Two methods are available for setting up security inheritance in an object store:
  - The Security Folder method uses folders to set security on objects.
    - Inheriting objects have exactly one folder as the security parent.
    - Set the Security Folder property on the inheriting object.
  - The Security proxy method can use any class of object as a security parent.
    - Inheriting objects can have multiple security sources of this type.
    - Set the Security Proxy Type property on the inheriting object.
- An inheriting object can inherit whatever its security source inherited.

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-7. Methods for configuring security inheritance

Help path

FileNet P8 Platform 5.2.1>Security>How to>Configure security inheritance

http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh005.htm

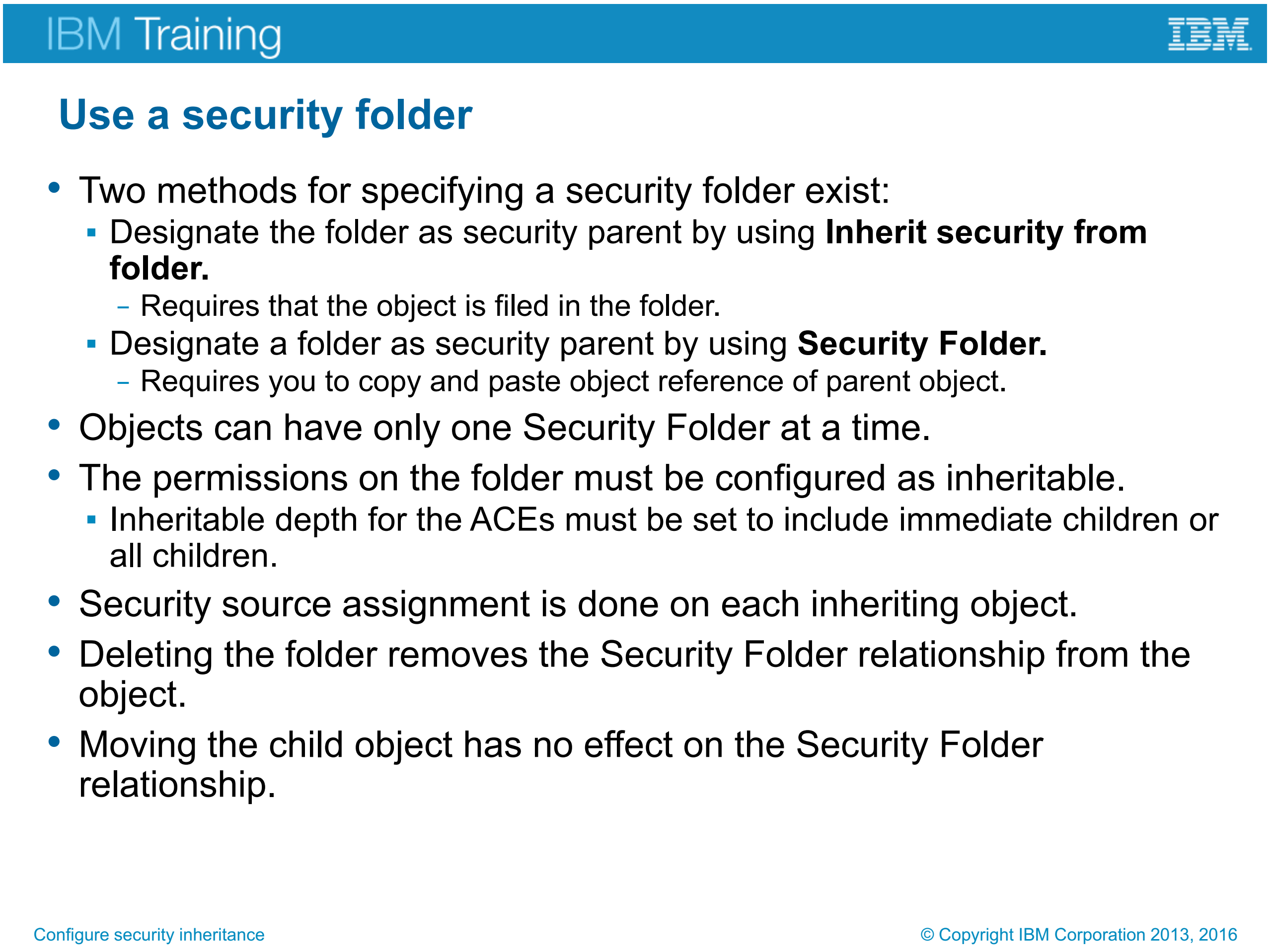
Two methods to set up security inheritance exist. The first method uses a folder as the security source.

- **Security Folder method**
  - A Security Folder is a folder from which an object inherits security, but no requirement to file its security children in the folder exists. A folder inherits the security of its parent folder by default. Therefore, any security permissions that a folder inherits from its parent folder can be passed down to objects that have the child folder as their security parent. The behavior of how the security is inherited can be controlled by using the *Inheritable depth* property on the ACEs for the Security Folder.

The second method uses a custom object-valued property as the security source.

- **Security Proxy Type method**

- This method is a little more complex than the previous method. However, it allows for a more flexible security model to be used. Any class of object in an object store can be specified as the security parent, and an object can have more than one security parent if needed. This method can be combined with the previous method. This method of setting security parents can also be applied by a class definition. You can use this technique to automate the process of establishing security inheritance. The reference to the security parent object can be changed or deleted later if necessary.



IBM Training

Use a security folder

- Two methods for specifying a security folder exist:
  - Designate the folder as security parent by using **Inherit security from folder.**
    - Requires that the object is filed in the folder.
  - Designate a folder as security parent by using **Security Folder.**
    - Requires you to copy and paste object reference of parent object.
- Objects can have only one Security Folder at a time.
- The permissions on the folder must be configured as inheritable.
  - Inheritable depth for the ACEs must be set to include immediate children or all children.
- Security source assignment is done on each inheriting object.
- Deleting the folder removes the Security Folder relationship from the object.
- Moving the child object has no effect on the Security Folder relationship.

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-8. Use a security folder

Help path

FileNet P8 Platform 5.2.1>Security>How to>Configure security inheritance>Designating a folder as a security parent by using Inherit security from folder

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh006.htm

FileNet P8 Platform 5.2.1>Security>How to>Configure security inheritance>Designating a folder as a security parent by using Security Folder

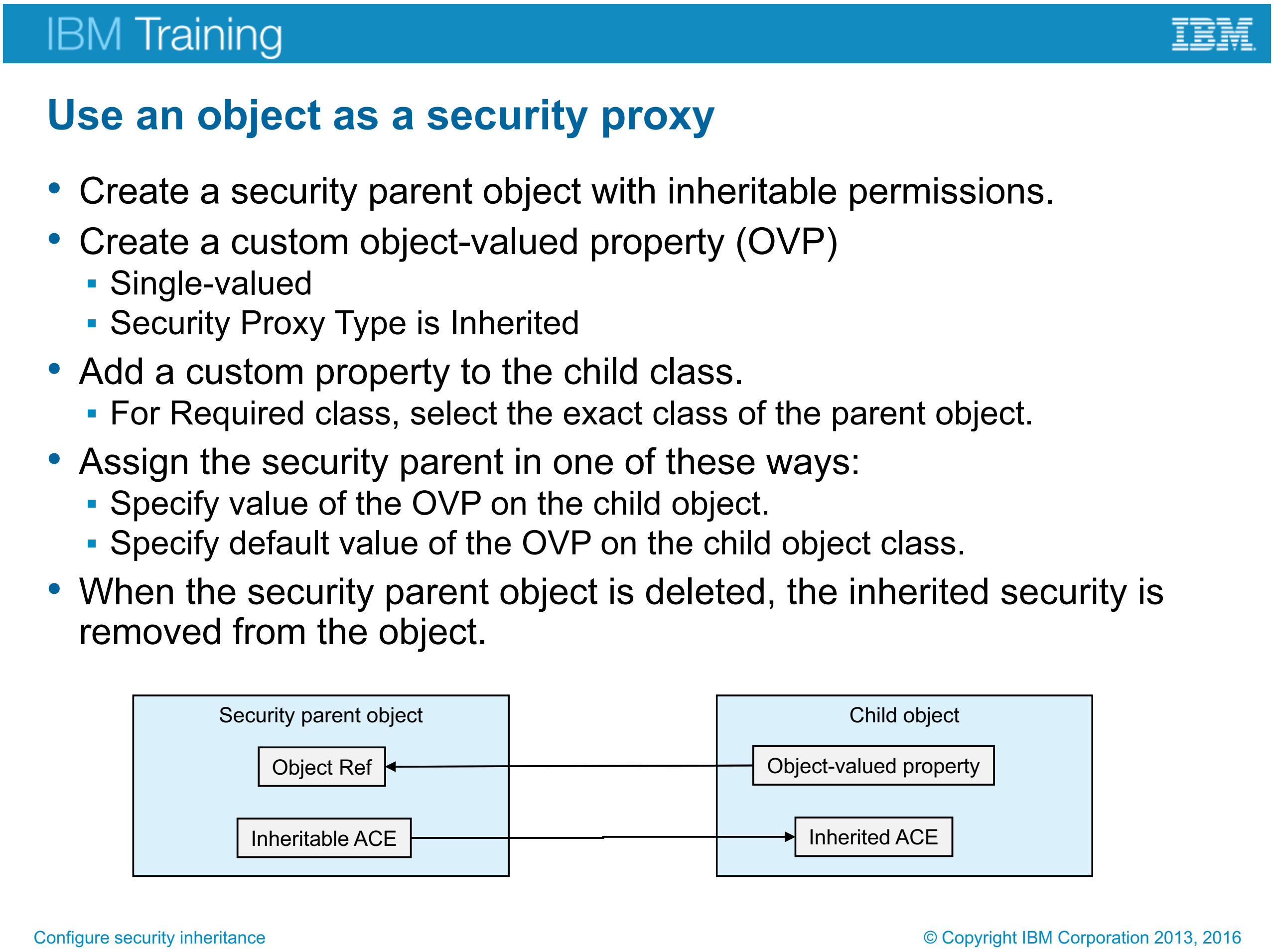
> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh007.htm

The two methods for setting the security folder property have equal outcomes, but have slightly different methods. The Inherit Security from Folder method does not require that you copy the object reference, but does require that the object is filed in that folder. You can select the folder from a menu. The second method (the Security Folder property method) does not require that the object is filed anywhere, but does require you to copy and paste an object reference.

Folder security inheritance can be automated by using a custom application. The Security Folder property value can be assigned to documents automatically.

Consequences of deleting folders or moving child objects

- If a Security Folder is deleted, those documents that had that folder as their security parent and that still exist in the object store no longer have a setting for Security Folder. They can be reassigned to another Security Folder.
- If an object that has a Security Parent is moved out of that folder, the Security Parent relationship is maintained.



IBM Training

Use an object as a security proxy

- Create a security parent object with inheritable permissions.
- Create a custom object-valued property (OVP)
  - Single-valued
  - Security Proxy Type is Inherited
- Add a custom property to the child class.
  - For Required class, select the exact class of the parent object.
- Assign the security parent in one of these ways:
  - Specify value of the OVP on the child object.
  - Specify default value of the OVP on the child object class.
- When the security parent object is deleted, the inherited security is removed from the object.

Configure security inheritance

Figure 5-9. Use an object as a security proxy

Help path

FileNet P8 Platform 5.2.1>Security>How to>Configure security inheritance>Configuring security inheritance by using a custom object-valued property

> http://www.ibm.com/support/knowledgecenter/SSNW2F_5.2.1/com.ibm.p8.security.doc/p8psh008.htm

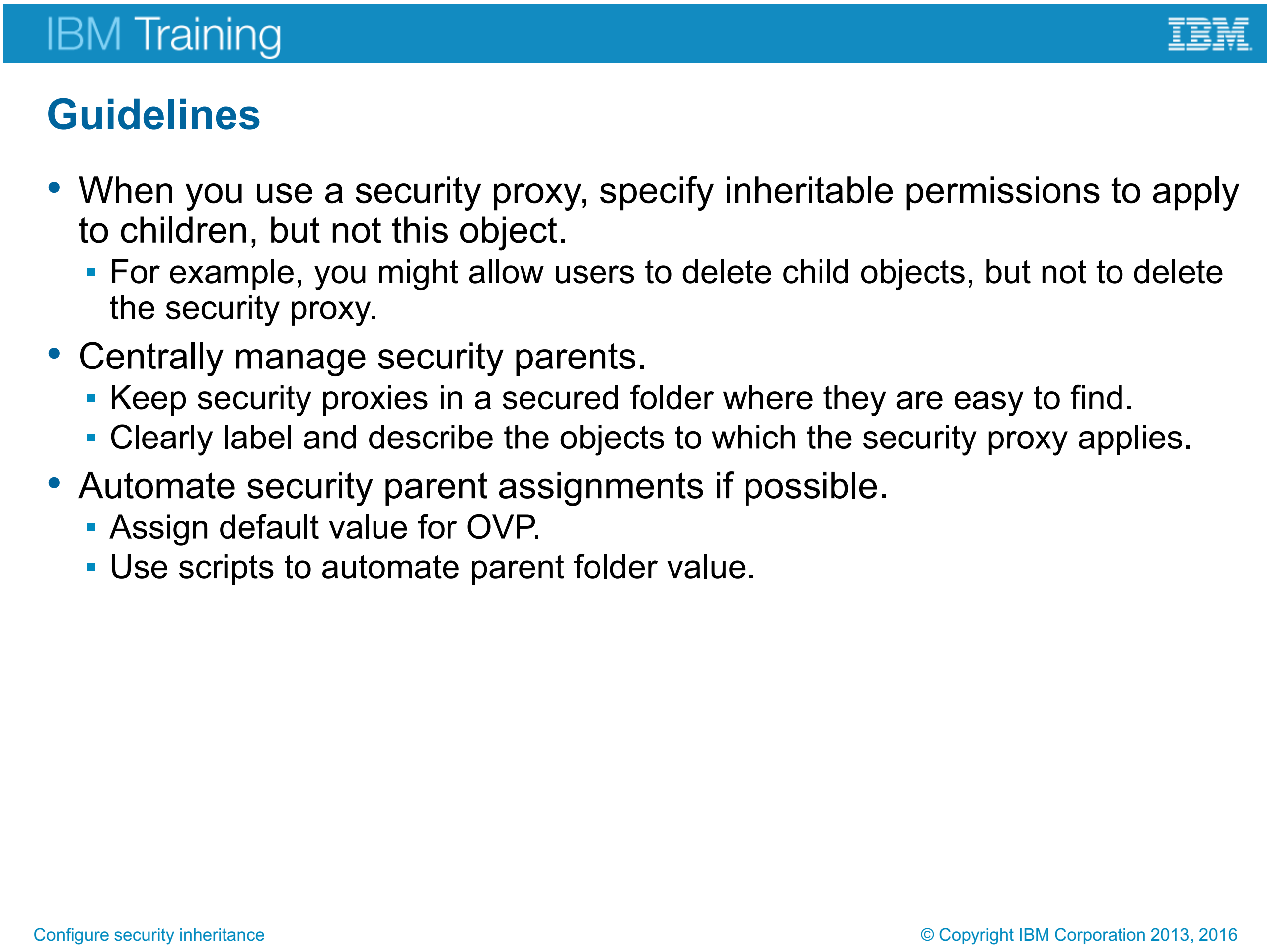
This method is more complex than using the Security Folder method, but it provides more flexibility. You can specify as many security parents as you need, and the security sources are not limited to being folders. For some business applications, the freedom to use other objects besides folders might allow for a more natural and simpler solution. This method can also be combined with the Security Folder method so that the final security on an object includes the inherited security from all sources.

An example scenario

A legal requirement exists for contracts that are used in the Finance department. From time to time, contracts must be viewable by auditors, who do not usually have access to the contracts. You want to be able to change the security on all of the contracts to allow auditors to access them, and then to remove that access when the audit ends.

Many folders act as security sources for the contracts that are filed within them, and other document types are also filed in these same folders and inherit security from them . You do not want to manually change the security on all of the folders, and you do not want the auditors to have access to the other documents that are filed in those folders. Therefore, you cannot change the security on the folders when the auditors need access to the contracts.

You can set up a custom property on a document class so that all contracts have a property that specifies the security proxy from which to inherit security. In this way, you can allow the documents to use their folder as a security parent, and provide an extra level of access that can be disabled or modified when needed.



IBM Training

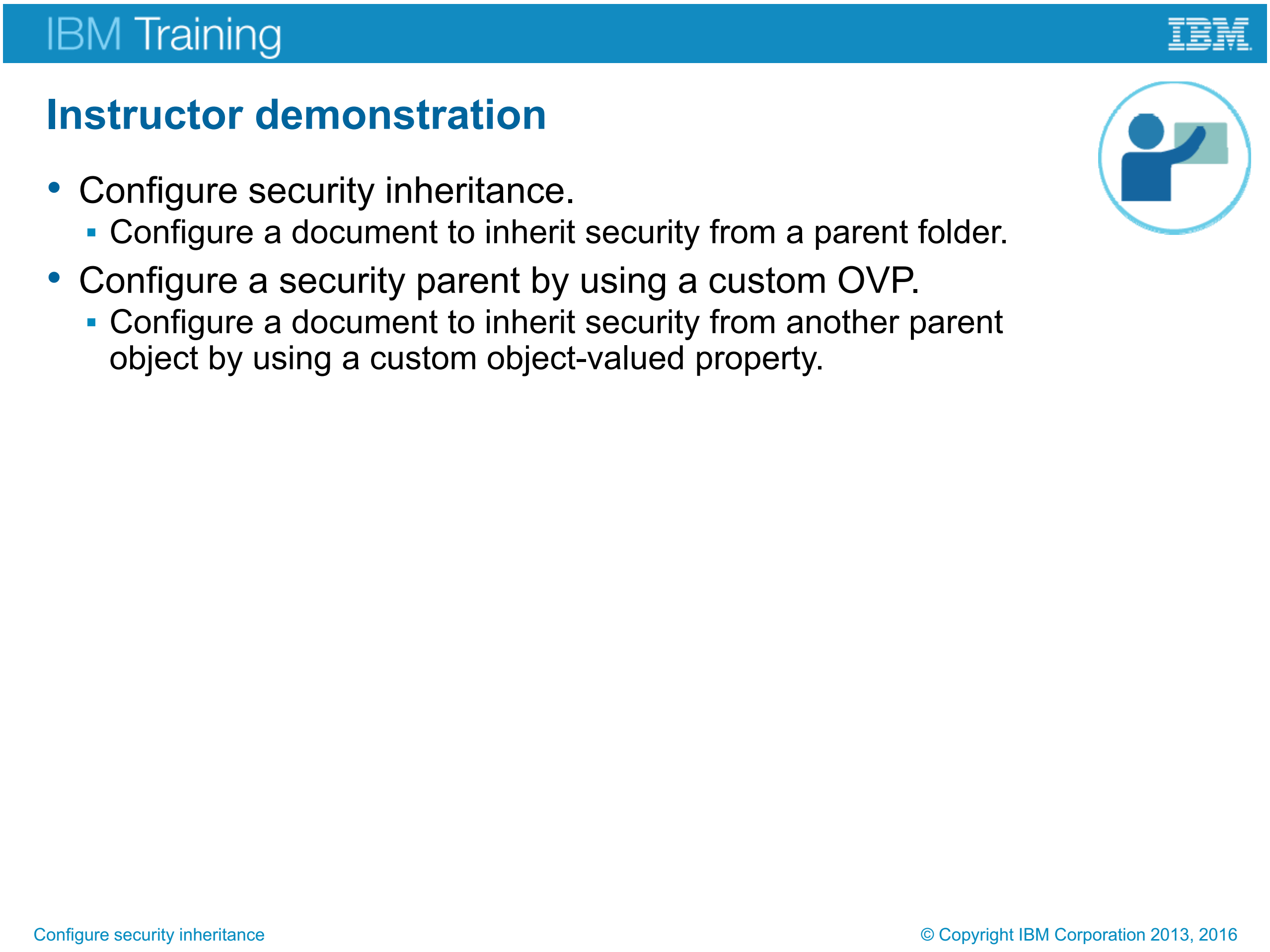
Guidelines

- When you use a security proxy, specify inheritable permissions to apply to children, but not this object.
  - For example, you might allow users to delete child objects, but not to delete the security proxy.
- Centrally manage security parents.
  - Keep security proxies in a secured folder where they are easy to find.
  - Clearly label and describe the objects to which the security proxy applies.
- Automate security parent assignments if possible.
  - Assign default value for OVP.
  - Use scripts to automate parent folder value.

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-10. Guidelines



IBM Training

IBM

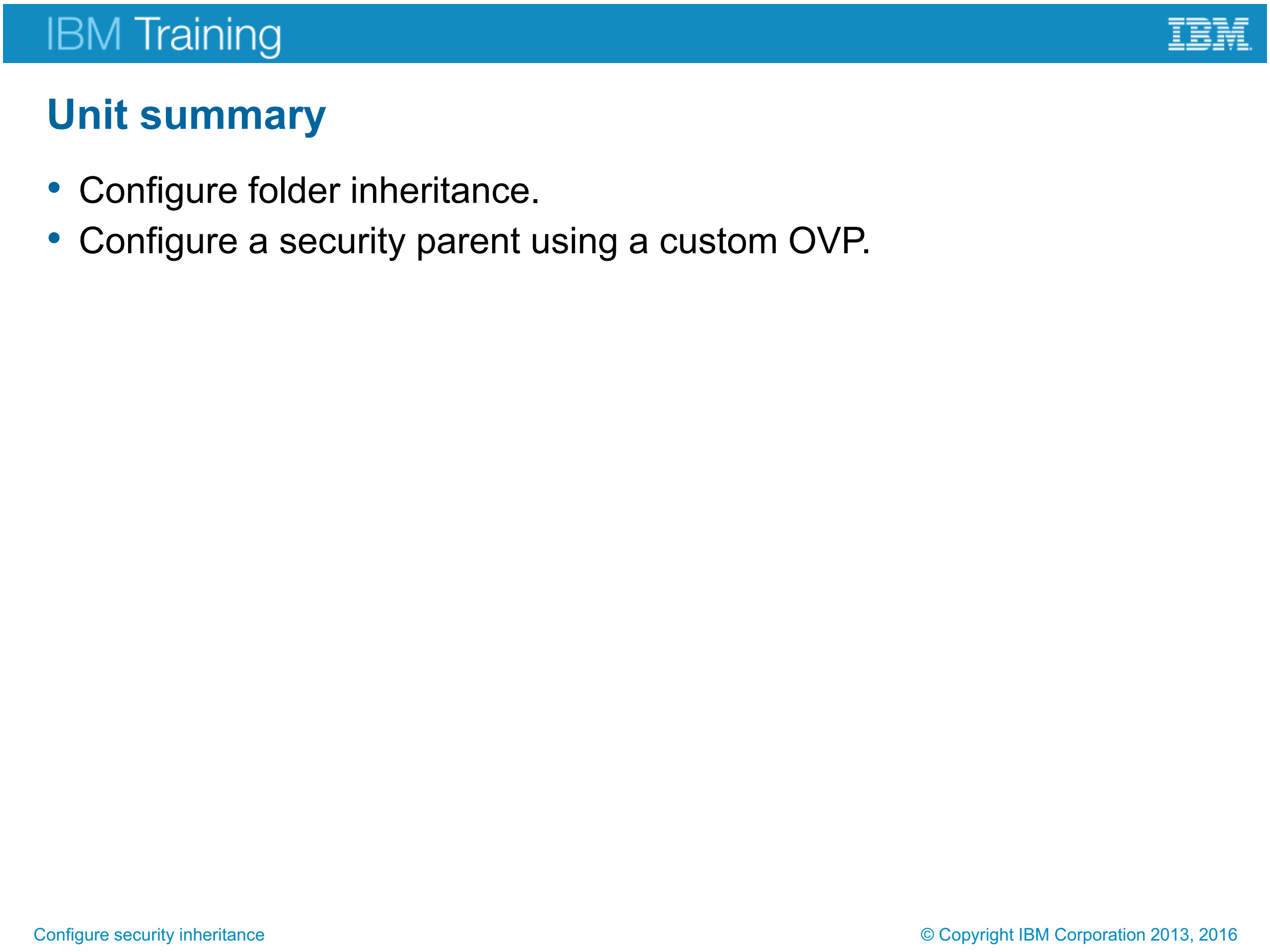
Instructor demonstration

- Configure security inheritance.
  - Configure a document to inherit security from a parent folder.
- Configure a security parent by using a custom OVP.
  - Configure a document to inherit security from another parent object by using a custom object-valued property.

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-11. Instructor demonstration



IBM Training

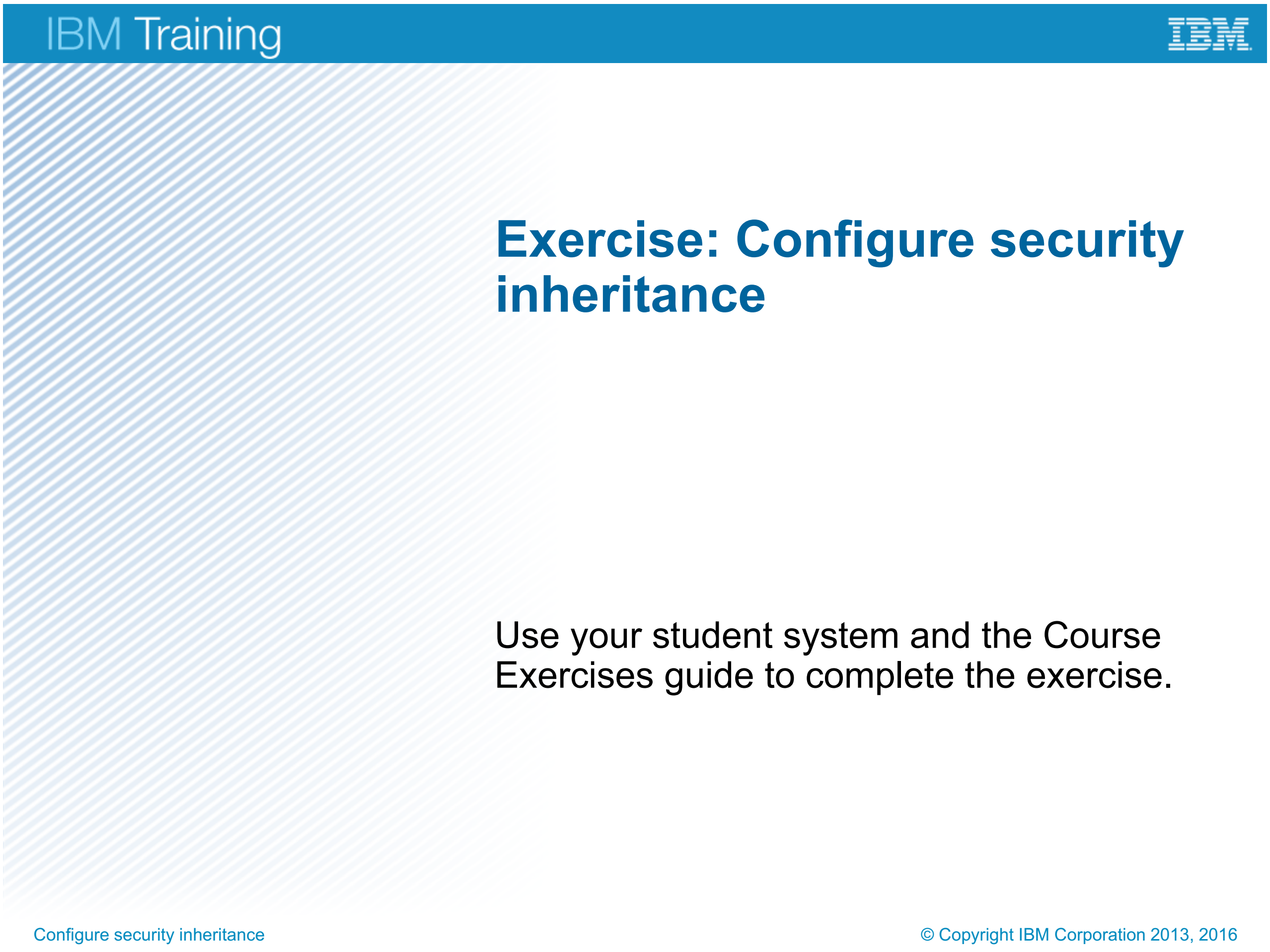
Unit summary

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

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-12. Unit summary



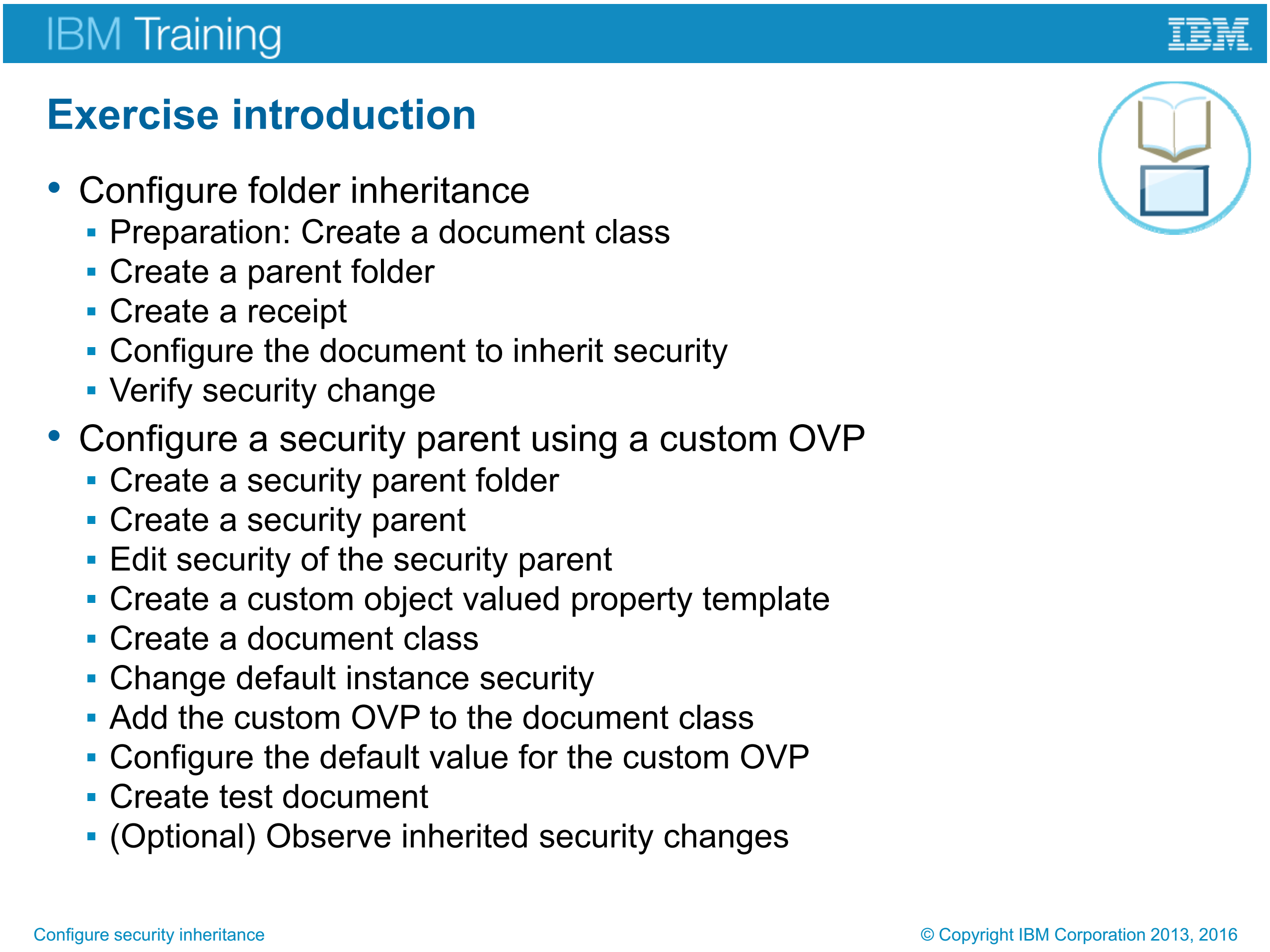
IBM Training

Exercise: Configure security inheritance

Use your student system and the Course Exercises guide to complete the exercise.

Configure security inheritance

Figure 5-13. Exercise: Configure security inheritance



IBM Training

Exercise introduction

- Configure folder inheritance
  - Preparation: Create a document class
  - Create a parent folder
  - Create a receipt
  - Configure the document to inherit security
  - Verify security change
- Configure a security parent using a custom OVP
  - Create a security parent folder
  - Create a security parent
  - Edit security of the security parent
  - Create a custom object valued property template
  - Create a document class
  - Change default instance security
  - Add the custom OVP to the document class
  - Configure the default value for the custom OVP
  - Create test document
  - (Optional) Observe inherited security changes

Configure security inheritance

© Copyright IBM Corporation 2013, 2016

Figure 5-14. Exercise introduction

IBM Training