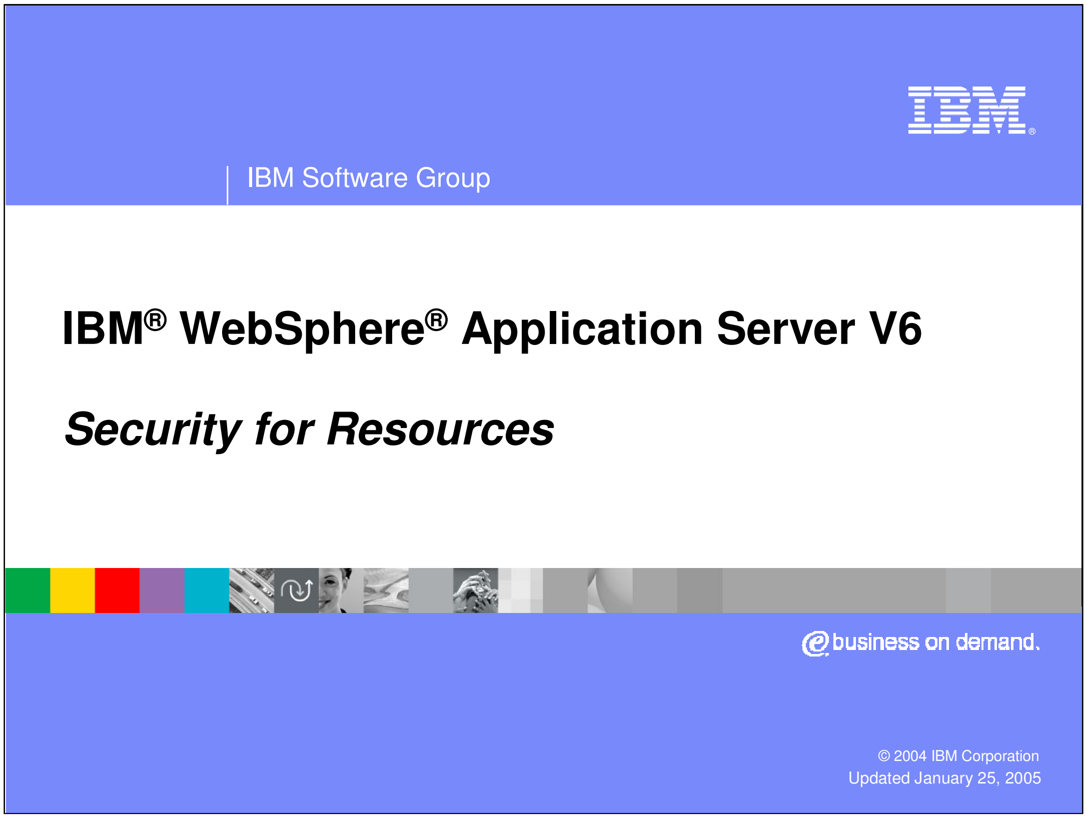


IBM Software Group

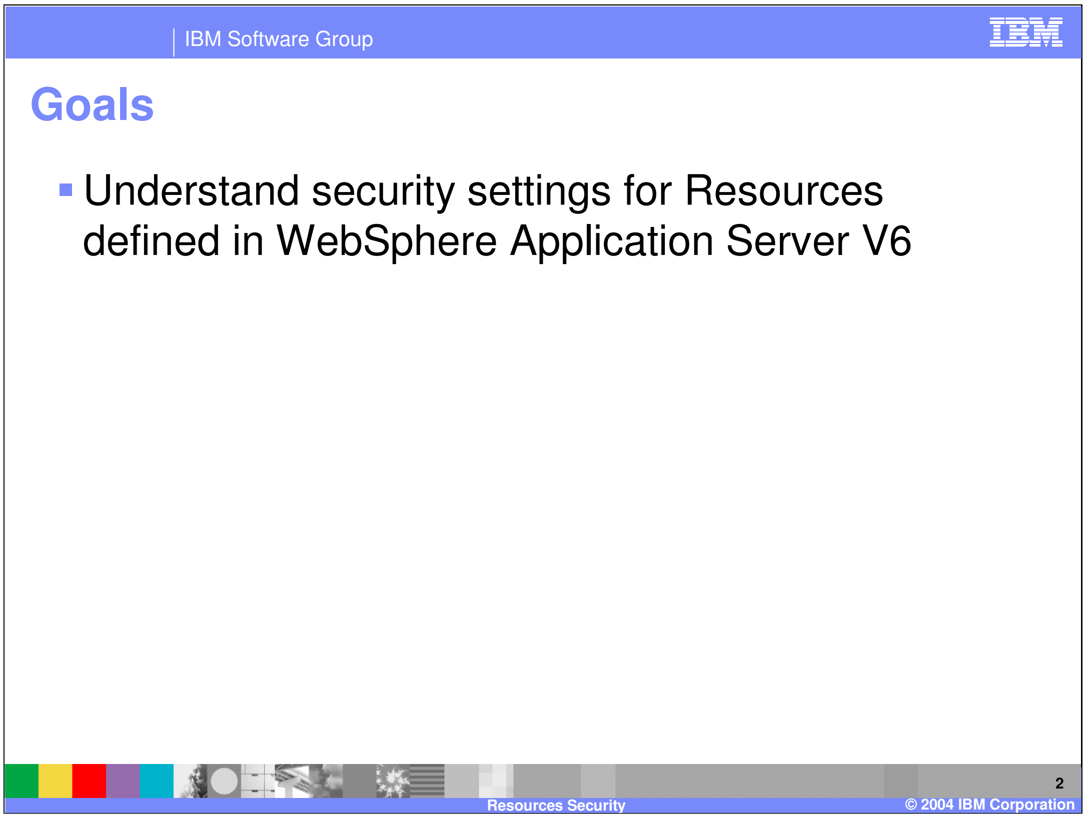
IBM® WebSphere® Application Server V6

Security for Resources

business on demand.

Updated January 25, 2005

This presentation will focus on security for resources.



Goals

- Understand security settings for Resources defined in WebSphere Application Server V6

The goals for this presentation are to help you understand security settings for resources defined in WebSphere Application Server V6.

Agenda

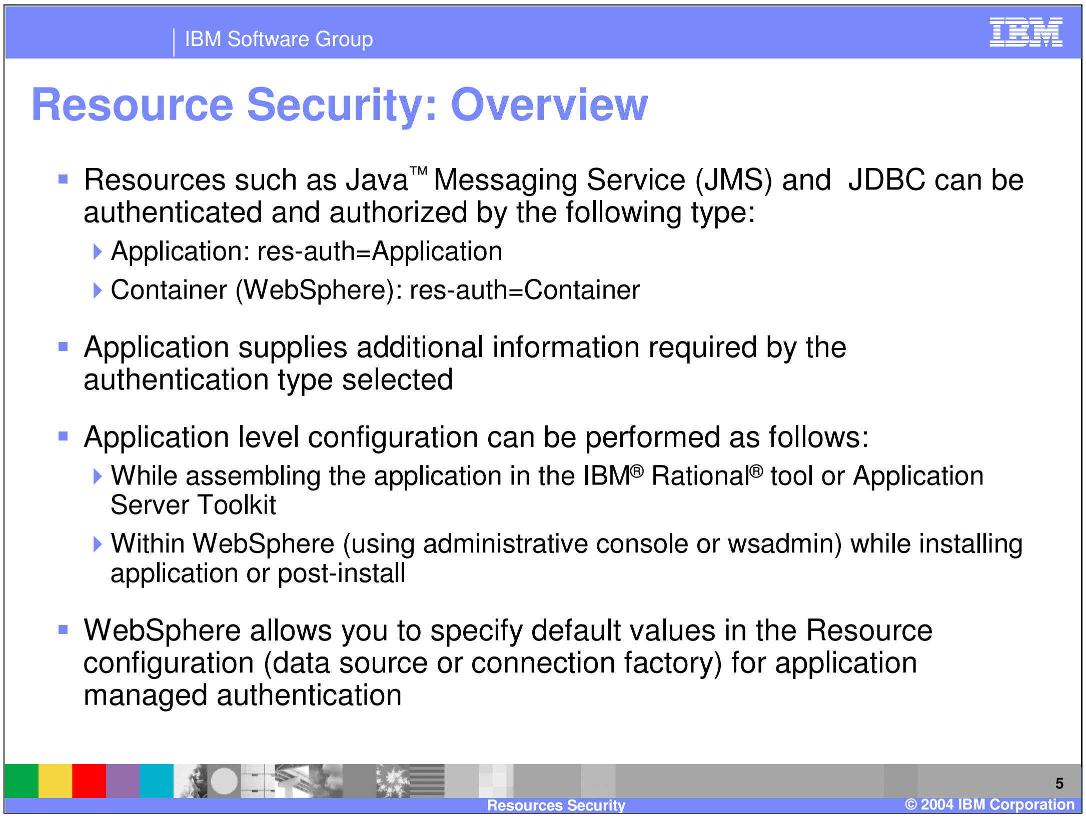
- Resource Security Overview
- Application level Authentication/Authorization settings
- Application Managed Authentication
- Container Managed Authentication
- Examples

The agenda for this presentation is listed in the above slide.

Section

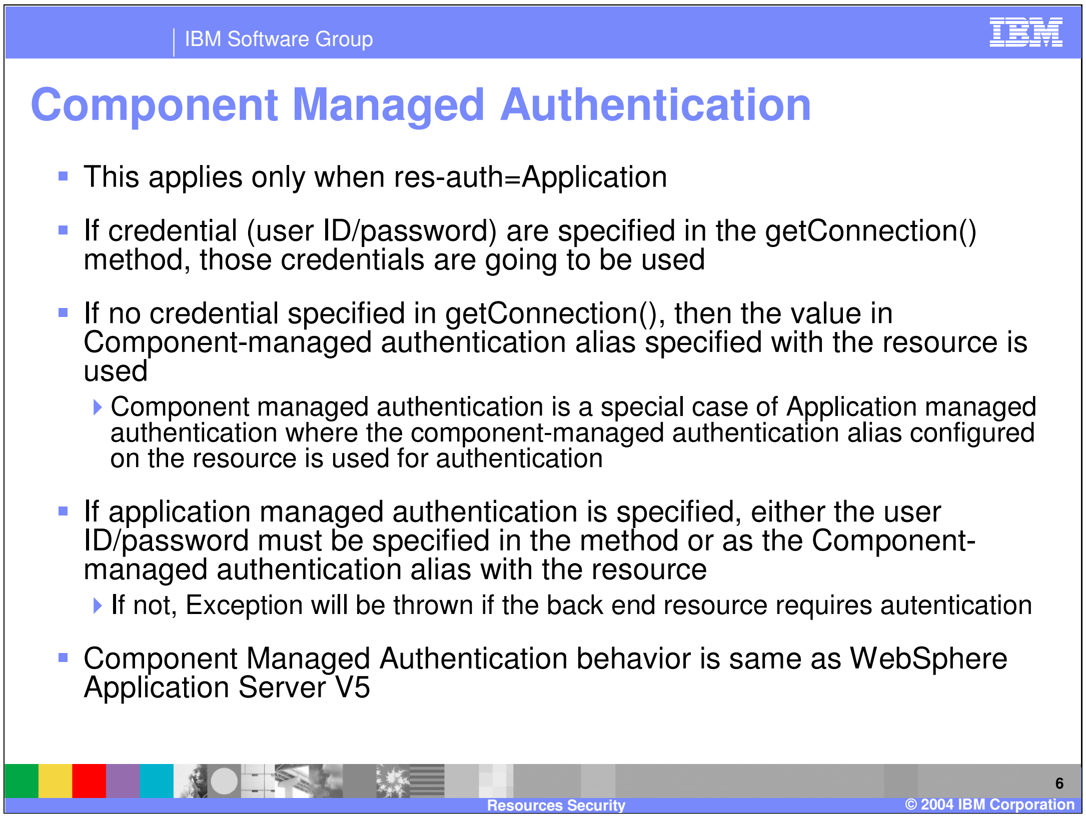
WebSphere Application Server V6 Resource Security

The next section will discuss resource security within WebSphere Application Server V6.



Resource Security: Overview

- Resources such as Java™ Messaging Service (JMS) and JDBC can be authenticated and authorized by the following type:
  - Application: res-auth=Application
  - Container (WebSphere): res-auth=Container
- Application supplies additional information required by the authentication type selected
- Application level configuration can be performed as follows:
  - While assembling the application in the IBM® Rational® tool or Application Server Toolkit
  - Within WebSphere (using administrative console or wsadmin) while installing application or post-install
- WebSphere allows you to specify default values in the Resource configuration (data source or connection factory) for application managed authentication



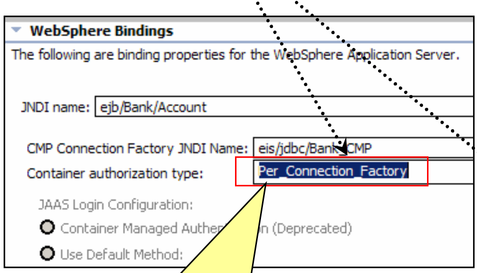
Component Managed Authentication

- This applies only when res-auth=Application
- If credential (user ID/password) are specified in the getConnection() method, those credentials are going to be used
- If no credential specified in getConnection(), then the value in Component-managed authentication alias specified with the resource is used
  - Component managed authentication is a special case of Application managed authentication where the component-managed authentication alias configured on the resource is used for authentication
- If application managed authentication is specified, either the user ID/password must be specified in the method or as the Component-managed authentication alias with the resource
  - If not, Exception will be thrown if the back end resource requires autentication
- Component Managed Authentication behavior is same as WebSphere Application Server V5

Note that if res-auth=Container, the specified user ID/password will be ignored

Component Managed Authentication Settings

Values in Application Deployment Descriptor		Corresponding Values in the WebSphere for Resource Authentication (Datasource or J2C connection factory)	
Auth. Type	**Authentication Method**	**Specify Authentication Alias as:**	**Mapping Login Configuration Alias**
Component (called “Per_Connection_Factory” in tools and “Per_application” in Admin console)	N/A	Component Managed	N/A



WebSphere Bindings

The following are binding properties for the WebSphere Application Server.

JNDI name: ejb/Bank/Account

CMP Connection Factory JNDI Name: eis/jdbc/BankCMP

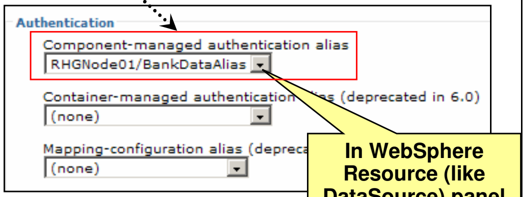
Container authorization type: Per_Connection_Factory

JAAS Login Configuration:

○ Container Managed Auther n (Deprecated)

○ Use Default Method:

In Tools, specified as “Per_Connection_Factory” Done during Application Assembly



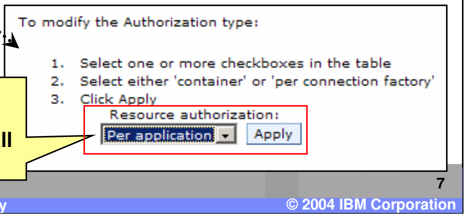
Authentication

Component-managed authentication alias: RHGNode01/BankDataAlias

Container-managed authentication ias (deprecated in 6.0): (none)

Mapping-configuration alias (depreca: (none)

In WebSphere Resource (like DataSource) panel

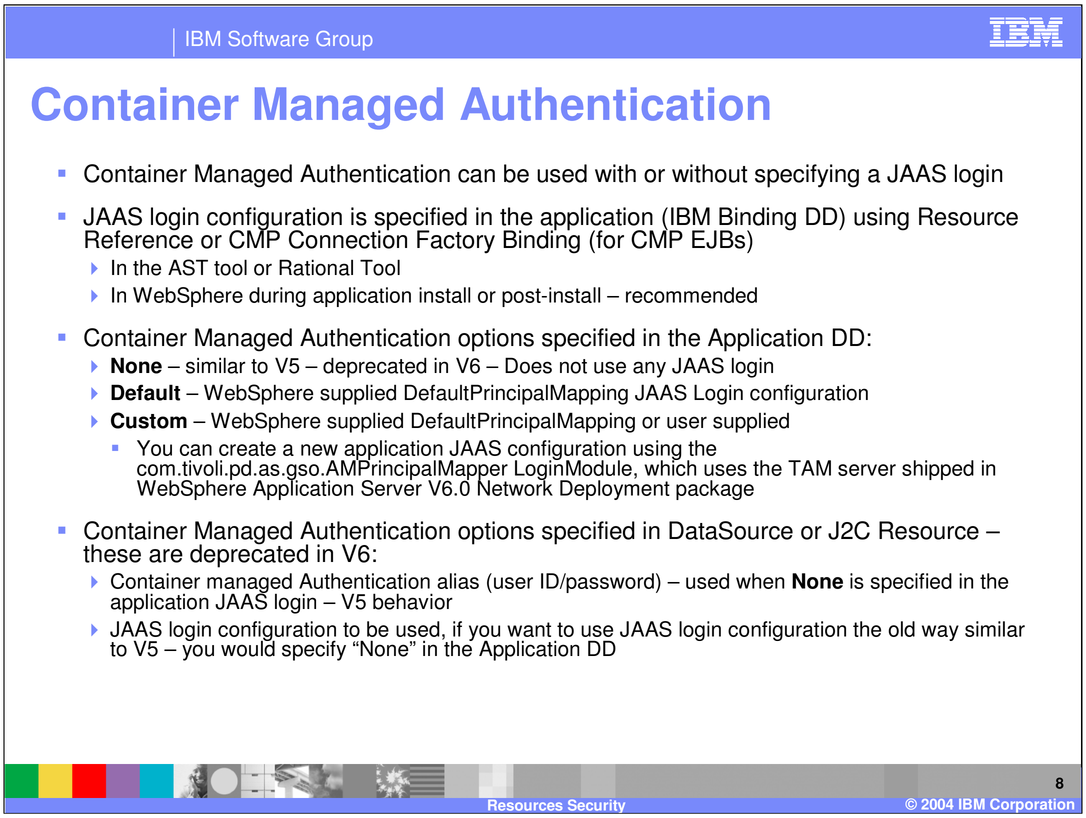


To modify the Authorization type:

1. Select one or more checkboxes in the table
2. Select either 'container' or 'per connection factory'
3. Click Apply

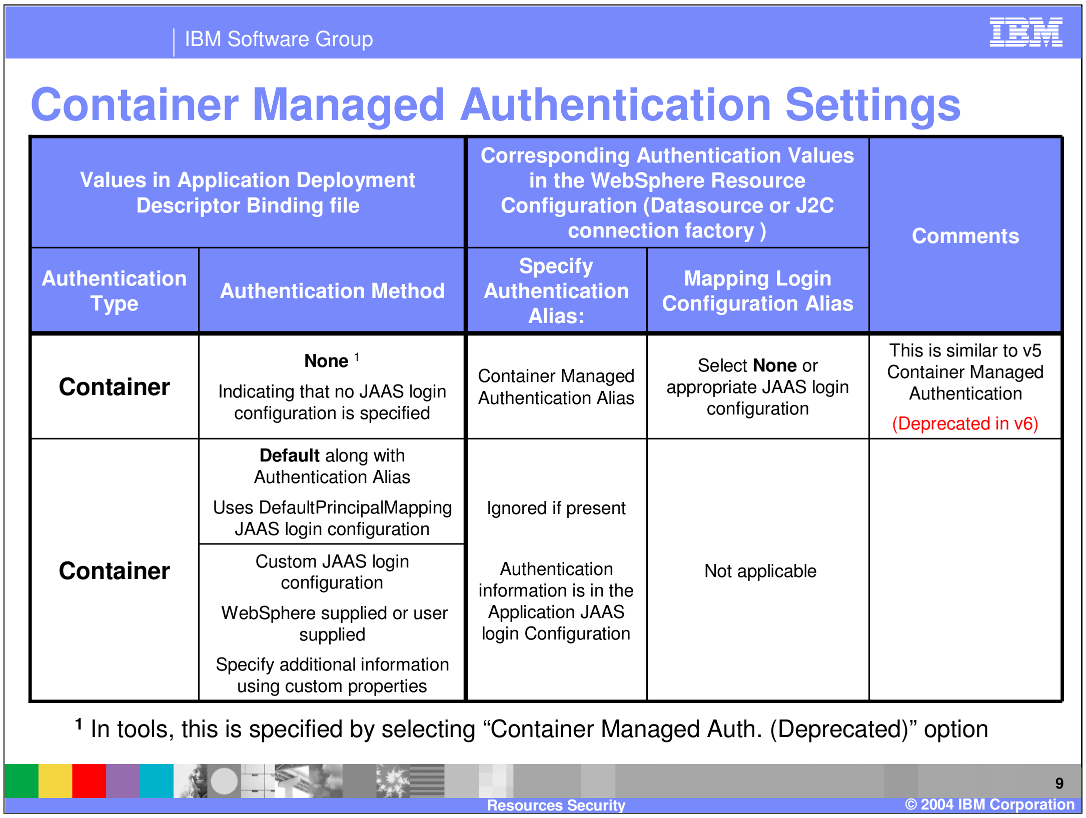
Resource authorization: Per application

In WebSphere Admininstrative Console, during install or post-install



Container Managed Authentication

- Container Managed Authentication can be used with or without specifying a JAAS login
- JAAS login configuration is specified in the application (IBM Binding DD) using Resource Reference or CMP Connection Factory Binding (for CMP EJBs)
  - In the AST tool or Rational Tool
  - In WebSphere during application install or post-install – recommended
- Container Managed Authentication options specified in the Application DD:
  - **None** – similar to V5 – deprecated in V6 – Does not use any JAAS login
  - **Default** – WebSphere supplied DefaultPrincipalMapping JAAS Login configuration
  - **Custom** – WebSphere supplied DefaultPrincipalMapping or user supplied
    - You can create a new application JAAS configuration using the com.tivoli.pd.as.gso.AMPrincipalMapper LoginModule, which uses the TAM server shipped in WebSphere Application Server V6.0 Network Deployment package
- Container Managed Authentication options specified in DataSource or J2C Resource – these are deprecated in V6:
  - Container managed Authentication alias (user ID/password) – used when **None** is specified in the application JAAS login – V5 behavior
  - JAAS login configuration to be used, if you want to use JAAS login configuration the old way similar to V5 – you would specify “None” in the Application DD



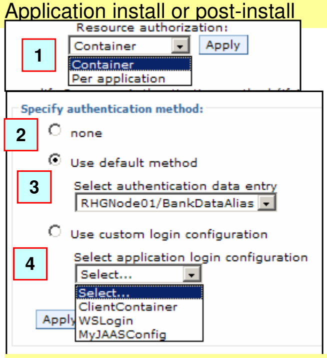
Container Managed Authentication Settings

Values in Application Deployment Descriptor Binding file		Corresponding Authentication Values in the WebSphere Resource Configuration (Datasource or J2C connection factory)		Comments
Authentication Type	Authentication Method	Specify Authentication Alias:	Mapping Login Configuration Alias	
Container	**None** [1] Indicating that no JAAS login configuration is specified	Container Managed Authentication Alias	Select **None** or appropriate JAAS login configuration	This is similar to v5 Container Managed Authentication (Deprecated in v6)
Container	**Default** along with Authentication Alias Uses DefaultPrincipalMapping JAAS login configuration	Ignored if present Authentication information is in the Application JAAS login Configuration	Not applicable	
	Custom JAAS login configuration WebSphere supplied or user supplied Specify additional information using custom properties			

[1] In tools, this is specified by selecting “Container Managed Auth. (Deprecated)” option

Container Managed Authentication Setting UI

Administrative Console - During Application install or post-install



Resource authorization: Container ▾ Apply
- Container
- Per application

Specify authentication method:

○ none

● Use default method

Select authentication data entry: RHGNode01/BankDataAlias ▾

○ Use custom login configuration

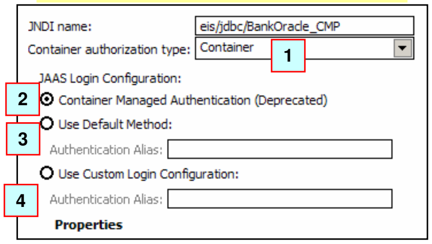
Select application login configuration: Select... ▾
- Select...
- ClientContainer
- WSLogin
- MyJAASConfig

Apply

OR

Application Config.

In Tools – setting Authentication type and other information



JNDI name: eis/jdbc/BankOracle_CMP

Container authorization type: Container ▾

JAAS Login Configuration:

● Container Managed Authentication (Deprecated)

○ Use Default Method:

Authentication Alias:

○ Use Custom Login Configuration:

Authentication Alias:

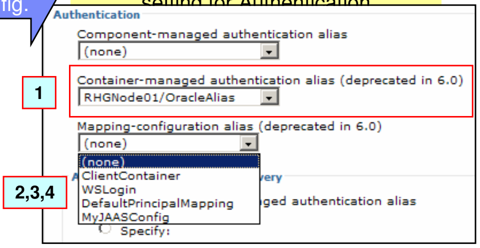
Properties

Match the numbers - Specify Auth. type and one of the authentication methods

1) **Specify Authentication Type = Container**
2) **Authentication method = NONE – similar to V5**
3) **Default Authentication Method and Auth. alias - “DefaultPrincipalMapping” Login configuration**
4) **Custom Login configuration can use any WebSphere or user supplied custom JAAS Login configuration**

Resource Config.

Administrative Console Resource setting for Authentication



Authentication

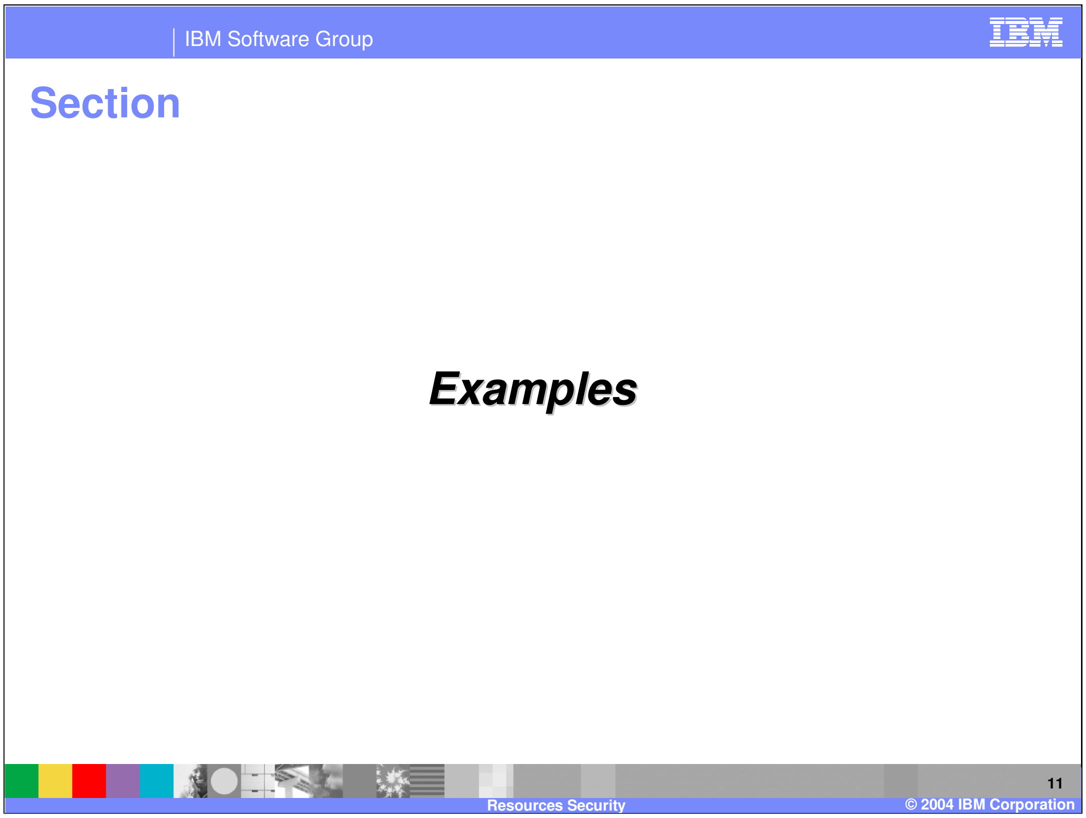
Component-managed authentication alias: (none) ▾

Container-managed authentication alias (deprecated in 6.0): RHGNode01/OracleAlias ▾

Mapping-configuration alias (deprecated in 6.0): (none) ▾
- (none)
- ClientContainer
- WSLogin
- DefaultPrincipalMapping
- MyJAASConfig

ged authentication alias

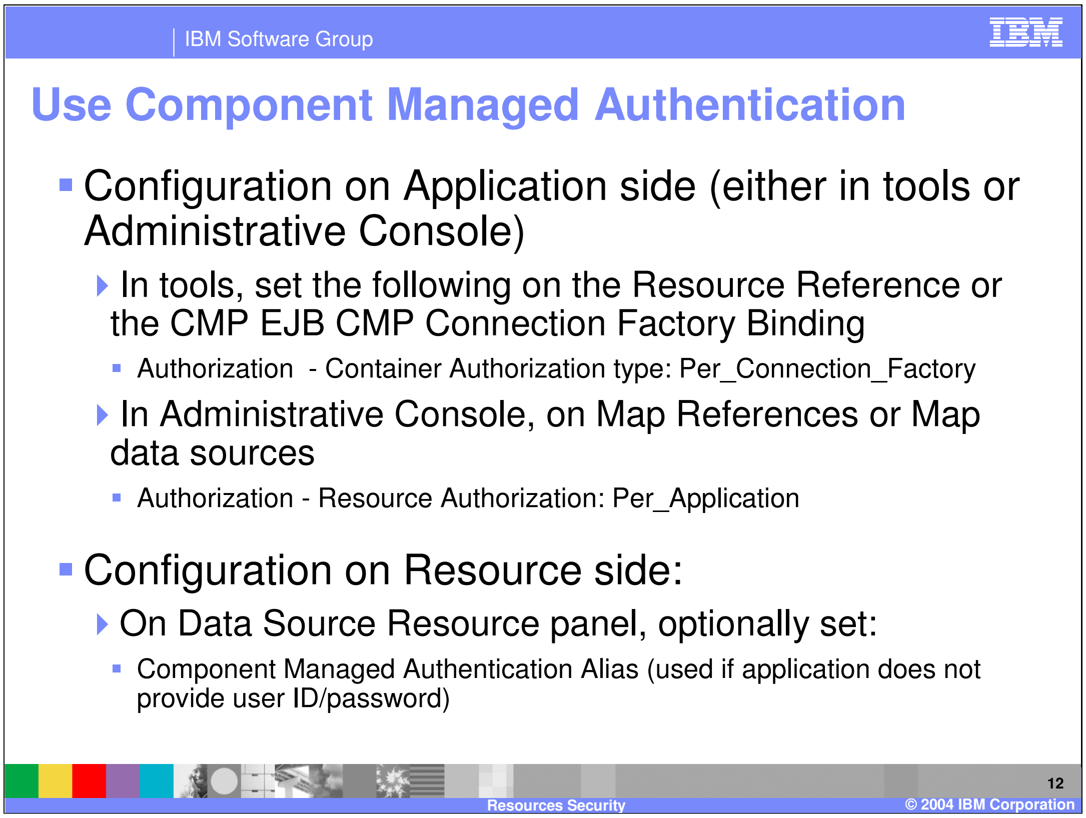
○ Specify:



Section

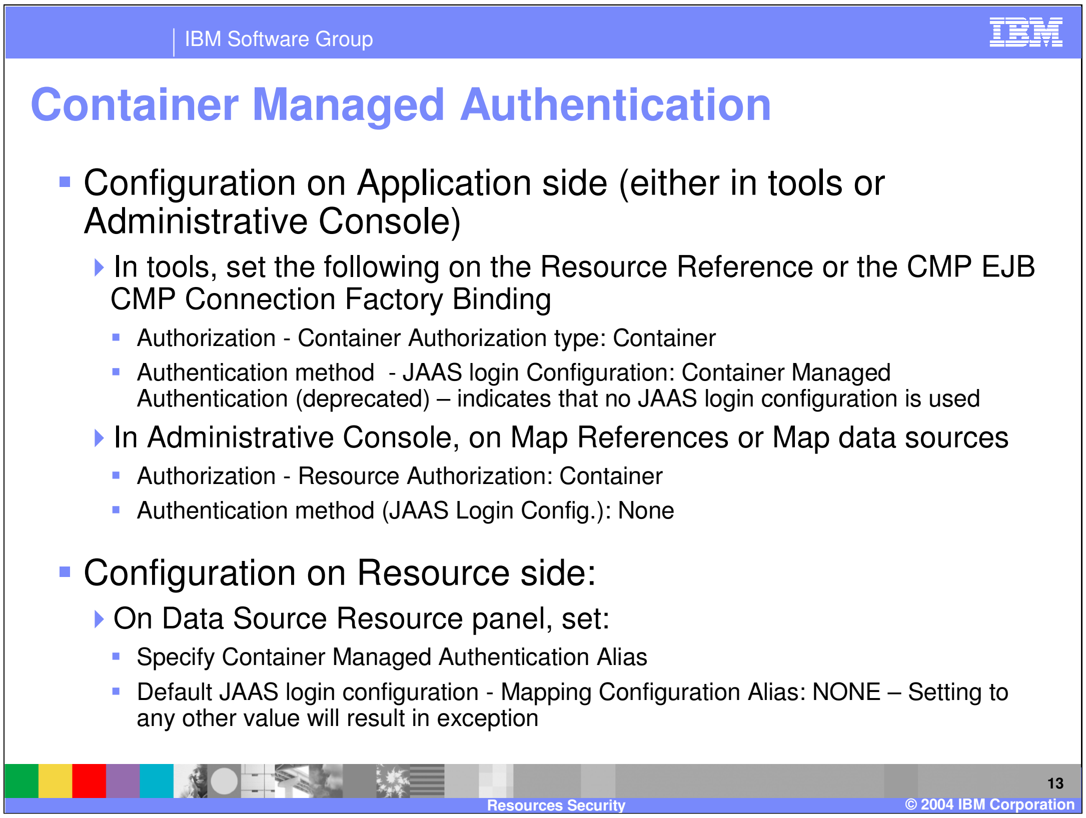
Examples

The next section will give some examples of resource security within WebSphere Application Server V6.



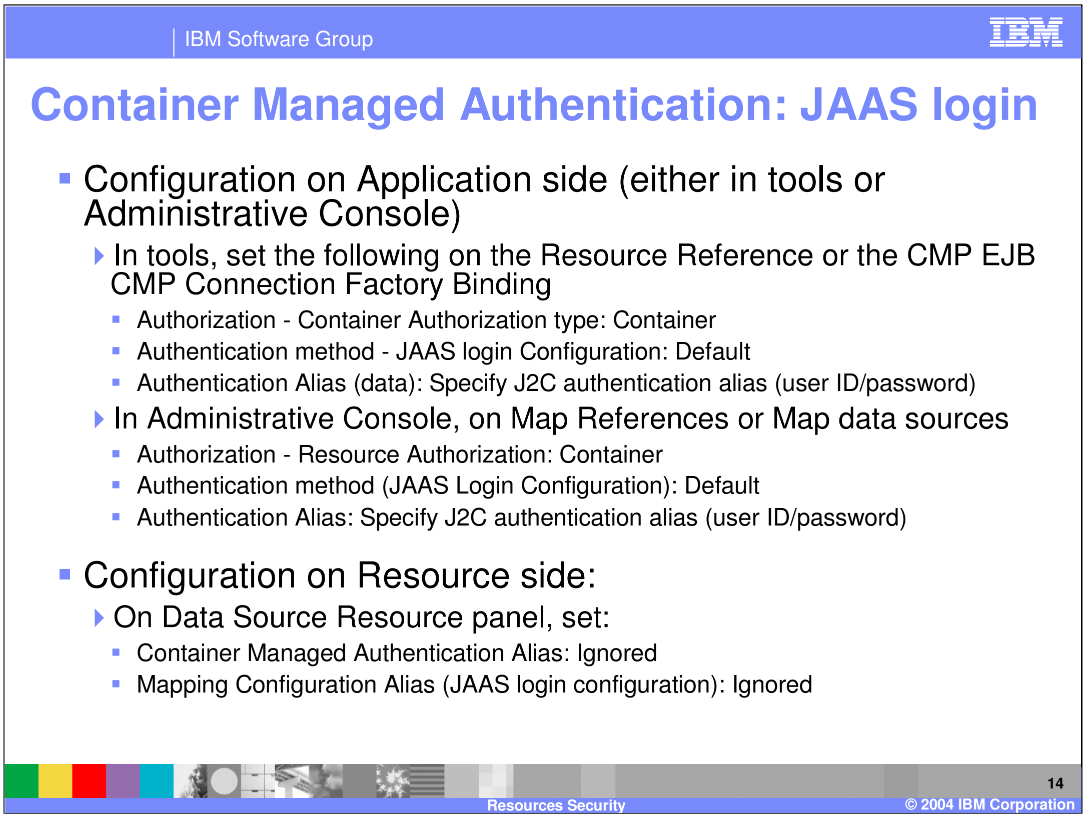
Use Component Managed Authentication

- Configuration on Application side (either in tools or Administrative Console)
  - In tools, set the following on the Resource Reference or the CMP EJB CMP Connection Factory Binding
    - Authorization - Container Authorization type: Per_Connection_Factory
  - In Administrative Console, on Map References or Map data sources
    - Authorization - Resource Authorization: Per_Application
- Configuration on Resource side:
  - On Data Source Resource panel, optionally set:
    - Component Managed Authentication Alias (used if application does not provide user ID/password)



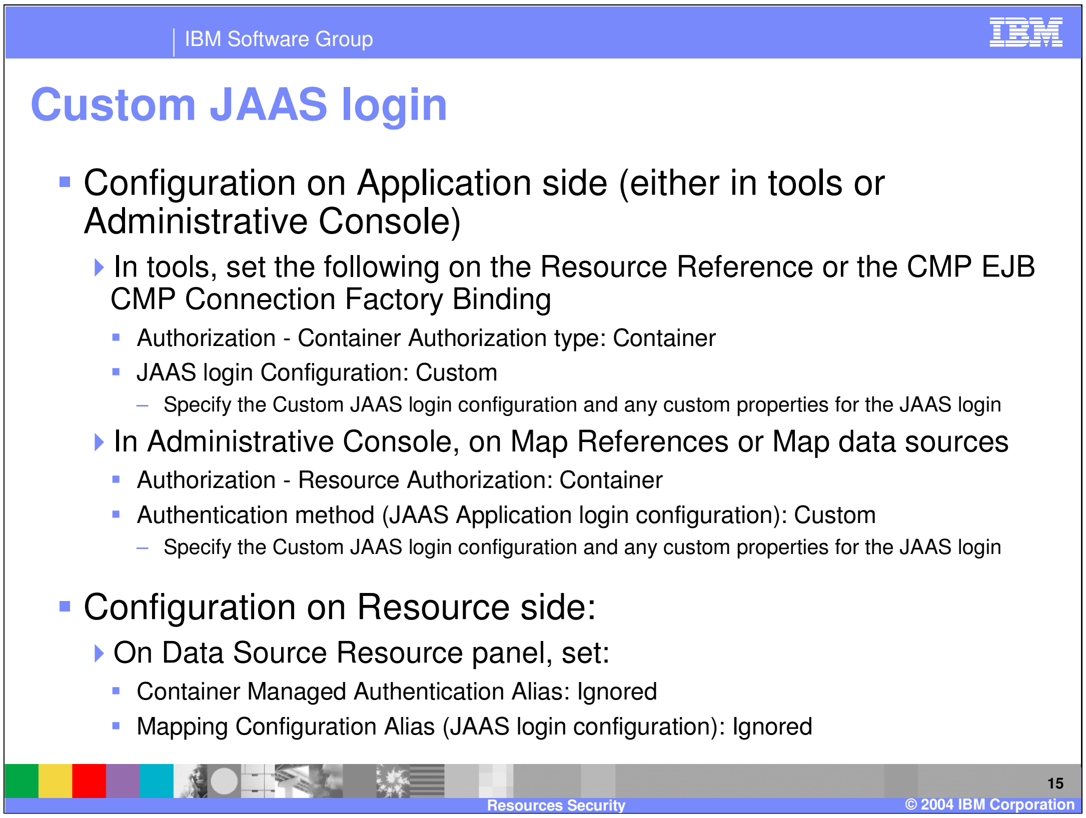
Container Managed Authentication

- Configuration on Application side (either in tools or Administrative Console)
  - In tools, set the following on the Resource Reference or the CMP EJB CMP Connection Factory Binding
    - Authorization - Container Authorization type: Container
    - Authentication method - JAAS login Configuration: Container Managed Authentication (deprecated) – indicates that no JAAS login configuration is used
  - In Administrative Console, on Map References or Map data sources
    - Authorization - Resource Authorization: Container
    - Authentication method (JAAS Login Config.): None
- Configuration on Resource side:
  - On Data Source Resource panel, set:
    - Specify Container Managed Authentication Alias
    - Default JAAS login configuration - Mapping Configuration Alias: NONE – Setting to any other value will result in exception



Container Managed Authentication: JAAS login

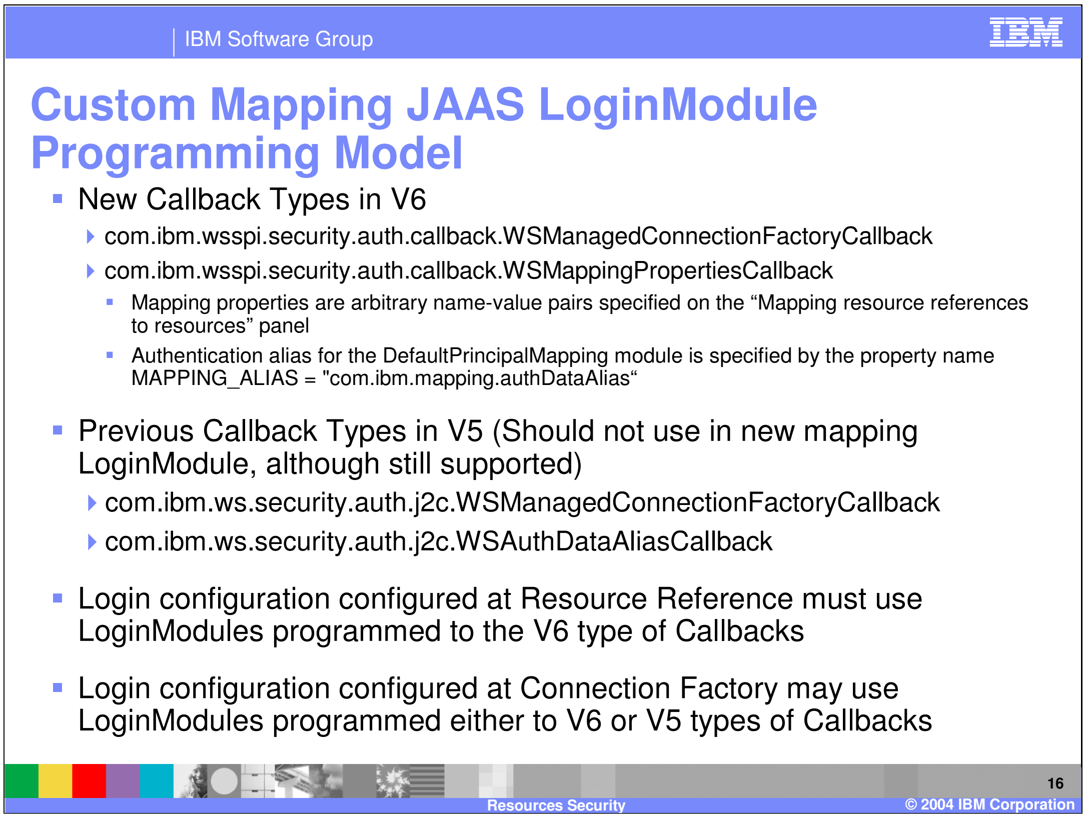
- Configuration on Application side (either in tools or Administrative Console)
  - In tools, set the following on the Resource Reference or the CMP EJB CMP Connection Factory Binding
    - Authorization - Container Authorization type: Container
    - Authentication method - JAAS login Configuration: Default
    - Authentication Alias (data): Specify J2C authentication alias (user ID/password)
  - In Administrative Console, on Map References or Map data sources
    - Authorization - Resource Authorization: Container
    - Authentication method (JAAS Login Configuration): Default
    - Authentication Alias: Specify J2C authentication alias (user ID/password)
- Configuration on Resource side:
  - On Data Source Resource panel, set:
    - Container Managed Authentication Alias: Ignored
    - Mapping Configuration Alias (JAAS login configuration): Ignored



Custom JAAS login

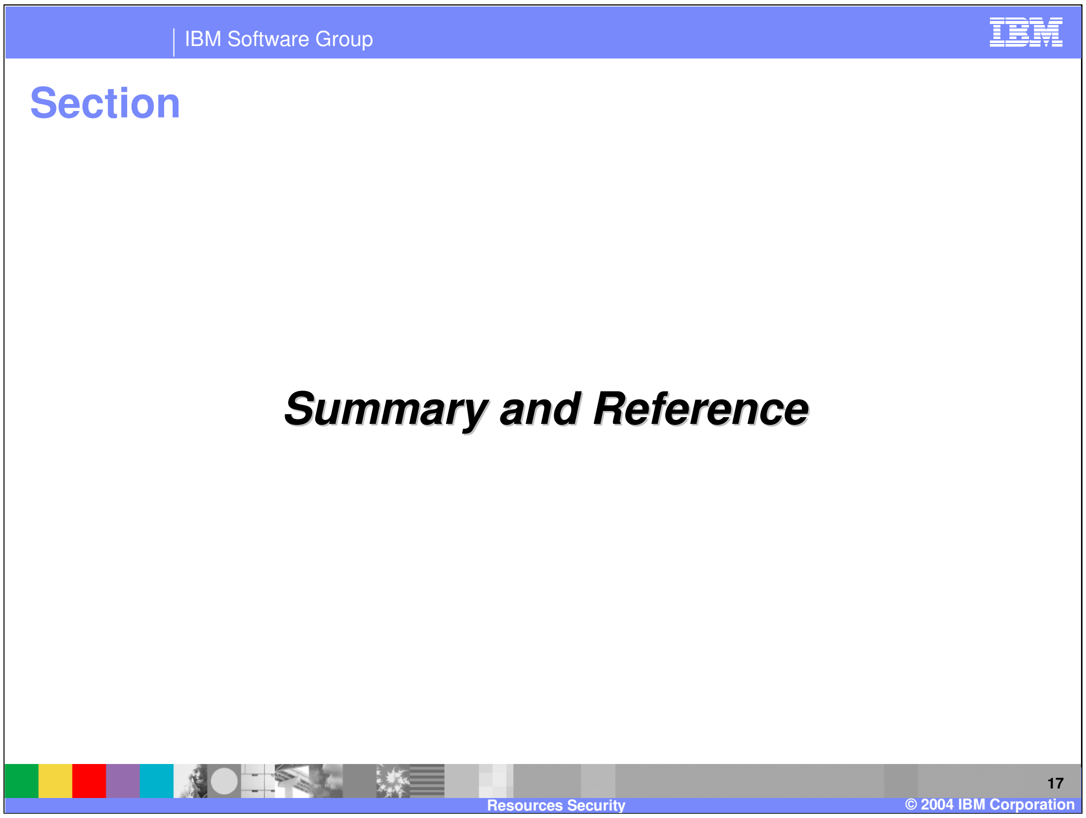
- Configuration on Application side (either in tools or Administrative Console)
  - In tools, set the following on the Resource Reference or the CMP EJB CMP Connection Factory Binding
    - Authorization - Container Authorization type: Container
    - JAAS login Configuration: Custom
      - Specify the Custom JAAS login configuration and any custom properties for the JAAS login
  - In Administrative Console, on Map References or Map data sources
    - Authorization - Resource Authorization: Container
    - Authentication method (JAAS Application login configuration): Custom
      - Specify the Custom JAAS login configuration and any custom properties for the JAAS login

- Configuration on Resource side:
  - On Data Source Resource panel, set:
    - Container Managed Authentication Alias: Ignored
    - Mapping Configuration Alias (JAAS login configuration): Ignored



Custom Mapping JAAS LoginModule Programming Model

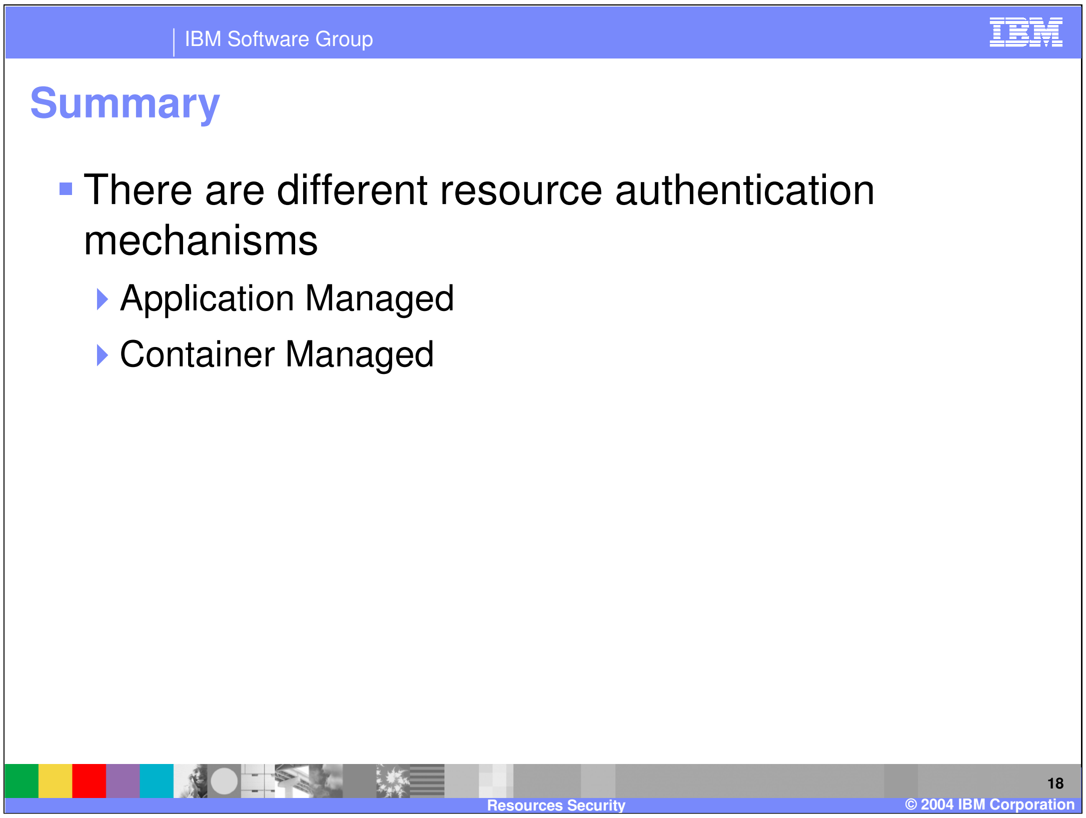
- New Callback Types in V6
  - com.ibm.wsspi.security.auth.callback.WSManagedConnectionFactoryCallback
  - com.ibm.wsspi.security.auth.callback.WSMappingPropertiesCallback
    - Mapping properties are arbitrary name-value pairs specified on the “Mapping resource references to resources” panel
    - Authentication alias for the DefaultPrincipalMapping module is specified by the property name MAPPING_ALIAS = "com.ibm.mapping.authDataAlias“
- Previous Callback Types in V5 (Should not use in new mapping LoginModule, although still supported)
  - com.ibm.ws.security.auth.j2c.WSManagedConnectionFactoryCallback
  - com.ibm.ws.security.auth.j2c.WSAuthDataAliasCallback
- Login configuration configured at Resource Reference must use LoginModules programmed to the V6 type of Callbacks
- Login configuration configured at Connection Factory may use LoginModules programmed either to V6 or V5 types of Callbacks



Section

Summary and Reference

The next section will discuss the summary.



IBM Software Group

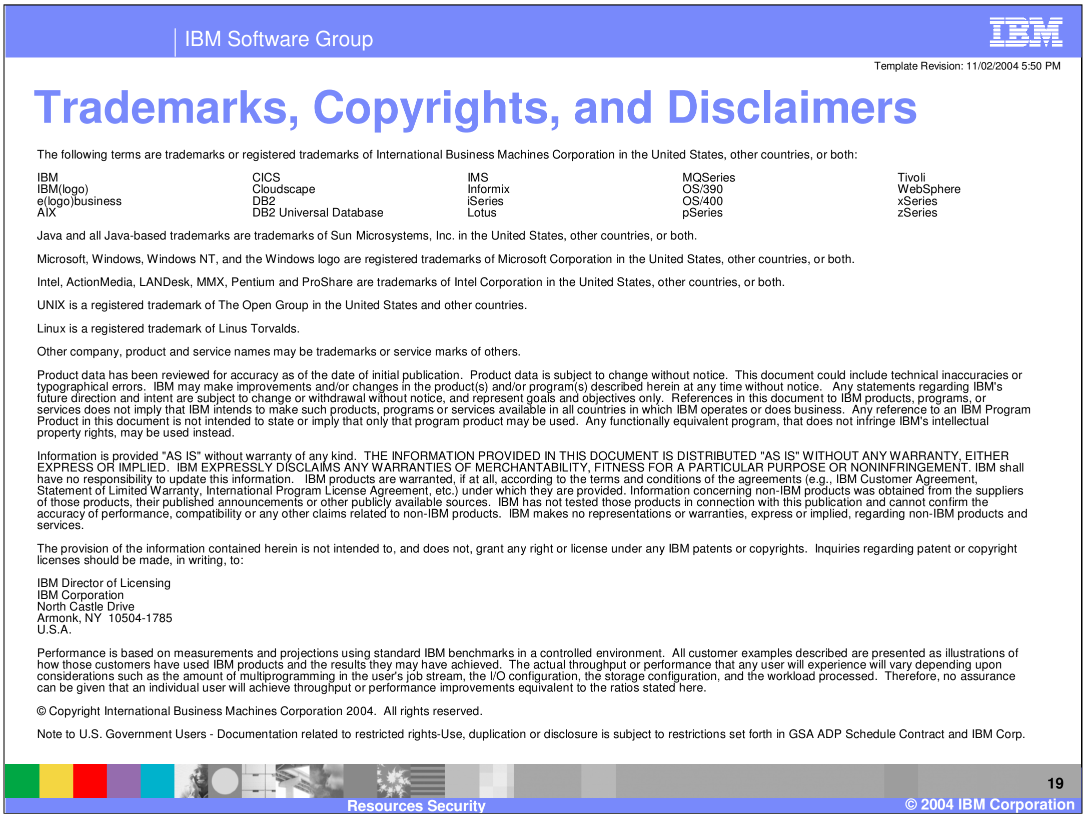
Summary

- There are different resource authentication mechanisms
  - Application Managed
  - Container Managed

18

Resources Security

In summary, this presentation has focused on both Component Managed, and Container Managed resource authentication mechanisms.



Template Revision: 11/02/2004 5:50 PM

Trademarks, Copyrights, and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM
IBM(logo)
e(logo)business
AIX
CICS
Cloudscape
DB2
DB2 Universal Database
IMS
Informix
iSeries
Lotus
MQSeries
OS/390
OS/400
pSeries
Tivoli
WebSphere
xSeries
zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

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

Linux is a registered trademark of Linus Torvalds.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. 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 in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.