IBM Software Group

IBM® WebSphere® Application Server V6

Service Integration Bus Security

e business on demand.

Updated January 25, 2005

Goals

- Understand Security settings for the Service Integration Bus and its components
- Learn how the security components of Service Integration Bus provide end-to-end security for sending and receiving messages via the Service Integration Bus
- Prerequisite
  - WebSphere Application Server V6 Security Architecture

Agenda

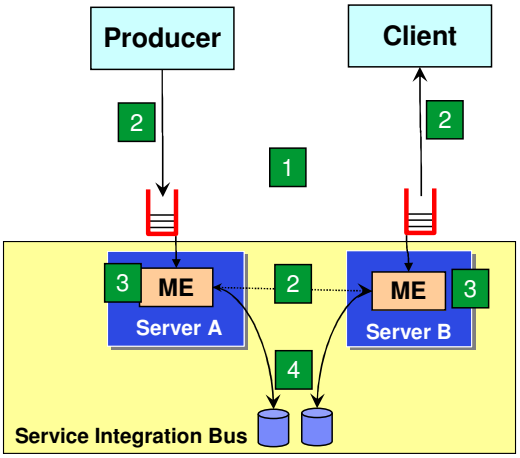
- Service Integration Bus Security
- Wsadmin tasks to configure Service Integration Bus Security
- Problem Determination
- Summary

Section

Service Integration Bus Resources Security

Service Integration Bus Security Overview

- Security coverage is as follows:
  1. Authentication and authorization of users, when connecting to a bus and when using the bus resources
  2. Secure communication transports (SSL, HTTPS) between the client and messaging engine (ME) and between messaging engines
  3. Authentication of messaging engines joining a bus
  4. Authentication of message store (database) users
- Message Security administration is done through wsadmin task commands



Service Integration Bus Resources

- Bus
- Foreign Bus
- Destination
  - queue
  - topicSpace
  - foreignDestination
  - webService
  - ports
  - alias
  - Temporary Destination
- Topic
  - Root – top level of Topic hierarchy
  - Any topic down the hierarchy

Messaging Security: Authentication/Authorization

- Authentication occurs when client creates a connection to Service Integration Bus resources
  - User ID/password are authenticated using the configured User Registry of the Application server
- Once authenticated, authorization occurs
  - Checks if the user has permission to access the resources
- Authorization is done for the following access/operation:
  - Connecting to a bus
  - Accessing a destination
  - Accessing topics
  - Creating a temporary destination
  - Accessing a foreign bus

Messaging Security and Role Based Security

- To enable messaging security
  - Global security must be on
  - Turn on security on Service Integration Bus, where needed
    - Administrative Console: Service Integration ➔ Buses ➔ <Your Bus> ➔ General Properties
- Once on, it applies to the entire bus and its resources
- Users/groups who connect to a bus must have permission to carry out any operations on the bus resources
  - Accomplished by assigning users/groups to the appropriate pre-defined role or roles
- Simple Role based Authorization scheme – similar to Java™ 2 Enterprise Edition (J2EE) Role based authorization
  - A role contains the authorization permission required to perform a given operation
  - Assign user/group to the Role - this grants the user/group all of the permissions that the role contains
  - User/group have to be defined in the appropriate Authentication User Registry (Local OS, LDAP or Custom Registry)

Pre-defined Roles for Messaging Security

Roles	Applicable Service Integration Bus Resources	Purpose
Connector	Bus, Foreign Bus	To connect to the bus
Sender	Foreign Bus, All Destination types	For message producer to connect to send messages or send a message from a Service Integration Bus to foreign bus
Receiver	All Destination types (except foreign Destination)	For message consumer to connect to receive message (destructive-read)
Browser	All Destination types (except Topic space and foreign Destination)	For message consumer to connect to receive message (non-destructive-read)
Creator	Queue Destination	To create temporary Destination from the queue destination
ContextKeeper	Foreign Bus, All Destination types and Topic Root	

- Two special groups (similar for J2EE Applications) can be used to assign to any of the pre-defined roles:
  - AllAuthenticated - contains all authenticated users
  - EveryOne - contains all users, authenticated or not

Service Integration Bus Resources and Applicable Roles

Destination type	Allowed Role Names for specific operations
Bus	Connector
Foreign Bus	Sender, ContextKeeper
Destination - queue	Sender, Receiver, Browser, Creator, ContextKeeper
Destination - port	Sender, Receiver, Browser, Creator, ContextKeeper
Destination - Web Service	Sender, Receiver, Browser, Creator, ContextKeeper
Destination - topicSpace	Sender, Receiver, ContextKeeper
Destination - foreignDestination	Sender, ContextKeeper
Destination - alias	Sender, Receiver, Browser, ContextKeeper
Topic “Root”	Sender, Receiver and ContextKeeper
Topic	Sender, Receiver

Additional Authorization Information

- Bus
  - If a user (from a local bus) wants to send a message to a destination in a foreign bus, the user must also be authorized to access the foreign bus (discussed later)
- Destinations
  - Can assign default permission on all local destinations at the Bus level. All Destinations inherit those permissions or the inheritance can be turned off
  - In the case of local destinations where the inheritance of defaults is allowed, the default permissions are added to local permissions specified on an individual destination
  - When a message is routed to multiple destinations using the Forward Routing Path, the user's authorization should be checked each time the message is forwarded on to its next destination
  - Reverse Routing Path does not require any authorization checks itself but might become the Forward Routing Path of a return message

Authorization: Topic Space and Topics

- Topics are contained in a topic space (a type of destination)
  - Can have more than one independent topic spaces within a bus
- Within a topic space, topics are organized into hierarchies based on the topic names
  - More than 1 topic hierarchy can exist within the topic space – all of them are joined at a virtual “root” (created when topic space is created)
  - Topic inherits roles from its parent, unless you explicitly block the inheritance
  - If required, you can disallow the role inheritance or define new roles for any topic in the hierarchy
- Topic does not need to exist, when you define roles for it

Configuring JMS Connections

- When a JMS client connects to a bus, the username and password must be correctly configured
  - Component managed – specified by the application
  - Connection Managed – specified in the connection factory used to create the connection to the bus
- Configuring JMS Connections is covered in the J2C Security presentation

Messaging Engine (ME) joining a secure Bus

- When Messaging security is enabled, only authorized messaging engines are allowed to join a bus
- How:
  - Set the Inter-engine authentication alias property to specify a user ID/password used for authentication of ME joining the bus
  - If Mediations are used, set the Mediations authentication alias property to specify a user ID and password for mediations that access the bus
  - If SSL is required, configure the SSL certificate stores to restrict who can make an SSL connection, and hence join the bus

Access Control for Multiple Buses

- Buses can exchange messages securely with each other (within the same cell or different cell) and with WebSphere MQ
- When a message is sent to a destination in a foreign bus, the access control check consists of two stages:
  1. When message is send, check is performed if the sender has permission to access the foreign bus
  2. When the message enters the foreign bus, a check is performed to ensure that the sender has the permission to access the destination of the foreign bus

Access Control for Multiple Buses - Process

- A proxy definition of the foreign destination itself or a definition of the foreign bus is defined in WebSphere and it contains security permission attributes
  - The permissions that are associated with a foreign destination are used to control access to the foreign bus when that destination is the target destination on the foreign bus.
    - This enables you to give users permission to send messages to some destinations on a foreign bus, but not others
- When the message enters the foreign bus, the sender's permissions to access the destination are checked
  - Check is based on the user ID that is stored in the message
  - If the user ID in messages entering or leaving the foreign bus is replaced by values specified by the Inbound user ID or Outbound user ID properties, the check is performed on the Inbound or Outbound user ID, not the original user ID
  - Checks on Inbound and Outbound user IDs also apply when messages are routed through multiple buses, and when messages are being sent to a WebSphere MQ network
- You specify Inbound and Outbound user IDs when you create a routing definition (virtual link) for the link to a foreign bus

REDO

Section

Specific wsadmin tasks to Manage Messaging Security on Service Integration Bus Resources

Authorization: Bus commands

- Valid Role: Connect

Administrative tasks	"wsadmin" Command
Add user[1] who to connect to Bus	addUserToBusConnectorRole -bus *busName* -user *userName*
Remove user[1] from connecting to Bus	removeUserFromBusConnectorRole -bus *busName* -user *userName*
List users[1] who can connect to Bus	listUsersInDefaultRoleRole -bus *busName* -role *roleName*

[1] Similar commands available for groups

Authorization on Bus: Default permissions for all Local Destinations

- Valid Role: Sender, Receiver, Browser, Creator, ContextKeeper

Administrative tasks	"wsadmin" Command
Add a default user[1] to all Local Destination	addUserToDefaultRoleRole -bus *busName* -role *roleName* -user *userName*
Remove a default user[1] from all Local Destination	removeUserFromDefaultRoleRole -bus *busName* -role *roleName* -user *userName*
List default users[1] on local destinations	listUsersInDefaultRoleRole -bus *busName* -role *roleName*

[1] Similar commands available for groups

Authorization: Destinations

Destination type	Allowed Role Names for specific operations
queue	Sender, Receiver, Browser, Creator, ContextKeeper
port	Sender, Receiver, Browser, Creator, ContextKeeper
webService	Sender, Receiver, Browser, Creator, ContextKeeper
topicSpace	Sender, Receiver, ContextKeeper
foreignDestination	Sender, ContextKeeper
alias	Sender, Receiver, Browser, ContextKeeper

- Can assign default permission on all local destinations at the Bus level. All Destinations inherit those permissions or the inheritance can be turned off
- In the case of local destinations, where the default inheritance is allowed, the default permissions are added to any specific permissions for an individual destination
- When a message is routed to multiple destinations using the Forward Routing Path, the user's authorization should be checked each time the message is forwarded on to its next destination
- Reverse Routing Path does not require any authorization checks itself but might become the Forward Routing Path of a return message

Authorization: Destinations commands

- Valid Roles: listed on previous page, based on the destination type

Administrative tasks	"wsadmin" Command
Add a user[1]	addUserToDestinationRole -type *destinationType* -bus *busName* -foreignBus *foreignBusName* -destination *destinationName* -role *roleName* -user *userName*
Remove a user[1]	removeUserFromDestinationRole -type *destinationType* -bus *busName* -foreignBus *foreignBusName* -destination *destinationName* -role *roleName* -user *userName*
List users[1]	listUsersInDestinationRole -type *destinationType* -bus *busName* -foreignBus *foreignBusName* -destination *destinationName* -role *roleName*
Set Default Inheritance on a Local Destination	setInheritDefaultsForDestination -type *destinationType* -bus *busName* -destination *destinationName* -inherit <true|false>
List Default Inheritance on a Local Destination	listInheritDefaultsForDestination -type *destinationType* -bus *busName* -destination *destinationName*

[1] Similar commands available for groups

Authorization: Temporary Destination

Required Role for specific operations	"wsadmin" Command
▪**Creator (on the permanent destination**): To create temporary destination ▪Appropriate **Sender, Receiver and/or Browser** roles on the permanent destination	Use the command shown on the previous page for Destination commands

- Temporary destinations are created at run-time
- Temporary destination has the same authorization permissions as the permanent prefix destination on which it is based
- Once created, temporary destinations are subject to the same authorization checks
- Names of temporary destinations include a user prefix, which can be up to 13 characters long, and are specified in the connection factory

Authorization: Foreign Bus commands

- Valid Roles: Sender and ContextKeeper

Administrative tasks	"wsadmin" Command
Add a user[1]	addUserToForeignBusRole -bus *busName* -foreignBus *foreignBusName* -role *roleName* -user *userName*
Remove a user[1]	removeUserFromForeignBusRole -bus *busName* -foreignBus *foreignBusName* -role *roleName* -user *userName*
List users[1]	listUsersInForeignBusRole -bus *busName* -foreignBus *foreignBusName* -role *roleName*

[1] Similar commands available for groups

Authorization for Top-level Topic "Root"

- Valid Roles: Sender, Receiver and ContextKeeper
- Applies to the top-level topic of the topic space, called Root
  - Does not apply to the topic space itself, since topic space is a destination, not a topic

Administrative tasks	"wsadmin" Command
Add a user[1]	addUserToTopicSpaceRootRole -bus *busName* -topicSpace *topicSpaceName* -role *roleName* -user *userName*
Remove a user[1]	removeUserFromTopicSpaceRootRole -bus *busName* -topicSpace *topicSpaceName* -role *roleName* -user *userName*
List users[1]	listUsersInTopicSpaceRootRole -bus *busName* -topicSpace *topicSpaceName* -role *roleName*

[1] Similar commands available for groups

Authorization for Topic Permission

- Valid Roles: Sender, Receiver
- Be default, topic inherits the parent topic's permissions and roles - any permission and roles defined at the topic level are added to the inherited permission and roles

Administrative tasks	"wsadmin" Command
Add user[1]	addUserToTopicRole -bus *busName* -topicSpace *topicSpaceName* –topic *topicName* -role *roleName* -user *userName*
Remove user[1]	removeUserFromTopicRole -bus *busName* -topicSpace *topicSpaceName* –topic *topicName* -role *roleName* -user *userName*
List users[1]	listUsersInTopicRole -bus *busName* -topicSpace *topicSpaceName* –topic *topicName* -role *roleName*
Set topic permission inheritance for Sender	setInheritSenderForTopic -bus *busName* -topicSpace *topicSpaceName* -topic *topicName* -inherit <true|false>
List topic permission inheritance for Sender	listInheritSenderForTopic -bus *busName* -topicSpace *topicSpaceName* -topic *topicName*
Set topic permission inheritance for Receiver	setInheritReceiverForTopic -bus *busName* -topicSpace *topicSpaceName* -topic *topicName* -inherit <true|false>
List topic permission inheritance for Receiver	listInheritResceiverForTopic -bus *busName* -topicSpace *topicSpaceName* -topic *topicName* -inherit <true|false>

[1] Similar commands available for groups

Global Authorization commands

Administrative tasks	Allowed Role Names for specific operations
List all destinations that have roles	listAllDestinationsWithRoles -bus *busname* -type *destinationType*
List all foreign buses with roles	listAllForeignBusesWithRoles -bus *busname*
List all topics within a topic space with roles	listAllTopicsWithRoles -bus *busname* -topicSpace *topicSpaceName*
List all the roles that a user[1] belongs	listAllRolesForUser -bus *busname* -user *userName*
Remove a user[1] from all the roles and then delete this user	removeUserFromAllRoles -bus *busname* -user *userName*
Remove all authorization data for the defaults	removeDefaultRoles -bus *busname*
Remove all authorization data for a destination	removeDestinationRoles -type *destinationType* -bus *busname* -foreignBus *foreignBusName* -destination *destinationName*
Remove all authorization data for a foreign destination	removeForeignBusRoles -bus *busname* -foreignBus *foreignBusName*

[1] Similar commands available for groups

Section

Problem Determination

Security Event logging

- Following events are logged in the System log file:
  - An audit record is written for authentication success
  - An error record is written for authentication failure
  - An audit record is written for authorization failure
- No record is written for an authorization success

Section

Summary and Reference

Summary

- Explained different resource authentication mechanisms for the Service Integration Bus resources
- Showed Wsadmin commands to provide the authorization information for the Bus resource

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