



IBM Software Group

IBM® WebSphere® Application Server V7 Feature Pack for Service Component Architecture

Quality of service - Overview



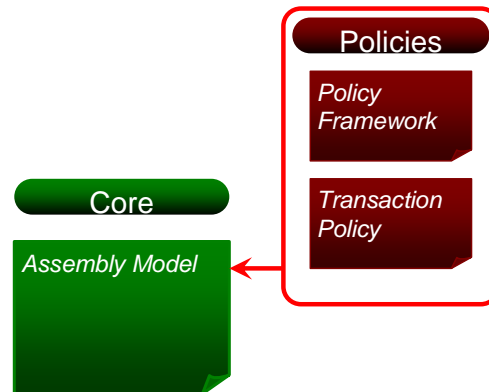
@business on demand.

© 2008 IBM Corporation
Updated December 10, 2008

This presentation provides an overview of Quality of service for the SCA feature pack.

Overview: Quality of service

- Quality of service is covered by two SCA V1.0 specifications:
 - SCA Policy Framework
 - SCA Transactions Policy



SCA provides an enhanced Quality of Service through integration with WebSphere security management, transaction management and Web services policy management. Quality of service is addressed by two of the SCA v1.0 specifications; SCA Policy framework and SCA Transactions policy. SCA policy framework supports specification of constraints, capabilities, and QoS expectations from component design through to concrete deployment by allowing policies and policy subjects specified using WS-Policy and WS-PolicyAttachment to be associated with SCA components.

SCA policy framework

- A framework for specifying Qualities of Service
 - ▶ Constraints
 - ▶ Capabilities
 - ▶ Expectations
- Based on existing standards
 - ▶ WS-Policy
 - ▶ WS-PolicyAttachment
- Intents, Policies and PolicySets.



The capture and expression of non-functional requirements such as security is an important aspect of service definition, and has impact on SCA throughout the life cycle of components and compositions. SCA provides the [Policy Framework](#) to support specification of constraints, capabilities, and quality of service expectations, from component design through to concrete deployment. This specification describes the framework and its use. It also covers intents, policies, and policySets.

SCA transaction policy

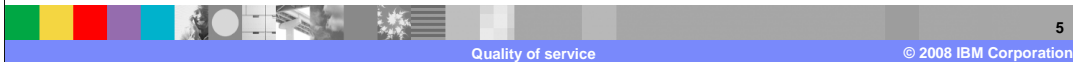
- A framework for specifying Qualities of Service in the area of transactions
- The SCA transaction policies are specified as intents which represent the transaction quality of service behavior offered by specific component implementations or bindings
- Transaction policy can be specified either in the SCDL or annotatively



This specification defines implementation and interaction policies that relate to transactional QoS in components and their interactions. The SCA transaction policies are specified as intents which represent the transaction quality of service behavior offered by specific component implementations or bindings. The specification describes the set of abstract policy intents – both implementation intents and interaction intents – that can be used to describe the requirements on a concrete service component and binding. SCA transaction policy can be specified either in the SCDL or annotatively in the implementation code.

Terminology

- XML namespace
 - ▶ <http://www.oxa.org/xmlns/sca/1.0>
 - ▶ Assumed to be the default namespace
- **Policy**
 - ▶ Constraint that can be applied to service components
- **PolicySets**
 - ▶ contain concrete policies that may be applied to SCA binding and implementations.
- **Intents**
 - ▶ represent abstract assertions about a specific Quality of Service (QoS)



The XML namespace is assumed to be the default namespace. The term **Policy** is used to describe some capability or constraint that can be applied to service components or to the interactions between service components represented by services and references. An example of a policy is that messages exchanged between a service client and a service provider be encrypted, so that the exchange is confidential and cannot be read by someone who intercepts the conversation. PolicySets hold policies that may be applied to SCA binding and implementations. Intents are abstract assertions that describe requirements of Components, Services and References.

Intents

- An intent is an abstract assertion about a specific Quality of Service (QoS)
- Intents describe the requirements of components, services and references
- Intents provide a means to state requirements in a high-level abstract form
- A service intent should have a matching policy set during deployment



SCA **intents** are used to describe the abstract policy requirements of a component or the requirements of interactions between components represented by services and references. Intents provide a means to state these requirements in a high-level abstract form, independent of the detailed configuration of the runtime and bindings which is the role of the application deployer. If a service is marked with an intent, then the deployer should use a policy set that covers that intent. For example, a deployer should use a policy set that provides for the encryption of the messages for a service marked with “confidentiality” intent.

SCA security intents

- **Authentication**
 - ▶ Indicates that a client must authenticate itself in order to use an SCA service
- **Confidentiality**
 - ▶ Indicates that the contents of a message are accessible only to those authorized to have access
- **Integrity**
 - ▶ Indicates that assurance is required that the contents of a message have not been tampered with and altered between sender and receiver



The SCA security specification defines these intents:

authentication – is used to indicate that a client must authenticate itself in order to use an SCA service.

confidentiality – is used to indicate that the contents of a message are accessible only to those authorized to have access (typically the service client and the service provider).

integrity – is used to indicate that assurance is required that the contents of a message have not been tampered with and altered between sender and receiver.

Qualifiers

- The security intents can be qualified

- ▶ Transport

- specifies that the qualified intent should be realized at the transport layer

- ▶ Message

- specifies that the qualified intent should be realized at the message level

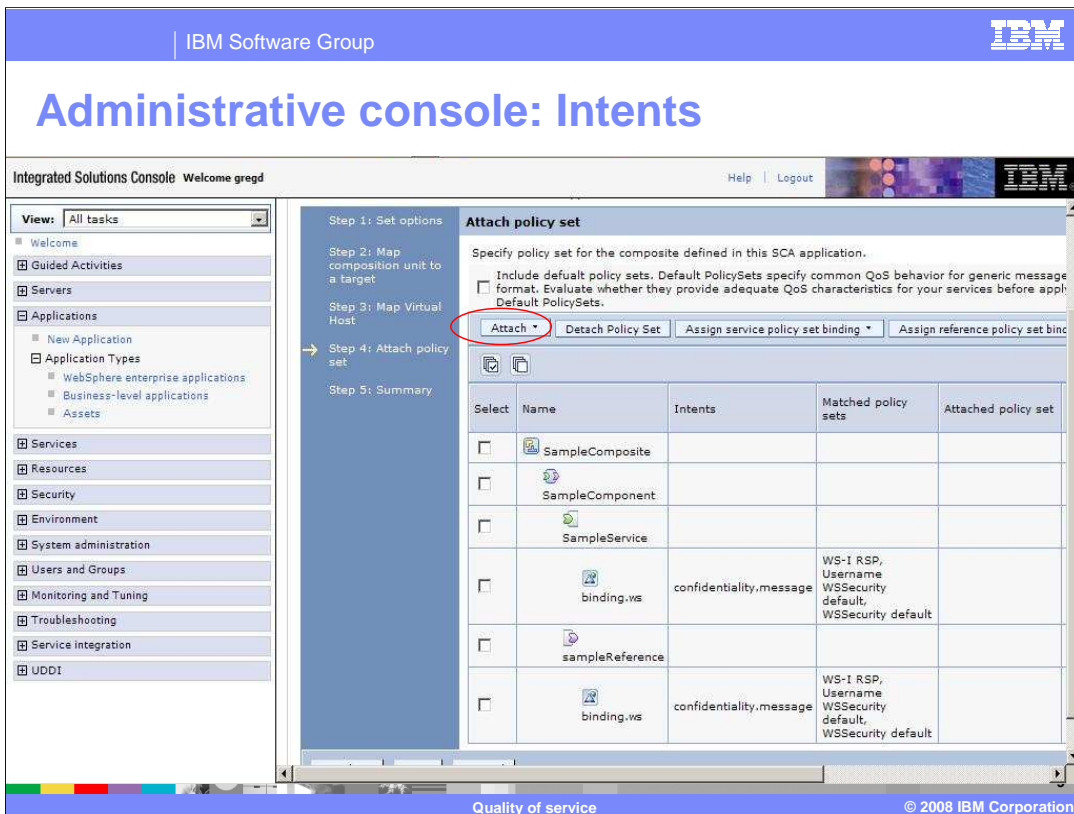
- ▶ Example snippet using the message qualifier

```
<reference name="sampleReference">  
  <binding.ws requires="confidentiality.message"/>  
</reference>
```



Any one of the three security intents mentioned in the previous slide can be further qualified to specify more specific business requirements. Two qualifiers are defined by the SCA security specification: **transport** and **message**, which can be applied to any of the above three intents. The **transport** qualifier specifies the qualified intent should be realized at the transport layer of the communication protocol. The **Message** qualifier specifies that the qualified intent should be realized at the message level of the communication protocol.

See the sample snippet provided, which is using the message qualifier applied to confidentiality intent.



Intents can be specified from the administrative console services menu. Intents tell the deployer which policy sets can be attached to satisfy the QOS requirement. The deployer must use the 'Attach' button on the panel to attach a policy set.

This panel opens during the addition of composition unit (CU) to a business level application if the composite involved uses the Web service binding and has policy intents.

Reliable messaging intents

Intent	binding.ws	binding.ejb binding.sca
atLeastOnce atMostOnce exactlyOnce	Requires the attachment of a Web services policy set that contains the WSReliableMessaging policy type	Not supported



Reliable messaging intents include atLeastOnce, atMostOnce and exactlyOne. These intents require the attachment of a Web services policy set that contains the WSReliableMessaging policy type, therefore they are not supported for SCA and EJB binding.

Summary

- The feature pack provides a framework to describe abstract policy requirements through "intents" and apply particular capability or constraints on services and references through PolicySets
- The SCA policy framework allows developers and designers of a service to specify the constraints at a broader level using SCA intents, leaving the choice of concrete policy to the assembler, deployer or administrator



The feature pack provides a framework to describe abstract policy requirements through "intents" and to apply particular capabilities or constraints on services and references through PolicySets. The SCA policy framework allows developers and designers of a service to specify the constraints at a broader level using SCA intents, leaving the choice of concrete policy to the assembler, deployer or administrator. This empowers the assembler to provide a combination of services that can behave differently based on operating environment and need, without changing the underlying business logic, keeping with the SCA concepts. The following Appendix contains lists of supported intents.

Section

Appendix

Intents supported by each binding

Intent	binding.ws	binding.ejb binding.sca
authentication.message	Requires the attachment of a WebSphere policy set and policy binding that contains the WS-Security policy type	Not supported; CSiv2 can be configured to use basic auth and security token (LTPA, Kerberos)
confidentiality.message integrity.message	Requires the attachment of a WebSphere policy set and policy binding that contains the Security policy type	Not supported

Intents supported by each binding.

Intents supported by each binding

Intent	binding.ws	binding.ejb binding.sca
authentication.transport	Basic auth only. Reference requires the attachment of a WebSphere policy set that contains the HTTPTransport policy type. Service does not require any attachments.	Intent is not supported. CSiv2 can be configured to use client certificates for authentication.
confidentiality.transport integrity.transport	Requires the attachment of a WebSphere policy set that contains the SSLTransport policy type	Intent is not supported. CSiv2 can be configured to require SSL.

Intents supported by each binding

Intent	binding.ws	binding.ejb binding.sca
propagatesTransaction	Requires the attachment of a Web services policy set that contains the WS-Transaction policy type	Supported; no configuration required

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv7SCA_QOS_overview.ppt

This module is also available in PDF format at: [../WASv7SCA_QOS_overview.pdf](..WASv7SCA_QOS_overview.pdf)



You can help improve the quality of IBM Education Assistant content by providing feedback on this module.

Trademarks, copyrights, and disclaimers

IBM, the IBM logo, ibm.com, and the following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

WebSphere

If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of other IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>

Other company, product, or 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 or changes in the products or programs 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.

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 NON-INFRINGEMENT. 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 (for example, 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.

© Copyright International Business Machines Corporation 2008. All rights reserved.

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.

