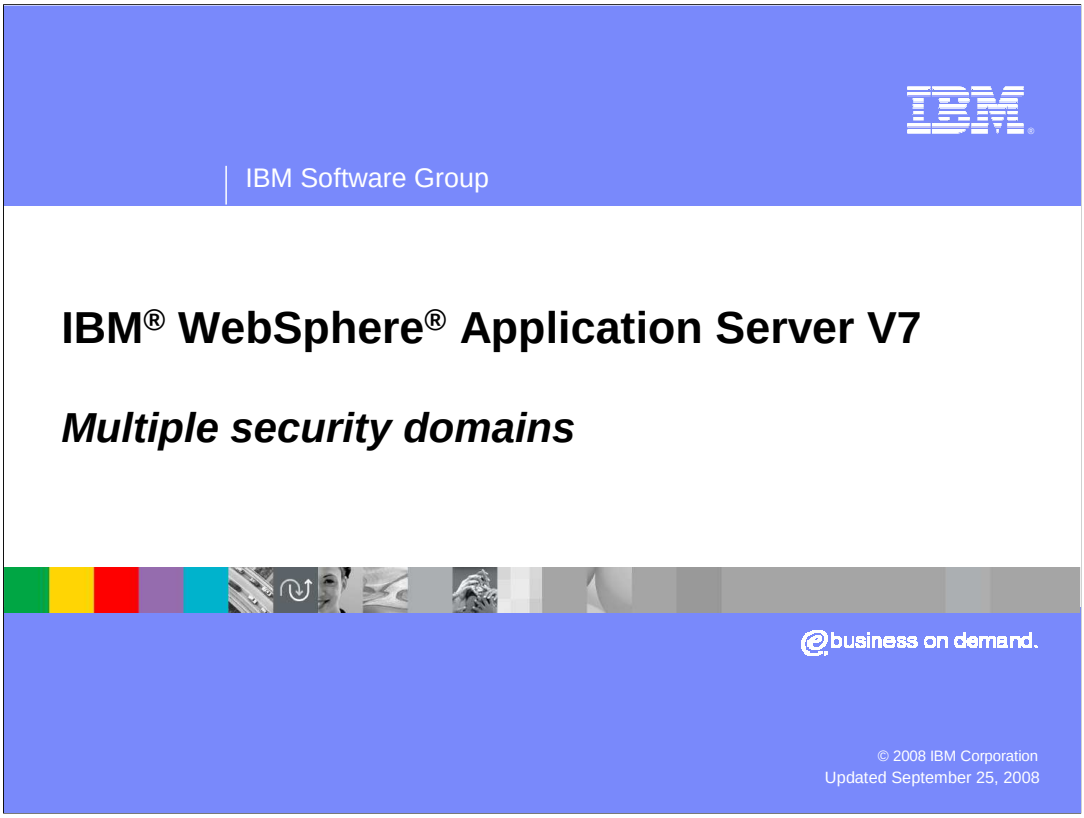


This presentation covers the new multiple security domains feature in WebSphere Application Server version 7.

Agenda

- Multiple security domains support
- Administration of multiple security domains

First, an explanation of a new feature that allows multiple security domains with a WebSphere Application Server cell is provided, followed by a discussion of how to configure this new feature using the administrative console.

Section

Multiple security domains

This section explains the new multiple security domains capabilities in WebSphere Application Server V7.

Security domains

- In previous releases most security attributes can be configured only at the cell level
  - Configurations, like user registries, have to be common for all applications
  - Data is stored at a cell level in security.xml
- Individual servers can override only a few specific configurations

In the past there was traditionally a cell-wide security domain. Most security configurations must be common for all applications within a cell and the configuration data has been stored within the security.xml at the cell level. Individual servers within a cell have only been able to override certain specific data.

Multiple security domains

- Multiple security configurations are designed to be more flexible
  - Allow different security settings in the same cell
- Separate security configurations for administrative applications and user applications
- More flexibility for security providers
  - Previous releases only allowed plug-in points at the cell level
- Provide cross realm communication

WebSphere Application Server V7.0 provides the ability to configure multiple security domain configurations that can be used with the same cell. This allows for greater flexibility in configuring and applying security settings within a cell environment. It can also be used to configure separate security configurations for administrative applications versus end user applications. Multiple security domains also provides greater flexibility for third party security providers, allowing more configurable plug-in points. Multiple security domains can also be used to configure for cross realm communication.

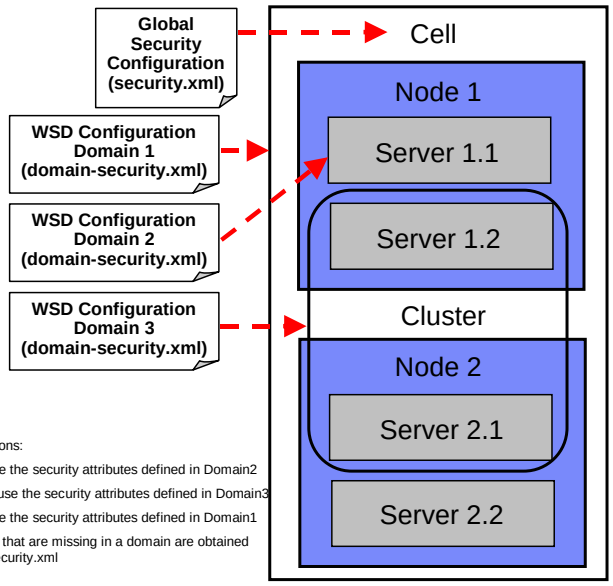
WebSphere security domains

- WebSphere Application Server V7 is designed to provide support for multiple security domains using WebSphere security domains
  - Can be scoped to specific cells, servers, clusters or service integration buses in an environment
- Configuration data stored in domains overrides the data from the global security configuration
  - The global security configuration is the security configuration used by the administrative applications, also represents the default configuration for user applications
- Administrative applications continue to use the data from global security

WebSphere security domains are now more flexible and can be scoped to specific cells, servers, clusters, or service integration buses in an environment. Security configuration data stored with these domains will override the data from the global security configuration stored at the cell level. The global security configuration is still used by administrative applications, and is the default configuration used by user applications.

WebSphere security domains: configuration

- **Global security**
  - User registry
  - Trust Association Interceptor (TAI)
  - SPNEGO
  - Authorization
  - Login configurations
  - Application security enablement
  - Java 2 security
  - RMI/IIOP (CSIv2 protocol)
  - Custom Properties
  - Authentication mechanisms
  - SSL
  - Web attributes (SSO)
  - Audit
- **Server security**
  - User registry
  - Trust Association Interceptor (TAI)
  - SPNEGO
  - Authorization
  - Login configurations
  - Application security enablement
  - Java 2 security
  - RMI/IIOP (CSIv2 protocol)
  - Custom Properties
  - LTPA Timeout



User applications:

in S1.1 will use the security attributes defined in Domain2

in cluster will use the security attributes defined in Domain3

in S2.2 will use the security attributes defined in Domain1

Any attributes that are missing in a domain are obtained from global security.xml

Various security configuration data and where that data can be applied is shown in this picture. Most of the same types of data can also be configured at the server level, including user registries, trust association interceptors, and authorization information. Some configurations such as SSL and security audit data are still configured at the cell level and store in global security. The diagram on the right shows an example cell, that contains four separate security configurations. User applications in server 1.1 will use the security attributes defined in Domain 2. User applications in the cluster will use the security attributes defined in Domain 3. User applications in server 2.2 will use the security attributes defined in Domain1 which has been applied at the cell level. Any security attributes that are missing in these domains are obtained from the global security configuration. Administrative applications will use the global security configuration.

Section

Administration

This section explains the administration of multiple security domains in WebSphere Application Server V7.

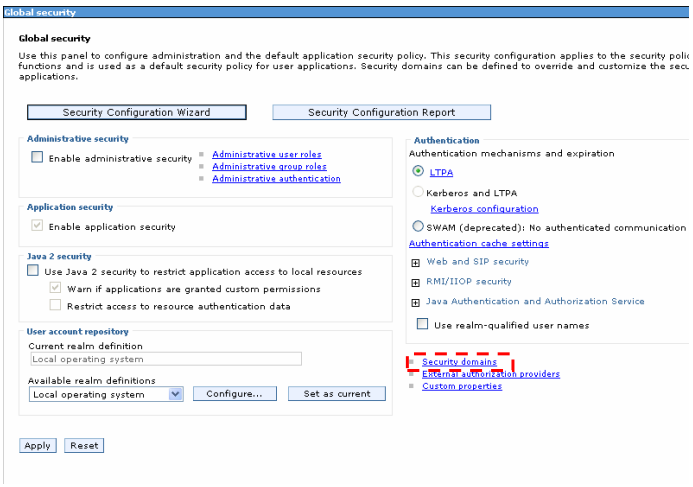
Security tasks

- Global security task has added links to support multiple security domains
- Security domains task allows users to manage and configure the domains in their environment

Under the security tab in the administrative console, the security domains task is now shown. The global security task is still available and provides links to configure multiple security domains.

Global security

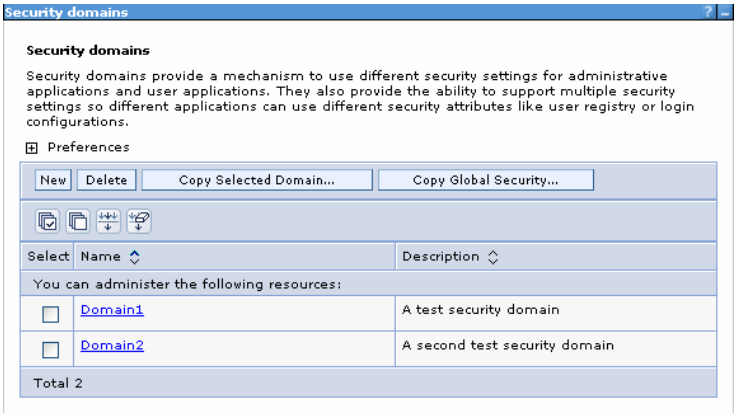
- Provides a new link to the security domains panel



The global security panel is similar to past releases, still providing a security configuration wizard and the security configuration report. In the lower right side a link has been added to configure security domains.

Security domains

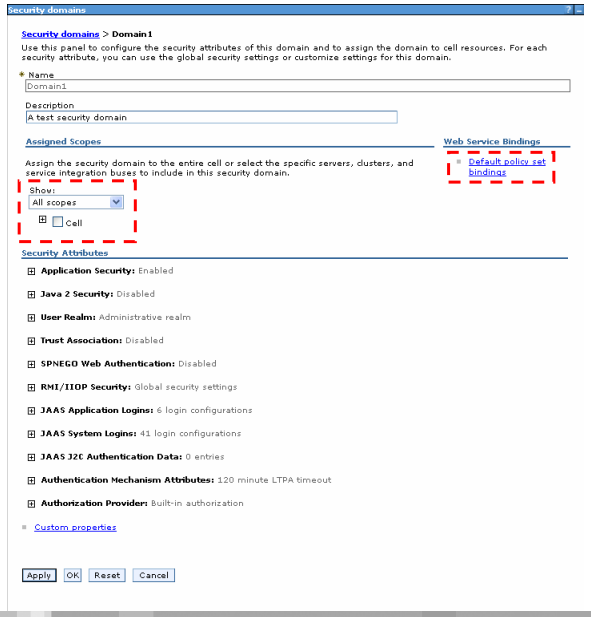
- Lists the configured security domains
- Create and manage security domains



You can list out the various security domains configurations that have been created. You can manage the security domains by creating new domains, deleting existing domains, or copying domains.

Security domain attributes

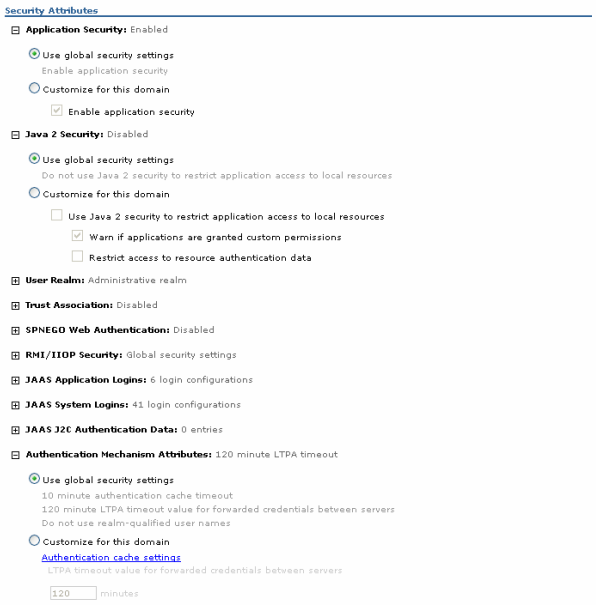
- Configure the scope for a security domain
  - Entire cell
  - Specific servers, clusters or service integration buses



A security domain is associated with a scope, which can be the entire cell or a specific server, cluster, or service integration bus.

Security attributes

- Attribute sections can be expanded to show the security settings used by the domain
- Attributes can be customized and saved

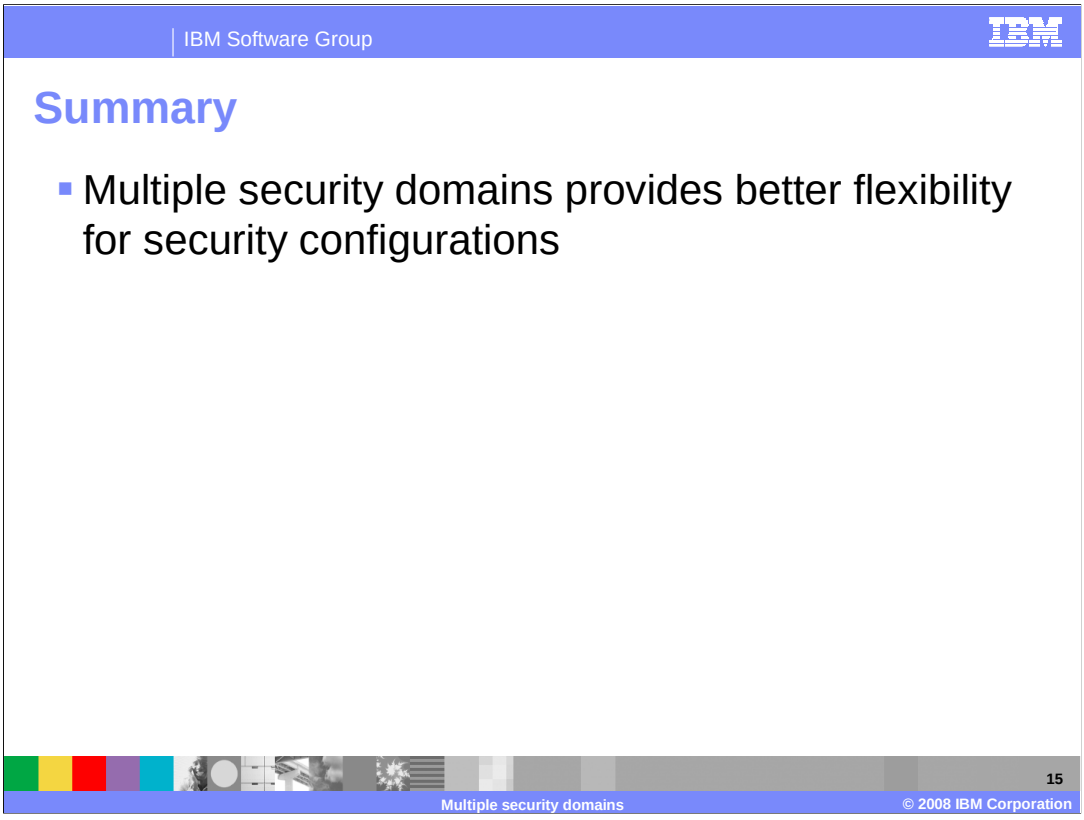


There are multiple security attributes for each security domain, including application security, Java 2 security or authentication mechanism attributes. These attribute sections can be expanded to show the various configuration options available. These can then be customized and saved based on the needs of the security domain.

Restrictions in WSD

- Federated repositories
  - Can be only one configuration or instance of a federated repository in a cell
  - Multiple security domains can use federated repositories but need to share the same instance
- Tivoli Access Manager
  - There can be only one Tivoli Access Manager or Java Authorization Contract for Containers configured at the global level
  - Cannot be configured at the domain level

In WebSphere Application Server version 7 there are some restrictions associated with security domains. Federated repositories can only have a single configuration within a cell. Multiple security domains within a cell can use federated repositories, but they must be configured to all use the same repository. Tivoli Access Manager has a similar restriction, in that there can be only a single configuration, which can only be configured at the global security level.



In summary, WebSphere Application Server version 7 has introduced several new features for security. Multiple security domains offer a more flexible means of configuring security.

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_WASv7_MultipleSecurityDomains.ppt

This module is also available in PDF format at: ../WASv7_MultipleSecurityDomains.pdf

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

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 WebSphere

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

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.

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 (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.

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.