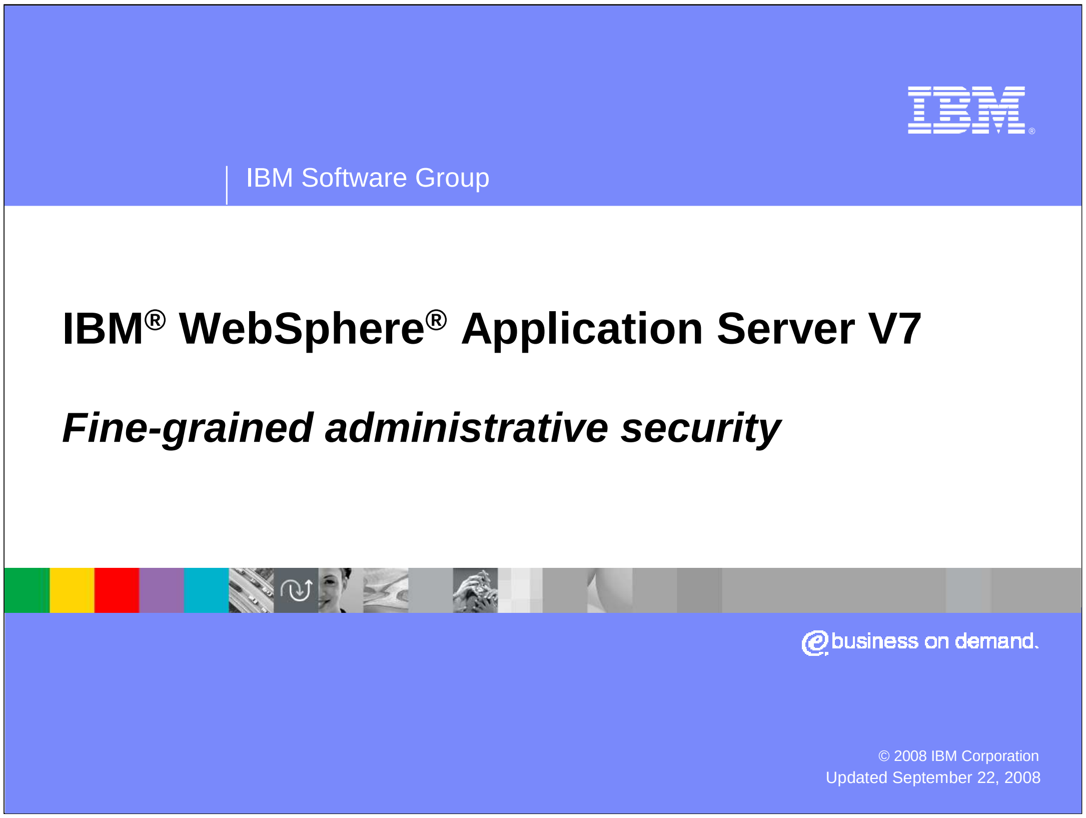


IBM Software Group

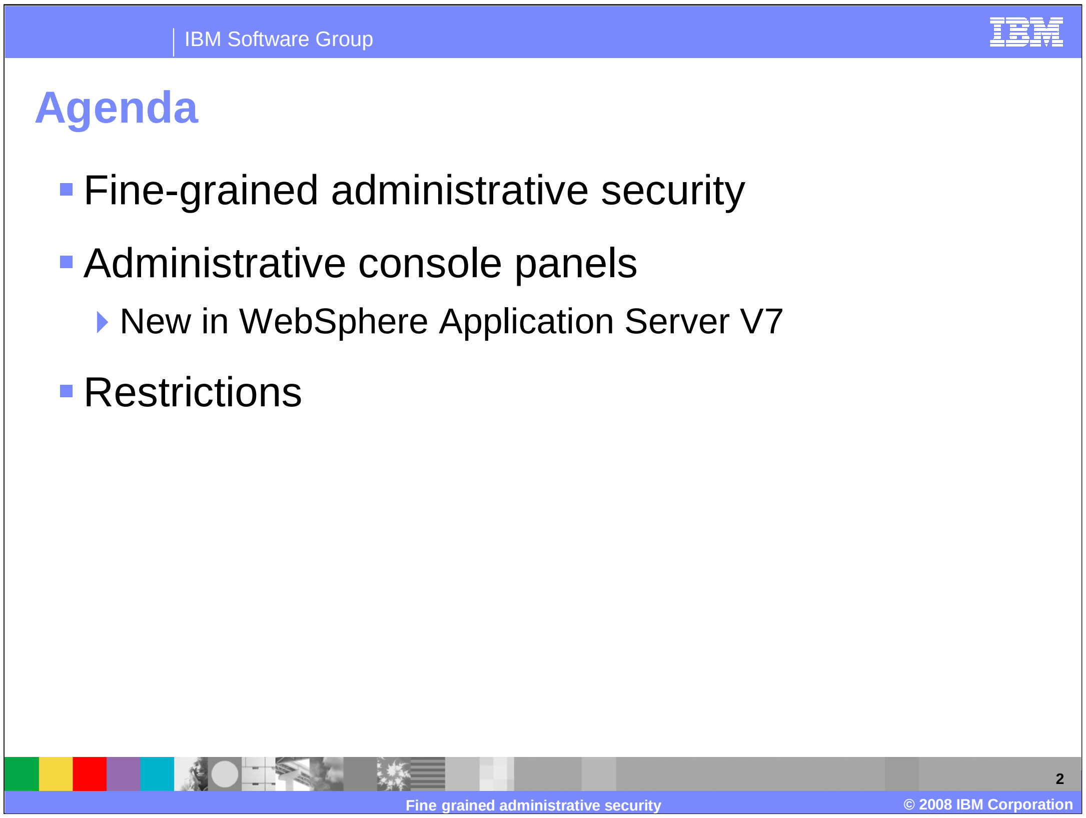
IBM® WebSphere® Application Server V7

Fine-grained administrative security

e business on demand.

Updated September 22, 2008

This presentation covers WebSphere Application Server version 7 fine-grained administrative security.



Agenda

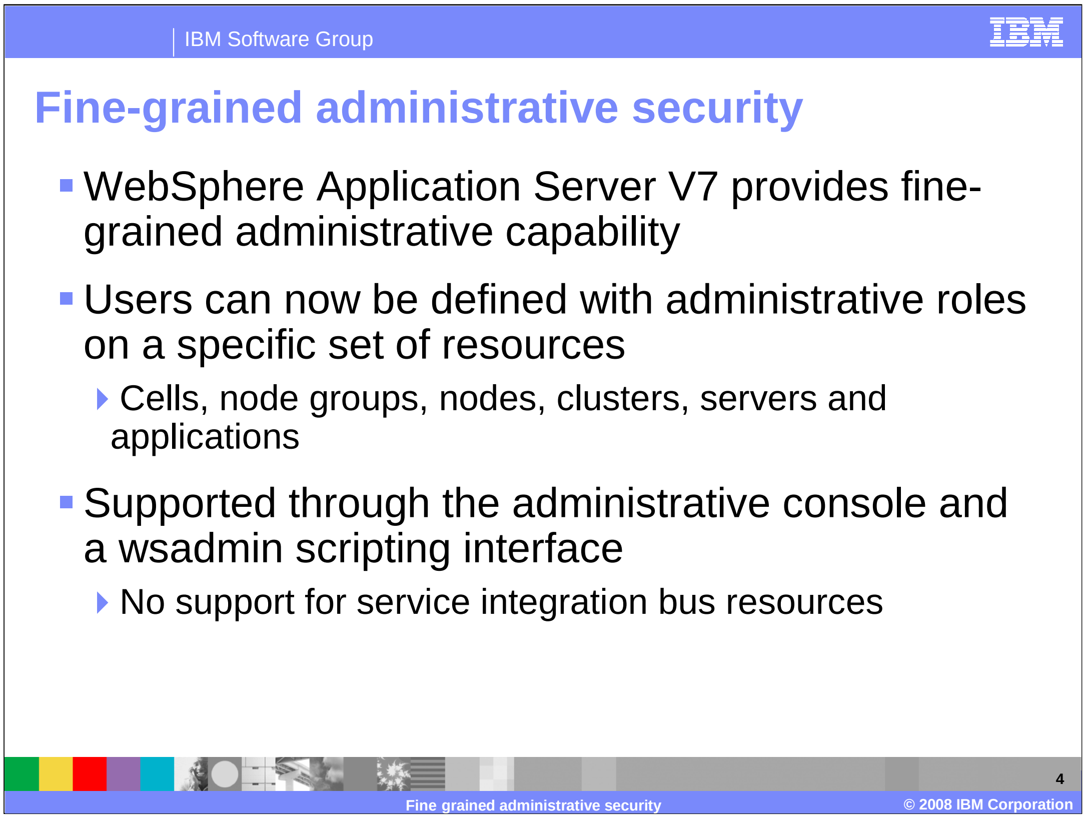
- Fine-grained administrative security
- Administrative console panels
  - New in WebSphere Application Server V7
- Restrictions

First, an overview of the fine-grained administrative security feature is provided, followed by a discussion of some updates that have been made to this feature in version 7, in particular the new ability to configure this feature from the administrative console. Finally, some specific limitations for this feature are identified.

Section

Fine-grained security overview

This section provides an overview of fine-grained security, which was first introduced in WebSphere Application Server version 6.1.



IBM Software Group

Fine-grained administrative security

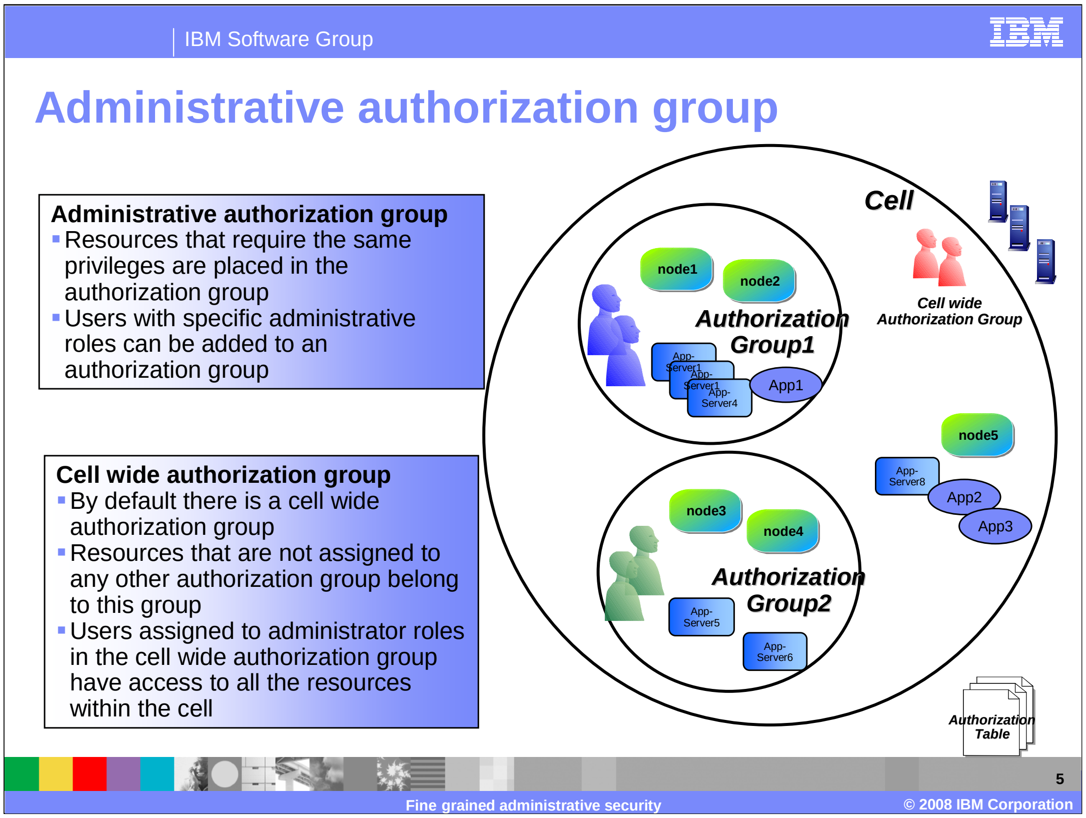
- WebSphere Application Server V7 provides fine-grained administrative capability
- Users can now be defined with administrative roles on a specific set of resources
  - Cells, node groups, nodes, clusters, servers and applications
- Supported through the administrative console and a wsadmin scripting interface
  - No support for service integration bus resources

4

Fine grained administrative security

© 2008 IBM Corporation

In WebSphere Application Server version 7, administrative security is more fine-grained, allowing more specific configuration options. The administrative roles are now scoped to resource instances instead of the entire cell. Access can be granted to each user per resource instance. For example a user can only be granted configurator access to specific application, an application server or a node. That user cannot access any other resources outside assigned resources. In this release fine-grained security can be configured through the administrative console or using with wsadmin scripts. There is no support offered to use fine-grained security with service integration bus resources.



Administrative authorization group

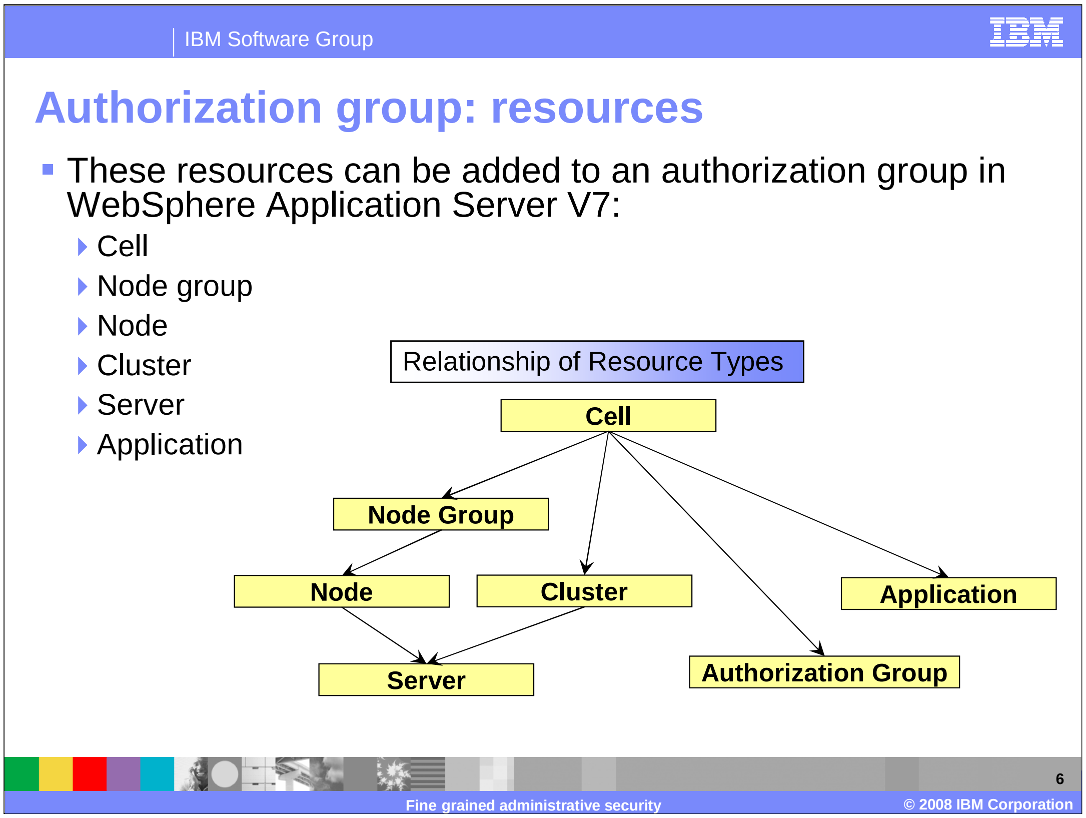
Administrative authorization group

- Resources that require the same privileges are placed in the authorization group
- Users with specific administrative roles can be added to an authorization group

Cell wide authorization group

- By default there is a cell wide authorization group
- Resources that are not assigned to any other authorization group belong to this group
- Users assigned to administrator roles in the cell wide authorization group have access to all the resources within the cell

To configure fine-grained security, the resources that require similar privileges are placed in a group called administrative authorization group or authorization group. Users can then be granted access to an authorization group with the required administrative role. For compatibility with earlier versions, by default there is a cell-wide authorization group, and users assigned to administrative roles in the cell wide authorization group can access all the resources within the cell. In the diagram shown, users in authorization group 1 have access to nodes 1 and 2. Users in authorization group 2 have access rights to nodes 3 and 4, while users in the cell-wide group have access to all the resources in the cell. The configuration data for fine-grained authorization is stored in authorization tables.



IBM Software Group

Authorization group: resources

- These resources can be added to an authorization group in WebSphere Application Server V7:
  - Cell
  - Node group
  - Node
  - Cluster
  - Server
  - Application

Relationship of Resource Types

Cell

Node Group

Node

Cluster

Application

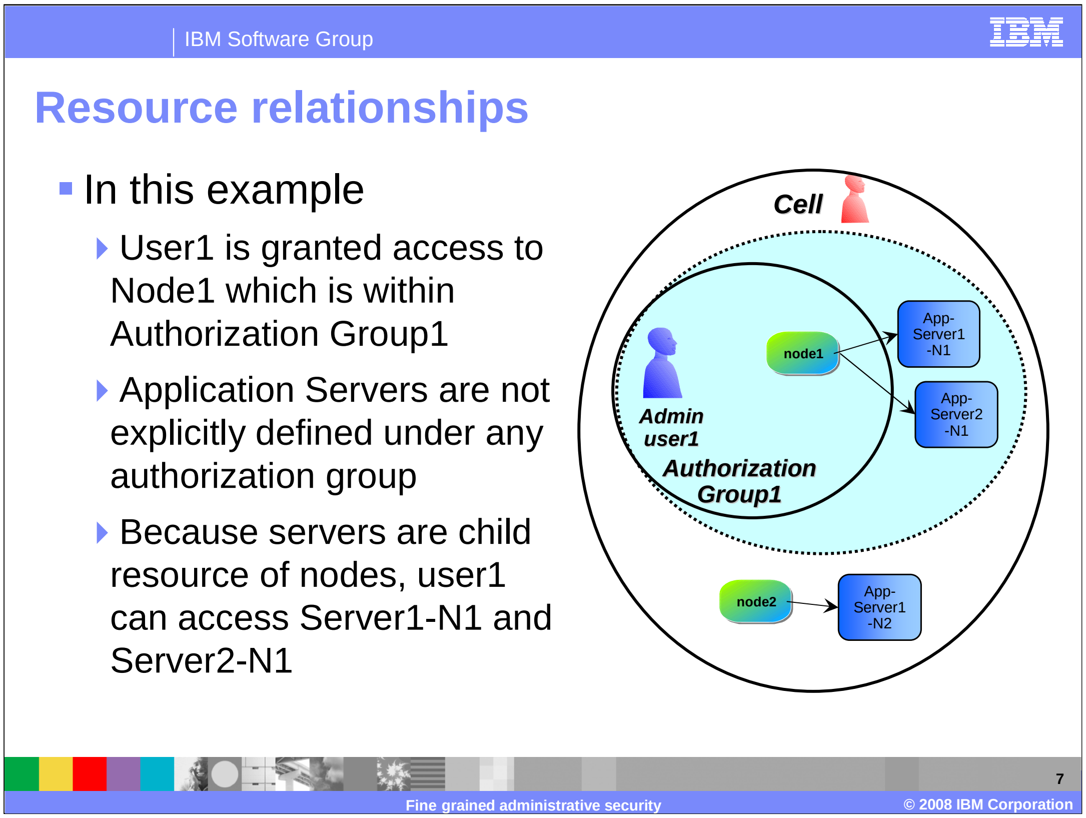
Server

Authorization Group

6

Fine grained administrative security

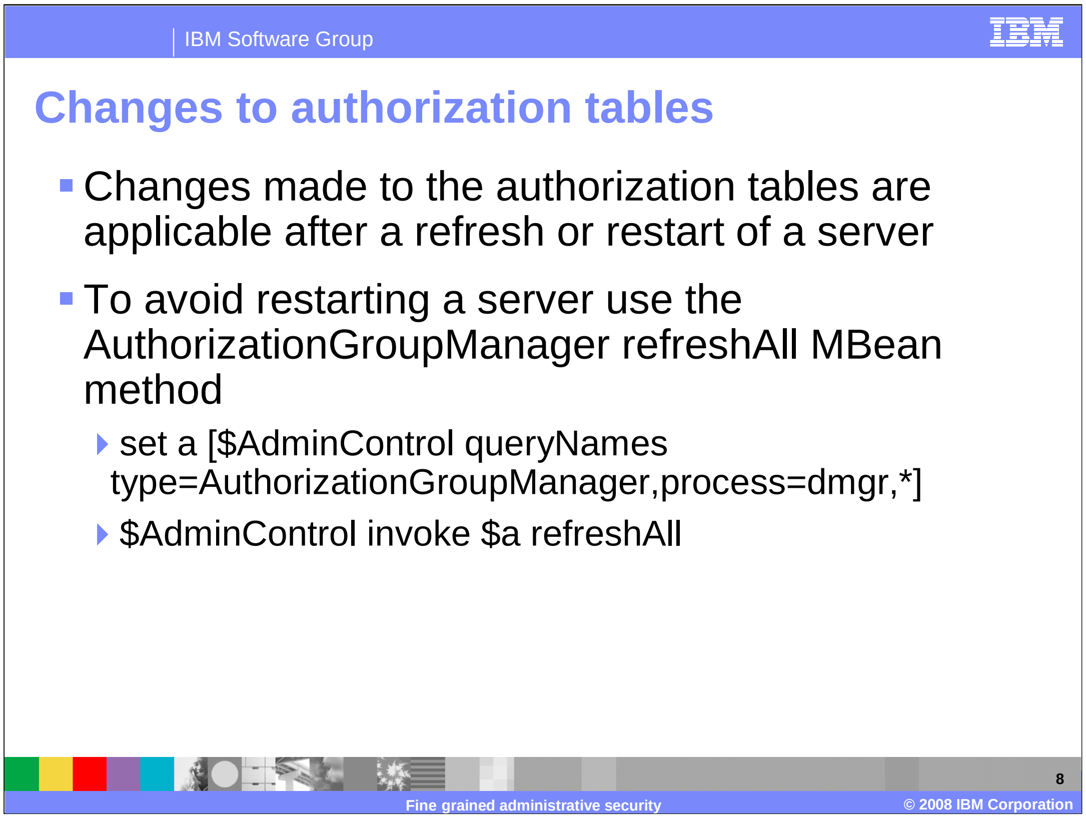
Various resources can be added to an authorization group, there is an associated inheritance scheme that makes configuration easier. For instance a user granted access to a node, also gains access to all the servers on that node. As a cell grows it may not be practical to add all the servers in a node to an authorization group. To solve this problem, just place the node in the authorization group and all the servers in that node are considered a child resource of that node. It is assumed that the server is implicitly present in the same authorization group as that of its node. Applications are kept separate in the inheritance scheme from the servers they may be installed on, this prevents users from accidentally getting access to applications.



Resource relationships

- In this example
  - User1 is granted access to Node1 which is within Authorization Group1
  - Application Servers are not explicitly defined under any authorization group
  - Because servers are child resource of nodes, user1 can access Server1-N1 and Server2-N1

This resource example helps show how the inheritance affects authorization groups. User1 is granted access to authorization group 1 in this example. Authorization group 1 has access to node 1. Even though no application servers are explicitly part of the authorization group, user 1 will also have access to application server 1 and 2 that are included on that node.

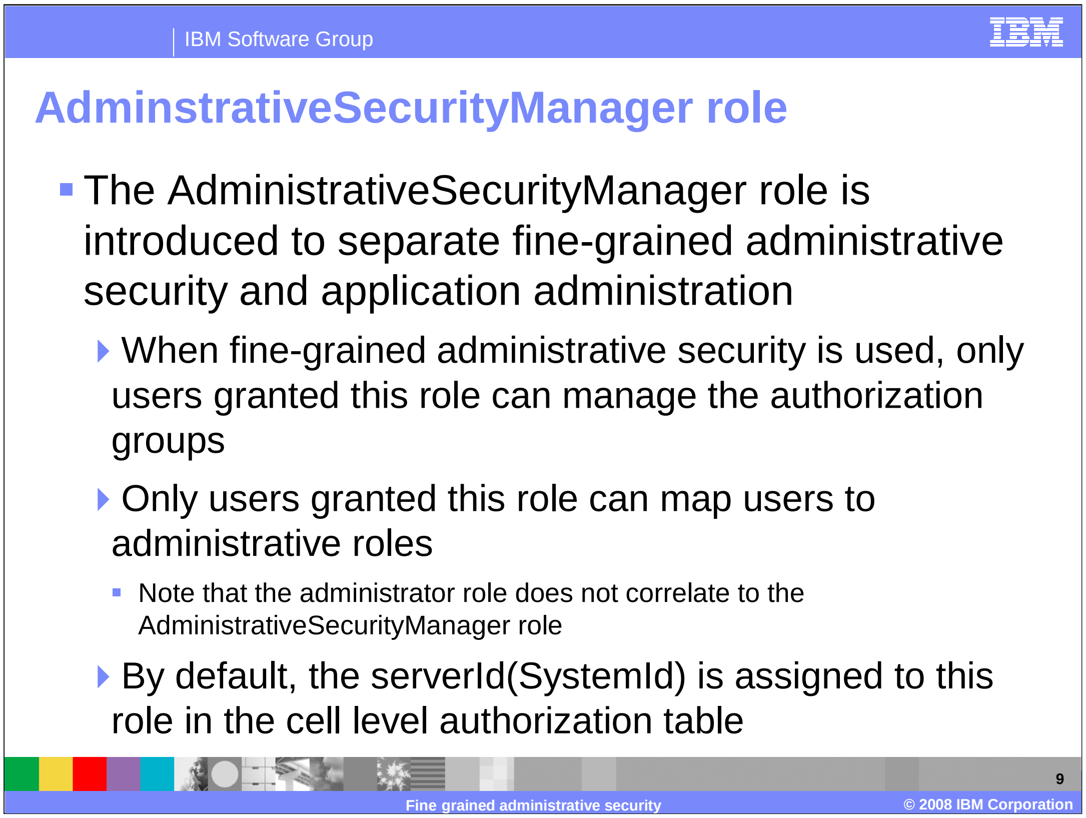


Changes to authorization tables

- Changes made to the authorization tables are applicable after a refresh or restart of a server
- To avoid restarting a server use the AuthorizationGroupManager refreshAll MBean method

```
set a [$AdminControl queryNames type=AuthorizationGroupManager,process=dmgr,*]
$AdminControl invoke $a refreshAll
```

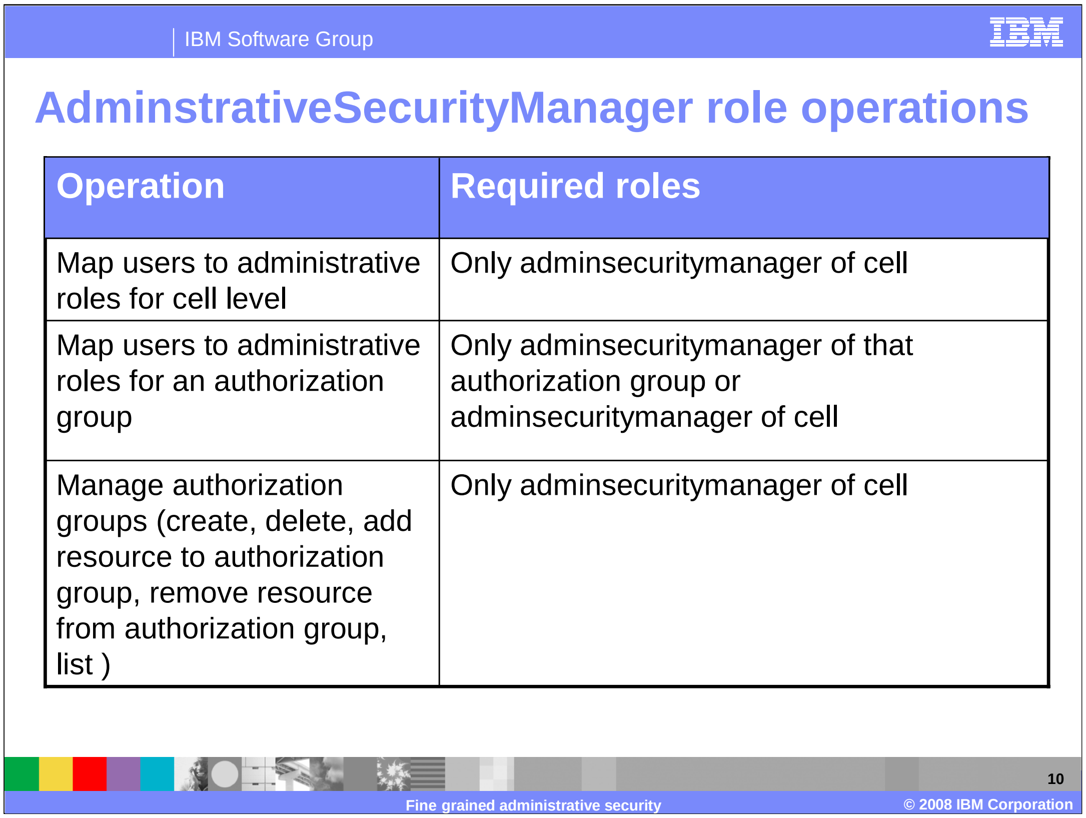
Changes made to the authorization tables are applicable after a refresh or restart of a server. This means normally after updating the fine-grained security configuration it is necessary to restart the server. To avoid restarting a server, the MBean for the authorization group manager can be refreshed. Use the AuthorizationGroupManager refreshAll MBean method as shown in the example.



AdminstrativeSecurityManager role

- The AdministrativeSecurityManager role is introduced to separate fine-grained administrative security and application administration
  - When fine-grained administrative security is used, only users granted this role can manage the authorization groups
  - Only users granted this role can map users to administrative roles
    - Note that the administrator role does not correlate to the AdministrativeSecurityManager role
  - By default, the serverId(SystemId) is assigned to this role in the cell level authorization table

The AdministrativeSecurityManager role is used to separate fine-grained administrative security and application administration capabilities. This allows the administrator of fine-grained security to be kept separate from standard administrators for the WebSphere Application Server environment. When fine-grained administrative security is used, only users granted this role can manage the authorization groups. By default, the serverId, also called the SystemId, is assigned to this role in the cell level authorization table.



IBM Software Group

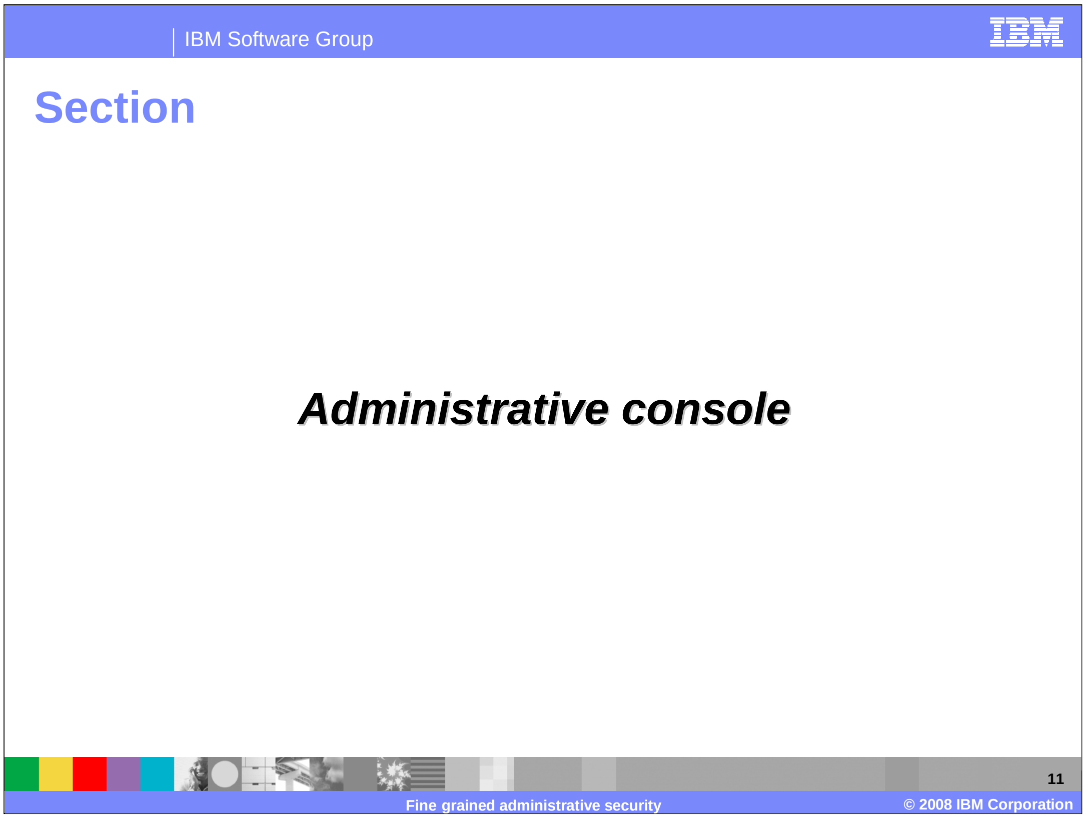
AdminstrativeSecurityManager role operations

Operation	Required roles
Map users to administrative roles for cell level	Only adminsecuritymanager of cell
Map users to administrative roles for an authorization group	Only adminsecuritymanager of that authorization group or adminsecuritymanager of cell
Manage authorization groups (create, delete, add resource to authorization group, remove resource from authorization group, list)	Only adminsecuritymanager of cell

10

Fine grained administrative security

This table shows the operations that can be performed by a user with the administrative security manager role. This role can map users to administrative roles, map administrative roles to specific authorization groups, and manage the authorization groups. These tasks make up the configuration tasks needed to create and manage fine-grained security.

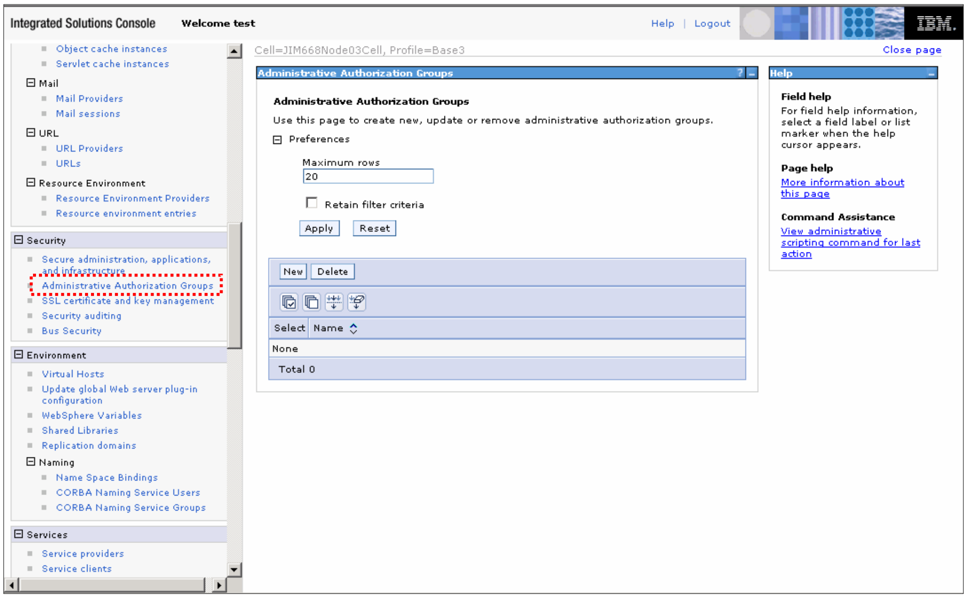


Section

Administrative console

This section covers administrative console updates for fine-grained security available in version 7.

Administrative console



Cell=JIM668Node03Cell, Profile=Base3

Administrative Authorization Groups

Administrative Authorization Groups

Use this page to create new, update or remove administrative authorization groups.

⊟ Preferences

Maximum rows: 20

□ Retain filter criteria

Select	Name
None	
Total 0	

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

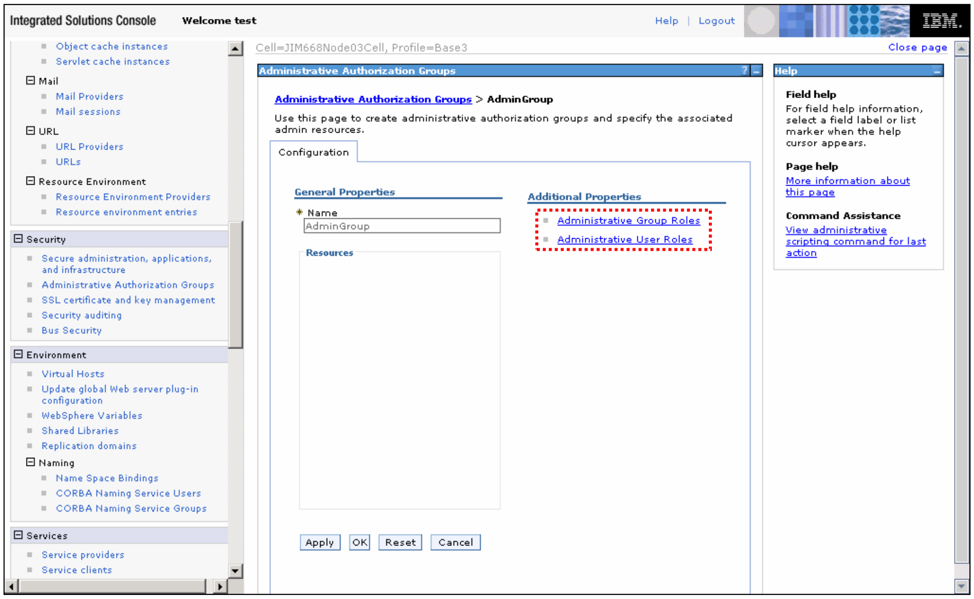
More information about this page

Command Assistance

View administrative scripting command for last action

The panels used to configure fine-grained security can be accessed in the administrative console under the security tab. From this panel a user with appropriate permissions can create new authorization groups.

Administrative console



Cell=JIM668Node03Cell, Profile=Base3

Administrative Authorization Groups

Administrative Authorization Groups > AdminGroup

Use this page to create administrative authorization groups and specify the associated admin resources.

General Properties

* Name: AdminGroup

Resources

Additional Properties

- Administrative Group Roles
- Administrative User Roles

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

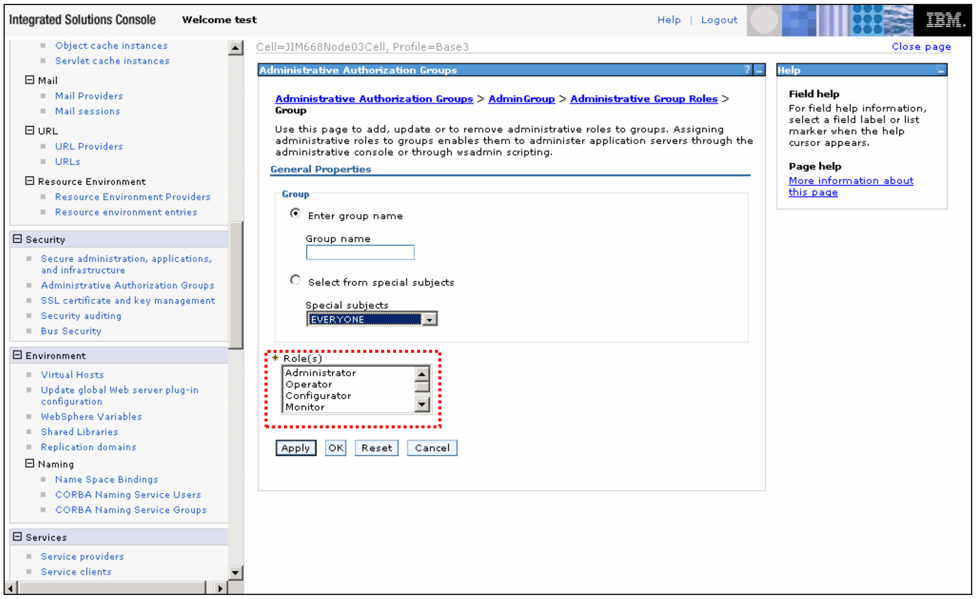
More information about this page

Command Assistance

View administrative scripting command for last action

Once an authorization group has been created, it can be further configured using the additional properties. These allow you to map administrative group roles, and user roles to the authorization group.

Administrative console



Cell=JIM668Node03Cell, Profile=Base3

Administrative Authorization Groups

Administrative Authorization Groups > AdminGroup > Administrative Group Roles > **Group**

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting.

General Properties

Group

● Enter group name

Group name

○ Select from special subjects

Special subjects EVERYONE

* Role(s)

- Administrator
- Operator
- Configurator
- Monitor

Help

Field help

For field help information, select a field label or list marker when the help cursor appears.

Page help

More information about this page

This panel can be used to add, update, or remove administrative roles to authorization groups. Assigning administrative roles to these groups enables them to administer the resources available to the authorization group.

IBM Software Group

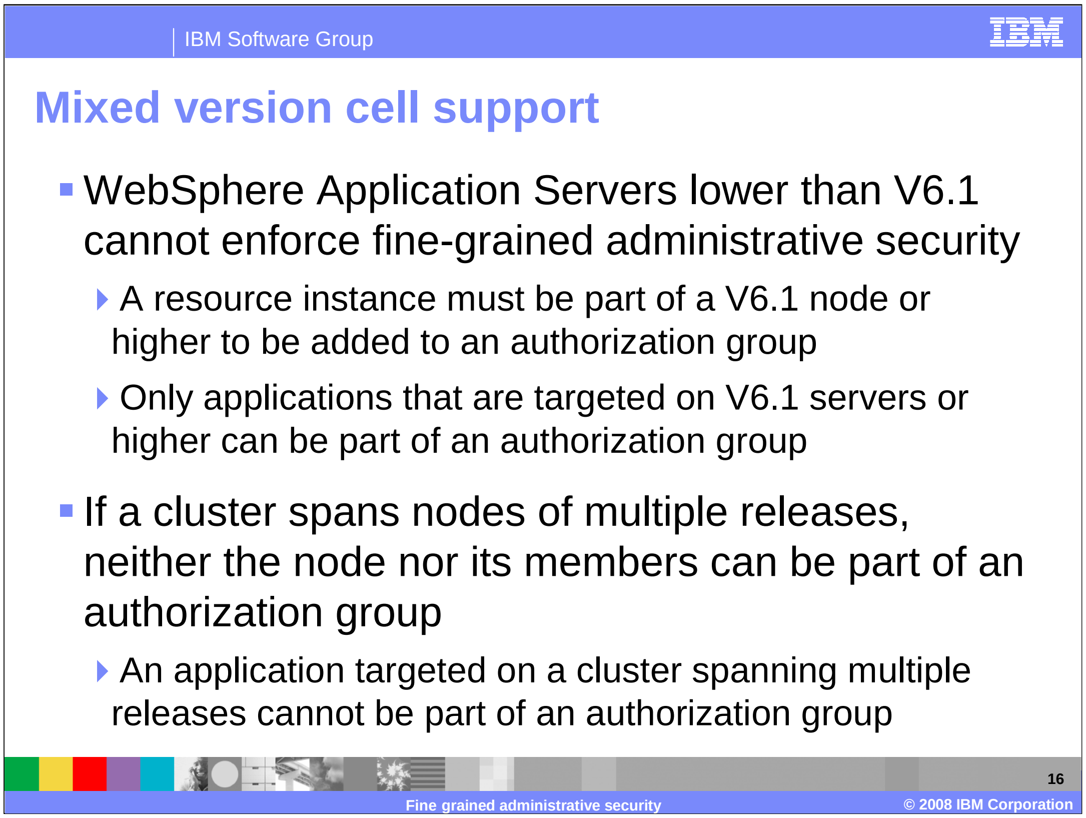
Section

Restrictions

15

Fine grained administrative security

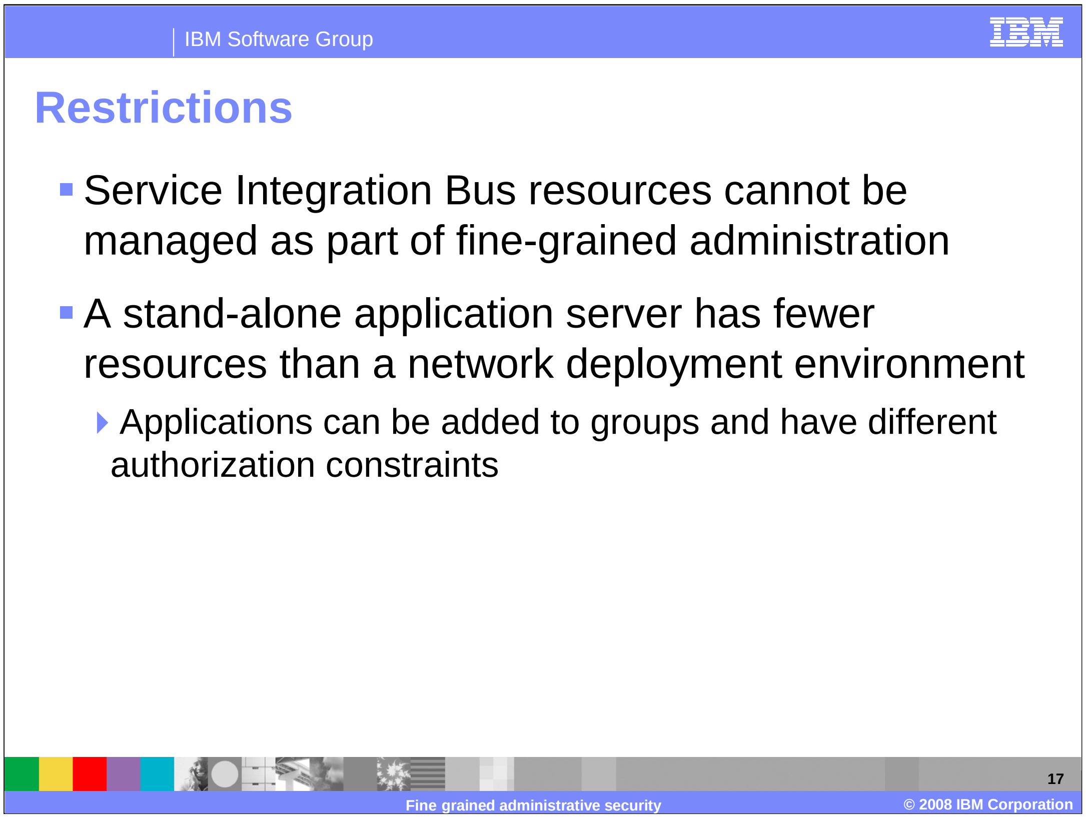
This section covers restrictions and limitations for fine-grained security.



Mixed version cell support

- WebSphere Application Servers lower than V6.1 cannot enforce fine-grained administrative security
  - A resource instance must be part of a V6.1 node or higher to be added to an authorization group
  - Only applications that are targeted on V6.1 servers or higher can be part of an authorization group
- If a cluster spans nodes of multiple releases, neither the node nor its members can be part of an authorization group
  - An application targeted on a cluster spanning multiple releases cannot be part of an authorization group

Fine-grained security has limited capabilities in a mixed version cell environment. WebSphere Application Servers lower than version 6.1 cannot enforce fine-grained administrative security. A resource instance must be part of a version 6.1 node or higher to be added to an authorization group. Only applications that are targeted on version 6.1 servers or higher can be part of an authorization group. If a cluster spans nodes of multiple releases, neither the node nor its members can be part of an authorization group. Also, an application targeted on a cluster spanning multiple releases cannot be part of an authorization group.



IBM Software Group

Restrictions

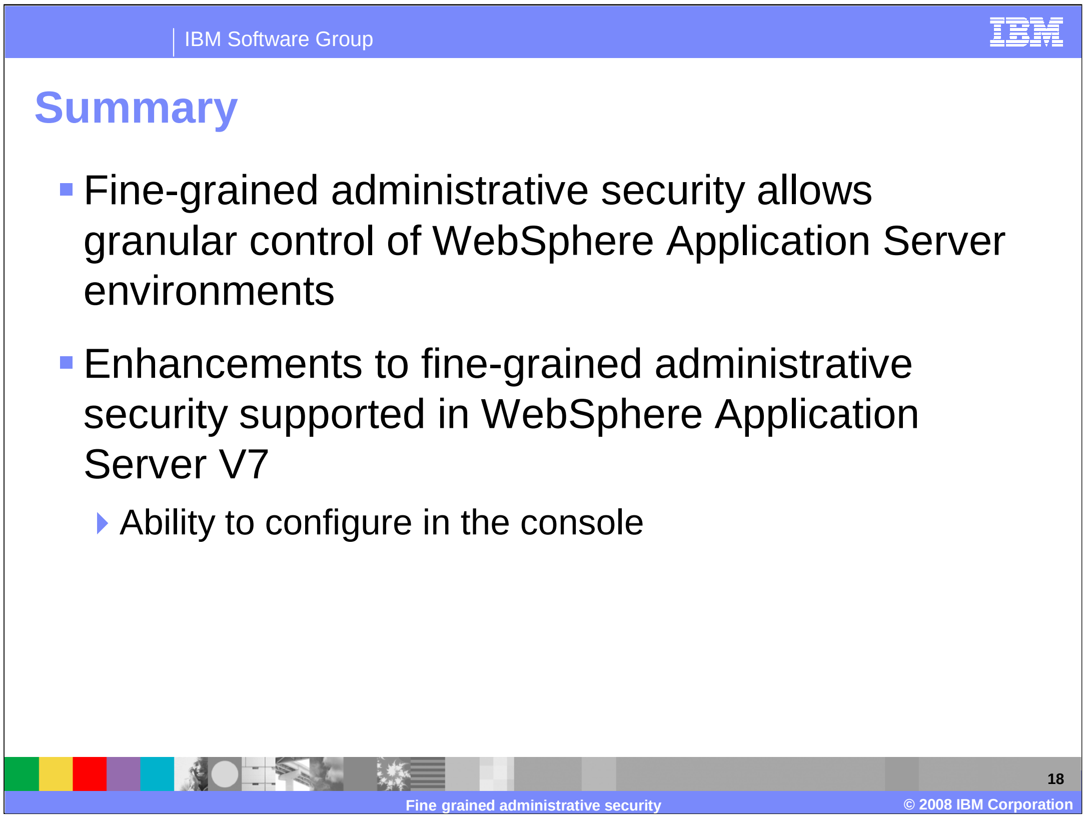
- Service Integration Bus resources cannot be managed as part of fine-grained administration
- A stand-alone application server has fewer resources than a network deployment environment
  - Applications can be added to groups and have different authorization constraints

17

Fine grained administrative security

© 2008 IBM Corporation

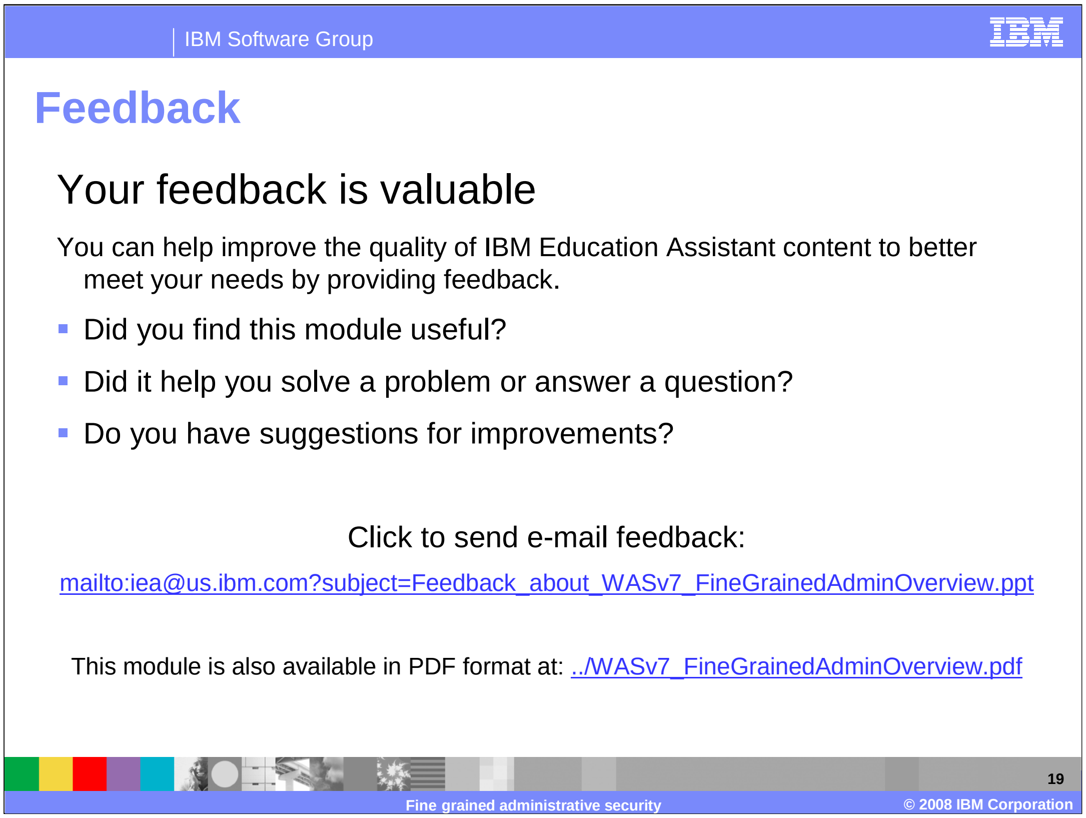
There are a few other restrictions to be considered. Service Integration Bus resources cannot be managed as part of fine-grained administration. Also consider that a stand-alone application server environment has fewer resources than a network deployment environment; applications can be added to groups and have different authorization constraints.



Summary

- Fine-grained administrative security allows granular control of WebSphere Application Server environments
- Enhancements to fine-grained administrative security supported in WebSphere Application Server V7
  - Ability to configure in the console

In summary, fine-grained administrative security allows more granular control of WebSphere Application Server environments. Version 7 has added the ability to configure fine-grained security from the administrative console.



Feedback

Your feedback is valuable

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

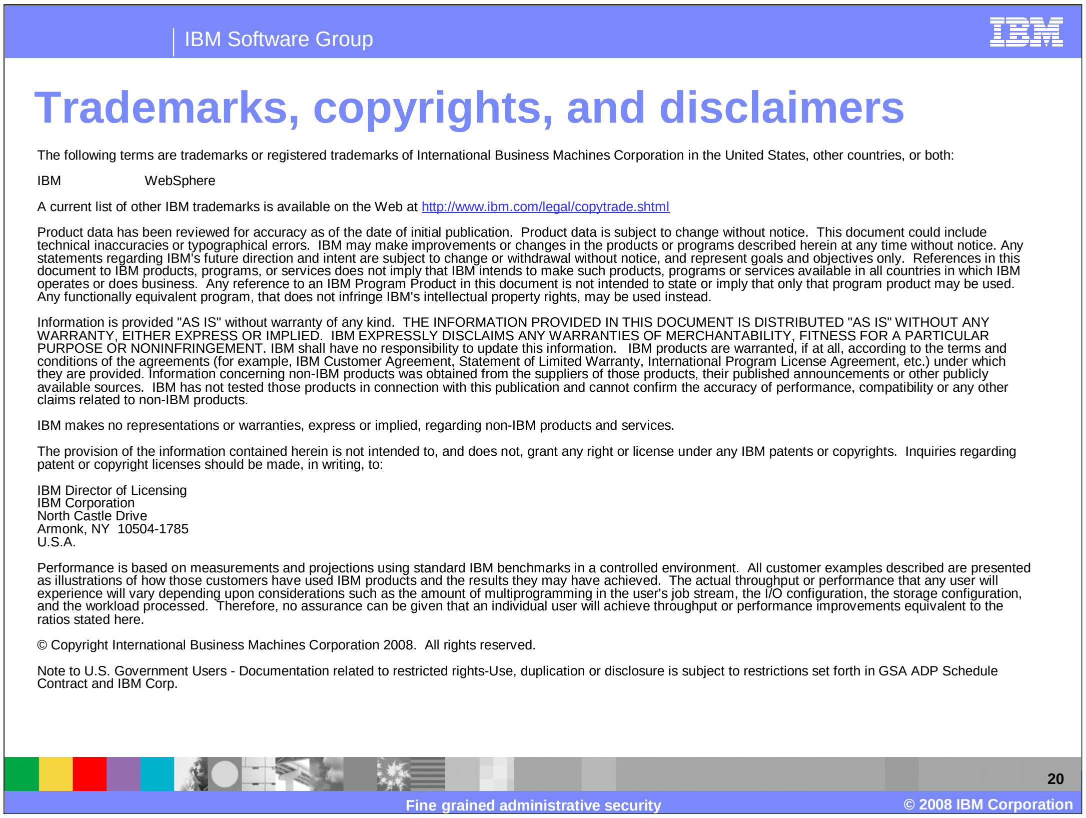
- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv7_FineGrainedAdminOverview.ppt

This module is also available in PDF format at: ../WASv7_FineGrainedAdminOverview.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.