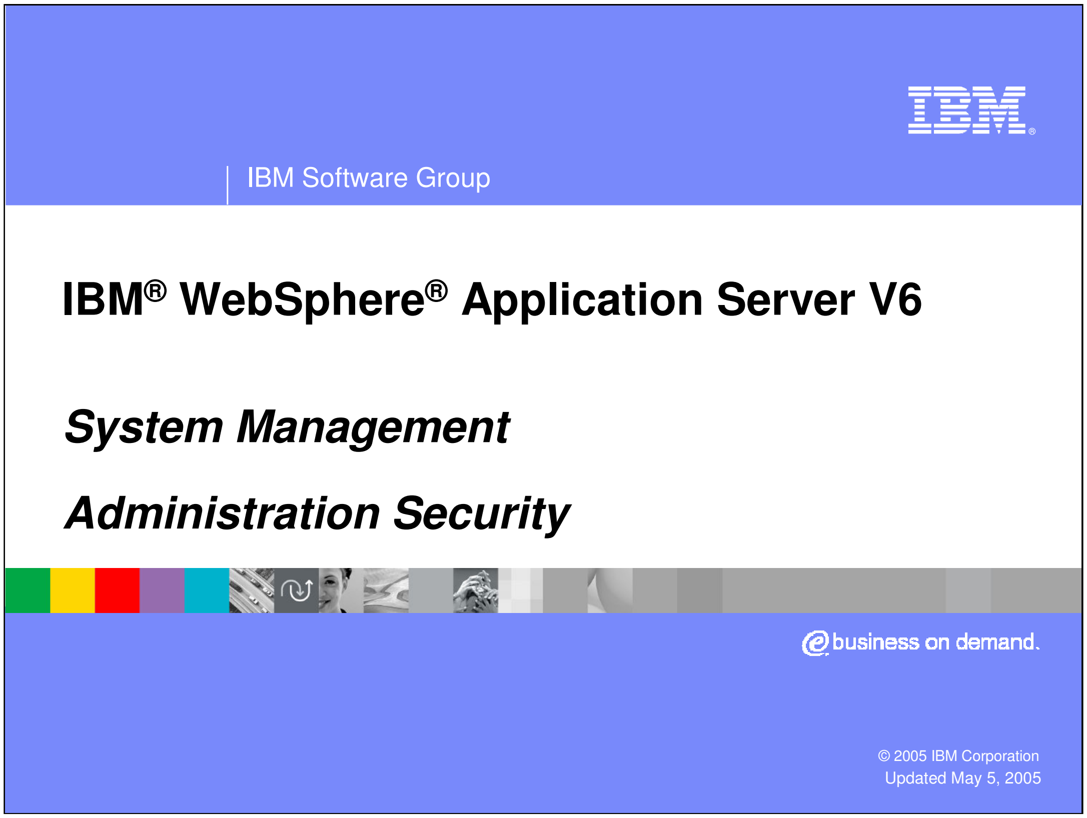


IBM Software Group

IBM® WebSphere® Application Server V6

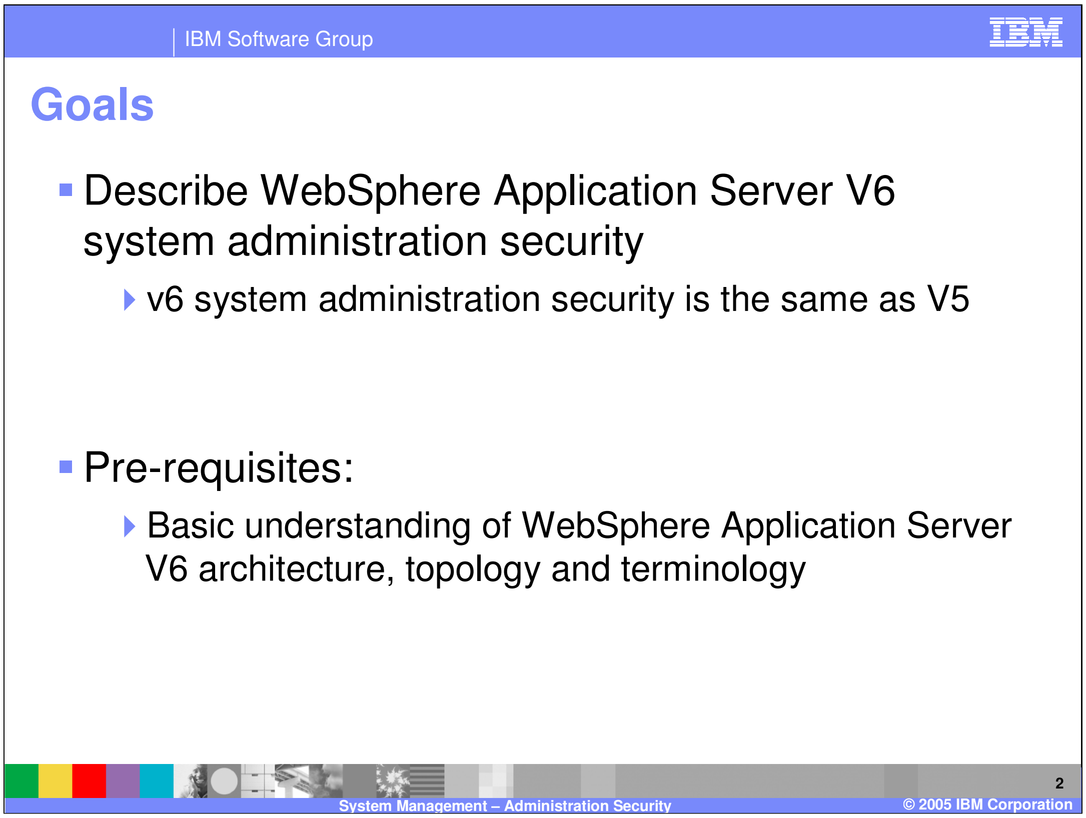
System Management

Administration Security

@business on demand.

Updated May 5, 2005

This presentation will focus on WebSphere Application Server Administrative Security.

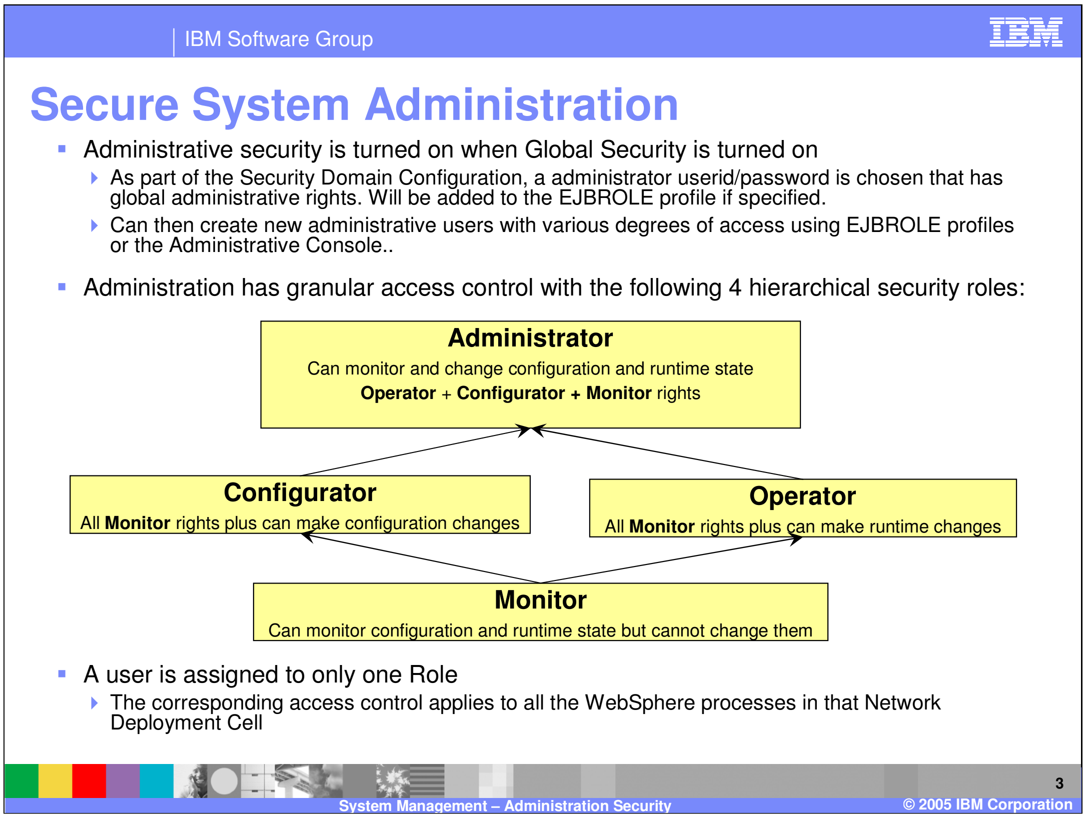


Goals

- Describe WebSphere Application Server V6 system administration security
  - v6 system administration security is the same as V5

- Pre-requisites:
  - Basic understanding of WebSphere Application Server V6 architecture, topology and terminology

The goal of this module is to briefly describe security of the Administrative Console.



IBM Software Group

Secure System Administration

- Administrative security is turned on when Global Security is turned on
  - As part of the Security Domain Configuration, a administrator userid/password is chosen that has global administrative rights. Will be added to the EJBROLE profile if specified.
  - Can then create new administrative users with various degrees of access using EJBROLE profiles or the Administrative Console..
- Administration has granular access control with the following 4 hierarchical security roles:

Administrator

Can monitor and change configuration and runtime state

Operator + **Configurator** + **Monitor** rights

Configurator

All **Monitor** rights plus can make configuration changes

Operator

All **Monitor** rights plus can make runtime changes

Monitor

Can monitor configuration and runtime state but cannot change them

- A user is assigned to only one Role
  - The corresponding access control applies to all the WebSphere processes in that Network Deployment Cell

3

System Management – Administration Security

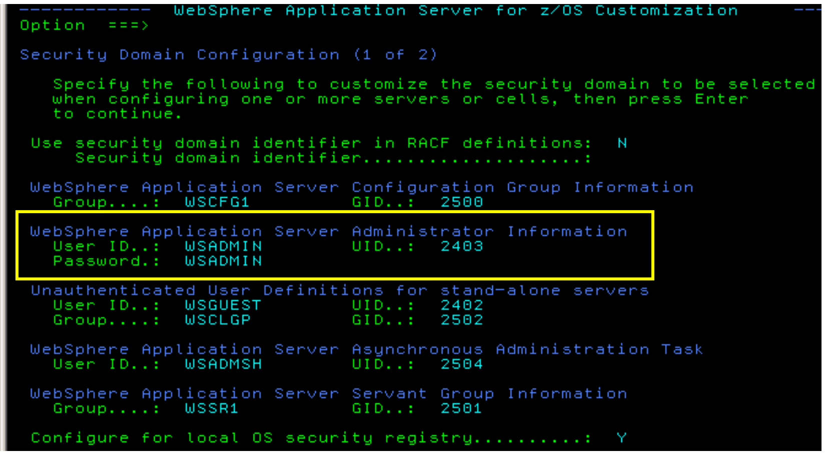
Once security is enabled, the administrative console is secured. Users will be required to authenticate with a valid ID and password. Some installations will elect to disable Java™ 2 security and application security, but protect the integrity of the configuration by restricting administrative access.

Since WebSphere version 5, the Administrative Security subsystem defines four security roles: monitor, configurator, operator, and administrator. A monitor can observe system state and configuration data but cannot make changes. A configurator security role is a monitor who can make changes to the configuration data. The operator security role is a monitor who can change runtime state. For complete capabilities the administrator role, which is essentially a configurator and an operator, can be assigned.

If a user is assigned the operator role, they will have the ability to start and stop servers throughout the entire cell. Monitors will have the ability to view all the servers in the cell and configurators will have the ability to change any server in the cell as the role is applied to all the servers and resources in the cell.

It is not possible for a user to have administrative access control such as Operator on one set of servers in a cell and access control such as Configurator on another set of servers in the same cell.

Security Administrator



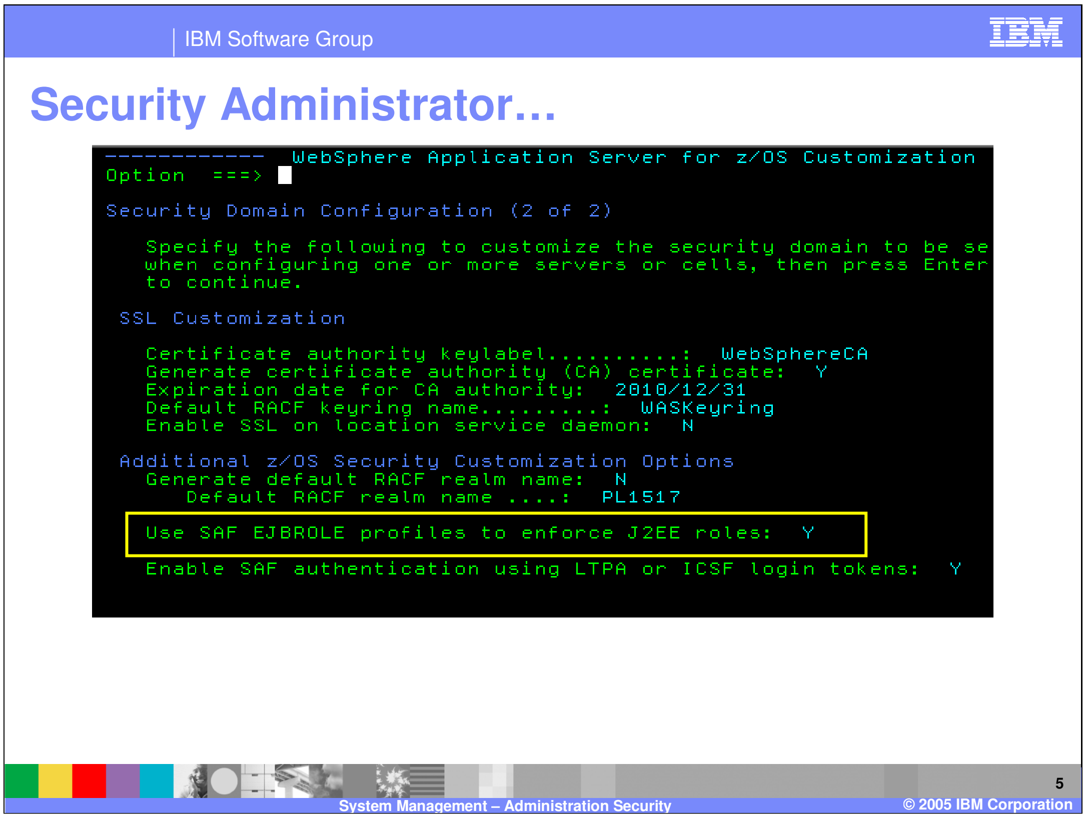
```
------------  WebSphere Application Server for z/OS Customization    ---
Option  ===>

Security Domain Configuration (1 of 2)

   Specify the following to customize the security domain to be selected
   when configuring one or more servers or cells, then press Enter
   to continue.

 Use security domain identifier in RACF definitions:  N
     Security domain identifier....................:

 WebSphere Application Server Configuration Group Information
   Group....:  WSCFG1         GID..:  2500

 WebSphere Application Server Administrator Information
   User ID..:  WSADMIN        UID..:  2403
   Password.:  WSADMIN

 Unauthenticated User Definitions for stand-alone servers
   User ID..:  WSGUEST        UID..:  2402
   Group....:  WSCLGP         GID..:  2502

 WebSphere Application Server Asynchronous Administration Task
   User ID..:  WSADMSH        UID..:  2504

 WebSphere Application Server Servant Group Information
   Group....:  WSSR1          GID..:  2501

 Configure for local OS security registry..........:  Y
```

Administrator defined in the Security Domain Configuration. Will be added to the administrator EJBROLE:

ADDUSER,WSADMIN,DFLTGRP(WSCFG1)….

PERMIT administrator CLASS(EJBROLE) ,ID(WSCFG1),ACCESS(READ)

When configuring the Security Domain, an Administrator userid and password is supplied. The BBOSBRAK job that runs as part of the configuration will define the userid selected to SAF, making it a part of the **configuration group**. As you will see on the next slide, if SAF EJBROLEs are specified to enforce J2EE roles, the configuration will be added to the **administrator** EJBROLE RACF profile. Other profiles that will be defined are **monitor**, **configurator** and **operator**. Other users can be PERMITed to these EJBROLES as needed.



IBM Software Group

Security Administrator…

```
-------------  WebSphere Application Server for z/OS Customization
Option  ===>

Security Domain Configuration (2 of 2)

   Specify the following to customize the security domain to be se
   when configuring one or more servers or cells, then press Enter
   to continue.

 SSL Customization

   Certificate authority keylabel..........:  WebSphereCA
   Generate certificate authority (CA) certificate:  Y
   Expiration date for CA authority:  2010/12/31
   Default RACF keyring name.........:  WASKeyring
   Enable SSL on location service daemon:  N

 Additional z/OS Security Customization Options
   Generate default RACF realm name:  N
      Default RACF realm name ....:  PL1517

   Use SAF EJBROLE profiles to enforce J2EE roles:  Y

   Enable SAF authentication using LTPA or ICSF login tokens:  Y
```

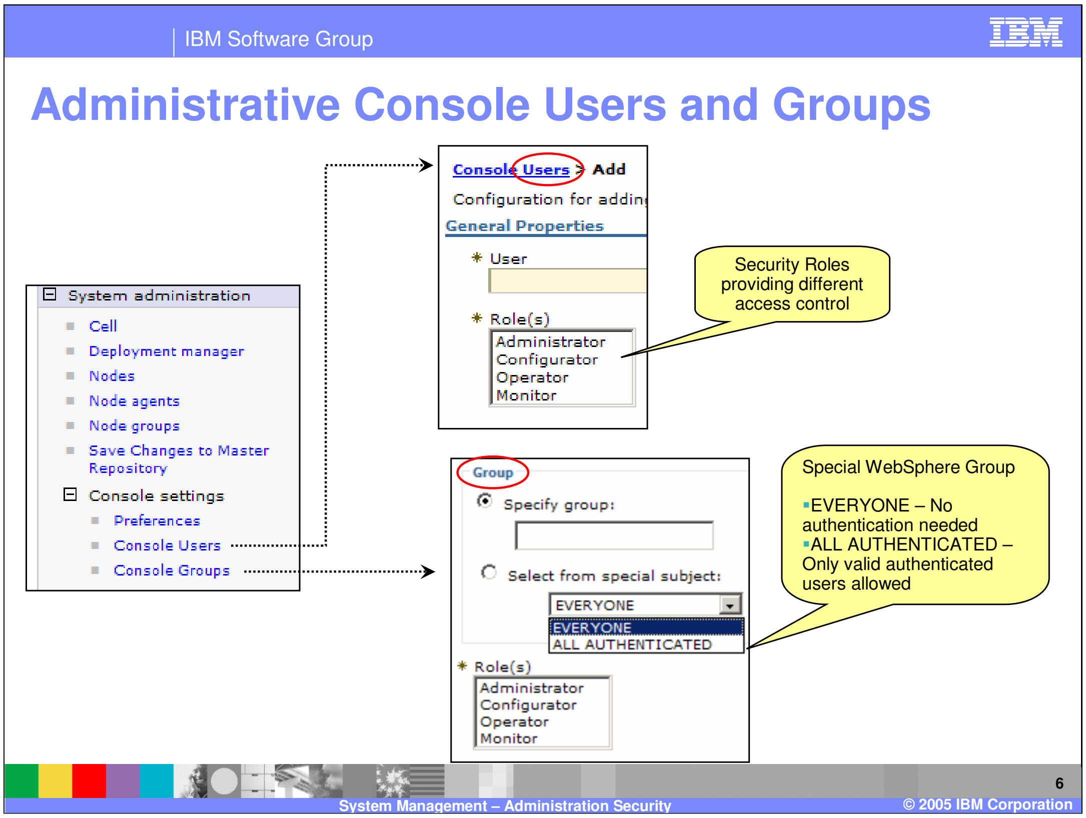
5

System Management – Administration Security

© 2005 IBM Corporation

By specifying **Y** for the question highlighted on this slide, the SAF EJBROLE profiles will be used to determine user authority to use the Administrative Console. This will translate to setting the custom property ‘com.ibm.security.SAF.authorization’ to **true**. If SAF EJBROLE profiles are not used, the next slide shows how to add console users and groups.

Administrative Console Users and Groups

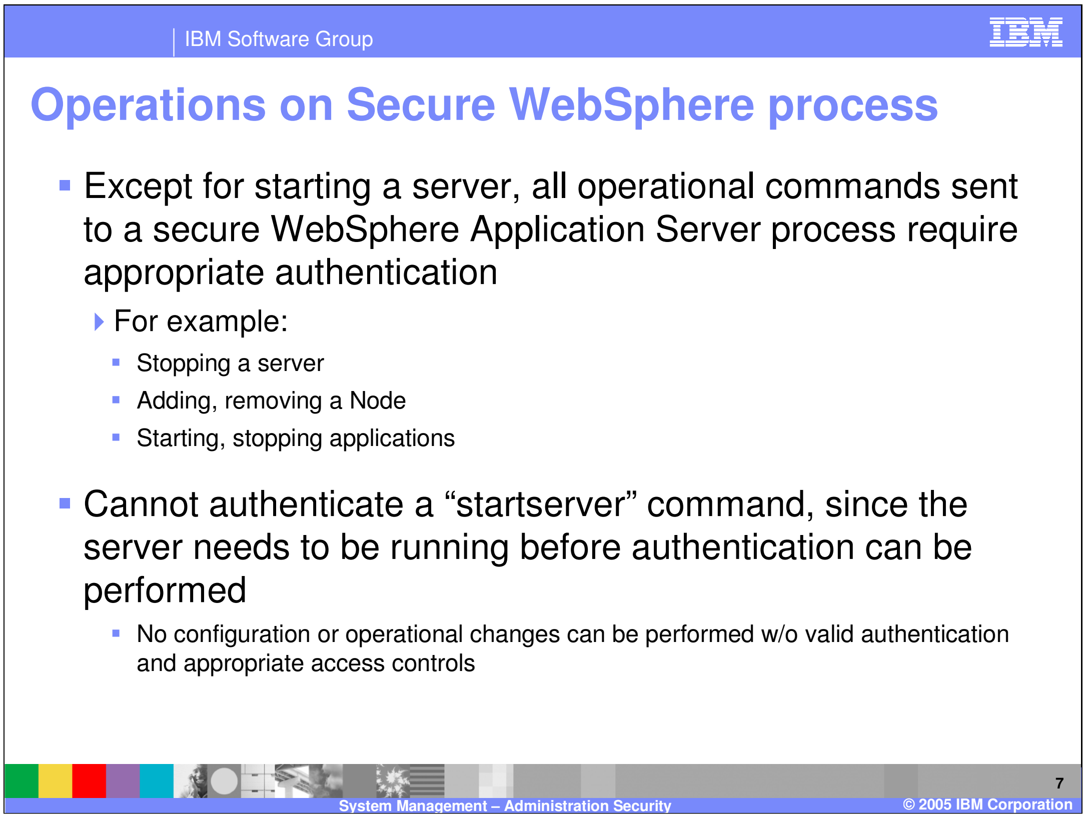


Security Roles providing different access control

Special WebSphere Group

- EVERYONE – No authentication needed
- ALL AUTHENTICATED – Only valid authenticated users allowed

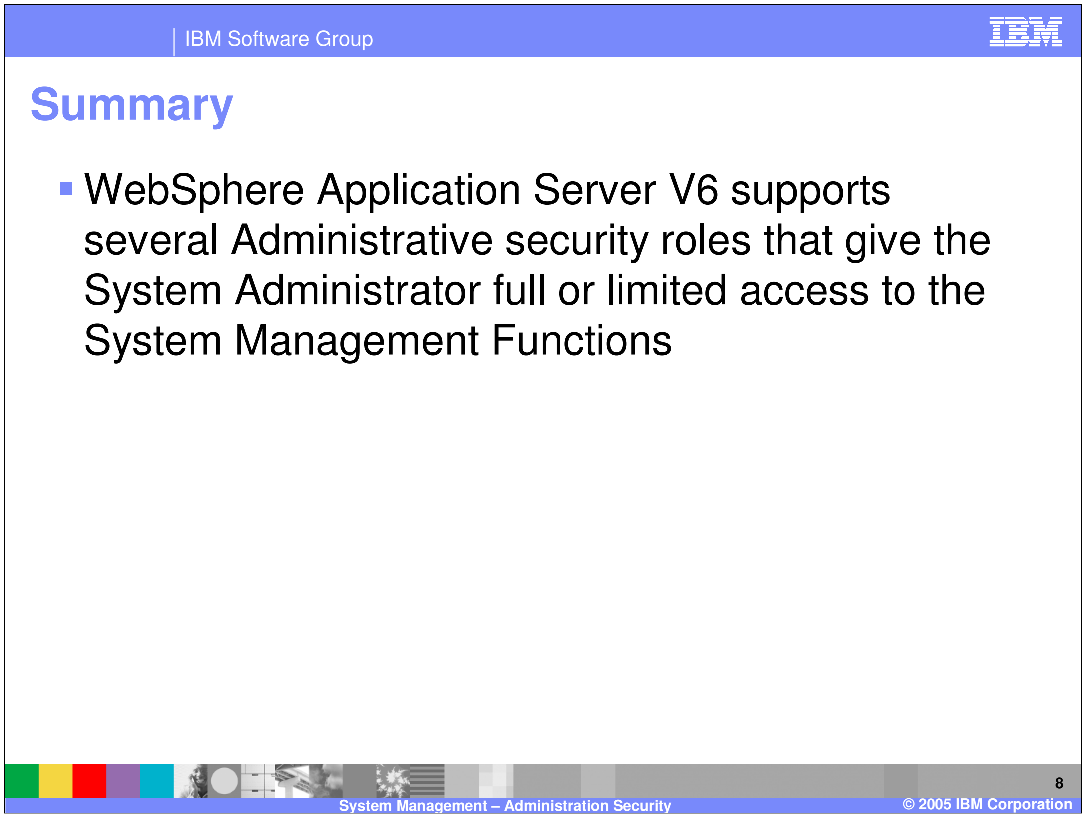
This slide illustrates where in the administrative console the various roles can be configured if you are not using SAF EJBROLE profiles to enforce J2EE roles. The System administration panel is on the left side of the Administrative Console. You can add users individually to the Administrative Console roles, or you can specify a group to have certain access. The groups or users must already be defined in SAF before being added here in the Administrative Console.



Operations on Secure WebSphere process

- Except for starting a server, all operational commands sent to a secure WebSphere Application Server process require appropriate authentication
  - For example:
    - Stopping a server
    - Adding, removing a Node
    - Starting, stopping applications
- Cannot authenticate a “startserver” command, since the server needs to be running before authentication can be performed
    - No configuration or operational changes can be performed w/o valid authentication and appropriate access controls

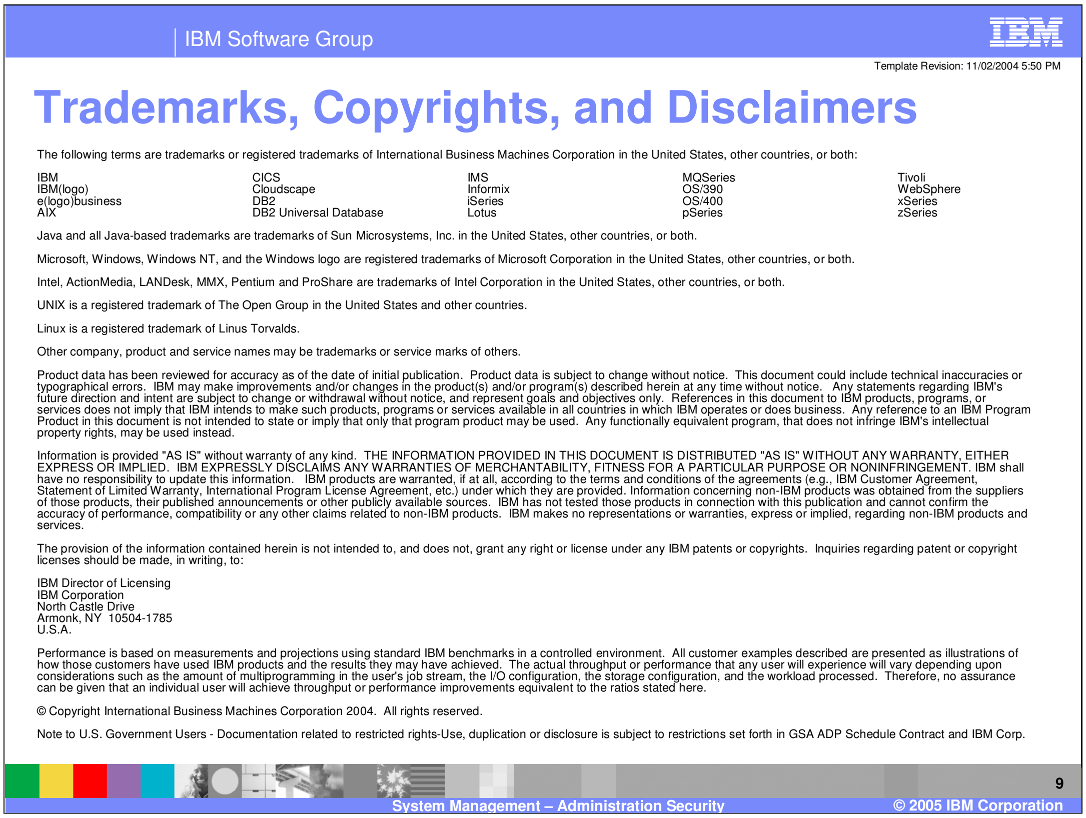
Once security is enabled, it is necessary to restart the application servers so that the security configuration information is implemented by the running processes. From that point on, all operations will require authentication except for starting the server. The reason for this exception is that until the server starts, it cannot authenticate a user.



Summary

- WebSphere Application Server V6 supports several Administrative security roles that give the System Administrator full or limited access to the System Management Functions

In summary, the administrative roles provide a level of granularity that allow you to give different access controls to different users, based on the four security roles.



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.