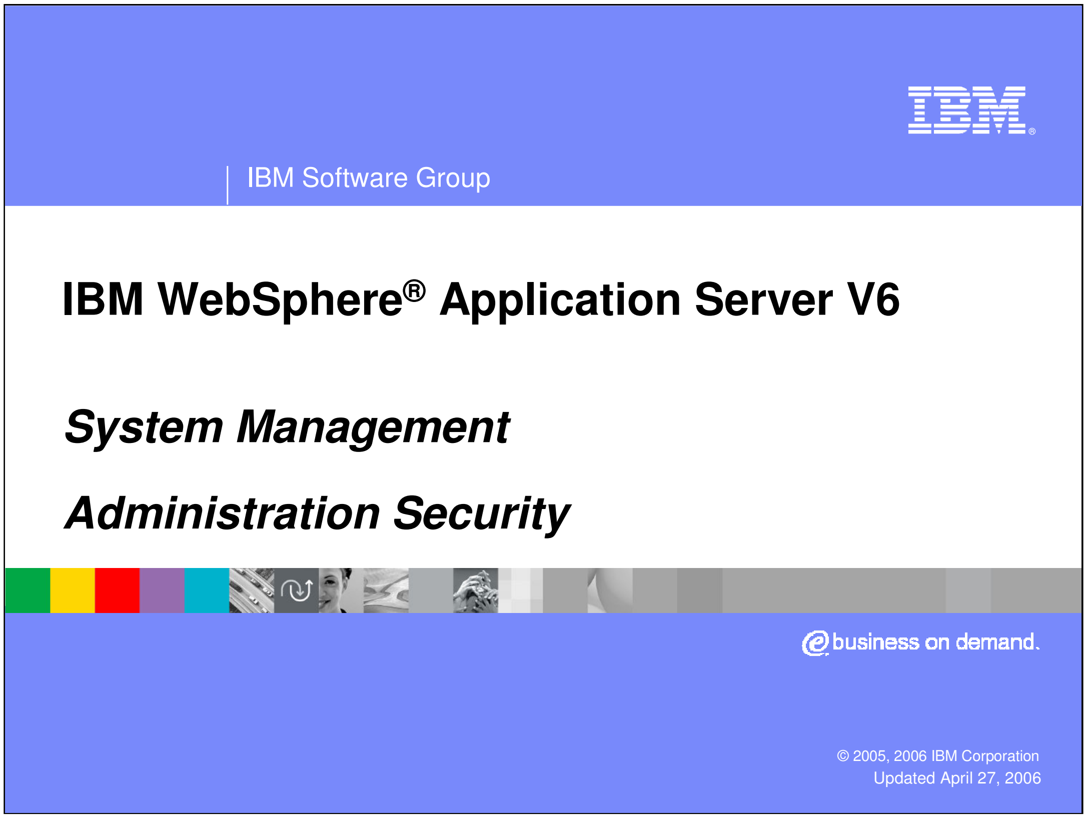


IBM Software Group

IBM WebSphere® Application Server V6

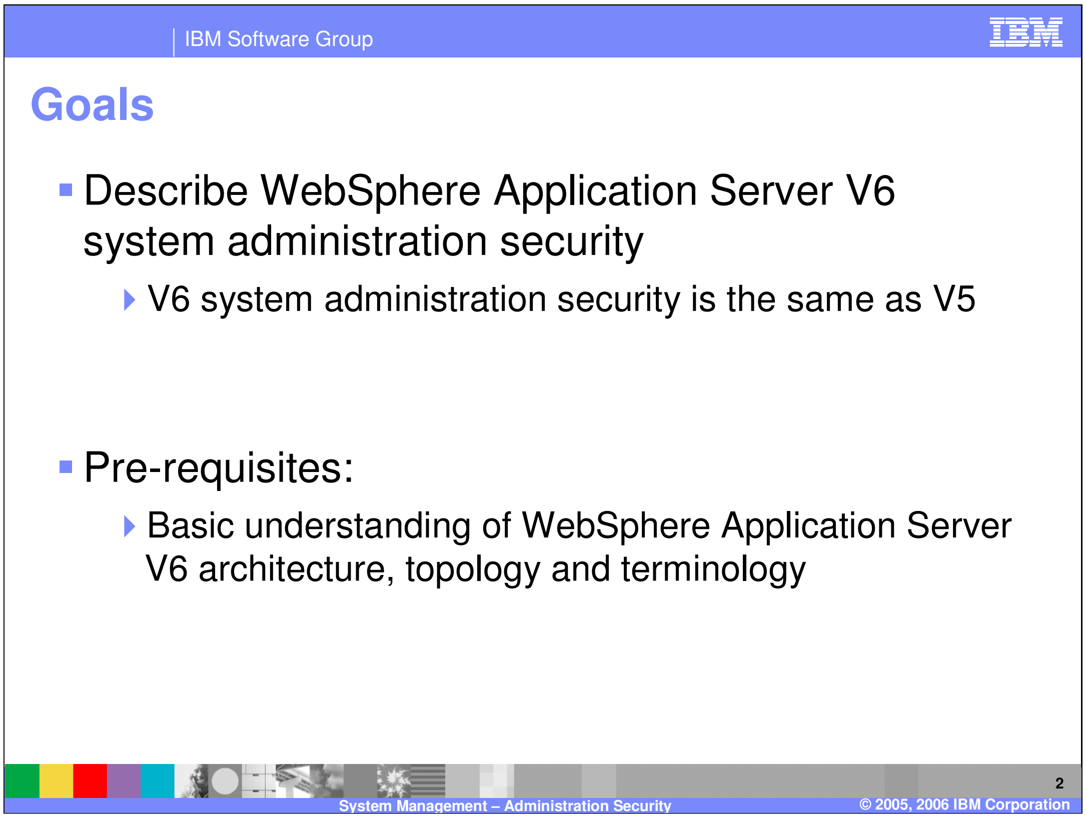
System Management

Administration Security

business on demand.

Updated April 27, 2006

This presentation will focus on WebSphere Application Server Administrative Security.

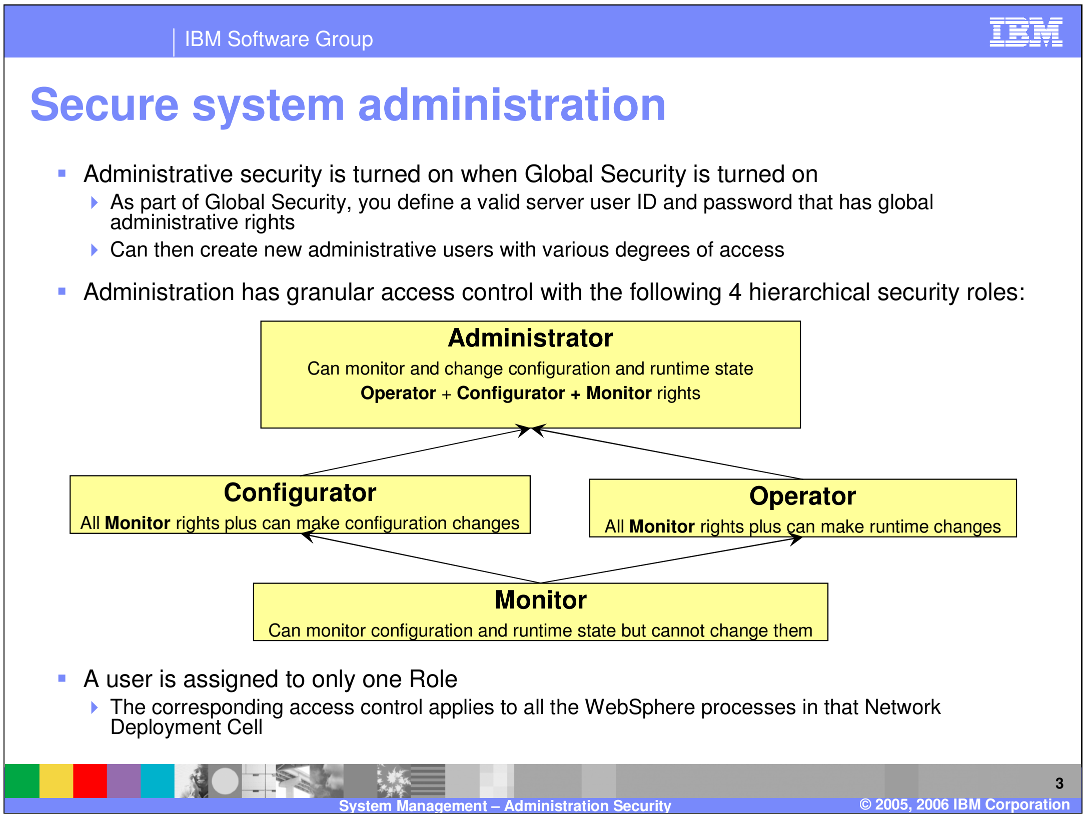


Goals

- 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 Global Security, you define a valid server user ID and password that has global administrative rights
  - Can then create new administrative users with various degrees of access
- 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

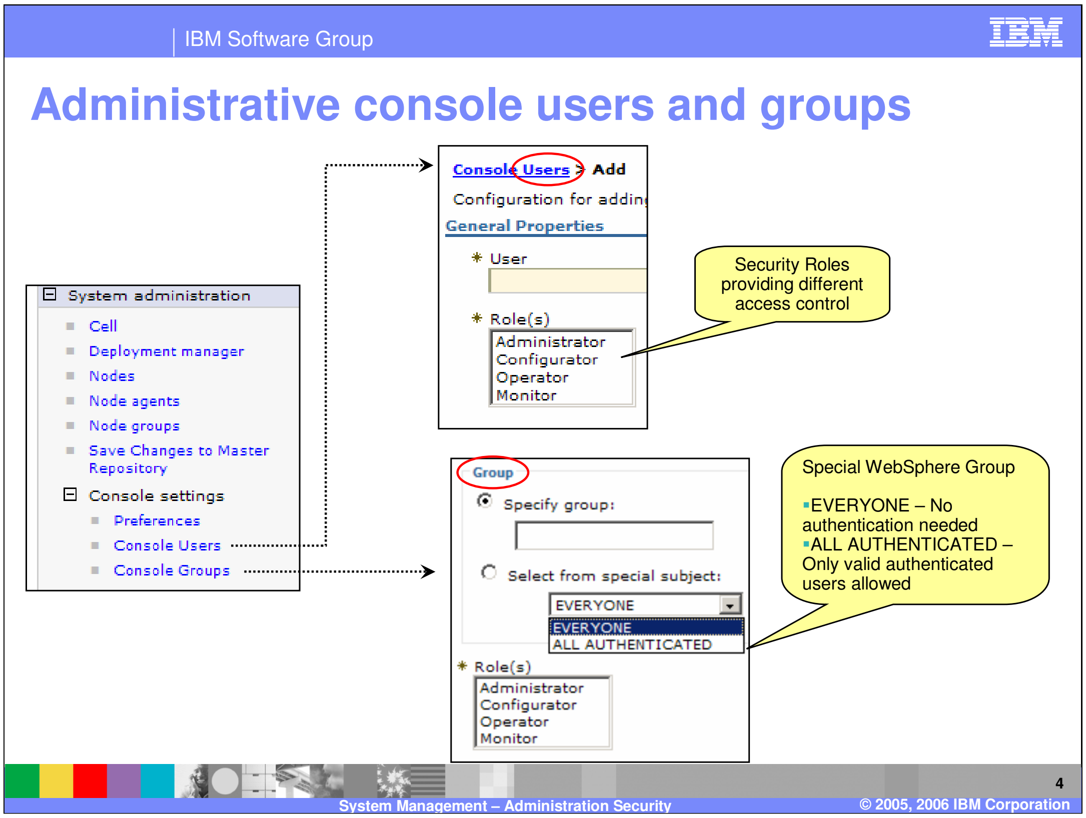
3
System Management – Administration Security

Once security is enabled, the administrative console is secured. You will be required to authenticate with an 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 also 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 also an operator, can be assigned and is a fourth security role.

The Operator role has the permission to start and stop servers throughout the entire cell. Monitors can view all the servers in the cell and Configurators can change any server in the cell. This is because roles are applied to all of the servers and resources in the cell.

It is not possible to have one set of administrative access control, like Operator, on a set of servers in a cell, and another set of access control, like Configurator, on another set of servers within the same cell.



IBM Software Group

Administrative console users and groups

Security Roles providing different access control

Special WebSphere Group

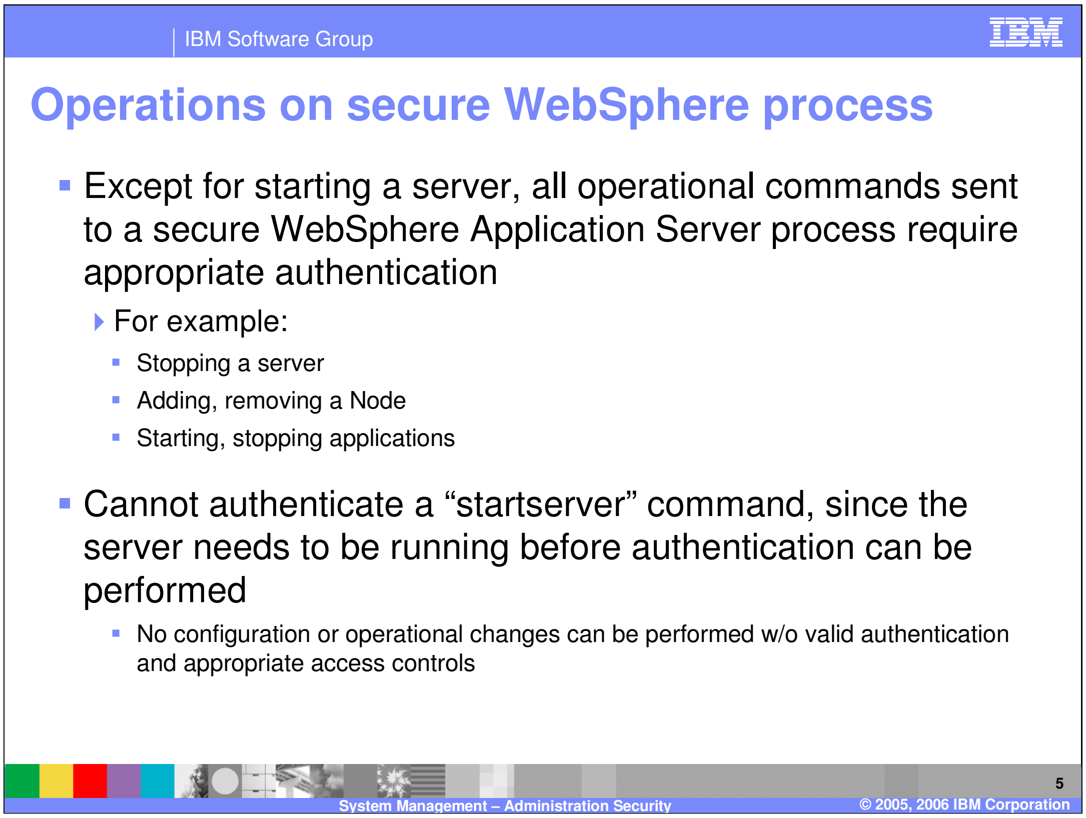
- EVERYONE – No authentication needed
- ALL AUTHENTICATED – Only valid authenticated users allowed

4

System Management – Administration Security

© 2005, 2006 IBM Corporation

This slide illustrates where in the administrative console the administrative roles can be configured. 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 rights. The groups will be defined in whatever authentication repository is being used.



IBM Software Group

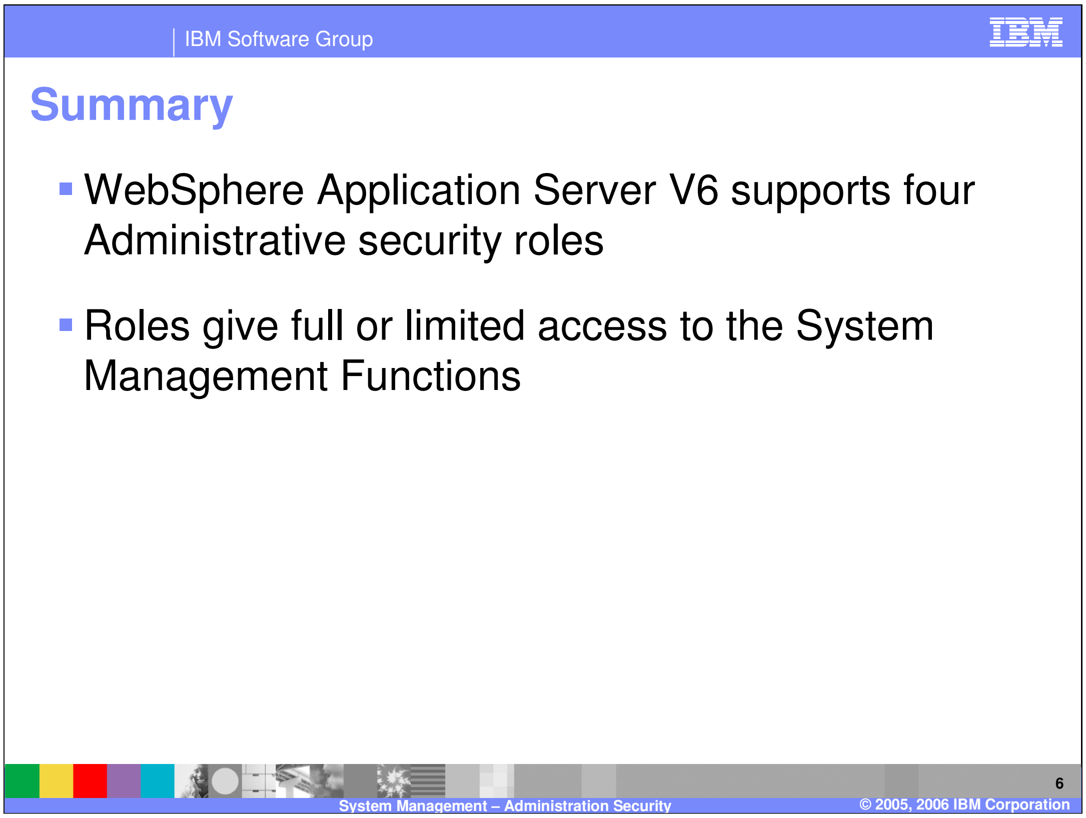
Operations on secure WebSphere process

- 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

5

System Management – Administration Security

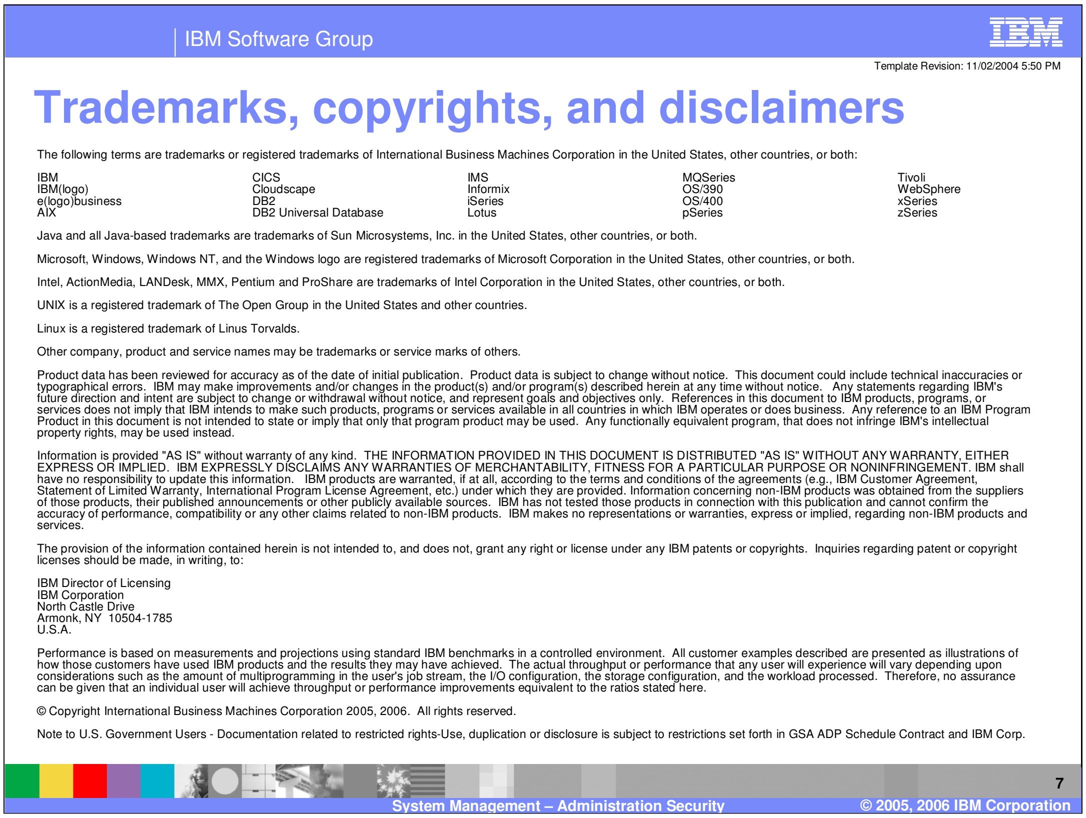
Once security is enabled, it is necessary to restart the application servers so that the security configuration information is implemented by the running processes. From that point on, all operations will require authentication except for starting the server. The reason for this exception is that until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



Summary

- WebSphere Application Server V6 supports four Administrative security roles
- Roles give 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.