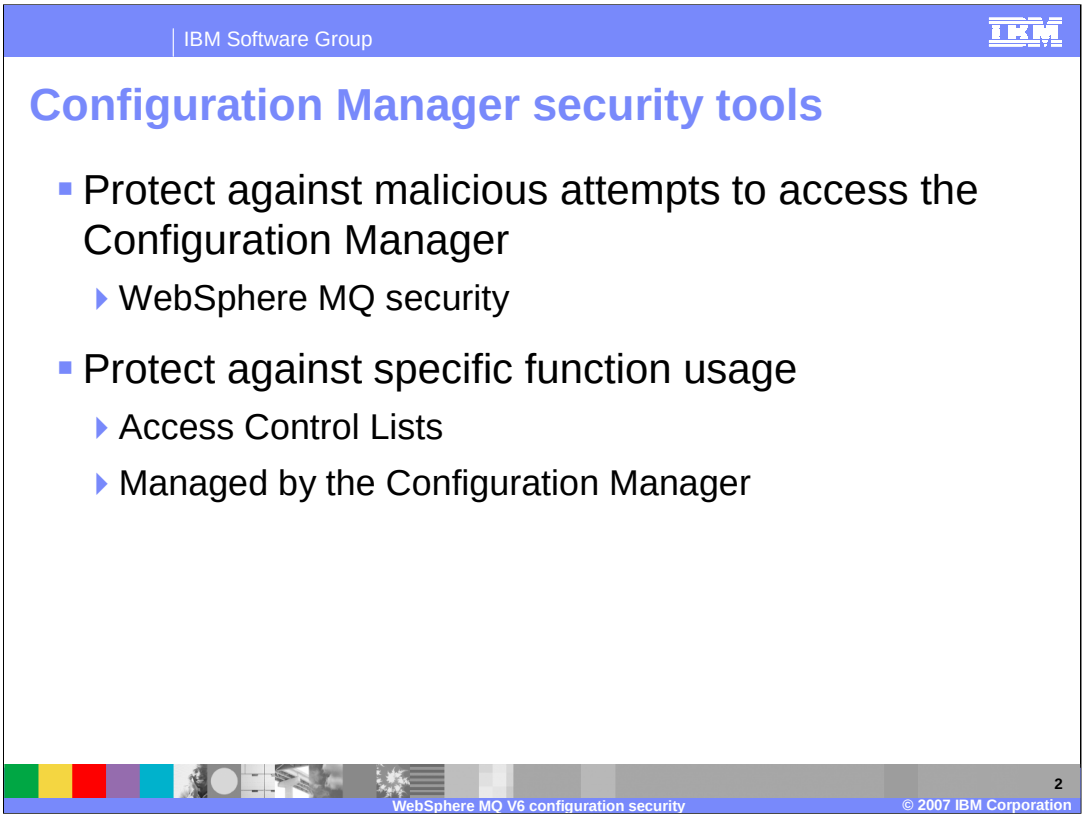
This presentation discusses the new capabilities for Security Management in WebSphere Message Broker Version 6, and in particular the security tools provided by the Configuration Manager.



The Configuration Manager security tools are designed to do two things:

•Provide protection from malicious attempts to access the Configuration Manager. This will be done in conjunction with WebSphere MQ security.

•Provide protection against accidental attempts to perform certain types of functions by users who have some partial security capability. This is done with Access Control Lists, which are managed by the Configuration Manager.

Malicious intrusion – WebSphere MQ security

- The Configuration Manager Proxy (CMP) connects to the Configuration Manager using WebSphere MQ as the transport
- For successful communication to occur, the client (tool) user ID must have the following set up correctly:
  - Queue manager/queue authorizations
  - Security Exit (optional)
  - SSL (optional)
- Depending on the amount of protection required, a combination of the above can be used to guard against malicious attacks

Access to the Configuration Manager is provided by the Configuration Manager Proxy API. This is used by the Broker Toolkit and the broker Line Command interface, and by any user application that needs to access the Configuration Manager.

The Proxy API connects to the Configuration Manager using normal WebSphere MQ channel connectivity, and normal queue authorizations. So, the queue manager and queues used by the Configuration Manager must have the correct security authorizations for users attempting to use them.

In addition, WebSphere MQ security exits can be used; and encrypting the message data that is transmitted over the WebSphere MQ channels using SSL is supported.

Queue manager and queue authorizations

- The Configuration Manager Proxy API (and therefore the Toolkit) connects to the Configuration Manager's queue manager, puts messages to a request queue and gets replies from a reply queue
- The appropriate WebSphere MQ authorizations are therefore required for:
  - The Queue Manager (+connect, and so on.)
  - SYSTEM.BROKER.CONFIG.QUEUE (+put, and so on.)
  - SYSTEM.BROKER.CONFIG.REPLY (+get, and so on.)
  - SYSTEM.DEAD.LETTER.QUEUE (+put, and so on.)
- In general, on distributed platforms, these are automatically added for you when you create ACL entries (more later)
- On z/OS® – you need to set these up separately (see Information Center for further info)

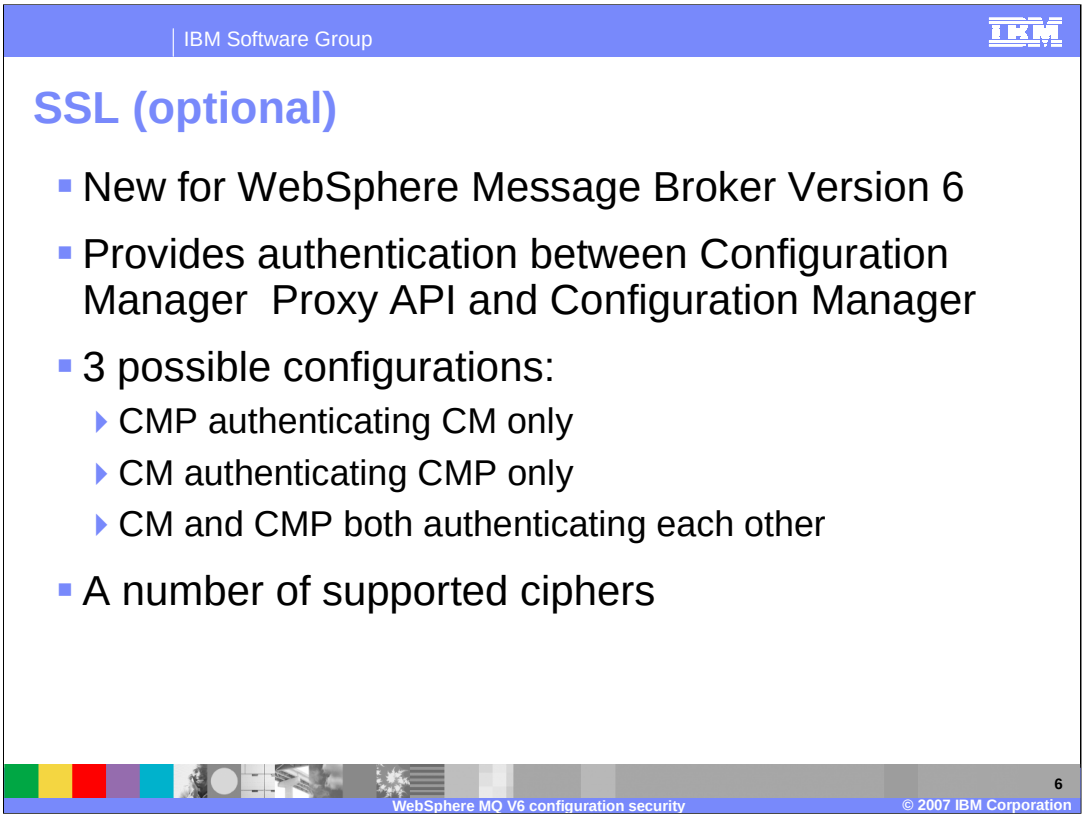
This slide shows the queues that are used to enable communication with the Configuration Manager. These queues are defined when the Configuration Manager is created, and specific authorizations for these queues are normally created when Access Control List entries for specific users or groups are created. These can then be further changed as required, by making changes to the WebSphere MQ authorizations.

On z/OS, the authorizations are not created automatically. This step needs to be done explicitly, and details are given in the Information Center.

Security exits (optional)

- For additional security, you can use WebSphere MQ Security Exits
  - Will prevent any clients without the appropriate security exit from connecting to the Configuration Manager's queue manager
  - Sophisticated security schemes possible (challenge/response and so on.)

Security control can be extended using WebSphere MQ security exits. This has not changed between broker versions 5 and 6, but does allow the possibility of sophisticated security controls for access to the Configuration Manager.



In addition to the existing WebSphere MQ authorization controls, WebSphere Message Broker Version 6 has introduced the facility to use Secure Socket Layer (SSL) between the Configuration Manager and any applications which use the Configuration Manager Proxy API to connect to the Configuration Manager.

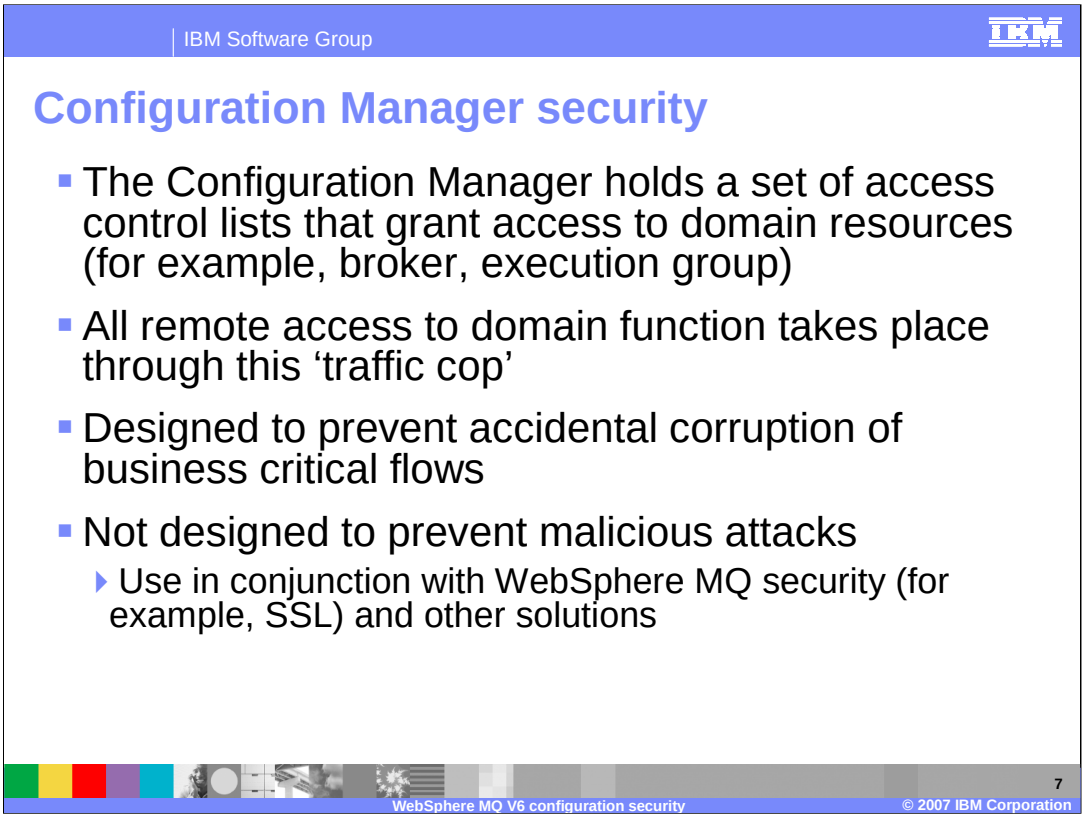
This provides the SSL authentication capability and encryption of messages between the Proxy API application and the Configuration Manager. For example, if using the Broker Toolkit to connect to the Configuration Manager, the Toolkit provides a set of GUI tools to enable SSL configuration.

Following normal SSL behavior, this SSL capability provides for uni-directional authentication, or for bi-directional authentication. All of the common SSL ciphers are supported.

To use this facility, SSL first needs to be configured on the WebSphere MQ connection between the WebSphere MQ Client and the Configuration Manager's queue manager. Follow normal WebSphere MQ techniques for SSL.

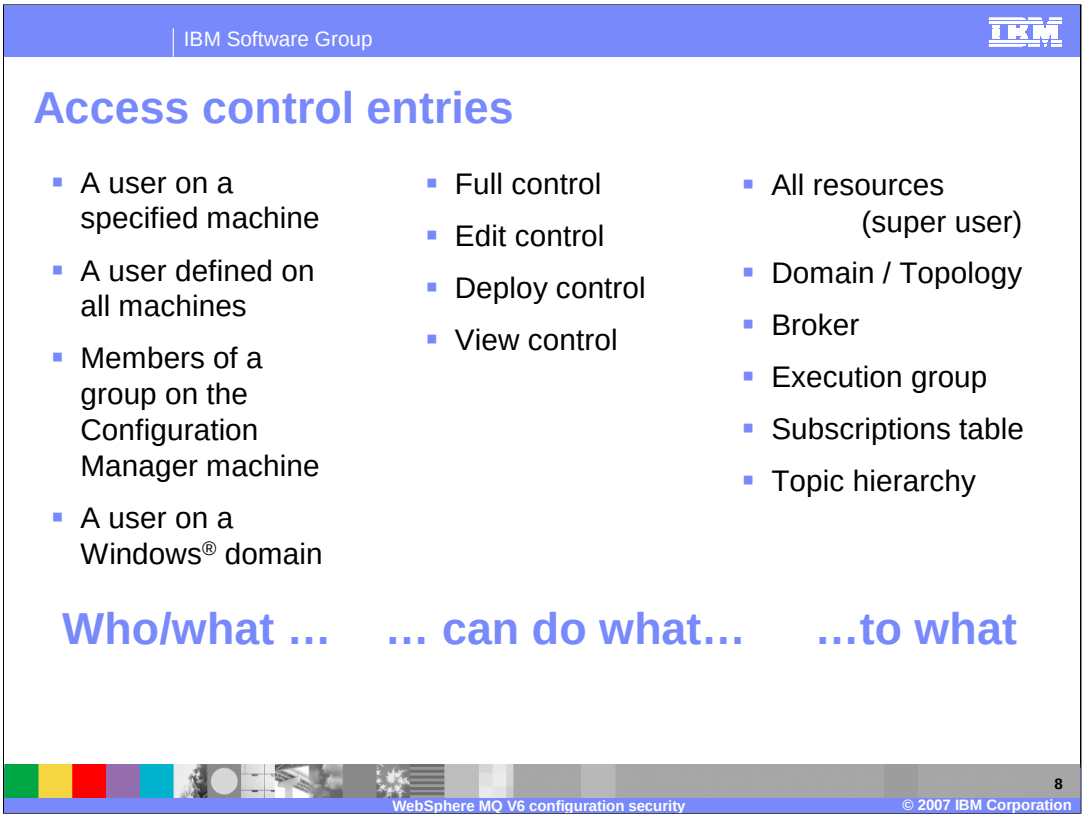
Once the WebSphere MQ channels have been configured to use SSL, the Broker Toolkit can be used to set specific parameters on the Configuration Manager connection document, which will enable the Toolkit to take advantage of the SSL connection.

If you are using either the Broker Console Line Commands, or the API Proxy exerciser, the connection document created by the Toolkit can be used to connect to the Configuration Manager from these other types of clients.

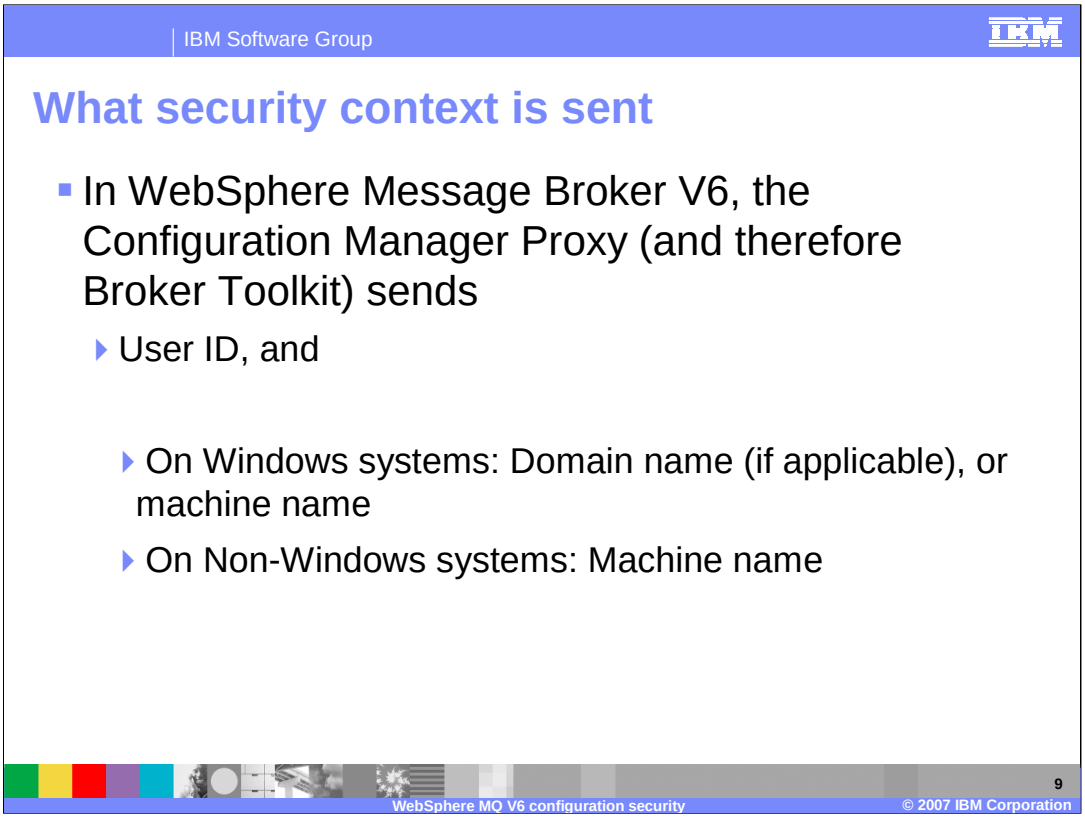


To provide authorization control for access to the Configuration Manager, users are granted specific access to resources using an Access Control List, or ACL.

Access to different types of resources such as Brokers, or Execution Groups, can be controlled using the ACL. The ACLs are used to prevent accidental corruption or update of Broker resources. However, to prevent attacks from malicious users or applications, ACL security should be extended to use security functions provided by the base WebSphere MQ security functions.



Access Control entries can be used to control access to different types of users. For example, this can be as general as any member of a group, on any machine, or as specific as an individual user, and restricted to access from a specific computer.



When the Configuration Manager Proxy connects to the nominated Configuration Manager, it sends different pieces of information, depending on the nature of the client environment.

In all cases, the user ID of the user issuing the command is sent.

On Windows systems where the user is managed as part of a Windows security domain, the name of the domain is sent. If the user is a local user, and not part of a Windows domain, the name of the client machine is sent.

If the client is a Linux system, then the name of the Linux system is sent.

This approach applies to the Proxy API, and is therefore used by the Broker Toolkit, the Broker Console Line commands, and to any user-written application using the Proxy API.

Manipulating access control entries

- Three new commands (can be run remotely)
  - Create ACL entries - mqsicreateaclentry
  - Delete ACL entries - mqsideleteaclentry
  - List ACL entries - mqsilistaclentry
- ACL entries are also created when objects are created
- Positive access only; cannot create a “deny” access permission
- No ACLs for the broker event log; this is automatically filtered on a per-user basis

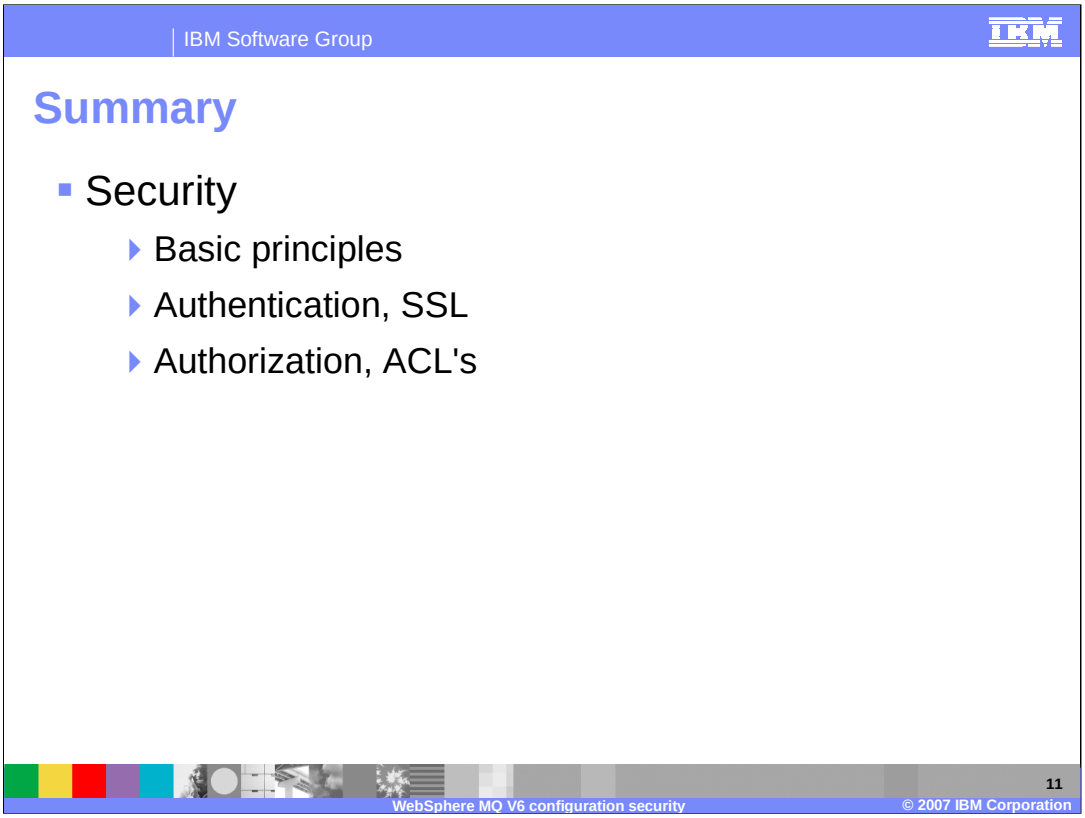
The entries in the Configuration Manager security database are maintained by a set of commands, which all end with “aclentry”. These are used to create or delete entries, or to enquire on the status of ACL entries by using the “list” command.

These commands are also available from the Configuration Manager Proxy API, and the Proxy API Exerciser. However, they are not available through the Broker Toolkit.

ACL entries are automatically created when objects are created in the Configuration Manager.

The default level of access to any object in the Configuration Manager is none; therefore, to permit access to a resource for a user, a specific ACL entry will need to be created for this.

The broker event log is a special case; all event log messages are available to the user who generated them, and they are filtered and shown only to that user.



This session covered the WebSphere Message Broker Version 6 capabilities for security of the broker Configuration Manager, and how access to the Configuration Manager is authenticated and authorized.

References

- WebSphere Message Broker library:

http://www-306.ibm.com/software/integration/wbimessagebroker/library/

- WebSphere Message Broker Information Center:

http://publib.boulder.ibm.com/infocenter/wmbhelp/v6r0m0/index.jsp

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 z/OS

Windows, and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

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.