

Enabling Global Security in Single Server and Network Deployment environment

Global security

This paper discusses only global security on WebSphere Application Server as security could be enabled in a number of different ways and different level, parts, or components in WebSphere Application Server.

What is global security?

Global security can be thought of as a "big switch" which activates wide variety of WebSphere security settings. Values for these settings may be specified, but they will not take effect until global security is activated. The setting applies to all applications running in the environment and determines whether security is used at all, the type of registry against which authentication takes place, the use of SSL, Java 2 Security Manager, Java Authentication and Authorization Service (JAAS), Java 2 Connector authentication data entries, Common Secure Interoperability Version 2 (CSIv2)/Security Authentication Service (SAS) authentication protocol (Remote Method Invocation over the Internet Inter-ORB Protocol (RMI/IIOP) security), and other miscellaneous values, many of which act as defaults. In particular, application security, including authentication and role-based authorization, is not enforced unless global security is active.

Why turn on global security?

At the very least, you should turn on global security because turning on global security activates the settings which protect your server from unauthorized users and making changes to your production environment.

When you enable security, you are enabling security settings on a global level so there is a small performance overhead with security enabled. Therefore, consider disabling security when it is not needed, for example, on a development system.

Global security is disabled by default, in order to simplify the installation of the server. When you enable security, you are enabling security settings on a global level so proper planning is required. Incorrectly enabling global security can lock you out of the administrative console, or you can not start or stop the server anymore.

Enabling global security in Single Server environment

1. Start the WebSphere Application Server administrative console by clicking `http://yourhost.domain:9090/admin` after starting the WebSphere Application Server. Log in with any user ID.
2. Click **Security -> User Registries -> Local OS.**

Local OS User Registry

The user registry for the local operating system of the application server. When security is enabled and any of these properties are changed, please go to the GlobalSecurity panel and click Apply or OK to validate the changes. [i](#)

Configuration		
General Properties		
Server User ID	* db2admin	i The user ID under which the server will execute (for security purposes).
Server User Password	*	i The password corresponding to the serverid.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		
Additional Properties		
Custom Properties A set of arbitrary user registry configuration properties whose names are specific to a given type of pluggable registry.		

Server User ID:

On **Windows** systems, **Server User ID** must have the **Administrative** and **Act as Part of Operating System** privileges. The server user ID needs this authority for authentication using the LocalOS user registry.


On **UNIX system**: the process ID must have **root** privileges on a UNIX system. This privilege is needed to call the UNIX operating system APIs to authenticate or to collect user and group information.













Server User Password: enter the user password that corresponds to the **Server User ID**

Note: This Server User ID and password are used to log into the administrative console after security is turned on. You can use other users to log in if those users are part of the administrative roles. When security is enabled in the product, this server ID and password are authenticated with the registry during product startup. If authentication fails, the server does not come up. So it is important to choose an ID and password that do not expire or change often.

3. Click **OK**.

Global Security

Specifies global security configuration for a managed domain. The following steps are required to turn on security. 1) Select the desired User Registry from the left navigation panel and set the properties in that panel. 2) Enable security in this panel. 

Configuration		
General Properties		
Enabled	<input checked="" type="checkbox"/>	 Enables security for this WebSphere domain.
Enforce Java 2 Security	<input checked="" type="checkbox"/>	 If Java 2 Security is enabled and the application policy file is not set up correctly, the application may fail to run.
Use Domain Qualified User IDs	<input type="checkbox"/>	 When true, user names returned by methods such as <code>getUserPrincipal()</code> will be qualified with the security domain in which they reside.
Cache Timeout	<input type="text" value="600"/>	 Timeout value for security cache in seconds.
Issue Permission Warning	<input checked="" type="checkbox"/>	 When enabled, a warning will be issued during application installation, if an application requires a Java 2 Permission that normally should not be granted to an application.
Active Protocol	CSI and SAS 	 Specifies the active security authentication protocol when security is enabled. Possible values are CSI (CSIv2), or CSI and SAS.
Active Authentication Mechanism	* SWAM (Simple WebSphere Authentication Mechanism) 	 Specifies the active authentication mechanism when security is enabled.
Active User Registry	Local OS 	 Specifies the active user registry when security is enabled.
Use FIPS	<input type="checkbox"/>	 This will enable the use of FIPS (Federal Information Processing Standard) approved cryptographic algorithms. Note that setting this flag does not automatically change the existing JSSE provider in the Secure Socket Layer configuration. Also note that a FIPS approved JSSE provider only allows TLS as the protocol. Moreover, the FIPS approved LTPA authentication mechanism is not backward compatible with the non-FIPS approved LTPA implementation that is used in all prior versions of WebSphere Application Server products.
<input type="button" value="Apply"/> <input type="button" value="OK"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

4. Click **Security -> Global Security** from the left navigation menu. Configure the authentication mechanism, user registry, and so on. The configuration order is not important. However, when you select the **Enabled** flag in the **Global Security** panel, verify that all these tasks are completed. When you click **Apply** or **OK** and the **Enabled** flag is set, verification occurs to see if the administrative user ID and password can be authenticated to the configured user registry. If you do not configure the administrative user ID and password, the validation fails.

➤ To enable Global Security, certain criteria must be met.

Active Authentication Mechanism: An authentication mechanism must be selected. SWAM is selected initially. Select the default **SWAM**. The Application Server supports two authentication mechanisms by default, SWAM and LTPA.

Note: SWAM (Simple WebSphere Authentication Mechanism): the SWAM authentication mechanism is intended for simple, non-distributed, single application server type runtime environments. The single application server restriction is due to the fact that SWAM does not support *forwardable* credentials. Since SWAM is intended for a single application server process, single-sign-on (SSO) is not supported. The SWAM authentication mechanism is suitable for simple environments, software development environments, or other environments that do not require a distributed security solution. SWAM relies on the session ID; it is not as secure as Lightweight Third-Party Authentication (LTPA), therefore using SSL with SWAM is strongly recommended. Use the LTPA option for multi-server distributed requirements. Credentials for LTPA are forwardable to other machines and for security reasons do expire.

Active User Registry: A user registry must be selected. Ensure that the Active User Registry option is set to **LocalOS**. The Application Server supports the concept of a custom registry, which makes the integration of WebSphere with any type of appropriate registry fairly straightforward.

Other configuration options on the Global Security panel are as follows:

Enforce Java 2 Security: By default, Java 2 security is disabled. However, enabling global security automatically enables Java 2 security. You can choose to disable Java 2 security, even when global security is enabled.

Note: When Java 2 security is enabled and if an application requires more Java 2 security permissions than are granted in the default policy, then the application might fail to run properly until the required permissions are granted in either the `app.policy` file or the `was.policy` file of the application. AccessControl exceptions are generated by applications that do not have all the required permissions.

User Domain Qualified User IDs: if this option is enabled, user names will appear with their fully-qualified domain attribute when retrieved programmatically.

Cache Timeout: when the timeout is reached, the Application Server clears the security cache and rebuilds the security data. Since this affects performance, this value should not be set too low. This value is a relative timeout so specify the value by determining the best trade off for the application and by looking at usage patterns and security needs for the site.

Issue Permission Warning: the `filter.policy` file contains a list of permissions that an application should *not* have according to the J2EE 1.3 Specification. If an application is installed with a permission specified in this policy file and this option is enabled, a warning will be issued.

Active Protocol: this determines which ORB-based authentication protocols are accepted by the Application Server. There are two authentication protocols supported by IBM. IBM Secure Authentication Service (SAS) is the authentication protocol used by all previous releases of the WebSphere product. Common Secure Interoperability Version 2 (CSIv2) is implemented in WebSphere Application Server, Version 5 and is considered the strategic protocol.

SAS performs authentication for Java clients of enterprise beans and helps to provide message protection or encryption between such clients and WebSphere application servers using RMI/IIOP over SSL for communication. SAS also provides message protection between WebSphere application services.

CSIv2 allows vendors to securely interoperate and provides a greater number of features over SAS. It supports enabling interoperable authentication, delegation, and privileges by offering a secure protocol above the transport layer.

____ 5. Before restarting the server, log off the administrative console. You can log off by clicking **Logout** at the top menu bar.

____ 6. Stop the server by going to the command line in the WebSphere Application Server /bin directory and issue the command:

```
stopServer <server name>
```

UNIX system: /opt/WebSphere/AppServer/bin/stopServer.sh server1

____ 7. Restart the server in secure mode by issuing the command `startServer <server_name>`. Once the server is secure, you cannot stop the server again without specifying an administrative user name and password. To stop the server once security is enabled, issue the command, `stopServer <server_name> -username <user_id> -password <password>`. Alternatively, you can edit the `soap.client.props` file in the `<install_root>/properties` directory and edit the `com.ibm.SOAP.loginUserId` or `com.ibm.SOAP.loginPassword` properties to contain these administrative IDs.

UNIX system: restart the server with these commands:

```
cd /opt/WebSphere/AppServer/bin
./stopServer.sh -username <user_id> -password <password> server1;
./startServer.sh server1
```

Testing the configuration

After restarting the server in secure mode, run a couple of simple tests to verify that most facets of security are working properly.

____ 8. Test basic authentication with snoop by accessing the following URL:
`http://hostname.domain:9080/snoop`. A login panel appears. Type in any valid user ID and password in your configured user registry. If the login panel fails to appear, there is a problem.

____ 9. Test form login by bringing up the administrative console:
`http://hostname.domain:9090/admin`. A form-based login page appears. Type in the administrative user ID and password that was used for configuring your user registry when configuring security. If the login panel fails to appear, there is a problem.

Enabling global security in the Network Deployment environment


Enabling global security in the Network Deployment environment differs from a stand-alone base application server. In the Network Deployment environment, the configuration is stored temporarily in the Deployment Manager until it is synchronized with all of the node agents.

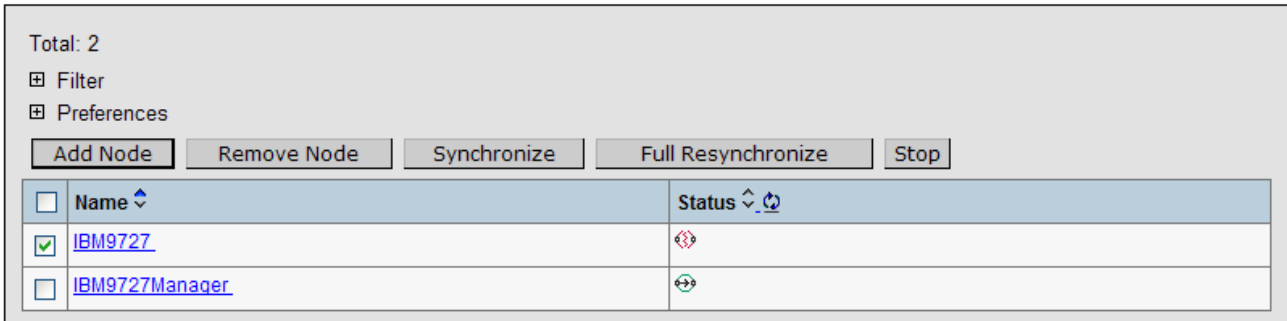
After setting the **Enabled** flag to on and to save the configuration has been saved to the repository. Verify that the validation that occurs after you click **OK** in the **Security > Global Security** panel is successful (see previous steps on how to do it in the Enabling global security in Single Server or Base environment section)

Note: Lightweight Third Party Authentication (LTPA) is the configured authentication mechanism because distributed security tokens are required. The user registry is typically Lightweight Directory Access Protocol (LDAP) or Custom, as Local OS only works for a single machine setup.

1. Issue the **force file sync** command from the administrative console to push a copy of the new configuration to all of the running node agents. If a node agent fails to get the security-enabled configuration, communication with the deployment manager fails due to a lack of access (it will not be security enabled). To force a file sync at any specific node, complete the following steps from the administrative console:

Nodes






A list of nodes in this cell. You can add new nodes into the cell by clicking on "Add Node" and specifying a remote, running WebSphere Application Server instance. 



Total: 2

Filter

Preferences

<input type="checkbox"/>	Name 	Status  
<input checked="" type="checkbox"/>	IBM9727	
<input type="checkbox"/>	IBM9727Manager	

- a. Go to **System Administration > Nodes** and select the check box of all of the nodes (you do not need to select the deployment manager node).
- b. Click **Full Resynchronize** to verify that the file sync has occurred. The message might indicate that the nodes already are synchronized. This message is OK. When synchronization is initiated, verify that the Synchronized status displays for all nodes.

- ___ 2. Stop the Deployment Manager. Manually restart the Deployment Manager from the command line or service. To stop the Deployment Manager, complete the following:

Go to **System Administration > Deployment Manager** and click **Stop**. This action logs you out of the administrative console and stops the Deployment Manager process. Also from the command line, you can locate `<installation_root>/DeploymentManager/bin` and type `stopManager.bat`

UNIX system: `/opt/WebSphere/DeploymentManager/bin/stopManager.sh`

- ___ 3. Restart the Deployment Manager process. To restart the Deployment Manager process, locate the `<install_root>/bin` directory and type `startManager.bat` or `startManager.sh` on **UNIX** System.

Once the Deployment Manager initialization is complete, go back into the administrative console to complete this task. Remember that security now is enabled in only the Deployment Manager. If you enabled single sign on (SSO), specify the fully qualified domain name of your URL, for example, `http://myhost.domain:9090/admin`. When you are prompted for a user ID and password, type the one you entered as the administrator ID in the configured user registry.

UNIX system: `/opt/WebSphere/DeploymentManager/bin/startManager.sh`

- ___ 4. Restart all node agents to make them security enabled. You must have restarted the Deployment Manager in a previous step before completing this step. To stop all node agents, complete the following:

Node agents

Defines a physical machine upon which server processes may execute, as well as ping timeouts, nanny config, as well as other config settings required by the Node Agents components [\[1\]](#)

The screenshot shows a web interface for managing Node Agents. At the top, it says "Total: 1". Below this are sections for "Filter" and "Preferences". There are three buttons: "Stop", "Restart", and "Restart all Servers on Node". Below the buttons is a table with the following data:

<input checked="" type="checkbox"/>	Name	Node	Status
<input checked="" type="checkbox"/>	nodeagent	IBM9727	

- ___ a. Go to **System Administration > Node Agents** and select the check box beside all node agents. Click **Restart**. A message similar to the following displays at the top of the panel: The node agent on node NODE NAME was restarted successfully.
- ___ b. Alternatively, if you previously did not stop your application servers, restart all of the servers within any given node by clicking **System Administration > Node Agents** and clicking the node agents you want to restart all the servers. Then, click **Restart all Servers on Node**. This action restarts the node agent and any started application servers.

- ___ 5. Verify that all of the node agents are up and running in the domain. It is recommended that you stop all application servers during this process. If any node agent fails to restart, run a manual file synchronization utility from the node agent machine to synchronize the security configuration from the deployment manager. Otherwise, the malfunctioning node agent does not communicate with the deployment manager after security is enabled on the deployment manager. This step consists of going to the physical node and running the client `syncNode` command. This client logs into the Deployment Manager and pulls down all of the configuration files to the node agent. This action ensures that the configuration is security-enabled. To resynchronize, complete the following:

- ___ a. If the node agent is started, but not communicating with the Deployment Manager, stop the node agent by issuing a command:

```
stopServer
```

If security is enabled on this node agent, issue the command in the `<installation_root>/AppServer/bin` directory:

```
stopNode -username <administrative_user_name> -password
<administrative_password>
```

The `administrative_user_name` is the administrative user configured for the user registry.

UNIX system: `/opt/WebSphere/AppServer/bin/stopNode.sh -username <administrative_user_name> -password <administrative_password>`

- ___ b. Issue the command:

```
syncNode CELL_HOST 8879 -username <administrative_user_name> -
password <administrative_password>
```

The `CELL_HOST` is the host name where the Deployment Manager resides. The port **8879** is the default SOAP connector port. If that port number has changed, you must specify the changed port. The `administrative_user_name` is the administrative user configured for the user registry.

- ___ c. Restart the node agent by issuing the following command: `startNode`

UNIX system: `/opt/WebSphere/AppServer/bin/startNode.sh`

- ___ 6. Restart all application servers on each node agent. If you have not already stopped your application servers before performing these steps, restart them now. To restart application servers on a node agent (they must already be started), go to **System Administration > Node Agents**. Click a node agent and select **Restart all Servers on Node**. If all servers already are stopped, start the servers by going to **Servers > Application Servers** and selecting the servers that you want to start. Click **Start**.

___ 7. If you go to **System Management > Nodes** and the status of the node is Unknown, go to that node and physically stop and restart the node agent.

___ a. To stop the node agent, issue the following command: `stopNode -username <administrative_user_name> -password <administrative_password>`

___ b. To start the node agent, issue the following command: `startNode`

UNIX system: `/opt/WebSphere/AppServer/bin/stopNode.sh -username <administrative_user_name> -password <administrative_password>`

Testing the configuration

After restarting the server in secure mode, run a couple of simple tests to verify that most facets of security are working properly.

___ 1. Test basic authentication with snoop by accessing the following URL:
`http://hostname.domain:9080/snoop`. A login panel appears. Type in any valid user ID and password in your configured user registry. If the login panel fails to appear, there is a problem.

Note: The snoop servlet is only available in the domain if you included the `DefaultApplication` when adding the application server to the cell. The `-includeapps` option for the `addNode` command migrates `DefaultApplication` to the cell. Otherwise, skip this test.

___ 2. Test form login by bringing up the administrative console:
`http://hostname.domain:9090/admin`. A form-based login page appears. Type in the administrative user ID and password that was used for configuring your user registry when configuring security. If the login panel fails to appear, there is a problem.

Security Problem Determination

If you encountered a problem with any of those tests, check the WebSphere Application Server `/logs/server_name/SystemOut.log` file for hints about the problems that occurred. There are no special requirements to view this log. It is located in the `installation_directory/logs/applicationServerName` directory, and by default is named `SystemOut.log`.

Network Deployment: If you have any problems restarting the node agents or application servers, review the output logs in the `WAS/logs/nodeagent` or `WAS /logs/server_name` directory, respectively.

There are two techniques that you can use to view the log for an application server.

- ___ 1. View the JVM log from the administrative console.
 - ___ a. Start the administrative console.
 - ___ b. Click **Troubleshooting > Logs and Trace** in the console navigation tree. To view the logs for a particular server, click on the server name to select it, and then click **JVM Logs**.
 - ___ c. Select the runtime tab.
 - ___ d. Click **View** corresponding to the log you want to view.
- ___ 2. View the log from the machine where they are stored.
 - ___ a. Go to the machine where the logs are stored.
 - ___ b. Open the file in a text editor or drag and drop the file into an editing and viewing program.

➤ **Did security appear to initialize properly?**

A lot of security code is visited during initialization so you will likely see problems there first if the problem is configuration related. The following sequence of messages generated in the `SystemOut.log` indicates normal code initialization of an application server in which the security service has started successfully:

This sequence will vary based on the configuration, but the messages are similar:

```
SASRas      A JSAS0001I: Security configuration initialized.
SASRas      A JSAS0002I: Authentication protocol: CSIV2/IBM
SASRas      A JSAS0003I: Authentication mechanism: SWAM
SASRas      A JSAS0004I: Principal name: MYHOSTNAME/aServerID
SASRas      A JSAS0005I: SecurityCurrent registered.
SASRas      A JSAS0006I: Security connection interceptor initialized.
SASRas      A JSAS0007I: Client request interceptor registered.
SASRas      A JSAS0008I: Server request interceptor registered.
SASRas      A JSAS0009I: IOR interceptor registered.
NameServerImp I NMSV0720I: Do Security service listener registration.
SecurityCompo A SECJ0242A: Security service is starting
UserRegistryI A SECJ0136I: Custom Registry:com.ibm.ws.security.registry.nt.NTLocalDomainRegistryImpl
has been initialized
SecurityCompo A SECJ0202A: Admin application initialized successfully
SecurityCompo A SECJ0203A: Naming application initialized successfully
SecurityCompo A SECJ0204A: Rolebased authorizer initialized successfully
SecurityCompo A SECJ0205A: Security Admin mBean registered successfully
SecurityCompo A SECJ0243A: Security service started successfully
SecurityCompo A SECJ0210A: Security enabled true
```

The following is an example of messages from a server which cannot start the security service. In this case the administrative user ID and password were given to communicate with the user registry is wrong, or the user registry itself is down or misconfigured:

```
SASRas      A JSAS0001I: Security configuration initialized.
SASRas      A JSAS0002I: Authentication protocol: CSIV2/IBM
SASRas      A JSAS0003I: Authentication mechanism: SWAM
SASRas      A JSAS0004I: Principal name: MYHOSTNAME/aServerID
SASRas      A JSAS0005I: SecurityCurrent registered.
SASRas      A JSAS0006I: Security connection interceptor initialized.
SASRas      A JSAS0007I: Client request interceptor registered.
SASRas      A JSAS0008I: Server request interceptor registered.
SASRas      A JSAS0009I: IOR interceptor registered.
NameServerImp I NMSV0720I: Do Security service listener registration.

SecurityCompo A SECJ0242A: Security service is starting
UserRegistryI A SECJ0136I: Custom Registry:com.ibm.ws.security.
registry.nt.NTLocalDomainRegistryImpl has been initialized
Authentication E SECJ4001E: Login failed for badID/<null> javax.security.auth.login.LoginException:
authentication failed: bad user/password
```

If none of these steps solves the problem, check to see if the problem has been identified and documented using the links in **Troubleshooting security configurations** section of the Websphere Application Server Information Center:

http://publib.boulder.ibm.com/infocenter/ws51help/topic/com.ibm.websphere.base.doc/info/aes/ae/tsec_trouble.html

If you do not see a problem that resembles yours, or if the information provided does not solve your problem, contact **IBM support** for further assistance:

<http://www-1.ibm.com/support/docview.wss?rs=180&context=SSEQTP&uid=swg21145599>

Reference:

- **WebSphere Application Server Information Center Version 5**

<http://www-306.ibm.com/software/webservers/appserv/infocenter.html>

- **IBM WebSphere V5.0 Security Handbook**

<http://www.redbooks.ibm.com/redbooks/SG246573.html>

Trademarks and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	iSeries	OS/400	Informix	WebSphere
IBM(logo)	pSeries	AIX	Cloudscape	MQSeries
e(logo)business	xSeries	CICS	DB2 Universal Database	DB2
Tivoli	zSeries	OS/390	IMS	Lotus

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.

This page is left intentionally blank.