Rational. Directory Server

IBM.

Administration Guide

IBM Rational Directory Server

Administration Guide

Release 5.1

Before using this information, be sure to read the general information under Appendix, "Notices"on page 23.

This edition applies to **VERSION 5.1, IBM Rational Directory Server** and to all subsequent releases and modifications until otherwise indicated in new editions.

Table of contents

1 About this manual

This manual guides you through the IBM® Rational® Directory Server (RDS) administration. This document contains step-by-step instructions for administering the RDS.

RDS documentation

This section provides the information on the related documents available for RDS. The following RDS documents are available on the Product Support Web site, http://www.ibm.com/software/rational/support/.

Document name	Description
IBM Rational Directory Server Installation Guide	Provides information on how to install the RDS.
IBM Rational Directory Server Product Manual	Provides detailed information on RDS features supported in this release.

Contacting IBM Rational Software Support

If the self-help resources have not provided a resolution to your problem, you can contact IBM® Rational® Software Support for assistance in resolving product issues.

Note If you are a heritage Telelogic customer, a single reference site for all support resources is located at http://www.ibm.com/software/rational/support/telelogic/

Prerequisites

To submit your problem to IBM Rational Software Support, you must have an active Passport Advantage® software maintenance agreement. Passport Advantage is the IBM comprehensive software licensing and software maintenance (product upgrades and technical support) offering. You can enroll online in Passport Advantage from http://www.ibm.com/software/lotus/passportadvantage/howtoenroll.html

- To learn more about Passport Advantage, visit the Passport Advantage FAQs at http://www.ibm.com/software/lotus/passportadvantage/brochures_faqs_quickguides.html.
- For further assistance, contact your IBM representative.

To submit your problem online (from the IBM Web site) to IBM Rational Software Support, you must additionally:

- Be a registered user on the IBM Rational Software Support Web site. For details about registering, go to http://www.ibm.com/software/support/.
- Be listed as an authorized caller in the service request tool.

Submitting problems

To submit your problem to IBM Rational Software Support:

1. Determine the business impact of your problem. When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting.

Use the following table to determine the severity level.

Severity	Description
1	The problem has a *critical* business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
2	This problem has a *significant* business impact: The program is usable, but it is severely limited.
3	The problem has *some* business impact: The program is usable, but less significant features (not critical to operations) are unavailable.
4	The problem has *minimal* business impact: The problem causes little impact on operations or a reasonable circumvention to the problem was implemented.

2. Describe your problem and gather background information, When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Rational Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:
   - What software versions were you running when the problem occurred?

     To determine the exact product name and version, use the option applicable to you:

     - Start the IBM Installation Manager and select **File** > **View Installed Packages**. Expand a package group and select a package to see the package name and version number.
     - Start your product, and click **Help** > **About** to see the offering name and version number.
   - What is your operating system and version number (including any service packs or patches)?
   - Do you have logs, traces, and messages that are related to the problem symptoms?
   - Can you recreate the problem? If so, what steps do you perform to recreate the problem?

- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, or other system components?
- Are you currently using a workaround for the problem? If so, be prepared to describe the workaround when you report the problem.

3. Submit your problem to IBM Rational Software Support. You can submit your problem to IBM Rational Software Support in the following ways:
   - **Online**: Go to the IBM Rational Software Support Web site at https://www.ibm.com/software/rational/support/ and in the Rational support task navigator, click **Open Service Request.** Select the electronic problem reporting tool, and open a Problem Management Record (PMR), describing the problem accurately in your own words.

     For more information about opening a service request, go to http://www.ibm.com/software/support/help.html

     You can also open an online service request using the IBM Support Assistant. For more information, go to http://www.ibm.com/software/support/isa/faq.html.
   - **By phone**: For the phone number to call in your country or region, go to the IBM directory of worldwide contacts at http://www.ibm.com/planetwide/ and click the name of your country or geographic region.
   - **Through your IBM Representative**: If you cannot access IBM Rational Software Support online or by phone, contact your IBM Representative. If necessary, your IBM Representative can open a service request for you. You can find complete contact information for each country at http://www.ibm.com/planetwide/.

Conventions used in this guide

Typeface	Description
Italic	Used for book titles and terminology.
Bold	Used for items that you can select and menu paths, also used for emphasis.
`Courier`	Used for commands, file names, and directory paths. Represents command syntax to be entered verbatim. Signifies computer output that displays on-screen.
`Courier Italic`	Represents values in a command string that you supply. For example, `(drive:\username\commands)`.

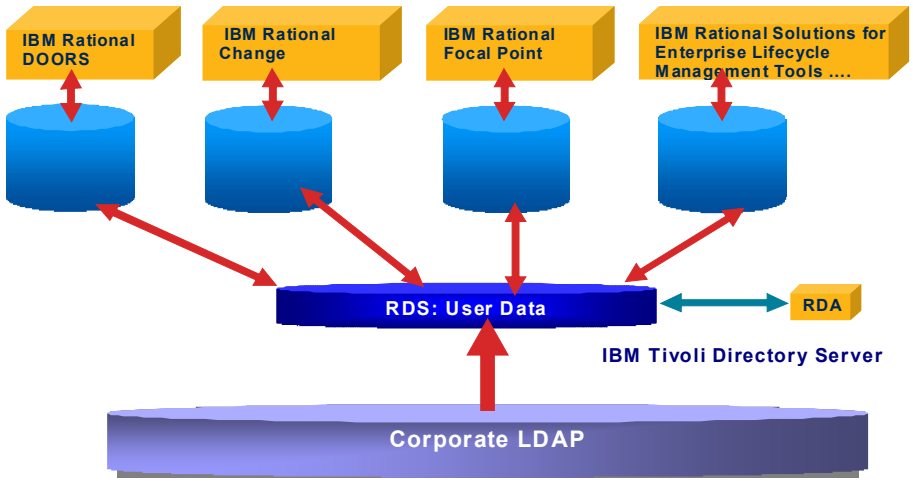
2 Introduction

The RDS is a single enterprise directory solution designed for user authentication and administration for IBM® Rational® Solutions for Enterprise Lifecycle Management tools. RDS allows the users to log on using the same credentials across IBM® Rational® Solutions for Enterprise Lifecycle Management tools for which they have authorized access.

RDS 5.1 supports a wide range of platforms. For more information about the platform support, see the *IBM Rational Directory Server Installation Guide*.

RDS architecture

The following diagram shows the RDS architecture.



Who should use this guide

This guide is intended for the RDS administrator. The administrator is responsible for the day-to-day operations of the server such as how to run the RDS backup programs and how to recover the directory manager password in case of password loss.

The *IBM Rational Directory Server Administration Guide* contains some of the administration commands and utilities used for administering the RDS. If you are installing the RDS for the first time, refer to the *IBM Rational Directory Server Installation Guide for Windows* located on the Product Support Web site http://www.ibm.com/software/rational/support/ for step-by-step instructions.

3 Directory Server Administration

This chapter describes some of the utilities used for the directory server administration on Windows.

Note The general guidelines specified for IBM® Tivoli® Directory Server 6.2 administration apply. Refer to http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml for details.

Starting the directory server

From the command line, use the following command to start the directory server.

In Windows

```
<RDS_Home>/IBM/Rational/RDS_5.1/RDSUtility/
Start_RDS_Server.bat
```

For example:

```
C:\Program Files\IBM\Rational\RDS_5.1\RDSUtility\
Start_RDS_Server.bat
```

You can also double-click the `Start_RDS_Server.bat` located under the same path to start the server.

Note The RDS is setup as a Windows service, ensuring the server starts up on system reboot.

In UNIX:

On Solaris

```
$ cd <RDS_Home>/RDSUtility
$ ./star_rds_server.sh
```

OR

```
$ ./ibmslapd -I tdsadmin -n
```

On Linux

```
$ cd <RDS_Home>/RDSUtility
$ ./start_rds_server.sh
```

OR

```
$ ./ibmslapd -I tdsadmin -n
```

Stopping the directory server

From the command line, use the following command to stop the directory server.

```
<RDS_Home>/IBM/Rational/RDS_5.1/RDSUtility/
Stop_RDS_Server.bat
```

Windows example:

```
C:\Program Files\IBM\Rational\RDS_5.1\RDSUtility\
Stop_RDS_Server.bat
```

UNIX example:

On Solaris

```
$ cd <RDS_Home>/RDSUtility
$ ./stop_rds_server.sh
```

On Linux

```
$ cd <RDS_Home>/RDSUtility
$ ./stop_rds_server.sh
```

Backing up the Rational Directory Server

Backing up the RDS allows you to save a snapshot of the contents should the data be lost or become corrupt. The RDS backup essentially means the backing up of the IBM Tivoli Directory Server 6.2. The backup can be done on Windows, Solaris, and Linux platforms.

When these backup procedures are followed, the system automatically stores a copy of the server files on the same host. For greater security, copy and store these files on a different machine or file system.

Backing up the data

When you back up the server, all contents of the directory are saved in a backup location. This section tells you how to use the `idsdbback` command to back up the directory.

To back up your directory, do the following:

1. Stop the RDS server.
2. Change directory to the following path.

   ```
   cd <RDS_Home>\IBM\ldap\V6.2\sbin (Windows)
   $ cd /opt/IBM/ldap/V6.2/sbin (Unix)
   ```

3. Set the permission for the backup folder using the following command.

   ```
   $ chown tdsadmin:idsldap /var/backup
   ```

4. Backup the server using the following command.

   ```
   dbback -I instance_name backup directory path
   Example:
   $ dbback -I tdsadmin /var/backup
   ```

5. It prompts for the option. Type 1 to continue or 2 to exit.
6. Start the RDS server.

Note Post Tivoli/DB2 installation on Unix, creation of *tdsadmin* user should be accompanied by setting the user home directory to be the install directory (/ appended with instance). For more information on creating the user see, *IBM Rational Directory Server Installation Guide.*

Restoring the Directory Server

Use the `restore` command to restore the server. Shut the server down before running this script.

To restore your directory, do the following:

1. Stop the RDS server.
2. Restore the backup using the following command:

   ```
   $ dbrestore -I instance_name backup directory path
   Example:
   $ dbrestore -I tdsadmin /var/backup
   ```

3. Start the RDS server.

Note For more information on backup, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.IBMDS.doc/toc.xml.

Authenticating the OS through PAM

The RDS uses Pluggable Authentication Modules (PAM) to authenticate users on Solaris, and LINUX systems. To allow RDS to authenticate the users, the PAM configuration must be updated to specify the authentication methods to use for the *osauth* service, unless a reasonable default already exists.

Refer to the following tables for updating the PAM configuration.

1. On Solaris 10, the following are the example additions to `/etc/pam.conf` file:

`osauth`	`auth`	`sufficient`	`pam_unix_auth.so.1`
`osauth`	`auth`	`requisite`	`pam_authtok_get.so.1`
`osauth`	`auth`	`required`	`pam_unix_auth.so.1`
`osauth`	`account`	`required`	`pam_unix_account.so.1`

Note On Solaris, if the server is running with non-root privileges, ensure that server process can read the `/etc/shadow` file.

2. On Red Hat Linux®, the following are the example additions to the `/etc/pam.d/osauth` file:

`auth`	`sufficient`	`pam_unix.so`	`1ikeauth`	`nullok`
`auth`	`required`	`pam_deny.so`	`-`	`-`
`account`	`required`	`pam_unix.so`	`-`	`-`

3. On SUSE® Linux, the following are the example additions to the `/etc/pam.d/ cmsynergy` file.

`auth`	`sufficient`	`pam_unix.so`
`auth`	`required`	`pam_deny.so`
`account`	`required`	`pam_unix.so`

Note If the *osauth* PAM service is not defined, the default definitions are used. The default definitions are configured with the service name *other*.

On UNIX systems, the Administrator will need to provide read access to the `/etc/shadow` file to *tdsadmin* user (/created during RDS installation) for OS Authentication mode to function.

For example, `$>chmod 444 /etc/shadow`

4. On AIX®, the Base Operating System performs the authentication.

Changing the RDS operation mode

The RDS provides the `rdsconfig` utility to change the RDS operation mode from the command line. The RDS uses the operation mode to perform the authentication. For example, if the operation mode is changed to OS authentication mode, the authentication is done based on the domain name on Windows.

You can change the operation mode by doing the following:

On Windows:

1. On the command line, change the directory path to the following `<RDS_Install>\RDS_5.1\IBM\IBM\Rational\RDS_5.1\RDSUtility`
2. Type `rdsconfig.exe` to run the utility.

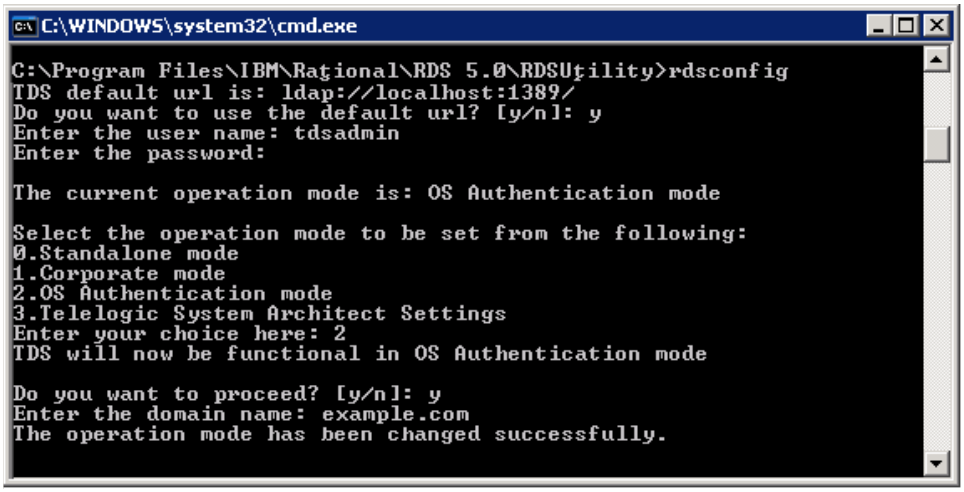
   `For example:`

   `C:\Program Files\RDS_5.1\IBM\Rational\RDS_5.1\RDSUtility\rdsconfig.exe`
3. The default URL for server authentication is displayed.
4. Type the following details as shown in the following example:

Field name	Value
RDS default URL is: ldap://localhost:1389/ Do you want to use the default url? [y/n]:	Type *`y`* to use the default URL or if you type *`n`*, the program asks you to type the RDS url. Type the valid RDS url and press **Enter**. **Note** To open the RDS in secure mode, you can include the letter "s" in the ldap URL (where the "s" refers to the secure port), followed by a valid server name and a port number. For example: `ldaps://dirserv:1636`.
Enter the user name:	*`tdsadmin`*

Enter the password:	Type the *tdsadmin* password. It displays the current operation mode along with the list of operation modes to select from.
Select the operation mode to be set from the following: 0.Standalone mode 1.Corporate mode 2.OS authentication mode 3.Trusted OS Authentication	Enter your choice: `2`
Do you want to proceed? [y/n]:	Type `y` to proceed
Enter the domain name:	`example.com`

Once you have entered all the details, the operation mode is changed and the message for successful mode change appears.



Note Whenever the operation mode is changed, the **Web server** needs to be restarted.

If the operation mode is changed from **Stand-Alone** to **Corporate**, the users must be migrated as corporate users.

5. Restart the RDS.

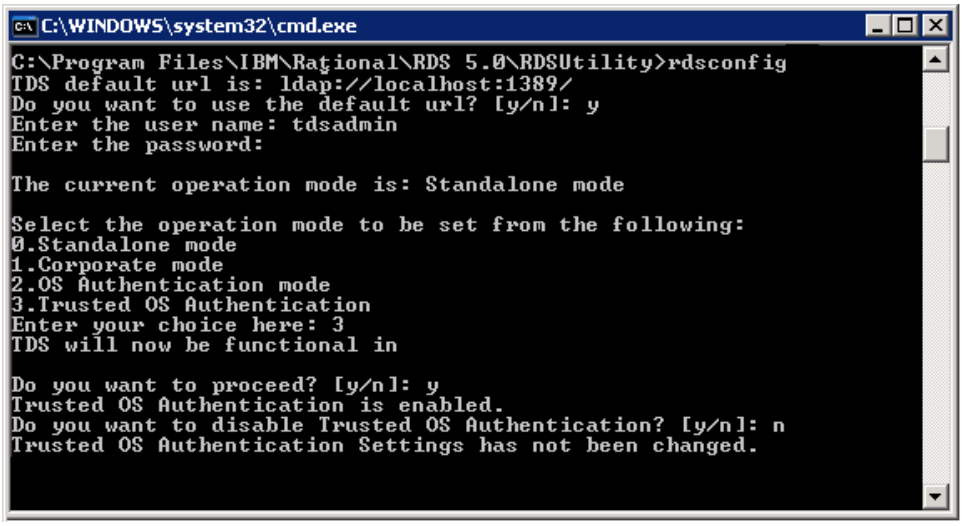
Trusted OS authentication settings

The RDS additionally supports specific settings for the IBM® Rational® System Architect®, and IBM® Rational® Synergy tools. The System Architect tool by default uses the Trusted Operating System (OS) authentication. The Trusted OS setting is enabled by default within RDS.

This configuration is designed to allow the IBM Rational System Architect and IBM Rational Synergy tool to use the existing OS authentication to log on to the RDS. The user is not prompted for user login dialog for tool connectivity to RDS.

Use the `rdsconfig` utility to enable or disable the Trusted OS authentication. For more details, see Changing the RDS operation mode section.

The image below shows an example of this setting.



Note When the Trusted OS authentication is disabled, the RDS login dialog box appears.

Settings for assigning license feature

This section describes the settings that must be done for assigning the license features to users.

Standalone mode

The users must have their NT logon name or UNIX logon name configured in RDS to assign a license feature.

Corporate mode

The attribute `CORPORATE_LICENSING_FEATURE_LOGON_ATTRIBUTE` is configured in **TDSConfiguration.xml** file. By default, the value for this attribute is set to `samAccountName` for Active Directory Server corporate partition.

For other corporate partitions such as the IBM Tivoli Directory Server, the administrator must configure this value to a valid system login name (For example, uid).

Enabling Secure Sockets Layer (SSL) security

The following section describes the steps for enabling the SSL security. To enable the secure connectivity between the Rational tools such as IBM® Rational® DOORS®, IBM® Rational® System Architect® and the Active Directory Server, follow steps given in the following sections.

Exporting the certificate from the Active Directory server

To export the CA certificate from the Active Directory server, follow these steps:

1. Log on as a Domain Administrator to the Active Directory domain server that is being used to create the RDS partition.
2. Export the certificate from the Active Directory server to a file. To do so, follow these steps:
   a. Click **Start>Control Panel> Administrative Tools>Certificate Authority** to open the CA Microsoft® Management Console (MMC) GUI.
   b. Highlight the CA machine and right-click to select **Properties** for the CA.
   c. From **General** menu, click **View Certificate**.
   d. Select the **Details** view, and click the **Copy to File** button on the lower-right corner of the window.
   e. Use the **Certificate Export** Wizard to save the CA certificate in a file.

Note You can save the CA certificate in either DER Encoded Binary X-509 format or Based-64 Encoded X-509 format.

Importing the certificate to the IBM Rational products

You must import the certificate to each IBM Rational tools such as DOORS, System Architect etc. You need IBM JRE 1.5.1 to configure the SSL.

To import the CA certificate to the IBM Rational products, follow these steps:

On Windows:

- Run the following command to import the certificate for `.cer, .crt` files:

```
<GSkit Install path>/ibm/gsk7/bin/gsk7cmd.exe -cert  -add -db
<Gskit Install path>/lib/certdb/tdsclientkey.kdb -pw
tdskey4client -label My_LABEL -file <extracted certificate
file>
```

- Run the following command to import the certificate for `.jks` files:

  ```
  gsk7cmd -cert -import -db <filename> -pw <password> -label
  "mylabel" -target tdsclient.kdb -target_pw  tdskey4client
  ```

  where:

  `-db <filename>` is the name of the database.

  `-pw <password>` is the password to access the key database.

- The SSL setup is complete.

On Solaris:

- Run the following command to import the certificate:

  ```
  /opt/ibm/gsk7/bin/gsk7cmd -cert -add -db tdsclientkey.kdb -pw
  tdskey4client -label My_LABEL -file <extracted
  certificate.cer file>
  ```

- The SSL setup is complete.

Note GSkit can be installed along with the RDS or separately.

For more details on enabling the SSL security, see http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itame.doc/am61_install318.htm.

4 Troubleshooting RDS

This chapter describes the possible problem and solutions for RDS users.

Problem	Solution
Changing or resetting the password with Non-ASCII characters does not work.	Changing or resetting the password with Non-ASCII characters are not supported by RDS.
Web RDA cannot be used for License Configuration on Solaris platform.	License Configuration on Web RDA does not function with RDA Web Access Server installed on Solaris. The RDA Web Access Server needs to be installed on Windows or Linux platforms to achieve the license configuration functionality.
Users cannot login after migration.	The RDS server needs to be restarted otherwise the data inconsistency is observed. For more information on starting the server, see Starting the directory server (page 9).

Appendix: Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send written license inquiries to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send written inquiries to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions. Therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Intellectual Property Dept. for Rational Software
IBM Corporation
1 Rogers Street
Cambridge, Massachusetts 02142
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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 and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.html

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

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product or service names may be trademarks or service marks of others.

Index