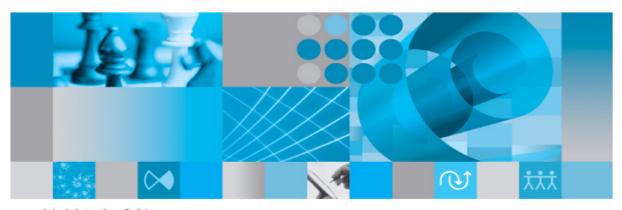**Rational.** Directory Server

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 19.

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 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.

Frequently Asked Questions

1. *Which are the external LDAP servers supported by RDS?*

   Sun Java^(tm) System Directory Server and Microsoft^(r) Active Directory Server.

2. *What is the schema required by RDS in the external corporate server?*

   The user information are extracted from the corporate servers based on the `person/inetOrgPerson` schema class and the primary attributes `cn, sn, email, uid, givenname, telephoneNumber, mail, facsimileTelephoneNumber, description, postalAddress, and sAMAccountName.`

   The group information are extracted based on the `group/groupOfUniqueNames` schema class and the attributes `member/uniqueMember, description`.

3. *Do we need an Administrator privileges to create a partition?*

   You need a corporate LDAP server user with a *Read* access to the search bases specified in the partition.

4. *Is the Apache Server installed as a service?*

   No. This functionality will be added in a future release.

5. *I cannot use RDA on Solaris to create a partition with SSL enabled?*

   This is a known limitation. You need to install RDA on Windows as a workaround.

6. *Why DOORS do not show up a user after changing the name of the user from one ou to another in the corporate LDAP?*

If the name of a user (firstname, lastname, cn etc.) is changed keeping the same UID, or if a user is moved from one OU to another in the corporate LDAP, DOORS may not show up the user. The reason is, the RDS has already created an extended user object with the `uid` as the user logon name (based on the logon attribute selected in the corporate partition) and `tdsCorporateDn` as the corporate DN of the user. If the corporate DN of the user changes in the corporate LDAP server, RDS will try to recreate the extended user object with the same user logon name (which is not changed in corporate LDAP) and would fail, as the user object with the same logon name already exists in the corporate LDAP. Hence, the particular user would not be shown in DOORS.

To solve this issue, it is recommended to modify the required attributes of the extended user object in RDS. Deleting the extended user object also solves the issue but it may delete the DOORS specific values for that user object, which may lead to information loss.

7. *Will error opening *.cat files messages affect functionality of RDS 5.1 for Tivoli in anyway?*

No. You can ignore such error messages, they keep coming because of a minor localization issue with Tivoli which will no way affect RDS and its functionalities.

8. *Is RDS supported on VMWare?*

Currently, the RDS is not supported on a virtual environment.

9. *I installed RDS as user root, is there a way to start the Apache version of the Rational Directory Server as any other user then root?*

This can be accomplished by changing the group and ownership to another user. Run the following command from within the `...IBM/Rational`

```
chown ccm_root RDS_5.X -R

chgrp ccm_root RDS_5.X -R

chown ccm_root RDA_5.X -R

chgrp ccm_root RDA_5.X -R
```

After the permissions have been changed, start the RDS and RDA Web server as user `ccm_root`.

10. *How do you change the Webserver port from 8080 to any other values for IBM Rational Directory Administration (RDA)?*

To change the default port number:

a. Edit the following lines in the `Server.xml` file located under <RDS_HOME/RDA_HOME>\WebAccessServer\apache-tomcat-6.0.16 (-6.0.24 for 5.1.0.1 and 5.1.0.2)\conf folder:

```
Connector port="8090" protocol="HTTP/1.1"
connectionTimeout="20000"
redirectPort="8443" />
<!-- A "Connector" using the shared thread pool-->
```

b. Restart the RDA for the changes to take effect.

Note The new port number is changed to 8090 in the above example.

3 *Directory Server Administration*

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

Administrator User

After RDS is installed, a *Directory Administrator* group is created. You can add users to this group.

The directory administrator is a superuser with all rights for administering the server. The users added to this group becomes the administrator, and can perform maintenance operations, such as backup, recovery, and so forth.

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/rdsctl.bat start
```

For example:

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

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

In UNIX:

On Solaris

```
$ cd <RDS_Home>/RDSUtility
$ ./rdsctl.sh start
```

On Linux

```
$ cd <RDS_Home>/RDSUtility
$ ./rdsctl.sh start
```

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/rdsctl.bat stop`

Windows example:

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

UNIX example:

On Solaris

```
$ cd <RDS_Home>/RDSUtility
$ ./rdsctl.sh stop
```

On Linux

```
$ cd <RDS_Home>/RDSUtility
$ ./rdsctl.sh stop
```

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 Apache Directory Server. 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. You can backup the data online, while the server is running.

To back up your directory, do the following:

1. Stop the RDS server.

2. Change directory to the following path.

   ```
   cd <RDS_Home>\RDSUtility
   ```

3. Backup the server using the following command. Make sure that the backup directory does not exist.

   - `backup.cmd <backup_directory_path> (Windows)`
   - `backup.sh <backup_directory_path> (Unix)`

   Example on Windows:

   backup.cmd c:\rds_backup

   Example on Unix:

   $ backup.sh /var/rds_backup

4. Start the RDS server.

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. Change directory to the following path.

   ```
   cd <RDS_Home>\RDSUtility
   ```

3. Restore the backup using the following command:

    - `restore.cmd <backup_directory_path> (Windows)`
    - `restore.sh <backup_directory_path> (Unix)`

    Example on Windows:

    restore.cmd c:\rds_backup

    Example on Unix:

    $ restore.sh /var/rds_backup

4. Start the RDS server.

Note On Unix, set the execute permission to the `backup.sh` and `restore.sh` files. For example, `chmod +x backup.sh.`

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 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 example additions to `/etc/pam.conf` file:

osauth	auth	required	pam_dhkeys.so.1
osauth	auth	required	pam_unix_auth.so.1
osauth	account	requisite	pam_roles.so.1
osauth	account	required	pam_projects.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 example additions to the `/etc/pam.d/osauth` file:

auth	required	/lib/security/pam_stack.so service=system-auth
auth	required	/lib/security/pam_nologin.so
account	required	/lib/security/pam_stack.so service=system-auth

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

4. On IBM-AIX, the Base Operating System performs the authentication.

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`

Changing the RDS operation mode

Post installation, after the data is created in RDS, the operation mode change using the `rdsconfig` utility is not supported.

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 Apache Directory Server, the administrator must configure this value to a valid system login name (For example, uid).

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 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).
When the RDS in corporate mode is configured to DOORS, the users are displayed in RDA but not in DOORS.	If a custom attribute name is used in the corporate user DN, the custom DN attribute name should be added to the RDS schema. To add the custom DN: 1. Create the following script. ``` dn: cn=schema changetype: modify add: attributetypes attributeTypes: (1.3.6.1.4.1.15265.0.100 NAME '<custom_attribute_name>' SYNTAX 1.3.6.1.4.1.1466.115.121.1.27 SINGLE-VALUE) ``` 2. Save the script in a text file with the file extension as `<filename>.ldif`. 3. Use the `ldapmodify` command to apply the schema change.

Appendix: Notices

© Copyright 2000, 2010

U.S. Government Users Restricted Rights - Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

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.

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

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Index

B

backing up the data 11

I

IBM Customer Support 1
installation guide 6

L

license configuration on solaris 17
license feature settings 15

O

operation mode change 14
OS authentication 13

P

PAM 13
password with non-ascii 17

R

RDS architecture 5
restore server 11
restoring the data 11

S

server backup 11
starting the directory server 9
starting the server 9
stopping the directory server 10
stopping the server 10

U

using PAM 13

W

who should use this guide 6