AUTHORIZED DOCUMENTATION

Implementation Guide

Novell®
Identity Manager Driver for Mainframes: RACF*

3.6.1

June 5, 2009

www.novell.com

Legal Notices

Novell, Inc. and Omnibond Systems, LLC. make no representations or warranties with respect to the contents or use of this documentation, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems, LLC. reserve the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, Novell, Inc. and Omnibond Systems, LLC. make no representations or warranties with respect to any software, and specifically disclaim any express or implied warranties of merchantability or fitness for any particular purpose. Further, Novell, Inc. and Omnibond Systems, LLC. reserve the right to make changes to any and all parts of the software, at any time, without any obligation to notify any person or entity of such changes.

Any products or technical information provided under this Agreement may be subject to U.S. export controls and the trade laws of other countries. You agree to comply with all export control regulations and to obtain any required licenses or classification to export, re-export, or import deliverables. You agree not to export or re-export to entities on the current U.S. export exclusion lists or to any embargoed or terrorist countries as specified in the U.S. export laws. You agree to not use deliverables for prohibited nuclear, missile, or chemical biological weaponry end uses. See the the Novell International Trade Services Web page (http://www.novell.com/info/exports/) for more information on exporting Novell software. Novell assumes no responsibility for your failure to obtain any necessary export approvals.

Novell, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed on the Novell Legal Patents Web page (http://www.novell.com/company/legal/patents/) and one or more additional patents or pending patent applications in the U.S. and in other countries.

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see the Novell Documentation Web page (http://www.novell.com/documentation).

Novell Trademarks

For Novell trademarks, see the Novell Trademark and Service Mark list (http://www.novell.com/company/legal/trademarks/tmlist.html).

Third-Party Materials

All third-party trademarks are the property of their respective owners.

Contents

About This Guide

This guide describes implementation of the Novell® Identity Manager 3.6.1 driver for RACF on mainframes (z/OS* operating system).

The driver synchronizes data from a connected mainframe system using RACF with Identity Manager, the comprehensive identity management suite that allows organizations to manage the full user life cycle, from initial hire, through ongoing changes, to ultimate retirement of the user relationship.

This guide includes the following sections:

Audience

This guide is for system administrators and others who plan, install, configure, and use the Identity Manager Driver for RACF on z/OS. It assumes that you are familiar with Identity Manager, Novell eDirectory™, and the administration of systems and platforms you connect to Identity Manager.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation, or go to the Novell Documentation Feedback site (http://www.novell.com/documentation/feedback.html) and enter your comments there.

Documentation Updates

For the most recent version of this guide, visit the Identity Manager 3.6.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm36drivers).

Additional Documentation

For additional documentation about Identity Manager drivers, see the Identity Manager 3.6.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm36drivers).

For additional documentation about Identity Manager, see the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

For documentation about other related Novell products, such as eDirectory and iManager, see the Novell Documentation Web site’s product index (http://www.novell.com/documentation).

Documentation Conventions

In Novell documentation, a greater-than symbol (>) is used to separate actions within a step and items in a cross-reference path.

A trademark symbol (®, ™, etc.) denotes a Novell trademark. An asterisk (*) denotes a third-party trademark.

When a single pathname can be written with a backslash for some platforms or a forward slash for other platforms, the pathname is presented with a backslash. Users of platforms that require a forward slash, such as Linux* or UNIX*, should use forward slashes as required by your software.

RACF Driver Overview

1

The Novell® Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system) synchronizes data between the Identity Vault and a connected system running RACF. The driver runs on the target z/OS system. The Identity Vault runs on any Identity Manager supported platform and communicates with the driver on the target z/OS system over a secure network link.

The driver gives you access to RACF user and group attributes through the z/OS RACF schema. The driver also allows you to issue arbitrary TSO commands on the z/OS system. Identity Manager gives you access to eDirectory™ objects and their attributes.

This section includes the following major topics:

1.1 Component Introduction

An Identity Manager driver package includes

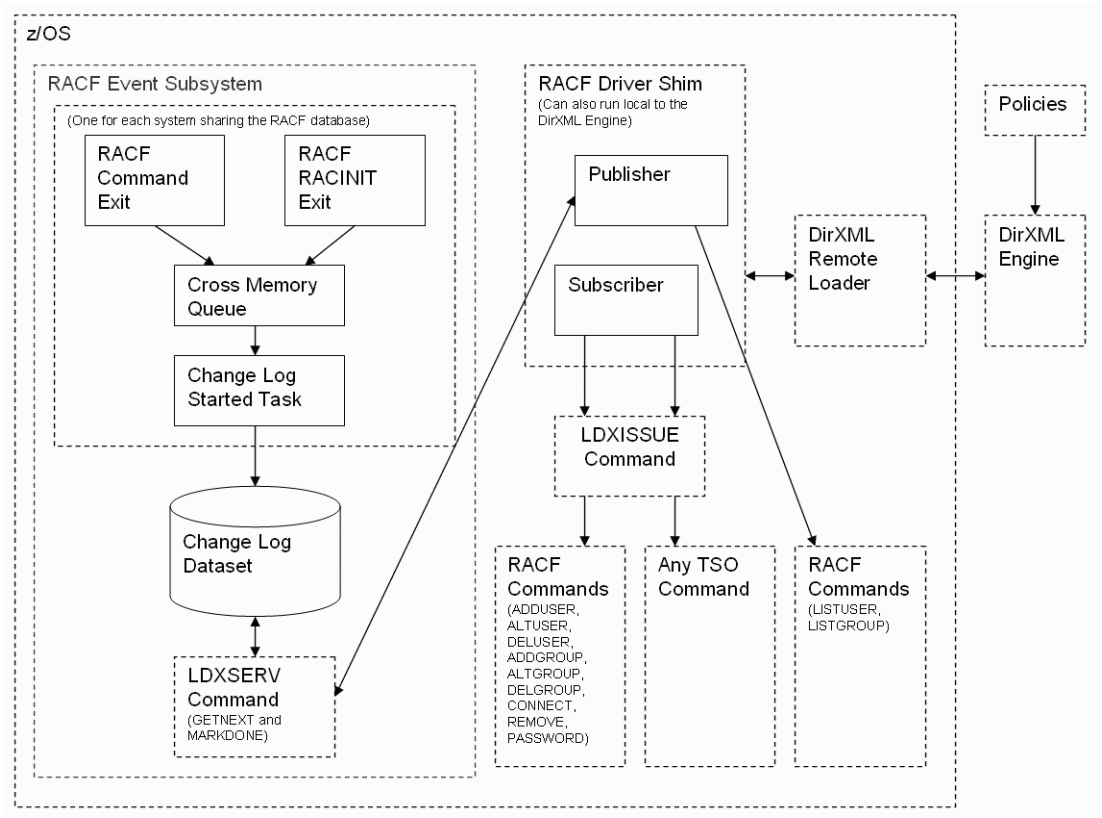
- **The Identity Manager driver shim:** The driver shim serves as an interface between the Identity Manager engine and the application. The Identity Manager driver shim contains two channels: the Subscriber channel and the Publisher channel.
- **A starter set of sample policies and filters:** Policies and filters are used by the Identity Manager engine to control the bidirectional flow of data between eDirectory and the driver shim.

The z/OS RACF driver includes these components. The z/OS RACF driver package also includes the *RACF Event Subsystem*. The RACF Event Subsystem captures RACF events of interest, and provides the application interface to the Publisher and Subscriber channels.

1.2 Component Details

This section describes the components of the z/OS RACF driver package. Topics include

Figure 1-1 *Component Overview*



1.2.1 RACF Event Subsystem

The RACF Event Subsystem uses standard RACF exits to capture events of interest and place them on a *cross memory queue*. The *Change Log Started Task* moves events to the *Change Log data set*. The LDXSERV TSO command provides the Publisher channel with access to the Change Log data set. The LDXISSUE TSO command is used by the Subscriber channel to issue TSO commands and capture their output.

RACF Exits

The RACF exits detect RACF activity of interest and place events in a cross memory queue. When the RACF exits place an event in the cross memory queue, they notify the Change Log Started Task. The Change Log Started Task then moves the event to the Change Log data set.

Each system that shares a RACF database must run the RACF Event Subsystem RACF exits.

The Common Command exit: Receives control when a RACF command is issued. The RACF Event Subsystem uses this exit to create an event for commands that affect users or groups.

The RACROUTE REQUEST=VERIFY(X) (RACINIT) postprocessing exit: Receives control after user verification. The RACF Event Subsystem uses this exit to create an event when a user changes the password upon logging on to the system.

Cross Memory Queue

The cross memory queue is an in-storage buffer that holds events. Events are added to the cross memory queue by the RACF exits, and removed from the queue by the Change Log Started Task. The cross memory queue is located in Subpool 231 (fetch-protected ECSA).

Change Log Started Task

The Change Log Started Task is notified of events added to the cross memory queue by the RACF exits, and moves them to the Change Log data set.

Each system that shares a RACF database must run the Change Log Started Task. The Change Log Started Task must be started as part of your normal z/OS system initialization procedure and stopped during normal system shutdown.

Change Log Data Set

The Change Log data set stores events for processing by the Publisher channel.

The Change Log data set is a standard z/OS direct access (DSORG=DA) data set. There is one Change Log data set for the set of systems that share a RACF database. The Change Log data set must reside on a shared device unless the RACF database is not shared.

LDXSERV TSO Command

LDXSERV is an APF-authorized TSO command that is used by the driver through a Telnet interface to access and control the RACF Event Subsystem.

The Publisher channel calls LDXSERV to retrieve the next event from the Change Log data set, and to mark an event complete after processing is finished.

The Subscriber channel calls LDXSERV upon startup to identify itself to the RACF command exit. This prevents the RACF command exit from generating events for RACF commands issued by the Subscriber channel (loopback).

Syntax

```
LDXSERV [ STATUS | GETNEXT | MARKDONE EVENTID(token) | NOLOG | LOG ]
```

`STATUS`: Reports the status of the RACF Event Subsystem in an XML document.

`GETNEXT`: Obtains the next event from the Change Log data set.

`MARKDONE`: Marks the designated event complete in the Change Log data set.

`NOLOG`: Causes the RACF command exit to not log events for commands that originate from the current address space. The Subscriber channel issues this command at logon to prevent loopback.

`LOG`: Removes the address space token that prevents RACF commands from being logged.

LDXISSUE TSO Command

LDXISSUE is a TSO command that is used by the Subscriber channel through a Telnet interface to issue commands and capture their output.

Syntax

```
LDXISSUE command
```

LDXISSUE executes the supplied TSO command, and returns the command output and return code in an XML document.

1.2.2 Publisher Channel

The Publisher channel obtains RACF events from the Change Log data set, encodes them as XDS documents, and passes them to the Identity Manager engine. The Publisher channel marks events complete in the Change Log data set after they have been processed.

The Publisher channel accesses the Change Log data set by issuing LDXSERV TSO commands through a Telnet interface. A logon ID with appropriate authority is required for the Telnet interface.

1.2.3 Subscriber Channel

The Subscriber channel receives XDS command documents for users and groups from the Identity Manager engine, converts them to RACF TSO commands, and executes them.

The Subscriber channel does not perform validation of attribute values in the XDS command document. If the requirements of RACF are not met, the results of the RACF commands are unpredictable.

The Subscriber channel can also execute arbitrary TSO commands generated in the Command class by the policies. For details, see “Using the Subscriber Channel Command Class” on page 44.

The Subscriber channel uses the LDXISSUE command through a Telnet interface to issue TSO commands. A logon ID with appropriate authority is required for the Telnet interface.

1.2.4 The z/OS RACF Schema

The Identity Manager 3.6.1 driver for RACF uses the z/OS RACF schema to describe the attributes of user and group profiles in RACF. For a description of the z/OS RACF schema, see Section A.1, “z/OS RACF Schema,” on page 57. For a description of how attributes in the z/OS RACF schema relate to RACF command parameters, see Section A.2, “RACF Command Parameter Mapping,” on page 68 and Section A.3, “Driver Processing of Attributes and Commands,” on page 84.

1.2.5 Auxiliary Classes

The Identity Manager Driver for z/OS RACF provides auxiliary classes to add z/OS RACF schema attributes to User and Group objects in eDirectory. You can use the driver to maintain the RACF attributes between corresponding users and groups in RACF and eDirectory.

1.2.6 Configuration

The behavior of an Identity Manager driver is governed by its configuration of options, policies, and filters. The configuration of the z/OS RACF driver is stored in its driver object in eDirectory.

A preconfigured starter set of sample policies is provided with the Identity Manager driver for z/OS RACF. You must customize these as appropriate for your needs.

For a description of the processing of the sample policies, see Section 1.4, "Processing Description," on page 16. For details about customizing the driver, see Chapter 3, "Customizing the Driver," on page 41.

1.3 Differences between eDirectory and RACF

There are major differences in the way information is organized and processed between eDirectory and RACF.

For example, there is not a one-to-one correspondence between the eDirectory and RACF representations of users, groups, and group membership.

In eDirectory, users are represented by User objects. Groups are represented by Group objects. User objects have a Group Membership attribute that lists the groups the user belongs to. Group objects have a Member attribute that includes the users that belong to it. When a user is added to a group, both objects are modified.

In RACF, users are represented by a *user profile*. Groups are represented by a *group profile*. Users and groups are associated by a *connect profile*. User profiles do not contain a list of the groups the user belongs to. Ordinary groups contain a list of all of their members, but universal groups do not.

This disparity places requirements on the way the driver processes events for users and groups. For example, when a user is added to a group in eDirectory, a RACF CONNECT command must be issued to perform the equivalent change in RACF.

RACF connect profiles have attributes that have no direct counterpart in eDirectory. These attributes control some of the privileges a user has when connected to the group. For example, a user can be designated as a security auditor for the group.

The z/OS RACF driver specifies a default set of attributes when creating connect profiles. You can change the way that connect profiles are created by modifying the Output transformation.

While eDirectory is hierarchical, RACF is flat—there is no concept of a move function. RACF provides no rename function. The Subscriber channel rejects move and rename commands. The sample Subscriber Event policy vetoes move and rename events. You can change this policy to perform installation-specific processing of move or rename events if required.

RACF does not perform any implicit cleanup activity when user profiles or group profiles are deleted. RACF installations typically perform special cleanup processing periodically to remove users and groups that are no longer used. The sample Subscriber Event policy vetoes delete group events and converts delete user events into a RACF revoke. You can modify these actions as appropriate for your installation.

Much of the processing in the sample Input and Output policies provided with the z/OS RACF driver deals with converting commands and events between their eDirectory representation and their RACF representation.

You can change the behavior and decisions of Identity Manager by modifying the policies and filters. For more information about changing the behavior of Identity Manager, see Chapter 3, "Customizing the Driver," on page 41.

An overview of z/OS RACF driver processing for various commands and events follows this topic.

IMPORTANT: Because not all mapped attributes correspond precisely, changes made in eDirectory or RACF cannot always be sent round trip through the driver and return unchanged. Furthermore, certain RACF behavior places limitations on the faithful correspondence of processing between RACF and eDirectory. For more information, see Section A.3, “Driver Processing of Attributes and Commands,” on page 84.

1.4 Processing Description

This section discusses the processing of commands and events by the driver and the preconfigured starter set of policies and filters. For information about customizing this processing, see Chapter 3, “Customizing the Driver,” on page 41. Topics include

1.4.1 Subscriber and Publisher Channel Processing

The Subscriber channel processes XDS commands for users and groups subject to the limitations of RACF. The Subscriber channel constructs RACF commands using the values of z/OS RACF schema attributes in the XDS documents that it receives. Some values or combinations of values are invalid, not meaningful, or subject to other RACF restrictions.

The Publisher channel generates XDS event documents based on values specified on RACF commands. Certain RACF command parameters and values, or combinations of parameters and values can cause side effects that are not reflected in the events that are generated. Other RACF processing, such as a user being revoked because of an excessive number of invalid password attempts, does not cause an event. Changes made directly to the RACF database, such as those made using ICHEINTY, do not generate events.

For more details about driver processing for z/OS RACF schema attributes, see Section A.2, “RACF Command Parameter Mapping,” on page 68. For details about the handling of certain special cases, see Section A.3, “Driver Processing of Attributes and Commands,” on page 84.

1.4.2 Policy Summary

The following tables summarize the preconfigured sample policies and filter.

Schema Mapping Policy

Class User in eDirectory corresponds to class User in z/OS RACF.

Table 1-1 *Preconfigured Mapping Policy - Class User*

eDirectory	z/OS RACF
CN	DirXML-RACF-userid
Group Membership	DirXML-RACF-groups
Login Disabled	DirXML-RACF-revoked
Login Expiration Time	DirXML-RACF-revokedate
Password Expiration Interval	DirXML-RACF-password-interval

Class Group in eDirectory corresponds to class Group in z/OS RACF.

Table 1-2 *Preconfigured Mapping Policy - Class Group*

eDirectory	z/OS RACF
CN	DirXML-RACF-group

Filter

Classes and their attributes can be synchronized or ignored by each channel. The flow of data is specified during installation, and can be changed later using iManager. The preconfigured filter contains the attributes shown in the following list.

- Class User
  - CN
  - Group Membership
  - Login Disabled
  - Login Expiration Time
  - Password Expiration Interval
  - nspmDistributionPassword
  - DirXML-SPEntitlements
- Class Group
  - CN

Subscriber Channel

Table 1-3 *Preconfigured Sample Policies - Subscriber Channel*

Policy	Processing
Event	Changes delete commands for a User object to set Login Disabled to true. Vetoes delete commands for a Group object. Vetoes rename and move commands.

Policy	Processing
Matching	If configured to do so, vetoes all operations for objects with no association.
	If entitlements are not configured, vetoes events for User objects not in the specified subtree.
	Vetoes events for Group objects not in the specified subtree.
	Matches User and Group objects by CN.
	If entitlements are configured, vetoes commands for users that do not have the racfAccount entitlement.
Create	Requires the CN attribute for User and Group objects.
	If entitlements are configured, vetoes commands for users that do not have the racfAccount entitlement.
Placement	Not used.
Command	If configured to do so, blocks subscribing to password information.
	Converts add commands with nspmDistributionPassword to use the password element.
	Converts modify-attr for nspmDistributionPassword to modify-password.
	If configured to do so, blocks modifies for failed password publish operations.
	If entitlements are configured, processes addition and removal of racfAccount entitlement according to choices made during installation.
	Adds password payload to operation data for use in e-mail notification of failures.
Output	Converts DirXML-RACF-revokedate from eDirectory format to *mm/dd/yy*.
	Converts DirXML-RACF-password-interval from seconds to days.
	Adds RACF command parameters to RACF-groups.
	Provides default attribute values for new users.
	If configured to do so, notifies users by e-mail of failed password publications.

Publisher Channel

Table 1-4 *Preconfigured Sample Policies - Publisher Channel*

Policy	Processing
Input	Converts DirXML-RACF-revokedate from *mm/dd/yy* to eDirectory Time format.
	Converts DirXML-RACF-password-interval from days to seconds.
	Removes RACF command parameters from RACF-groups.
	Removes old-password from modify-password events.
	Converts password values (add User and modify-password) to lowercase.
	Converts user ID and group names to lowercase.
	If configured to do so, notifies users by e-mail of failed password subscriptions.
Event	Not used.
Matching	If configured to do so, vetoes all operations for objects without an association.
	Matches User and Group objects by CN to eDirectory objects in the specified container.
Create	Generates Surname from CN for User objects.
	Requires CN and Surname for User objects. Requires CN for Group objects.
Placement	Places User and Group objects in the specified container.
Command	If configured to do so, blocks publishing passwords.
	If configured to do so, publishes passwords to nspmDistributionPassword.
	If configured to do so, blocks publishing passwords to NDS® password.
	Adds password payload to operation data for use in e-mail notification of failures.

1.4.3 Add and Modify Commands and Events

This section describes how certain attributes of User and Group objects are processed by the preconfigured sample policies for add and modify commands and events. All other schema attributes are passed unchanged if allowed by the filters.

CN - DirXML-RACF-userid and DirXML-RACF-group

The CN attribute of an eDirectory User object is mapped by the Schema Mapping policy with the DirXML-RACF-userid attribute of a RACF User object.

The CN attribute of an eDirectory Group object is mapped by the Schema Mapping policy with the DirXML-RACF-group attribute of a RACF Group object.

Publisher Channel

The CN attribute value for an add event is converted to lowercase by the sample Input policy.

Surname

Surname is a mandatory attribute for an eDirectory User object.

Subscriber Channel

The Subscriber channel does not use the Surname attribute.

Publisher Channel

The sample Publisher Create policy inserts the Surname attribute for an add event, using the value of the CN attribute.

Login Disabled - DirXML-RACF-revoked

Logon Disabled and DirXML-RACF-revoked, if set to true, prevent the user from accessing the system.

The Login Disabled attribute of an eDirectory User object is mapped by the Schema Mapping policy with the DirXML-RACF-revoked attribute of a RACF User object.

For details about the interaction of RACF REVOKE and RESUME dates for a user, see your RACF documentation.

Login Expiration Time - DirXML-RACF-revokedate

Login Expiration Time specifies a date and time after which an eDirectory user cannot log in.

DirXML-RACF-revokedate specifies a starting date for when a RACF user cannot enter the system. For details about the interaction of RACF REVOKE and RESUME dates for a user, see your RACF documentation.

The Login Expiration Time attribute of an eDirectory User object is mapped by the Schema Mapping policy with the DirXML-RACF-revokedate attribute of a RACF User object.

Subscriber Channel

If a value for the Login Expiration Time attribute is present in an add or modify command for a User object, the sample Output policy converts the value from eDirectory Time format to the *mm/dd/yy* format used by RACF.

Publisher Channel

If a value for the RACF-revokedate attribute is present in an add or modify event for a User object, the sample Input policy converts the value from the *mm/dd/yy* format used by RACF to eDirectory Time format.

Password Expiration Interval - DirXML-RACF-password-interval

Password Expiration Interval and DirXML-RACF-password-interval specify how long a password remains valid.

The Password Expiration Interval attribute of an eDirectory User object is mapped by the Schema Mapping policy with the DirXML-RACF-password-interval attribute of a RACF User object.

The eDirectory Password Expiration Interval value is in seconds. The DirXML-RACF-password-interval value is in days, and must be between 1 and 254 inclusive.

Subscriber Channel

If a value for the DirXML-RACF-password-interval attribute is present in an add or modify command for a User object, the sample Output policy converts the value from number of seconds to number of days. If the number of days is less than 1, the value is set to 1. If the number of days is greater than 254, the value is set to 254.

Note that the value actually used by RACF is affected by the value, if any, specified using the INTERVAL operand of the SETROPTS command.

Publisher Channel

If a value for the DirXML-RACF-password-interval attribute is present in an add or modify event for a User object, the sample Input policy converts the value from number of days to number of seconds.

Group Membership - DirXML-RACF-groups

The Group Membership attribute of an eDirectory User object lists the groups the user belongs to.

The DirXML-RACF-groups attribute of a RACF User object lists the groups the user belongs to, together with related CONNECT or REMOVE command parameters.

The Group Membership attribute of an eDirectory User object is mapped by the Schema Mapping policy with the DirXML-RACF-groups attribute of a RACF User object.

An add-value to a User object's group membership is processed as a RACF CONNECT command by the Subscriber channel. A remove-value is processed as a RACF REMOVE command. The sample Output policy appends a default set of parameters for these commands to the value element. You can modify these parameters according to your own business requirements. For details, see Chapter 3, “Customizing the Driver,” on page 41.

The value element for an add-value to a user's Group Membership constructed by the Publisher channel contains the group name followed by the parameters from the RACF CONNECT command. Similarly, the value element for a remove-value includes parameters from the RACF REMOVE command.

Subscriber Channel

If a DirXML-RACF-groups attribute is present in an add or modify command for a User object, the sample Output policy adds RACF information as follows:

- For an add-attr, remove-value, or add-value element, if there is no association-ref, the value is discarded.
- A default set of parameters for the CONNECT (for an add-attr or add-value element) command is appended to each value element. No parameters are added for the REMOVE (for a remove-value element) command by the sample policy, but an example is provided in the comments to guide you if you choose to add your own.

Publisher Channel

If a DirXML-RACF-groups attribute is present in an add or modify event, the sample Input policy operates as follows:

- The CONNECT or REMOVE command parameters are removed from the group name values.
- The group name values are converted to lowercase.

1.4.4 Delete Commands and Events

The RACF DELUSER command does not perform access list or resource ownership cleanup when deleting a user. This could result in security exposures if a new user is created with the same name as a deleted user with residual references.

The RACF DELGROUP command does not clean up references to a group from such places as resource access lists, and cannot be used to delete a universal group.

IBM* recommends that you use the RACF Remove ID utility (IRRRID00) when deleting users and groups. For more information, see your *Security Server RACF Security Administrators Guide*.

Subscriber Channel

The preconfigured sample Subscriber Event policy converts a delete command for a user into a modify command for the user, setting the Login Disabled attribute to true.

The preconfigured sample Subscriber Event policy vetoes delete commands for Group objects.

1.4.5 Rename and Move Commands and Events

RACF does not provide a rename function.

The RACF database is not hierarchical. There is no move function.

Subscriber Channel

The preconfigured sample Subscriber Event policy vetoes rename and move commands. If you change the policies so that rename or move commands reach the Subscriber channel, the Subscriber channel rejects them with an error status.

Publisher Channel

The Publisher channel does not produce rename or move events.

1.4.6 Password Synchronization

Identity Manager uses the nspmDistributionPassword attribute to provide passwords from eDirectory.

The Publisher channel of the driver uses password elements for add events to provide password information. The Publisher channel uses modify-password events for password changes.

You can specify configuration options to control the processing of passwords by the preconfigured sample policies.

For more about Identity Manager password synchronization, see the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

Subscriber Channel

Based on configuration options that you specify, the Subscriber Command policy controls the processing of passwords in the Subscriber channel.

- You can block the subscription of passwords.

For details about configuring password processing options, see "Setting Global Configuration Values" on page 37.

When the password is changed in eDirectory, Identity Manager sends a modify XDS command to the Subscriber channel.

```
<modify class-name="User" src-dn="\DAL\users\eleu">
  <association>USER\ELEU</association>
  <modify-attr attr-name="nspmDistributionPassword">
    <remove-all-values/>
    <add-value>
      <value>secret</value>
    </add-value>
  </modify-attr>
</modify>
```

The Subscriber Command policy changes this to a modify-password event.

```
<modify-password class-name="User" src-dn="\DAL\users\eleu">
    <association>USER\ELEU</association>
    <password>secret</password>
</modify-password>
```

The Subscriber channel converts this to an ALTUSER TSO command and issues the command through the Telnet interface.

```
ALTUSER ELEU NOEXPIRED PASSWORD(SECRET)
```

z/OS requires that passwords be one to eight alphanumeric characters. An installation can define additional password syntax rules. The ALTUSER command rejects invalid or nonconforming passwords.

Publisher Channel

When a RACF user password is changed, either during logon, by the use of the PASSWORD command, or by the ALTUSER command, the RACF Event Subsystem adds a corresponding event to the Change Log data set. The Publisher channel obtains the event and encodes it as an XDS event.

```
<modify-password class-name="user" src-dn="\ELEU">
    <association>USER\ELEU</association>
    <old-password>GUESS<old-password>
    <password>SECRET<password>
</modify-password>
```

Based on configuration options that you specify, the Publisher Command policy controls the processing of passwords in the Publisher channel.

- You can block the publication of passwords.
- You can specify that passwords be published to nspmDistributionPassword.
- You can specify that passwords be published to the NDS password.

For details about configuring password processing options, see "Setting Global Configuration Values" on page 37.

For changes to the NDS password in eDirectory, if the old-password element is present, Identity Manager uses the modifyPassword API to modify the password. If the old-password element is not present, Identity Manager uses the GenerateKeyPair API. Note that using GenerateKeyPair can invalidate authentication credentials for any existing session authenticated as the target object.

The preconfigured sample Input policy removes the old-password element from the event.

```
<xsl:template match="old-password"/>
```

You can comment this out if you prefer that the modifyPassword API be used. If the ALTUSER command is used to change the password, the old password is not available.

z/OS passwords are case-insensitive. The preconfigured sample Input policy converts passwords to lowercase. If you are using Universal Password, which is case-sensitive, you should consider the handling of passwords by z/OS in your deployment planning.

The modify-password Event After the Input Policy

```
<modify-password class-name="user" src-dn="\ELEU">
    <association>USER\ELEU</association>
    <password>secret<password>
</modify-password>
```

Installing the RACF Driver

2

The Novell® Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system) includes two parts. They are installed in separate operations.

1. **The RACF Event Subsystem:** Serves as an interface between the driver shim and RACF.

   The RACF Event Subsystem must be installed on each system that shares the RACF database.

2. **The driver shim:** Provides the conduit for information transfer between eDirectory™ (through Identity Manager) and the RACF Event Subsystem.

   The driver shim can be installed on an z/OS system that runs the RACF Event Subsystem, and configured to use the Java* Remote Loader; or the driver shim can be installed on a server that runs eDirectory.

   The driver shim communicates with the RACF Event Subsystem through Telnet connections. Unless your network provides the level of security required to ensure the privacy of data transmitted over these Telnet connections, we recommend that you install the driver shim on an z/OS system with the RACF Event Subsystem and configure the Telnet connections to use localhost.

Before you install the Novell Identity Manager Driver for RACF on z/OS in a production environment, you should install the driver in a test environment for use in developing your full deployment plan.

2.1 Software Requirements

For information about supported platforms and operating environments, see the Identity Manager 3.6.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm36drivers). From this index page, you can select a readme file associated with the platform(s) for which you need support.

IMPORTANT: Before you begin your installation, check the Novell Support Web site (http://support.novell.com) for the latest support pack and product update information, and review the Release Notes and Readme files.

2.2 Other Requirements

Before placing the Novell Identity Manager Driver for RACF on z/OS in a production environment, you should have a clear deployment strategy in place. The detailed planning of a deployment solution that is necessary to meet a given installation's unique business needs is beyond the scope of this guide. For technical information about customizing the driver, see Chapter 3, “Customizing the Driver,” on page 41.

Although different tasks can be performed by different people, your installation and deployment team must collectively have expertise with eDirectory, iManager, Identity Manager, z/OS, RACF, and XSLT.

Full administrative rights are required, both in eDirectory and on z/OS.

2.3 Overview of the Installation Process

The following outline summarizes the steps to install the Identity Manager driver for z/OS RACF. Details about each step can be found in the topics that follow this outline.

1. Install the RACF Event Subsystem on each z/OS system that shares the RACF database.

   For details, see Section 2.4, "Installing the RACF Event Subsystem," on page 26.

   Installing the RACF Event Subsystem includes the following tasks:

   - **1a** "Setting Up the Libraries on Your z/OS System" on page 27
   - **1b** "Allocating and Initializing the Change Log Data Set" on page 28
   - **1c** "Setting Up the Change Log Started Task" on page 28
   - **1d** "Authorizing the LDXSERV TSO Command" on page 29
   - **1e** "Installing the LDXPROC TSO Logon Procedure" on page 29
   - **1f** "Creating an Administrative User ID for the Driver TSO Session" on page 30
   - **1g** "Testing the RACF Event Subsystem before Installing the RACF Exits" on page 30
   - **1h** "Installing the RACF Exits" on page 31
   - **1i** "Testing the Completed RACF Event Subsystem Installation" on page 32

2. Install the driver shim.

   For details, see Section 2.5, "Installing the Driver Shim," on page 32.

3. Set up the initial driver configuration.

   - **3a** Section 2.6, "Setting Up the Driver," on page 35.
   - **3b** Section 2.7, "Customizing the Policy Starter Set," on page 40.

4. Activate the driver.

   Identity Manager drivers must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can activate Identity Manager products to a fully licensed state. For further information, see Section 2.8, "Activating the Driver," on page 40.

After you have installed and tested the preconfigured Novell Identity Manager Driver for z/OS RACF, implement the deployment plan that you have developed to meet your own specific business requirements.

2.4 Installing the RACF Event Subsystem

An experienced z/OS system programmer familiar with the use of RACF at the local installation should install the RACF Event Subsystem. You should plan about a day to perform the installation tasks. Because the RACF exits reside in LPA, an IPL is required to complete the installation.

To publish RACF events to eDirectory, you must install the RACF Event Subsystem on each system that shares the RACF database.

If you will only subscribe to eDirectory commands, you need only one instance of the RACF Event Subsystem. You do not need to install the RACF exits, you do not need to run the Change Log Started Task, and you do not need a Change Log data set.

The instructions that follow assume that you will install both the Publisher and Subscriber channels.

2.4.1 Setting Up the Libraries on Your z/OS System

The RACF Event Subsystem is packaged as TRANSMIT unloaded z/OS partitioned data sets (PDS).

- **Samples Library:** LDXSAMP.XMT Contains sample cataloged procedures and other JCL.
- **Load Library:** LDXLOAD.XMT Contains executable code.

To prepare the samples library and load library for use:

1 Use ftp to upload these files to your z/OS system from a PC or file server.

1a `FTP your-z/OS-hostname`

1b Authenticate to z/OS using your user ID and password.

1c `QUOTE SITE LRECL=80 RECFM=FB`

1d If you need the files to be stored on a specific disk volume, enter `QUOTE SITE VOL=` *`volser`*

1e `BINARY`

1f `PUT LDXSAMP.XMT`

1g `PUT LDXLOAD.XMT`

1h `QUIT`

2 Use RECEIVE to unpack the samples and load library data sets.

2a Log on to z/OS using the same user ID that you used for the ftp session. The names of the files you sent begin with your user ID unless you have changed your TSO profile prefix.

2b Enter `RECEIVE INDATASET(LDXSAMP.XMT)`

When RECEIVE prompts you for parameters, enter `DSNAME(' hlq.SAMPLIB') VOLUME( volser)` where: *hlq.SAMPLIB* is the name you want to give the samples library, and *volser* is the volume where the samples library is to be created.

2c Enter `RECEIVE INDATASET(LDXLOAD.XMT)`

When RECEIVE prompts you for parameters, enter `DSNAME(' hlq.LDXLOAD') VOLUME( volser)` where: *hlq.LDXLOAD* is the name you want to give the load library, and *volser* is the volume where the load library is to be created.

TIP: RECEIVE errors are typically caused by failure to specify BINARY transfer type or LRECL and RECFM parameters when transferring the files to z/OS with ftp.

---

3 Add the LDX load library to the APF list.

Use the PARMLIB IEAAPF *xx* or PROG *xx* member as appropriate. If you use the dynamic APF facility, you can use the SET PROG command to activate your changes. Otherwise, you must IPL for the change to take effect.

4 Verify that the load library is APF authorized by entering the following:

```
D PROG,APF,DSNAME=LDX.LOAD
```

This should return a listing that includes the load library.

5 For best practices in security, restrict access to authorized administrator IDs and tasks, such as IDXLOGR and IDXDRVP. Also do not include the library in the linklist.

To verify that the load library is not in the linklist, enter the following:

```
D PROG,LNKLST
```

This should return a listing that does *not* include the load library.

2.4.2 Allocating and Initializing the Change Log Data Set

The Change Log data set is a standard z/OS direct access data set. The Change Log data set must reside on a shared device unless it is used by only a single system.

Create one Change Log data set. It is shared by each z/OS system that shares the RACF database.

The Log File utility LDXUTIL is used to initialize the Change Log data set. The Change Log data set must be initialized before you start the Change Log Started Task for the first time.

To allocate and initialize the Change Log data set:

1. Customize the samples library member LOGINIT.

   Update the JCL to conform to your local installation requirements, and specify

   - The name of your LDX load library.
   - A name for your Change Log data set.
   - The shared disk volume where the Change Log is to be allocated. Specify a different unit name if appropriate.
2. Run the LOGINIT job.

   An IEC031I D37 message is normal and should be ignored.
3. Ensure that your Change Log data set is given RACF protection appropriate for the sensitive nature of its contents.

WARNING: If you initialize a Change Log data set that contains data, the data is lost.

2.4.3 Setting Up the Change Log Started Task

1. Copy member LDXLOGRP from the samples library to your started task procedure library (SYS1.PROCLIB or its equivalent). You can give the Change Log Started Task a different name if necessary.
2. Update the JCL to specify
   - The name of your LDX load library
   - The name of your Change Log data set
3. Add the Change Log Started Task to your system startup and shutdown procedures.

   For information about starting and stopping the Change Log Started Task, see “Starting the Change Log Started Task” on page 49 and “Stopping the Change Log Started Task” on page 49.

   The Change Log Started Task should be started during your IPL procedure before user processing begins. Any RACF events of interest that occur are stored in the cross memory queue until the Change Log Started Task has initialized.

The Change Log Started Task should be stopped during your system shutdown procedure after all user processing has ended. Any RACF events of interest that occur after the Change Log Started Task shuts down remain in the cross memory queue and are lost when the system is shut down.

4 Review your Workload Manager definitions to ensure that the Change Log Started Task is assigned to a Service Class appropriate for its role.

2.4.4 Authorizing the LDXSERV TSO Command

LDXSERV requires APF authorization. LDXSERV resides in the LDX load library, which you added to the APF list in Step 3 on page 27. You must also add LDXSERV to the list of authorized TSO commands.

To authorize the LDXSERV TSO command:

1 Add LDXSERV to the AUTHCMD NAMES(...) statement in member IKJTSOxx of SYS1.PARMLIB or its equivalent.

Example:

```
AUTHCMD NAMES( +
  ...other commands... +
  LDXSERV)
```

For more information about IKJTSO *xx*, see the *Initialization and Tuning Reference* for your system.

2 Use the PARMLIB TSO command to activate your changes.

Example:

```
PARMLIB CHECK(00)
PARMLIB UPDATE(00)
```

For more information about the PARMLIB command, see the *TSO/E System Programming Command Reference* for your system.

3 Verify that the LDXSERV command is authorized under TSO by entering the following:

```
PARMLIB LIST(AUTHCMD)
```

This should return a listing that includes LDXSERV.

NOTE: The LDXISSUE command does not require APF authorization.

2.4.5 Installing the LDXPROC TSO Logon Procedure

The LDXPROC TSO logon procedure provides the environment needed by the driver TSO sessions.

To set up the LDXPROC logon procedure:

1 Copy member LDXPROC from the samples library to your TSO logon procedure library. You can give the logon procedure a different name if necessary.

2 Update the JCL to specify the name of your LDX load library on the STEPLIB DD statement.

2.4.6 Creating an Administrative User ID for the Driver TSO Session

The Subscriber channel uses the administrative user ID primarily to issue RACF commands. The Publisher channel uses the administrative user ID primarily to access the Change Log data set.

To set up the administrative user ID:

NOTE: Do this once for each set of systems that share a RACF database.

---

1. Define the user with the ADDUSER command.

   Specify values for the various parameters as appropriate for your standards. There are no restrictions placed by the driver on the name of the user ID.

   The user ID used by the driver must be given the RACF SPECIAL and TSO attributes, and must have no restrictions placed on it that could prevent its intended processing.

   Example:

   ```
   ADDUSER LDXUSER DFLTGRP(mygroup) -
    NAME('RACF DRIVER') PASSWORD(initial) SPECIAL -
    TSO(PROC(LDXPROC) SIZE(32768))
   ```

2. Set the password of the user ID to never expire.

   Example:

   ```
   PASSWORD USER(LDXUSER) NOINTERVAL
   ```

3. Reset the password of the user ID and mark it not expired. (RACF marks the value specified on the ADDUSER command as being expired.)

   Example:

   ```
   ALTUSER LDXUSER NOEXPIRED PASSWORD(xxx)
   ```

When you set up the Driver object, you specify the user ID and password you create here. For details, see Section 2.6, “Setting Up the Driver,” on page 35.

Changing the Password of the Administrative User ID

To change the password of the administrative user ID after installation has been completed:

1. Use the ALTUSER command as shown in Step 3 on page 30.
2. Update the driver configuration with the new Application Password.

   For details, see “Configuring Driver Parameters after Setup Has Been Completed” on page 39.

2.4.7 Testing the RACF Event Subsystem before Installing the RACF Exits

You can use the LDXSERV command to test your installation before you install the RACF exits.

To test the RACF Event Subsystem:

1. If it is not already running, start the Change Log Started Task.

For information about starting the Change Log Started Task, see "Starting the Change Log Started Task" on page 49.

2 Log on to TSO using the administrative user ID you created for the driver.

3 Issue this command: `LDXSERV STATUS`

Examine the output of the command. You should see information about the cross memory queue, information about the Change Log Started Task, and a valid, empty Change Log data set.

For details about interpreting LDXSERV STATUS output, see "Output of the LDXSERV STATUS Command" on page 52.

2.4.8 Installing the RACF Exits

Follow your normal procedure for applying such changes to your z/OS system. We recommend that you

- Install and test the exits on a test system or partition first.
- Make a copy of your system volumes before applying any changes.
- Consider packaging the exits as SMP/E usermods.

To install the RACF exits:

1 Install LDXEVX01, the Common Command exit, using the Dynamic Exit Facility.

For testing, we recommend that you set up two PROGxx members in SYS1.PARMLIB (or equivalent), to allow for easy removal of the exit if desired.

1. Edit SAMPLIB members PROGAD and PROGDL. Change <LDX load library> to your LDX load library name.
2. Copy these two members to your system PARMLIB data set. If you already have a PROGAD or PROGDL member, rename the LDX members to a PROGxx name that's not in use.
3. When ready, use the console command `SET PROG=AD` to activate LDXEVX01 as an IRREVX01 exit point.
4. To uninstall the LDX exit, issue `SET PROG=DL` as a console command.

For permanent installation, do one of the following:

- Add the EXIT ADD statement in PROGAD to your production PROG *xx* PARMLIB member.
- Add a `SET PROG=AD` command to CONSOL00 or an automation script, so that it is issued during your IPL procedure.

2 Install ICHRIX02, the RACROUTE REQUEST=VERIFY(X) (RACINIT) postprocessing exit.

- If you do not have an existing ICHRIX02 exit, run the job in the samples library member RIX0A. This job uses SMP/E to linkedit LDXRIX02 into SYS1.LPALIB as exit ICHRIX02.
- If you have an existing ICHRIX02 exit, update samples library member RIX0B as appropriate. RIX0B installs a router that calls the driver postprocessing exit and your existing exit.

NOTE: To uninstall this exit, use the SMP/E RESTORE function and then IPL with the CLPA option.

3 After you have installed these two exits, IPL the z/OS system with the CLPA option.

2.4.9 Testing the Completed RACF Event Subsystem Installation

To test the complete RACF Event Subsystem before installing the driver shim:

1 If it is not already running, start the Change Log Started Task.

For information about starting the Change Log Started Task, see "Starting the Change Log Started Task" on page 49.

2 Perform some actions to exercise the two RACF exits and create some sample events.

2a Change a password using the logon screen.

2b Create new user ID.

3 Log on to TSO using the administrative user ID you created for the driver.

4 Issue this command: `LDXSERV STATUS`

Examine the output of the command. You should see the RACF exits loaded, information about the cross memory queue, information about the Change Log Started Task, and a valid, non-empty Change Log data set.

For details about interpreting LDXSERV STATUS output, see "Output of the LDXSERV STATUS Command" on page 52.

2.5 Installing the Driver Shim

You can install the driver shim on an eDirectory server, or you can use the Java Remote Loader to install the driver shim on z/OS.

Because the driver shim uses Telnet to access the RACF Event Subsystem, we recommend that you use the Remote Loader. If your network security can ensure the privacy of the transmitted data, you can install the driver shim on an eDirectory server. This section includes the following topics:

- Section 2.5.1, "Installing the Driver Shim on z/OS Using the Java Remote Loader," on page 32
- Section 2.5.2, "Setting Up the Remote Loader Started Task," on page 35

2.5.1 Installing the Driver Shim on z/OS Using the Java Remote Loader

Before you can install the driver shim on z/OS, you must install the Java Remote Loader. The Java Remote Loader requires Java. If you have not already installed Java on z/OS, you must install it first.

- "Installing Java on z/OS" on page 33
- "Installing the Driver Shim Using the Identity Manager Remote Loader for z/OS" on page 33
- "Configuring the Driver Shim" on page 34

Installing Java on z/OS

The Java Remote Loader requires Java. If you have not installed and configured Java on the target z/OS system, you must do so now.

To install Java on z/OS:

1. Obtain and install Java 2 Technology Edition from the IBM Java 2 on the z/OS Platforms Web site (http://www.ibm.com/servers/eserver/zseries/software/java).

   Be sure to install the prerequisite APARs, and to review the install information, restrictions, and other considerations detailed on the Web site.

2. Add the following lines to your /etc/profile:

   ```
   #  Java installation directory
   export JAVA_HOME=your_Java_Installation_Directory
   export PATH=$JAVA_HOME/bin:$PATH
   ```

   Substitute the name of your Java installation directory for *your_Java_Installation_Directory*. Example:

   ```
   export JAVA_HOME=/usr/lpp/java/IBM/J1.4
   ```

Java 1.4 does not require a classpath for standard Java classes as long as the directory structure is maintained.

Java runtime options can be passed using the environment variable IBM_JAVA_OPTIONS. For example, to turn on verbose mode:

```
export IBM_JAVA_OPTIONS=-verbose
```

Installing the Driver Shim Using the Identity Manager Remote Loader for z/OS

1. Consult the IBM Web site (http://www.ibm.com) to determine and, if necessary, install the correct Java software for your implementation of z/OS.
2. Obtain the `zos_remoteloader.tar` from the Identity Manager installation media and transfer it to your z/OS RACF system, using ftp. Enter the following commands:

   2a `ftp` *`hostname`*

   where *hostname* is the name of your z/OS server.

   2b Authenticate to z/OS using your user ID and password.

   2c Change to the installation directory. For example:

   ```
   cd /usr/dirxml
   ```

   2d `binary`

   2e `put zos_remoteloader.tar`

   2f `quit`

3. Extract the contents of zos_remoteloader.tar into your installation directory, as follows:

   Change to the installation directory. For example:

   ```
   cd /usr/dirxml
   ```

   ```
   tar xvf zos_remoteloader.tar
   ```

   This creates the following files and directories in your installation directory:

File	Contents
`config.txt`	sample configuration file
`create_keystore`	sample script to create keystore
`dirxml_jremote`	sample script to run Remote Loader
`lib`	java .jar files
`doc`	documentation

4 Set the loader and driver passwords. For example:

```
./dirxml_jremote -sp loaderpassword driverpassword
```

5 Configure the Remote Loader for SSL.

For more information, see the section on "Setting Up a Connected System" in the *Identity Manager 3.6.1 Administration Guide* (http://www.novell.com/documentation/idm36).

6 Start the Remote Loader on z/OS.

You can start the Remote Loader either from the command line or as a started task.

If you plan on using latter method, you will first need to set up the started task as explained in Section 2.5.2, "Setting Up the Remote Loader Started Task," on page 35.

Once you are ready to start the Remote Loader, see Section 4.5.3, "Starting the z/OS Remote Loader," on page 49 for more information.

7 Continue with "Configuring the Driver Shim."

Configuring the Driver Shim

IMPORTANT: If you did not include the RACF driver during your Identity Manager installation, run that installation program again, ensuring that you select the RACF driver check box.

1 In iManager, select *Identity Manager Utilities* > *Create Driver*, and designate the driver set for the new driver.

2 Choose *Import a Driver Configuration from the Server* > *RACF.xml*. Respond to the prompts.

NOTE: You will be asked to enter information from the RACF Event Subsystem installation.

3 Start the driver in eDirectory.

NOTE: If you are upgrading from a previous version of the RACF driver, you will need to restart eDirectory before you start the driver.

4 Test according to your installation plan.

5 Customize the preconfigured starter set policies as appropriate for your deployment plan.

2.5.2 Setting Up the Remote Loader Started Task

The sample JCL for the Remote Loader Task is in LDXDRVRP. You will need to copy LDXDRVRP from the samples library to your started task procedure library. You will need to copy three more members of the samples library to your Remote Loader installation directory. Once these files are in place, you will need to customize text variables within their code as follows:

Variable	Replace It With...	Example
<directory>	The directory where the remote loader is installed.	/usr/dirxml
<loadlib>	The load library dataset name.	LDX.LOAD
<samplib>	The samples library dataset name.	LDX.SAMPLIB
<logfile>	The log file dataset name.	LDX.LOGFILE

To set up the Remote Loader started task:

1. Copy member LDXDRVRP from the samples library to your started task procedure library (SYS1.PROCLIB or its equivalent). You can give the Remote Loader started task a different name if necessary.
2. Copy the following members to your Remote Loader installation directory:

Member	File Name in Directory
STDENV	driverstc.stdenv
START	START
STOP	STOP

NOTE: File names are case-sensitive.

You can use TSO commands to make these copies. For example:

```
oput '<samplib>(STDENV)' '<directory>/driverstc.stdenv'
oshell chmod 644 <directory>/driverstc.stdenv
oput '<samplib>(START)' '<directory>/START'
oshell chmod 755 <directory>/START
oput '<samplib>(STOP)' '<directory>/STOP'
shell chmod 755 <directory>/STOP
```

3. Customize the text variables within the code for all of the items copied to the started task procedure library and Remote Loader installation directory, according to your specific library, file, and directory names.

2.6 Setting Up the Driver

After you have installed the various components, you must create a Driver object and configure it for operation.

- Section 2.6.1, “Creating and Configuring the Driver Object,” on page 36

- Section 2.6.2, “Setting Global Configuration Values,” on page 37
- Section 2.6.3, “Configuring Driver Parameters after Setup Has Been Completed,” on page 39

2.6.1 Creating and Configuring the Driver Object

1. In iManager, select *Identity Manager Utilities* > *Create Driver*, and designate the driver set for the new driver.
2. Choose *Import a Driver Configuration from the Server* > *RACF.xml*.
3. Specify driver configuration information.
   - **Driver Name:** Specify a name for your driver.
   - **Enable Role-Based Entitlements:** Choose whether or not you want this driver configured to use entitlements.
   - **RACF Host Address:** Specify the IP address or DNS name the driver should use for its Telnet interface to the RACF system.

     If the driver uses the Remote Loader, specify 127.0.0.1, which is the local host.
   - **RACF Telnet Port:** Specify the Telnet port number the driver should use. This should normally be 23.
   - **Administrator:** Specify the name of the administrative user ID you created for the driver in Step 1 on page 30.
   - **Administrator Password:** Specify the password you specified for the administrative user ID in Step 3 on page 30.
   - **RACF TSO Name:** Specify the APPLID the driver should use on its VTAM logon command to access TSO.
   - **RACF TSO Account Number:** Specify the account number information the driver should provide on the TSO logon screen for the administrative user ID.
   - **RACF TSO Procedure:** Specify the TSO logon JCL procedure name the driver should provide on the TSO logon screen for the administrative user ID.
   - **Configure Data Flow:** Choose the data flow configuration you want set in the filter.
     - To synchronize in both the Publisher and Subscriber channels, choose Bi-directional.
     - To synchronize only for the Publisher channel, choose RACF to eDirectory.
     - To synchronize only for the Subscriber channel, choose eDirectory to RACF.
   - **Polling Interval:** Specify the number of seconds the Publisher Channel should wait after processing all available events before issuing the next LDXSERV GETNEXT command to see if new events are available for processing.
   - **Heartbeat Interval:** Specify the minimum number of minutes between publication heartbeat documents. To disable heartbeat document publication, set this value to zero.
   - **Users Container:** Specify the eDirectory container where users are to be synchronized.
   - **Groups Container:** Specify the eDirectory container where groups are to be synchronized.
   - **Default Group:** Specify the default group for new RACF users.
   - **Use Default Matching Rules:** Choose whether or not the default Matching policies are enabled.

You should not use the preconfigured sample default Matching policies for a production environment without a careful review of installation-dependent considerations.

- **Install Driver As Remote/Local:** Specify whether the driver is to use the Remote Loader or to run local to the eDirectory server.

The following options pertain only to configurations that use the Remote Loader.

- **Remote Host Name and Port:** Specify the IP address or DNS name and TCP port number to be used to access the Remote Loader service.
- **Driver Password:** Specify the driver object password used by the Remote Loader to authenticate itself to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Identity Manager Remote Loader.
- **Remote Password:** Specify the Remote Loader password used by Identity Manager to authenticate itself to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Identity Manager Remote Loader.

4 Define appropriate Security Equivalences for the Driver object so that it can perform the necessary eDirectory operations.

5 Exclude Administrative roles from replication.

6 Restart eDirectory.

7 Start the driver:

7a In iManager, select *Identity Manager Management > Overview*.

7b Locate the driver in its driver set.

7c Click the driver status indicator in the upper right corner of the driver icon and click *Start Driver*.

2.6.2 Setting Global Configuration Values

After you have created and configured the Driver object, review the Global Configuration Values settings and customize them as appropriate.

To review and change global configuration values:

1 In iManager, select *Identity Manager Management > Overview*.

2 Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.

3 Click *Identity Manager > Global Config Values*.

4 Update the values as desired, then click *OK*.

- **Action on Applying RACF Account Entitlement:** Specifies the policy action to be taken for a RACF user when it is granted the RACF Account Entitlement.
- **Action on Removing RACF Account Entitlement:** Specifies the policy action to be taken for a RACF user when its RACF Account Entitlement is removed.
- **RACF Accepts Passwords from Identity Manager Data Store:** Specifies whether or not the policies permit password values to flow from eDirectory to RACF.
- **Identity Manager Accepts Passwords from RACF:** Specifies whether or not the policies permit password values to flow from RACF to eDirectory.

- **Publish Passwords to NDS Password:** Specifies whether or not the policies publish passwords to the NDS password in eDirectory (if Identity Manager accepts passwords from RACF).
- **Publish Passwords to Distribution Password:** Specifies whether or not the policies publish passwords to the eDirectory Distribution Password (if Identity Manager accepts passwords from RACF).
- **Require Password Policy Validation Before Publishing Passwords:** Specifies whether or not eDirectory password policies are enforced for passwords being published from RACF.

  IMPORTANT: Ensure that your password policies are compatible with RACF password rules and restrictions before enabling this facility.

- **Reset User's External System Password to the Identity Manager Password on Failure:** Specifies whether or not the RACF password is to be reset from the eDirectory password if an eDirectory password change fails.

  IMPORTANT: Ensure that your password policies are compatible with RACF password rules and restrictions before enabling this facility.

- **Notify the User of Password Synchronization Failure via E-mail:** Specifies whether or not message is to be sent to the user if a password synchronization fails.

  For information about e-mail notification prerequisites and configuration, see Configuring E-Mail Notification in the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).
- **Connected System or Driver Name:** Specifies the name to be used to identify the RACF system to the user in password synchronization failure messages.
- **Users Container:** Specifies the eDirectory container where users are to be synchronized.
- **Groups Container:** Specifies the eDirectory container where groups are to be synchronized.
- **Default TSO Acctnum:** Specifies the default TSO accounting information for new RACF users.
- **Default TSO Maxsize:** Specifies the default TSO MAXSIZE value for new RACF users.
- **Default TSO Procedure:** Specifies the default TSO logon procedure name for new RACF users.
- **Default TSO Size:** Specifies the default TSO SIZE value for new RACF users.
- **Default Group:** Specifies the default group for new RACF users.
- **Use Default Matching Rules:** Specifies whether or not the default Matching policies are enabled.

  You should not use the preconfigured sample default Matching policy for a production environment without a careful review of installation-dependent considerations.

  The default Subscriber Matching policy matches User objects without an association by CN. RACF does not use a hierarchical directory structure and does not provide a globally unique identifier. A pre-existing RACF user profile could be matched with a User object in eDirectory that represents a different person.

Given an appropriate installation management policy, you could implement a Matching policy that requires two attributes to be identical before matching users by CN. For example, you could use the RACF installation-defined data field to contain an employee identification number and populate a corresponding field in eDirectory, such as Employee ID.

2.6.3 Configuring Driver Parameters after Setup Has Been Completed

You can change the configuration of the driver after setup has been completed.

To change driver parameters:

1. In iManager, select *Identity Manager > Overview*.
2. Select the driver set containing the driver, click the driver icon to see the driver overview, then click the driver icon again to edit driver parameters.
3. Click *Identity Manager > Driver Configuration*.
4. Update the parameters as desired, then click *OK*.
   - **Driver Module:** Select Java or Connect to Remote Loader, as appropriate.
   - **Driver Object Password:** Specify the driver object password used by the Remote Loader to authenticate itself to the Identity Manager server. It must be the same password that is specified as the Driver Object Password on the Identity Manager Remote Loader.
   - **Authentication:** Common driver authentication information.
     - **Authentication ID:** Specify the name of the administrative user ID you created for the driver in Step 1 on page 30.
     - **Authentication Context:** Not used.
     - **Remote Loader Connection Parameters:** Specify the IP address or DNS name and TCP port number to be used to access the Remote Loader service. Use the form shown in the following example:

       ```
       hostname=127.5.222.17 port=8090
       ```

     - **Driver Cache Limit:** Specify 0.
     - **Application Password:** Specify the password you specified for the administrative user ID in Step 3 on page 30.
     - **Remote Loader Password:** Specify the Remote Loader password used by Identity Manager to authenticate itself to the Remote Loader. It must be the same password that is specified as the Remote Loader password on the Identity Manager Remote Loader.
   - **Startup Option:** Specify Auto Start for a driver used in production.
   - **Driver Settings:** RACF Driver Settings.
     - **RACF Host Address:** Specify the IP address or DNS name the driver should use for its Telnet interface to the RACF system.

       If the driver uses the Remote Loader, specify 127.0.0.1, which is the local host.
     - **RACF Telnet Port:** Specify the Telnet port number the driver should use. This should normally be 23.

- **RACF TSO Name:** Specify the APPLID the driver should use on its VTAM logon command to access TSO.
- **RACF TSO Account Number:** Specify the account number information the driver should provide on the TSO logon screen for the administrative user ID.
- **RACF TSO Procedure:** Specify the TSO logon JCL procedure name the driver should provide on the TSO logon screen for the administrative user ID.

- **Subscriber Settings:** Subscriber channel settings.
  - **Additional Handlers:** Not used.
- **Publisher Settings:** Publisher channel settings.
  - **Additional Servlets:** Not used.
  - **Publisher Disabled:** Specify Yes or No for whether or not the driver suppresses publishing RACF events.
  - **Polling Interval:** Specify the number of seconds the Publisher Channel should wait after processing all available events before issuing the next LDXSERV GETNEXT command to see if new events are available for processing.
  - **Heartbeat Interval:** Specify the minimum number of minutes between publication heartbeat documents. To disable heartbeat document publication, set this value to zero.

2.7 Customizing the Policy Starter Set

The preconfigured starter set of sample policies and filters is not intended for use in a production environment. Before running the driver you must modify the policies and filters to suit your own business rules. For detailed information, see Chapter 3, “Customizing the Driver,” on page 41.

2.8 Activating the Driver

Identity Manager and Identity Manager drivers must be activated within 90 days of installation, or they will shut down. At any time during the 90 days, or afterward, you can activate Identity Manager products to a fully licensed state.

To activate Identity Manager products:

1. Purchase the appropriate licenses.
2. Generate a Product Activation Request.
3. Submit the Product Activation Request to Novell.
4. Install the Product Activation Credential received from Novell.

For detailed information about completing these steps, see the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

Customizing the Driver

3

This section provides information about available resources for customizing the Novell® Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system).

The driver includes a sample starter set configuration that you can use as a starting point for your customization. You must customize the driver to conform to the requirements of your installation before running it for production work.

Customization of the driver is accomplished by tailoring the global configuration values, policies, and filters. The event filters determine whether eDirectory™, RACF, both, or neither is the source of User and Group objects and their various attributes. The policies control the way that information flows from the source to the destination. Global configuration values are used by the sample policies to control their processing.

- For information about customizing the global configuration values, see "Setting Global Configuration Values" on page 37.
- For information about customizing the flow of data through the filters, see "Controlling Which Objects and Attributes Are Synchronized" on page 43.
- For information about customizing the policies, see "Customizing the Policies" on page 43.
- For details about customizing password synchronization, see the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

3.1 Guidelines for Customization

The Subscriber channel issues RACF commands to process XDS commands received for objects and attributes represented in the z/OS RACF schema. For details of how these attributes relate with RACF command parameters, see Section A.2, "RACF Command Parameter Mapping," on page 68.

The Subscriber channel constructs RACF commands using the values provided in XDS command documents for users and groups. If the Subscriber channel can successfully construct and issue commands, it returns success status-regardless of the command results. If the values provided in the XDS documents do not conform to RACF requirements, the RACF commands can produce invalid or undesired results.

The Publisher channel generates XDS event documents based on RACF commands and the parameters that are specified on them. Not all of the RACF processing implied by certain combinations of command parameters can be accurately codified in XDS event documents.

As a policy writer, it is your responsibility to understand the limitations of RACF and its command semantics. You must ensure that the values you pass to the Subscriber channel are valid and consistent. You must account for side effects and possible multiple meanings of RACF command parameters and combinations of parameters. You must understand and provide for the differences and limitations in the way eDirectory and RACF attributes with similar functions whose values are derived from one another are implemented by eDirectory and RACF.

For information about how the driver shim processes certain commands and events, see Section A.3, "Driver Processing of Attributes and Commands," on page 84.

3.2 RACF Restrictions

RACF places restrictions on user and group profile names, passwords, and other values. You must do what is necessary in your policies and filters to ensure that no objects or attributes are added or migrated from eDirectory that do not conform to the RACF restrictions. The Subscriber channel performs no validity checking on the values in the XDS command documents that are passed to it. The RACF commands that the Subscriber channel generates to process the command documents validate their parameter values. Invalid values can cause the commands issued by the Subscriber channel to produce erroneous results.

The following sections describe some common RACF command parameter syntax rules. For a complete description of RACF command parameter syntax rules, see your *Security Server RACF Command Language Reference*. For tables relating RACF command parameters and z/OS RACF schema attributes, see Section A.2, “RACF Command Parameter Mapping,” on page 68.

3.2.1 User Profile Naming Restrictions

The following is a summary of the RACF restrictions for naming user profiles. For complete details, see your RACF documentation.

- A RACF TSO user ID must be between 1 and 7 characters in length.
- A RACF TSO user ID must consist of characters in: A-Z, 0-9, #, $, @ (case-insensitive).
- A RACF TSO user ID must not begin with a numeric character (0-9).
- No user ID can be the same as the name of another user ID or the name of a group.

3.2.2 Group Profile Naming Restrictions

The following is a summary of the RACF restrictions for naming group profiles. For complete details, see your RACF documentation.

- A RACF group name must be between 1 and 8 characters in length.
- A RACF group name must consist of characters in: A-Z, 0-9, #, $, @ (case-insensitive).
- A RACF group name must not begin with a numeric character (0-9).
- No group name can be the same as the name of another group or the name of a user ID.

3.2.3 Password Restrictions

z/OS requires that passwords be one to eight alphanumeric characters. z/OS passwords are case-insensitive. An installation can define additional password syntax rules using the RACF SETROPTS command.

3.3 Customizing the Driver

Before you use Novell Identity Manager driver for RACF on z/OS, review the global configuration values to ensure that you have specified appropriate values, such as the names of your eDirectory containers for users and groups. For details about global configuration values, see “Setting Global Configuration Values” on page 37.

3.3.1 Controlling Which Objects and Attributes Are Synchronized

Synchronization can be controlled with filters, event policies, and entitlements.

Filter

Identity Manager uses filters to control the data flow for which objects and attributes are synchronized, and to define the authoritative data source for these objects and attributes. The initial data flow configuration was specified during installation. For details, see "Creating and Configuring the Driver Object" on page 36.

The preconfigured filter is illustrated in "Filter" on page 17.

To change the filter:

1. In iManager, click Identity Manager Management > Overview.
2. Locate the driver in its driver set.
3. Click the driver to open the Driver Overview Page.
4. Click the Driver Filter icon and make the desired changes.

Event Policies

You can use the Event Transformation policies to perform custom filtering of objects based on criteria according to your business rules.

Entitlements

If you enabled role-based entitlements during installation, you can use entitlements to control access to RACF accounts.

3.3.2 Conforming to RACF Requirements

If your eDirectory object names and attributes do not meet RACF restrictions, you must use filters and policies to block or modify them to conform before they are delivered to the Subscriber channel. For example, you can use the Subscriber Create policy to edit check CN for length and character set requirements.

3.3.3 Customizing the Policies

You can modify, replace, or supplement the preconfigured sample policies to perform whatever processing is necessary to meet your business requirements. For examples and guidance, you can study the sample policies distributed with this and other Identity Manager drivers.

For details about the z/OS RACF Schema, see Appendix A, "z/OS RACF Schema and Driver Processing," on page 57.

For general information about customizing policies, see the *Policy Builder and Driver Customization Guide at* the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

3.4 Advanced Topics

This section discusses additional information that can be of interest as you develop your customization plan. Topics include

3.4.1 Using the Subscriber Channel Command Class

Besides the z/OS RACF schema User and Group classes, which are mapped to their eDirectory counterparts, the Subscriber channel of the driver supports the Command class. You can use the Command class in your policies to issue arbitrary TSO commands.

The Subscriber channel processes XDS add commands for class Command. The text value of the type="string" value element of an add-attr element is executed as a TSO command through the Telnet interface.

You can use this facility to perform custom processing on the z/OS system for eDirectory events.

How the Driver Processes the Command Class

- You can specify as many add-attr elements in one XDS add command as necessary.
- Only one value element is processed for each add-attr element.
- The text value of the value element is issued as a TSO command through the Telnet interface by the administrative user ID using the LDXISSUE command.
- You can specify any TSO command, CLIST, or REXX exec as the command to be executed.

  NOTE: You must modify the LDXPROC logon procedure used by the administrative user ID to provide any DD statements required by your processing.
- The response from the command is returned in the status document from the driver.
- The attr-name of the add-attr element is ignored.
- Elements other than add-attr are ignored.
- XDS commands other than add are ignored.

Command Class Example

```
<add class-name="Command" event-id="1234">
  <add-attr attr-name="MAKEUSER">
    <value type="string">%MAKEUSER GURNEY</value>
  </add-attr>
</add>
```

3.4.2 Using the RACF Query Processor

The RACF Query Processor is called by Identity Manager during migration and by other processing.

You can use the RACF Query Processor for your own purposes as required.

Queries for Scope Entry

Queries to the RACF Query Processor for a single user are processed using the RACF LISTUSER command for that user. Queries to the RACF Query Processor for a single group are processed using the RACF LISTGRP command for that group.

Queries for Scope Other Than Entry

Queries to the RACF Query Processor that are not limited to just a single base entry use the RACF LISTUSER * or RACF LISTGRP * command, depending on the class. These commands return information for all profiles of the class. The RACF Query Processor then returns the information requested by the query.

If you use the RACF Query Processor with a scope other than entry, you should expect the query to take a long time-possibly many hours.

3.4.3 Using Java Utility Class DateConv

The Novell Identity Manager driver for z/OS RACF includes the Java utility class DateConv. DateConv is used by the starter set sample policies for date conversion. You can use this class for your own purposes.

To use DateConv in your policies:

1. Add a namespace declaration as shown in the following example taken from the Input Transformation policy.

   ```
   xmlns:util="http://www.novell.com/nxsl/java/
   com.Omnibond.nds.dirxml.util.DateConv"
   ```

2. Call the desired method as shown in the following example taken from the Input Transformation policy.

   ```
   <xsl:value-of select="util:racfToEdirTime(.)"/>
   ```

Overview

The Login Expiration Time attribute of an eDirectory User object is mapped by the Schema Mapping policy with the RACF-revokedate attribute of a RACF User object. RACF represents dates in the *mm/dd/yy* format, while eDirectory uses number of seconds since the beginning of 1970.

The Java DateConv class is provided for transforms to use in converting date values between these formats.

The following sections describe the methods of DateConv.

edirToRacfDate

```
public static String edirToRacfDate(String seconds)
```

Returns a date in the *mm/dd/yy* format used by the RACF ALTUSER command RESUME and REVOKE parameters. The input is assumed to be an eDirectory Time value, coded as a string.

Parameters

seconds - String value of number of seconds since 1970-01-01 00:00 UTC

Returns

String value *mm/dd/yy* local time

Example

```
edirToRacfDate("1068440400")
```

Returns the string 11/10/03.

Notes

If an exception occurs, a string of 00/00/00 is returned. This can happen if the input string cannot be converted to a number.

racfToEdirTime

```
public static String racfToEdirTime(String mmddyy)
```

Returns an eDirectory Time value as a string. The input is assumed to be the date value in the format *mm/dd/yy*, specified for the RESUME or REVOKE parameter of a RACF ALTUSER command.

Parameters

mmddyy - String value representing a date in the form *mm/dd/yy*

Returns

String value of number of seconds since 1970-01-01 00:00 UTC

Example

```
racfToEdirTime("11/10/03")
```

Returns the string 1068440400.

Notes

If an exception occurs, a string of 0 is returned. If the input string cannot be parsed into three strings using a ’/’ as a separator, a string of 000 is returned.

RACF interprets the two-digit year value as being in the range 1971–2070.

eDirectory Time values appear to be limited to the integer (int) number of seconds since 1970-01-01 00:00 UTC. This overflows on 2038-01-18. Novell utilities limit Login Expiration Time to not exceed the year 2037. A RACF date beyond 2037 is set to 2037-12-31.

No explicit conversion is performed between UTC and local time. The RACF date values are local time. The result corresponds to the default time zone of the default locale.

Operating Procedures

4

This section provides information about operational tasks commonly used with the Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system).

Topics include

4.1 Migrating and Synchronizing Data

Identity Manager synchronizes data as it changes. If you want to synchronize all data immediately, you can choose from the following options:

- **Migrate Data From eDirectory:** Allows you to select containers or objects you want to migrate from eDirectory™ to an application. When you migrate an object, the Identity Manager engine applies all of the Matching, Placement, and Create policies, as well as the Subscriber filter, to the object.
- **Migrate Data Into eDirectory:** Allows you to define the criteria Identity Manager uses to migrate objects from an application into eDirectory. When you migrate an object, the Identity Manager engine applies all of the Matching, Placement, and Create policies, as well as the Publisher filter, to the object. Objects are migrated into eDirectory using the order you specify in the Class list.
- **Synchronize:** Identity Manager processes all objects for classes listed in the Subscriber class filter. Associated objects are merged. Objects without an association are processed as Add events.

To use one of these options:

1. In iManager, select *Identity Manager* > *Overview*.
2. Locate the driver set containing the z/OS RACF driver, then double-click the driver icon.
3. Click the appropriate migration button.

4.1.1 Migrating Users and Groups from RACF to eDirectory

To migrate users and groups from RACF, you must migrate all of the groups first, and then migrate all of the users. This is because RACF group profiles do not always contain a complete list of their member users. Add group and modify group events never contain group members in the Publisher channel of the z/OS RACF driver.

4.1.2 Migrating Users and Groups from eDirectory to RACF

To migrate users and groups from eDirectory, you must migrate all of the groups first, and then migrate all of the users. This is because the Subscriber channel policies process the User object Group Membership attribute, but not the Group Object Member attribute.

4.2 Deleting Groups in eDirectory

If you want to delete a group from eDirectory and ensure that the corresponding RACF group is not used until you can schedule the RACF Remove ID utility, remove each user from the Group object's Member list before you delete it.

Because the RACF DELGROUP command does not clean up references to a group from such places as resource access lists, and cannot be used to delete a universal group, the Subscriber Event policy vetoes delete commands for Group objects. IBM recommends that you use the RACF Remove ID utility (IRRRID00) when deleting groups. For more information, see your *Security Server RACF Security Administrators Guide*.

4.3 Deleting Users in eDirectory

RACF performs no cleanup actions when deleting a user. This could result in security exposures if a new user is created with the same name. The preconfigured Subscriber Event policy converts a delete command for a User object into a modify command that sets the Login Disabled attribute. The Subscriber channel processes this as a RACF ALTUSER command to revoke the user's access to the system.

4.4 Performing Administrative Password Resets

Administrative password resets on a RACF system result in the new password being marked as expired. The user must change the password immediately upon using it for the first time. Administrative password resets in eDirectory result in similar behavior if periodic password changes are required.

The driver cannot detect that a new password is marked as expired, and RACF provides no mechanism to mark an existing password as being expired.

Users should be instructed to change the password upon first usage after an administrative password reset even if the system does not prompt them to do so.

4.5 Controlling the Change Log Started Task

The RACF exits add information about events to an in-storage cross memory queue as they occur. The Change Log Started Task moves events from this queue to the Change Log data set, where they await processing by the driver.

Start the Change Log Started Task during your IPL procedure before user processing begins. Any RACF events of interest that occur are stored in the cross memory queue until the Change Log Started Task has initialized.

You can briefly stop the Change Log Started Task if necessary. Any RACF events of interest that occur while the Change Log Started Task is not running remain in the cross memory queue, and are written to the Change Log data set when the Change Log Started Task is restarted.

Stop the Change Log Started Task during your system shutdown procedure after all user processing has ended. Any RACF events of interest that occur after the Change Log Started Task shuts down remain in the cross memory queue and are lost when the system is shut down.

4.5.1 Starting the Change Log Started Task

To start the Change Log Started Task, use the z/OS START command.

```
START LDXLOGRP
```

If you have used a different name for the Change Log Started Task cataloged procedure, substitute the name that you used into the preceding command.

4.5.2 Stopping the Change Log Started Task

To stop the Change Log Started Task, use the z/OS STOP command.

```
STOP LDXLOGRP
```

If you have used a different name for the Change Log Started Task cataloged procedure, substitute the name that you used into the preceding command.

4.5.3 Starting the z/OS Remote Loader

You can choose from two methods to run the Java Remote Loader on z/OS:

- from the command line
- as a started task

To run from the command line:

1. Change to the installation directory. For example:

   ```
   cd /usr/dirxml
   ```

2. Enter the command to run the Remote Loader:

   ```
   ./dirxml_jremote -config zos_config.txt&
   ```

To run as a started task, use the z/OS START command:

```
START LDXDRVRP
```

4.5.4 Stopping the z/OS Remote Loader

You can choose from two methods to stop the Java Remote Loader on z/OS:

- from the command line
- as a started task

To stop from the command line:

1. Change to the installation directory. For example:

   ```
   cd /usr/dirxml
   ```

2. Enter the command to stop the Remote Loader:

```
./dirxml_jremote -config zos_config.txt -u -p loaderpassword
```

To stop as a started task, use the z/OS START command:

```
START LDXDRVRP,OPTION=STOP
```

Troubleshooting

5

This section provides information about troubleshooting the Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system). Topics include

5.1 Using DSTrace

You can gather extensive troubleshooting information for the driver by using the DSTrace utility. For each event or operation received, the driver returns an XML document containing a status report. If the operation fails, the status report contains information about the error.

For information about gathering Identity Manager trace information with DSTrace, see TID 10065332 at the Novell Support Web site (http://support.novell.com).

For additional information about using DSTrace in troubleshooting Identity Manager, see the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

5.2 Understanding LDX Messages

RACF Event Subsystem components write numbered status and diagnostic messages prefixed with the characters “LDX.” For detailed information about each LDX message, see Appendix B, “Messages,” on page 89.

5.3 Using Novell Audit

You can use Novell Audit to control how and where Identity Manager messages are delivered. Using this service in combination with the driver log level setting provides you with tracking control at a very granular level and with the option for immediate notice when problems occur. For more information, see the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

5.4 Using JCL and Job Logs

The JCL and Job logs, and other SYSOUT from the Change Log Started Task and from the TSO sessions used by the driver can be useful for troubleshooting. Ensure that these are retained as appropriate.

5.5 Conforming to RACF Requirements and Limitations

Ensure that RACF restrictions, such as length and character set of a user ID, are met by all commands that reach the driver shim. For more information about these restrictions, see Section 3.2, "RACF Restrictions," on page 42.

For information about driver processing subject to other RACF limitations, see "Subscriber and Publisher Channel Processing" on page 16, Section 3.1, "Guidelines for Customization," on page 41, and Section A.3, "Driver Processing of Attributes and Commands," on page 84.

5.6 Using the LDSXSERV STATUS Command

You can use the LDXSERV STATUS command to check the status of the RACF Event Subsystem.

5.6.1 Issuing the LDXSERV STATUS Command

1. Log on to TSO using a user ID with a STEPLIB DD statement for the LDX load library. The LDXPROC logon JCL procedure includes this STEPLIB.
2. Enter `LDXSERV STATUS`.

5.6.2 Output of the LDXSERV STATUS Command

LDXSERV STATUS command output is in XML form for the use of the driver, but you can use the output for yourself as well.

```
<ldx>
  <source>
    <product build="20040225" instance="ldxserv" version="1.1">
      RACF Event Subsystem Utility Command
    </product>
    <contact>Novell, Inc.</contact>
  </source>
  <output>
    <status level="success">
      <exit name="LDXRIX02" state="active" version="0.99" build-date="20031205"
times-called="885" events-queued="0" info="ok"/>
      <exit name="LDXEVX01" state="active" version="0.99" build-date="20040220"
times-called="0" events-queued="0" info="ok"/>
      <queue version="0.99" state="active" created-by="LDXRIX02" entries="0"/>
      <logger version="0.99" state="active" taskid="LDXLOGR"/>
      <logfile name="LDX.EVENTLOG" state="empty"/>
    </status>
  </output>
</ldx>
```

Table 5-1 LDXSERV STATUS Output Elements

Element Name	Content
<exit>	Information about the RACF exits
<queue>	Information about the cross memory event queue
<logger>	Information about the Change Log Started Task
<logfile>	Information about the Change Log data set

5.7 Using Association Values

The general format of an association value produced by the Identity Manager driver for z/OS RACF is *ClassName\ ObjectName*. These association values are all uppercase.

Examples:

```
USER\ANDREW
USER\CLAIRE
GROUP\ADMIN
```

5.8 Other Troubleshooting Tips

- Ensure that the Driver object has appropriate rights.
- Ensure that the driver parameters have the appropriate and correct values. For information about the driver parameters, see "Configuring Driver Parameters after Setup Has Been Completed" on page 39.
- Ensure that the global configuration values have the appropriate and correct settings. For information about setting global configuration values, see "Setting Global Configuration Values" on page 37.
- If the LDXSERV command does not have APF authorization, it ABENDs with a code of S047.
- Ensure that all JCL on all systems specifies the correct (same) Change Log data set.

5.9 Common Problems

Following are common problems and solutions.

Invalid Password Supplied

Problem: A trace shows the following:

```
  <description>Driver exception.</description>
<exception class-
name="com.Omnibond.system.Command.CommandSessionException">
<message>Error occured during writeLine():
com.Omnibond.system.Command.ScriptException: linenum=4 cursor=0
: Invalid password supplied
</message>
```

Possible Cause: The password for the administrative user ID is not specified correctly in the driver parameters.

Action: Specify the correct Application Password in the driver parameters. For details, see "Configuring Driver Parameters after Setup Has Been Completed" on page 39.

User Is Not Authorized

Problem: A trace shows the following:

```
  <description>Driver exception.</description>
<exception class-
name="com.Omnibond.system.Command.CommandSessionException">
<message>Error occured during writeLine():
com.Omnibond.system.Command.ScriptException: linenum=3 cursor=0
: User is not authorized
  </message>
</exception>
```

Possible Cause: The administrative user ID is not specified correctly in the driver parameters.

Action: Specify the correct Authentication ID in the driver parameters. For details, see "Configuring Driver Parameters after Setup Has Been Completed" on page 39.

No Route to Host

Problem: A trace shows the following:

```
  <description>Driver exception.</description>
<exception class-
name="com.Omnibond.system.Command.CommandSessionException">
<message>Error connecting: java.net.NoRouteToHostException: No
route to host
</message>
</exception>
```

Possible Cause: The RACF host address or Telnet port is not specified correctly in the driver parameters.

Action: Specify the correct RACF host address and Telnet port in the driver parameters. For details, see "Configuring Driver Parameters after Setup Has Been Completed" on page 39.

Account Number Has Not Been Defined for Use

Problem: A trace shows the following:

```
  <description>Driver exception.</description>
<exception class-
name="com.Omnibond.system.Command.CommandSessionException">
<message>Error occured during writeLine():
com.Omnibond.system.Command.ScriptException: linenum=6 cursor=0
: Account Number has not been defined for use
</message>
</exception>
```

Possible Cause: The RACF TSO account number is not specified correctly in the driver parameters.

Action: Specify the correct RACF TSO account number in the driver parameters. For details, see "Configuring Driver Parameters after Setup Has Been Completed" on page 39.

Operation Vetoed by Object Matching Policy

Problem: A trace shows the following:

```
Code(-8016) Operation vetoed by object matching policy.
```

Possible Cause: Your Matching policy rejected the operation.

Action: Verify that your Matching policy is working as intended.

Possible Cause: No Matching Policy is in use.

Action: Ensure that a Matching policy that properly implements your installation management policies is provided. Upon installation, Use Default Matching Rules is not enabled by default. For details, see "Setting Global Configuration Values" on page 37.

User Already Logged On

Problem: A trace shows the following:

```
  <description>Driver exception.</description>
<exception class-
name="com.Omnibond.system.Command.CommandSessionException">
<message>Error occured during writeLine():
com.Omnibond.system.Command.ScriptException: linenum=3 cursor=0
: User already logged on
</message>
</exception>
```

Possible Cause: The administrative user ID is specified in the driver parameters could not be logged on by the driver because it is already in use. z/OS does not allow multiple concurrent logons for the same user ID.

Action: Ensure that only the driver uses the administrative user ID.

5.10 Additional Troubleshooting Information Sources

For additional Identity Manager troubleshooting tips see the various troubleshooting topics in the *Identity Manager 3.6.1 Administration Guide* at the Identity Manager 3.6.1 Documentation Web site (http://www.novell.com/documentation/idm36).

z/OS RACF Schema and Driver Processing

A

The Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system) converts commands and events between the eDirectory™ and RACF representations of their information.

This section provides information about the z/OS RACF schema and the driver shim processing relationships between z/OS RACF objects and attributes and RACF commands and their parameters.

Topics include

A.1 z/OS RACF Schema

The following tables describe the schema used by the driver.

Table A-1 *Class User Attribute Descriptions*

Attribute Name	Description
DirXML-RACF-adsp	Automatic Data Set Protection (ADSP) attribute for the user.
DirXML-RACF-auditor	AUDITOR attribute for the user.
DirXML-RACF-category	Installation-defined security categories.
DirXML-RACF-cics-opclass	CICS operator class numbers for basic mapping support (BMS) messages,
DirXML-RACF-cics-opident	CICS operator identification for BMS.
DirXML-RACF-cics-opprty	CICS operator priority.
DirXML-RACF-cics-timeout	CICS operator idle timeout value in hours and minutes.
DirXML-RACF-cics-xrfsoff	CICS user signoff for XRF takeover.
DirXML-RACF-clauth	Classes for which user is allowed to define profiles.
DirXML-RACF-data	Installation-defined data for the user.
DirXML-RACF-dce-autologin	Whether z/OS UNIX DCE is to automatically log this user in.

Attribute Name	Description
DirXML-RACF-dce-dcename	DCE principal name for the user.
DirXML-RACF-dce-homecell	DCE cell name for the user.
DirXML-RACF-dce-homeuuid	DCE universal unique identifier (UUID) for the cell user is defined to.
DirXML-RACF-dce-uuid	DCE universal unique identifier (UUID) of the DCE principal defined in DCENAME.
DirXML-RACF-dfltgrp	Default group for the user.
DirXML-RACF-dfp-dataappl	DFP data application for the user.
DirXML-RACF-dfp-dataclas	Default data class for the user.
DirXML-RACF-dfp-mgmtclas	Default management class for the user.
DirXML-RACF-dfp-storclas	Default storage class for the user.
DirXML-RACF-eim-ldapprof	Name of profile in the LDAPBIND class for the user.
DirXML-RACF-groups	Group connection information for the user.
DirXML-RACF-grpacc	Specifies whether group data sets protected by DATASET profiles defined by the user are automatically accessible to other users in the group.
DirXML-RACF-kerb-encrypt-des	Whether DES encrypted keys are allowed for use.
DirXML-RACF-kerb-encrypt-des3	Whether DES3 encrypted keys are allowed for use.
DirXML-RACF-kerb-encrypt-desd	Whether DESD encrypted keys are allowed for use.
DirXML-RACF-kerb-kerbname	User’s local kerberos-principal-name.
DirXML-RACF-kerb-maxtktlfe	The max-ticket-life in seconds.
DirXML-RACF-language-primary	User’s primary language.
DirXML-RACF-language-secondary	User’s secondary language.
DirXML-RACF-lnotes-sname	Lotus Notes* short-name.
DirXML-RACF-model	User’s model data set profile.
DirXML-RACF-name	User name.
DirXML-RACF-nds-uname	Novell Directory Services® for OS/400 user-name.
DirXML-RACF-netview-consname	Default MCS console name identifier.
DirXML-RACF-netview-ctl	Whether a security check is performed for this NetView operator for span or cross-domain logon.
DirXML-RACF-netview-domains	NetView program identifiers in another NetView domain where this operator can start a cross-domain session.
DirXML-RACF-netview-ic	NetView initial command list string.
DirXML-RACF-netview-msgrecvr	Whether this operator receives unsolicited messages not routed to a specific NetView operator.

Attribute Name	Description
DirXML-RACF-netview-ngmfadmn	Whether NetView operator has administrator authority to NetView Graphic Monitor Facility (NGMF).
DirXML-RACF-netview-ngmfvspn	Reserved for future use by the NetView Graphic Monitor Facility.
DirXML-RACF-netview-opclass	NetView scope classes for which the operator has authority.
DirXML-RACF-omvs-assizemax	The RLIMIT_AS hard limit resource value the user's processes receive when they are dubbed a process.
DirXML-RACF-omvs-cputimemax	The RLIMIT_CPU hard limit resource value the user's processes receive when they are dubbed a process.
DirXML-RACF-omvs-fileprocmax	The maximum number of files the user is allowed to have concurrently active or open.
DirXML-RACF-omvs-home	The user's hierarchical file system (HFS) home directory pathname.
DirXML-RACF-omvs-mmapareamax	The maximum amount of data space storage, in pages, that can be allocated by the user for HFS file memory mapping.
DirXML-RACF-omvs-procusermax	The maximum number of processes the user is allowed to have active at the same time.
DirXML-RACF-omvs-program	The pathname of the user's UNIX shell program.
DirXML-RACF-omvs-threadsmax	The maximum number of pthread_created threads the user can have concurrently active.
DirXML-RACF-omvs-uid	The user's UID.
DirXML-RACF-operations	OPERATIONS attribute for the user.
DirXML-RACF-operparm-altgrp	Console group used in recovery.
DirXML-RACF-operparm-auth	User's authority to issue operator commands.
DirXML-RACF-operparm-auto	Whether the user's MCS console session receives messages which have been automated by the Message Processing Facility (MPF) in the sysplex.
DirXML-RACF-operparm-cmdsys	The system to which commands from the user's MCS console session are sent.
DirXML-RACF-operparm-dom	Which delete operator message (DOM) requests the user's MCS console session receives.
DirXML-RACF-operparm-key	User's name for DISPLAY CONSOLES,KEY.
DirXML-RACF-operparm-level	Message levels the user's MCS console session receives.
DirXML-RACF-operparm-logcmdresp	Whether command responses the user's MCS console session are logged.
DirXML-RACF-operparm-mform	Message format for the user's MCS console session.
DirXML-RACF-operparm-migid	Whether a migration ID is assigned to the user's MCS console session.

Attribute Name	Description
DirXML-RACF-operparm-monitor	Which information is displayed at the user's MCS console session when monitoring jobs, TSO sessions, or data set status.
DirXML-RACF-operparm-mscope	Systems from which the user's MCS console session receives messages not directed to a specific console.
DirXML-RACF-operparm-routcode	Routing codes of messages the user's MCS console session receives.
DirXML-RACF-operparm-storage	Amount of storage in the TSO/E address space that can be used for message queuing to the user's MCS console session.
DirXML-RACF-operparm-ud	Whether the user's MCS console session receives undelivered messages.
DirXML-RACF-ovm-fsroot	The pathname for the file system root.
DirXML-RACF-ovm-home	The user's home directory pathname.
DirXML-RACF-ovm-program	The pathname of the user's UNIX shell program.
DirXML-RACF-ovm-uid	The user's UID.
DirXML-RACF-password-interval	The number of days a password remains valid for the user.
DirXML-RACF-password-passdate	Date the user's password expires.
DirXML-RACF-proxy-binddn	Distinguished name (DN) the z/OS LDAP Server uses when acting as a proxy.
DirXML-RACF-proxy-bindpw	Password the z/OS LDAP Server uses when acting as a proxy.
DirXML-RACF-proxy-ldaphost	URL of the LDAP server the z/OS LDAP Server contacts when acting as a proxy.
DirXML-RACF-restricted	Whether global access checking is bypassed when resource access checking is performed for the user, and neither ID(*) on the access list nor the UACC allow access.
DirXML-RACF-resumedate	Future date the user will be allowed access to the system again.
DirXML-RACF-revoked	Whether the user is prevented from accessing the system.
DirXML-RACF-revokedate	Future date the user will be prevented from accessing the system.
DirXML-RACF-seclabel	The user's default security label.
DirXML-RACF-seclevel	The user's security level.
DirXML-RACF-special	SPECIAL attribute for the user.
DirXML-RACF-tso-acctnum	Default TSO account number on the TSO/E logon panel.
DirXML-RACF-tso-command	Command to be run during TSO/E logon.
DirXML-RACF-tso-dest	Default SYSOUT destination.
DirXML-RACF-tso-holdclass	Default hold class.
DirXML-RACF-tso-jobclass	Default job class.

Attribute Name	Description
DirXML-RACF-tso-maxsize	The maximum region size the user can request at logon.
DirXML-RACF-tso-msgclass	Default message class.
DirXML-RACF-tso-proc	Default logon procedure on the TSO/E logon panel.
DirXML-RACF-tso-seclabel	User's security label.
DirXML-RACF-tso-size	Minimum region size if not requested at logon.
DirXML-RACF-tso-sysoutclass	Default SYSOUT class.
DirXML-RACF-tso-unit	Default UNIT name for allocations.
DirXML-RACF-tso-userdata	Installation-defined data for the user.
DirXML-RACF-uaudit	Whether RACF performs audit logging for the user.
DirXML-RACF-userid	The user's user ID.
DirXML-RACF-when-days	Days of the week when the user is allowed to log on to the system.
DirXML-RACF-when-time	Hours of the day when the user is allowed to log on to the system.
DirXML-RACF-workattr-waaccnt	Account number for APPC/MVS processing.
DirXML-RACF-workattr-waaddr1	Address line 1 for SYSOUT delivery.
DirXML-RACF-workattr-waaddr2	Address line 2 for SYSOUT delivery.
DirXML-RACF-workattr-waaddr3	Address line 3 for SYSOUT delivery.
DirXML-RACF-workattr-waaddr4	Address line 4 for SYSOUT delivery.
DirXML-RACF-workattr-wabldg	Building for SYSOUT delivery.
DirXML-RACF-workattr-wadept	Department for SYSOUT delivery.
DirXML-RACF-workattr-waname	User name for SYSOUT delivery.
DirXML-RACF-workattr-waroom	Room for SYSOUT delivery.

Table A-2 *Class User Attributes*

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-adsp	false	false	false	false	false	state
DirXML-RACF-auditor	false	false	false	false	false	state
DirXML-RACF-category	false	true	false	false	false	string
DirXML-RACF-cics-opclass	false	true	false	false	false	int
DirXML-RACF-cics-opident	false	false	false	false	false	string

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-cics-opprty	false	false	false	false	false	int
DirXML-RACF-cics-timeout	false	false	false	false	false	string
DirXML-RACF-cics-xrfsoff	false	false	false	false	false	string
DirXML-RACF-clauth	false	true	false	false	false	string
DirXML-RACF-data	false	false	false	false	false	string
DirXML-RACF-dce-autologin	false	false	false	false	false	state
DirXML-RACF-dce-dcename	false	false	false	false	false	string
DirXML-RACF-dce-homecell	false	false	false	false	false	string
DirXML-RACF-dce-homeuuid	false	false	false	false	false	string
DirXML-RACF-dce-uuid	false	false	false	false	false	string
DirXML-RACF-dfltgrp	false	false	false	false	false	dn
DirXML-RACF-dfp-dataappl	false	false	false	false	false	string
DirXML-RACF-dfp-dataclas	false	false	false	false	false	string
DirXML-RACF-dfp-mgmtclas	false	false	false	false	false	string
DirXML-RACF-dfp-storclas	false	false	false	false	false	string
DirXML-RACF-eim-ldapprof	false	false	false	false	false	string
DirXML-RACF-groups	false	true	false	false	false	dn
DirXML-RACF-grpacc	false	false	false	false	false	state
DirXML-RACF-kerb-encrypt-des	false	false	false	false	false	state
DirXML-RACF-kerb-encrypt-des3	false	false	false	false	false	state
DirXML-RACF-kerb-encrypt-desd	false	false	false	false	false	state
DirXML-RACF-kerb-kerbname	false	false	false	false	false	string

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-kerb-maxtktlfe	false	false	false	false	false	int
DirXML-RACF-language-primary	false	false	false	false	false	string
DirXML-RACF-language-secondary	false	false	false	false	false	string
DirXML-RACF-lnotes-sname	false	false	false	false	false	string
DirXML-RACF-model	false	false	false	false	false	string
DirXML-RACF-name	false	false	false	false	false	string
DirXML-RACF-nds-uname	false	false	false	false	false	string
DirXML-RACF-netview-consname	false	false	false	false	false	string
DirXML-RACF-netview-ctl	false	false	false	false	false	string
DirXML-RACF-netview-domains	false	true	false	false	false	string
DirXML-RACF-netview-ic	false	false	false	false	false	string
DirXML-RACF-netview-msgrecvr	false	false	false	false	false	state
DirXML-RACF-netview-ngmfadmn	false	false	false	false	false	state
DirXML-RACF-netview-ngmfvspn	false	false	false	false	false	string
DirXML-RACF-netview-opclass	false	true	false	false	false	string
DirXML-RACF-omvs-assizemax	false	false	false	false	false	int
DirXML-RACF-omvs-cputimemax	false	false	false	false	false	int
DirXML-RACF-omvs-fileprocmax	false	false	false	false	false	int
DirXML-RACF-omvs-home	false	false	false	false	false	string
DirXML-RACF-omvs-mmapareamax	false	false	false	false	false	int
DirXML-RACF-omvs-procusermax	false	false	false	false	false	int

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-omvs-program	false	false	false	false	false	string
DirXML-RACF-omvs-threadsmax	false	false	false	false	false	int
DirXML-RACF-omvs-uid	false	false	false	false	false	int
DirXML-RACF-operations	false	false	false	false	false	state
DirXML-RACF-operparm-altgrp	false	false	false	false	false	string
DirXML-RACF-operparm-auth	false	false	false	false	false	string
DirXML-RACF-operparm-auto	false	false	false	false	false	state
DirXML-RACF-operparm-cmdsys	false	false	false	false	false	string
DirXML-RACF-operparm-dom	false	false	false	false	false	string
DirXML-RACF-operparm-key	false	false	false	false	false	string
DirXML-RACF-operparm-level	false	false	false	false	false	string
DirXML-RACF-operparm-logcmdresp	false	false	false	false	false	string
DirXML-RACF-operparm-mform	false	false	false	false	false	string
DirXML-RACF-operparm-migid	false	false	false	false	false	state
DirXML-RACF-operparm-monitor	false	false	false	false	false	string
DirXML-RACF-operparm-mscope	false	true	false	false	false	string
DirXML-RACF-operparm-routcode	false	false	false	false	false	string
DirXML-RACF-operparm-storage	false	false	false	false	false	int
DirXML-RACF-operparm-ud	false	false	false	false	false	state
DirXML-RACF-ovm-fsroot	true	false	false	false	false	string

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-ovm-home	true	false	false	false	false	string
DirXML-RACF-ovm-program	true	false	false	false	false	string
DirXML-RACF-ovm-uid	false	false	false	false	false	int
DirXML-RACF-password-interval	false	false	false	false	false	string
DirXML-RACF-password-passdate	false	false	false	true	false	string
DirXML-RACF-proxy-binddn	false	false	false	false	false	string
DirXML-RACF-proxy-bindpw	false	false	false	false	false	string
DirXML-RACF-proxy-ldaphost	false	false	false	false	false	string
DirXML-RACF-restricted	false	false	false	false	false	state
DirXML-RACF-resumedate	false	false	false	false	false	string
DirXML-RACF-revoked	false	false	false	false	false	state
DirXML-RACF-revokedate	false	false	false	false	false	string
DirXML-RACF-seclabel	false	false	false	false	false	string
DirXML-RACF-seclevel	false	false	false	false	false	string
DirXML-RACF-special	false	false	false	false	false	state
DirXML-RACF-tso-acctnum	false	false	false	false	false	string
DirXML-RACF-tso-command	false	false	false	false	false	string
DirXML-RACF-tso-dest	false	false	false	false	false	string
DirXML-RACF-tso-holdclass	false	false	false	false	false	string
DirXML-RACF-tso-jobclass	false	false	false	false	false	string

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-tso-maxsize	false	false	false	false	false	int
DirXML-RACF-tso-msgclass	false	false	false	false	false	string
DirXML-RACF-tso-proc	false	false	false	false	false	string
DirXML-RACF-tso-seclabel	false	false	false	false	false	string
DirXML-RACF-tso-size	false	false	false	false	false	int
DirXML-RACF-tso-sysoutclass	false	false	false	false	false	string
DirXML-RACF-tso-unit	false	false	false	false	false	string
DirXML-RACF-tso-userdata	false	false	false	false	false	string
DirXML-RACF-uaudit	false	false	false	false	false	state
DirXML-RACF-userid	false	false	true	true	true	string
DirXML-RACF-when-days	false	false	false	false	false	string
DirXML-RACF-when-time	false	false	false	false	false	string
DirXML-RACF-workattr-waaccnt	false	false	false	false	false	string
DirXML-RACF-workattr-waaddr1	false	false	false	false	false	string
DirXML-RACF-workattr-waaddr2	false	false	false	false	false	string
DirXML-RACF-workattr-waaddr3	false	false	false	false	false	string
DirXML-RACF-workattr-waaddr4	false	false	false	false	false	string
DirXML-RACF-workattr-wabldg	false	false	false	false	false	string
DirXML-RACF-workattr-wadept	false	false	false	false	false	string
DirXML-RACF-workattr-waname	false	false	false	false	false	string
DirXML-RACF-workattr-waroom	false	false	false	false	false	string

Table A-3 *Class Group Attribute Descriptions*

Attribute Name	Description
DirXML-RACF-data	Installation-defined data for the group profile.
DirXML-RACF-dfp-dataappl	DFP data application for group data sets.
DirXML-RACF-dfp-dataclas	Default data class for group data sets.
DirXML-RACF-dfp-mgmtclas	Default management class for group data sets.
DirXML-RACF-dfp-storclas	Default storage class for group data sets.
DirXML-RACF-group	The name of the group.
DirXML-RACF-model	Group's model data set profile.
DirXML-RACF-omvs-gid	The group's OMVS GID.
DirXML-RACF-ovm-gid	The group's OVM GID.
DirXML-RACF-owner	Owner of the group.
DirXML-RACF-subgroup	Subordinate groups of the group.
DirXML-RACF-supgroup	Superior group of the group.
DirXML-RACF-termuacc	Whether RACF uses universal access authority for a terminal when checking whether a user in the group is authorized to access a terminal.
DirXML-RACF-tme-roles	TME roles that reference the group.
DirXML-RACF-universal	Whether this is a universal group.

Table A-4 *Class Group Attributes*

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-data	false	false	false	false	false	string
DirXML-RACF-dfp-dataappl	false	false	false	false	false	string
DirXML-RACF-dfp-dataclas	false	false	false	false	false	string
DirXML-RACF-dfp-mgmtclas	false	false	false	false	false	string
DirXML-RACF-dfp-storclas	false	false	false	false	false	string
DirXML-RACF-group	false	false	true	false	true	string
DirXML-RACF-model	false	false	false	false	false	string
DirXML-RACF-omvs-gid	false	false	false	false	false	int

Attribute Name	Case Sensitive	Multivalue	Naming	Read-Only	Required	Type
DirXML-RACF-ovm-gid	false	false	false	false	false	int
DirXML-RACF-owner	false	false	false	false	false	string
DirXML-RACF-subgroup	false	true	false	true	false	dn
DirXML-RACF-supgroup	false	false	false	false	false	dn
DirXML-RACF-termuacc	false	false	false	false	false	state
DirXML-RACF-tme-roles	false	true	false	false	false	string
DirXML-RACF-universal	false	false	false	false	false	state

A.2 RACF Command Parameter Mapping

The following tables show how the driver relates schema attributes to RACF command parameters. For details about RACF command parameters, see your RACF documentation.

IMPORTANT: The driver performs no validation or consistency checking of attribute values received in command documents. If RACF limitations are not met, RACF command processing can produce incomplete, inconsistent, or invalid results.

Table A-5 *ADDUSER Command Mapping*

Parameter	RACF Schema Attribute Name
ADDCATEGORY	DirXML-RACF-category
ADSP	DirXML-RACF-adsp
NOADSP	DirXML-RACF-adsp
AUDITOR	DirXML-RACF-auditor
NOAUDITOR	DirXML-RACF-auditor

Parameter	RACF Schema Attribute Name
CICS OPCLASS	DirXML-RACF-cics-opclass
CICS OPIDENT	DirXML-RACF-cics-opident
CICS OPPRTY	DirXML-RACF-cics-opprty
CICS TIMEOUT	DirXML-RACF-cics-timeout
CICS XRFSOFF	DirXML-RACF-cics-xrfsoff
NOCICS	DirXML-RACF-cics-opclass
NOCICS	DirXML-RACF-cics-opident
NOCICS	DirXML-RACF-cics-opprty
NOCICS	DirXML-RACF-cics-timeout
NOCICS	DirXML-RACF-cics-xrfsoff
CLAUTH	DirXML-RACF-clauth
NOCLAUTH	DirXML-RACF-clauth
DATA	DirXML-RACF-data
DCE AUTOLOGIN	DirXML-RACF-dce-autologin
DCE DCENAME	DirXML-RACF-dce-dcename
DCE HOMECELL	DirXML-RACF-dce-homecell
DCE HOMEUUID	DirXML-RACF-dce-homeuuid
DCE UUID	DirXML-RACF-dce-uuid
DFLTGRP	DirXML-RACF-dfltgrp
DFP DATAAPPL	DirXML-RACF-dfp-dataappl
DFP DATACLAS	DirXML-RACF-dfp-dataclas
DFP MGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP STORCLAS	DirXML-RACF-dfp-storclas
EIM LDAPPROF	DirXML-RACF-eim-ldapprof
GRPACC	DirXML-RACF-grpacc
NOGRPACC	DirXML-RACF-grpacc
KERB DES	DirXML-RACF-kerb-encrypt-des
KERB NODES	DirXML-RACF-kerb-encrypt-des
KERB DES3	DirXML-RACF-kerb-encrypt-des3
KERB NODES3	DirXML-RACF-kerb-encrypt-des3
KERB DESD	DirXML-RACF-kerb-encrypt-desd
KERB NODESD	DirXML-RACF-kerb-encrypt-desd

Parameter	RACF Schema Attribute Name
KERB KERBNAME	DirXML-RACF-kerb-kerbname
KERB MAXTKTLFE	DirXML-RACF-kerb-maxtktlfe
LANGUAGE PRIMARY	DirXML-RACF-language-primary
LANGUAGE SECONDARY	DirXML-RACF-language-secondary
LNOTES SNAME	DirXML-RACF-lnotes-sname
MODEL	DirXML-RACF-model
NAME	DirXML-RACF-name
NDS UNAME	DirXML-RACF-nds-uname
NETVIEW CONSNAME	DirXML-RACF-netview-consname
NETVIEW CTL	DirXML-RACF-netview-ctl
NETVIEW DOMAINS	DirXML-RACF-netview-domains
NETVIEW IC	DirXML-RACF-netview-ic
NETVIEW MSGRECVR	DirXML-RACF-netview-msgrecvr
NETVIEW NGMFADMN	DirXML-RACF-netview-ngmfadmn
NETVIEW NGMFVSPN	DirXML-RACF-netview-ngmfvspn
NETVIEW OPCLASS	DirXML-RACF-netview-opclass
OMVS ASSIZEMAX	DirXML-RACF-omvs-assizemax
OMVS UID	DirXML-RACF-omvs-uid
OMVS CPUTIMEMAX	DirXML-RACF-omvs-cputimemax
OMVS FILEPROCMAX	DirXML-RACF-omvs-fileprocmax
OMVS HOME	DirXML-RACF-omvs-home
OMVS MMAPAREAMAX	DirXML-RACF-omvs-mmapareamax
OMVS PROCUSERMAX	DirXML-RACF-omvs-procusermax
OMVS PROGRAM	DirXML-RACF-omvs-program
OMVS THREADSMAX	DirXML-RACF-omvs-threadsmax
OPERATIONS	DirXML-RACF-operations
NOOPERATIONS	DirXML-RACF-operations
OPERPARM ALTGRP	DirXML-RACF-operparm-altgrp
OPERPARM AUTO	DirXML-RACF-operparm-auto
OPERPARM CMDSYS	DirXML-RACF-operparm-cmdsys
OPERPARM DOM	DirXML-RACF-operparm-dom
OPERPARM KEY	DirXML-RACF-operparm-key

Parameter	RACF Schema Attribute Name
OPERPARM LEVEL	DirXML-RACF-operparm-level
OPERPARM LOGCMDRESP	DirXML-RACF-operparm-logcmdresp
OPERPARM MFORM	DirXML-RACF-operparm-mform
OPERPARM MIGID	DirXML-RACF-operparm-migid
OPERPARM MONITOR	DirXML-RACF-operparm-monitor
OPERPARM MSCOPE	DirXML-RACF-operparm-mscope
OPERPARM ROUTCODE	DirXML-RACF-operparm-routcode
OPERPARM STORAGE	DirXML-RACF-operparm-storage
OPERPARM UD	DirXML-RACF-operparm-ud
OVM FSROOT	DirXML-RACF-ovm-fsroot
OVM HOME	DirXML-RACF-ovm-home
OVM PROGRAM	DirXML-RACF-ovm-program
OVM UID	DirXML-RACF-ovm-uid
PROXY LDAPHOST	DirXML-RACF-proxy-ldaphost
PROXY BINDDN	DirXML-RACF-proxy-binddn
PROXY BINDPW	DirXML-RACF-proxy-bindpw
RESTRICTED	DirXML-RACF-restricted
NORESTRICTED	DirXML-RACF-restricted
REVOKE	DirXML-RACF-revoked
RESUME	DirXML-RACF-revoked
SECLABEL	DirXML-RACF-seclabel
SECLEVEL	DirXML-RACF-seclevel
SPECIAL	DirXML-RACF-special
NOSPECIAL	DirXML-RACF-special
TSO ACCTNUM	DirXML-RACF-tso-acctnum
TSO COMMAND	DirXML-RACF-tso-command
TSO DEST	DirXML-RACF-tso-dest
TSO HOLDCLASS	DirXML-RACF-tso-holdclass
TSO JOBCLASS	DirXML-RACF-tso-jobclass
TSO MAXSIZE	DirXML-RACF-tso-maxsize
TSO MSGCLASS	DirXML-RACF-tso-msgclass
TSO PROC	DirXML-RACF-tso-proc

Parameter	RACF Schema Attribute Name
TSO SECLABEL	DirXML-RACF-tso-seclabel
TSO SIZE	DirXML-RACF-tso-size
TSO SYSOUTCLASS	DirXML-RACF-tso-sysoutclass
TSO UNIT	DirXML-RACF-tso-unit
TSO USERDATA	DirXML-RACF-tso-userdata
WHEN DAYS	DirXML-RACF-when-days
WHEN TIME	DirXML-RACF-when-time
WORKATTR WAACCNT	DirXML-RACF-workattr-waaccnt
WORKATTR WAADDR1	DirXML-RACF-workattr-waaddr1
WORKATTR WAADDR2	DirXML-RACF-workattr-waaddr2
WORKATTR WAADDR3	DirXML-RACF-workattr-waaddr3
WORKATTR WAADDR4	DirXML-RACF-workattr-waaddr4
WORKATTR WABLDG	DirXML-RACF-workattr-wabldg
WORKATTR WADEPT	DirXML-RACF-workattr-wadept
WORKATTR WANAME	DirXML-RACF-workattr-waname
WORKATTR WAROOM	DirXML-RACF-workattr-waroom

Table A-6 *ALTUSER Command Mapping*

Parameter	RACF Schema Attribute Name
ADDCATEGORY	DirXML-RACF-category
DELCATEGORY	DirXML-RACF-category
ADSP	DirXML-RACF-adsp
NOADSP	DirXML-RACF-adsp
AUDITOR	DirXML-RACF-auditor
NOAUDITOR	DirXML-RACF-auditor
CICS OPCLASS	DirXML-RACF-cics-opclass
CICS ADDOPCLASS	DirXML-RACF-cics-opclass
CICS DELOPCLASS	DirXML-RACF-cics-opclass
CICS NOOPCLASS	DirXML-RACF-cics-opclass
CICS OPIDENT	DirXML-RACF-cics-opident
CICS NOOPIDENT	DirXML-RACF-cics-opident
CICS OPPRTY	DirXML-RACF-cics-opprty

Parameter	RACF Schema Attribute Name
CICS NOOPPRTY	DirXML-RACF-cics-opprty
CICS TIMEOUT	DirXML-RACF-cics-timeout
CICS NOTIMEOUT	DirXML-RACF-cics-timeout
CICS XRFSOFF	DirXML-RACF-cics-xrfsoff
CICS NOXRFSOFF	DirXML-RACF-cics-xrfsoff
NOCICS	DirXML-RACF-cics-opclass
NOCICS	DirXML-RACF-cics-opident
NOCICS	DirXML-RACF-cics-opprty
NOCICS	DirXML-RACF-cics-timeout
NOCICS	DirXML-RACF-cics-xrfsoff
CLAUTH	DirXML-RACF-clauth
NOCLAUTH	DirXML-RACF-clauth
DATA	DirXML-RACF-data
NODATA	DirXML-RACF-data
DCE AUTOLOGIN	DirXML-RACF-dce-autologin
DCE NOAUTOLOGIN	DirXML-RACF-dce-autologin
DCE DCENAME	DirXML-RACF-dce-dcename
DCE NODCENAME	DirXML-RACF-dce-dcename
DCE HOMECELL	DirXML-RACF-dce-homecell
DCE NOHOMECELL	DirXML-RACF-dce-homecell
DCE HOMEUUID	DirXML-RACF-dce-homeuuid
DCE NOHOMEUUID	DirXML-RACF-dce-homeuuid
DCE UUID	DirXML-RACF-dce-uuid
DCE NOUUID	DirXML-RACF-dce-uuid
NODCE	DirXML-RACF-dce-autologin
NODCE	DirXML-RACF-dce-dcename
NODCE	DirXML-RACF-dce-homecell
NODCE	DirXML-RACF-dce-homeuuid
NODCE	DirXML-RACF-dce-uuid
DFLTGRP	DirXML-RACF-dfltgrp
DFP DATAAPPL	DirXML-RACF-dfp-dataappl
DFP NODATAAPPL	DirXML-RACF-dfp-dataappl

Parameter	RACF Schema Attribute Name
DFP DATACLAS	DirXML-RACF-dfp-dataclas
DFP NODATACLAS	DirXML-RACF-dfp-dataclas
DFP MGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP NOMGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP STORCLAS	DirXML-RACF-dfp-storclas
DFP NOSTORCLAS	DirXML-RACF-dfp-storclas
NODFP	DirXML-RACF-dfp-dataappl
NODFP	DirXML-RACF-dfp-dataclas
NODFP	DirXML-RACF-dfp-mgmtclas
NODFP	DirXML-RACF-dfp-storclas
EIM LDAPPROF	DirXML-RACF-eim-ldapprof
EIM NOLDAPPROF	DirXML-RACF-eim-ldapprof
NOEIM	DirXML-RACF-eim-ldapprof
GRPACC	DirXML-RACF-grpacc
NOGRPACC	DirXML-RACF-grpacc
KERB DES	DirXML-RACF-kerb-encrypt-des
KERB NODES	DirXML-RACF-kerb-encrypt-des
KERB DES3	DirXML-RACF-kerb-encrypt-des3
KERB NODES3	DirXML-RACF-kerb-encrypt-des3
KERB DESD	DirXML-RACF-kerb-encrypt-desd
KERB NODESD	DirXML-RACF-kerb-encrypt-desd
KERB NOENCRYPT	DirXML-RACF-kerb-encrypt-des
KERB NOENCRYPT	DirXML-RACF-kerb-encrypt-des3
KERB NOENCRYPT	DirXML-RACF-kerb-encrypt-desd
KERB KERBNAME	DirXML-RACF-kerb-kerbname
KERB NOKERBNAME	DirXML-RACF-kerb-kerbname
KERB MAXTKTLFE	DirXML-RACF-kerb-maxtktlfe
KERB NOMAXTKTLFE	DirXML-RACF-kerb-maxtktlfe
NOKERB	DirXML-RACF-kerb-encrypt-des
NOKERB	DirXML-RACF-kerb-encrypt-des3
NOKERB	DirXML-RACF-kerb-encrypt-desd
NOKERB	DirXML-RACF-kerb-kerbname

Parameter	RACF Schema Attribute Name
NOKERB	DirXML-RACF-kerb-maxtktlfe
LANGUAGE PRIMARY	DirXML-RACF-language-primary
LANGUAGE NOPRIMARY	DirXML-RACF-language-primary
LANGUAGE SECONDARY	DirXML-RACF-language-secondary
LANGUAGE NOSECONDARY	DirXML-RACF-language-secondary
NOCICS	DirXML-RACF-cics-opclass
NOCICS	DirXML-RACF-cics-opident
NOCICS	DirXML-RACF-cics-opprty
NOCICS	DirXML-RACF-cics-timeout
NOCICS	DirXML-RACF-cics-xrfsoff
LNOTES SNAME	DirXML-RACF-lnotes-sname
LNOTES NOSNAME	DirXML-RACF-lnotes-sname
NOLNOTES	DirXML-RACF-lnotes-sname
MODEL	DirXML-RACF-model
NOMODEL	DirXML-RACF-model
NAME	DirXML-RACF-name
NDS UNAME	DirXML-RACF-nds-uname
NDS NOUNAME	DirXML-RACF-nds-uname
NONDS	DirXML-RACF-nds-uname
NETVIEW CONSNAME	DirXML-RACF-netview-consname
NETVIEW NOCONSNAME	DirXML-RACF-netview-consname
NETVIEW CTL	DirXML-RACF-netview-ctl
NETVIEW NOCTL	DirXML-RACF-netview-ctl
NETVIEW DOMAINS	DirXML-RACF-netview-domains
NETVIEW ADDDOMAINS	DirXML-RACF-netview-domains
NETVIEW DELDOMAINS	DirXML-RACF-netview-domains
NETVIEW NODOMAINS	DirXML-RACF-netview-domains
NETVIEW IC	DirXML-RACF-netview-ic
NETVIEW NOIC	DirXML-RACF-netview-ic
NETVIEW MSGRECVR	DirXML-RACF-netview-msgrecvr
NETVIEW NOMSGRECVR	DirXML-RACF-netview-msgrecvr
NETVIEW NGMFADMN	DirXML-RACF-netview-ngmfadmn

Parameter	RACF Schema Attribute Name
NETVIEW NONGMFADMN	DirXML-RACF-netview-ngmfadmn
NETVIEW NGMFVSPN	DirXML-RACF-netview-ngmfvspn
NETVIEW NONGMFVSPN	DirXML-RACF-netview-ngmfvspn
NETVIEW OPCLASS	DirXML-RACF-netview-opclass
NETVIEW ADDOPCLASS	DirXML-RACF-netview-opclass
NETVIEW DELOPCLASS	DirXML-RACF-netview-opclass
NETVIEW NOOPCLASS	DirXML-RACF-netview-opclass
NONETVIEW	DirXML-RACF-netview-consname
NONETVIEW	DirXML-RACF-netview-ctl
NONETVIEW	DirXML-RACF-netview-domains
NONETVIEW	DirXML-RACF-netview-ic
NONETVIEW	DirXML-RACF-netview-msgrecvr
NONETVIEW	DirXML-RACF-netview-ngmfadmn
NONETVIEW	DirXML-RACF-netview-ngmfvspn
NONETVIEW	DirXML-RACF-netview-opclass
OMVS ASSIZEMAX	DirXML-RACF-omvs-assizemax
OMVS NOASSIZEMAX	DirXML-RACF-omvs-assizemax
OMVS UID	DirXML-RACF-omvs-uid
OMVS NOUID	DirXML-RACF-omvs-uid
OMVS CPUTIMEMAX	DirXML-RACF-omvs-cputimemax
OMVS NOCPUTIMEMAX	DirXML-RACF-omvs-cputimemax
OMVS FILEPROCMAX	DirXML-RACF-omvs-fileprocmax
OMVS NOFILEPROCMAX	DirXML-RACF-omvs-fileprocmax
OMVS HOME	DirXML-RACF-omvs-home
OMVS NOHOME	DirXML-RACF-omvs-home
OMVS MMAPAREAMAX	DirXML-RACF-omvs-mmapareamax
OMVS NOMMAPAREAMAX	DirXML-RACF-omvs-mmapareamax
OMVS PROCUSERMAX	DirXML-RACF-omvs-procusermax
OMVS NOPROCUSERMAX	DirXML-RACF-omvs-procusermax
OMVS PROGRAM	DirXML-RACF-omvs-program
OMVS NOPROGRAM	DirXML-RACF-omvs-program
OMVS THREADSMAX	DirXML-RACF-omvs-threadsmax

Parameter	RACF Schema Attribute Name
OMVS NOTHREADSMAX	DirXML-RACF-omvs-threadsmax
NOOMVS	DirXML-RACF-omvs-assizemax
NOOMVS	DirXML-RACF-omvs-uid
NOOMVS	DirXML-RACF-omvs-cputimemax
NOOMVS	DirXML-RACF-omvs-fileprocmax
NOOMVS	DirXML-RACF-omvs-home
NOOMVS	DirXML-RACF-omvs-mmapareamax
NOOMVS	DirXML-RACF-omvs-procusermax
NOOMVS	DirXML-RACF-omvs-program
NOOMVS	DirXML-RACF-omvs-threadsmax
OPERATIONS	DirXML-RACF-operations
NOOPERATIONS	DirXML-RACF-operations
OPERPARM ALTGRP	DirXML-RACF-operparm-altgrp
OPERPARM NOALTGRP	DirXML-RACF-operparm-altgrp
OPERPARM AUTO	DirXML-RACF-operparm-auto
OPERPARM NOAUTO	DirXML-RACF-operparm-auto
OPERPARM CMDSYS	DirXML-RACF-operparm-cmdsys
OPERPARM NOCMDSYS	DirXML-RACF-operparm-cmdsys
OPERPARM DOM	DirXML-RACF-operparm-dom
OPERPARM NODOM	DirXML-RACF-operparm-dom
OPERPARM KEY	DirXML-RACF-operparm-key
OPERPARM NOKEY	DirXML-RACF-operparm-key
OPERPARM LEVEL	DirXML-RACF-operparm-level
OPERPARM NOLEVEL	DirXML-RACF-operparm-level
OPERPARM LOGCMDRESP	DirXML-RACF-operparm-logcmdresp
OPERPARM NOLOGCMDRESP	DirXML-RACF-operparm-logcmdresp
OPERPARM MFORM	DirXML-RACF-operparm-mform
OPERPARM NOMFORM	DirXML-RACF-operparm-mform
OPERPARM MIGID	DirXML-RACF-operparm-migid
OPERPARM NOMIGID	DirXML-RACF-operparm-migid
OPERPARM MONITOR	DirXML-RACF-operparm-monitor
OPERPARM NOMONITOR	DirXML-RACF-operparm-monitor

Parameter	RACF Schema Attribute Name
OPERPARM MSCOPE	DirXML-RACF-operparm-mscope
OPERPARM ADDMSCOPE	DirXML-RACF-operparm-mscope
OPERPARM DELMSCOPE	DirXML-RACF-operparm-mscope
OPERPARM NOMSCOPE	DirXML-RACF-operparm-mscope
OPERPARM ROUTCODE	DirXML-RACF-operparm-routcode
OPERPARM NOROUTCODE	DirXML-RACF-operparm-routcode
OPERPARM STORAGE	DirXML-RACF-operparm-storage
OPERPARM NOSTORAGE	DirXML-RACF-operparm-storage
OPERPARM UD	DirXML-RACF-operparm-ud
OPERPARM NOUD	DirXML-RACF-operparm-ud
NOOPERPARM	DirXML-RACF-operparm-altgrp
NOOPERPARM	DirXML-RACF-operparm-auth
NOOPERPARM	DirXML-RACF-operparm-auto
NOOPERPARM	DirXML-RACF-operparm-cmdsys
NOOPERPARM	DirXML-RACF-operparm-dom
NOOPERPARM	DirXML-RACF-operparm-key
NOOPERPARM	DirXML-RACF-operparm-level
NOOPERPARM	DirXML-RACF-operparm-logcmdresp
NOOPERPARM	DirXML-RACF-operparm-mform
NOOPERPARM	DirXML-RACF-operparm-migid
NOOPERPARM	DirXML-RACF-operparm-monitor
NOOPERPARM	DirXML-RACF-operparm-mscope
NOOPERPARM	DirXML-RACF-operparm-routcode
NOOPERPARM	DirXML-RACF-operparm-storage
NOOPERPARM	DirXML-RACF-operparm-ud
OVM FSROOT	DirXML-RACF-ovm-fsroot
OVM NOFSROOT	DirXML-RACF-ovm-fsroot
OVM HOME	DirXML-RACF-ovm-home
OVM NOHOME	DirXML-RACF-ovm-home
OVM PROGRAM	DirXML-RACF-ovm-program
OVM NOPROGRAM	DirXML-RACF-ovm-program
OVM UID	DirXML-RACF-ovm-uid

Parameter	RACF Schema Attribute Name
OVM NOUID	DirXML-RACF-ovm-uid
NOOVM	DirXML-RACF-ovm-fsroot
NOOVM	DirXML-RACF-ovm-home
NOOVM	DirXML-RACF-ovm-program
NOOVM	DirXML-RACF-ovm-uid
PROXY LDAPHOST	DirXML-RACF-proxy-ldaphost
PROXY NOLDAPHOST	DirXML-RACF-proxy-ldaphost
PROXY BINDDN	DirXML-RACF-proxy-binddn
PROXY NOBINDDN	DirXML-RACF-proxy-binddn
PROXY BINDPW	DirXML-RACF-proxy-bindpw
PROXY NOBINDPW	DirXML-RACF-proxy-bindpw
NOPROXY	DirXML-RACF-proxy-ldaphost
NOPROXY	DirXML-RACF-proxy-binddn
NOPROXY	DirXML-RACF-proxy-bindpw
RESTRICTED	DirXML-RACF-restricted
NORESTRICTED	DirXML-RACF-restricted
REVOKE	DirXML-RACF-revoked
RESUME	DirXML-RACF-revoked
SECLABEL	DirXML-RACF-seclabel
NOSECLABEL	DirXML-RACF-seclabel
SECLEVEL	DirXML-RACF-seclevel
NOSECLEVEL	DirXML-RACF-seclevel
SPECIAL	DirXML-RACF-special
NOSPECIAL	DirXML-RACF-special
TSO ACCTNUM	DirXML-RACF-tso-acctnum
TSO NOACCTNUM	DirXML-RACF-tso-acctnum
TSO COMMAND	DirXML-RACF-tso-command
TSO NOCOMMAND	DirXML-RACF-tso-command
TSO DEST	DirXML-RACF-tso-dest
TSO NODEST	DirXML-RACF-tso-dest
TSO HOLDCLASS	DirXML-RACF-tso-holdclass
TSO NOHOLDCLASS	DirXML-RACF-tso-holdclass

Parameter	RACF Schema Attribute Name
TSO JOBCLASS	DirXML-RACF-tso-jobclass
TSO NOJOBCLASS	DirXML-RACF-tso-jobclass
TSO MAXSIZE	DirXML-RACF-tso-maxsize
TSO NOMAXSIZE	DirXML-RACF-tso-maxsize
TSO MSGCLASS	DirXML-RACF-tso-msgclass
TSO NOMSGCLASS	DirXML-RACF-tso-msgclass
TSO PROC	DirXML-RACF-tso-proc
TSO NOPROC	DirXML-RACF-tso-proc
TSO SECLABEL	DirXML-RACF-tso-seclabel
TSO NOSECLABEL	DirXML-RACF-tso-seclabel
TSO SIZE	DirXML-RACF-tso-size
TSO NOSIZE	DirXML-RACF-tso-size
TSO SYSOUTCLASS	DirXML-RACF-tso-sysoutclass
TSO NOSYSOUTCLASS	DirXML-RACF-tso-sysoutclass
TSO UNIT	DirXML-RACF-tso-unit
TSO NOUNIT	DirXML-RACF-tso-unit
TSO USERDATA	DirXML-RACF-tso-userdata
TSO NOUSERDATA	DirXML-RACF-tso-userdata
NOTSO	DirXML-RACF-tso-acctnum
NOTSO	DirXML-RACF-tso-command
NOTSO	DirXML-RACF-tso-dest
NOTSO	DirXML-RACF-tso-holdclass
NOTSO	DirXML-RACF-tso-jobclass
NOTSO	DirXML-RACF-tso-maxsize
NOTSO	DirXML-RACF-tso-msgclass
NOTSO	DirXML-RACF-tso-proc
NOTSO	DirXML-RACF-tso-seclabel
NOTSO	DirXML-RACF-tso-size
NOTSO	DirXML-RACF-tso-sysoutclass
NOTSO	DirXML-RACF-tso-unit
NOTSO	DirXML-RACF-tso-userdata
UAUDIT	DirXML-RACF-uaudit

Parameter	RACF Schema Attribute Name
NOUAUDIT	DirXML-RACF-uaudit
WHEN DAYS	DirXML-RACF-when-days
WHEN TIME	DirXML-RACF-when-time
WORKATTR WAACCNT	DirXML-RACF-workattr-waaccnt
WORKATTR NOWAACCNT	DirXML-RACF-workattr-waaccnt
WORKATTR WAADDR1	DirXML-RACF-workattr-waaddr1
WORKATTR NOWAADDR1	DirXML-RACF-workattr-waaddr1
WORKATTR WAADDR2	DirXML-RACF-workattr-waaddr2
WORKATTR NOWAADDR2	DirXML-RACF-workattr-waaddr2
WORKATTR WAADDR3	DirXML-RACF-workattr-waaddr3
WORKATTR NOWAADDR3	DirXML-RACF-workattr-waaddr3
WORKATTR WAADDR4	DirXML-RACF-workattr-waaddr4
WORKATTR NOWAADDR4	DirXML-RACF-workattr-waaddr4
WORKATTR WABLDG	DirXML-RACF-workattr-wabldg
WORKATTR NOWABLDG	DirXML-RACF-workattr-wabldg
WORKATTR WADEPT	DirXML-RACF-workattr-wadept
WORKATTR NOWADEPT	DirXML-RACF-workattr-wadept
WORKATTR WANAME	DirXML-RACF-workattr-waname
WORKATTR NOWANAME	DirXML-RACF-workattr-waname
WORKATTR WAROOM	DirXML-RACF-workattr-waroom
WORKATTR NOWAROOM	DirXML-RACF-workattr-waroom
NOWORKATTR	DirXML-RACF-workattr-waaccnt
NOWORKATTR	DirXML-RACF-workattr-waaddr1
NOWORKATTR	DirXML-RACF-workattr-waaddr2
NOWORKATTR	DirXML-RACF-workattr-waaddr3
NOWORKATTR	DirXML-RACF-workattr-waaddr4
NOWORKATTR	DirXML-RACF-workattr-wabldg
NOWORKATTR	DirXML-RACF-workattr-wadept
NOWORKATTR	DirXML-RACF-workattr-waname
NOWORKATTR	DirXML-RACF-workattr-waroom

Table A-7 *ADDGROUP Command Mapping*

Parameter	RACF Schema Attribute Name
DATA	DirXML-RACF-data
DFP DATAAPPL	DirXML-RACF-dfp-dataappl
DFP DATACLAS	DirXML-RACF-dfp-dataclas
DFP MGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP STORCLAS	DirXML-RACF-dfp-storclas
MODEL	DirXML-RACF-model
OMVS GID	DirXML-RACF-omvs-gid
OVM GID	DirXML-RACF-ovm-gid
OWNER	DirXML-RACF-owner
SUPGROUP	DirXML-RACF-supgroup
TERMUACC	DirXML-RACF-termuacc
TME ROLES	DirXML-RACF-tme-roles
UNIVERSAL	DirXML-RACF-universal

Table A-8 *ALTGROUP Command Mapping*

Parameter	RACF Schema Attribute Name
DATA	DirXML-RACF-data
NODATA	DirXML-RACF-data
DFP DATAAPPL	DirXML-RACF-dfp-dataappl
DFP NODATAAPPL	DirXML-RACF-dfp-dataappl
DFP DATACLAS	DirXML-RACF-dfp-dataclas
DFP NODATACLAS	DirXML-RACF-dfp-dataclas
DFP MGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP NOMGMTCLAS	DirXML-RACF-dfp-mgmtclas
DFP STORCLAS	DirXML-RACF-dfp-storclas
DFP NOSTORCLAS	DirXML-RACF-dfp-storclas
NODFP	DirXML-RACF-dfp-dataappl
NODFP	DirXML-RACF-dfp-dataclas
NODFP	DirXML-RACF-dfp-mgmtclas
NODFP	DirXML-RACF-dfp-storclas
MODEL	DirXML-RACF-model

Parameter	RACF Schema Attribute Name
NOMODEL	DirXML-RACF-model
OMVS GID	DirXML-RACF-omvs-gid
OMVS NOGID	DirXML-RACF-omvs-gid
NOOMVS	DirXML-RACF-omvs-gid
OVM GID	DirXML-RACF-ovm-gid
OVM NOGID	DirXML-RACF-ovm-gid
NOOVM	DirXML-RACF-ovm-gid
OWNER	DirXML-RACF-owner
SUPGROUP	DirXML-RACF-supgroup
TERMUACC	DirXML-RACF-termuacc
NOTERMUACC	DirXML-RACF-termuacc
TME ROLES	DirXML-RACF-tme-roles
TME ADDROLES	DirXML-RACF-tme-roles
TME DELROLES	DirXML-RACF-tme-roles
TME NOROLES	DirXML-RACF-tme-roles
NOTME	DirXML-RACF-tme-roles

Table A-9 *CONNECT Command Mapping*

Parameter	RACF Schema Attribute Name
GROUP	DirXML-RACF-groups

Table A-10 *REMOVE Command Mapping*

Parameter	RACF Schema Attribute Name
GROUP	DirXML-RACF-groups

Table A-11 *PASSWORD Command Mapping*

Parameter	RACF Schema Attribute Name
USER	DirXML-RACF-userid
INTERVAL	DirXML-RACF-password-interval
NOINTERVAL	DirXML-RACF-password-interval

A.3 Driver Processing of Attributes and Commands

XDS Commands involving z/OS RACF schema attributes are processed by the Subscriber channel subject to the limitations of RACF. If operations that do not conform to the RACF design are specified, the results are unpredictable. For detailed information about the processing of RACF commands, see your RACF documentation.

Some RACF command parameters and values, or combinations of parameters and values can produce results that cannot be directly codified in the events generated by the Publisher channel. Other RACF processing, such as a user being revoked because of an excessive number of invalid password attempts, does not cause an event. Changes made directly to the RACF database, such as those made using ICHEINTY, do not cause events.

Changes made in eDirectory or RACF cannot always be sent round trip through the driver into the other and then back again unchanged because not all mapped attributes correspond precisely.

Certain combinations of RACF command parameters, and other RACF processing, can result in an inconsistent state between the RACF database and the z/OS RACF schema attributes stored in the auxiliary classes.

The following sections describe the handling of certain special cases by the driver.

A.3.1 DirXML-RACF-revoked, DirXML-RACF-revokedate, and DirXML-RACF-resumedate

RACF maintains a future REVOKE date (which can be not-specified), a future RESUME date (which can be not-specified), and a revoked state for each user in the RACF database. Setting and unsetting the revoked state clears both date fields. If RACF revokes a user due to inactivity or due to excessive invalid password attempts, it clears both date fields.

DirXML-RACF-revoked, DirXML-RACF-revokedate, and DirXML-RACF-resumedate are processed by the Subscriber channel using the REVOKE and RESUME parameters of the ALTUSER RACF command.

The Publisher channel publishes changes to DirXML-RACF-revoked, DirXML-RACF-revokedate, and DirXML-RACF-resumedate when a RACF ALTUSER command with a REVOKE or RESUME parameter is issued. It also provides these attributes when requested by a query operation. Changes that occur as a side effect of some action, such as the revoking of a user because of excessive invalid password attempts, do not generate events to be published.

The following sections describe the processing of XDS modify command elements for these schema attributes by the Subscriber channel.

Except as noted, XDS modify commands that contain changes for these attributes in combination produce unpredictable results.

DirXML-RACF-revoked Value=true

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-revoked">
    <remove-all-values/>
    <add-value>
      <value>true</value>
    </add-value>
  </modify-attr>
</modify>
```

The Subscriber channel treats a remove-all-values followed by an add-value as a replace operation for the attribute value.

```
ALTUSER (MEI) REVOKE
```

RACF processes a REVOKE without a date to take effect immediately. Any pending REVOKE date or RESUME date is cleared. If REVOKE is already in effect for the user, RACF ignores the REVOKE parameter and issues a message. This message appears in the status document returned by the Subscriber channel.

DirXML-RACF-revoked Value=false

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-revoked">
    <remove-all-values/>
    <add-value>
      <value>false</value>
    </add-value>
  </modify-attr>
</modify>
```

The Subscriber channel treats a remove-all-values followed by an add-value as a replace operation for the attribute value.

```
ALTUSER (MEI) RESUME
```

RACF processes a RESUME without a date to take effect immediately. Any pending REVOKE date or RESUME date is cleared. If no REVOKE or pending REVOKE is in effect for the user, RACF ignores the RESUME parameter.

DirXML-RACF-revoked Remove-All-Values

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-revoked">
    <remove-all-values/>
  </modify-attr>
</modify>
```

The Subscriber channel treats a remove-all-values for DirXML-RACF-revoked as a RESUME.

```
ALTUSER (MEI) RESUME
```

DirXML-RACF-revokedate Value= *mm/dd/yy*

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-revokedate">
    <remove-all-values/>
    <add-value>
      <value>08/13/18</value>
    </add-value>
  </modify-attr>
</modify>
```

The Subscriber channel treats a remove-all-values followed by an add-value as a replace operation for the attribute value.

```
ALTUSER (MEI) REVOKE(08/13/18)
```

RACF establishes a pending REVOKE for the user that will take effect on August 13, 2018. If REVOKE is already in effect for the user, RACF ignores the REVOKE parameter and issues a message. This message appears in the status document returned by the Subscriber channel.

DirXML-RACF-revokedate Remove-All-Values

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-revokedate">
    <remove-all-values/>
  </modify-attr>
</modify>
```

There is no RACF command to explicitly clear the RACF REVOKE date. The Subscriber channel does not process remove-all-values for DirXML-RACF-revokedate.

DirXML-RACF-resumedate Value= *mm/dd/yy*

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-resumedate">
    <remove-all-values/>
    <add-value>
      <value>09/11/25</value>
    </add-value>
  </modify-attr>
</modify>
```

The Subscriber channel treats a remove-all-values followed by an add-value as a replace operation for the attribute value.

```
ALTUSER (MEI) RESUME(09/11/25)
```

RACF establishes a pending RESUME for the user that will take effect on September 11, 2025. If no REVOKE or pending REVOKE is in effect for the user, RACF ignores the RESUME parameter.

DirXML-RACF-resumedate Remove-All-Values

Assume the following modify command.

```
<modify class-name="User" event-id="27" src-dn="\DigitalAirLines\users\mei">
  <association>USER/MEI</association>
  <modify-attr attr-name="DirXML-RACF-resumedate">
    <remove-all-values/>
  </modify-attr>
</modify>
```

There is no RACF command to explicitly clear the RACF RESUME date. The Subscriber channel does not process remove-all-values for DirXML-DirXML-RACF-resumedate.

Modify Commands for Combinations of DirXML-RACF-revoked, DirXML-RACF-revokedate, and DirXML-RACF-resume

The Subscriber channel processes modify commands for combinations of DirXML-RACF-revoked, DirXML-RACF-revokedate, and DirXML-RACF-resume the same way it processes these attributes individually, as described in the preceding sections.

The Subscriber channel constructs RACF commands using the values provided in the XDS documents that it receives. It is important to note that some combinations are not meaningful.

A.3.2 Password Synchronization

If you omit the PASSWORD parameter or specify a PASSWORD parameter with no value on a RACF ADDUSER command, RACF sets the default password the same as the name of the user's default group. If you specify a PASSWORD parameter with no value on a RACF ALTUSER command, RACF sets the password the same as the name of the user's default group. The driver publishes a password with the value of the default group in these cases.

If you enter an ALTUSER command for a user with a DFLTGRP parameter and a PASSWORD parameter with no value, RACF sets the password value to the name of the previous default group. It is not possible to determine the name of the previous default group. The driver does not publish a password in this case.

A.3.3 ADDUSER and ALTUSER: NOPASSWORD and OIDCARD/NOOIDCARD Parameters

User IDs with NOPASSWORD and NOOIDCARD are known to RACF as *protected user IDs*. Protected user IDs cannot access the system by any means that requires a password and cannot be revoked by excessive invalid password attempts. Protected user IDs are used for started tasks, production batch processing, and other similar purposes. Protected user IDs are not intended for end users or other systems.

The Publisher channel does not publish events for protected user IDs. The Subscriber channel rejects commands for protected user IDs.

If you specify the OIDCARD parameter on an ADDUSER or ALTUSER RACF command, the system prompts you to enter the operator identification card at the terminal reader. No other method is provided for entering the OIDCARD data. NOOIDCARD is the default for users when they are created.

No z/OS RACF schema attribute is provided for the NOPASSWORD, OIDCARD, and NOOIDCARD parameters of the ADDUSER and ALTUSER RACF commands

For more information about protected user IDs and operator identification cards, see your RACF documentation.

Example ADDUSER NOPASSWORD Processing

The driver does not publish events for protected user IDs.

Command

```
ADDUSER (JES2) NOPASSWORD
```

Result Document

No event is published.

Example ALTUSER NOPASSWORD Processing

If an existing user is altered to become protected, the driver removes its association.

Command

```
ALTUSER (PROC) NOPASSWORD
```

Result Document

```
<remove-association>USER\PROC</remove-association>
```

Example OIDCARD Parameter Processing

If you specify the OIDCARD or NOOIDCARD parameter on an ADDUSER or ALTUSER command, the Publisher channel does not represent the parameter in the event document.

Command

```
ADDUSER (KIRSTEN) NAME('KIRSTEN WAGNER') OIDCARD
```

Result Document

```
<add class-name="User" event-id="2764" src-dn="\KIRSTEN">
  <association>USER\KIRSTEN</association>
  <add-attr attr-name="RACF-userid">
    <value type="string">KIRSTEN</value>
  </add-attr>
  <add-attr attr-name="RACF-name">
    <value type="string">KIRSTEN WAGNER</value>
  </add-attr>
</add>
```

Messages

B

Components of the Identity Manager 3.6.1 driver for RACF on mainframes (z/OS operating system) write messages recording key processing occurrences, diagnostic information, and general statistical information.

Each message begins with a four-character code associated with the driver component that generated the message. Use this code to find message information quickly as follows:.

B.1 LDX0 Messages

Following are explanations, possible causes and actions for LDX0 messages.

LDX0001E There are old events on the LDX queue. Ensure that LDXLOGRP is started.

Explanation: The cross memory queue access routine in a RACF exit found events in the cross memory queue that have been unprocessed for at least fifteen minutes. During normal operation, the Change Log Started Task processes events from the queue immediately.

Message Destination: WTO.

Possible Cause: The Change Log Started task is not running.

Action: Ensure that the Change Log Started Task is running.

LDX0002I Unexpected RC *xxxxxxxx* during token processing routine.

Explanation: An unexpected return code was received from z/OS Name/Token Services by a RACF Event Subsystem component.

Message Destination: WTO.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide job logs and the console log with the exact contents of the message received.

LDX0103E Unable to parse command line.

Explanation: The LDXSERV command contained invalid operands, and LDXSERV was unable to prompt for correct information.

Message Destination: SYSTSPRT.

Action: Correct the syntax of the LDXSERV command and reissue it.

If the command was issued by the driver shim, contact software support. Be ready to provide driver logs and logs for the Telnet session showing the faulty command.

LDX0104E EventID required for MARKDONE function.

Explanation: An LDXSERV MARKDONE command was missing the required event token operand.

Message Destination: SYSTSPRT.

Possible Cause: Internal error in driver shim.

Action: If the command was issued by the driver shim, contact software support. Be ready to provide driver logs and logs for the Telnet session for the Telnet session showing the faulty command.

LDX0105E Internal error: *description*

Explanation: An unexpected error occurred in the LDXSERV command. The message contains a description of the problem.

Message Destination: SYSTSPRT.

Possible Cause: Internal error.

Action: Contact software support. Be ready to provide driver logs and logs for the Telnet session.

LDX0106E Unable to open the log file.

Explanation: LDXSERV was unable to open the Change Log data set.

Message Destination: SYSTSPRT.

Possible Cause: The user ID running the LDXSERV command does not have access to the Change Log data set.

Action: Check the TSO session log and message files for additional messages concerning the failure.

If you are unable to determine and correct the cause of the error, contact software support. Be ready to provide driver logs and logs for the Telnet session.

LDX0107E No preallocated log file and no valid environment.

Explanation: The LDXSERV command was unable to find the Change Log data set because there was no LOGFILE DD statement and there was no valid LDX environment. The LDX environment is created when either of the RACF exits is invoked for the first time after an IPL or when the Change Log Started Task first starts.

Message Destination: SYSTSPRT.

Action: Ensure that you are logged on to a system where the RACF Event Subsystem is installed and that the RACF exits have been properly installed and are active.

If you are unable to determine and correct the cause of the error, contact software support. Be ready to provide driver logs and logs for the Telnet session.

LDX0108E No preallocated log file and logger is not active.

Explanation: The LDXSERV command was unable to find the Change Log data set because there was no LOGFILE DD statement and the Change Log Started Task was not active.

Message Destination: SYSTSPRT.

Action: If you are unable to determine and correct the cause of the error, contact software support. Be ready to provide driver logs and logs for the Telnet session.

LDX0109E Dynamic allocation failed for log file *dsname*, s99rc= *rc*, s99error= *err*.

Explanation: The LDXSERV command was unable to dynamically allocate the Change Log data set. The dynamic allocation return code and reason codes are given in the message by *rc* and *err* respectively.

Dynamic allocation return codes and reason codes are documented in the IBM publication *MVS Programming: Authorized Assembler Services Guide*.

Message Destination: SYSTSPRT.

Action: If you are unable to determine and correct the cause of the error, contact software support. Be ready to provide driver logs and logs for the Telnet session.

B.2 LDXL Messages

Following are explanations, possible causes and actions for LDXL messages.

LDXL000 LOGGING STARTED AT *hh:mm:ss* ON *mm/dd/yyyy*

Explanation: The Change Log Started Task has initialized.

Message Destination: WTO.

Action: Informational only. No action is required.

LDXL001 MESSAGE LOG DISABLED, SYSPRINT DD MISSING

Explanation: During initialization, the Change Log Started Task was unable to open the SYSPRINT DD statement.

The Change Log Started Task continues processing, but no messages are written to SYSPRINT.

Message Destination: WTO.

Possible Cause: The SYSPRINT DD statement is missing from the JCL for the Change Log Started Task.

Action: Ensure that a SYSPRINT DD statement is present in the JCL and that it defines a file that the Change Log Started Task can write to.

LDXL002 EXECUTE STATEMENT PARAMETERS: *parm-values*

Explanation: During initialization, the Change Log Started Task found the listed parameters present on the EXEC statement PARM parameter.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL003 START COMMAND PARAMETERS: *parameters*

Explanation: During initialization, the Change Log Started Task found the listed parameters present on the START command.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL004 STOP COMMAND RECEIVED.

Explanation: An operator entered a STOP command for the Change Log Started Task. The Change Log Started Task ends.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL005 MODIFY COMMAND PARAMETERS: *parameters*

Explanation: An operator entered a MODIFY command for the Change Log Started Task with the listed parameters.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL006 UNRECOGNIZED CIBVERB TYPE: X'hh', COMMAND IGNORED

Explanation: During processing, the Change Log Started Task received a command input buffer (CIB) with a verb other than STOP or MODIFY. Processing continues.

Message Destination: SYSPRINT.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide the console log and the SYSPRINT data set with the exact contents of the message received.

LDXL007 OPERATOR CANCEL DETECTED, ATTEMPTING NORMAL SHUTDOWN

Explanation: An operator has issued a CANCEL command without the DUMP parameter for the Change Log Started Task. The Change Log Started Task attempts a clean shutdown.

Message Destination: SYSPRINT.

Action: Wait for the Change Log Started Task to end. If the Change Log Started Task does not end within a reasonable amount of time, issue another CANCEL command, specifying the DUMP parameter. If the cause of the failure to end normally is not evident, contact software support. Be ready to provide the contents of the system dump, job and console logs, and SYSPRINT data set.

NOTE: Use the STOP command for normal shutdown of the Change Log Started Task.

LDXL008 EVENT TRACING ENABLED.

Explanation: An operator has issued a MODIFY command for TRACE ON to the Change Log Started Task.

Event tracing is turned on.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL009 EVENT TRACING DISABLED.

Explanation: An operator has issued a MODIFY command for TRACE OFF to the Change Log Started Task.

Event tracing is turned off.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL010 MODIFY COMMAND IGNORED, INVALID OR MISSING PARAMETERS.

Explanation: An operator has issued a MODIFY command to the Change Log Started Task, but the command parameters are not recognized.

The MODIFY command is ignored.

Message Destination: SYSPRINT.

Action: Reissue the MODIFY command with the intended parameters.

LDXL011 EVENT RC(*rc*) DATA: *event_data*

Explanation: Event tracing is turned on and an event has been processed.

The return code from ProcessEvent is *rc*. The content of the event record is *event_data*.

Processing continues.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL012 TERMINATING BECAUSE LOGGING ALREADY ACTIVE.

Explanation: Upon startup, the Change Log Started Task has detected that another Change Log Started Task is already running.

This instance of the Change Log Started Task terminates.

To detect this condition, the Change Log Started Task enqueues exclusively on qname “ldxlogr” rname “#LDXENVIRONTOKEN” when it initializes. If the enq macro fails, this message is issued. The Change Log Started Task dequeues this resource upon shutdown.

Message Destination: SYSPRINT.

Possible Cause: A START command for the Change Log Started Task has been issued more than once.

Action: Do not start more than one instance of the Change Log Started Task at a time.

LDXL013 LOGGING TO DATASET: *dsname*

Explanation: The name of the Change Log data set in use is *dsname*.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXL999 LOGGING ENDED AT *hh:mm:ss* ON *mm/dd/yyyy*

Explanation: The Change Log Started Task is ending.

Message Destination: SYSPRINT.

Possible Cause: An operator entered a STOP command for the Change Log Started Task.

Action: Informational only. No action is required.

B.3 LDXU Messages

Following are explanations, possible causes and actions for LDXU messages.

LDXU000I Log File Utility started on *mm/dd/yyyy* at *hh:mm:ss*.

Explanation: The Log File utility has initialized.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU001W Message log disabled, SYSPRINT DD missing.

Explanation: During initialization, the Log File utility was unable to open the SYSPRINT DD statement. The Log File utility continues processing, but no messages are written to SYSPRINT.

Message Destination: WTO.

Possible Cause: The SYSPRINT DD statement is missing from the JCL for the Log File utility.

Action: Ensure that a SYSPRINT DD statement is present in the JCL and that it defines a file that the Log File utility can write to.

LDXU002I Execute statement parameters: *parm-values*

Explanation: During initialization, the Log File utility found the listed parameters present on the EXEC statement PARM parameter.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU003E Open failed for log file.

Explanation: The Log File utility could not open the Change Log data set.

Message Destination: SYSPRINT.

Possible Cause: The LOGFILE DD statement is missing from the JCL for the Log File utility.

Action: Ensure that a LOGFILE DD statement is present in the JCL and that it defines a data set that the Log File utility can write to.

LDXU004I Log file blocksize: *blksize*

Explanation: The Log File utility is initializing the Change Log data set with a blocksize of *blksize*

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU005I Log file blocks written: *block-count*

Explanation: While initializing the Change Log data set, the Log File utility has written *block-count* blocks of empty records.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU006E Open failed for LOADIN file.

Explanation: The Log File utility Load function could not open the LOADIN ddname.

Message Destination: SYSPRINT.

Possible Cause: The LOADIN DD statement is missing from the JCL for the Log File utility.

Action: Ensure that a LOADIN DD statement is present in the JCL and that it defines a file that the Log File utility can read.

LDXU007E Unrecognized or missing execute statement parameter.

Explanation: The Log File utility found an unknown parameter in the EXEC statement PARM parameter.

Processing ends.

Message Destination: SYSPRINT.

Possible Cause: The EXEC statement PARM value is missing or does not contain one of the following functions:

- INITIALIZE
- DUMP
- LOAD

Action: Correct the PARM value and resubmit the job.

LDXU008I Log file events loaded: *event-count*

Explanation: The Log File utility Load function has successfully loaded *event-count* events into the Change Log data set from the input file.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU009E Add event failed, error code *code*

Explanation: The Log File utility Load function was unable to add an event record to the Change Log data set. The LDXLADD LDXIOERR code was *code*.

Message Destination: SYSPRINT.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide the job log and SYSPRINT data set with the exact contents of the message received.

LDXU010E Read header failed, error code *code*

Explanation: The Log File utility Dump function was unable to read the header record of the Change Log data set. The LDXLGETE LDXIOERR code was *code*.

Message Destination: SYSPRINT.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide the job log and SYSPRINT data set with the exact contents of the message received.

LDXU011E Read event failed, error code *code*

Explanation: The Log File utility Dump function was unable to read an event record from the Change Log data set. The LDXLGETE LDXIOERR code was *code*.

Message Destination: SYSPRINT.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide the job log and SYSPRINT data set with the exact contents of the message received.

LDXU990I Open BDAM log succeeded.

Explanation: The Log File utility has initialized the Change Log data set with empty records and has successfully opened it to complete the initialization by updating the header information.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.

LDXU991E Open BDAM log failed.

Explanation: The Log File utility has initialized the Change Log data set with empty records, but could not reopen it to complete the initialization by updating the header information.

Message Destination: SYSPRINT.

Possible Cause: Internal system error.

Action: Contact software support. Be ready to provide job logs and the console log with the exact contents of the messages received.

LDXU999I Log File Utility ended on *mm/dd/yyyy* at *hh:mm:ss*

Explanation: The Log File utility has completed processing.

Message Destination: SYSPRINT.

Action: Informational only. No action is required.