Novell
Identity Manager Fan-Out Driver

3.5.1

September 28, 2007

CONCEPTS AND FACILITIES GUIDE

Novell®

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.

The Solaris* standard IO library has kernel limitations that interfere with the operation of the Provisioning Manager. Therefore, components for Solaris use the AT&T* SFIO library. Use of this library requires the following notice:

The authors of this software are Glenn Fowler, David Born and Kim-Phone Do.

Copyright (c) 1991, 1996, 1998, 2000, 2001, 2002 by AT&T Labs - Research.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

This software is being provided as is, without any express or implied warranty. In particular, neither the authors nor AT&T Labs make any representation or warranty of any kind concerning the merchantability of this software or its fitness for any particular purpose.

Contents

About This Guide

This guide describes the concepts and facilities of the Novell® Identity Manager Fan-Out driver.

The Fan-Out driver supports multi-platform implementation of Novell Identity Manager 3.5.1, 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.

The guide includes the following sections:

Audience

This guide is for system administrators and others who plan, install, configure, and use the Identity Manager Fan-Out driver. 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 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 3.5.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers).

Additional Documentation

For additional documentation about Identity Manager drivers, see the Identity Manager 3.5.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers).

For documentation about Identity Manager, see the Identity Manager 3.5.1 Documentation Web site (http://www.novell.com/documentation/idm35).

For documentation about other related Novell products, such as eDirectory and iManager, see the 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.

Introduction

1

The Novell® Identity Manager Fan-Out driver is an identity provisioning solution, based on Novell eDirectory™, Identity Manager, and related technology.

With Identity Manager, you can manage the full user life cycle, delivering first-day access to essential resources, providing single login, and modifying or revoking access rights. Identity Manager also provides self-service features that enable users to maintain their own passwords and profile information.

By adding the Fan-Out driver, you can use Identity Manager to *fan out* identity provisioning to hundreds of systems with minimal effort. You can centrally manage user accounts and have them automatically created, configured, maintained, and removed when appropriate. It uses extensible scripts to manage account rights, home directories, and other resources as well as the user definitions themselves. Meanwhile, system administrators for the individual platforms in your enterprise can retain control over their areas.

1.1 Driver Highlights

The Fan-Out driver differs from bidirectional drivers in the following ways:

- **Fan-Out Scalability** A single instance of the Fan-Out driver can provision centrally managed account information to hundreds of dissimilar platform systems throughout your enterprise.

- **Scripts** The Fan-Out driver scripts process data change events on all supported platforms. This enables platform system administrators to automatically manage local resources associated with accounts as well as the definitions of those accounts.

- **Authentication Redirection** It supports the Novell Universal Password feature, which employs access to a central repository for login and password rules. This includes support of bidirectional password synchronization.

- **Application Programming Interface (API)** An easy-to-use API enables programmers to extend applications from individual platforms to fully leverage eDirectory.

1.2 Driver Organization

The Fan-Out driver has two functional divisions.

- **Authentication Services** Provides real-time eDirectory access for user authentication and related purposes.
- **Identity Provisioning** Provides user and group management.

The Fan-Out driver has two principal parts.

- **The Core Driver** Interfaces with eDirectory to provide Authentication Services (such as password verification) and provisioning events (such as Add User or Remove Group).

- **Platform Services** Uses the core driver to bring common authentication and account life cycle management to a broad selection of supported platforms.

1.3 System Requirements

Two sets of system requirements, one for the core driver and one for Platforms Services, need to be considered.

1.3.1 Core Driver System Requirements

❑ Novell Identity Manager

❑ eDirectory verson(s) supported by the Identity Manager version in use.

❑ Any version of the following OS platforms supported by the Identity Manager version in use:
  ◆ Netware®
  ◆ Windows*
  ◆ Linux*
  ◆ Solaris*

1.3.2 Platform Services System Requirements

For information about required systems and software, as well as supported platforms and operating environments, see the Identity Manager 3.5.1 Drivers Documentation Web site (http://www.novell.com/documentation/idm35drivers). From this index page, you can select a Readme file associated with the platform(s) for which you need Fan-Out driver support.

Structure and Function

There are two structural divisions of the Novell® Identity Manager Fan-Out driver: the core driver and Platform Services.

Figure 2-1 *Driver Components*
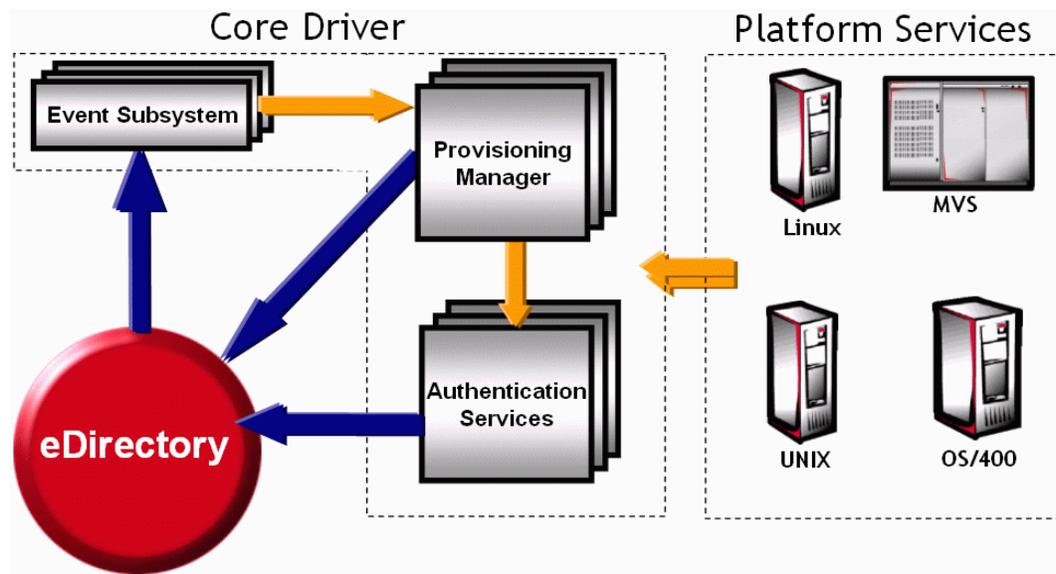
The core driver provides Authentication Services and information about changes to users and groups to target platforms that have been configured to run Platform Services.

The driver obtains and stores the information it uses in eDirectory™. To access eDirectory, the core driver uses LDAP Services for eDirectory.

For ease of management, target platforms that share the same user and group population are grouped together into Platform Sets.

Communication between the driver components occurs throuth TCP/IP and is encrypted.

The driver includes a secure Web interface that works as an iManager plug-in for administration and monitoring.

The core driver records significant occurrences in an Audit Log, and each component writes an Operational Log. Each core driver component maintains performance statistics, which can be viewed in the Web interface.

The Fan-Out driver includes an application programming interface (API). This allows programmers to extend applications to use Authentication Services, which allows them to take advantage of your existing eDirectory constructs.

Binary files, configuration files, and other files used by the driver components are stored in the `ASAM` directory in the file system of the host server.

Additional Resources

For details about configuring and administering the Fan-Out driver, see the *Core Driver Administration Guide*, the *Platform Services Planning Guide and Reference*, and any of the following administration guides, depending on your platform needs:

- *Platform Services Administration Guide for Linux and UNIX*
- *Platform Services Administration Guide for z/OS* (mainframes)
- *Platform Services Administration Guide for OS/400* (midrange)

For more information about the API, see the *API Developer Guide*.

For explanations of the messages written to logs by the Fan-Out driver components, see the *Messages Reference*.

For information about eDirectory, see the *Novell eDirectory Administration Guide*.

Section Topics

The topics in this section describe the structure and function of the Identity Manager Fan-Out driver.

2.1 Core Driver

The core driver provides Authentication Services, such as password verification, to target platforms.

The core driver also provides Identity Provisioning events, such as add, modify, and delete for users and groups, to target platforms. Platform Services uses these events to maintain user accounts and groups locally.

The core driver uses eDirectory objects to store its properties. Configuration information for the core driver is stored in the Driver object. Component configuration and user management information is stored in the ASAM System container object.

A writable replica of the partition holding the ASAM System container must reside on the LDAP host server used by a core driver.

A User object called the ASAM Master User is created during core driver installation. The core driver processes use ASAM Master User to perform an LDAP Bind for access to eDirectory.

The core driver provides

- eDirectory access to platforms for Authentication Services, such as password verification
- Provisioning events to Platform Services for the maintenance of local user accounts and groups
- The Web interface that you use to configure and manage the driver
- Management of the objects inside the ASAM System container
- An audit trail of significant occurrences

You can run multiple core drivers to provide redundancy for Authentication Services and Identity Provisioning functions.

One core driver is designated as the primary core driver. Other core drivers are secondary core drivers. Only the primary core driver listens for events from eDirectory. The primary core driver also serves the Web interface and provides environmental information during the installation process for other core drivers.

The core driver includes seven components.

- Section 2.1.1, "Object Services," on page 13
- Section 2.1.2, "Event Journal Services," on page 14
- Section 2.1.3, "Audit Services," on page 14
- Section 2.1.4, "Certificate Services," on page 14
- Section 2.1.5, "Web Services," on page 14
- Section 2.1.6, "Authentication Services," on page 14
- Section 2.1.7, "Event Subsystem," on page 14

Object Services, Event Journal Services, Audit Services, Certificate Services, and Web Services are sometimes referred to collectively as the Provisioning Manager component of a core driver.

2.1.1 Object Services

Object Services maintains the objects within the ASAM System container. Some of these objects store configuration information for the various driver components. Others represent users and groups of users that can be defined on target platforms. The object that contains these users and groups is called the Census.

Object Services on the primary core driver is notified by the Event Subsystem of events, such as add, modify, or delete, pertaining to users and groups of users in eDirectory. These events are used to maintain the Census.

To initially build and periodically ensure the integrity of the Census, Object Services examines specified portions of eDirectory for users and groups. This process is called a Trawl. You can use the Web interface to set the Trawl schedule. Only the primary core driver performs Trawls.

Census Search objects that you define using the Web interface describe which objects in eDirectory are included in the Census. Platform Set Search objects that you define using the Web interface describe which users and groups are managed for a given set of platforms.

For more information about Object Services and the Census, see "Census Container" on page 20. For more information about associating users and groups with sets of platforms, see "Platform Set Objects" on page 22.

2.1.2 Event Journal Services

Event Journal Services receives provisioning events from Object Services and makes them available to sets of platforms according to the rules you specify. Event Journal Services ensures that provisioning events for a platform are delivered, even if the platform is not always available.

Platforms can periodically connect to Event Journal Services to receive provisioning events, or they can maintain a persistent connection and receive events as they occur.

By defining multiple core drivers to provide events to platforms, you can provide for improved availability.

2.1.3 Audit Services

Audit Services maintains the Audit Log and Operational Logs for a core driver.

2.1.4 Certificate Services

Certificate Services mints the certificates used by Secure Sockets Layer (SSL) to authenticate and secure connections between the components.

2.1.5 Web Services

Web Services provides the secure Web interface for monitoring and administering the Identity Manager Fan-Out driver. The Web interface is provided through an iManager plug-in.

2.1.6 Authentication Services

Authentication Services provides Platform Services with the time-critical interface to eDirectory. This interface is used for such functions as checking the passwords of users logging in to the platform. This interface is also used by the AS Client API.

By defining multiple core drivers to provide Authentication Services to platforms, you can provide for improved performance and availability.

Authentication Services supports platform communications using SSL and DES encryption.

2.1.7 Event Subsystem

The Event Subsystem uses Identity Manager to subscribe to eDirectory events and provides them to Object Services. Objects of interest must be replicated on the core driver server.

2.2 Platform Services

Platform Services enables a system to utilize the core driver functions. A platform can use Authentication Services for some or all users, and can use Identity Provisioning in maintaining some or all local user accounts and groups. For a complete account redirection solution, a platform can use the Name Service Switch and Platform Services Cache Daemon for some or all users.

Some types of platforms communicate with Authentication Services using SSL, and others use DES encryption. All platform communication with Event Journal Services uses SSL.

A platform that uses SSL-based communication must have a valid certificate to communicate with the core driver for most functions. A platform that uses DES encryption must use the same DES key as defined for it in the core driver configuration.

The Identity Manager Fan-Out driver does not support authentication or password changes for eDirectory users who have a null password.

Figure 2-2 *Platform Services*
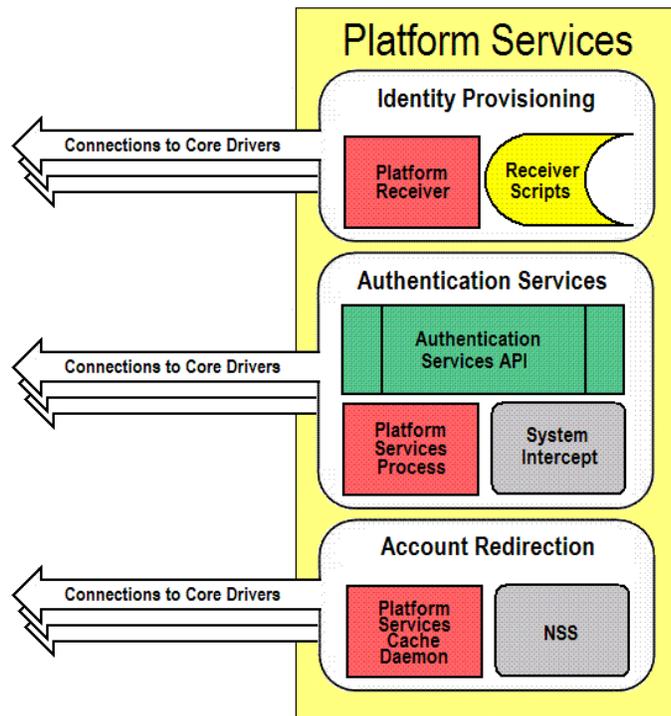
2.2.1 User and Group Management

Management of users and groups on the platform is carried out by Receiver scripts, which are called by the Platform Receiver based on provisioning events obtained from the core driver.

Platform Receiver

The Platform Receiver connects to the Event Journal Services component of the core driver, requests provisioning events, and runs a script to carry out the appropriate platform-specific processing for the given type of event. The Platform Receiver provides failover support for connections to Event Journal Services if more than one core driver is available.

Receiver Scripts

Receiver scripts are run by the Platform Receiver to process provisioning events.

The Identity Manager Fan-Out driver provides a set of fully functional base scripts in the customary scripting language for each supported platform. You can extend these base scripts as appropriate for your needs.

The Receiver script functions are

- Add User
- Modify User
- Delete User
- Delete User Pending
- Enable User
- Disable User
- Rename User
- Add User to Group
- Remove User from Group
- Add Group
- Modify Group
- Delete Group
- Delete Group Pending
- Rename Group

2.2.2 User Authentication

Authentication redirection is handled by the Platform Services Process, which is called by the System Intercept. The Platform Services Process is also called by applications using the AS Client API.

Platforms that use password replication receive notification of password changes in eDirectory through the Platform Receiver and send notification of local password changes detected by the password change intercept to the core driver using the Platform Services Process.

Account redirection is handled by the Platform Services Cache Daemon, which is called by the Name Service Switch. Platforms that are configured for account redirection use a local memory cache pool for account records and retrieve all account and password information from this cache.

Platform Services Process

The Platform Services Process establishes and maintains connections to core drivers for Authentication Services, and provides load balancing and failover among them. These connections are used to provide Authentication Services to the platform.

Platform Services Cache Daemon

The Platform Services Cache Daemon establishes and maintains a connection to a core driver and receives event data from Event Journal Services. This data is stored away in memory cache and used to supply account information to the Name Service Switch.

AS Client API

The AS Client API provides a programming interface to Authentication Services. It is furnished as routines that can be called from C and Java*. The AS Client API incudes functions to

- Validate a user ID/password combination
- Change a user's password, given the current password
- Perform an administrative password reset
- Obtain the fully distinguished name for a user ID
- Determine if a user has Security Equal To a given object
- Determine if an object has the specified effective rights to the specified attribute of a given object
- Obtain a list of members of a group
- Obtain a list of security equivalences for a user
- Obtain the eDirectory Home Directory attribute value for a user
- Determine if a given user is in the Authentication Services Include/Exclude list

For details about using the AS Client API, see the *API Developer Guide*.

System Intercept

The System Intercept is called by the native security system for password verification and password change. Because passwords are checked using eDirectory or, on supported platforms, replicated from eDirectory, a user has the same password throughout the enterprise, regardless of the platform used.

System Intercepts are implemented using standard, vendor-provided mechanisms.

Authentication Services Methods

There are two methods for providing users with the same password across the platforms in your enterprise.

Password Redirection: Requests to check passwords are intercepted at the platform and redirected to objects in eDirectory. The end result is that the user has the same password on all systems.

Password Replication: Changes to passwords are intercepted and replicated between eDirectory and participating platforms. As with password redirection, the end result is that the user has the same password on all systems.

The following table shows the Authentication Services methods available for each platform OS type:

Table 2-1   *Authentication Services by Operating System*

Platform OS Type	Authentication Services Method
z/OS	Password redirection, Password replication (optional)
OS/400	Password replication

Platform OS Type	Authentication Services Method
UNIX	Password redirection, Password replication (optional)

Password Redirection

Platforms that use password redirection employ a System Intercept to gain control when a password is to be verified. The System Intercept passes the request to Authentication Services, through the Platform Services Process. Authentication Services uses the Census to identify the User or Alias object in eDirectory that corresponds to the request. Then Authentication Services verifies the password using that object and returns the result to the platform.

The System Intercepts for z/OS and UNIX systems store the password in the local security system upon a successful authentication or password change. For logins, if Authentication Services cannot be reached, the user's password is verified using the local security system.

Password Replication

Platforms that use password replication receive notification of password changes through the Platform Receiver.

The core driver must be notified of changes to passwords as follows:

- If your eDirectory is configured to fully support Universal Password, the driver is notified of password changes in eDirectory.
- If you do not use Universal Password, you must install and configure the appropriate password intercepts.
  - The Novell Client™ Password Intercept is installed on a Windows workstation and captures password change information from the Novell Client or an administrative utility.
  - The NetWare® Password Intercept is installed on NetWare systems that run an NDK application that changes passwords.
- The Password Validation Program Exit is installed on an OS/400 system and captures password change information.

It is crucial that these intercepts be installed and properly configured. Otherwise replication cannot occur reliably. Properly configured, Universal Password can be used in lieu of the Novell Client Password Intercept and the NetWare Password Intercept.

When Authentication Services receives notification of a password change, it verifies the authenticity of the notification and then stores the encrypted password. This is detected by the Event Subsystem, which generates the appropriate provisioning event to notify those platforms that are authorized to receive password information.

By default, passwords are converted to lowercase before they are sent to a platform.

Account Redirection: Requests for Posix user and group information are intercepted at the platform Name Service Switch and redirected to objects in eDirectory. This information includes loginName, uidNumber, gidNumber, gecos, homeDirectory, loginShell, groupName, memberUid and passwords.

2.2.3 Platform Configuration File

You use the platform configuration file to specify Platform Services configuration information, such as

- Which users are authenticated using Authentication Services and which users are authenticated using the local security system
- Which user accounts and groups are managed using Identity Provisioning and which are managed locally
- Information used to locate the core driver servers.

2.3 Directory Objects

The Identity Manager Fan-Out driver maintains objects in eDirectory with configuration information for the core driver and platforms as well as users and groups of users available to the platforms. These are stored in the ASAM System container.

You maintain configuration information by using the Web interface. Do not use any other method of changing objects in the ASAM System container unless advised by support personnel.

A writable replica of the partition holding the ASAM System container must reside on the LDAP host server used by a core driver.

2.3.1 The ASAM Master User Object

The core driver processes perform an LDAP Bind as the ASAM Master User to gain access to eDirectory. The ASAM Master User object is created during installation.

The ASAM Master User must have Supervisor rights to the container in eDirectory that holds the users and groups that can be added to the Census. This is known as the User and Group Subtree. These rights are granted during installation.

To use the AS Client API to access objects outside of the User and Group Subtree, you must grant additional rights to the ASAM Master User.

- You must grant the ASAM Master User Browse object rights and Compare property rights to any object that is accessed through the AS Client API.
- You must grant the ASAM Master User Read property rights to any object whose Security Equals list or Group Membership list, or other attribute value is accessed through the AS Client API.

2.3.2 Configuration-Oriented Objects

Configuration information for Identity Manager Fan-Out driver components is stored in objects that correspond to them.

- Audit Services object
- Certificate Services object
- Event Journal Services object
- Object Services object

- Web Services object
- Event Subsystem objects
- Authentication Services objects
- UID/GID Set objects
- Platform Set objects
- Platform objects

Identity Manager Fan-Out driver program component configuration objects list each of their host server network addresses. Before accepting a communication connection from another component, driver components verify that the connection originates from a network address listed in the corresponding configuration object.

2.3.3 Census Container

Based on your specifications, Object Services maintains a Census of users and groups of users for use with target platforms. Users in the Census are represented by Enterprise User (eUser) objects. Groups of users in the Census are represented by Enterprise Group (eGroup) objects.

Object Services uses events from the Event Subsystem to maintain the Census. Object services of the primary core driver also periodically trawls eDirectory for information to ensure the validity of the Census.

Authentication Services uses eUser objects in the Census to locate the corresponding User objects in eDirectory for password verification and other functions. For information about associating eUsers and eGroups from the Census with sets of platforms for provisioning purposes, see "Platform Set Objects" on page 22.

You use the Web interface to specify Census Search objects that identify the users and groups that are to be included in the Census.

Search objects can get Enterprise Users from

- Specifically identified User objects
- Group object membership
- Organizational Role object occupant lists
- Objects in containers (and subcontainers, to whatever depth you set)

Search objects can get Enterprise Groups from

- Specifically identified Group objects
- Group objects in containers (and subcontainers, to whatever depth you set)
- Identity Manager entitlements

Dynamic Groups as Search Objects

Dynamic groups use an LDAP search filter to define a set of rules that, when matched by eDirectory User objects, define the members of the group. Membership in the group is evaluated dynamically by eDirectory. There is no actual list of members for a dynamic group like there is for a static group.

Events involving users who are already in the Census that affect their membership in a dynamic group that is a Search object are seen by the Event Subsystem as they happen. This is because the

core driver interrogates Search objects to discover if an event involving a given User object is of interest.

Events involving users not already in the Census and events involving the LDAP search filter of a dynamic group that is a Search object are not seen by the Event Subsystem. This is because there is nothing to drive the LDAP search. Such changes are not detected until the next Trawl is run.

Naming Exceptions

Because Enterprise User objects and Enterprise Group objects share the same name space, their names must be unique. If a duplicate name is found based on your Census Search objects, the resulting Enterprise User or Enterprise Group object is placed in the Exceptions container rather than being made available in the Census. You can use the Web interface to review naming exceptions.

Enterprise User Objects

Enterprise User (eUser) objects reside in the Census container. An eUser object represents a single User object, or an Alias object that references a User object, in eDirectory.

An eUser object includes a reference to the User object or Alias object that it represents in eDirectory. The User object referenced by an Alias object is provisioned to platforms, not the Alias object itself.

Enterprise Group Objects

Enterprise Group (eGroup) objects reside in the Census container. An eGroup object represents a group of users, and is based on a Group object, or an Alias object that references a Group object, in eDirectory. Enterprise Group objects must be based on static Group objects. Dynamic Group objects are not provisioned.

An eGroup object includes a reference to the Group object or Alias object that it represents in eDirectory. The Group object referenced by an Alias object is provisioned to platforms, not the Alias object itself.

Enterprise Group objects in the Census contain a list of the eUser objects that are represented in the corresponding Group object in eDirectory (but not any users that are not present in the Census).

Inactive Users and Groups

You can choose to have Enterprise User and Enterprise Group objects whose corresponding User or Group object is deleted from eDirectory or is no longer covered by a Census Search object remain in the Census in an inactive state. Because Enterprise User objects relate to User objects in eDirectory through a globally unique identifier, this prevents another person from receiving access to resources as an unintended result of the reuse of the user name. Inactive users cannot authenticate through Authentication Services.

Delete Pending Duration

You can use the Web interface to specify a Delete Pending Duration. During this interval, eUser and eGroup objects whose corresponding User and Group objects have either been deleted from eDirectory or are no longer covered by a Search object are not deleted from target platforms. The results of a Delete User or Delete Group Receiver script can be difficult to reverse. Delete Pending Duration provides a grace period to allow recovery from a disastrous mistake affecting many users.

The Delete User Pending or Delete Group Pending Receiver script is called when a delete event becomes pending for a user or group. The Delete User or Delete Group script is not called until the Delete Pending Duration expires.

2.3.4 Platform Objects

A Platform object represents a specific target platform that runs Platform Services.

2.3.5 Platform Set Objects

Platform Set objects provide the relationship between Search objects and Platform objects. You can use Platform Sets to group together multiple platforms that share the same user and group population.

The following example illustrates how you can fan out your user and group population to platforms that are grouped into Platform Sets.

Table 2-2 *Platform Set Example*

Containers with Users	**OU=Students** Henri Markus Rie	**OU=Faculty** Carmen Eleu Mario	**OU=Staff** Isabel Claire Kenji
Search Objects	OU: Students Include Users: Yes	OU: Faculty Include Users: Yes	OU: Staff Include Users: Yes
Platform Sets	**Academic** Search Objects: Students, Faculty Platforms: StudentDataServer, LabWorkstation1, LabWorkstation2, LabWorkstation3	**Employee** Search Objects: Faculty, Staff Platforms: BenefitsServer, EmployeeDataServer	**Everyone** Search Objects: Students, Faculty, Staff Platforms: MailServer, LibraryServer

Platforms	StudentDataServer	BenefitsServer	MailServer Platform Set: Everyone Users: Henri, Markus, Rie, Carmen, Eleu, Mario, Isabel, Claire, Kenji
	Platform Set: Academic Users: Henri, Markus, Rie, Carmen, Eleu, Mario	Platform Set: Employee Users: Carmen, Eleu, Mario, Isabel, Claire, Kenji	
	LabWorkstation1	**EmployeeDataServer**	**LibraryServer** Platform Set: Everyone Users: Henri, Markus, Rie, Carmen, Eleu, Mario, Isabel, Claire, Kenji
	Platform Set: Academic Users: Henri, Markus, Rie, Carmen, Eleu, Mario	Platform Set: Employee Users: Carmen, Eleu, Mario, Isabel, Claire, Kenji	
	LabWorkstation2		
	Platform Set: Academic Users: Henri, Markus, Rie, Carmen, Eleu, Mario		
	LabWorkstation3		
	Platform Set: Academic Users: Henri, Markus, Rie, Carmen, Eleu, Mario		

2.4 Migration

In some cases, a system other than eDirectory might contain the users that you want to participate with the driver. There are tools, such as LDIF, that you can use to import these users into eDirectory.

If you cannot extract the passwords for the affected user accounts, you can use the driver Password Migration component. This component can help you accomplish a smooth transition to basing your user accounts in eDirectory. The Password Migration component is available only on z/OS platforms. For details about the Password Migration component, see the *Platform Services Administration Guide for z/OS.*

Examples 3

This section presents some examples of processing to illustrate how the various components of the Novell®-Identity Manager Fan-Out driver work together. These examples do not exhaustively describe each detail involved in the processing, but give a representative account of the steps involved.

Use Figure 3-1 and Figure 3-2 for reference as you study the examples.
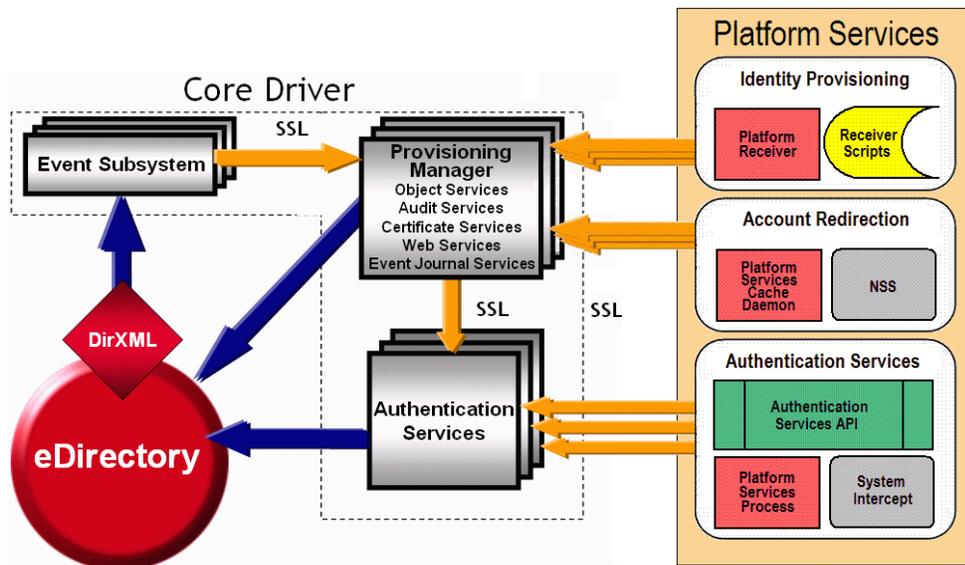
Figure 3-1 *Driver Components*

Figure 3-2   *User and Group Population Information Flow*
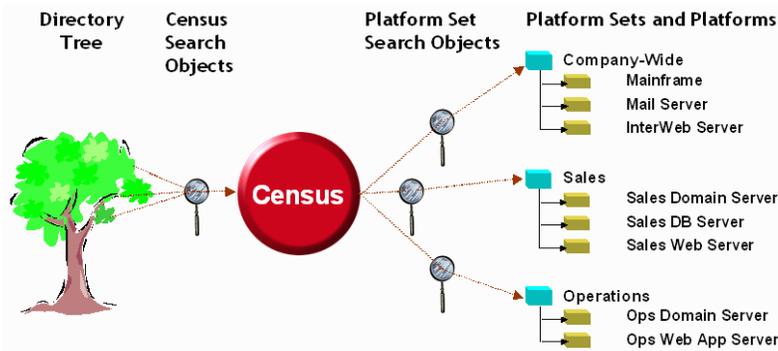
3.1 Password Check for Login

A user logs in to a platform.

1. The user enters user ID and password information in response to a login prompt from the operating system, and the System Intercept receives control.

2. The System Intercept calls the Check Password API function (unless the user is excluded from processing based on the specifications in the platform configuration file).

3. The Platform Services Process uses its load-balancing algorithm to select a core driver for Authentication Services. (Platform Services establishes a connection with each core driver for Authentication Services upon startup.)

4. The Platform Services Process makes a Check Password request to Authentication Services.

5. Authentication Services obtains from the Census the eUser object whose name matches the user ID. Authentication Services gets from that eUser object the distinguished name of the corresponding User object (or Alias object) in eDirectory™.

6. Authentication Services checks the password against the object in eDirectory that corresponds to the eUser.

7. If the password is not already present in the eUser object, Authentication Services stores the password there for the Provisioning Manager to use for password replication.

8. Authentication Services returns the result of the Check Password request to the Platform Services Process.

9. Authentication Services notifies Audit Services, which records the action in the Audit Log.

10. The Platform Services Process returns the result to the System Intercept.

11. The System Intercept returns the result to the local security system.

3.2 User Added to eDirectory

An administrator adds a new user to eDirectory. The user is covered by a Census Search object.

1. An administrator adds the new user to eDirectory.

2. The Event Subsystem receives the change and notifies Object Services.

3. If the user is covered by a Census Search object, Object Services of the primary core driver creates an eUser object for the user in the Census container, and associates the user with the Platform Set container objects whose Platform Set Search objects cover the user.

If the common name of the new user is the same as a name that already exists in the Census container, its eUser object is instead created in the Exceptions container, and the exception must be resolved by an administrator. For guidance in avoiding and resolving exceptions, see the *Core Driver Administration Guide*.

4. Object Services notifies Event Journal Services.

5. When each Platform Receiver of the associated Platform Sets requests an event and this event is the next one for that platform, Event Journal Services obtains detailed information about the new user by reading its object from eDirectory and passes the provisioning event to the Platform Receiver.

    If Event Journal Services cannot obtain the new user information yet because directory synchronization is not complete, the next event for the platform is processed and this one is tried again later.

6. Each Platform Receiver that receives the provisioning event checks to see if a user by that name already exists (unless the user is excluded from processing based on specifications in the platform configuration file).

    If the user already exists, the Platform Receiver notifies Event Journal Services.

    If the user does not exist, the Platform Receiver calls the Add User Receiver script, which adds the new user to the local security system and prepares it for use. The Platform Receiver then notifies Event Journal Services of the script outcome.

7. Event Journal Services notifies Audit Services, which records the action in the Audit Log.

3.3 Census Trawl

Object Services of the primary core driver periodically performs a Trawl to verify the contents of the Census. A Trawl is also run to initially build the Census, or a part of it, whenever you use the Web interface to define a new Census Search object.

The following steps are performed for each Census Search object:

1. Object Services scans the Census Search object for users and groups.

2. For any user or group that does not have a corresponding eUser or eGroup in the Census container:

    a. Object Services creates an eUser or eGroup object in the Census container, and associates the user or group with the Platform Set container objects whose Platform Set Search objects cover the user or group.

        If the common name of the new user or new group is the same as a user or group that already exists in the Census container, the eUser or eGroup object is instead created in the Exceptions container, and the exception must be resolved by an administrator. For guidance in avoiding and resolving exceptions, see the *Core Driver Administration Guide*.

    b. Object Services notifies Event Journal Services.

    c. When each Platform Receiver of the associated Platform Sets requests an event and this event is the next one for that Platform, Event Journal Services obtains detailed information about the new user or group by reading its object from eDirectory and passes the provisioning event to the Platform Receiver.

        If Event Journal Services cannot obtain the information yet because directory synchronization is not complete, the next event for the platform is processed and this one is tried again later.

d. Each Platform Receiver that receives the provisioning event checks to see if a user or group by that name already exists (unless the user or group is excluded from processing based on specifications in the platform configuration file).

If the user or group already exists, the Platform Receiver notifies Event Journal Services.

If the user or group does not exist, the Platform Receiver calls the Add User or Add Group Receiver script, which adds the new user or group to the local security system and prepares it for use. The Platform Receiver then notifies Event Journal Services of the script outcome.

e. Event Journal Services notifies Audit Services, which records the action in the Audit Log.

The following steps are performed for each user and group in the Census.

1. Object Services verifies that the user or group is still covered by a Search object.

   If it does not, the same steps are followed as for .

2. Object Services verifies that the User object or Group object that corresponds to the user or group still exists in eDirectory.

   If it does not, the same steps are followed as for .

3.4 User Deleted from eDirectory

A User object that is covered by a Census Search object is deleted from eDirectory.

1. An administrator deletes a user from eDirectory.

2. The Event Subsystem receives the deletion and notifies Object Services.

3. If the user is covered by a Census Search object, then Object Services takes one of the following actions based on configuration information that you have specified:

   Object Services marks the corresponding eUser object in the Census as inactive. (Inactive users cannot authenticate through Authentication Services.)

   or

   Object Services marks the eUser object for deletion after the event has been processed by all associated platforms.

4. Object Services notifies Event Journal Services.

5. When each Platform Receiver of the associated Platform Sets requests an event and this event is the next one for that Platform, Event Journal Services passes the provisioning event to the Platform Receiver. When the last Platform Receiver of a Platform Set has received the event, the next Trawl removes the Platform Set association for the eUser (if you have defined your configuration to remove deleted users rather than mark them inactive).

6. Each Platform Receiver that receives the provisioning event calls its Disable/Delete User Receiver script to disable the user in the local security system or to delete it and clean up its resources (unless the user is excluded from processing based on specifications in the platform configuration file).

7. Event Journal Services notifies Audit Services, which records the action in the Audit Log.

If you have specified a Delete Pending Duration, Event Journal Services indicates to the Platform Receiver that a delete is pending for the user. When the Delete Pending Duration has expired, Event Journal Services delivers the delete event.

3.5 Group Deleted from eDirectory

A Group object that is covered by a Census Search object is deleted from eDirectory.

1. An administrator deletes a group from eDirectory.

2. The Event Subsystem receives the deletion and notifies Object Services.

3. If the group is covered by a Census Search object, then Object Services takes one of the following actions based on configuration information that you have specified:

   Object Services marks the corresponding eGroup object in the Census inactive.

   or

   Object Services marks the eGroup object for deletion after the event has been processed by all associated platforms.

4. Object Services notifies Event Journal Services.

5. When each Platform Receiver of the associated Platform Sets requests an event and this event is the next one for that platform, Event Journal Services passes the provisioning event to the Platform Receiver. When the last Platform Receiver of a Platform Set has received the event, the next Trawl removes the Platform Set association for the eGroup.

6. Each Platform Receiver that receives the provisioning event calls its Delete Group Receiver script to delete the group from the local security system and clean up its resources.

7. Event Journal Services notifies Audit Services, which records the action in the Audit Log.

If you have specified a Delete Pending Duration, Event Journal Services indicates to the Platform Receiver that a delete is pending for the group. When the Delete Pending Duration has expired, Event Journal Services delivers the delete event.

3.6 User Added to a Group

A user for which there is an eUser object in the Census is added to the member list of a Group object in eDirectory.

1. An administrator adds the user to the member list of the Group object.

2. The Event Subsystem receives the change and notifies Object Services.

3. Object Services notifies Event Journal Services.

4. When each Platform Receiver of the Platform Sets associated with both the eUser and the eGroup requests an event and this event is the next one for that platform, Event Journal Services obtains detailed information about the user by reading its object from eDirectory, and passes the provisioning event to the Platform Receiver.

   If Event Journal Services cannot yet obtain updated user information due to incomple directory synchronization, the next event for the platform is processed and this one is tried again later.

5. Each Platform Receiver that receives the provisioning event calls its Add User to Group Receiver script, which adds the user to the group in the local security system.

6. Event Journal Services notifies Audit Services, which records the action in the Audit Log.

What's New

A

This section describes the major differences between the Novell®Identity Manager 3.5.1 Fan-Out driver and Novell Account Management 3.0. For information about migrating to the Identity Manager Fan-Out driver, see the Migrating from Novell Account Management 3.0 topic in the *Core Driver Administration Guide*.

A.1 Terminology

Several components have been renamed to more accurately reflect their updated roles and functions.

- Core Services is now called the core driver.
- The Manager is now called the Provisioning Manager, although we usually just refer to a specific core driver component of interest, such as Event Journal Services.
- The Agent function is now part of the core driver, and is called Authentication Services.
- The Event Listener is now part of the core driver, and is called the Event Subsystem.
- Access Management is now called Identity Provisioning.
- Access Management Events are now called provisioning events.

For definitions of common terms, see the "Glossary" on page 33.

A.2 Core Driver

Core Services functions have been restructured to run as an Identity Manager driver. This driver subscribes to eDirectory™ events for use in provisioning target platforms and provides authentication services to those platforms.

All driver configuration information is now maintained in eDirectory. There is no Core Services Configuration file.

With Account Management 3.0, you could run multiple Agents for performance and redundancy. With the Identity Manager Fan-Out driver, you can run multiple core drivers to provide performance and redundancy for Authentication Services.

With Account Management 3.0, there was one Manager. With the Identity Manager Fan-Out driver, you can run multiple core drivers. Platform Services now includes failover support for Manager functions.

The Identity Manager Fan-Out driver does not support Manual Platform Sets.

A.3 Web Interface

The Web interface is now provided as an iManager plug-in.

A.4 Platform Services

A.4.1 Platform Configuration File

Three platform configuration file statements have been renamed to correspond with the new terminology. To provide for migration, the old names are still accepted.

Table A-1   *Changes to Configuration File Statements*

Old Statement Name	New Statement Name
AGENT	AUTHENTICATION
DIRECTTOAGENT	DIRECTTOAUTHENTICATION
MANAGER	PROVISIONING

A.4.2 Full Sync Mode

The first time a Platform Receiver is run for a new platform, it automatically receives provisioning events for all users and groups for the platform. If this process is interrupted, processing resumes the next time the Platform Receiver is run. There is no need to run the Platform Receiver in Full Sync Mode during routine installation.

A.4.3 z/OS

The Identity Manager Fan-Out driver z/OS Platform Receiver supports optional password replication.

A.4.4 Windows

The Identity Manager Fan-Out driver does not include a Platform Services component for Windows. Novell Account Management 3.0 Platform Services for Windows platforms are supported by the Identity Manager Fan-Out driver.

A.5 Distribution

There is no longer a distribution directory or a file distribution function provided through the Web interface. Individual components for the Identity Manager Fan-Out driver are distributed from the installation CD. There is a separate installation CD for each supported platform type.

Glossary

Account Redirecion

The process of ensuring that users and groups are the same accross all platforms by redirecting account information requests to a User or Group object in eDirectory.

AS Client API

The Authentication Services application programming interface (API). The AS Client API can be used by applications to perform functions, such as user ID/password verification, password changes, and obtaining information from eDirectory™.

ASAM directory

The file system directory that contains the binaries, configuration information, and other related files used by Identity Manager Fan-Out driver components.

ASAM Master User object

The User object that core driver components use for LDAP Bind operations.

ASAM System container object

The container object in eDirectory that holds component configuration and user and group management objects.

Audit Log

The log of occurrences of interest for auditing purposes. The Audit Log is maintained by the Audit Services component of each core driver.

Audit Services

The core driver component that performs logging.

Authentication Services

The set of services that provides access to information from eDirectory for authentication purposes. The principal components of Authentication Services are the core driver Authentication Services component, the Platform Services Process, the AS Client API, and the System Intercept.

Census

The collection of Enterprise User and Enterprise Group objects that represent users and groups from eDirectory that can be associated with a Platform Set. Object Services maintains the Census using provisioning events. Object Services on the primary core driver initially builds and periodically verifies the Census through the use of Trawls.

Census Search object

An eDirectory object used to specify users and groups to be included in the Census.

certificate

A digital object used to authenticate and secure SSL communications.

Certificate Services

The core driver component that issues certificates for other components.

context

The location of an object within the eDirectory tree.

core driver

The components that provide Identity Provisioning and Authentication Services to platforms, and provide for the management of the Identity Manager Fan-Out driver.

DES

Data Encryption Standard, approved by the U.S. government.

Enterprise Group (eGroup)

An object that represents a group of users that can be defined on a platform. Enterprise Group objects reside in the Census container.

Enterprise User (eUser)

An object that represents a user that can be defined on a platform. It is used by Authentication Services to locate the corresponding User object in eDirectory. Enterprise User objects reside in the Census container.

entropy daemon

A process that collects and provides cryptographically strong random data.

Event Driven Objects

A container in the ASAM System container that holds objects affected by provisioning events.

Event Journal Services

The core driver component that manages event information and provides provisioning events to Platform Receivers.

Event Subsystem

The core driver component that receives provisioning events from eDirectory and provides them to Object Services.

Identity Provisioning

The automatic provisioning of account related information from eDirectory to a target platform. The principal components of Identity Provisioning are the Event Subsystem, Object Services, Event Journal Services, Platform Receivers, and Receiver scripts.

Name Service Switch

A library for Linux and UNIX operating systems that implements a set of system functions used by programs to retrieve user and group account information. The Fan-Out driver provides a Name Service Switch that allows a Linux or UNIX system to redirect account information from eDirectory.

naming exception

A conflict detected by Object Services between multiple User or Group objects having the same common name.

Object Services

The core driver component that maintains the Census.

Operational Log

A log of occurrences pertaining to the processing of a component. Audit Services maintains the Operational Log for the core driver.

PAM

Pluggable Authentication Module. PAM is a standard framework for UNIX defined by OSF RFC 86.0 that provides for authentication of users by facilities external to the original UNIX operating system.

password redirection

The process of ensuring that users' passwords are the same across all platforms by redirecting authentication requests to a User object in eDirectory.

password replication

The process of ensuring that users' passwords are the same across all platforms by replicating password information between the platforms and eDirectory.

platform

A system that uses the core driver for Identity Provisioning, Authentication Services, or both.

platform configuration file

The file that contains configuration information for Platform Services. It identifies users to include or exclude from processing, and contains information used to locate the core driver servers.

Platform object

The object in the ASAM System container that contains information about a platform.

Platform Receiver

The Platform Services component that obtains provisioning events from Event Journal Services and runs Receiver scripts to process them as appropriate for the platform.

Platform Services

The Identity Manager Fan-Out driver components that run on a platform. These include the System Intercept, the Platform Services Process, the AS Client API, the Platform Receiver, and Receiver scripts.

Platform Services Cache Daemon

The process that runs on a platform and communicates with the core driver for Posix account information. Along with the Name Service Switch, the Platform Service Cache Daemon provides complete account redirection.

Platform Services Process

The process that runs on a platform and communicates with the core driver for Authentication Services. The Platform Services Process provides core driver server connection management, load balancing, and failover capability.

Platform Set

A group of platforms that share a common set of users and groups.

Platform Set Search object

An eDirectory object used to specify users and groups to be included in a Platform Set.

primary core driver

The core driver that serves the Web interface, provides environmental information during the installation of other core drivers, performs Census Trawls, and listens for events from eDirectory.

provisioning event

An event, such as an add, modify, or delete, originating from eDirectory, that pertains to a user account or group. The Event Subsystem subscribes to events from eDirectory and passes them to Object Services. Object Services records provisioning events in eUser and eGroup objects. Event Journal Services passes the events to Platform Receivers. Platform Receivers run Receiver scripts to process provisioning events as appropriate for the platform.

Provisioning Manager

The core driver component that comprises Object Services, Audit Services, Certificate Services, Event Journal Services, and Web Services. Platforms access the Provisioning Manager to obtain a security certificate and to obtain provisioning events.

Receiver script

A script invoked by the Platform Receiver to process provisioning events. A fully functional set of base scripts, written in the customary scripting language for the platform, is provided. You can extend these scripts as appropriate for your needs.

secondary core driver

Any core driver other than the primary core driver.

Secure Sockets Layer (SSL)

The communications protocol used for communication between components. SSL is a standard security protocol that provides communications privacy. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

System Intercept

A vendor-provided control point into the system that is used to interface with Authentication Services for a platform.

system log

The operating system log of information that is of system-wide interest.

Trawl

The process used by Object Services to collect information from eDirectory to initially build and periodically ensure the validity of the Census.

Universal Time

By international agreement, the world-wide standard for systematic time keeping. Universal Time is based on the mean solar time at zero degrees longitude. Formerly known as GMT, Universal Time is abbreviated as Z or as UT.

User and Group Subtree

The high level container object that you specify during installation of the core driver that holds users and groups that can be included in the Census. The ASAM Master User is granted Supervisor rights to this container.

Web interface

The Web-based interface that is used to administer and monitor the Identity Manager Fan-Out driver.

Web Services

The core driver component that provides the Web interface.