

# Fedora Directory Server 紹介

日本LDAPユーザ会  
2007/4/23  
武田 保真

# 目次

- Fedora Directory Serverの**紹介**
- Fedora Directory Serverの**インストール**
- Fedora Directory Serverの**起動と停止**

# Fedora Directory Serverとは？

- Fedora Projectによって開発されているオープンソースの Directory Server
- もともとは、RedHatが買収したNetscape Directory Server製品をオープンソース化し、Fedora Directory Serverとして開発、提供

<http://directory.fedoraproject.org/>

# Fedora Directory Serverの歴史

1996年: NetscapeがLDAPサーバの開発開始

1999年: Netscapeを買収したAOLがSunとiPlanetとして共同開発

2001年: iPlanetの共同開発が終了し、NetscapeとSunはそれぞれ独自のDirectory Server開発へ

2004年: RedHatがNetscape Directory Serverを買収

SunはiPlanetをもとにSun One Directory Serverとして開発

2005年: RedHatがFedora Directory Server(FDS)を発表

Sun Java System Directory Serverに名称変更(Sun JDS)

# Fedora Directory Serverの特徴

- 4ノードマルチマスタ構成のサポート
- Berkley DBによる高性能DBバックエンドの採用
- 高いスケーラビリティ
- Active Directoryとのユーザ情報の同期機能
- TLSなどによるLDAP認証の暗号化
- LDAPv3準拠
- 設定情報のオンラインアップデート対応
- GUIインタフェースによる管理

# FDSとOpenLDAPの関係

- 両者とも起源は、ミシガン大学のslapdプロジェクト。
- コンセプトは共通部分が多い
  - LDAPv3準拠
  - Berkley DBバックエンドの利用
  - レプリケーション(複製)のモデル
  - アクセスコントロール機能
- 実装は大きく異なる
  - 管理方法
  - レプリケーションの実装

## FDSとSun JDSの関係

- 両者ともiPlanetから発展。現在も多くの共通点を持つ
- レプリケーションプロトコルの互換性
  - Sun JDSのレガシーレプリケーションモードとFDSのレプリケーションの互換性
  - 共通した管理インターフェース

# FDSのライセンス

- Fedora Directory Serverの全てのコンポーネントがオープンソースのライセンス
- 一部のコンポーネントはGPL以外のオープンソースライセンス適用(MPLやApache License)

利用、改造、再配布は基本的に自由



# FDSの情報

- FDSのWiki
  - <http://directory.fedoraproject.org/>
- FDSのメーリングリスト
  - [http://directory.fedoraproject.org/wiki/Mailing\\_Lists](http://directory.fedoraproject.org/wiki/Mailing_Lists)
    - \* Announcements: [Fedora-directory-announce@redhat.com](mailto:Fedora-directory-announce@redhat.com)
    - \* Users: [Fedora-directory-users@redhat.com](mailto:Fedora-directory-users@redhat.com)
    - \* Developers: [Fedora-directory-devel@redhat.com](mailto:Fedora-directory-devel@redhat.com)
    - \* CVS Commits: [Fedora-directory-commits@redhat.com](mailto:Fedora-directory-commits@redhat.com)
- 日本語の書籍
  - LDAP Expert(**技術評論社**)
    - <http://www.gihyo.co.jp/magazines/ldap-se>

# Fedora Directory Serverのダウンロード

- **対応OS**

- Fedora Core 2 ~ Fedora Core 6
- RedHat Enterprise Linux 3、4

- **RPM形式のバイナリで配布**

<http://directory.fedoraproject.org/wiki/Download>

- **その他のOS**

- **ビルド方法**

- <http://directory.fedoraproject.org/wiki/Building>

# FDSをCentOS5(x86)にインストール

- Fedora Core 6用のFDS 1.0.4のRPMをダウンロード  
<http://directory.fedoraproject.org/wiki/Download>
  - fedora-ds-1.0.4-1.FC6.i386.opt.rpm(x86用)
- Sun JDK 1.5(JDK 5.0 Update11)をダウンロード
  - [http://java.sun.com/javase/download/index\\_jdk5.jsp](http://java.sun.com/javase/download/index_jdk5.jsp)
    - jdk-1\_5\_0\_11-linux-i586-rpm.bin

# Sun Javaのインストール(1)

- JDKのrpmパッケージのインストール

```
# sh ./jdk-1_5_0_11-linux-i586-rpm.bin
```

- gcjのjavaから、Sun JDKのjavaへ変更

```
# ls -l /etc/alternatives/java
```

```
lrwxrwxrwx 1 root root 35 Apr 21 07:52 /etc/alternatives/java ->
/usr/lib/jvm/jre-1.4.2-gcj/bin/java
```

- gcjのJavaの優先度を確認

```
# /usr/sbin/alternatives --display java
```

```
java - status is auto.
```

```
link currently points to /usr/lib/jvm/jre-1.4.2-gcj/bin/java
```

```
/usr/lib/jvm/jre-1.4.2-gcj/bin/java - priority 1420
```

## Sun Javaのインストール(2)

- gcjのJavaが優先度1420に設定されているため、それより高い優先度をSun Javaに設定

```
# /usr/sbin/alternatives --install /usr/bin/java java  
  /usr/java/jdk1.5.0_11/bin/java 1500 (1行で)
```

- javaのalternativesを更新

```
# /usr/sbin/alternatives --auto java
```

```
# ls -l /etc/alternatives/java
```

```
lrwxrwxrwx 1 root root 30 Apr 23 08:58 /etc/alternatives/java ->  
  /usr/java/jdk1.5.0_11/bin/java
```

# JAVA\_HOME環境変数設定

- Sun Java**を利用するために**JAVA\_HOME**環境変数を設定**
- **[設定例]** /etc/profile.d/sun\_java.sh

```
rpm -q jdk > /dev/null
```

```
[ "$?" = 1 ] && exit 1
```

```
JAVA_VER=`rpm -q --qf "%{VERSION}" jdk`
```

```
if [ -z "$JAVA_HOME" ] ; then
```

```
JAVA_HOME=/usr/java/jdk$JAVA_VER
```

```
fi
```

```
export JAVA_HOME
```

# FDSのインストール

```
# rpm -ihv fedora-ds-1.0.4-1.FC6.i386.opt.rpm
```

```
準備中...
```

```
##### [100%]
```

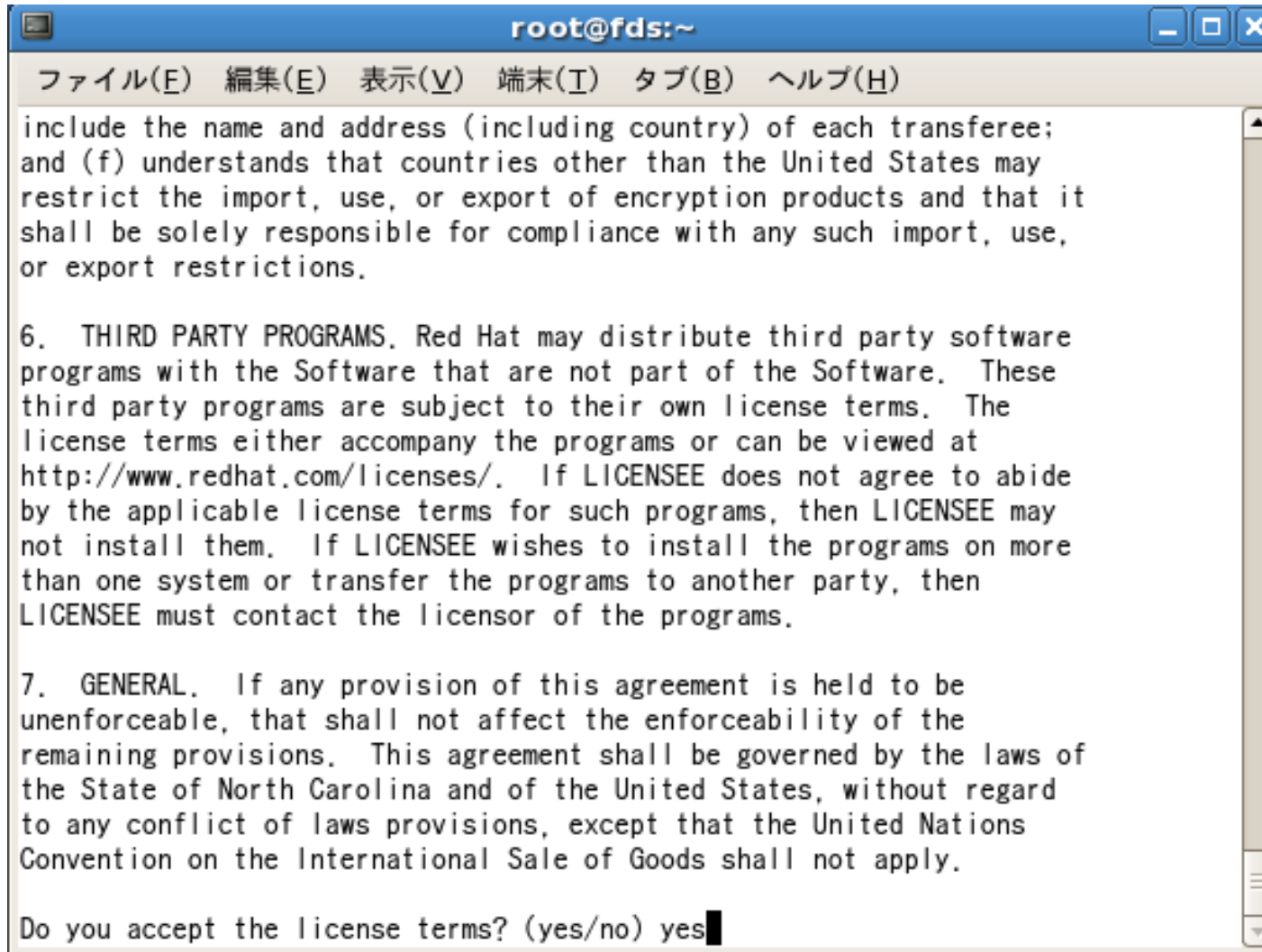
```
1:fedora-ds
```

```
##### [100%]
```

Install finished. **Please run /opt/fedora-ds/setup/setup** to complete installation and set up the servers.

```
# /opt/fedora-ds/setup/setup
```

# ライセンス条項の確認

A terminal window titled 'root@fds:~' with standard window controls. The menu bar includes 'ファイル(E)', '編集(E)', '表示(V)', '端末(T)', 'タブ(B)', and 'ヘルプ(H)'. The main text area contains several paragraphs of license terms, including sections for transferees, third-party programs, and general provisions. At the bottom, it asks 'Do you accept the license terms? (yes/no) yes' with a cursor at the end.

```
root@fds:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
include the name and address (including country) of each transferee;
and (f) understands that countries other than the United States may
restrict the import, use, or export of encryption products and that it
shall be solely responsible for compliance with any such import, use,
or export restrictions.

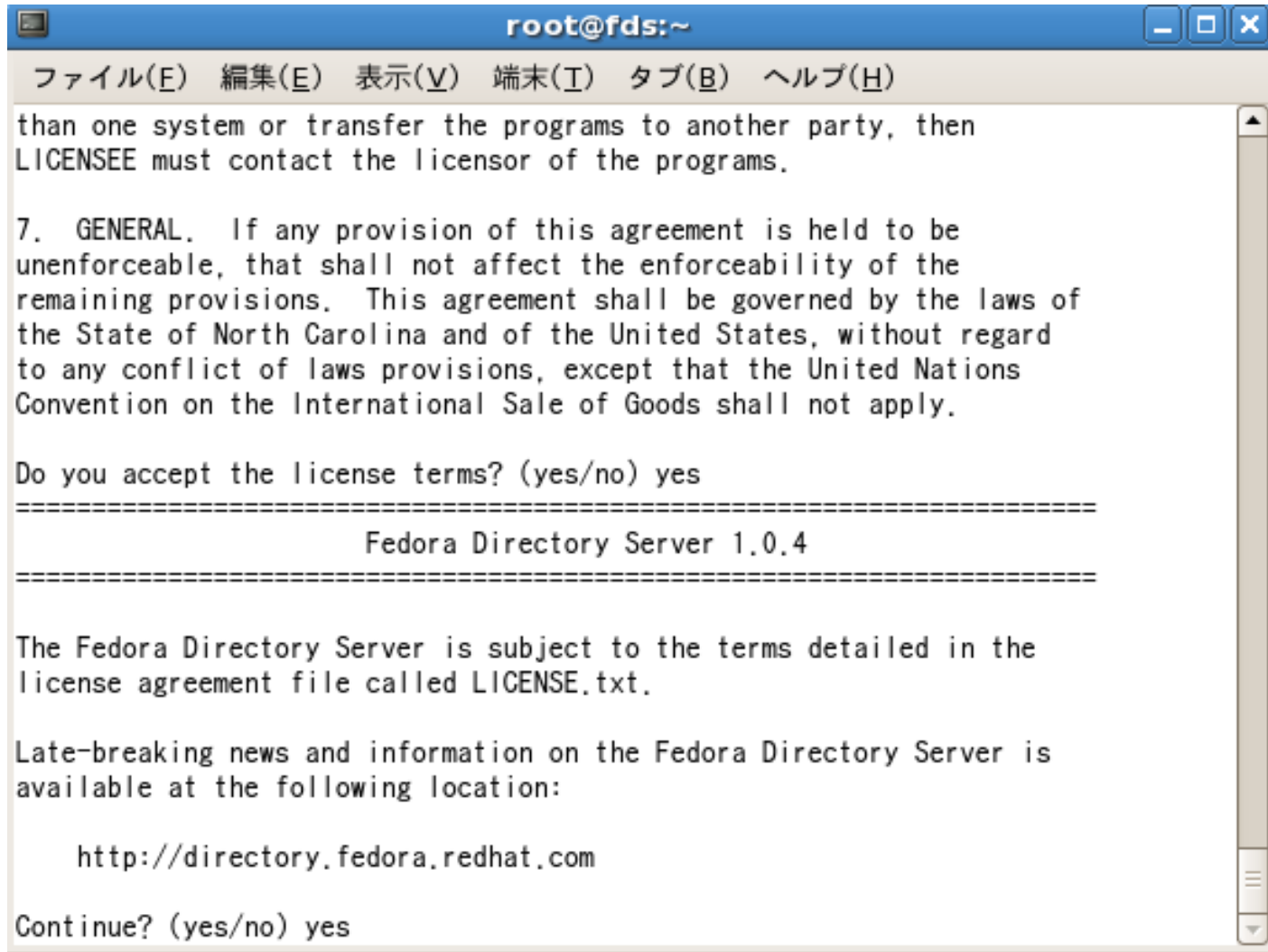
6.  THIRD PARTY PROGRAMS. Red Hat may distribute third party software
programs with the Software that are not part of the Software. These
third party programs are subject to their own license terms. The
license terms either accompany the programs or can be viewed at
http://www.redhat.com/licenses/. If LICENSEE does not agree to abide
by the applicable license terms for such programs, then LICENSEE may
not install them. If LICENSEE wishes to install the programs on more
than one system or transfer the programs to another party, then
LICENSEE must contact the licensor of the programs.

7.  GENERAL. If any provision of this agreement is held to be
unenforceable, that shall not affect the enforceability of the
remaining provisions. This agreement shall be governed by the laws of
the State of North Carolina and of the United States, without regard
to any conflict of laws provisions, except that the United Nations
Convention on the International Sale of Goods shall not apply.

Do you accept the license terms? (yes/no) yes
```



# FDSの最新情報のURL



```
root@fds:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
than one system or transfer the programs to another party, then
LICENSEE must contact the licensor of the programs.

7. GENERAL. If any provision of this agreement is held to be
unenforceable, that shall not affect the enforceability of the
remaining provisions. This agreement shall be governed by the laws of
the State of North Carolina and of the United States, without regard
to any conflict of laws provisions, except that the United Nations
Convention on the International Sale of Goods shall not apply.

Do you accept the license terms? (yes/no) yes
=====
                          Fedora Directory Server 1.0.4
=====

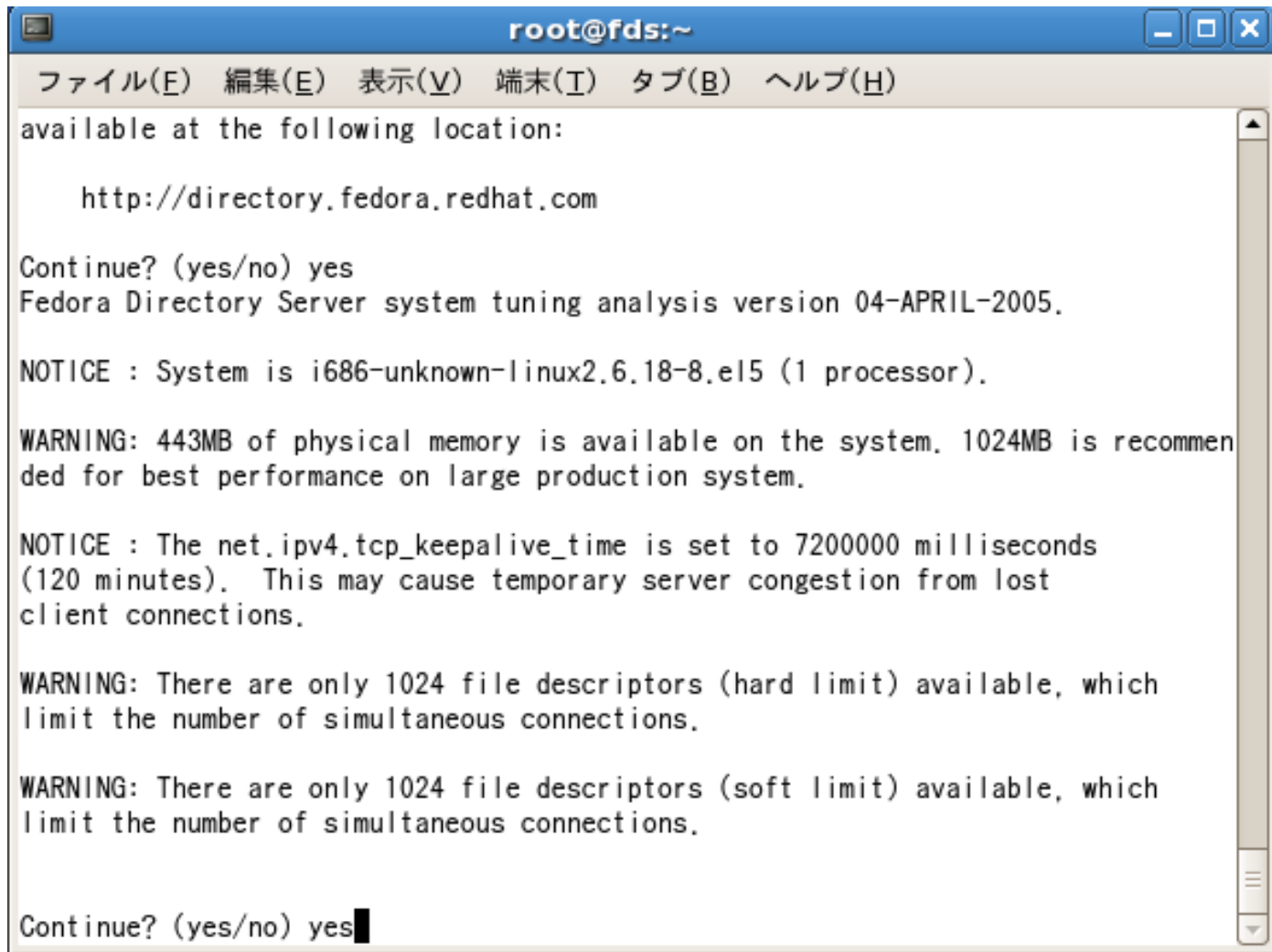
The Fedora Directory Server is subject to the terms detailed in the
license agreement file called LICENSE.txt.

Late-breaking news and information on the Fedora Directory Server is
available at the following location:

    http://directory.fedora.redhat.com

Continue? (yes/no) yes
```

# システム要件の確認



```
root@fds:~
ファイル(E) 編集(E) 表示(V) 端末(T) タブ(B) ヘルプ(H)
available at the following location:

    http://directory.fedora.redhat.com

Continue? (yes/no) yes
Fedora Directory Server system tuning analysis version 04-APRIL-2005.

NOTICE : System is i686-unknown-linux2.6.18-8.el5 (1 processor).

WARNING: 443MB of physical memory is available on the system, 1024MB is recommended for best performance on large production system.

NOTICE : The net.ipv4.tcp_keepalive_time is set to 7200000 milliseconds (120 minutes). This may cause temporary server congestion from lost client connections.

WARNING: There are only 1024 file descriptors (hard limit) available, which limit the number of simultaneous connections.

WARNING: There are only 1024 file descriptors (soft limit) available, which limit the number of simultaneous connections.

Continue? (yes/no) yes
```

## インストールモードの選択

- デフォルトは2番のTypical

```
Please select the install mode:  
1 - Express - minimal questions  
2 - Typical - some customization (default)  
3 - Custom - lots of customization  
  
Please select 1, 2, or 3 (default: 2)
```

## ホスト名の設定

- デフォルトはシステムに設定されているホスト名

```
Hostname to use (default: fds.example.com)
```

# FDSサーバの実行ユーザID

- デフォルトのnobody/nobodyのまま

```
Server user ID to use (default: nobody)
```

```
Server group ID to use (default: nobody) █
```

# FDSのconfigurationサーバの設定

- 最初は「No」を選択

```
Fedora Project
Directory Installation/Uninstallation
-----
Fedora server information is stored in the Fedora configuration
directory server, which you may have already set up.  If so, you
should configure this server to be managed by the configuration
server.  To do so, the following information about the configuration
server is required: the fully qualified host name of the form
<hostname>.<domainname>(e.g. hostname.domain.com), the port number,
the suffix, and the DN and password of a user having permission to
write the configuration information, usually the Fedora
configuration directory administrator.

If you want to install this software as a standalone server, or if you
want this instance to serve as your Fedora configuration directory
server, press Enter.

Do you want to register this software with an existing
Fedora configuration directory server? [No]:
```

# 既存のLDAPエントリの利用

- 最初は「No」を選択

```
Fedora Project
Directory Installation/Uninstallation
```

---

```
If you already have a directory server you want to use to store your
data, such as user and group information, answer Yes to the following
question. You will be prompted for the host, port, suffix, and bind
DN to use for that directory server.
```

```
If you want this directory server to store your data, answer No.
```

```
Do you want to use another directory to store your data? [No]: █
```

# LDAPサーバのポート番号

- 通常はデフォルトの389番ポート

```
Fedora Project  
Directory Installation/Uninstallation
```

---

```
The standard directory server network port number is 389. However, if  
you are not logged as the superuser, or port 389 is in use, the  
default value will be a random unused port number greater than 1024.  
If you want to use port 389, make sure that you are logged in as the  
superuser, that port 389 is not in use, and that you run the admin  
server as the superuser.
```

```
Directory server network port [389]:
```

# ディレクトリサーバーの識別子

- デフォルトはホスト名

```
Fedora Project
Directory Installation/Uninstallation
```

---

```
Each instance of a directory server requires a unique identifier.
Press Enter to accept the default, or type in another name and press
Enter.
```

```
Directory server identifier [fds]: █
```



# 管理用コンソールの管理者ユーザ名

- デフォルトは「admin」
- 管理者用パスワードの設定

```
Fedora Project  
Directory Installation/Uninstallation
```

---

```
Please enter the administrator ID for the Fedora configuration  
directory server. This is the ID typically used to log in to the  
console. You will also be prompted for the password.
```

```
Fedora configuration directory server  
administrator ID [admin]:  
Password:  
Password (again):
```

## root suffixの設定

- 通常はDNS名をもとに割り当てることが多い

```
Fedora Project  
Directory Installation/Uninstallation
```

---

```
The suffix is the root of your directory tree. You may have more than  
one suffix.
```

```
Suffix [dc=example, dc=com]: █
```

# LDAP管理者の設定

- デフォルトは「cn=Directory Manager」

```
Fedora Project
Directory Installation/Uninstallation
```

```
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and typically has a
bind Distinguished Name (DN) of cn=Directory Manager. Press Enter to
accept the default value, or enter another DN. In either case, you
will be prompted for the password for this user. The password must
be at least 8 characters long.
```

```
Directory Manager DN [cn=Directory Manager]: █
```

# 管理ドメインの設定

- 分散管理する場合などに設定
- 通常はデフォルト値

```
Fedora Project
Directory Installation/Uninstallation
```

---

```
The Administration Domain is a part of the configuration directory
server used to store information about Fedora software.  If you are
managing multiple software releases at the same time, or managing
information about multiple domains, you may use the Administration
Domain to keep them separate.
```

```
If you are not using administrative domains, press Enter to select the
default.  Otherwise, enter some descriptive, unique name for the
administration domain, such as the name of the organization responsible
for managing the domain.
```

```
Administration Domain [example.com]: █
```

# 管理サーバのポート番号

- 管理サーバ用のポート番号はランダムに選択される

```
Fedora Project
Administration Installation/Uninstallation
```

---

```
The Administration Server is separate from any of your application
servers since it listens to a different port and access to it is
restricted.
```

```
Pick a port number between 1024 and 65535 to run your Administration
Server on. You should NOT use a port number which you plan to
run an application server on, rather, select a number which you
will remember and which will not be used for anything else.
```

```
The default in brackets was randomly selected from the available
ports on your system. To accept the default, press return.
```

```
Administration port [4867]: █
```

# 管理サーバの実行ユーザ

- 通常はデフォルトの「root」

```
Fedora Project
Administration Installation/Uninstallation
```

---

```
The Administration Server program runs as a certain user on your
system. This user should be different than the one which your
application servers run as. Only the user you select will be
able to write to your configuration files. If you run the
Administration Server as "root", you will be able to use the Server
Administration screen to start and stop your application servers.
```

```
Run Administration Server as [root]: █
```

# Webサーバ(httpd)の実行ファイル

- RedHat系は/usr/sbin(デフォルト値)

```
Fedora Project  
Administration Installation/Uninstallation
```

---

```
The Administration Server runs on the Apache web server. Please provide the  
directory where the Apache binary (httpd or httpd.worker) may be found. The  
Administration Server needs an Apache compiled with the worker model.
```

```
Apache Directory [/usr/sbin/]: █
```

# 設定完了

- 設定に問題なければFDSがスタート

```
Server group ID to use (default: nobody)
[slapd-fds]: starting up server ...
[slapd-fds]:   Fedora-Directory/1.0.4 B2006.312.1539
[slapd-fds]:   fds.example.com:389 (/opt/fedora-ds/slapd-fds)
[slapd-fds]:
[slapd-fds]: [23/Apr/2007:09:39:50 +0900] - Fedora-Directory/1.0.4 B2006.312.1539
9 starting up
[slapd-fds]: [23/Apr/2007:09:39:51 +0900] - slapd started.  Listening on All Int
erfaces port 389 for LDAP requests
Your new directory server has been started.
Created new Directory Server
Start Slapd Starting Slapd server configuration.
Success Slapd Added Directory Server information to Configuration Server.
Configuring Administration Server...
Setting up Administration Server Instance...
Configuring Administration Tasks in Directory Server...
Configuring Global Parameters in Directory Server...

You can now use the console.  Here is the command to use to start the console:
cd /opt/fedora-ds
./startconsole -u admin -a http://fds.example.com:4867/

INFO Finished with setup, logfile is setup/setup.log
```



# 管理コンソールの起動

- サーバ起動時のメッセージに管理コンソールの起動方法

```
You can now use the console. Here is the command to use to start the console:  
cd /opt/fedora-ds  
./startconsole -u admin -a http://fds.example.com:4867/
```

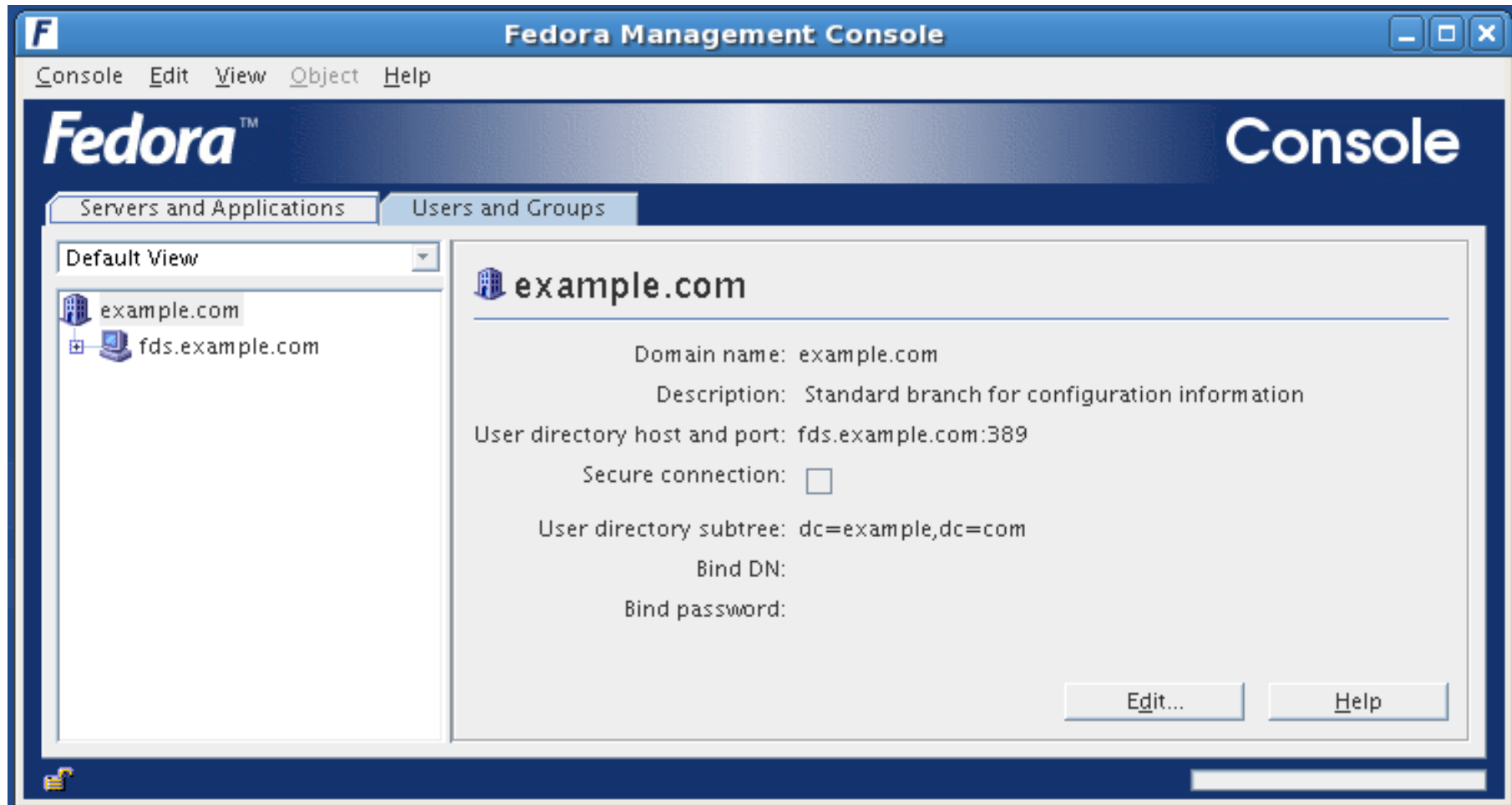
- **必ず「cd /opt/fedora-ds 」をしてから、コマンド実行**
- **ポート番号などを忘れた場合は、/opt/fedora-ds/admin-serv/config/adm.confを確認**

# 管理コンソールのログイン画面

- adminユーザのパスワードを入力してログイン

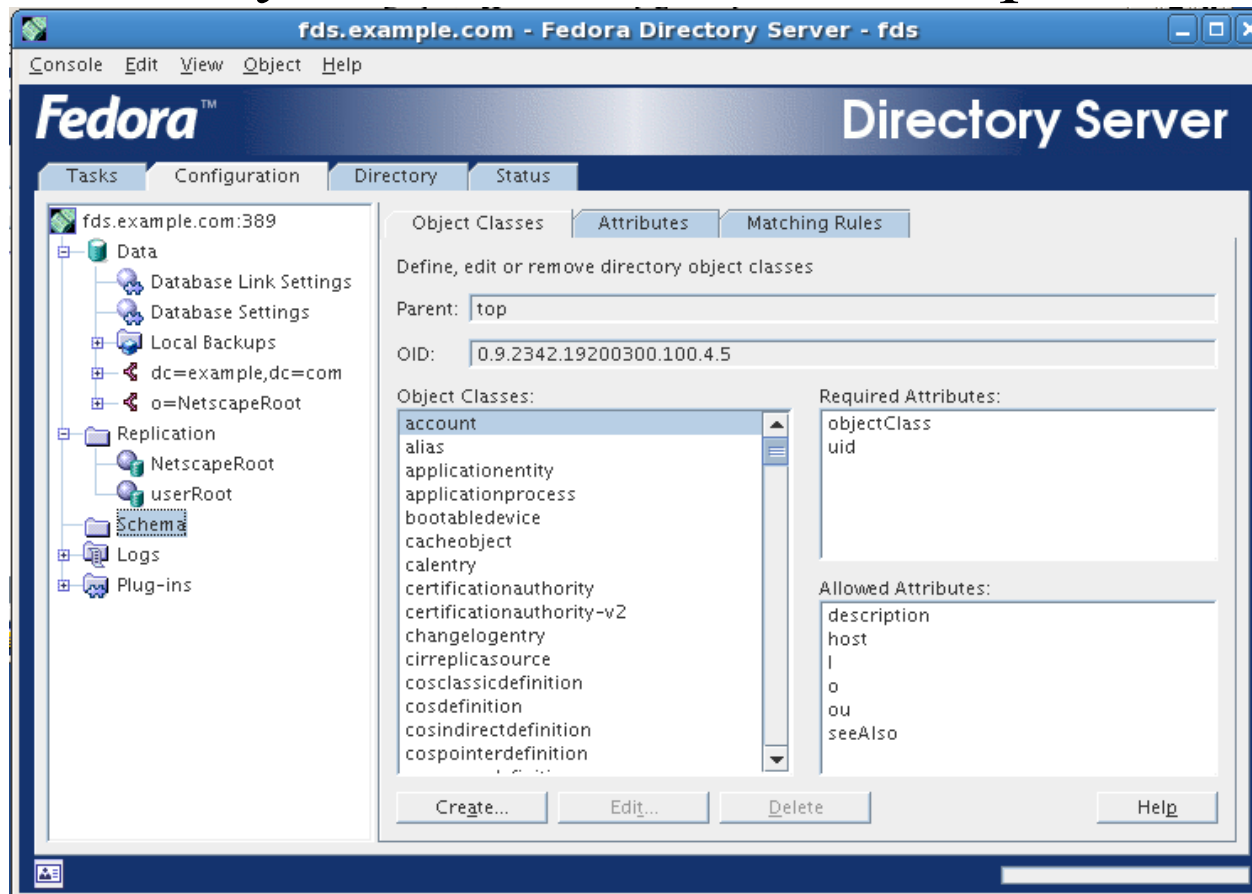


# 管理コンソール



# LDAPサーバの管理画面

- 「Directory Server」を選択して、「open」をクリック



# ディレクトリサーバーの起動と停止

- ディレクトリサーバーの起動

- # `cd /opt/fedora-ds/slapd-[識別子]`
- # `./start-slapd`

- ディレクトリサーバーの停止

- # `cd /opt/fedora-ds/slapd-[識別子]`
- # `./stop-slapd`

- 起動の確認

- # `ps -ef | grep ns-slapd`

```
nobody 3082 1 0 09:39 ? 00:00:02 ./ns-slapd -D
/opt/fedora-ds/slapd-fds -i /opt/fedora-ds/slapd-fds/logs/pid -w
/opt/fedora-ds/slapd-fds/logs/startpid
```

# 管理サーバの起動と停止

- **管理サーバの起動**
  - 前もってディレクトリサーバを起動しておく
  - # `cd /opt/fedora-ds`
  - # `./start-admin`
- **管理サーバの停止**
  - # `cd /opt/fedora-ds`
  - # `./stop-admin`

## スキーマの追加

- /opt/fedora-ds/slaped-[識別子]/config/schemaディレクトリに追加
- [例] Samba 3.0用のスキーマの追加
  - # cp /usr/share/doc/samba-3.0.23c/LDAP/samba-schema-netscapeds5.x /opt/fedora-ds/slaped-[識別子]/config/schema/61samba.ldif (1行で)
- スキーマ追加後は、ディレクトリサーバを再起動

# CentOS5のLDAP認証設定

- authconfig-gtkコマンドで設定

