インストールガイド v2.0

オープンソース・ソリューション・テクノロジ(株)

作成日: 2011 年 1 月 19 日

リビジョン: 2.0

目次

はじめに....1
Linux 版 Unicorn ID Manager パッケージ....2
1 システム要件....2
1.1 ソフトウェア要件....2
1.2 ハードウェア要件....2
2 パッケージ構成....2
3 Linux 版パッケージのインストール....3
3.1 準備....3
3.2 パッケージのインストール....3
4 Unicorn ID Manager の起動....3
Unicorn ID Manager の設定....5
1 対象組織の設定....5
2 バックエンド(LDAP サーバー)の設定....8
3 バックエンド(Active Directory サーバー)の設定....12
4 バックエンド(Google Apps)の設定....16
インストールガイド更新履歴....18
1 2010/12/18 Unicorn ID Manager インストールガイド　V1.0....18
2 2011/01/19 Unicorn ID Manager インストールガイド V2.0....18

. はじめに

本ドキュメントは、弊社提供の Unicorn ID Manager を導入するための手順書です。

Unicorn ID Manager のインストールの際に、必ず本ドキュメントの内容を確認してから、作業を実施してください。

本ドキュメントに関する記載内容について、疑問点等がある場合には、弊社サポート窓口までお問い合わせください。

. Linux 版 Unicorn ID Manager パッケージ

1 システム要件

1.1 ソフトウェア要件

以下のいずれかの OS 環境が必要です。

- RedHat Enterprise Linux 5 / CentOS 5 (x86, x86-64)

1.2 ハードウェア要件

ソフトウェア要件に記載の OS が動作する以下のハードウェア環境が必要です。

CPU:	Intel Pentium III 1GHz 以上あるいは互換 CPU	
メモリ:	512MB 以上	
ディスク:	ソフトウェア: /opt/osstech	512MB 以上
	データ、ログ: /var/opt/osstech	1GB 以上(推奨)

2 パッケージ構成

弊社が提供する Solaris 版 ソフトウェアは以下のパッケージにより構成されています。

- OSSTech ソフトウェア製品基本パッケージ
  - osstech-base
  - osstech-support
  - osstech-daemontools
- Unicorn ID Manager パッケージ
  - osstech-unicornIDM
  - osstech-Django
  - osstech-Django-docs
  - osstech-googleapps-account
  - osstech-python-gdata
  - osstech-python-googleapps-utils
  - osstech-python-ntlm
  - osstech-python-sqlite2
  - osstech-python-ymailutils
  - osstech-winexe
  - m2crypto
  - python-ldap-2.2.0-2.1.1.x86_64.rpm (x86-64 環境のみ)

python-ldap パッケージは、RHEL5/CentOS5 の標準パッケージに含まれる x86-64 環境のみで発生する問題を修正するために必要です。

3 Linux 版パッケージのインストール

3.1 準備

パッケージのインストールは、root ユーザーのみに許可されていますので、最初に su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（画面には表示されません）
```

次に弊社から提供されたパッケージ一式をインストール先ホストの任意のディレクトリに展開します。下記の例では/srv/osstech/software/RPMS に展開したことを前提とて記述します。

3.2 パッケージのインストール

弊社提供の Unicorn ID Manager パッケージは、/opt/osstech ディレクトリに新規インストールされます。

“/srv/osstech/software/RPMS/”に弊社提供のパッケージ一式がコピーしてあることを確認します。

```
# cd /srv/osstech/software/RPMS
# ls
base  unicornIDM
```

まず最初に、base ディレクトリにある osstech-base、osstech-support、osstech-daemontools パッケージをインストールします。 既にこれらのパッケージがインストールされている場合は、この手順は不要です。

```
# rpm -ihv base/*rpm
```

続いて、Unicorn ID Manager パッケージ一式をインストールします。

```
# rpm -Uhv unicornIDM/*rpm
```

以上で、Unicorn ID Manager パッケージのインストールは完了です。

4 Unicorn ID Manager の起動

パッケージのインストール完了後、次の手順で Unicorn ID Manager の初期化を行ないます。

最初に su コマンドで root ユーザーになります。

```
$ su -
Password: root のパスワードを入力（画面には表示されません）
```

Unicorn ID Manager の初期セットアップコマンドを実行します。

途中で、Unicorn ID Manager にログインする際の管理者ユーザーの登録を促されますので、管理者名とメールアドレス、パスワードを入力してください。なお、現在の Unicorn ID Manager では、ここで登録した管理者のメールアドレスへのメール送信は行なっていません。

```
# /opt/osstech/sbin/unicornidm-setup
....
Would you like to create one now? (yes/no): yes  ← yes を入力して管理者を作成します
Username (Leave blank to use 'root'): admin ← 管理者ユーザー名
E-mail address: admin@example.com ← 管理者のメールアドレス
Password: ********
Password (again): ********
Superuser created successfully.
```

セットアップコマンドが完了したら、Apache を起動します。

```
# /sbin/service httpd start
```

Unicorn ID Manager の管理画面にアクセスして、初期設定を行なってください。

http://<サーバー>/unicornIDM/admin/

. Unicorn ID Manager の設定

Unicorn ID Manager の設定画面にログインすると、次の画面が表示されます。

Unicorn ID Manager の基本的な設定は、

1. 「対象組織」
2. 「バックエンド」

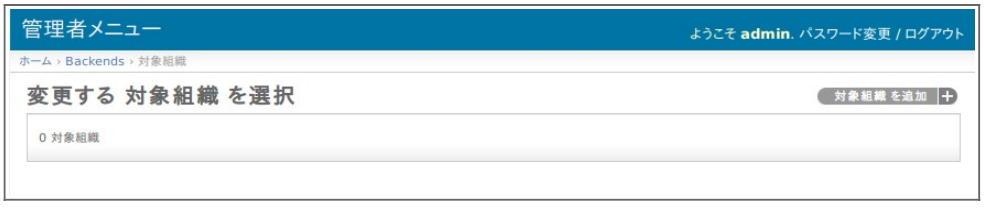
の設定を行うことで完了します。

1 対象組織の設定

Unicorn ID Manager では、バックエンドのサーバー群に対する一連の動作の動作単位を「対象組織」として設定します。

対象組織に対して、管理する LDAP、Active Directory、Google Apps をバックエンドとして追加します。

「対象組織」の設定は、管理画面で「対象組織」を選択します。



画面右端上部の「対象組織を追加」のボタンを選択します。
「対象組織」に設定可能なパラメーターの設定画面が表示されます。

各項目の意味を説明します。

基本設定

- 対象組織の識別子
  - 組織を特定するための名称です。英字、数字のみ利用可能です。
- 対象組織名
  - 対象組織を表す組織名です。日本語を含めて設定可能です。

ログ設定

- ログレベル
  - Unicorn ID Manager のデバッグログの出力レベルです。運用時は 1 を設定してください。大きい数字にすると詳細なログが出力されます。
- ログファイルの最大サイズ
  - デバッグログの 1 ファイルの最大サイズです。
- ログローテート数
  - デバッグログのログファイルを最大いくつまでローテーションするか指定します。
- ログファイルのディレクトリ
  - デバッグログの出力先です。(変更不要です。)
- syslog 機能を有効

- この設定を有効にすると、Unicorn IDM 経由でのユーザーアカウントの操作履歴が syslog に出力されます。(出力される内容はデバッグログではありません)

- Syslog の Facility 設定
  - syslog 機能を有効にしているときに、syslog の出力先となる Facility を選択します。

表示設定

- CSV ファイルのエンコーディング
  - 管理者が CSV ファイルを一括操作のためにアップロードする時の、CSV ファイルのエンコーディングです。「選択」を指定した場合は、アップロード時に「UTF-8」か「シフト JIS」を選択することができます。
- プレビュー時に表示されるエントリ数
  - CSV ファイルのアップロード時に、CSV の内容をプレビューします。このときに、先頭からいくつのエントリ数をプレビューするか指定します。
- サマリに表示されるエントリ数
  - CSV の一括操作の操作結果を、直近のものからいくつ表示するか指定します。

パスワードの複雑性

- ユーザーのパスワードの最大文字数
  - パスワード変更画面でパスワードとして設定可能な最大文字数を指定します。
- ユーザーのパスワードの最小文字数
  - パスワード変更画面でパスワードとして設定可能な最小文字数を指定します。
- パスワードの複雑性をチェック
  - この設定を有効にすると、一般ユーザーがパスワード変更画面でパスワードを設定する際に、パスワードの複雑性がチェックされます。
  - 管理者ページでパスワードを変更する場合には、複雑性のチェックは行われません。
  - パスワードの複雑性は次の条件を組み合わせて設定します。
    - パスワードに含めなければならない英字(大文字、小文字)の数
    - パスワードに含めなければならない英字(大文字)の数
    - パスワードに含めなければならない英字(小文字)の数
    - パスワードに含めなければならない数字の数
    - パスワードに含めなければならない記号の数
- パスワード変更時のユーザー向けの注意書き
  - この欄に記載したテキストが、パスワード変更画面に注意書きとして表示されます。

システム設定

- 操作完了後にアップロードしたファイルを削除

    - CSV ファイルの一括処理時に、アップロードした CSV ファイルを削除する場合は、この設定を有効にしてください。
- 属性を削除するための値
    - CSV ファイルの一括操作時に、設定済みの属性を削除したいときに、CSV ファイルのエントリに記載する文字列を設定します。デフォルトは「Null」です。

以上の項目を入力したら、最下段の「保存」をクリックします。
「対象組織」に入力した組織が登録されます。

続いて、バックエンドの設定を行いますので、左上のリンクの「ホーム」をクリックします。

2 バックエンド(LDAP サーバー)の設定

LDAP サーバーのアカウント管理を行う場合、「バックエンド(LDAP サーバー)」を選択します。

画面右上の「バックエンド(LDAP サーバー)を追加」のボタンをクリックします。

各項目の意味を説明します。

基本設定

- Org
  - この LDAP サーバーを、どの「対象組織」の管理下に置くか選択します。
- サーバーの識別子
  - この LDAP サーバーを特定できる名称を指定します。Unicorn ID Manager の表示等で利用されます。
- プライオリティ
  - 対象組織内で、この LDAP サーバーに対して何番目に処理を行うか１以上の数値で指定します。
- バックグラウンドでの CSV 一括処理
  - CSV ファイルを一括処理する際に、LDAP サーバーに対してバックグラウンドで処理を行う場合は、この設定を有効にします。
  - この設定が無効な場合は、LDAP サーバーへの一括処理が完了してから、ブラウザに応答が返ります。
- IP アドレス
  - LDAP サーバーの IP アドレスを指定します。
- ホスト名
  - LDAP サーバーのホスト名を指定します。

- プロトコル
  - LDAP サーバーに接続するときのプロトコルとして、LDAP か LDAPS を指定します。
- LDAP 管理者の DN
  - LDAP のエントリの更新権を持つユーザーの DN を指定します。
- LDAP 管理者のパスワード
  - LDAP に接続する DN のパスワードを指定します。
- LDAP のベース Suffix
  - LDAP サーバーのベース Suffix を指定します。
- ユーザーエントリの Suffix
  - ユーザーが格納されているツリーの DN を指定します。Unicorn ID Manager は、ここで指定した DN のサブツリーをユーザーの検索対象とします。
- グループエントリの Suffix
  - グループが格納されているツリーの DN を指定します。Unicorn ID Manager は、ここで指定した DN のサブツリーをグループの検索対象とします。

同期設定

- ユーザーのパスワード変更時にこのサーバーのパスワードを同期する
  - パスワード変更画面からパスワードを変更したときに、この LDAP サーバーのパスワードを変更します。
- ユーザーのアカウント操作時に、このサーバーのアカウントを同期する
  - 管理者が CSV やアカウントの操作を行なった時に、この LDAP サーバーのユーザーエントリを更新します。
- このサーバーでユーザーを認証する
  - パスワード変更ページでユーザーを認証するときに、この LDAP サーバーで認証が成功した場合に、パスワード変更を許可します。パスワード変更時には、「対象組織」に含まれるいずれかのバックエンドで認証が成功すれば、パスワード変更を許可します。
- パスワード変更時に「ユーザーが存在しない」エラーを無視する
  - この LDAP サーバー上でのパスワード変更が失敗しても、パスワード更新としては成功としてみなすための設定です。通常は無効に設定してください。

デフォルト値

- パスワードの暗号化方式
  - LDAP サーバーに格納するパスワードの暗号化方式を選択します。
- UNIX のホームディレクトリのデフォルトのパス
  - CSV ファイルでユーザーを登録する際に、UNIX 用のホームディレクトリの値(unixHomeDirectory)を指定しなかった場合のデフォルト値です。

- 「%USERNAME%」の部分はユーザー名に置換されます。

- デフォルトの GID
  - CSV ファイルでユーザーを登録する際に、UNIX 用の GID 番号(gidNumber)の値を指定しなかった場合のデフォルト値です。
- ユーザーのデフォルトのログインシェル
  - CSV ファイルでユーザーを登録する際に、UNIX 用のログインシェル(loginShell)の値を指定しなかった場合のデフォルト値です。
- Gecos フィールドを sn と givenName で設定する
  - CSV ファイルでユーザーを登録する際に、UNIX 用の GECOS(gecos)の値を指定しなかった場合に、「sn givenName」の設定値で gecos フィールドを設定します。
  - gecos フィールドには英数字以外含めることができないため、この設定を有効にした場合、「sn」「givenName」のフィールドにも英数字以外含めることができなくなります。

追加コマンド実行

- ユーザー登録後に追加のコマンドを実行
  - ユーザーアカウント登録操作の後にコマンドを実行したい場合に有効にします。
  - ユーザー登録後に実行するコマンドのパスを指定します。
  - コマンドの引数を、LDAP に登録する属性名で指定します。指定した順番で属性に設定した値がコマンドの引数に渡されます。
- ユーザー更新後に追加のコマンドを実行
  - ユーザーアカウント更新操作の後にコマンドを実行したい場合に有効にします。
  - ユーザー更新後に実行するコマンドのパスを指定します。
  - コマンドの引数を、LDAP に登録する属性名で指定します。指定した順番で属性に設定した値がコマンドの引数に渡されます。
- ユーザー削除前にコマンドを実行
  - ユーザーアカウントの削除操作の前にコマンドを実行したい場合に有効にします。
  - ユーザー削除前に実行するコマンドのパスを指定します。
  - コマンドの引数には、ユーザー名、ユーザーのホームディレクトリが渡されます。
- ユーザー有効化後にコマンドを実行
  - ユーザーアカウントの有効化操作の後にコマンドを実行したい場合に有効にします。
  - ユーザーアカウントの有効化操作後に実行するコマンドのパスを指定します。
  - コマンドの引数には、ユーザー名が渡されます。
- ユーザー無効化後にコマンドを実行
  - ユーザーアカウントの無効化操作の後にコマンドを実行したい場合に有効にします。
  - ユーザーアカウントの無効化操作後に実行するコマンドのパスを指定します。
  - コマンドの引数には、ユーザー名が渡されます。

UID 番号関連設定

- UID 番号を自動的に割り当て
  - CSV でのユーザー一括登録時に、uidNumber が指定されていないユーザーに対して、自動的に利用されていない UID 番号を割り当てます。
- 自動的に割り当てる UID 番号の最小値
  - 自動的に割り当てる UID 番号の最小値です。
- 自動的に割り当てる UID 番号の最大値
  - 自動的に割り当てる UID 番号の最大値です。
- 自動的に割り当てる次の UID 番号
  - 次にユーザーを登録したときに割り当てられる UID 番号です。通常は変更する必要はありません。

ランダム文字列設定

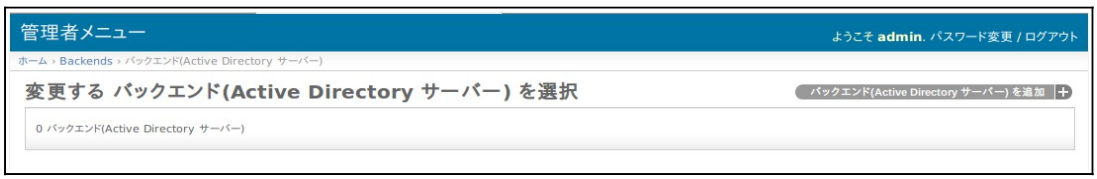
- ランダムに生成した文字列を自動で追加
  - LDAP にユーザーを登録する際に、ある属性にランダムな文字列を自動的に割り当てたい場合に有効に設定します。指定した文字数で、ランダムな英数字からなる文字列が登録されます。
- ランダムに生成した文字列の属性名
  - 文字列を登録する LDAP の属性名を指定します。
- ランダムに生成する文字列の文字数
  - 生成する文字列の文字数を指定します。

ユーザーエントリのオブジェクトクラス

ユーザー登録時に、ユーザーのエントリの objectClass として登録するオブジェクトクラス名を選択します。

3 バックエンド(Active Directory サーバー)の設定

Active Directory サーバーの管理を行う場合、「バックエンド(Active Directory サーバー)」を選択します。



画面右上の「バックエンド(Active Directory サーバー)を追加」をクリックします。

各項目の設定を完了後、最下部の「保存」ボタンをクリックして設定を保存します。

各項目の意味を説明します。

基本設定

- Org
  - この Active Directory サーバーを、どの「対象組織」の管理下に置くか選択します。
- サーバーの識別子
  - この Active Directory サーバーを特定できる名称を指定します。Unicorn ID Manager の表示等で利用されます。
- プライオリティ
  - 対象組織内で、この Active Directory サーバーに対して何番目に処理を行うか 1 以上の数値で指定します。
- バックグラウンドでの CSV 一括処理
  - CSV ファイルを一括処理する際に、Active Directory サーバーに対してバックグラウンドで処理を行う場合は、この設定を有効にします。
  - この設定が無効な場合は、Active Directory サーバーへの一括処理が完了してから、ブラウザに応答が返ります。
- IP アドレス
  - Active Directory サーバーの IP アドレスを指定します。

- ホスト名
  - Active Directory サーバーのホスト名を指定します。
- Active Directory のドメイン名
  - 接続先の Active Directory のドメイン名を指定します。
- Active Directory 管理者のユーザー名
  - Domain Admins 権限を持つ Active Directory の管理者ユーザー名を指定します。
- Active Directory 管理者のパスワード
  - 指定した Active Directory 管理者のパスワードを指定します。

同期設定

- ユーザーのパスワード変更時にこのサーバーのパスワードを同期する
  - パスワード変更画面からパスワードを変更したときに、この Active Directory サーバーのパスワードを変更します。
- ユーザーのアカウント操作時に、このサーバーのアカウントを同期する
  - 管理者が CSV やアカウントの操作を行なった時に、この Active Directory サーバーのユーザーエントリを更新します。
- このサーバーでユーザーを認証する
  - パスワード変更ページでユーザーを認証するときに、この Active Directory サーバーで認証が成功した場合に、パスワード変更を許可します。パスワード変更時には、「対象組織」に含まれるいずれかのバックエンドで認証が成功すれば、パスワード変更を許可します。
- パスワード変更時に「ユーザーが存在しない」エラーを無視する
  - この Active Directory サーバー上でのパスワード変更が失敗しても、パスワード更新としては成功としてみなすための設定です。通常は無効に設定してください。

デフォルト値

- ユーザーのデフォルトのプライマリグループ名
  - ユーザー登録時に、ユーザーが所属するデフォルトのプライマリグループです。通常は「Domain Users」です。
- ユーザーのデフォルトの OU
  - ユーザー登録時に、CSV で OU が指定されない場合のデフォルトの OU です。通常は「CN=Users」です。
- ユーザーのデフォルトのホームドライブ
  - ユーザー登録時に、CSV で homeDrive 属性が指定されない場合のデフォルトのドライブ名です。
- ユーザーのデフォルトのホームディレクトリ
  - ユーザー登録時に、CSV で homeDirectory 属性が指定されない場合のデフォルトのホームドライブのパスです。パスに「%USERNAME%」を含めると、登録時にユーザー名に置換されて、登録されます。

- ユーザーのデフォルトのプロファイルパス
  - ユーザー登録時に、CSV で profilePath 属性が指定されない場合のデフォルトのプロファイルのパス名です。パスに「%USERNAME%」が含まれると、登録時にユーザー名に置換されて、登録されます。
- ユーザーのデフォルトのログオンパス
  - ユーザー登録時に、CSV で scriptPath 属性が指定されない場合のデフォルトのプロファイルのパス名です。

ホームディレクトリ関連設定

- Active Directory のユーザー登録時にホームディレクトリを作成する
  - 有効に設定すると、ユーザー登録時に Active Directory サーバー上の内蔵ディスクにホームディレクトリを作成します。
- Active Directory のホームディレクトリ作成時のコマンド
  - ホームディレクトリ作成のために実行するバッチコマンドを指定します。通常は変更の必要はありません。
- Active Directory のユーザー削除時にホームディレクトリを削除する
  - 有効に設定すると、ユーザー削除時に Active Directory サーバー上のホームディレクトリを削除します。
- Active Directory のホームディレクトリ削除時のコマンド
  - ホームディレクトリ削除のために実行するバッチコマンドを指定します。通常は変更の必要はありません。
- Winexe コマンドのパス
  - ホームディレクトリの作成・削除のために利用する winexe コマンドのパスです。通常は変更の必要はありません。

ユーザーエントリのオブジェクトクラス(Active Directory)

Active Directory のユーザー登録時のオブジェクトクラスを指定します。

通常は、次の 4 つを指定してください。

- top
- person
- user
- organizationalPerson

4 バックエンド(Google Apps)の設定

Google Apps の管理を行う場合、「バックエンド(Google Apps)」を選択します。

画面右上の「バックエンド(Google Apps)を追加」をクリックします。

各項目の意味を説明します。

基本設定

- Org
  - この Google Apps を、どの「対象組織」の管理下に置くか選択します。
- サーバーの識別子
  - この Google Apps を特定できる名称を指定します。Unicorn ID Manager の表示等で利用されます。
- プライオリティ
  - 対象組織内で、この Google Apps に対して何番目に処理を行うか１以上の数値で指定しま

す。

- バックグラウンドでの CSV 一括処理
  - CSV ファイルを一括処理する際に、Google Apps に対してバックグラウンドで処理を行う場合は、この設定を有効にします。
  - Google Apps への操作は時間がかかるため、この設定は有効にしてください。
  - この設定が無効な場合は、Google Apps への一括処理が完了してから、ブラウザに応答が返ります。
- Google Apps のドメイン名
  - Google Apps のドメイン名を指定します。
- Google Apps の管理者ユーザー名
  - Google Apps に接続するための管理者ユーザー名を指定します。
- Google Apps の管理者のパスワード
  - Google Apps に接続するための管理者ユーザーのパスワードを指定します。

同期設定

- ユーザーのパスワード変更時にこのサーバーのパスワードを同期する
  - パスワード変更画面からパスワードを変更したときに、この Google Apps のパスワードを変更します。
- ユーザーのアカウント操作時に、このサーバーのアカウントを同期する
  - 管理者が CSV やアカウントの操作を行なった時に、この Google Apps のユーザーエントリを更新します。

ユーザーエントリのオブジェクトクラス(Google Apps)

Google Apps 用のオブジェクトクラスとして、「basic」のみを選択してください。

. インストールガイド更新履歴

1 2010/12/18 Unicorn ID Manager インストールガイド V1.0

- 初版

2 2011/01/19 Unicorn ID Manager インストールガイド V2.0

- 初期設定方法の追加