ShapeLDAP

ShapeLDAP は、オープンなディレクトリサーバ 389-ds を中心に、ユーザエントリ管理を容易にする WEB アプリケーションです。

389-ds の機能により Windows Active Directory と LDAP のエントリ同期をサポートします。パスワードは双方向で同期可能です。

主要機能

389-ds に基づく機能

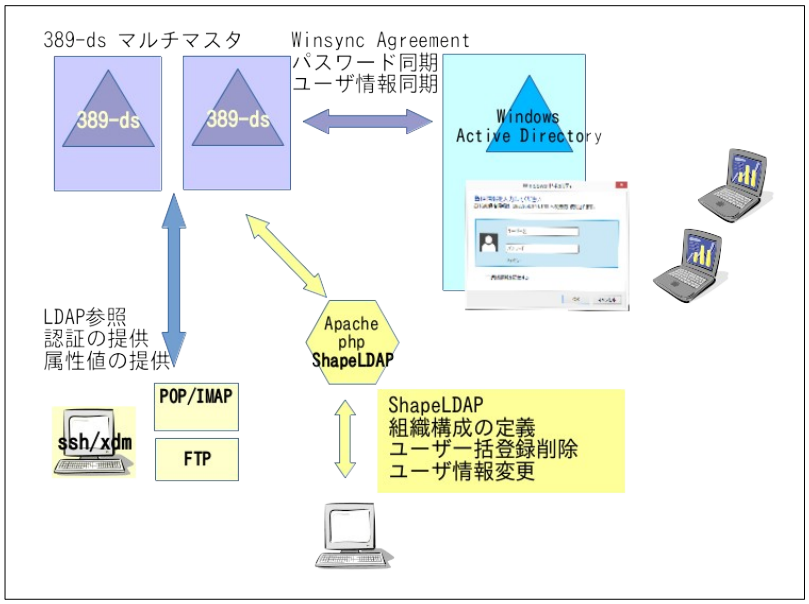
- LDAP に基づいた認証情報の他システムへの提供
- Replication 機能に基づいた、Windows ドメインへのユーザ追加、削除機能（複数ドメインを設定可能）
- passsync 機能に基づいた、Windows パスワード変更の LDAP 同期機能
- 4 台までのマルチマスタによる冗長化

ShapeLDAP が提供する機能

- LDAP 認証に基づいたログイン機能
- ユーザ自身のパスワード変更機能
- 管理ユーザのパスワード初期化機能
- 条件指定によるユーザ検索機能
- 検索ユーザに対する一括属性変更（パスワード初期化）
- 検索ユーザに対する個別属性修正
- 検索ユーザの一括削除
- 新規ユーザの登録
- CSV ファイル指定によるユーザー括登録
- CSV ファイル指定によるユーザー括削除
- 検索結果の CSV ファイルダウンロード
- ユーザ登録時、削除時の外部コマンド実行

389-ds は、Netscape Directory Server を起源とする、オープンソースのディレクトリサーバで、RedHat Inc. が標準ディレクトリサーバとして提供しているものです。
389-ds には、ディレクトリレプリケーションを基盤とした Windows Active Directory の同期機能を標準搭載し、同時に提供される Windows パスワード同期モジュールにより、Windows のパスワード変更をオンデマンドに LDAP に同期することが可能です。

ShapeLDAP は、389-ds によって提供される認証基盤に対し、LDAP ツリーのエントリ管理操作を容易にする機能を提供します。十分な設計によって構築された LDAP エントリの運用において、最も煩雑になるのはユーザエントリの更新作業です。運用サイト毎にはそれぞれエントリが持つ属性やエントリの配置に個別のポリシーがあります。LDAP エントリの更新作業を汎用的に行うユーザインタフェースは数多くありますが、運用サイト毎の個別エントリに対するポリシーは扱えないため操作を必ずしも的確に行うことができません。そのために一括処理ができないなど使いにくく、間違いも起こしやすくなります。



ShapeLDAP は、LDAP ツリー設計時に必ず必要となるエントリのポリシーを LDAP 上のテンプレートに定義することにより、通常のエントリ操作を csv ファイルから一括で登録/削除を行うことが可能です。これらの登録情報は、389-ds の機能によって Windows Active Directory にも伝達され、すべてのユーザエントリ管理を ShapeLDAP のみで行うことができます。
登録された LDAP ユーザーが LDAP に対してパスワードを更新すると、389-ds の標準機能により、非常に短い時間で Windows Active Directory に同期されます。Windows ユーザが Windows ネイティブの環境において Active Directory のパスワードを更新した場合は、Windows にインストールされるパスワード同期モジュールによって、LDAP に同期されます。

LDAP から認証情報の提供を受けるシステムは、必ずしも LDAP に対する認証情報の更新を提供するとは限りません。特にメールボックス認証(pop/imap)やファイル転送認証(ftp)に認証情報を利用するものは、パスワード変更の方法が提供されません。このようなシステムのユーザに対しては、ShapeLDAP がパスワード変更画面を提供します。すべてのユーザは簡便な WEB インタフェースにより LDAP の情報を更新すればよく、個別のパスワード変更システムを利用する必要はありません。

動作環境

389-ds 動作環境

- Red Hat Enterprise Linux 7/8
- CentOS 7/8

（RHEL7 の場合は管理用に JRE が必要）

ShapeLDAP の動作環境

- Red Hat Enterprise Linux 7/8
- CentOS 7/8 以上
- その他: Apache2.x 及び PHP5.5 以上を構成でき得るオペレーティングシステム環境（Symfony2 フレームワークが必要）

ShapeLDAP では、ユーザエントリ毎にアクセス権限情報を持ちます。管理権限を持つユーザはユーザの検索登録削除が可能です。利用権限しか持たないユーザは自身の情報を更新する以外の操作はできません。また、パスワードの初期化権限などは別途個別に与えることができますので、ヘルプデスク権限として利用するなどが可能です。
管理権限とパスワード初期化以外の権限は任意に設計することができます。例えば
「pop/imap は利用できるが ftp できないユーザ」などを設定することも可能です。
（schema の追加は任意に可能です）

ユーザの登録は csv ファイルによって行うことができます。ユーザ情報に関して多くの組織では管理部門が基礎データを持つ場合が多くあります。そのため、メールシステム等のエントリ登録は、管理部門から情報を得て別途登録となる場合も少なくありません。このような場合にも、データ交換を行いやすい csv ファイル形式で一括登録することができ、登録の手間を低減することができます。LDAP から検索したユーザの情報も同じ形式の csv ファイルとして取得することができ、更に、この csv ファイルに従い一括でユーザを削除することもできます。

Sunbit System

開発：有限会社サンビットシステム
〒062-0932 札幌市豊平区平岸２条７丁目 4-20 アークパレス平岸 203 号
URL: http://www.3bit.co.jp/　　E-Mail: info@3bit.co.jp