

OpenLDAP 機能拡張

パスワードポリシー機能とバインド処理に対する Sun Java System Directory Server 5 互換機能の実装(案)



オープンソース・ソリューション・テクノロジー(株)

文書番号: FIXME
更新日: 2011 年 9 月 15 日
作成日: 2011 年 9 月 14 日
リビジョン: 1.1

目次

1. 概要	1
2. OpenLDAP パスワードポリシー機能の改修	2
2.1 応答コントロールの改修.....	2
2.2 応答コードの改修.....	3
2.3 設定方式.....	3
2.4 制限事項.....	3
2.4.1 オブジェクトクラスと属性の違い.....	3
2.4.2 パスワード有効/失敗数カウント期間とアカウントロック期間の算出方法の違い.....	3
3. OpenLDAP のバインド処理の改修	4
3.1 応答コードの改修.....	4
3.2 設定方式.....	4
4. 改版履歴	5

1. 概要

Sun Java System Directory Server (以下「Sun JSDS」と略記) と OpenLDAP にはいくつかの仕様や振舞いの差が存在する。

Sun JSDS バージョン 5 には Netscape Directory Server 由来の独自のパスワードポリシー機能が実装されている。一方、OpenLDAP や最新の Sun JSDS 6 はこれとは異なる仕様の実装となっている。それぞれの仕様書は以下の URL にある。

- Sun JSDS 5 が実装するパスワードポリシーの仕様書
 - <http://tools.ietf.org/html/draft-vchu-ldap-pwd-policy-00>
- OpenLDAP が実装するパスワードポリシーの仕様書
 - <http://tools.ietf.org/html/draft-behera-ldap-password-policy-10>

また、クライアントからのバインド要求時に示されたユーザーエントリーが LDAP DIT に存在しなかった場合の LDAP 応答コードが Sun JSDS と OpenLDAP で異っている。

本書では、Sun JSDS 5 のパスワードポリシーを利用しているサイトを容易に OpenLDAP に移行するための、OpenLDAP のパスワードポリシー機能とバインド処理の改修仕様(案)について述べる。

2. OpenLDAP パスワードポリシー機能の改修

2.1 応答コントロールの改修

下記の場合の LDAP 応答に Sun JSDS 5 のパスワードポリシー機能が用いる LDAP コントロール情報を含める。

- パスワード有効期限の警告時の応答とコントロール:
 - 応答コード: LDAP_SUCCESS
 - コントロール: 2.16.840.1.113730.3.4.5 (password expiring control)
 - 値: パスワードが期限切れになるまでの秒数
- パスワード有効期限切れ時の応答とコントロール:
 - 応答コード: LDAP_INVALID_CREDENTIALS
 - コントロール: 2.16.840.1.113730.3.4.4 (password expired control)
 - 値: 0
 - 備考: IETF にある仕様書には、パスワード期限切れの場合にコントロールを付加する旨の記述はされていない。
- パスワードリセット強制時の応答とコントロール:
 - 応答コード: LDAP_SUCCESS
 - コントロール: 2.16.840.1.113730.3.4.4 (password expired control)
 - 値: 0
- パスワードリセット強制時にパスワード変更意外の要求に対する応答とコントロール:
 - 応答コード: LDAP_UNWILLING_TO_PERFORM
 - コントロール: 2.16.840.1.113730.3.4.4 (password expired control)
 - 値: 0

2.2 応答コードの改修

- アカウントロック時の応答コードを 19 (Constraint violation) にする。

※ OpenLDAP 標準は 49 (Invalid Credentials)

2.3 設定方式

以上の機能を OpenLDAP サーバー (slapd) 起動時の環境変数により有効化・無効化できるようにする。

2.4 制限事項

2.4.1 オブジェクトクラスと属性の違い

Sun JSDS 5 のパスワードポリシー専用のオブジェクトクラス (passwordPolicy) と属性 (passwordMaxAge など) は提供しない。これらを参照している LDAP クライアントアプリケーションは、OpenLDAP のオブジェクトクラス (pwdPolicy) と属性 (pwdMaxAge など) を使用するよう改修する必要がある。

FIXME

passwordExpirationTime

retryCountResetTime

accountUnlockTime

属性情報を仮想的に返す。制限事項: この属性をフィルターにしての検索はできない。

2.4.2 パスワード有効/失敗数カウント期間とアカウントロック期間の算出方法の違い

FIXME: パスワード期限の算出方法の違い

passwordExpirationTime

retryCountResetTime

accountUnlockTime

3. OpenLDAP のバインド処理の改修

3.1 応答コードの改修

- クライアントからのバインド要求の処理時、バインドユーザーのエントリーが存在しなかった場合の LDAP 応答を Sun JSDS 5 と互換の応答コード 32 (No such object) にする。

※ OpenLDAP 標準は応答コード 49 (Invalid Credentials)

3.2 設定方式

以上の機能を OpenLDAP サーバー (slapd) 起動時の環境変数により有効化・無効化できるようにする。

4. 改版履歴

- 2011 年 9 月 15 日 佐藤文優
 - FIXME
- 2011 年 9 月 14 日 佐藤文優
 - 初版。