認証DBとしてのOpenLDAPの利用

はじめに

OpenLDAPはHP IceWall SSOの動作環境であるRHELにバンドルされ、ソフトウェアサポート対象製品にも含まれるディレクトリサービスです。HP IceWall SSOにもOpenLDAP版が用意されており、簡単に使用を開始できます。

本稿では、OpenLDAPをHP IceWall SSOの認証DBとして使用するときの留意事項や参考性能についてご紹介します。

冗長化構成

HP IceWall SSOにはOpenLDAPの障害を検知して、自動的にフェイルオーバーする機能があります。このため、ロードバランサーを用いずとも、冗長化構成のOpenLDAPに対応することが可能(※1)です。

HP IceWall SSOの主要ユースケースであるログイン、ログアウト、パスワード変更では、OpenLDAPへの書き込み処理を伴います。このため、OpenLDAPの冗長化にマスターレプリカ構成を選択することはできません。

OpenLDAPの冗長化構成において、障害時の書き込み処理を許可するのは、N-Way Multi-Master構成、MirrorMode構成のいずれかになります。特別な要件がない限りは、よりシンプルなMirrorMode構成を選択(※2)します。

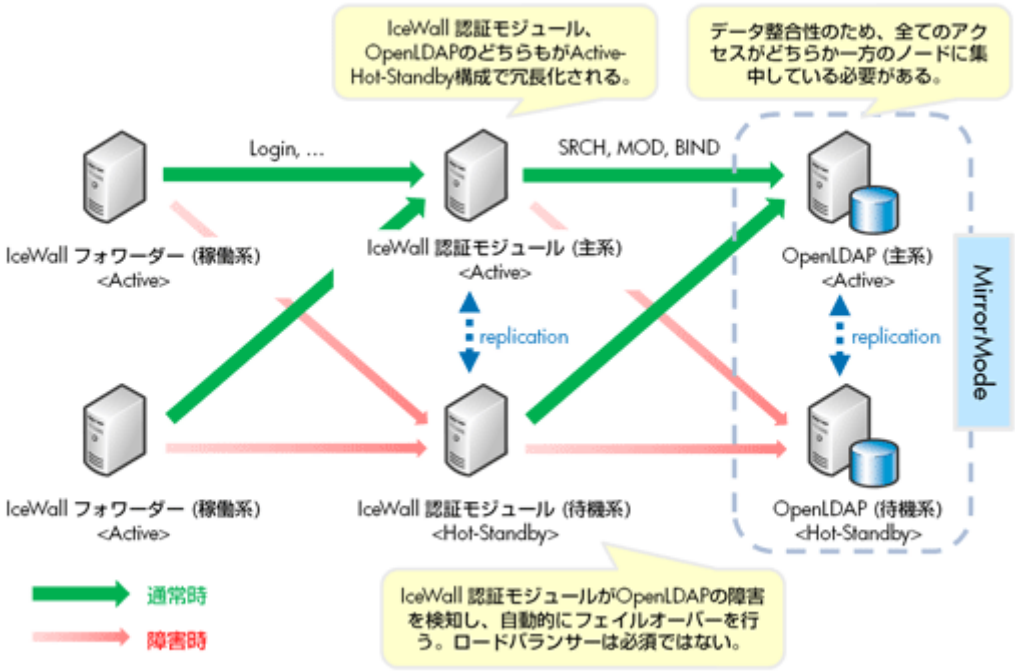

図1. 冗長化構成イメージ

※1. 必要に応じて、ロードバランサーを使用した構成やクラスター構成をご利用して頂くこともできます。
※2. 特殊な構成や状況下では、IceWall認証モジュールからの書き込み処理がMirrorModeを構成する2ノードに分散し、書き込みの衝突が発生する可能性はゼロではありません。データが不整合となると、アカウントロック、パスワード有効期限、最終ログイン日付などの処理が一時的に正しく機能しないことも考えられます。リスクを評価し、必要に応じて、ロードバランサーを使用した構成など、分散を防ぐことのできる他の冗長化方式をご検討ください。

障害時動作

HP IceWall SSOの起動時には主系とするOpenLDAPに対してコネクションプール生成が行われます。主系の障害を検知すると、まずリトライを試み、それでも障害状態が継続していれば、コネクションを待機系へと順次切り替えていきます。ログイン時における流れは以下の通りです。

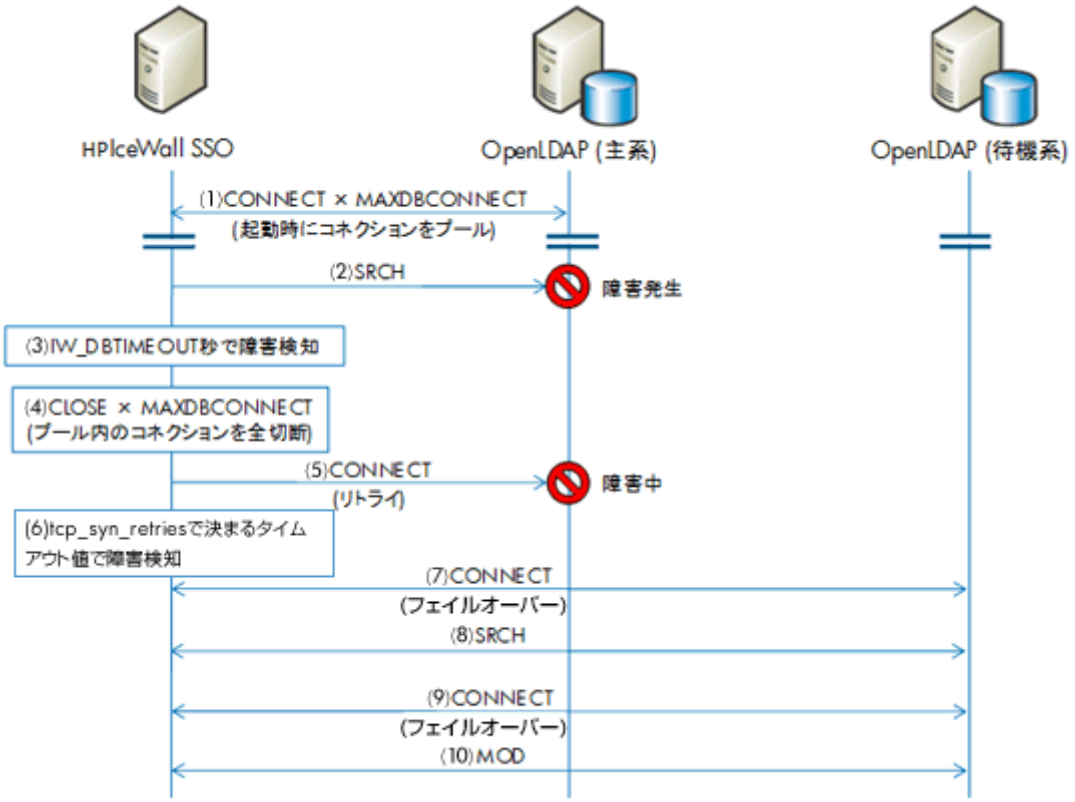

図2. ログイン処理におけるフェイルオーバーの流れ
(HP IceWall SSO 10.0 certdlib patch 7適用環境の例)

タイムアウト

OpenLDAPの障害が検知され、フェイルオーバーが行われるまでの時間は、IceWall SSOのIW_DBTIMEOUTパラメータ値とOSのtcp_syn_retriesで決まるタイムアウト値の合計(※3)となります。

障害時にもユーザーにエラー画面を表示せず、シームレスに処理を継続させるためには、検知時間をWEBサーバーのタイムアウト(※4)よりも短くします。

tcp_syn_retriesで決まるタイムアウト値はデフォルトで189秒(※5)に設定されています。tcp_syn_retriesを変更する場合、HP IceWall SSO以外のアプリケーションにも影響がありますのでご注意ください。

但し、RHEL環境においては、HP IceWall SSOの認証モジュールとOpenLDAPが同一のネットワークセグメントで動作している場合、ローカルループバックからのICMP(Destination Unreachable)応答により、約3秒でタイムアウト(※6)が行われるようです。例えば、フェイルオーバーが行われるまでの時間を「約43秒」とするには、HP IceWall SSOの認証モジュール起動スクリプト(start-cert)に以下のような設定を行うことで実現できます。

```
export IW_DBTIMEOUT=40
```

ログメッセージ

フェイルオーバー時には以下のようなログメッセージが出力(※7)されます。

```
Fatal: DBErrNo[-5] DBErrMsg[Timed out] <省略> TID=*** [EP11001-50006] (3)
Fatal: ldap_search_s() Error. [Timed out] TID=*** [EP10802-50055] (3)
Warning: DB connection closed. TID=*** [EP71342-50098] (4)
Warning: DB connection closed. id=[***] TID=*** [EP71343-50099] (4)
Warning: DB connection closed. id=[***] TID=*** [EP71343-50099] (4)
Fatal: LDAP Server Down. Host=[192.168.0.1:389] TID=*** [EP10602-50031] (5)(6)
Fatal: DBErrNo[-1] DBErrMsg[Can't contact LDAP server] <省略> TID=*** [EP10603-50006] (5)(6)
Warning: Database Reconnect succeeded. TID=*** [EP13403-50021] (7)
Warning: Database Reconnected. Host=[192.168.0.2:389] TID=*** [EP13405-50074] (7)
Fatal: IW_DBSelect() Error. Retry Select. TID=*** [EP10801-50056] (8)
```

```
Warning: Database Reconnect succeeded. TID=*** [EP13403-50021] (9)
Warning: Database Reconnected. Host=[192.168.0.2:389] TID=*** [EP13405-50074] (9)
```

※3. OpenLDAPの動作するサーバ自体がダウンしていた場合、もしくはIceWall SSOからOpenLDAPの動作するサーバまでのネットワーク経路がダウンしていた場合です。OpenLDAPプロセスだけがダウンしていた場合には即時に障害が検知されます。また、IceWall SSOにパッチ(certdlib patch 7)が未適用の場合、IW_DBTIMEOUTパラメータの代わりにOSのtcp_retries2で決まるタイムアウト値が使用されます。
※4. Apacheの場合、Timeoutディレクティブ(デフォルト60秒)で指定されます。
※5. tcp_syn_retriesで決まるタイムアウト値がデフォルトで21秒となるバグを含むカーネルバージョンがありますのでご注意ください。
※6. このように、タイムアウトまでの時間は個別の環境に左右されるため、実際の環境に合わせてご調整ください。
※7. メッセージフォーマットは実際と異なる部分があります。メッセージの右側の( )内番号は図2に示される( )内番号に対応しています。

認証方式

ユーザーの認証方式には、入力されたユーザーIDとパスワードをHP IceWall SSOが照合する方式(BIND認証なし)と、ユーザーIDとパスワードでOpenLDAPにbindすることで照合を行う方式(BIND認証あり)とが存在します。

「BIND認証あり」の場合、まず、入力されたユーザーIDをフィルターとして検索することでdn(識別名)を取得します。その後、取得したdnでbindを実施しますので、「BIND認証なし」の場合に比べると、オーバーヘッドが発生します。

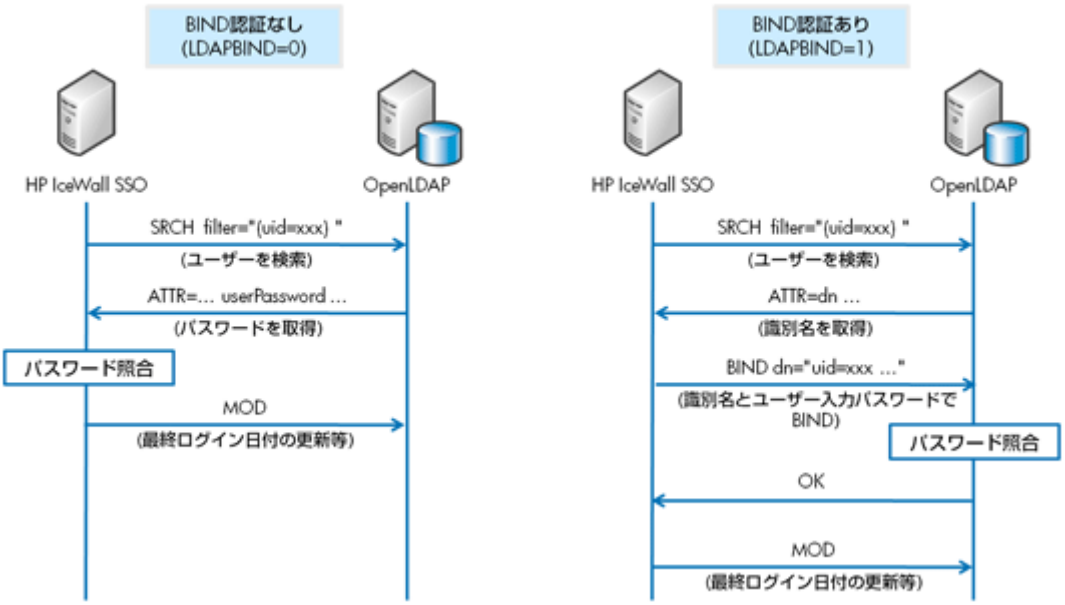

図3. BIND認証あり、BIND認証なしのシーケンス比較

パスワードは一般的にハッシュされた状態で保存されています。ハッシュアルゴリズムには、照合を行う主体がサポートするものだけを使用することが可能です。

BIND認証	ユーザーID・パスワードの照合主体	使用可能なハッシュアルゴリズム
なし	HP IceWall SSO	SHA, MD5, SHA256
あり(※8)	OpenLDAP	SHA, MD5, SSHA, SMD5, CRYPT(※9)

表1. 使用可能なハッシュアルゴリズム

通常は、よりオーバーヘッドの小さな「BIND認証なし」を認証方式として選択、よりセキュアな「SHA256」をハッシュアルゴリズムとして選択(※10)します。認証モジュール設定ファイル(cert.conf)の設定例は以下の通りです。

```
LDAPBIND=0
PWDLOGINHASH=SHA256
PWDCHGHASH=SHA256
```

パスワードポリシー

HP IceWall SSOはパスワードの有効期限、長さ、複雑さ、履歴、アカウントロックなど、きめ細かなパスワードポリシーを製品の標準機能で実現します。

インデックス、一意性

HP IceWall SSOはuid属性(※11)をフィルターとして使用するため、インデックスを作成(※12)します。使用される比較条件はEQUALITY(一致)のみです。OpenLDAP設定ファイル(slapd.conf)の設定例は以下の通りです。

```
index     uid     eq
```

uid属性値はHP IceWall SSOの検索開始位置となるツリー以下で必ず一意でなければなりません。ユーザー追加時に一意性を担保してください。OpenLDAPのAttribute Uniqueness (uniqueness) Overlayを用いることも可能です。

※8. 「BIND認証あり」の場合、認証DBカラム情報ファイル(dbattr.conf)におけるPASSWORD項目のマッピングにかかわらず、パスワードの照合にはuserPassword属性値が固定的に用いられます。
※9. ハッシュアルゴリズムにSSHA、SMD5、CRYPTを選択した場合、利用可能なパスワードポリシーが一部制限されます。
※10. OpenLDAPクライアントツールのldappasswdではSSHAがデフォルトのハッシュアルゴリズムになっていますので、同ツール、もしくは同等製品をご利用の場合にはご注意ください。また、SSHAを利用するにはLDAPBIND=1とする必要があります。
※11. 認証DBカラム情報ファイルでUID項目にマッピングされた属性です。OpenLDAP版の初期設定ではuid属性となっていますが、任意の属性をマッピングすることもできます。
※12. HP IceWall Identity Managerなど、他にOpenLDAPにアクセスする製品がある場合には、別途、必要なインデックスを作成します。

参考性能

MirrorMode構成のOpenLDAPを認証DBとした状態で、4スレッド、5,000ループによる2万件のログイン処理を実行し、参考性能を測定した結果は以下の通りです。

BIND認証	ログイン性能	HP IceWall SSO (Xeon 3.16GHz 2P8C)	OpenLDAP (Xeon 2.00GHz 1P1C)	
		CPU使用率	CPU使用率	IOWAIT
なし	800 ログイン/秒	30%	60%	20%
あり	560 ログイン/秒	30%	80%	7%

表2. ログイン処理の参考性能

- 計測にはRHEL6.0上で動作させたHP IceWall SSO 10.0を使用しており、ログイン性能は参考値となります。
- IceWall 認証モジュールのアクセスログ、エラーログは共に「警告レベル以上」のメッセージを出力、リクエストスレッド数は「10」、認証DB接続数は「2」と設定しています。
- OpenLDAPのログレベルは「256」、バックエンドは「BDB(Berkeley DB)」、DB_CONFIGはデフォルト、インデックスは「uid属性」にのみ作成しています。
- ユーザーID・パスワードによるログイン方式です。パスワードのハッシュアルゴリズムは、BIND認証なし、BIND認証ありに共通で使用可能な「SHA」を選択しています。
- ログイン件数はiwpmc、CPU使用率はtop、IOWAITはiostatコマンドで計測しています。
- BIND認証なしではOpenLDAPのIOWAIT、BIND認証ありではOpenLDAPのCPU使用率がボトルネックに到達しています。

おわりに

ここで述べた内容な技術的観点に基づいて検証した結果を示したもので特定の環境での動作や性能を保証するものではありません。実際の構築に関しては、HPまたはIceWall販売パートナーへご相談ください。

ご参考URL

≫RHEL 6 ソフトウェアサポート対象製品リスト

≫Red Hat Bugzilla – Bug 688989

≫OpenLDAP 2.4 Admin Guide (Password Policy Overlay)

≫OpenLDAP 2.4 Admin Guide (Attribute Uniqueness Overlay)

2011.7.28 日本ヒューレット・パッカード テクノロジーサービス統括本部　テクニカルコンサルタント　有坂 剛志
2011.12.15 「障害時動作」の項を加筆
2012.7.3 「障害時動作」、および「参考URL」の項を加筆