

PassLogic Enterprise Edition

Ver.2.4.0

レプリケーション セットアップ & リカバリガイド



本書について

本書は、PassLogic 認証サーバソフトウェア レプリケーション構成環境 セットアップ&リカバリ ガイドです。

表示画面

表示画面などは、操作の一例として掲載しているため、実際に表示される画面とは異なる場合があります。

商標および免責事項

PassLogic およびパスロジは、パスロジ株式会社の登録商標です。

その他、本書に記載されている会社名、製品名は、それぞれ各社の商標または登録商標です。

本製品は医療機器、原子力施設、航空関連機器、軍備機器、輸送設備やその他人命に直接関わる施設や設備など、高い安全性が要求される用途での使用は意図されていません。該当する施設や設備には使用しないでください。

著作権/注意

本書の内容の一部または全部を無断で複製転載することを禁じます。

本書に掲載の内容及び製品の仕様などは、予告なく変更されることがあります。

本書の内容は万全を期して作成しておりますが、万一ご不明な点や誤り、記載漏れ、乱丁、落丁などお気づきの点がございましたら、弊社までご連絡ください。

目次

目次.....	2
1 レプリケーションの概要.....	4
1.1 正常稼働.....	5
1.2 pgsql 障害発生.....	6
2 監視対象.....	7
2.1 監視対象ポート.....	7
2.2 監視対象ログ.....	8
3 ゲートウェイサーバ×2 + 認証サーバ×2 Active/Active 構成.....	9
3.1 セットアップ手順.....	9
①【認証サーバ】PassLogic 認証ソフトウェア インストール.....	9
②【認証サーバ】データベース レプリケーション設定.....	9
③【認証サーバ】データベース レプリケーション状況確認.....	10
④【認証サーバ】ライセンス登録.....	10
⑤【ゲートウェイサーバ】PassLogic ゲートウェイサーバ セットアップ.....	10
⑥PassLogic ユーザインターフェース アクセス確認.....	11
3.2 ゲートウェイサーバ リカバリ手順.....	11
3.3 認証サーバ 0 リカバリ手順.....	11
①【認証サーバ 0】OS シャットダウン.....	12
②【認証サーバ 1】認証サーバ 0 への接続停止状態の確認とバックアップ取得.....	12
③【認証サーバ 0】サーバ再構築.....	12
④【認証サーバ 1】データベース レプリケーション設定.....	12
⑤【認証サーバ 1】認証サーバ 0 リカバリ.....	12
⑥【認証サーバ 0】稼働状況の確認.....	12
3.4 認証サーバ 1 リカバリ手順.....	13
①【認証サーバ 1】OS シャットダウン.....	13
②【認証サーバ 0】認証サーバ 1 への接続停止状態の確認とバックアップ取得.....	13
③【認証サーバ 1】サーバ再構築.....	13
④【認証サーバ 0】データベース レプリケーション設定.....	13
⑤【認証サーバ 0】認証サーバ 1 リカバリ.....	13
⑥【認証サーバ 1】稼働状況の確認.....	14
4 その他.....	15
4.1 pgpool フェイルオーバー時のメール配信.....	15
4.2 pgpool フェイルバック時のメール配信.....	15
4.3 データベース(pgsql)管理情報.....	15
4.4 PassLogic 認証サーバ 停止・起動手順.....	16
PassLogic 認証サーバ OS 停止手順.....	16

PassLogic 認証サーバ OS 起動手順	16
4.5 PassLogic 認証サーバ ソフトウェア アップデート	17
PassLogic 認証サーバ アップデート手順	17
4.6 PassLogic 認証サーバに http でアクセスできるようにする	17
4.7 認証サーバとゲートウェイサーバに http でアクセスできるようにする	18

1 レプリケーションの概要

Active/Active 構成により PassLogic サーバを 2 重化した場合、PassLogic 認証サーバ内のデータベースはレプリケーション構成となります。

レプリケーションを構成する PassLogic 認証サーバ間のネットワーク品質は、PassLogic 利用者への応答時間と pgpool 障害検知性能に影響します。レプリケーション環境を構築する場合は、これらを考慮してネットワーク構成をご検討ください。

通信遅延やパケットロスなどが見込まれるネットワークでのレプリケーション構成は推奨できません。

【参考情報】 PassLogic 認証サーバ間 ping 応答時間別 レスポンス

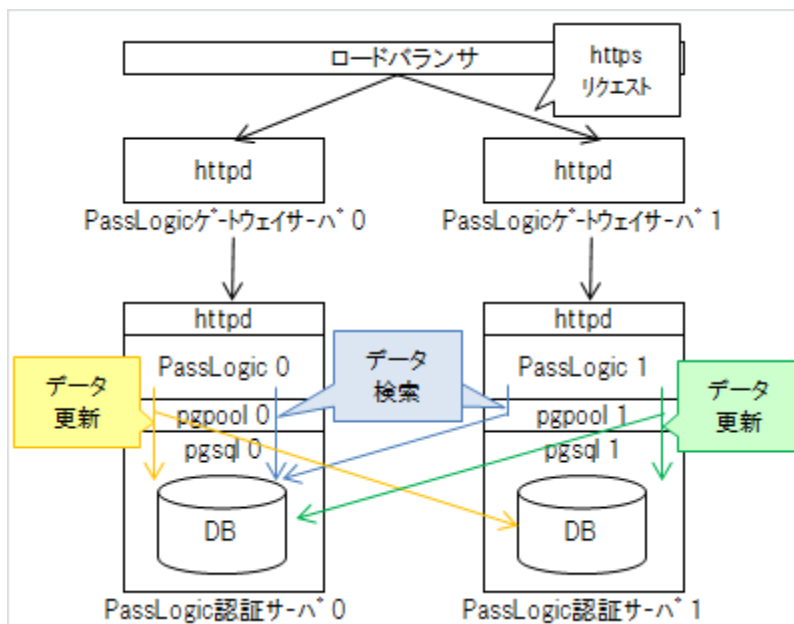
	ネットワーク品質	応答時間		
	ping 応答時間	uid 入力画面	乱数表画面	認証処理
レプリケーション① (同拠点内)	0.6 ms	86 ms	113 ms	130 ms
レプリケーション② (国内別拠点)	10.0 ms	277 ms	752 ms	1,023 ms
レプリケーション③ (国外別拠点)	72.0 ms	2,172 ms	3,320 ms	5,274 ms

* レプリケーション②と③は 拠点間に公衆インターネット回線を利用した場合の計測結果です

1.1 正常稼働

pgsql(PostgreSQL データベース)はpgpool(pgsql 専用コネクションプーリング・プロキシサーバ)により常に同期が取られ、データの変更は双方の DB に同時に書き込まれます。

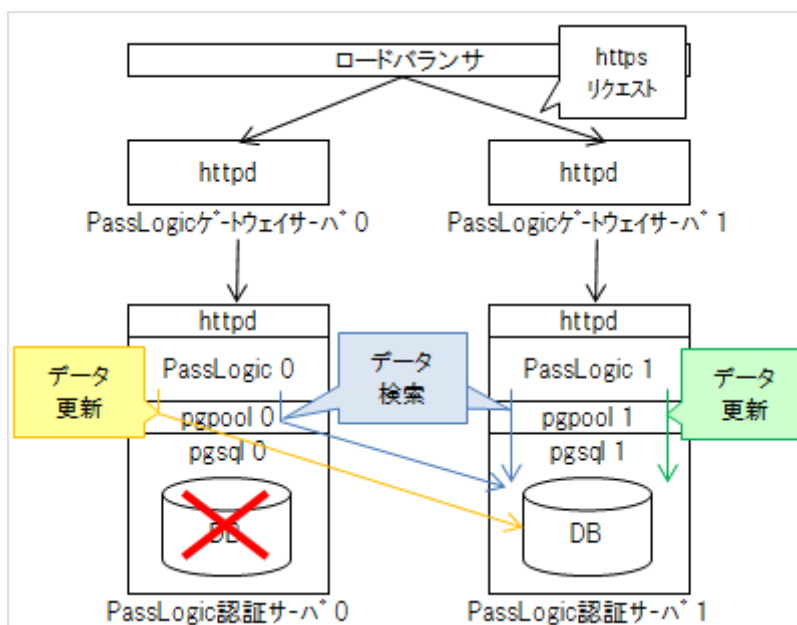
データ検索処理はいずれの pgpool も pgsql0 を参照します。



PassLogic Enterprise Edition ver.2.3.0 から ロードバランサー 振分仕様に「スティッキーセッション」以外を利用することができるようになりました。

1.2 postgresql 障害発生

postgresqlに障害が発生しpgpoolが接続できない場合は、データの変更の書き込みとデータ参照は片方のDBだけに行われます。



*PassLogic から pgpool に対してデータベース処理要求が発生したとき、pgpool から postgresql に接続できないことが判明した時点で対象の postgresql を即時切り離します。切り離したことは、後述の アラートメール および pgpool ログファイル で把握することができます。

*postgresql 以外のトラブル「pgpool 障害」「httpd 障害」「AD 接続障害」などは、PassLogic ユーザログイン画面への http(s)接続応答結果で確認することができます。

2 監視対象

2.1 監視対象ポート

PassLogic ゲートウェイサーバ

ユーザインターフェース	443	tcp	https
-------------	-----	-----	-------

PassLogic 認証サーバ

ユーザインターフェース	443	tcp	https
管理ツール	8443	tcp	https
RADIUS	1812	udp	radius
データベースレプリケーション	5439	tcp	postgresql
	9915	tcp	pgpool
	9925	tcp	pgpool

*RADIUS 監視は RADIUS 認証を利用する場合のみ監視をしてください。

*iptables などファイアウォールを動作させている場合には、必要に応じて PassLogic が利用するポートにアクセスできるように設定してください。

2.2 監視対象ログ

PassLogic 認証サーバ

PassLogic ログ
/var/log/passlogic/passlogic.log

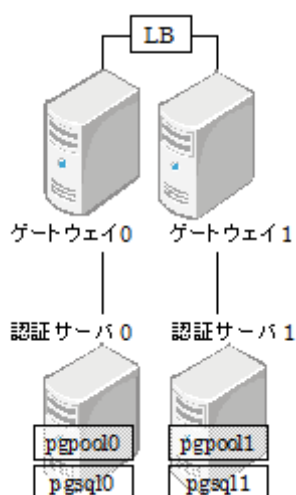
*出力ログ定義は インストール・運用管理ガイド「ログ・リファレンス」をご覧ください。

pgpool ログ
/var/log/passlogic-pgpool/pgpool**.log
pgsql に接続できなかったときのサンプルログ <pre> 2014-11-04 15:32:56 LOG: pid 1860: connection closed. retry to create new connection pool. 2014-11-04 15:32:56 ERROR: pid 1860: connect_inet_domain_socket: getsockopt() detected error: Connection refused 2014-11-04 15:32:56 ERROR: pid 1860: connection to 172.31.19.43(5439) failed 2014-11-04 15:32:56 ERROR: pid 1860: new_connection: create_cp() failed 2014-11-04 15:32:56 LOG: pid 1860: degenerate_backend_set: 0 fail over request from pid 1860 2014-11-04 15:32:56 LOG: pid 1828: starting degeneration. shutdown host 172.31.19.43(5439) 2014-11-04 15:32:56 LOG: pid 1828: Restart all children 2014-11-04 15:32:56 LOG: pid 1828: execute command: /opt/passlogic/pgsql/data/failover_mail.sh 172.31.19.43 172.31.23.59 2014-11-04 15:32:57 LOG: pid 1828: failover: set new primary node: -1 2014-11-04 15:32:57 LOG: pid 1828: failover: set new master node: 1 2014-11-04 15:32:57 LOG: pid 1863: worker process received restart request 2014-11-04 15:32:57 LOG: pid 1828: failover done. shutdown host 172.31.19.43(5439) 2014-11-04 15:32:58 LOG: pid 1862: pcp child process received restart request 2014-11-04 15:32:58 LOG: pid 1828: PCP child 1862 exits with status 256 in failover() 2014-11-04 15:32:58 LOG: pid 1828: fork a new PCP child pid 2003 in failover() 2014-11-04 15:32:58 LOG: pid 1828: worker child 1863 exits with status 256 2014-11-04 15:32:58 LOG: pid 1828: fork a new worker child pid 2004 </pre>

*赤字のログは後述のアラートメールを送信したことを表します。

3 ゲートウェイ × 2 + 認証サーバ × 2 Active/Active 構成

構成例



全てのサーバOSは

- ・ Red Hat Enterprise Linux 6.1 以降 x86_64
- ・ CentOS 6.1 以降 x86_64
- ・ Red Hat Enterprise Linux 7.1 以降
- ・ CentOS 7.1 以降

のいずれかを準備し、すべてのサーバは同じ OS で統一して下さい。

3.1 セットアップ手順

① 【認証サーバ】 PassLogic 認証ソフトウェア インストール

認証サーバ 0 と認証サーバ 1 に PassLogic 認証サーバソフトウェアをインストールしてください。

インストール手順は、インストール・運用管理ガイド「必要なパッケージをインストールする」「PassLogic をインストールする」を参照してください。

*データベース間の齟齬を防ぐため、レプリケーション設定完了まで PassLogic 管理ツールにアクセスしないでください。誤ってアクセスした場合はアンインストール(インストール・運用管理ガイド「アンインストール」)後に再インストールしてください。

② 【認証サーバ】 データベース レプリケーション設定

レプリケーション対象サーバ定義

認証サーバ 0 の下記のファイルを編集してください。

編集ファイル: /opt/passlogic/data/conf/redundant.conf

編集内容:

```
SERVER0={認証サーバ 0 の IP アドレス}
SERVER1={認証サーバ 1 の IP アドレス}
```

アラートメール定義

認証サーバ 0 の下記 2 ファイルの FROM と TO のメールアドレスを編集してください。

編集ファイル:

/opt/passlogic/pgsql/data/failover_mail.sh (pgsql 障害発生時のメール送信機能)

/opt/passlogic/pgsql/data/failback_mail.sh (pgsql 障害復旧時のメール送信機能)

編集例:

```
#!/bin/sh

FROM="DB_system@passlogy.com"
TO="admin@passlogy.com"
```

レプリケーション設定コマンド

認証サーバ 0 で下記のコマンドを実行してください。

```
# /opt/passlogic/apps/tools/passlogic_redundant.sh
```

③【認証サーバ】データベース レプリケーション状況確認

認証サーバ 0 と認証サーバ 1 両方の管理ツールにログインし、メイン画面(ログイン直後の画面)の DB Status 欄「DB0」と「DB1」のデータベースが稼働中(Node Running & Connect)であることを確認してください。

管理ツール URL:

<https:// {サーバ名または IP アドレス}:8443/passlogic-admin/>

*管理ツールログイン手順は インストール・運用管理ガイド「管理ツールにアクセスする」をご覧ください。
(管理アカウント「admin」の作成はいずれか一方の認証サーバだけで行ってください)

④【認証サーバ】ライセンス登録

認証サーバ 0 と認証サーバ 1 両方の管理ツールでライセンスファイルを登録してください。

*ライセンスファイル登録手順は インストール・運用管理ガイド「ライセンスを登録する」をご覧ください

⑤【ゲートウェイサーバ】PassLogic ゲートウェイサーバ セットアップ

*ゲートウェイサーバには PassLogic インストーラ(install.sh)で PassLogic 認証サーバソフトウェアをインストールしないでください。

rpm インストール

ゲートウェイサーバ 0 とゲートウェイサーバ 1 で下記のコマンドを実行して PassLogic ゲートウェイサーバに必要なパッケージソフトウェアをインストールしてください。

```
(root 権限で実行)
# yum -y install ntp      (RHEL6 のみ)
# yum -y install chrony   (RHEL7 のみ)
```

```
# yum -y install httpd
# yum -y install mod_ssl
```

設定ツールコマンド実行

認証サーバ 0 から下記のファイルをゲートウェイサーバ 0 とゲートウェイサーバ 1 にコピーしてください。

コピー元:

認証サーバ 0 PassLogic インストールディレクトリ/install_gateway.sh

コピー先:

ゲートウェイサーバ 0 の任意のディレクトリ(例 /usr/local/src/install_gateway.sh)

ゲートウェイサーバ 1 の任意のディレクトリ(例 /usr/local/src/install_gateway.sh)

ゲートウェイサーバ 0 で下記のコマンドを実行してください。

```
(root 権限で実行)
# cd {設定ツールをコピーしたディレクトリ}(例 /usr/local/src)
# sh install_gateway.sh {認証サーバ 0 の IP アドレス または FQDN}
```

ゲートウェイサーバ 1 で下記のコマンドを実行してください。

```
(root 権限で実行)
# cd {設定ツールをコピーしたディレクトリ}(例 /usr/local/src)
# sh install_gateway.sh {認証サーバ 1 の IP アドレス または FQDN}
```

⑥PassLogic ユーザインターフェース アクセス確認

下記の URL にアクセスしユーザ用ログイン画面が表示されることを確認してください。

ゲートウェイサーバ 0:

<https:// {ゲートウェイサーバ 0 サーバ名または IP アドレス}/ui/>

ゲートウェイサーバ 1:

<https:// {ゲートウェイサーバ 1 サーバ名または IP アドレス}/ui/>

3.2 ゲートウェイサーバ リカバリ手順

本マニュアル「【ゲートウェイサーバ】PassLogic ゲートウェイサーバ セットアップ」を参照して、リカバリ対象のゲートウェイサーバの手順のみを実施してください。

3.3 認証サーバ 0 リカバリ手順

認証サーバ 0 に障害が発生し、認証サーバ 1 が正常稼働しているときに本手順を実施してください。

*リカバリ対象サーバ(認証サーバ 0 / 認証サーバ 1)によりリカバリ手順が異なります。

*リカバリ前後で認証サーバの役割(認証サーバ "0"と "1")は入れ替わりません。

①【認証サーバ 0】OS シャットダウン

認証サーバ 0 の OS をシャットダウンしてください。

②【認証サーバ 1】認証サーバ 0 への接続停止状態の確認とバックアップ取得

認証サーバ 1 の管理ツールにログインし、メイン画面「DB Status」欄 DB0 が「Node Down」と表示されていることを確認し、管理ツール>メンテナンス>バックアップ より、バックアップファイルを取得してください。

*障害復旧が正常に終了しなかった場合に備えてバックアップを必ず取得してください。

③【認証サーバ 0】サーバ再構築

認証サーバ 0 に PassLogic 認証サーバソフトウェアをインストールしてください。

*本マニュアル「【認証サーバ】PassLogic 認証ソフトウェア インストール」を参照してください。

*すでに PassLogic がインストールされている場合はアンインストール後にインストールしてください。

*障害発生前に PassLogic 認証サーバに適用していたパッチプログラムがある場合はこのタイミングでパッチを適用してください。

*レプリケーション設定完了まで認証サーバ 0 の PassLogic 管理ツールにアクセスしないでください。誤ってアクセスした場合は再インストールしてください。

④【認証サーバ 1】データベース レプリケーション設定

認証サーバ 1 で下記のコマンドを実行してください。

```
# /opt/passlogic/apps/tools/passlogic_redundant.sh
```

⑤【認証サーバ 1】認証サーバ 0 リカバリ

認証サーバ 1 の管理ツールにログインし、メイン画面「DB Status」欄 DB0 の「recovery」リンクをクリックしてください。リカバリが正常終了すると DB0 が「Node Running & Connect」と表示されます。

*「リカバリ」ではデータベースで管理されている全ての情報とファイルで管理されている設定情報 (/opt/passlogic/data/以下全て)を認証サーバ 1 から認証サーバ 0 へコピーします。

⑥【認証サーバ 0】稼働状況の確認

認証サーバ 0 の管理ツールにログインし、メイン画面「DB Status」欄 で DB0 と DB1 が「Node Running & Connect」と表示されていることを確認してください。

3.4 認証サーバ 1 リカバリ手順

認証サーバ 1 に障害が発生し、認証サーバ 0 が正常稼働しているときに本手順を実施してください。

*リカバリ対象サーバ(認証サーバ 0 / 認証サーバ 1)によりリカバリ手順が異なります。

*リカバリ前後で認証サーバの役割(認証サーバ "0"と "1")は入れ替わりません。

①【認証サーバ 1】OS シャットダウン

認証サーバ 1 の OS をシャットダウンしてください。

②【認証サーバ 0】認証サーバ 1 への接続停止状態の確認とバックアップ取得

認証サーバ 0 の管理ツールにログインし、メイン画面「DB Status」欄 DB1 が「Node Down」と表示されていることを確認し、管理ツール>メンテナンス>バックアップ より、バックアップファイルを取得してください。

*障害復旧が正常に終了しなかった場合に備えてバックアップを必ず取得してください。

③【認証サーバ 1】サーバ再構築

認証サーバ 1 に PassLogic 認証サーバソフトウェアをインストールしてください。

*本マニュアル「【認証サーバ】PassLogic 認証ソフトウェア インストール」を参照してください。

*すでに PassLogic がインストールされている場合はアンインストール後にインストールしてください。

*障害発生前に PassLogic 認証サーバに適用していたパッチプログラムがある場合はこのタイミングでパッチを適用してください。

*レプリケーション設定完了まで認証サーバ 1 の PassLogic 管理ツールにアクセスしないでください。誤ってアクセスした場合は再インストールしてください。

④【認証サーバ 0】データベース レプリケーション設定

認証サーバ 0 で下記のコマンドを実行してください。

```
# /opt/passlogic/apps/tools/passlogic_redundant.sh
```

⑤【認証サーバ 0】認証サーバ 1 リカバリ

認証サーバ 0 の管理ツールにログインし、メイン画面「DB Status」欄 DB1 の「recovery」リンクをクリックしてください。リカバリが正常終了すると DB1 が「Node Running & Connect」と表示されます。

*「リカバリ」ではデータベースで管理されている全ての情報とファイルで管理されている設定情報 (/opt/passlogic/data/以下全て)を認証サーバ 0 から認証サーバ 1 へコピーします。

⑥【認証サーバ 1】稼働状況の確認

認証サーバ 1 の管理ツールにログインし、メイン画面「DB Status」欄 でDB0 とDB1 が「Node Running & Connect」と表示されていることを確認してください。

4 その他

4.1 pgpool フェイルオーバー時のメール配信

pgpool が管理中の postgresql に対して接続要求を送信したとき(ユーザまたは管理者が PassLogic にアクセスしたとき)に postgresql の障害を検知し、フェイルオーバー(障害検知)メールを送信します。

*送信されるメールは failover_mail.sh に定義した内容です。

*フェイルオーバーメールは稼働中の全 pgpool が送信元になるため、postgresql がダウンした場合にはレプリケーションしている DB サーバの数(稼働中の pgpool の数)分のメールが届きます。例えば認証サーバ0の postgresql がダウンした場合は、認証サーバ0上の pgpool が postgresql のダウンを検知したときに1通、認証サーバ1上の pgpool が postgresql のダウンを検知したときに1通、計2通のフェイルオーバーメールが通知されます。

4.2 pgpool フェイルバック時のメール配信

認証サーバの管理ツール「recovery」リンククリック後、リカバリが完了したときにフェイルバック(障害復旧)メールが送信されます。

*送信されるメールは failback_mail.sh に定義した内容です。

*フェイルバックメールはリカバリ元の pgpool が送信元となります。

4.3 データベース (postgresql) 管理情報

データベースで管理される情報は下記の情報です。

ユーザ情報	: 管理ツール > ユーザ管理メニュー で登録・編集できる情報
管理者情報	: 管理ツール > 管理者メニュー で登録・編集できる情報
ログ情報	: 管理ツール > ログ閲覧メニュー で参照できる情報

上記以外の情報は認証サーバのファイル上で管理されており、同期されません。ファイル管理情報の同期は下記の手順で実施してください。

1: 認証サーバ 同期元/opt/passlogic/data/ 以下全てを 同期先サーバへコピー

*ファイルの所有者と権限は変えないでください

*ファイル間での設定情報の整合性を保つため、ファイルを個別で同期せず、対象ディレクトリ以下全てを同期してください。

2: 認証サーバ 同期先 radiusd 再起動

(RHEL6 系の場合) # /sbin/service radiusd restart	(RHEL7 系の場合) # systemctl restart radiusd
---	---

3: 認証サーバ 同期先 httpd 再起動

(RHEL6 系の場合) # /sbin/service httpd restart	(RHEL7 系の場合) # systemctl restart httpd
---	---

4: 認証サーバ 同期先 キャッシュ削除

cd /opt/passlogic/tmp/ # rm -f *.cache

4.4 PassLogic 認証サーバ 停止・起動手順

システムメンテナンス等で、レプリケーション構成の PassLogic 認証サーバの OS を停止・起動する場合は、下記の手順を実施してください。

PassLogic 認証サーバ OS 停止手順

1: 【停止対象サーバ】プロセス停止

(RHEL6 系の場合) # service httpd stop # service passlogic-pgpool stop # service passlogic-pgsql stop	(RHEL7 系の場合) # systemctl stop httpd # systemctl stop passlogic-pgpool # systemctl stop passlogic-pgsql
---	---

2: 【稼働中サーバ】DB 切り離し状態確認

管理ツールにログインして Main ページで停止対象サーバのデータベースが「Node Down」であることを確認してください。

3: 【停止対象サーバ】OS 停止

*続いて残りの PassLogic 認証サーバも停止する場合は、対象サーバで手順 1 を実施してください。

PassLogic 認証サーバ OS 起動手順

全ての PassLogic 認証サーバが停止している場合は、最後に停止したサーバ OS を起動後に下記の手順を実施してください。

1: 【起動対象サーバ】OS 起動

2: 【稼働中サーバ】データベースリカバリ

管理ツールにログインして Main ページで起動対象サーバのデータベース欄「recovery」リンクをクリックしてください。

*手順 1 から 2(データベースリカバリ)完了までの間、起動対象サーバの PassLogic(管理ツール、ユーザインターフェース、radius サーバを含む全て)に一切アクセスしないでください。

4.5 PassLogic 認証サーバ ソフトウェア アップデート

レプリケーション構成の PassLogic 認証サーバをアップデートする場合、全ての PassLogic 認証サーバへのユーザアクセスを遮断した状態で1台ずつアップデートを実施してください。

PassLogic 認証サーバ アップデート手順

1: ユーザアクセス遮断

ロードバランサー または ゲートウェイサーバ のサービスを停止するなどして PassLogic 認証サーバへのアクセスを遮断してください。

2: 【認証サーバ 0】ソフトウェア アップデート

インストールガイドのアップデート手順に従い認証サーバ 0 をアップデートしてください。

3: 【認証サーバ 1】ソフトウェア アップデート

認証サーバ 0 のアップデートが終わってから、認証サーバ 1 をアップデートしてください。

4: ユーザアクセス遮断解除

PassLogic 認証サーバへのアクセス遮断状態を解除してください。

4.6 PassLogic 認証サーバに http でアクセスできるようにする

ゲートウェイサーバ ~ PassLogic 認証サーバ間を https ではなく http でアクセスできるようにする場合は、PassLogic をインストール後に下記の設定を変更してください。

【PassLogic 認証サーバ】

/etc/php.ini の下記の設定値を変更 (http の場合にも cookie の利用を許可する)

(変更前) session.cookie_secure = 1

(変更後) session.cookie_secure = 0

Apache を再起動 (設定変更内容を反映)

(RHEL6 の場合) # service httpd restart

(RHEL7 の場合) # systemctl restart httpd.service

【PassLogic ゲートウェイサーバ】

/etc/httpd/conf.d/ssl.conf (プロキシ定義を https から http に変更する)

(変更前) ProxyPass / https://{PassLogic 認証サーバ IP アドレス}/

ProxyPassReverse / https://{PassLogic 認証サーバ IP アドレス}/

(変更後) ProxyPass / http://{PassLogic 認証サーバ IP アドレス}/

ProxyPassReverse / http://{PassLogic 認証サーバ IP アドレス}/

Apache を再起動 (設定変更内容を反映)

4.7 認証サーバとゲートウェイサーバに http でアクセスできるようにする

ロードバランサー ～ ゲートウェイサーバ ～ PassLogic 認証サーバ間を、https ではなく http でアクセスできるようにする場合は、PassLogic をインストール後に下記の設定を変更してください。

【PassLogic 認証サーバ】

/etc/php.ini の下記の設定値を変更（http の場合にも cookie の利用を許可する）

（変更前）`session.cookie_secure = 1`

（変更後）`session.cookie_secure = 0`

Apache を再起動（設定変更内容を反映）

(RHEL6 の場合) `# service httpd restart`

(RHEL7 の場合) `# systemctl restart httpd.service`

【PassLogic ゲートウェイサーバ】

/etc/httpd/conf.d/ssl.conf（以下のプロキシ定義を削除する）

`## Proxy Settings for PassLogic`

`ProxyPass / https://{PassLogic 認証サーバ IP アドレス}/`

`ProxyPassReverse / https://{PassLogic 認証サーバ IP アドレス}/`

`SSLProxyEngine ON`

`SSLProxyVerify none`

`SSLProxyCheckPeerCN off`

`SSLProxyCheckPeerName off`

`SSLProxyCheckPeerExpire off`

/etc/httpd/conf/httpd.conf（以下のプロキシ定義をファイルの最後に追記する）

`## Proxy Settings for PassLogic`

`ProxyPass / http://{PassLogic 認証サーバ IP アドレス}/`

`ProxyPassReverse / http://{PassLogic 認証サーバ IP アドレス}/`

Apache を再起動（設定変更内容を反映）