

PassLogic Enterprise Edition

Ver.4.3.2

インストールガイド

第 1.0 版

(Manual 1-1)



本書について

本書は、PassLogic エンタープライズエディションのインストールガイドです。

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もあります。

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。

本書に掲載の内容およ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。

特許/Patent

本製品の米国にて取得した特許は下記 URL に記載されております。

PAT.: <https://www.passlogy.com/en/patents/>

目次

目次.....	2
1 はじめに.....	5
1.1 PassLogic サーバ構成.....	6
1.2 動作環境.....	7
ディスク容量.....	7
1.3 SSL 証明書のインストールについて.....	8
1.4 ウィルス対策ソフトを利用する場合.....	10
1.5 推奨ブラウザ.....	11
1.6 使用ポート.....	12
2 インストール.....	13
2.1 OS のタイムゾーンの設定の確認.....	13
2.2 必要なパッケージのインストール.....	13
2.3 PassLogic をインストールする.....	16
2.4 Apache 推奨設定.....	20
2.5 global_setting 設定.....	21
2.6 メンテナンスツールに初めてアクセスする.....	22
2.7 ライセンスを登録する.....	23
3 アップデート.....	24
3.1 PassLogic をアップデートする.....	24
4 アンインストール.....	24
4.1 PassLogic をアンインストールする.....	24
5 サーバ運用管理.....	25
5.1 監視対象プロセス.....	25
5.2 監視 API.....	25
5.3 ログファイル.....	30
PassLogic アプリケーションログ.....	30
pgpool ログ.....	30
LDAP 認証連携ユーザ削除ログ.....	30
5.4 サーバ固有情報.....	31
5.5 メンテナンス.....	31
ライセンス管理.....	32
バックアップ.....	32
リストア.....	33
テクニカルサポート.....	36
6 分離構成.....	38

6.1	ゲートウェイサーバのセットアップ	38
	必要なパッケージのインストール	38
	ゲートウェイサーバのインストール	38
	PKI 設定の追加	39
	PassLogic ユーザインターフェース アクセス確認	39
6.2	ゲートウェイサーバ 接続先の変更	39
6.3	ゲートウェイサーバ リカバリ手順	40
6.4	PassLogic 認証サーバに http でアクセスできるようにする	40
6.5	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	41
6.6	ゲートウェイサーバアップデート	42
7	冗長化構成	43
7.1	概要	43
7.2	冗長化構成のセットアップ	45
7.3	PassLogic 認証サーバ 停止・起動手順	47
	PassLogic 認証サーバ OS 停止手順	47
	PassLogic 認証サーバ OS 起動手順	48
7.4	認証サーバリカバリ手順	49
	認証サーバ0に障害が発生した場合	49
	認証サーバ1に障害が発生した場合	50
7.5	認証サーバ 切り離し/再接続 手順	51
	切り離し/再接続 対象が認証サーバ1の場合	51
	切り離し/再接続 対象が認証サーバ0の場合	53
7.6	メンテナンス(冗長化構成)	54
	データベースの再同期	54
	メインサーバ・サブサーバ切り替え	58
	ログファイル強制同期	59
7.7	移設手順(冗長化構成)	60
	①移設元認証サーバよりバックアップの取得および必要ファイルの用意	60
	②移設先サーバに PassLogic を新規インストール冗長化構成構築	61
	③移設先のサーバにバックアップファイルをリストア	64
	④passlogic_config の設定	64
8	注意事項	65
8.1	PassLogic 認証サーバ利用全般	65
	IE の互換表示を使用する場合の注意点	65
	PKI 利用時の制限事項	65
	TLS1.3 非サポート	65
	ハードディスク容量およびハードウェア障害、ミドルウェア障害の監視	66
	PassLogic for Windows Desktop の制限事項	66

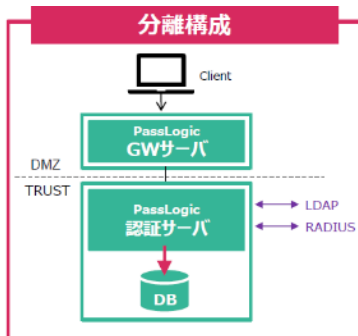
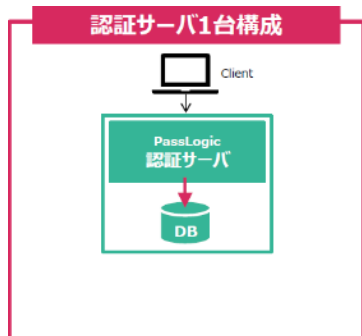
管理者用(admin)パスワードを忘れた場合	67
ミドルウェアのパフォーマンスチューニングについて	68
パフォーマンスに関する補足事項	68
FreeRADIUS 仕様変更における注意点	68
8.2 冗長化構成時の注意事項	69
認証サーバ間の同期対象データ	69
冗長化構成リカバリ処理実行時の注意事項	69
pgpool フェイルオーバー時のメール配信	70
pgsql と pgpool の再起動	70
認証セッション情報の削除	71
DB0 と DB1 のデータ齟齬の検知	71
pgpool フェイルオーバーの検知	72
8.3 災害対策構成(DR)時の注意事項	72
8.4 NFS 領域への配置についての注意事項	73
付録 A メールテンプレート初期文面の一覧	74
新規ユーザ送信メール	74
パスワード再発行送信メール	77
パスワードリマインダー送信メール	78
TOTP 交換トークン設定送信メール	78
PassClip 再セットアップ送信メール	79
端末登録送信メール	80
PKI 認証用クライアント証明書の発行メール	80
有効期限送信メール	81
アカウントロック通知メール	82
新規ユーザ送信メール(管理者)	82
パスワード再発行送信メール(管理者)	84
有効期限送信メール(管理者)	85
アカウントロック通知メール(管理者)	86

1 はじめに

PassLogic を分離構成(ゲートウェイサーバと認証サーバに分離)で構築する場合 および 認証サーバを冗長化構成(冗長化構成)で構築する場合は、それぞれ「6 分離構成」、あるいは「7 冗長化構成」の項目も合わせてご覧ください。

1.1 PassLogic サーバ構成

PassLogic は下記のサーバ構成で構築することができます。本資料では、認証サーバを構築する手順、および下図で示した「分離構成」と「冗長化構成」での構築手順をご案内いたします。

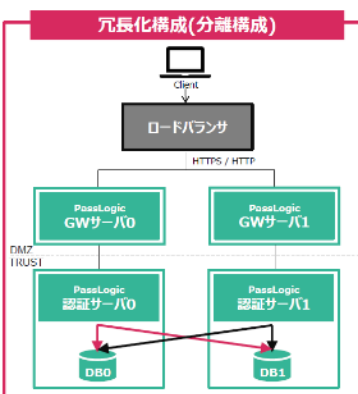
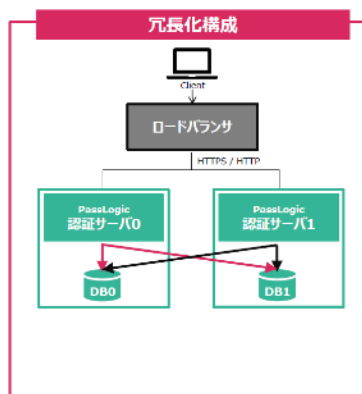


・認証サーバ 1 台構成

PassLogic 認証サーバを外部公開する必要が無い場合の構成 (Windows ログイン、H/W トークンなど)

・分離構成

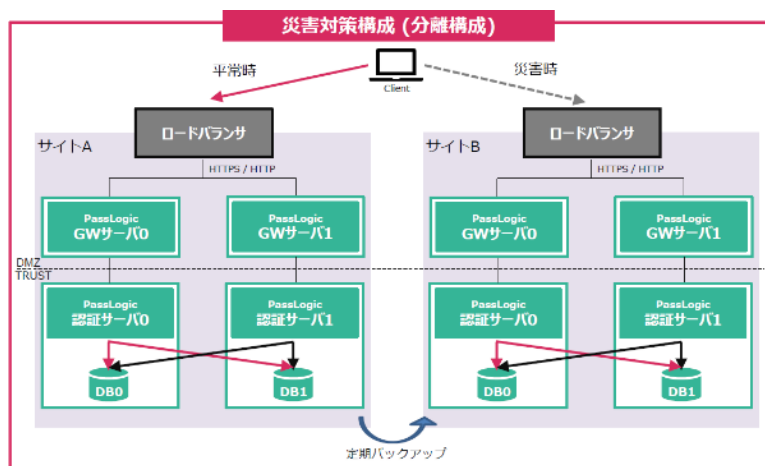
ゲートウェイサーバ (GW サーバ) 経由で PassLogic 認証サーバにアクセスさせる構成。LDAP や RADIUS 通信も内部セグメントで完結



・冗長化構成

Postgresql (pgpool) により、DB0 と DB1 双方に書き込むことで、DB の同一性を担保する方式を取っています。

異なる拠点間で冗長化構成 (災害対策構成) を実施される場合は、十分なネットワーク品質が求められます。詳細は冗長化構成の項をご参照ください。



・災害対策構成

上記構成を応用することで、さらに高い可用性が期待される構成も可能です。

(注意) 災害対策構成の一例です。

(注意) 災害対策構成 (ディザスタリカバリ) の場合は、「8.3 災害対策構成 (DR) 時の注意事項」をご確認ください。

1.2 動作環境

PassLogic 認証サーバの動作環境は以下の通りです。

なお、動作環境に関する最新の情報は下記 URL で公開しておりますので、必ずご確認ください。

https://passlogic.jp/auth_server/

Red Hat Enterprise Linux 8.3 以降 (x86_64)	
httpd	Apache HTTP Server version: 2.4.37 release: 21.module_el8.2.0 以降
php	version: 7.4.6 以降. release: 4.module_el8.3.0

(注意)上記以外のオペレーティング・システム、ディストリビューションの動作に関しましては、弊社サポートまでお問い合わせください。

(注意)各モジュールは、OS ベンダ提供パッケージのみのサポートとなります。独自コンパイルしたものはサポート対象外です。

(注意)NSA Security-Enhanced Linux(SELinux)を有効にした環境での動作は保証されませんので OS インストール時に「無効」に設定してください。

(注意)IPv6 無効化については、ブートオプション `ipv6.disable=1` で無効化した場合のみ動作を確認しています。カーネルパラメータ `net.ipv6.conf.all.disable_ipv6 = 1` で無効化した環境での動作は保証されません。なお、IPv6 を無効化する場合は、postfix の `ipv6` の無効化の設定も実施して下さい。

(注意)サーバ OS およびサーバ OS が提供するミドルウェアはサーバ OS のサポート範囲となり、それらの脆弱性や不具合のパッチ提供およびお問合せはサーバ OS のサポート窓口から提供されます。

(注意)冗長化構成の場合、両系の認証サーバのタイムゾーンは同一にしてください。

(注意)/opt/passlogic にインストールされていることを前提に設計を行っております。それ以外の場所にインストールされた環境での動作の保証はされませんので、あらかじめご了承の上、ご利用ください。

(注意)php の OPcache モジュールは PassLogic インストール時に無効化されます。無効化した環境のみ動作が保証されます。

ディスク容量

PassLogic で利用するディレクトリの内、以下のディレクトリでは容量の確保が必要となります。最低容量、推奨容量は以下の通りです。

ディレクトリ	最低	推奨(5000ID)	推奨(10000ID)
/opt/passlogic	64GB	128GB 以上	256GB 以上

/var/log/httpd, /var/log/passlogic と /var/log/passlogic-pgpool, /var/log/radius の合計	64GB	128GB 以上	256GB 以上
---	------	----------	----------

ユーザ数、ご利用方法(連携先)、ログレベルやログファイルのローテーション、保存期間によって必要な容量は変わってきます。上記は目安とお考えください。

尚、/opt/passlogic はマウントポイントとして指定できません。そのため、上記をご参照の上、ルートパーティション (/) の容量を決定してください。

/dev/shm に一時ファイルを作成します。

通常の使用では高負荷時でも 1MB 以下の使用ですが、理論値の最大は下記の通りとなります。

apache の MaxClient 設定値 x 0.1MB

1.3 SSL 証明書のインストールについて

SSL 証明書のインストール手順を説明いたします。設定を行う際は SSL サーバ証明書の発行機関のマニュアルも併せてご確認ください。

【ロードバランサをご利用の場合】

ロードバランサのマニュアルに従い、インストールしてください。

【ゲートウェイサーバに設定する場合】

「6.1 ゲートウェイサーバのセットアップ」を実施後に以下の手順で設定します。

(i) /etc/httpd/conf.d/passlogic-gw.conf を編集します。

ユーザアクセスに適用する場合

```
<VirtualHost _default_:443>
..... (省略) .....
    SSLCertificateFile {サーバ証明書}
    SSLCertificateKeyFile {秘密鍵ファイル}
..... (省略) .....
</VirtualHost>
```

管理コンソールアクセスに適用する場合

```
<VirtualHost _default_:8443>
..... (省略) .....
```

```
        SSLCertificateFile {サーバ証明書}
        SSLCertificateKeyFile {秘密鍵ファイル}
        ..... (省略) .....
</VirtualHost>
```

(ii) コマンドラインから httpd を再起動します。

```
# systemctl restart httpd
```

【認証サーバに設定する場合】

「2.2 PassLogic をインストールする」を実施後に以下の手順で設定します。

(i) /opt/passlogic/data/conf/passlogic-apache.conf を編集します。

ユーザアクセスに適用する場合

```
<VirtualHost _default_:443>
..... (省略) .....
        SSLCertificateFile {サーバ証明書}
        SSLCertificateKeyFile {秘密鍵ファイル}
        ..... (省略) .....
</VirtualHost>
```

API アクセスに適用する場合

```
<VirtualHost _default_:7443>
..... (省略) .....
        SSLCertificateFile {サーバ証明書}
        SSLCertificateKeyFile {秘密鍵ファイル}
        ..... (省略) .....
</VirtualHost>
```

管理コンソールアクセスに適用する場合

```
<VirtualHost _default_:8443>
..... (省略) .....
        SSLCertificateFile {サーバ証明書}
        SSLCertificateKeyFile {秘密鍵ファイル}
        ..... (省略) .....
</VirtualHost>
```

メンテナンス画面アクセスに適用する場合

```
<VirtualHost _default_:12443>
..... (省略) .....
    SSLCertificateFile {サーバ証明書}
    SSLCertificateKeyFile {秘密鍵ファイル}
..... (省略) .....
</VirtualHost>
```

(ii) コマンドラインから httpd を再起動します。

```
# systemctl restart httpd
```

【注意事項】

(i) 中間 CA 証明書、およびクロスルート証明書がある場合は、サーバ証明書、中間 CA 証明書、クロスルート証明書の順番にファイルへまとめ、SSLCertificateFile ディレクティブに指定してください。

1 つにまとめた署名書(fullchain.crt)

```
-----BEGIN CERTIFICATE-----
{サーバ証明書}
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
{中間 CA 証明書}
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
{クロスルート証明書(オプション)}
-----END CERTIFICATE-----
```

ディレクティブ設定

```
SSLCertificateFile fullchain.crt
```

1.4 ウィルス対策ソフトを利用する場合

PassLogic 認証サーバの下記ディレクトリをスキャン対象から外してください。

```
/var/lib/php/session
```

1.5 推奨ブラウザ

PassLogic のユーザインターフェイスは、HTML5、CSS3、JavaScript で開発されています。またセッション情報の保持に Cookie を使用します。

	ブラウザ	文字コード
管理ツール メンテナンスツール	[PC] Internet Explorer11	UTF-8
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
ユーザインターフェイス	[PC] Internet Explorer 11	
	[PC] Edge	
	[PC] Firefox	
	[PC] Chrome	
	[iPhone / iPad] Safari (iOS / iPadOS 15)	
	[Android] Chrome (Android 8,9,10,11)	

- (注意) Edge ブラウザでは信頼できない証明書が設定されている https サイトへの SSO が正常動作しません。
- (注意) Edge ブラウザの「Internet Explorer モード」は、サポート対象外です。
- (注意) Internet Explorer の「互換表示」機能は、サポート対象外です。なお、互換表示機能を利用する際の参考情報を「IE の互換表示を使用する場合の注意点」に記載しております。
- (注意) ブラウザのバージョンアップなどにより、ブラウザの仕様が変更となった場合には、PassLogic の動作に影響する可能性があります。

1.6 使用ポート

ポート番号	プロトコル	送信元	送信先	内容
22/tcp	ssh	PassLogic サーバ	PassLogic サーバ	冗長化構成の場合に利用(注意)0
80/tcp	http	クライアント	PassLogic サーバ	ユーザインターフェイス (注意)1
443/tcp	https	クライアント	PassLogic サーバ	ユーザインターフェイス (注意)1
1812/udp	radius	RADIUS クライアント	PassLogic サーバ	RADIUS 認証
5439/tcp	postgres	PassLogic サーバ	PassLogic サーバ	データベース
7080/tcp	http	API クライアント	PassLogic サーバ	API 通信 (注意)2
		PassLogic サーバ	PassLogic サーバ	冗長化構成の場合に利用
7443/tcp	https	API クライアント	PassLogic サーバ	API 通信 (注意)2
8080/tcp	http	クライアント	PassLogic サーバ	管理ツールインターフェイス (注意)3
8443/tcp	https	クライアント	PassLogic サーバ	管理ツールインターフェイス
9915/tcp	postgres	PassLogic サーバ	PassLogic サーバ	データベース (注意)4
9925/tcp	pgpool	PassLogic サーバ	PassLogic サーバ	データベース (注意)4
12080/tcp	http	クライアント	PassLogic サーバ	メンテナンスツールインターフェイス (注意)3
12443/tcp	https	クライアント	PassLogic サーバ	メンテナンスツールインターフェイス

(注意)0: 相手方の認証サーバだけでなく、自サーバにも SSH が実行できるようファイアウォールを設定してください

(注意)1:分離構成時、ゲートウェイサーバでクライアントとの SSL 通信を終端し、ゲートウェイサーバと認証サーバ間で http 通信を行う場合、443/tcp は利用しません。その一方、クライアントから認証サーバまでの経路で https 通信を行う場合、80/tcp は利用しません。

(注意)2: API を利用しない場合は、外部からアクセスできないように設定することを推奨します。

(注意)3:管理ツール、メンテナンスツールに http でアクセスしない場合、8080/tcp および 12080/tcp は利用しません。

iptables や firewalld 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 認証サーバソフトウェア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。また連携機器へのアクセスを行えるようにアウトバウンド通信を許可してください。

(注意)4:9915/tcp および 9925/tcp は http サーバと pgpool 間の通信に使用するので、ローカルホスト内での通信となります。

2 インストール

2.1 OS のタイムゾーンの設定の確認

下記のコマンドで OS のタイムゾーンが正しく設定されている事を確認して下さい。

```
(root 権限で実行)
# timedatectl show | grep ^Timezone
```

(注意) 運用開始後に TZ を変更しないようにして下さい。運用開始後に TZ を変更した場合、動作が意図した通りにならない場合があります。

2.2 必要なパッケージのインストール

下記は PassLogic サーバソフトウェアを動作させるのに必要なパッケージソフトのインストールコマンドです。

```
(root 権限で実行)
# dnf module reset php
# dnf module install php:7.4

# dnf -y install tar
# dnf -y install sed
# dnf -y install sudo
# dnf -y install gnupg2
# dnf -y install rpm
# dnf -y install openssl
# dnf -y install openssh-clients
# dnf -y install tmpwatch
# dnf -y install httpd
# dnf -y install mod_ssl
# dnf -y install chrony
# dnf -y install zip
# dnf -y install unzip
# dnf -y install crontabs
# dnf -y install postfix
# dnf -y install php
# dnf -y install php-ldap
```

```
# dnf -y install php-pgsql
# dnf -y install php-json
# dnf -y install php-xml
# dnf -y install php-pecl-zip
# dnf -y install net-snmp-utils
# dnf -y install curl
# dnf -y install libtool-ltdl
# dnf -y install libxslt
# dnf -y install rsync
# dnf -y install mailx
# dnf -y install xmlsec1
# dnf -y install xmlsec1-openssl
# dnf -y install freeradius
# dnf -y install net-tools
# dnf -y install libnsl
# dnf -y install php-mbstring
# dnf -y install php-process
# dnf -y install apr-util-pgsql

# dnf -y upgrade libzip
```

インターネットに接続できない環境で dnf コマンドによるインストールを行えない場合、下記の手順で Red Hat Enterprise Linux のインストールディスクから必要なパッケージソフトをインストールできます。

```
(root 権限で実行)
① Red Hat Enterprise Linux のインストールディスクをマウントします。
# /usr/bin/mount -r /dev/sr0 /media (ディスクデバイスが/dev/sr0 にマッピングされている場合)

② dnf のリポジトリに設定を追加します。
# /usr/bin/vi /etc/yum.repos.d/passlogic.repo
  以下の内容を記載します。
[passlogic-BaseOS]
name=passlogic-BaseOS
baseurl=file:///media/BaseOS/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

```
[passlogic-AppStream]
name=passlogic-AppStream
baseurl=file:///media/AppStream/
gpgcheck=1
enabled=0
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
```

③ 下記のコマンドで追加パッケージをインストールします。

```
# dnf --disablerepo=* --enablerepo=passlogic-* module reset php
# dnf --disablerepo=* --enablerepo=passlogic-* module install php:7.4

# dnf -y --disablerepo=* --enablerepo=passlogic-* install tar
# dnf -y --disablerepo=* --enablerepo=passlogic-* install sed
# dnf -y --disablerepo=* --enablerepo=passlogic-* install sudo
# dnf -y --disablerepo=* --enablerepo=passlogic-* install gnupg2
# dnf -y --disablerepo=* --enablerepo=passlogic-* install rpm
# dnf -y --disablerepo=* --enablerepo=passlogic-* install openssl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install openssh-clients
# dnf -y --disablerepo=* --enablerepo=passlogic-* install tmpwatch
# dnf -y --disablerepo=* --enablerepo=passlogic-* install httpd
# dnf -y --disablerepo=* --enablerepo=passlogic-* install mod_ssl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install chrony
# dnf -y --disablerepo=* --enablerepo=passlogic-* install zip
# dnf -y --disablerepo=* --enablerepo=passlogic-* install unzip
# dnf -y --disablerepo=* --enablerepo=passlogic-* install crontabs
# dnf -y --disablerepo=* --enablerepo=passlogic-* install postfix
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-ldap
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-pgsql
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-json
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-xml
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-pecl-zip
# dnf -y --disablerepo=* --enablerepo=passlogic-* install net-snmp-utils
# dnf -y --disablerepo=* --enablerepo=passlogic-* install curl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install libtool-ltdl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install libxslt
# dnf -y --disablerepo=* --enablerepo=passlogic-* install rsync
# dnf -y --disablerepo=* --enablerepo=passlogic-* install mailx
```



```
# dnf -y --disablerepo=* --enablerepo=passlogic-* install xmlsec1
# dnf -y --disablerepo=* --enablerepo=passlogic-* install xmlsec1-openssl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install freeradius
# dnf -y --disablerepo=* --enablerepo=passlogic-* install net-tools
# dnf -y --disablerepo=* --enablerepo=passlogic-* install libnsl
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-mbstring
# dnf -y --disablerepo=* --enablerepo=passlogic-* install php-process
# dnf -y --disablerepo=* --enablerepo=passlogic-* install apr-util-pgsql
```

④ パッケージの更新を行います。

```
# dnf -y --disablerepo=* --enablerepo=passlogic-* upgrade libzip
```

⑤ Red Hat Enterprise Linux のインストールディスクを取り出します。

```
# /usr/bin/umount /media
```

```
# /usr/bin/eject
```

2.3 PassLogic をインストールする

① PassLogic パッケージの展開

「その他のユーザ」にアクセス権限が付与されたディレクトリにインストーラを転送してください。ここでは、`/usr/local/src/`に `PassLogic-ent-x.x.x-el8.tar.gz` を転送している前提で説明します。

(注意) `/root/`配下など、「その他ユーザ」にアクセス権限のないディレクトリへのパッケージ展開ではインストール処理が正常に動作しません。

(注意) 適宜、修正パッチの適用をお願いします。(https://passlogic.jp/pl_supportinfo/)

```
(root 権限で実行)
# cd /usr/local/src/
# tar zxvf PassLogic-ent-x.x.x-el8.tar.gz
# cd passlogic-ent-... /
```

(注意) インストール時以下のファイルを更新します。SSL 証明書を下記ファイルに設定している場合は再設定が必要となります。

```
/etc/pki/tls/certs/localhost.crt
/etc/pki/tls/private/localhost.key
```

② SSH 鍵の再作成（任意）

展開したインストール用パッケージ内には、PassLogic 認証サーバソフトウェアが「passlogic」ユーザとして利用する SSH 鍵があります。（上記の例であれば、/usr/local/src/passlogic-ent-x.x.x/ssh/*）デフォルトでパッケージされている SSH 鍵は弊社が事前に用意した共通のものとなりますが、インストール前に、以下の sshkey_generate.sh を実行することで、新しい SSH 鍵に置き換えることができます。

```
(root 権限で実行)
# ./sshkey_generate.sh
```

(注意)冗長化構成にて構築する場合は、SSH 鍵ファイルは認証サーバ間で同一の必要があります。認証サーバ0にて SSH 鍵を再作成した際には、その SSH 鍵ファイルを以下のように認証サーバ1にコピーした上で、次に説明する認証サーバ1での PassLogic インストールコマンドを実行してください。

また、冗長化構成の障害発生時にリカバリ処理をする際に、同 SSH 鍵が必要になります。再作成した SSH 鍵は大切に保管しておいてください。

コピー対象ファイル(3 ファイル):

```
{認証サーバ0 の PassLogic インストーラディレクトリ}/ssh/authorized_keys
{認証サーバ0 の PassLogic インストーラディレクトリ}/ssh/id_rsa
{認証サーバ0 の PassLogic インストーラディレクトリ}/ssh/id_rsa.pub
例: /usr/local/src/passlogic-ent-x.x.x/ssh/authorized_keys
     /usr/local/src/passlogic-ent-x.x.x/ssh/id_rsa
     /usr/local/src/passlogic-ent-x.x.x/ssh/id_rsa.pub
```

コピー先:

```
{認証サーバ1 の PassLogic インストーラディレクトリ}/ssh/
例: /usr/local/src/passlogic-ent-x.x.x/ssh/
```

③ 共通暗号鍵の再作成（任意）

共通暗号鍵の作成を行います。暗号鍵はデータベースの一部のデータの暗号化・復号化に利用されます。共通暗号鍵の作成を省略した場合、プログラムに内包のデフォルト共通暗号鍵が利用されます。独自の暗号鍵を設定する場合、インストール前に、以下のコマンドを実行してください。半角英数字 16 文字の暗号鍵ファイルが作成され、インストール時に取り込まれます。

```
(root 権限で実行)
# cat /dev/urandom | tr -dc 'a-zA-Z0-9' | fold -w 16 | head -1 | xargs echo -n >
lib/plcrypt.conf
```

以下のファイルにランダムな半角英数字 16 文字が書き込まれていれば、正しく生成されています。

```
/usr/local/src/passlogic-ent-x.x.x/lib/plcrypt.conf
```

再インストール時は、保管していた plcrypt.conf を /usr/local/src/passlogic-ent-x.x.x/lib/plcrypt.conf に配置してください。

(注意)冗長化構成にて構築する場合は、共通暗号鍵ファイルは認証サーバ間で同一の必要がありません。認証サーバ0にて共通暗号鍵を再作成した際には、その暗号鍵ファイルを以下のように認証サーバ

バ1にコピーした上で、次に説明する認証サーバ1での PassLogic インストールコマンドを実行してください。

また、障害発生時にサーバを再構築する場合、同共通暗号鍵が必要になります。再作成した共通暗号鍵は大切に保管しておいてください。

コピー対象ファイル(1ファイル):

```
{認証サーバ0 の PassLogic インストーラディレクトリ}/lib/plcrypt.conf
例: /usr/local/src/passlogic-ent-x.x.x/lib/plcrypt.conf
```

コピー先:

```
{認証サーバ1 の PassLogic インストーラディレクトリ}/lib/plcrypt.conf
例: /usr/local/src/passlogic-ent-x.x.x/lib/plcrypt.conf
```

④PassLogic 認証サーバソフトウェアのインストール

展開先のディレクトリで以下のコマンドを実行するとインストールを開始します。

```
(root 権限で実行)
# ./install.sh install
```

(注意)install.sh と同じディレクトリにログファイル(install.log)が出力されます。エラーの有無を確認してください。

インストール時に、以下の設定が自動で追加・変更されます。

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
#AddDefaultCharset	コメントアウトして設定値を無効化
ServerSignature	Off
TraceEnable	Off
LogFormat	“%h %l %u %t ¥”¥r¥” %>s %b ¥”%{Referer}i¥” ¥”%{User- Agent}i¥” %T %D” combined

/etc/openldap/ldap.conf

TLS_REQCERT	never (TLS_REQCERT が未指定の場合)
-------------	-----------------------------

/etc/php.ini

post_max_size	128M
upload_max_filesize	128M
memory_limit	256M
session.cookie_secure	1

expose_php	Off
error_reporting	E_ALL & ~E_NOTICE & ~E_STRICT & ~E_DEPRECATED
session.cookie_httponly	On
short_open_tag	On

/etc/php.d/10-opcache.ini

zend_extension	コメントアウト
opcache.enable	0
opcache.enable_cli	0

/etc/sudoers

defaults requiretty	設定がある場合、コメントアウトして設定値を無効化
#includedir /etc/sudoers.d	設定がない場合に追記し /etc/sudoers.d/passlogic を読み込むようにする。

/etc/systemd/logind.conf

RemoveIPC=no	追加
--------------	----

(注意)logind の IPC オブジェクト削除機能を無効化します。

systemctl コマンドによる自動起動

<pre> httpd chronyd (注意) crond (注意) postfix (注意) passlogic-pgsql passlogic-pgpool radiusd </pre>
--

(注意)該当サービスの rpm パッケージインストール時に自動起動が有効化されます。

Linux ユーザ”passlogic”が自動で追加されます。

(注意)”passlogi”ユーザはリカバリ等で使用されます。パスワードの有効期限切れ等によって無効な ID とならないようにして下さい。

2.4 Apache 推奨設定

Web サーバ脆弱性対策のために、Apache のデフォルト設定を下記のとおり変更することを推奨します。

ディレクトリ リスティング機能 無効化

/etc/httpd/conf/httpd.conf

(変更前) Options Indexes FollowSymLinks

(変更後) Options FollowSymLinks

TRACE メソッド 無効化(インストーラで追記します)

/etc/httpd/conf/httpd.conf

(追記) TraceEnable Off

(注意)X-Frame-Options の設定(クリックジャッキング対策;連携先機器にて読み込む設定がない場合に設定)

/etc/httpd/conf/httpd.conf

(追記) Header always set X-Frame-Options "sameorigin"

不要なディレクトリを削除

/var/www/cgi-bin/

TLSv1.2 を有効化

/etc/httpd/conf.d/ssl.conf

(追記) SSLProtocol TLSv1.2

不要な設定ファイルをリネーム

ディレクトリリスティングを無効化

(変更前)/etc/httpd/conf.d/autoindex.conf

(変更後)/etc/httpd/conf.d/autoindex.conf.org

mod_userdir 設定を無効化

(変更前)/etc/httpd/conf.d/userdir.conf

(変更後)/etc/httpd/conf.d/userdir.conf.org

Apache デフォルトトップページ設定を無効化

(変更前)/etc/httpd/conf.d/welcome.conf

(変更後)/etc/httpd/conf.d/welcome.conf.org

(注意)リバースプロキシ連携を利用する際に連携先が応答する前にタイムアウトし 502 エラーが発生する場合、PassLogic 認証サーバでは、デフォルトのタイムアウトは 60 秒に設定されております。サーバ構成上タイムアウトまでの時間を長くとりたい場合は、Apache の設定で ProxyTimeout の値を変更してください。

設定例:

```
# echo -e "\nProxyTimeout 1000" >>
/opt/passlogic/data/conf/xauth_passlogic_00.conf
```

(注意)連携先にリバースプロキシが存在する場合は、そちらのタイムアウト値も確認ください。

(注意) Apache の設定ファイルは httpd のアップデートで変更される事があります。推奨設定を実施されている場合は、dnf 等でアップデートを実施した際には、再度ご確認頂く事を推奨します。

(注意)PassLogic では TLSv1.3 をサポート対象としていません。また、

/opt/passlogic/data/conf/passlogic-apache.conf にある下記の設定を変更しないでください。

```
SSLProtocol TLSv1.2
```

(注意)設定変更後に Apache の再起動が必要です。

2.5 global_setting 設定

下記の設定は、/opt/passlogic/apps/lib/settings/global_setting.php を編集することで設定可能であり、システムで一意となります。

設定項目	設定内容	設定値
URL_HANDLER_SHOW	RADIUS > SSO 設定 にて、「スマートフォン用認証の送信先 URL」に設定がある場合、ブラウザの User-Agent の値と当設定を比較し、該当する User-Agent であれば、「スマートフォン用認証の送信先 URL」のアドレスへ SSO します。	デフォルト 『Android iPhone iPad』

(注意)バックアップ/リストア/リカバリの対象外となります。追加修正を行った場合、手動でのバックアップをお願いいたします。

(注意)設定変更にあたりサービスの再起動は不要です。

(注意) iPadOS のユーザエージェントは、デスクトップ用の表示をする場合には MacOS と同じ値になります。ユーザエージェントで動作をコントロールする場合にはお客様環境に合わせてご検討ください。

2.6 メンテナンスツールに初めてアクセスする

次のコマンドで、初期の管理者(ユーザ ID: admin)を作成します。

```
(root 権限で実行)
# /opt/passlogic/apps/tools/modify_admin_passwd.php
-----
(コマンド実行結果例)
modified admin password: 3nEG0uJY ← ユーザ ID: admin の初期パスワード
```

(注意)上記コマンド実行結果例の“3nEG0uJY”の部分は、コマンド実行のたびに変わります。この部分が管理者(ユーザ ID: admin)の初期パスワードです。

PassLogic の管理コンソールには、「メンテナンスツール」と「管理ツール」の 2 種類あり、それぞれ同一の ID とパスワードでログインできます。

メンテナンスツール	ライセンス管理、バックアップ/リストア、サポートファイル取得、データベース同期などメンテナンス機能を提供します。
管理ツール	ユーザ管理、連携設定、ポリシー設定、ログ閲覧などを提供します。

ライセンスの登録を行う場合は、メンテナンスツールにウェブブラウザでアクセスします。メンテナンスツールのユーザ ID 入力欄に“admin”と入力し次ページに進み、パスワード入力欄に上記で生成した初期パスワードを入力します(乱数表からランダムパスワードを生成する必要はありませんが、乱数表が表示されてから一定時間内(初期設定:60 秒以内)に入力する必要があります。)

```
https://{PassLogic サーバ FQDN}:12443/passlogic-maintenance/
```

(注意) firewalld 等のファイアウォールを起動している場合は、12443 番ポートでアクセスできるよう設定を行ってください。

(注意)admin アカウントのパスワードを変更する場合は、管理ツールにログインしてください。詳細は 2-1 運用管理ガイド「管理ツールへのアクセス」をご参照ください。

(注意)初期の管理者ユーザ admin は削除できません。



メンテナンス画面トップ

2.7 ライセンスを登録する

ライセンスファイル(license-ent.asc)を登録します。詳細は「5.5 メンテナンス > ライセンス管理」の項目をご確認ください。

3 アップデート

3.1 PassLogic をアップデートする

旧バージョン(エンタープライズ版 Ent-v3.1.0 or Ent-v3.1.0-SP1, Ent-4.x)からのバージョンアップ方法は、バックアップコンバータのマニュアルをご参照ください。バックアップ コンバータで変換したバックアップファイルをリストアする際、「リストア」の章の注意点をご参照ください。

エンタープライズ版、v1.x.x と v2.x.x からアップデートをする場合は、一度 Ent-v3.1.0 or Ent-v3.1.0-SP1 へのアップデートが必要になります。

スタンダード版をご利用の場合は、エンタープライズ版 Ent-v3.1.0 or Ent-v3.1.0-SP1 のいずれかのバージョンの経由が必要になります。Ent-v3.1.0 or Ent-v3.1.0-SP1 へのアップデート方法は、それらのマニュアルをご参照ください。

4 アンインストール

4.1 PassLogic をアンインストールする

PassLogic 認証サーバソフトウェアをアンインストールします。

```
(root 権限で実行)
```

```
# cd /usr/local/src/passlogic-ent-x.x.x/
```

```
# ./install.sh uninstall
```

```
[./install.sh START] (uninstall)
```

```
PassLogic Authentication Server Software をアンインストールするとすべてのデータが削除されます。よろしいですか? - Are you sure to uninstall PassLogic Authentication Server Software? All data will be deleted. [yes/no]
```

```
(yes を入力してください。)
```

(注意)インストール時に利用した install.sh を実行してください(異なるバージョンの PassLogic の install.sh を利用してアンインストールを実行しないでください)。

(注意)アンインストール後 OS を再起動してください。

(注意)rpm パッケージは別途アンインストールしてください。

5 サーバ運用管理

5.1 監視対象プロセス

PassLogic 認証サーバのプロセス監視を行う場合は、以下のプロセスを対象としてください。

/usr/sbin/httpd	ユニット名: httpd.service
/usr/sbin/radiusd	ユニット名: radiusd.service
/opt/passlogic/pgpool/bin/pgpool	ユニット名: passlogic-pgpool.service
/opt/passlogic/pgsql/bin/postgres	ユニット名: passlogic-pgsql.service
(注意) コマンド "# systemctl status ユニット名" で起動状態とプロセス一覧の取得が可能	

(注意) UI 画面を監視する場合は下記 URL をご利用ください。

`https://{PassLogic サーバ FQDN}/ui/index.php`

5.2 監視 API

PassLogicAPI の URL は SSL 有りとなしの 2 種類でそれぞれポートを設定しております。

- API(SSL 有り): `https://{PassLogic サーバ FQDN}:7443/passlogic/api/api`
- API(SSL 無し): `http://{PassLogic サーバ FQDN}:7080/passlogic/api/api`

*監視 API は、PassLogicAPI オプションライセンス費用不要でご利用いただけます。

*内部ネットワークからご利用ください。7443, 7080 ポートへ外部ネットワークからアクセス可能な状態で、利用することは非推奨です。

① DB ステータス取得

監視 API のリクエストを受けた PassLogic サーバで稼働する pgpool と postgres データベースの接続ステータスを取得します。

【送信パラメータ】

パラメータ	必須	説明
mode	○	dbstatus
db	○	DB 番号(注意)

※ ステータスを取得する DB 番号は、db=0 または、db=1 を指定してください。

【レスポンスコード】

Code	状態	説明
10000	準正常	ノード未設定

10001	準正常	ノード稼働・切断中
10002	正常	ノード稼働・接続中
10003	準正常	ノード停止・切断中
10010	異常	送信パラメータ不正
10011	異常	ノード稼働・切断中。リカバリ処理が必要です。
10012	異常	ノード稼働・接続中。リカバリ処理が必要です。

【受信 XML(data 内容)】

DB 接続ステータスを返却します。

【送受信例】

送信 URL
{PassLogic API URL}?mode=dbstatus&db=0
受信 XML
<pre><PassLogic:Response xmlns:PassLogic="https://www.passlogy.com/xmlns/PassLogic"> <code>10002</code> <level>notice</level> <message>Node running - Connect.</message> <message_ja>ノード稼働・接続中。</message_ja> <data>127.0.0.1 5439 2 1.000000 up</data> </PassLogic:Response></pre>

② ミドルウェア ステータス取得

PassLogic サーバに関連するミドルウェアのステータスを取得します。

【送信パラメータ】

パラメータ	必須	説明
mode	○	middlewarestatus
type	○	サービス名称指定(注意)

【サービス名称】

名称	説明
httpd	httpd のステータス取得。
postfix	postfix のステータス取得。
radiusd	radiusd のステータス取得。
chronyd	chronyd のステータス取得。
pgsql	pgsql のステータス取得。

pgpool	pgpool のステータス取得。
vmstat	vmstat コマンドの結果を取得。

(注意)pgpool のノード 1 のステータスは、冗長化構成時のみ取得できます。

(注意)取得サービス名称のパラメータは、サービス毎に指定してください。

【レスポンスコード】

code	状態	説明
10005	正常	ミドルウェアステータス取得成功
10010	異常	送信パラメータ不正

【受信 XML(data 内容)】

サービスのステータスを返却します。

【送受信例】

送信 URL
{PassLogic API URL}?mode=middlewarestatus&type=httpd
受信 XML
<pre><PassLogic:Response xmlns:PassLogic="https://www.passlogy.com/xmlns/PassLogic"> <code>10005</code> <level>notice</level> <message>Middleware Status.</message> <message_ja>ミドルウェアステータス</message_ja> <data>Active: active (running) since Thu 2018-07-12 10:27:13 JST; 6h ago Main PID: 1338 (httpd)</data> </PassLogic:Response></pre>

③ ユーザ数調査

条件に一致するユーザ数を取得します。

【送信パラメータ】

パラメータ	必須	説明
mode	○	usercountstatus
filter		抽出条件
tenant		テナント名。未指定の場合は全テナントが対象。

【抽出条件】

条件	説明
未指定	ユーザ数、管理者数、テストユーザ数をカウント。
locked	ロックされたユーザをカウント。
invalid	無効ユーザをカウント。
expired	有効期限切れユーザをカウント。

【レスポンスコード】

code	状態	説明
10006	正常	登録ユーザ数取得成功
10010	異常	送信パラメータ不正

【受信 XML(data 内容)】

以下のパラメータを返却します。

パラメータ	説明
adminCount	条件に一致する管理者数
userCount	条件に一致する登録ユーザ数
testUserCount	条件に一致するテストユーザ数
maxUserNum	テナントの最大ユーザ数
userLimit	ライセンス上限ユーザ数

(注意)testUserCount、maxUserNum はマルチテナントモード用のパラメータです。

(注意)maxUserNum は、テナント未指定時は userLimit と同じ値になります。

【送受信例】

送信 URL
{PassLogic API URL}?mode=usercountstatus
受信 XML
<pre><PassLogic:Response xmlns:PassLogic="https://www.passlogy.com/xmlns/PassLogic"> <code>10006</code> <level>notice</level> <message>User Numbers.</message> <message_ja>ユーザ数ステータス</message_ja> <data> <adminCount>8</adminCount> <userCount>11</userCount> <testUserCount>0</testUserCount> <maxUserNum>100000</maxUserNum> </data> </PassLogic:Response></pre>

```

    <userLimit>100000</userLimit>
  </data>
</PassLogic:Response></PassLogic:Response>

```

④ ディスク空き容量取得

ディスクの空き容量を取得します。

【送信パラメータ】

パラメータ	必須	説明
mode	○	dfstatus

レスポンスコード】

code	状態	説明
10007	正常	ディスク空き容量ステータス取得成功

【受信 XML(data 内容)】

”df - h”コマンドの実行結果を返却します。

【送受信例】

送信 URL
{PassLogic API URL}?mode=dfstatus
受信 XML
<pre> <PassLogic:Response xmlns:PassLogic="https://www.passlogy.com/xmlns/PassLogic"> <code>10007</code> <level>notice</level> <message>Disk Space Status</message> <message_ja>ディスク空き容量ステータス</message_ja> <data> <Filesystem>/dev/xvda2</Filesystem> <Total>6.2G</Total> <Used>1.8G</Used> <Available>4.5G</Available> <UseRate>29%</UseRate> <MountedOn>/</MountedOn> </data> <data> (省略) </pre>

```
</data>
</PassLogic:Response>
```

5.3 ログファイル

PassLogic アプリケーションログ

管理ツール上の「ログ閲覧」で参照できるログは、以下のファイルに出力されます。

ファイルパス	/var/log/passlogic/passlogic.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic (定義内容の変更可能・アンインストール時に削除されます)

pgpool ログ

pgpool プロセスの開始・停止ログとデータベース障害ログが出力されます。

ファイルパス	/var/log/passlogic-pgpool/pgpool.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic-pgpool (定義内容の変更可能・アンインストール時に削除されます)

LDAP 認証連携ユーザ削除ログ

LDAP 認証連携ユーザ削除スクリプトの実行ログが出力されます。

ファイルパス	/var/log/passlogic/passlogic_adsync.log
ログローテーション	/usr/sbin/logrotate
ローテーション定義	/etc/logrotate.d/passlogic (定義内容の変更可能・アンインストール時に削除されます)

(注意)LDAP 認証連携ユーザ削除スクリプトは手動コマンド実行、または cron による定期実行で行ってください。

5.4 サーバ固有情報

認証サーバ内で、ファイルで管理している下記の4ファイルをサーバ固有情報と呼びます。

- (i) redundant.conf (/opt/passlogic/data/conf/redundant.conf)
認証サーバ 2 台で冗長化構成を構築する場合に、各認証サーバの IP アドレスを設定するファイルです。2 台の認証サーバで redundant.conf の内容は**同一になります**(「7 冗長化構成」参照)。認証サーバが 1 台の場合、このファイルに IP アドレスを設定する必要はありません。
- (ii) ライセンスファイル (/opt/passlogic/data/license-ent.asc)
「2.7 ライセンスを登録する」参照。
- (iii) UI ログファイル (/opt/passlogic/data/logo_images.png)
ユーザインターフェイスに表示されるロゴイメージファイル。デフォルトの PassLogic ログとは別のイメージに変更した場合のみ存在するファイルです(運用管理ガイド・UI ログ変更手順参照)。冗長化構成の場合、両系の認証サーバに登録してください。
- (iv) passlogic_config (/opt/passlogic/data/conf/flag/passlogic_config)
冗長化構成の場合、認証サーバ毎に異なる設定を持たせたい時に利用するフラグファイルです。当ファイルの有無によって VPN 等の設定情報を読み込む DB テーブルが切り替わります。通常は DB0、DB1 共に同一の設定を使用するため意識する必要はありません。

5.5 メンテナンス

メンテナンス画面では以下の操作を行うことができます。

- (i) ライセンス管理
- (ii) バックアップ
- (iii) リストア
- (iv) テクニカルサポートファイル取得

冗長化構成の場合、加えて以下の操作を行うことができます(7 冗長化構成参照)。

- (v) データベースの再同期
- (vi) メインサーバ・サブサーバ切り替え
- (vii) ログファイル強制同期

メンテナンス画面は通常の管理画面とは異なる URL が設定されています。

`https://{PassLogic サーバ FQDN}:12443/passlogic-maintenance/`

(注意)管理者およびパスワードは通常の管理画面と共通です(運用管理ガイド「システム管理ガイド」参照)。

(注意)admin 権限の管理者のみログインできます。

ライセンス管理

PassLogic の利用にはライセンスファイル(license-ent.asc)の登録が必要です。ライセンスファイルにはユーザ数上限や利用期間が埋め込まれており、この内容に従って動作します。ライセンスの追加や契約更新の場合にもライセンスファイルが納品されますので、既存のライセンスの有効期限内に登録を済ませるようお願いいたします。

(注意)インストール直後のライセンスファイル未登録状態ではユーザ数の上限は 1 ユーザです。

(注意)ライセンス登録操作にて各種サービスが停止することはありません。

(注意)ゲートウェイサーバと認証サーバが分離構成の場合は、認証サーバのみライセンスを登録してください。

(注意)冗長化構成の場合は、全ての認証サーバにライセンスを登録してください。

(注意)ライセンスファイルは編集しないでください。

【 手順 】

- (i)メンテナンスツール左側メニュー > ライセンス管理 をクリック。
- (ii)「参照」ボタンからライセンスファイルを選択し、「次へ」ボタンをクリック。
- (iii)「新しいライセンスを適用する」ボタンをクリック。

バックアップ

PassLogic 認証サーバの全てのデータベースおよび設定情報のバックアップが行えます。ただし、下記情報はバックアップの対象外となります。修正を行った場合、手動でのリストアを実施してください。

特殊ハンドラ設定

`/opt/passlogic/apps/lib/settings/global_setting.php`

pgsql 障害発生時のメール送信設定(冗長化構成時)

`/opt/passlogic/pgsql/data/failover_mail.sh`

SSH 鍵 (2.3 PassLogic をインストールするを参照)

`{PassLogic インストーラディレクトリ}/ssh/authorized_keys`

`{PassLogic インストーラディレクトリ}/ssh/id_rsa`

`{PassLogic インストーラディレクトリ}/ssh/id_rsa.pub`

共通暗号鍵 (2.3 PassLogic をインストールするを参照)

```
{PassLogic インストーラディレクトリ}/lib/plcrypt.conf
PassLogic リバースプロキシ設定
/opt/passlogic/data/conf/xauth_passlogic_00.conf
PassLogic アプリケーションログ
/var/log/passlogic/ 以下
```

【 手順 】

- (i) メンテナンスツール左側メニュー > バックアップ をクリック。
 - (ii) パスワード(リストアの際に必要・半角英数字のみ指定可)を入力し、[送信] をクリック。
 - (iii) バックアップファイルのダウンロードを行う。
- (注意)バックアップファイルのサイズが128MB を超える場合、Web メンテナンス画面からのバックアップファイル取得が失敗します。その場合、コマンドラインからバックアップファイルの作成を行ってください。

コマンドラインからもバックアップファイルを作成することができます。

```
# sh /opt/passlogic/apps/tools/backup.sh {バックアップファイルのパスワード}
```

(注意)バックアップファイルは /opt/passlogic/tmp/passlogicbackup.zip に出力されます。

リストア

PassLogic 認証サーバの全てのデータベースおよび設定情報のリストアが行えます。冗長化構成の環境にリストアを行う場合、下記の【冗長化構成の環境にリストアする際の注意事項】も合わせてご確認ください。

【 手順 】

- (i) メンテナンスツール左側メニュー > リストア をクリック。
- (ii) バックアップファイルを選択し、バックアップの際に設定したパスワードを入力。
- (iii) リストアモードを選択し、[送信]をクリック。

【 リストアモード 】

データベースおよびサーバ固有情報をリストア	全てのデータベースとサーバ固有情報が置き換わります
データベース情報をリストア	全てのデータベースのみ置き換わります
サーバ固有情報をリストア	サーバ固有情報のみ置き換わります
データベースおよびサーバ固有情報をリストア ※冗長化設定を除く	全てのデータベースと以下を除くサーバ固有情報が置き換わります。 /opt/passlogic/data/conf/redundant.conf 冗長化構成時のみ、この項目は表示されます。

また、コマンドラインからもバックアップファイルをリストアすることができます。バックアップファイルを /opt/passlogic/tmp/passlogicbackup.zip にアップロード後、以下のコマンドを実行してください。

```
# sh /opt/passlogic/apps/tools/restore.sh {バックアップファイルのパスワード} [オプション] > /var/log/passlogic/passlogic-restore.log
```

restore.sh のオプションは以下の通りです。

(指定なし)	全てのデータベースとサーバ固有情報が置き換わります
-c	サーバ固有情報のみ置き換わります
-d	データベースのみ置き換わります
-e	全てのデータベースと以下を除くサーバ固有情報が置き換わります。 /opt/passlogic/data/conf/redundant.conf

(注意)「> /var/log/passlogic/passlogic-restore.log」を省略すると、実行結果が標準出力に出力されます。

(注意)リストア実行後、アップロードしたファイルは削除されます。

(注意)実行結果(/var/log/passlogic/passlogic-restore.log 等)にエラー出力がないことを確認してください。

【 冗長化構成の環境にリストアする際の注意事項 】

冗長化構成の環境にリストアする場合、以下の注意事項をご確認ください。

- (i) リストア処理を実行する前に、冗長化構成が構築済である必要があります(「7 冗長化構成」参照)。
- (ii) バックアップを取得した環境と、リストアする環境で認証サーバの IP アドレスが異なる場合、リストアモードは必ず「データベース情報をリストア」又は「データベースおよびサーバ固有情報をリストア※冗長化設定を除く」を選択してください。ライセンスファイルは 2 台の認証サーバで再登録してください。

【 ファイルサイズの注意事項 】

バックアップファイルのサイズが 128MB を超える場合、下記の設定ファイルの修正が必要です。下記はデフォルトの設定値です。バックアップファイルのサイズやサーバ環境に応じて適切な設定値に修正してください。また、設定変更を行った際は必ず Apache の再起動を行ってください。

```
PHP 設定ファイル (/etc/php.ini)
処理サイズに関連する設定
memory_limit 256M (スクリプトが確保できる最大メモリ)
post_max_size 128M (POST データに許可される最大サイズ)
upload_max_filesize 128M (アップロードされるファイルの最大サイズ)
処理時間に関連する設定
max_execution_time 30 (スクリプトが強制終了されるまでの最大時間)
max_input_time 60 (スクリプトが POST、GET などの入力をパースする最大の時間)
```

【 メッセージ/終了コード 一覧 】

リストア完了時のメッセージ(メンテナンス画面)と終了コード(コマンドライン)の一覧です。

メッセージ	終了コード	対応方法
リストアが完了しました。	0	正常終了です。
パスワードが間違っています。もう一度確認して入力してください。	1	入力したパスワードをご確認ください。
バックアップファイルを読み込めませんでした。	2	ファイルが本製品のバックアップファイルであるかご確認ください。
リストアに失敗しました。コマンドラインからリストアしてください。	3	<p>以下をご確認のうえ、コマンドラインからリストアを再実行してください。</p> <ul style="list-style-type: none"> - 本章の【冗長化構成の環境にリストアする際の注意事項】に該当していないこと - リストアを実行したサーバから見て対向のサーバが起動していること
ロックの取得に失敗しました。	4	<p>データベースへの書き込みを伴うバッチ処理が動作中の可能性があります。該当するバッチ処理が動作していないことを確認した後か、数分お待ちいただいた後に、リストアを再実行してください。該当するバッチ処理は以下の通りです：</p> <ul style="list-style-type: none"> - LDAP ID 同期 - 有効期限切れお知らせメール送信 - スタンダード版データ取り込み - CSV 一括登録 (コマンド名: userimport.php) - LDAP 認証連携ユーザ削除スクリプト(コマンド名: passlogic_adsync.php) - ログ削除バッチ (passlogic_log_db_delete.sh) - リストア処理 (リストア処理実行中に、リストア処理を新たに実行する場合)
バックアップファイルのバージョンが異なります。	5	バックアップファイルの取得バージョンがインストールバージョン(/opt/passlogic/VERSION)と同じであるかご確認ください。サービスパック(-SPx)、パッチ(_txxxx)の違いは許容されます。
コンフィグファイルの再生成に失敗しました。	6	サポートまでお問い合わせください。

radiusd サービスの再起動に失敗しました。	7	本章の【冗長化構成の環境にリストアする際の注意事項】に該当していないかご確認ください。
httpd サービスの再起動に失敗しました。	8	
テナントフラグファイルの再生成に失敗しました。	9	
対向へのログファイル転送に失敗しました。	10	
対向のコンフィグファイルの再生成に失敗しました。	106	
対向の radiusd サービスの再起動に失敗しました。	107	
対向の httpd サービスの再起動に失敗しました。	108	
リストア処理が異常終了しました。	上記以外	サポートまでお問い合わせください。

テクニカルサポート

テクニカルサポートの際にサポートスタッフがサポートファイルの取得をお願いする場合があります。

テクニカルサポートのため取得されるファイル・ディレクトリ、DB テーブル

OS の種類(バージョンなど) サーバ設定ファイル(/etc/httpd/conf, /etc/httpd/conf.d, /etc/php.ini, /etc/sysctl.*) PassLogic バージョン情報、および設定ファイル(/opt/passlogic/VERSION, /opt/passlogic/data) ログファイル(/var/log/httpd, /var/log/radius, /var/log/messages, /var/log/passlogic, /var/log/passlogic-pgpool, /opt/passlogic/pgsql/data/serverlog) DB 中の設定情報格納テーブル passlogic_config, passlogic_config2

(注意)ファイルには設定、ログが含まれています。

(注意)ファイルを取得するにはサーバの空き容量が 2GB 以上必要です。

【 手順 】

(i) メンテナンスツール左側メニュー > テクニカルサポート をクリック。

(ii) パスワードを入力し、[送信] をクリック。

ここで指定したパスワードはサポートファイルと合わせてお知らせいただくものになります。

(iii) サポートファイルのダウンロードを行う。

また、コマンドラインからもサポートファイルを取得することができます。

```
# sh /opt/passlogic/apps/tools/support_info.sh {サポートファイルのパスワード}
```

(注意) サポートファイルは /opt/passlogic/tmp/support_info.zip に出力されます

6 分離構成

6.1 ゲートウェイサーバのセットアップ

ゲートウェイサーバには PassLogic インストーラ(install.sh)ではなく、ゲートウェイサーバ用のインストーラ(install_gateway.sh)をお使いください。また、インストールするゲートウェイサーバは、認証サーバと同じバージョンのパッケージに含まれているものをご利用ください。

必要なパッケージのインストール

ゲートウェイサーバ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)
# dnf -y install chrony
# dnf -y install httpd
# dnf -y install mod_ssl
```

ゲートウェイサーバのインストール

認証サーバから下記のファイルをゲートウェイサーバにコピーしてください。

コピー元:

```
{認証サーバの PassLogic インストーラディレクトリ}/install_gateway.sh
```

コピー先:

```
ゲートウェイサーバ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 {認証サーバの IP アドレス または FQDN} {インストールモード}
```

(注意)インストールモードは、以下の数値になります。

PKI 機能利用時:1、PKI 不利用時:0 空白の場合は、0 として実行されます。

(注意)install_gateway.sh は、/etc/httpd/conf.d/passlogic-gw.conf を作成します。このファイルを削除することで、install_gateway.sh 実行前の状態になります。

インストール時に、以下の設定が自動で追加・変更されます。

/etc/httpd/conf/httpd.conf

ServerTokens	Prod
#AddDefaultCharset	コメントアウトして設定値を無効化

ServerSignature	Off
TraceEnable	Off

/etc/httpd/conf.modules.d/00-mpm.conf

LoadModule mpm_prefork_module	有効化
#LoadModule mpm_event_module	コメントアウトして設定値を無効化

/etc/httpd/conf.modules.d/10-h2.conf

#LoadModule http2_module	コメントアウトして設定値を無効化
--------------------------	------------------

/etc/httpd/conf.modules.d/10-proxy_h2.conf

#LoadModule proxy_http2_module	コメントアウトして設定値を無効化
--------------------------------	------------------

PKI 設定の追加

PKI 認証機能を利用する場合は、認証サーバで作成したルート証明書をゲートウェイサーバにコピーする必要があります。(認証サーバがルート証明書を変更した場合、この作業を再度実施ください)

(注意)認証サーバで設定したルート証明書は以下のフォルダに格納されます。

```
/opt/passlogic/data/conf/cert/
```

(注意)上記フォルダを、ゲートウェイサーバの以下のパスに上書き保存してください。

(既存の中身は削除してください)

```
/etc/httpd/conf.d/cert/
```

(注意)Apache を再起動 (設定変更内容を反映)

PassLogic ユーザーインターフェース アクセス確認

下記の URL にアクセスして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。

```
https://{ゲートウェイサーバのサーバ名または IP アドレス}/ui/
```

6.2 ゲートウェイサーバ 接続先の変更

認証サーバアドレス変更後の接続先を指定の上、前項「6.1 ゲートウェイサーバのセットアップ」を参照して、設定ツール `install_gateway.sh` を再実行して下さい。

6.3 ゲートウェイサーバ リカバリ手順

リカバリ対象のゲートウェイサーバに対して、前項「6.1 ゲートウェイサーバのセットアップ」を参照して手順を再度実施してください。

6.4 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と 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。(注意)この場合、PKI は利用できません。

<通信イメージ>

クライアント -[https]- ゲートウェイサーバ -[http]- 認証サーバ

PassLogic 認証サーバ側の設定

内部ネットワークから http でメンテナンスツールや管理ツールにアクセスする場合等、セッション維持を http で実施する必要がある場合は、下記の設定を実施して下さい。(但し、この場合、セッション維持 cookie に secure 属性が設定されなくなります。)

(注意)下記の設定値を変更 (http の場合にも cookie の利用を許可する)

/etc/php.ini

(変更前) session.cookie_secure = 1

(変更後) session.cookie_secure = 0

(注意)Apache を再起動 (設定変更内容を反映)

PassLogic ゲートウェイサーバ側の設定

(注意)下記ファイルを修正 (プロキシ定義を https から http に変更し、SSLProxy 設定を削除する)

/etc/httpd/conf.d/passlogic-gw.conf

変更前:

```
## 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
```

変更後:

```
## 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}/
```

(注意)Apache を再起動 (設定変更内容を反映)

6.5 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

ゲートウェイサーバと PassLogic 認証サーバのどちらとも、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。

(注意)この場合、PKI は利用できません。PKI を利用するモードでインストールした場合は、PKI 設定部分を手動で削除するか、再インストールして下さい。

<通信イメージ>

クライアント -[https]- ロードバランサ -[http]- ゲートウェイサーバ -[http]- 認証サーバ

PassLogic 認証サーバ側の設定

内部ネットワークから http でメンテナンスツールや管理ツールにアクセスする場合等、セッション維持を http で実施する必要がある場合は、下記の実装を実施して下さい。(但し、この場合、セッション維持 cookie に secure 属性が設定されなくなります。)

(注意)下記の設定値を変更 (http の場合にも cookie の利用を許可する)

/etc/php.ini

(変更前) session.cookie_secure = 1

(変更後) session.cookie_secure = 0

(注意)Apache を再起動 (設定変更内容を反映)

PassLogic ゲートウェイサーバ側の設定

(注意)下記ファイルを修正

ポートを 80 番に変更、SSL 設定を削除、プロキシ定義を http に変更、SSLProxy 設定を削除する
/etc/httpd/conf.d/passlogic-gw.conf

変更前:

```
<VirtualHost _default_:443>
    SSLEngine on
    SSLProtocol TLSv1.2
    SSLCipherSuite ALL:!ADH:!EXPORT:!SSLv2:RC4+RSA:+HIGH:+MEDIUM:+LOW
    SSLCertificateFile /etc/pki/tls/certs/localhost.crt
    SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

```
## 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

変更後:
<VirtualHost _default_:80>
    ## 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}/
```

(注意)Apache を再起動 (設定変更内容を反映)

6.6 ゲートウェイサーバアップデート

PassLogic エンタープライズ版 v3.1 系で利用していたゲートウェイサーバを PassLogic エンタープライズ版 v4系で利用する場合は、v3.1.0 SP1 インストールガイド改訂版の「6. 1ゲートウェイサーバのセットアップ」の章をご参照の上、一旦 /etc/httpd/conf.d/ssl.conf をゲートウェイサーバセットアップ前の状態に戻す必要があります。v4 系で利用していたゲートウェイサーバのアップデートの場合は、一旦 /etc/httpd/conf.d/passlogic-gw.conf を削除したうえで、本書の「6. 1ゲートウェイサーバのセットアップ手順」を実施してください。

7 冗長化構成

7.1 概要

Active/Active 構成により PassLogic サーバを二重化した場合、PassLogic 認証サーバ内のデータベースは冗長化構成となります。

冗長化を構成する 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。冗長化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冗長化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

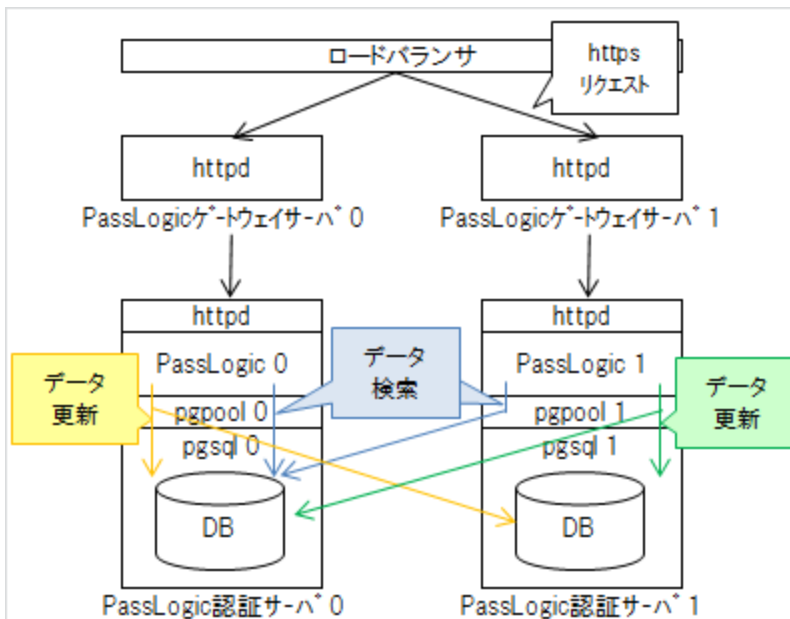
	ネットワーク品質	応答時間		
	ping 応答時間	uid 入力画面	乱数表画面	認証処理
レプリケーション① (同拠点内)	0.6 ms	86 ms	113 ms	130 ms
レプリケーション② (国内別拠点)	10.0 ms	277 ms	752 ms	1,023 ms
レプリケーション③ (国外別拠点)	72.0 ms	2,172 ms	3,320 ms	5,274 ms

(注意)レプリケーション①は弊社環境での ping 応答時間とサービス応答時間の結果です。

(注意)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。

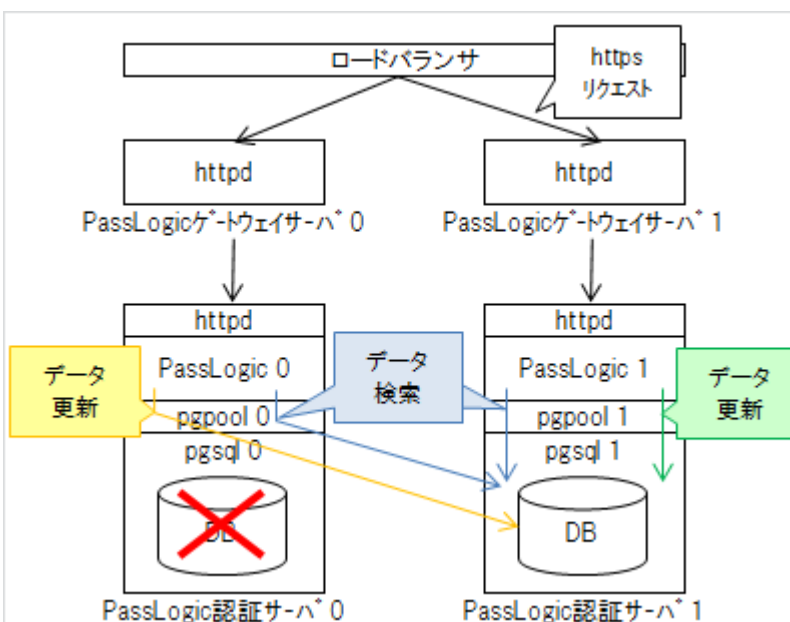
正常稼働

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(pgsql 0, pgsql 1) 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。



DB (pgsql) 切断発生

pgpool が DB(pgsql)へ接続できない場合、データの書き込みとデータ参照は、接続できる片方の DB(pgsql)だけに行われます。



(注意)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。切り離れたことは、後述の アラートメール および pgpool ログファイル、監視 API で把握することができます。DB 切断発生を検知するために、アラートメールの設定、pgpool ログファイルの監視を実施してください。

(注意) DB 切断の主な原因は、対向サーバ/DB サービス再起動等、運用上の操作によるもの、認証サーバ間ネットワークの一時的(1, 2分程度)な障害、サーバ故障、disk full、サーバ処理負荷の過多によるタイムアウト等です。

(注意) 対向側 DB が切断された状態であっても、PassLogic 自体は両系とも稼働している場合があります。その状態で、両系の PassLogic へのアクセスが発生すると、相互の DB に異なる情報が更新されてしまいます。復旧させる際には、片系の DB をマスターとして DB リカバリを実施します。そのため障害発生後すぐに、ロードバランサの振り分けが片系に PassLogic に固定されるように設計にしてください(DB が切断された側の PassLogic に対するアクセスを停止するように設計してください)。

(注意) DB 切断が起きた場合は、管理画面での DB 接続状態が正常状態表示であった場合でも、必ず DB リカバリ処理を実行してください。

(注意)「pgpool 障害」の場合は、PassLogic ユーザログイン画面にその旨のエラーが表示されます。

「pgpool 障害」の監視をする場合には、ユーザログイン画面の HTML 内容を取得することで判断できません。なお、ゲートウェイサーバは認証サーバに対するリバースプロキシですので、ゲートウェイサーバを導入されている場合は、ゲートウェイサーバに対して上記ログイン画面の確認でも同様な結果となります。

メインサーバ・サブサーバ

PassLogic では、設定により定期的な LDAP ID 同期処理および PassLogic 認証用有効期限メール送信処理を行うことができます(運用管理ガイド・「ドメイン管理」LDAP ID 同期、および「ポリシー設定」PassLogic 認証」参照)。これらの機能を有効にした場合、cron.dによりバッチ処理が実行されます。冗長化構成ではこれらのバッチ処理は片系の認証サーバでのみ実施されます。バッチ処理を実行する認証サーバをメインサーバ、実行しない認証サーバをサブサーバと呼びます。

(認証サーバ0、認証サーバ1とは別の概念となります。)

メインサーバ・サブサーバは、インストールおよびリカバリの処理を行ったサーバをメインサーバ、対向サーバをサブサーバとして自動で設定が行われます。また、メンテナンスツールから任意のタイミングで切り替えを行うことが可能です。

7.2 冗長化構成のセットアップ

①PassLogic 認証ソフトウェア インストール

「2 インストール」を参照して、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。なお、データベース間の齟齬を防ぐため、冗長化設定完了まで PassLogic への下記アクセスをしないでください。

- ・ユーザ向けログイン画面、管理画面、メンテナンス画面、API へのアクセス(死活監視含む)
- ・cronによる定期自動処理(LDAP ID 同期、CSV ユーザー一括登録、有効期限前の自動メール送信処理)

誤ってアクセスした場合はアンインストール後に再インストールしてください。

②データベース 冗長化設定

認証サーバ 0 の下記のファイルを編集して、冗長化対象サーバを定義してください。

```
/opt/passlogic/data/conf/redundant.conf
```

編集箇所:

```
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}
```

認証サーバの IP アドレスは、認証サーバに接続されたネットワークデバイスに割り振られるもの(ip コマンドで表示される IP アドレス)を設定してください。

次に、認証サーバ 0 の下記ファイルの FROM と TO のメールアドレスを編集して、障害時のアラートメール送信元、および送付先を設定してください。このメール送信は postfix を利用して行っています。お客様の環境に応じて postfix の設定をお願いします。

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

編集例:

```
#!/bin/sh  
  
FROM="DB_system@passlogy.com"  
TO="admin@passlogy.com"  
  
...以降は省略...
```

以上の設定が完了したら、認証サーバ 0 で下記の冗長化設定コマンドを実行してください。このコマンドを実行する認証サーバ 0 がバッチ処理を行うメインサーバに設定されます。メインサーバはメンテナンスツールにて後から変更可能です。

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

③データベース 冗長化状況確認

管理アカウント「admin」の作成を、いずれか一方の認証サーバだけで実施してください。

その後、認証サーバ0と認証サーバ1 両方のメンテナンスツールにログインし、メイン画面で「DB Status」の欄にある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。

メンテナンスツール URL:

```
https:// {認証サーバ名または IP アドレス}:12443/passlogic-maintenance/
```

(注意)メンテナンスツールのログイン手順は、「2.6 メンテナンスツールに初めてアクセスする」をご覧ください。

④ライセンス登録

認証サーバ0と認証サーバ1 両方のメンテナンスツールでライセンスファイルを登録してください。

(注意)ライセンスファイル登録手順は、「5.5 メンテナンス> ライセンス管理」をご覧ください。

冗長化構成を設定した後に、「認証サーバ1 台構成」および「分離構成」に戻す場合は、一旦PassLogicのアンインストールを実施して、再度インストールをしてください。

7.3 PassLogic 認証サーバ 停止・起動手順

システムメンテナンス等で、冗長化構成の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 片系のみ OS 停止する場合、事前に停止対象認証サーバへのネットワークアクセス振り分けを停止してください。

② 【停止対象サーバ】プロセス停止

```
# systemctl stop httpd
# systemctl stop radiusd
# systemctl stop passlogic-pgpool
# systemctl stop passlogic-pgsql
```

③ 【稼働中サーバ】DB 切り離し状態確認

稼働中(上記手順①を実施していない方のサーバ)のメンテナンスツールにログインして、メイン画面で停止対象サーバのデータベースが「Node Down OR Not Connected」であることを確認してください。

④ 【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

冗長化されていない状態でアクセスされた場合、片系の DB のみが更新されてしまい DB 不整合が発生します。(注意)ユーザや管理者のアクセスの他、定期監視、cron 等による自動処理にもご注意ください。OS 停止・起動の際は、**必ずデータベースリカバリ処理を実行してください。**

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

メンテナンスツールにログインして、メイン画面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。起動対象サーバのデータベース欄に「recovery」リンクが表示されていない場合は、「detach」リンクをクリックして起動対象サーバのデータベースを切り離し状態にしますと、「recovery」リンクが表示されます。こちらの「recovery」リンクをクリックしてください。

*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 を起動後に上記の手順を実施してください。

(注意)「8.2 冗長化構成時の注意事項」「冗長化構成リカバリ処理実行時の注意事項」を合わせてご参照ください。

7.4 認証サーバリカバリ手順

認証サーバ0に障害が発生した場合

障害を検知し pgsq1 が切り離されると、リカバリ処理をするまで切り離された状態が継続します。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は本手順でリカバリを実施してください。

(注意)リカバリ処理を実施する前に障害の原因を解消してください

(注意)自動的にリカバリ処理を実行することはありません

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のメンテナンスツールにログインし、メイン画面「DB Status」欄 DB0が「Node Down OR Not Connected」と赤く表示されていることを確認し、「メンテナンスツール左側メニュー > 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。

(注意)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がインストールされていない場合、インストールしてください。詳細手順は「2 インストール」の項目を参照してください。

(注意)リカバリ手順では、冗長化設定コマンド(`passlogic_redundant.sh`)を実行しないでください。

(注意)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。

(注意)認証サーバ0でPassLogicの再インストールする場合は、SSH鍵および共通暗号鍵の再作成は行わないでください。下記を参考に、認証サーバ1のSSH鍵ファイルと共通暗号鍵ファイルを、認証サーバ0にコピーし、認証サーバ0でインストールコマンドを実行してください。

コピー対象ファイル(SSH鍵3ファイル):

```
/home/passlogic/.ssh/authorized_keys
/home/passlogic/.ssh/id_rsa
/home/passlogic/.ssh/id_rsa.pub
```

コピー先:

```
{再構築する認証サーバ0のPassLogicインストーラディレクトリ}/ssh/
例: /usr/local/src/passlogic-ent-x.x.x/ssh/
```

コピー対象ファイル(共通暗号鍵1ファイル):

```
/opt/passlogic/lib/plcrypt.conf
```

コピー先:

```
{再構築する認証サーバ0のPassLogicインストーラディレクトリ}/lib/
例: /usr/local/src/passlogic-ent-x.x.x/lib/plcrypt.conf
```

④【認証サーバ1】認証サーバ0リカバリ

認証サーバ1のメンテナンス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」と緑色で表示されます。

(注意)リカバリ処理中、認証サービスが全断します。

(注意)[recovery]リンクをクリックした場合、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を認証サーバ1から認証サーバ0へコピーします。(コピーされるファイルの詳細は7.6 メンテナンス(冗長化構成)【rebuild_p1】をご参照ください。)

(注意)リカバリ処理を実行した認証サーバがメインサーバになります。

(注意)ログファイルに差異が発生している場合があります。認証サーバ1のログで同期を行いたい場合、「7.6 メンテナンス(冗長化構成)」ご参照の上、ログの強制同期を実行してください。

⑤【認証サーバ0】稼働状況の確認

認証サーバ0のメンテナンス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」と緑色で表示されていることを確認してください。

⑥メインサーバ・サブサーバ設定(任意)

リカバリ実行後は、[recovery]リンクをクリックした復旧元の認証サーバ1がメインサーバに、復旧先の認証サーバ0がサブサーバになります。LDAP ID同期処理およびPassLogic認証用有効期限メール送信処理はメインサーバ(本章の例の場合、認証サーバ1)が行います。認証サーバ0で同期処理・メール送信処理を実行するには、7.6 メンテナンス(冗長化構成)【メインサーバ・サブサーバ切り替え】をご参照の上、認証サーバ0をメインサーバに設定してください。

認証サーバ1に障害が発生した場合

「認証サーバ0に障害が発生した場合」の手順内の「認証サーバ0」と「認証サーバ1」を読み替えてください。

7.5 認証サーバ 切り離し/再接続 手順

サーバの OS メンテナンスなどで 認証サーバのデータベースを強制的に切り離し、OS 再起動後に切り離れたデータベースを再接続する場合の手順です。

切り離し/再接続 対象が認証サーバ 1 の場合

①【ロードバランサ】 リクエスト振分設定を更新

ユーザからのリクエストが認証サーバ 0 にだけ振り分けられるように設定を変更してください。

(ゲートウェイサーバ 1 の httpd プロセスの停止 または ロードバランサの振り分け先の設定変更 など)

また、認証サーバ 1 の管理ツールおよびメンテナンスツールへのログインも行わないようにしてください。

い。

(注意)以降の手順を実施する前に、必ず認証サーバ 0 と認証サーバ 1 の各メンテナンスツールからバックアップを取得してください。

②【認証サーバ 0】 認証サーバ 1 データベースを切り離し

認証サーバ 0 にログイン後、メンテナンスツールのメイン画面から「DB Status DB1」の「detach」リンクをクリックしてください。

(注意)切り離しが正常終了すると DB Status が「Node Down OR Not Connected」と表示されます。

(注意)切り離し直後 /opt/passlogic/pgsql/data/failover_mail.sh に設定した宛先にメールが送信されます。

③【認証サーバ 1】 メンテナンス作業

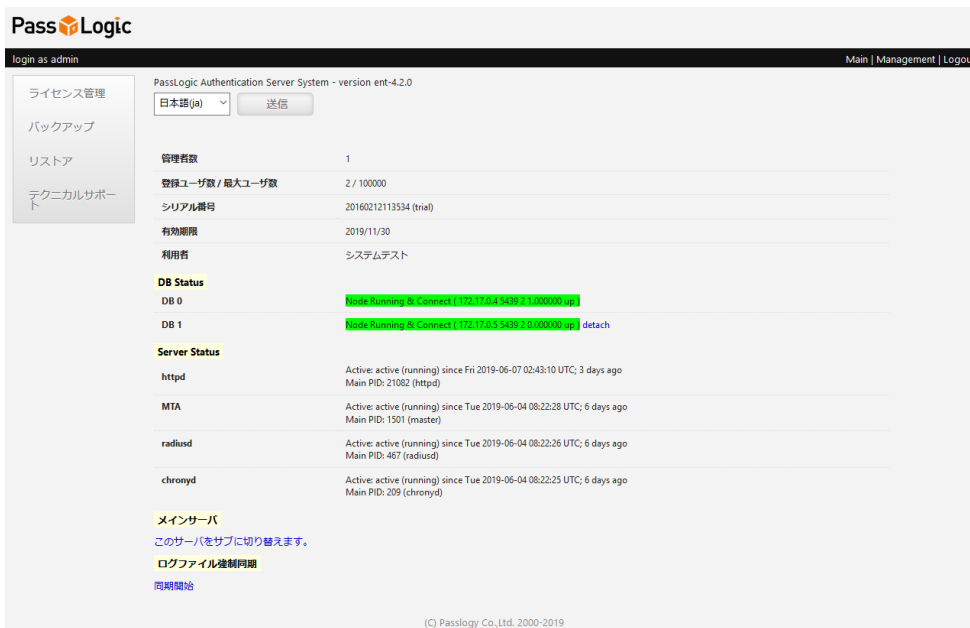
認証サーバ 1 の OS 更新等、メンテナンス作業を行ってください。

④【認証サーバ 0】 認証サーバ 1 データベースをリカバリ

認証サーバ 0 にログイン後、メンテナンスツールのメイン画面から「DB Status DB1」の[recovery]リンクをクリックしてください。

(注意)リカバリ処理中、認証サービスが全断します。

(注意)リカバリが正常終了すると下図のように DB Status が「Node Running & Connect」と緑色で表示されます。



PassLogic Authentication Server System - version ent-4.2.0

日本語(ja) 送信

管理用数 1

登録ユーザ数 / 最大ユーザ数 2 / 100000

シリアル番号 20160212113534 (trial)

有効期限 2019/11/30

利用者 システムテスト

DB Status

DB 0 Node Running & Connect (172.17.0.4 5439 2 1.000000 up)

DB 1 Node Running & Connect (172.17.0.5 5439 2 0.000000 up) detach

Server Status

httpd Active: active (running) since Fri 2019-06-07 02:43:10 UTC; 3 days ago
Main PID: 21082 (httpd)

MTA Active: active (running) since Tue 2019-06-04 08:22:28 UTC; 6 days ago
Main PID: 1501 (master)

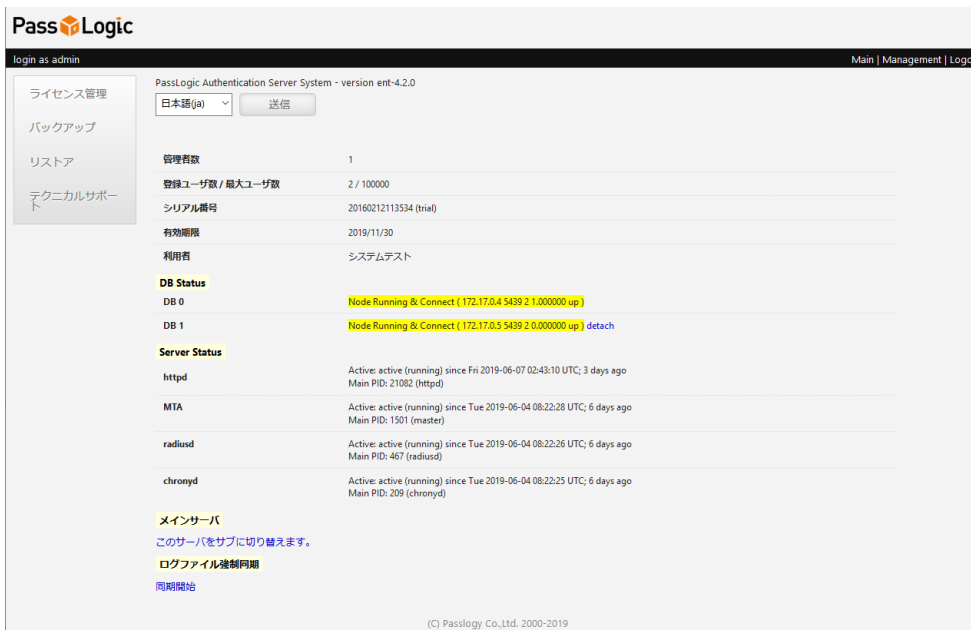
radiusd Active: active (running) since Tue 2019-06-04 08:22:26 UTC; 6 days ago
Main PID: 467 (radiusd)

chronyd Active: active (running) since Tue 2019-06-04 08:22:25 UTC; 6 days ago
Main PID: 209 (chronyd)

メインサーバ
このサーバをサブに切り替えます。
[ログファイル強制同期](#)
[同期開始](#)

(C) Passlogy Co.,Ltd. 2000-2019

リカバリ処理を実施せずに認証サーバ0を再起動すると下図のように DB Status が黄色で表示されます。この場合再度②【認証サーバ0】認証サーバ1 データベースの切り離しを行い、リカバリを実施してください。



PassLogic Authentication Server System - version ent-4.2.0

日本語(ja) 送信

管理用数 1

登録ユーザ数 / 最大ユーザ数 2 / 100000

シリアル番号 20160212113534 (trial)

有効期限 2019/11/30

利用者 システムテスト

DB Status

DB 0 Node Running & Connect (172.17.0.4 5439 2 1.000000 up)

DB 1 Node Running & Connect (172.17.0.5 5439 2 0.000000 up) detach

Server Status

httpd Active: active (running) since Fri 2019-06-07 02:43:10 UTC; 3 days ago
Main PID: 21082 (httpd)

MTA Active: active (running) since Tue 2019-06-04 08:22:28 UTC; 6 days ago
Main PID: 1501 (master)

radiusd Active: active (running) since Tue 2019-06-04 08:22:26 UTC; 6 days ago
Main PID: 467 (radiusd)

chronyd Active: active (running) since Tue 2019-06-04 08:22:25 UTC; 6 days ago
Main PID: 209 (chronyd)

メインサーバ
このサーバをサブに切り替えます。
[ログファイル強制同期](#)
[同期開始](#)

(C) Passlogy Co.,Ltd. 2000-2019

(注意)[[recovery](#)]リンクをクリックした場合、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を認証サーバ0 から認証サーバ1 へコピーします。(コピーされるファイルの詳細は 7.6 メンテナンス(冗長化構成)【[rebuild_p1](#)】をご参照ください。)

(注意)リカバリ処理を実行した認証サーバがメインサーバになります。

(注意)ログファイルに差異が発生している場合があります。認証サーバ0 のログで同期を行いたい場合、「7.6 メンテナンス(冗長化構成)」ご参照の上、ログの強制同期を実行してください。

⑤ 【認証サーバ 1】稼働状況の確認

認証サーバ 1 のメンテナンス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」と緑色で表示されていることを確認してください。

⑥ 【認証サーバ 0/1】 ユーザリクエスト受付再開

ユーザからのリクエストをいずれの認証サーバでも受け付けられるように設定を変更してください。

切り離し/再接続 対象が認証サーバ 0 の場合

「認証サーバ 1 の場合」の手順内の「認証サーバ 0」と「認証サーバ 1」を読み替えてください。

7.6 メンテナンス（冗長化構成）

「5.5 メンテナンス」に記載している項目以外の下記項目について記載します。

- (v) データベースの再同期
- (vi) メインサーバ・サブサーバ切り替え
- (vii) ログファイル強制同期

データベースの再同期

メンテナンスツールから対向サーバの切り離しおよび再接続を行うことができます。ソフトウェアのアップデートやリカバリなどを行う際、ご利用いただけます。具体的な手順に関しましては、「7.5 認証サーバ 切り離し/再接続 手順」の章をご参照ください。

【 切り離し手順 】

- (i) メンテナンスツール > メイン画面を表示。
- (ii) メイン画面「DB Status」欄 切り離したい DB の[detach]リンクをクリック。

【 再接続手順 】

- (i) メンテナンスツール > メイン画面を表示。
- (ii) メイン画面「DB Status」欄 再接続したい DB の[recovery]リンクをクリック。

また、コマンドラインからもリカバリを行うことができます。コマンドラインから冗長化構成を再構築する場合、**復旧元の認証サーバ**で以下の3つのコマンドを利用します。コマンドは1つずつ、正常終了を確認しながら下記の順番で全て実行する必要があります。各コマンドの終了コードでは正常終了の判定は出来ないので注意してください。

手順は以下の3つになります。

rebuild_p1

復旧元のデータを復旧先に転送します。その間復旧元の認証サービスは停止しません。

rebuild_p2

復旧元のデータベースを停止し、再度データを復旧先に転送します。**この間は復旧元の認証サービスも停止します**。データ転送後、復旧元の認証サービスを再開します。このコマンドが正常終了しなかった場合、コマンド rebuild_p1 から実行しなおす必要があります。

rebuild_p3

復旧先の認証サービスを再開します。

【 rebuild_p1 】

設定情報を復旧元から復旧先へコピーします。復旧元のデータベースを停止せずにコピーしますので、復旧先のデータベースはまだ利用可能な状態ではありません。

```
# /opt/passlogic/apps/tools/rebuild_p1
```

1. 復旧先との疎通確認
2. 復旧先へファイルコピー
 - /opt/passlogic/pgpool/etc/pgpool.conf
 - /opt/passlogic/data/conf/redundant.conf
3. 復元元のディレクトリ/opt/passlogic/data/配下にある設定ファイルを
 - /home/passlogic/配下の一時領域に書き出し
4. 3. で一時領域に書き出したファイルを、復旧先の一時的領域にコピー
5. 4. で転送した復旧元設定ファイルから、ロゴイメージファイルを復旧先に配置。
 - /opt/passlogic/data/logo_images.png(存在する場合)
6. 4. で転送した復旧元設定ファイルから、ライセンスファイルを復旧先に配置
 - /opt/passlogic/data/conf/license-ent.asc
7. 復旧元の pgpool から復旧先の postgres を切り離し
8. 復旧先の httpd 停止
9. 復旧先の pgpool 停止
10. 復旧先の postgres を停止
11. 復旧先のキャッシュファイル削除
12. 復旧先のメインサーバフラグファイル削除
 - /opt/passlogic/data/conf/flag/main_server
13. 復旧先の冗長化設定ファイル作成
 - /opt/passlogic/data/conf/flag/redundant
 - /opt/passlogic/data/conf/flag/redundant_status
 - /opt/passlogic/data/conf/flag/server_0
 - /opt/passlogic/data/conf/flag/server_1
 - /opt/passlogic/data/conf/flag/my_server
 - /opt/passlogic/data/conf/flag/other_server
14. 復旧元のメインサーバフラグファイル作成
 - /opt/passlogic/data/conf/flag/main_server
15. 復旧元の cron 設定再読み込み
16. 復旧元の 不要なセッション情報を削除
17. 復旧元の postgres データ領域を復旧先にコピー

1. - 17. の処理で、エラーが発生した場合、処理はエラーが発生した箇所で中断します。

下記のように、:ok が最後まで出れば、正常終了です。

```
# /opt/passlogic/apps/tools/rebuild_p1
remote_ping
:ok
copy_pgpool_redundant_conf
:ok
export_settings
:ok
transfer_settings
:ok
deploy_remote_conf
:ok
deploy_remote_license
:ok
detach_remote
:ok
remote_httpd_down
:ok
remote_pgpool_down
:ok
remote_pgsqldb_down
:ok
remote_remove_cache
:ok
remote_main_server_down
:ok
remote_create_redundant_files
:ok
main_server_up
:ok
reloadCronsetting
:ok
cleanup_session_table
:ok
copy_pgsqldb_archives_data_dirs rsync_lax
:ok
```

【 rebuild_p2 】

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を復旧元から復旧先にコピーします。復旧元のデータベースを停止しますので、処理が終了するまで認証サービスが停止します。(停止時間の目安は 10~20 秒程度です。)

```
# /opt/passlogic/apps/tools/rebuild_p2
```

1. 復旧元の pgpool 停止
2. 復旧元の postgres 停止
3. 復旧元の postgres データ領域を復旧先にコピー
4. 復旧元の postgres 起動
5. 復旧先の postgres 起動
6. 復旧元の pgpool 起動
7. 復旧元の pgpool と復旧元・復旧先の postgres との接続状態を表示

1.-7.の処理で、途中でエラーが発生した場合でも、処理は中断せず、残りの処理を継続します。

下記のように、DB0 is attached および DB1 is attached が表示された場合、正常終了しています。

```
# /opt/passlogic/apps/tools/rebuild_p2
:ok
:ok
DB0 is attached
DB1 is attached
```

【 rebuild_p3 】

復旧先の認証サービスを再開します。

```
# /opt/passlogic/apps/tools/rebuild_p3
```

1. 復旧先の pgpool を起動
2. 復旧先のメインサーバフラグファイル削除
3. 復旧先の連携設定の再作成
4. 復旧先の radiusd 再起動
5. 復旧先の httpd 起動

下記のように、:ok が最後まで出力されれば、正常終了です。

```
# /opt/passlogic/apps/tools/rebuild_p3
remote_pgpool_up
:ok
remote_main_server_down
:ok
remote_recreate_setting
:ok
remote_radiusd_restart
:ok
remote_httpd_up
:ok
reloadTenant
:ok
```

メインサーバ・サブサーバ切り替え

メインサーバ・サブサーバの設定は、インストール時、リカバリ実行時に自動で行われます。また、メンテナンス画面から任意のタイミングで切り替えを行うことが可能です。

【 メインサーバへの切り替え手順 】

- (i)メンテナンスツール > メイン画面を表示。
- (ii)メイン画面「サブサーバ」表示の下にある[このサーバをメインに切り替えます。]リンクをクリック。
- (iii)「このサーバをメインに切り替えます。よろしいですか？」に[OK]をクリック。

【 サブサーバへの切り替え手順 】

- (i)メンテナンスツール > メイン画面を表示。
- (ii)メイン画面「メインサーバ」表示の下にある[このサーバをサブに切り替えます。]リンクをクリック。
- (iii)「このサーバをサブに切り替えます。よろしいですか？」に[OK]をクリック。

また、コマンドラインからも切り替えを行うことができます。

```
# /opt/passlogic/apps/tools/main_server.sh [n]
```

オプションは下記の通りです。

0	実行したサーバをサブサーバに、対向サーバをメインサーバに切り替えます。
1	実行したサーバをメインサーバに、対向サーバをサブサーバに切り替えます。

ログファイル強制同期

PassLogic4.0.1以降は、管理画面のログ閲覧機能にログファイルを使用しています。冗長化構成の場合、メンテナンスや障害など片側の停止に際して両系のログファイルの不一致が発生する場合があります。ログの不一致が発生した状態でも PassLogic の機能は正常に動作しますが、両系でログファイルを一致させた場合にメンテナンスツールから強制同期を行うことが可能です。強制同期は実行したサーバのログファイルを正とし、対向サーバのログファイルの上書きを行います。

【 手順 】

- (i) メンテナンスツール > メイン画面を表示。
- (ii) メイン画面「ログファイル強制同期」表示の下にある [同期開始]リンクをクリック。

また、コマンドラインからも強制同期を行うことができます。

```
# /opt/passlogic/apps/tools/log_transfers
```

7.7 移設手順（冗長化構成）

冗長化構成の認証サーバを移設する手順について説明します。

移設作業は、以下5つ手順で実施することができます。

- ① 移設元認証サーバよりバックアップの取得および必要ファイルの用意
- ② 移設先サーバに PassLogic を新規インストール冗長化構成構築
- ③ 移設先のサーバにバックアップファイルをリストア
- ④ passlogic_config の設定

（注意）認証サーバの IP アドレスが変更となる場合、RADIUS 連携機器の設定を変更する必要があります。

（注意）RADIUS 連携機器の IP アドレスが変更となる場合、移設前の RADIUS 機器の登録内容をご参照の上、新規に RADIUS 機器の登録を実施してください。詳細は運用管理ガイド「RADIUS 設定」の項をご参照ください。

①移設元認証サーバよりバックアップの取得および必要ファイルの用意

【メンテナンス画面から、バックアップファイルの取得】

「5.5 メンテナンス>バックアップ」をご参照の上、移設元の認証サーバよりバックアップファイルを取得してください。（バックアップファイルはメイン・サブサーバいずれで取得しても問題ありませんが、通常はメインサーバから取得してください。）

【その他の必要ファイルの用意】

ライセンスファイルの用意、および移設元でインストール時に設定した以下のファイル群を移設元の認証サーバ 0、認証サーバ 1 それぞれから取得してください。

SSH 鍵3ファイル

```
/home/passlogic/.ssh/authorized_keys  
/home/passlogic /.ssh/id_rsa  
/home/passlogic/.ssh/id_rsa.pub
```

特殊ハンドラ設定ファイル

pgsql 障害発生時のメール送信設定ファイル

```
/opt/passlogic/pgsql/data/failover_mail.sh
```

```
/opt/passlogic/apps/lib/settings/global_setting.php
```

テンプレートファイル

```
/opt/passlogic/apps/passlogic-lang.xml
```

```
/opt/passlogic/apps/passlogic-log.xml
```

```
/opt/passlogic/apps/admin/tmpl/json/userimport.json
```

```
/opt/passlogic/配下で拡張子が ihtml.php であるファイル
```

上記のファイルのうち、カスタマイズしているファイルはバックアップが必要です。

②移設先サーバに PassLogic を新規インストール冗長化構成構築

【移設先認証サーバ PassLogic インストール前準備】

移行先認証サーバに PassLogic がインストールされていた場合、事前にアンインストールしてください。「2.3 PassLogic をインストールする」をご参照の上、PassLogic パッケージを移設先に展開してください。以下の説明では、/usr/local/src 配下にインストーラ・ディレクトリが展開してある前提で説明します。

SSH 鍵 3 ファイルをインストーラ・ディレクトリに配置

移設元認証サーバより取得した SSH 鍵3ファイルを、以下のインストーラ・ディレクトリにコピーしてください。(コピー先ディレクトリには同名のデフォルト SSH 鍵ファイル3つが既に存在しますが、上書きコピーしてください。)

```
/usr/local/src/passlogic-ent-x.x.x/ssh/
```

【インストール実行】

「2.3 PassLogic をインストールする」をご参照の上、PassLogic のインストールを移設先の認証サーバ 2 台で実施してください。インストール前準備の操作で、SSH 鍵、共通暗号鍵のインストール設定は実施済の為、SSH 鍵の再作成、および共通暗号鍵の再作成は行わないでください。また、「2.6 メンテナンスツールに初めてアクセスする」、「2.7 ライセンスを登録する」で説明されている手順は、移行先の認証サーバに冗長化構成をセットアップした後に行いますので、この段階では実施しないでください。

【各種ファイル配置】**特殊ハンドラ設定ファイル配置**

移設元で取得した特殊ハンドラ設定ファイルを移設先認証サーバ0, 1の同ファイルに上書きコピーし、ファイルの所有者・グループ、ファイルの権限を以下の通りに設定してください。

ファイル名	/opt/passlogic/apps/lib/settings/global_setting.php
所有者:グループ	root:root
権限	644

テンプレートファイル配置

移設元で取得したテンプレートファイルを移設先認証サーバ0, 1の同ファイルに上書きコピーし、ファイルの所有者・グループ、ファイルの権限を以下の通りに設定してください。(テンプレートファイルをカスタマイズしている場合のみ必要な手順です。)

所有者:グループ	root:root
権限	644

また、テンプレートファイルをコピー後以下の2ファイルを削除してください。

```
/opt/passlogic/tmp/passlogic-lang.cache  
/opt/passlogic/tmp/passlogic-log.cache
```

【ミドルウェアの設定ファイル httpd.conf, ssl.conf, php.ini 等の確認】

OS が提供するミドルウェアの設定ファイルが移設前のものと同じであることを確認してください。

```
/etc/httpd/conf/httpd.conf  
/etc/httpd/conf.d/ssl.conf  
/etc/php.ini  
その他(SSL 証明書, カスタマイズ設定ファイル等)
```

【移設先認証サーバの冗長化構成のセットアップ】

「7.2 冗長化構成のセットアップ」をご参照の上、移行先認証サーバの冗長化構成をセットアップし、データベース冗長化状況確認、ライセンス登録を実施してください。

pgsql 障害発生時のメール送信設定ファイル配置

「7.2 冗長化構成のセットアップ」手順にあるアラートメール送信設定は、移設元で取得したメール送信設定を移設先認証サーバ0, 1の同ファイルに上書きコピーし、ファイルの所有者・グループ、ファイルの権限を以下に設定することで行ってください。

ファイル名	/opt/passlogic/pgsql/data/failover_mail.sh
所有者:グループ	passlogic:passlogic
権限	755

アラートメール送信は OS 付属の Postfix を利用します。管理画面で設定するメール送信設定とは別に、移設先のネットワーク環境に応じて適切に Postfix が設定されている必要があります。

データベース冗長化状況確認

「7.2 冗長化構成のセットアップ」手順にあるデータベース冗長化状況確認には、管理アカウント「admin」が必要になります。管理アカウントの作成方法は、「2.6 メンテナンスツールに初めてアクセスする」をご参照ください。

③移設先のサーバにバックアップファイルをリストア

「5.5 メンテナンス>リストア」をご参照の上、移設先認証サーバのメンテナンス画面より、移設元で取得したバックアップファイルをリストアします。

リストアモードは、「データベースおよびサーバ固有情報をリストア※冗長化設定を除く」を選択してください。

メンテナンス画面で「DB Status」の欄にある DB0 と DB1 のデータベースが「Node Running & Connected」と緑色で表示されている状態でリストアを実施してください。「Node Running & Connected」が黄色で表示されている、あるいは「Node Down OR Not Connected」と赤色で表示されている場合は、リストアを実施する前に、「7.5 認証サーバ切り離し・再接続手順」をご参照の上、データベースの再同期処理を実施してください。

リストアモードに「データベースおよびサーバ固有情報をリストア」設定してリストアした場合、正常なリストアが行えません。移行先の認証サーバにて「②移設先サーバに Passlogic を新規インストール・冗長化構成構築」の手順からやり直しを行ってください。

④passlogic_config の設定

移行元で設定情報を読み込む DB テーブルを切り替えていた場合、移行先でも同様に passlogic_config の設定を行ってください。（通常は、認証サーバ 0, 認証サーバ 1 共に同一の設定を使用するため passlogic_config の再設定は必要ありません。）

8 注意事項

8.1 PassLogic 認証サーバ利用全般

IE の互換表示を使用する場合の注意点

IE の下位互換表示機能を使用している場合、PassLogic の表示が崩れてしまいます。以下の設定をすることで適切な表示とすることが可能です。

(注意)互換表示設定 ON での PassLogic の利用はサポート対象外です。あくまでも参考情報となります。

編集対象ファイル

```
/opt/passlogic/apps/user/tmpl/html_header.ihtml.php
```

更新方法

```
12 行目      <meta charset="utf-8">
追記→      <meta http-equiv="X-UA-Compatible" content="IE=edge">
13 行目      <meta name="copyright" content="Secured by PassLogic">
```

注意事項

- ・対象ファイルは文字コード utf-8、改行コード LF で保存してください。
- ・対象ファイルを更新した場合、PassLogic のバージョンアップ時に更新内容はリセットされます。

更新内容についての情報

[https://msdn.microsoft.com/ja-jp/library/ff955275\(v=vs.85\).aspx](https://msdn.microsoft.com/ja-jp/library/ff955275(v=vs.85).aspx)

[https://msdn.microsoft.com/ja-jp/library/Cc288325\(v=VS.85\).aspx](https://msdn.microsoft.com/ja-jp/library/Cc288325(v=VS.85).aspx)

PKI 利用時の制限事項

PKI クライアント認証を利用する場合、L4 ロードバランサをご利用ください。また、https の終端を認証サーバで行ってください。

(注意)SSL 通信のハンドシェイク時にクライアント証明書の要求がサーバ側から送られてきます。SSL 通信の終端での証明書提出ができる設定にしてください。ロードバランサ上でクライアント証明書の提出が可能で、リクエストヘッダの『X-CLIENT-CERT』に証明書を乗せることが可能でしたら、L4 以外のロードバランサも利用可能です。

TLS1.3 非サポート

PassLogic では TLSv1.3 をサポート対象としていません。Apache の設定変更をする際には、2.4 Apache 推奨設定の(注意)をご確認ください。

ハードディスク容量およびハードウェア障害、ミドルウェア障害の監視

本製品では冗長化構成時、pgpool が pgsql と接続できない場合、障害のあった pgsql を切り離し、縮退運用に切り替わります。しかし、ハードディスク容量が100%に達した場合や、ハードディスク障害発生時、pgsql の切り離しが行われず、サービス全断に陥る場合があります。別途ハードディスク残量やハードウェア障害の監視を実施してください。

ハードディスク容量監視用に、ディスク容量をチェックし、制限値を超えた場合メール通知をするツールを用意しています。制限値やメール設定を変更の上、cron 設定などで定期実行を行うと、ハードディスク容量のオーバーフローを事前に検知しサービス全断を防止することが可能です。

```
/opt/passlogic/apps/tools/diskchk.sh
```

また、DB およびミドルウェアの障害検知としまして API 経由での監視を行うことが可能です。「5.2 監視 API」をご確認の上、監視を実施してください。

PassLogic for Windows Desktop の制限事項

以下のことを PassLogic for Windows Desktop で行うことはできません。

(注意) PKI 認証ポリシーのユーザのログイン制御

PKI 認証機能が有効なポリシーのユーザでログインする場合、証明書を要求することなくログインします。

(注意) ゲスト PC のリモートデスクトップ(RDP)アプリでのアクセス認証

ゲスト PC の RDP アプリからホスト PC へのアクセス認証は、Windows 標準認証となります。

初回アクセス認証成功後、ホスト PC のログイン画面が表示され、これ以後のログイン認証は本製品が適用されます。

(注意) AD の ID 認証連携での初回ログイン不可

本製品で PassLogic 認証を行う際、ユーザが PassLogic サーバに登録されている必要があります。

AD の ID 認証連携設定されている場合は、以下いずれの方法で事前にユーザを登録する必要があります。

- ① ユーザー一括登録機能を利用してユーザを登録。
- ② PassLogic サーバ UI でログイン成功。

(注意) PassLogic for Windows Desktop を用いた PassLogic パスワードの変更

Ctrl+Alt+Del キー押しで「パスワード変更」では、通常の Windows パスワード変更となります。

PassLogic パスワードの変更は、PassLogic サーバ UI にログインしてから変更を行ってください。

(注意) PassLogic 認証のオフライン認証データの有効期限設定

PassLogic 認証のオフライン認証データに有効期限はなく、保存件数分の認証を行えます。

サーバ管理者が必要に応じて、オフライン認証データ件数(デフォルトで 1000 件)で調整してください。

オフライン認証有効の場合、オンライン認証成功時、WindowsPC で動作する PassLogic for Windows Desktop モジュールは認証サーバに対してオフライン認証データ要求を行います。認証サーバで生成するオフライン認証データ件数が大きい場合、認証サーバに相応の負荷がかかります。特に初回オンライン認証成功時には、連続オフライン認証上限回数分のデータを生成します。この為、ご利用ユーザ数が多い場合、PassLogic for Windows Desktop のユーザ様へのご利用開始のタイミングをずらし、初回オンライン認証後のオフライン認証データ要求が集中することを回避してください。

(注意) ログイン端末特定

PassLogic サーバではログイン端末を特定する情報を記録していません。

(注意) クライアントアプリケーションのアップデートインストール

旧バージョンからのアップデートインストールには対応していません。

旧バージョンをアンインストールした後、新しいバージョンをインストールしてください。

(注意) Windows システム復元後のオフライン認証

Windows システム復元でオフライン認証データの暗号キーのみが回帰してしまい、オフライン認証データを復号できなくなります。

Windows システム復元実施後は、オンライン認証を行ってください。

また、Windows Update などの Windows システム変更において、オフライン認証データの暗号キーが回帰することがあります。

オフライン認証が正しく機能しない場合は、オンライン認証を成功することで解消されます。

管理者用 (admin) パスワードを忘れた場合

本マニュアルの「2.6 メンテナンスツールに初めてアクセスする」を参照して admin のパスワードを再作成してください。

ミドルウェアのパフォーマンスチューニングについて

PassLogic は単体で動作する製品ではなく、他製品と連携して動作する製品であり、連携対向製品の作りによって適切なチューニングパラメータの値が大きく異なる性質があります。

ミドルウェアのチューニングパラメータがシステムにどのような影響を与えるかは、実際のシステム上で動作させて確認する他ないため、本番環境と近い試験環境が構築できる場合のみご検討ください。(パラメータが適切ではない場合、サービス停止を伴う可能性があるため検証なく本番環境へ適用されることはお勧めできません。)

なお、環境要因が大きく適切な値を算出できない背景から、チューニングについては自己の責任において実施をお願いします。チューニングパラメータおよび、チューニングに起因して発生したお問合せやログ解析についてはお受けできかねますことご了承ください。

パフォーマンスに関する補足事項

RHEL8 にてデフォルトで起動されるようになった、`sssd-kcm.socket`、`sssd-kcm` は、PassLogic のパフォーマンスを低下させる要素となっています。

パフォーマンスを重視される場合には、この 2 つのサービスを停止し、無効化するようにして下さい。

```
・ sssd-kcm.socket の停止と無効化
# systemctl stop sssd-kcm.socket
# systemctl disable sssd-kcm.socket

・ sssd-kcm の停止と無効化
# systemctl stop sssd-kcm
# systemctl disable sssd-kcm
```

FreeRADIUS 仕様変更における注意点

FreeRADIUSv3.0.20 以降では、インストールから 60 日経過後にリストアなどの処理が失敗する可能性があります。以下のリンクにて対応方法を記載しておりますので、ご確認ください。

https://passlogic.jp/doc/pdf/announce_20210406_radius.pdf

8.2 冗長化構成時の注意事項

【重要】OS 停止・起動・再起動、あるいは pgsql,pgpool の停止・起動・再起動の際は、必ずデータベースリカバリ処理を実行してください。

認証サーバ間の同期対象データ

下記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。下記のファイルを変更しており、再インストールを伴うリカバリを行う際は、手動での反映を実施してください。

特殊ハンドラ設定 /opt/passlogic/apps/lib/settings/global_setting.php
pgsql 障害発生時のメール送信設定 /opt/passlogic/pgsql/data/failover_mail.sh
SSH 鍵 {PassLogic インストーラディレクトリ}/ssh/authorized_keys {PassLogic インストーラディレクトリ}/ssh/id_rsa {PassLogic インストーラディレクトリ}/ssh/id_rsa.pub
共通暗号鍵 {PassLogic インストーラディレクトリ}/lib/plcrypt.conf

冗長化構成リカバリ処理実行時の注意事項

冗長化構成のリカバリ処理を実行するとデータベースサービスが一時停止します。以下の3つの処理は、処理中にデータベースへのアクセスを行いますので、リカバリ処理とタイミングが重なると、データベースへのアクセスが失敗し、異常終了します。リカバリ処理は、以下の処理が行われていないことをご確認の上実行してください。

- ・LDAP ID 同期処理
- ・LDAP 認証連携ユーザ削除スクリプト (passlogic_adsync.php)
- ・ユーザー一括登録処理 (userimport.php)
- ・PassLogic 認証用有効期限メールの送信処理

冗長化構成のリカバリ処理を実行した時、下記に示すファイルはリカバリの対象となりません。修正を行った場合、手動でのリカバリを実施してください。

特殊ハンドラ設定 /opt/passlogic/apps/lib/settings/global_setting.php
PassLogic リバースプロキシ設定 /opt/passlogic/data/conf/xauth_passlogic_00.conf
設定情報 DB 切り替えフラグ /opt/passlogic/data/conf/flag/passlogic_config

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。

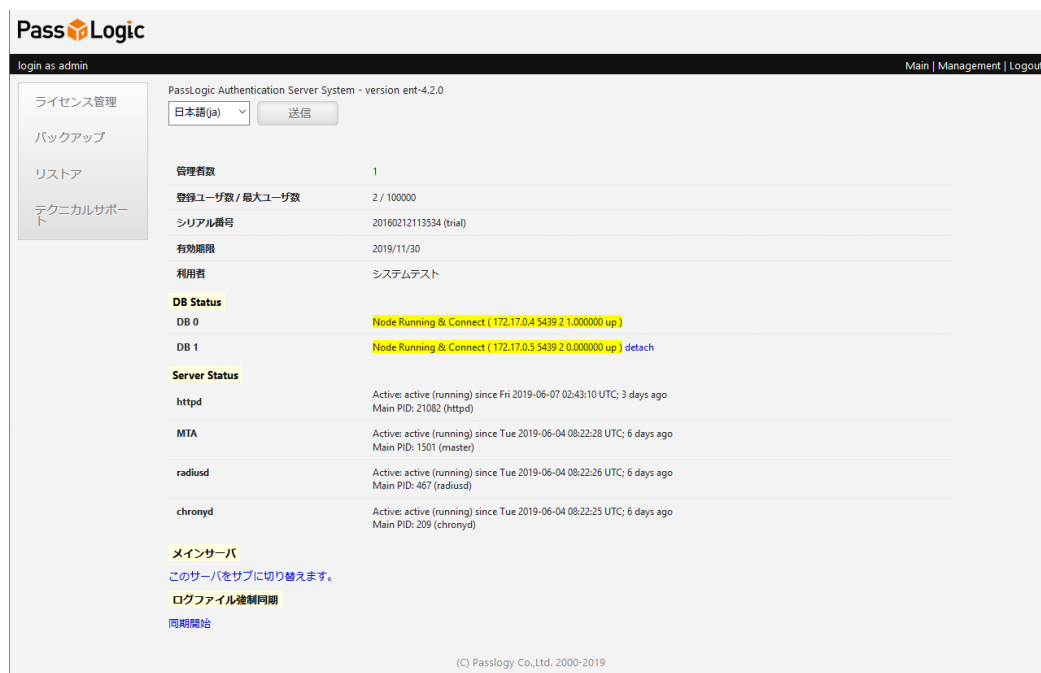
(注意)送信されるメールは failover_mail.sh に定義した内容です。

(注意)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冗長化している 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。

(注意)アラートメール送信は OS 付属の Postfix を利用します。管理画面で設定するメール送信設定とは別に、移設先のネットワーク環境に応じて適切に Postfix が設定されている必要があります。

postgresql と pgpool の再起動

ミドルウェアチューニングやメンテナンスなどにより、passlogic-postgresql、passlogic-pgpool の再起動を実施した場合は、必ずリカバリを実施してください。(メンテナンス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」が下図のように黄色で表示されている場合、リカバリが必要です。)



The screenshot shows the PassLogic Administration Console interface. The main content area displays system information for the PassLogic Authentication Server System (version ent-4.2.0). The interface includes a sidebar with navigation options like 'ライセンス管理', 'バックアップ', 'リストア', and 'テクニカルサポート'. The main content area shows system details such as '管理者数' (1), '登録ユーザー数 / 最大ユーザー数' (2 / 100000), 'シリアル番号' (20160212113534 (trial)), '有効期限' (2019/11/30), and '利用者' (システムテスト). Below this, there are sections for 'DB Status', 'Server Status', and 'メインサーバ'. The 'DB Status' section shows 'DB 0' and 'DB 1' both as 'Node Running & Connect'. The 'Server Status' section lists services like 'httpd', 'MTA', 'radiusd', and 'chrony' as active. The 'メインサーバ' section includes a link to switch servers and a link for 'ログファイル強制同期'.

認証セッション情報の削除

不要になった認証セッション情報をデータベースから削除する処理を、1日1回深夜帯にメインサーバで、実行します(実行スクリプト:/etc/cron.daily/passlogic_session_gc.sh)。メンテナンス等でDB0あるいはDB1が切り離された状況でも削除処理は実行されます。この場合削除処理は切り離されていないDBのセッション情報のみを削除します。メンテナンス終了後は必ずリカバリを実施して、DB0—DB1間のデータの整合性を回復してください。また、認証セッション情報削除処理時DB0とDB1でセッション情報の齟齬が検出された際は、DB0とDB1の全ての認証セッション情報を削除します。**この場合認証状態が解除されます。**

DB0とDB1のデータ齟齬の検知

DB0とDB1のデータ齟齬をpgpoolが検知した場合、下記の例のようにメッセージを/var/log/passlogic-pgpool/pgpool.logに出力します。

【pgpool.log メッセージ例】

```
YYYY-mm-DD HH:MM:SS: pid xxxx: LOG:  pgpool detected difference of the number  
of inserted, updated or deleted tuples. Possible last query was: "DELETE FROM  
passlogic_session WHERE updated_at < xxxxxx"
```

このメッセージを検出する場合、以下のような検索文字列をご利用ください。

【検索文字列 例】

```
pgpool detected difference of the number of inserted, updated or deleted tuples
```

pgpool フェイルオーバーの検知

pgpool が対向の postgres を切り離しを行った場合、下記の例のようにメッセージを /var/log/passlogic-pgpool/pgpool.log に出力します。

【pgpool.log メッセージ例】

```
YYYY-mm-DD HH:MM:SS: pidxxxx: LOG:  starting degeneration. shutdown host  
xxx.xxx.xxx.xxx(5439)
```

このメッセージを検出する場合、以下のような検索文字列をご利用ください。

【検索文字列 例】

```
starting degeneration. shutdown host
```

8.3 災害対策構成（DR）時の注意事項

SAML 利用時

災害系と平常系の認証サーバ FQDN は同一である必要があります。

RADIUS 利用時

認証サーバに RADIUS 認証要求を送信する radius 機器の ip アドレスは、平常系と災害系で同一である必要があります。運用管理ガイド「3.1 SSL-VPN(RADIUS)」の【項目解説】内 IP アドレス も合わせて参照ください。

SSL-VPN 機器の Web ログイン画面へ SSO を行う場合、radius 機器の Web 画面の FQDN は、平常系と災害系で同一である必要があります。

Reverse Proxy > SSO 設定 利用時

認証方式が クライアント自動認証(JavaScript) および BASIC 認証の場合、「ログインページの URL」および「認証送信先 URL」で指定する URL の FQDN 部分は平常系と災害系で同一である必要があります。

8.4 NFS 領域への配置についての注意事項

認証サーバで利用する以下のディレクトリを NFS 領域に配置しないでください。

また、/opt/passlogic/ はマウントポイントにしないでください。

```
/opt/passlogic/  
/var/log/passlogic/  
/var/log/passlogic-pgpool/
```

付録A メールテンプレート初期文面の一覧

新規ユーザ送信メール

<p>【件名】 PassLogic 利用開始のお知らせ</p> <p>【本文】 =====</p> <p>利用する認証方式やポリシーの設定、利用方法に合わせてメール本文を編集してください。 下記のメッセージは、メール本文のサンプルとなりますので適宜ご活用ください。 ★マークはコメント行となります。</p> <p>=====</p> <p><%UNAME%> 様</p> <p>[御社名]業務システムのログイン用情報と利用手順をお知らせします。 ※本メールには重要な内容が含まれておりますので大切に保管して下さい。</p> <p>[設定 > ポリシー設定 > 端末固定 ON の場合 ★OFF の場合は以下の説明は不要] 最初にログインした端末がシステムに登録され、以降別の端末ではログインができなくなります。 ログインしたい端末で最初のログインを行ってください。</p> <p>以下、ログインの手順です。</p> <p>[★ 認証方式:PassLogic を利用する場合の手順]</p> <p>-----</p> <p>0 はじめに</p> <p>-----</p> <p>パスロジック認証を初めてご利用になる場合は 下記のページをお読みください。 https://www.passlogy.com/pattern_staticpass</p> <p>-----</p> <p>1 ログインページにアクセス</p> <p>-----</p> <p>ログインする端末のブラウザで、下記ログインページにアクセスしてください。 https://[PassLogic サーバ FQDN]/ui/</p> <p>-----</p> <p>2 ユーザ ID とドメインの入力</p> <p>-----</p> <p>下記のユーザ ID を入力します。 その後ドメインを選択して、「次へ」を押してください。</p> <p>ユーザ ID: <%UID%> ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]</p> <p>-----</p> <p>3 パスワードの入力</p> <p>-----</p> <p>画面内に乱数表が表示されます。</p> <p>下記の「*」と数字で作られた表が、ブラウザ上の乱数表と対応しています。 下記表の「1」と同じマスにある乱数表上の数字をパスワードとして入力し、</p>

「2」以降も同様につづけて入力してください。

パターン:

<%PASSLOGICPATTERN%>

[★追加フレーズを使用しない場合は以下の説明は不要]

パターンの入力が終わりましたら、その後につづけて、
下記の追加フレーズ(旧スタティックパスワード)を入力してください。

追加フレーズ(旧スタティックパスワード):

<%SPASSWORD%>

パスワードを入力したら、「ログイン」を押してください。

4 パターン(パスワード)の変更

パターンと追加フレーズ(旧スタティックパスワード)を変更する場合は
下記のパスワードポリシーにしたがって、変更してください。

【パスワードポリシーについて】

パターンの長さ:[●桁~●桁]の範囲で設定できます。

追加フレーズの長さ:[●桁~●桁]の範囲で設定できます。

※ パターン(パスワード)は定期的な変更が必要です。([●毎日])

※ 簡単なパターンの登録は禁止されています。

登録できなかった場合は別のパターン(パスワード)をお試しください。

[★認証方式:PassClip を利用する場合の手順]

0 はじめに

本システムでは、ワンタイムパスワードを生成するアプリ
(ソフトウェアトークン)を使ったログインを行います。

使用するアプリの名称は PassClip L (パスクリップ エル)です。

1 PassClip L の利用準備

次の手順にしたがい、PassClip L の利用準備をしてください。

(手順 1) スマートフォンに PassClip L をインストール

・iOS 版 PassClip L

<https://itunes.apple.com/jp/app/id1167322433?mt=8>

・Android 版 PassClip L

<https://play.google.com/store/apps/details?id=com.passlogy.passclip.local>

(手順 2) PassClip L がインストールされたスマートフォン上で

下記の PassClip L アクティベート URL にアクセスしてください。

<%PASSCLIP_URL%>

(手順 3) PassClip L に「PassLogic」スロットが追加されたことを確認してください。

2 ログインページにアクセス

パソコンのブラウザから、下記ログインページにアクセスしてください。

https://[PassLogic サーバ FQDN]/ui/

3 ユーザ ID とドメインの入力

下記のユーザ ID を入力します。
その後ドメインを選択して、「次へ」を押してください。

ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

4 パスワードの入力

ブラウザ画面にパスワード入力フォームが表示されます。

スマートフォンにインストールした PassClip L を立ち上げて、
「PassLogic」スロットをタップするとワンタイムパスワードが表示されます。

そのワンタイムパスワードをパスワード有効時間内に
ブラウザ画面のパスワード入力フォームに入力して[ログイン]をクリックしてください。

[★ 認証方式:TOTP を利用する場合の手順]

0 はじめに

本システムでは、ワンタイムパスワードを生成する装置
(ハードウェアトークン)を使ったログインを行います。

1 ハードウェアトークン の準備

ログインをするためには、ハードウェアトークンと PIN コードが
必要になります。
下記シリアル番号のハードウェアトークンとその PIN コードを
お手元にご準備ください。

ハードウェアトークンのシリアル番号:<%TOKEN_SERIAL%>

2 ログインページにアクセス

パソコンのブラウザから、下記ログインページにアクセスしてください。

https://[PassLogic サーバ FQDN]/ui/

3 ユーザ ID とドメインの入力

下記のユーザ ID を入力します。
その後ドメインを選択して、「次へ」を押してください。

ユーザ ID: <%UID%>
ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

ブラウザ画面上にパスワード入力フォームが表示されます。

4 パスワードの入力

ハードウェアトークンに表示されるワンタイムパスワードを
有効時間内にブラウザ画面上のパスワード入力フォームに入力して
[ログイン]をクリックしてください。

[★ 其他のお知らせ内容は設定やご利用環境に合わせて適宜ご変更ください]

お問い合わせの前にご確認ください

(1)アカウントがロックされた場合
ロックアウト後、[●]分間経過すると自動でロックが解除されます。

(2)パターン(パスワード)を忘れた場合
パスワードを忘れた場合は下記 URL からパスワード再設定の手続きを行ってください。
入力するメールアドレスは事前に登録されているアドレス(本メールの受信アドレス)のご入力が必要です。
[https://\[PassLogic サーバ FQDN\]/ui/reminder.php](https://[PassLogic サーバ FQDN]/ui/reminder.php)

【 パスワードポリシーについて 】
※アカウントがロックされ、ログインできなくなった場合
ロックされた時点から、[●]分間経過すると自動でロックが解除されます。

【 PassLogic の利用に関するお問い合わせ先 】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

パスワード再発行送信メール

【件名】
PassLogic パスワード再発行のお知らせ

【本文】
<%UNAME%> 様

[御社名]業務システムのパスワードを再発行しましたことをお知らせします。
※本メールには重要な内容が含まれておりますので大切に保管して下さい。

■ ログインページの URL

[https://\[PassLogic サーバ FQDN\]/ui/](https://[PassLogic サーバ FQDN]/ui/)

■ アカウント情報

ユーザ ID: <%UID%>
ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]
初期パターン:
<%PASSLOGICPATTERN%>

[★追加フレーズを使用しない場合は以下は不要]

初期追加フレーズ(旧スタティックパスワード):
<%SPASSWORD%>

【 ログイン手順 】

1)ログインページの URL へアクセス
2)ユーザ ID を入力し[次へ]をクリック
3)パターンを入力して[ログイン]をクリック
※初回ログイン後はパターンの変更が必須となります。
※ヘルプ: パターンと追加フレーズ(旧スタティックパスワード)について
https://www.passlogy.com/pattern_staticpass

【 パスワードポリシーについて 】

パターンの長さ: ●桁～●桁 の範囲で設定できます。
追加フレーズの長さ: ●桁～●桁 の範囲で設定できます。
※ パターン(パスワード)は定期的な変更が必要です。(●日毎)
※ 簡単なパターンの登録は禁止されています。
登録できなかった場合は別のパターン(パスワード)をお試しください。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

パスワードリマインダー送信メール

【 件名 】

PassLogic パスワード再発行

【 本文 】

<%UNAME%> 様

以下の URL をクリックすると、[御社名]業務システムのパスワードが再発行され
同じメールアドレス宛に新しいパスワード(パターン)が案内されます。
[https://\[PassLogic サーバ FQDN\]/ui/resetter.php?key=<%REMINDER_URLKEY%>](https://[PassLogic サーバ FQDN]/ui/resetter.php?key=<%REMINDER_URLKEY%>)

※この URL は本メールが配信されてから 24 時間有効です。
有効期限が切れた場合は、以下の URL より改めてパスワード再発行の手続きを行ってください。
[https://\[PassLogic サーバ FQDN\]/ui/reminder.php](https://[PassLogic サーバ FQDN]/ui/reminder.php)

※パスワード再発行のメールを複数受信した場合は、最新のメールに記載されている URL をご利用ください。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

TOTP 交換トークン設定送信メール

【 件名 】

PassLogic TOTP 交換トークン設定の通知

【 本文 】

<%UNAME%> 様

[御社名] 業務システムのログイン用の交換用トークンの準備が完了しました。
 交換用のハードウェアトークンとその PIN コードをお手元にご準備ください。
 ※ハードウェアトークンが到着していない場合は管理者にご確認ください。

 交換用トークンのシリアル番号

<%NEXT_TOKEN_SERIAL%>

交換用トークンで [御社名] 業務システムにログインすることで、
 旧トークンから切り替えることができます。

■ ログインページの URL

[https://\[PassLogic サーバ FQDN\]/ui/](https://[PassLogic サーバ FQDN]/ui/)

ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

【 パスワードポリシーについて 】

ロックアウト後、●●分間経過すると自動でロックが解除されます。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]

メールアドレス:[メールアドレス]

内線番号:[内線番号]

PassClip 再セットアップ送信メール

【件名】

PassLogic PassClip アプリ初期化のご案内

【本文】

<%UNAME%> 様

[御社名] 業務システムのログイン時の PassClip アプリを下記の手順で再設定してください。
 ※本メールには重要な内容が含まれておりますので大切に保管して下さい。

 ■ スマートフォンセットアップ

次の手順にしたがい、PassClip L の利用準備をしてください。

(手順 1) スマートフォンに PassClip L をインストール

・iOS 版 PassClip L

<https://itunes.apple.com/jp/app/id1167322433?mt=8>

・Android 版 PassClip L

<https://play.google.com/store/apps/details?id=com.passlogy.passclip.local>

(手順 2) PassClip L がインストールされたスマートフォン上で

下記の PassClip L アクティベート URL にアクセスしてください。

<%PASSCLIP_URL%>

(手順 3) PassClip L に「PassLogic」スロットが追加されたことを確認してください。

 ■ PassLogic ログインページの URL

[https://\[PassLogic サーバ FQDN\]/ui/](https://[PassLogic サーバ FQDN]/ui/)

■ ログイン情報

ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

■ ログイン手順

1)Web ブラウザでログインページの URL へアクセスしてください。

2)ユーザ ID を入力し[次へ]をクリックしてください。

3)PassClip アプリの「PassLogic」スロットから取得した
ワンタイムパスワードを入力して[ログイン]をクリックしてください。

【 パスワードポリシーについて 】

ロックアウト後、●●分間経過すると自動でロックが解除されます。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]

メールアドレス:[メールアドレス]

内線番号:[内線番号]

端末登録送信メール

【件名】

PassLogic 新規端末登録

【本文】

<%UNAME%> 様

当メールから、[御社名]業務システムにログイン可能な端末を追加することができます。

ログインを許可したい端末から、以下の端末登録用の URL にアクセスしログインしてください。
ログインが完了することでシステムに端末が登録され、それ以降もログインできるようになります。

■ 端末登録用の URL

[https://\[PassLogicサーバFQDN\]/ui/?key=<%ENTRYKEY%>](https://[PassLogicサーバFQDN]/ui/?key=<%ENTRYKEY%>)

※本端末登録用 URL は 1 端末のみ登録可能です。

■ ログインページの URL

[https://\[PassLogicサーバFQDN\]/ui/](https://[PassLogicサーバFQDN]/ui/)

ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]

メールアドレス:[メールアドレス]

内線番号:[内線番号]

PKI 認証用クライアント証明書の発行メール

【件名】

クライアント証明書の発行

【本文】

<%UNAME%> 様

[御社名]業務システムの PKI 認証用に必要なクライアント証明書の発行準備ができました。

[御社名]業務システムへのアクセスを許可したい端末上で、下記の証明書ダウンロードの URL にアクセスし、クライアント証明書をダウンロードの上でインストールしてください。

証明書のインストールが完了するとシステムにログインできるようになります。

■ 証明書ダウンロードの URL

[https://\[PassLogic サーバ FQDN\]/ui/?downloadkey=<%DOWNLOADKEY%>](https://[PassLogic サーバ FQDN]/ui/?downloadkey=<%DOWNLOADKEY%>)

■ 証明書パスワード

<%CERT_PASSWORD%>

■ 証明書のインストール方法

証明書のインストール方法はご利用環境によって異なります。

以下の URL よりご確認ください。

https://www.passlogy.com/register_cert

※ 証明書を有効化させるためにはブラウザの再起動が必要となるため、証明書インストール完了後にブラウザを再起動してください。

■ ログインページの URL

[https://\[PassLogic サーバ FQDN\]/ui/](https://[PassLogic サーバ FQDN]/ui/)

■ アカウント情報

ユーザ ID: <%UID%>

ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

【 登録したクライアント証明書を削除したい場合 】

登録したクライアント証明書を削除したい場合はこちらをご参照ください。

https://www.passlogy.com/delete_cert

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]

メールアドレス:[メールアドレス]

内線番号:[内線番号]

有効期限送信メール

【件名】
PassLogic パスワード有効期限のお知らせ

【本文】
<%UNAME%> 様

[御社名] 業務システムのパスワード(パターン+追加フレーズ)の有効期限についてお知らせします。

パスワード有効期限: <%EXPIRE_DATE%>

期限が切れる前にパスワードを再設定してください。
期限が切れた場合は、パスワード変更が完了するまで
[御社名] 業務システムのアプリケーションが利用できません。

■ ログインページの URL

https://[PassLogic サーバ FQDN]/ui/

■ アカウント情報

ユーザ ID: <%UID%>
ドメイン: <%DOMAIN%> [★localドメインを使用する場合は本項目は不要]

【 パスワードポリシーについて 】
パターンの長さ: ●桁～●桁 の範囲で設定できます。
追加フレーズの長さ: ●桁～●桁 の範囲で設定できます。
※ パターン(パスワード)は定期的な変更が必要です。(●日毎)
※ 簡単なパターンの登録は禁止されています。
登録できなかった場合は別のパターン(パスワード)をお試しください。

【 PassLogic の利用に関するお問い合わせ先 】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

アカウントロック通知メール

【件名】
PassLogic アカウントロック通知

【本文】
<%UNAME%> 様

[御社名] 業務システムのログイン連続失敗回数が規定値を超えたためアカウントをロックしました。
アカウントのロック解除につきましては、管理者までお問い合わせください。

【PassLogic の利用に関するお問い合わせ先】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

新規ユーザ送信メール(管理者)

【件名】
PassLogic 利用開始のお知らせ

【本文】

=====

利用する認証方式やポリシーの設定、利用方法に合わせてメール本文を編集してください。

下記のメッセージは、メール本文のサンプルとなりますので適宜ご活用ください。

★マークはコメント行となります。

=====

<%UNAME%> 様

PassLogic の管理者用ログイン情報と利用手順をお知らせします。

※本メールには重要な内容が含まれておりますので大切に保管して下さい。

以下、ログインの手順です。

0 はじめに

パスロジック認証を初めてご利用になる場合は

下記のページをお読みください。

https://www.passlogy.com/pattern_staticpass

1 ログインページにアクセス

ログインする端末のブラウザで、下記ログインページにアクセスしてください。

<管理ツール>

[https://\[PassLogicサーバFQDN\]:8443/passlogic-admin/](https://[PassLogicサーバFQDN]:8443/passlogic-admin/)

<メンテナンスツール>

[https://\[PassLogicサーバFQDN\]:12443/passlogic-maintenance/](https://[PassLogicサーバFQDN]:12443/passlogic-maintenance/)

2 ユーザ ID の入力

下記のユーザ ID を入力して、「次へ」を押してください。

ユーザ ID: <%UID%>

3 パスワードの入力

画面内に乱数表が表示されます。

下記の「*」と数字で作られた表が、ブラウザ上の乱数表と対応しています。

下記表の「1」と同じマスにある乱数表上の数字をパスワードとして入力し、

「2」以降も同様につづけて入力してください。

パターン:

<%PASSLOGICPATTERN%>

[★追加フレーズを使用しない場合は以下の説明は不要]

パターンの入力が終わりましたら、その後につづけて、

下記の追加フレーズ(旧スタティックパスワード)を入力してください。

追加フレーズ(旧スタティックパスワード):

<%SPASSWORD%>

パスワードを入力したら、「ログイン」を押してください。

 4 パターン(パスワード)の変更

パターンと追加フレーズ(旧スタティックパスワード)を変更する場合は
 下記のパスワードポリシーにしたがって、変更してください。

【 パスワードポリシーについて 】

パターンの長さ:[●桁~●桁] の範囲で設定できます。

追加フレーズの長さ:[●桁~●桁] の範囲で設定できます。

※ パターン(パスワード)は定期的な変更が必要です。([● 毎日])

※ 簡単なパターンの登録は禁止されています。

登録できなかった場合は別のパターン(パスワード)をお試しください。

[★ その他のお知らせ内容は設定やご利用環境に合わせて適宜ご変更ください]

 お問い合わせの前にご確認ください

(1)アカウントがロックされた場合

ロックアウト後、[●]分間経過すると自動でロックが解除されます。

(2)パターン(パスワード)を忘れた場合

パスワードを忘れた場合は admin 権限を持つ管理者にご連絡ください。

【 パスワードポリシーについて 】

※アカウントがロックされ、ログインできなくなった場合

ロックされた時点から、[●]分間経過すると自動でロックが解除されます。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]

メールアドレス:[メールアドレス]

内線番号:[内線番号]

パスワード再発行送信メール(管理者)

【件名】

PassLogic パスワード再発行のお知らせ

【本文】

<%UNAME%> 様

PassLogic の管理者パスワードを再発行しましたことのお知らせします。

※本メールには重要な内容が含まれておりますので大切に保管して下さい。

 ■ ログインページの URL

<管理ツール>

https://[PassLogic サーバ FQDN]:8443/passlogic-admin/

<メンテナンスツール>

https://[PassLogic サーバ FQDN]:12443/passlogic-maintenance/

 ■ アカウント情報

ユーザ ID: <%UID%>
初期パターン:
<%PASSLOGICPATTERN%>

[★追加フレーズを使用しない場合は以下は不要]
初期追加フレーズ(旧スタティックパスワード):
<%SPASSWORD%>

【 ログイン手順 】
1)ログインページの URL へアクセス
2)ユーザ ID を入力し[次へ]をクリック
3)パターンを入力して[ログイン]をクリック
※ヘルプ: パターンと追加フレーズ(旧スタティックパスワード)について
https://www.passlogy.com/pattern_staticpass

【 パスワードポリシーについて 】
パターンの長さ: ●桁～●桁 の範囲で設定できます。
追加フレーズの長さ: ●桁～●桁 の範囲で設定できます。
※ パターン(パスワード)は定期的な変更が必要です。(●日毎)
※ 簡単なパターンの登録は禁止されています。
登録できなかった場合は別のパターン(パスワード)をお試しください。

【 PassLogic の利用に関するお問い合わせ先 】
[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

有効期限送信メール(管理者)

【件名】
PassLogic パスワード有効期限のお知らせ

【本文】
<%UNAME%> 様

PassLogic の管理者パスワード(パターン+追加フレーズ)の有効期限についてお知らせします。

パスワード有効期限: <%EXPIRE_DATE%>

期限が切れる前にパスワードを再設定してください。

■ ログインページの URL

<管理ツール>
[https://\[PassLogicサーバFQDN\]:8443/passlogic-admin/](https://[PassLogicサーバFQDN]:8443/passlogic-admin/)

■ アカウント情報

ユーザ ID: <%UID%>

【 パスワードポリシーについて 】
パターンの長さ: ●桁～●桁 の範囲で設定できます。
追加フレーズの長さ: ●桁～●桁 の範囲で設定できます。

- ※ パターン(パスワード)は定期的な変更が必要です。(●日毎)
- ※ 簡単なパターンの登録は禁止されています。
登録できなかった場合は別のパターン(パスワード)をお試しください。

【 PassLogic の利用に関するお問い合わせ先 】

[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]

アカウントロック通知メール(管理者)

【件名】

PassLogic アカウントロック通知

【本文】

<%UNAME%> 様

PassLogic 管理者用アカウントのログイン連続失敗回数が規定値を超えたためアカウントをロックしました。
アカウントのロック解除につきましては、admin 権限を持つ管理者までお問い合わせください。

【PassLogic の利用に関するお問い合わせ先】

[御社名 部署名 担当者名]
メールアドレス:[メールアドレス]
内線番号:[内線番号]