ZJTM181126101

ManageEngine
ADSelfService Plus

ADSelfService Plus をインターネットで安全に利用するためのガイド

目次

本ドキュメントの概要 **2**

ADSelfService Plus をインターネットで利用する **2**

シナリオ 1: ADSelfService Plus を LAN にインストールした場合 2

シナリオ 2: ADSelfService Plus を DMZ にインストールした場合 3

リバースプロキシを設定してセキュリティを向上させる **4**

リバースプロキシの概要と機能 4

Apache HTTP Server を ADSelfService Plus のリバースプロキシとして設定する手順 5

本ドキュメントの概要

このガイドでは、インターネット経由で ADSelfService Plus をリモートユーザーに安全に利用する手順を紹介します。また Apache HTTP Server をリバースプロキシとして使用して、ADSelfService Plus をリモートユーザーに安全に配布する手順を説明します。

始める前に:

製品をインターネットでホストする前に、SSL を ADSelfService Plus で有効化してください。

ADSelfService Plus をインターネットで利用する

シナリオ 1: ADSelfService Plus を LAN にインストールした場合

ADSelfService Plus がローカルエリアネットワーク(LAN)内にインストールされており、サーバーの IP アドレスが *192.168.200.254* 、ポート番号が *9251*、ホスト名が *adselfserviceplus-lan* である場合を想定します。

LAN 内のユーザーの場合は、ADSelfService Plus にアクセスする URL は https://adselfserviceplus-lan:9251 、または https://192.168.200.254:9251 となります。

ADSelfService Plus にインターネットからアクセスする場合、以下の手順が必要です:

- ネットワークサービスプロバイダーの IP アドレスとパブリックホスト名を登録します。
  この場合、IP アドレス 64.12.13.11 と、パブリックホスト名 selfservice.yourdomain.com を使用します。
- selfservice.yourdomain.com の IP アドレスを 64.12.13.11 に解決します。
  これは主にインターネットサービスプロバイダーによって処理されます。
- ファイアウォールのルール(またはルーターのアクセスリスト)を設定して、
  IP アドレス 64.12.13.11 への HTTPS リクエストを LAN IP アドレス 192.168.200.254 に
  リダイレクトします。
- ADSelfService Plus のアクセス URL 設定を新しいパブリック IP で更新します。
  管理者 > 製品設定 > 設定に移動して、アクセス URL の設定をクリックします。

ADSelfService Plus が生成したすべての通知は、パブリック URL で送信されますのでご注意ください。パブリック URL は LAN でも到達可能です。

シナリオ 2: ADSelfService Plus を DMZ にインストールした場合

ADSelfService Plus が、DMZ にインストールされており、サーバーの IP アドレスが *192.168.225.254* 、ポート番号が *9251* 、ホスト名が *adselfserviceplus-dmz* となっている 場合を想定します。この場合においては、ADSelfService Plus に組み込まれている PostgreSQL を使用することをお勧めします。この組み合わせであれば、追加の設定が必要ありません。

MS SQL データベースを使用する場合は、以下の手順に従ってください:

- **LAN 内の MS SQL データベース**:アプリケーションが MS SQL ポート経由で LAN 内のデータベースサーバーに到達できるようにファイアウォールのルールを設定してください。
  (既定のポートは 1433 です)。

- **DMZ 内の MS SQL データベース**:ポート 1433 が、DMZ 内の ADSelfService Plus サーバーから到達可能になっている必要があります。

データベース設定を終えた PostgreSQL のユーザーと MS SQL のユーザーの場合:

- LAN 内のユーザーが ADSelfService Plus に https://adselfserviceplus-dmz:443 でアクセスすることができるようにファイアウォールのルールを設定します。アプリケーションは 9251 にインストールされますが、ユーザーは 443 からアクセスする必要がありますので、ご注意ください。
  IP アドレス 192.168.225.254、ポート 443 からポート 9251 への HTTPS リクエストが必要になります。

- ネットワークサービスプロバイダーの IP アドレスとパブリックホスト名を登録します。
  この場合、IP アドレス 64.12.13.11 と、パブリックホスト名 selfservice.yourdomain.com を使用します。

- selfservice.yourdomain.com の IP アドレスを 64.12.13.11 に解決します。
  これは主にインターネットサービスプロバイダーによって処理されます。

- ファイアウォールルール(またはルーターのアクセスリスト)を設定して、HTTPS リクエストを IP アドレス 64.12.13.11 ポート 443 から、LAN IP アドレス 192.168.225.254 ポート 9251 にリダイレクトします。

- ADSelfService Plus のアクセス URL 設定を新しいパブリック IP で更新します。
  管理者 > 製品設定 > 設定 に移動して、アクセス URL の設定をクリックします。

ADSelfService Plus が生成したすべての通知は、パブリック URL で送信されますのでご注意ください。
パブリック URL は LAN でも到達可能です。

以上より、リモートユーザーがインターネットから ADSelfService Plus にアクセスできるようになります。

リバースプロキシを設定してセキュリティを向上させる

リバースプロキシの概要と機能

始めに、リバースプロキシについてご説明します。コンピューターネットワークにおいて、リバースプロキシはプロキシサーバーの一種であり、1 つ以上のサーバー（ADSelfService Plus）からクライアント（ユーザー）の代わりにリソースを取得します。これらのリソースはリバースプロキシ自体から取得されたかのようにクライアントに送信されます。リバースプロキシはウェブアプリケーションのセキュリティを補強し、ネットワークにおける戦略拠点として活用できます。

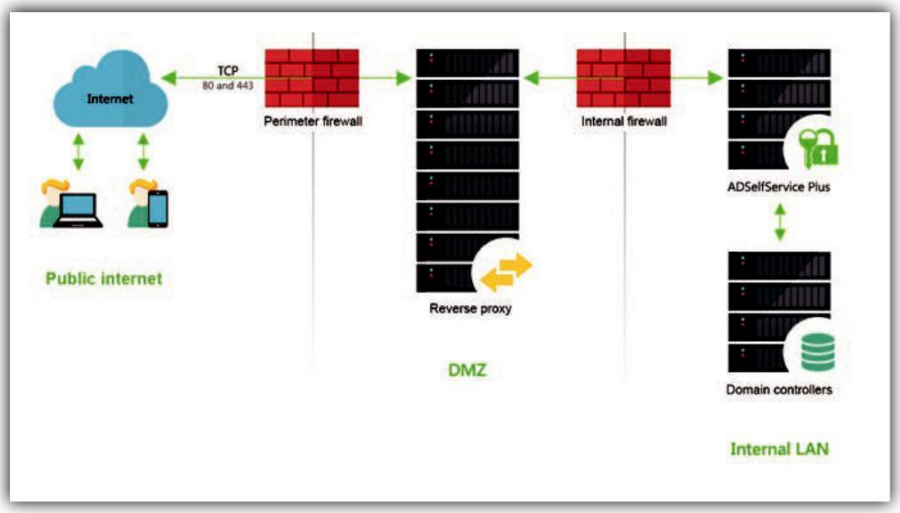

図 1：ADSelfService Plus がインターネットでホストされている場合の、DMZ のリバースプロキシサーバー。

上の図で示されているように、ADSelfService Plus はリバースプロキシサーバーに対応しています。上図では、クライアント（ユーザー）からのリクエストは DMZ のリバースプロキシサーバー（Apache サーバー）から受信します。そして、リバースプロキシサーバーが、これらのリクエストを LAN 内の ADSelfService Plus のサーバーに転送します。必要に応じて、ADSelfService Plus のサーバーは DMZ に配置することもできます。いずれの場合も、外部の端末が ADSelfService Plus のサーバーに直接接続することはありません。

ファイアウォールは ADSelfService Plus のサーバーへのアクセスを、プロキシサーバーの必要なポートへのアクセスのみ許可します。

重要：リバースプロキシを有効化した場合、管理者 > 製品設定 > 接続に移動して、アクセス URL の設定をクリックして、ADSelfService Plus のアクセス URL 設定を更新してください。

Apache HTTP Server を ADSelfService Plus のリバースプロキシとして設定する手順

それでは、Apache サーバーを使用して、ADSelfService Plus のリバースプロキシを設定する方法を説明いたします。この設定では、Apache HTTP Server のバージョン 2.2 を使用します。

重要:

- この設定は、リバースプロキシサーバーが DMZ に配置されており、ADSelfService Plus サーバーとドメインコントローラーが内部 LAN に配置されていることを想定しています。
- 各ステップでは、既定の IP アドレス、ポート番号、ファイルの場所などを使用しています。ADSelfService Plus、または Apache サーバーの既定の設定を変更している場合は、それらの変更を各ステップに反映させてください。
- Windows ファイアウォールにおける Apache サーバーの TCP アクセス設定で使用するポート(既定では、HTTP の場合 80、HTTPS の場合 443)を開いていることを確認してください。

ステップ 1:Apache サーバーで変更を適用する

A) **C:¥Program Files¥Apache Software Foundation¥Apache2.2¥conf** に移動します。

B) **httpd.conf** のファイルをテキストエディターで開きます。

C) 以下の行をコメントアウトします:

```
LoadModule proxy_module modules/mod_proxy.so LoadModule
proxy_ajp_module modules/mod_proxy_ajp.so LoadModule
proxy_balancer_module modules/mod_proxy_balancer.so LoadModule
proxy_connect_module modules/mod_proxy_connect.so LoadModule
proxy_ftp_module modules/mod_proxy_ftp.so LoadModule
proxy_http_module modules/mod_proxy_http.so LoadModule
proxy_scgi_module modules/mod_proxy_scgi.so Include
conf/extra/httpd-vhosts.conf
```

D) **C:¥Program Files¥Apache Software oundation¥Apache2.2¥conf¥extra** へ移動します。

E) **http-vhost.conf** のファイルをテキストエディターで開きます。

F) 以下のエントリーを追加します:

```
NameVirtualHost *:443
<VirtualHost *:443> ServerAdmin
```

admin@test.com
ServerName
adselfserviceplus.yourdomain.com
SSLEngine on
SSLProxyEngine on
SSLCertificateFile "C:¥Program Files¥Apache
Software
Foundation¥Apache2.2¥conf¥server.crt"
SSLCertificateKeyFile "C:¥Program
Files¥Apache Software
Foundation¥Apache2.2¥conf¥server.key"
<Location />
ProxyPass https://192.168.200.254:9251/
ProxyPassReverse
https://192.168.200.254:9251/
</Location>
ErrorLog "logs/ADSelfServicePlus.log"
CustomLog "logs/ADSelfServicePlus.log"
common
</VirtualHost>

G) **Apache サーバー**を**再起動**して、変更を適用します。

ステップ 2：ADSelfService Plus で変更を適用する

HTTPS の有効化により、ADSelfService Plus で変更を適用するステップが異なる場合があります。

ADSelfService Plus が HTTPS モードの場合

A) **<install_dir>¥conf** に移動します。既定では、このフォルダーは、
C:¥ManageEngine¥ ADSelfService Plus¥conf にあります。

B) **server.xml** のファイルをテキストエディターで開きます。

C) SSLEnabled="true"のエレメントを含むコネクタータグを検索します。
(i.e. <Connector SSLEnabled="true")

D) 以下のエントリーを追加します：

proxyName="<apache-server-ip-address>" proxyPort="443"

E) 変更を保存します。

F) **ADSelfService Plus** を再起動して、変更を適用します。

HTTP モードにおける ADSelfService Plus

A) **<install_dir>¥conf** に移動します。既定では、このフォルダーは、
C:¥ManageEngine¥ ADSelfService Plus¥conf にあります。

B） **server.xml** のファイルをテキストエディターで開きます。

C） name="WebServer" element の要素を含むコネクタータグを検索します。
(i.e. <Connector name="WebServer")

D） 以下のエントリーを追加します:

scheme="https" proxyName="<apache-server-ip-address>" proxyPort="443"

E） 変更を保存します。

F） **ADSelfService Plus** を再起動して、変更を適用します。

以上より、Apache HTTP Server を使用して、ADSelfService Plus のリバースプロキシの設定が完了しました。

ManageEngine ADSelfService Plus について

ADSelfService Plus は、 Active Directory 用のセルフサービスパスワード管理およびシングルサインオンソリューションです。これは、パスワードのセルフサービス、パスワードの失効リマインダー、セルフサービスでのディレクトリアップデーター、マルチプラットフォームのパスワード同期、クラウドアプリケーションのシングルサインオン機能を提供します。ADSelfService Plus は、パスワードリセットチケットを減らし、コンピューターのダウンタイムに起因するエンドユーザーのフラストレーションを緩和することで、IT ヘルプデスクをサポートします。詳細については、www.manageengine.jp/products/ADSelfService_Plus/.をご覧ください。