BIG-IP APM SAML機能

BIG-IP SAML機能による クラウド対応 認証連携・SSOソリューション

- この機能によるメリット
  - セキュリティ
    - 企業はクラウド上に展開されるアプリケーションアクセスのためのユーザアカウント管理を自社内認証ディレクトリを用いることができます
    - 認証ディレクトリを一元化できるためパスワードポリシーを手元でコントロールできます
  - 柔軟性
    - Google, Salesforce, Office365などパブリッククラウドサービスと認証連携ができます
  - 利便性
    - ユーザはクラウドを含む複数アプリケーションへのアクセス時、都度クレデンシャル入力を求められることなく使うことができます

APM SAML機能ハイライト ①

- APMがSAML Identity Provider(IdP)として機能
  - ユーザ認証実施（認証サーバと連携）およびアサーションの発行
- APMがSAML Service Provider(SP)として機能
  - アサーションの評価をし、ACLなどのアクセスポリシーに従いアプリケーションアクセスを提供
- SAML version 2.0 サポート

※BIG-IP v11.3 リリース時現在の機能
※詳細はマニュアル参照：
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-saml-config-guide-11-3-0/1.html

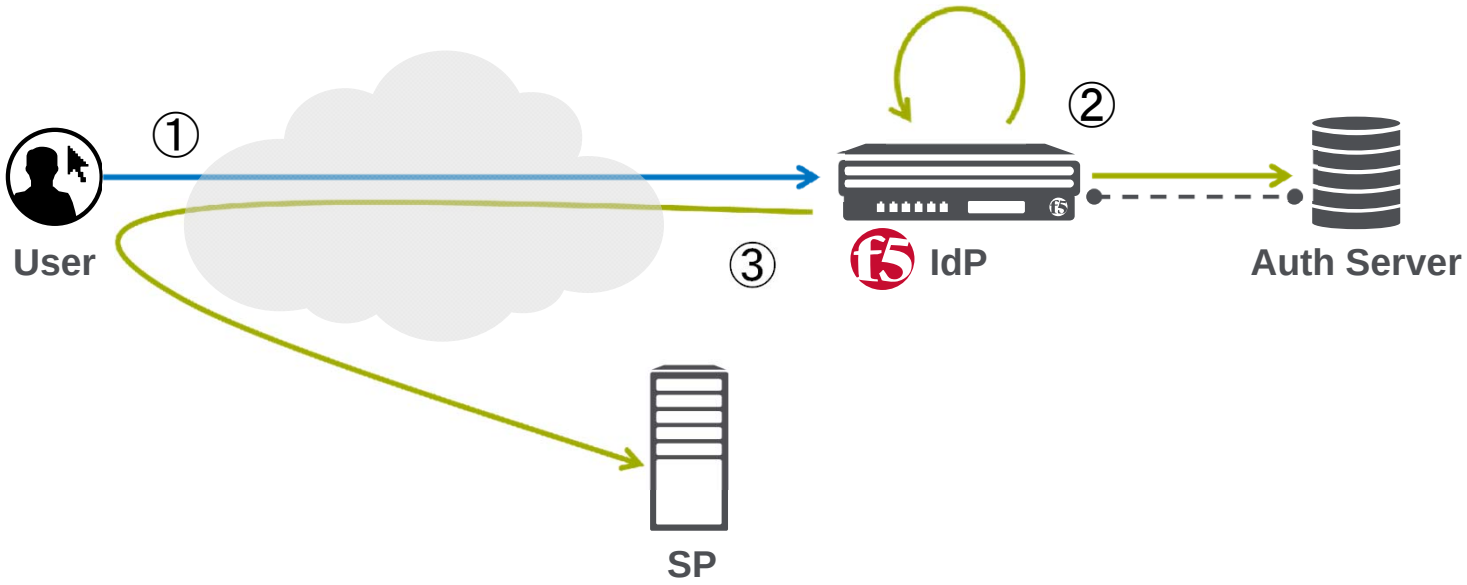
APM SAML機能ハイライト ②

- メタデータのインポート・エクスポート機能
  - SAMLコンフィグレーションを含んだメタデータのインポート・エクスポートに対応
- テンプレートの提供
  - 連携するIdP、SP設定用テンプレートを用意
  - APMがIdPの時：Google SP, Shibboleth SP, BIG-IP SP
  - APMがSPの時：ADFS IdP, SecureAuth IdP, Shibboleth IdP, Open SSO IdP, BIG-IP IdP
- idPイニシエーテッド、SPイニシエーテッドアクセスのサポート
- 暗号化アサーションのサポート
  - より強固なセキュリティのために AES128, AES192, AES256 を利用可能

※BIG-IP v11.3 リリース時現在の機能
※詳細はマニュアル参照：
http://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-saml-config-guide-11-3-0/1.html

アプリケーションアクセスフロー ①

APMをIdPとして利用（IdPイニシエーテッド アクセス）



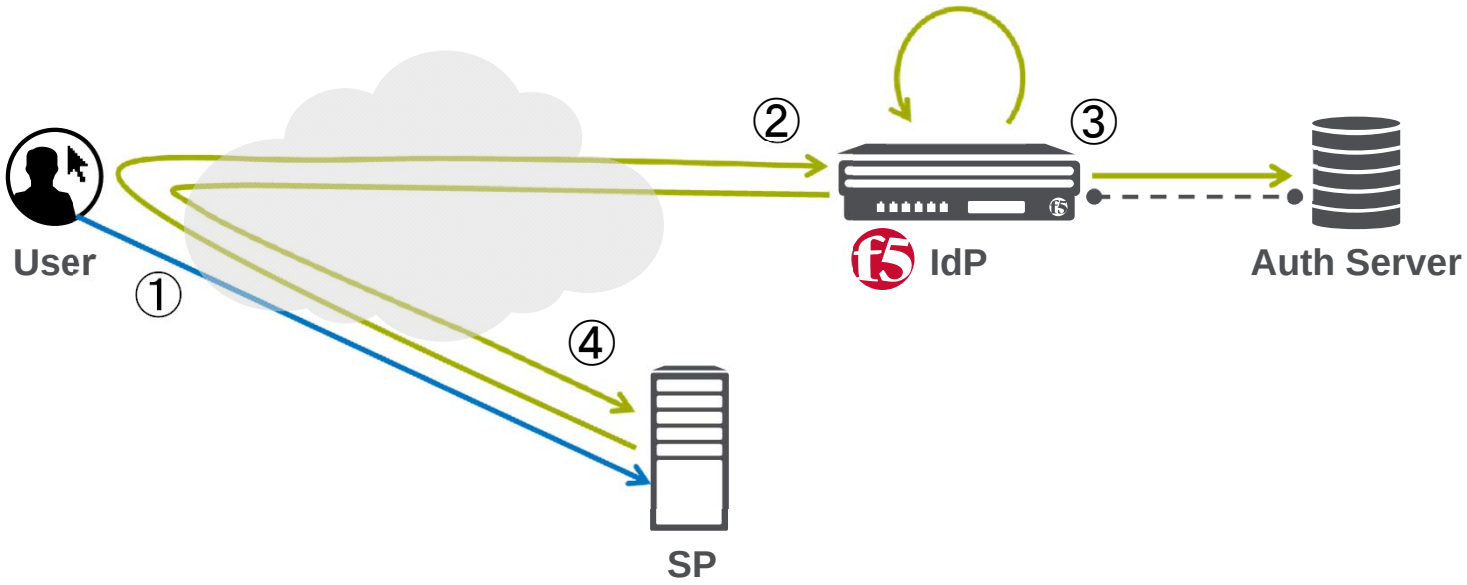
① ユーザがAPM(IdP)にアクセス。

② APM上にセッション情報がないためAccess PolicyによりAuth Serverを利用しユーザ認証を実施。Webtopによりアプリケーションを提供。

③ ユーザがアプリケーションを選択時アサーションが作成され、SP上のACSにリダイレクト。

アプリケーションアクセスフロー ②

APMをIdPとして利用（SPイニシエーテッド アクセス）



① ユーザがSPにアクセス。

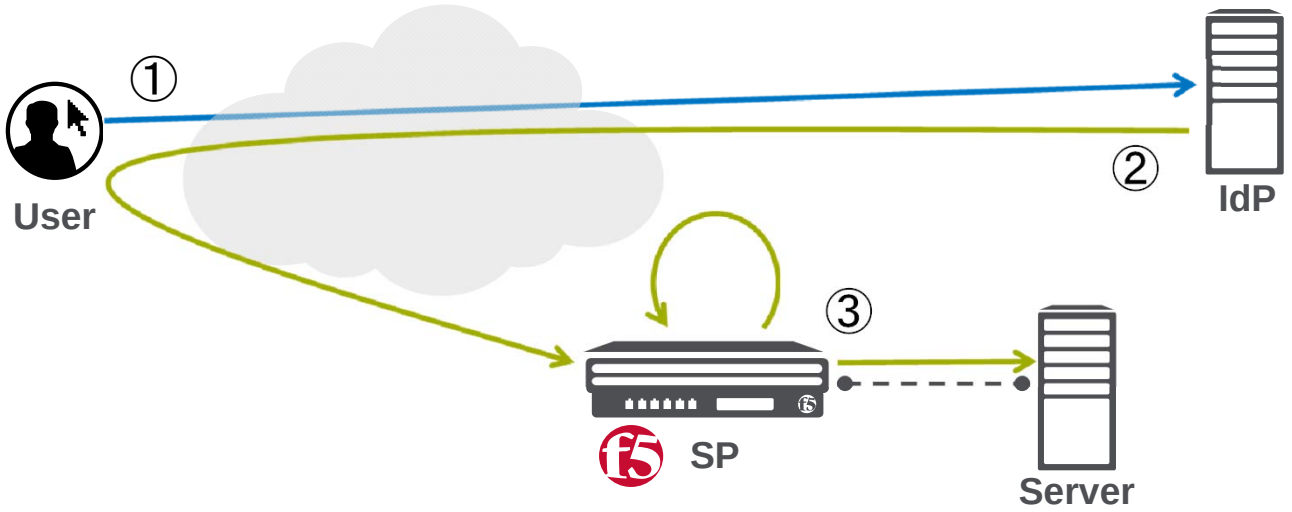
② SPはユーザ認証のためにAPM(IdP)にリダイレクト。

③ APM上にセッション情報がないためAccess PolicyによりAuth Serverを利用しユーザ認証を実施。

④ アサーションが作成され、SP上のACSにリダイレクト。

アプリケーションアクセスフロー ③

APMをSPとして利用（IdPイニシエーテッド アクセス）



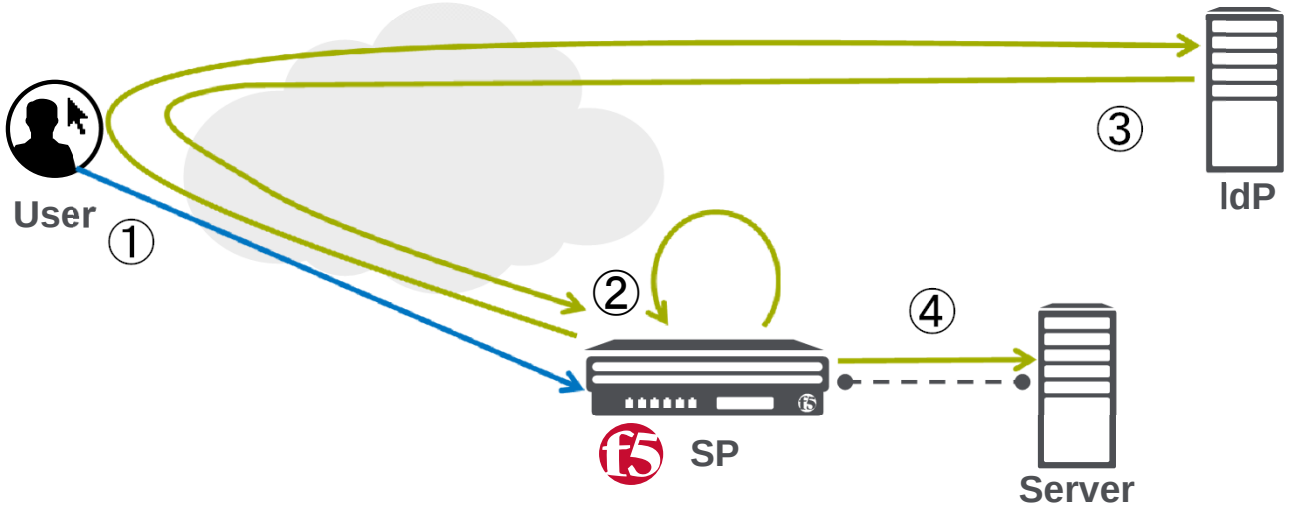
① ユーザがIdPにアクセス。

② IdPがユーザ認証後アサーションと共にAPM(SP)にリダイレクト。

③ APM(SP)でアサーションを検証しサーバへのアクセスを許可。

アプリケーションアクセスフロー ④

APMをSPとして利用（SPイニシエーテッド アクセス）



① ユーザがAPM(SP)にアクセス。

② APM上にセッション情報がないためAccess Policy実行後、IdPにリダイレクト。

③ IdPがユーザ認証後アサーションと共にAPM(SP)にリダイレクト。

④ APM(SP)でアサーションを検証しサーバへのアクセスを許可。

www.f5networks.co.jp