D210070

「Citrix ADC」と「Themis」の SAML 連携

株式会社ディー・ディー・エス
シトリックス・システムズ・ジャパン株式会社

1. 「Citrix ADC」との SAML 連携

アプリケーションデリバリーと負荷分散機能を提供する「Citrix ADC」と多要素認証を可能とする「万能認証基盤 Themis」を連携することで、顔認証などの多要素認証を利用して、目的のリソースにセキュアにリモートアクセスできるようになります。

2. 「Citrix ADC」について

Citrix ADC（旧称 NetScaler ADC）は包括的なアプリケーションデリバリーソリューションであり、ハイブリッドマルチクラウド環境において負荷分散を含む柔軟なトラフィックコントロールによりサイトパフォーマンスを最大化するとともに、認証連携、暗号化、リモートアクセス、アプリケーションファイアウォールなど、近年のサービスに不可欠なセキュリティ機能を提供します。

アプリケーションサーバ単体では実装できない付加機能も、物理/仮想アプライアンスもしくはクラウド上にインスタンスを配置する事で容易に構成する事が可能になります。

3. 連携イメージ

4. SAML 登録方法

(1) サービスプロバイダー情報（以下 SP と記述）の登録

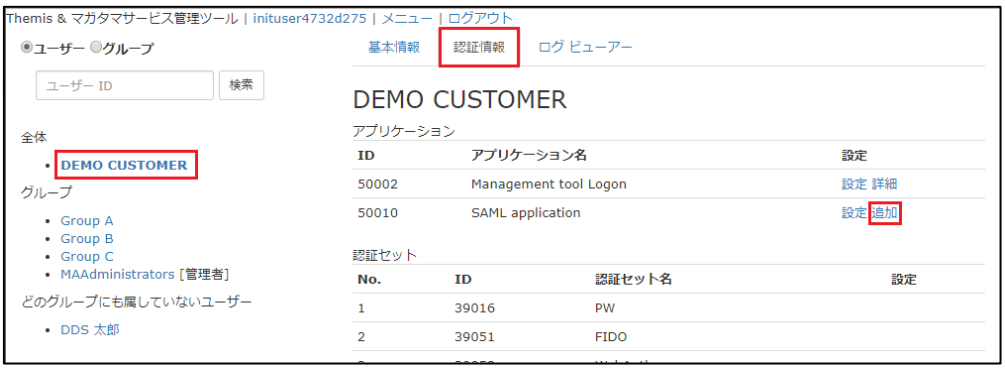
i. アプリケーションの登録

Citrix ADC の SP としての情報を Themis 管理ツールへ登録します。ブラウザで管理ツールを開き、「管理ツールにログイン」をクリックします。

管理者用のユーザー名とパスワードを入力して「認証」をクリックし、管理者としてログインします。

全体で設定されている「DEMO CUSTOMER」（名称は任意で設定いただけま

す）を選択し、「認証情報」タブをクリックします。アプリケーションの「50010 SAML application」の「追加」をクリックしてアプリケーションの新規作成を行います。

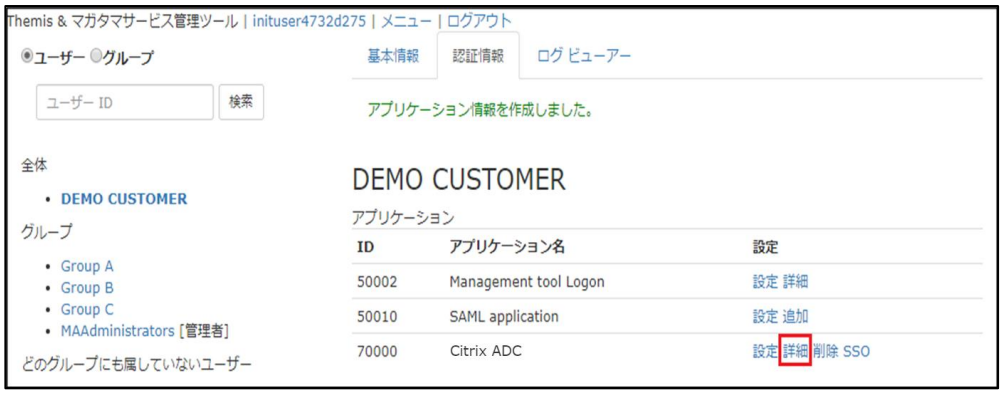


「アプリケーション名」と「概要」を入力し、必要な認証要素にチェックを入れて「保存」をクリックします。

「アプリケーション情報を作成しました。」と表示されます。登録した名前のアプリケーションが作成されていればアプリケーションの登録が完了となります。

ii. Citrix ADC の SP 情報の登録

管理ツール画面で全体の「DEMO CUSTOMER」を選択し、「認証情報」タブをクリックします。その後、アプリケーションの「Citrix ADC」の「詳細」をクリックします。



「Service Provider 情報の設定」の画面に遷移します。ここに、XXXX の SP としての情報を登録します。

Service Provider 情報の設定

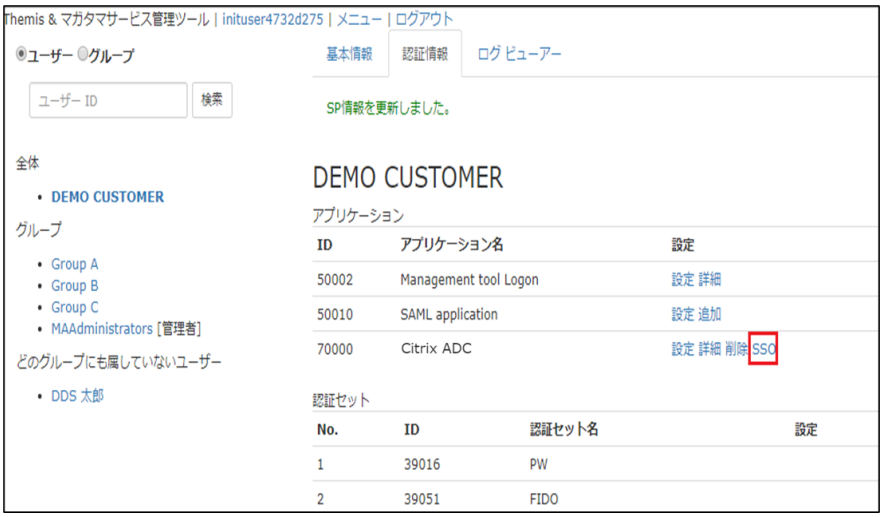
設定変数	値
SP の名前	任意の名称を設定ください
Issuer	※1
SSO エンドポイント	※1
SLO エンドポイント	※1
メタデータ URL	※1
フィンガープリント	-

RelayState	-

※1 お使いの Citrix ADC のメタデータに従って設定ください。

(2) ID プロバイダー（以下 Idp と記述）情報の登録
Themis の Idp としての情報を Citrix ADC へ登録します。

管理ツール画面で全体の「DEMO CUSTOMER」を選択し、「認証情報」タブをクリックします。その後、アプリケーションの「Citrix ADC」の「SSO」をクリックします。



「SSO 設定情報」が表示されます。ここで表示される「SSO エンドポイント」、「SLO エンドポイント」、「メタデータ」、「X.509 証明書」の情報を Citrix ADC のポータルサイトに登録します。

（例）SSO 設定情報ページ

ここまでの登録手順を実施することで、次回ログイン以降、「Citrix ADC」の SAML 専用ログイン URL から「Themis」の認証ページにリダイレクトされ、Themis 認証を利用してフェデレーションを行うことができるようになります。

以上