AppDynamicsでのシングルサインオンの設定およびトラブルシューティング

内容

はじめに

このドキュメントでは、AppDynamicsでシングルサインオン(SSO)を設定し、問題をトラブルシューティングする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- シングルサインオンを設定するには、ユーザーはアカウント所有者（デフォルト）の役割、または管理、エージェント、作業の開始ウィザードの権限を持つカスタムロールを持っている必要があります。
- yourIdPaccountへの管理者アクセス。
- AppDynamicsからのメタデータまたは構成の詳細（エンティティID、ACS URLなど）。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- AppDynamicsコントローラー

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

シングルサインオン(SSO)は、ユーザが1回ログインするだけで複数のアプリケーション、システム、またはサービスにアクセスできる認証メカニズムです。各アプリケーション、システム、またはサービスごとに再認証する必要はありません。

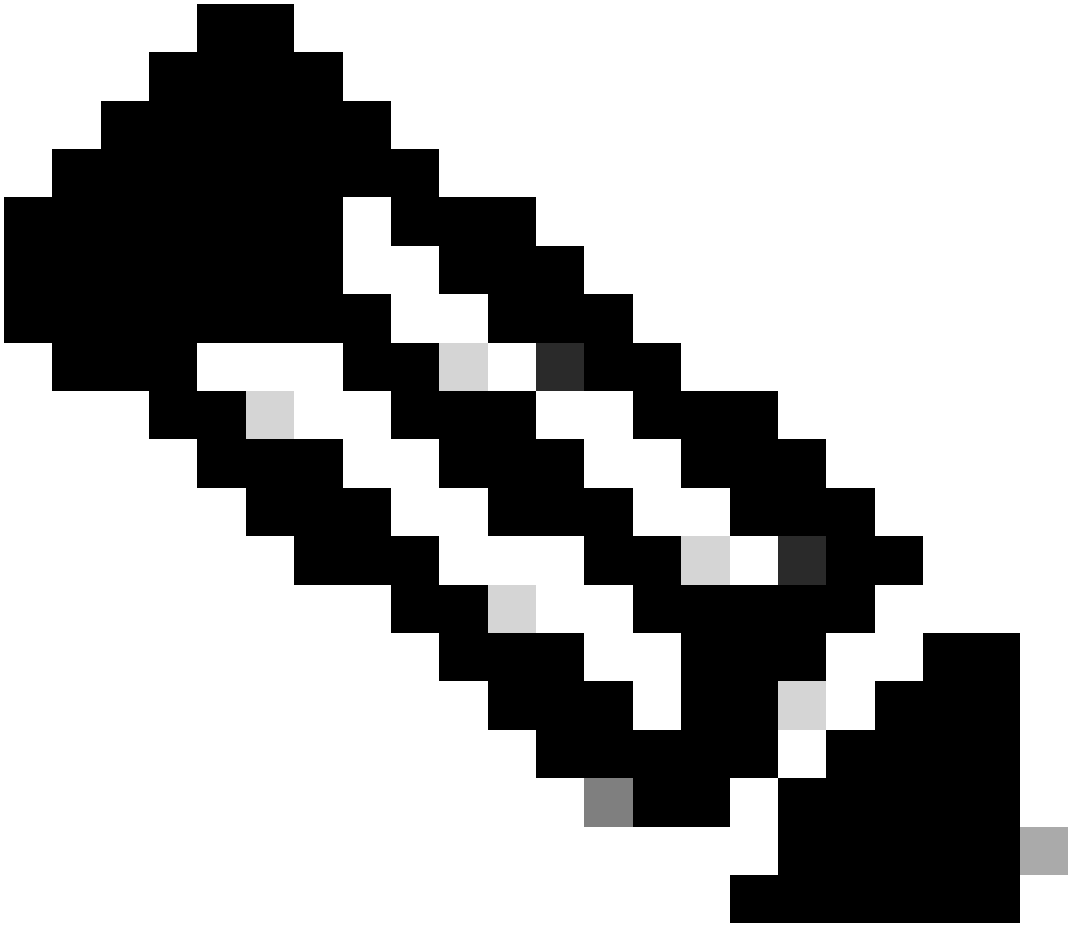
Security Assertion Markup Language(SAML)は、SSOの実装に使用されるテクノロジーの1つです。アイデンティティプロバイダー(IdP)とサービスプロバイダー(SP)の間で認証および許可データを安全に交換することで、SSOを可能にするフレームワークとプロトコルを提供します。

SAMLアサーション

- XMLベースのメッセージは、IdPとSPの間で交換されます。
- 次の3種類のアサーションが提供されます。
  - 認証アサーション：ユーザが認証されたことを確認します。
  - 属性アサーション：ユーザ名やロールなどのユーザ属性を共有します。
  - Authorization Decision Assertions（許可決定主張）：ユーザに許可されている操作を示します。

SAMLの主な役割

- アイデンティティプロバイダー(IdP)
  - ユーザのIDを確認します。
  - ユーザの識別情報を含むSAMLアサーションを生成します。
- サービスプロバイダー(SP)
  - ユーザがアクセスするアプリケーションまたはシステム。
  - IdPを使用してユーザを認証します。
  - SAMLアサーションを受け入れ、リソースまたはアプリケーションへのユーザアクセスを許可します。
- ユーザー（プリンシパル）
  - 要求を開始する実際のユーザ、またはサービスプロバイダーからリソースにアクセスしようとしている実際のユーザ。
  - IdP（認証）とSPの両方と通信します。



注:AppDynamicsは、IdPによる開始とSPによる開始の両方のSSOをサポートしています。

SP開始フロー：

- ユーザは、アプリケーションのURL（AppDynamicsなど）を入力するか、リンクをクリックして、サービスプロバイダーに移動します。
- SPは既存のセッションを確認します。セッションが存在しない場合、SPはユーザーが認証されていないことを認識し、SSOプロセスを開始します。
- SPはSAML認証要求を生成し、認証のためにユーザをIdPにリダイレクトします。
    - この要求には次のものが含まれます。
        - エンティティID：サービスプロバイダーの固有識別子。
        - Assertion Consumer Service(ACS)URL：認証後にIdPがSAMLアサーションを送信する場所。
        - SPに関するメタデータとセキュリティの詳細（署名済み要求、暗号化要件など）。
- ユーザはIdPログインページにリダイレクトされます。

- IdPはユーザを認証します（たとえば、ユーザ名/パスワードまたは多要素認証を介して）。
- 認証に成功すると、IdPはSAMLアサーション（セキュリティトークン）を生成します。
- SAMLアサーションは、HTTP POSTバインディング（ほとんどの場合）またはHTTPリダイレクトバインディングを使用して、ユーザブラウザ経由でSPに返送されます。
- SPはSAMLアサーションを検証して、次のことを確認します。
    - 信頼できるIdPによって発行されました。
    - SPエンティティIDを使用してSPにアドレス指定されます。
    - 有効期限が切れていないか、改ざんされていません（IdP公開キーを使用して検証されます）。

- SAMLアサーションが有効な場合、SPはユーザのセッションを作成します。
- ユーザには、アプリケーションまたはリソースへのアクセス権が付与されます。

IdPが開始したフロー：

- ユーザはIdPログインポータルに移動し、クレデンシャルを入力します。
- IdPはユーザを認証します（ユーザ名/パスワードの組み合わせ、多要素認証など）。
- 認証後、IdPはユーザに対して、ユーザがアクセスできる利用可能なアプリケーションまたはサービス(SP)のリストを提示します。
- ユーザは目的のSP（AppDynamicsなど）を選択します。
- IdPは、選択されたSPのSAMLアサーションを生成します。

- IdPはユーザをSP Assertion Consumer Service(ACS)URLにリダイレクトし、SAMLアサーションをそのURLとともに送信します（HTTP POSTバインディングまたはHTTPリダイレクトバインディングを使用）。
- SPはSAMLアサーションを受信し、検証します。
    - アサーションが信頼できるIdPによって発行されていることを確認します。
    - アサーションの整合性と有効期限を確認します。
    - ユーザーIDおよびその他の属性を確認します。

- SAMLアサーションが有効な場合、SPはユーザのセッションを作成します。
- ユーザには、アプリケーションまたはリソースへのアクセス権が付与されます。

設定

AppDynamics Controllerは、Cisco Customer Identityまたは外部のSAML IDプロバイダー(IdP)を使用して、ユーザを認証および許可できます。

サポートされるIDプロバイダー

AppDynamicscertifiesは、次のアイデンティティプロバイダー(IdP)のサポートを認定します。

- オクタ
- ワンロギン
- IDのPing
- Azure AD
- IBMクラウドID

- Active Directoryフェデレーションサービス(AD FS)

HTTP POSTバインディングをサポートする他のIdPも、AppDynamics SAML認証と互換性があります。

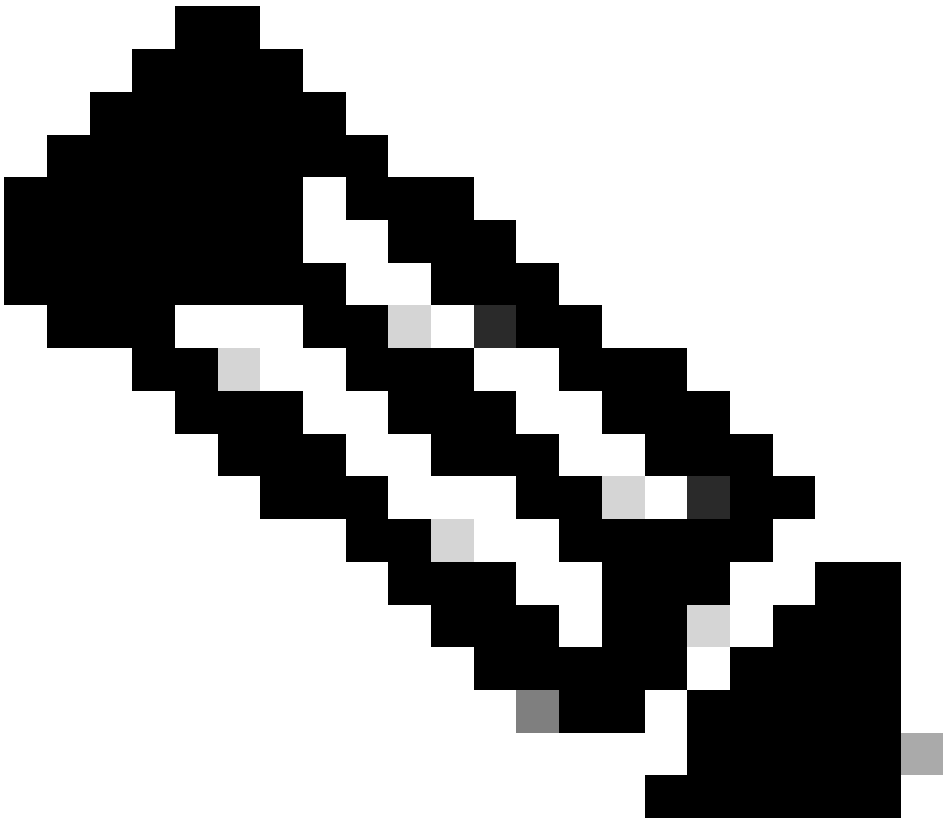
AppDynamicsでSAMLを構成する手順

ステップ 1：AppDynamicsコントローラーの詳細の収集

- エンティティID（SPエンティティID）: AppDynamicsの一意の識別子(例：https://<controller-host>:<port>/controller)。
  - 構文： https://<controller_domain>/controller
  - 例：https://<your_controller_domain>/controller

- 応答URL(Assertion Consumer Service、ACS URL)：サービスプロバイダー（AppDynamicsなど）上のエンドポイント。IdPは認証後にSAML応答を送信します。
  - 構文：https://<controller_domain>/controller/saml-auth?accountName=<account_name>
  - 例： https://your_controller_domain/controller/saml-auth?accountName=youraccountname

---



注：オンプレミスコントローラの場合、異なるaccountNameのマルチテナントコントローラがない限り、デフォルトのアカウント名はcustomer1です。

- Single Logout URL（オプション）:SAMLログアウト要求を処理するSP上のエンドポイント(https://<controller_domain>/controllerなど)。

ステップ 2：IdPで新しいアプリケーションを作成し、メタデータをダウンロードする

- アプリケーション作成領域の特定：これは通常、IdP管理コンソールまたはダッシュボード内にあり、アプリケーション、Webおよびモバイルアプリケーション、エンタープライズアプリケーション、証明書利用者などのラベルが付いています。
- カスタムまたは汎用SAMLアプリケーションの追加：カスタムSAMLアプリケーションまたは汎用SAMLサービスプロバイダー統合を構成できるオプションを選択します。
- アプリケーションの詳細を入力します。アプリケーションに名前を付け、アイコンをアップロードして識別できるようにします（オプション）。
- 属性マッピング（Username、displayName、email、またはroles）を追加して、AppDynamicsにユーザー情報を渡します。
- IdPメタデータファイルをダウンロードするか、または次の詳細をメモします。
  - IdPログインURL
  - ログアウトURL
  - 属性名
  - 証明書

ステップ 3：AppDynamics ControllerでのSAML認証の設定

- アカウント所有者ロール、または管理、エージェント、作業の開始ウィザード権限を持つロールとして、コントローラUIにログインします。
- ユーザ名（右上隅）> Administration > Authentication Provider > Select SAMLの順にクリックします。

- SAML Configurationセクションで、次の詳細を追加します。

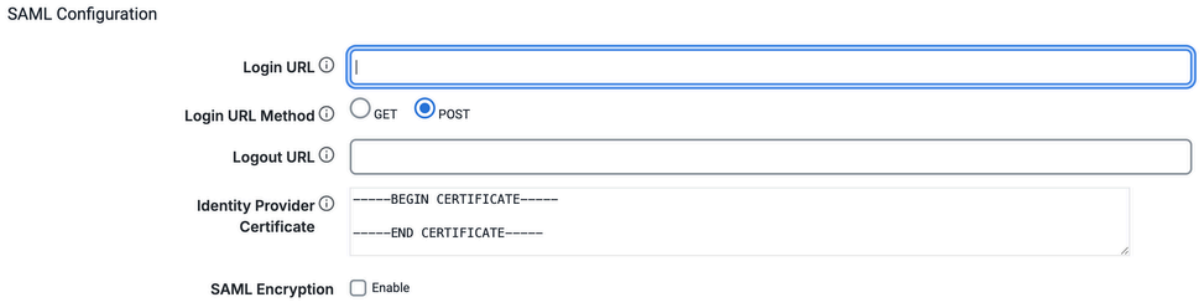
  - ログインURL: AppDynamicsコントローラーがサービスプロバイダー(SP)が開始したログイン要求をルーティングするIdPログインURL。

  - Logout URL（オプション）：ユーザーがログアウトした後、AppDynamics Controllerがユーザーをリダイレクトするurl。ログアウトURLを指定しない場合、ユーザーはログアウト時にAppDynamicsログイン画面を取得します。

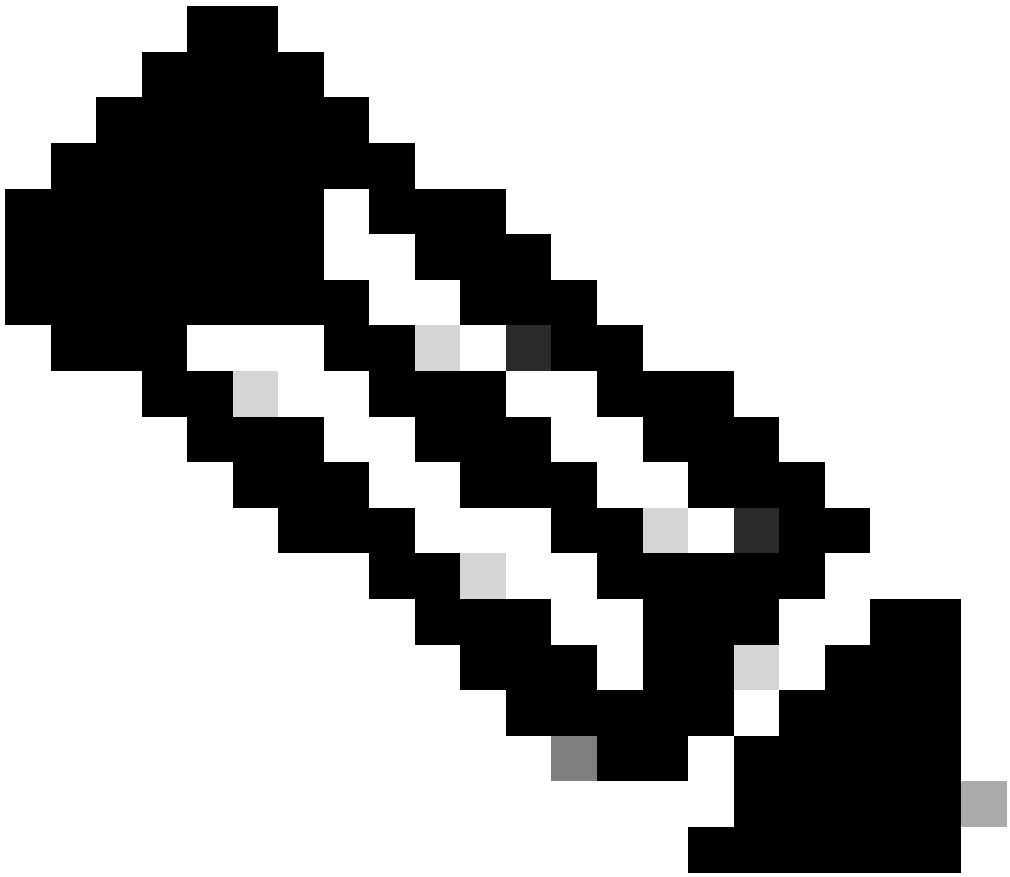
  - Certificate:IdPからのX.509証明書。BEGIN CERTIFICATEとEND CERTIFICATEの区切り記号の間に証明書を貼り付けます。ソース証明書自体からBEGIN CERTIFICATEとEND CERTIFICATEの区切り文字を複製しないでください。

  - SAML暗号化（オプション）:IdPからサービスプロバイダーへのSAML応答を暗号化することで、SAML認証のセキュリティを向上させることができます。 AppDynamicsでSAML応答を暗号化するには、SAMLアサーションを暗号化するようにアイデンティティプロバイダー(IdP)を設定し、復号化に特定の証明書と秘密キーを使用するように

AppDynamics Controllerを設定する必要があります。



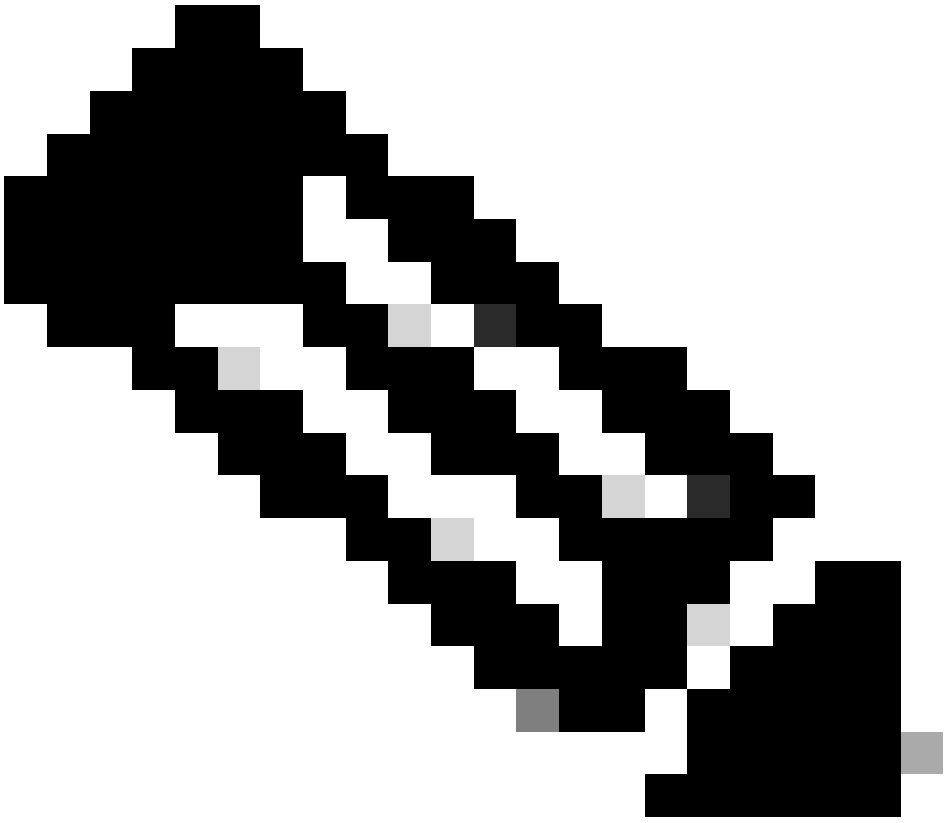
- SAML Attribute Mappingsセクションで、SAML属性（例：Username、DisplayName、Email）をAppDynamicsの対応するフィールドにマップします。



注:AppDynamicsは、SAMLユーザのユーザ名、電子メール、および表示名を表示します。デフォルトでは、SAML応答のNameID属性を使用してユーザ名が作成されます。このユーザ名はdisplayNameとしても使用されます。この動作は、username、email、およびdisplayname属性をSAML応答に含めることでカスタマイズできます。AppDynamicsでIdP設定を構成するときに、ユーザーはこれらの属性名を指定で

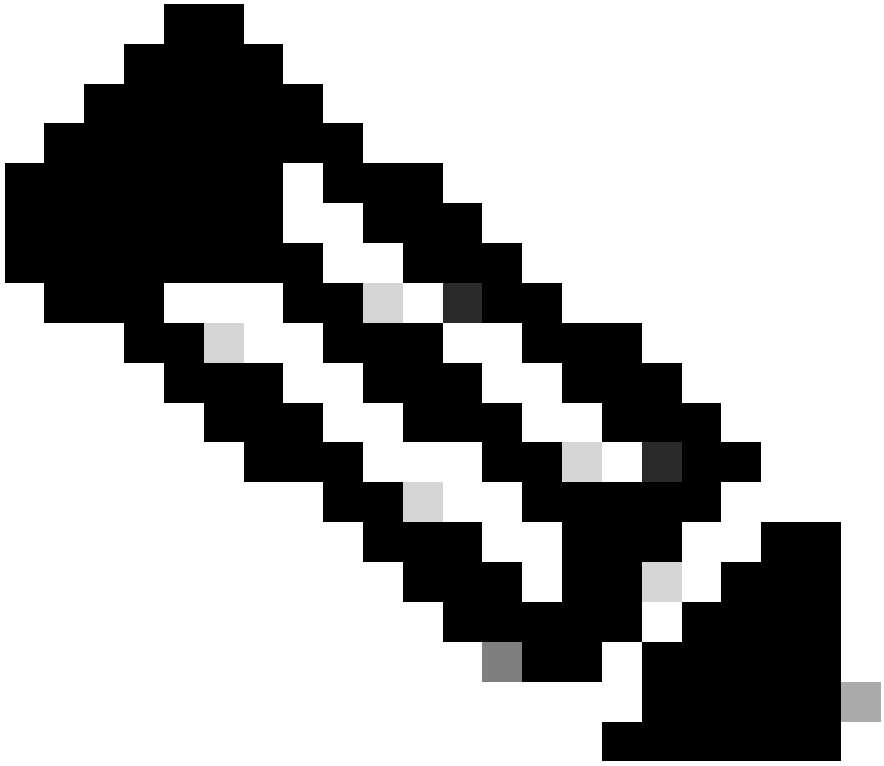
きます。ログイン中、AppDynamicsは属性マッピングが構成されているかどうかを確認します。マッピングが設定され、一致する属性がSAML応答に存在する場合、AppDynamicsはこれらの属性値を使用してユーザ名、電子メール、表示名を設定します。

- SAML Group Mappingsセクションで、これらの詳細を追加します。
  - SAMLグループ属性名：グループ情報を含むSAML属性の名前を入力します。 通常は、グループ、グループまたはロール、ロールまたはグループメンバーシップです。
  - グループ属性値：グループ属性に適切な値フォーマットを選択します。 一般的なオプションには、IdPによるグループ情報の構造に応じて、「複数のネストされたグループ値」または「単一値」があります。

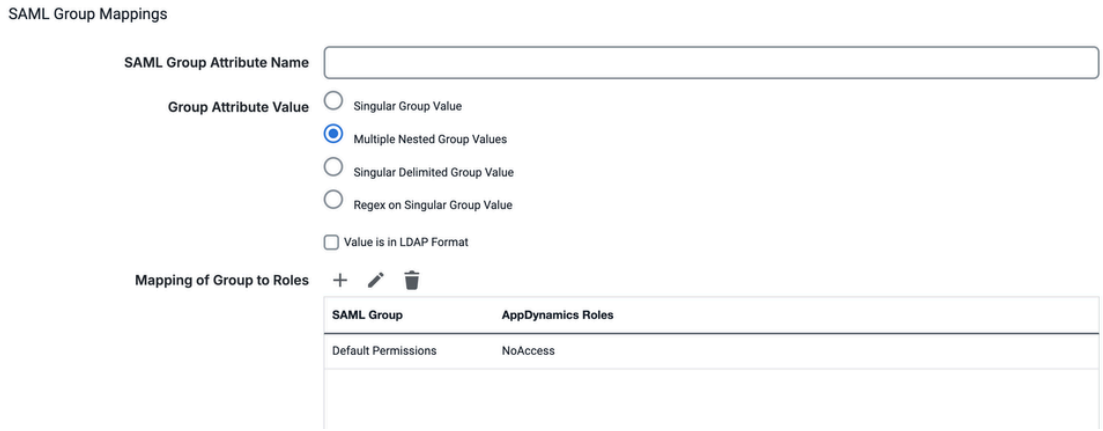


注：グループ情報がLDAP(Lightweight Directory Access Protocol)形式である場合は、「値がLDAP形式である」を選択します。

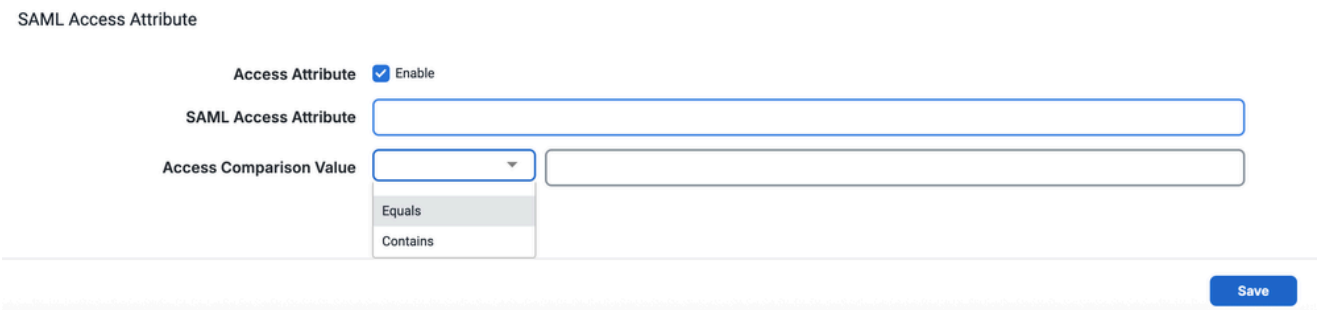
- グループからロールへのマッピング：+ボタンをクリックして、新しいマッピングを追加します。
  - SAMLグループ： AppDynamicsロールにマップするSAMLグループの名前（IdPで定義）を入力します。
  - ロール：使用可能なリストから、SAMLグループに属するユーザに割り当てる対応するAppDynamicsロールを選択します。
  - デフォルトの権限：SAMLグループマッピングが設定されていない場合、またはユーザのSAMLアサーションにグループ情報が含まれていない場合、AppDynamicsはデフォルトの権限の使用にフォールバックします。



注：最小限の権限を持つロールをデフォルト権限に割り当てることをお勧めします。



- SAML Access Attributeセクションで、次の詳細を追加します（オプション）。
  - SAMLアクセス属性： SAML応答の属性の名前を入力します。これは、アクセスの検証に使用されます。
  - アクセス比較値：次の2つのオプションを使用できます。
    1. 等しい：アクセスが許可されるのは、SAML応答の属性値が構成で指定された値と正確に一致する場合のみです。
    2. Contains:SAML応答の属性値に構成で指定された値が含まれている場合は、アクセスが許可されます。
  - 有効にした場合の動作：
    1. AppDynamicsは、SAMLアクセス属性フィールドで指定された属性をSAML応答から取得します。
    2. 属性の値は、選択したメソッド（等しいか含む）に基づいて、ユーザー定義のアクセス比較値と比較されます。
    3. 比較が成功すると、ユーザにアクセス権が付与されます。
    4. 比較が失敗すると、ログイン試行が拒否されます。
- Save（右下隅）をクリックして、設定を保存します。



確認

- ブラウザを開き、AppDynamics Controllerに移動します。サードパーティIdPサービスのログインダイアログが表示されます。
- Log in with Single Sign-Onをクリックします。IdPにリダイレクトされます。
- クレデンシャルを入力して送信します。

- 認証に成功すると、IdPによってAppDynamicsコントローラーにリダイレクトされます。

一般的な問題と解決策

400件の不正な要求

- 問題： AppDynamics Controllerにログインしようとすると、400 Bad Requestエラーが発生します。
- サンプルエラー：

```
HTTP status 400 - Bad Request
Message: Error while processing SAML Authentication Response - see server log for details
Description: The request sent by the client was syntactically incorrect.
```

- 一般的な根本原因：
  - 無効なSAML証明書
  - SAML応答が最大長を超えています
  - 無効なエンティティIDまたはACS URL
- ソリューション：
  - 無効なSAML証明書
    - IDプロバイダー(IdP)から提供された証明書が有効で最新であることを確認してください。
    - IdP証明書の有効期限を確認します。有効期限が切れている場合は、IdPから新しい証明書を取得します。
    - 証明書がIdP側で更新されている場合は、新しい証明書がAppDynamicsにアップロードされ、構成されていることを確認します。
    - AppDynamicsで証明書を更新する手順：
      - アカウント所有者ロール、または管理、エージェント、入門ウィザード権限を持つロールとして、コントローラUIにログインします。
      - ユーザ名（右上隅）> Administration > Authentication Provider > Select SAMLの順にクリックします。
      - SAML Configurationセクションで、certificate フィールドを探し、古い証明書をIdPによって提供される新しい証明書で置き換えます。
      - Saveをクリックして、SAML設定を更新します。
  - SAML応答が最大長を超えています。
    - この問題は、コントローラをGlassFishからJetty Serverに移行した場合に発生します。コントローラのバージョンは23.11以降です。Jettyサーバーには、-Dorg.eclipse.jetty.serverという名前のプロパティがあります。Request.maxFormContentSizeは、.../appserver/jetty/start.d/start.iniファイルにあります。 SAML応答サイズがこのプロパティに設定されている値を超えると、コントローラはペイロードを拒否し、400 Bad Requestを返します エラー。
    - 大量のSAML応答の原因：
      - 過剰な属性：SAMLアサーションに含まれる属性が多すぎます。

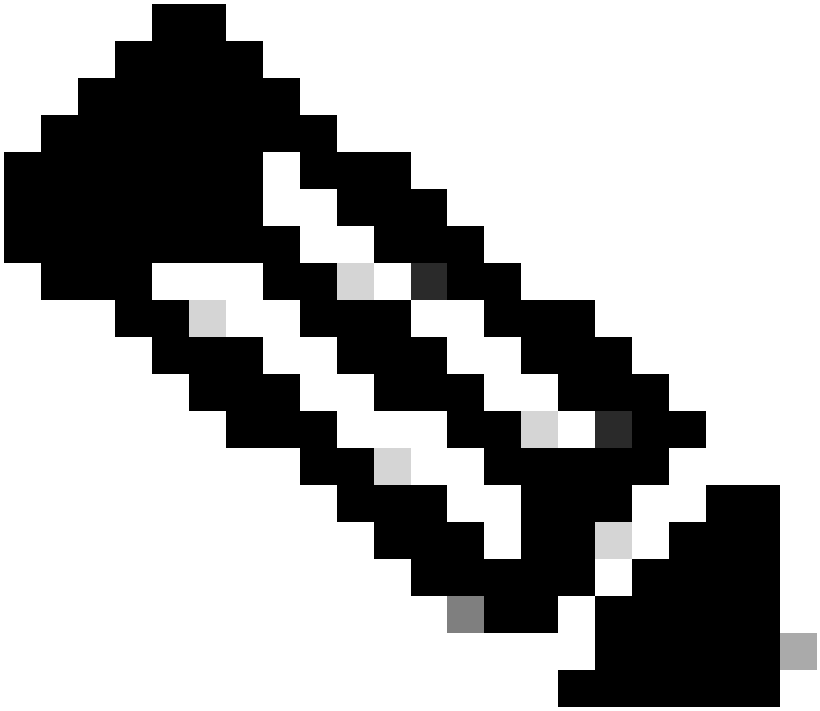
- 署名付きまたは暗号化されたSAML応答：署名または暗号化によって応答のサイズが大きくなります。
- 追加のユーザーまたはグループのデータ：アイデンティティプロバイダー(IdP)には、追加のユーザーまたはグループのデータがあります。

- この問題を解決するには、2つの方法があります。 これらのソリューションのいずれかまたは両方を実装することで、問題を解決し、ペイロードが拒否されないようにすることができます。
  1. maxFormContentSizeの値を大きくします
     - オンプレミスコントローラの場合：.../appserver/jetty/start.d/start.iniファイルの –Dorg.eclipse.jetty.server.Request.maxFormContentSizeプロパティをより大きな値に更新し、コントローラを再起動します。
     - SaaSコントローラの場合：サポートチームがこの問題に対処できるように、サポートチケットを発行します。

  2. SAML応答の最適化

     アイデンティティプロバイダー(IdP)と連携し、次の調整を行ってSAML応答のサイズを削減します。

     - 不要な属性の除外：IdP設定を使用して、未使用または重複する属性をSAMLアサーションから削除します。
     - 暗号化を無効にする（許可されている場合）：暗号化によりSAML応答サイズが増加します。接続がすでにHTTPS経由で保護されている場合は、暗号化を無効にしてサイズを縮小することを検討してください。
- 無効なエンティティIDまたはACS URL
  - Idpで次の手順を実行します。
    - エンティティIDがhttps://your_controller_domain/controllerであることを確認します。エンティティIDが異なる場合は更新します。
    - ACS URLがhttps://your_controller_domain/controller/saml-auth?accountName=youraccountnameであることを確認します。ACS URLが異なる場合は、それに応じて更新します。



注: accountNameはAppDynamicsアカウント名と一致する必要があります。（customer1など）。

- ユーザ権限の欠落
  - 問題：コントローラに正常にログインしました。 ただし、目的のロールと権限を受け取っていません。
  - 設定例とSAML応答：
    - SAMLユーザのGroup属性では、名前はGroupsであり、値はAppD_Adminおよび AppD_Power_Userです。

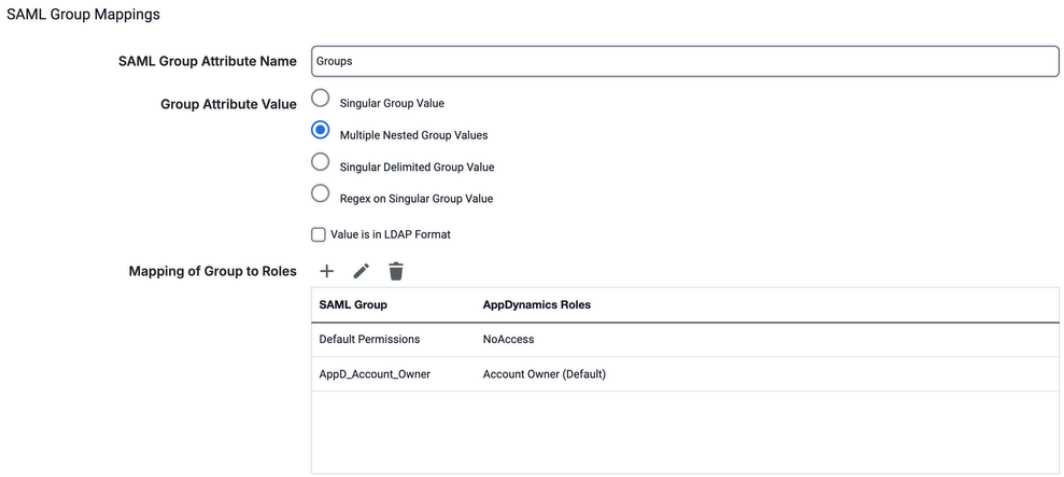
```
AppD_Admin
```

```
AppD_Power_User
```

- AppDynamicsのSAML Group Mappingsセクションで、これらが設定されます。
  - SAMLグループ属性名：Groups
  - グループ属性値：複数のネストされたグループ値
  - グループロールへのマッピング：

SAMLグループ	AppDynamicsロール
アプリケーション D_アカウント_所有者	アカウント所有者（デフォルト）
既定のアクセス許可	アクセスなし

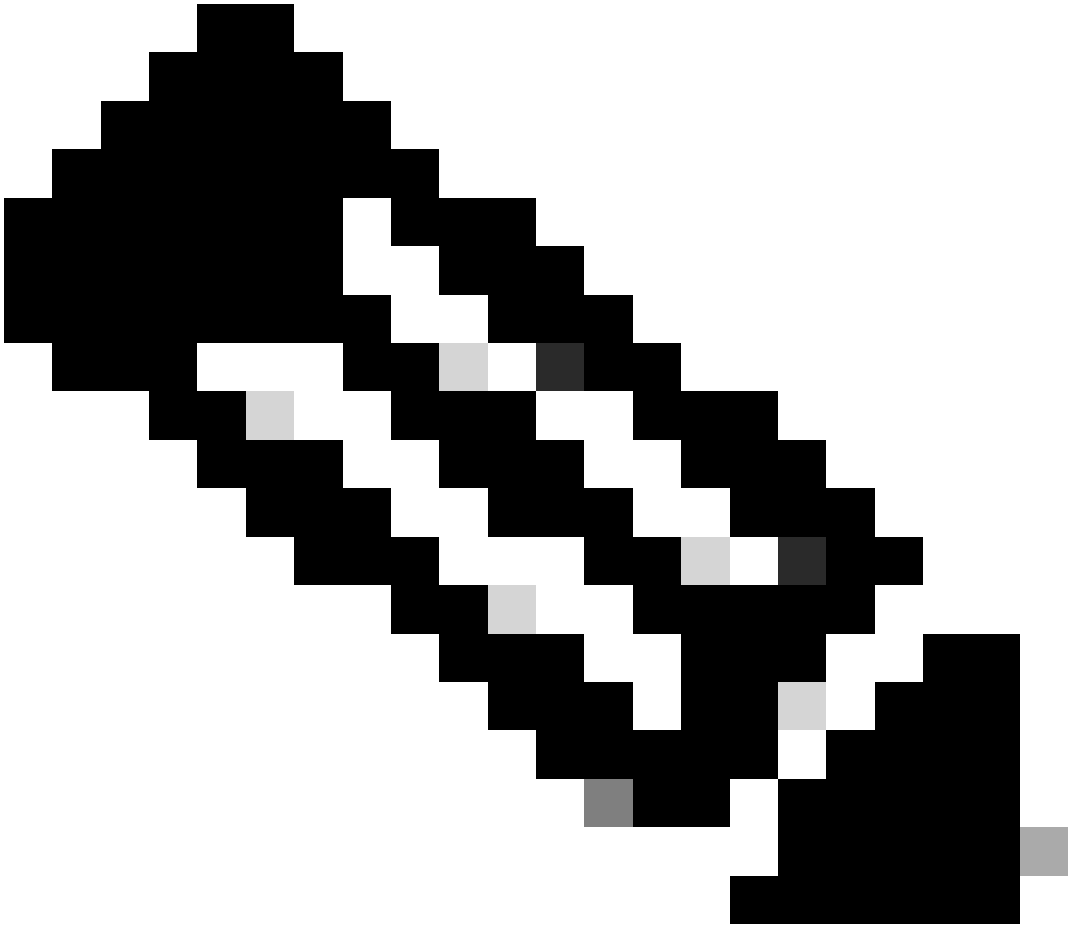
No Accessは、権限のないカスタムロールです。



- 一般的な問題と解決策
  - SAML応答にグループ属性が見つかりませんでした。
    - IdPからのSAML応答に必要なグループ属性がないか、SAML応答内のグループの属性名がロールとして設定されているのに対し、AppDynamicsではグループとして設定されています。
    - グループ属性が指定されていない場合、AppDynamicsの既定のアクセス許可に関連付けられているロールがユーザーに自動的に割り当てられます。
    - この問題を解決するには、SAML応答に正しいグループ属性を含めるようにIdPを設定し、グループの属性名がAppDynamicsの構成と一致していることを確認します。

  - SAML応答で指定されたユーザーグループに対応するSAMLグループマッピングがAppDynamicsで構成されていません。
    - SAML応答では、Groups属性に値AppD_AdminおよびAppD_Power_Userが含まれます。ただし、AppDynamicsでは、グループのマッピングはAppD_Account_Ownerグループに対してのみ存在します。

- AppD_AdminまたはAppD_Power_Userに対応するマッピングがないため、ユーザにはロールや権限が割り当てられていません。
- これを解決するには、AppDynamicsで不足しているグループマッピング（AppD_AdminとAppD_Power_Userなど）を追加し、ロールと権限の割り当てが適切であることを確認します。



注：デフォルトの権限は、AppDynamicsで設定されているSAMLグループ属性名がSAML応答のグループ属性と同じでない場合にのみSAMLユーザに適用されます。

- SAMLユーザの電子メールまたは名前が見つからないか、正しくない
  - 問題：これは通常、AppDynamicsの属性の設定がSAML応答に含まれる属性と一致しない場合に発生します。
  - SAML応答の例：属性SAML応答には、User.email、User.fullName、およびGroupsがあります

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- AppDynamicsでのSAML属性マッピングの例
  - ユーザ名属性：User.name
  - 表示名の属性： User.firstNameまたは空白
  - 電子メール属性： User.userPrincipalまたは空白

- 根本原因： AppDynamicsで構成されている表示名と電子メール属性が、SAML応答で指定されているどの属性とも一致しません。
  - その結果、
    - 電子メールは空白に設定されています。
    - 表示名はデフォルトでユーザ名に設定されます。

- 解決方法： AppDynamicsで構成されている表示名と電子メールの属性が、SAML応答の対応する属性と一致していることを確認してください。
  - 例：
    - [表示名]属性をUser.fullNameに更新します。
    - Email属性をUser.emailに更新します。

- HTTP 404 Error

- 問題：ユーザがコントローラにログインできず、「404 not found」エラーが表示される。
- サンプルエラー：コントローラログ（オンプレミスコントローラのみ）に次のエラーが表示されます。

```
[#|2025-01-10T21:16:35.222+0000|SEVERE|glassfish 4.1|com.singularity.ee.controller.auth.saml.SAMLA
com.appdynamics.platform.services.auth.exception.SamlException: Requested url validation failed
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.validateRequest
    at com.appdynamics.platform.services.auth.impl.saml.SamlRequestResponseHandler.getSamlAuthenti
```

- 根本原因：このエラーは通常、コントローラデータベースに設定されているコントローラURLが、ログインに使用されるコントローラURLまたはIdPで設定されているURLと一致しない場合に発生します
- ソリューション：
  - オンプレミスコントローラの場合：
    - コントローラURLを更新するには、次のコマンドを実行します（推奨）。

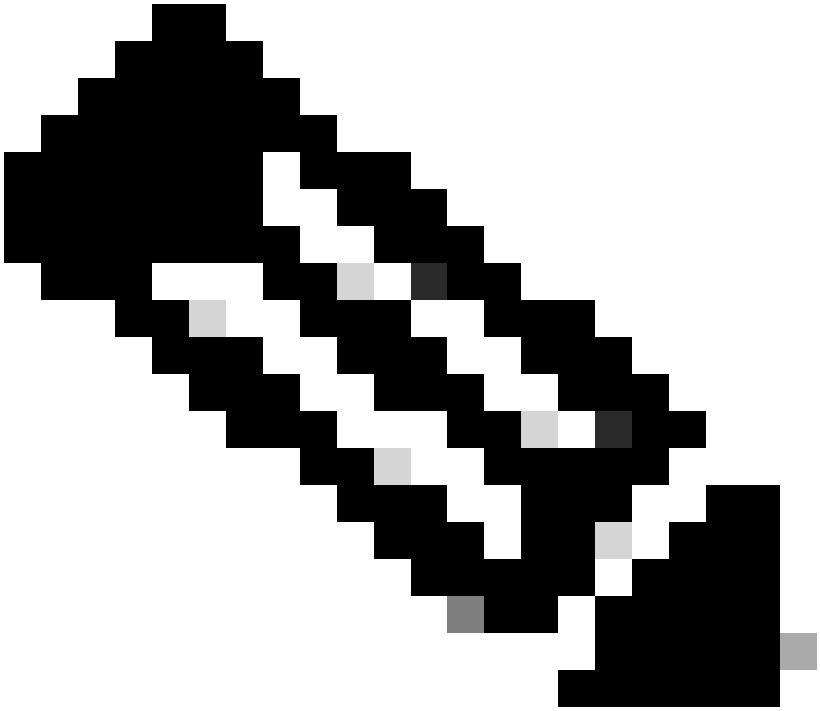
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- または、コントローラデータベースで次のコマンドを実行して、コントローラURLを更新することもできます。

```
UPDATE controller.account SET controller_url ='

             ' WHERE id=

              ;
UPDATE mds_auth.account SET controller_url='

               ' WHERE name='

                ';
```

- 次のコマンドを実行して<ACCOUNT_ID>を取得します。

```
Select id from controller.account where name = '

                  ';
```



注：引き続き同じ問題が発生する場合は、curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAllを実行します。

- 置換：
  - <NEW_CONTROLLER_URL>に、コントローラへのアクセスに使用している実際のコントローラURLを入力します。
  - <controller_domain>コマンドを使用します。
  - <youraccountname>にアカウント名を入力します。

- SaaSコントローラの場合：サポートチームがこの問題に対処できるように、サポートチケットを発行します。

さらなる支援が必要

質問がある場合、または問題が発生した場合は、次の詳細情報を記載したサポートチケットを作成してください。

- エラーの詳細またはスクリーンショット：特定のエラーメッセージまたは問題のスクリーンショットを提供します。
- SAML応答：SAMLトレースおよびHARファイルの収集
- Controller Server.log（オンプレミスのみ）：必要に応じて、<controller-install-

dir>/logs/server.logからコントローラサーバログを提供します。

関連情報

AppDynamicsドキュメント

SaaS導入向けSAML

SaaS展開のSAML応答の暗号化

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。