Configurer et dépanner l'authentification unique dans AppDynamics

Table des matières

Introduction

Ce document décrit comment configurer l'authentification unique (SSO) dans AppDynamics et résoudre les problèmes.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Pour configurer l'authentification unique, l'utilisateur doit disposer du rôle Propriétaire de compte (par défaut) ou d'un rôle personnalisé avec l'autorisation Administration, Agents, Assistant Mise en route.
- Accès administrateur à votre compte IdP.
- Métadonnées ou détails de configuration d'AppDynamics (par exemple, ID d'entité, URL ACS).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Contrôleur AppDynamics

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'authentification unique (SSO) est un mécanisme d'authentification qui permet aux utilisateurs de se connecter une seule fois et d'accéder à plusieurs applications, systèmes ou services sans devoir s'authentifier à nouveau pour chacun d'eux.

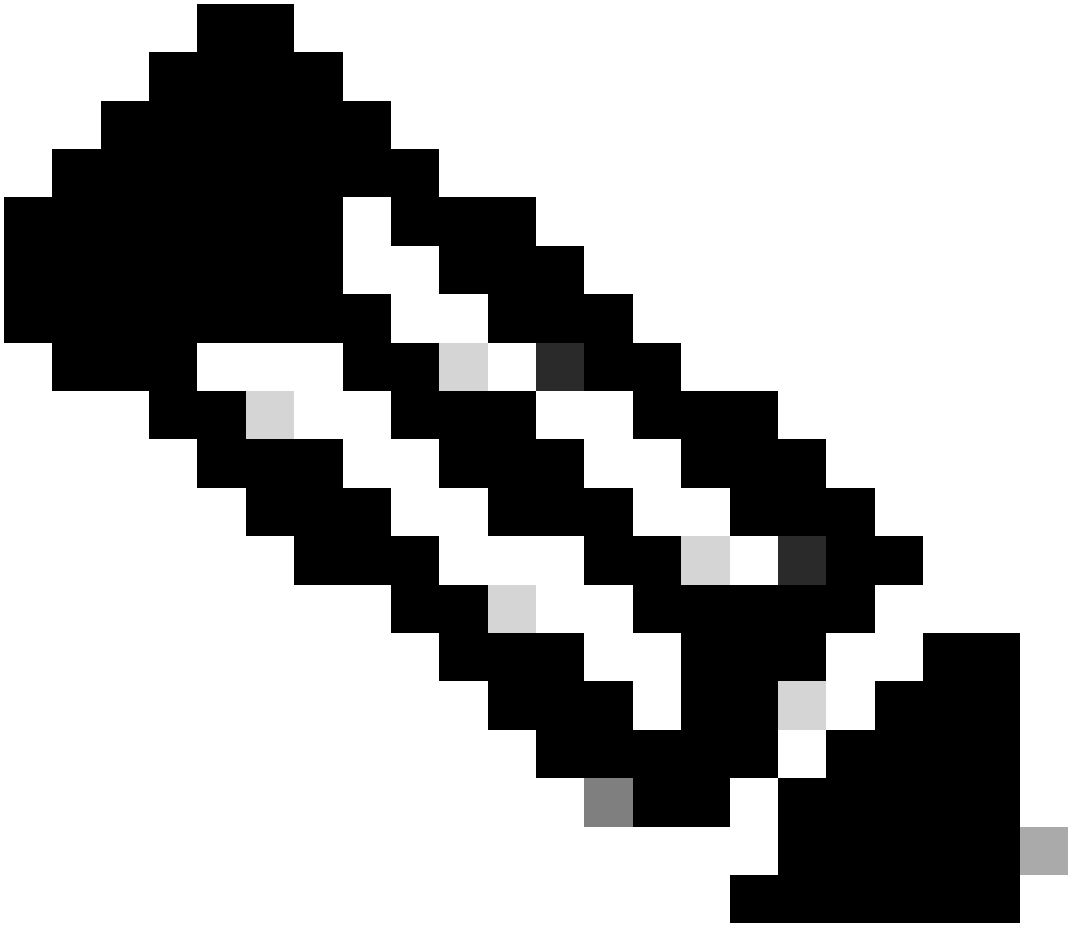
Le langage SAML (Security Assertion Markup Language) est l'une des technologies utilisées pour implémenter SSO. Il fournit le cadre et les protocoles qui permettent l'authentification unique en échangeant en toute sécurité des données d'authentification et d'autorisation entre un fournisseur d'identité (IdP) et un fournisseur de services (SP).

Assertion SAML

- Les messages XML échangés entre le fournisseur d'identité et le fournisseur de services.
- Il fournit trois types d'assertions :
  - Assertions d'authentification : Confirme que l'utilisateur a été authentifié.
  - Assertions d'attribut : Partage les attributs utilisateur, tels que le nom d'utilisateur ou les rôles.
  - Affirmations de décision d'autorisation : Indique ce que l'utilisateur est autorisé à faire.

Rôles clés dans SAML

- Fournisseur d'identité (IdP)
  - Vérifie l'identité de l'utilisateur.
  - Générez l'assertion SAML qui contient les informations d'identification de l'utilisateur.
- Fournisseur de services (SP)
  - Application ou système auquel l'utilisateur souhaite accéder.
  - Se fie au fournisseur d'identité pour authentifier l'utilisateur.
  - Accepte l'assertion SAML pour accorder à l'utilisateur l'accès à ses ressources ou à son application.
- Utilisateur (Principal)
  - Utilisateur ayant initié la demande ou essayant d'accéder à une ressource à partir du fournisseur de services.
  - Interagit à la fois avec le fournisseur d'identité (authentification) et le fournisseur de services.



Remarque : AppDynamics prend en charge les SSO initiés par IdP et SP.

Flux initié par SP :

- L'utilisateur accède au fournisseur de services en tapant l'URL de l'application (par exemple, AppDynamics) ou en cliquant sur un lien.
- Le SP recherche une session existante. S'il n'existe aucune session, le SP reconnaît que l'utilisateur n'est pas authentifié et lance le processus SSO.
- Le SP génère une demande d'authentification SAML et redirige l'utilisateur vers le fournisseur d'identité pour authentification.
    - Cette demande inclut :
        - ID d'entité : Identificateur unique du fournisseur de services.
        - URL ACS (Assertion Consumer Service) : où le fournisseur d'identité envoie l'assertion SAML après authentification.
        - Métadonnées relatives au SP et aux détails de sécurité (par exemple, demande signée, exigences de cryptage).
- L'utilisateur est redirigé vers la page de connexion du fournisseur d'identité.

- Le fournisseur d'identité authentifie l'utilisateur (par exemple, via un nom d'utilisateur/mot de passe ou une authentification multifacteur).
- Après une authentification réussie, le fournisseur d'identité génère une assertion SAML (jeton de sécurité).
- L'assertion SAML est renvoyée au SP via le navigateur de l'utilisateur à l'aide de la liaison HTTP POST (dans la plupart des cas) ou de la liaison HTTP Redirect.
- Le SP valide l'assertion SAML pour s'assurer :
    - Il a été émis par le fournisseur d'identité approuvé.
    - Il est adressé au SP (via l'ID d'entité SP).
    - Il n'a pas expiré ou n'a pas été falsifié (validé à l'aide de la clé publique IdP).

- Si l'assertion SAML est valide, le SP crée une session pour l'utilisateur.
- L'utilisateur a accès à l'application ou aux ressources.

Flux initié par IdP :

- L'utilisateur accède au portail de connexion IdP et entre ses informations d'identification.
- Le fournisseur d'identité authentifie l'utilisateur (par exemple, avec une combinaison nom d'utilisateur/mot de passe, authentification multifacteur).
- Après l'authentification, le fournisseur d'identité présente à l'utilisateur une liste des applications ou des services (SP) auxquels il peut accéder.
- L'utilisateur sélectionne le SP souhaité (par exemple, AppDynamics).
- Le fournisseur d'identité génère une assertion SAML pour le fournisseur de services sélectionné.

- L'IdP redirige l'utilisateur vers l'URL du service client d'assertion SP (ACS) et envoie l'assertion SAML avec elle (à l'aide de la liaison HTTP POST ou de la liaison de redirection HTTP).
- Le SP reçoit l'assertion SAML et la valide :
    - Garantit que l'assertion est émise par un fournisseur d'identité approuvé.
    - Vérifie l'intégrité et l'expiration des assertions.
    - Confirme l'identité de l'utilisateur et d'autres attributs.

- Si l'assertion SAML est valide, le SP crée une session pour l'utilisateur.
- L'utilisateur a accès à l'application ou aux ressources.

Configurer

Le contrôleur AppDynamics peut utiliser l'identité du client Cisco ou un fournisseur d'identité SAML externe (IdP) pour authentifier et autoriser les utilisateurs.

Fournisseurs d'identités pris en charge

AppDynamics certifie la prise en charge de ces fournisseurs d'identité (IdP) :

- Okta
- Onelogin

- Identité Ping
- Azure AD
- Identité cloud IBM
- Service de fédération Active Directory (AD FS)

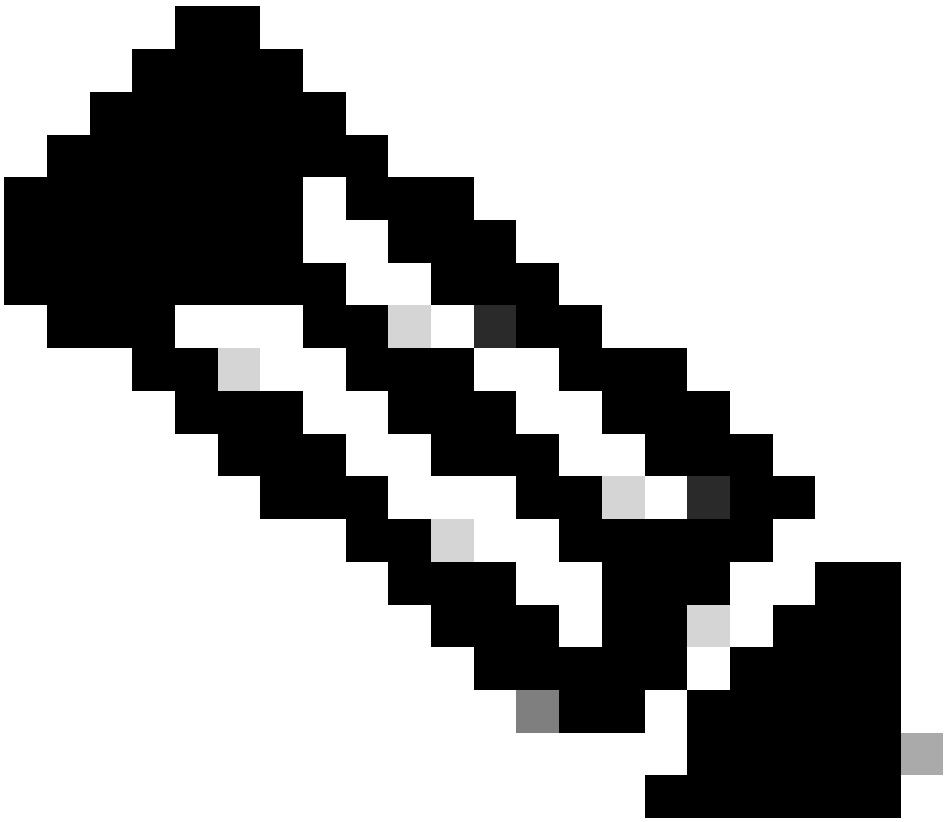
D'autres IdP prenant en charge la liaison HTTP POST sont également compatibles avec l'authentification SAML AppDynamics.

Étapes de configuration de SAML dans AppDynamics

Étape 1. Collecter les détails du contrôleur AppDynamics

- Entity ID (SP Entity ID) : identifiant unique pour AppDynamics (par exemple, https://<controller-host>:<port>/controller).
  - Syntaxe: https://<domaine_contrôleur>/contrôleur
  - exemple : https://<votre_domaine_contrôleur>/contrôleur

- URL de réponse (Assertion Consumer Service, ACS URL) : point de terminaison sur le fournisseur de services (par exemple, AppDynamics) où le fournisseur d'identité envoie la réponse SAML après l'authentification.
  - Syntaxe: https://<domaine_contrôleur>/contrôleur/saml-auth?accountName=<nom_compte>
  - exemple : https://your_controller_domain/controller/saml-auth?accountName=youraccountname



Remarque : Dans le cas d'un contrôleur On-Prem, le nom de compte par défaut est customer1, sauf si vous avez un contrôleur multilocataire avec un accountName différent.

- URL de déconnexion unique (Facultatif) : point de terminaison sur le SP pour gérer les demandes de déconnexion SAML (par exemple, https://<controller_domain>/controller).

Étape 2. Créer une nouvelle application dans IdP et télécharger les métadonnées

- Localisez la zone de création d'applications : elle se trouve généralement dans la console d'administration ou le tableau de bord du fournisseur d'identités, souvent appelée Applications, Applications Web et mobiles, Applications d'entreprise ou Parties utilisatrices.
- Add a custom or generic SAML application : sélectionnez une option qui vous permet de configurer une application SAML personnalisée ou une intégration de fournisseur de services SAML générique.
- Fournir les détails de l'application : donnez un nom à l'application et téléchargez éventuellement une icône pour identification (facultatif).
- Ajoutez des mappages d'attributs (Username, displayName, email ou roles) pour transmettre les informations utilisateur à AppDynamics.
- Téléchargez le fichier de métadonnées IdP ou notez les détails suivants :
  - URL de connexion IdP

- URL de déconnexion
- Noms des attributs
- Certificat

Étape 3. Configuration de l'authentification SAML dans AppDynamics Controller

- Connectez-vous à l'interface utilisateur du contrôleur en tant que propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Assistant Mise en route.
- Cliquez sur votre nom d'utilisateur(coin supérieur droit)> Administration > Authentication Provider > Select SAML.

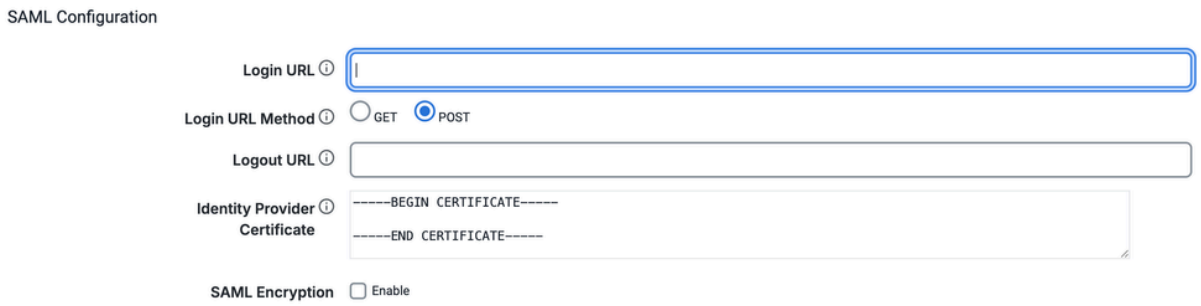
- Dans la section Configuration SAML, ajoutez ces détails :

  - URL de connexion : URL de connexion IdP où AppDynamics Controller route les demandes de connexion initiées par le fournisseur de services.

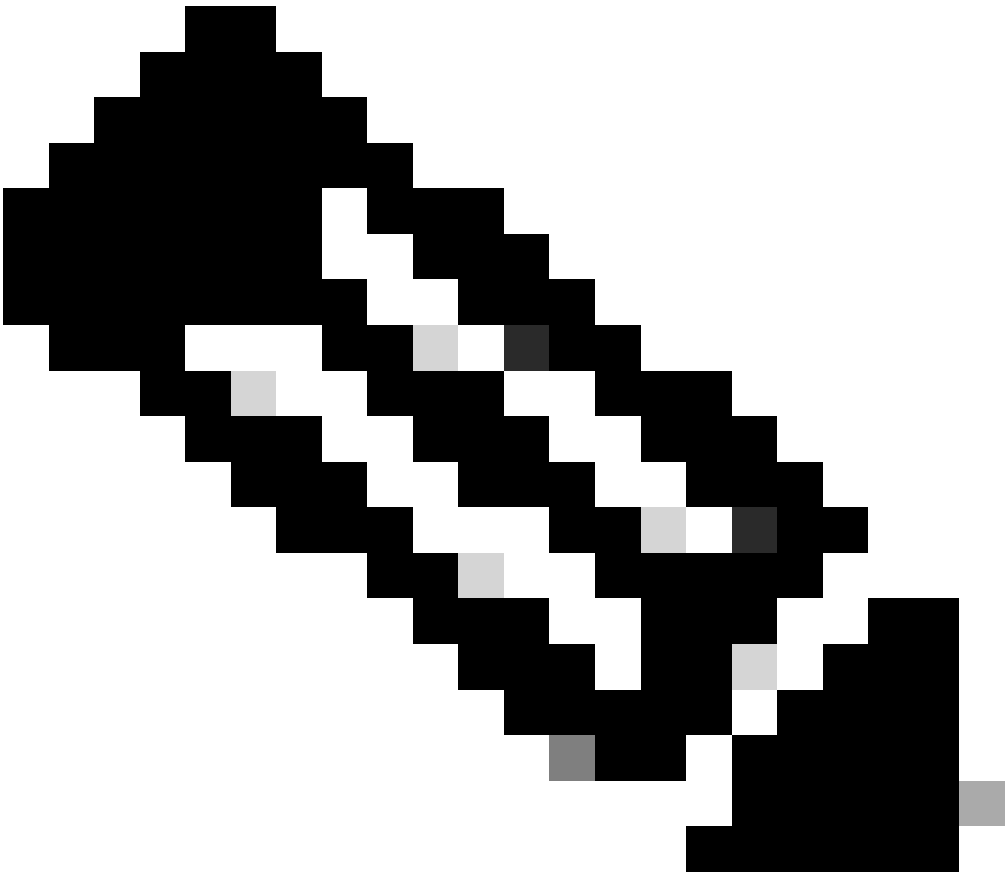
  - URL de déconnexion (facultatif) : URL vers laquelle AppDynamics Controller redirige les utilisateurs après leur déconnexion. Si vous ne spécifiez pas d'URL de déconnexion, les utilisateurs obtiennent l'écran de connexion AppDynamics lorsqu'ils se déconnectent.

  - Certificat: Certificat X.509 du fournisseur d'identité. Collez le certificat entre les délimiteurs BEGIN CERTIFICATE et END CERTIFICATE. Évitez de dupliquer les délimiteurs BEGIN CERTIFICATE et END CERTIFICATE à partir du certificat source.

  - Chiffrement SAML (Facultatif) : vous pouvez améliorer la sécurité de l'authentification SAML en chiffrant la réponse SAML du fournisseur d'identités vers le fournisseur de services. Pour chiffrer les réponses SAML dans AppDynamics, vous devez configurer votre fournisseur d'identités (IdP) pour chiffrer l'assertion SAML, puis configurer le contrôleur AppDynamics pour utiliser un certificat et une clé privée spécifiques pour le déchiffrement.



- Dans la section Mappages d'attributs SAML, mappez les attributs SAML (exemple : Nom d'utilisateur, DisplayName, Email) à leurs champs correspondants dans AppDynamics.

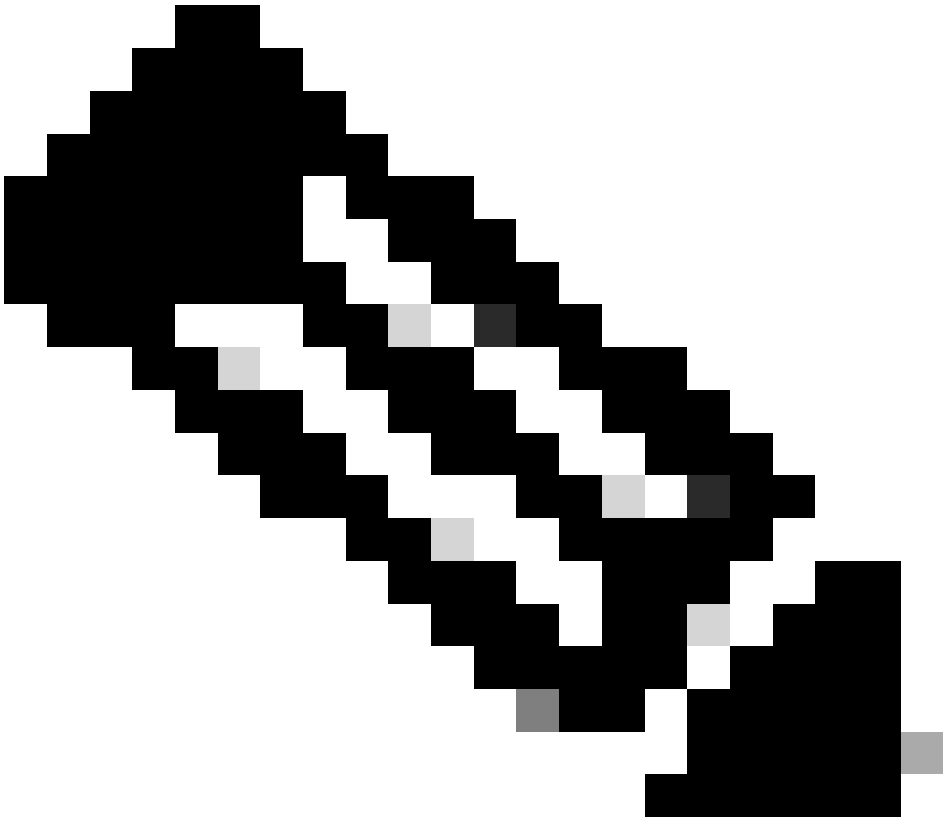


Remarque : AppDynamics affiche le nom d'utilisateur, le courrier électronique et le nom d'affichage d'un utilisateur SAML. Par défaut, il utilise l'attribut NameID de la réponse SAML pour créer un nom d'utilisateur, qui est également utilisé comme displayName. Ce comportement peut être personnalisé en incluant les attributs username, email et displayname dans la réponse SAML. Lors de la configuration des paramètres IdP dans AppDynamics, l'utilisateur peut spécifier ces noms d'attribut. Lors de la connexion, AppDynamics vérifie si le mappage d'attribut est configuré. Si des mappages sont configurés et que des attributs correspondants sont présents dans la réponse SAML, AppDynamics utilise ces valeurs d'attribut pour définir le nom d'utilisateur, l'e-mail et le nom d'affichage.

- Dans la section Mappages de groupes SAML, ajoutez ces détails.
  - Nom d'attribut de groupe SAML : saisissez le nom de l'attribut SAML qui contient les

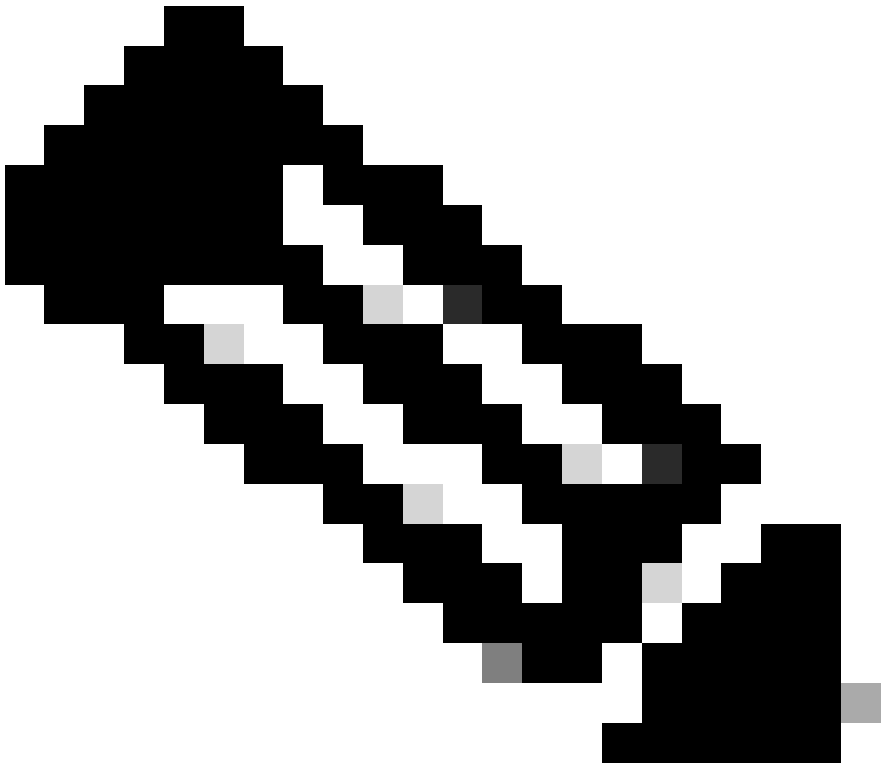
informations de groupe. Il s'agit généralement de Groupes, ou de groupes ou de rôles, ou de Rôles ou d'appartenance à un groupe.

- Valeur d'attribut de groupe : sélectionnez le format de valeur approprié pour l'attribut de groupe. Les options courantes sont Valeurs de groupe imbriquées multiples ou Valeur unique, selon la façon dont votre fournisseur d'identité structure les informations de groupe.

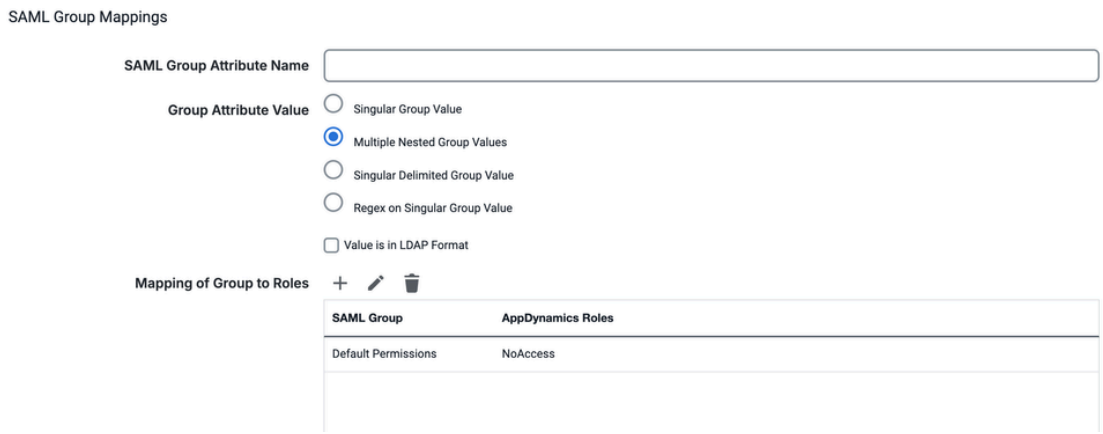


Remarque : Sélectionnez Valeur au format LDAP si les informations de groupe sont fournies au format LDAP (Lightweight Directory Access Protocol).

- Mapping of Group to Roles : cliquez sur le bouton + pour ajouter un nouveau mapping.
  - Groupe SAML : saisissez le nom du groupe SAML (tel que défini dans votre fournisseur d'identité) que vous souhaitez mapper à un rôle AppDynamics.
  - Rôle(s) : sélectionnez le ou les rôles AppDynamics correspondants dans la liste disponible que vous souhaitez attribuer aux utilisateurs appartenant au groupe SAML.
  - Autorisations par défaut : si le mappage de groupe SAML n'est pas configuré ou si une assertion SAML d'utilisateur n'inclut pas d'informations de groupe, AppDynamics revient à utiliser les autorisations par défaut.

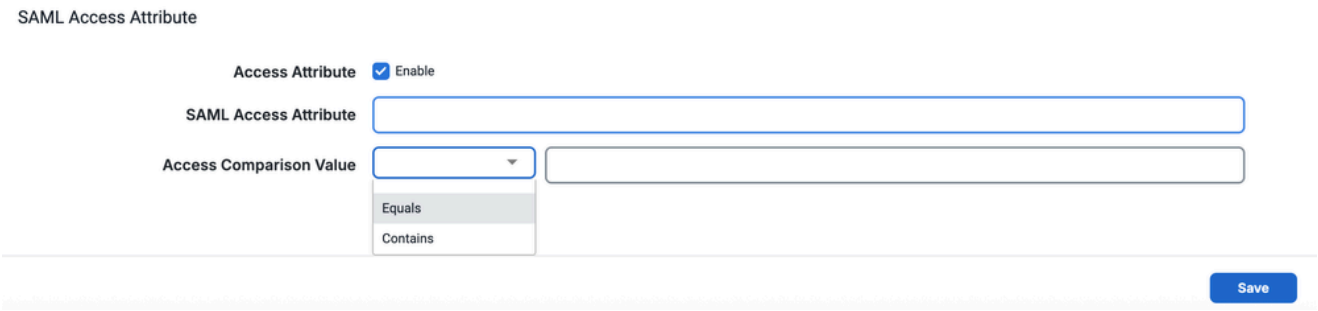


Remarque : Il est recommandé d'attribuer un rôle avec des autorisations minimales aux autorisations par défaut.



- Dans la section Attribut d'accès SAML, ajoutez les détails suivants (facultatif) :
  - Attribut d'accès SAML : Saisissez le nom des attributs de la réponse SAML. Il sera utilisé pour la validation de l'accès.

    - Valeur de comparaison d'accès : deux options sont disponibles :
        1. Égal : L'accès est accordé uniquement si la valeur d'attribut de la réponse SAML correspond exactement à la valeur spécifiée dans la configuration.
        2. Contient : L'accès est accordé si la valeur d'attribut de la réponse SAML contient la valeur spécifiée dans la configuration.
    - Fonctionnement si cette option est activée :
        1. AppDynamics récupère l'attribut spécifié dans le champ Attribut d'accès SAML à partir de la réponse SAML.
        2. Il compare la valeur de l'attribut à la valeur de comparaison d'accès définie par l'utilisateur en fonction de la méthode sélectionnée (Égal à ou Contient).
        3. Si la comparaison réussit, l'utilisateur est autorisé à y accéder.
        4. Si la comparaison échoue, la tentative de connexion est refusée.
- Cliquez sur Save (Save (Bas à droite) pour enregistrer la configuration.



Vérifier

- Ouvrez un navigateur et accédez à AppDynamics Controller. La boîte de dialogue Connexion de votre service fournisseur d'identité tiers s'affiche.
- Cliquez sur Connexion avec authentification unique. Le système vous redirige vers votre fournisseur d'identité.
- Saisissez et envoyez vos informations d'identification.
- Une fois l'authentification réussie, le fournisseur d'identité vous redirige vers votre AppDynamics Controller.

Problèmes courants et solution

400 Requête incorrecte

- Problème : les utilisateurs rencontrent une erreur 400 Bad Request lors de leur tentative de connexion à AppDynamics Controller.
- Exemple d'erreur :

```
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.
```

- Causes profondes courantes :
    - Certificat SAML non valide
    - La réponse SAML est supérieure à la longueur maximale
    - ID d'entité ou URL ACS non valide
- Solution :
    - Certificat SAML non valide
        - Assurez-vous que le certificat fourni par le fournisseur d'identité (IdP) est valide et à jour.
        - Vérifiez la date d'expiration du certificat IdP. S'il a expiré, obtenez un nouveau certificat auprès du fournisseur d'identité.
        - Si le certificat a été mis à jour côté IdP, assurez-vous que le nouveau certificat est chargé et configuré dans AppDynamics.
        - Étapes de mise à jour du certificat dans AppDynamics :
            - Connectez-vous à l'interface utilisateur Controller en tant que rôle de propriétaire de compte ou rôle avec l'autorisation Administration, Agents, Getting Started Wizard.
            - Cliquez sur votre nom d'utilisateur(coin supérieur droit)> Administration > Authentication Provider > Select SAML.
            - Dans la section Configuration SAML, localisez le champ certificate et remplacez l'ancien certificat par le nouveau fourni par l'IdP.
            - Cliquez sur Save pour mettre à jour la configuration SAML.

    - La réponse SAML est supérieure à la longueur maximale.
        - Ce problème survient lorsque le contrôleur est déplacé de GlassFish vers Jetty Server, en commençant par la version 23.11 du contrôleur et les versions ultérieures. Dans Jetty Server, il existe une propriété nommée -Dorg.eclipse.jetty.server. Request.maxFormContentSize situé dans le .../appserver/jetty/start.d/start.ini. Si la taille de réponse SAML dépasse la valeur définie pour cette propriété, le contrôleur rejette la charge utile et renvoie une requête 400 erronée erreur .
        - Causes des réponses SAML importantes :
            - Attributs excessifs : Trop d'attributs inclus dans l'assertion SAML.
            - Réponses SAML signées ou chiffrées : La signature ou le chiffrement augmente la taille de la réponse.
            - Données d'utilisateur ou de groupe supplémentaires : Le fournisseur d'identité (IdP) a des données d'utilisateur ou de groupe supplémentaires.

        - Il existe deux façons de résoudre ce problème. En implémentant l'une de ces solutions ou les deux, vous pouvez résoudre le problème et empêcher le rejet de la charge utile.
            1. Augmenter la valeur maxFormContentSize
                - Pour Les Contrôleurs Sur Site : Mettez à jour la propriété -Dorg.eclipse.jetty.server.Request.maxFormContentSize dans le .../appserver/jetty/start.d/start.ini à une valeur plus élevée et

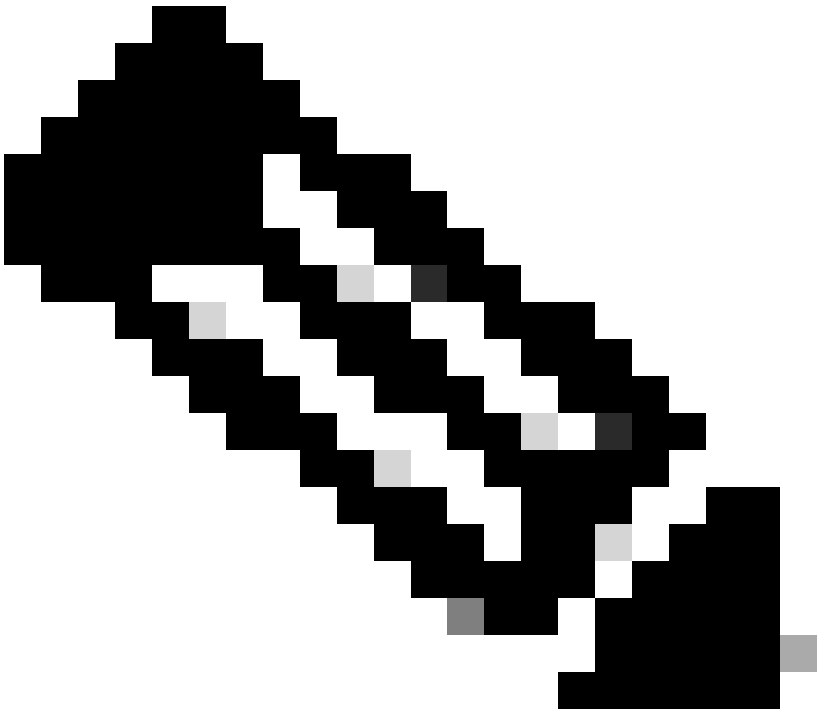
redémarrez le contrôleur.
- Pour les contrôleurs SaaS : Déposez une demande d'assistance pour que l'équipe d'assistance puisse résoudre ce problème.

2. Optimiser la réponse SAML

   Travaillez avec votre fournisseur d'identité (IdP) pour réduire la taille de la réponse SAML en effectuant les ajustements suivants :

   - Exclure les attributs inutiles : Supprimez les attributs inutilisés ou redondants de l'assertion SAML via la configuration IdP.
   - Désactiver le chiffrement (si autorisé) : Le chiffrement augmente la taille de la réponse SAML. Si la connexion est déjà sécurisée via HTTPS, pensez à désactiver le cryptage pour réduire la taille.

- ID d'entité ou URL ACS non valide
  - Sur l'Idp :
    - Vérifiez que l'ID d'entité est https://your_controller_domain/controller. Si l'ID d'entité est différent, mettez-le à jour.
    - Vérifiez que l'URL ACS est https://your_controller_domain/controller/saml-auth?accountName=youraccountname. Si l'URL ACS est différente, mettez-la à jour en conséquence.



Remarque : accountName doit correspondre à votre nom de compte AppDynamics. (par exemple, client1)

- Autorisations utilisateur manquantes
    - Problème : vous vous êtes correctement connecté au contrôleur. Cependant, vous n'avez pas reçu les rôles et autorisations prévus.
    - Exemple de configuration et de réponse SAML :
        - Dans l'attribut Group de l'utilisateur SAML, le nom est Groupes avec les valeurs AppD_Admin et AppD_Power_User.

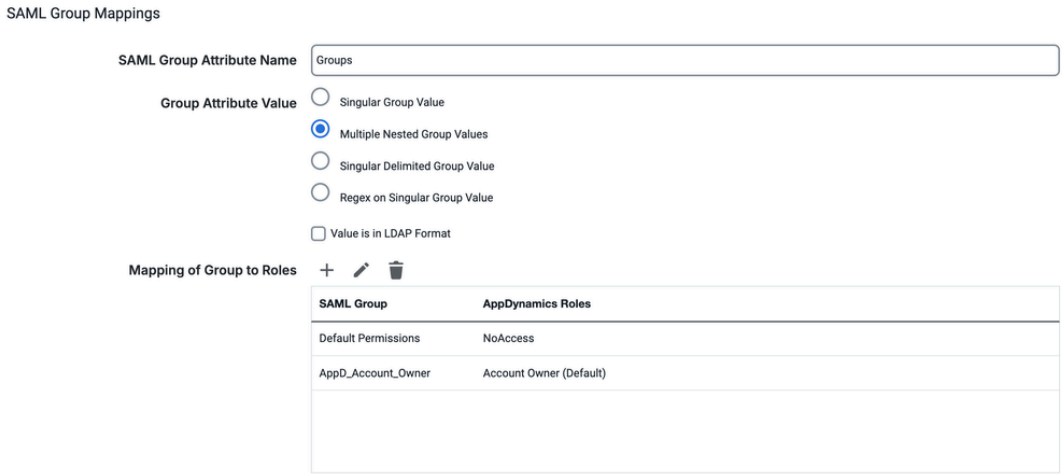
```
AppD_Admin
```

```
AppD_Power_User
```

        - Dans AppDynamics, sous la section Mappages de groupes SAML, ils sont configurés.
            - Nom d'attribut de groupe SAML : Groupes
            - Valeur d'attribut de groupe : Valeurs de groupes imbriqués multiples
            - Mappage vers des rôles de groupe :

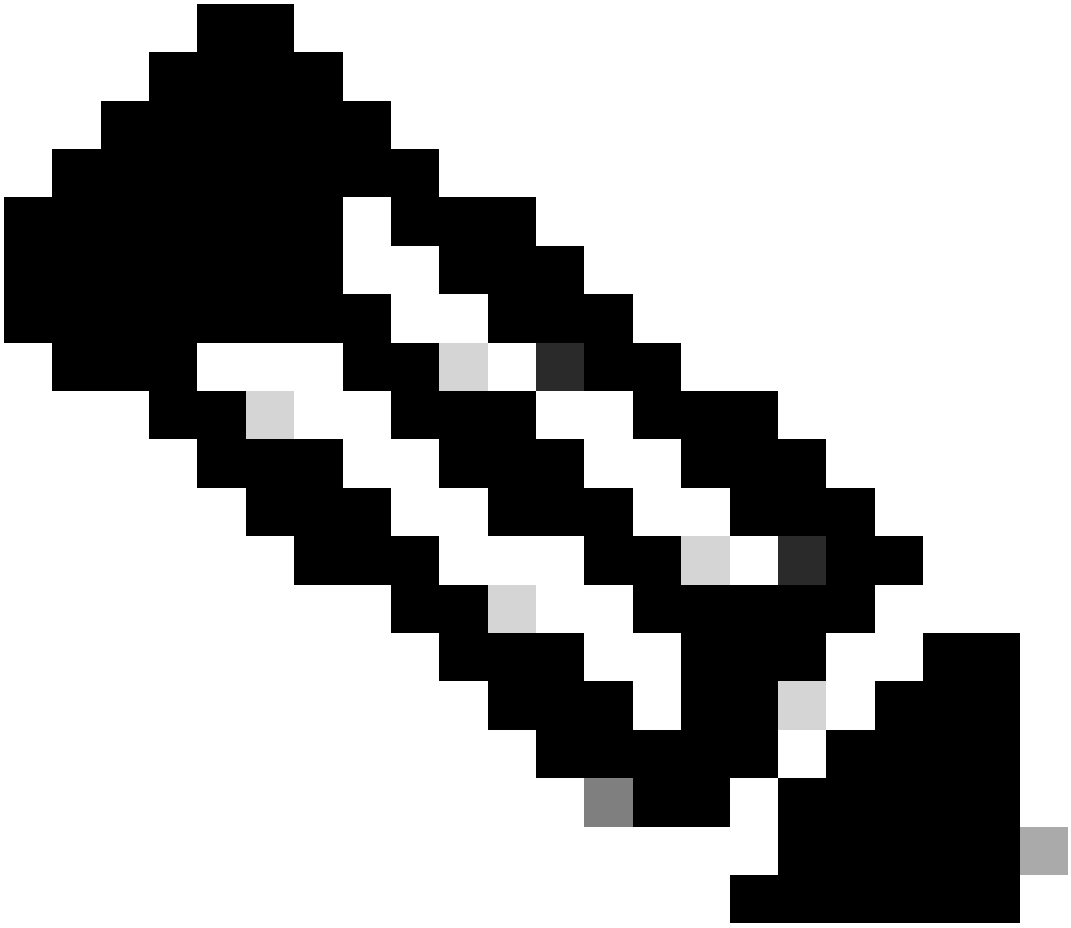
Groupe SAML	Rôles AppDynamics
AppD_Account_Owner	Propriétaire du compte (par défaut)
Autorisations par défaut	Aucun accès

            Aucun accès est un rôle personnalisé sans autorisation.



- Problèmes courants et solution
  - Aucun attribut de groupe trouvé dans la réponse SAML.
    - Les attributs de groupe requis sont manquants dans la réponse SAML du fournisseur d'identité ou le nom d'attribut des groupes dans la réponse SAML est défini comme Rôles alors que dans AppDynamics, il est configuré comme Groupes.
    - Lorsqu'aucun attribut de groupe n'est fourni, les rôles associés aux autorisations par défaut dans AppDynamics sont automatiquement affectés à l'utilisateur.
    - Pour résoudre ce problème, assurez-vous que le fournisseur d'identité est configuré pour inclure les attributs de groupe corrects dans la réponse SAML et que le nom d'attribut des groupes correspond à la configuration dans AppDynamics.

  - Aucun mappage de groupe SAML correspondant n'est configuré dans AppDynamics pour les groupes d'utilisateurs fournis dans la réponse SAML.
    - Dans la réponse SAML, l'attribut Groups contient les valeurs AppD_Admin et AppD_Power_User. Toutefois, dans AppDynamics, les mappages de groupe existent uniquement pour le groupe AppD_Account_Owner.
    - Comme il n'existe aucun mappage correspondant pour AppD_Admin ou AppD_Power_User, aucun rôle ni aucune autorisation n'est attribué à l'utilisateur.
    - Pour résoudre ce problème, ajoutez les mappages de groupe manquants (par exemple, AppD_Admin et AppD_Power_User) dans AppDynamics pour garantir l'attribution correcte des rôles et des autorisations.



Remarque : Les autorisations par défaut ne sont appliquées aux utilisateurs SAML que lorsque le nom d'attribut de groupe SAML configuré dans AppDynamics est différent des attributs Groupes de la réponse SAML.

- E-mail et/ou nom manquants ou incorrects pour les utilisateurs SAML
  - Problème : Cela se produit généralement lorsque la configuration d'attribut dans AppDynamics ne correspond pas aux attributs entrant dans la réponse SAML.
  - Exemple de réponse SAML : Attributs Dans la réponse SAML : User.email, User.fullName et Groups

example@domain.com

FirstName LastName

AppD_Admin

AppD_Power_User

- Exemple de mappages d'attributs SAML dans AppDynamics
  - Attribut de nom d'utilisateur : Nom.utilisateur
  - Attribut du nom d'affichage : User.firstName ou vide
  - Attribut de messagerie : User.userPrincipal ou vide

- Cause première : les attributs Display Name et Email configurés dans AppDynamics

ne correspondent à aucun des attributs fournis dans la réponse SAML.
    - En conséquence :
        - L'e-mail est défini sur vide.
        - Le nom d'affichage est par défaut le nom d'utilisateur.

- Solution : Assurez-vous que les attributs Display Name et Email configurés dans AppDynamics correspondent aux attributs correspondants dans la réponse SAML.
    - Exemple :
        - Mettez à jour l'attribut Display Name en User.fullName.
        - Mettez à jour l'attribut Email en User.email.

- Erreur HTTP 404

- Problème : l'utilisateur ne peut pas se connecter au contrôleur et obtenir l'erreur 404 not found.
- Exemple d'erreur : Dans les journaux du contrôleur (uniquement pour le contrôleur On-Prem), vous voyez cette erreur :

```
[#|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
```

- Cause première : cette erreur se produit généralement lorsque l'URL du contrôleur configurée dans la base de données du contrôleur ne correspond pas à l'URL du contrôleur utilisée pour la connexion ou à l'URL configurée sur le fournisseur d'identité
- Solution :
    - Pour Les Contrôleurs Sur Site :
        - Exécutez cette commande pour mettre à jour l'URL du contrôleur (recommandé).

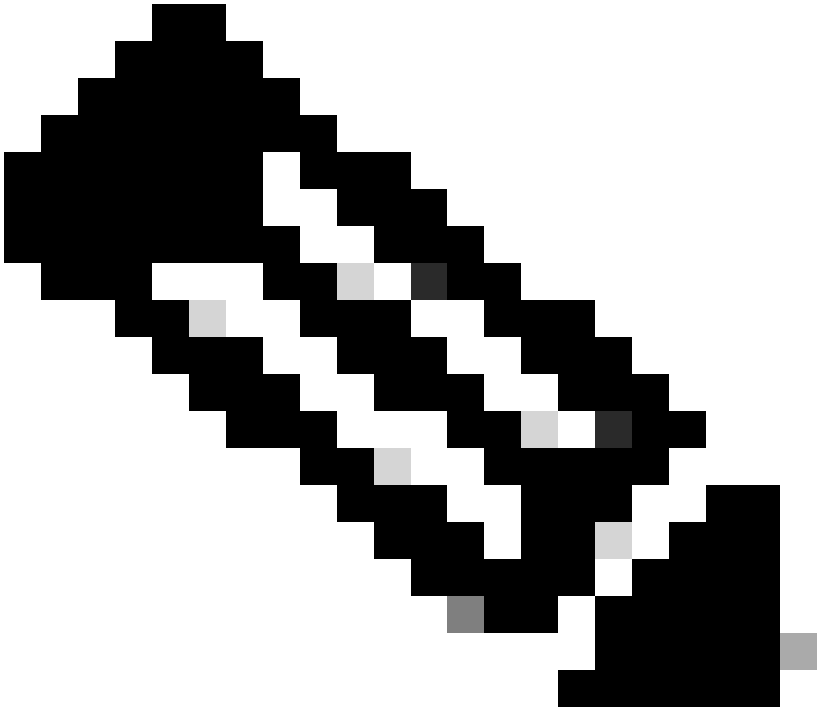
```
curl -k --basic --user root@system --header "Content-Type: application/json" --data '{

/controller" }' http://

/controller/rest/accounts/

/update-controller-url
```

- Vous pouvez également exécuter ces commandes dans la base de données du contrôleur pour mettre à jour l'URL du contrôleur.

```
UPDATE controller.account SET controller_url ='


            ' WHERE id=


             ;
UPDATE mds_auth.account SET controller_url='


              ' WHERE name='


               ';
```

  - Exécutez cette commande pour obtenir l'<ID_COMPTE>.

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


                ';
```



Remarque : Exécutez curl -X POST -u root@system https://<controller_domain>/controller/api/controllermds/syncAll si vous observez toujours le même problème.

- Remplacer :
  - <NEW_CONTROLLER_URL> avec l'URL réelle du contrôleur que vous utilisez pour accéder au contrôleur.
  - <controller_domain> avec votre domaine de contrôleur.
  - <votrenomcompte> avec votre nom de compte.

- Pour les contrôleurs SaaS : Déposez une demande d'assistance pour que l'équipe d'assistance puisse résoudre ce problème.

Besoin d'une assistance supplémentaire

Si vous avez une question ou rencontrez des problèmes, créez un ticket d'assistance avec les informations suivantes :

- Error Details or Screenshot : fournissez un message d'erreur spécifique ou une capture d'écran du problème.
- Réponse SAML : collecte des fichiers SAML-Trace et HAR
- Controller Server.log (On-Prem uniquement) : le cas échéant, fournissez les journaux du serveur contrôleur à partir de <controller-install-dir>/logs/server.log

Informations connexes

Documentation AppDynamics

SAML pour les déploiements SaaS

Chiffrer les réponses SAML pour les déploiements SaaS

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.