Configurez le portail de sponsor ISE 2.1 avec PingFederate SAML SSO

Contenu

Introduction

Ce document décrit comment configurer un serveur de PingFederate SAML avec des gestions d'identité Engine(ISE) 2.1 de Cisco pour fournir des capacités simples d'On(SSO) de signe pour commanditer des utilisateurs.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Services d'invité de Logiciel Cisco Identity Services Engine.
- Connaissance de base au sujet des déploiements SAML SSO.

Composants utilisés

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

- Version 2.1 de Logiciel Cisco Identity Services Engine
- Serveur de PingFederate 8.1.3.0 d'identité de ping.
- Windows Server 2012 R2 avec des services de Répertoire actif.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un

environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de toutes les commandes.

Conventions

Référez-vous au Conventions relatives aux conseils techniques Cisco pour plus d'informations sur des conventions de document

Aperçu d'écoulement

Le Langage SAML (SAML) est une norme de XML pour permuter des données d'authentification et d'autorisation entre les domaines de sécurité.

La spécification SAML définit trois rôles : le directeur (utilisateur de sponsor), le fournisseur d'identité (IDP) (serveur fédéré de ping), et le fournisseur de services (fournisseur de services) (ISE). Dans un SAML typique SSO circulent, le fournisseur de services demande et obtient une assertion d'identité à l'IDP. Basé sur ce résultat, ISE peut exécuter des décisions politiques pendant que l'IDP peut inclure des attributs configurables qu'ISE peut l'utiliser pendant les décisions politiques. Une fois l'authentification initiale se produit, l'utilisateur ne devrait pas être incitée pour des qualifications de nouveau à accéder au service tant que la session d'assertion est encore en activité sur l'IDP.

C'est l'écoulement prévu pour ce cas d'utilisation :

1. Les tentatives d'utilisateur d'ouvrir une session au portail de sponsor en lançant le nom de domaine complet fait sur commande du portail configuré de sponsor (FQDN).
2. ISE vérifie s'il y a une assertion active associée à la session du navigateur de ce client en émettant un redirect to rapide l'IDP. S'il n'y a aucune session active, l'IDP imposera l'ouverture de session utilisateur.
3. L'IDP authentifie l'utilisateur par l'intermédiaire du LDAP et passe des attributs de memberOf et d'email à ISE(SP).
4. ISE traite la réponse de l'IDP XML et basé sur l'attribut de memberOf et sur la configuration de groupes de sponsor l'utilisateur sera permis ou rejeté (contrôle d'état d'adhésion à des associations pour apparier un groupe configuré de sponsor).
5. Le Time to Live de session variera sur chaque solution. Dans ce cas d'utilisation, le ping Federate sera configuré avec une **Session Timeout de** 60 minutes (s'il n'y a aucune demande de procédure de connexion SSO d'ISE en 60 minutes après que l'authentification initiale, la session est supprimée) et un **délai d'attente maximum de session de** 480 minutes (même si l'IDP avait reçu des demandes constantes de procédure de connexion SSO d'ISE pour cet utilisateur que la session expirera en 8 heures). Une fois les temps de session, une nouvelle authentification de l'utilisateur est imposée par l'IDP.
6. Tandis que la session est encore en activité, l'utilisateur de sponsor devrait pouvoir clôturer le navigateur et le retour au portail sans entrer dans des qualifications.

Configurez

La section suivante discutera les étapes de configuration pour intégrer ISE avec le ping fédéré et comment activer le navigateur SSO pour le portail de sponsor.

Remarque: Bien que les diverses options et possibilités existent quand vous authentifiez des utilisateurs de sponsor, non toutes les combinaisons sont décrites dans ce document. Cependant, cet exemple te fournit les informations nécessaires pour comprendre comment modifier l'exemple à la configuration précise que vous voulez réaliser.

Étape 1. Préparez ISE pour utiliser un fournisseur externe d'identité SAML

1. Sur Cisco ISE, naviguez vers la **gestion > la Gestion de l'identité > des sources extérieures d'identité > des fournisseurs d'id SAML**.
2. Cliquez sur Add
3. Sous l'onglet Général, écrivez un nom de fournisseur d'id et cliquez sur la **sauvegarde**. Le reste de la configuration dans cette section dépendra des métadonnées qui doit être importée de l'IDP.

Étape 2. Configurez le portail de sponsor pour utiliser un fournisseur externe d'identité

1. Naviguez vers des **centres > l'accès invité de travail > configurent > des portails de sponsor**
2. Cliquez sur en fonction le **sponsor portail (par défaut)** ou créez un nouveau portail.
3. Sous les **configurations portailes** écrivez un nom de domaine complet fait sur commande (FQDN) lié à ce portail de sponsor.
4. Choisissez parmi l'**ordre de source d'identité que l'**IDP externe SAML a précédemment défini.
5. Vérifiez que l'organigramme représente la **sauvegarde** suivante et de clic :

Étape 3. Configurez PingFederate comme IDP pour traiter des demandes d'authentification ISE

1. Naviguez vers la **gestion > la Gestion de l'identité** ISE **> des sources extérieures d'identité > des fournisseurs >** PingFederate d'**id SAML**
2. Onglet de l'**information de fournisseur de services de** clic et **exportation de** clic

3. Sauvegardez et extrayez le fichier zip généré. Le fichier XML contenu ici sera utilisé tout en créant le profil dans PingFederate.

4. Ouvrez le portail d'admin de PingFederate (typiquement https://ip:9999/pingfederate/app).

5. Sous l'**onglet de configuration d'IDP > la** section de **connexions de fournisseur de services** choisis créez nouveau.

6. Sous le **type de connexion** cliquez sur Next

7. Sous des **possibilités de connexion** cliquez sur Next

8. Sous des **métadonnées d'importation**, le **fichier** choisi, a choisi le fichier et sélectionne le fichier XML précédemment exporté d'ISE.

9. Sous le **résumé de métadonnées**, cliquez sur en fonction **ensuite**.

10. À la page des informations générales, sous le **nom de la connexion** écrivez un nom (IE. ISEsponsorPortal) et cliquent sur Next.

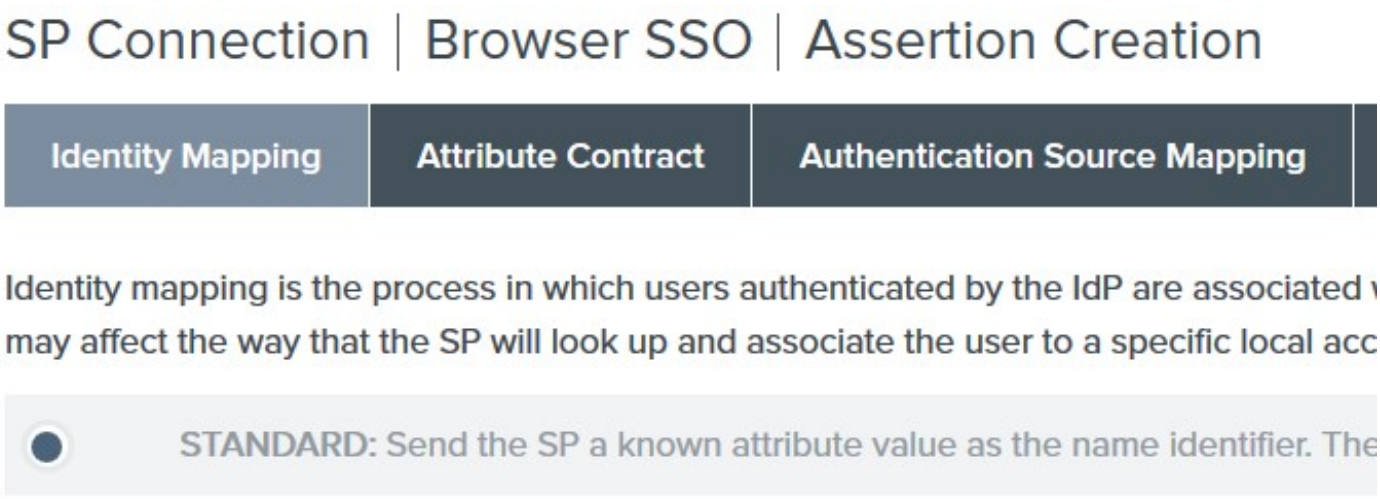
11. Sous le **navigateur SSO** cliquent sur Configure le **navigateur SSO** et sous le **SAML les profils**

vérifient ces options et cliquent sur Next :

12. Sur la **vie d'assertion** cliquez sur Next

13. Sur la **création d'assertion** cliquez sur Configure la **création d'assertion**

14. Sous **standard** choisi de **mappage d'identité** et cliquez sur Next



15. Sur le **contrat d'attribut > étendez le contrat** écrivent la **messagerie d'**attributs et le **memberOf** et le clic **ajoutent.** Cliquez ensuite sur **Next**.

> Remarque: C'est une étape essentielle car ISE se fonde sur ces attributs pour le mappage correct de groupe de sponsor et envoie également est nécessaire pour des fonctions correctes de notification.

16. Sous **exemple d'adaptateur de carte de** clic de **mappage de source d'authentification le nouvel**.

17. Sur l'**adaptateur** choisi de **formulaire HTML d'exemple d'adaptateur**. Cliquez sur **Next** (Suivant).

18. Sous la **méthode de mappage** sélectionnez la deuxième option et cliquez sur Next

19. Sur l'**attribut les sources et la consultation d'utilisateur** cliquent sur Add la case de **source d'attribut**.

20. Sous le **magasin de données** écrivez une description, puis choisissez parmi le **magasin de données actif** votre exemple de connexion de LDAP et définissez quel type de service d'annuaire c'est. S'il n'y a aucun magasin de données configuré pourtant cliquez sur en fonction les **magasins de données Manage** pour ajouter le nouveau citent.

21. Sous la **recherche de répertoire LDAP** définissez le **DN de base** pour la consultation d'utilisateur de LDAP dans le domaine et cliquez sur Next.

> Remarque: C'est important car il définira le DN de base pendant la consultation d'utilisateur

de LDAP. Le DN de base inexactement défini aura comme conséquence une erreur « objet non trouvé dans le schéma de LDAP ».

22. Sous le **filtre de LDAP** ajoutez la chaîne **sAMAccountName=$ {nom d'utilisateur}** et cliquez sur Next.

23. Sous l'**exécution de contrat d'attribut** sélectionnez ces options et cliquez sur Next

24. Vérifiez la configuration à la **partie récapitulative** et cliquez sur **fait**.

25. De retour dans l'**attribut la consultation de sources et d'utilisateur** cliquent sur Next.

26. Sous la **source de sécurité d'attribut** cliquez sur Next.

27. Sous l'**exécution de contrat d'attribut** sélectionnez ces options et cliquez sur Next :

27. Vérifiez la section et le clic de configuration en résumé **faits**.

28. De retour sur le **mappage de source d'authentification** cliquez sur Next.

29. Une fois que la configuration a été vérifiée sous le clic de **partie récapitulative fait**.

30. De retour sur la **création d'assertion** cliquez sur Next.

31. Sous **Protocol les configurations** cliquent sur Configure des **configurations de Protocol**.

En ce moment il devrait y avoir 3 entrées déjà remplies. Cliquez sur Next

32. Sous **SLO entretenez l'URLs** cliquent sur Next

33. Sur le **SAML permis les attaches** décochent les options **OBJET FAÇONNÉ** et **SAVON** et cliquent sur Next.

34. Dans le cadre de la **stratégie de signature** cliquez sur Next.

35. Dans le cadre de la **stratégie de chiffrement** cliquez sur Next.

36. Passez en revue la configuration dans la page **récapitulative** et cliquez sur **fait**.

37. De retour sur le **navigateur les configurations SSO >** de **Protocol** cliquent sur Next, valident la configuration et cliquent sur **fait**. Ceci rapportera le **navigateur que SSO** tableau cliquent sur Next.

38. Sous des **qualifications** cliquez sur Configure les **qualifications** et choisissez le certificat de signature à utiliser pendant l'IDP aux transmissions ISE et vérifiez l'option **incluent le certificat dans la signature**. Cliquez ensuite sur **Next**.

Remarque: S'il n'y a aucun Certificats configuré, le clic **gèrent des Certificats** et suivent les demandes pour générer un certificat Auto-signé à utiliser pour signer l'IDP aux transmissions ISE.

39. Validez la configuration sous la page **récapitulative** et cliquez sur **fait**.

40. De retour sur l'onglet de **qualifications** cliquez sur Next.

41. Sous le **lancement et le résumé** choisis sur l'**ACTIVE d'état de la connexion**, validez le reste de la configuration et cliquez sur la **sauvegarde**.

Étape 4. Importez les métadonnées d'IDP dans le profil externe de fournisseur d'IDP ISE SAML

1. Sous la console de gestion de PingFederate, naviguez vers la **configuration du serveur > les fonctions d'administration > les métadonnées exportent** si le serveur a été configuré pour de plusieurs rôles (IDP et fournisseur de services) sélectionnent l'option que **je suis l'identité Provider(IdP).** Cliquez sur Next

2. Sous les **informations choisies** choisies de mode de **métadonnées « à inclure dans les métadonnées manuellement ».** Cliquez sur **Next** (Suivant).

3. Sous **Protocol** cliquez sur Next.

4. Sur le **contrat d'attribut** cliquez sur Next.

5. Sous la **clé de signature** sélectionnez le certificat précédemment configuré sur le profil de connexion. Cliquez sur **Next** (Suivant).

6. Sous la **signature de métadonnées** sélectionnez le certificat de signature et le contrôle **incluent la clé publique de ce certificat dans l'élément d'information principale.** Cliquez sur **Next** (Suivant).

7. Sous le **certificat de cryptage XML** cliquez sur Next. L'option d'imposer le cryptage ici est jusqu'à l'admin de réseau.

8. Sous la sauvegarde d'**exportation de** clic de **partie récapitulative les** métadonnées classent généré et puis cliquent sur **fait**.

9. Sous ISE, naviguez vers la **gestion** > la **Gestion de l'identité** > des **sources extérieures d'identité** > des **fournisseurs** > **PingFederate d'id SAML**.

10. Cliquez sur en fonction le **fournisseur d'identité que le** >Click de **config parcourent** et poursuivez pour importer les métadonnées enregistrées de l'exécution d'exportation de métadonnées de Pingfederate.

11. L'onglet choisi de **groupes** et sous l'**attribut d'adhésion à des associations** ajoutent le **memberOf** et puis cliquent sur **ajoutent**

12. Sous le nom de **dans l'assertion** ajoutez le **nom unique** que l'IDP devrait renvoyer de retour quand l'attribut de **memberOf** est authentification LDAP récupérée de forme. Ce groupe sera lié au groupe de sponsor.

Une fois que vous ajoutez le DN et le « nom description dans ISE » cliquent sur OK.

13. L'onglet choisi d'**attributs** et cliquent sur Add. À cette étape nous ajouterons l'attribut **« messagerie »**. Ceci est contenu dans l'authentification SAML ; résultat passé de l'IDP (basé sur l'attribut d'email pour cet objet utilisateur dans le Répertoire actif).

Remarque: Cette étape est tout important qu'ISE devrait pouvoir traiter l'email lié à la session du sponsor pour pouvoir tracer tous les comptes dans l'état en suspens des écoulements auto-enregistrés. Autrement les comptes demeureront dans un état fictif car la « personne étant » email visité ne sera pas tracée à une session valide de sponsor. Il est également important pour la notification électronique propose.

14. Sous l'**onglet Avancé** sélectionnez les configurations suivantes :

Remarque: Cette section demandera à ISE d'inclure l'attribut d'email dans des demandes de déconnexion au serveur de LDP. C'est important quand l'utilisateur de sponsor se ferme une session manuellement du portail.

15. Cliquez sur **Save**.

16. Dans cette étape l'administrateur tracera le groupe de Répertoire actif récupéré par l'IDP à un groupe de sponsor. Naviguez vers des **centres** > l'**accès invité de travail** > **configurent** > **sponsor groupe** > **ALL_ACCOUNTS** (ou sélectionnez le groupe approprié). Cliquez sur les **membres** et sélectionnez le **PingFederate** : **Groupez-**nous a tracé dans les étapes précédentes et l'ajoute à la colonne de groupes d'utilisateur sélectionné. Cliquez ensuite sur **OK**.

17. Quand l'écoulement enregistré par individu est configuré, les comptes seront en attendant l'approbation. Dans ce cas, choisi **« approuvez et des demandes de vue des invités auto-enregistrés »** et sélectionnez **« seulement en attendant des comptes assignés à ce sponsor »** car une méthode facile de vérifier l'adresse e-mail d'objet est AD et transférés vers l'identité de sponsor dans ISE par le serveur d'IDP utilisant l'attribut de **messagerie**.

18. Cliquez sur **Save**. Ceci termine la configuration dans ISE.

Vérifiez

1. Lancez le portail de sponsor utilisant le FQDN configuré de coutume. ISE devrait réorienter l'utilisateur au portail d'authentification de l'utilisateur de PingFederate.
2. Entrez dans les qualifications de Répertoire actif et le hit se connectent. L'écran de connexion d'IDP réorientera l'utilisateur à l'AUP d'initiale sur le portail du sponsor d'ISE.

En ce moment l'utilisateur de sponsor devrait avoir l'accès complet au portail.

3. Vérifiez simple se connectent. Quand la caractéristique « **URL portail de test** » est utilisée ISE devrait demander des qualifications de sponsor chaque fois si SSO n'est pas configuré.

Lancez le portail de sponsor avec le lien portail URL de test. L'URL de sponsor ISE commutera rapidement à l'URL d'IDP pour vérifier l'état de session et une fois que le jeton de session est confirmé le client est réorienté de nouveau au portail de sponsor sans besoin d'entrer dans des qualifications.

4. Vérifiez que l'attribut d'email est passé correctement de l'objet de Répertoire actif à l'IDP à ISE. Le moyen le plus simple de tester est en créant un nouveau compte dans le sponsor portail et en sélectionnant l'option de **notification**. Si l'email est récupéré correctement il apparaîtra sous le champ de l'**adresse e-mail du** sponsor.

5. Vérifiez la fonction de **déconnexion**. Il est crucial dans l'intégration vérifier ce que la déconnexion de sponsor déclenche la session symbolique à terminer sur le côté serveur d'identité. Déconnectez-vous du sponsor portail et assurez-vous que la prochaine fois que les essais d'utilisateur pour accéder au portail de sponsor, il seront réorientés de nouveau à l'écran d'authentification d'IDP.

Dépannez

N'importe quelle transaction d'authentification SAML sera côté ouvert une session ISE sous **ise-psc.log**. Il y a un composant dédié (**SAML**) sous la **gestion > se connectant > configuration de log de debug >** sélectionnent le noeud en question **>** a placé le **SAML** composant **pour mettre au point** de niveau.

Nous pouvons accéder à ISE par le CLI et émettre « une queue d'ise-psc.log d'application de show logging » et surveiller les événements SAML vivez, ou nous pouvons télécharger **ise-psc.log** pour l'analyse approfondie sous des **exécutions > dépannons >** des **logs de téléchargement >** sélectionnons l'onglet de **logs de** noeud **>** de **debug** ISE **>** le clic **ise-psc.log** pour télécharger les logs.

Typiquement le log initial d'authentification ressemblera à ceci :

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>


2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Après événement de procédure de connexion initiale, chaque fois que les accès client le portail de sponsor nous verront ISE récupérant les informations d'assertion pour vérifier que le jeton est encore en activité. Le résultat devrait ressembler à ceci :

```
2016-06-13 10:18:58,560 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML request -
spUrlToReturnTo:https://torsponsor21.rtpaaa.net:8443/sponsorportal/SSOLoginResponse.action

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response:
statusCode:urn:oasis:names:tc:SAML:2.0:status:Success

2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
```

```
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
mail
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<mail> add value=<antontor@rtpaaa.net>


2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Found attribute name :
memberOf
2016-06-13 08:39:36,925 DEBUG  [http-bio-14.36.157.210-8443-exec-7][]
cpm.saml.framework.impl.SAMLAttributesParser -:::::- [parseAttributes] Delimeter not configured,
Attribute=<memberOf> add value=<CN=TOR,DC=rtpaaa,DC=net>
```

Informations connexes

Notes en version pour le Logiciel Cisco Identity Services Engine, version 2.1

Guide de l'administrateur de Logiciel Cisco Identity Services Engine, version 2.1