Contenu

Introduction

Ce document décrit comment configurer la version 2.1 d'Engine(ISE) de gestions d'identité de Cisco aux capacités simples d'On(SSO) de signe de provoide pour les utilisateurs portaiux d'invité par le markup Language(SAML) d'assertion de Sécurité.

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 de 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 comme identité Provider(IdP) SAML

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 n'importe quelle configuration appliquée.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

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 d'invité), le fournisseur d'identité [IDP] (serveur fédéré d'IPing), 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 (c.-à-d. groupe et adresse e-mail associés à l'objet d'AD).

Écoulement prévu pour ce cas d'utilisation :

1. WLC ou commutateur d'accès Est configuré pour un écoulement central typique de l'authentification Web (CWA).

   Conseil : Veuillez trouver les exemples de configuration pour CWA entre dans la **section Informations connexes au** bas de l'article

2. Le client se connecte et la session obtient authentifié contre ISE. L'accès au réseau Device(NAD) applique les paires de valeur d'attributs de réorientation (AVPs) retournées par ISE (l'URL-réorienter-acl et URL-réorientent).

3. Le client ouvre le navigateur, génère le trafic de HTTP ou HTTPS et l'obtient réorienté à ISE ? portail d'invité s.

4. Une fois dans le portail le client pourra entrer dans les qualifications précédemment assignées d'invité (**sponsor créé**), auto-disposition un nouveau compte d'invité ou employer ses qualifications d'AD pour ouvrir une session (**procédure de connexion des employés**) qui fournira simple connectez-vous les capacités par le SAML.

5. Une fois que l'utilisateur sélectionne l'option de ? Procédure de connexion des employés ? ISE vérifie s'il y a une assertion active associée à ce client ? gainst de session du navigateur s l'IDP. S'il n'y a aucune session active, l'IDP imposera l'ouverture de session utilisateur. À cette étape l'utilisateur sera incité à entrer dans des qualifications d'AD dans le portail d'IDP directement.

6. L'IDP authentifie l'utilisateur par l'intermédiaire du LDAP et il crée une nouvelle assertion qui restera active pendant un temps configurable.

   Remarque: Le ping fédéré par défaut appliquera une **Session Timeout de** 60 minutes (ceci signifie que s'il n'y a aucune demande de procédure de connexion SSO d'ISE en 60 minutes après 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).

Tant que la session d'assertion est encore en activité, l'employé éprouvera SSO quand portail d'invité de gthe d'usin. Une fois la session chronomètre une nouvelle authentification de l'utilisateur sera imposée par l'IDP.

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 d'invité.

> Remarque: Bien que les diverses options et possibilités existent quand vous authentifiez des utilisateurs d'invité, 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 naviguent 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 de **Genaral** écrivez un **nom de fournisseur d'id**. Cliquez sur en fonction la **sauvegarde**. Le reste de la configuration dans cette section dépendra des métadonnées qui doit être importée de l'IDP dans les étapes postérieures.

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

1. Naviguez vers des **centres > l'accès invité de travail > configurent > des portails d'invité**
2. Créez un nouveau **portail Auto-enregistré** portail et choisi d'**invité**.

> Remarque: Ce ne sera pas le portail principal que l'utilisateur éprouvera mais un subportal qui interagira avec l'IDP pour vérifier l'état de session. J'appellerai ce SSOSubPortal portail.

3. Développez les **configurations portailes** et sélectionnez **PingFederate** pour la **méthode d'authentification**.

4. Choisissez parmi l'**ordre de source d'identité le** defined(PingFederate) externe d'IDP SAML précédemment.

5. Développez les sections de **mises en page de bannière d'Acceptable Use Policy(AUP)** et de POST-**procédure de connexion** et désactivez chacun des deux.

Écoulement portail :

6. Sauvegardez les modifications.

7. Retournez aux portails d'invité et créez un neuf utilisant l'option Auto-**enregistrée de portail d'invité.**

> Remarque: Ce sera le visible portail primaire au client. Le portail primaire utilisera le SSOSubportal comme interface entre ISE et l'IDP. Nous nommerons ce PrimaryPortal portail.

8. Développez les **mises en page de procédure de connexion** et sélectionnez le **SSOSubPortal** précédemment créé dessous ? **Permettez le portail suivant d'invité d'identité-fournisseur à utiliser pour la procédure de connexion** ?.

9. Développez les **mises en page de bannière AUP et de POST-procédure de connexion de Politique d'Utilisation Acceptable** et décochez-les.

En ce moment l'écoulement portail devrait ressembler à ceci :

10. Cliquez sur en fonction la **personnalisation > les pages > la procédure de connexion portailes**. Nous devrions maintenant avoir l'option de personnaliser les **options alternatives de procédure de connexion** (icône, texte, etc.).

> Remarque: Notez cela du côté droit, sous l'aperçu portail, l'option supplémentaire de procédure de connexion est visible.

11. Cliquez sur **Save**.

Maintenant les deux portails devraient apparaître sous la liste portaile d'invité.

Étape 3. Configurez PingFederate pour agir en tant que fournisseur d'identité pour le portail d'invité ISE

1. Dans ISE, naviguez vers la **gestion > la Gestion de l'identité > des sources extérieures d'identité > des fournisseurs > PingFederate d'id SAML** et cliquez sur les **informations de fournisseur de services**
2. Sous l'**exportation de** clic de l'**information de fournisseur de services d'exportation**

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

> Remarque: À partir de là, nous couvrirons la configuration de PingFederate. Cette configuration sera identique pour de plusieurs solutions comme le portail de sponsor, le MyDevices et les portails BYOD. (Ces solutions ne sont pas couvertes en cet article)

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.

le résumé des métadonnées 9.Under, cliquent sur en fonction ensuite.

la page des informations générales 10.On, sous le nom de la connexion écrivent un nom (IE. ISEGuestWebAuth) et cliquent sur Next.

11. Sous le navigateur SSO cliquent sur Configure le navigateur SSO et sous le SAML les profils vérifient les options suivantes et cliquent sur Next :

la vie de l'assertion 12.On cliquent sur Next

la création de l'assertion 13.On cliquent sur Configure la création d'assertion

standard choisis de mappage de l'identité 14.Under et cliquent sur Next

15. Sur le contrat d'attribut > étendez le contrat écrivent la messagerie d'attributs et le clic de memberOfand ajoutent. Cliquez sur Next alors

Configurer cette option permettra au fournisseur d'identité pour passer le MemberOf et pour envoyer des attributs fournis par le Répertoire actif à ISE, qu'ISE peut utiliser plus tard comme condition pendant la décision politique.

exemple d'adaptateur de carte de clic de mappage de source de l'authentification 16.Under nouvel.

adaptateur choisi de formulaire HTML d'exemple de l'adaptateur 17.On. Cliquez sur Next

18. Sous le mappage les méthodes sélectionnent la deuxième option vers le bas et cliquent 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, et 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 le clic parviennent des magasins de données 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 l'objet non trouvé dans le schéma de LDAP.

le filtre du LDAP 22.Under ajoutent la chaîne sAMAccountName=$ {nom d'utilisateur} et cliquent sur Next.

23. Sous l'**exécution de contrat d'attribut** sélectionnez les options suivantes 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 :

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

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

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

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

32. Sous le clickNext de **configurations de Protocol configurez les configurations de Protocol**. En ce moment il devrait y avoir 2 entrées déjà remplies. Cliquez sur **Next** (Suivant).

33. Sous SLO entretenez l'URLs cliquent sur Next

34. Sur les attaches permises SAML, décochez les options OBJET FAÇONNÉ et SAVON et cliquez sur Next**.**

35. Dans le cadre de la stratégie de signature cliquez sur Next.

36. Dans le cadre de la stratégie de chiffrement cliquez sur Next.

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

38. De retour sur le navigateur les configurations SSO > de Protocol cliquent sur Next, valident la configuration et cliquent sur **fait**.

39. Ceci nous amènera de nouveau au navigateur que SSO tableau cliquent sur Next.

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

> Remarque: S'il n'y a aucun clic configuré par Certificats **gérez les Certificats** et suivez les demandes pour générer un **certificat Auto-signé** à utiliser pour signer l'IDP aux transmissions ISE.

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

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

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

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 > l'exportation de métadonnées.** Si le serveur a été configuré pour de plusieurs rôles (IDP et fournisseur de services) sélectionnez l'option que **je suis l'identité Provider(IdP).** Cliquez sur Next
2. Sous le mode de **métadonnées** choisi **? Sélectionnez les informations pour 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-ils ce certificat ? clé publique s dans l'élément d'information principale.** Cliquez sur **Next** (Suivant).

7. Sous le **certificat de cryptage XML** cliquez sur Next.

Remarque: L'option d'imposer le cryptage ici est jusqu'à l'admin de réseau.

8. Sous l'**exportation de** clic de **partie récapitulative**. Sauvegardez 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 le **config de fournisseur d'identité > parcourent** et poursuivent pour importer les métadonnées enregistrées de l'exécution d'exportation de métadonnées de PingFederate.

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

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 récupérée de la forme LADP. Dans ce cas le groupe configuré est lié au groupe de sponsor du MASSIF DE ROCHE et le DN pour ce groupe est comme suit :

Une fois que vous ajoutez le DN et ? Nom dans ISE ? la description cliquent sur OK.

12. L'onglet choisi d'**attributs** et cliquent sur Add.

Àcette étape nous ajouterons l'attribut ? messagerie ? cela est contenu dans le jeton SAML passé de l'IDP qui a basé sur le ping ? requête s au-dessus de LDAP, il devrait contenir l'attribut d'email pour cet objet.

Remarque: Étapes 11 et 12 s'assurent qu'ISE recevra l'email d'objet d'AD et des attributs de MemberOf par l'IDP ouvrent une session l'action.

Vérifiez

1. Lancez le portail d'invité utilisant l'URL portail de test ou en suivant les CWA circulent. L'utilisateur aura les options d'entrer dans des qualifications d'invité, crée leur compte personnel et procédure de connexion des employés.

2. **Procédure de connexion des employés de** clic. Puisqu'il n'y a aucune session active l'utilisateur sera réorienté au portail de procédure de connexion d'IDP.

3. Entrez dans les qualifications d'AD et le clic **se connectent**.

4. L'écran de connexion d'IDP réorientera l'utilisateur à la page portaile de succès d'invité.

5. En ce moment, chaque fois que l'utilisateur revient au portail d'invité et sélectionne ? **Procédure de connexion des employés** ? on leur permettra dans le réseau tant que la session est encore en activité dans l'IDP.

Dépannez

N'importe quelle question d'authentification SAML sont enregistré 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 la commande ? queue d'ise-psc.log d'application de show logging ? et surveillez les événements SAML, 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.

Informations connexes

- Authentification Web centrale avec le Cisco WLC et l'exemple de configuration ISE.
- Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine.
- 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