Sécurité Web de nuage : Configurez ADFS pour inclure les groupes spécifiques au moment de l'authentification

Contenu

Introduction

Ce document décrit comment configurer les services fédérés par Microsoft Active Directory (ADFS) comme fournisseur d'identité (IDP), qui envoie les petits groupes spécifiques de groupe au service de la sécurité Web de nuage de Cisco (CWS), plutôt qu'une liste complète d'adhésions à des associations.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de sécurité Web de nuage avec le portail de ScanCenter
- Authentification du Langage SAML (SAML)
- Gestion de serveur de Microsoft ADFS

Composants utilisés

Les informations dans ce document sont basées sur la version 2.0 de Microsoft ADFS, cette s'exécutent sur les Windows Server 2008 R2.

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 opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Quand la procédure d'authentification entre un navigateur de client se produit, le serveur ADFS (l'IDP) et CWS (le fournisseur de services (le fournisseur de services)), toutes les informations sont chiffrées et ajoutées à la chaîne d'URL dans le navigateur de client. Ceci signifie que la chaîne d'URL est plus longue quand plus d'informations sont envoyées à CWS.

Quand vous configurez l'authentification SAML (avec Microsoft ADFS) pour l'usage avec le service CWS, vous devriez configurer une confiance comptante d'interlocuteur pour fournir le nom d'utilisateur et l'information du groupe. Sécurité Web de nuage : Configurez l'utilisateur/groupe d'attributs avec PingFederate et ADFS tout en utilisant le SAML décrit cette étape plus en détail.

Le nombre de groupes qu'un utilisateur est ajouté à augmente la taille URL. Si un utilisateur appartient à un grand nombre de groupes de Répertoire actif (AD), l'URL devient une taille par lequel la limite URL imposée par navigateur soit atteinte, et la procédure d'authentification échoue.

Chaque navigateur pourrait définir leur propre longueur URL de maximum autorisé. RFC 2616 ne spécifie pas une longueur maximale, mais des limites pratiques sont imposées par des constructeurs de navigateur.

> Remarque: Il n'est pas possible de définir explicitement un nombre maximal de groupes parce qu'un groupe n'a pas un nombre fixe de caractères. Par exemple, GroupA a moins de caractères que Test_Group_A. Pour définir un certain nombre de groupes qui reste au-dessous de la limite URL dépend du décompte de caractères du nom de nom de domaine + de groupe.

Configurez

Vous pouvez configurer le serveur de Microsoft ADFS pour inclure les groupes spécifiques dans la procédure d'authentification. Typiquement vous sélectionneriez seulement les groupes utilisés dans les règles de filtrage de Web CWS. Quand vous exécutez un audit des stratégies qui existent, elles aident à déterminer les groupes qui sont déjà en service.

Nouveau et les déploiements qui existent déjà devrait suivre la configuration de pratique recommandée qui fournit ces indemnités :

- Garde la taille URL à un minimum
- Accélère la procédure d'authentification entre l'IDP (ADFS) et le fournisseur de services (CWS)
- Enregistre la bande passante sur chaque demande d'authentification

Configuration de pratique recommandée

Les confiances de fournisseur de sinistres certains non encore réglés et créent deux que l'acceptation transforment des règles :

Le modèle de règle de demande d'utilisation envoient des attributs de LDAP comme demandes

Mémoire d'attribut : AD ;

Attribut de LDAP : Jeton-groupes - Noms sans réserve ;

Type sortant de demande : Groupe

Le modèle de règle de demande d'utilisation envoient des attributs de LDAP comme demandes

Mémoire d'attribut : AD ;

Attribut de LDAP : Sam-Compte-nom ;

Type sortant de demande : Nom

Créez l'émission transforment des règles en ouvrant des confiances comptantes de partie et en créant deux transformez les règles :

L'utilisation transforment un modèle entrant de demande

Type entrant de demande : Nom

Format : non spécifié

Type sortant de demande : ID de nom

Format : Non spécifié

Choisi traversez toutes les valeurs de demande

La fonction émulation d'utilisation ou filtrent une demande entrante

Type entrant de demande : Groupe

Choisi traversez seulement les valeurs de demande qui commencent par une valeur spécifique :

Spécifiez vos noms de groupe d'AD

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- Tandis qu'ouvert une session en tant qu'utilisateur final, parcourez à http://whoami.scansafe.net.
- La sortie devrait répertorier seulement les groupes spécifiés dans la procédure précédemment mentionnée, plutôt qu'une liste complète d'adhésions à des associations.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.