ISE Access portail administratif avec l'exemple de configuration de qualifications d'AD

Contenu

Introduction

Ce document décrit un exemple de configuration pour l'usage de la Microsoft Active Directory (AD) comme mémoire externe d'identité pour l'accès administratif au GUI de Gestion du Logiciel Cisco Identity Services Engine (ISE).

Conditions préalables

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration des versions 1.1.x ou ultérieures de Cisco ISE
- AD de Microsoft

Componenets l'a utilisé

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

- Version 1.1.x de Cisco ISE
- Version 2 2008 de Windows Server

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.

Configurez

Employez cette section afin de configurer pour l'usage de l'AD de Microsoft comme mémoire externe d'identité pour l'accès administratif au GUI de Gestion de Cisco ISE.

Joignez ISE à l'AD

1. Naviguez vers la **gestion > la Gestion de l'identité > les sources extérieures > le Répertoire actif d'identité**.
2. Écrivez le nom de domaine d'AD et le nom de mémoire d'identité, et le clic **se joignent**.
3. Entrez dans les qualifications du compte d'AD qui peut ajouter et apporter des modifications aux objets d'ordinateur, et cliquez sur la **save configuration**.

Groupes choisis de répertoire

1. Naviguez vers la **gestion > la Gestion de l'identité > les sources extérieures > le Répertoire actif > les groupes d'identité > ajoutent > répertoire choisi de forme de groupes**.
2. Importez au moins un groupe d'AD auquel votre administrateur appartient.

Accès administratif d'enable pour l'AD

Terminez-vous ces étapes afin d'activer l'authentification basée sur mot de passe pour l'AD :

1. Naviguez vers la **gestion > le système > l'admin Access > authentification**.
2. De l'onglet de **méthode d'authentification**, sélectionnez le **mot de passe basé** option.
3. **AD** choisi du menu déroulant de **source d'identité**.
4. **Modifications de sauvegarde de** clic.

Configurez le groupe d'admin au mappage de groupe d'AD

Définissez un groupe d'admin de Cisco ISE et tracez-le à un groupe d'AD. Ceci permet l'autorisation de déterminer les autorisations du contrôle d'accès basées par rôle (RBAC) pour l'administrateur basé sur l'adhésion à des associations dans l'AD.

1. Naviguez vers la **gestion > le système > l'admin Access > administrateurs > groupes d'admin**.
2. Cliquez sur Add dans l'en-tête de table afin de visualiser le nouveau volet de configuration de

groupe d'admin.
3. Écrivez le nom pour le nouveau groupe d'admin.
4. Dans le champ de type, cochez la case **externe**.
5. Du menu déroulant **externe de groupes**, sélectionnez le groupe d'AD auquel vous voulez que ce groupe d'admin trace, comme défini dans la section choisie de groupes de répertoire.
6. **Modifications de sauvegarde de** clic.

Placez les autorisations RBAC pour le groupe d'admin

Terminez-vous ces étapes afin d'assigner des autorisations RBAC aux groupes d'admin créés dans la section précédente :

1. Naviguez vers la **gestion > le système > l'admin Access > autorisation > stratégie**.
2. Du menu déroulant d'**actions** sur la bonne, choisie **nouvelle stratégie d'insertion ci-dessous** afin d'ajouter une nouvelle stratégie.
3. Créez une nouvelle règle appelée **ISE_administration_AD**, tracez-la avec le groupe d'admin défini dans l'accès administratif d'enable pour la section d'AD, et assignez-lui les autorisations.Remarque: Dans cet exemple, le groupe d'admin appelé **Super Admin** est assigné, qui est équivalent au compte standard d'admin.
4. **La sauvegarde de** clic **change**, et la confirmation des modifications enregistrées sont affichées dans l'angle inférieur droit du GUI.

Access ISE avec des qualifications d'AD

Terminez-vous ces étapes afin d'accéder à ISE avec des qualifications d'AD :

1. Déconnectez de-vous le GUI administratif.
2. **AD1** choisi du menu déroulant de **source d'identité**.
3. Écrivez le nom d'utilisateur et mot de passe de la base de données d'AD, et de la procédure de connexion.

Remarque: Les par défaut ISE à la mémoire d'utilisateur interne au cas où l'AD serait inaccessible, ou les qualifications de compte utilisées n'existent pas dans l'AD. Ceci facilite la procédure de connexion rapide si vous utilisez la mémoire interne tandis que l'AD est configuré pour l'accès administratif.

Vérifiez

Afin de confirmer que votre configuration fonctionne correctement, vérifiez le nom d'utilisateur authentifié au coin haut droit du GUI ISE.

Dépannez

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

Informations connexes

- Guide de l'utilisateur de Logiciel Cisco Identity Services Engine, version 1.1 - Gérer l'accès d'Indentities et d'admin
- Support et documentation techniques - Cisco Systems