Contenu

Introduction
Q. Quelle configuration est exigée pour ajouter un point final dans le cache de restriction d'Access d'ordinateur (MARS) ?
R. Il y a deux scénarios de configuration basés sur la méthode d'authentification utilisée par le point final.
Mot de passe basé
Certificat basé
Références

Introduction

La restriction d'Access d'ordinateur (MARS) était une fonctionnalité introduite dans ISE et ACS comme manière de vérifier une authentification de machine réussie. Cette caractéristique permet la création des stratégies qui peuvent autoriser un utilisateur basé sur une authentification de machine précédente.

Le comportement ci-dessous est vu dans des versions 4.x et 5.x du serveur de contrôle d'accès (ACS) aussi bien que toutes les versions du Cisco Identity Services Engine (ISE).

Q. Quelle configuration est exigée pour ajouter un point final dans le cache de restriction d'Access d'ordinateur (MARS) ?

R.

Mot de passe basé

Si l'ordinateur authentifie contre le Répertoire actif (AD) utilisant l'ordinateur password(MSCHAPv2), aucune configuration supplémentaire n'est nécessaire car le point final sera ajouté au cache de MARS.

Certificat basé

Si l'ordinateur authentifie contre le Répertoire actif (AD) utilisant le certificat d'ordinateur (EAP-TLS), vous devez configurer la comparaison binaire pour que l'hôte soit caché en mars quand la comparaison binaire est activée, ISE/ACS vérifierez les informations parasites du certificat d'ordinateur et les comparerez aux informations parasites éditées de certificat associées à l'objet d'ordinateur enregistré dans l'AD. Sans comparaison binaire vérifiée, la demande d'authentification de machine ne peut pas être validée contre l'AD. En conséquence, l'authentification de machine ne serait pas ajoutée au cache de MARS.

Références

Usinez les avantages de restriction d'Access - et - des inconvénients