Utiliser le connecteur Active Directory Umbrella pour l'authentification

Table des matières

Introduction

Ce document décrit comment utiliser le connecteur Umbrella Active Directory pour l'authentification via 802.1x, Radius ou ISE.

Aperçu

Le connecteur Cisco Umbrella Active Directory (AD) fonctionne en mappant les utilisateurs/ordinateurs AD aux adresses IP internes. Pour que le mappage soit correct, les utilisateurs AD doivent s'authentifier auprès d'un contrôleur de domaine qui a été configuré pour communiquer avec un connecteur AD Cisco Umbrella.

Si vos utilisateurs AD s'authentifient par d'autres moyens, il est possible qu'un événement de connexion ne soit pas du tout généré sur le contrôleur de domaine ou qu'un mappage inattendu entraîne l'application d'une stratégie incorrecte.

Authentification via 802.1x, RADIUS ou ISE

L'authentification via 802.1x, RADIUS ou ISE n'est pas prise en charge en raison des limites du fonctionnement des connexions Active Directory avec ces solutions. Les événements de connexion recherchés par le connecteur AD ne sont souvent pas générés.

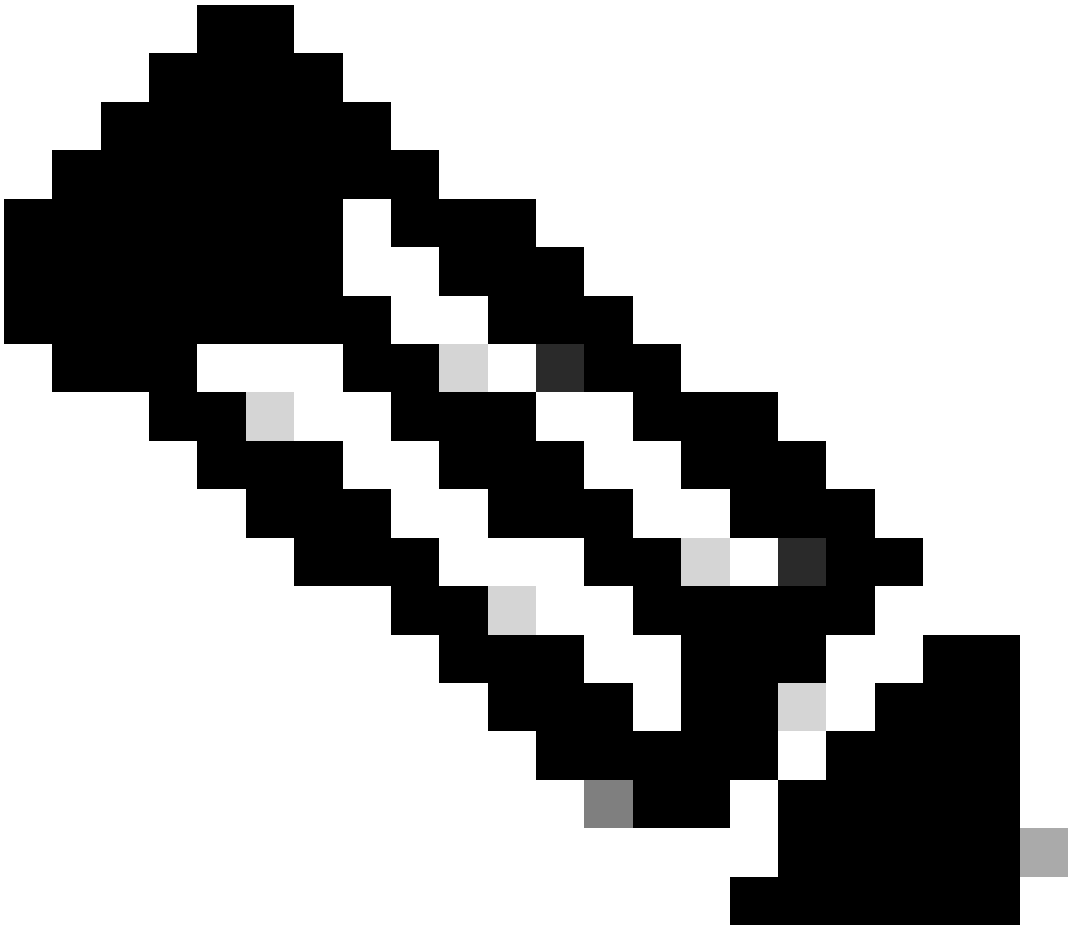
Pour en savoir plus sur les ID d'événements recherchés par le connecteur AD, cliquez ici : Quels événements/ID d'événement Windows le service Connector recherche-t-il ?

Le plus souvent, l'adresse IP du service d'authentification est mappée à l'utilisateur AD au lieu de l'adresse IP de l'ordinateur de l'utilisateur.

Solutions alternatives

L'intégration AD peut également être réalisée par l'utilisation du client d'itinérance avec la fonctionnalité de prise en charge des identités activée. Pour plus d'informations sur cette

fonctionnalité, reportez-vous à notre documentation de déploiement.



> Remarque : Cette solution nécessite que les appliances virtuelles ne soient pas présentes sur le réseau, car cela entraîne le passage du client itinérant à l'état désactivé « derrière VA ».

Si des appareils virtuels sont utilisés sur le réseau, des adresses IP internes peuvent être utilisées pour l'identification. Par exemple, vous pouvez créer une identité de réseau interne pour la plage d'adresses de votre réseau sans fil, puis appliquer une stratégie à cette identité. Le seul inconvénient de cette méthode est que tous les périphériques de cette plage d'adresses reçoivent la même stratégie.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.