Échecs d'inscription ZTNA pour les utilisateurs invités disposant de comptes Google personnels dans Cisco Secure Access

Table des matières

Problème

Lors du déploiement de Private Access avec ZTNA (Zero Trust Network Access), l'inscription d'un utilisateur invité avec un compte Google personnel échoue après l'enregistrement réussi dans Entra ID et la mise en service dans Secure Access. Les symptômes spécifiques rencontrés sont les suivants :

- Inscription basée sur le client : Le processus d'inscription atteint l'authentification SSO, les informations d'identification sont fournies, mais ZTNA affiche une « erreur d'E/S » et le processus d'inscription est bloqué
- Accès sans client : Renvoie le message d'erreur « Échec de la connexion à Cisco Secure Access. Vérifier la configuration IDP avec un ID de transaction

Ces défaillances empêchent l'accès aux ressources privées et les tests d'impact de la fonctionnalité ZTNA pour l'accès de type entrepreneur utilisant des identités non-entreprise.

Environnement

- Cisco Secure Access avec déploiement ZTNA
- Microsoft Entra ID (anciennement Azure AD) en tant que fournisseur d'identité
- Compte Google personnel (@gmail.com) enregistré en tant qu'utilisateur invité dans Entra ID
- Compte invité provisionné et visible dans Secure Access
- Authentification SAML configurée entre Entra ID et Cisco Secure Access

Résolution

L'échec d'inscription a été résolu en modifiant la configuration du mappage d'attribut SAML dans Microsoft Entra ID. Les mesures suivantes ont été prises pour régler le problème :

Étape 1: Analyser le bundle DART et le comportement du client

Examinez l'offre groupée DART pour vérifier que les composants Cisco Secure Client et ZTA fonctionnent normalement. L'analyse doit vérifier que le flux d'inscription atteint correctement Cisco Secure Access et que l'échec se produit lors de l'authentification SAML avec le fournisseur d'identité.

Étape 2: Examiner les journaux d'authentification Entra ID

Vérifiez les journaux d'authentification Entra ID pour confirmer que le processus d'authentification s'est terminé correctement du point de vue du fournisseur d'identité. Les journaux doivent indiquer que l'authentification a réussi, mais Secure Access rejette la connexion en raison d'une non-concordance des attributs.

Étape 3: Identifier le problème de mappage d'attribut SAML

Déterminez si Entra ID émet le nom d'utilisateur principal (UPN) en tant que demande SAML, qui ne correspond pas à l'identité de compte Gmail personnelle attendue par Secure Access. L'attribut IdP affirmé ne correspond pas à l'identificateur d'utilisateur attendu.

Étape 4: Modifier le mappage d'attribut SAML

Modifiez le mappage d'attribut SAML dans Microsoft Entra ID de UPN à Adresse e-mail. Cela garantit que la demande d'adresse e-mail correspond à l'identité du compte Google personnel.

Étape 5: Vérifier la réussite de l'inscription

Après avoir implémenté la modification de mappage d'attribut, recommencez le processus d'inscription ZTNA. Cisco Secure Access ZTA doit maintenant reconnaître l'adresse Gmail et permettre l'inscription.

Motif

L'échec de l'inscription est dû à une non-correspondance entre l'attribut SAML revendiqué par Microsoft Entra ID et l'identificateur d'utilisateur attendu dans Cisco Secure Access. Entra ID a été configuré pour envoyer l'UPN (User Principal Name) en tant que demande SAML, mais pour les comptes Google personnels (@gmail.com), cet UPN ne correspondait pas à l'identité de l'adresse e-mail réelle. Cisco Secure Access s'attendait à recevoir l'adresse e-mail en tant qu'attribut d'identification à comparer au compte d'utilisateur invité provisionné, ce qui a entraîné le rejet de l'authentification malgré une authentification IdP réussie.

Autres informations utiles

- Assistance technique de Cisco et téléchargements

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.