Invite d'authentification Cisco Secure Client SAML à chaque tentative avec Microsoft Entra ID SSO

Table des matières

Problème

Cisco Secure Client (AnyConnect) intégré à Microsoft Entra ID pour l'authentification SAML rencontrait plusieurs problèmes liés à l'authentification qui ont perturbé la fonctionnalité SSO (Single Sign-On) :

- Les utilisateurs étaient invités à s'authentifier à chaque tentative de connexion VPN, même lorsqu'une session Entra ID active existait dans le navigateur
- Le client lançait le navigateur intégré au lieu du navigateur externe/système, bien que l'authentification du navigateur externe soit explicitement activée pour SAML
- Les utilisateurs ont fréquemment rencontré l'erreur : "Erreur d'authentification en raison d'un problème de redirection vers l'URL SSO"
- Le comportement SSO a changé par rapport à l'état de fonctionnement précédent où les utilisateurs pouvaient se connecter au VPN en cliquant simplement sur Connect sans invites d'authentification

Environnement

- Produit : Client sécurisé Cisco (AnyConnect)
- Technologie : VPN d'accès sécurisé avec authentification SAML
- Fournisseur d'identité : Microsoft Entra ID (Azure AD)
- Méthode d'authentification : Intégration de SAML SSO
- Authentification du navigateur externe activée pour SAML

Résolution

La résolution impliquait l'adressage des problèmes sous-jacents d'état de jointure des périphériques Azure AD et de configuration du navigateur à l'origine des problèmes d'authentification :

Étape 1: Diagnostiquer l'état de jointure Azure AD

Exécutez la commande suivante pour vérifier l'état actuel de la jointure Azure AD du périphérique affecté :

```
dsregcmd /status
```

Vérifiez le résultat pour déterminer si l'appareil affiche AzureAdJoained = NO, ce qui indique un état de jointure Azure AD incorrect.

Étape 2: État de jointure Azure AD correct

Exécutez la commande dsregcmd pour corriger l'état de jointure Azure AD sur le périphérique affecté. Après avoir exécuté les opérations dsregcmd appropriées,

```
dsregcmd /status
dsregcmd /leave
dsregcmd /join`
```

Vérifiez que l'état du périphérique indique :

```
AzureAdJoined = YES
```

Cette correction résout le problème d'état d'authentification sous-jacent qui entraînait l'invite du client sécurisé Cisco à fournir des informations d'identification sur chaque connexion.

Étape 3: Réinitialiser les applications du navigateur par défaut

Pour résoudre le problème de comportement entre le navigateur externe et le navigateur intégré :

Réinitialisez les paramètres d'application par défaut du périphérique pour vous assurer que Cisco Secure Client lance correctement le navigateur externe/système pour l'authentification SAML au lieu du navigateur intégré.

```
Settings → Apps → Default apps → Reset
```

Étape 4: Vérification

Après avoir implémenté les modifications ci-dessus, vérifiez les comportements suivants :

- Cisco Secure Client ne demande plus de mot de passe ou d'authentification Windows Hello sur chaque connexion VPN
- Le client lance correctement le navigateur externe pour l'authentification SAML au lieu du navigateur intégré
- La fonctionnalité SSO est restaurée, ce qui permet aux utilisateurs de se connecter sans invites d'authentification répétées lorsqu'une session Entra ID active existe
- L'erreur « Erreur d'authentification due à un problème de redirection vers l'URL SSO » ne se produit plus

Motif

Les problèmes d'authentification ont été causés par un état de jointure Azure AD incorrect sur l'appareil affecté, où l'appareil affichait AzureAdJoained = NO au lieu de l'état AzureAdJoained = YES requis. Cet état de jointure incorrect a empêché la validation correcte du jeton SSO et a forcé Cisco Secure Client à demander l'authentification à chaque tentative de connexion.

En outre, les paramètres d'application par défaut du périphérique ont été mal configurés, ce qui a conduit Cisco Secure Client à lancer le navigateur intégré au lieu du navigateur externe pour

l'authentification SAML, bien que le paramètre du navigateur externe soit activé dans la configuration du client.

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.