Synchronisation des identités Cisco Secure Access avec Active Directory et Microsoft EntraID

Table des matières

Problème

Les utilisateurs ont rencontré des difficultés lorsqu'ils ont tenté de provisionner des utilisateurs et des groupes à partir de deux sources d'identité avec le même nom de domaine dans Cisco Secure Access. Le scénario spécifique impliquait la synchronisation d'identités à partir d'Active Directory local et de Microsoft EntraID (anciennement Azure AD) où les deux sources utilisaient le même nom de domaine (par exemple, domain.com).

Les principales préoccupations étaient les suivantes :

- Comprendre le comportement de la propriété d'identité et du mappage d'appartenance à un groupe lorsque les mêmes utilisateurs et groupes existent dans les deux sources d'identité
- Garantir l'application cohérente de politiques d'accès sécurisé pour les utilisateurs hybrides accédant à la fois aux ressources sur site et cloud
- Maintien de la visibilité IP interne pour les utilisateurs dans cette configuration d'identité hybride
- Déterminer si la synchronisation simultanée des deux sources peut entraîner des problèmes dans un environnement de production

La documentation indique que « la synchronisation simultanée des mêmes utilisateurs et groupes à partir du connecteur Cisco AD et de l'application Cisco User Management for Secure Access n'est pas prise en charge et entraîne une application incohérente des règles d'accès. »

Environnement

- Accès sécurisé Cisco avec connecteur AD et intégration EntraID
- Active Directory local avec un nom de domaine correspondant au domaine EntraID
- Microsoft EntraID (Azure AD) avec le même nom de domaine qu'Active Directory local
- Configuration de SAML SSO pour la fédération des identités
- Module Secure Web Gateway (SWG) pour l'application des stratégies
- Environnement hybride nécessitant un accès aux ressources sur site et cloud

Résolution

Le comportement suivant a été confirmé pour la synchronisation simultanée à partir des sources Active Directory et EntraID :

Comportement de synchronisation de groupe

Lors de la synchronisation de groupes portant le même nom à partir des deux sources :

- Deux objets de groupe distincts sont créés dans Cisco Secure Access, un pour chaque source
- Les groupes peuvent être distingués par leur préfixe source dans les stratégies d'accès
- Les groupes AD locaux apparaissent comme suit : AD-Domain/GroupName
- Les groupes EntraID apparaissent sous la forme : NomGroupe

La vérification en laboratoire a montré que la synchronisation a réussi avec le message « Success ». <<<< Synchronized » pour les groupes de plusieurs domaines EntraID.

Comportement de synchronisation utilisateur

Lors de la synchronisation d'utilisateurs avec le même ID utilisateur à partir des deux sources :

- L'identité de l'utilisateur est écrasée pendant la synchronisation
- Un seul ID utilisateur unique reste visible dans Secure Access
- La source de synchronisation finale détermine les attributs de l'utilisateur et les appartenances au groupe
- La synchronisation EntraID est généralement prioritaire sur AD sur site lorsque les deux sont configurés

Configuration de la politique d'accès

Les deux types de groupes peuvent être utilisés dans les politiques d'accès :

- Référencer les groupes AD locaux à l'aide du chemin d'accès complet : AD-Domain/GroupName
- Référencez les groupes EntraID à l'aide du nom simple : NomGroupe
- Les politiques peuvent différencier les utilisateurs en fonction de leur appartenance à un groupe

Le suivi de la configuration fonctionne bien pour de nombreux clients.

```
1    Only provision identities from on-prem AD - for VA DNS protection
2    Use Azure entra for SSO/user authentication (no identities to be provisioned from Azure) - for SWG
```

Motif

Au cours de notre test, nous avons confirmé que chaque fois qu'un utilisateur est synchronisé à partir du connecteur AD sur site, il « revendique » effectivement cette identité dans le tableau de bord Umbrella. Si ce même utilisateur existe déjà via la synchronisation Azure AD, la synchronisation locale remplacera les données utilisateur EntraID existantes.

Ce comportement est une limitation documentée. Selon la documentation technique officielle de Cisco : https://securitydocs.cisco.com/docs/csa/china/olh/129444.dita

"La synchronisation simultanée des mêmes identités d'utilisateur et de groupe à partir du connecteur Cisco Umbrella AD et de l'application Cisco Umbrella Azure AD n'est pas prise en charge et entraîne une application incohérente de la stratégie."

Conclusion: La configuration souhaitée (visibilité VA pour les utilisateurs existant à la fois dans Azure et On-Prem) est confirmée comme étant une configuration non prise en charge.Le chemin d'accès vers l'avant nécessite l'utilisation de clients d'itinérance pour assurer une application cohérente de l'identité.

Autres informations utiles

- Provisionner les identités à partir d'Azure AD - Documentation Cisco Umbrella
- 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.