Cisco Secure Access - Renouvellement de certificat SAML avec IDP (Microsoft Entra ID)

Table des matières

Problème

Lors de l'utilisation de l'authentification SSO avec Microsoft Entra ID SAML comme fournisseur d'identité (IdP) pour Cisco Secure Access, les certificats de vérification SAML arrivent bientôt à expiration.

Les organisations doivent comprendre le processus de renouvellement de certificat correct pour éviter les interruptions d'authentification et déterminer si une nouvelle configuration d'authentification unique doit être créée dans Secure Access lors du renouvellement des certificats SAML d'ID d'entrée.

Environnement

- Cisco Secure Access avec authentification SSO configurée
- Microsoft Entra ID SAML en tant que fournisseur d'identité
- Certificats de vérification SAML avec dates d'expiration à venir
- Configuration SSO existante pour SWG (Secure Web Gateway) et ZTNA (Zero Trust Network Access)

Résolution

Étape 1 - Détectez le renouvellement du certificat

- Le fournisseur d'identité (IdP) renouvelle ou fait pivoter son certificat de signature SAML.

- Cela se produit généralement lorsque le certificat approche de son expiration.

Étape 2 - Obtenez les métadonnées IdP mises à jour

- Exportez le nouveau XML de métadonnées IdP ou le nouveau certificat de signature depuis l'IdP.

Étape 3 - Vérifiez la modification du certificat

Confirmez que le certificat a été modifié.

Vérifier :

- Empreinte
- Date d'expiration
- Émetteur

Cela garantit que le SP est mis à jour avec le certificat correct

Mettre à jour la configuration Service Provider

Connectez-vous au tableau de bord Cisco Secure Access et mettez à jour la configuration.

Accédez à Connexion - Utilisateur et groupes.

Cliquez sur Configuration Management

Sous Authentification SSO - Modifier le profil d'authentification SSO - téléchargez le fichier de métadonnées à l'aide du nouveau certificat ou téléchargez le certificat en cas de configuration manuelle.

Étape 5 - Enregistrez et appliquez la configuration

- Enregistrer la configuration mise à jour

Étape 6 - Validez l'authentification SSO

Effectuez un test de connexion SSO.

Motif

Le certificat de signature du fournisseur d'identité (IdP) est utilisé par le fournisseur de services pour vérifier la signature d'assertion SAML. Lorsque le fournisseur d'identité renouvelle le certificat, le fournisseur de services doit mettre à jour son certificat sécurisé pour continuer à valider les demandes d'authentification

Autres informations utiles

- Cisco Secure Access - Présentation et configuration de l'authentification unique SAML
- Configurer l'authentification unique SAML pour Cisco Secure Access (exemple d'ID supplémentaire Microsoft)
- 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.