Échec de l'authentification SAML VPNaaS avec " ; Le déchiffrement de l'état du relais a échoué" ; Erreur lors de l'utilisation de Duo IdP

Table des matières

Problème

Lorsque vous tentez d'établir une connexion VPNaaS à l'aide de l'accès à distance client sécurisé avec authentification SAML et Duo en tant que fournisseur d'identité (IdP), cette erreur est observée :

- Échec lors du traitement de la demande d'authentification SSO. Contactez votre administrateur système
- Échec du déchiffrement de relaystate

L'authentification avec la même configuration IdP et Duo fonctionne correctement pour ZTNA (Zero Trust Network Access), mais échoue pour les connexions VPN. Il existe deux applications distinctes configurées dans Duo pour ZTNA et VPN, les deux utilisant le même IdP.

Environnement

- Technologie : Assistance pour les solutions (SSPT - contrat requis)
- Sous-technologie : Accès sécurisé : accès à distance sécurisé pour le client (VPN, position, ressource privée)
- Méthode d'authentification : SAML avec IDp duo
- Deux applications Duo configurées : un pour ZTNA, un pour VPN
- L'authentification fonctionne pour ZTNA, échoue pour VPN
- Version du logiciel: TOUS
- Aucune modification récente de la version matérielle/logicielle spécifiée

Résolution

Le problème a été résolu en corrigeant la configuration de l'ID d'entité et de l'URL ACS (Assertion Consumer Service) sur l'application Duo pour VPN. Les métadonnées correctes ont été téléchargées à partir de Secure Access et téléchargées vers l'application VPN Duo, ce qui a résolu l'erreur de déchiffrement d'état de relais SAML.

1. Connectez-vous au tableau de bord CSA. Accédez à Connect > Enduser Connectivity -> Virtual Private Networks. Découvrez le profil auquel vous êtes connecté.
2. Cliquez sur ce profil et sur Modifier. Accédez à l'onglet Authentification.

3. Téléchargez les métadonnées SAML pour un accès sécurisé.
4. Vérifiez entityID="https://X.vpn.sse.cisco.com/saml/sp/metadata/saml" et <AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://X.vpn.sse.cisco.com/+CSCOE+/saml/sp/acs?tgname=Profilename"></AssertionCo
5. Assurez-vous que entityID et AssertionConsumerService correspondent à l'application Duo configurée pour l'authentification SSO VPN.

Motif

Une configuration incorrecte de l'ID d'entité et de l'URL ACS sur l'application Duo VPN a entraîné l'échec du déchiffrement SAML relaystate. La configuration correcte n'était pas présente dans Duo pour VPN, même si l'authentification ZTNA fonctionnait avec le même IdP. La mise à jour de l'application Duo VPN avec des métadonnées précises de Secure Access a résolu le problème.

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.