Dépannage de l'intégration UCCE SSO avec Azure IdP

Table des matières

Introduction

Ce document décrit comment dépanner certains problèmes courants rencontrés lors de l'exécution de l'intégration UCCE SSO avec Microsoft Azure IdP.

Contribution d'Anurag Atul Agarwal, ingénieur du centre d'assistance technique Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Langage SAML (Security Assertion Markup Language) 2.0
- Cisco Unified/Packaged Contact Center Enterprise UCCE/PCCE
- Authentification unique (SSO)
- Cisco Identity Service (IdS)
- Fournisseur d'identité (IdP)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Azure IdP
- UCCE 12.0.1
- ID Cisco 12.0.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit certains des problèmes courants rencontrés lors de l'intégration de Cisco Identity Service (IdS) et de l'Identity Provider (IdP) pour l'authentification unique basée sur Azure et leurs correctifs potentiels. Il est toujours recommandé de collecter ces journaux pour résoudre les problèmes liés à l'intégration SSO :

- Journaux Cisco IdS : lien vers la collection : journaux IDS
- Journaux de console du navigateur
- Tous les journaux de IdP

Problème : le certificat ne correspond pas

Le test SSO échoue avec le message 'IdS n'a pas pu traiter la réponse SAML même si l'authentification a réussi' et les journaux IdS impriment le message d'erreur : "Le traitement de la réponse SAML a échoué avec l'exception com.sun.identity.saml2.common.SAML2Exception : le certificat de signature ne correspond pas à ce qui est défini dans les métadonnées d'entité'"

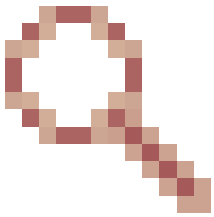
Solution

Vérifiez le certificat et le paramètre Algorithme de signature dans Azure. Assurez-vous qu'il correspond à l'algorithme de hachage pris en charge basé sur la version IdS. Reportez-vous au chapitre « Single Sign-On » du Guide des fonctionnalités et vérifiez l'algorithme de hachage sécurisé pris en charge. Téléchargez le dernier fichier de métadonnées IdP et téléchargez-le vers Cisco IdS via l'interface utilisateur Identity Service Management.

Problème : AADSTS900235 - Problème de contexte d'authentification

Test SSO redirige vers la page Microsoft et échoue avec le message : « Désolé, mais nous rencontrons des problèmes pour vous connecter. »
AADSTS900235 : la valeur de comparaison RequestedAuthenticationContext de la demande d'authentification SAML doit être Exact. Valeur reçue : minimum

Solution



AuthContext peut nécessiter un réglage comme décrit dans le bogue CSCvm69290
. Veuillez contacter le TAC Cisco pour effectuer la solution de contournement dans les ID.

Problème : la réponse SAML n'est pas signée

Le test SSO échoue avec le message, IdS n'a pas pu traiter la réponse SAML même si l'authentification a réussi.' et les journaux IdS impriment le message d'erreur : "Le traitement de la réponse SAML a échoué avec l'exception com.sun.identity.saml2.common.SAML2Exception : Response is not signed."

Solution

Azure IdP doit envoyer une assertion signée à IdS. Modifier le paramètre Azure pour avoir l'option de signature : Signer la réponse et l'assertion SAML

Problème : problème avec les règles de demande

Le test SSO échoue avec le message 'Erreur de configuration IdP : le traitement SAML a échoué. Impossible de récupérer l'identité de l'utilisateur à partir de la réponse SAML.' et les journaux IdS impriment le message d'erreur : "Le traitement de la réponse SAML a échoué avec l'exception com.sun.identity.saml.common.SAMLException : Impossible de récupérer l'identité de l'utilisateur à partir de la réponse SAML."

Solution

Cette erreur indique des 'noms de revendications' incorrects configurés dans Azure. Cela peut se produire avec d'autres attributs comme UID, NameID, etc. et des erreurs similaires avec des noms d'attributs différents sont générées. Pour résoudre ce problème, localisez n'importe quel attribut dans Azure dans ce format, 'schemas.xmlsoap.org/ws/2005/05/identity/claims/<nom_attribut>'. Supprimez tout ce qui précède le nom d'attribut réel.

Cette section fournit l'exemple de configuration pour ADFS dans le guide des fonctionnalités et qui doit être répliqué dans Azure.

Exemple de configuration ADFS

Problème : AADSTS50011 - L'URL de réponse ne correspond

pas

Test SSO redirige vers la page Microsoft et échoue avec le message : « Désolé, mais nous rencontrons des problèmes pour vous connecter.
AADSTS50011 : l'URL de réponse spécifiée dans la demande ne correspond pas à l'URL de réponse configurée pour l'application.

Solution

Contactez le TAC Cisco. Le paramètre « Assertion Consumer Service » doit être vérifié à la racine sur le noeud IdS où cela échoue. Si le paramètre est correct, Microsoft Azure doit le résoudre.

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.