Dépannage et problèmes courants ADFS/IdS

Contenu

Introduction

L'interaction du Langage SAML (SAML) entre la gestion d'identité de Cisco (id) et les services de fédération de Répertoire actif (AD FS) par l'intermédiaire d'un navigateur est le noyau du Simple-signe sur l'écoulement de la procédure de connexion (SSO). Ce document vous aidera dans le problème lié d'élimination des imperfections aux configurations dans les id et l'AD FS de Cisco, avec l'action recommandée de les résoudre.

Modèles de déploiement d'id de Cisco

Produit	Déploiement
UCCX	Co-résident
PCCE	Co-résident avec CUIC (centre d'intelligence de Cisco Unified) et LD (données vivantes)
UCCE	Co-résident avec CUIC et LD pour les déploiements 2k. Autonome pour les déploiements 4k et 12k.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Version 11.5 de version 11.5 ou de Cisco Unified Contact Center Enterprise du Cisco Unified Contact Center Express (UCCX) ou version 11.5 emballée du Contact Center Enterprise (PCCE) comme applicable.
- Microsoft Active Directory - AD installé sur des Windows Server
- IDP (fournisseur d'identité) - Version 2.0/3.0 de service de fédération de Répertoire actif (AD FS)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Informations générales

Après que les relations de confiance soient établies entre les id et l'AD FS de Cisco (voyez ici pour des détails, commun pour UCCX et UCCE), on s'attend à ce que l'administrateur exécute le programme d'installation du test SSO dans la page Settings de la Gestion de gestion d'identité pour s'assurer que la configuration entre les id et l'AD FS de Cisco fonctionne bien. Si le test échoue, utilisez les applications appropriées et les suggestions données de ce guide pour résoudre le problème.

Applications et logs qui peuvent être pratiques dans l'élimination des imperfections

Application/log	Détails	Où trouver l'outil
Log d'id de Cisco	L'enregistreur d'id de Cisco se connectera n'importe quelle erreur qui s'est produite dans des id de Cisco.	Utilisation RTMT d'obtenir des logs d'id de Cisco. Pour les informations sur la façon dont utiliser RTMT voyez, guidez pour utiliser RTMT Veuillez noter que le nom RTMT est **gestion d'identité de Cisco**. Afin de trouver les logs, naviguez vers la **gestion d'identité de Cisco**

		> le log
Logs de Fedlet	Les logs de Fedlet fourniront plus de détails au sujet de toutes les erreurs SAML qui se produit dans des id de Cisco	Utilisation RTMT d'obtenir des logs de Fedlet. L'emplacement pour le log de Fedlet correspond les id de Cisco se connecte. Le début de logs de fedlet avec le **fedlet- de** préfixe
Mesures des id API de Cisco	Des mesures API peuvent être utilisées pour regarder dans et pour valider toutes les erreurs que les id API de Cisco ont pu avoir renvoyées et nombre de requêtes qui sont traités par des id de Cisco	Utilisation RTMT d'obtenir des mesures API. Veuillez noter que le nom RTMT est **gestion d'identité de Cisco** Ceci apparaîtra sous des **mesures** distinctes d'un répertoire. Veuillez noter que **saml_metrics.csv et** authorize_metrics.csv **sont les** mesures appropriées pour ce document.
Visualisateur d'événements dans l'AD FS	Permet à des utilisateurs pour visualiser l'événement ouvre une session le système. N'importe quelle erreur dans l'AD FS tandis que le traitement de la demande SAML/l'envoi de la réponse SAML sont enregistré ici.	Dans l'ordinateur FS d'AD, naviguez vers des **>Applications de visualisateur d'événements** et les **services se connectent le >AdDFS 2.0 > admin** Dans Windows 2008, le visualisateur d'événements de lancement du **panneau de configuration > de la représentation et la maintenance > des outils d'administration** Dans Windows 2012, lancez-le du panneau de configuration \ du système et de la Sécurité \ des outils d'administration. Veuillez regarder votre documentation de fenêtres pour voir où trouver le visualisateur d'événements.
Visualiseur SAML	Un visualiseur SAML aidera en regardant la demande et la réponse SAML qui sont envoyées de/à des id de Cisco. Cette application de navigateur est très utile pour l'analyse de la demande/réponse SAML.	Ce sont quelques visualiseurs suggérés SAML que vous pouvez utiliser pour regarder la demande et la réponse SAML 1. Violoneur Comment utiliser le violoneur avec l'AD FSModule d'extension de Chrome de violoneur 2. Traceur SAML - Firefox 3. Panneau SAML Chrome

Organigramme avec des options d'élimination des imperfections

Les diverses étapes pour l'authentification SSO est affichées dans l'image avec et les objets façonnés d'élimination des imperfections à chaque étape en cas de panne dans cette étape.

Cette table fournit les détails sur la façon dont identifier des pannes à chaque étape de SSO dans le navigateur. Les autres outils et comment pouvez ils aident dans l'élimination des imperfections est aussi bien spécifiés.

Étape	Comment identifier la panne dans le navigateur	Outils/log	Configurations aux regarder
Demande d'AuthCode traitant par	En cas de panne, le navigateur n'est pas réorienté au point final ou à l'AD FS SAML, une erreur	Les logs d'id de Cisco indique les erreurs qui se produisent tandis que la demande	Enregistrement de client

des id de Cisco	JSON est affichée par des id de Cisco, qui indique que l'id de client ou réoriente l'URL est non valide.	d'authcode est validée et traitée. Mesures des id API de Cisco - Indique le nombre de requêtes traité et manqué.	
Initiation de demande SAML par des id de Cisco	Pendant la panne, le navigateur n'est pas réorienté à l'AD FS, et une page/message d'erreur sera affichée par des id de Cisco.	Les logs d'id de Cisco indique s'il y a une exception ou pas tandis que la demande est initiée. Mesures des id API de Cisco - Indique le nombre de requêtes traité et manqué.	Id de Cisco dans l'état NOT_CONFIGURED.
Demande SAML traitant par l'AD FS	N'importe quel manque de traiter cette demande aura comme conséquence une page d'erreur affiché par le serveur FS d'AD au lieu de la page de connexion.	Le visualisateur d'événements dans l'AD FS indique les erreurs qui se produisent tandis que la demande est traitée. Module d'extension de navigateur SAML - Aides pour voir la demande SAML qui est envoyée à l'AD FS.	Configuration comptante de confiance d'interlocuteur dans l'IDP
Envoi de la réponse SAML par l'AD FS	N'importe quel manque d'envoyer la réponse a comme conséquence une page d'erreur affiché par le serveur FS d'AD après que les qualifications valides soient soumises.	Visualisateur d'événements dans l'AD FS - Indique les erreurs qui se produisent tandis que la demande est traitée.	• Configuration comptante de confiance d'interlocuteur dans l'IDP • Formez la configuration d'authentification dans l'AD FS.
Réponse SAML traitant par des id de Cisco	Les id de Cisco afficheront une erreur 500 avec la raison d'erreur et une page de contrôle rapide.	Visualisateur d'événements dans l'AD FS - Indique l'erreur si l'AD FS envoie une réponse SAML sans code d'état réussi. Module d'extension de navigateur SAML - Aides pour voir la réponse SAML envoyée par l'AD FS pour identifier ce qui est erroné. Log d'id de Cisco - Indique que l'erreur/exception s'est produite pendant le traitement. Mesures des id API de Cisco - Indique le nombre de requêtes traité et manqué.	• La demande ordonne la configuration • Signature de message et d'assertion

Demande d'Authcode traitant par des id de Cisco

Le point commençant de procédure de connexion SSO, en ce qui concerne les id de Cisco, est la demande d'un code d'autorisation d'une application activée par SSO. La validation de demande API est faite pour vérifier si c'est une demande d'un client enregistré. Une validation réussie a comme conséquence le navigateur étant réorienté au point final SAML des id de Cisco. N'importe quelle panne dans la validation de demande a comme conséquence une erreur page/JSON

(notation d'objet de Javascript) étant renvoyée des id de Cisco.

Erreurs communes produites pendant ce processus

1. **Enregistrement de client non fait**

Résumé du problème	La demande de procédure de connexion échoue avec l'erreur 401 sur le navigateur.
	Navigateur :
	erreur 401 avec ce message : {« erreur » : « invalid_client », « error_description » : « Clien
	Log d'id de Cisco :
	`2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] AVERTISSENT com.cisco.ccbu.ids IdSC`
	`de client : fb308a80050b2021f974f48a72ef9518a5e7ca69 n'existe pas l'ERREUR com.cisco.ccb`
	`IdSOAuthEndPoint.java:45 de 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] - excep`
	`d'autorisation. org.apache.oltu.oauth2.common.exception.OAuthProblemException : ClientId`
	`valide. à org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProble`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthori`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAu`
	`à org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)`

Cause possible	L'enregistrement de client avec des id de Cisco n'est pas complet.
Action recommandée	Naviguez vers la console de gestion d'id de Cisco et confirmez si le client est enregistré av enregistrez alors les clients avant de commencer avec SSO.

2. **Application d'accès client utilisant le nom d'hôte d'adresse IP/remplaçant**

Résumé du problème	La demande de procédure de connexion échoue avec l'erreur 401 sur le navigateur. **Navigateur :** erreur 401 avec ce message : {« erreur » : « invalid_redirectUri », « error_description » : « Invlalid réorientent Uri »} Application d'accès client utilisant le nom d'hôte d'adresse IP/remplaçant.
Cause possible	En mode SSO, si l'application est accédée à utilisant l'IP, cela ne fonctionne pas. Des applications devraient être accédées à par l'adresse Internet par laquelle elles sont enregistrées dans des id de Cisco. Cette question peut se produire si l'utilisateur accédait un nom d'hôte alternatif qui n'est pas inscrit aux id de Cisco.
Action recommandée	Naviguez vers la console de gestion d'id de Cisco et confirmez si le client est inscrit au correct réorientent URLand que le même est utilisé pour accéder à l'application.

Initiation de demande SAML par des id de Cisco

Le point final SAML des id de Cisco est le point commençant de l'écoulement SAML dans la procédure de connexion basée par SSO. L'initiation de l'interaction entre les id et l'AD FS de Cisco est déclenchée dans cette étape. La condition préalable ici est que les id de Cisco devraient connaître l'AD FS pour se connecter à pendant que les métadonnées correspondantes d'IDP devraient être téléchargées aux id de Cisco pour que cette étape réussisse.

Erreurs communes produites pendant ce processus

1. **Métadonnées FS d'AD non ajoutées aux id de Cisco**

Résumé du problème	La demande de procédure de connexion échoue avec l'erreur 503 sur le navigateur.

	Navigateur : erreur 503 avec ce message : {« erreur » : « service_unavailable », « error_description » : Des « métadonnées SAML n'est pas initialisées »}
Cause possible	Les métadonnées d'IDP n'est pas disponible dans des id de Cisco. L'établissement de confiance entre les id et l'AD FS de Cisco n'est pas complet.
Action recommandée	Naviguez vers la console de gestion d'id de Cisco et voyez si les id est dans l'état **non configuré**. Confirmez si des métadonnées d'IDP est téléchargées ou pas. Sinon, téléchargez les métadonnées d'IDP téléchargées de l'AD FS. Pour plus de détails voyez ici.

Demande SAML traitant par l'AD FS

Le traitement de demande SAML est la première étape dans l'AD FS dans le SSO circulent. La requête envoyée SAML par les id de Cisco est lue, validée et déchiffrée par l'AD FS dans cette étape. Le traitement réussi de cette demande a comme conséquence deux scénarios :

1. Si c'est une procédure de connexion fraîche dans un navigateur, l'AD FS affiche la forme de procédure de connexion.Si c'est un relogin d'un utilisateur déjà authentifié d'une session du navigateur existante, des tentatives FS d'AD d'envoyer le dos de réponse SAML directement.

Note: Le préalable principal à cette étape est pour l'AD FS de faire configurer la confiance répondante d'interlocuteur.

Erreurs communes produites pendant ce processus

1. AD FS n'ayant pas des plus défunts le certificat SAML id de Cisco.

Résumé du problème	L'AD FS n'affichant pas la page de connexion, au lieu de cela affiche une page d'erreur.

	Navigateur
	L'AD FS affiche une page d'erreur semblable à ceci :
	Il y avait un problème d'accès le site. Essayez de parcourir au site de nouveau.
	Si le problème persiste, contactez l'administrateur de ce site et fournissez le numéro de référence pour identifier le problème.
	Numéro de référence : 1ee602be-382c-4c49-af7a-5b70f3a7bd8e
	Visualisateur d'événements FS d'AD
	Le service de fédération a rencontré une erreur tout en traitant la demande d'authentificati
	SAML.
	Les informations supplémentaires
	`Détails d'exception :`
	`Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException :`
	`MSIS0038 : Le message SAML a la signature fausse. Émetteur : « myuccx.cisco.com ». à`
	`Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage`
	`(message de MSISSamlBindingMessage) à`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage`
	`(CreateErrorMessageRequest createErrorMessageRequest) à`
	`Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest`
	`(requestMessage de message)`

Cause possible	La confiance comptante d'interlocuteur n'est pas établie ou le certificat d'id de Cisco a cha mais le même n'est pas téléchargé à l'AD FS.
Action	Établissez la confiance entre l'AD FS et les id de Cisco avec le dernier certificat d'id de Cis

recommandée	Veuillez s'assurer que le certificat d'id de Cisco n'est pas expiré. Vous pouvez voir le table de bord d'état en Gestion de gestion d'identité de Cisco. Si oui, régénérez le certificat dans page Settings. Pour plus de détails sur la façon dont établir des métadonnées faites confiance à travers ADFS et id de Cisco voient, ici

Réponse SAML envoyant par l'AD FS

L'ADFS envoie la réponse SAML de nouveau aux id de Cisco par l'intermédiaire du navigateur après que l'utilisateur soit avec succès authentifié. ADFS peut renvoyer une réponse SAML avec code d'état qui indique le succès ou échec. Si l'authentification de forme n'est pas activée dans l'AD FS puis ceci indiquera une réponse de panne.

Erreurs communes produites pendant ce processus

1. L'authentification de forme n'est pas activée dans l'AD FS

Résumé du problème	Le navigateur affiche la procédure de connexion NTLM, et puis échoue sans réorienter av succès à Cisco des id.
Étape de panne	Envoi de la réponse SAML
Cause possible	**Navigateur :** Le navigateur affiche la procédure de connexion NTLM, mais après procédure de connexi réussie, elle échoue avec beaucoup réoriente. Les id de Cisco prend en charge seulement l'authentification basée par forme, authentifica de forme n'est pas activés dans l'AD FS.
Action recommandée	Pour plus de détails sur la façon dont activer l'authentification de forme voyez : Configuration d'authentification de forme ADFS 2.0 Configuration d'authentification de forme ADFS 3.0

Réponse SAML traitant par des id de Cisco

Dans cette étape, les id de Cisco obtient une réponse SAML de l'AD FS. Cette réponse pourrait contenir code d'état qui indique le succès ou échec. Une réponse d'erreur de l'AD FS résulte dans une page d'erreur et le même doit être mis au point.

Pendant une réponse réussie SAML, le traitement de la demande peut échouer pour ces raisons :

- Métadonnées incorrectes d'IDP (AD FS).
- Le manque de récupérer a attendu les demandes sortantes de l'AD FS.
- Des horloges FS d'id et d'AD de Cisco ne sont pas synchronisées.

Erreurs communes produites pendant ce processus

1. Le certificat FS d'AD dans des id de Cisco n'est pas le plus tardif.

Résumé du problème	La demande de procédure de connexion échoue avec l'erreur 500 sur le navigateur avec c comme invalidSignature.
Étape de panne	Traitement de réponse SAML
	Navigateur :

	erreur 500 avec ce message dans le navigateur :
	« Error Code: invalidSignature
	Message : Le certificat de signature n'apparie pas ce qui est défini dans les métadonnées
	Visualisateur d'événements FS d'AD :
	Aucune erreur
	Log d'id de Cisco :
	`2016-04-13 ERREUR par défaut [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 de`
	`IST(+0530) - exception traitant la demande com.sun.identity.saml2.common.SAML2Exception`
	`certificat de signature n'apparie pas ce qui est défini dans les métadonnées d'entité. à`
	`com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) à`
	`com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseIm`
	`à com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) à`
	`com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)`

Cause possible	Le traitement de réponse SAML manqué comme certificat d'IDP est différent de ce qui est dans des id de Cisco.
Action recommandée	Téléchargez les dernières métadonnées FS d'AD de : **https://<ADFSServer>/federationmetadata/2007-06/federationmetadata.xml** Et téléchargez-le aux id de Cisco par l'intermédiaire de l'interface utilisateur de Managame gestion d'identité. Pour des détails, voyez pour configurer les id et l'AD FS de Cisco

2. Des horloges FS d'id et d'AD de Cisco ne sont pas synchronisées.

Résumé du problème	La demande de procédure de connexion échoue avec l'erreur 500 sur le navigateur avec c urn:oasis:names:tc:SAML:2.0:status:Success
Étape de panne	Traitement de réponse SAML

	Navigateur :
	erreur 500 avec ce message :
	Erreur de configuration d'IDP : Traitement SAML manqué
	L'assertion SAML a manqué de l'IDP avec code d'état : urn:oasis:names:tc:SAML:2.0:statu
	la configuration et l'essai d'IDP de nouveau.
	Log d'id de Cisco
	`2016-08-24 l'ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 de 18:46:56.780 IST(-`
	`SAML-22] - traitement de réponse SAML a manqué à l'exception com.sun.identity.saml2.commo`
	`temps dans SubjectConfirmationData est non valide. à`
	`com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:766)`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) à`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) à`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA`
	`à com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncSer`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSer`
	`com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) à`
	`java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) à`
	`java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) à`
	`java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-1]`
	Visualiseur SAML :
	Recherchez les champs de NotBefore et de NotOnOrAfter
	<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:0

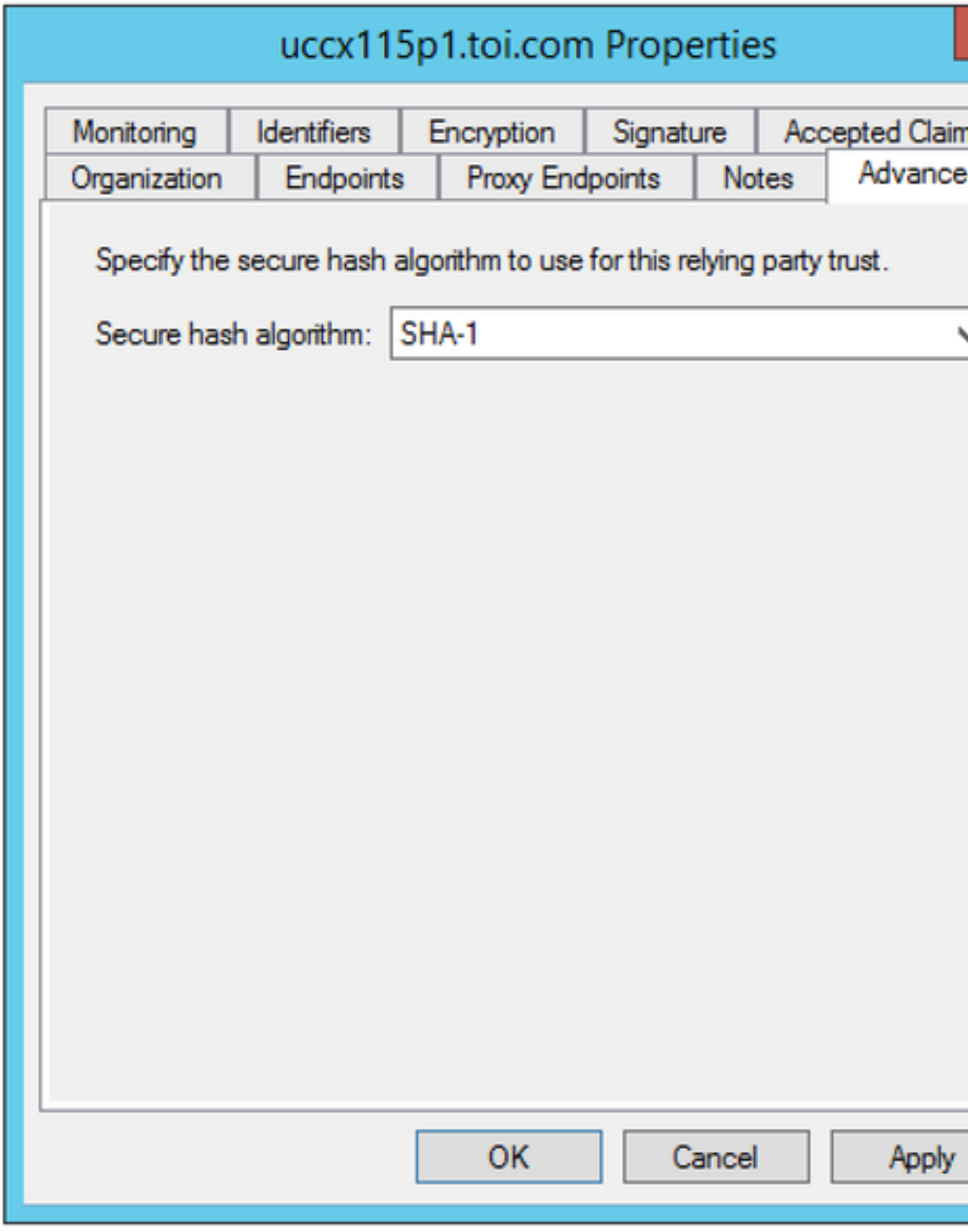
Cause possible	Chronométrez dans des id de Cisco et le système d'IDP est hors de sync.
Action recommandée	Synchronisez le temps dans les id de Cisco et le système FS d'AD. Le système FS d'AD d que et les id de Cisco sont temps synchronisé utilisant le serveur de NTP.

3. Algorithme faux de signature (SHA256 contre SHA1) dans l'AD FS

[Résumé du problème]	La demande de procédure de connexion échoue avec l'erreur 500 sur le navigateur avec l code:urn:oasis:names:tc:SAML:2.0:status:Responder Message d'erreur dans le log de vue d'événement FS d'AD – signature fausse Algorithm(S SHA1) dans l'AD FS
Étape de panne	Traitement de réponse SAML

	Navigateur
	erreur 500 avec ce message :
	Erreur de configuration d'IDP : Traitement SAML manqué
	L'assertion SAML a manqué de l'IDP avec code d'état : urn:oasis:names:tc:SAML:2.0:statu
	Vérifiez la configuration et l'essai d'IDP de nouveau.
	Visualisateur d'événements FS d'AD :
	La demande SAML n'est pas signée avec l'algorithme prévu de signature. La demande SA
	l'algorithme http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 de signature.
	L'algorithme prévu de signature est http://www.w3.org/2000/09/xmldsig#rsa-sha1
	Log d'id de Cisco :
	`ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - Le traitement de réponse SAML a`
	`com.sun.identity.saml2.common.SAML2Exception : Code d'état non valide dans la réponse. à`
	`com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) à`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) à`
	`com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA`

Cause possible	L'AD FS est configuré pour utiliser SHA-256.
	Mettez à jour l'AD FS pour utiliser SHA-1 pour la signature et le cryptage. 1. La RDP au système FS d'AD. 2. Ouvrez la console FS d'AD. 3. Sélectionnez la **confiance comptante d'interlocuteur** et cliquez sur **Properties** 4. Sélectionnez l'**onglet Avancé**. 5. SHA-1 choisi de la liste déroulante.
Action recommandée	



4. Règle sortante de demande non configurée correctement

[Résumé du problème](#)	La demande de procédure de connexion échoue avec 500 que l'erreur sur le navigateur a pourrait pas récupérer l'identifiant d'utilisateur de la réponse SAML. /Could ne pas récupér d'utilisateur de la réponse SAML. » uid et/ou user_principal non réglés dans les demandes sortantes.
Étape de panne	Traitement de réponse SAML
	Navigateur : erreur 500 avec ce message : Erreur de configuration d'IDP : Traitement SAML manqué.

N'a pas pu récupérer l'identifiant d'utilisateur de la réponse SAML. /Could ne pas récupére
d'utilisateur de la réponse SAML.

Visualisateur d'événements FS d'AD :

Aucune erreur

Log d'id de Cisco :

```
ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Le traitement de réponse SAML a
com.sun.identity.saml.common.SAMLException : N'a pas pu récupérer l'identifiant d'utilisa
SAML. à com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsy
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServ
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSe
```

Cause possible

Des demandes sortantes obligatoires (uid et user_principal) ne sont pas configurées corre
règles de demande.

Si vous n'avez pas configuré la règle de demande de NameID ou l'uid ou user_principal n'
correctement.

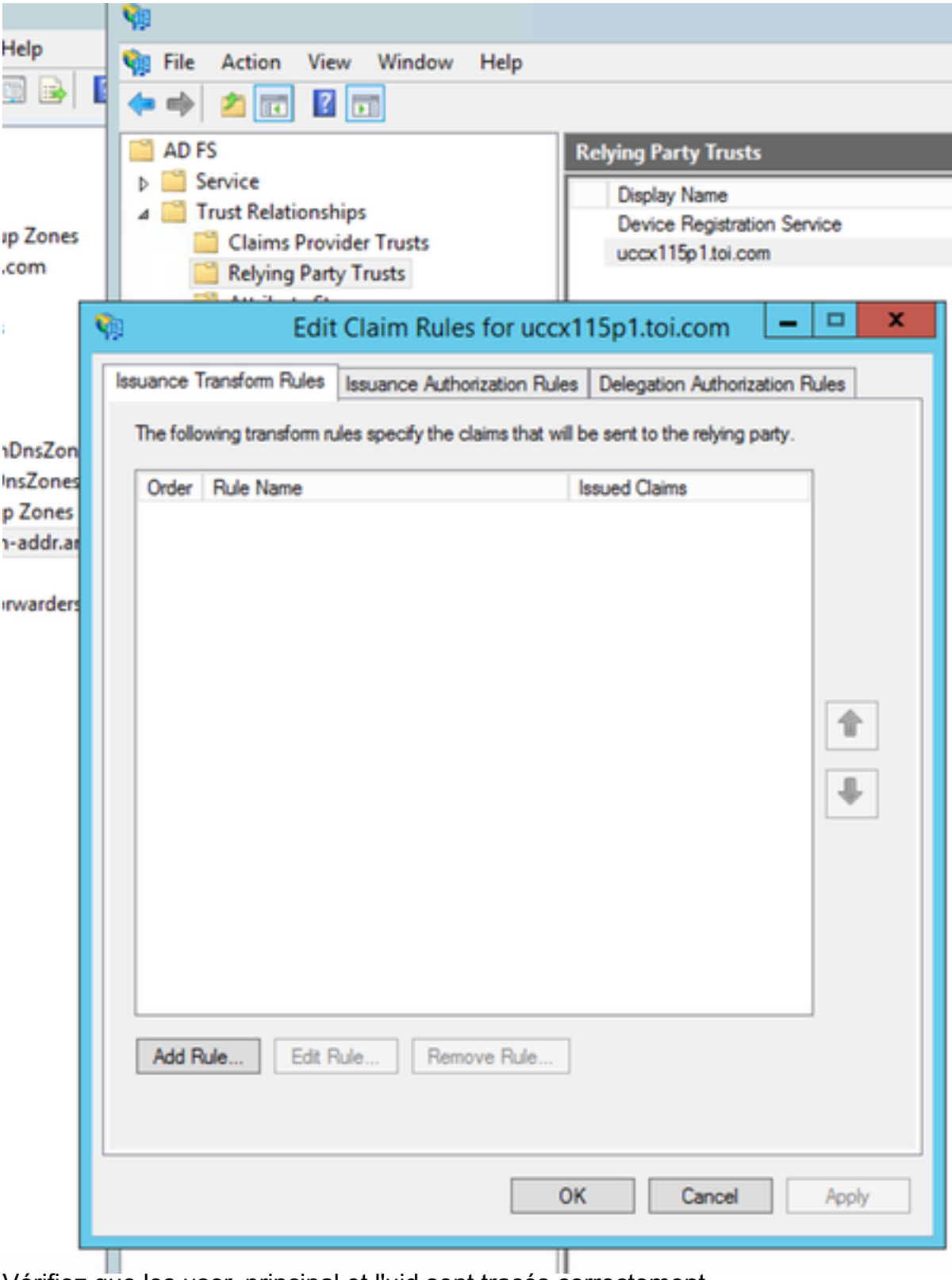
Si la règle de NameID est non configurée ou user_principal n'est pas tracé correctement, l
qu'user_principal n'est pas récupéré puisque c'est la propriété que les id de Cisco recherc

Si l'uid n'est pas tracé correctement, les id de Cisco indique que l'uid n'est pas récupéré.

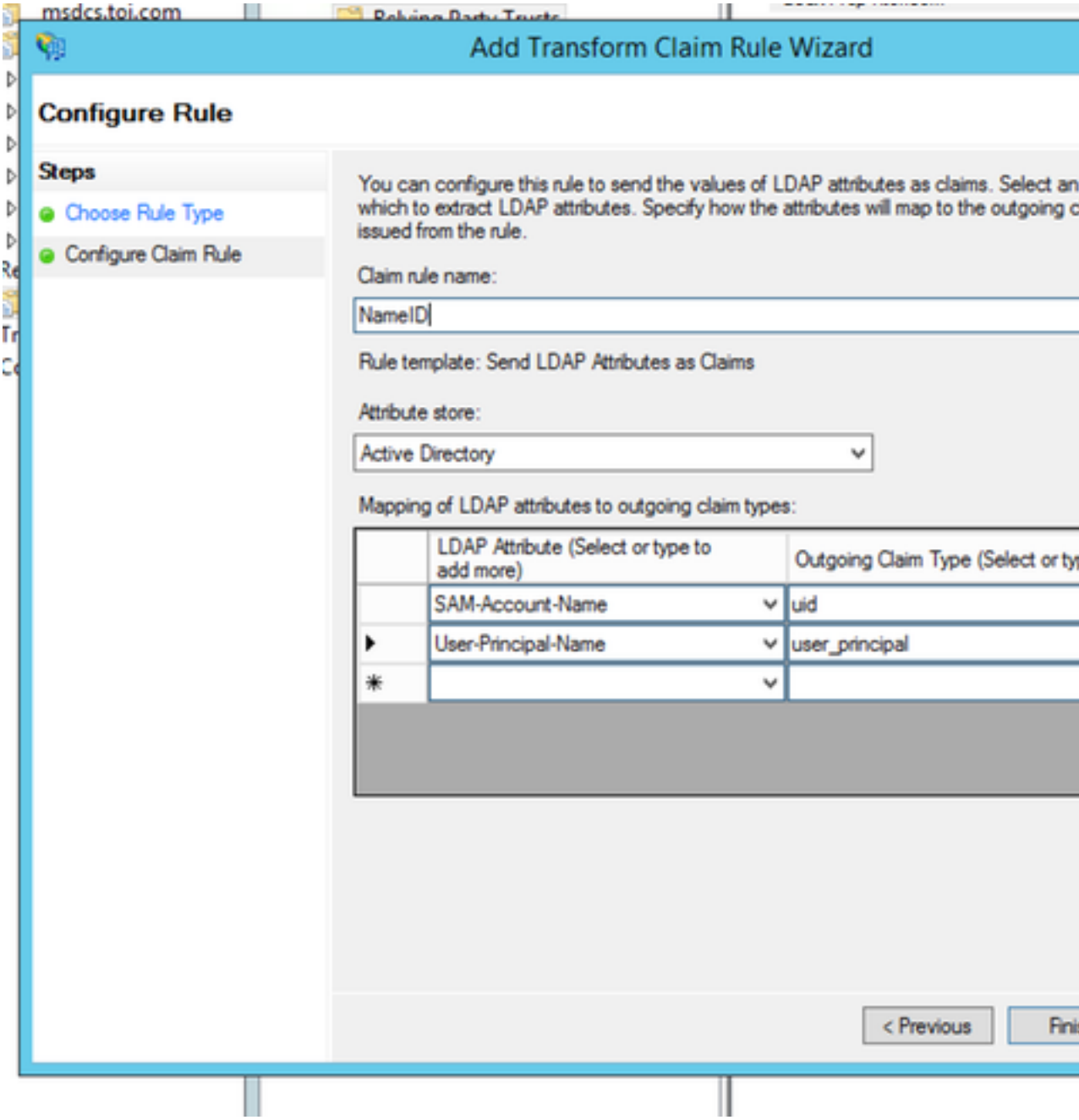
Selon des règles de demande FS d'AD, assurez-vous que des attributs traçant pour « use
« uid » sont définis comme dans guide de configuration d'IDP (qui guident ?).

1. La RDP au système FS d'AD.
2. Éditez les règles de demande pour la confiance comptante d'interlocuteur.

Action recommandée



3. Vérifiez que les user_principal et l'uid sont tracés correctement



5. La règle sortante de demande n'est pas configurée correctement dans un AD fédéré FS

[Résumé du problème](#)

La demande de procédure de connexion échoue avec 500 que l'erreur sur le navigateur av
message « ne pourrait pas récupérer l'identifiant d'utilisateur de la réponse SAML. ou n'a p
récupérer le principal d'utilisateur de la réponse SAML. » quand l'AD FS est un AD fédéré

Étape de panne

Traitement de réponse SAML

Navigateur
erreur 500 avec ce message :
Erreur de configuration d'IDP : Traitement SAML manqué
N'a pas pu récupérer l'identifiant d'utilisateur de la réponse SAML. /N'a pas pu récupérer le
d'utilisateur de la réponse SAML.
Visualisateur d'événements FS d'AD :
Aucune erreur
Log d'id de Cisco :

```
ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - Le traitement de réponse SAML a
l'exception com.sun.identity.saml.common.SAMLException : N'a pas pu récupérer l'identifia
d'utilisateur de la réponse SAML. à
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServle
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServ
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSer
```

Cause possible Dans un AD fédéré FS il y a plus de configurations a exigé qui pourraient manquer.

Action recommandée Vérifiez si la configuration FS d'AD dans l'AD fédéré est faite selon la section **pour une con Multi-domaine pour l'AD fédéré FS** configurent dedans les id et l'AD FS de Cisco

6. Règles faites sur commande de demande non configurées correctement

Résumé du problème La demande de procédure de connexion échoue avec 500 que l'erreur sur le navigateur av pourrait pas récupérer l'identifiant d'utilisateur de la réponse SAML. /Could ne pas récupér d'utilisateur de la réponse SAML. »
uid et/ou user_principal non réglés dans les demandes sortantes.

Étape de panne Traitement de réponse SAML

Navigateur
erreur 500 avec ce message :
L'assertion SAML a manqué de l'IDP avec code d'état : urne : oasis : noms : comité techni **SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy**. Vé et l'essai d'IDP de nouveau.

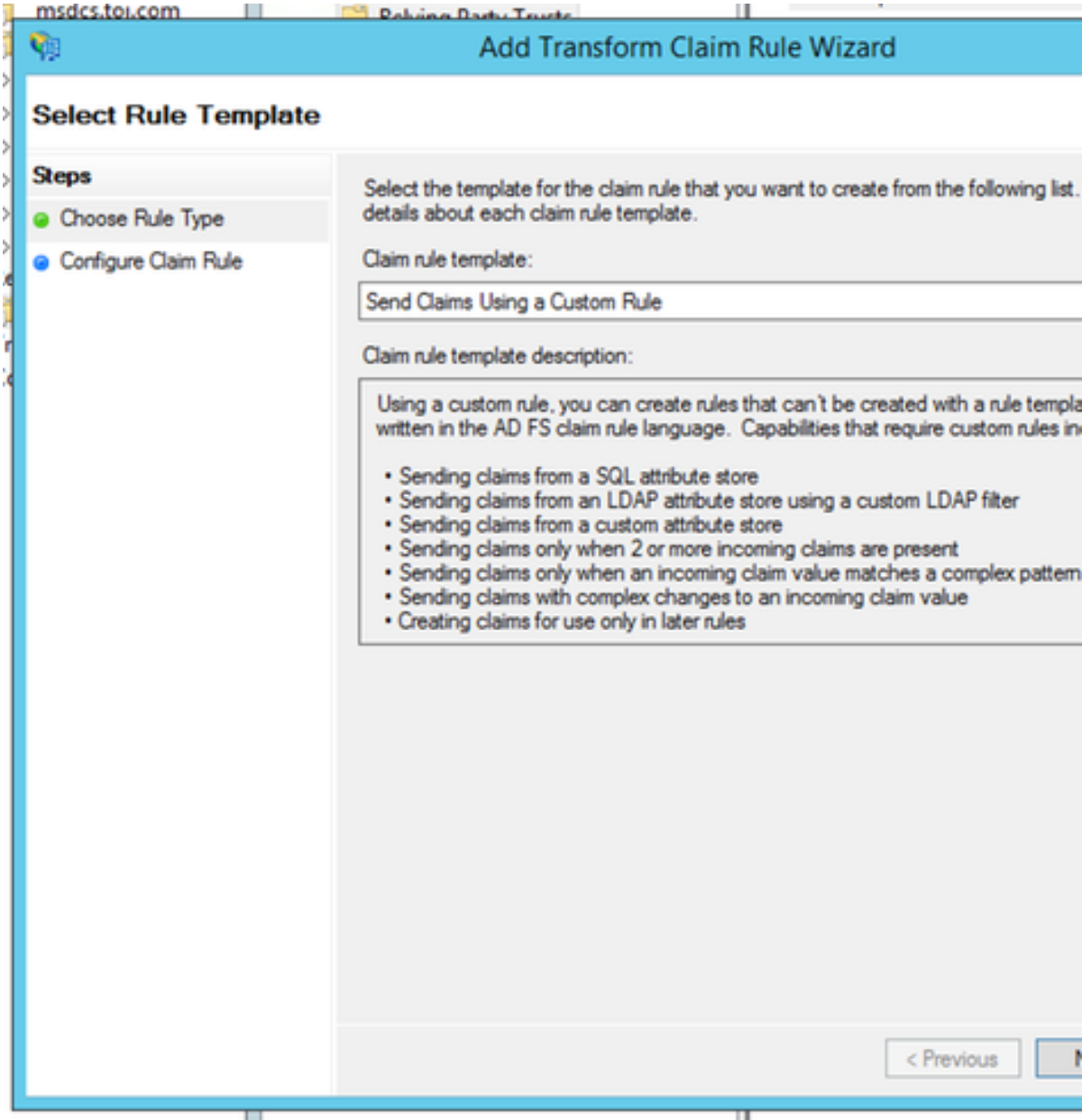
Visualisateur d'événements FS d'AD :
La demande d'authentification SAML a eu une stratégie de NameID qui ne pourrait pas êt
Demandeur : myids.cisco.com
Format d'identifiant de nom : urn:oasis:names:tc:SAML:2.0:nameid-format:transient
SPNameQualifier : myids.cisco.com
Détails d'exception :
MSIS1000 : La demande SAML a contenu un NameIDPolicy qui n'a pas été satisfait par le NameIDPolicy demandé : AllowCreate : Format vrai : urn:oasis:names:tc:SAML:2.0:namei SPNameQualifier : myids.cisco.com. Propriétés réelles de NameID : null.
Cette demande a manqué.
Action de l'utilisateur
Employez la Gestion FS 2.0 d'AD SNAP-dans pour configurer la configuration qui émet l'ic
Log d'id de Cisco :

```
2016-08-30 les INFORMATIONS com.cisco.ccbu.ids SAML2SPAdapter.java:76 de 09:45:30.471 IST
SAML-82] - SSO ont manqué avec le code : 1. État de réponse : <samlp : <samlp de Status>
statut Value="urn:oasis:names:tc:SAML:2.0:status:Requester"> : Code statut
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp : StatusCode> </s
</samlp : Status> pour AuthnRequest : l'ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet.jav
applicable 2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] - traitement de répo
l'exception com.sun.identity.saml2.common.SAML2Exception : Code d'état non valide dans la
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) à
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) à
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
```

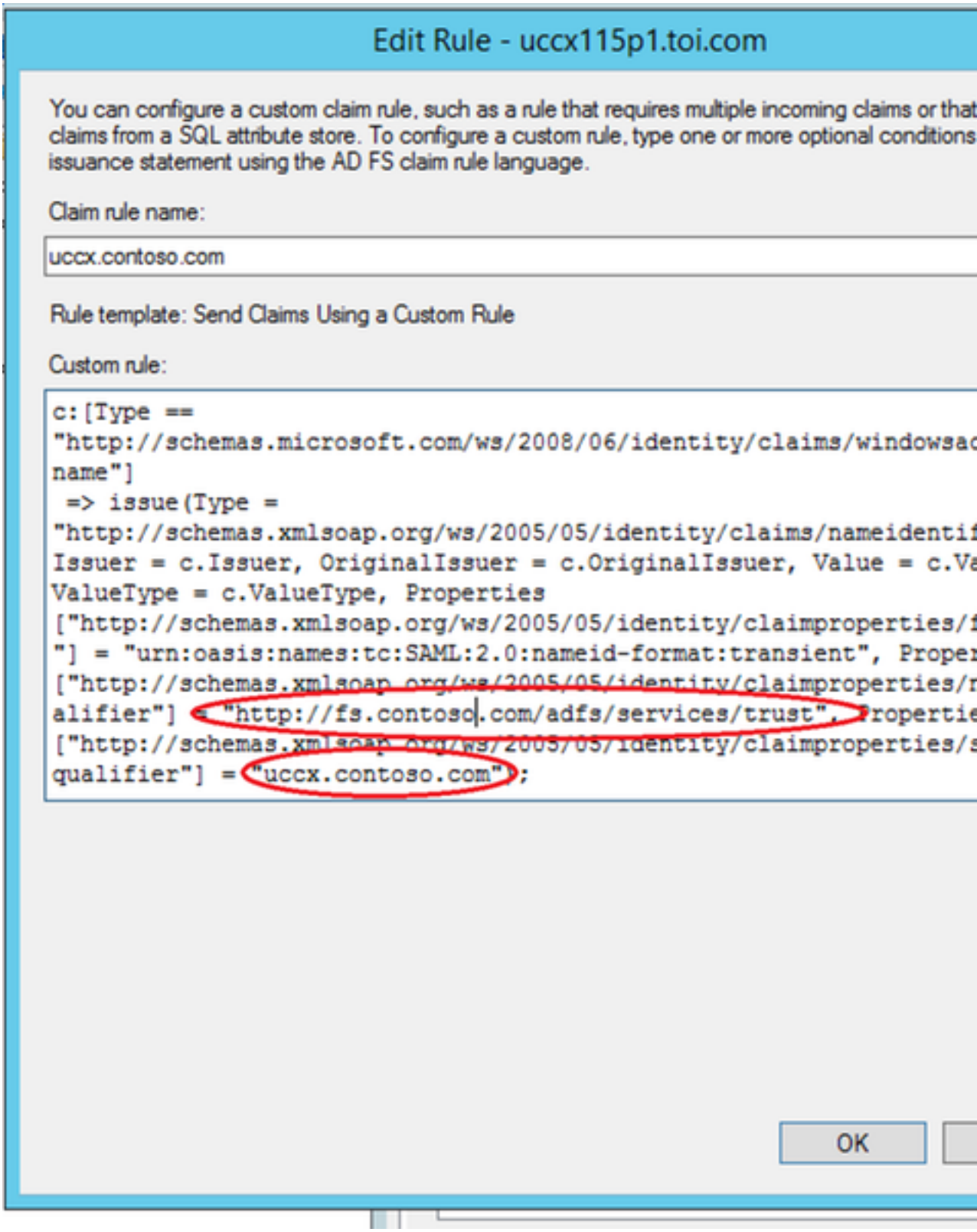
Cause possible La règle faite sur commande de demande n'est pas configurée correctement.

Action recommandée
Selon des règles de demande FS d'AD, assurez-vous que des attributs traçant pour « use « uid » sont définis en tant que dans guide de configuration (qui guident ?).

1. La RDP au système FS d'AD.
2. Éditez les règles de demande pour des règles faites sur commande de demande.



3. Vérifiez que l'AD FS et des noms de domaine complet d'id de Cisco sont donnés.



7. Trop de demandes à l'AD FS.

[Résumé du problème](#)	La demande de procédure de connexion échoue avec l'erreur 500 sur le navigateur avec l code:urn:oasis:names:tc:SAML:2.0:status:Responder Le message d'erreur dans le log de vue d'événement FS d'AD indique qu'il y a trop de de
Étape de panne	Traitement de réponse SAML **Navigateur** erreur 500 avec ce message : Erreur de configuration d'IDP : Traitement SAML manqué L'assertion SAML a manqué de l'IDP avec code d'état : urn:oasis:names:tc:SAML:2.0:statu

Vérifiez la configuration et l'essai d'IDP de nouveau.
Visualisateur d'événements FS d'AD :
Microsoft.IdentityServer.Web.InvalidRequestException :
MSIS7042 : **La même session du navigateur de client a fait des demandes de '6' dans dur**
secondes '16'. Contactez votre administrateur pour des détails.
àMicrosoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionC
àMicrosoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse (
MSISSignInResponse)

```
Événement Xml : <Data >Microsoft.IdentityServer.Web.InvalidRequestException de <EventData
http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> de " Name= "
Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}"/> <EventID>364</EventID> <Version>0</Versio
<Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000001</Keywords> <TimeCreated Sy
19T12:14:58.474662600Z" xmlns:auto-ns2=" le <UserData> </System> UserID="S-1-5-21-168062
1502263146-1105"/> le <Security <Computer>myadfs.cisco.com</Computer> 2.0/Admin</Channel>
ThreadID="392" ProcessID="2264" le <Execution ActivityID="{98778DB0-869A-4DD5-B3B6-0565A0
<Correlation <EventRecordID>29385</EventRecordID>/> http://schemas.microsoft.com/win/2004
<Event le » de <Provider de <System> http://schemas.microsoft.com/win/2004/08/events/even
: MSIS7042 : La même session du navigateur de client a fait des demandes de '6' pendant
'16'. Contactez votre administrateur pour des détails. à
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie()
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse (réponse
MSISSignInResponse) </Data> </EventData> </Event> </UserData> </Event>
```

Log d'id de Cisco

```
2016-04-15 ERREUR par défaut [IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102 de
0400) - exception traitant la demande com.sun.identity.saml2.common.SAML2Exception : Code
dans la réponse. à com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.jav
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) à
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA
```

Cause possible

Il y a trop de demandes étant livré à l'AD FS de la même session du navigateur.

Ceci ne devrait pas typiquement se produire dans la production. Mais si vous rencontrez c

Action recommandée

1. Visualisateur d'événements FS Windows d'AD de contrôle.
2. Revérifiez les configurations comptantes de confiance d'interlocuteur. Pour plus de d
   configurer les id et l'AD FS de Cisco
3. Relogin.

8. L'AD FS n'est pas configuré pour signer l'assertion et le message.

Résumé du problème

La demande de procédure de connexion échoue avec l'erreur 500 sur le navigateur avec c
invalidSignature

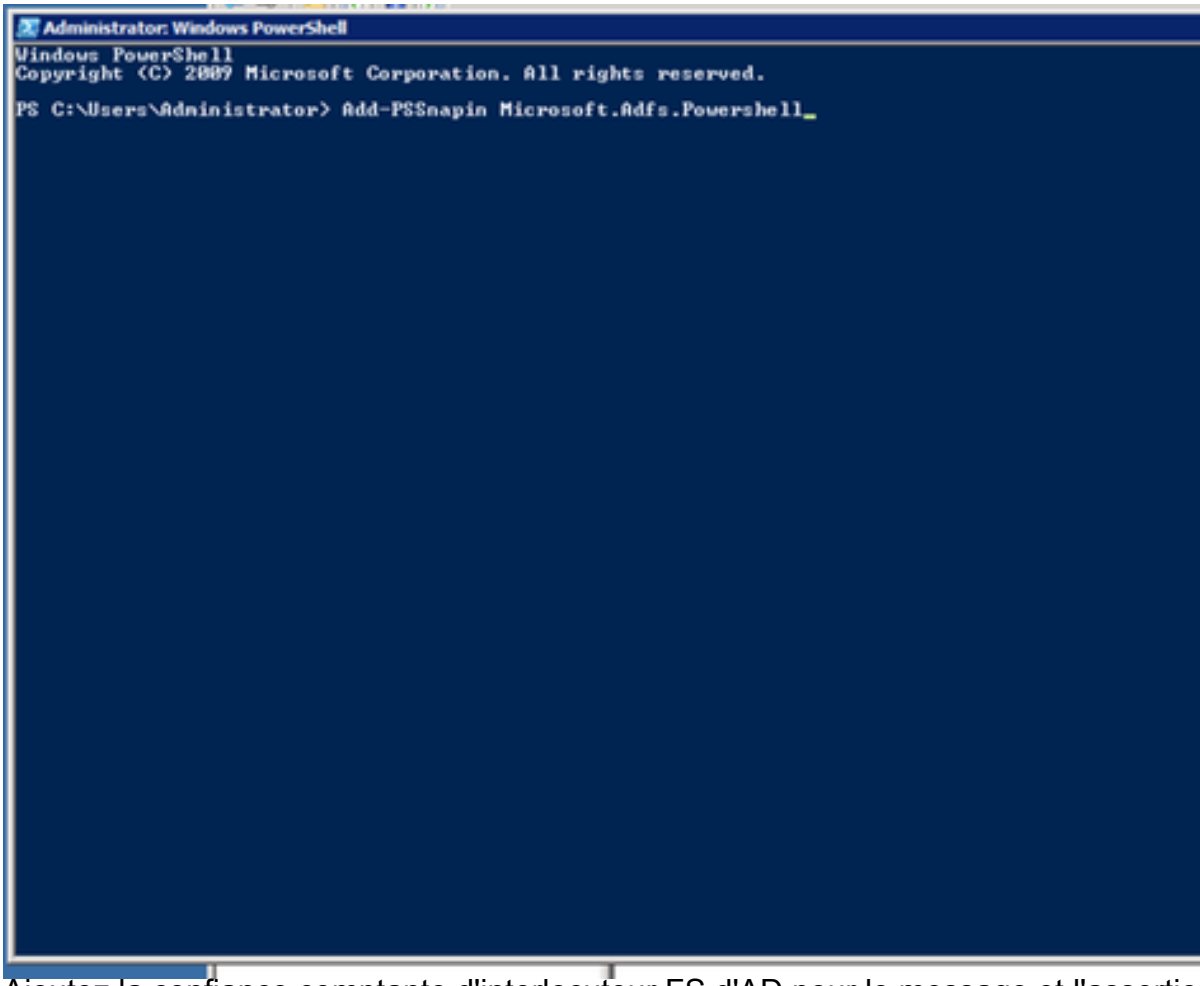
Étape de panne

Traitement de réponse SAML

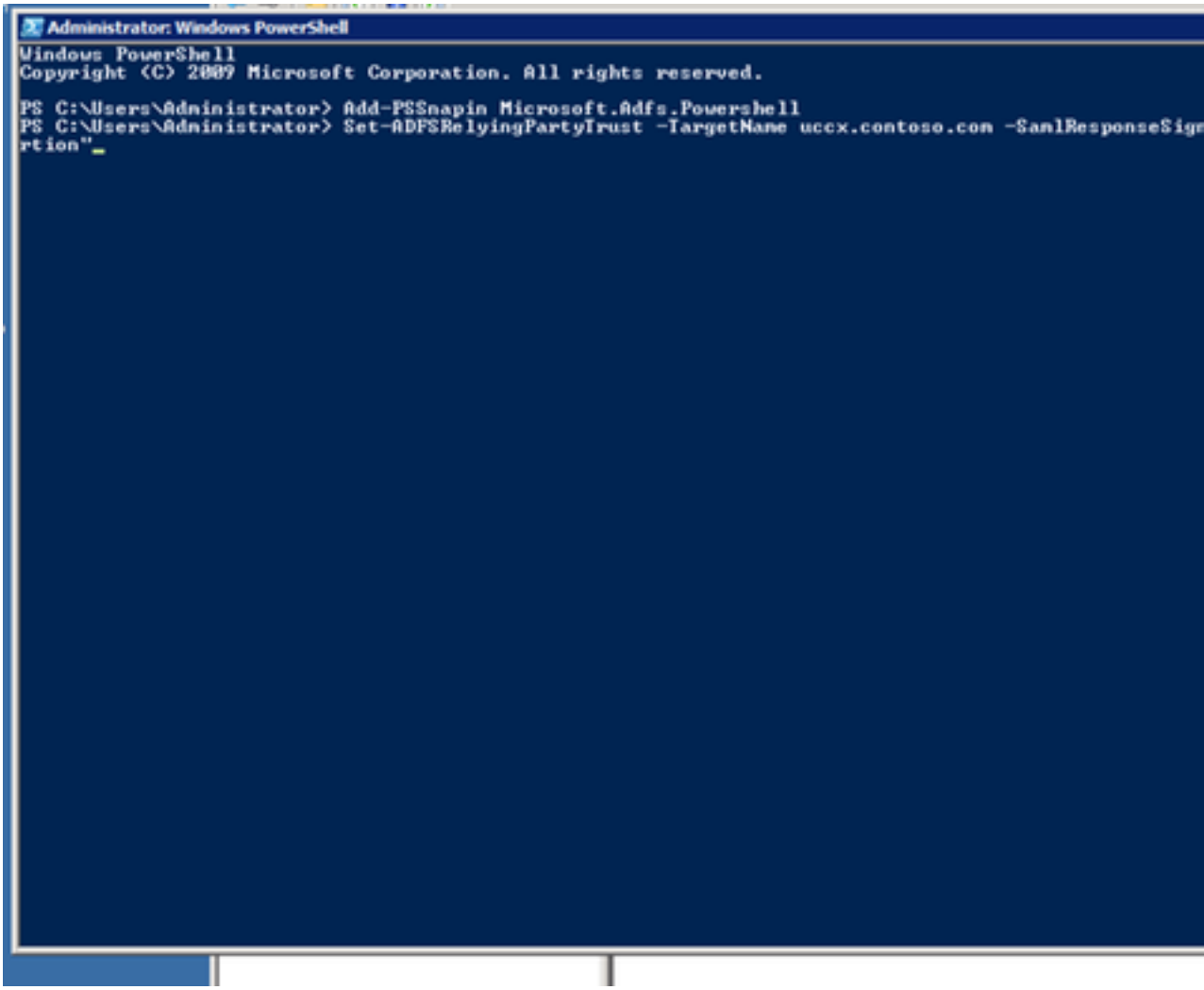
Navigateur
erreur 500 avec ce message :
« Error Code: invalidSignature
Message : Signature non valide dans ArtifactResponse.
Log d'id de Cisco :

```
2016-08-24 les INFORMATIONS saml2error.jsp saml2error_jsp.java:75 de 10:53:10.494 IST(+05
SAML-241] - traitement de réponse SAML ont manqué avec le code : invalidSignature ; messa
valide dans ArtifactResponse. 2016-08-24 l'ERREUR com.cisco.ccbu.ids IdSSAMLAsyncServlet
10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] - traitement de réponse SAML a manqué à
com.sun.identity.saml2.common.SAML2Exception : Signature non valide dans la réponse. à
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994) à
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) à
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2028)
```

Cause possible	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAML` L'AD FS n'est pas configuré pour signer l'assertion et le message.
Action recommandée	1. Exécutez la commande de powershell FS d'AD : **Positionnement-ADFSRelyingParty** **<Relying Identifier> d'interlocuteur de TargetName - SamlResponseSignature « Mes** 2. La RDP au système d'AD. 3. Ouvrez **Powershell**. 4. Ajoutez le SNAP-Institut central des statistiques de Windows PowerShell à la sessio ne peut être exigée dedans si vous utilisez ADFS 3.0 puisque le CmdLet est déjà ins d'ajouter les rôles et les caractéristiques.



5. Ajoutez la confiance comptante d'interlocuteur FS d'AD pour le message et l'assertio



Informations connexes

Ceci est lié à la configuration du fournisseur d'identité décrite dans l'article :

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- Support et documentation techniques - Cisco Systems