Troubleshooting y problemas comunes ADFS/IdS

Contenido

Introducción

La interacción del lenguaje de marcado de la aserción de la Seguridad (SAML) entre el servicio de la identidad de Cisco (IdS) y los servicios de la federación del Active Directory (AD FS) vía un navegador es la base de la Solo-muestra en el flujo del login (SSO). Este documento le ayudará en los problemas del debugging relacionados con las configuraciones en el Cisco IDS y AD FS, junto con la acción recomendada para resolverlos.

Modelos de despliegue del Cisco IDS

Producto	Despliegue
UCCX	Coresidente
PCCE	Coresidente con CUIC (centro unificado Cisco de la inteligencia) y LD (datos vivos)
UCCE	Coresidente con CUIC y el LD para las implementaciones 2k. Independiente para las implementaciones 4k y 12k.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Versión 11.5 del Cisco Unified Contact Center Express (UCCX) o versión 11.5 del Cisco Unified Contact Center Enterprise o versión embalada 11.5 de la empresa del Centro de contacto (PCCE) como aplicables.
- Microsoft Active Directory - AD instalado en el Servidor Windows
- IdP (proveedor de la identidad) - Versión 2.0/3.0 del servicio de la federación del Active Directory (AD FS)

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Después de que la relación de confianza se establezca entre el Cisco IDS y AD FS (véase aquí para los detalles, común para UCCX y UCCE), se espera que al administrador funcione con la configuración de la prueba SSO en la página Configuración de la Administración del servicio de la identidad para asegurarse de que la configuración entre el Cisco IDS y AD FS trabaja muy bien. Si la prueba falla, utilice las aplicaciones apropiadas y las sugerencias dadas en esta guía para resolver el problema.

Aplicaciones y registros que pueden ser prácticos en el debugging

Aplicación/registro	Detalles	Donde encontrar la herramienta
Registro del Cisco IDS	El maderero del Cisco IDS registrará cualquier error que sucediera en el Cisco IDS.	Utilice RTMT para conseguir los registros d Cisco IDS. Para la información sobre cómo utilizar RTMT vea, dirija para utilizar RTMT Observe por favor que RTMT el nombre es

		servicio de la identidad de Cisco. Para encontrar los registros, navegue al **servicio al registro de la identidad de Cisco**
Registros de Fedlet	Los registros de Fedlet darán más detalles sobre cualquier error de SAML que sucede en el Cisco IDS	Utilice RTMT para conseguir los registros d Fedlet. La ubicación para el registro de Fedlet es lo mismo que los registros del Cisco IDS. Los registros del fedlet comienzan con el **fedlet- del** prefijo
Métrica del Cisco IDS API	La métrica API se puede utilizar para mirar en y para validar cualquier error que el Cisco IDS API pudo haber vuelto y el número de peticiones que sean procesadas por el Cisco IDS	Utilice RTMT para conseguir la métrica API Observe por favor que RTMT el nombre es **servicio de la identidad de Cisco** Esto aparecerá bajo **métrica** separada de la carpeta. Observe por favor que **saml_metrics.csv y** authorize_metrics.csv **s las** métricas relevantes para este document
Visor de eventos en AD FS	Permite que los usuarios vean el evento abre una sesión el sistema. Cualquier error en AD FS mientras que el proceso de la petición de SAML/el envío de la respuesta de SAML será registrado aquí.	En la máquina AD FS, navegue a los **>Applications del visor de eventos** y **mantie el >AdDFS 2.0 de los registros > Admin** En Windows 2008, el visor de eventos del lanzamiento del **panel de control > del funcionamiento y el mantenimiento > Administrative Tools** En Windows 2012, póngalo en marcha del panel de control \ del sistema y de la Seguridad \ Administrative Tools. Mire por favor su documentación de las ventanas para ver donde encontrar el visor eventos.
SAML Visualizador	Un Visualizador de SAML ayudará en la mirada de la petición y de la respuesta de SAML que se envían desde/hasta el Cisco IDS. Esta aplicación del buscador es muy útil para el análisis de la petición/de la respuesta de SAML.	Éstos son algunos SAML sugeridos Visualizadores que usted puede utilizar par mirar la petición y la respuesta de SAML 1. Fiddler Cómo utilizar al fiddler con AD FSFiddler Chrome plug-in 2. SAML trazalíneas - Firefox 3. SAML el panel de Chrome

Diagrama de flujo con las opciones de debugging

Los diversos pasos para la autenticación SSO se muestran en la imagen junto con y los artefactos del debugging en cada paso en caso de un error en ese paso.

Esta tabla da los detalles en cómo identificar los errores en cada paso del SSO en el navegador. Las diversas herramientas y cómo pueda ayudan en el debugging se especifican también.

Paso	Cómo identificar el error en el navegador	Herramientas/registro	Configuraciones a mirar
Petición de AuthCode que procesa por el Cisco IDS	En caso del error, no reorientan al navegador al punto final o a AD FS de SAML, un error JSON es mostrado por el Cisco IDS, que indica que el ID de cliente o reorienta el URL es	Los registros del Cisco IDS indican los errores que ocurren mientras que se valida y se procesa la petición del authcode. Métricas del Cisco IDS API -	Registro del cliente

	inválido.	Indica el número de peticiones procesadas y falladas.	
SAML lanzamiento de la petición por el Cisco IDS	Durante el error, no reorientan al navegador a AD FS, y una página/un mensaje del error será mostrada por el Cisco IDS.	Los registros del Cisco IDS indican si hay una excepción o no mientras que se inicia la petición. Métricas del Cisco IDS API - Indica el número de peticiones procesadas y falladas.	Cisco IDS en el estado NOT_CONFIGURED.
SAML petición que procesa por AD FS	Cualquier error procesar esta petición dará lugar a una página del error que es visualizada por el servidor AD FS en vez de la página de registro.	El visor de eventos en AD FS indica los errores que ocurren mientras que se procesa la petición. SAML navegador plug-in - Ayudas para ver la petición de SAML que se envía al AD FS.	Configuración de confianza de la confianza del partido en IdP
Envío SAML de la respuesta por AD FS	Someten a cualquier error enviar los resultados de la respuesta en una página del error que es visualizada por el servidor AD FS después de las credenciales válidas.	Visor de eventos en AD FS - Indica los errores que ocurren mientras que se procesa la petición.	• Configuración de confianza de la confianza del partido en IdP • Forme la configuración de la autenticación en AD FS.
SAML respuesta que procesa por el Cisco IDS	El Cisco IDS mostrará un error 500 con el Motivo de error y una página de la verificación rápida.	Visor de eventos en AD FS - Indica el error si el AD FS envía una respuesta de SAML sin un código de estado acertado. SAML navegador plug-in - Ayudas para ver la respuesta de SAML enviada por AD FS para identificar cuál es incorrecto. Registro del Cisco IDS - Indica que el error/la excepción ocurrió durante el proceso. Métricas del Cisco IDS API - Indica el número de peticiones procesadas y falladas.	• La demanda gobierna la configuración • Firma del mensaje y de la aserción

Petición de Authcode que procesa por el Cisco IDS

El punto de partida de login SSO, por lo que el Cisco IDS, es el pedido un código de autorización de una aplicación habilitada SSO. La validación de la petición API se hace para marcar si es una petición de un cliente registrado. Una validación acertada da lugar al navegador que es reorientado al punto final de SAML del Cisco IDS. Cualquier error en la validación de la petición da lugar a un error page/JSON (notación del objeto del Javascript) que es enviado detrás del Cisco IDS.

Errores comunes encontrados durante este proceso

1. Registro del cliente no hecho

Resumen de problemas	El pedido de registro falla con el error 401 en el navegador.

Mensaje de error	Navegador:
	error 401 con este mensaje: {“error”: “invalid_client”, “error_description”: “ClientId inválido.
	Registro del Cisco IDS:
	`2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] ADVIERTE com.cisco.ccbu.ids IdSConf`
	`cliente: fb308a80050b2021f974f48a72ef9518a5e7ca69 no existe el ERROR com.cisco.ccbu.ids`
	`de 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] - excepción que procesa el pedid`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException: ClientId invalid_client,`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemExceptio`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthori`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAu`
	`en org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)`

Posible Causa	El registro del cliente con el Cisco IDS no es completo.
Acción Recomendada	Navegue a la consola de administración del Cisco IDS y confirme si registran al cliente co registre a los clientes antes de proceder con el SSO.

2. Aplicación de accesos del usuario usando la dirección IP/el nombre del host del suplente

Resumen de problemas	El pedido de registro falla con el error 401 en el navegador.
Mensaje de error	Navegador: error 401 con este mensaje: {“error”: “invalid_redirectUri”, “error_description”: “Invlalid reorienta a Uri”}
Posible Causa	Aplicación de accesos del usuario usando la dirección IP/el nombre del host del suplente. En el modo SSO, si la aplicación se accede usando el IP, no trabaja. Las aplicaciones se deben acceder por el nombre de host por el cual son registradas en el Cisco IDS. Este problema puede suceder si el usuario accedió un nombre del host alterno que no se regis con el Cisco IDS.
Acción Recomendada	Navegue a la consola de administración del Cisco IDS y confirme si registran al cliente co el correcto reorienta URLand que utilizan lo mismo para acceder la aplicación.

SAML pida el lanzamiento por el Cisco IDS

SAML el punto final del Cisco IDS es el punto de partida del flujo de SAML en el login basado SSO. El lanzamiento de la interacción entre el Cisco IDS y AD FS se acciona en este paso. El requisito previó aquí es que el Cisco IDS debe conocer el AD FS para conectar con mientras que los meta datos correspondientes de IdP se deben cargar al Cisco IDS para que este paso tenga éxito.

Errores comunes encontrados durante este proceso

1. Meta datos AD FS no agregados al Cisco IDS

Resumen de problemas	El pedido de registro falla con el error 503 en el navegador.
Mensaje de error	Navegador: error 503 con este mensaje: {“error”: “service_unavailable”, “error_description”: “SAML lc meta datos no se inicializan”}
Posible Causa	Los meta datos de Idp no están disponibles en el Cisco IDS. El establecimiento de confi entre el Cisco IDS y AD FS no es completo.

Acción Recomendada	Navegue a la consola de administración del Cisco IDS y vea si los IdS están en el **estad configurado**. Confirme si los meta datos de IdP están cargados o no. Si no, cargue los meta datos de IdP descargados de AD FS. Para más detalles vea aquí.

SAML pida el proceso por AD FS

SAML el proceso de la petición es el primer paso en el AD FS en el flujo SSO. La petición de SAML enviada por el Cisco IDS es leída, validada y descifrada por AD FS en este paso. El proceso acertado de esta petición da lugar a dos escenarios:

1. Si es un login fresco en un navegador, el AD FS muestra el formulario de inicio de sesión.Si es un relogin ya de un usuario autenticado de una sesión del buscador existente, el AD FS intenta enviar la parte posterior de la respuesta de SAML directamente.

Note: El requisito previó principal para este paso es para el AD FS hacer la confianza de contestación del partido configurar.

Errores comunes encontrados durante este proceso

1. AD FS que no tiene el certificado de los últimos idS de Cisco SAML.

Resumen de problemas	El AD FS que no muestra la página de registro, en lugar muestra una página del error.
Mensaje de error	**Navegador** El AD FS muestra una página del error similar a esto: Había un problema que accedía el sitio. Intente hojear al sitio otra vez. Si persiste el problema, entre en contacto al administrador de este sitio y proporcione el número de referencia para identificar el problema. Número de referencia: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e **Visor de eventos AD FS** El servicio de la federación encontró un error mientras que procesaba el pedido de autenticación de SAML. **Datos adicionales** `Detalles de la excepción: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException: MSIS0038: SAML el mensaje tiene firma incorrecta. Emisor: “myuccx.cisco.com”. en Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage (mensaje de MSISSamlBindingMessage) en Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage (CreateErrorMessageRequest más createErrorMessageRequest) en Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest (requestMessage del mensaje)`
Posible Causa	La confianza de confianza del partido no se establece o el certificado del Cisco IDS ha cambiado, pero lo mismo no está cargada al AD FS.
Acción Recomendada	Establezca la confianza entre AD FS y Cisco IDS con el último certificado del Cisco IDS. Asegúrese por favor de que no esté expirado el certificado del Cisco IDS. Usted puede ve panel del estatus en la identidad de Cisco mantener la Administración. Si es así regenere certificado en la página Configuración. Para más detalles en cómo establecer los meta datos confíe en a través de ADFS y del C IDS ven, aquí

SAML respuesta que envía por AD FS

El ADFS envía la respuesta de SAML de nuevo al Cisco IDS vía el navegador después de que autentiquen al usuario con éxito. ADFS puede devolver una respuesta de SAML con un código de estado que indique el éxito o el error. Si la autenticación de la forma no se habilita en AD FS entonces ésta indicará una respuesta del error.

Errores comunes encontrados durante este proceso

1. La autenticación de la forma no se habilita en AD FS

Resumen de problemas	El login de las demostraciones NTLM del navegador, y entonces falla sin con éxito la reorientación al Cisco IDS.
Paso del error	Envío SAML de la respuesta
Mensaje de error	**Navegador:** Login de las demostraciones NTLM del navegador, pero después de la registración satisfactoria, falla con muchos reorienta.
Posible Causa	El Cisco IDS soporta solamente la autenticación basada forma, autenticación de la forr se habilita en AD FS.
Acción Recomendada	Para más detalles en cómo habilitar la autenticación de la forma vea: Configuración de la autenticación de la forma ADFS 2.0 Configuración de la autenticación de la forma del 3.0 ADFS

SAML respuesta que procesa por el Cisco IDS

En esta etapa, el Cisco IDS consigue una respuesta de SAML de AD FS. Esta respuesta podría contener un código de estado que indica el éxito o el error. Una respuesta de error de los resultados AD FS en una página del error y lo mismo tiene que ser hecha el debug de.

Durante una respuesta acertada de SAML, el proceso de la petición puede fallar por estas razones:

- Meta datos incorrectos de IdP (AD FS).
- El error extraer contaba con las demandas salientes de AD FS.
- El Cisco IDS y los relojes AD FS no se sincronizan.

Errores comunes encontrados durante este proceso

1. El certificado AD FS en el Cisco IDS no es el más último.

Resumen de problemas	El pedido de registro falla con el error 500 en el navegador con el código de error como invalidSignature.
Paso del error	SAML proceso de la respuesta
Mensaje de error	**Navegador:** error 500 con este mensaje en el navegador: Código de error: invalidSignature Mensaje: El certificado de firma no hace juego qué se define en los meta datos de la entic **Visor de eventos AD FS:** Ningún error **Registro del Cisco IDS:** `2016-04-13 ERROR predeterminado [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102`

	12:42:15.896 IST(+0530) - excepción que procesa la petición com.sun.identity.saml2.common.SAML2Exception: El certificado de firma no hace juego qué los meta datos de la entidad. en com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) en com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseI en com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985) en com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196)
Posible Causa	SAML el proceso de la respuesta fallado como certificado de IdP es diferente de cuál está en el Cisco IDS.
Acción Recomendada	Descargue los últimos meta datos AD FS de: **https://<ADFSServer>/federationmetadata/2006/federationmetadata.xml** Y carguelo al Cisco IDS vía la interfaz de usuario de Managament del servicio de la identi Para los detalles, vea el Cisco IDS y AD FS de la configuración

2. El Cisco IDS y los relojes AD FS no se sincronizan.

Resumen de problemas	El pedido de registro falla con el error 500 en el navegador con el código de estado: urn:oasis:names:tc:SAML:2.0:status:Success
Paso del error	SAML proceso de la respuesta
Mensaje de error	**Navegador:** error 500 con este mensaje: Error de configuración de IdP: SAML proceso fallado SAML aserción fallada de IdP con el código de estado: urn:oasis:names:tc:SAML:2.0:statu la configuración y el intento de IdP otra vez. **Registro del Cisco IDS** 2016-08-24 ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 de 18:46:56.780 IST(+05 SAML-22] - SAML el proceso de la respuesta falló con la excepción com.sun.identity.saml2.common.SAML2Exception: El tiempo en SubjectConfirmationData es in com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:766 com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) en com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) en com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038) com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAML en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncS com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSe com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) en java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) en java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) en java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-1 **SAML Visualizador:** Busque los campos de NotBefore y de NotOnOrAfter <Conditions el NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:4
Posible Causa	El tiempo en el sistema del Cisco IDS y de IdP está fuera de sincroniza.
Acción Recomendada	Sincronice el tiempo en el Cisco IDS y el sistema AD FS. Se recomienda que el sistema y son tiempo sincronizado usando el servidor NTP.

3. Algoritmo incorrecto de la firma (SHA256 contra el SHA1) en AD FS

Resumen de problemas	El pedido de registro falla con el error 500 en el navegador con el estatus code:urn:oasis:names:tc:SAML:2.0:status:Responder Mensaje de error en el View log del evento AD FS – Firma incorrecta Algorithm(SHA256 AD FS
Paso del error	SAML proceso de la respuesta
Mensaje de error	**Navegador** error 500 con este mensaje: Error de configuración de IdP: SAML proceso fallado SAML aserción fallada de IdP con el código de estado: urn:oasis:names:tc:SAML:2.0:statu

Verifique la configuración y el intento de IdP otra vez.

Visor de eventos AD FS:

SAML la petición no se firma con el algoritmo previsto de la firma. SAML la petición se firm
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 de la firma.
El algoritmo previsto de la firma es rsa-sha1

Registro del Cisco IDS:

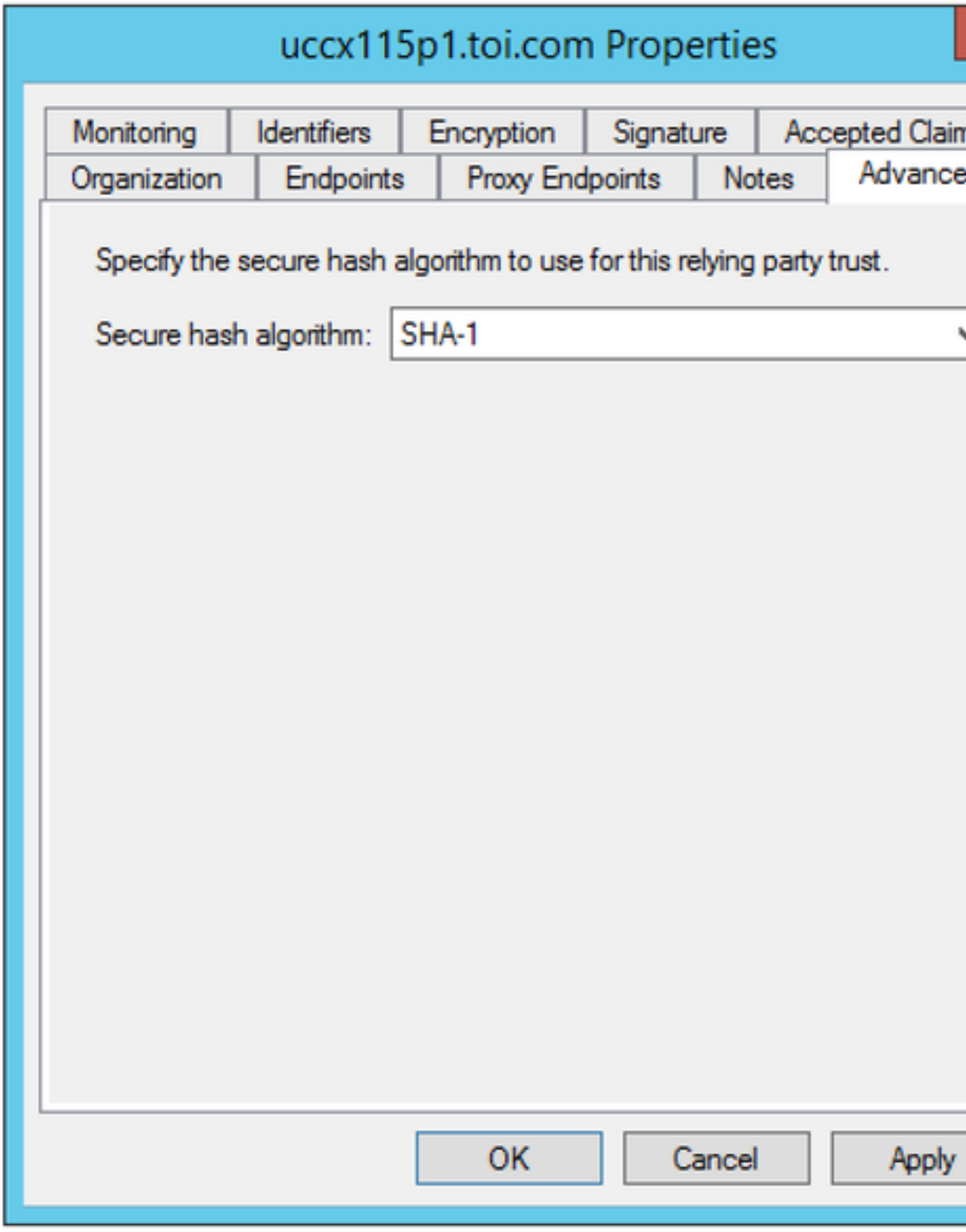
```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAML proceso de la respuesta fal
com.sun.identity.saml2.common.SAML2Exception: Código de estado inválido en la respuesta.
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) en
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) en
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAML
```

Posible Causa El AD FS se configura para utilizar el SHA-256.

Acción Recomendada

Ponga al día AD FS para utilizar el SHA-1 para firmar y el cifrado.

1. RDP al sistema AD FS.
2. Abra la consola AD FS.
3. Seleccione la **confianza de confianza del partido** y haga clic las **propiedades**
4. Seleccione la ficha Advanced (Opciones avanzadas).
5. Seleccione el SHA-1 de la lista desplegable.



4. Regla saliente de la demanda no configurada correctamente

Resumen de problemas	El pedido de registro falla con 500 que el error en el navegador con el mensaje “no podría Identificación de usuario de la respuesta de SAML. /Could no extraer el principal del usua SAML.” uid y/o user_principal no fijados en las demandas salientes.
Paso del error	SAML proceso de la respuesta
Mensaje de error	**Navegador:** error 500 con este mensaje: Error de configuración de IdP: SAML proceso fallado. No podía extraer la Identificación de usuario de la respuesta de SAML. /Could no extraer

de la respuesta de SAML.

Visor de eventos AD FS:

Ningún error

Registro del Cisco IDS:

```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAML proceso de la respuesta fal
com.sun.identity.saml.common.SAMLException: No podía extraer la Identificación de usuari
SAML. en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLA
en com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncS
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSe
```

Posible Causa

Las demandas salientes obligatorias (uid y user_principal) no se configuran correctamente
demanda.

Si usted no ha configurado la regla de la demanda de NameID o el uid o user_principal no
correctamente.

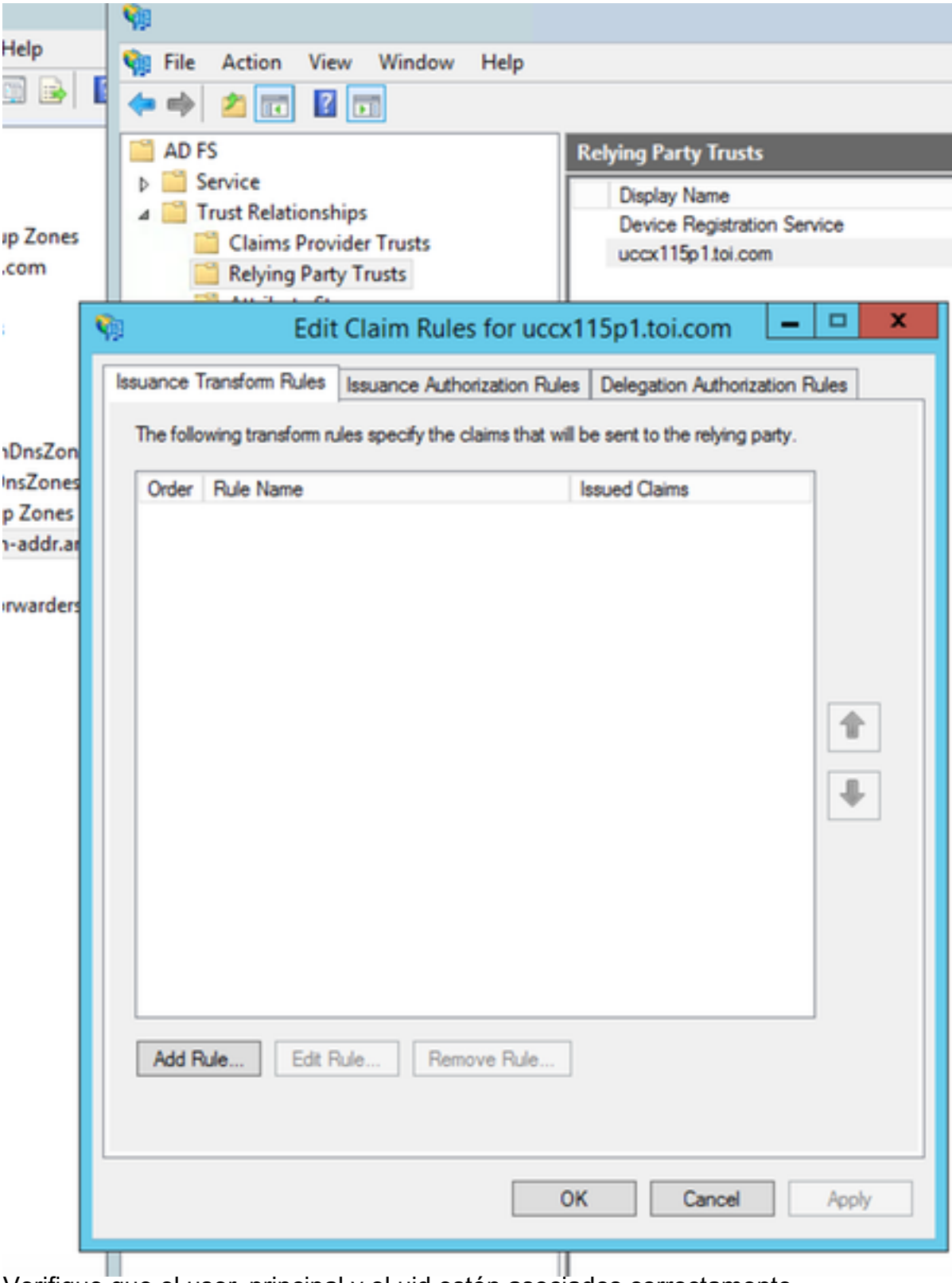
Si la regla de NameID es no configurada o user_principal no se asocia correctamente, el C
user_principal no se extrae puesto que ésta es la propiedad que el Cisco IDS busca.

Si el uid no se asocia correctamente, el Cisco IDS indica que el uid no está extraído.

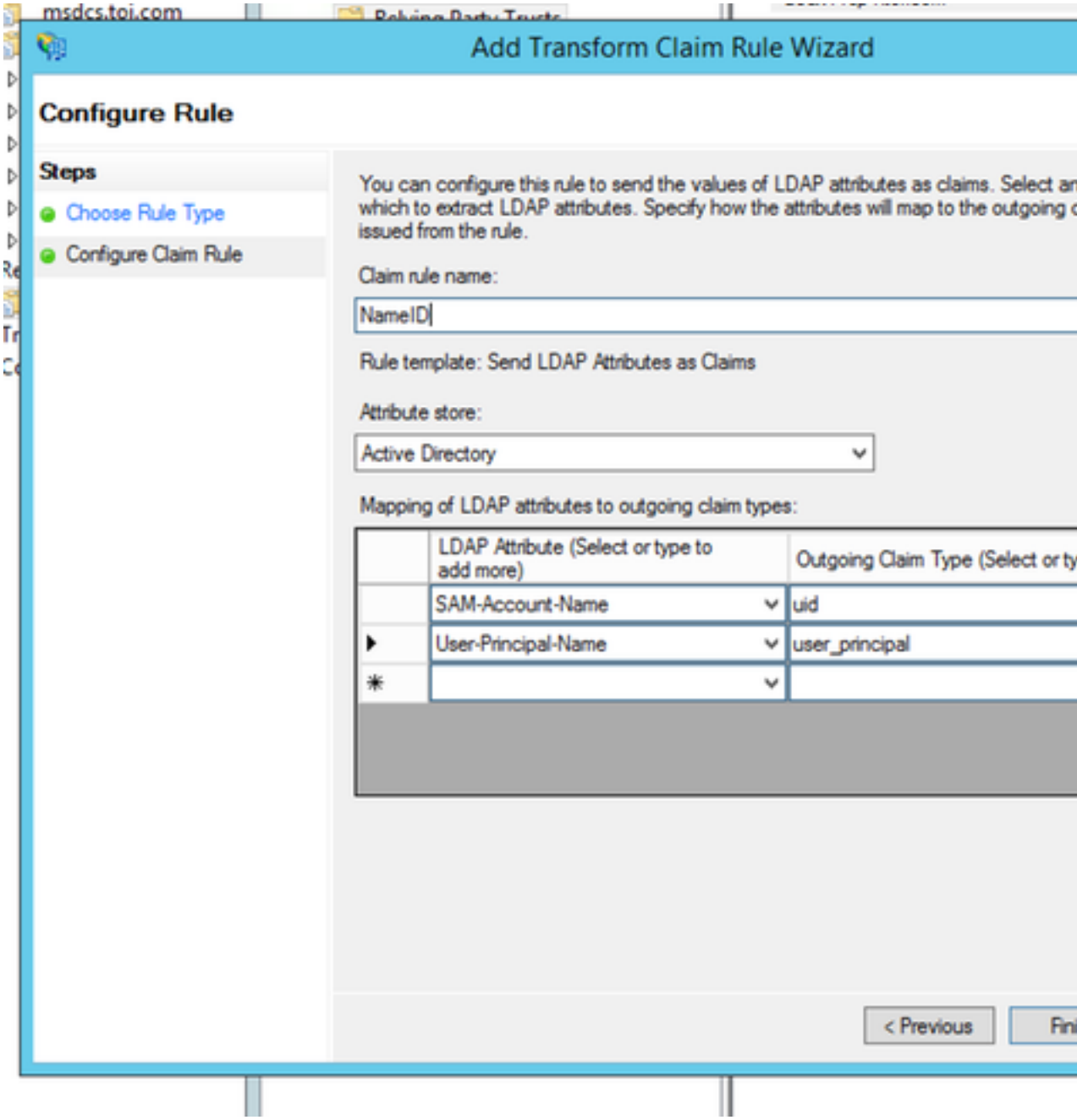
Bajo reglas de la demanda AD FS, asegúrese de que los atributos que asocian para “user
estén definidos como en la guía de configuración de IdP (que dirijan?).

Acción Recomendada

1. RDP al sistema AD FS.
2. Edite las reglas de la demanda para la confianza de confianza del partido.



3. Verifique que el user_principal y el uid estén asociados correctamente



5. La regla saliente de la demanda no se configura correctamente en un AD federado FS

Resumen de problemas	El pedido de registro falla con 500 que el error en el navegador con el mensaje “no podría Identificación de usuario de la respuesta de SAML. o no podía extraer el principal del usua respuesta de SAML.” cuando el AD FS es un AD federado FS.
Paso del error	SAML proceso de la respuesta

Mensaje de error	**Navegador**
	error 500 con este mensaje:
	Error de configuración de IdP: SAML proceso fallado
	No podía extraer la Identificación de usuario de la respuesta de SAML. /No podía extraer usuario de la respuesta de SAML.
	Visor de eventos AD FS:
	Ningún error
	Registro del Cisco IDS:
	`ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAML proceso de la respuesta fal`
	`excepción com.sun.identity.saml.common.SAMLException: No podía extraer la Identificación`
	`la respuesta de SAML. en`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.validateSAMLAttributes(IdSSAMLAsyncServl`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processSamlPostResponse(IdSSAMLAsyncServ`

en
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncSe

Posible Causa En un AD federado FS hay más configuraciones requirió que podrían faltar.

Acción Recomendada Marque si la configuración AD FS en el AD federado se hace según la sección **para una c del Multi-dominio para AD federado FS** en el Cisco IDS de la configuración y AD FS

6. Reglas de encargo de la demanda no configuradas correctamente

Resumen de problemas El pedido de registro falla con 500 que el error en el navegador con el mensaje “no podría Identificación de usuario de la respuesta de SAML. /Could no extraer el principal del usua SAML.”
uid y/o user_principal no fijados en las demandas salientes.

Paso del error SAML proceso de la respuesta
Navegador
error 500 con este mensaje:
SAML aserción fallada de IdP con el código de estado: urna: oasis: nombres: tc: **SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy**. Ve y el intento de IdP otra vez.

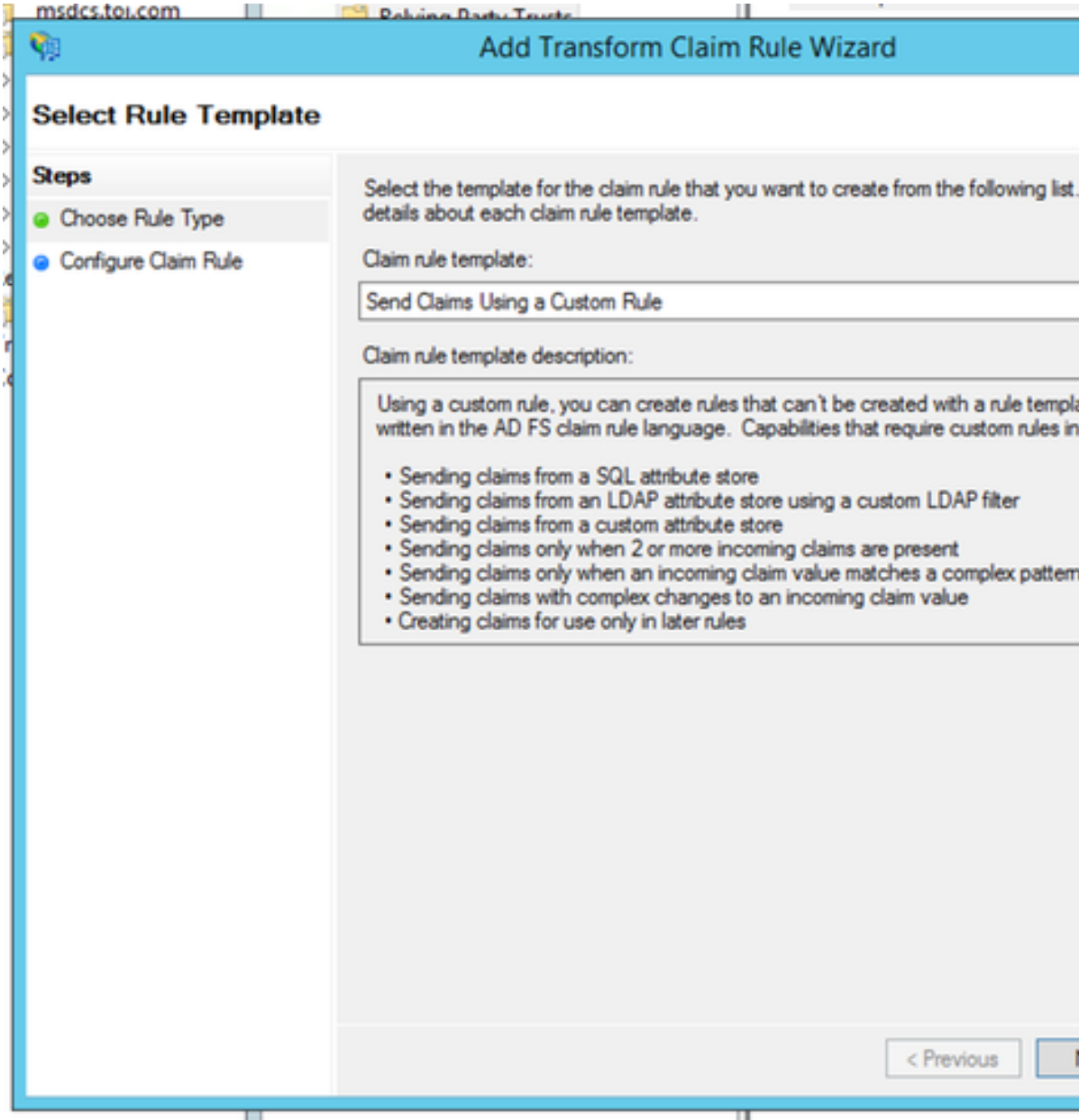
Mensaje de error
Visor de eventos AD FS:
El pedido de autenticación de SAML tenía una directiva de NameID que no podría ser sat
Solicitante: myids.cisco.com
Formato del identificador del nombre: urn:oasis:names:tc:SAML:2.0:nameid-format:transie
SPNameQualifier: myids.cisco.com
Detalles de la excepción:
MSIS1000: La petición de SAML contuvo un NameIDPolicy que no fue satisfecho por el to NameIDPolicy pedido: AllowCreate: Formato verdadero: urn:oasis:names:tc:SAML:2.0:na SPNameQualifier: myids.cisco.com. Propiedades reales de NameID: falta de información.
Esta petición fallada.
Acción de usuario
Utilice la Administración AD FS 2.0 broche-en para configurar la configuración que emite e requerido del nombre.
Registro del Cisco IDS:

```
2016-08-30 la INFORMACIÓN com.cisco.ccbu.ids SAML2SPAdapter.java:76 de 09:45:30.471 IST(
SAML-82] - SSO falló con el código: 1. Estado de respuesta: <samlp: <samlp de Status>: <
estado Value="urn:oasis:names:tc:SAML:2.0:status:Requester">: Código de estado
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp: StatusCode> </s
</samlp: Status> para AuthnRequest: ERROR n/a com.cisco.ccbu.ids IdSSAMLAsyncServlet.jav
09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] - SAML proceso de la respuesta fallado co
com.sun.identity.saml2.common.SAML2Exception: Código de estado inválido en la respuesta.
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) en
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) en
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
```

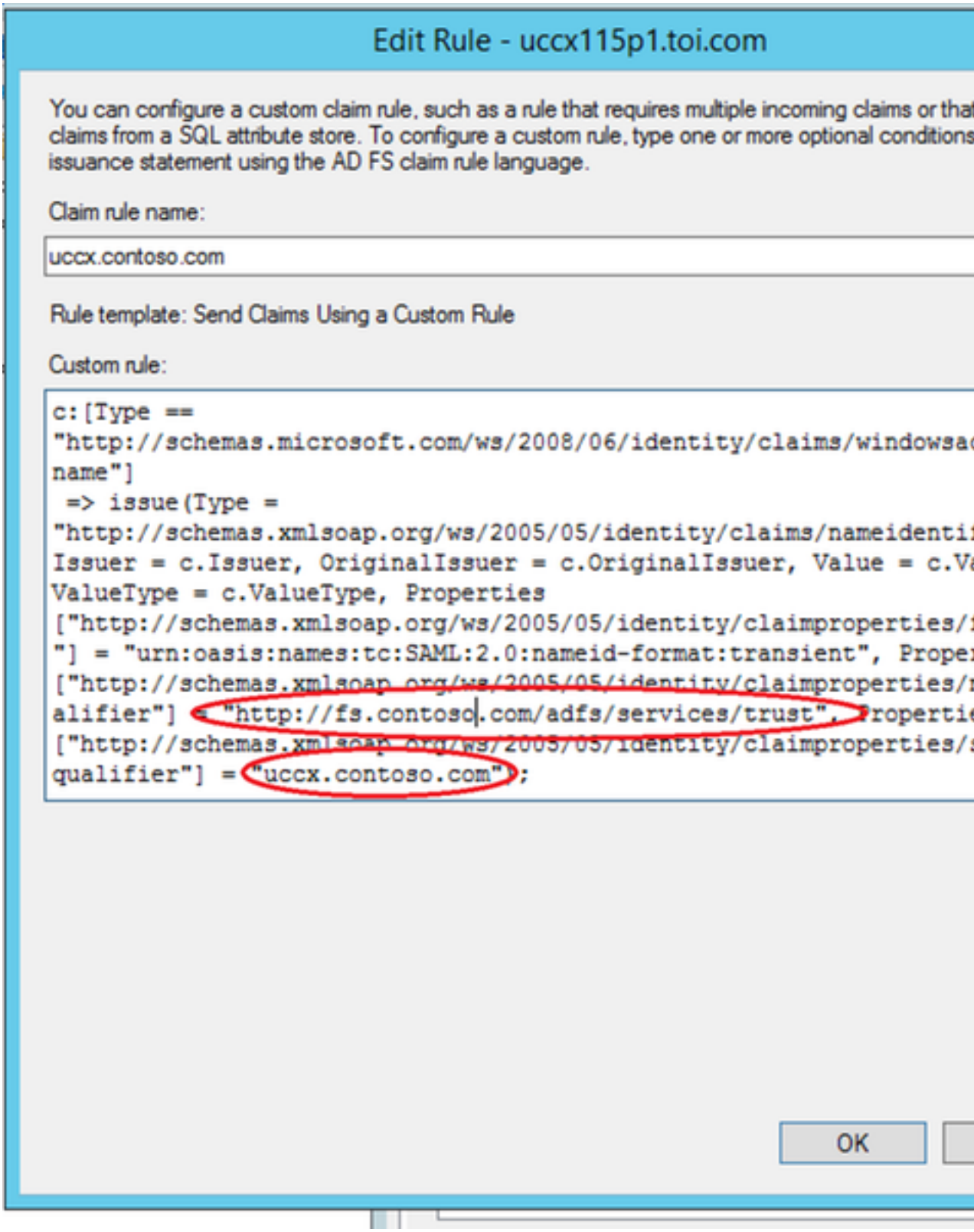
Posible Causa La regla de encargo de la demanda no se configura correctamente.
Bajo reglas de la demanda AD FS, asegúrese de que los atributos que asocian para “user estén definidos como en guía de configuración (que dirijan?).

1. RDP al sistema AD FS.
2. Edite las reglas de la demanda para las reglas de encargo de la demanda.

Acción Recomendada



3. Verifique que el AD FS y los nombres de dominio completamente calificado del Cisc



7. Demasiadas peticiones a AD FS.

Resumen de problemas	El pedido de registro falla con el error 500 en el navegador con el estatus code:urn:oasis:names:tc:SAML:2.0:status:Responder El mensaje de error en el View log del evento AD FS indica que hay demasiadas peticion
Paso del error	SAML proceso de la respuesta **Navegador**
Mensaje de error	error 500 con este mensaje: Error de configuración de IdP: SAML proceso fallado SAML aserción fallada de IdP con el código de estado: urn:oasis:names:tc:SAML:2.0:statu Verifique la configuración y el intento de IdP otra vez.

Visor de eventos AD FS:
Microsoft.IdentityServer.Web.InvalidRequestException:
MSIS7042: **La misma sesión del buscador del cliente ha hecho las peticiones del '6' en du**
segundos '16'. Entre en contacto a su administrador para los detalles.
en Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetection
en Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse
MSISSignInResponse)

```
Xml del evento: <Data >Microsoft.IdentityServer.Web.InvalidRequestException del <EventDa
http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> name= " el A
Guid="{20E25DDB-09E5-404B-8A56-EDAE2F12EE81}"/> <EventID>364</EventID> <Version>0</Versi
<Task>0</Task> <Opcode>0</Opcode> <Keywords>0x8000000000000001</Keywords> <TimeCreated e
19T12:14:58.474662600Z" el xmlns:auto-ns2=" <UserData> </System> UserID="S-1-5-21-168062
1502263146-1105"/> <Security <Computer>myadfs.cisco.com</Computer> 2.0/Admin</Channel> F
ThreadID="392" el ProcessID="2264" <Execution ActivityID="{98778DB0-869A-4DD5-B3B6-0565A
<Correlation <EventRecordID>29385</EventRecordID>/> http://schemas.microsoft.com/win/200
<Event el" del <Provider del <System> http://schemas.microsoft.com/win/2004/08/events/ev
<Event del ": MSIS7042: La misma sesión del buscador del cliente ha hecho las peticiones
segundos del último '16'. Entre en contacto a su administrador para los detalles. en
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCookie()
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse (respues
MSISSignInResponse </Data> </EventData> </Event> </UserData> </Event>
```

Registro del Cisco IDS

```
2016-04-15 ERROR predeterminado [IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102
0400) - excepción que procesa la petición com.sun.identity.saml2.common.SAML2Exception:
inválido en la respuesta. en com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAM
com.sun.identity.saml2.profile.SPACSUtils.processResponse(SPACSUtils.java:1050) en
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAML
```

Posible Causa Hay demasiadas peticiones que vienen a AD FS de la misma sesión del buscador.
Esto no debe suceder típicamente en la producción. Pero si usted encuentra esto, usted p

Acción Recomendada

1. Visor de eventos del control AD FS Windows.
2. Vuelva a inspeccionar los parámetros de confianza de confianza del partido. Para m
   Cisco IDS y AD FS de la configuración
3. Relogin.

8. El AD FS no se configura para firmar la aserción y el mensaje.

Resumen de problemas El pedido de registro falla con el error 500 en el navegador con el código de error: invalidS

Paso del error SAML proceso de la respuesta

Mensaje de error

Navegador
error 500 con este mensaje:
Código de error: invalidSignature
Mensaje: Firma no válida en ArtifactResponse.

Registro del Cisco IDS:

```
2016-08-24 INFORMACIÓN saml2error.jsp saml2error_jsp.java:75 de 10:53:10.494 IST(+0530)
- SAML proceso de la respuesta fallado con el código: invalidSignature; mensaje: Firma n
ArtifactResponse. 2016-08-24 ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 de 10
[IdSEndPoints-SAML-241] - SAML proceso de la respuesta fallado con la excepción
com.sun.identity.saml2.common.SAML2Exception: Firma no válida en la respuesta. en
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994) en
com.sun.identity.saml2.profile.SPACSUtils.getResponse(SPACSUtils.java:196) en
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2028)
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAML
```

Posible Causa El AD FS no se configura para firmar la aserción y el mensaje.

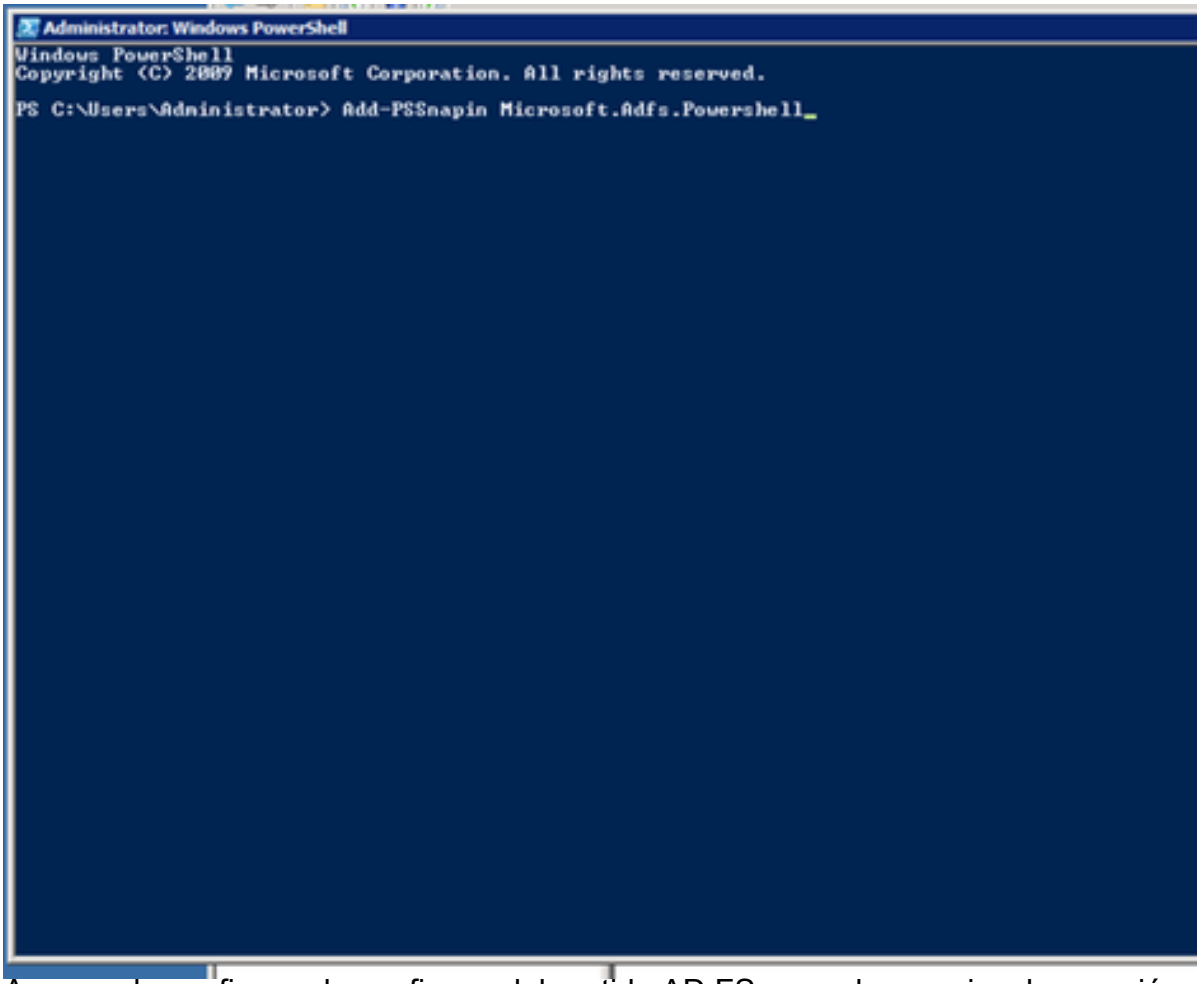
Acción

1. Funcione con el comando del powershell AD FS: **Conjunto-ADFSRelyingPartyTrust -**

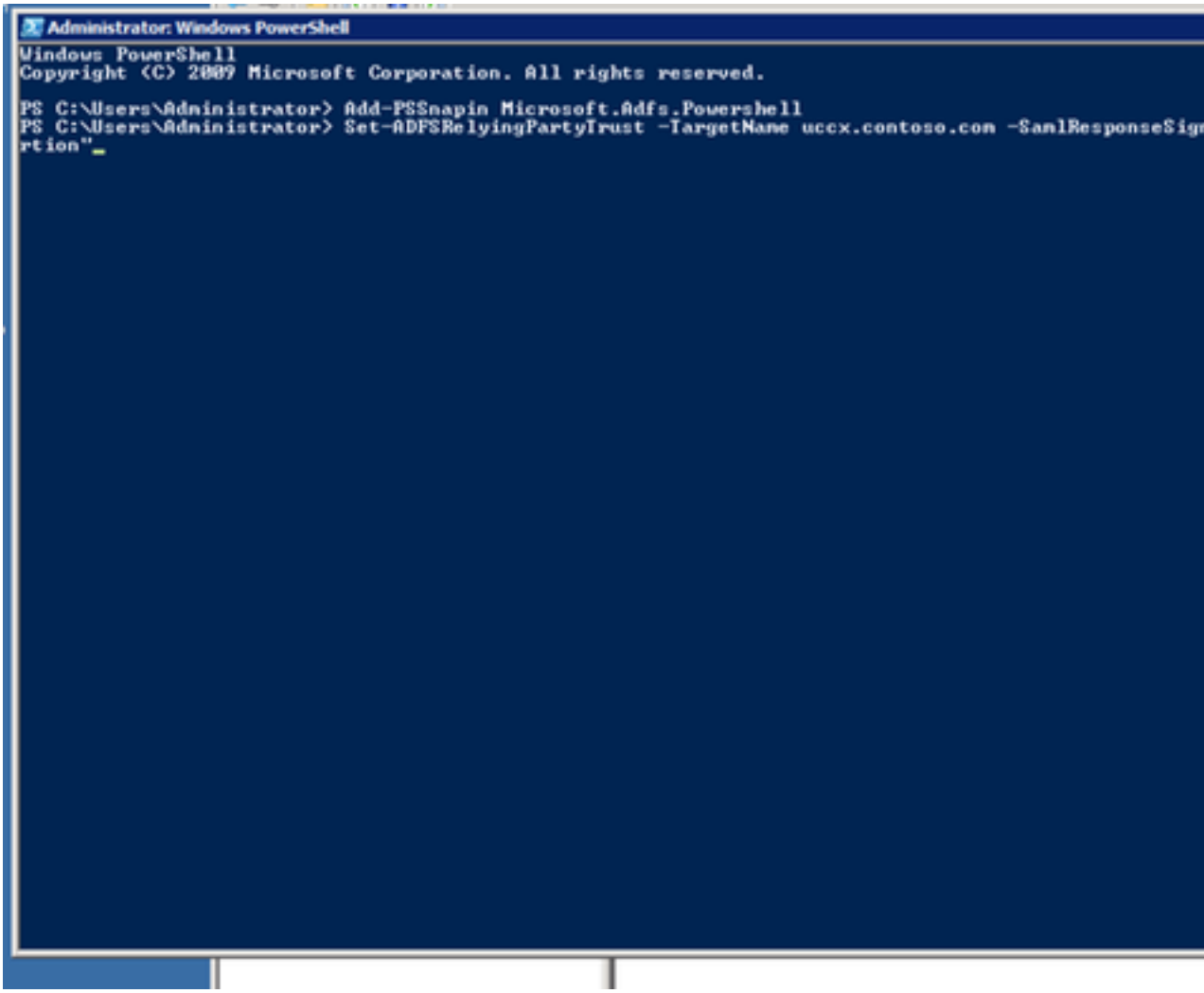
Identifier> del partido de TargetName - SamlResponseSignature “MessageAndAsse

2. RDP al sistema AD.
3. Abra **Powershell**.
4. Agregue Windows PowerShell broche-INS a la sesión en curso. Este paso no puede si usted está utilizando el 3.0 ADFS puesto que el CmdLet está instalado ya como pa papeles y las características.

Recomendada



5. Agregue la confianza de confianza del partido AD FS para el mensaje y la aserción.



Información Relacionada

Esto se relaciona con la configuración del proveedor de la identidad descrita en el artículo:

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- Soporte Técnico y Documentación - Cisco Systems