

Troubleshooting e problemas comuns ADFS/IdS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Aplicativos e logs que podem ser acessíveis na eliminação de erros](#)

[Diagrama de fluxo com opções de debugging](#)

[Pedido de Authcode que processa pelo Cisco IDS](#)

[Erros comuns encontrados durante este processo](#)

1. [Registro do cliente não feito](#)
2. [Aplicativo de acessos de usuário usando o endereço IP de Um ou Mais Servidores Cisco ICM NT/nome de host da substituição](#)

[Iniciação do pedido de SAML pelo Cisco IDS](#)

[Erros comuns encontrados durante este processo](#)

1. [Metadata AD FS não adicionados ao Cisco IDS](#)

[Pedido de SAML que processa por AD FS](#)

[Erros comuns encontrados durante este processo](#)

1. [AD FS que não tem o certificado de SAML dos idS os mais atrasados de Cisco.](#)

[Resposta de SAML que envia por AD FS](#)

[Erros comuns encontrados durante este processo](#)

1. [A autenticação do formulário não é permitida em AD FS.](#)

[Resposta de SAML que processa pelo Cisco IDS](#)

[Erros comuns encontrados durante este processo](#)

1. [O certificado AD FS no Cisco IDS não está o mais atrasado.](#)
2. [O Cisco IDS e os pulsos de disparo AD FS não são sincronizados.](#)
3. [Algoritmo errado da assinatura \(SHA256 contra o SHA1\) em AD FS](#)
4. [Regra que parte da reivindicação não configurada corretamente](#)
5. [A regra que parte da reivindicação não é configurada corretamente em um AD federado FS](#)
6. [Regras feitas sob encomenda da reivindicação não configuradas corretamente](#)
7. [Pedidos demais a AD FS.](#)
8. [O AD FS não é configurado para assinar a afirmação e a mensagem.](#)

[Informações Relacionadas](#)

Introdução

A interação do linguagem de marcação da afirmação da Segurança (SAML) entre o serviço da identidade de Cisco (IdS) e os serviços da federação do diretório ativo (AD FS) através de um navegador é o núcleo do Único-sinal no fluxo do início de uma sessão (SSO). Este original ajudá-lo-á nas edições da eliminação de erros relativas às configurações no Cisco IDS e no AD FS, junto com a ação recomendada resolvê-los.

Modelos de distribuição do Cisco IDS

Produto Desenvolvimento

UCCX Co-residente

PCCE Co-residente com CUIIC (centro unificado Cisco da inteligência) e LD (dados vivos)

UCCE Co-residente com CUIIC e LD para as disposições 2k.

Autônomo para as disposições 4k e 12k.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Liberação 11.5 do Cisco Unified Contact Center Express (UCCX) ou liberação 11.5 do Cisco Unified Contact Center Enterprise ou liberação empacotada 11.5 da empresa do centro de contato (PCCE) como aplicáveis.
- Microsoft active directory - AD instalado em Windows Server
- IdP (fornecedor da identidade) - Versão 2.0/3.0 do serviço da federação do diretório ativo (AD FS)

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Depois que a relação de confiança está estabelecida entre o Cisco IDS e o AD FS (veja [aqui](#) para detalhes, comum para UCCX e UCCE), o administrador está esperado executar o teste SSO estabelecido na página dos ajustes do Gerenciamento do serviço da identidade para assegurar-se de que a configuração entre o Cisco IDS e o AD FS trabalhe muito bem. Se o teste falha, use os aplicativos apropriados e as sugestões dados neste guia para resolver a edição.

Aplicativos e logs que podem ser acessíveis na eliminação de erros

Aplicativo/log Detalhes

Log do Cisco IDS O registador do Cisco IDS registrará todo o erro que aconteça no Cisco IDS.

Onde encontrar a ferramenta

Use RTMT para obter logs do Cisco IDS. Para obter informações sobre de como usar RTMT veja, [guie para usar RTMT](#)
Note por favor que o nome RTMT é **serviço da identidade de Cisco**. A fim encontrar os logs, navegue ao **serviço > ao log da identidade de**

| | | |
|----------------------------------|---|---|
| Logs de Fedlet | Os logs de Fedlet dão mais detalhes sobre todos os erros de SAML que acontece no Cisco IDS | Cisco Use RTMT para obter logs de Fedlet. O lugar para o log de Fedlet é mesmo que os logs do Cisco IDS. Os logs do fedlet começam com o fedlet- do prefixo Use RTMT para obter o medidor API. |
| Medidor do Cisco IDS API | O medidor API pode ser usado para olhar em e validar todos os erros que o Cisco IDS API puder ter retornado e número de pedidos que são processados pelo Cisco IDS | Note por favor que o nome RTMT é serviço da identidade de Cisco Isto aparecerá sob um medidor separado do dobrador. Note por favor que saml_metrics.csv e authorize_metrics.csv são o medidor relevante para este original. Na máquina AD FS, navegue aos >Applications do visualizador de eventos e preste serviços de manutenção ao >AdDFS 2.0 dos logs > Admin Em Windows 2008, no visualizador de eventos do lançamento do Control Panel > do desempenho e na manutenção > nas ferramentas administrativas Em Windows 2012, lance-o do Control Panel \ sistema e da Segurança \ ferramentas administrativas. |
| Visualizador de eventos em AD FS | Permite que os usuários ver o evento entra o sistema. Algum erro em AD FS quando processar o pedido de SAML/enviar a resposta de SAML será registrado aqui. | Olhe por favor sua documentação dos indicadores para ver onde encontrar o visualizador de eventos. Estes são alguns visores sugeridos de SAML que você pode usar para olhar o pedido e a resposta de SAML |
| Visor de SAML | Um visor de SAML ajudará em olhar o pedido e a resposta de SAML que são enviados desde/até o Cisco IDS. Este aplicativo de navegador é muito útil para a análise do pedido/resposta de SAML. | <ol style="list-style-type: none"> 1. Violinista Como usar o violinista com AD FSViolinista Chrome de encaixe 2. Projétil luminoso de SAML - Firefox 3. Painel de SAML Chrome |

Diagrama de fluxo com opções de debugging

As várias etapas para a autenticação SSO são mostradas na imagem junto com e nos produtos manufaturados da eliminação de erros em cada etapa em caso de uma falha nessa etapa.

Esta tabela dá os detalhes em como identificar falhas em cada etapa do SSO no navegador. As ferramentas diferentes e como possa ajudam na eliminação de erros são especificados também.

| Etapa | Como identificar a falha no navegador | Ferramentas/log | Configurações a olhar |
|--|---|--|-------------------------------------|
| Pedido de AuthCode que processa pelo Cisco IDS | Em caso da falha, o navegador não é reorientado ao valor-limite de SAML ou ao AD FS, um erro JSON é mostrado pelo Cisco IDS, que indique que a identificação de cliente ou reorienta a URL seja inválido. | Os registros do Cisco IDS indicam os erros que ocorrem quando o pedido do authcode for validado e processado. Medidor do Cisco IDS API - Indica o número de pedidos processados e falhados. | Registro do cliente |
| Iniciação do pedido | Durante a falha, o navegador não é reorientado a AD FS, e | Os registros do Cisco IDS indicam se há uma exceção ou | Cisco IDS no estado NOT_CONFIGURED. |

de SAML pelo Cisco IDS

uma página/mensagem do erro será mostrada pelo Cisco IDS.

Pedido de SAML que processa por AD FS

Toda a falha processar este pedido conduzirá a uma página do erro que está sendo indicada pelo server AD FS em vez da página de login.

Enviando a resposta de SAML por AD FS

Toda a falha enviar a resposta conduz a uma página do erro que está sendo indicada pelo server AD FS depois que as credenciais válidas são submetidas.

Resposta de SAML que processa pelo Cisco IDS

O Cisco IDS mostrará um erro 500 com o motivo de erro e uma página da verificação rápida.

não quando o pedido for iniciado.

Medidor do Cisco IDS API - Indica o número de pedidos processados e falhados.

O visualizador de eventos em AD FS indica os erros que ocorrem quando o pedido for processado.

Navegador de SAML de encaixe - Ajudas para ver o pedido de SAML que é enviado ao AD FS.

Visualizador de eventos em AD FS - Indica os erros que ocorrem quando o pedido for processado.

Visualizador de eventos em AD FS - Indica o erro se o AD FS envia uma resposta de SAML sem um código de status bem sucedido.

Navegador de SAML de encaixe - Ajudas para ver a resposta de SAML enviada por AD FS para identificar o que é errado.

Log do Cisco IDS - Indica que o erro/exceção ocorreu durante o processamento.

Medidor do Cisco IDS API - Indica o número de pedidos processados e falhados.

Configuração de confiança da confiança do partido em IdP

- Configuração de confiança da confiança do partido em IdP
- Forme o ajuste da autenticação em AD FS.

- A reivindicação ordena a configuração
- Assinatura da mensagem e da afirmação

Pedido de Authcode que processa pelo Cisco IDS

O ponto de início do início de uma sessão SSO, tanto quanto o Cisco IDS, é o pedido para um código de autorização de um aplicativo permitido SSO. A validação do pedido API está feita para verificar se é um pedido de um cliente registrado. Uma validação bem sucedida conduz ao navegador que está sendo reorientado ao valor-limite de SAML do Cisco IDS. Toda a falha na validação do pedido conduz a um erro page/JSON (notação do objeto do Javascript) que está sendo enviado para trás do Cisco IDS.

Erros comuns encontrados durante este processo

1. Registro do cliente não feito

Resumo de problema

A solicitação de login falha com erro 401 no navegador.

Navegador:

erro 401 com esta mensagem: {"erro": "invalid_client", "error_description": "ClientId inválido"}

Log do Cisco IDS:

```
2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] ADVERTEM com.cisco.ccbu.ids IdSConfi
identificação de cliente: fb308a80050b2021f974f48a72ef9518a5e7ca69 não existe o ERRO com.
IdSOAuthEndPoint.java:45 de 2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51] - exceçã
solicitação de autorização. org.apache.oltu.oauth2.common.exception.OAuthProblemException
invalid_client, inválido. em
org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemException
com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthorize
com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequiredParameters(IdSAut
em org.apache.oltu.oauth2.as.request.OAuthRequest.validate(OAuthRequest.java:63)
```

Mensagem de erro

Possível causa

O registro do cliente com Cisco IDS não está completo.

Ação

Navegue ao console de gerenciamento do Cisco IDS e confirme se o cliente é registrado o

recomendada registrar então os clientes antes de continuar com SSO.

2. Aplicativo de acessos de usuário usando o endereço IP de Um ou Mais Servidores Cisco ICM NT/nome de host da substituição

Resumo de problema

A solicitação de login falha com erro 401 no navegador.

Mensagem de erro

Navegador:

erro 401 com esta mensagem: {"erro": "invalid_redirectUri", "error_description": "Invalid reorienta Uri"}

Aplicativo de acessos de usuário usando o endereço IP de Um ou Mais Servidores Cisco ICM NT/nome de host da substituição.

Possível causa

No modo SSO, se o aplicativo é alcançado usando o IP, não trabalha. Os aplicativos devem ser alcançados pelo hostname por que são registrados no Cisco IDS. Esta edição pode acontecer se o usuário alcançou um nome de host alternativo que não seja registrado com Cisco IDS.

Ação

Navegue ao console de gerenciamento do Cisco IDS e confirme se o cliente está registrado com o correto reorienta URLand que o mesmo está usado para alcançar o aplicativo.

recomendada

Iniciação do pedido de SAML pelo Cisco IDS

O valor-limite de SAML do Cisco IDS é o ponto de início do fluxo de SAML no início de uma sessão baseado SSO. A iniciação da interação entre o Cisco IDS e o AD FS é provocada nesta etapa. A condição prévia aqui é que o Cisco IDS deve conhecer o AD FS para conectar a enquanto os metadata correspondentes de IdP devem ser transferidos arquivos pela rede ao Cisco IDS para que esta etapa suceda.

Erros comuns encontrados durante este processo

1. Metadata AD FS não adicionados ao Cisco IDS

Resumo de problema

A solicitação de login falha com erro 503 no navegador.

Mensagem de erro

Navegador:

erro 503 com esta mensagem: {"erro": "service_unavailable", "error_description": "De "os Metadata SAML não são inicializados"}

Possível causa

Os Metadata de Idp não estão disponíveis no Cisco IDS. O estabelecimento de confiança o Cisco IDS e o AD FS não está completo.

Ação

Navegue ao console de gerenciamento do Cisco IDS e veja se os IdS estão no **not config state**.

recomendada

Confirme se os metadata de IdP são transferidos arquivos pela rede ou não.
Se não, transfira arquivos pela rede os metadata de IdP transferidos de AD FS.
Veja para mais detalhes [aqui](#).

Pedido de SAML que processa por AD FS

O processamento do pedido de SAML é a primeira etapa no AD FS no fluxo SSO. O pedido de SAML enviado pelo Cisco IDS é lido, validado e decifrado por AD FS nesta etapa. O processamento bem sucedido deste pedido conduz a duas encenações:

1. Se é um início de uma sessão fresco em um navegador, o AD FS mostra o formulário do início de uma sessão. Se é um relogin já de um usuário autenticado de uma sessão de navegador existente, o AD FS tenta enviar diretamente a parte traseira da resposta de SAML.

Note: A condição prévia principal para esta etapa é para o AD FS ter a confiança de resposta do partido configurada.

Erros comuns encontrados durante este processo

1. AD FS que não tem o certificado de SAML dos idS os mais atrasados de Cisco.

| | |
|---------------------------|--|
| Resumo de problema | <p>O AD FS que não mostra a página de login, em lugar de mostra uma página do erro.</p> <p>Navegador O AD FS mostra uma página do erro similar a esta: Havia um problema que alcança o local. Tente consultar outra vez ao local. Se o problema persiste, contacte o administrador deste local e forneça o número de referência para identificar o problema. Número de referência: 1ee602be-382c-4c49-af7a-5b70f3a7bd8e</p> <p>Visualizador de eventos AD FS</p> |
| Mensagem de erro | <p>O serviço da federação encontrou um erro ao processar o pedido de autenticação de SAML</p> <p>Dados adicionais Detalhes da exceção: Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException: MSIS0038: A mensagem de SAML tem a assinatura errada. Expedidor: "myuccx.cisco.com". em Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage (mensagem de MSISSamlBindingMessage) em Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage (CreateErrorMessageRequest o mais createErrorMessageRequest) em Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest (requestMessage da mensagem)</p> |
| Possível causa | <p>A confiança de confiança do partido não é estabelecida ou o certificado do Cisco IDS mudou mas o mesmo não é transferido arquivos pela rede ao AD FS. Estabeleça a confiança entre AD FS e Cisco IDS com o certificado o mais atrasado do Cisco IDS.</p> |
| Ação recomendada | <p>Assegure-se de por favor que o certificado do Cisco IDS não esteja expirado. Você pode ver o painel do estado na identidade de Cisco prestar serviços de manutenção ao Gerenciamento de Identidade. Em caso afirmativo, regenere o certificado na página dos ajustes. Para mais detalhes em como estabelecer metadata confie através de ADFS & de Cisco IDS veem, aqui</p> |

Resposta de SAML que envia por AD FS

O ADFS envia a resposta de SAML de volta ao Cisco IDS através do navegador depois que o usuário é autenticado com sucesso. ADFS pode enviar uma resposta de SAML para trás com um código de status que indique o sucesso ou a falha. Se a autenticação do formulário não é permitida em AD FS então esta indicará uma resposta da falha.

Erros comuns encontrados durante este processo

1. A autenticação do formulário não é permitida em AD FS

| | |
|---------------------------|---|
| Resumo de problema | O navegador mostra o início de uma sessão NTLM, e falha então sem com sucesso reorientar ao Cisco IDS. |
| Etapa da falha | Enviando a resposta de SAML |
| Mensagem de erro | Navegador: O navegador mostra o início de uma sessão NTLM, mas após o login bem-sucedido, falha com muitos reorienta. |
| Possível causa | O Cisco IDS apoia somente a autenticação baseada formulário, autenticação do formulário não é permitido em AD FS. |
| Ação recomendada | Para mais detalhes em como permitir a autenticação do formulário veja: Ajuste da autenticação do formulário ADFS 2.0 Ajuste da autenticação do formulário do 3.0 ADFS |

Resposta de SAML que processa pelo Cisco IDS

Nesta fase, o Cisco IDS obtém uma resposta de SAML de AD FS. Esta resposta poderia conter um código de status que indicasse o sucesso ou a falha. Uma resposta de erro de AD FS resulta em uma página do erro e o mesmo tem que ser debugado.

Durante uma resposta bem sucedida de SAML, o processamento do pedido pode falhar por estas razões:

- Metadata incorretos de IdP (AD FS).
- A falha recuperar esperou reivindicações que parte de AD FS.
- O Cisco IDS e os pulsos de disparo AD FS não são sincronizados.

Erros comuns encontrados durante este processo

1. O certificado AD FS no Cisco IDS não está o mais atrasado.

| | |
|---------------------------|---|
| Resumo de problema | A solicitação de login falha com erro 500 no navegador com código de erro como o invalidSignature |
| Etapa da falha | Processamento da resposta de SAML |
| Mensagem de erro | Navegador: erro 500 com esta mensagem no navegador: Código de erro: invalidSignature Mensagem: O certificado de assinatura não combina o que é definido nos metadata da entidade. Visualizador de eventos AD FS: Nenhum erro Log do Cisco IDS: 2016-04-13 ERRO [IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 do padrão de 12: IST(+0530) - exceção que processa o pedido com.sun.identity.saml2.common.SAML2Exception: certificado de assinatura não combina o que é definido nos metadata da entidade. em |


```
com.sun.identity.saml2.xmlsig.FMSigProvider.verify(FMSigProvider.java:331) em
com.sun.identity.saml2.protocol.impl.StatusResponseImpl.isSignatureValid(StatusResponseImpl
em com.sun.identity.saml2.profile.SPACSUtills.getResponseFromPost(SPACSUtills.java:985) em
com.sun.identity.saml2.profile.SPACSUtills.getResponse(SPACSUtills.java:196)
```

**Possível
causa**

O processamento da resposta de SAML falhado como o certificado de IdP é diferente do q disponível no Cisco IDS.

Transfira os metadata os mais atrasados AD FS de: <https://<ADFSServer>/federationmeta06/federationmetadata.xml>

**Ação
recomendada**

E transfira-o arquivos pela rede ao Cisco IDS através da interface do utilizador de Managa serviço da identidade.

Para detalhes, veja [para configurar o Cisco IDS e o AD FS](#)

2. O Cisco IDS e os pulsos de disparo AD FS não são sincronizados.

**Resumo de
problema
Etapa da
falha**

A solicitação de login falha com erro 500 no navegador com o código de status: urn:oasis:names:tc:SAML:2.0:status:Success

Processamento da resposta de SAML

Navegador:

erro 500 com esta mensagem:

Erro de configuração de IdP: Processamento de SAML falhado

Afirmação de SAML falhada de IdP com código de status: urn:oasis:names:tc:SAML:2.0:st

Verifique a configuração de IdP e tente-a outra vez.

Log do Cisco IDS

```
2016-08-24 o ERRO com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:298 de 18:46:56.780 IST(+05
SAML-22] - processamento da resposta de SAML falhou com exceção com.sun.identity.saml2.co
O tempo em SubjectConfirmationData é inválido. em
```

```
com.sun.identity.saml2.common.SAML2Utils.isBearerSubjectConfirmation(SAML2Utils.java:766)
```

```
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:609) em
```

```
com.sun.identity.saml2.profile.SPACSUtills.processResponse(SPACSUtills.java:1050) em
```

```
com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2038)
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getMapFromSAMLResponse(IdSSAMLA
```

```
em com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncSe
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncSer
```

```
com.cisco.ccbu.ids.auth.api.IdSEndPoint$1.run(IdSEndPoint.java:269) em
```

```
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145) em
```

```
java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:615) em
```

```
java.lang.Thread.run(Thread.java:745)2016-08-24 18:24:20.510 IST(+0530) [pool-4-thread-1]
```

Visor de SAML:

Procure os campos de NotBefore e de NotOnOrAfter

<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.325Z">

**Possível
causa**

O tempo no sistema do Cisco IDS e do IdP é fora da sincronização.

**Ação
recomendada**

Sincronize o tempo no Cisco IDS e no sistema AD FS. Recomenda-se que o sistema e o C tempo sincronizado usando o servidor de NTP.

3. Algoritmo errado da assinatura (SHA256 contra o SHA1) em AD FS

**Resumo de
problema**

A solicitação de login falha com erro 500 no navegador com estado

code:urn:oasis:names:tc:SAML:2.0:status:Responder

Mensagem de Erro no View Log do evento AD FS – Assinatura errada Algorithm(SHA256 AD FS

**Etapa da
falha**

Processamento da resposta de SAML

**Mensagem
de erro**

Navegador

erro 500 com esta mensagem:

Erro de configuração de IdP: Processamento de SAML falhado

Afirmção de SAML falhada de IdP com código de status: urn:oasis:names:tc:SAML:2.0:st
Verifique a configuração de IdP e tente-a outra vez.

Visualizador de eventos AD FS:

O pedido de SAML não é assinado com algoritmo previsto da assinatura. O pedido de SAM
algoritmo <http://www.w3.org/2001/04/xmldsig-more#rsa-sha256> da assinatura.

O algoritmo previsto da assinatura é [rsa-sha1](#)

Log do Cisco IDS:

```
ERRO com.cisco.ccbu.ids.IdSSAMLSyncServlet.java:298 - Processamento da resposta de SAML  
com.sun.identity.saml2.common.SAML2Exception: Código de status inválido na resposta. em  
com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) em  
com.sun.identity.saml2.profile.SPACSUtills.processResponse(SPACSUtills.java:1050) em  
com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2038)  
com.cisco.ccbu.ids.auth.api.IdSSAMLSyncServlet.getMapFromSAMLResponse(IdSSAMLA
```

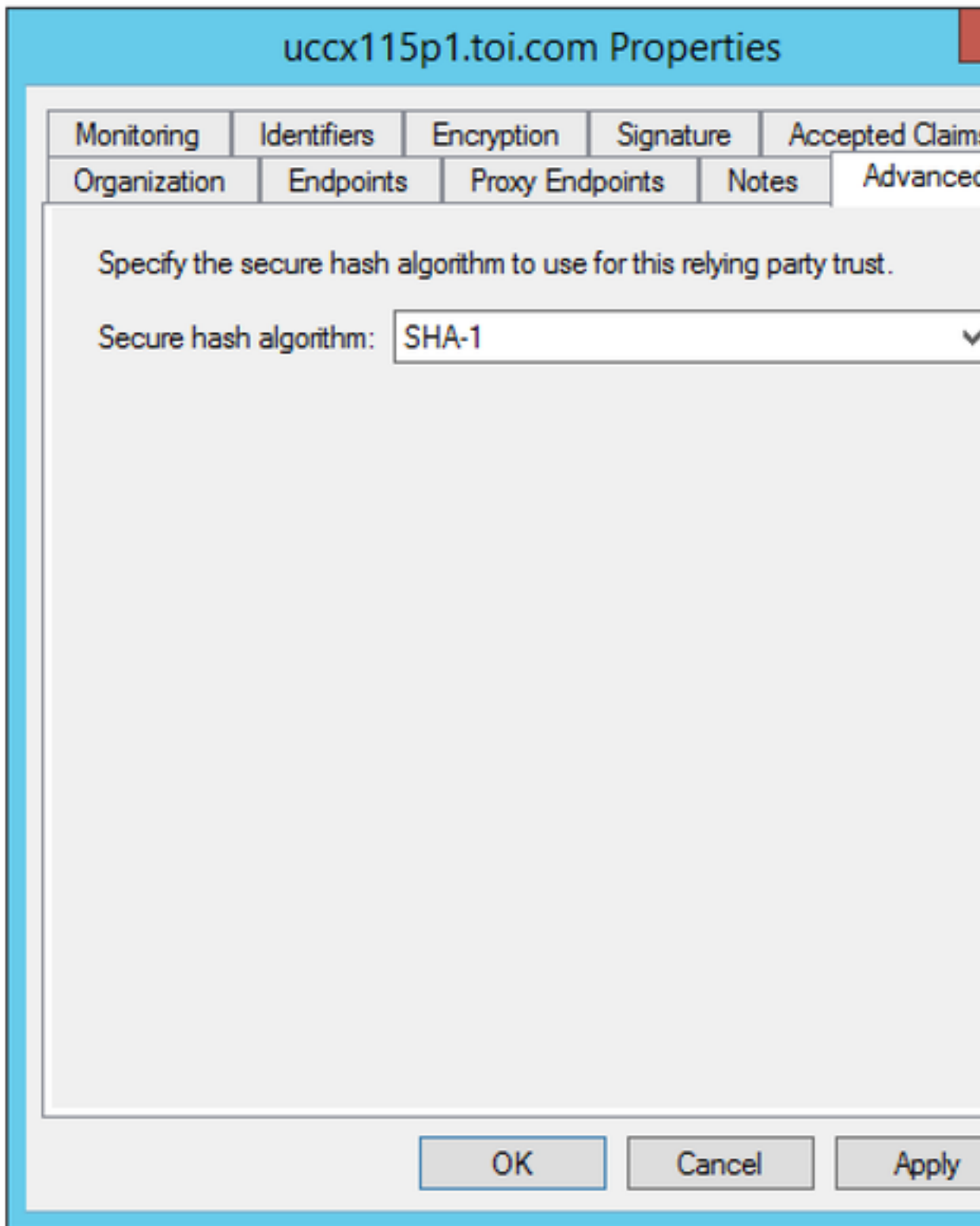
**Possível
causa**

O AD FS é configurado para usar o SHA-256.

Atualize AD FS para usar o SHA-1 para a assinatura e a criptografia.

1. RDP ao sistema AD FS.
2. Abra o console AD FS.
3. Selecione a **confiança de confiança do partido** e clique **propriedades**
4. Selecione a guia **Advanced**.
5. Selecione o SHA-1 da lista de drop-down.

**Ação
recomendada**



4. Regra que parte da reivindicação não configurada corretamente

| | |
|---------------------------|--|
| Resumo de problema | A solicitação de login falha com 500 que o erro no navegador com mensagem "não poderia identificar de usuário da resposta de SAML. /Could para não recuperar o principal do usuário SAML." |
| Etapa da falha | uid e/ou user_principal não ajustados nas reivindicações que parte. Processamento da resposta de SAML |
| Mensagem de erro | Navegador: erro 500 com esta mensagem: Erro de configuração de IdP: Processamento de SAML falhado. |

Não podia recuperar o identificador de usuário da resposta de SAML. /Could para não recuperar o usuário da resposta de SAML.

Visualizador de eventos AD FS:

Nenhum erro

Log do Cisco IDS:

```
ERRO com.cisco.ccbu.ids.IdSSAMLAyncServlet.java:294 - Processamento da resposta de SAML  
com.sun.identity.saml.common.SAMLException: Não podia recuperar o identificador de usuário  
em com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.validateSAMLAttributes(IdSSAMLAyncServlet  
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet  
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet
```

As reivindicações que parte imperativas (uid e user_principal) não são configuradas corretamente para a reivindicação.

Possível causa

Se você não configurou a regra da reivindicação de NameID ou o uid ou user_principal não está configurado corretamente.

Se a regra de NameID é não configurada ou user_principal não está traçado corretamente, o uid ou user_principal não é recuperado desde que esta é a propriedade que o Cisco IDS procura.

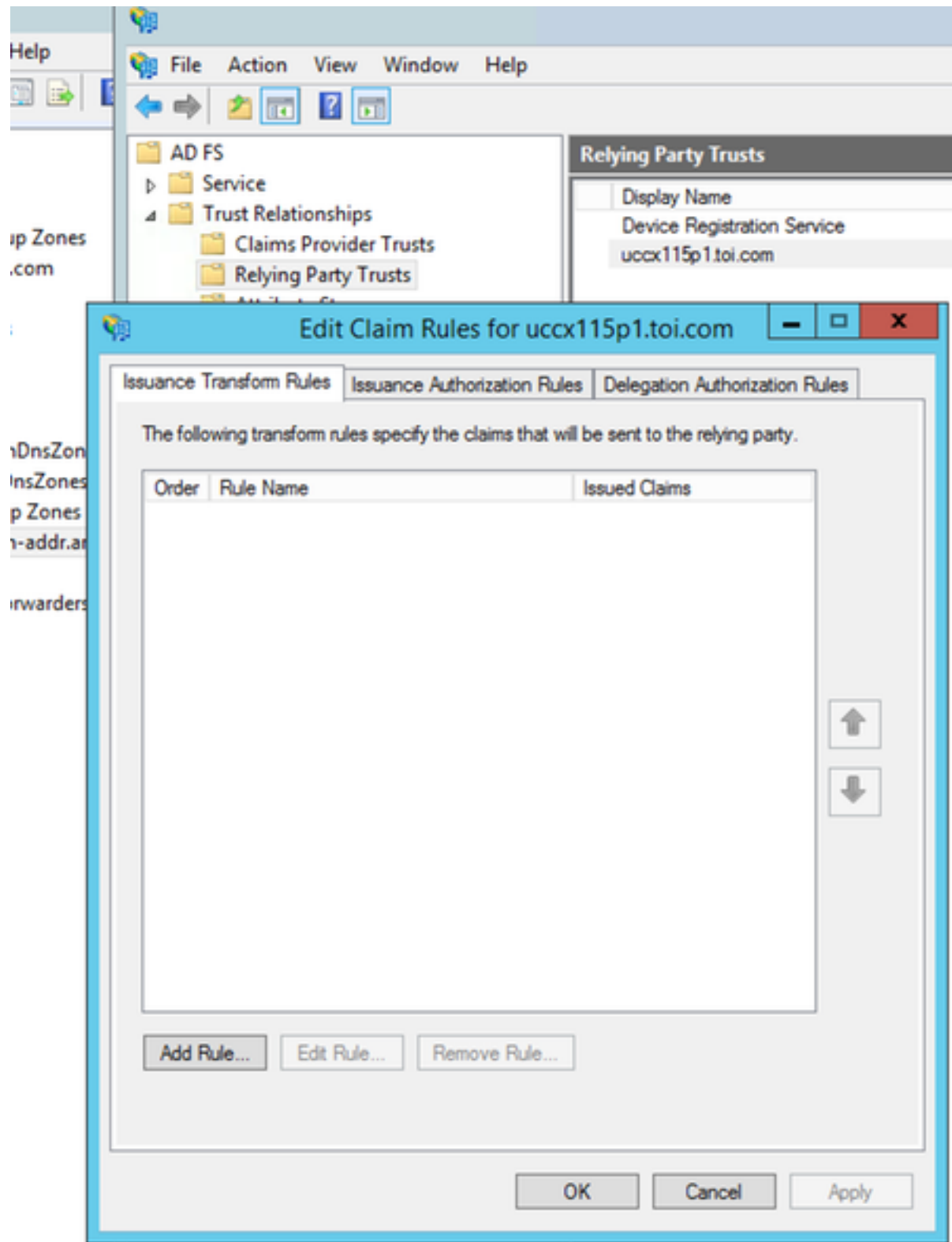
Se o uid não é traçado corretamente, o Cisco IDS indica que o uid não está recuperado.

Sob regras da reivindicação AD FS, assegure-se de que os atributos que traçam para "userPrincipalName" estejam definidos como no manual de configuração de IdP (que guiam?).

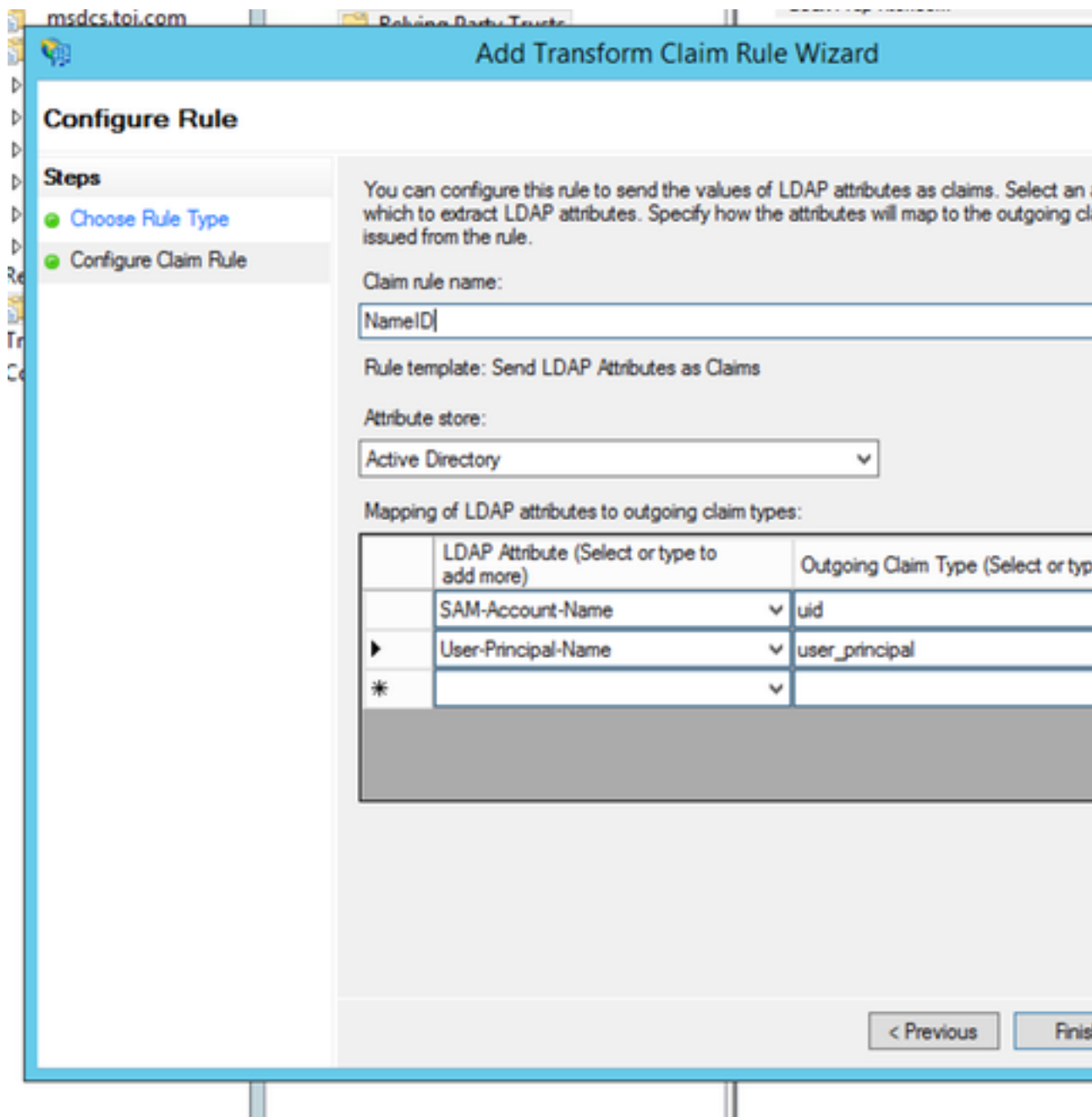
1. RDP ao sistema AD FS.

2. Edite as regras da reivindicação para a confiança de confiança do partido.

Ação recomendada



3. Verifique que o user_principal e o uid estão traçados corretamente



5. A regra que parte da reivindicação não é configurada corretamente em um AD federado FS

Resumo de problema

A solicitação de login falha com 500 que o erro no navegador com mensagem “não poderia recuperar o identificador de usuário da resposta de SAML. ou não podia recuperar o principal do usuário da resposta de SAML.” quando o AD FS for um AD federado FS.

Etapas da falha

Processamento da resposta de SAML

Navegador

erro 500 com esta mensagem:

Erro de configuração de IdP: Processamento de SAML falhado

Não podia recuperar o identificador de usuário da resposta de SAML. /Não podia recuperar o principal do usuário da resposta de SAML.

Mensagem de erro

Visualizador de eventos AD FS:

Nenhum erro

Log do Cisco IDS:

```
ERRO com.cisco.ccbu.ids IdSSAMLAyncServlet.java:294 - Processamento da resposta de SAML falhou com exceção com.sun.identity.saml.common.SAMLException: Não podia recuperar o identificador de usuário da resposta de SAML. em com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.validateSAMLAttributes(IdSSAMLAyncServlet)
```

```
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processSamlPostResponse(IdSSAMLAyncServlet)
em
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.processIdSEndPointRequest(IdSSAMLAyncServlet)
```

Possível causa

Em um AD federado FS há mais configurações exigiu que poderiam faltar.

Ação

Verifique se a configuração AD FS no AD federado é feita conforme a seção **para uma configuração recomendada Multi-domínio para AD federado FS** [configura](#) dentro o [Cisco IDS e o AD FS](#)

6. Regras feitas sob encomenda da reivindicação não configuradas corretamente

Resumo de problema

A solicitação de login falha com 500 que o erro no navegador com mensagem “não poderia identificar o usuário da resposta de SAML. /Could para não recuperar o principal do usuário SAML.”
uid e/ou user_principal não ajustados nas reivindicações que parte.

Etapa da falha

Processamento da resposta de SAML

Navegador

erro 500 com esta mensagem:

Afirmção de SAML falhada de IdP com código de status: urn:oasis:names:tc:

SAML:2.0:status:Requester/urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy. Verifique de IdP e tente-a outra vez.

Visualizador de eventos AD FS:

O pedido de autenticação de SAML teve uma política de NameID que não poderia ser satisfeita

Utilizador: [myids.cisco.com](#)

Formato do identificador do nome: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SPNameQualifier: [myids.cisco.com](#)

Detalhes da exceção:

MSIS1000: O pedido de SAML conteve um NameIDPolicy que não fosse satisfeito pelo token

Mensagem de erro

NameIDPolicy pedido: AllowCreate: Formato verdadeiro: urn:oasis:names:tc:SAML:2.0:nameid-format:transient

SPNameQualifier: [myids.cisco.com](#). Propriedades reais de NameID: zero.

Este pedido falhado.

Ação de usuário

Use o Gerenciamento AD FS 2.0 pressão-em para configurar a configuração que se emite para o nome.

Log do Cisco IDS:

```
2016-08-30 a INFORMAÇÃO com.cisco.ccbu.ids SAML2SPAdapter.java:76 de 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] - SSO falhou com código: 1. Status de resposta: <samlp: <samlp de Status>: <samlp: Status Code> </samlp: Status> para AuthnRequest: ERRO n/a com.cisco.ccbu.ids IdSSAMLAyncServlet.java:09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] - processamento da resposta de SAML falhada com.sun.identity.saml2.common.SAML2Exception: Código de status inválido na resposta. em com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425) em com.sun.identity.saml2.profile.SPACSUtills.processResponse(SPACSUtills.java:1050) em com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2038)
```

Possível causa

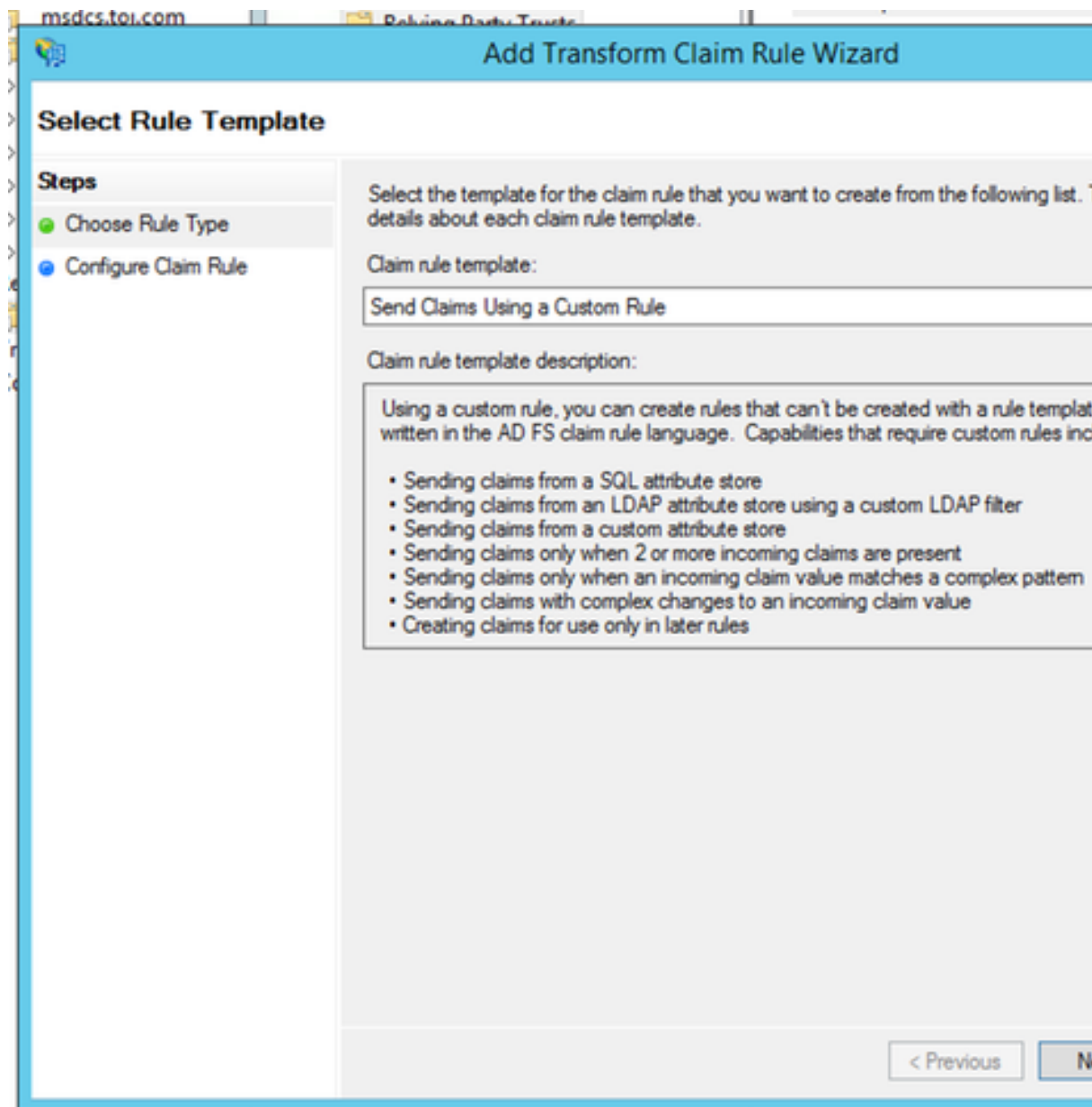
A regra feita sob encomenda da reivindicação não é configurada corretamente.

Sob regras da reivindicação AD FS, assegure-se de que os atributos que traçam para “use” estejam definidos como no manual de configuração (que guiam?).

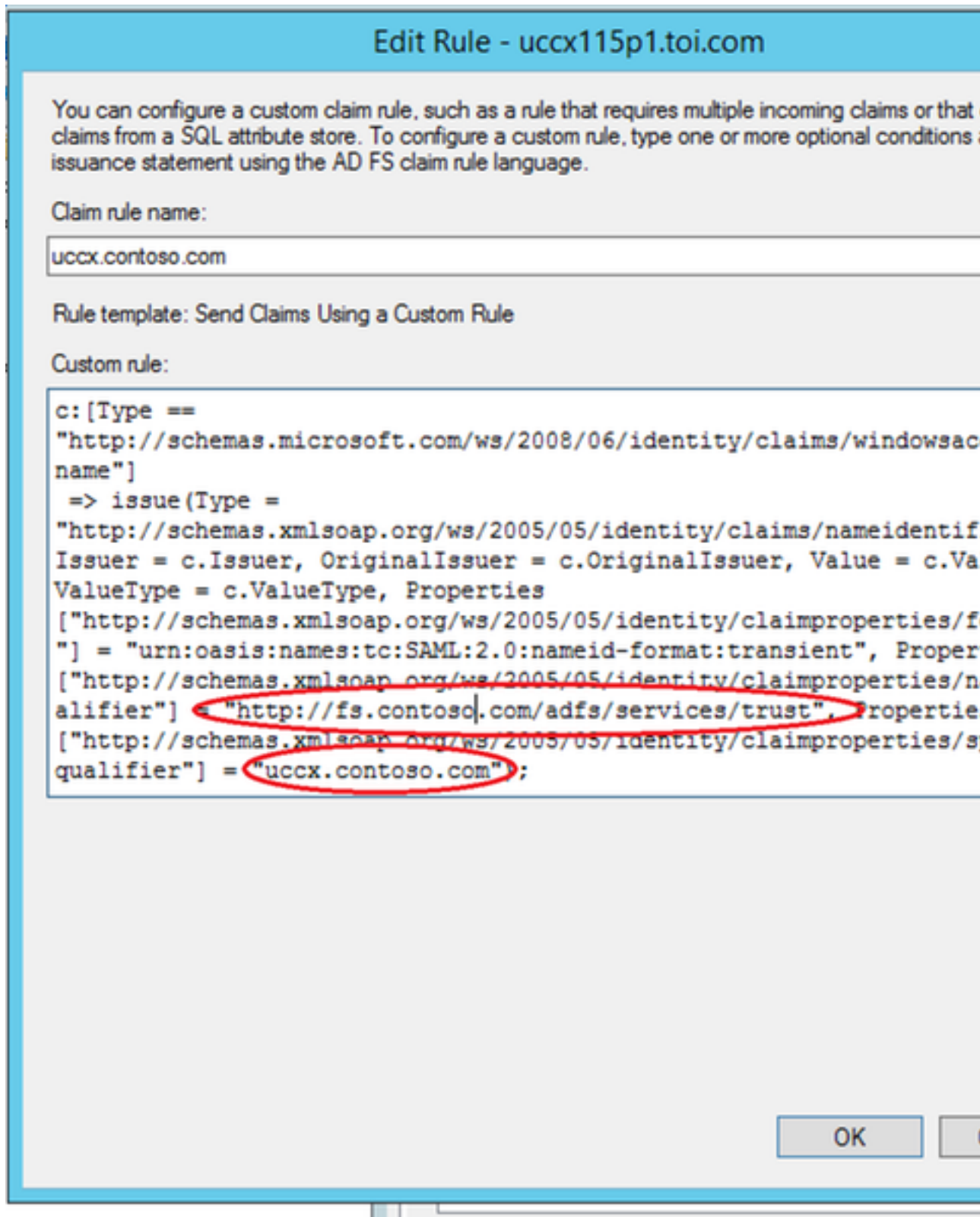
Ação recomendada

1. RDP ao sistema AD FS.

2. Edite as regras da reivindicação para regras feitas sob encomenda da reivindicação.



3. Verifique que o AD FS e os nomes de domínio totalmente qualificados do Cisco IDS e



7. Pedidos demais a AD FS.

Resumo de problema

A solicitação de login falha com erro 500 no navegador com estado code:urn:oasis:names:tc:SAML:2.0:status:Responder

O Mensagem de Erro no View Log do evento AD FS indica que há pedidos demais a AD FS.

Etapa da falha

Processamento da resposta de SAML

Navegador

Mensagem de erro

erro 500 com esta mensagem:

Erro de configuração de IdP: Processamento de SAML falhado

Afirmção de SAML falhada de IdP com código de status: urn:oasis:names:tc:SAML:2.0:st

Verifique a configuração de IdP e tente-a outra vez.

Visualizador de eventos AD FS:

Microsoft.IdentityServer.Web.InvalidRequestException:

MSIS7042: A mesma sessão do navegador cliente fez pedidos do '6' no dura segundos '16'. Contacte seu administrador para detalhes.

em Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetection

em Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse

MSISSignInResponse)

Evento Xml: [o <Data >Microsoft.IdentityServer.Web.InvalidRequestException do <EventData>](#)
<http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events>" do name= " o
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=" <UserData> </System> UserID="S-1-5-21-1680627477
1502263146-1105"/> <Security <Computer>myadfs.cisco.com</Computer> 2.0/Admin</Channel> FS
ThreadID="392" ProcessID="2264" <Execution ActivityID="{98778DB0-869A-4DD5-B3B6-0565AC17B
<EventRecordID>29385</EventRecordID>/> <http://schemas.microsoft.com/win/2004/08/events>" xm
<Provider do <System> <http://schemas.microsoft.com/win/2004/08/events/event>"> do xmlns= <
mesma sessão do navegador cliente fez pedidos do '6' nos últimos segundos '16'. Contacte
para detalhes. em Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoop
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse (resposta
</EventData> </Event> </UserData> </Event> de MSISSignInResponse

Log do Cisco IDS

2016-04-15 ERRO [IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102 do padrão de 16:
- exceção que processa o pedido com.sun.identity.saml2.common.SAML2Exception: Código de s
resposta. em com.sun.identity.saml2.common.SAML2Utils.verifyResponse(SAML2Utils.java:425)
com.sun.identity.saml2.profile.SPACSUtills.processResponse(SPACSUtills.java:1050) em
com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2038)
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA

Possível causa

Há pedidos demais que vêm a AD FS da mesma sessão de navegador.

Isto não deve tipicamente acontecer na produção. Mas se você encontra este, você pode:

Ação recomendada

1. Verifique o visualizador de eventos AD FS Windows.
2. Verifique novamente as configurações confiável de confiança do partido. Para mais d
[configurar o Cisco IDS e o AD FS](#)
3. Relogin.

8. O AD FS não é configurado para assinar a afirmação e a mensagem.

Resumo de problema

A solicitação de login falha com erro 500 no navegador com código de erro: invalidSignatu

Etapa da falha

Processamento da resposta de SAML

Navegador

erro 500 com esta mensagem:

Código de erro: invalidSignature

Mensagem: Assinatura inválida em ArtifactResponse.

Log do Cisco IDS:

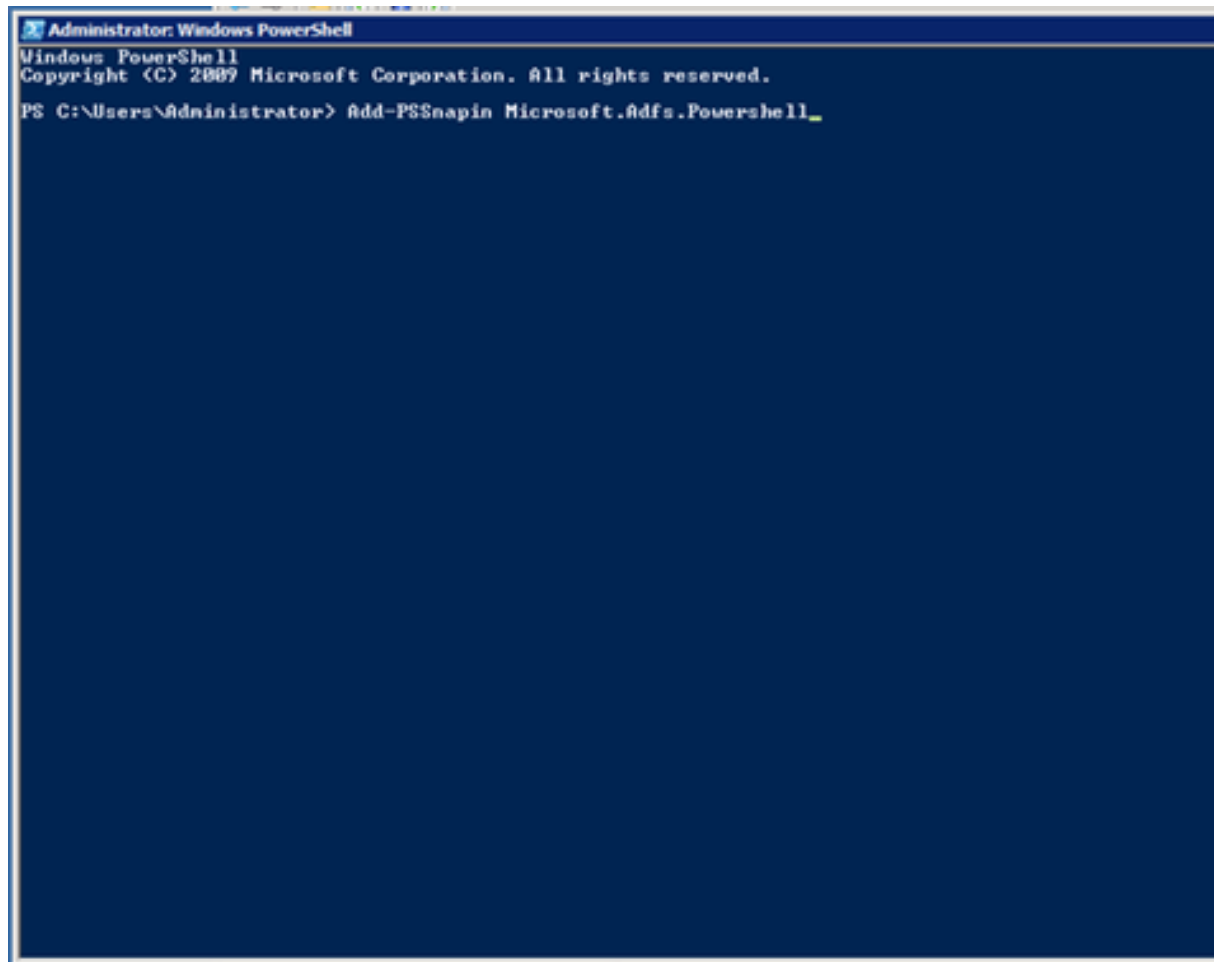
Mensagem de erro

2016-08-24 INFORMAÇÃO saml2error.jsp saml2error_jsp.java:75 de 10:53:10.494 IST(+0530) [I
- processamento da resposta de SAML falhado com código: invalidSignature; mensagem: Assin
ArtifactResponse. 2016-08-24 ERRO com.cisco.ccbu.ids IdSSAMLAyncServlet.java:298 de 10:5
[IdSEndPoints-SAML-241] - processamento da resposta de SAML falhado com exceção
com.sun.identity.saml2.common.SAML2Exception: Assinatura inválida na resposta. em
com.sun.identity.saml2.profile.SPACSUtills.getResponseFromPost(SPACSUtills.java:994) em
com.sun.identity.saml2.profile.SPACSUtills.getResponse(SPACSUtills.java:196) em
com.sun.identity.saml2.profile.SPACSUtills.processResponseForFedlet(SPACSUtills.java:2028)
com.cisco.ccbu.ids.auth.api.IdSSAMLAyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLA

**Possível
causa**

O AD FS não é configurado para assinar a afirmação e a mensagem.

1. Execute o comando do powershell AD FS: **Grupo-ADFSRelyingPartyTrust - Confiança do partido de TargetName - SamlResponseSignature "MessageAndAssertion"**
2. RDP ao sistema AD.
3. Abra **Powershell**.
4. Adicionar Windows PowerShell pressão-INS à sessão atual. Esta etapa não pode ser se você está usando o 3.0 ADFS desde que o CmdLet é instalado já como parte de adicionais características.



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.PowerShell_
```

**Ação
recomendada**

5. Adicionar a confiança de confiança do partido AD FS para a mensagem e a afirmação

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-PSSnapin Microsoft.Adfs.Powershell
PS C:\Users\Administrator> Set-ADFSRelyingPartyTrust -TargetName uccx.contoso.com -SamlResponseSignature" _
```

Informações Relacionadas

Isto é relacionado à configuração do fornecedor da identidade descrita no artigo:

- <https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html>
- [Suporte Técnico e Documentação - Cisco Systems](#)