ADFS/IdS排除故障和常见问题

Contents

Introduction

Cisco身份服务(ID)和激活目录联邦服务(AD FS)之间的安全主张标记语言(SAML)交互作用通过浏览器是单一符号核心在(SSO)登录流的。 本文在调试问题将帮助您与在Cisco IDS和AD FS的配置有关，与推荐的行为一起解决他们。

Cisco IDS部署模型

产品　配置

UCCX coresident
PCCE 与CUIC (Cisco Unified智力中心)和LD (实际数据)的共同驻留
UCCE 与CUIC和LD的共同驻留2k配置的。
独立为4k和12k配置。

Prerequisites

Requirements

Cisco 建议您了解以下主题：

- Cisco Unified Contact Center Express (UCCX)版本11.5或Cisco Unified Contact Center Enterprise Release 11.5或者被包的联系中心企业(PCCE)版本11.5如可适用。
- Microsoft Active Directory -在Windows服务器上安装的AD
- IdP (身份供应商) -激活目录联邦服务(AD FS)版本2.0/3.0

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

背景信息

在信任关系被建立在Cisco IDS和AD FS之间(请参阅这里关于详细资料，普通为UCCX和UCCE)后，管理员预计运行测试在Settings页的SSO设置身份服务管理保证在Cisco IDS和AD FS之间的配置良好工作。 如果测试失败，请使用产生的适当应用程序和建议在此指南解决问题。

可以是方便的在调试的应用程序和日志

应用程序/日志	详细资料	在哪里查找工具
Cisco IDS日志	Cisco IDS日志记录器将记录在Cisco IDS发生的所有错误。	请使用RTMT获得Ci 阅，指导使用RTMT 请注意: RTMT名字是
Fedlet日志	Fedlet日志将给予关于在Cisco IDS发生的所有SAML错误的更多详细资料	Cisco身份Service> 请使用RTMT获得Fe Fedlet日志的位置同 fedlet日志从前缀fed
Cisco IDS API权值	API权值可以用于查找到和验证Cisco IDS API可能返回了的所有由Cisco IDS处理请求的错误和编号	请使用RTMT获得AP 请注意: RTMT名字是 这将出现在一个独立 authorize_metrics.c
在AD FS的事件浏览器	允许用户查看事件登陆系统。在AD FS的任何错误，当处理SAML请求/发送SAML回应将被记录这里时。	在AD FS机器中，请 >AdDFS 2.0 > Admi 在Windows 2008， >Administrative的事 在Windows 2012，

SAML查看器	SAML查看器在查看将帮助被发送从/至Cisco IDS的SAML请求和回应。 此浏览器应用程序为请求/响应对SAML的分析是非常有用的。

在哪里请查看您的窗
这些是您能使用查看
1. 提琴手 如何以
2. SAML跟踪程序
3. SAML镀铬物面

与调试选项的流程图

SSO认证的多种步骤在每个步骤的镜像与一起和调试人工制品显示在故障的情况下在该步骤的一个故障。

此表给予关于怎样的详细资料识别故障在每个步骤在浏览器的SSO。不同的工具，并且如何请能他们在调试帮助指定。

步骤	如何识别在浏览器的故障	工具/日志
处理由Cisco IDS的AuthCode请求	在故障的情况下，浏览器没有重定向对SAML终端或AD FS， JSON错误由Cisco IDS显示，表明客户端ID或重定向URL无效。	Cisco IDS日志指示生成的错理时。 Cisco IDS API权值-指示被处
SAML由Cisco IDS的请求开始	在故障期间，浏览器没有重定向对AD FS，并且错误页/消息将由Cisco IDS表示。	Cisco IDS日志指示是否有例 Cisco IDS API权值-指示被处
处理由AD FS的SAML请求	所有疏忽处理此请求将导致AD FS服务器显示的错误页而不是登录页。	在AD FS的事件浏览器指示生 插件SAML的浏览器-看到被发
发送SAML回应由AD FS	在有效证件被提交后，所有疏忽发送回应导致AD FS服务器显示的错误页。	在AD FS的事件浏览器-指示生
处理由Cisco IDS的SAML回应	Cisco IDS将显示与错误原因和快速检查页的一个500错误。	在AD FS的事件浏览器-，如果一个成功的状态码，指示错误 插件SAML的浏览器-看到SAM是错误的。 Cisco IDS日志-指示错误/例外 Cisco IDS API权值-指示被处

处理由Cisco IDS的Authcode请求

起始点SSO登录，就Cisco IDS而言，是要求从SSO被启用的应用程序的授权码。API请求验证完成检查它是否是自一个注册的客户端的一个请求。成功验证导致重定向对Cisco IDS SAML终端的浏览器。在请求验证的所有故障导致从Cisco IDS page/JSON (Javascript对象符号)被退还的错误。

在此进程中遇到的常见错误

1. **没完成的客户端注册**

问题汇总	登录请求失效与401在浏览器的错误。

错误消息	**浏览器：**
	401与此消息的错误：{error ：“invalid_client”， “error_description” ：“无效ClientId。”}
	Cisco IDS日志：
	`2016-09-02 00:16:58.604 IST(+0530) [IdSEndPoints-51]com.cisco.ccbu.ids IdSConfigImpl.java:12`
	`org.apache.oltu.oauth2.common.exception.OAuthProblemException.error(OAuthProblemException.ja`

可能的原因	客户端注册用Cisco IDS不完成。
推荐的行为	连接到Cisco IDS管理控制台并且确认客户端是否成功注册。否则，请在继续进行然后注册客户

2. **用户访问应用程序使用IP地址/Alternate主机名**

问题汇总	登录请求失效与401在浏览器的错误。

错误消息	**浏览器：** 401与此消息的错误：{error ：“invalid_redirectUri”，“error_description”：“Invlalid重定向Uri”}
可能的原因	用户访问应用程序使用IP地址/Alternate主机名。 在SSO模式下，如果使用IP，应用程序被获取，它不工作。应该由主机名获取应用程序-由哪些IDS注册。此问题能发生，如果用户访问了没有向Cisco IDS登记的一个备选主机名。
推荐的行为	连接到Cisco IDS管理控制台并且确认同样用于访问应用程序的客户端是否向正确的重定向URL

SAML由Cisco IDS的请求开始

Cisco IDS SAML终端是SAML流的起始点在SSO基于登录的。交互作用的开始Cisco IDS和AD FS之间的在此步骤被触发。这里前提是Cisco IDS应该认识AD FS连接对，当应该加载对应的IdP元数据到此步骤的Cisco IDS能成功。

在此进程中遇到的常见错误

1. AD FS元数据没被添加到Cisco IDS

问题汇总	登录请求失效与503在浏览器的错误。
错误消息	**浏览器：** 503与此消息的错误：{error ：“service_unavailable”，“error_description”：“SAML元数据没有化”}
可能的原因	Idp元数据不是可用的在Cisco IDS。在Cisco IDS和AD FS之间的信任建立不完成。
推荐的行为	连接到Cisco IDS管理控制台并且检查ID是否在没**被配置的**状态。 确认，如果IdP元数据被加载。 否则，请加载从AD FS下载的IdP元数据。 欲了解更详细的信息请参阅这里。

处理由AD FS的SAML请求

SAML请求处理是在AD FS的第一步在SSO流。Cisco IDS发送的SAML请求由在此步骤的AD FS读，验证并且解密。成功处理此请求导致两个方案：

1. 如果它是在浏览器的新登录， AD FS显示登录表。如果它是一个已经认证的用户的relogin从一次现有的浏览器会话的， AD FS尝试直接地退还SAML回应。

Note:主要前提对于此步骤是为了AD FS能安排回复的当事人信任被配置。

在此进程中遇到的常见错误

1. 有AD的FS最新的Cisco身份证的SAML认证。

问题汇总	不显示AD的FS登录页，反而显示错误页。
错误消息	**浏览器** AD FS显示错误页类似于此： 有访问站点的问题。设法再访问到站点。 如果问题持续，与此站点的管理员联系并且提供参考编号识别问题。 参考编号：1ee602be-382c-4c49-af7a-5b70f3a7bd8e **AD FS事件浏览器** 联邦服务遇到错误，当处理SAML认证请求时。

其它数据

```
Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException MSIS0038
Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage (MSIS
Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.CreateErrorMessage (create
CreateErrorMessageRequest)Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.
```

可能的原因 取决于的当事人信任没有设立或Cisco IDS认证更改了，但是同样没有被加载到AD FS。

推荐的行为 设立在AD FS和Cisco IDS之间的信任有最新的Cisco IDS认证的。
请保证Cisco IDS认证不过期。您在Cisco身份服务管理方面能看到状态显示板。如果那样，请
欲了解更详细的信息关于怎样设立在ADFS间的元数据信任& Cisco IDS请参阅，这里

发送由AD FS的SAML回应

在用户成功验证后， ADFS发送SAML回应回到Cisco IDS通过浏览器。ADFS能发送SAML回应与指示成功或故障的状态码。如果表认证在AD FS没有允许那么这将指示一个故障响应。

在此进程中遇到的常见错误

1. 表认证在AD FS没有被启用

问题汇总 浏览器显示NTLM登录，然后失效，无需成功重定向到Cisco IDS。

步骤故障 发送SAML回应

错误消息
浏览器：
浏览器显示NTLM登录，但是在成功的登录以后，失效与许多重定向。

可能的原因 Cisco IDS在AD FS支持表仅基于认证，表认证没有被启用。

推荐的行为 欲了解更详细的信息关于怎样Enable表认证请参阅：
ADFS 2.0表验证设置
ADFS 3.0表验证设置

处理由Cisco IDS的SAML回应

在此阶段， Cisco IDS从AD FS得到SAML回应。此回应可能包含指示成功或故障的状态码。自AD FS的一个错误反应结果到错误页，并且同样必须调试。

在一种成功的SAML回应期间，处理请求可以发生故障对于这些原因：

- 不正确IdP (AD FS)元数据。
- 疏忽检索期待从AD FS的流出的要求。
- Cisco IDS和AD FS时钟没有同步。

在此进程中遇到的常见错误

1. AD在Cisco IDS的FS认证不最晚。

问题汇总 登录请求失效与500在浏览器的错误有错误代码的作为invalidSignature。

步骤故障 SAML回应处理

错误消息
浏览器：
500与此消息的错误在浏览器：
错误代码：invalidSignature
消息：签署的认证不匹配什么在实体元数据被定义。
AD FS事件浏览器：
没有错误
Cisco IDS日志：

2016-04-13 12:42:15.896 IST(+0530) DEFAULT[IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.ja
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:985)com.sun.id

可能的原因 SAML被舍弃的回应处理，因为IdP认证是与什么不同是可用的在Cisco IDS。

推荐的行为 下载最新的AD FS元数据从：**https://<ADFSServer>/federationmetadata/2007-06/federationm**
并且请加载它到Cisco IDS通过身份服务Managament用户界面。
关于详细资料，请参阅配置Cisco IDS和AD FS

2. Cisco IDS和AD FS时钟没有同步。

问题汇总 登录请求失效与500在浏览器的错误有状态码的：urn:oasis:names:tc:SAML:2.0:status:Succes

步骤故障 SAML回应处理

浏览器：
500与此消息的错误：
IdP配置错误：被舍弃的SAML处理
从IdP的SAML assertion failed与状态码：urn:oasis:names:tc:SAML:2.0:status:Success.再验证

错误消息

Cisco IDS日志
2016-08-24 18:46:56.780 IST(+0530) [IdSEndPoints-SAML-22]com.cisco.ccbu.ids IdSSAMLAsyncServ
java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1145)java.util.con

SAML查看器：
寻找NotBefore和NotOnOrAfter字段
<Conditions NotBefore="2016-08-28T14:45:03.325Z" NotOnOrAfter="2016-08-28T15:45:03.3

可能的原因 在Cisco IDS和IdP系统的时间是不同步的。

推荐的行为 同步在Cisco IDS和AD FS系统的时间。建议AD FS系统和Cisco IDS是使用Ntp server同步的时

3. 错误的签名算法(SHA256与SHA1)在AD FS

问题汇总 登录请求失效与500在浏览器的错误以状态code:urn:oasis:names:tc:SAML:2.0:status:Respond
在AD FS事件View Log的错误信息–错误的签名Algorithm(SHA256与SHA1)在AD FS

步骤故障 SAML回应处理

浏览器
500与此消息的错误：
IdP配置错误：被舍弃的SAML处理
从IdP的SAML assertion failed与状态码：urn:oasis:names:tc:SAML:2.0:status:Responder.再验

错误消息

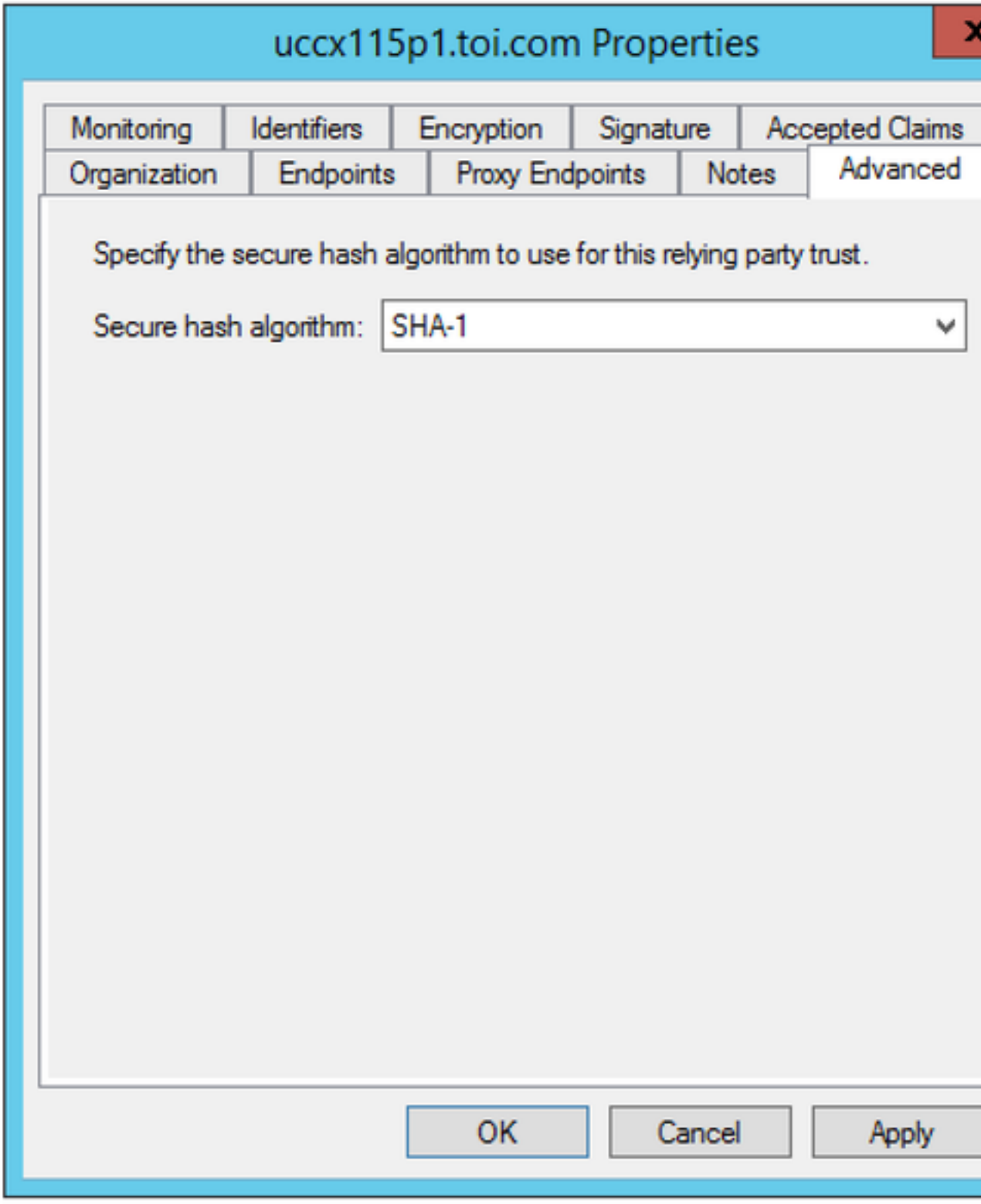
AD FS事件浏览器：
SAML请求没有签字与期望的签名算法。SAML请求签字与签名算法http://www.w3.org/2001/04
期望的签名算法是rsa-sha1

Cisco IDS日志：
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAMLcom.sun.identity.saml2.common.SAML2Exc
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn

可能的原因 配置AD FS使用SHA-256。

推荐的行为 更新AD FS使用SHA-1签字和加密。

1. AD FS系统的RDP。
2. 打开AD FS控制台。
3. 选择**取决于的当事人信任**并且点击**属性**
4. 选择**高级选项卡**。
5. 选择SHA-1从下拉列表。



4. 没正确地被配置的流出的要求规则

问题汇总	登录请求失效与在浏览器的错误有消息的“不可能从SAML回应的检索用户标识的500。/Could从在流出的要求并且/或者user_principal没设置的uid。
步骤故障	SAML回应处理
错误消息	**浏览器：** 500与此消息的错误： IdP配置错误：被舍弃的SAML处理。 不可能从SAML回应的检索用户标识。/Could从SAML回应的不是检索用户负责人。 **AD FS事件浏览器：** 没有错误

Cisco IDS日志：

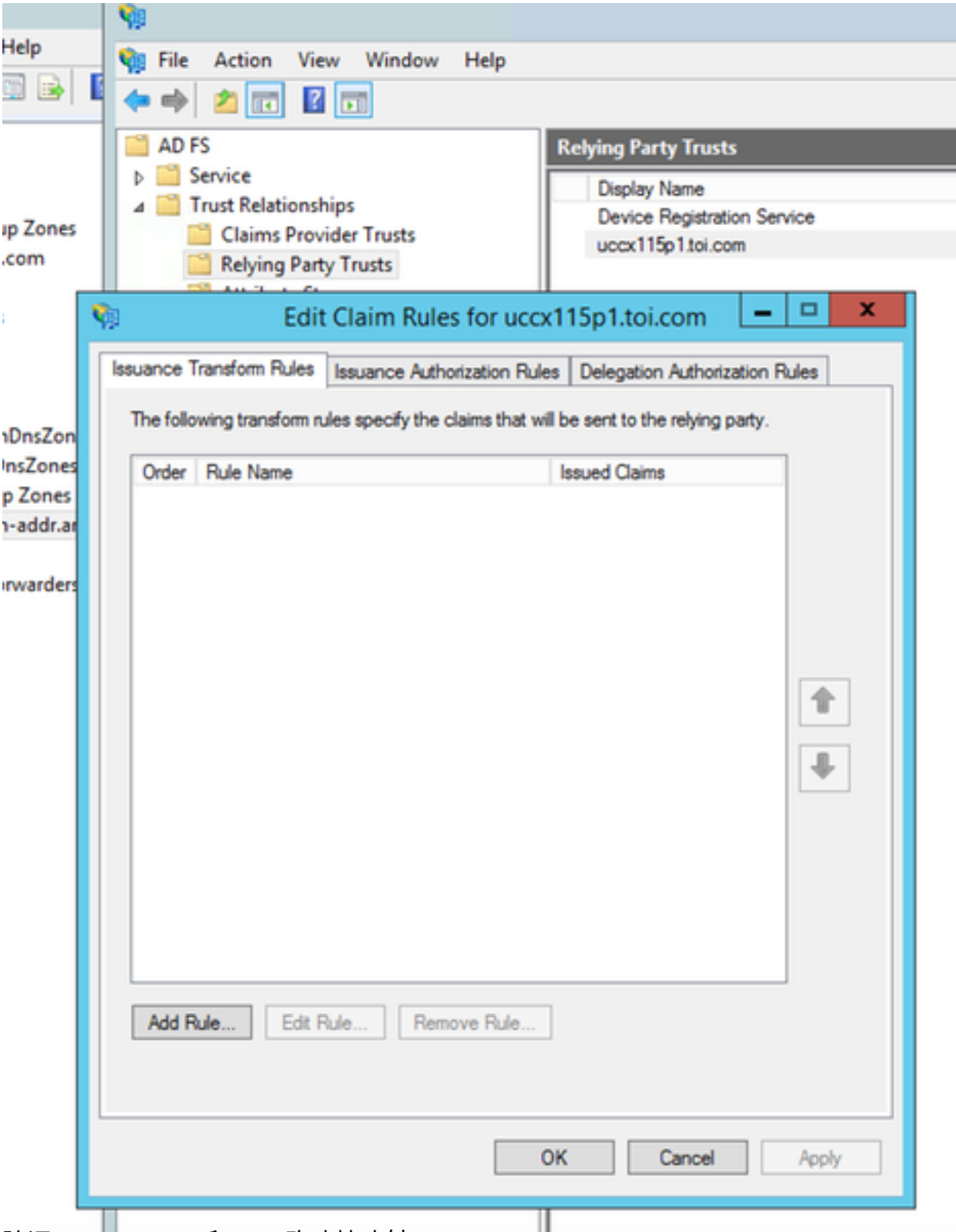
```
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAMLExcep
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServle
```

可能的原因

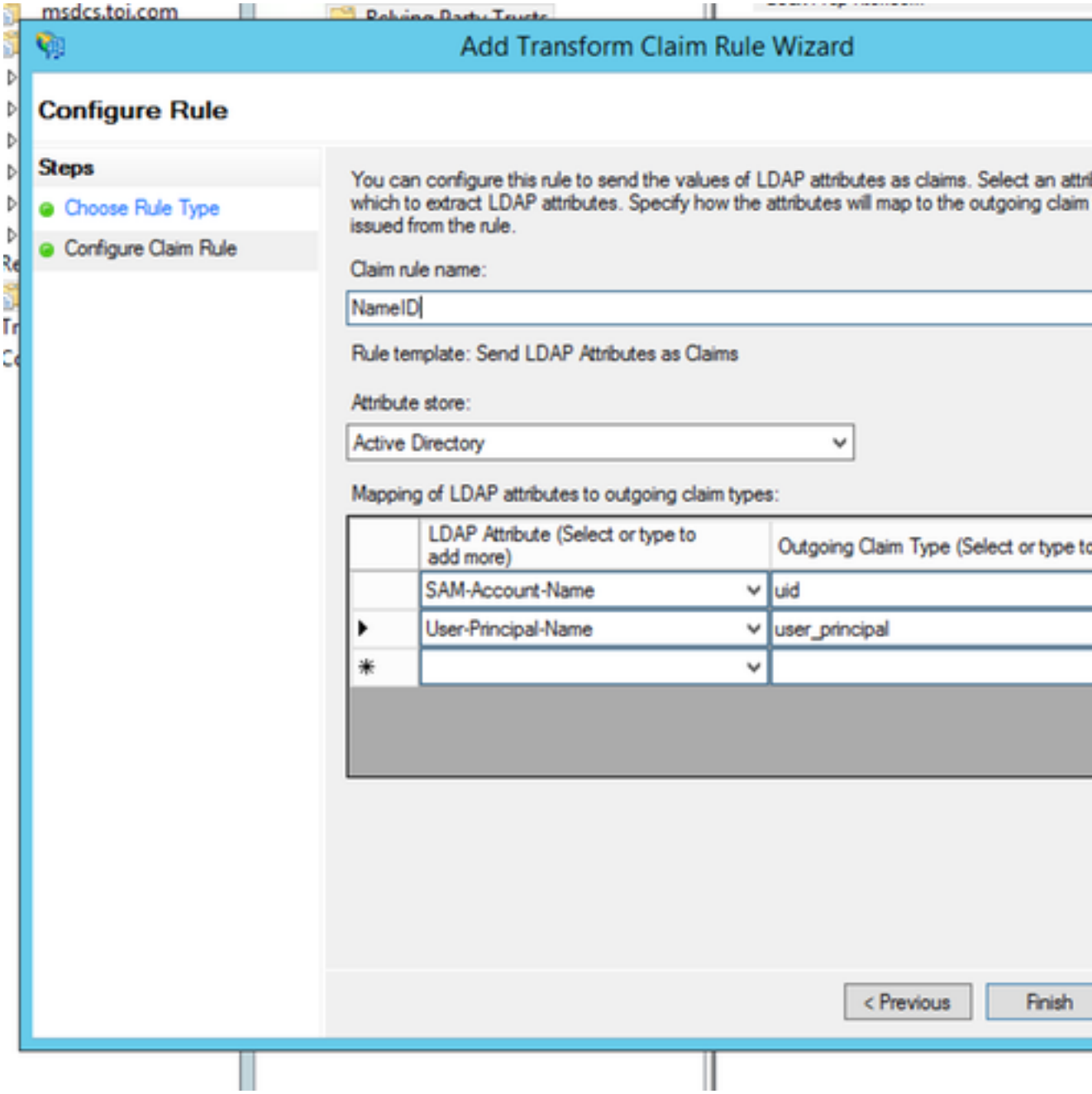
必须的流出的要求(uid和user_principal)在要求规则没有正确地被配置。
如果未配置NameID要求规则或没有适当配置uid或user_principal。
如果NameID规则是没被配置或user_principal没有正确地被映射， user_principal没有被检索的
如果uid没有正确地被映射， Cisco IDS表明uid没有被检索。
根据AD FS要求规则，请保证映射为“user_principal”和“uid的”属性被定义作为在(指导？)的IdP

1. AD FS系统的RDP。
2. 编辑取决于的当事人信任的要求规则。

推荐的行为



3. 验证user_principal和uid正确地被映射



5. 流出的要求规则在联盟的AD FS没有正确地被配置

问题汇总	登录请求失效与在浏览器的错误有消息的“不可能从SAML回应的检索用户标识的500。或者不可
步骤故障	SAML回应处理 **浏览器** 500与此消息的错误： IdP配置错误：被舍弃的SAML处理 不可能从SAML回应的检索用户标识。/不可能从SAML回应的检索用户负责人。

错误消息	**AD FS事件浏览器：**
	没有错误
	Cisco IDS日志：
	`com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAMLExcep`
	`com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServle`

可能的原因	在联盟的AD FS中有可能失踪的更多配置要求了。
推荐的行为	检查在联盟的AD的AD FS配置是否根据**多域配置的**部分被执行**的联盟的AD FS**配置Cisco IDS和

6. 没正确地被配置的自定义要求规则

问题汇总

登录请求失效与在浏览器的错误有消息的“不可能从SAML回应的检索用户标识的500。/Could从
在流出的要求并且/或者user_principal没设置的uid。

步骤故障

SAML回应处理

浏览器

500与此消息的错误：

从IdP的SAML assertion failed与状态码：缸：绿洲：名字：tc ：**SAML:2.0:status:Requester/u**

AD FS事件浏览器：

SAML认证请求有不可能是满足的一个NameID策略。

申请人：myids.cisco.com

命名标识格式：urn:oasis:names:tc:SAML:2.0:nameid-format:transient

错误消息

SPNameQualifier ：myids.cisco.com

例外详细资料：

MSIS1000 ：SAML请求包含了未由发出的令牌满足的NameIDPolicy。被请求的NameIDPolicy
出故障的此请求。

用户动作

请使用卡扣式AD FS 2.0的管理配置散发必需的命名标识的配置。

Cisco IDS日志：

```
2016-08-30 09:45:30.471 IST(+0530) [IdSEndPoints-SAML-82] INFO com.cisco.ccbu.ids SAML2SPAda
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp StatusCode> </samlp
SAMLcom.sun.identity.saml2.common.SAML2Exception com.sun.identity.saml2.common.SAML2Utils.ve
com.sun.identity.saml2.profile.SPACSUtils.processResponseForFedlet(SPACSUtils.java:2038)
```

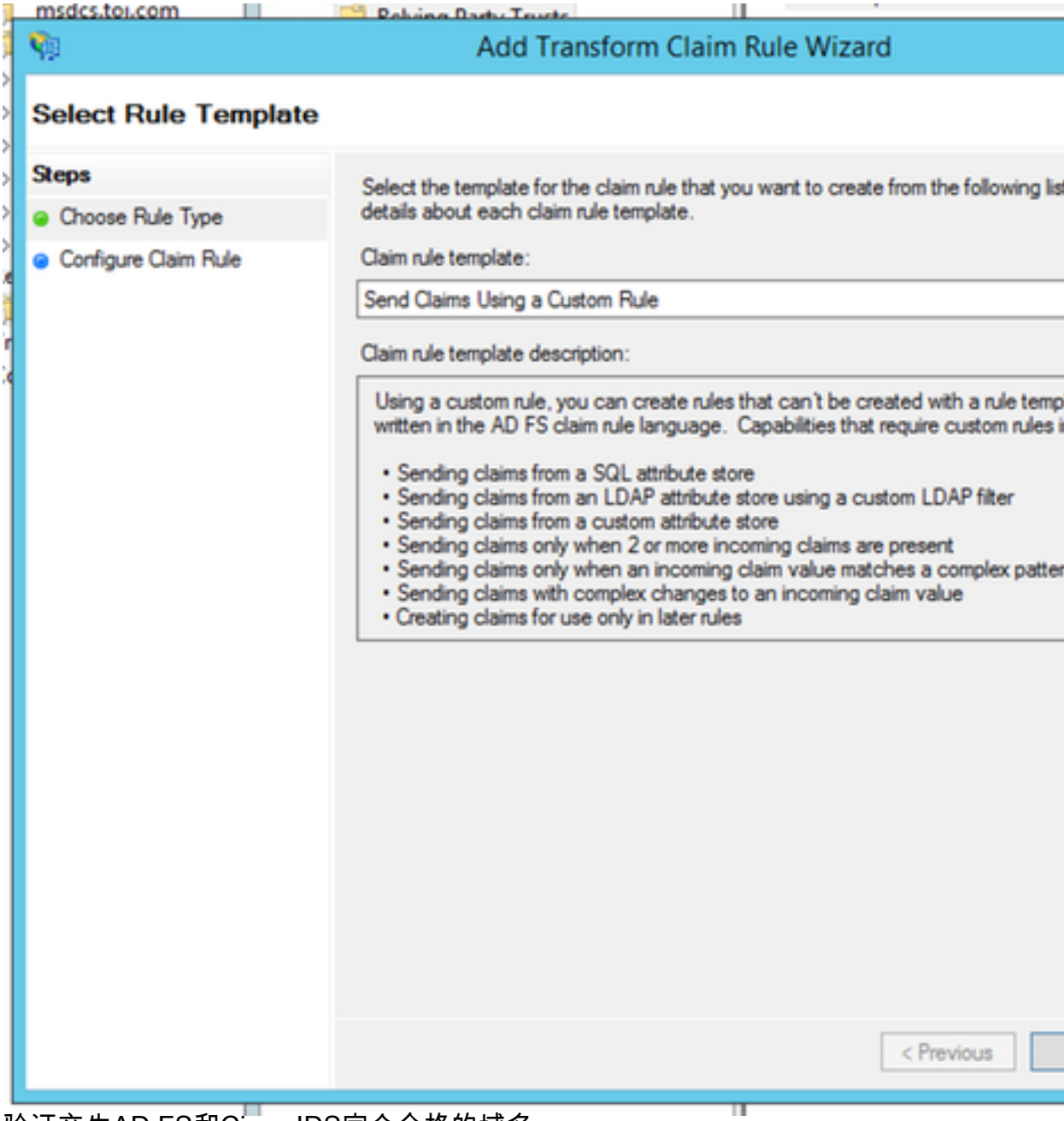
可能的原因

没有正确地配置自定义要求规则。

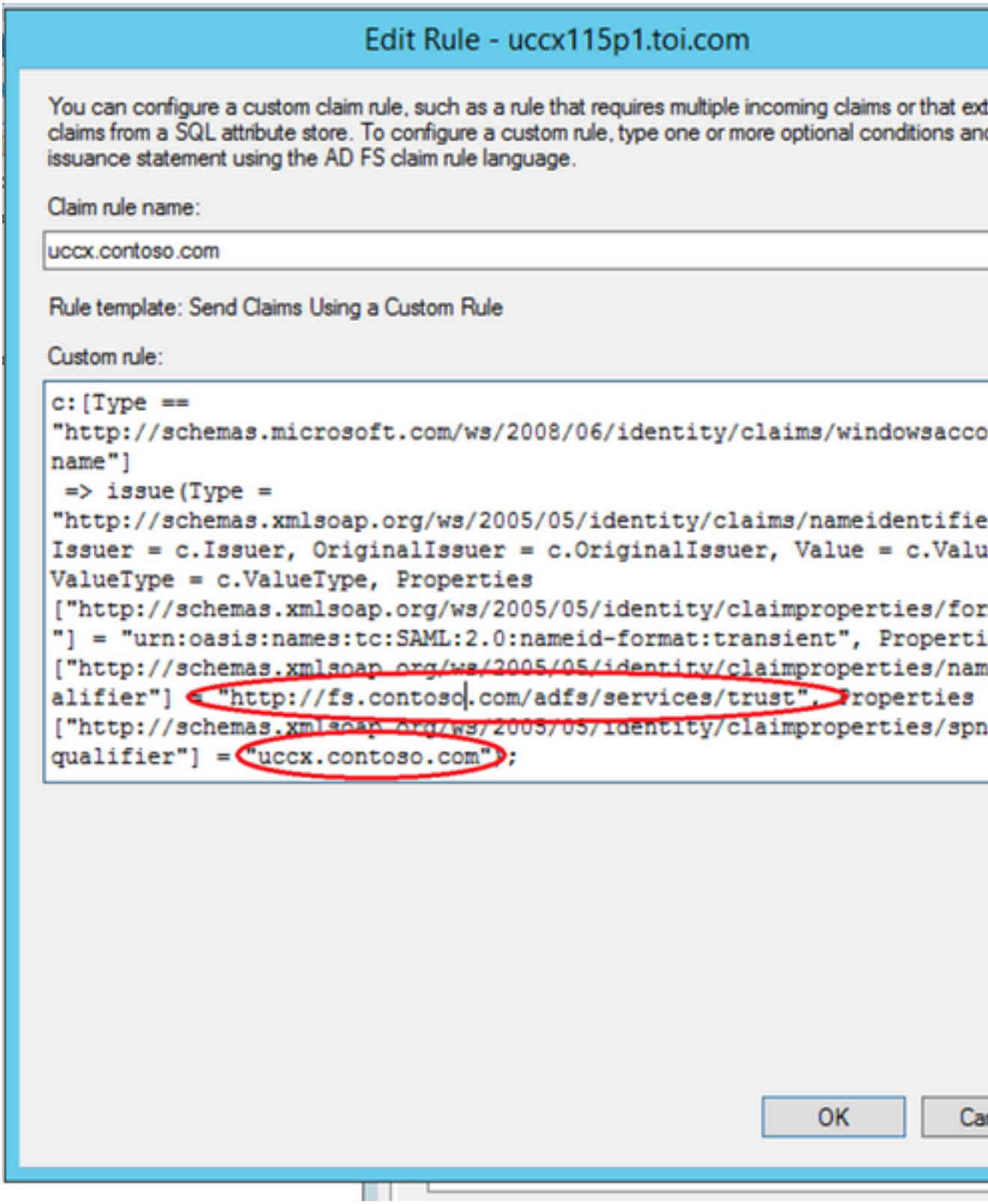
根据AD FS要求规则，请保证映射为“user_principal”和“uid的”属性被定义成在(指导？)的配置指

1. AD FS系统的RDP。
2. 编辑自定义要求规则的要求规则。

推荐的行为



3. 验证产生AD FS和Cisco IDS完全合格的域名。



7. 对AD FS的许多请求。

问题汇总	登录请求失效与500在浏览器的错误以状态code:urn:oasis:names:tc:SAML:2.0:status:Respond 在AD FS事件View Log的错误信息指示有许多请求对AD FS。
步骤故障	SAML回应处理
错误消息	**浏览器** 500与此消息的错误： IdP配置错误：被舍弃的SAML处理 从IdP的SAML assertion failed与状态码：urn:oasis:names:tc:SAML:2.0:status:Responder.再验 **AD FS事件浏览器：** Microsoft.IdentityServer.Web.InvalidRequestException ：

MSIS7042 ：**同一次客户端浏览器会话做了在的'6'请求持续**
'16'秒钟。与您的管理员联系关于详细资料。
在Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCoo
在Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse (MS

```
Xml <Event xmlns= " http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provid
<Correlation ActivityID="{98778DB0-869A-4DD5-B3B6-0565AC17BFFE}"/> <Execution ProcessID="226
http://schemas.microsoft.com/ActiveDirectoryFederationServices/2.0/Events"> <EventData> <Dat
</Event>
```

Cisco IDS日志

```
2016-04-15 16:19:01.220 EDT(-0400) DEFAULT[IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.ja
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn
```

可能的原因 有来自到AD FS的许多请求同一次浏览器会话。
这在生产不应该典型地发生。但是，如果遇到此，您能：

推荐的行为

1. 检查AD FS Windows事件浏览器。
2. 复校取决于的当事人信任设置。欲了解更详细的信息，*请参阅*配置Cisco IDS和AD FS
3. Relogin。

8. 没有配置AD FS签署主张和消息。

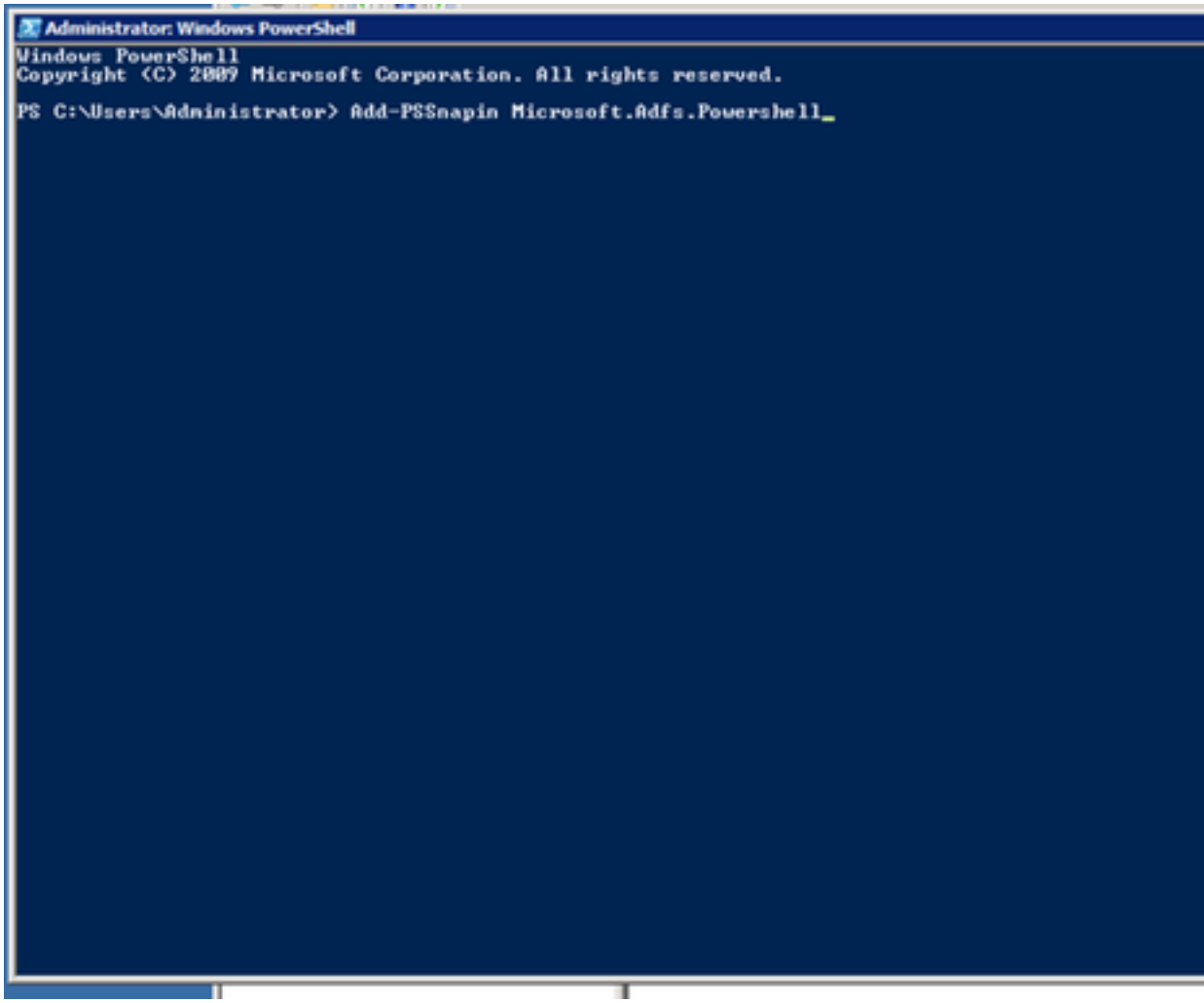
问题汇总 登录请求失效与500在浏览器的错误有错误代码的：invalidSignature
步骤故障 SAML回应处理
浏览器
500与此消息的错误：
错误代码：invalidSignature
错误消息 消息：无效签名在ArtifactResponse。
Cisco IDS日志：

```
2016-08-24 10:53:10.494 IST(+0530) [IdSEndPoints-SAML-241] INFO saml2error.jsp saml2error_js
com.sun.identity.saml2.profile.SPACSUtils.getResponseFromPost(SPACSUtils.java:994)com.sun.id
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn
```

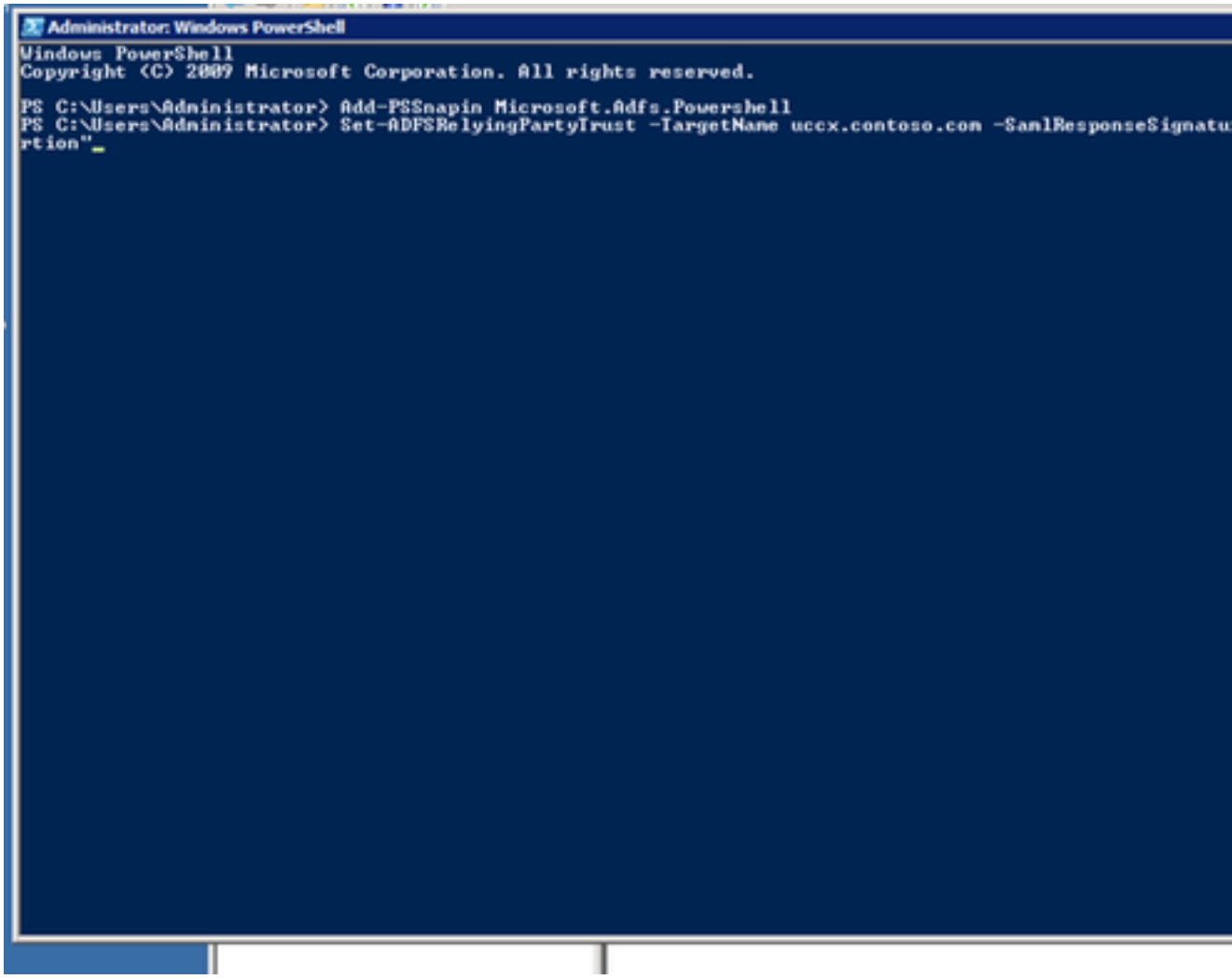
可能的原因 没有配置AD FS签署主张和消息。

1. 运行AD FS powershell命令： **SETADFSRelyingPartyTrust - TargetName <Relying的当事**
2. AD系统的RDP。
3. 打开**Powershell**。
4. 添加Windows PowerShell SNAP INS到当前会话。不可以需要此步骤，如果使用ADFS 3

推荐的行为



5. 添加消息和主张的AD FS取决于的当事人信任。



Related Information

这与在条款描述的身份供应商的配置有关：

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