ADFS/IdS故障排除和常见问题

目录

简介
先决条件
要求
使用的组件
背景信息
可以是方便的在调试的应用程序和日志
与调试选项的流程图
处理由Cisco IDS的Authcode请求
在此进程中遇到的常见错误
1. 没完成的客户端注册
2. 用户访问应用程序使用IP地址/Alternate主机名
SAML由Cisco IDS的请求开始
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
处理由AD FS的SAML请求
在此进程中遇到的常见错误
1. 有AD的FS最新的思科身份证的SAML证书。
发送由AD FS的SAML答复
在此进程中遇到的常见错误
1. 表验证在AD FS没有启用
处理由Cisco IDS的SAML答复
在此进程中遇到的常见错误
1. AD在Cisco IDS的FS证书不最晚。
2. Cisco IDS和AD FS时钟没有同步。
3. 错误的签名算法(SHA256与SHA1)在AD FS
4. 没正确地配置的流出的声明规则
5. 流出的声明规则在联盟的AD FS没有正确地配置
6. 没正确地配置的自定义声明规则
7. 对AD FS的许多请求。
8. AD FS没有配置签署断言和消息。
相关信息

简介

思科身份服务(ID)和活动目录联邦服务(AD FS)之间的安全断言标记语言(SAML)交互作用通过浏览器是单一符号核心在(SSO)登录流的。 本文在与在Cisco IDS和AD FS的配置涉及的调试问题将帮助您，与推荐的操作解决他们一起。

Cisco IDS部署模型

产品　部署

UCCX 共存
PCCE 有CUIC (Cisco Unified智能中心)和LD的(Live数据)共存
UCCE 有CUIC和LD的共存2k部署的。
4k和12k部署的独立。

先决条件

要求

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版本11.5或被包的Contact Center企业(PCCE)版本11.5如可适用。
- Microsoft Active Directory -在Windows服务器安装的AD
- IdP (标识供应商) -活动目录联邦服务(AD FS)版本2.0/3.0

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

在信任关系被建立在Cisco IDS和AD FS之间(请参阅此处关于详细信息，普通为UCCX和UCCE)后，管理员预计运行测验在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，请使用给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	详细信息	在哪里查找工具
Cisco IDS日志	Cisco IDS记录器将记录在Cisco IDS发生的所有错误。	请使用RTMT获得Ci 参阅，指导使用RTM 请注意: RTMT名称是
Fedlet日志	Fedlet日志将给予关于在Cisco IDS发生的所有SAML错误的更多详细信息	**科身份服务>日志** 请使用RTMT获得Fe Fedlet日志的位置同 fedlet日志从前缀**fed**
Cisco IDS API量度	API量度可以用于查找到和验证Cisco IDS API可能返回的所有由Cisco IDS处理请求的错误和编号	请使用RTMT获得AP 请注意: RTMT名称是 这将出现在一个独立
在AD FS的事件查看器	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答复将被记录此处时。	**saml_metrics.csv和** 在AD FS计算机，请 **志>AdDFS 2.0 > Ad** 在Windows 2008年 **>Administrative的**启 在Windows 2012， 在哪里请查看您的窗

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

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验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该步骤的一失败。

此表给予关于怎样的详细信息识别失败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	如何识别浏览器的失败	工具/日志
处理由Cisco IDS的AuthCode请求	在失败的情况下，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量度-指示处理
SAML由Cisco IDS的请求开始	在失败期间，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量度-指示处理
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的事件查看器指示生 SAML浏览器插件-看到发送对
发送由AD FS的SAML答复	在有效凭证提交后，所有疏忽发送答复导致AD FS服务器显示的错误页。	在AD FS的事件查看器-指示生 在AD FS的事件查看器-，如果一个成功的状态码，指示错误
处理由Cisco IDS的SAML答复	Cisco IDS将显示与错误原因和快速检查页的一个500错误。	SAML浏览器插件-看到SAML么是错误的。 Cisco IDS日志-指示在处理期 Cisco IDS API量度-指示处理

处理由Cisco IDS的Authcode请求

SSO登录起点，就Cisco IDS而言，是要求从SSO启用的应用程序的授权码。API请求验证完成检查它是否是从一个已注册客户端的一请求。成功验证导致重定向对Cisco IDS SAML终端的浏览器。请求验证的所有失败导致的错误page/JSON (Javascript对象符号)被退还的从Cisco IDS。

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`
	`com.cisco.ccbu.ids.auth.validator.IdSAuthorizeValidator.validateRequestParams(IdSAuthorizeVa`

可能的原因	客户端注册用Cisco IDS不完成。
建议操作	导航到Cisco IDS管理控制台并且确认客户端是否顺利地注册。否则，请在继续进行然后注册客

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”} 用户访问应用程序使用IP地址/Alternate主机名。
可能的原因	在SSO模式，如果使用IP，应用程序访问，它不工作。应该由他们在Cisco IDS注册的主机名访 用程序。此问题能发生，如果用户访问没有用Cisco IDS注册的一个备选主机名。
建议操作	导航到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注册与正确重定向 URLand。

SAML由Cisco IDS的请求开始

Cisco IDS SAML终端是SAML流的起点在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。此处前提条件是Cisco IDS应该认识AD FS连接对，当应该上传对应的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。 **浏览器：**
错误消息	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之间的托拉斯建立不完成。
建议操作	导航到Cisco IDS管理控制台并且检查ID是否在**未配置的状态**。 确认，如果IdP元数据上传。 否则，请上传从AD FS下载的IdP元数据。 欲了解更详细的信息请参阅此处。

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一新登录， AD FS显示登录表。如果它已经是一已认证的用户的relogin从一现有浏览器会话的， AD FS尝试直接地退还SAML答复。

注意：主要前提对于此步骤是为了AD FS能安排应答的当事人信任配置。

在此进程中遇到的常见错误

1. 有AD的FS最新的思科身份证的SAML证书。

问题汇总	不显示AD的FS登录页，反而显示错误页。 **浏览器**
错误消息	AD FS显示错误页类似于此： 有访问站点的问题。设法再浏览到站点。 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事件查看器** 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	取决于当事人信任没有设立或Cisco IDS证书更改，但是同样没有上传对AD FS。 设立在AD FS和Cisco IDS之间的信任有最新的Cisco IDS证书的。
建议操作	请保证Cisco IDS证书没有超时。您在思科身份服务管理方面能看到状态控制板。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，此处

发送由AD FS的SAML答复

在用户顺利地验证后， ADFS发送SAML答复回到Cisco IDS通过浏览器。ADFS能退还有指示成功或失败的状态码的SAML答复。如果表验证在AD FS没有启用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. 表验证在AD FS没有启用

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。
步骤失败	发送SAML答复
错误消息	**浏览器：** 浏览器显示NTLM登录，但是在成功登录以后，失效与许多重定向。
可能的原因	Cisco IDS支持在AD FS只形成基于验证，表验证没有启用。
建议操作	欲了解更详细的信息关于怎样Enable表验证请参阅： ADFS 2.0表验证设置 ADFS 3.0表验证设置

处理由Cisco IDS的SAML答复

在此阶段， Cisco IDS从AD FS得到SAML答复。此答复可能包含指示成功或失败的状态码。从AD FS的一个错误反应结果到错误页，并且同样必须调试。

在一成功的SAML答复期间，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。
- 疏忽从AD FS获取预计流出的要求。
- 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证书不最晚。

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。
步骤失败	SAML答复处理
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：签署的证书不匹配什么在实体元数据定义。 **AD FS事件查看器：** 无错误 **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失败的答复处理，因为IdP证书是与什么不同是可用的在Cisco IDS。

建议操作 下载最新的AD FS元数据从：**https://<ADFSServer>/federationmetadata/2007-06/federationm**
并且请上传它到Cisco IDS通过身份服务Managament用户界面。
关于详细信息，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

步骤失败 SAML答复处理

浏览器：
500与此消息的错误：
IdP配置错误：失败的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。

建议操作 同步在Cisco IDS和AD FS系统的时间。推荐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的错误消息–错误的签名Algorithm(SHA256与SHA1)在AD FS

步骤失败 SAML答复处理

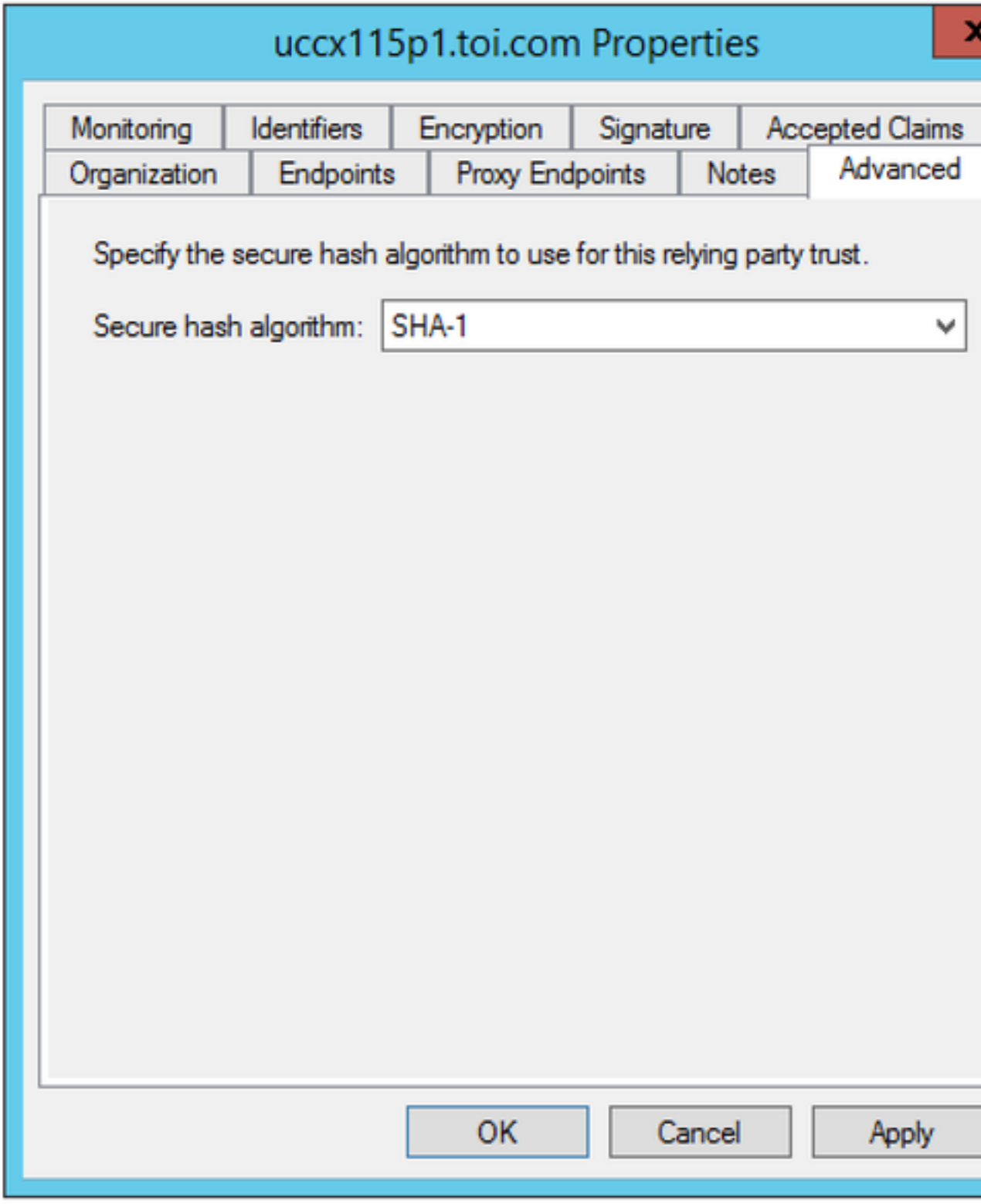
浏览器
500与此消息的错误：
IdP配置错误：失败的SAML处理
从IdP的SAML assertion failed与状态码：urn:oasis:names:tc:SAML:2.0:status:Responder.再验

错误消息
AD FS事件查看器：
SAML请求没有签字与预计签名算法。SAML请求签字与签名算法http://www.w3.org/2001/04/x
预计签名算法是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 AD FS配置使用SHA-256。

建议操作 更新AD FS使用SHA-1签字和加密。

1. AD FS系统的RDP。
2. 开放AD FS控制台。
3. 选择**取决于的Party托拉斯**并且点击**属性**
4. 选择**Advanced 选项卡**。
5. 选择从下拉列表的SHA-1。



4. 没正确地配置的流出的声明规则

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答复的检索用户标识符的500。/Coul 在流出的要求并且/或者user_principal没设置的uid。
步骤失败	SAML答复处理
错误消息	**浏览器：** 500与此消息的错误： IdP配置错误：失败的SAML处理。 不可能从SAML答复的检索用户标识符。/Could从SAML答复的不是检索用户负责人。 **AD FS事件查看器：** 无错误

Cisco IDS日志：

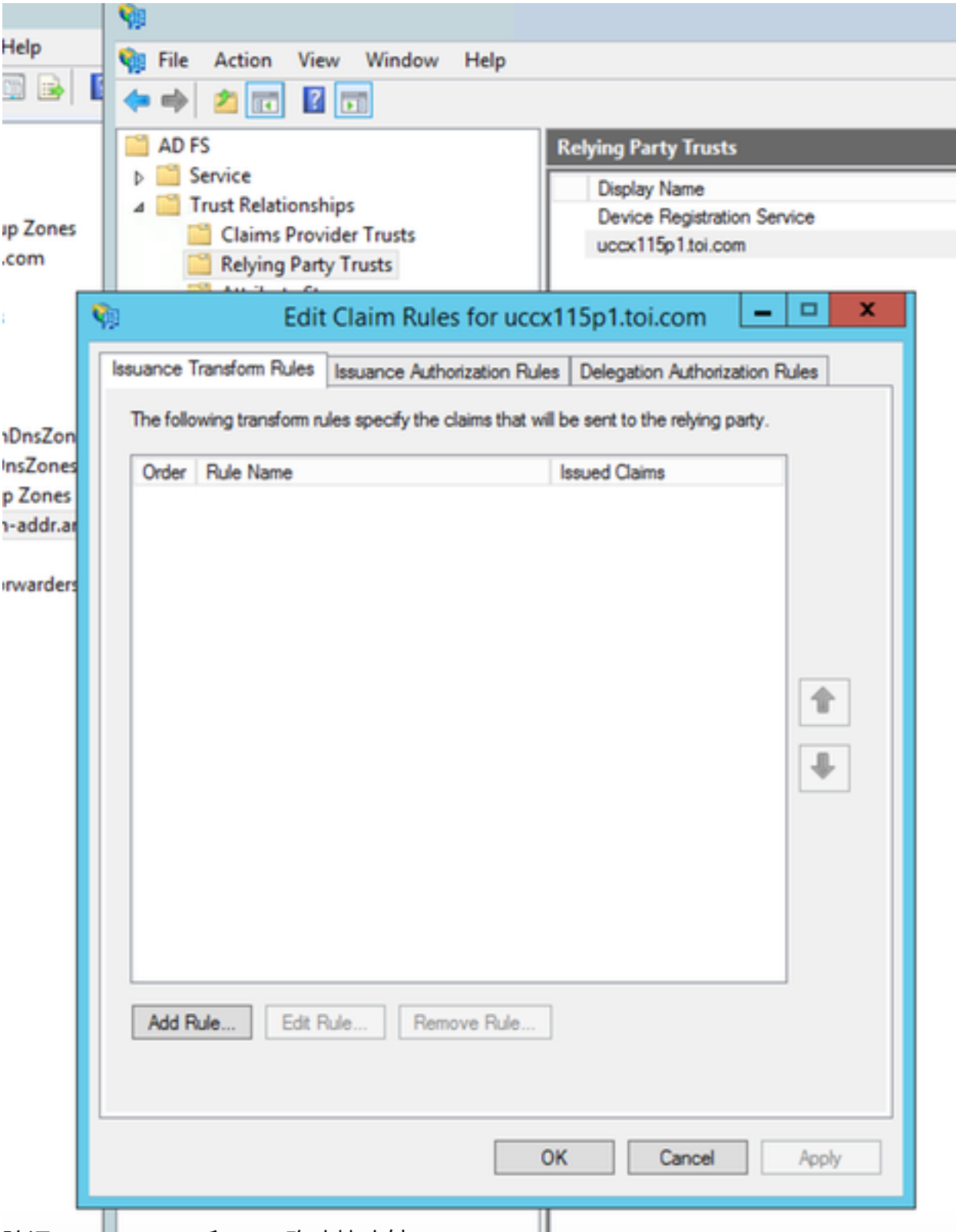
```
com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAMLExcep
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServle
```

可能的原因

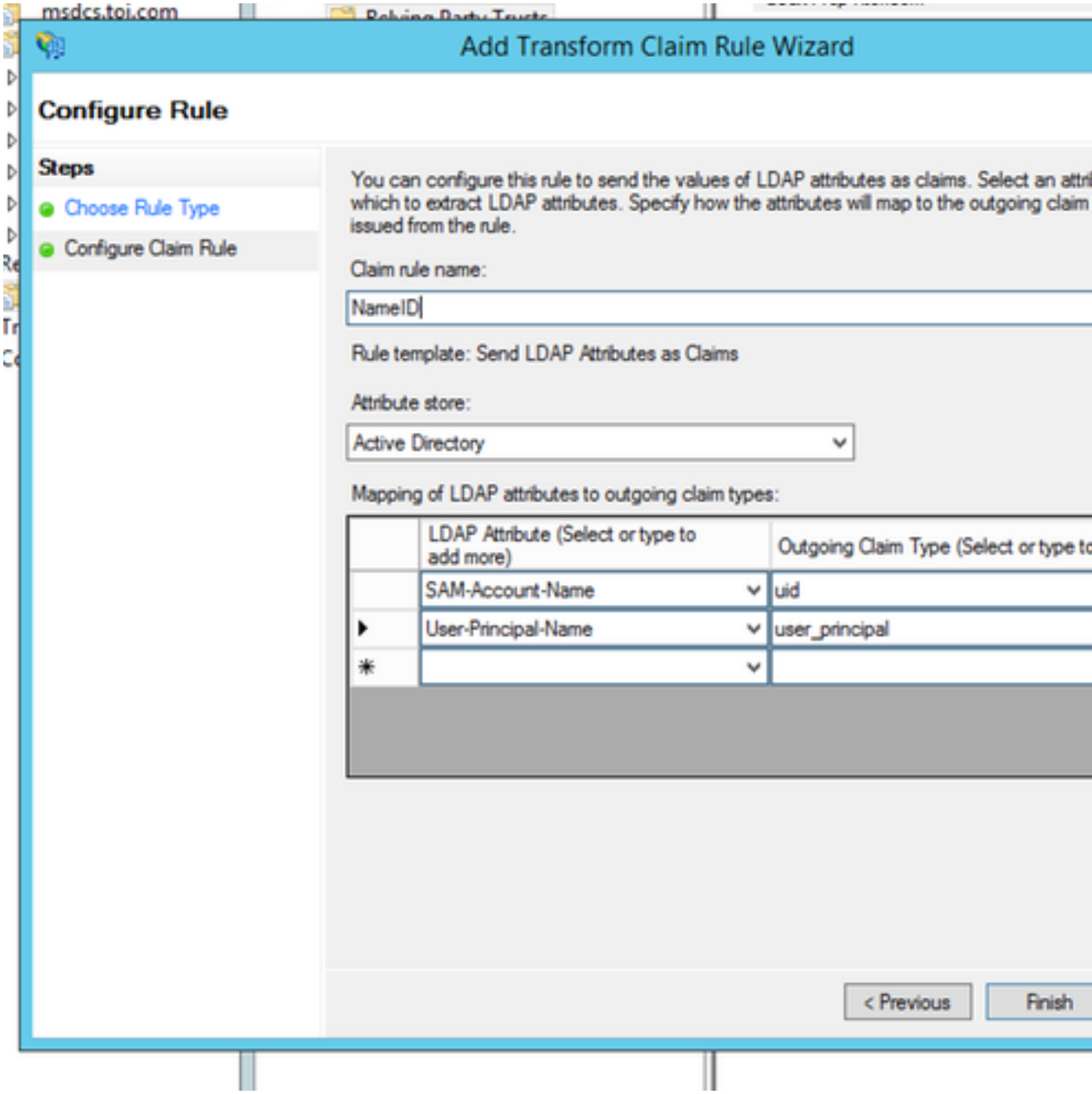
必须流出的要求(uid和user_principal)在声明规则没有正确地配置。
如果未配置NameID声明规则或uid或user_principal没有适当地配置。
如果NameID规则是没配置或user_principal没有正确地被映射， user_principal没有获取的Cisc
如果uid没有正确地被映射， Cisco IDS表明uid没有获取。
根据AD FS声明规则，请保证映射为“user_principal”和“uid的”属性定义作为在(指导？)的IdP配

1. AD FS系统的RDP。
2. 编辑取决于的当事人信任的声明规则。

建议操作



3. 验证user_principal和uid正确地被映射



5. 流出的声明规则在联盟的AD FS没有正确地配置

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答复的检索用户标识符的500。或者不
步骤失败	SAML答复处理

错误消息	**浏览器**
	500与此消息的错误：
	IdP配置错误：失败的SAML处理
	不可能从SAML答复的检索用户标识符。/不可能从SAML答复的检索用户负责人。
	AD FS事件查看器：
	无错误
	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中有可能未命中要求的更多配置。
建议操作	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**Federated AD FS的**配置Cisco I

6. 没正确地配置的自定义声明规则

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答复的检索用户标识符的500。/Coul
在流出的要求并且/或者user_principal没设置的uid。

步骤失败

SAML答复处理

浏览器

500与此消息的错误：

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

错误消息

AD FS事件查看器：

SAML认证请求有不可能是满足的一项NameID策略。

申请人：myids.cisco.com

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

SPNameQualifier ：myids.cisco.com

例外详细信息：

MSIS1000 ：SAML请求包含未由发出的标记满足的NameIDPolicy。请求的NameIDPolicy ：A
失败的此请求。

用户动作

请使用AD FS 2.0管理管理单元配置散发需要的命名标识符的配置。

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)
```

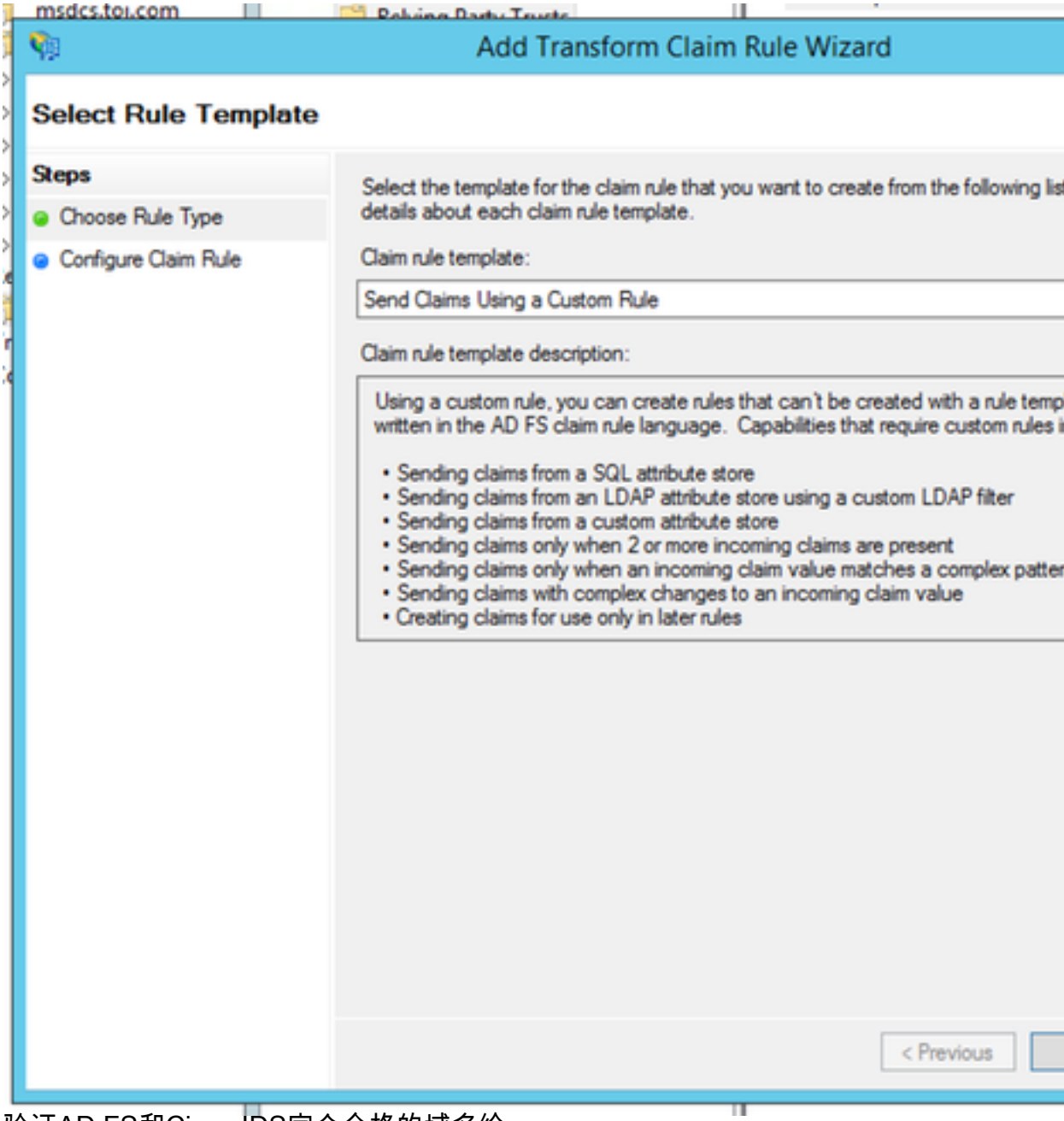
可能的原因

自定义声明规则没有正确地配置。

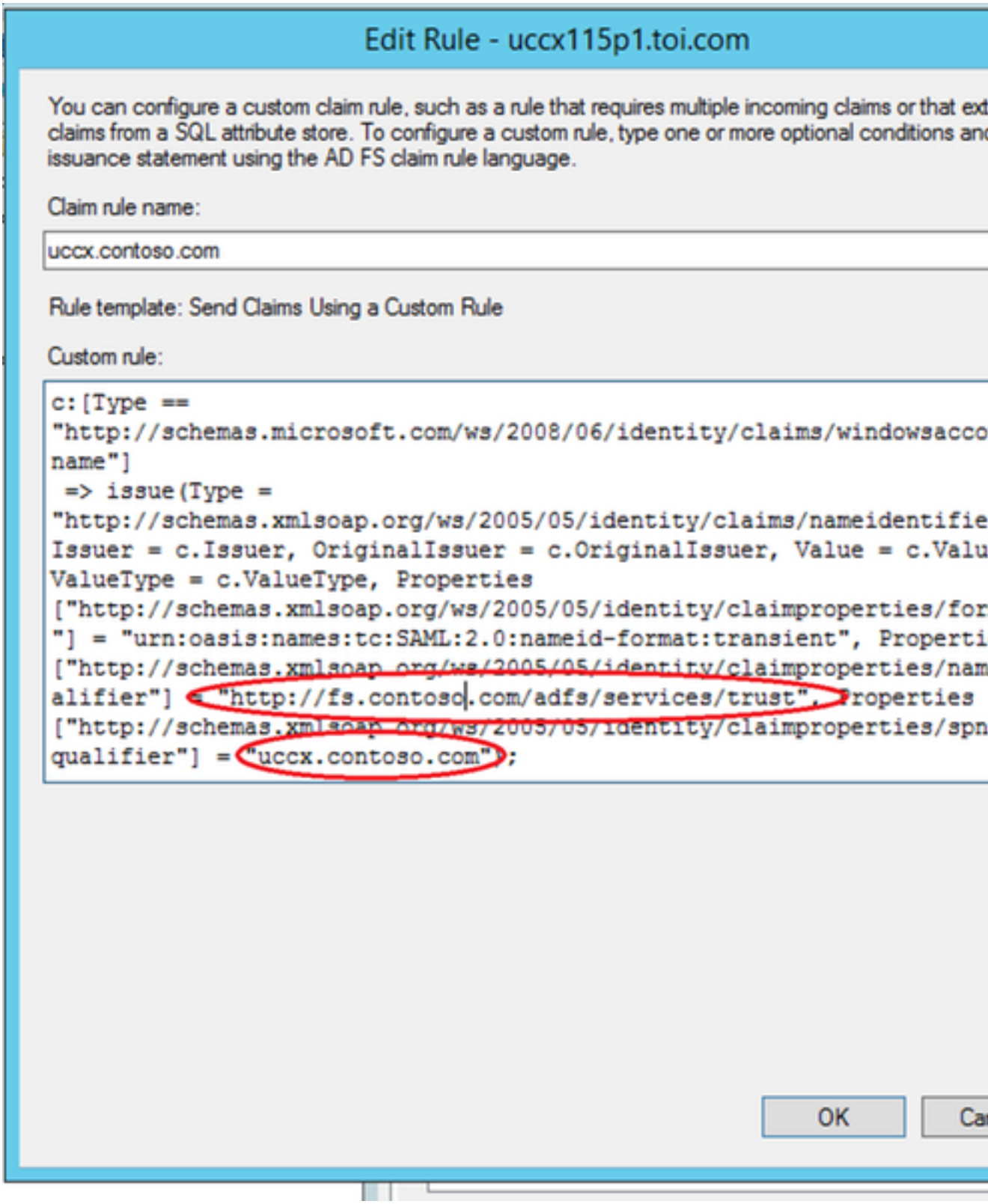
根据AD FS声明规则，请保证映射为“user_principal”和“uid的”属性定义作为在(指导？)的配置指

1. AD FS系统的RDP。
2. 编辑自定义声明规则的声明规则。

建议操作



3. 验证AD FS和Cisco IDS完全合格的域名给。



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的错误消息指示有许多请求对AD FS。
步骤失败	SAML答复处理
错误消息	**浏览器** 500与此消息的错误： IdP配置错误：失败的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事件查看器：** Microsoft.IdentityServer.Web.InvalidRequestException ：

MSIS7042 ：**同一客户端浏览器会话做了在的'6'请求持续**
'16'秒钟。有关详细信息，请联系您的管理员。
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的许多请求同一浏览器会话。
这在制作不应该典型地发生。但是，如果遇到此，您能：

建议操作

1. 检查AD FS Windows事件查看器。
2. 复校取决于的Party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. AD FS没有配置签署断言和消息。

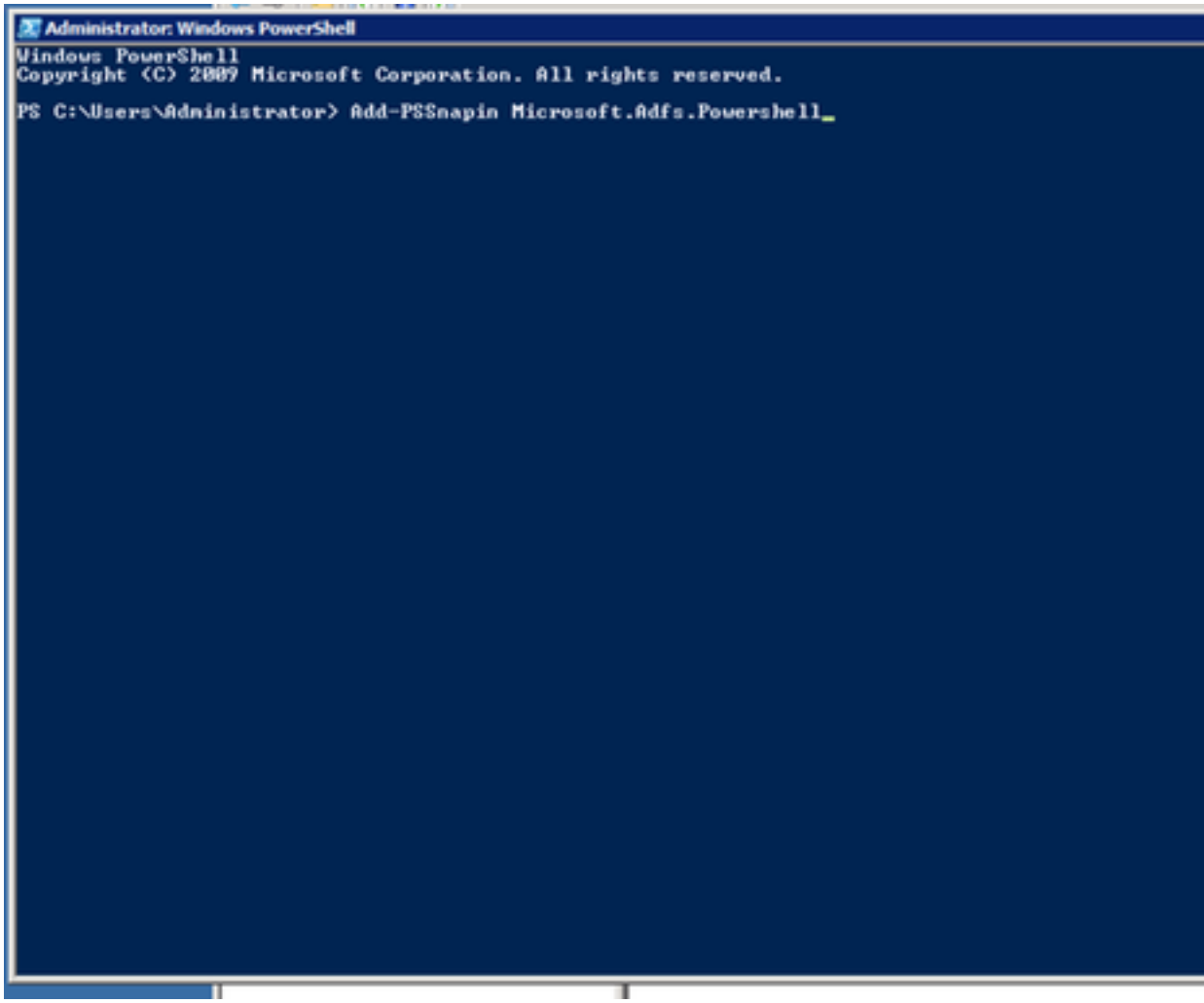
问题汇总 登录请求失效与500在浏览器的错误有错误代码的：invalidSignature
步骤失败 SAML答复处理
浏览器
500与此消息的错误：
错误代码:invalidSignature
错误消息 消息：无效签名在ArtifactResponse。
Cisco IDS日志：

```
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
```

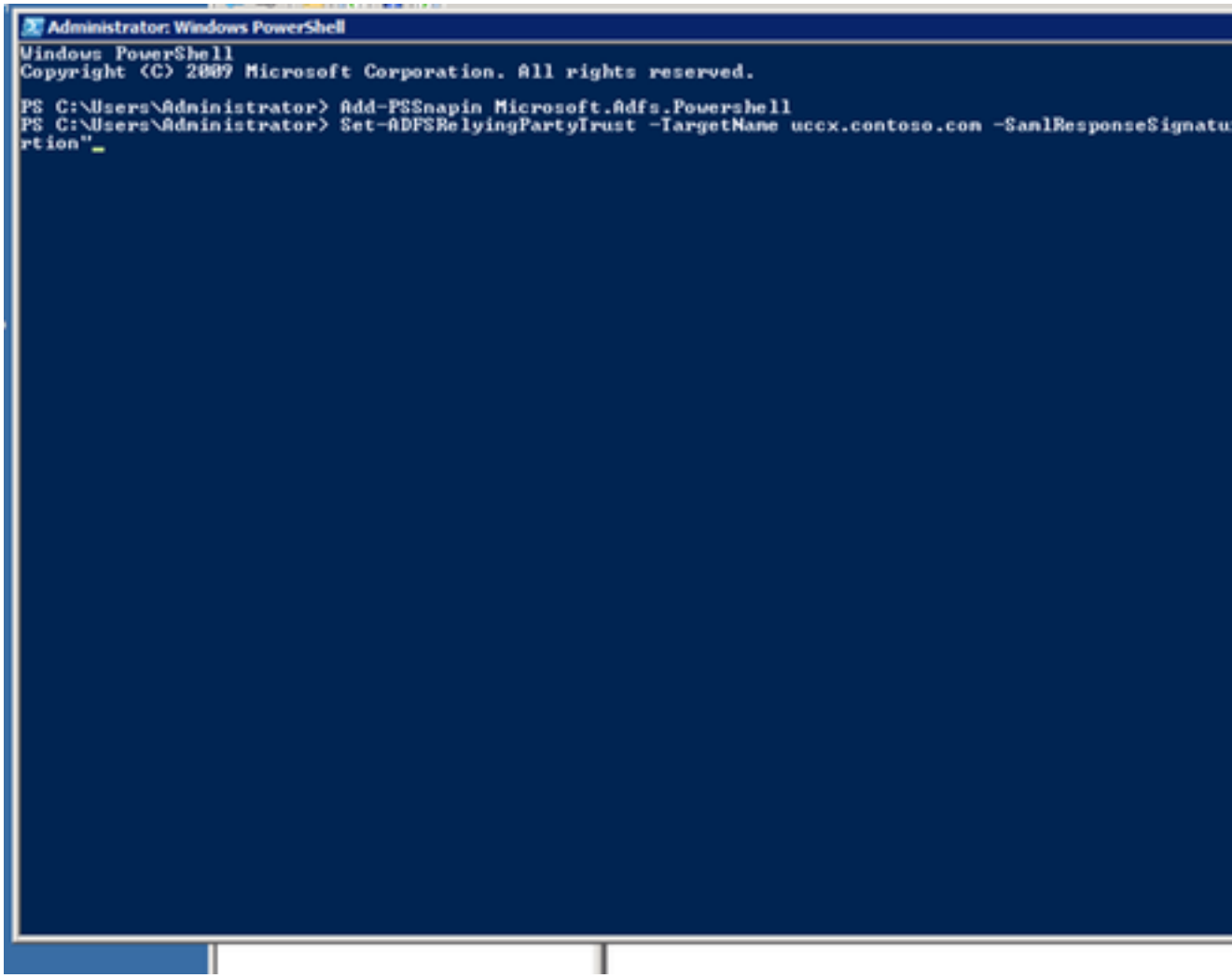
可能的原因 AD FS没有配置签署断言和消息。

建议操作

1. 运行AD FS powershell命令： **设置ADFSRelyingPartyTrust - TargetName <Relying的Pa**
2. AD系统的RDP。
3. 打开**Powershell**。
4. 添加Windows PowerShell SNAP INS到当前会话。此步骤不可以要求，如果使用ADFS 3



5. 添加取决于消息和断言的AD FS当事人信任。



相关信息

这与在条款涉及描述的标识供应商的配置：

- https://www.cisco.com/c/en/us/support/docs/customer-collaboration/unified-contact-center-express/200612-Configure-the-Identity-Provider-for-UCCX.html
- 技术支持和文档 - Cisco Systems