ADFS/IdS故障排除和常见问题

目录

简介

通过浏览器在思科身份服务(IdS)和Active Directory联合服务(AD FS)之间进行安全断言标记语言(SAML)交互是单点登录(SSO)登录流的核心。本文档将帮助您调试与Cisco IdS和AD FS中的配置相关的问题，以及建议的解决措施。

思科IDs部署模式

产品　部署

UCCX 同居
PCCE 与CUIC（思科统一情报中心）和LD（实时数据）共存
UCCE 与CUIC和LD共存，用于2000部署。
独立式，适用于4k和12k部署。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科统一联系中心快捷版(UCCX)11.5版或思科统一联系中心企业版11.5版或套装联系中心企业版(PCCE)11.5版（如果适用）。
- Microsoft Active Directory — 安装在Windows Server上的AD
- IdP（身份提供程序） — Active Directory联合身份验证服务(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Cisco IdS和AD FS之间建立信任关系后（请参阅此处了解详细信息，对于UCCX和UCCE是常见的），管理员应运行身份服务管理的“设置”页中的“测试SSO设置”，以确保Cisco IdS和AD FS之间的配置正常工作。如果测试失败，请使用本指南中提供的适当应用和建议来解决问题。

在调试中可以方便使用的应用程序和日志

应用/日志	详细信息	工具的查找位置
思科IdS日志	Cisco IdS记录器将记录在Cisco IdS中发生的任何错误。	使用RTMT获取 RTMT指南》 请注意，RTMT
Fedlet日志	Fedlet日志将提供有关在Cisco IdS中发生的任何SAML错误的更多详细信息	服务>日志 使用RTMT获取 Fedlet日志的位 fedlet日志以前
思科IdS API指标	API度量可用于查看和验证Cisco IdS API可能返回的任何错误以及由Cisco idS处理的请求数	使用RTMT获取 请注意，RTMT 这将显示在单独 authorize_metr
AD FS中的事件查看器	允许用户查看系统中的事件日志。处理SAML请求/发送SAML响应时AD FS中的任何错误都将记录在此处。	在AD FS计算机 >管理 在Windows 20 查看器” 在Windows 20 请查看您的窗口

SAML查看器	SAML查看器将帮助查看从/发送到思科IdS的SAML请求和响应。此浏览器应用程序对分析SAML请求/响应非常有用。

以下是一些建议
1. 菲德勒 如
2. SAML Tra
3. SAML Ch

带调试选项的流程图

SSO身份验证的各个步骤在映像中显示，并在每个步骤中调试假象，以防该步骤发生故障。

下表提供了如何在浏览器中识别SSO每个步骤的故障的详细信息。还指定了不同的工具以及它们如何帮助调试。

步骤	如何识别浏览器中的故障	工具/日志
按思科ID处理身份验证代码请求	如果失败，浏览器不会重定向到SAML终端或AD FS,Cisco IdS会显示JSON错误，表明客户端ID或重定向URL无效。	Cisco IdS日志 - 生的错误。 Cisco IdS API度
由思科IdS发起SAML请求	在故障期间，浏览器不会重定向到AD FS,Cisco IdS将显示错误页面/消息。	Cisco IdS日志 - Cisco IdS API度
AD FS处理SAML请求	如果处理此请求失败，将导致AD FS服务器显示错误页，而不是登录页。	AD FS中的事件 SAML浏览器插 。
由AD FS发送SAML响应	如果无法发送响应，则会在提交有效凭证后，AD FS服务器显示错误页面。	AD FS中的事件
由思科IdS处理SAML响应	Cisco IdS将显示500错误，错误原因和快速检查页。	AD FS中的事件 没有成功的状态 SAML浏览器插 ，以确定错误。 Cisco IdS日志 - Cisco IdS API度

按思科ID处理授权码请求

就思科ID而言，SSO登录的起点是从启用SSO的应用请求授权代码。API请求验证完成，以检查它是否来自注册客户端的请求。成功的验证会导致浏览器重定向到思科IdS的SAML终端。请求验证中的任何失败都会导致从Cisco IdS发回错误页/JSON（JavaScript对象表示法）。

此过程中遇到的常见错误

1.客户端注册未完成

问题汇总 登录请求失败，浏览器上出现401错误。

错误消息
浏览器：
401错误消息：{"error":"invalid_client","error_description":"Invalid ClientId."}
思科IDs日志：

```
2016-09-02 00:16:58.604 IST(+0530)[IdSEndPoints-51] WARN com.cisco.ccbu.ids IdSConfigImpl.ja
IdSOAuthEndPoint.java:45 — org.apache.oltu.oauth2.common.exception.OAuthProblemException:inv
com.cisco.ccbu.ids.auth.validator.validateRequestParams(Idator:55)org.apache.oltu.oauth2.as
```

可能的原因 使用思科ID的客户端注册尚未完成。
建议的操作 导航至Cisco IdS管理控制台，确认客户端是否注册成功。否则，请在继续SSO之前注册客户端

2.用户使用IP地址/备用主机名访问应用

问题汇总 登录请求失败，浏览器上出现401错误。

错误消息	**浏览器：** 401错误消息：{"error":"invalid_redirectUri","error_description":"Invlalid重定向URI"}
可能的原因	用户使用IP地址/备用主机名访问应用。 在SSO模式下，如果使用IP访问应用，则该应用不工作。应通过在Cisco IdS中注册的主机名访用。如果用户访问的备用主机名未注册到思科ID，则可能会发生此问题。
建议的操作	导航至Cisco IdS管理控制台，确认客户端是否注册了正确的重定向URL，并使用该URL访问应

由思科IdS发起SAML请求

思科IdS的SAML终端是基于SSO的登录中SAML流的起点。思科IdS和AD FS之间的交互在此步骤中触发。此处的前提条件是思科ID应知道要连接的AD FS，因为相应的IdP元数据应上传到思科ID才能成功执行此步骤。

此过程中遇到的常见错误

1. AD FS元数据未添加到思科ID

问题汇总	登录请求失败，浏览器上出现503错误。
错误消息	**浏览器：** 此消息为503错误：{"error":"service_unavailable","error_description":"SAML元数据未初始化"}
可能的原因	思科ID中不提供IDP元数据。思科ID和AD FS之间的信任建立尚未完成。
建议的操作	导航至Cisco IdS管理控制台，查看IdS是否处于“未**配置**”状态。 确认是否上载了IdP元数据。 否则，上传从AD FS下载的IdP元数据。 有关详细信息，请参阅此处。

AD FS处理SAML请求

SAML请求处理是SSO流中AD FS的第一步。思科IdS发送的SAML请求由AD FS在此步骤中读取、验证和破译。成功处理此请求会导致两种情况：

1. 如果是浏览器中的新登录，AD FS将显示登录表单。如果是已通过身份验证的用户从现有浏览器会话重新登录，AD FS会尝试直接发回SAML响应。

注意：此步骤的主要先决条件是AD FS配置了回复方信任。

此过程中遇到的常见错误

1. AD FS没有最新的Cisco IdS SAML证书。

问题汇总	AD FS不显示登录页，而是显示错误页。
错误消息	**浏览器** AD FS显示类似以下的错误页： 访问站点时出现问题。尝试再次浏览到该站点。 如果问题仍然存在，请与此站点的管理员联系，并提供参考号以确定问题。 参考编号：1ee602be-382c-4c49-af7a-5b70f3a7bd8e **AD FS事件查看器** 联合身份验证服务在处理SAML身份验证请求时遇到错误。 **其他数据**

```
Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException:MSIS0038
Microsoft.IdentityServer.Service.SamlProtocolService.CreateErrorMessage(CreateErrorRequestMi
```

可能的原因	信赖方信任未建立或思科IdS证书已更改，但不会将其上传到AD FS。 在AD FS和具有最新思科IdS证书的思科IdS之间建立信任。
建议的操作	请确保思科IDs证书未过期。您可以在思科身份服务管理中查看状态控制面板。如果是，请在“ 有关如何跨ADFS和思科IdS建立元数据信任的详细信息，请参阅，此处

AD FS发送SAML响应

在用户成功通过身份验证后，ADFS通过浏览器将SAML响应发送回Cisco IdS。ADFS可以发回SAML响应，并返回一个状态代码，该代码指示成功或失败。如果AD FS中未启用表单身份验证，则这将指示故障响应。

此过程中遇到的常见错误

1. AD FS中未启用表单身份验证

问题汇总	浏览器显示NTLM登录，然后在未成功重定向到思科ID的情况下失败。
故障步骤	发送SAML响应
错误消息	**浏览器：** 浏览器显示NTLM登录，但在成功登录后，它会失败，并会进行许多重定向。
可能的原因	思科ID仅支持基于表单的身份验证，AD FS中未启用表单身份验证。
建议的操作	有关如何启用表单身份验证的详细信息，请参阅： ADFS 2.0表单身份验证设置 ADFS 3.0表单身份验证设置

按思科IdS处理SAML响应

在此阶段，思科IdS从AD FS获取SAML响应。此响应可能包含指示成功或失败的状态代码。来自AD FS的错误响应会导致错误页，必须调试该错误页。

在成功的SAML响应期间，请求处理可能会因以下原因失败：

- IdP(AD FS)元数据不正确。
- 无法从AD FS检索预期的传出声明。
- 思科ID和AD FS时钟不同步。

此过程中遇到的常见错误

1.思科ID中的AD FS证书不是最新证书。

问题汇总	登录请求失败，浏览器上出现500错误，错误代码为invalidSignature。
故障步骤	SAML响应处理
错误消息	**浏览器：** 浏览器中出现500错误： 错误代码：无效签名 消息：签名证书与实体元数据中定义的内容不匹配。 **AD FS事件查看器：** 无错误 **思科IDs日志：**

```
2016-04-13 12:42:15.896 IST(+0530)[IdSEndPoints-0] com.cisco.ccbu.ids IdSEndPoint.java:102 -
s.s.s.s.2.profile.SPACSUtils.getResponseFromPost(SPASSUtils.java:985)com.sun.identity.saml2.
```

可能的原因 SAML响应处理失败，因为IdP证书与Cisco IdS中的可用证书不同。

建议的操作 从以下位置下载最新的AD FS元数据：**https://<ADFSServer>/federationmetadata/2007-06/fed**
并通过身份服务管理用户界面将其上传到思科ID。
有关详细信息，请参阅[配置思科ID和AD FS]

2.思科ID和AD FS时钟不同步。

问题汇总 登录请求失败，浏览器上出现500错误，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Su

故障步骤 SAML响应处理

浏览器：
此消息为500错误：
IdP配置错误：SAML处理失败
SAML断言从IdP失败，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Success。验证IdP配

错误消息

思科IDs日志

```
2016-08-24 18:46:56.780 IST(+0530)[IdSEndPoints-SAML-22] ERROR com.cisco.ccbu.ids IdSSAMLAsy
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServle
```

SAML查看器：
查找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 思科IdS和IdP系统中的时间不同步。

建议的操作 同步思科ID和AD FS系统中的时间。建议使用NTP服务器同步AD FS系统和思科ID。

3. AD FS中的错误签名算法（SHA256与SHA1）

问题汇总 登录请求失败，浏览器上出现500错误，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Re
AD FS事件视图日志中的错误消息 — AD FS中的错误签名算法（SHA256与SHA1）

故障步骤 SAML响应处理

浏览器
此消息为500错误：
IdP配置错误：SAML处理失败
SAML断言从IdP失败，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Responder。验证Id

错误消息

AD FS事件查看器：
SAML请求未使用预期签名算法签名。SAML请求使用签名算法http://www.w3.org/2001/04/xml
预期签名算法为http://www.w3.org/2000/09/xmldsig#rsa-sha1

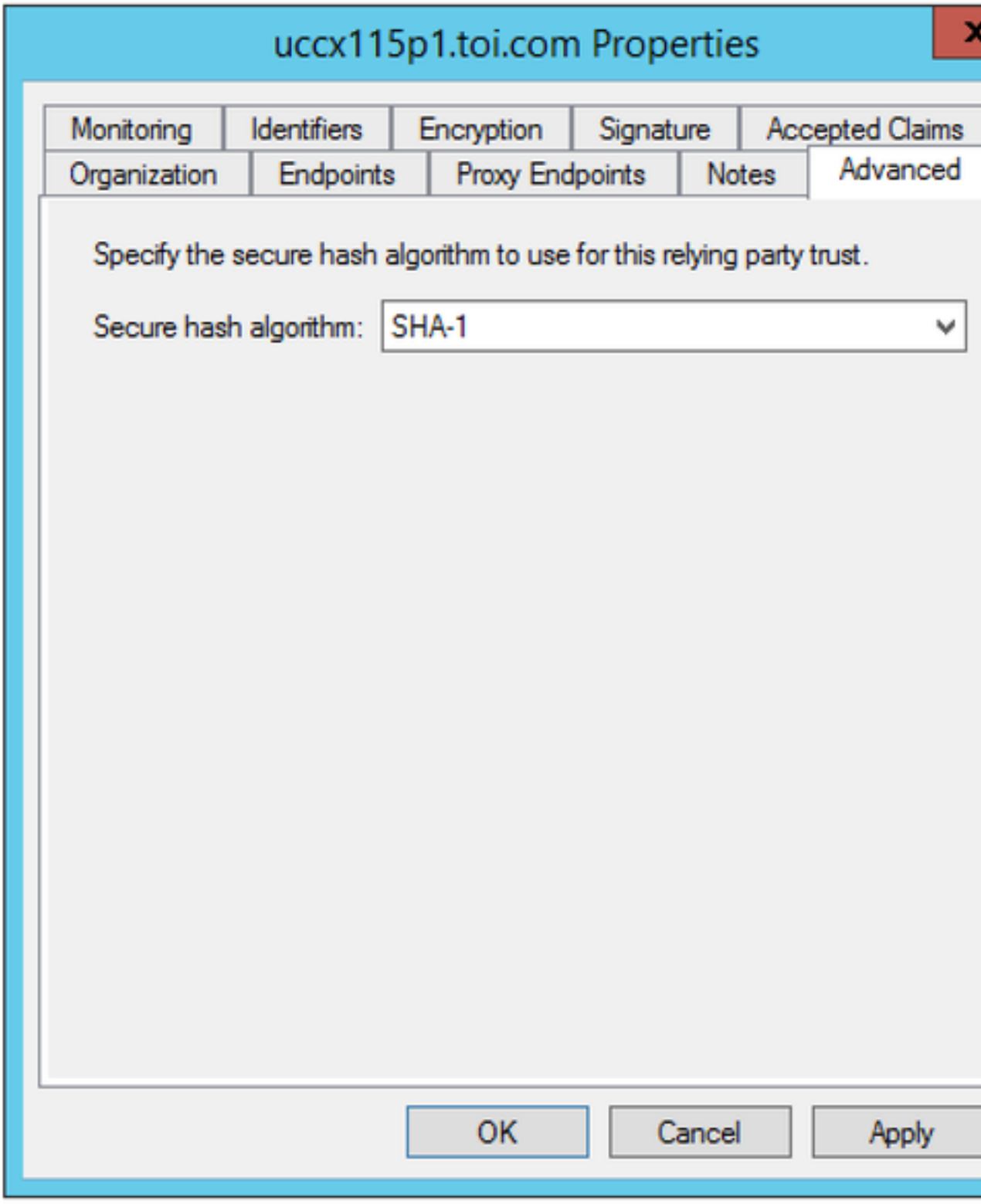
思科IDs日志：

```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:298 - SAMLcom.sun.identity.saml2.common.SA
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn
```

可能的原因 AD FS配置为使用SHA-256。

建议的操作
更新AD FS以使用SHA-1进行签名和加密。

1. RDP到AD FS系统。
2. 打开AD FS控制台。
3. 选择信赖**方信任并**单击**属性**
4. 选择**Advanced 选项卡。**
5. 从下拉列表中选择SHA-1。



4.传出领款申请规则配置不正确

问题汇总	登录请求失败，浏览器上出现500错误，消息为“Could not retrieve user identifier from SAML r uid和/或user_principal未在传出声明中设置。
故障步骤	SAML响应处理
错误消息	**浏览器：** 此消息为500错误： IdP配置错误：SAML处理失败。 无法从SAML响应检索用户标识符。/无法从SAML响应检索用户主体。 **AD FS事件查看器：** 无错误

思科IDs日志：

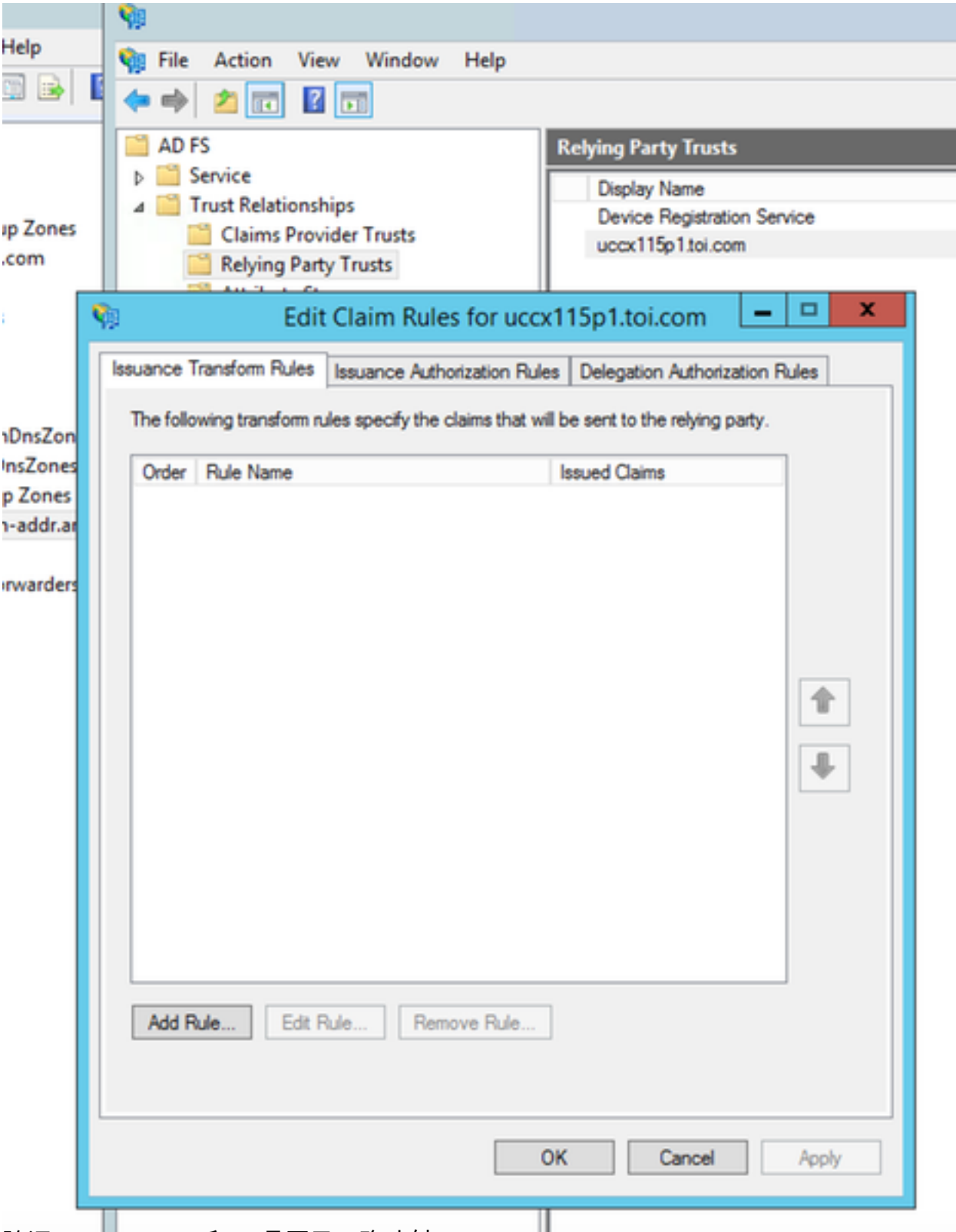
```
ERROR com.cisco.ccbu.ids IdSSAMLAsyncServlet.java:294 - SAMLcom.sun.identity.saml.common.SAM
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.processIdSEndPointRequest(IdSSAMLAsyncServle
```

可能的原因

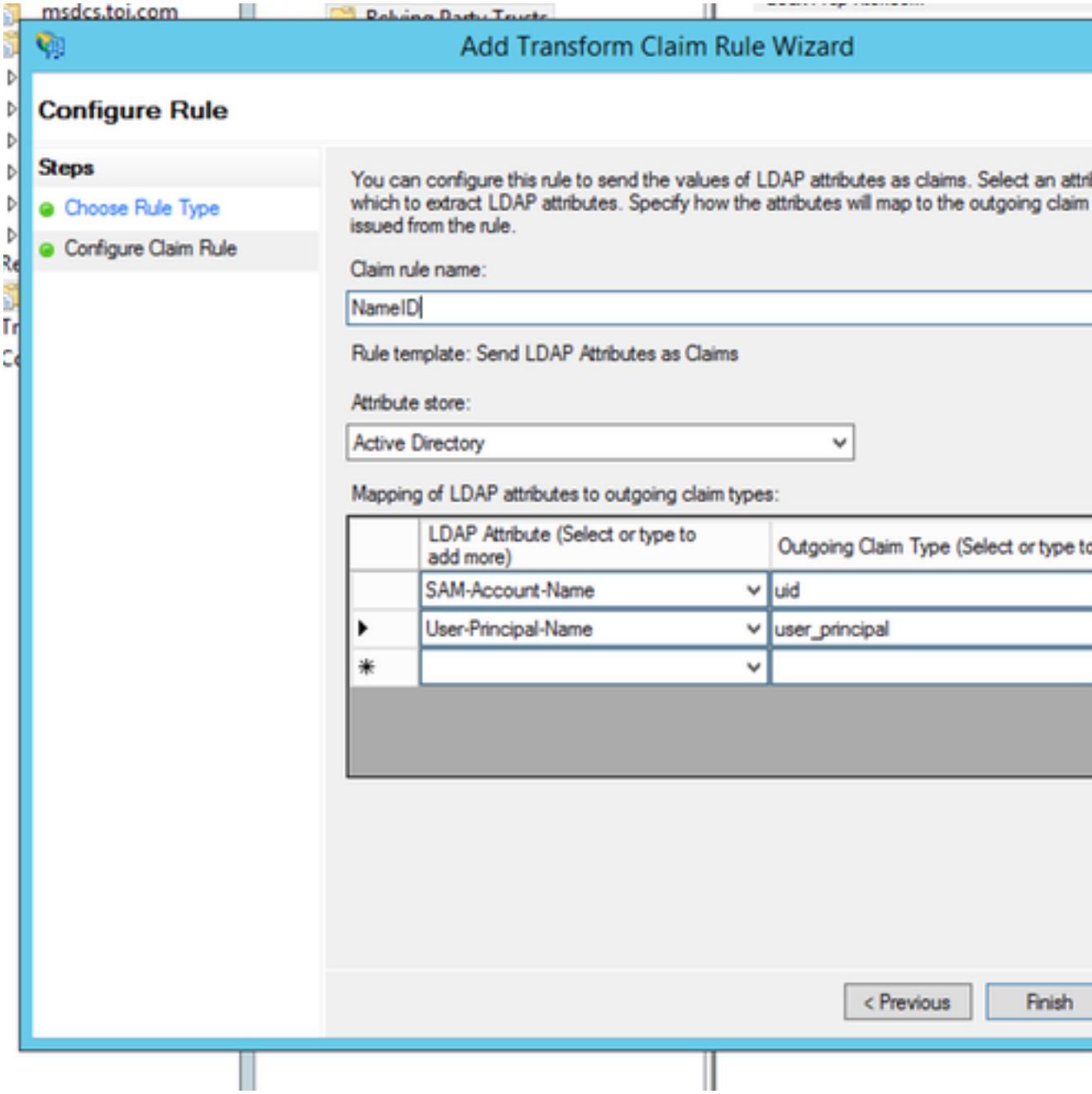
声明规则中未正确配置强制传出声明（uid和user_principal）。
如果尚未配置NameID声明规则，或者uid或user_principal未正确配置。
如果未配置NameID规则或userprincipal映射不正确，则思科ID表示未检索userprincipal，因为
如果uid映射不正确，思科IDS表示未检索uid。
在AD FS声明规则下，确保“user_principal”和“uid”的属性映射按照《IdP配置指南》（哪本指南

1. RDP到AD FS系统。
2. 编辑信赖方信任的领款申请规则。

建议的操作



3. 验证user_principal和uid是否已正确映射



5.联合AD FS中未正确配置传出声明规则

问题汇总 登录请求失败，浏览器上出现500错误，并显示消息“Could not retrieve user identifier from SA

故障步骤 SAML响应处理

浏览器

此消息为500错误：

IdP配置错误：SAML处理失败

无法从SAML响应检索用户标识符。/无法从SAML响应检索用户主体。

错误消息 **AD FS事件查看器：**

无错误

思科IDs日志：

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

可能的原因 在联合AD FS中，需要的配置可能会丢失。

建议的操作 检查联合AD中的AD FS配置是否按照配置**Cisco IdS和AD FS中的联合AD FS的多域配置**一节完

6.自定义声明规则配置不正确

问题汇总

登录请求失败，浏览器上出现500错误，消息为“Could not retrieve user identifier from SAML r
uid和/或user_principal未在传出声明中设置。

故障步骤

SAML响应处理

浏览器

此消息为500错误：

SAML断言从IdP失败，状态代码为：urn:oasis:names:tc:**SAML:2.0:status:Requester/urn:oasis**

AD FS事件查看器：

SAML身份验证请求具有无法满足的NameID策略。

申请人：myids.cisco.com

名称标识符格式：urn:oasis:names:tc:SAML:2.0:nameid-format:transient

错误消息

SPNameQualifier:myids.cisco.com

例外详细信息：

MSIS1000:SAML请求包含未被颁发的令牌满足的NameIDPolicy。请求的NameIDPolicy:允许创
此请求失败。

用户操作

使用AD FS 2.0管理管理单元配置发出所需名称标识符的配置。

思科IDs日志:

```
2016-08-30 09:45:30.471 IST(+0530)[IdSEndPoints-SAML-82] INFO com.cisco.ccbu.idsSPAdapter.ja
Value="urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy"> </samlp:StatusCode>samlp:Sta
com.sun.identity.saml2.common.SAML2Exception:com.sun.identity.saml2.common.SAML2Utils.verify
```

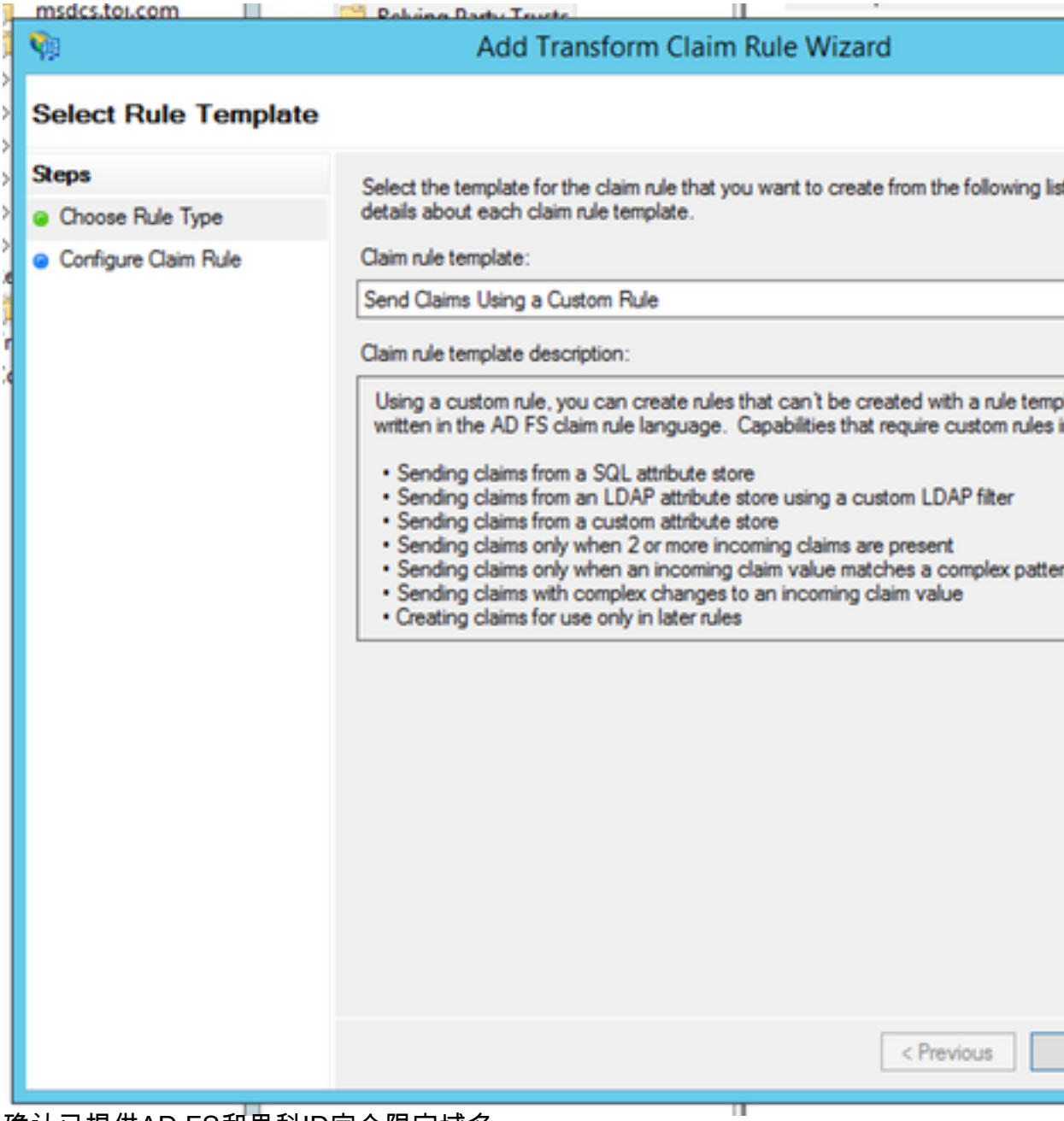
可能的原因

自定义声明规则配置不正确。

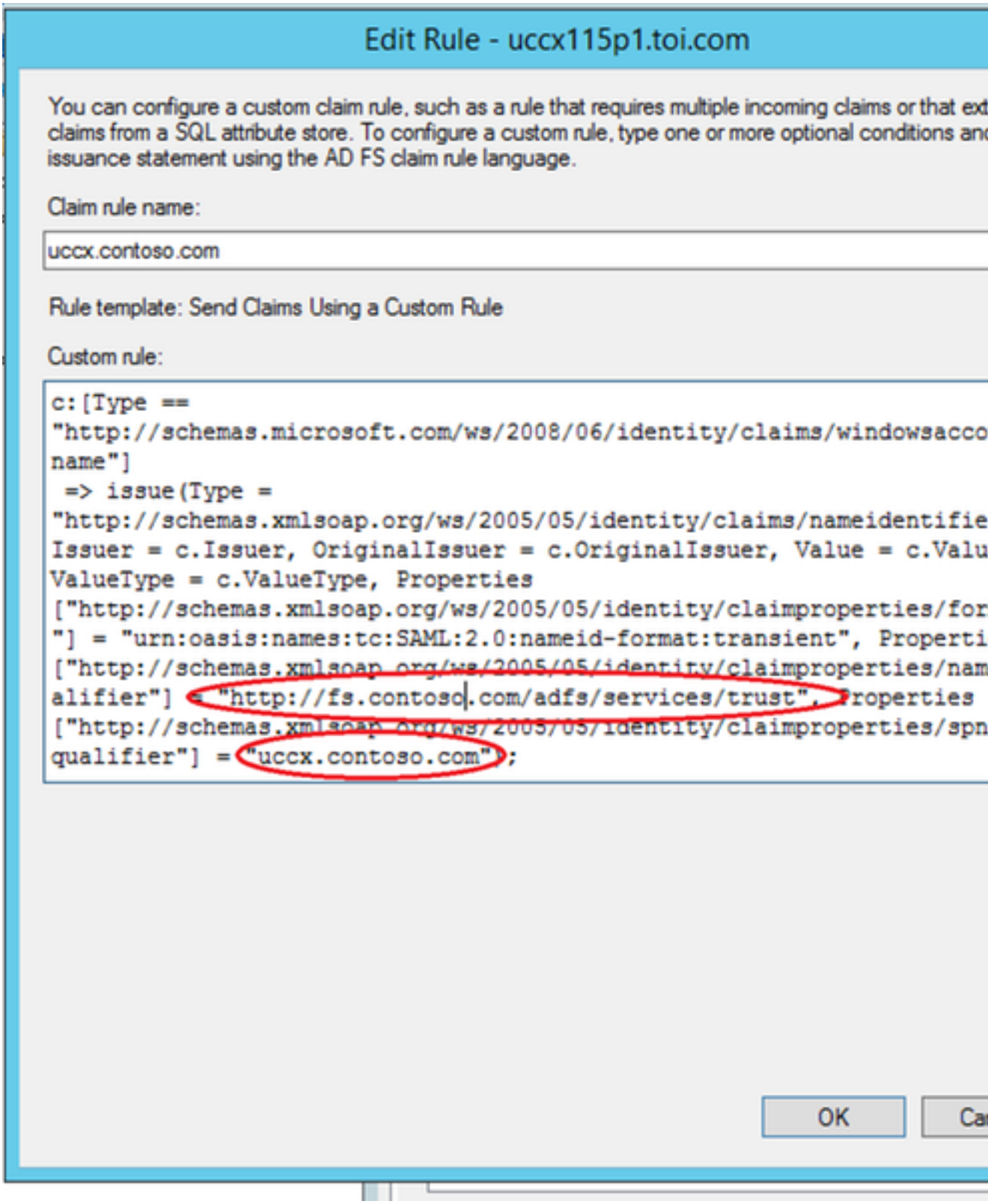
在AD FS声明规则下，确保“user_principal”和“uid”的属性映射按照配置指南（哪个指南？）中的

1. RDP到AD FS系统。
2. 编辑自定义声明规则的声明规则。

建议的操作



3. 确认已提供AD FS和思科ID完全限定域名。



7.向AD FS提出的请求太多。

问题汇总	登录请求失败，浏览器上出现500错误，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Re AD FS事件视图日志中的错误消息表示向AD FS发出的请求过多。
故障步骤	SAML响应处理
错误消息	**浏览器** 此消息为500错误： IdP配置错误：SAML处理失败 SAML断言从IdP失败，状态代码为：urn:oasis:names:tc:SAML:2.0:status:Responder。验证Id **AD FS事件查看器：** Microsoft.IdentityServer.Web.InvalidRequestException:

MSIS7042:**同一客户端浏览器会话在上一个**
16秒。有关详细信息，请联系您的管理员。
at Microsoft.IdentityServer.Web.FederationPassiveAuthentication.UpdateLoopDetectionCoo
在Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse（M

```
XML:<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event"> <System> <Provider
<EventRecordID>29385</EventRecordID> <Correlation ActivityID="{98778DB0-869A-4DD5-B3B6-0565A
ns2="http://schemas.microsoft.com/win/2004/08/events" xmlns="http://schemas.microsoft.com/Ac
Microsoft.IdentityServer.Web.FederationPassiveAuthentication.SendSignInResponse(MSISSignInRe
```

思科IDs日志

```
2016-04-15 16:19:01.220 EDT(-0400)[IdSEndPoints-1] com.cisco.ccbu.ids IdSEndPoint.java:102 -
com.cisco.ccbu.ids.auth.api.IdSSAMLAsyncServlet.getAttributesMapFromSAMLResponse(IdSSAMLAsyn
```

可能的原因 从同一浏览器会话进入AD FS的请求太多。
这在生产中通常不会发生。但是，如果遇到这种情况，您可以：

建议的操作

1. 选中AD FS Windows事件查看器。
2. 重新选中信赖方信任设置。有关详细信息，*请参阅*配置思科ID和AD FS
3. 重新登录。

8. AD FS未配置为同时签署断言和消息。

问题汇总 登录请求失败，浏览器上出现500错误，错误代码：invalidSignature

故障步骤 SAML响应处理

浏览器

错误消息
此消息为500错误：
错误代码：invalidSignature
消息：ArtifactResponse中的签名无效。

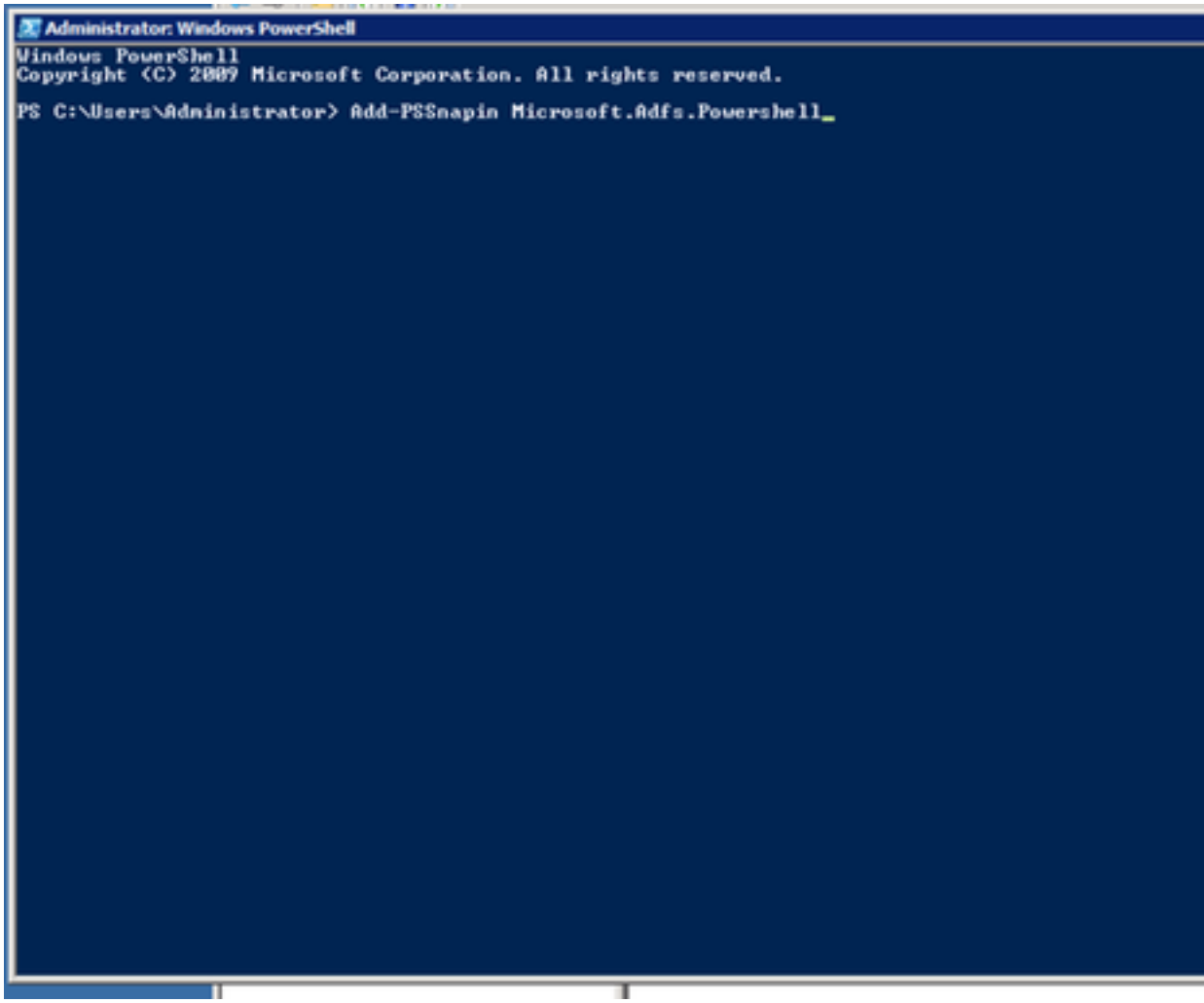
思科IDs日志：

```
2016-08-24 10:53:10.494 IST(+0530)[IdSEndPoints-SAML-241] INFO saml2error.saml2error_jsp.jav
com.sun.identity.saml2.profile.SPASSUtils.getResponse(SPASSUtils.java:196)com.sun.identity.i
```

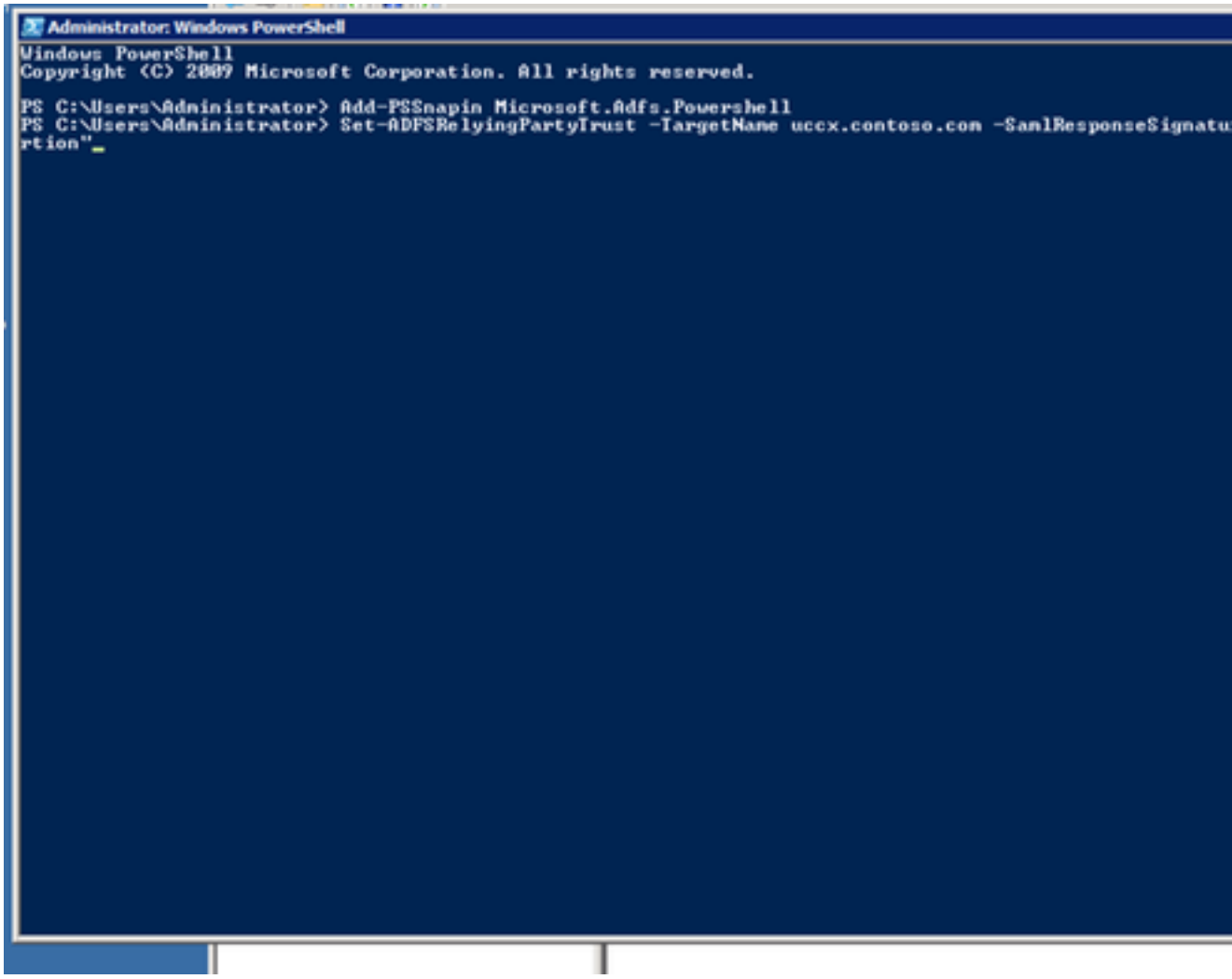
可能的原因 AD FS未配置为同时签署断言和消息。

建议的操作

1. 运行AD FS powershell命令:**Set-ADFSRelingPartyTrust -TargetName <Reling Party Trus**
2. RDP到AD系统。
3. 打开**Powershell**。
4. 将Windows PowerShell管理单元添加到当前会话。如果您使用ADFS 3.0，则中可能不需



5. 为消息和断言添加AD FS信赖方信任。



相关信息

这与本文所述的身份提供程序的配置相关：

- 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