

排除UCCE SSO与Azure IdP集成的故障

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[问题：证书不匹配](#)

[解决方案](#)

[问题：AADSTS900235 — 身份验证环境问题](#)

[解决方案](#)

[问题：SAML响应未签名](#)

[解决方案](#)

[问题：索赔规则问题](#)

[解决方案](#)

[问题：AADSTS50011 — 回复URL不匹配](#)

[解决方案](#)

简介

本文档介绍如何解决与Microsoft Azure IdP进行UCCE SSO集成时面临的一些常见问题。

作者：Anurag Atul Agarwal，思科TAC工程师。

先决条件

要求

Cisco 建议您了解以下主题：

- [安全断言标记语言\(SAML\)2.0](#)
- [Cisco Unified/Packaged Contact Center Enterprise UCCE/PCCE](#)
- [单点登录\(SSO\)](#)
- [思科身份服务\(IdS\)](#)
- [身份提供程序\(IdP\)](#)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Azure IdP

- UCCE 12.0.1
- 思科IdS 12.0.1

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍在集成基于Azure的SSO的思科身份服务(IdS)和身份提供程序(IdP)期间面临的一些常见问题及其可能的修复。始终建议收集以下日志以排除SSO集成问题：

- Cisco IdS日志：收集链接：[IDS日志](#)
- 浏览器控制台日志
- 来自IdP的任何日志

问题：证书不匹配

测试SSO失败，并显示消息“IdS was unable to process the SAML response when the authentication was successful”，并且IdS日志打印错误消息：“SAML response processing failed with exception com.sun.identity.saml2.common.SAML2Exception: The signing certificate does not match the defined in the entity metadata”

解决方案

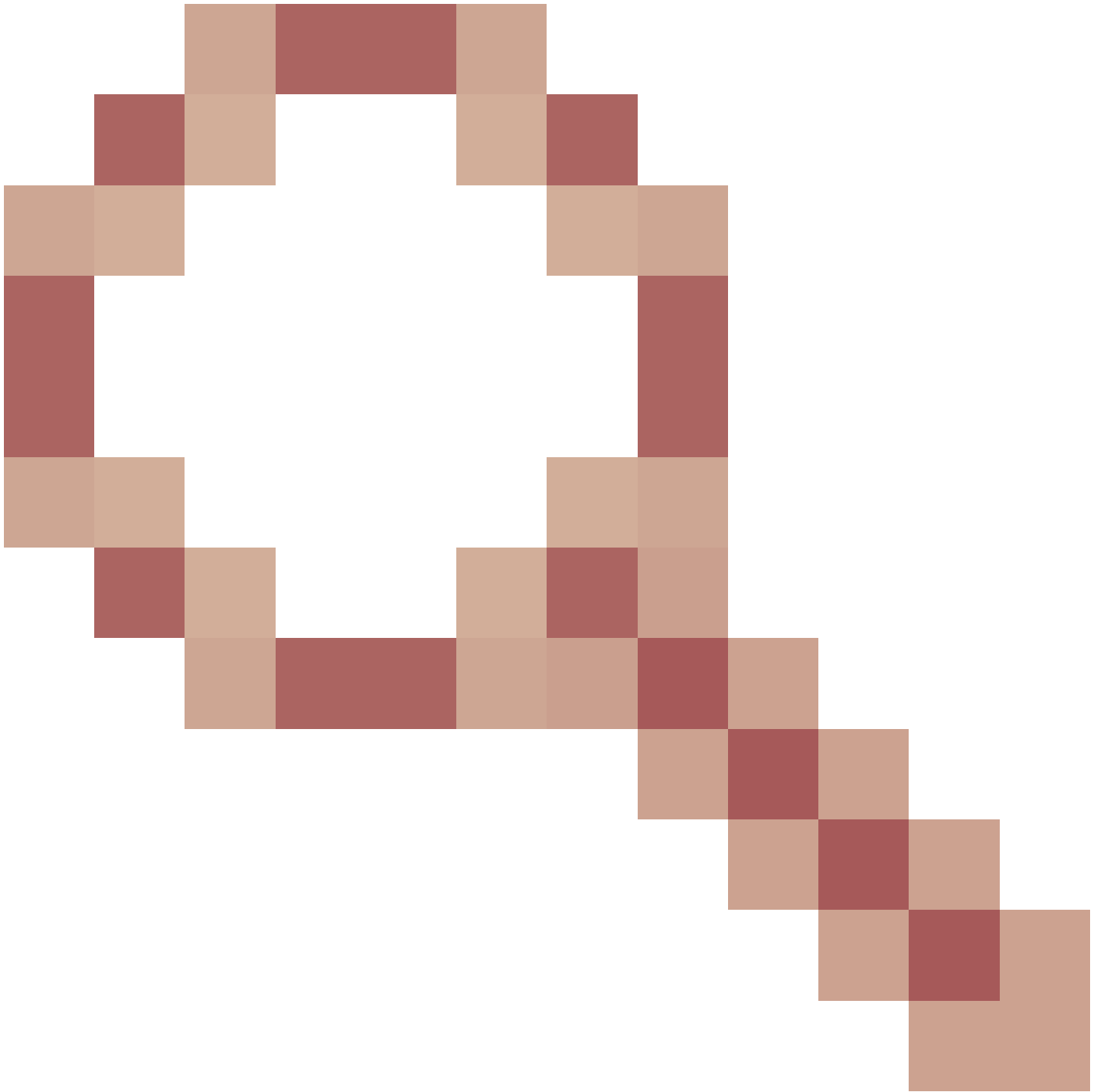
在Azure中验证证书并设置签名算法。确保它与基于IdS版本的支持哈希算法匹配。请参阅[功能指南](#)中的单点登录一章，并验证受支持的安全散列算法。下载最新的IdP元数据文件，并通过身份服务管理用户界面将其上传到Cisco IdS。

问题：AADSTS900235 — 身份验证环境问题

测试SSO重定向到Microsoft页面，失败并显示以下消息：“很抱歉，您登录时遇到问题。”
AADSTS900235:SAML身份验证请求的RequestedAuthenticationContext Comparison值必须是Exact。接收值：最小

解决方案

可能需要按照Bug [CSCvm](#)中所述调整AuthContext[69290](#)



.请联系Cisco TAC以使用IdS执行解决方法。

问题：SAML响应未签名

测试SSO失败，并显示消息，IdS无法处理SAML响应，即使，身份验证成功'，并且IdS日志打印错误消息：“SAML响应处理失败，异常com.sun.identity.saml2.common.SAML2Exception：响应未签名。”

解决方案

Azure IdP需要将签名声明发送到IdS。 修改Azure设置以具有签名选项：对SAML响应和断言签名

问题：索赔规则问题

测试SSO失败，并显示消息“IdP配置错误：SAML处理失败。无法从SAML响应检索用户主体。”和IdS日志打印错误消息：“SAML响应处理失败，异常
com.sun.identity.saml.common.SAMLException：无法从SAML响应检索用户主体。”

解决方案

此错误指向Azure中配置的“声明名称”错误。其他属性（如UID、NameID等）可能会出现这种情况，并生成具有不同属性名称的类似错误。若要解决此问题，请在Azure中找到“schemas.xmlsoap.org/ws/2005/05/identity/claims/<attribute_name>”格式的任何属性。删除实际属性名称之前的所有内容。

本节提供功能指南中需要在Azure中复制的ADFS的示例配置。

[ADFS配置示例](#)

问题：AADSTS50011 — 回复URL不匹配

测试SSO重定向到Microsoft页面，失败并显示以下消息：“很抱歉，您登录时遇到问题。
AADSTS50011：请求中指定的回复URL与为应用“ ”配置的回复URL不匹配

解决方案

请与思科TAC联系。“Assertion Consumer Service”参数需要在此失败的IdS节点上签入根目录。如果参数正确，Microsoft Azure必须对此进行故障排除。

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。