配置ISE 2.1有PingFederate SAML SSO的访客门户

目录

简介

本文描述如何配置思科身份服务引擎(ISE)版本2.1为了为访客门户用户提供单个符号On(SSO)功能通过安全断言标记语言(SAML)。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科身份服务引擎访客服务。
- 关于SAML SSO的基础知识。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科身份服务引擎版本2.1
- PingFederate从Ping标识的8.1.3.0服务器作为SAML标识Provider(IdP)

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。如果您的网络实际，请确保您了解应用的所有配置潜在影响。

流概述

SAML是交换的认证和授权数据一个基于XML的标准在安全域之间。

SAML规格定义了三个角色：首席(来宾用户)，标识供应商[IdP] (IPing联合的服务器)和服务提供商[SP] (ISE)。

在典型SAML SSO流， SP从IdP请求并且获取标识断言。凭此结果， ISE可进行政策决策，当IdP能包括可配置属性ISE能使用(即关联的组和电子邮件地址对AD对象)。

此用例的预计流

1. 无线局域网控制器(WLC)或接入交换机为一个典型的中央Web验证(CWA)流配置。

   提示：查找CWA流的配置示例在相关信息部分在条款的底部。

2. 客户端连接，并且会话得到验证ISE。网络访问Device(NAD)运用ISE (AVPs)返回的重定向属性值对(url-redirect-acl和url重新定向)。

3. 客户端打开浏览器，生成HTTP或HTTPS流量，并且重新定向到艾斯的访客门户。

4. 一旦在门户客户端能输入以前已分配访客凭证(**赞助商创建**)和赛弗提供一个新的访客帐户或使用其AD凭证登陆(**员工洛金**)将提供单个在功能签字通过SAML。

5. 一旦用户选择“员工洛金”的选项， ISE验证，如果有一活动断言关联对此客户端浏览器会话IdP。如果没有激活的会话， IdP将强制执行用户登录。在此步骤用户在IdP门户将被提示直接地进入AD凭证。

6. IdP通过LDAP验证用户，并且创建将坚持运行在可配置时间的一新的断言。

   注意：联合默认情况下的Ping应用**会话超时**60分钟(这意味着，如果没有从ISE的SSO登录请求在60分钟之内在最初的验证以后会话删除)和480分钟**会话最大值超时**(即使IdP接收从ISE的不变SSO登录请求会话在8个小时将超时)的此用户的。

只要断言会话是活跃的，员工将体验SSO，当他使用访客门户。一旦会话时间，新用户验证将由IdP强制执行。

配置

此部分讨论配置步骤集成与联合的Ping的ISE和如何启用访客门户的浏览器SSO。

注意：虽然多种选项和可能性存在，当您验证来宾用户，不是所有的组合在本文描述。然而，此示例提供您必要的信息知道如何修改示例成您要达到的准确的配置。

步骤1.准备ISE使用外部SAML标识供应商

1. 在思科ISE，请选择**Administration >身份管理>外部标识来源> SAML Id供应商**。
2. 单击 **Add**。
3. 在**Genaral**选项卡下，请输入**Id运营商名称**。单击 **Save**。 配置的其余在需要从在最新步骤的IdP导入的此部分的依靠元数据。

步骤2.配置访客门户使用外部标识供应商

1. 选择**工作区>访客访问>配置>访客门户。**
2. 创建一新门户并且选择赛弗**注册的访客门户**。

   注意：这不会是该主要的门户用户体验，然而将呼应以IdP为了验证会话状态的subportal。此门户呼叫SSOSubPortal。

3. 展开**门户设置**并且选择**认证方法的PingFederate。**

4. 从**标识来源顺序，**以前请选择外部SAML IdP defined(PingFederate)。

5. 扩展**Acceptable Use Policy(AUP)**和POST**洛金班纳页定位**部分并且禁用两个。

   门户流是：

6. 保存更改。

7. 使用赛弗**注册的访客门户**选项，去上一步访客门户并且创建新的**。**

   注意：这主要的门户可视给客户端。主要的门户将使用SSOSubportal作为ISE和IdP之间的一个接口。 此门户呼叫PrimaryPortal。

8.展开**洛金页定位**并且选择**SSOSubPortal**以前创建下面"**允许将用于登录以下标识供应商访客门户**"。

9. 展开**可接受的使用规定AUP和POST洛金班纳页定位**并且不选定他们。

   这时门户流如下所示: :

10. 选择**门户自定义>页>洛金。**您应该当前有选项定制**代替洛金选项**(图标，文本，等等)。

    注意：注意那在右侧，在门户预览下，另外的Login选项可视。

11. 单击 **Save。**

    现在两个门户出现在访客门户列表下。

步骤3.配置PingFederate作为ISE访客门户的标识供应商

1. 在ISE，请选择**Administration >身份管理>外部标识来源> SAML Id供应商> PingFederate**并且点击**服务提供商资讯台。**
2. 在**出口服务提供商资讯台下，请**点击**出口。**

3. 保存并且抽出生成的压缩文件。包含的XML文件此处用于创建在PingFederate的配置文件在最新步骤。

注意：从这时起，本文包括PingFederate配置。此配置是同样为多种解决方案类似赞助商门户、MyDevices和BYOD门户。(那些解决方案在此条款没有报道)。

4. 打开PingFederate admin门户(典型地https://ip:9999/pingfederate/app)。

5. 在**IdP Configuration选项> SP Connections部分下请**选择**创建新**。

6. 在**连接类型下，其次请**单击**。**

7. 在**连接选项下，其次请**单击**。**

8. 在**导入元数据下**，请点击**File单选按钮**，单击**选择文件**并且从ISE选择以前导出的XML文件。

9.Under**元数据摘要**，**其次**单击。

10.On一般信息页，在连接名下，回车名称(例如ISEGuestWebAuth)和**其次**单击。

11. 在**浏览器SSO下，请**单击**配置浏览器SSO**和在**SAML配置文件**检查下选项并且**其次**单击。

12.On**断言寿命其次**单击**。**

13.On**断言创建**单击**配置断言创建。**

14.Under标识**映射**选择**标准**并且**其次**单击**。**

15. 在**属性合同>延伸合同请**输入属性**邮件**和**memberOf**并且单击**添加**。单击 Next。**

此选项的配置允许标识供应商通过**MemberOf**和**给**活动目录提供的属性发电子邮件给ISE，在政策决策期间， ISE能使用以后作为情况。

16.Under**验证来源映射**点击**地图新建的适配器实例。**

17.On**适配器实例**选择**HTML表适配器**。单击“下一步”

18. 在**映射方法下请**选择第二个选项下来并且**其次**单击**。**

19. 在**属性来源&用户查找请**单击**添加属性来源方框。**

20. 在**数据存储下请**输入说明，并且从**活动数据存储**选择LDAP连接实例并且定义什么类型的目录服务这是。如果没有配置的**数据存储，**请单击**管理数据存储**为了添加新的实例。

21. 在**LDAP目录搜索下请**定义LDAP用户查找的**基础DN**在域并且**其次**单击。

注意：在LDAP用户查找期间，因为将定义基础DN这是重要。不正确地定义的基础DN将导致在LDAP模式没找到的对象。

22.Under **LDAP过滤器**添加字符串**sAMAccountName=$ {username}**并且**其次**单击。

23. 在**属性合同实现下请**选择给的选项并且**其次**单击。

24. 验证配置在Summary部分并且点击**完成。**

25. 返回在**属性来源&用户查找其次**单击。

26. 在**故障自动保险的属性来源下其次请**单击。

27. 在**属性合同实现下请**选择这些选项并且**其次**单击**。**

28. 总之验证配置部分并且点击**完成**。

29. 返回在**验证来源映射其次**单击。

30. 一旦配置验证在**汇总页下请**点击**完成**。

31. 返回在**断言创建其次**单击。

32. 在**协议设置下**，请单击**配置协议设置**。这时应该有已经填充的两个条目。单击 **Next**。

33. 在SLO服务URL下**其次请**单击**。**

34. 在允许的SAML捆绑，请不选定选项人工制品并且**其次**用肥皂擦洗并且单击**。**

35. 根据签名策略**其次请**单击。

36. 根据加密策略**其次请**单击。

37. 查看在汇总页的配置并且点击**完成**。

38. 返回在浏览器SSO >协议设置**其次**单击，验证配置，并且点击**完成**。

39. 浏览器SSO选项卡出现。单击 **Next**。

40. 在**凭证下请**单击**配置凭证**并且选择在IdP期间将用于的签署的证书ISE通信并且检查选项**包括证书在签名**。然后，单击**下一步**。

> **注意**：如果没有配置的证书单击**管理证书**并且按照提示符为了生成将使用的**自签名证书**签署IdP到ISE通信。

41. 验证配置在汇总页下并且点击**完成**。

42. 返回在**凭证**选项卡**其次**单击。

43. 在**激活&摘要下请**选择**连接状态激活**，验证配置的其余，并且点击**完成**。

步骤4.导入IdP元数据到ISE外部SAML IdP供应商配置文件

1. 在PingFederate管理控制台下，请选择**服务器配置>Administrative功能>元数据出口。** 如果服务器为多个角色配置(IdP和SP)，请选择**我是标识Provider(IdP)的**选项。单击 **Next**。
2. 在**元数据**模式下请选择"Select Information to Include In Metadata Manually"。单击 **Next**。
3. 在**协议下其次请**单击。

4. 在**属性合同其次请**单击。

5. 在**签署的密钥下请**选择在连接配置文件以前配置的证书。单击 **Next**。

6. 在**元数据签字下请**选择签署的证书，并且检查**在关键信息元素包括此证书的公共密钥。**单击 **Next**。

7. 在**XML加密证明下其次请**单击。

注意：选项强制执行此处加密是至网络Admin。

8. 在**Summary部分下请**点击**出口**。保存生成的元数据文件然后单击**完成**。

9. 在ISE下，请选择对**Administration >身份管理>外部标识来源> SAML Id供应商> PingFederate**。

10. 点击**标识供应商设置>浏览**并且继续导入从PingFederate元数据出口操作保存的元数据。

11. 选择**组**选项卡，在**组成员属性下请**添加**memberOf**然后单击**添加**

以**在断言名义请**添加**IdP**应该返回的辨别名称，当**memberOf**属性是获取的表LADP验证时。 在这种情况下组配置与突岩的赞助商组连接，并且此组的DN如下：

一旦添加DN，并且“请命名在ISE”说明点击OK键。

12. 选择**Attributes选项**并且单击**添加**。

在此步骤，请添加属性“邮件”在从根据在LDAP的Ping的查询的IdP通过的SAML标记包含，它应该包含该对象的电子邮件属性。

注意：步骤11和12保证ISE收到AD对象电子邮件，并且MemberOf属性通过IdP登陆操作。

验证

1. 启动访客门户使用门户测验URL或通过跟随CWA请流。用户将有选项输入访客凭证，创建他们自己的帐户和员工洛金。
2. 点击**员工洛金**。因为没有激活的会话用户将重定向到IdP登录门户。

3. 回车AD凭证和点击**符号**。

4. IdP登录屏幕将重定向用户对访客门户成功页。

5. 这时，在用户来上一步到门户的访客并且选择"Employee Login"时候他们在网络将允许，只要会话是活跃的在IdP。

故障排除

SAMLise-psc.log(SAML)**Administration >>Configuration>>**SAML

CLIISEshow logging**ise-psc.log**SAMLise-psc.log**>>>ISE>>ise-psc.log**

```
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAMLUtils::isOracle() - checking whether IDP URL
indicates that its OAM. IDP URL: https://14.36.147.1:9031/idp/sso.saml2
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SPProviderId for PingFederate is: http://CiscoISE
/5b4c0780-2da2-11e6-a5e2-005056a15f11
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- ResponseValidationContext:
        IdP URI: PingFederate
        SP URI: http://CiscoISE/5b4c0780-2da2-11e6-a5e2-005056a15f11
        Assertion Consumer URL: https://14.36.157.210:8443/portal/SSOLoginResponse.action
        Request Id: _5b4c0780-2da2-11e6-a5e2-005056a15f11_DELIMITERportalId_EQUALS5b4c0780-2da2-
11e6-a5e2-005056a15f11_SEMIportalSessionId_EQUALS309f733a-99d0-4c83-8
b99-2ef6b76c1d4b_SEMI_DELIMITER14.36.157.210
        Client Address: 14.0.25.62
        Load Balancer: null
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Determine the signing certificate
2016-06-27 16:15:39,366 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.BaseSignatureValidator -:::::- Validate signature to SAML standard
with cert:CN=14.36.147.1, OU=TAC, O=Cisco, L=RTP, C=US serial:1465409531352
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Creating XMLSignature object
2016-06-27 16:15:39,367 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
org.opensaml.xml.signature.SignatureValidator -:::::- Validating signature with signature
algorithm URI: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.SAMLSignatureValidator -:::::- Assertion signature validated
succesfully
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::::- Validating response
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.WebSSOResponseValidator -:::::- Validating assertion
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Assertion issuer succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Subject succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.validators.AssertionValidator -:::::- Conditions succesfully validated
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- SAML Response: validation succeeded for guest
IDPResponse
:
        IdP ID: PingFederate
        Subject: guest
        SAML Status Code:urn:oasis:names:tc:SAML:2.0:status:Success
        SAML Success:true
        SAML Status Message:null
        SAML email:guest@rtpaaa.net
        SAML Exception:null
2016-06-27 16:15:39,368 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- AuthenticatePortalUser - about to call
authenticateSAMLUser messageCode:null subject:guest
2016-06-27 16:15:39,375 DEBUG  [http-bio-14.36.157.210-8443-exec-3][]
cpm.saml.framework.impl.SAMLFacadeImpl -:::::- Authenticate SAML User - result:PASSED
```

相关信息

- 与思科WLC和ISE配置示例的中央Web验证。
- 与交换机和身份服务引擎配置示例的中央Web验证。
- 思科身份服务引擎的版本注释，版本2.1
- 思科身份服务引擎管理员指南，版本2.1