目录

SSO概览

金山云支持基于SAML 2.0的SSO（Single Sign On，单点登录），也称为身份联合登录。

使用场景

如果您的企业或组织已有自己的账号体系，同时希望管理组织内成员使用金山云资源，金山云提供SSO功能，您不必在金山云账户中为每一位组织成员创建子用户，您可以使用此功能管理外部用户身份，可以向这些外部用户身份授予权限使用您的金山云资源。为了更好的理解SSO，下面简要介绍与SAML/SSO相关的一些基本概念。

基本概念

身份提供商（IdP）

- 一个包含有关外部身份提供商元数据的实体，身份提供商可以提供身份管理服务。
- 企业本地IdP：Microsoft Active Directory Federation Service （AD FS）、Shibboleth等。
- Cloud IdP：Azure AD、Google G Suite、Okta、OneLogin等。

服务提供商（SP）

利用IdP的身份管理功能，为用户提供具体服务的应用，SP会使用IdP提供的用户信息。一些非SAML协议的身份系统（例如：OpenID Connect），也把服务提供商称作IdP的信赖方。

安全断言标记语言（SAML 2.0）

实现企业级用户身份认证的标准协议，它是SP和IdP之间实现沟通的技术实现方式之一。SAML 2.0已经是目前实现企业级SSO的一种事实标准。

SAML断言（SAML assertion）

SAML协议中用来描述认证请求和认证响应的核心元素。例如：用户的具体属性就包含在认证响应的断言里。

信赖（Trust）

建立在SP和IdP之间的互信机制，通常由公钥和私钥来实现。SP通过可信的方式获取IdP的SAML元数据，元数据中包含IdP签发SAML断言的签名验证公钥，SP则使用公钥来验证断言的完整性。

功能特性

- 无需创建金山云账号 企业客户无需为组织内每个成员创建金山云账号，避免因用户所分配的长期访问证书（例如云 API 密钥）泄露而导致的安全问题。
- 提供联合单点登录（SSO） 企业客户已有身份验证体系的场景下，通过身份提供商可实现联合单点登录（SSO）。
- 简化身份验证登录流程 因身份提供商提供登录代码，企业客户能够低成本完成与金山云的联合身份验证，便捷上云。

SSO方式

金山云支持两种 SSO 登录方式：

- 通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。
- 通过用户SSO，企业员工在登录后，将以 IAM 子用户身份访问金山云。

角色SSO配置步骤

为了建立金山云与企业IdP之间的互信关系，需要进行金山云云作为SP的SAML配置和企业IdP的SAML配置，配置完成后才能进行SSO。

第一步：在企业组织中配置基于 SAML 2.0 的身份提供商

1. 企业IdP的SAML SP配置需要使用金山云云的SAML服务提供商元数据URL：[http://fe.ksyun.com/fs/ksyun-sp-metadata.xml]。
2. 在企业IdP中创建一个SAML SP，并根据实际情况选择下面任意一种方式配置金山云为信赖方：

（1）直接使用上述金山云的元数据URL进行配置。

（2）如果您的IdP不支持URL配置，您可以根据上述URL下载元数据文件并上传至您的IdP。

（3）如果您的IdP不支持元数据文件上传，则需要手动配置以下参数：

- Entity ID：urn:ksyun:cloudcomputing
  - ACS URL：https://signin.ksyun.com/saml-role/sso
  - RelayState：只支持配置跳转到金山云云控制台首页。

第二步：在企业IdP中配置SAML断言属性

金山云要求企业IdP生成的SAML断言里包含一些必要的信息以确定企业用户的登录身份，因此企业IdP必须进行属性配置来IAM角色，从而实现企业用户与金山云的SSO。

第三步：在金山云创建SAML身份提供商

1. 登录访问控制控制台。
2. 选择左侧菜单**SSO管理** 。
3. 在**SSO管理**页面中单击**创建身份提供商**按钮。
4. 在弹窗中输入**身份提供商名称**和**备注**，**上传元数据文档**。

- 元数据文档由企业IdP提供
- 一般为XML格式，包含IdP的登录服务地址、用于验证签名的公钥及断言格式等信息

5. 单击提交，完成创建。

第四步：在金山云为SAML身份提供商配置权限

1. 登录访问控制控制台。
2. 在左侧导航栏，单击**角色管理**。
3. 在**角色管理**界面，单击**新建角色**。
4. 在**新建角色**页面中，**设置授权实体类型**为**身份提供商**。
5. 输入角色名称和备注。
6. 在设置载体信息， 选择身份提供商。
7. 单击**下一步**，完成角色创建。

角色创建成功后，进入设置角色权限页面，您可以为该角色添加权限策略。

SAML 角色SSO概览

背景说明

金山与企业进行角色SSO时，金山云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过角色SSO，企业可以在本地IdP中管理员工信息，无需进行金山云和企业IdP间的用户同步，企业员工将使用指定的角色来登录金山云。

基本流程

通过SSO，企业员工可以通过控制台访问金山云。

1. 企业员工A使用浏览器在IdP的登录页面中选择金山云作为目标服务。 例如：如果企业IdP使用AD FS（Microsoft Active Directory Federation Service），则登录URL为：https://ADFSServiceName/adfs/ls/IdpInitiatedSignOn.aspx。

   有些IdP会要求用户先登录，再选择代表金山云的SSO应用。

2. IdP生成一个SAML响应并返回给浏览器。
3. 浏览器重定向到SSO服务页面，并转发SAML响应给SSO服务。
4. SSO服务使用SAML响应向金山云STS服务请求临时安全凭证，并生成一个可以使用临时安全凭证登录金山云控制台的URL.

   如果SAML响应中包含映射到多个角色的属性，系统将会首先提示用户选择一个用于访问金山云的角色。

5. SSO服务将URL返回给浏览器。
6. 浏览器重定向到该URL，以指定角色身份登录到金山云控制台。

用户SSO概览

背景说明

金山云与企业进行用户SSO时，金山云是服务提供商（SP），而企业自有的身份管理系统则是身份提供商（IdP）。通过用户SSO，企业员工登录后将以IAM子用户访问金山云

基本流程

主账号完成用户SSO的相关登录设置后，企业员工可以通过控制台访问金山云

1. 企业员工A使用浏览器登录金山云，金山云将SAML认证请求返回给浏览器
2. 浏览器向IdP转发SAML认证请求
3. IdP提示企业员工A登录，并在企业员工A登录成功后生成SAML响应返回给浏览器
4. 浏览器将SAML响应转发给SSO服务
5. SSO服务通过SAML互信配置，验证SAML响应的数字签名来判断SAML断言的真伪，并通过SAML断言的NameID元素值，匹配到对应金山云账号中的IAM子用户。
6. SSO服务向浏览器返回控制台的URL
7. 浏览器重定向到金山云控制台

说明：以上第1步中 企业员工也可以在企业自有IdP的登录页直接单击登录到金山云的链接，向企业IdP发出登录到金山云的SAML认证请求。企业员工在金山云控制台登录并不是必须的。

用户SSO配置步骤

基于SAML 2.0的用户SSO，配置对应元数据来建立金山云对企业身份提供商（IdP）的信任，实现企业IdP通过用户SSO登录金山云。

第一步：金山云SP的SAML配置

1. 金山云主账号登录访问控制控制台。
2. 选择左侧菜单**SSO管理**
3. 在**用户SSO**标签页，可查看当前**SSO登录设置**相关信息
4. 点击 可进行**SSO登录设置**，包括设置SSO功能状态、上传IdP元数据文档、设置企业域名
   - SSO功能状态：可以设置开启或关闭

     该功能只对金山云账号下的所有IAM子用户生效，不影响主账号登录

     - 此功能状态默认为关闭，此时IAM子用户可以使用密码登录，SSO登录设置不生效
     - 选择开启该功能后，IAM子用户不可以使用密码登录，只能SSO登录，统一跳转到企业IdP登录进行身份验证。再次选择关闭后，子用户可以使用密码登录。
   - 元数据文档：点击上传文件，上传企业IdP提供的元数据文档

     元数据文档一般为XML格式，包括IdP的登录服务地址和X.509公钥证书(用户验证IdP所颁发的SAML断言的有效性)
   - 企业域名：SAML断言中的NameID元素只能使用该企业域名作为后缀

第二步：创建与企业IdP相匹配的IAM子用户：

1.方式一：登录访问控制控制台手动创建与企业IdP匹配的IAM子用户，详情参见创建IAM子用户 2.方式二：使用金山云OpenAPI创建IAM子用户，详情参见新建子用户

说明 请确保IAM子用户的登录账号与企业邮箱的用户名前缀保持一致

第三步：企业IdP的SAML配置

在企业身份提供商（IdP）中配置金山云为可信SAML服务提供商（SP） 1.从金山云控制台获取SAML服务提供商元数据URL。

- 金山云主账号登录访问控制控制台。
- 选择左侧菜单**SSO管理** 。
- 在**SSO管理**页面，单击**用户SSO**页签。
- 在**SSO登录设置**区域，查看当前金山云账号的**SAML服务提供商元数据URL**。
  2. 在企业IdP中创建一个SAML SP，并根据实际情况选择下面任意一种方式配置金山云为信赖方
- 直接使用第一步所述的金山云元数据URL进行配置。
- 如果您的IdP不支持URL配置，您可以通过第一步所述URL下载元数据文件并上传至您的IdP。
- 如果您的IdP不支持元数据文件上传，则需要手动配置以下参数：
  - Entity ID：元数据XML中，EntityDescriptor元素的entityID属性值。
  - ACS URL：元数据XML中，AssertionConsumerService元素的Location属性值。
  - RelayState：只支持配置跳转到金山云云控制台首页，可不填写

第四步：在企业IdP中配置SAML断言属性

在基于SAML 2.0的SSO流程中，当企业用户在IdP登录后，IdP将根据SAML 2.0 HTTP-POST绑定的要求生成包含SAML断言的认证响应，并由浏览器（或程序）自动转发给金山云。这个SAML断言会被用来确认用户登录状态并从中解析出登录的主体。因此，断言中必须包含金山云要求的元素，否则登录用户的身份将无法被确认，导致SSO失败。

SAML断言中的元素说明

- SAML 2.0协议的通用元素
- NameID元素

金山云需要通过UPN（User Principal Name）来定位一个IAM子用户，所以要求企业IdP生成的SAML断言包含用户的UPN。金山云通过解析SAML断言中的NameID元素，来匹配IAM子用户的UPN从而实现用户SSO。

因此，在配置IdP颁发的SAML断言时，需要将对应于IAM子用户UPN的字段映射为SAML断言中的NameID元素。

NameID元素：使用企业域名作为NameID元素的后缀，即 username@domain_name。其中username为IAM子用户的用户名，domain_name为企业域名。

使用Okta进行用户SSO的示例

本文以Okta与金山云进行用户SSO的示例，帮助您理解企业IdP与金山云进行SSO的端到端配置流程。

第一步：在金山云获取SAML服务提供商元数据

1. 登录访问控制控制台。
2. 选择左侧菜单**SSO管理**
3. 在**SSO管理**页面，单击**用户SSO**页签
4. 复制**SAML服务提供商元数据URL**
5. 在新的浏览器窗口中打开复制的链接，将元数据XML文件另存到本地

   说明 元数据XML文件保存了金山云作为一个SAML服务提供商的访问信息。您需要记录XML文件中EntityDescriptor元素的entityID属性值和AssertionConsumerService元素的Location属性值，以便后续在Okta的配置中使用。

第二步：在Okta创建支持SAML SSO的应用

1. 登录Okta门户。
2. 切换到管理员身份
3. 在左侧导航栏，选择**Applications > Applications**。
4. 在**Applications**页面，单击**Create App Integration**。
5. 在**Create a new app integration**对话框，单击**SAML 2.0**，然后单击**Next**。
6. 配置应用名称为Ksyun-SSO-Demo，单击**Next**。
7. 配置SAML，然后单击**Next**
8. SAML setting 如下图
   - Single sign on URL为第一步中：在金山云获取SAML服务提供商元数据中记录的Location。
   - Audience URI为第一步中：在金山云获取SAML服务提供商元数据中记录的entityID。
   - Default RelayState（非必填）当前仅支持跳转到金山云控制台首页，可不填写
   - Name ID format选择Persistent。
   - Application username选择Email。
9. 在Feedback页面，根据需要选择合适的应用类型，然后单击Finish。

第三步：在Okta获取SAML IdP元数据

1. 在应用程序Ksyun-SSO-Demo详情页，单击**Sign On**
2. 在SAML Signing Certificates右侧，单击View SAML setup instructions
3. 在页面下方，可查看IDP metadata
4. 复制IdP元数据另存为xml格式到本地

第四步：在金山云开启用户SSO

1. 金山云主账号登录访问控制控制台。
2. 左侧导航栏，单击**SSO管理**
3. 在**SSO管理**页面，单击**用户SSO**页签
4. 点击 进行**SSO登录设置**，开启**SSO功能状态**

   说明 用户SSO是一个全局功能，开启后，所有IAM子用户都需要使用SSO登录。（无法使用密码登录）

   5.上传**IdP元数据文档**

说明 此处为在第三步中获取的IdP元数据文档，xml格式

6.设置**企业域名**

说明 只有以此处配置的后缀结尾的Email地址可以登录到金山云

第五步：在Okta创建用户并分配应用

1. 在Okta左侧导航栏，选择Directory > People。
2. 单击Add Person。
3. 在Add Person页面，填写基本信息并将Primary email配置为 test@example.com，然后单击Save。
4. 在用户列表中，单击用户test@example.com Status列的Activate，然后根据页面提示激活test@example.com。
5. 在左侧导航栏，选择Applications > Applications。
6. 单击目标应用名称（Ksyun-SSO-Demo）后，在Assignments页签，选择Assign > Assign to People。
7. 单击目标用户（test@example.com）后的Assign。
8. 单击Save and Go Back。
9. 单击Done。

第六步：在金山云创建IAM子用户

1. 在IAM控制台的左侧导航栏，选择人员管理 >子用户。
2. 在子用户页面，单击新建用户。
3. 在新建用户页面，输入登录账号和显示名称

   说明 请确保IAM子用户的登录账号与Okta中的用户名前缀保持一致，本示例中为test。

4. 访问信息区域，访问方式区域，选择控制台密码登录（保持默认即可）
5. 点击确定

验证结果

完成上述配置后，您可以从金山云控制台发起SSO登录。

1. 浏览器打开子用户登录页
2. 单击企业SSO
   - 输入主账号ID或者用户名
   - 输入企业邮箱（test@example.com）， 单击登录
3. 单击企业SSO在Okta的登录界面，输入用户名（test@example.com）和密码，单击登录
4. 系统将自动SSO登录并重定向到金山云控制台首页.如果页面成功跳转到金山云控制台首页，表示配置成功。