



2023 INTERNET2
TECHNOLOGY
exchange

Azure AD Proxying For InCommon Federation

Jared Johnson

Senior Software Engineer, Childrens Mercy Research Institute

Table of Contents

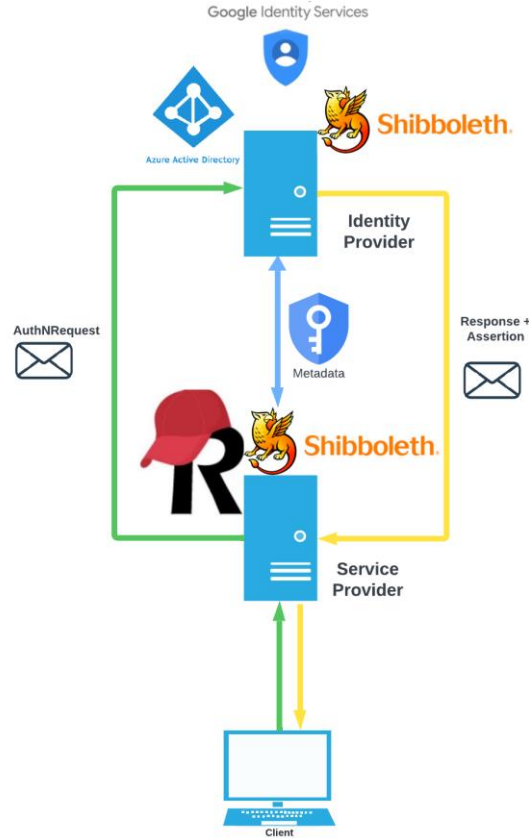
- SAML2 Flow and Concepts
- Azure Cloud Concepts
- Azure Resource Setup
- Shibboleth IdP Configuration
- Deployment and Federation
- Troubleshooting

SAML2 FLOW

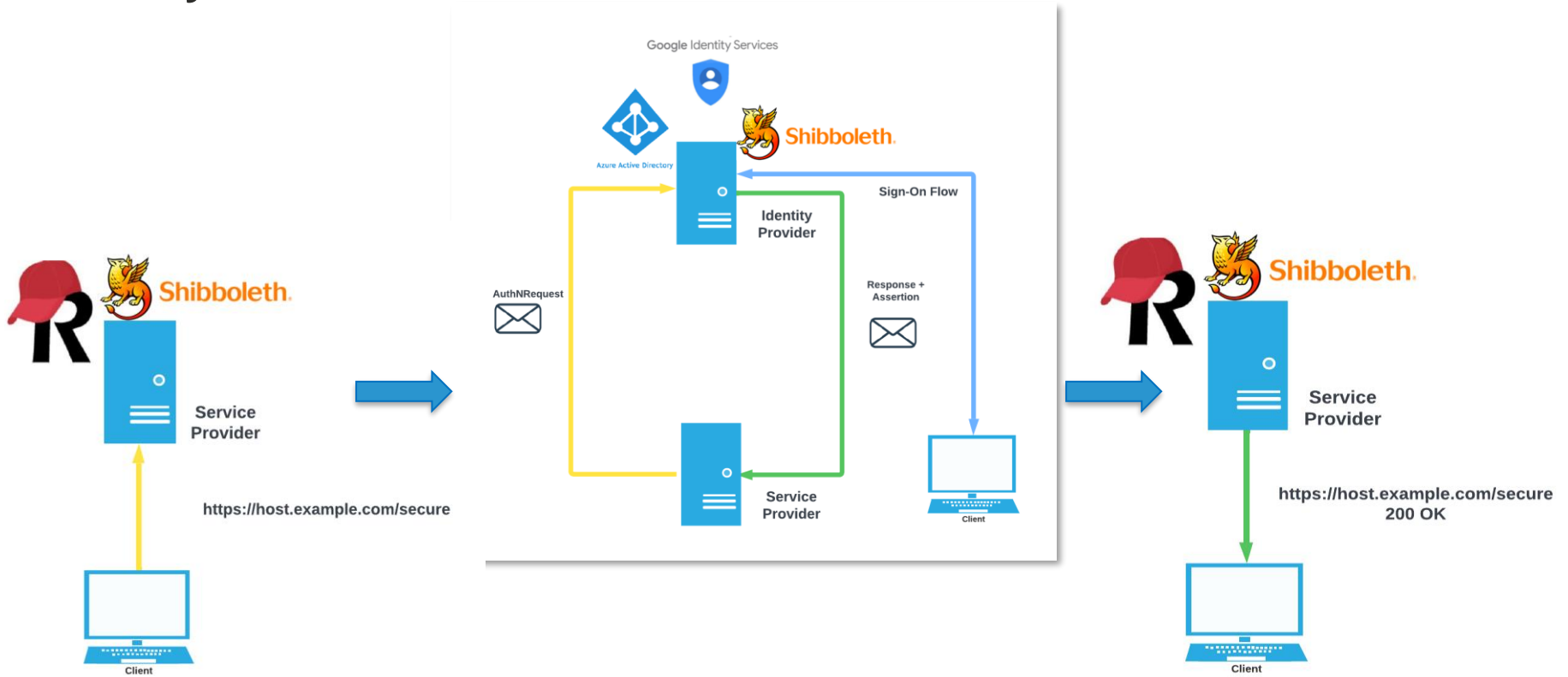
The background of the slide is abstract, featuring large, curved shapes in white, grey, and red. A bright red starburst light is visible in the lower right quadrant.

SAML 2 Key Concepts

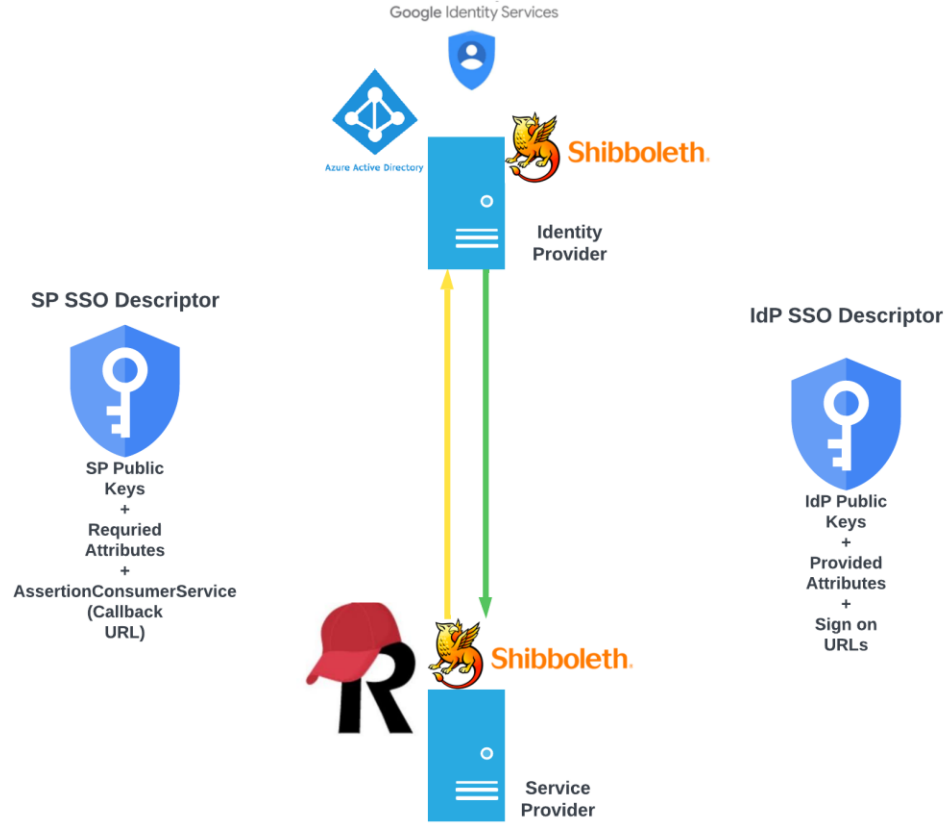
- Service Provider
- Identity Provider
- Metadata
- AuthNRequest
- Response + Assertion



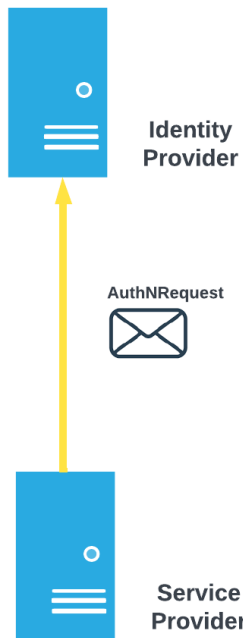
Identity\Service Provider



Metadata



AuthNRequest



```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="LOGIN_GUID_123123123129287837723"
  Version="2.0"
  ProviderName="Example SP"
  IssueInstant="2023-07-16T23:52:45Z"
  Destination="http://example.host.idp/signin"

  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AssertionConsumerServiceURL="http://sp.origin.example.com/protectedresource.html">
  <saml:Issuer>http://sp.origin.example/metadata</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" AllowCreate="true"/>
  <samlp:RequestedAuthnContext Comparison="exact">
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport</saml:AuthnContextClassRef>
  </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Response + Assertion



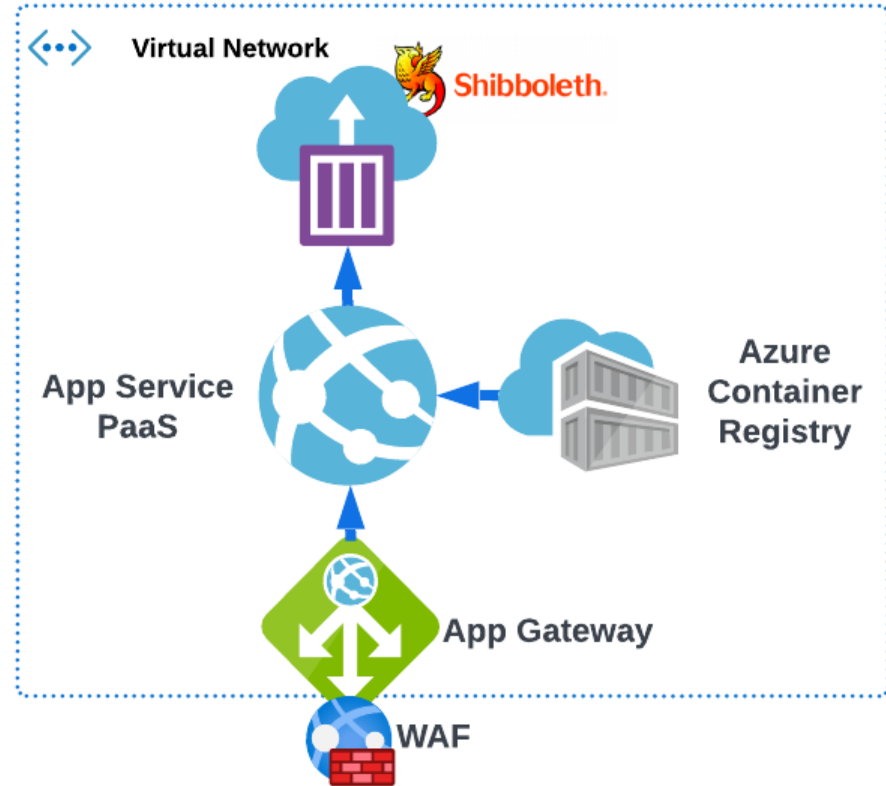
```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Ver
<saml:Issuer>http://example.host.idp</saml:Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="..." Version="2.0" IssueInstant="2023-07-17T01:01:48Z"
<saml:Issuer>http://example.host.idp</saml:Issuer>
<saml:Subject>
  <saml:NameID SPNameQualifier="http://sp.origin.exampe.com/protectedresource.html" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient">...</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData NotOnOrAfter="2024-01-18T06:21:48Z" Recipient="http://sp.origin.exampe.com/" InResponseTo="...">
  </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2023-07-17T01:01:18Z" NotOnOrAfter="2024-01-18T06:21:48Z">
  <saml:AudienceRestriction>
    <saml:Audience>http://sp.origin.exampe.com/acs</saml:Audience>
  </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2023-07-17T01:01:48Z" SessionNotOnOrAfter="2024-07-17T09:01:48Z" SessionIndex="_be9967abd904ddcae3c0eb4189adbe3f71e327c93">
  <saml:AuthnContext>
    <saml:AuthnContextClassRef urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextClassRef>
  </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
  <saml:Attribute Name="uid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xsi:type="xs:string">jtjohnson@cmh.edu</saml:AttributeValue>
  </saml:Attribute>
  <saml:Attribute Name="mail" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
    <saml:AttributeValue xsi:type="xs:string">jtjohnson@cmh.edu</saml:AttributeValue>
  </saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```


AZURE CLOUD CONCEPTS

The background features a dynamic composition of curved, overlapping shapes. On the left, a white triangular area transitions into a grey curved band. The right side is dominated by a large, vibrant red curved shape that frames a dark, circular inset. Within this inset, a bright red starburst light emanates from the bottom right, casting a glow over the scene. The overall aesthetic is modern and tech-oriented.

Cloud Key Concepts

- App Service
- App Service Plan
- App Gateway\WAF
- Azure Container Registry
- Virtual Networking
- App Registrations



App Service



An abstract layer for our web server. How we define and deploy behavior.

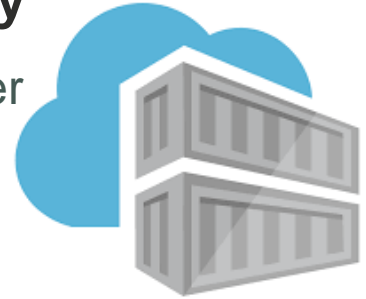
App Service Plan



The SLA, Compute capacity, and capabilities assigned to an App Service.

Container Registry

A repository for docker images

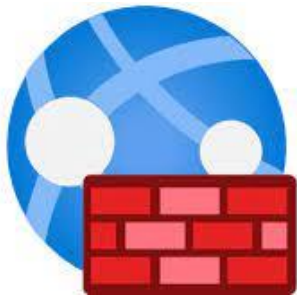


Virtual Network



Appliance for defining a networked environment that can be hidden from the public internet.

Web Application Firewall (WAF)



Firewall service mounted to our ingress to inspect requests and protect our resources

Application Gateway

Ingress controller for the Azure Virtual Network\Applications

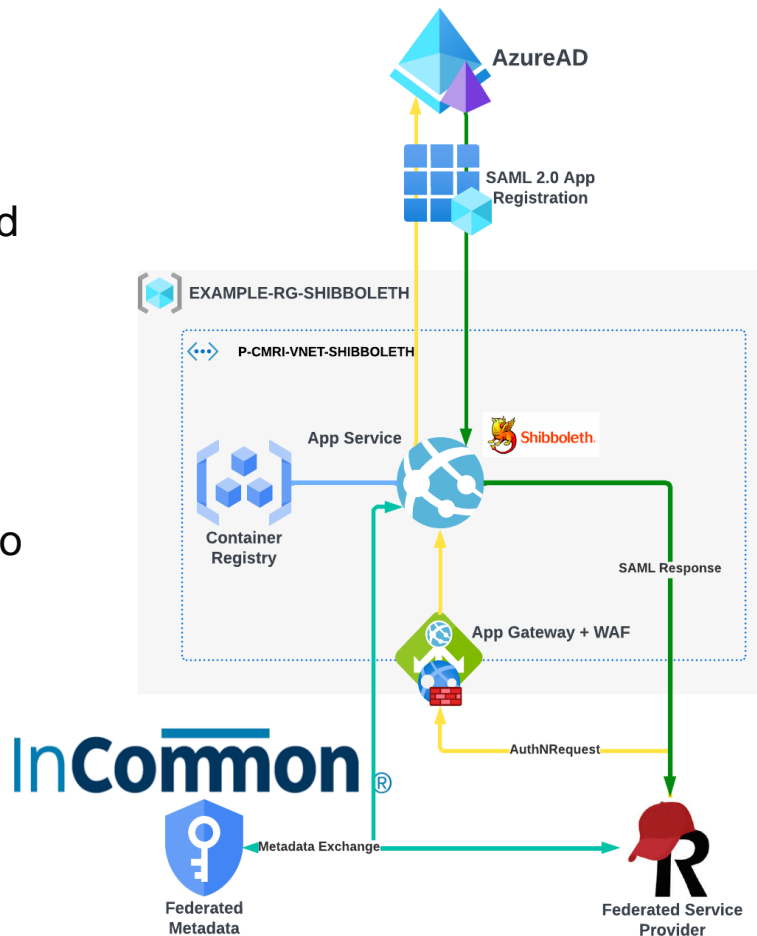


AZURE RESOURCE SETUP


The background features a white area on the left, a grey curved shape in the upper middle, and a large red curved shape on the right. A bright red starburst light is visible in the lower right quadrant.

Overall Architecture

- App Service hosts Shibboleth as SP and IdP
- Azure AD exposes SAML 2.0 sign on endpoints
- Gateway + WAF exposes App Service to public internet
- Container registry stores configured Shibboleth Docker image.



Resource Framing

 s-cmri-vnet-shibboleth | Subnets ☆ ...
Virtual network



[+ Subnet](#) [+ Gateway subnet](#) [Refresh](#) | [Manage users](#) [Delete](#)

[Overview](#)

[Activity log](#)

[Access control \(IAM\)](#)

[Tags](#)

[Diagnose and solve problems](#)

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓
s-cmri-snet-shibbolethapp	10.0.0.0/24	-	251	Microsoft.Web/serverfarms
s-cmri-snet-shibbolethagw	10.0.1.0/24	-	availability dependent on dyna...	-

Compute Resources

The image displays the Azure portal interface for configuring an App Service plan. The main view is the 'Settings' page for the App Service plan 'ASP-SCMRISHIBBOLETH-ab0f'. The 'Deployment Center' tab is selected, showing the following configuration:

- Container type: Single Container
- Registry source: Azure Container Registry
- Subscription ID: S-CMRI
- Authentication: Admin Credentials
- Registry: scmrishibbolethcontainerregistry
- Image: shib-idp
- Tag: testing

The 'Essentials' section shows the following details:

- Resource group: S-CMRI-SHIBBOLETH
- Status: Running
- Location: South Central US
- Subscription: S-CMRI
- Subscription ID: 07cot5164-8def-4125-889e-7cb54e3cf1a0
- Pricing plan: B1
- Instance count: 1
- App(s) / Slots: 1/0
- Operating System: Linux
- Zone redundant: Disabled

The 'Monitoring' section includes three charts:

- CPU Percentage:** Shows a fluctuating line graph with a current average of 15.55%.
- Memory Percentage:** Shows a fluctuating line graph with a current average of 75.2%.
- Data In:** Shows a line graph with a current average of 14.52 KB/s.

The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Microsoft Defender for Cloud, ASP-SCMRISHIBBOLETH-ab0f, Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Events (preview), Settings, Apps, File system storage, Networking, Scale up (App Service plan), Scale out (App Service plan), Properties, Locks, Monitoring, Alerts, Metrics, Logs, and Diagnostic settings.

WAF, Reverse Proxy, Load Balancer

Listeners [Listener TLS certificates \(Preview\)](#)

[+](#) Add listener [↻](#) Refresh

Application Gateway provides native support for WebSocket across all gateway sizes. There is no additional configuration required to enable or disable WebSocket support. If a Web automatically directed to the WebSocket enabled backend server using the appropriate backend pool as specified in application gateway rules. [Learn more about listeners and Web](#)

Name	Port	Protocol	Frontend IP	Associated rule
httplistener	443	HTTPS	Public	shibbolethhttp

shibbolethhttp

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name

Priority *

*Listener *Backend targets

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of Backend settings that define the behavior of the routing rule.

Target type Backend pool Redirection

Backend target *

Backend settings *

[+](#) Add

Name	Port	Protocol
httpbackendsettings	443	Https

Edit backend pool ...

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.

Name

Add backend pool without targets

Yes No

Backend targets

1 item

Target type	Target
IP address or FQDN	scmrshibboleth.azurewebsites.net ⓘ ⋮

Backend port *

Backend server's certificate is issued by a well-known CA Yes No

Additional settings

Cookie-based affinity Enable Disable

Connection draining Enable Disable

Request time-out (seconds) *

Override backend path

Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

Override with new host name Yes No

Use custom probe Yes No

Custom probe *

Enterprise App + Registration

App Registration

The screenshot shows the 'Authentication' configuration page for an Enterprise Application. The left-hand navigation pane includes sections for 'Overview', 'Quickstart', 'Integration assistant', 'Manage', and 'Manifest'. Under 'Manage', 'Authentication' is selected and highlighted. The main content area is titled 'Platform configurations' and contains a 'Web' section with 'Redirect URIs'. A text box lists the URI: `https://scmrishibboleth.azurewebsites.net/identity/profile/Authn/SAML2/POST/SSO`. Below the text box is an 'Add URI' button.

Enterprise Application

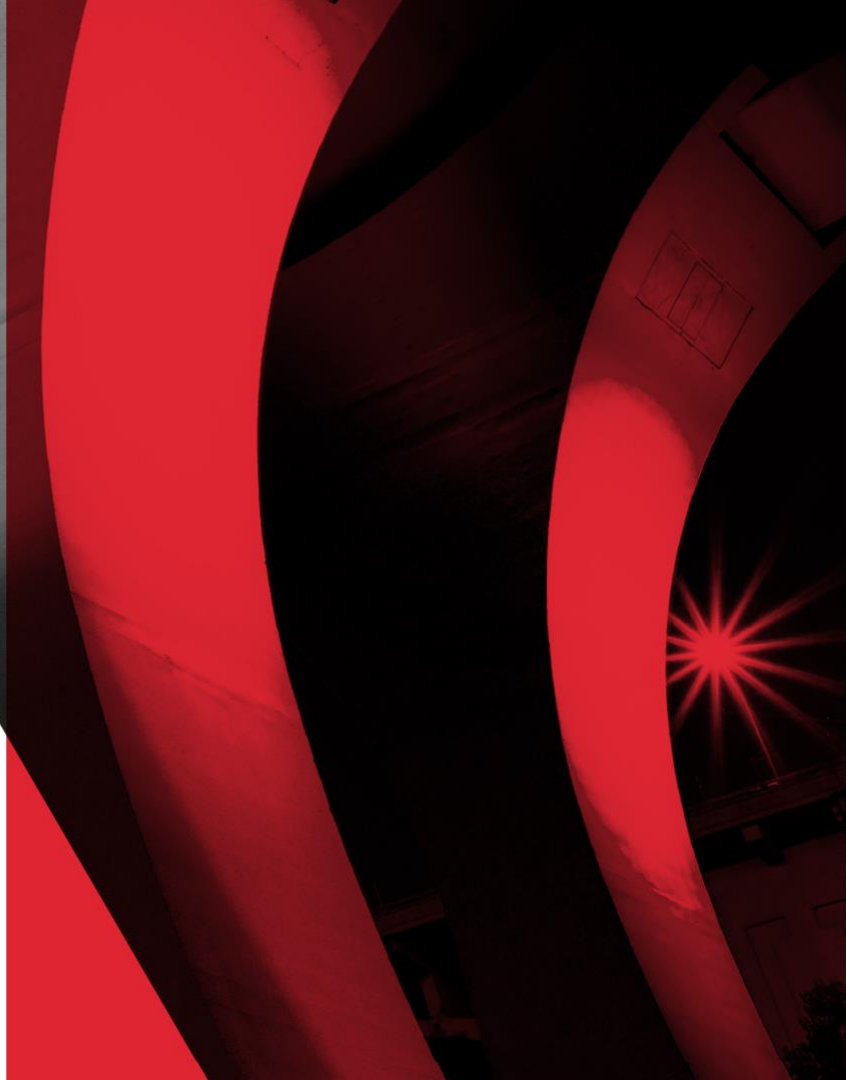
The screenshot shows the 'SAML-based Sign-on' configuration page for an Enterprise Application. The page title is 'SSO - InCommon Dev | SAML-based Sign-on'. The left-hand navigation pane includes sections for 'Overview', 'Deployment Plan', 'Diagnose and solve problems', 'Manage', and 'Security'. Under 'Manage', 'Single sign-on' is selected and highlighted. The main content area is titled 'Set up Single Sign-On with SAML' and contains two numbered sections:

- Basic SAML Configuration**

Identifier (Entity ID)	<code>https://scmrishibboleth.azurewebsites.net/identity/shibboleth</code>
Reply URL (Assertion Consumer Service URL)	<code>https://scmrishibboleth.azurewebsites.net/identity/profile/Authn/SAML2/POST/SSO</code>
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims**

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname

SHIBBOLETH IDP CONFIGURATION

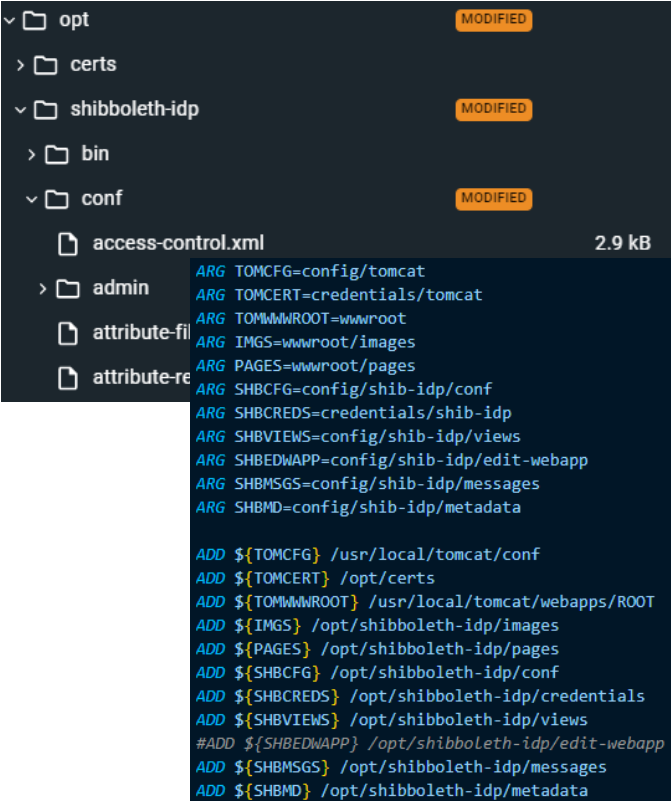


The TIER Idp Base Image & Configuration

[GitHub - docker/shib-idp: Shibboleth IDP container construction \(internet2.edu\)](https://github.com/docker/shib-idp)

[GitHub - docker/ShibbIdP_ConfigBuilder_Container \(internet2.edu\)](https://github.com/docker/ShibbIdP_ConfigBuilder_Container)

Shibboleth IdP v4.3.1
Tomcat v9.0.16

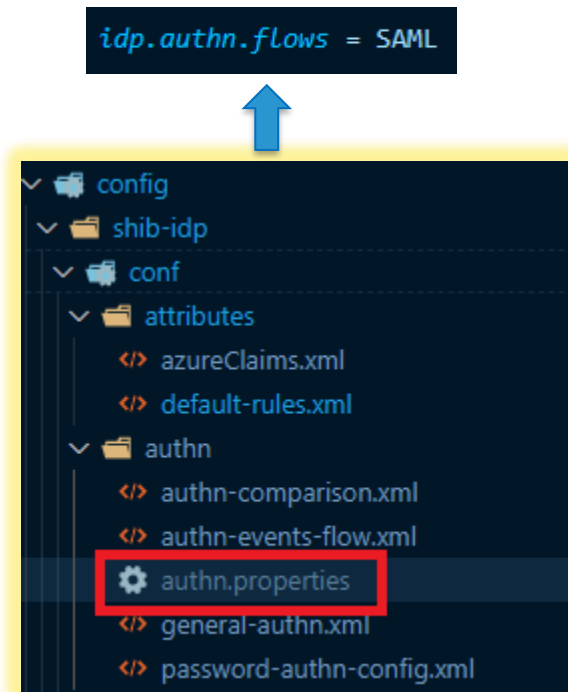


```
ARG TOMCFG=config/tomcat
ARG TOMCERT=credentials/tomcat
ARG TOMWWWROOT=wwwroot
ARG IMGs=wwwroot/images
ARG PAGES=wwwroot/pages
ARG SHBCFG=config/shib-idp/conf
ARG SHBCREDS=credentials/shib-idp
ARG SHBIEWS=config/shib-idp/views
ARG SHBEDWAPP=config/shib-idp/edit-webapp
ARG SHBMSGs=config/shib-idp/messages
ARG SHBMD=config/shib-idp/metadata

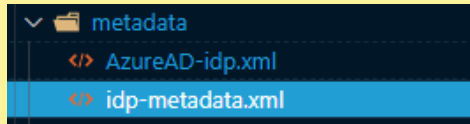
ADD ${TOMCFG} /usr/local/tomcat/conf
ADD ${TOMCERT} /opt/certs
ADD ${TOMWWWROOT} /usr/local/tomcat/webapps/ROOT
ADD ${IMGs} /opt/shibboleth-idp/images
ADD ${PAGES} /opt/shibboleth-idp/pages
ADD ${SHBCFG} /opt/shibboleth-idp/conf
ADD ${SHBCREDS} /opt/shibboleth-idp/credentials
ADD ${SHBIEWS} /opt/shibboleth-idp/views
#ADD ${SHBEDWAPP} /opt/shibboleth-idp/edit-webapp
ADD ${SHBMSGs} /opt/shibboleth-idp/messages
ADD ${SHBMD} /opt/shibboleth-idp/metadata
```

Steps to Configure IdP

- Signing and Encryption Tokens
- IdP Metadata, entity id
- Azure AD Metadata + InCommon Metadata\MDQ
- Attributes, Attribute Profile
- Transcoding and Claims
- Resolution and Mapping
- Filter policy



SP Metadata – Signing, Encryption, AssertionConsumerService



```
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <KeyDescriptor use="signing">
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
          ...
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </KeyDescriptor>
  <KeyDescriptor use="encryption">
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
          ...
        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </KeyDescriptor>
  <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[HOSTNAME]/idp/profile/Authn/SAML2/POST/SSO" index="0" />
</SPSSODescriptor>
</EntityDescriptor>
```

AzureAD Metadata

config

- shib-idp
 - conf
 - messages
 - metadata**
 - AzureAD-idp.xml**
 - idp-metadata.xml
- conf
 - attributes
 - authn
 - c14n
 - attribute-filter.xml
 - attribute-resolver.xml
 - global.xml
 - idp.properties
 - idp.properties.dist
 - ldap.properties
 - ldap.properties.dist
 - logback.xml
 - metadata-providers.xml**
 - relying-party.xml



SSO - InCommon | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Application proxy
 - Self-service

Upload metadata file Change single sign-on mode Test this application Got feedback?

SAML Certificates

Token signing certificate		Edit
Status	Active	
Thumbprint	593E43B1EFB49A6583E1BE8CAFD6DBF57F7C5C4	
Expiration	9/15/2025, 7:43:25 AM	
Notification Email	jtjohnson@cmh.edu	
App Federation Metadata Url	https://login.microsoftonline.com/fcdc7058-dd48-...	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XML	Download	

Verification certificates (optional)		Edit
Required	No	
Active	0	
Expired	0	



```
<MetadataProvider id="AzureAD-idp-metadata"
  xsi:type="FilesystemMetadataProvider"
  metadataFile="/opt/shibboleth-idp/metadata/AzureAD-idp.xml" />
</MetadataProvider>
```

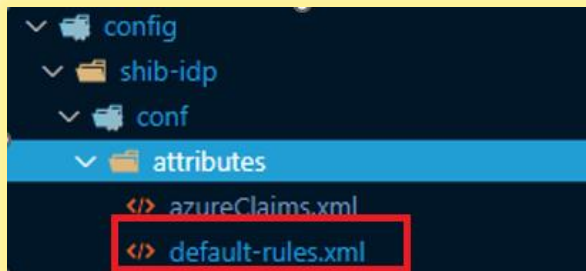

InCommon Metadata - MDQ

```
</ logback.xml  
</ metadata-providers.xml  
</ relying-party.xml
```

```
<MetadataProvider id="incommon" xsi:type="DynamicHTTPMetadataProvider" maxCacheDuration="PT24H" minCacheDuration="PT10M">  
  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true" certificateFile="%{idp.home}/credentials/inc-md-cert-mdq.pem" />  
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D" />  
  <MetadataQueryProtocol https://mdq.incommon.org/ /MetadataQueryProtocol>  
</MetadataProvider>
```

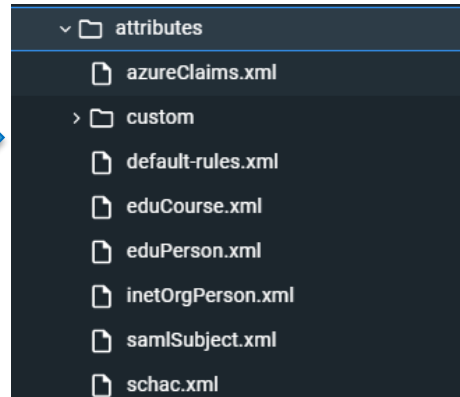
```
C: > Users > jjohnson > Documents > </> InCommon-metadata.xml  
1 <?xml version="1.0" encoding="UTF-8"?><EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:alg="urn:oasis:names:tc:SAML:metadata:algusupport" xmlns:ds="h  
2 iiAR+Y0+62I4BUQPRW5Mnp81u5qJxgcNurkwhES7y6zJgwMULG17m7V0ber6HntVza2PoeUOnEri&#13;  
3 xxFdWLaWmuue4NxfC4Yktc29TJfE2l62tMbS27BP14Yfe78j468+bHOXfhdc9ffbT7G41Vqx6+0u&#13;  
4 iawxPu6iG18XRbqqCLewmXRmrZiwt1bDQOr6QUOZqKcsU0fv/0ssXvG5LVcaBHY8uVnkt26u8cja&#13;  
5 N0axm5SxxcCG7XJtAe/etC23S2D6s7/2X1XzHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIDgTCCAmgAwIBAgIJAJRJzvdpkmNaM0GCSqGSIs3DQEBcWUAMFCzCzAJBgNVBAYTAVTRUw&  
6 EwYDVQQKDAxJbkNvbW1vb1BMTBMEMtAvBgnVBAMMKEluQ29tbW9uIEZlZGVyYXRpb24gTWV0YWRh&#13;  
7 dGgU2lnbluZyBLZXkwHhcNMTEwMjE2MTkzNDU1WhcNMzcxMjE4MTEzNDU1WjBXMQswCQYDVQQG&#13;  
8 EwJVUzEVBMBGA1UECgwMSW5Db212b24gTEwYDQDDChJbkNvbW1vb1BGMWV0YWRh&#13;  
9 IE1ldGFKYXRhIFNpZ25pbmcsS2V5MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBcGKAQEA0Chd&#13;  
10 krn+dG5Zj5L3Iw+xeWgNzm8ajw7/FyqRQ15jD4Lfg2Wcd1fJorYGNnVZMCTfItoXTSpG4rXxHQs&#13;  
11 ykeNiYRu2+02uMS+1pnBqkjjzdpJE0od+q8EbdvE6ShimjyNn0yQfGyQKcNdYuc+75MIHsaIOAetD&#13;  
12 ZUST9Sd4oeU1zRj2Vs6vUd+JFhveUAhrc0b+JEZfIEuq/LIU9qxm/+gFaawlmojZPyOWZ1Jlswbr&#13;  
13 rJYYyn10qgnJvjh9gZWKkjmPqxvHKJcATPhA2gWgabwTXBjCckMe1hrHCl/vbDLcmz0/oYuoasD&#13;  
14 zP6zE9YSA/xCp1AHA0moC1V52H5MOQGlEwIDAQAB0AwTjAdBgNVHQ4EFgQU5ij9YLUsZQ6K75kP&#13;  
15 gVpyQ2N/1PswHwYDVR0jBBgwFoAU51j9YLUsZQ6K75kPgpVpyQ2N/1PswdAYDVR0TBAUwAwEB/zAN&#13;  
16 BgkqhkiG9w0BAQsFAAOCAQEAAQEx9xvaLUt0PNLvhMtXXQPedCPw5xQBd2VW0sWPYsPRAOSNbU1&#13;  
17 V1oY+xUkUkorYtGkUY1q+uh2gDIeazW0uZZaQvWpP8xdxWqDh96n5US061szEc+Lj3dqdxkXRR&#13;  
18 qEbjhBFh/utXaeyeS0taX65GwD5svDhnJBcLAGkzeRlXqxmYG+I2zmm/JYgZEnbwToyC7yF6Q8CQ&#13;
```

Attribute Transcoding



```
<!-- Default Attribute transcoding rules. -->  
  
<import resource="inetOrgPerson.xml" />  
<import resource="eduPerson.xml" />  
<import resource="eduCourse.xml" />  
<import resource="schac.xml" />  
<import resource="samlSubject.xml" />  
  
<import resource="azureClaims.xml" />  
  
</beans>
```

Docker Container

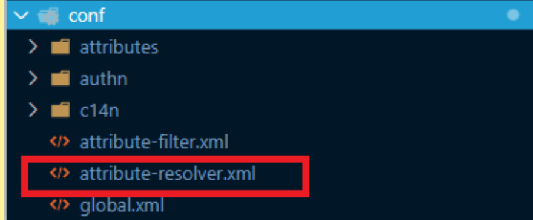


```
<bean parent="shibboleth.TranscodingRuleLoader">  
<constructor-arg>  
<list>  
<!-- claims relevant to person record -->  
<bean parent="shibboleth.TranscodingProperties">  
<property name="properties">  
<props merge="true">  
<prop key="id">azureName</prop>  
<prop key="transcoder">SAML2ScopedStringTranscoder</prop>  
<prop key="saml2.name">http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name</prop>  
<prop key="saml2.nameFormat">urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified</prop>  
<prop key="displayName.en">Name</prop>  
<prop key="description.en">Azure UPN of an account expected to be scoped thus transcoded that way</prop>  
</props>  
</property>  
</bean>
```

- example@abc.edu

Attribute Resolution (Derived Attributes)

Re-ID Azure claims, and make them available to Shibboleth



```
<AttributeResolver
  xmlns="urn:mace:shibboleth:2.0:resolver"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd">

  <!-- ===== -->
  <!-- Attribute Definitions -->
  <!-- ===== -->

  <!-- Schema: Core schema attributes-->

  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="mail"
    principalAttributeName="azureEmailAddress" />

  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="displayName"
    principalAttributeName="azureDisplayName" />
```

- example@abc.edu

```
<AttributeDefinition xsi:type="SubjectDerivedAttribute"
  forCanonicalization="true"
  id="canonicalNameToUseForJoin"
  principalAttributeName="azureName" />
```

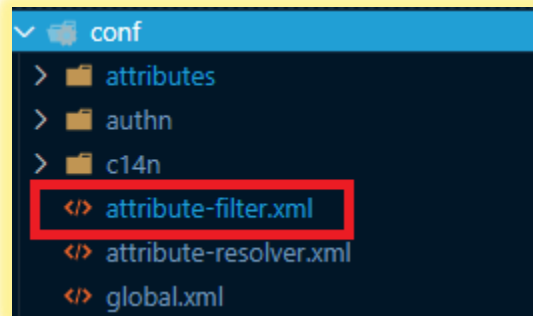
```
<DataConnector id="passthroughAttributes" xsi:type="Subject" exportAttributes="azureName azureEmailAddress" />
```

Attribute Release

- Release FROM Azure TO Shibboleth

```
<AttributeFilterPolicy id="FilterPolicyObject-Proxy-FromAzure-byIssuer-Type">
  <PolicyRequirementRule xsi:type="Issuer" value="https://sts.windows.net/fcdc7058-dd48-4a81-90b6-281159ae72e0/" />

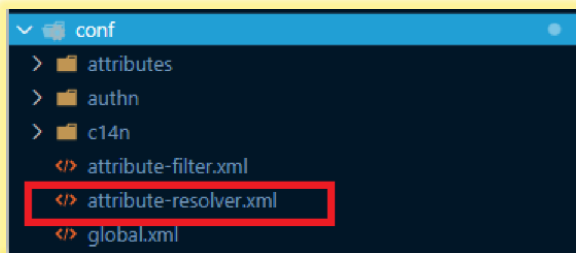
  <AttributeRule attributeID="azureDisplayname" permitAny="true" />
  <AttributeRule attributeID="azureGivenname" permitAny="true" />
  <AttributeRule attributeID="azureSurname" permitAny="true" />
  <AttributeRule attributeID="azureAuthmethodsreferences" permitAny="true" />
  <AttributeRule attributeID="azureIdentityprovider" permitAny="true" />
  <AttributeRule attributeID="azureTenantid" permitAny="true" />
  <AttributeRule attributeID="azureEmailaddress" permitAny="true" />
  <AttributeRule attributeID="azureObjectidentifier" permitAny="true" />
  <AttributeRule attributeID="azureAssurance" permitAny="true" />
  <AttributeRule attributeID="azureAffiliation" permitAny="true" />
  <AttributeRule attributeID="azureName">
    <PermitValueRule xsi:type="Scope" value="cmh.edu" ignoreCase="true" />
  </AttributeRule>
</AttributeFilterPolicy>
```



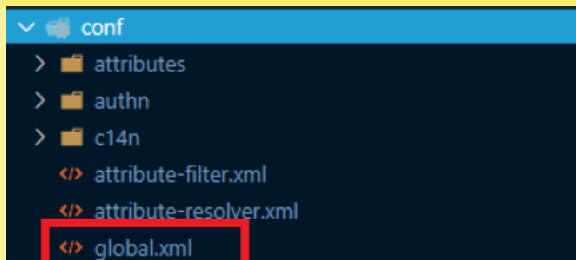
- Release FROM Shibboleth TO Relying Party (InCommon)

```
<!-- Attribute release for all InCommon SPs -->
<AttributeFilterPolicy id="releaseToInCommon">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
    attributeName="http://macedir.org/entity-category"
    attributeValue="http://id.incommon.org/category/registered-by-incommon"/>
  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="sn">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="displayName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="mail">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
</AttributeFilterPolicy>
```

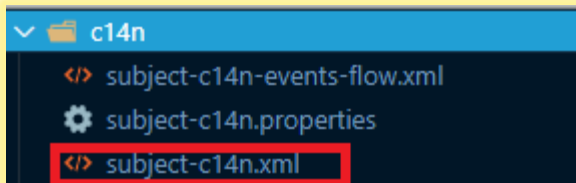
Canonicalization



```
<AttributeDefinition xsi:type="SubjectDerivedAttribute"
  forCanonicalization="true"
  id="canonicalNameToUseForJoin"
  principalAttributeName="azureName" />
```

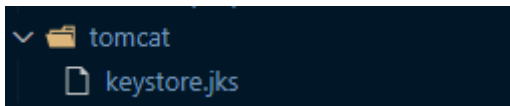
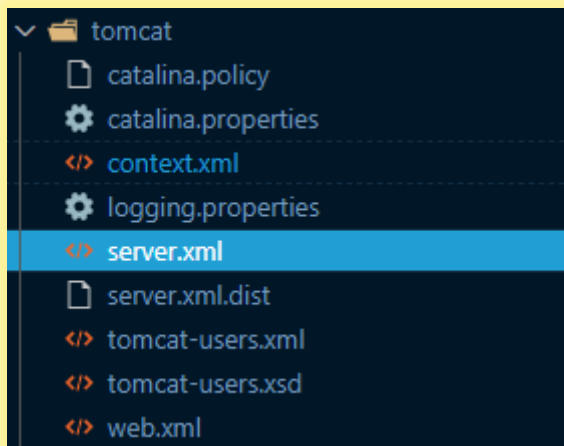


```
<util:list id="shibboleth.c14n.attribute.AttributesToResolve">
  <value>canonicalNameToUseForJoin</value>
</util:list>
<util:list id="shibboleth.c14n.attribute.AttributeSourceIds">
  <value>canonicalNameToUseForJoin</value>
</util:list>
```



```
<util:list id="shibboleth.PostLoginSubjectCanonicalizationFlows">
  <bean id="c14n/attribute" parent="shibboleth.PostLoginSubjectCanonicalizationFlow" />
</util:list>
```

Reverse Proxy, SSL Termination, Header Forwarding



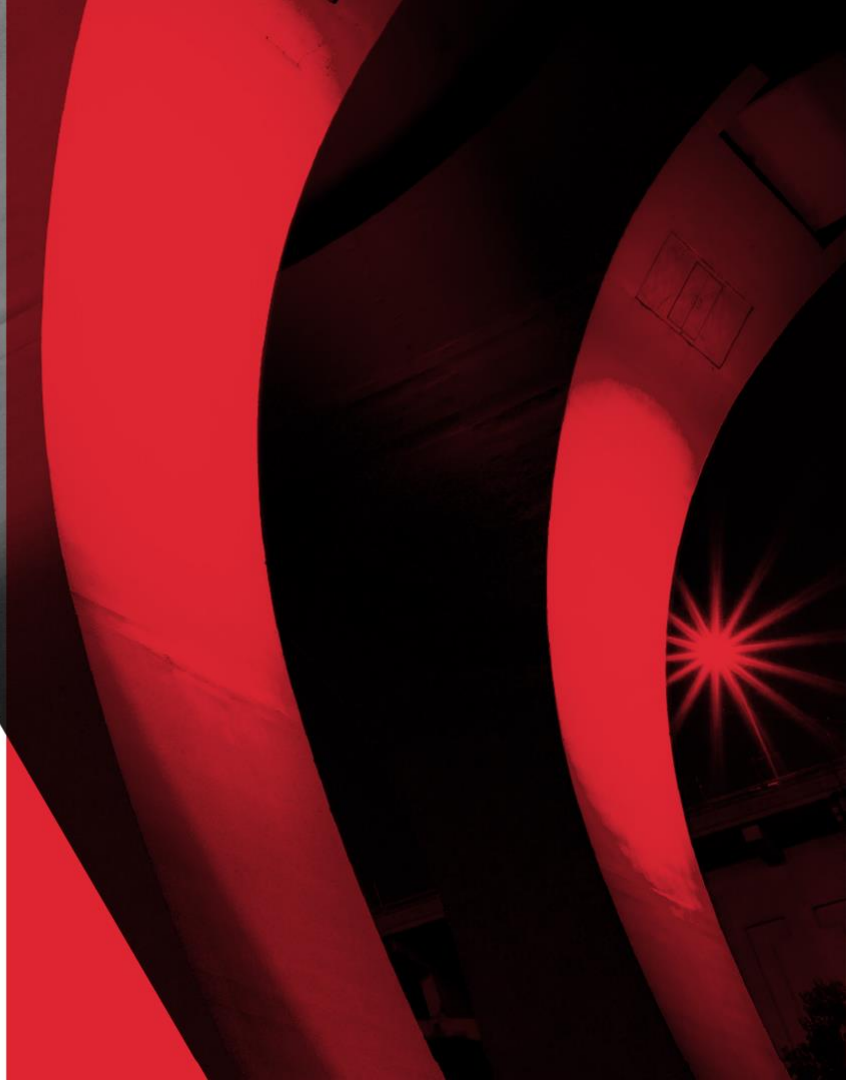
```
<?xml version='1.0' encoding='utf-8'?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />

  <Service name="Catalina">
    <Connector
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      port="443" maxThreads="200"
      scheme="https" secure="true" SSLEnabled="true"
      keystoreFile="/opt/certs/keystore.jks" keystorePass="
      clientAuth="false" sslProtocol="TLS"/>

    <Connector
      port="8080" maxThreads="150"
      enableLookups="false" connectionTimeout="20000" />

    <Engine name="Catalina" defaultHost="localhost">
      <Host name="localhost" appBase="webapps" unpackWARs="true" autoDeploy="true">
        <Valve className="org.apache.catalina.valves.RemoteIpValve"/>
        <Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"
          prefix="localhost_access_log." suffix=".txt"
          pattern="combined" />
        <Valve className="org.apache.catalina.valves.ErrorReportValve" showReport="false" showServerInfo="false" />
      </Host>
    </Engine>
  </Service>
</Server>
```

DEPLOYMENT AND FEDERATION



Build + Deployment

Login And Set Subscription

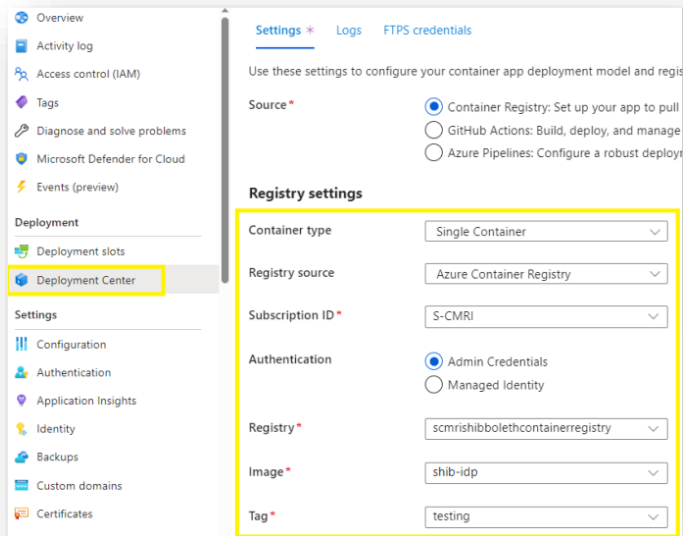
```
az login
az account set --subscription $SUB
```

Login to ACR (Azure Container Registry)

```
az acr login --name scmrishibbolethcontainerregistry
```

Build and Push Shibboleth Image to ACR

```
docker build . -t "scmrishibbolethcontainerregistry.azurecr.io/shib-idp:testing"
docker push "scmrishibbolethcontainerregistry.azurecr.io/shib-idp:testing"
```



Validation

```

https://scmrishibboleth.azurewebsites.net/idp/shibboleth
This XML file does not appear to have any style information associated with it. The document tree is shown below.

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:IDPSSODescriptor="urn:oasis:names:tc:SAML:2.0:protocol">
  <Extensions>
    <shibmd:Scope regexp="false">cmh.edu/shibmd:Scope</shibmd:Scope>
  </Extensions>
  <KeyDescriptor use="signing">
    <ds:KeyInfo>
      <ds:X509Data>
        <ds:X509Certificate>
          MIIDBDCCAeygAwIBAgIJAMxXhIgfW9SMAGCSgG5Ib3DQEBcUAMBoxEJAOBGMW BAWPKTEyNy4wLjAuHTAq
          ggEBAK8HqG0tLobBAZtTEoSrtA2Vv67HUXRnbfN4/7DlupkoA8gzE4jwky8V MaJTrcrysRdIMKLg/CQ1v4iF7P5bI2LAmAbxCO7m
          c0uaHmUrKVGSxNF7FXz2b1Cj1x3VmqNFScdn6rHefXfess3onZXm/FGBLNgZ /95Q0fArhk3UqRLs5MzInowM7yQNpxXGZDpRNM
          M4XhIBodHRwczovLzEyNy4wLjAuMS9pZHVhc2hpYmVzGVAADAgMHQ4EFGQU V4jbrF6MAswFglCoczHfokRkRjUpwQY3KoZiHvcm
          kq9Hz+66tlosezSHSUDTCxHxvwoDX/frAIttAyHZjBDDETPjaIHAk+0i6moyX Zhgc2hJ001K6lote+8DRsuk+U3iD5v6Q+V94UY1Y
          UTQMfHS21XA++c83Zs6XVmxGockRjHieUQornR1Z60g3pDP+ctefqno079V5a DBX+Tnd9eS= </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://scmrishib
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://scmrishiboleth
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://scmr
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://scmrishiboleth2.azure
  </IDPSSODescriptor>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
            MIIDBDCCAeygAwIBAgIJAO50zVhdGxrBMAgCSgG5Ib3DQEBcUAMBoxEJAOBGMW BAWPKTEyNy4wLjAuHTAq
            ggEBAK8HqG0tLobBAZtTEoSrtA2Vv67HUXRnbfN4/7DlupkoA8gzE4jwky8V MaJTrcrysRdIMKLg/CQ1v4iF7P5bI2LAmAbxCO7m
            c0uaHmUrKVGSxNF7FXz2b1Cj1x3VmqNFScdn6rHefXfess3onZXm/FGBLNgZ /95Q0fArhk3UqRLs5MzInowM7yQNpxXGZDpRNM
            M4XhIBodHRwczovLzEyNy4wLjAuMS9pZHVhc2hpYmVzGVAADAgMHQ4EFGQU V4jbrF6MAswFglCoczHfokRkRjUpwQY3KoZiHvcm
            aQyG0BgtsohqxShkbsu9Xu0bIbaxPr7YTO914a/Aath1PFpdd1lNXRr3r1DN 0C0f/0d3KpDh9LjKZGD3RSKApLFA3bR3PFDadgasa
            KIZzMHp9QxwulzKw/zlqK9ZQYMH0T21q/RctIsqW/0kgvzBBDTtS1xqM0Vq Se1gC0g1wo= </ds:X509Certificate>
          </ds:X509Data>
        </ds:KeyInfo>
      </KeyDescriptor>
      <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://scmrishib
    </SPSSODescriptor>
  </EntityDescriptor>

```

```

<AttributeFilterPolicy id="TestSP">
  <PolicyRequirementRule xsi:type="EntityAttributeExactMatch" value="https://[TESTHOST]" />
</PolicyRequirementRule>
  <AttributeRule attributeID="eduPersonPrincipalName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonAssurance">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="eduPersonScopedAffiliation">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
  <AttributeRule attributeID="givenName">
    <PermitValueRule xsi:type="ANY" />
  </AttributeRule>
</AttributeFilterPolicy>

```

Index of /

- [images/](#)
- [secure/](#)

Welcome

Attributes

eduPersonPrincipalName: jtjohnson@cmh.edu
 eduPersonScopedAffiliation: member@cmh.edu
 displayName: Johnson, Jared, T
 givenName: Jared
 sn: Johnson
 mail: jtjohnson@cmh.edu

Federation Manager

Add a New Identity Provider

EntityID: <https://iam.research.childrensmercy.org/idp/shibboleth>
Scope: cmh.edu

New

Entity ID and Scope: Contacts

Contact Type	Name	Email
Administrative	[REDACTED]	[REDACTED]
Technical	[REDACTED]	[REDACTED]
Security	[REDACTED]	[REDACTED]

Administrative

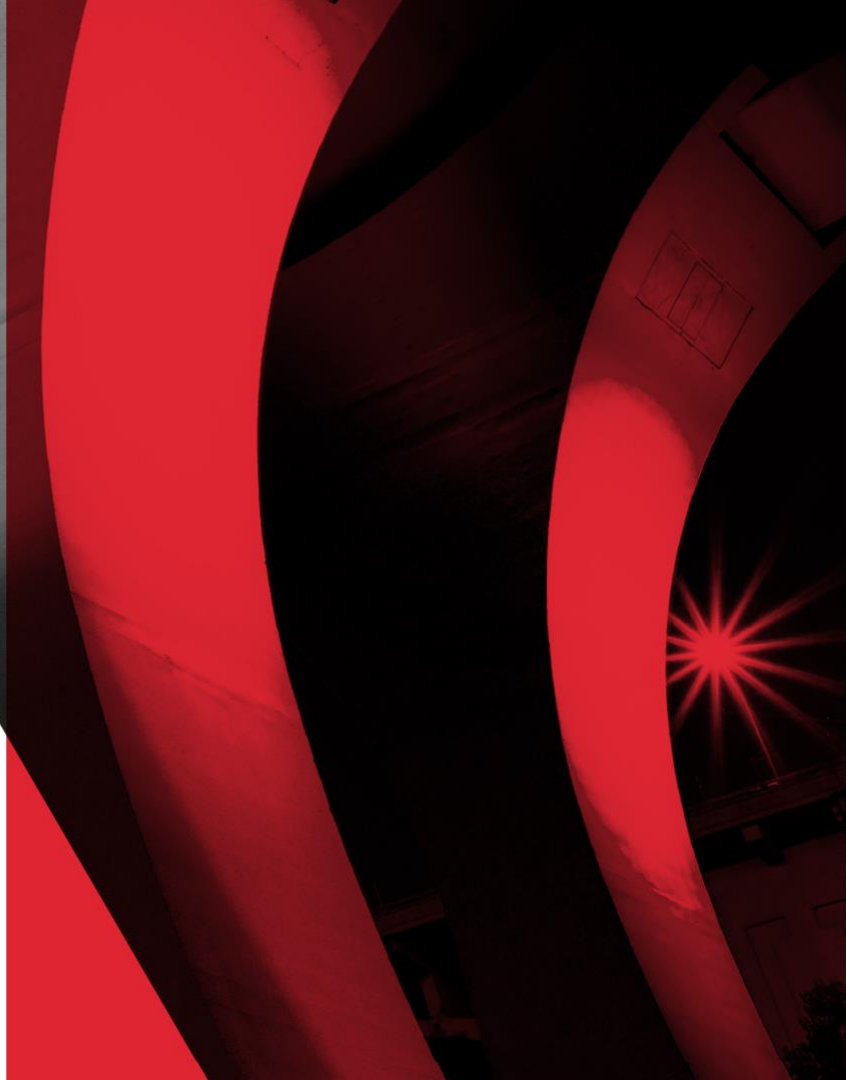
```
<ContactPerson contactType="administrative">
  <GivenName [REDACTED]/GivenName>
  <EmailAddress [REDACTED]/EmailAddress>
</ContactPerson>
<ContactPerson contactType="technical">
  <GivenName [REDACTED]/GivenName>
  <EmailAddress [REDACTED]/EmailAddress>
</ContactPerson>
<ContactPerson xmlns:remd="http://refeds.org/metadata" contactType="other" remd:contactType="http://r
  <GivenName [REDACTED]/GivenName>
  <EmailAddress [REDACTED]/EmailAddress>
</ContactPerson>
```

Previous Next



```
<EntityDescriptor entityID="https://iam.research.childrensmercy.org/idp/shibboleth">
  <Extensions>
    <mdrpi:RegistrationInfo registrationAuthority="https://incommon.org"/>
  </Extensions>
  <mdattr:EntityAttributes>
    <saml:Attribute Name="http://macedir.org/entity-category-support" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-1">
      <saml:AttributeValue>http://refeds.org/category/research-and-scholarship</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:oasis:names:tc:SAML:attribute:assurance-certification" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-1">
      <saml:AttributeValue>https://refeds.org/sirtfi</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="http://macedir.org/entity-category" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format-1">
      <saml:AttributeValue>http://id.incommon.org/category/registered-by-incommon</saml:AttributeValue>
    </saml:Attribute>
  </mdattr:EntityAttributes>
</EntityDescriptor>
<IDPSSODescriptor errorURL="https://iam.research.childrensmercy.org/pages/error.html" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" singleLogoutService="https://iam.research.childrensmercy.org/logout" singleSignOnService="https://iam.research.childrensmercy.org/identityprovider">
  <Extensions>
    <shibmd:Scope regexp="false">cmh.edu</shibmd:Scope>
  </Extensions>
  <mdul:UIInfo>
    <mdul:DisplayName xml:Lang="en">Children's Mercy Kansas City</mdul:DisplayName>
    <mdul:Description xml:Lang="en">Children's Mercy is a leading independent children's health organization dedicated to the prevention, diagnosis, and treatment of childhood diseases and conditions.
    <mdul:InformationURL xml:Lang="en">https://www.childrensmercy.org/about-us</mdul:InformationURL>
    <mdul:PrivacyStatementURL xml:Lang="en">https://www.childrensmercy.org/about-us/legal/notice-of-privacy-practices</mdul:PrivacyStatementURL>
    <mdul:Logo height="64" width="75" xml:Lang="en">https://www.childrensmercy.org/contentassets/fe72342d118245419
  </mdul:UIInfo>
  <Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <!-- Serial No. 14958619131350289721, expires on Fri Oct 22 23:23:18 2027 GMT -->
          <ds:X509Certificate>
```

TROUBLESHOOTING



Debug Logging – LogLevel Config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <variable file="{idp.home}/conf/idp.properties" />
  <variable name="idp.logfiles" value="{idp.logfiles:-{idp.home}/logs}" />
  <variable name="idp.loghistory" value="{idp.loghistory:-180}" />
  <variable name="idp.loglevel.idp" value="{idp.loglevel.idp:-DEBUG}" />
  <variable name="idp.loglevel.ldap" value="{idp.loglevel.ldap:-WARN}" />
  <variable name="idp.loglevel.messages" value="{idp.loglevel.messages:-INFO}" />
  <variable name="idp.loglevel.encryption" value="{idp.loglevel.encryption:-INFO}" />
  <variable name="idp.loglevel.opensaml" value="{idp.loglevel.opensaml:-INFO}" />
  <variable name="idp.loglevel.props" value="{idp.loglevel.props:-INFO}" />
  <variable name="idp.loglevel.httpClient" value="{idp.loglevel.httpClient:-INFO}" />
  <variable name="idp.loglevel.spring" value="{idp.loglevel.spring:-ERROR}" />
  <variable name="idp.loglevel.container" value="{idp.loglevel.container:-ERROR}" />
  <variable name="idp.loglevel.xmlsec" value="{idp.loglevel.xmlsec:-INFO}" />

```

Debug Logging – File System

The screenshot displays the Azure portal interface for an App Service web application named 'scmrishibboleth'. The main area shows a log stream with the following content:

```
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/TestSP.xml' will occur on '2023-09-04T00:04:41.556549Z' ('2023-09-04T00:04:41.556549Z')
2023-09-03T21:04:41.641845228Z shib-idp:udp-process.log:dev:nothing:2023-09-03 21:04:41.640 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:366] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' has not changed since last refresh
2023-09-03T21:04:41.644786855Z shib-idp:udp-process.log:dev:nothing:2023-09-03 21:04:41.643 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' will occur on '2023-09-04T00:04:41.641731Z' ('2023-09-04T00:04:41.641731Z')
/home/LogFiles/2023_09_03_lw1sd1wk0004L0_docker.log (https://scmrishibboleth2.scm.azurewebsites.net/api/vfs/2023-09-03T00:33:18.5642 INFO -
/home/LogFiles/2023_09_04_lw1sd1wk0004L0_default_docker.log (https://scmrishibboleth2.scm.azurewebsites.net/api/vfs/LogFiles/2023_09_04_lw1sd1wk0004L0_default_docker.log
2023-09-04T09:04:41.602524430Z shib-idp:udp-process.log:dev:nothing:2023-09-04 09:04:41.578 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:366] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/TestSP.xml' has not changed since last refresh
2023-09-04T09:04:41.602579234Z shib-idp:udp-process.log:dev:nothing:2023-09-04 09:04:41.596 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/TestSP.xml' will occur on '2023-09-04T12:04:41.581925Z' ('2023-09-04T12:04:41.581925Z')
2023-09-04T09:04:41.648733572Z shib-idp:udp-process.log:dev:nothing:2023-09-04 09:04:41.647 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:366] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' has not changed since last refresh
2023-09-04T09:04:41.651788999Z shib-idp:udp-process.log:dev:nothing:2023-09-04 09:04:41.648 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' will occur on '2023-09-04T12:04:41.647871Z' ('2023-09-04T12:04:41.647871Z')
2023-09-04T12:04:41.610793908Z shib-idp:udp-process.log:dev:nothing:2023-09-04 12:04:41.587 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:366] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/TestSP.xml' has not changed since last refresh
2023-09-04T12:04:41.632815976Z shib-idp:udp-process.log:dev:nothing:2023-09-04 12:04:41.631 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/TestSP.xml' will occur on '2023-09-04T15:04:41.593300Z' ('2023-09-04T15:04:41.593300Z')
2023-09-04T12:04:41.650861796Z shib-idp:udp-process.log:dev:nothing:2023-09-04 12:04:41.648 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:366] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' has not changed since last refresh
2023-09-04T12:04:41.662175699Z shib-idp:udp-process.log:dev:nothing:2023-09-04 12:04:41.650 - - INFO
[org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver:396] - Metadata Resolver Filesystem provider '/opt/shibboleth-idp/metadata/AzureAD-idp.xml' will occur on '2023-09-04T15:04:41.648551Z' ('2023-09-04T15:04:41.648551Z')
/home/LogFiles/2023_09_04_lw1sd1wk0004L0_docker.log (https://scmrishibboleth2.scm.azurewebsites.net/api/vfs/2023-09-04T15:04:41.648551Z INFO -
```

The left-hand navigation menu includes: SSH, Advanced Tools, API, API Management, API definition, CORS, Monitoring, Alerts, Metrics, Logs, Advisor recommendations, Health check, Diagnostic settings, App Service logs, Log stream (highlighted), Automation, Tasks (preview), and Export template.

The right-hand configuration panel shows: Application logging (Off, File System highlighted), Quota (MB) (35), Retention Period (Days), Download logs, FTP/deployment username (No FTP/de), FTP (ftp://waw), and FTPS (ftps://waw).

Debug Logging – Application Insights

The screenshot displays the Azure Application Insights interface for a web application named 'scmrishibboleth'. The left sidebar shows the 'Settings' menu with 'Application Insights' selected. A red box highlights the 'Turn on Application Insights' button. The main area shows a query editor with a 'Run' button and a table of results. The table has columns for timestamp, message, severityLevel, itemType, and customDimensions. The results show various trace messages from the application.

scmrishibboleth | Application Insights ☆ ...
Web App

Search

Settings

- Configuration
- Authentication
- Application Insights
- Identity

Enable Application Insights without redeploying your code

Turn on Application Insights

New Query 1* x +
scmrishibboleth Select scope Run Time range: Last 24 hours Save Share + New alert rule Export Pin to Format q

1 traces

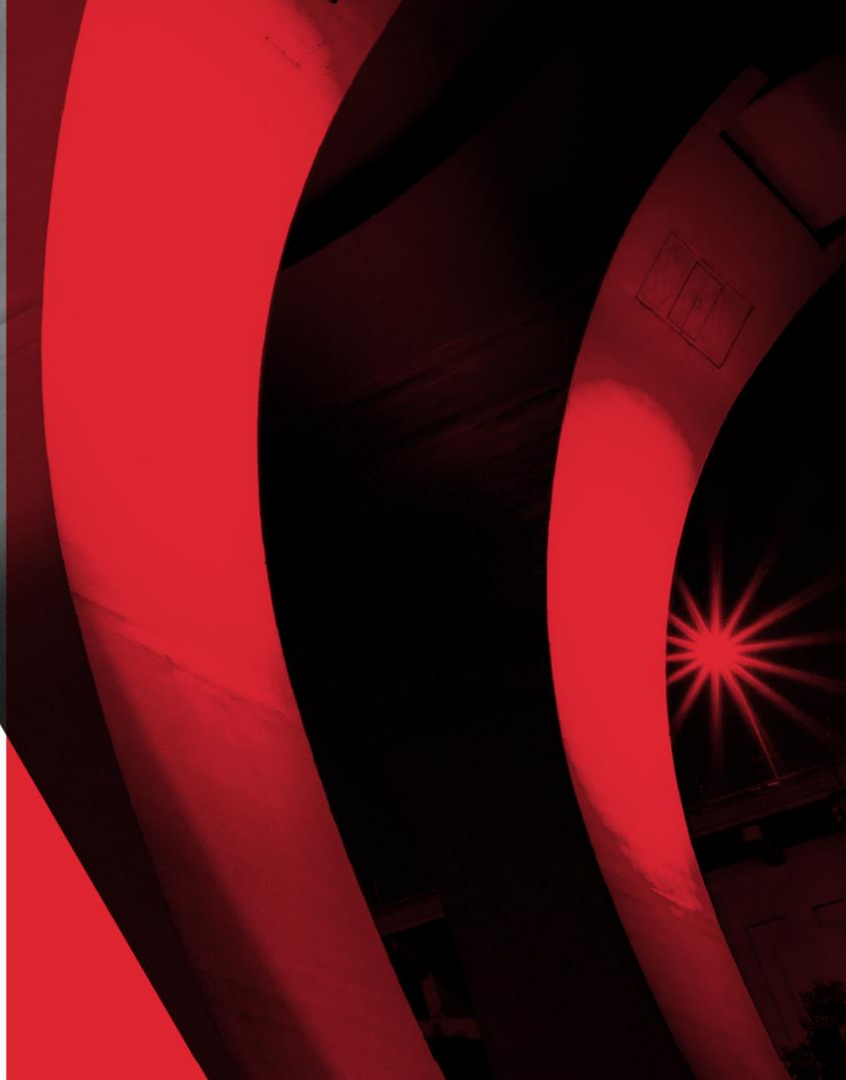
Search Filter Group by: Solution Collapse all Favorites You can add favorites by clicking on the ☆ icon

Application Insights

- availabilityResults
- browserTimings
- customEvents
- customMetrics
- dependencies
- exceptions
- pageViews
- performanceCounters
- requests
- traces

timestamp [UTC] ↑↓	message	severityLevel	itemType	customDimensions
> 9/4/2023, 1:59:50.050 PM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 1:59:50.050 PM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 1:59:49.878 PM	Metadata Resolver FilesystemMetadataResolver TestSP: Nex...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 1:59:49.877 PM	Metadata Resolver FilesystemMetadataResolver TestSP: Met...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 10:59:50.049 AM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 10:59:50.049 AM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 10:59:49.877 AM	Metadata Resolver FilesystemMetadataResolver TestSP: Met...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 10:59:49.877 AM	Metadata Resolver FilesystemMetadataResolver TestSP: Nex...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 10:25:01.586 AM	Metadata Resolver FunctionDrivenDynamicHTTPMetadataRe...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 7:59:50.047 AM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 7:59:50.047 AM	Metadata Resolver FilesystemMetadataResolver AzureAD-id...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 7:59:49.876 AM	Metadata Resolver FilesystemMetadataResolver TestSP: Met...	1	trace	{\"LoggerName\":\"org.opens
> 9/4/2023, 7:59:49.876 AM	Metadata Resolver FilesystemMetadataResolver TestSP: Nex...	1	trace	{\"LoggerName\":\"org.opens

QUESTIONS?



CONFIG TEMPLATES

The background features a dynamic composition of curved, overlapping shapes. On the left, a large white triangular area is bordered by a grey curved shape. To the right, a vibrant red curved shape dominates the foreground, partially overlapping a dark, almost black, curved shape. In the lower right quadrant, a bright red starburst light with multiple rays emanates from a point, adding a focal point of energy to the design.

global.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
  xmlns:context="http://www.springframework.org/schema/context"
  xmlns:util="http://www.springframework.org/schema/util"
  xmlns:p="http://www.springframework.org/schema/p"
  xmlns:c="http://www.springframework.org/schema/c"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd
  http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context.xsd
  http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util.xsd"

  default-init-method="initialize"
  default-destroy-method="destroy">

  <util:list id="shibboleth.c14n.attribute.AttributesToResolve">
  <value>canonicalNameToUseForJoin</value>
  </util:list>
  <util:list id="shibboleth.c14n.attribute.AttributeSourceIds">
  <value>canonicalNameToUseForJoin</value>
  </util:list>

  <bean id="shibboleth.authn.SAML.discoveryFunction"
parent="shibboleth.Functions.Constant"
  c:target="[AZURE REGISTRATION HOST]" />
</beans>
```

metadata-providers.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"
  xmlns="urn:mace:shibboleth:2.0:metadata"
  xmlns:security="urn:mace:shibboleth:2.0:security"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:alg="urn:oasis:names:tc:SAML:metadata:alg:support"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:ds11="http://www.w3.org/2009/xmldsig11#"
  xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:enc11="http://www.w3.org/2009/xmlenc11#"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:metadata
http://shibboleth.net/schema/idp/shibboleth-metadata.xsd
  urn:mace:shibboleth:2.0:security
http://shibboleth.net/schema/idp/shibboleth-security.xsd
  urn:oasis:names:tc:SAML:2.0:assertion http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-assertion-2.0.xsd
  urn:oasis:names:tc:SAML:2.0:metadata http://docs.oasis-
open.org/security/saml/v2.0/saml-schema-metadata-2.0.xsd
  urn:oasis:names:tc:SAML:metadata:alg:support
http://docs.oasis-open.org/security/saml/Post2.0/sssc-saml-metadata-alg:support-
v1.0.xsd
  http://www.w3.org/2000/09/xmldsig#
http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/xmldsig-core-schema.xsd
  http://www.w3.org/2009/xmldsig11#
http://www.w3.org/TR/2013/REC-xmldsig-core1-20130411/xmldsig11-schema.xsd
  http://www.w3.org/2001/04/xmlenc#
http://www.w3.org/TR/xmlenc-core/xenc-schema.xsd
  http://www.w3.org/2009/xmlenc11#
http://www.w3.org/TR/2013/REC-xmlenc-core1-20130411/xenc-schema-11.xsd"
  sortKey="1">
  <MetadataProvider id="incommon" xsi:type="DynamicHTTPMetadataProvider"
    maxCacheDuration="PT24H" minCacheDuration="PT10M">
    <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
      certificateFile="%{idp.home}/credentials/inc-md-cert-mdq.pem" />
    <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D" />
    <MetadataQueryProtocol>https://mdq.incommon.org/</MetadataQueryProtocol>
  </MetadataProvider>
  <MetadataProvider id="AzureAD-idp-metadata"
    xsi:type="FilesystemMetadataProvider"
    metadataFile="/opt/shibboleth-idp/metadata/AzureAD-idp.xml" />
</MetadataProvider>
```

idp-metadata.xml

```
<EntityDescriptor entityID="https://[HOST]/ldp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  <Extensions base="urn:mace:shibboleth:1.0" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" />
  <Extensions base="urn:mace:shibboleth:1.0" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" />
  <KeyDescriptor use="signing">
    <ds:KeyInfo>
      <ds:XB2Data>
        <ds:XB2Certificate>
          [SIGNING KEY]
        </ds:XB2Certificate>
      </ds:KeyInfo>
    </KeyDescriptor>
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect">
    Location="https://[HOST]/ldp/profile/SAML2/Redirect/SSO/"
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
    Location="https://[HOST]/ldp/profile/SAML2/POST/SSO/"
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign">
    Location="https://[HOST]/ldp/profile/SAML2/POST-SimpleSign/SSO/"
  <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP">
    Location="https://[HOST]/ldp/profile/SAML2/SOAP/ECSP/"
  </IDPSSODescriptor>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:XB2Data>
          <ds:XB2Certificate>
            [SIGNING KEY]
          </ds:XB2Certificate>
        </ds:KeyInfo>
      </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <ds:KeyInfo>
        <ds:XB2Data>
          <ds:XB2Certificate>
            [ENCRYPTION KEY]
          </ds:XB2Certificate>
        </ds:KeyInfo>
      </KeyDescriptor>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST">
      Location="https://[HOST]/ldp/profile/Authn/SAML2/POST/SSO" index="0"/>
  </SPSSODescriptor>
</EntityDescriptor>
```

subject-c14n.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
xmlns:context="http://www.springframework.org/schema/context"
xmlns:url="http://www.springframework.org/schema/url"
xmlns:ps="http://www.springframework.org/schema/ps"
xmlns:ds="http://www.springframework.org/schema/ds"
xmlns: xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://www.springframework.org/schema/beans http://www.springframework.org/schema/beans/spring-beans.xsd
http://www.springframework.org/schema/context http://www.springframework.org/schema/context/spring-context.xsd
http://www.springframework.org/schema/url http://www.springframework.org/schema/url/spring-url.xsd"
default-lazy="true">
  <default-method="initInit"/>
  <default-destroy="destroy"/>
  <util:list id="shibboleth.PostInitSubjectCanonicalizationFlows">
    <bean id="c14n/attribute" parent="shibboleth.PostInitSubjectCanonicalizationFlow" />
    <ref bean="c14n/SAMLTransform" />
    <ref bean="c14n/SIP" />
    <ref bean="c14n/SIPv1" />
  </util:list>
  <util:list id="shibboleth.ProxyNameTransformFormats">
    <valueurn:oasis:names:tc:SAML:1.1:namespace-format:unspecified/>
    <valueurn:oasis:names:tc:SAML:1.1:namespace-format:emailAddress/>
    <valueurn:oasis:names:tc:SAML:1.1:namespace-format:XB2SubjectName/>
    <valueurn:oasis:names:tc:SAML:1.1:namespace-format:windowsDomainQualifiedName/>
    <valueurn:oasis:names:tc:SAML:2.0:namespace-format:kerberos/>
  </util:list>
  <bean id="shibboleth.ProxyNameTransformPredicate" parent="shibboleth.Conditions.ProxyAuthentication">
    <constructor-arg name="collection">
      <list>
        </list>
      </constructor-arg>
    </bean>
    <util:list id="shibboleth.ProxyNameTransforms">
      </util:list>
    <util:list id="shibboleth.SAMLSubjectCanonicalizationFlows">
      <ref bean="c14n/SAMLTransform" />
      <ref bean="c14n/SAML2CryptoTransform" />
      <ref bean="c14n/SAMLTransform" />
      <ref bean="c14n/SAML2CryptoTransform" />
      <ref bean="c14n/SAMLTransform" />
    </util:list>
    <util:list id="shibboleth.NameTransformFormats">
      <valueurn:oasis:names:tc:SAML:1.1:namespace-format:unspecified/>
      <valueurn:oasis:names:tc:SAML:1.1:namespace-format:emailAddress/>
      <valueurn:oasis:names:tc:SAML:1.1:namespace-format:XB2SubjectName/>
      <valueurn:oasis:names:tc:SAML:1.1:namespace-format:windowsDomainQualifiedName/>
      <valueurn:oasis:names:tc:SAML:2.0:namespace-format:kerberos/>
    </util:list>
    <bean id="shibboleth.NameTransformPredicate" parent="shibboleth.Conditions.RelyingPartyId">
      <constructor-arg name="candidates">
        <list>
          </list>
        </constructor-arg>
      </bean>
    <util:list id="shibboleth.NameTransforms">
      </util:list>
  </beans>
```

attribute-filter.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeFilterPolicyGroup id="ShibbolethFilterPolicy"
  xmlns:urn:mace:shibboleth:2.0:afp
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:afp http://shibboleth.net/schema/idp/shibboleth-afp.xsd">
  <AttributeFilterPolicy id="releaseAndAttributeBundle">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
      attributeValue="http://macedir.org/entity-category">
      <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="eduPersonAssurance">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="sn">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
    </AttributeFilterPolicy>
  </>
  <!-- Attribute release for all InCommon SPs -->
  <AttributeFilterPolicy id="releaseInCommon">
    <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
      attributeValue="http://id.incommon.org/category/registered-by-incommon">
      <AttributeRule attributeID="eduPersonPrincipalName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="eduPersonScopedAffiliation">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="givenName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="sn">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="displayName">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
      <AttributeRule attributeID="mail">
        <PermitValueRule xsi:type="ANY" />
      </AttributeRule>
    </AttributeFilterPolicy>
  </>
  <AttributeFilterPolicy id="FilterPolicyObjectProxy-FromAzureByIssuer-Type">
    <PolicyRequirementRule xsi:type="Issuer" value="Azure REGISTRATION HDST" />
    <AttributeRule attributeID="azureDisplayName" permittAny="true" />
    <AttributeRule attributeID="azureGivenName" permittAny="true" />
    <AttributeRule attributeID="azureSurname" permittAny="true" />
    <AttributeRule attributeID="azureAuthnMethodReferences" permittAny="true" />
    <AttributeRule attributeID="azureIdentityProvider" permittAny="true" />
    <AttributeRule attributeID="azureTenantId" permittAny="true" />
    <AttributeRule attributeID="azureEmailAddress" permittAny="true" />
    <AttributeRule attributeID="azureObjectIdentifier" permittAny="true" />
    <AttributeRule attributeID="azureAssurance" permittAny="true" />
    <AttributeRule attributeID="azureAffiliation" permittAny="true" />
    <AttributeRule attributeID="azureName">
      <PermitValueRule xsi:type="Scope" value="SCOPE" ignoreCase="true" />
    </AttributeRule>
  </AttributeFilterPolicy>
</AttributeFilterPolicyGroup>
```

attribute-resolver.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<AttributeResolver
  xmlns:urn:mace:shibboleth:2.0:resolver"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="urn:mace:shibboleth:2.0:resolver
  http://shibboleth.net/schema/idp/shibboleth-attribute-resolver.xsd">
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="mail"
    principalAttributeName="azureEmailAddress" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="displayName"
    principalAttributeName="azureDisplayName" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="sn"
    principalAttributeName="azureSurname" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="givenName"
    principalAttributeName="azureGivenName" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="eduPersonTargetedID"
    principalAttributeName="azureObjectIdentifier" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="eduPersonAssurance"
    principalAttributeName="azureAssurance" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="eduPersonPrincipalName"
    principalAttributeName="azureName" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="false"
    id="eduPersonScopedAffiliation"
    principalAttributeName="azureAffiliation" />
  <AttributeDefinition xsi:type="SubjectDerivedAttribute"
    forCanonicalization="true"
    id="canonicalNameToUseForJoin"
    principalAttributeName="azureName" />
  <DataConnector id="passthroughAttributes" xsi:type="Subject" exportAttributes="azureName
  azureEmailAddress
  azureDisplayName azureGivenName azureSurname azureTenantId azureObjectIdentifier
  azureIdentityProvider
  azureAuthnMethodReferences azureAssurance azureAffiliation" />
</AttributeResolver>
```

default_rules.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<beans xmlns="http://www.springframework.org/schema/beans"
       xmlns:context="http://www.springframework.org/schema/context"
       xmlns:util="http://www.springframework.org/schema/util"
       xmlns:p="http://www.springframework.org/schema/p"
       xmlns:c="http://www.springframework.org/schema/c"
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:schemaLocation="http://www.springframework.org/schema/beans
http://www.springframework.org/schema/beans/spring-beans.xsd
                           http://www.springframework.org/schema/context
http://www.springframework.org/schema/context/spring-context.xsd
                           http://www.springframework.org/schema/util
http://www.springframework.org/schema/util/spring-util.xsd"

       default-init-method="initialize"
       default-destroy-method="destroy">
  <import resource="inetOrgPerson.xml" />
  <import resource="eduPerson.xml" />
  <import resource="eduCourse.xml" />
  <import resource="schac.xml" />
  <import resource="samlSubject.xml" />
  <import resource="azureClaims.xml" />
</beans>
```


idp.properties

```
idp.searchForProperties=true
idp.additionalProperties=/credentials/secrets.properties
idp.entityID=https://[HOST]/idp/shibboleth
idp.scope=[SCOPE (e.g. *.edu)]
idp.csrf.enabled=true
idp.sealer.storeResource=%{idp.home}/credentials/sealer.jks
idp.sealer.versionResource=%{idp.home}/credentials/sealer.kver
idp.signing.key=%{idp.home}/credentials/idp-signing.key
idp.signing.cert=%{idp.home}/credentials/idp-signing.crt
idp.encryption.key=%{idp.home}/credentials/idp-encryption.key
idp.encryption.cert=%{idp.home}/credentials/idp-encryption.crt
idp.encryption.config=shibboleth.EncryptionConfiguration.GCM
idp.trust.signatures=shibboleth.ExplicitKeySignatureTrustEngine
idp.trust.certificates=shibboleth.ExplicitKeyX509TrustEngine
idp.storage.htmlLocalStorage=true
idp.session.trackSPSessions=true
idp.session.secondaryServiceIndex=true
idp.bindings.inMetadataOrder=false
idp.ui.fallbackLanguages=en,fr,de
idp.audit.shortenBindings=true
```

authn.properties

```
idp.authn.flows = SAML
idp.authn.External.externalAuthnPath = contextRelative:external.jsp
idp.authn.SPNEGO.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos, \
    sam11/urn:ietf:rfc:1510
idp.authn.X509.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:X509, \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, \
    sam11/urn:ietf:rfc:2246
idp.authn.X509Internal.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:X509, \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, \
    sam11/urn:ietf:rfc:2246
idp.authn.IPAddress.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
idp.authn.Duo.supportedPrincipals = \
    sam12/http://example.org/ac/classes/mfa, \
    sam11/http://example.org/ac/classes/mfa
idp.authn.SAML.nonBrowserSupported = false
idp.authn.SAML.passiveAuthenticationSupported = true
idp.authn.SAML.forcedAuthenticationSupported = true
idp.authn.SAML.proxyScopingEnforced = true
idp.authn.SAML.discoveryRequired = true
idp.authn.SAML.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport, \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes>Password, \
    sam11/urn:oasis:names:tc:SAML:1.0:am:password, \
    https://refeds.org/profile/mfa
idp.authn.MFA.supportedPrincipals = \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol, \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes>PasswordProtectedTransport, \
    sam12/urn:oasis:names:tc:SAML:2.0:ac:classes>Password, \
    sam11/urn:oasis:names:tc:SAML:1.0:am:password
```

server.xml

```
<?xml version='1.0' encoding='utf-8'?>
<Server port="8005" shutdown="SHUTDOWN">
  <Listener className="org.apache.catalina.core.AprLifecycleListener"
  SSLEngine="on" />
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener" />

  <Service name="Catalina">
    <Connector
      protocol="org.apache.coyote.http11.Http11NioProtocol"
      port="443" maxThreads="200"
      scheme="https" secure="true" SSLEnabled="true"
      keystoreFile="/opt/certs/keystore.jks" keystorePass="[PWD]"
      clientAuth="false" sslProtocol="TLS"/>

    <Connector
      port="8080" maxThreads="150"
      enableLookups="false" connectionTimeout="20000" maxHttpHeaderSize="65536"
    />

  <Engine name="Catalina" defaultHost="localhost">
    <Host name="localhost" appBase="webapps" unpackWARs="true"
    autoDeploy="true">
      <Valve className="org.apache.catalina.valves.RemoteIpValve"/>
      <Valve className="org.apache.catalina.valves.AccessLogValve"
      directory="logs"
        prefix="localhost_access_log." suffix=".txt"
        pattern="combined" />
      <Valve className="org.apache.catalina.valves.ErrorReportValve"
      showReport="false" showServerInfo="false" />
    </Host>
  </Engine>
</Service>
</Server>
```

deployment.ps1

```
$SUB = ""
$ACR = ""
$RG = ""
$REGION = ""
$ACRPWD = ""

az login
az account set --subscription $SUB

az acr login --name $ACR

docker build . -t "$ACR.azurecr.io/shib-idp:testing"
docker push "$ACR.azurecr.io/shib-idp:testing"
```