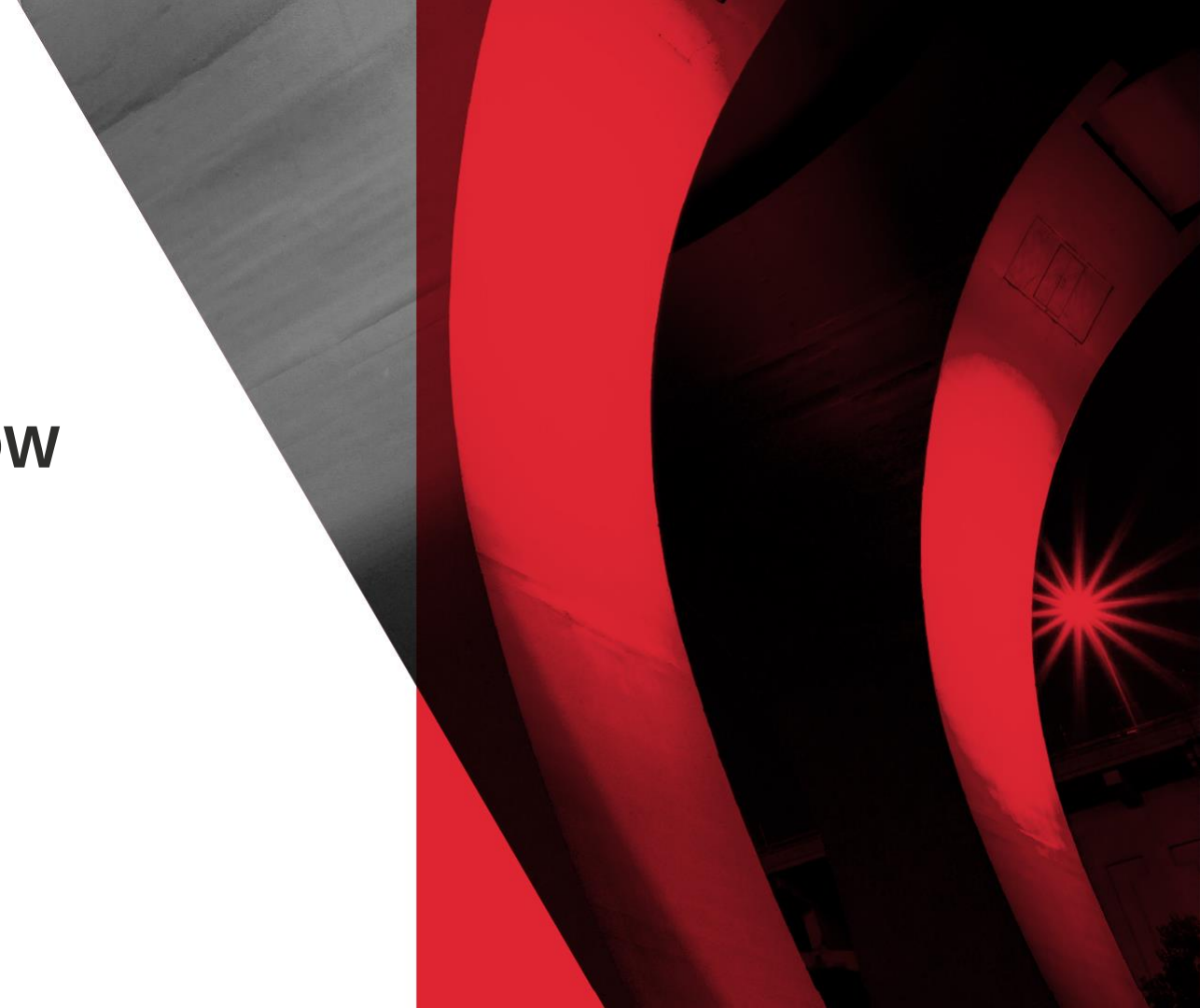
2023 INTERNET2 TECHNOLOGY exchange

Azure AD Proxying For InCommon Federation

Jared Johnson
Senior Software Engineer, Childrens Mercy Research Institute

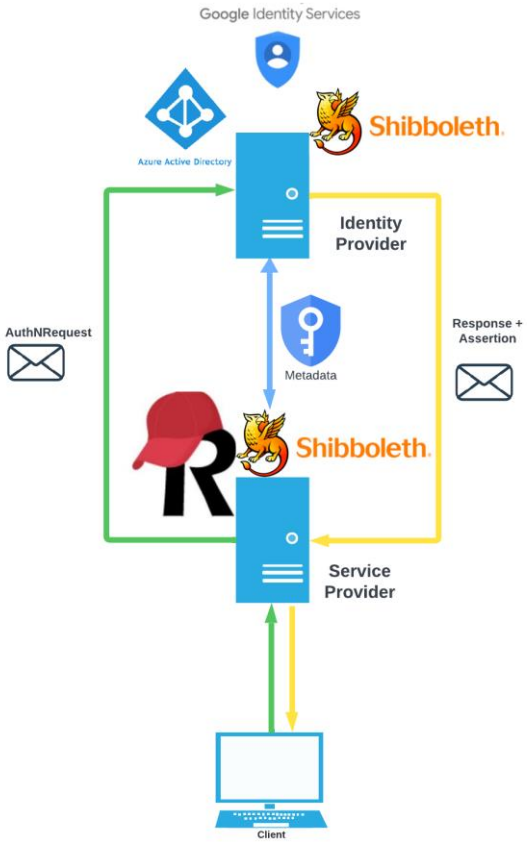
Table of Contents

SAML2 FLOW

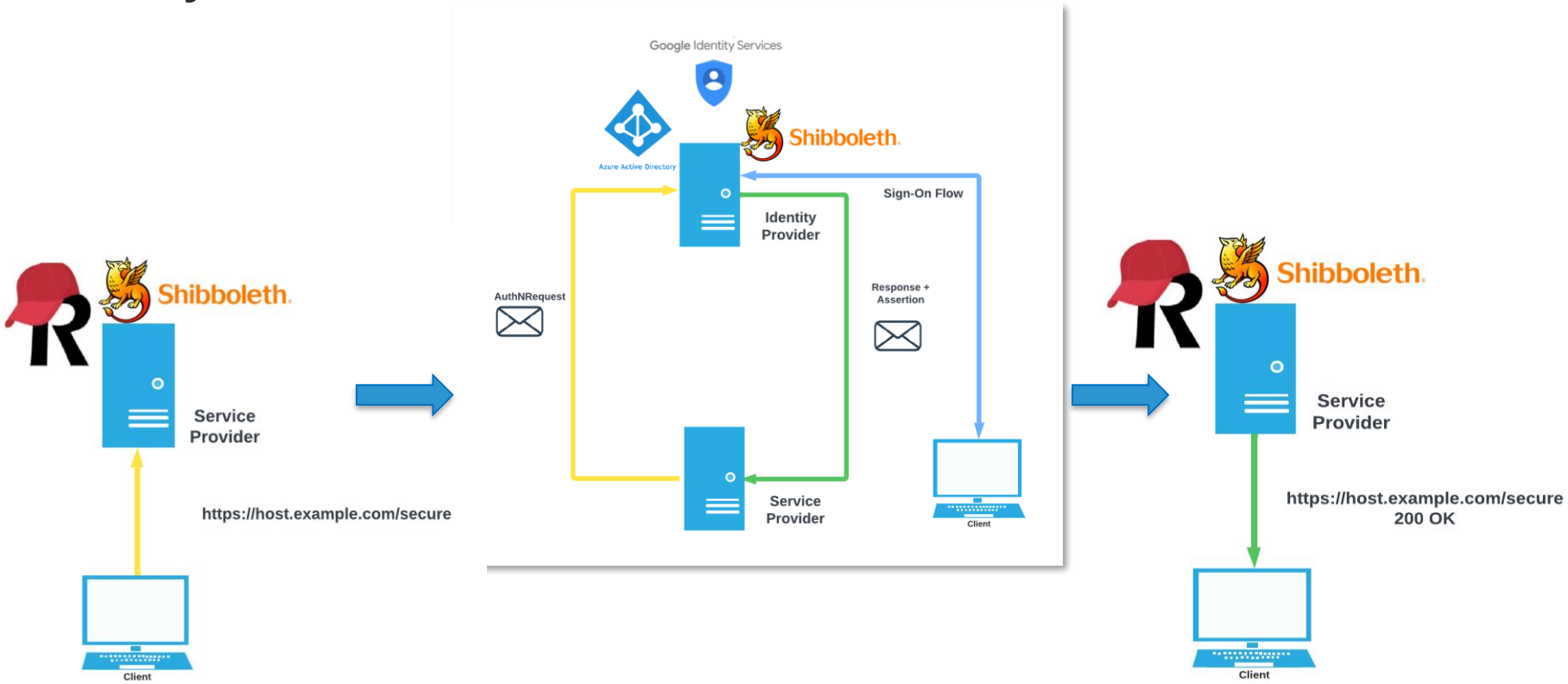


SAML 2 Key Concepts

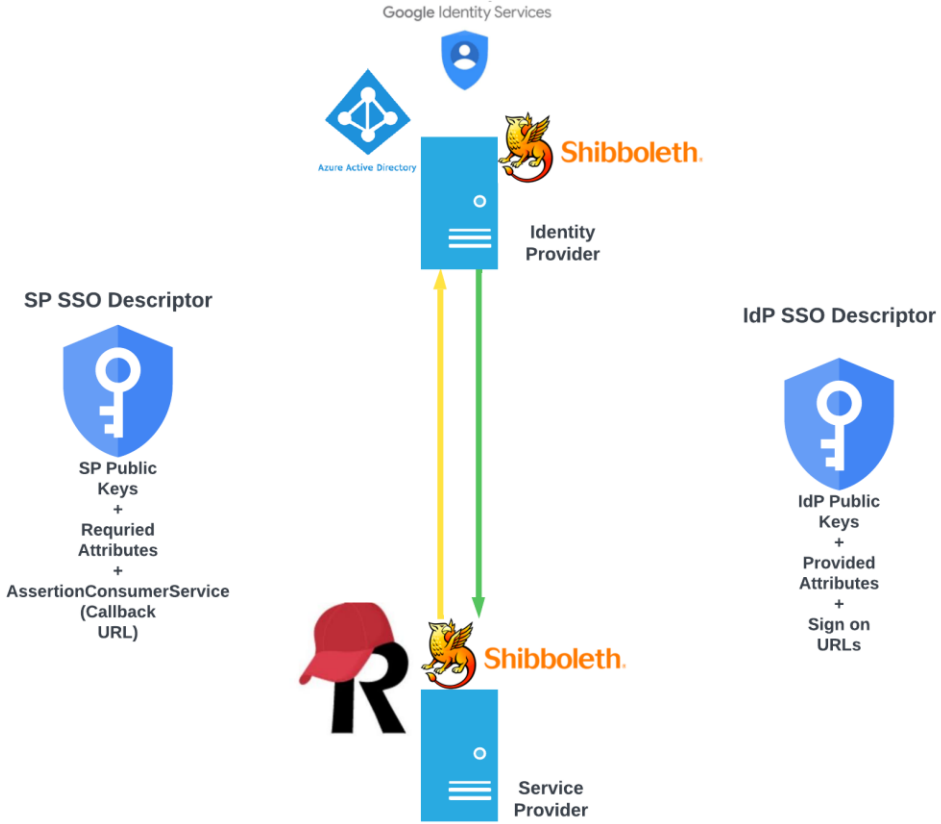
- Service Provider
- Identity Provider
- Metadata
- AuthNRequest
- Response + Assertion



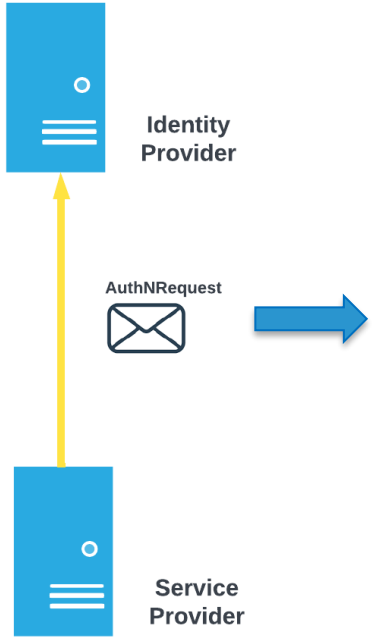
Identity\Service Provider



Metadata


Google Identity Services
Azure Active Directory
Shibboleth
Identity Provider
SP SSO Descriptor
SP Public Keys + Requried Attributes + AssertionConsumerService (Callback URL)
IdP SSO Descriptor
IdP Public Keys + Provided Attributes + Sign on URLs
Shibboleth
Service Provider

AuthNRequest

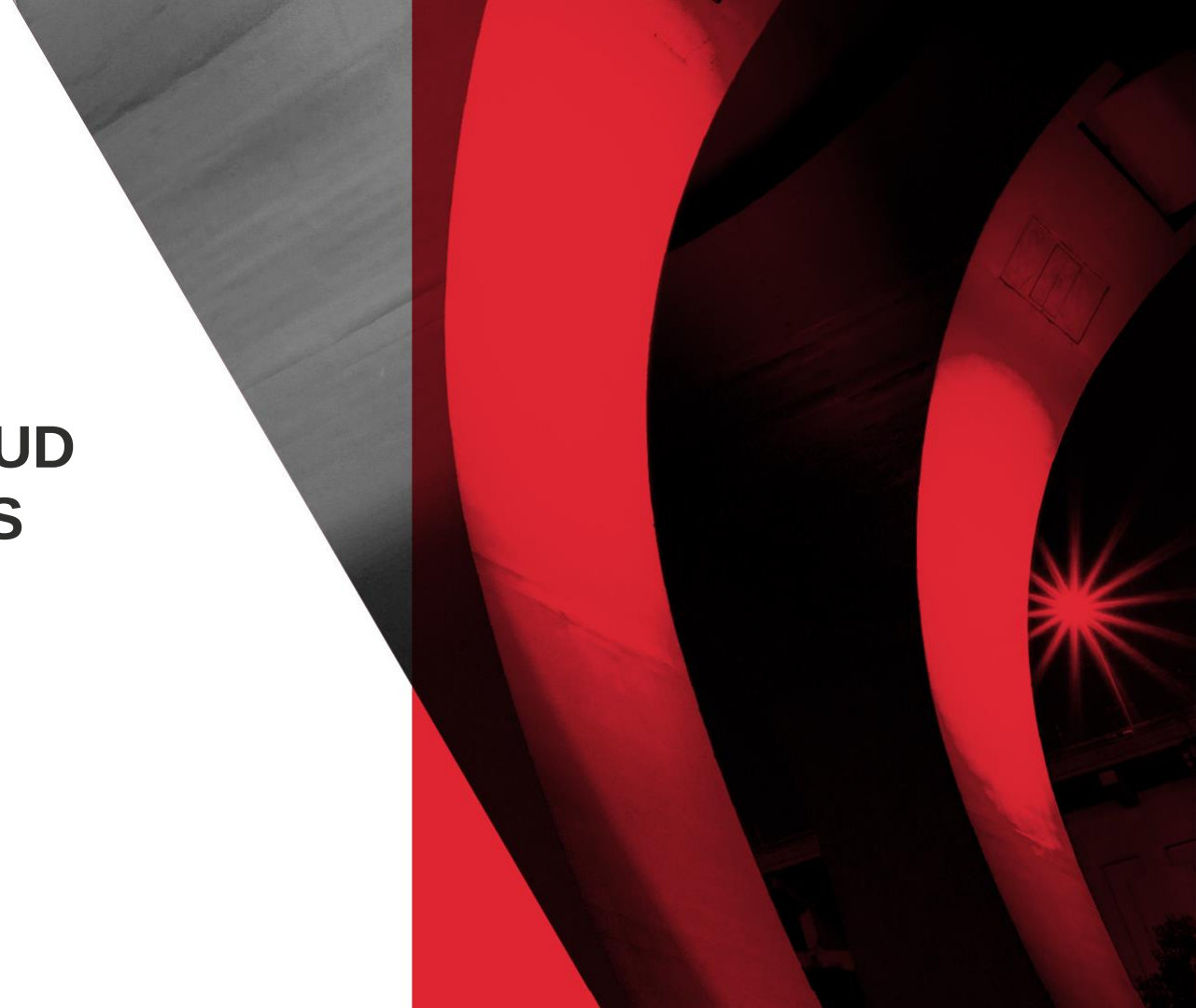



```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
                    ID="LOGIN_GUID_12312312312928783723"
                    Version="2.0"
                    ProviderName="Example SP"
                    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

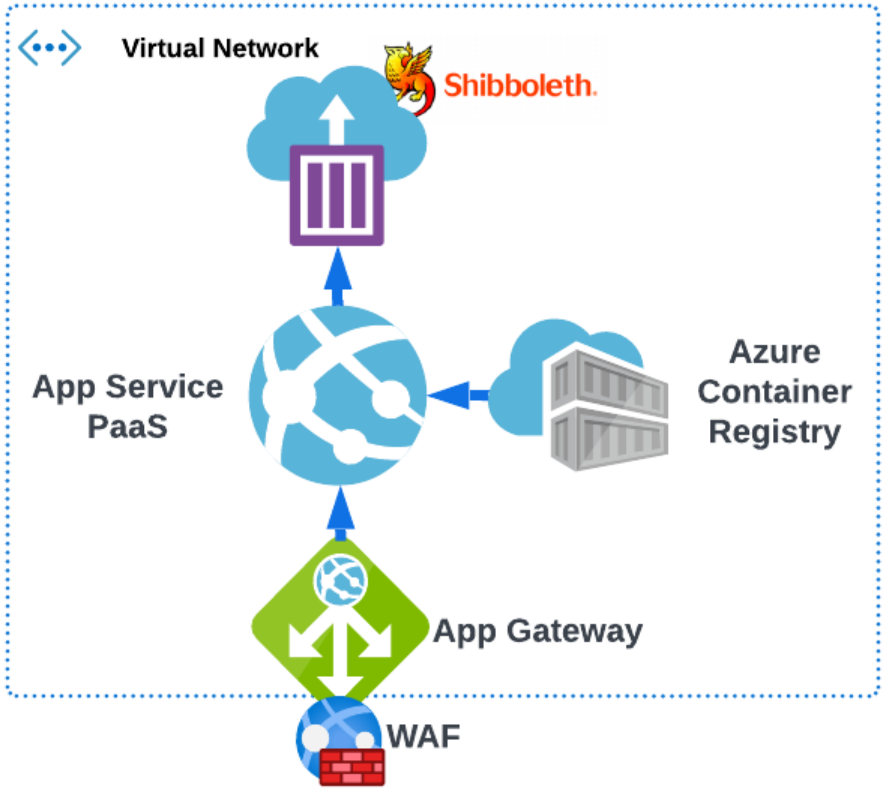

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="_8e8dc5f69a98cc4c1ff3427e5ce34606fd672f91e6" Ve
  <saml:Issuer>http://example.host.idp</saml:Issuer>
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </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
    <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="_be9967abd904ddcae3c0eb4189adbe3f71e327cf93">
      <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



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.

Container Registry

A repository for docker images

App Service Plan

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

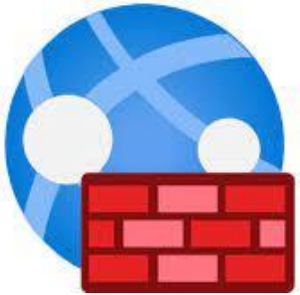
Virtual Network

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

Application Gateway

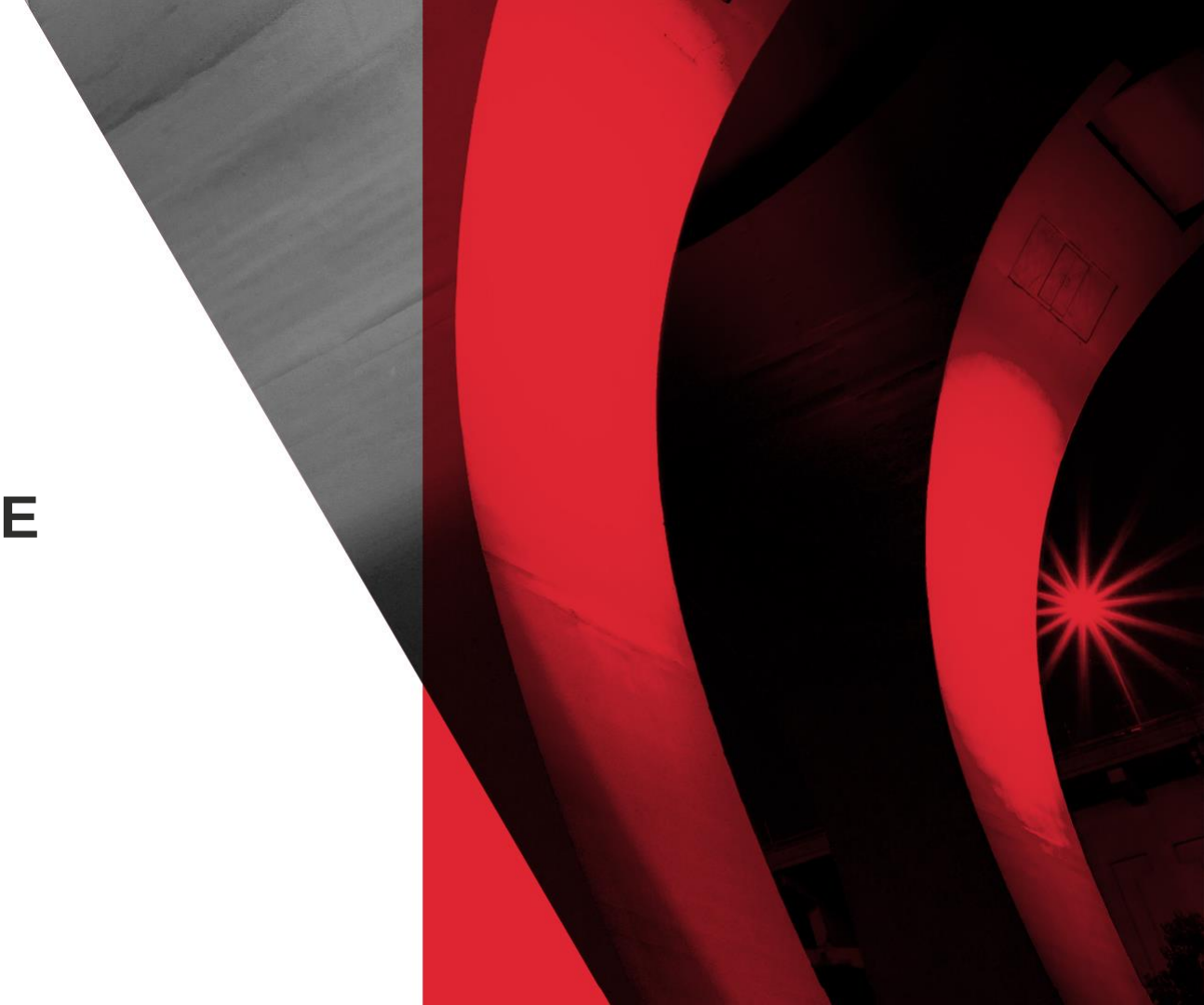
Ingress controller for the Azure Virtual Network\Applications

Web Application Firewall (WAF)



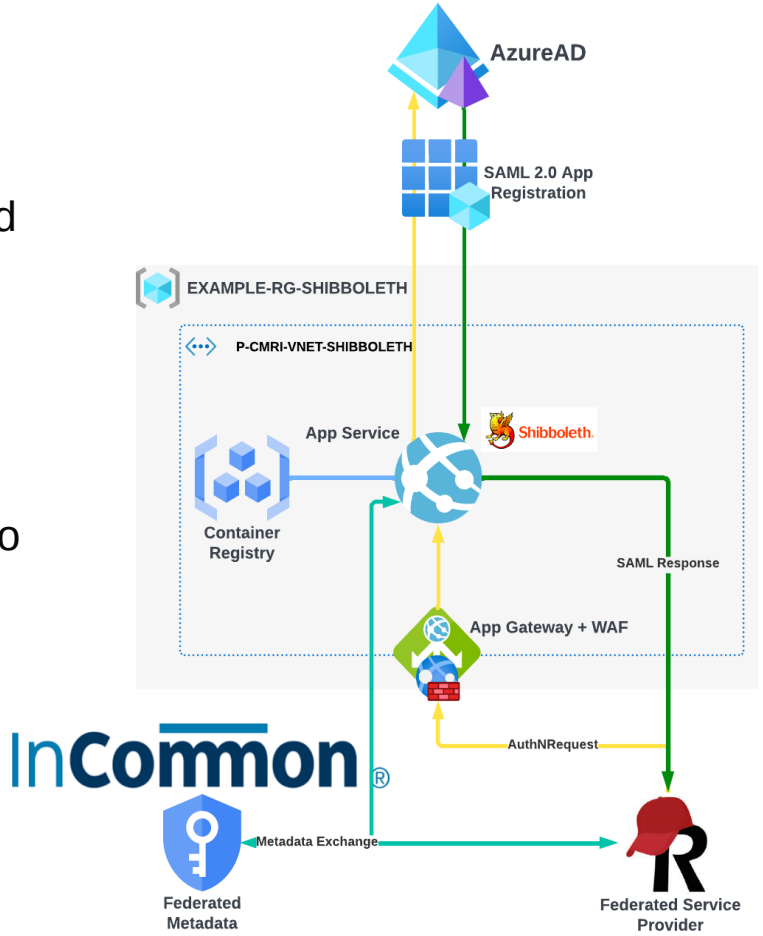
Firewall service mounted to our ingress to inspect requests and protect our resources

AZURE RESOURCE SETUP

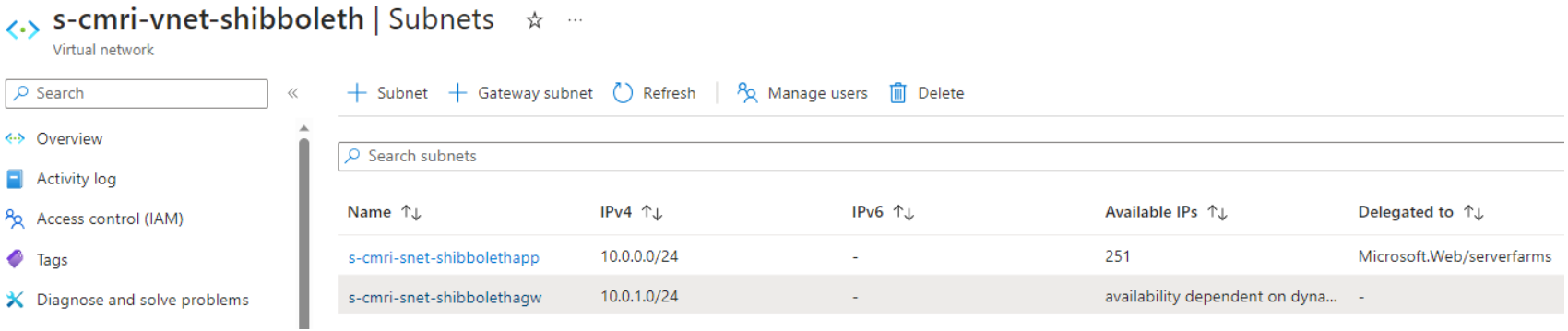


Overall Architecture

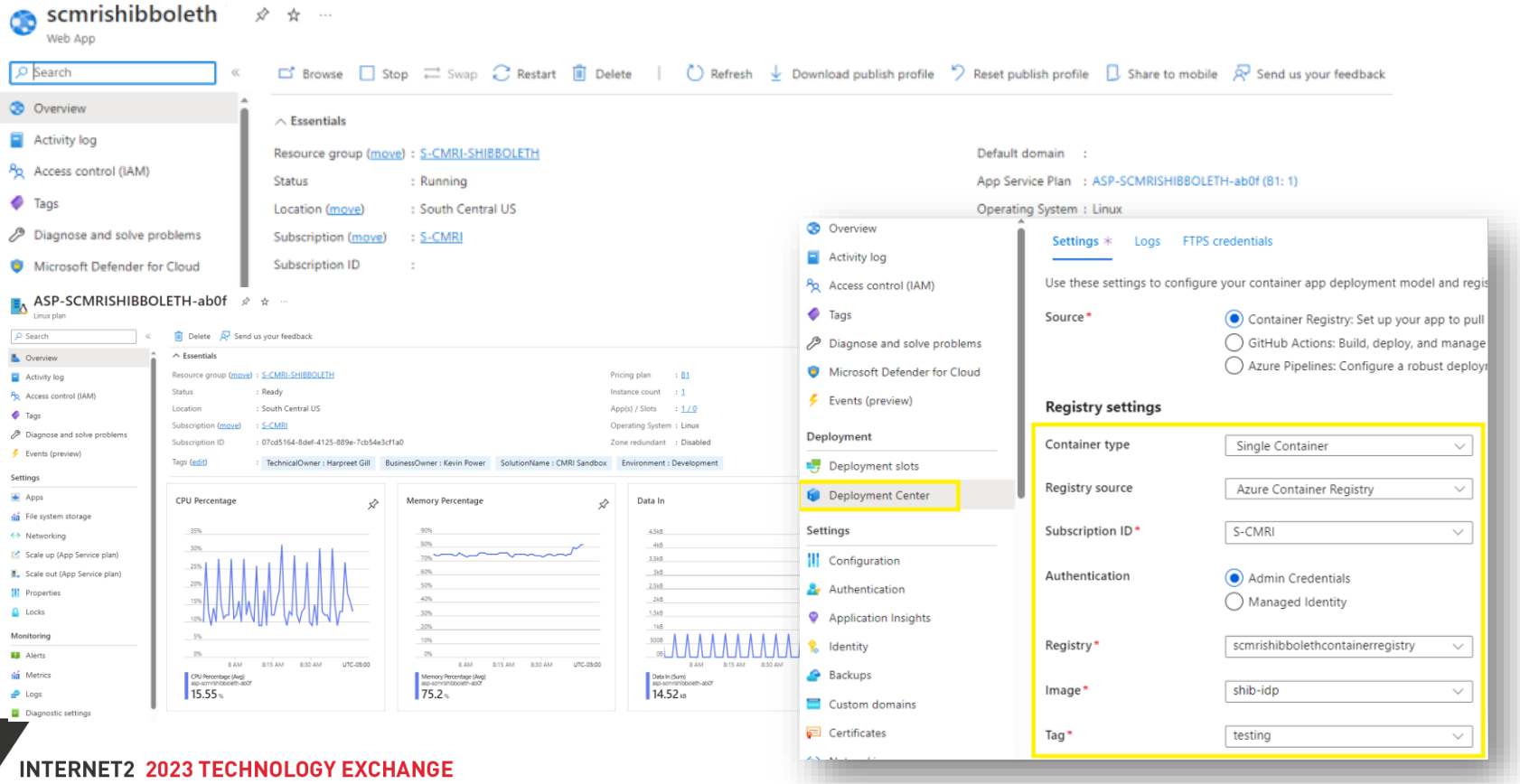
- App Service hosts Shibboleth as SP and IdP
- Azure AD exposes SAML 2.0 sign on endpoints
- Gateway + WAF exposes App Service to public internet
- Container registry stores configured Shibboleth Docker image.



Resource Framing



Compute Resources



WAF, Reverse Proxy, Load Balancer

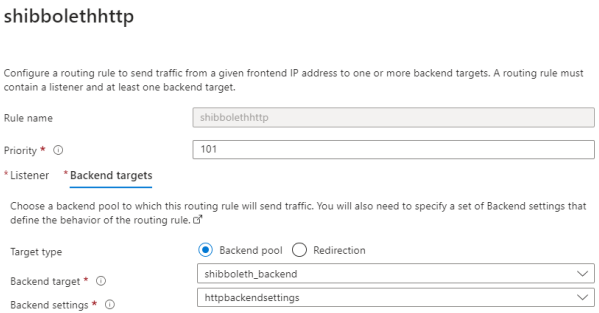
Listeners | Listener TLS certificates (Preview)

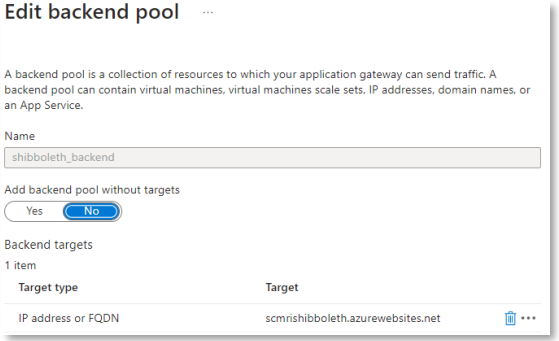
+ Add listener | Refresh

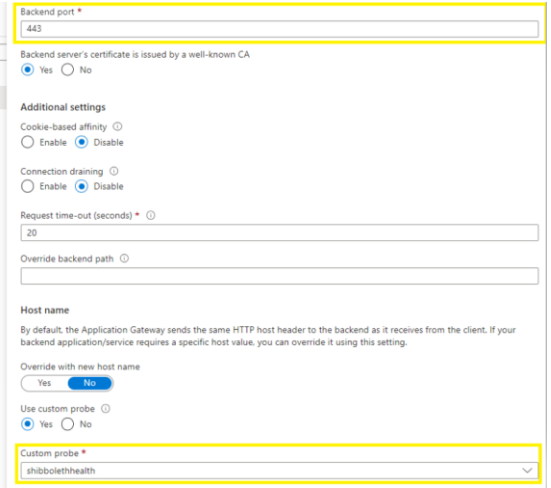
Application Gateway provides native support for WebSocket across all gateway sizes. There is no additional configuration required to enable or disable WebSocket support. If a Web automatically directed to the WebSocket enabled backend server using the appropriate backend pool as specified in application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

Search listeners

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

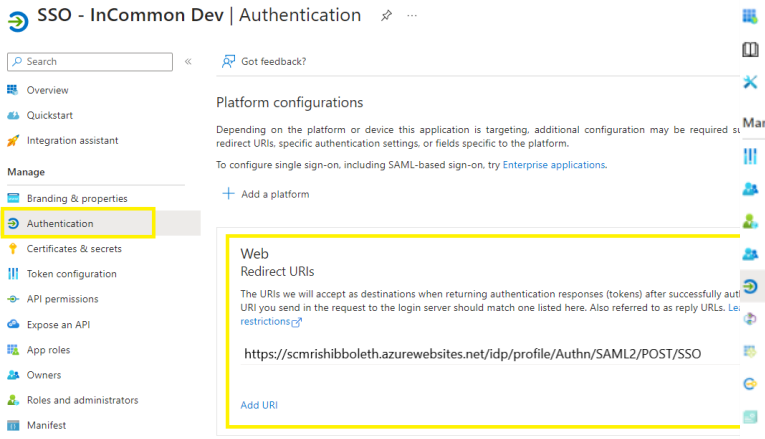




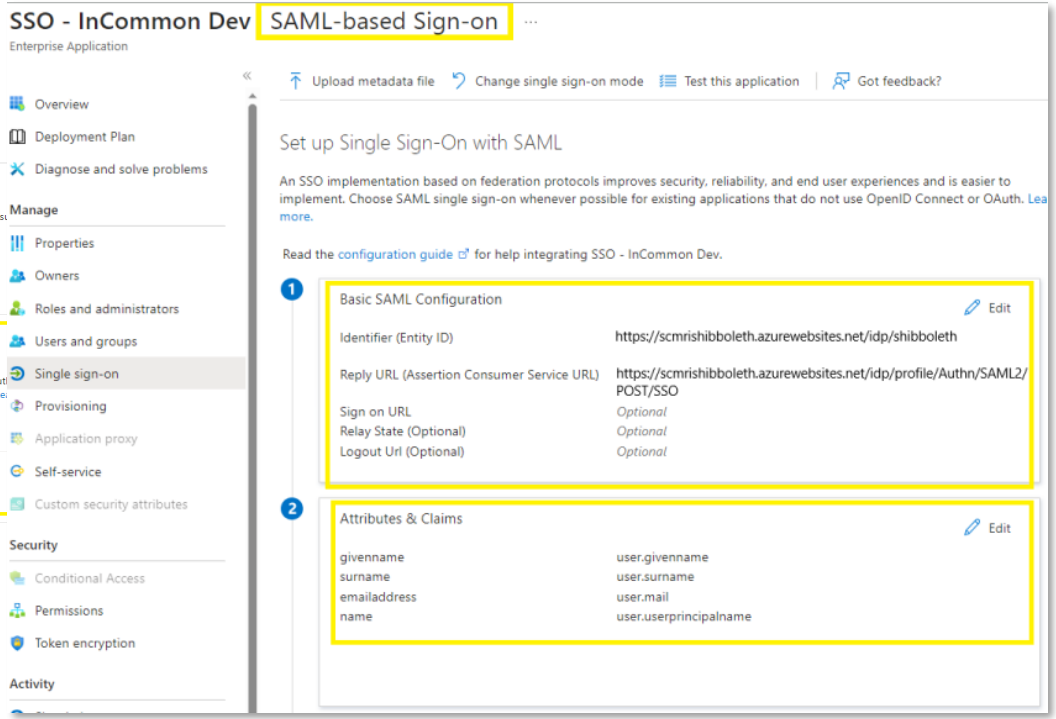


Enterprise App + Registration

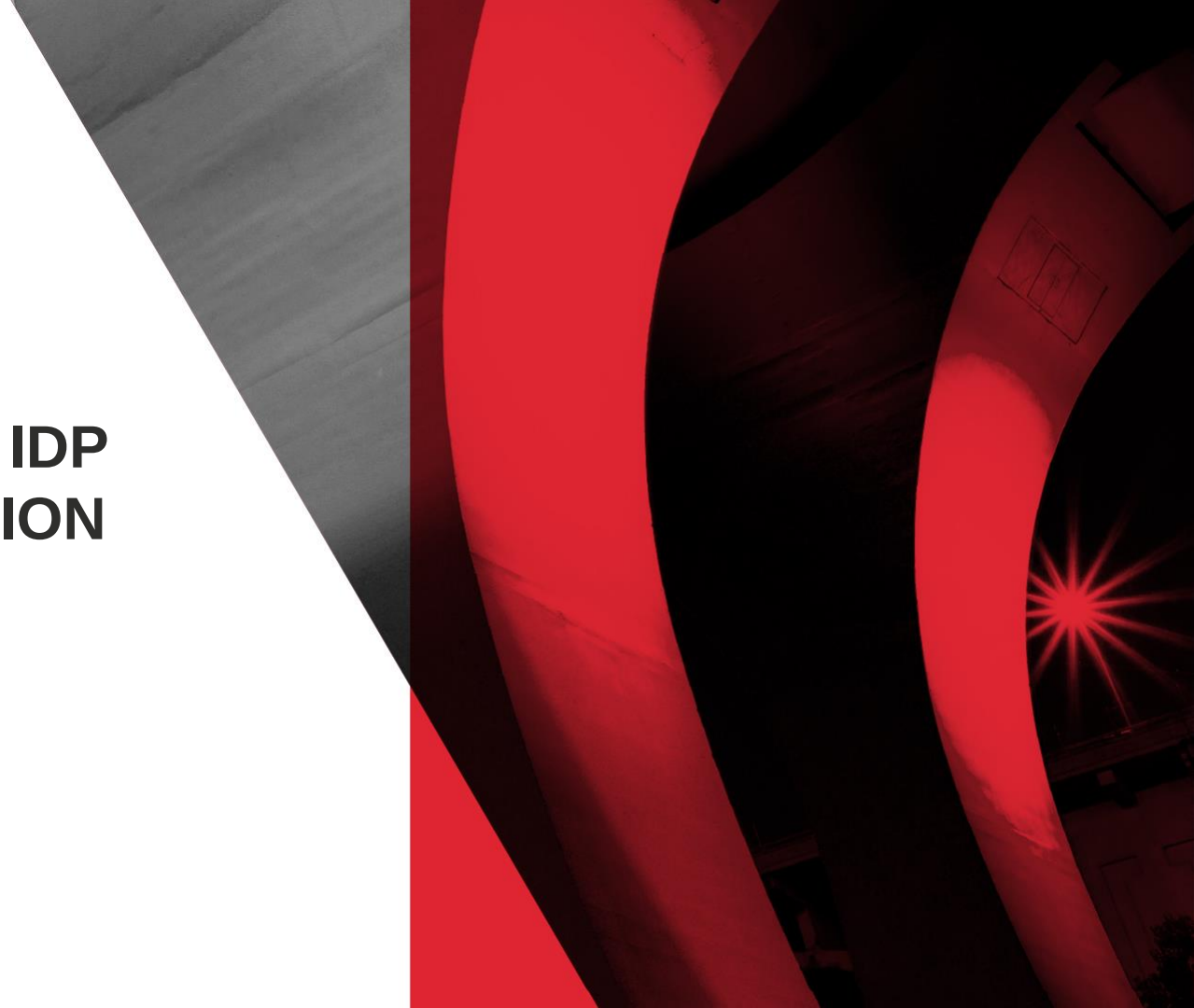
App Registration



Enterprise Application



SHIBBOLETH IDP CONFIGURATION

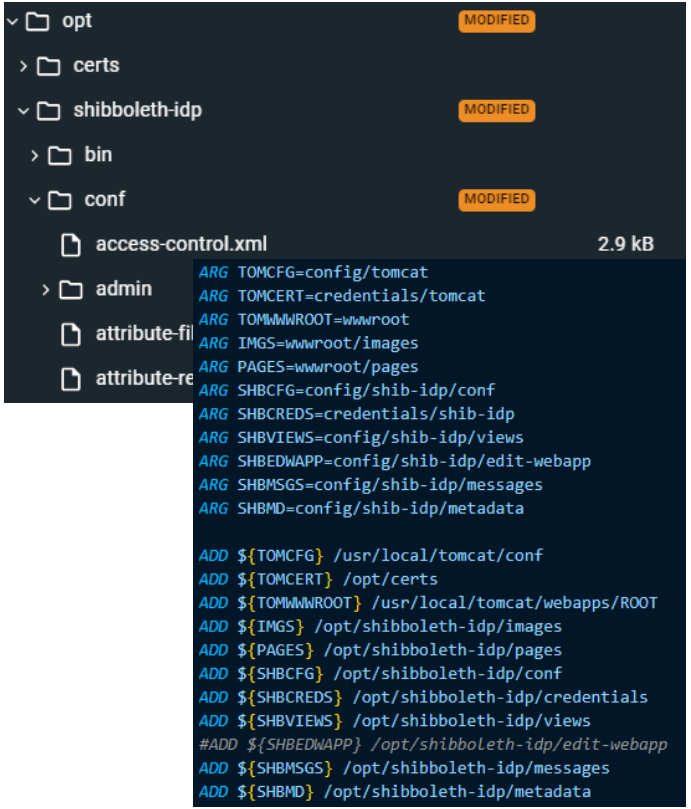


The TIER Idp Base Image & Configuration

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

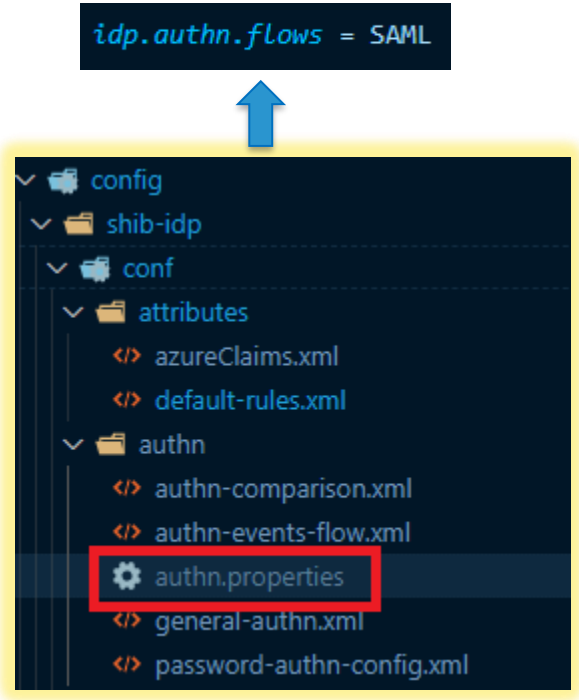
[GitHub - docker/ShibbIdP_ConfigBuilder_Container (internet2.edu)]

Shibboleth IdP v4.3.1
Tomcat v9.0.16

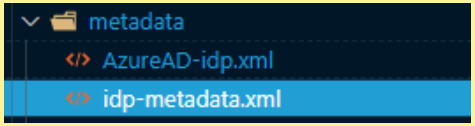


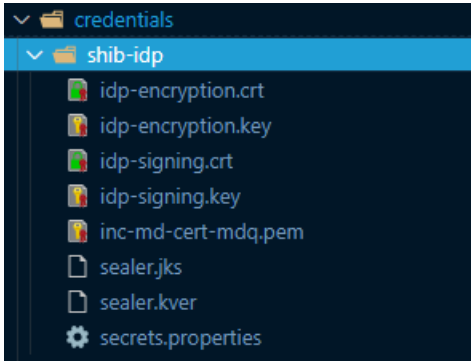
Steps to Configure IdP

- 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



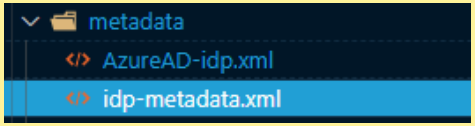
IdP Metadata – Signing, Encryption, EntityId





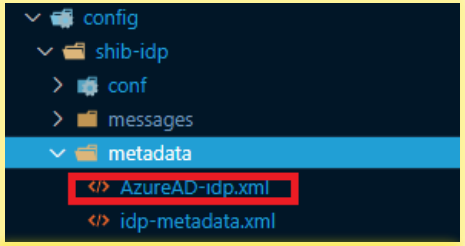

```
<EntityDescriptor entityID="https://[HOSTNAME]/idp/shibboleth" xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:shibmd="urn:mace:shibboleth:metadata:1.0" xmlns:ds=

  <IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <Extensions>
      <shibmd:Scope regexp="false">[org].edu</shibmd:Scope>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
          MIIDBDCCAeygAwIBAgIJAM+XsNiGfw05MA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV
BAMMCTEyNy4wLjAuMTAeFw0yMjEwMjMyMzIzMThaFw0yNzEwMjIyMzIzMThaMBQx
EjAQBgNVBAMMCTEyNy4wLjAuMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAMXwQElhJZk4L5WhpPEfcITVWGQ/B3qbauuR17RYDb+hTX5w9mj7jpAWwPsZ
5q5ARxcUHwhH0viEWPSTXzc98LUslj5YFDgrrdE4wJUx8Y1i6E7SO1zYtA+sxV5H
Qq/dnrtaQ6ixx/4gL570h8huvfrkpHysv8IrecVnx9msbTyK/6QhwkMZ/mqEH5XH
XIBiC42a01SAbscKRs1Nb8/VFJoB/CJXSDvN5r4lC3saFtUfOViAIRltxYVHOgJE
xm/JheIdBYIl6AaZy104Y/7Jy09xDJtErKoiacKjjvB7xM/g68yI765Sgrl8AptU
fdXZMz+VC5Tb/ikL3NQPl+LmjpMCAwEAAaNZMFcwNgYDVR0RBC8wLYIJMTI3LjAu
MC4xhiBodHRwczovLzEyNy4wLjAuMS9pZHAvc2hpYmJvbGV0aDAdBgNVHQ4EFgQU
V4jbrF6MASmfGlcOczhfoKRkMUgwDQYJKoZIhvcNAQELBQADggEBAFUvlNY0mKxk
9zBq4Um6zud2pDB9sva80iZccShpD6F5W88n2QbbgBFGMXKNFmA6bWYdJIogXIs2
kq9+Hz+66tlosezSHSUDTCxHxvwwoDX/frAi7ttAyMZjbDETPJjaIHAK+0i6WoyX
Zhgc2hJDOlK6lote+8DrSuk+UJ1D5v6Q+V94UY1Yh+Um2yP3wtUVpeVtt23zOkfv
m1db0lHiiRycLYakieVySrmkl/sLbbvVwFzIO8QnBIFBEQxrUDsOgrTQmSQOHjF6
UTQMFMS21XA++c83ZsGxVMxsGocKrjHieQUorwR1Z60gJbpDP+ctefqno0O79VSa
D8X+TNd9esE=
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://[HOSTNAME]/idp/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://[HOSTNAME]/idp/profile/SAML2/POST/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign" Location="https://[HOSTNAME]/idp/profile/SAML2/POST-SimpleSign/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="https://[HOSTNAME]/idp/profile/SAML2/SOAP/ECP"/>
  </IDPSSODescriptor>
```

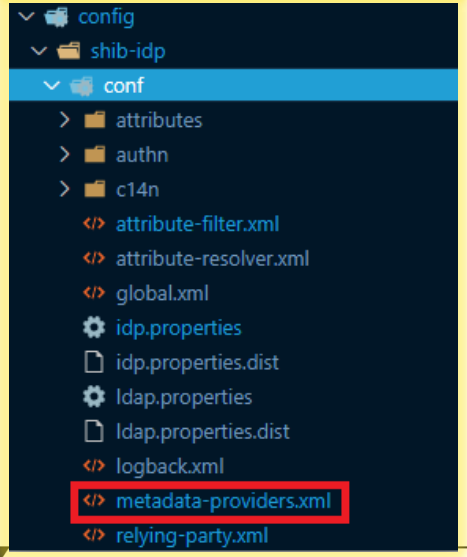
SP Metadata – Signing, Encryption, AssertionConsumerService

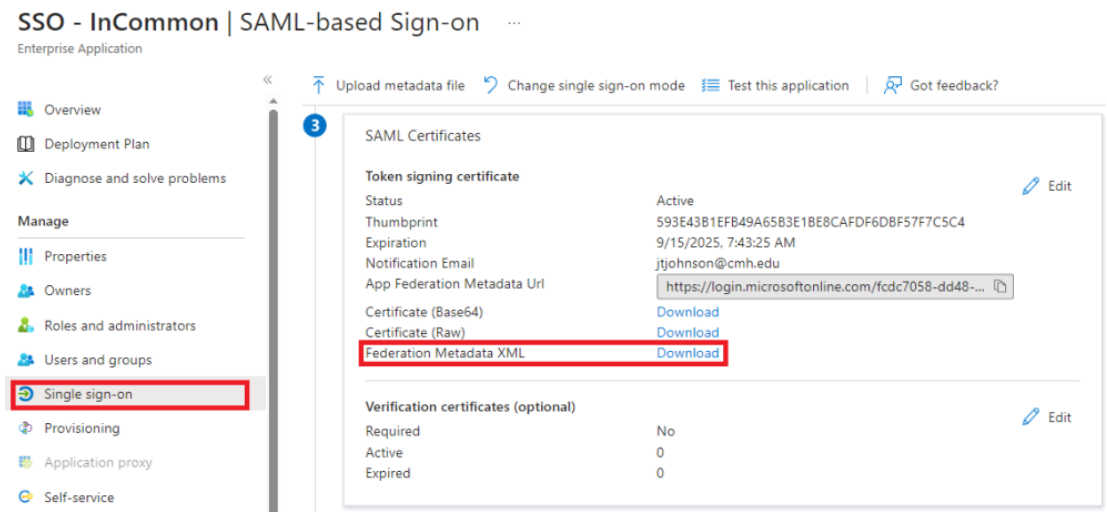



```
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
      <KeyDescriptor use="signing">
          <ds:KeyInfo>
              <ds:X509Data>
                  <ds:X509Certificate>
                  ...
                  </ds:X509Certificate>
              </ds:X509Data>
          </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








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

</MetadataProvider>
```

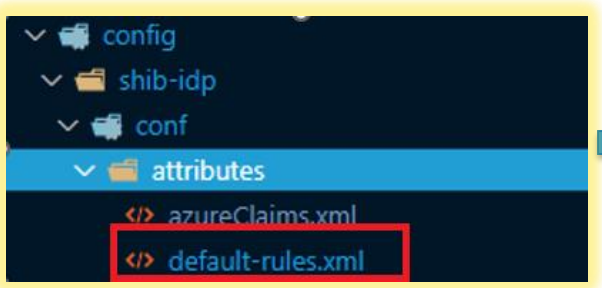
InCommon Metadata - MDQ


```
<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 > jtjohnson > Documents > InCommon-metadata.xml

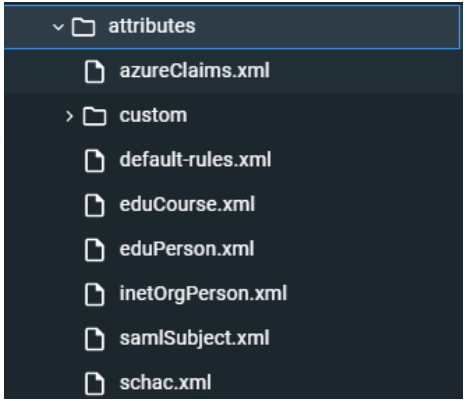
```
1  <?xml version="1.0" encoding="UTF-8"?><EntitiesDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:alg="urn:oasis:names:tc:SAML:metadata:algsupport" xmlns:ds="h
2  iiAR+YO+62I4BUQPRW5Mnp81u5qJxgcNurkwhES7y6zJgwMULGl7m7V0ber6HNtVza2PoeUOnEri&#13;
3  xXFdWLawWuue4NxfC4Ykt c29TJfE2l62tMbS27BPl4YFe78j468+bHOXfhdC9ffbT7G4lVqx6+0u&#13;
4  iawxPu6iGl8XRbqqClewmxRmrZiwt1bDQOr6QUOZqKcsUOfv/0ssXvG5LVcaBHY8uVnkT26u8cja&#13;
5  N0axm5SxxcCG7XJtAe/etC23S2D6s7/2X1XzHA==</SignatureValue><KeyInfo><X509Data><X509Certificate>MIIDgTCCAmmgAwIBAgIJAJRJzvdpkmNaMA0GCSqGSIb3DQEBCwUAMFcxCzAJBgNVBAYTAlVTMRUw&
6  EwYDVQQKDAxJbkNvbW1vbiBMTEMxMTAvBgNVBAMMKEluQ29tbW9uIEZlZGVyYXRpb24gTWV0YWRh&#13;
7  dGEgU2lnbmluZyBLZXkwHhcNMTMxMjE2MTkzNDU1WhcNMzcxMjE4MTkzNDU1WjBXMQswCQYDVQQG&#13;
8  EwJVUzEVMBMGA1UECgwMSW5Db21tb24gTExDMTEwLwYDVQQDDChJbkNvbW1vbiBGZWRlcmF0aW9u&#13;
9  IE1ldGFkYXRhIFNpZ25pbmcgS2V5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0Chd&#13;
10 krn+dG5Zj5L3UIw+xeWgNzm8ajw7/FyqRQ1SjD4Lfg2WCdlfjOrYGNnVZMCTfItoXTSpg4rXxHQs&#13;
11 ykeNiYRu2+02uMS+1pnBqWjzdPJE0od+q8EbdvE6ShimjyNn0yQfGyQKCNdYuc+75MIHsaIOAEtD&#13;
12 ZUST9Sd4oeU1zRjV2sGvUd+JFHveUAhRc0b+JEZfIEuq/LIU9qxm/+gFaawlmojZPyOWZ1Jlswbr&#13;
13 rJYYyn10qgnJvjh9gZWXKjmPxqvHKJcATPhAh2gWGabWTXBJCckMe1hrHCl/vbDLCmz0/oYuoaSD&#13;
14 zP6zE9YSA/xCplaHA0moC1Vs2H5MOQGlewIDAQABo1AwTjAdBgNVHQ4EFgQU5ij9YLU5zQ6K75kP&#13;
15 gVpyQ2N/lPswHwYDVR0jBBgwFoAU5ij9YLU5zQ6K75kPgVpyQ2N/lPswDAYDVR0TBAUwAwEB/zAN&#13;
16 BgkqhkiG9w0BAQsFAAOCAQEAaQkEx9xvaLUt0PNLvHMtxXQPedCPw5xQBd2VWOsWPYspRAOSNbU1&#13;
17 VloY+xUkUKorYTogKUY1q+uh2gDIEazW0uZZaQvWPp8xdxWqDh96n5US06lszEc+Lj3dqdxWkXRR&#13;
18 qEbjhBFh/utXaeyeSOtaX65GwD5svDHnJBclAGkzeRIXqxmYG+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>
```

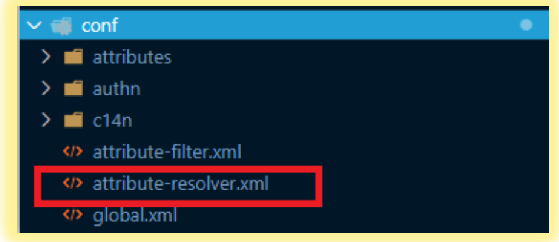
Docker Container




```
<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" />
```

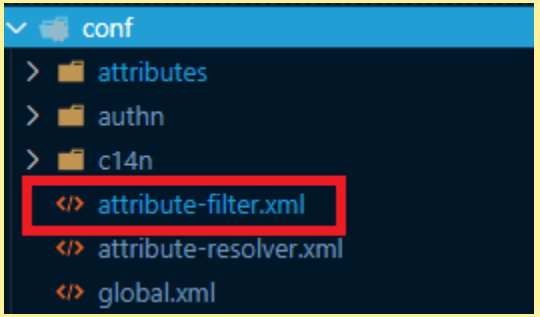
- example@abc.edu

```
<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

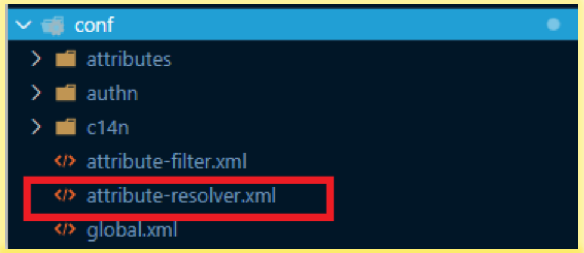



```
<AttributeFilterPolicy id="FilterPolicyObject-Proxy-FromAzure-byIssuer-Type">
    <PolicyRequirementRule xsi:type="Issuer" value="https://sts.windows.net/fcdc7058-dd48-4a81-90b6-281159ae72e0/" />

    <AttributeRule attributeID="azureDisplayname" permitAny="true" />
    <AttributeRule attributeID="azureGivenname" permitAny="true" />
    <AttributeRule attributeID="azureSurname" permitAny="true" />
    <AttributeRule attributeID="azureAuthnmethodsreferences" 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>
```

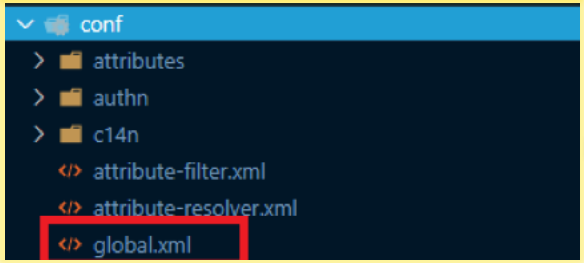
- Release FROM Shibboleth TO Relying Party (InCommon)

```
<!-- 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>
```

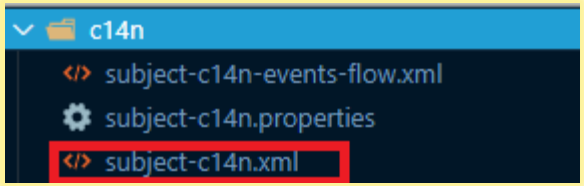
Canonicalization




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

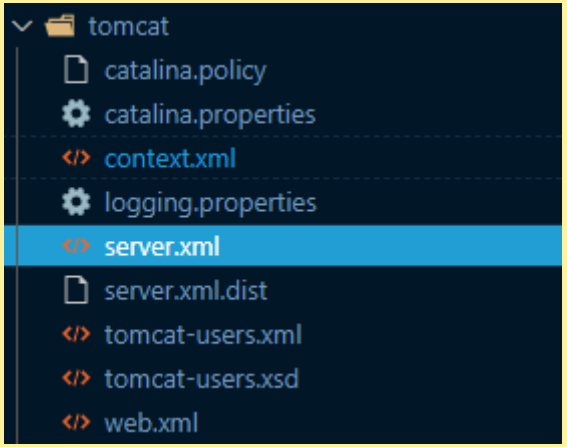


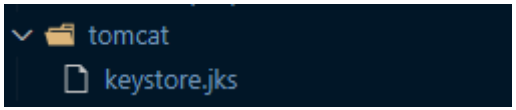

```
<util:list id="shibboleth.c14n.attribute.AttributesToResolve">
<value>canonicalNameToUseForJoin</value>
</util:list>
<util:list id="shibboleth.c14n.attribute.AttributeSourceIds">
    <value>canonicalNameToUseForJoin</value>
</util:list>
```




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

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="[redacted]"
               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

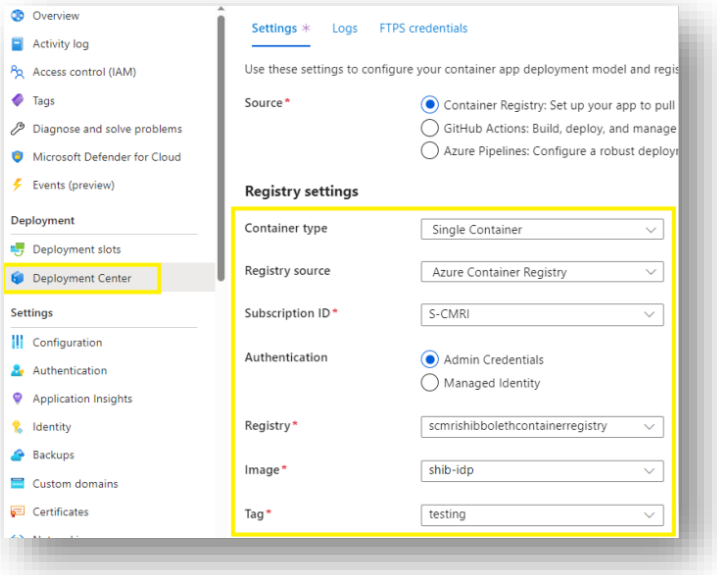
```
az login
az account set --subscription $SUB
```

Login to ACR (Azure Container Registry)

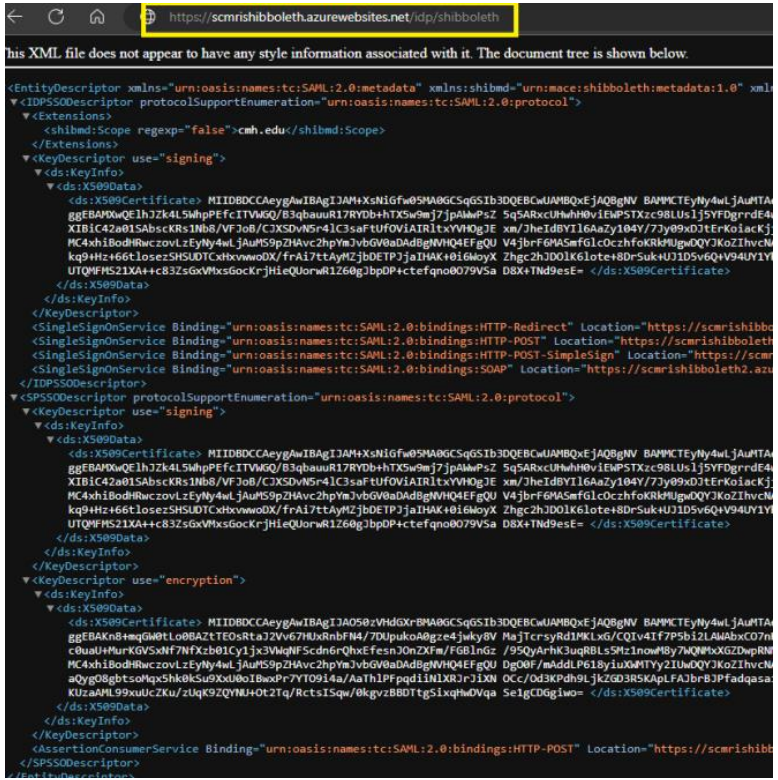
```
az acr login --name scmrishibbolethcontainerregistry
```

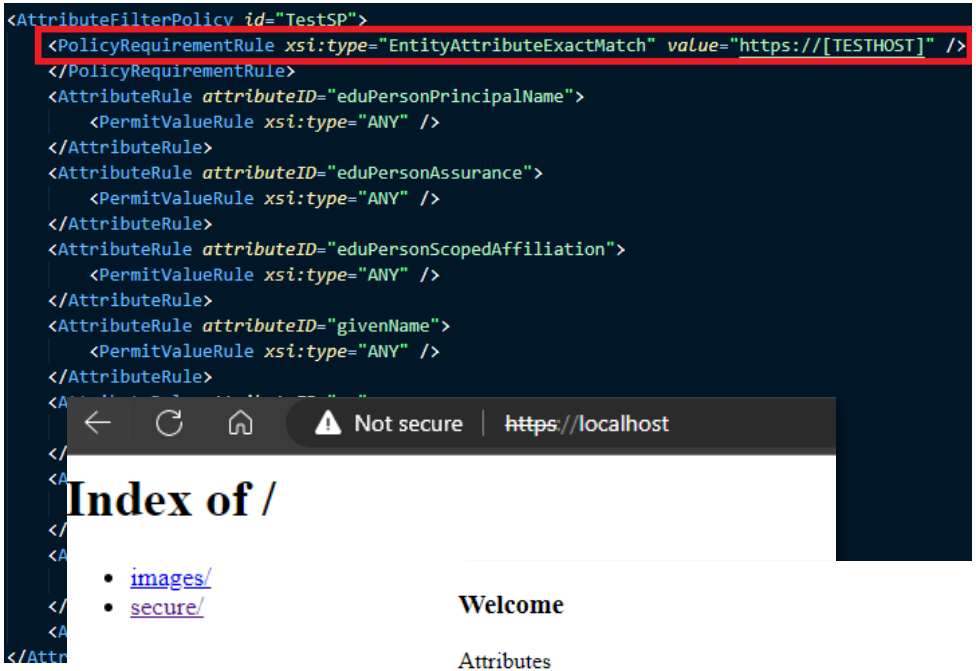
Build and Push Shibboleth Image to ACR

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

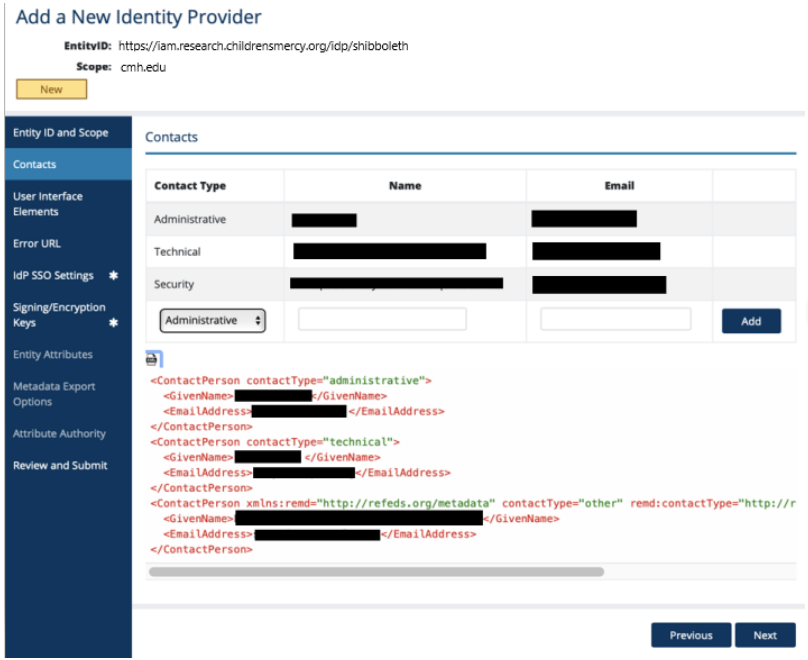


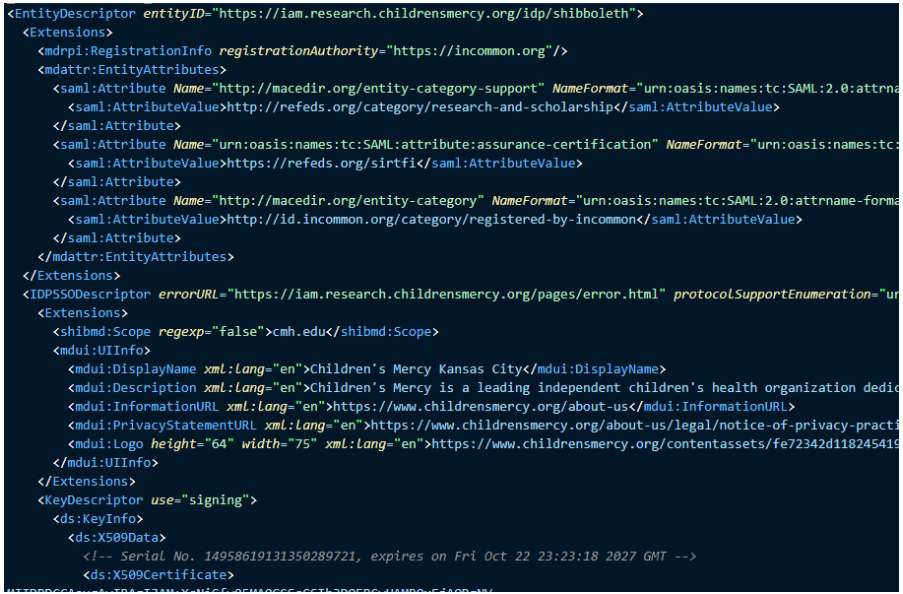
Validation


https://scmrishibboleth.azurewebsites.net/idp/shibboleth
his 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"
<IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<Extensions>
<shibmd:Scope regexp="false">cmh.edu</shibmd:Scope>
</Extensions>
<KeyDescriptor use="signing">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate> MIIDBDCCAeygAwIBAgIJAM+XsNiGfw0SMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV BAMMCTEyNy4wLjAuMTA
ggEBAMXwQElhJZk4L5WhpPEfcITVWGQ/B3qbauuR17RYDb+hTX5w9mj7jpAWwPsZ 5q5ARxcUHwhH0viEWPSTXzc98LUslj5YFDgrrdE4
XIBiC42a01SAbscKRs1Nb8/VFJoB/CJXSDvN5r4lC3saFtUfOViAIRltxYVHOgJE xm/JheIdBYIl6AaZy104Y/73y09xDJtErKoiacKj
MC4xhiBodHRwczovLzEyNy4wLjAuMS9pZHAvc2hpYmJvbGV0aDAdBgNVHQ4EFgQU V4jbrF6MASmfGlcOczhfoKRkMUgwDQYJKoZIhvcN
kq9+Hz+66tlosezSHSUDTCxHxvwwoDX/frAi7ttAyMZjbDETPJjaIHAK+0i6WoyX Zhgc2hJDOlK6lote+8DrSuk+UJ1D5v6Q+V94UY1Y
UTQMFMS21XA++c83ZsGxVMxsGocKrjHieQUorwR1Z60g3bpDP+ctefqno0O79VSa D8X+TNd9esE= </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://scmrishibbo
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://scmrishibboleth
<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://scmrishibboleth2.azu
</IDPSSODescriptor>
<SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
<KeyDescriptor use="signing">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate> MIIDBDCCAeygAwIBAgIJAM+XsNiGfw0SMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV BAMMCTEyNy4wLjAuMTA
ggEBAMXwQElhJZk4L5WhpPEfcITVWGQ/B3qbauuR17RYDb+hTX5w9mj7jpAWwPsZ 5q5ARxcUHwhH0viEWPSTXzc98LUslj5YFDgrrdE4
XIBiC42a01SAbscKRs1Nb8/VFJoB/CJXSDvN5r4lC3saFtUfOViAIRltxYVHOgJE xm/JheIdBYIl6AaZy104Y/73y09xDJtErKoiacKj
MC4xhiBodHRwczovLzEyNy4wLjAuMS9pZHAvc2hpYmJvbGV0aDAdBgNVHQ4EFgQU V4jbrF6MASmfGlcOczhfoKRkMUgwDQYJKoZIhvcN
kq9+Hz+66tlosezSHSUDTCxHxvwwoDX/frAi7ttAyMZjbDETPJjaIHAK+0i6WoyX Zhgc2hJDOlK6lote+8DrSuk+UJ1D5v6Q+V94UY1Y
UTQMFMS21XA++c83ZsGxVMxsGocKrjHieQUorwR1Z60g3bpDP+ctefqno0O79VSa D8X+TNd9esE= </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<KeyDescriptor use="encryption">
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate> MIIDBDCCAeygAwIBAgIJAO50zVHdGXrBMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNV BAMMCTEyNy4wLjAuMTA
ggEBAKn8+mqGW0tLo0BAZtTEOsRtaJ2Vv67HUxRnbFN4/7DUpukoA0gze4jwky8V MajTcrsyRd1MKLxG/CQIv4If7P5bi2LAWAbxCO7n
c0uaU+MurKGVSxNf7NfXzb01Cy1jx3VWqNFScdn6rQhxEfesnJOnZXFm/FGBlnGz /95QyArhK3uqRBLs5Mz1nowM8y7WQNMxXGZDwpRN
MC4xhiBodHRwczovLzEyNy4wLjAuMS9pZHAvc2hpYmJvbGV0aDAdBgNVHQ4EFgQU DgO0F/mAddLP618yiuXWMTYy2IUwDQYJKoZIhvcN
aQygO8gbtsoMqx5hk0kSu9XxU0oIBwxPr7YTO9i4a/AaThlPfpqdiiNlXRJrJiXN OCc/Od3KPdh9LjkZGD3R5KApLFAJbrBJPfadqasa
KUzaAML99xuUcZKu/zUqK9ZQYNU+Ot2Tq/RctsISqw/0kgvzBBDTtgSixqHwDVqa Se1gCDGgiwo= </ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</KeyDescriptor>
<AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://scmrishibb
</SPSSODescriptor>


<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>
Not secure
https://localhost
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



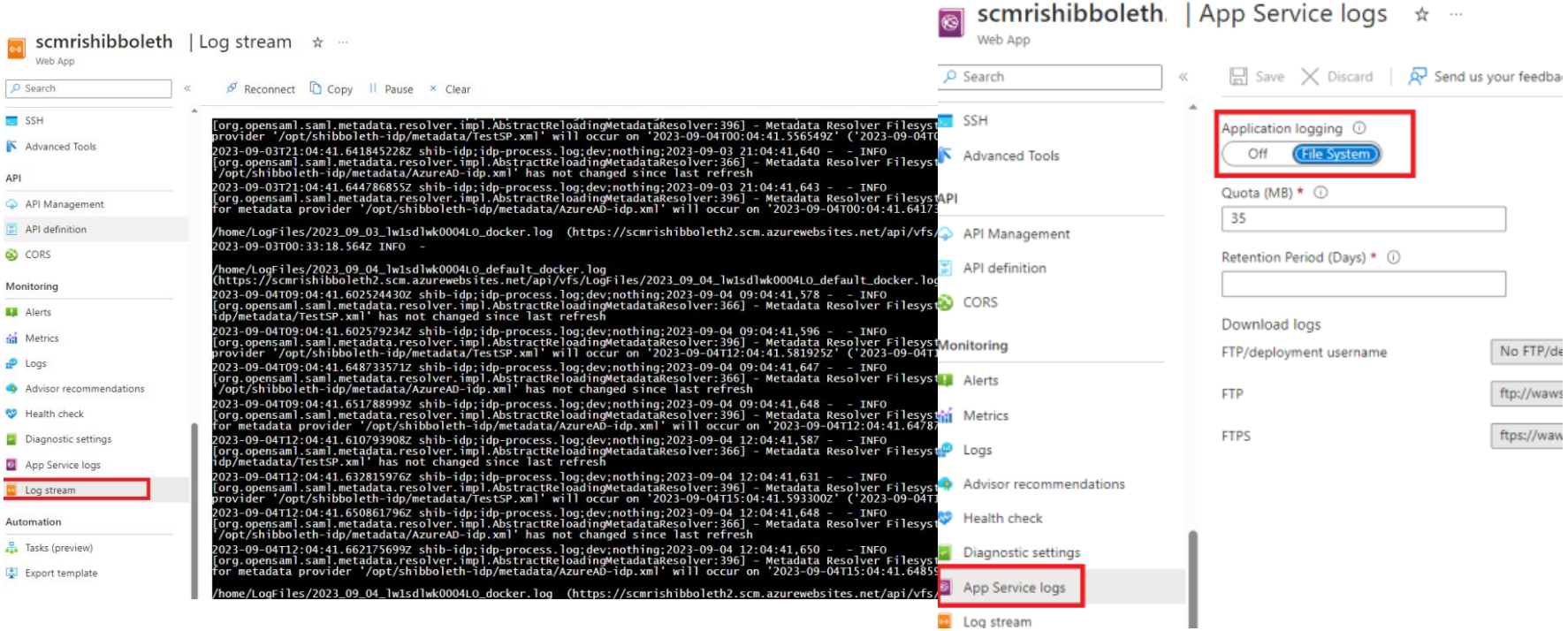


TROUBLESHOOTING

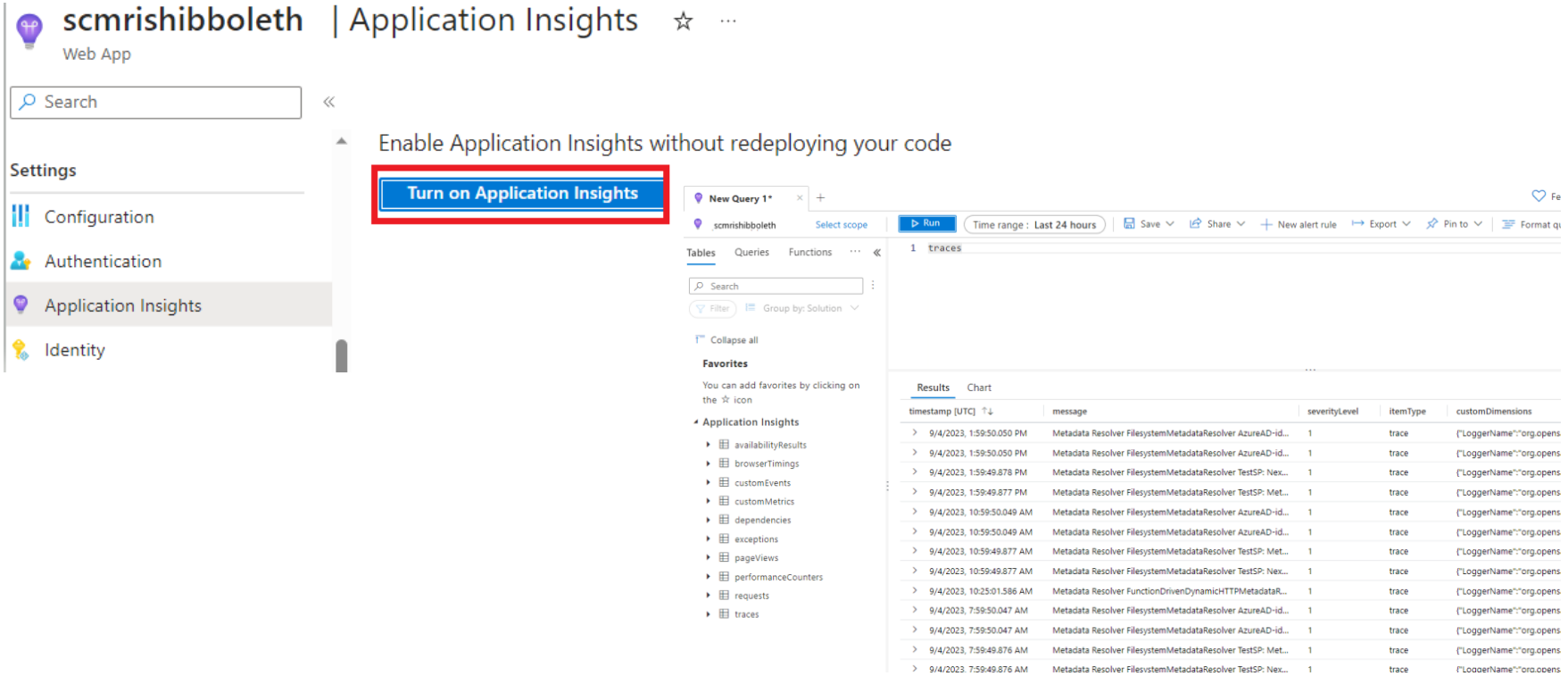
Debug Logging – LogLevel Config

```
<?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}" />
```

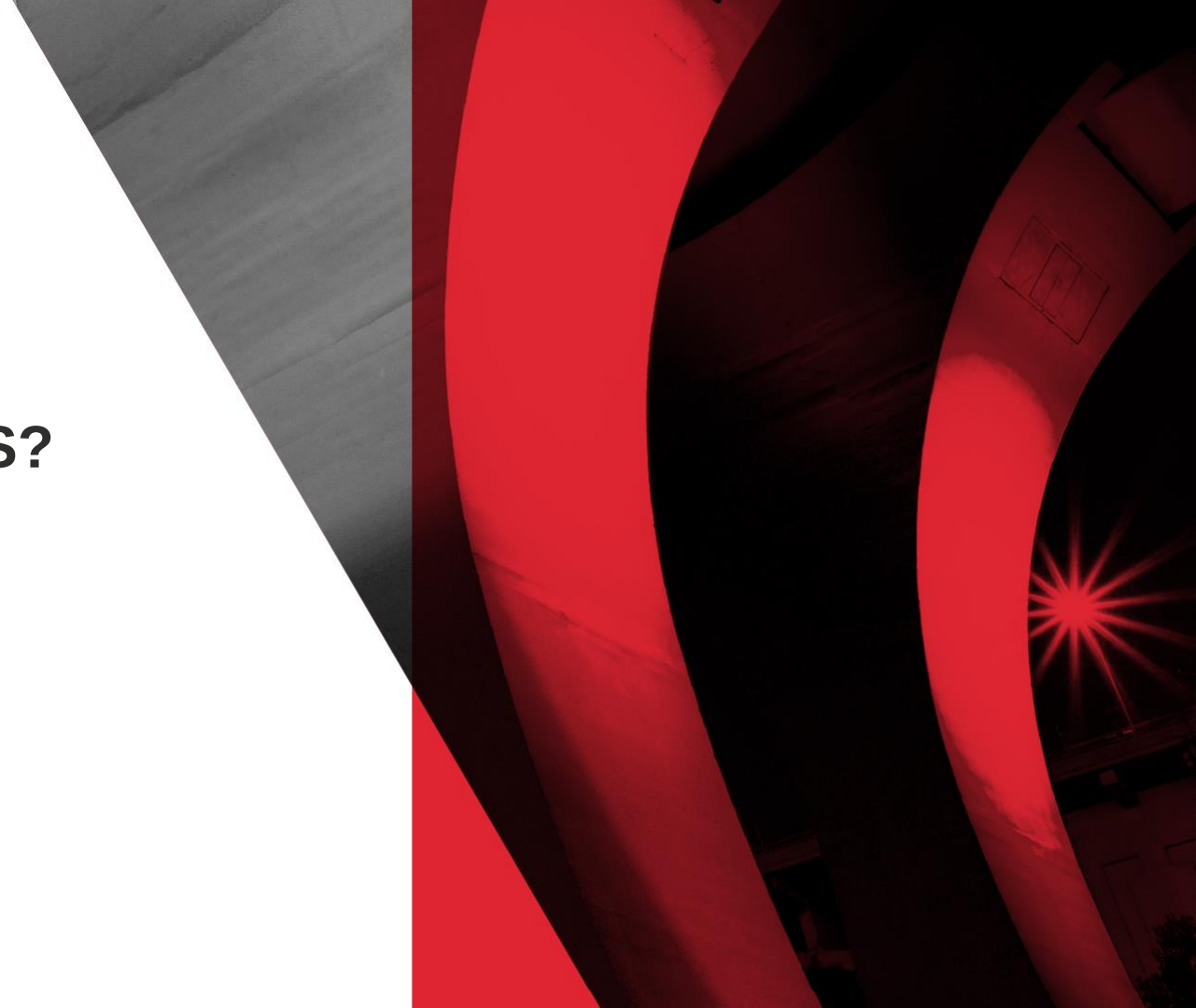
Debug Logging – File System



Debug Logging – Application Insights



QUESTIONS?



CONFIG TEMPLATES

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:algsupport"
    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:algsupport
http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-metadata-algsupport-
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]/idp/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>
      <shibmd:Scope regexp="false">cmh.edu</shibmd:Scope>
    </Extensions>
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
          [SIGNING KEY]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
      Location="https://[HOST]/idp/profile/SAML2/Redirect/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://[HOST]/idp/profile/SAML2/POST/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST-SimpleSign"
      Location="https://[HOST]/idp/profile/SAML2/POST-SimpleSign/SSO"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
      Location="https://[HOST]/idp/profile/SAML2/SOAP/ECP"/>
  </IDPSSODescriptor>
  <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo>
        <ds:X509Data>
            <ds:X509Certificate>
            [SIGNING KEY]
            </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
      </KeyDescriptor>
    <KeyDescriptor use="encryption">
      <ds:KeyInfo>
        <ds:X509Data>
          <ds:X509Certificate>
          [ENCRYPTION KEY]
          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
      Location="https://[HOST]/idp/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: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.PostLoginSubjectCanonicalizationFlows">
        <bean id="c14n/attribute" parent="shibboleth.PostLoginSubjectCanonicalizationFlow" />
         <ref bean="c14n/SAML2ProxyTransform" />
        <ref bean="c14n/x500" />
        <ref bean="c14n/simple" />
    </util:list>
    <util:list id="shibboleth.ProxyNameTransformFormats">
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</value>
        <value>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</value>
    </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/SAML2Transient" />
        <ref bean="c14n/SAML2CryptoTransient" />
        <ref bean="c14n/SAML1Transient" />
        <ref bean="c14n/SAML1CryptoTransient" />
        <ref bean="c14n/SAML2Transform" />
        <ref bean="c14n/SAML1Transform" />
    </util:list>
    <util:list id="shibboleth.NameTransformFormats">
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName</value>
        <value>urn:oasis:names:tc:SAML:1.1:nameid-format:WindowsDomainQualifiedName</value>
        <value>urn:oasis:names:tc:SAML:2.0:nameid-format:kerberos</value>
    </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="releaseRandSAttributeBundle">
        <PolicyRequirementRule xsi:type="EntityAttributeExactMatch"
                               attributeName="http://macedir.org/entity-category"
                               attributeValue="http://refeds.org/category/research-and-scholarship"/>
        <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="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>

    <AttributeFilterPolicy id="FilterPolicyObject-Proxy-FromAzure-byIssuer-Type">
        <PolicyRequirementRule xsi:type="Issuer" value="[AZURE REGISTRATION HOST]" />
        <AttributeRule attributeID="azureDisplayname" permitAny="true" />
        <AttributeRule attributeID="azureGivenname" permitAny="true" />
        <AttributeRule attributeID="azureSurname" permitAny="true" />
        <AttributeRule attributeID="azureAuthnmethodsreferences" 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="[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
    azureAuthnmethodsreferences 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>
```

logback.xml

```
<?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}" />

    <logger name="net.shibboleth.idp" level="${idp.loglevel.idp}"/>
    <logger name="org.opensaml.saml" level="${idp.loglevel.opensaml}"/>
    <logger name="org.ldaptive" level="${idp.loglevel.ldap}"/>
    <logger name="org.apache.http" level="${idp.loglevel.httpclient}"/>
    <logger name="PROTOCOL_MESSAGE" level="${idp.loglevel.messages}" />
    <logger name="org.opensaml.saml.saml2.encryption.Encrypter" level="${idp.loglevel.encryption}" />
    <logger name="net.shibboleth.idp.log.LogbackLoggingService" level="${idp.loglevel.props}" />

    <!-- Especially chatty. -->
    <logger name="org.apache.xml.security" level="${idp.loglevel.xmlsec}" />
    <logger name="org.springframework" level="${idp.loglevel.spring}"/>
    <logger name="org.apache.catalina" level="${idp.loglevel.container}"/>
    <logger name="org.eclipse.jetty" level="${idp.loglevel.container}"/>
    <appender name="IDP_PROCESS" class="ch.qos.logback.core.FileAppender">
        <File>/tmp/logidp-process</File>
        <encoder class="ch.qos.logback.classic.encoder.PatternLayoutEncoder">
            <charset>UTF-8</charset>
            <Pattern>%date{ISO8601} - %mdc{idp.remote_addr} - %level [%logger:%line] - %msg%n%ex{short}</Pattern>
        </encoder>
        <filter class="ch.qos.logback.core.filter.EvaluatorFilter">
            <evaluator>
                <matcher>
                    <Name>VelocityStatusMatcher</Name>
                    <regex>ResourceManager\$": unable to find resource 'status\.vm' in any resource loader\.</regex>
                </matcher>
                <expression>VelocityStatusMatcher.matches(formattedMessage)</expression>
            </evaluator>
            <OnMatch>DENY</OnMatch>
        </filter>
    </appender>
    <appender name="ASYNC_PROCESS" class="ch.qos.logback.classic.AsyncAppender">
        <appender-ref ref="IDP_PROCESS" />
        <discardingThreshold>0</discardingThreshold>
    </appender>
    <appender name="IDP_WARN" class="ch.qos.logback.core.FileAppender">
        <filter class="ch.qos.logback.classic.filter.ThresholdFilter">
            <level>WARN</level>
        </filter>
        <File>/tmp/logidp-warn</File>
        <encoder class="ch.qos.logback.classic.encoder.PatternLayoutEncoder">
            <charset>UTF-8</charset>
            <Pattern>%date{ISO8601} - %mdc{idp.remote_addr} - %level [%logger:%line] - %msg%n%ex{full}</Pattern>
        </encoder>
        <filter class="ch.qos.logback.core.filter.EvaluatorFilter">
            <evaluator>
                <matcher>
                    <Name>VelocityStatusMatcher</Name>
                    <regex>ResourceManager\$": unable to find resource 'status\.vm' in any resource loader\.</regex>
                </matcher>
                <expression>VelocityStatusMatcher.matches(formattedMessage)</expression>
            </evaluator>
            <OnMatch>DENY</OnMatch>
        </filter>
    </appender>
    <appender name="IDP_AUDIT" class="ch.qos.logback.core.FileAppender">
        <File>/tmp/logidp-audit</File>
        <encoder class="ch.qos.logback.classic.encoder.PatternLayoutEncoder">
            <charset>UTF-8</charset>
            <Pattern>%msg%n</Pattern>
        </encoder>
    </appender>
    <appender name="IDP_CONSENT_AUDIT" class="ch.qos.logback.core.FileAppender">
        <File>/tmp/logidp-consent-audit</File>
        <encoder class="ch.qos.logback.classic.encoder.PatternLayoutEncoder">
            <charset>UTF-8</charset>
            <Pattern>%msg%n</Pattern>
        </encoder>
    </appender>
    <appender name="IDP_FTICKS" class="ch.qos.logback.classic.net.SyslogAppender">
        <syslogHost>${idp.fticks.loghost:-localhost}</syslogHost>
        <port>${idp.fticks.logport:-514}</port>
        <facility>AUTH</facility>
        <suffixPattern>[%thread] %logger %msg</suffixPattern>
    </appender>
    <logger name="Shibboleth-Audit" level="ALL">
        <appender-ref ref="${idp.audit.appender:-IDP_AUDIT}"/>
    </logger>
    <logger name="Shibboleth-FTICKS" level="ALL" additivity="false">
        <appender-ref ref="${idp.fticks.appender:-IDP_FTICKS}"/>
    </logger>
    <logger name="Shibboleth-Consent-Audit" level="ALL">
        <appender-ref ref="${idp.consent.appender:-IDP_CONSENT_AUDIT}"/>
    </logger>
    <root level="${idp.loglevel.root:-INFO}">
        <appender-ref ref="${idp.process.appender:-IDP_PROCESS}"/>
        <appender-ref ref="${idp.warn.appender:-IDP_WARN}" />
    </root>
</configuration>
```

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 = \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos, \
    saml1/urn:ietf:rfc:1510
idp.authn.X509.supportedPrincipals = \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:X509, \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, \
    saml1/urn:ietf:rfc:2246
idp.authn.X509Internal.supportedPrincipals = \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:X509, \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:TLSClient, \
    saml1/urn:ietf:rfc:2246
idp.authn.IPAddress.supportedPrincipals = \
   saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol
idp.authn.Duo.supportedPrincipals = \
    saml2/http://example.org/ac/classes/mfa, \
    saml1/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 = \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:Password, \
    saml1/urn:oasis:names:tc:SAML:1.0:am:password, \
    https://refeds.org/profile/mfa
idp.authn.MFA.supportedPrincipals = \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:InternetProtocol, \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport, \
    saml2/urn:oasis:names:tc:SAML:2.0:ac:classes:Password, \
    saml1/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"
```