Shibboleth Metadata Config

Shibboleth Metadata Configuration

The Shibboleth software will not only consume metadata, it will also fetch and verify a fresh metadata file on a regular basis. The Shibboleth software is highly optimized with respect to metadata refresh.

Contents

Before you can verify the XML signature on a metadata aggregate, you need an authentic copy of the InCommon Metadata Signing Certificate. Do this first, before configuring Shibboleth for metadata refresh.

Configure the Shibboleth IdP

The IdP configuration examples in this section fetch the *main InCommon production metadata aggregate*. See the Metadata Aggregates wiki page for other options.

> **Protect Against Failed Metadata Processes**
>
> The Shibboleth IdP is known to be sensitive to large metadata aggregates. To protect against failed metadata processes, InCommon recommends that deployers **allocate at least 1500MB of heap space** in the JVM. Do this for all your Shibboleth IdP deployments, in both test and production, for both V3 and V2.

Configure Shibboleth IdP V3

To download and verify signed InCommon metadata every hour, configure Shibboleth IdP 3.2.0 (and later) as follows:

Configure Shibboleth IdP 3.2.0 (and later)

```
<!--
  Use a ChainingMetadataProvider in case you want to nest other metadata providers later on
-->
<MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"
                  xmlns="urn:mace:shibboleth:2.0:metadata">

  <!--
    Refresh the InCommon production metadata aggregate every hour.

    Note: The defaults for minRefreshDelay, maxRefreshDelay, and refreshDelayFactor
    are "PT5M", "PT4H", and "0.75", respectively. The value of maxRefreshDelay
    has been modified below such that the metadata is refreshed every hour ("PT1H").
    The other properties merely regurgitate their default values. They are included
    here for convenience, in case you want to change their default values.
  -->
  <MetadataProvider id="ICMD" xsi:type="FileBackedHTTPMetadataProvider"
                    xmlns="urn:mace:shibboleth:2.0:metadata"
                    metadataURL="http://md.incommon.org/InCommon/InCommon-metadata.xml"
                    backingFile="%{idp.home}/metadata/InCommon-metadata.xml"
                    minRefreshDelay="PT5M"
                    maxRefreshDelay="PT1H"
                    refreshDelayFactor="0.75">

      <!--
        To bootstrap the trust fabric of the federation, each relying party
        obtains and configures an authentic copy of the federation operator's
        Metadata Signing Certificate (https://spaces.at.internet2.edu/x/moHFAg).

        Fetch the InCommon Metadata Signing Certificate and check its integrity:

        $ IDP_HOME=/opt/shibboleth-idp
        $ /usr/bin/curl -s https://ds.incommon.org/certs/inc-md-cert.pem \
            | /usr/bin/tee $IDP_HOME/credentials/inc-md-cert.pem \
            | /usr/bin/openssl x509 -sha1 -fingerprint -noout
        SHA1 Fingerprint=7D:B4:BB:28:D3:D5:C8:52:E0:80:B3:62:43:2A:AF:34:B2:A6:0E:DD

        Verify the signature on the root element of the metadata aggregate
        (i.e., the EntitiesDescriptor element) using the trusted Metadata
        Signing Certificate.
      -->
      <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
              certificateFile="%{idp.home}/credentials/inc-md-cert.pem" />

      <!--
        Require a validUntil XML attribute on the EntitiesDescriptor element
        and make sure its value is no more than 14 days into the future.
      -->
      <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D" />

      <!-- Consume all SP metadata in the aggregate -->
      <MetadataFilter xsi:type="EntityRoleWhiteList">
        <RetainedRole>md:SPSSODescriptor</RetainedRole>
      </MetadataFilter>

  </MetadataProvider>

</MetadataProvider>
```

Configure Shibboleth IdP V2

Shibboleth IdP V2 is obsolete

The Shibboleth IdP V2 software has reached end-of-life. Upgrade to Shibboleth IdP V3 now!

To download and verify signed InCommon metadata every hour, configure Shibboleth IdP 2.2 (and later versions of V2) as follows:

Configure Shibboleth IdP 2.2 (and later versions of V2)

```
<!-- Chaining metadata provider defined in the default IdP relying-party configuration file -->
<MetadataProvider id="ShibbolethMetadata" xsi:type="ChainingMetadataProvider"
                  xmlns="urn:mace:shibboleth:2.0:metadata">

  <!--
    Refresh the InCommon production metadata aggregate every hour.

    Note: The defaults for minRefreshDelay, maxRefreshDelay, and refreshDelayFactor
    are "PT5M", "PT4H", and "0.75", respectively. The default for maxRefreshDelay
    has been modified below such that the metadata is refreshed every hour ("PT1H").
    The other properties merely regurgitate their default values. They are included
    here for convenience, in case you want to change their default values.
  -->
  <MetadataProvider id="ICMD" xsi:type="FileBackedHTTPMetadataProvider"
                    xmlns="urn:mace:shibboleth:2.0:metadata"
                    metadataURL="http://md.incommon.org/InCommon/InCommon-metadata.xml"
                    backingFile="/opt/shibboleth-idp/metadata/InCommon-metadata.xml"
                    minRefreshDelay="PT5M"
                    maxRefreshDelay="PT1H"
                    refreshDelayFactor="0.75">

    <!-- Use a chaining filter to allow multiple filters to be added -->
    <MetadataFilter xsi:type="ChainingFilter">

        <!--
          Require the metadata to be signed and use the trust engine
          labeled id="ICTrust" to determine its trustworthiness
        -->
        <MetadataFilter xsi:type="SignatureValidation"
                        trustEngineRef="ICTrust" requireSignedMetadata="true" />

        <!--
          Require a validUntil XML attribute on the EntitiesDescriptor element
          and make sure its value is no more than 14 days into the future
        -->
        <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D" />

        <!-- Consume all SP metadata in the aggregate -->
        <MetadataFilter xsi:type="EntityRoleWhiteList">
          <RetainedRole>samlmd:SPSSODescriptor</RetainedRole>
        </MetadataFilter>

    </MetadataFilter>
  </MetadataProvider>

</MetadataProvider>

<!--
  This TrustEngine (beneath the Security Configuration section) is an
  implementation of the Explicit Key Trust Model (https://spaces.at.internet2.edu/x/t43NAQ).

  To bootstrap the trust fabric of the federation, each relying party
  obtains and configures an authentic copy of the federation operator's
  Metadata Signing Certificate (https://spaces.at.internet2.edu/x/moHFAg).

  Fetch the InCommon metadata signing certificate and check its integrity:

  $ /usr/bin/curl -s https://ds.incommon.org/certs/inc-md-cert.pem \
      | /usr/bin/tee /opt/shibboleth-idp/credentials/inc-md-cert.pem \
      | /usr/bin/openssl x509 -sha1 -noout -fingerprint
  SHA1 Fingerprint=7D:B4:BB:28:D3:D5:C8:52:E0:80:B3:62:43:2A:AF:34:B2:A6:0E:DD
-->
<security:TrustEngine id="ICTrust" xsi:type="security:StaticExplicitKeySignature">

  <security:Credential id="MyFederation1Credentials" xsi:type="security:X509Filesystem">
    <security:Certificate>/opt/shibboleth-idp/credentials/inc-md-cert.pem</security:Certificate>
  </security:Credential>
</security:TrustEngine>
```

Configure the Shibboleth SP

The SP configuration examples in this section fetch the *IdP-only InCommon production metadata aggregate*. See the Metadata Aggregates wiki page for other options.

Basic Shibboleth SP Configuration

To download and verify signed InCommon metadata every hour, configure Shibboleth SP 2.5 (and later) as follows:

Configure Shibboleth SP 2.5 (and later)

```
<!--
  The following MetadataProvider attempts to refresh the InCommon
  IdP-only metadata aggregate every hour.
-->
<MetadataProvider type="XML"
    url="http://md.incommon.org/InCommon/InCommon-metadata-idp-only.xml"
    backingFilePath="InCommon-metadata-idp-only.xml"
    maxRefreshDelay="3600">

  <!--
    To bootstrap the trust fabric of the federation, each relying party
    obtains and configures an authentic copy of the federation operator's
    Metadata Signing Certificate (https://spaces.at.internet2.edu/x/moHFAg).

    Fetch the InCommon Metadata Signing Certificate and check its integrity:

    $ /usr/bin/curl -s https://ds.incommon.org/certs/inc-md-cert.pem \
        | /usr/bin/tee inc-md-cert.pem \
        | /usr/bin/openssl x509 -sha1 -fingerprint -noout
    SHA1 Fingerprint=7D:B4:BB:28:D3:D5:C8:52:E0:80:B3:62:43:2A:AF:34:B2:A6:0E:DD

    Verify the signature on the root element of the metadata aggregate
    (i.e., the EntitiesDescriptor element) using the trusted Metadata
    Signing Certificate.

    A large metadata file can cause a significant increase in startup
    time at the SP. This is due to the time it takes to verify the
    signature on the metadata, which is known to increase exponentially
    as the size of the metadata file increases. To disable signature
    verification at startup time only, add verifyBackup="false" to the
    MetadataFilter element below.
  -->
  <MetadataFilter type="Signature" certificate="inc-md-cert.pem"/>

  <!--
    Require a validUntil XML attribute on the EntitiesDescriptor element
    and make sure its value is no more than 14 days into the future
  -->
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1209600"/>

  <!--
    Consume all IdP metadata in the aggregate. TIP: If the SP supports
    SAML2 Web Browser SSO only, the md:AttributeAuthorityDescriptor
    elements in IdP metadata can be ignored.
  -->
  <MetadataFilter type="EntityRoleWhiteList">
    <RetainedRole>md:IDPSSODescriptor</RetainedRole>
    <RetainedRole>md:AttributeAuthorityDescriptor</RetainedRole>
  </MetadataFilter>

</MetadataProvider>
```

Shibboleth SP Configuration with Discovery

If your SP has a dynamic discovery interface, use this configuration instead:

Configure Shibboleth SP 2.5 (and later) with discovery

```
<!--
  The following MetadataProvider attempts to refresh the InCommon
  IdP-only metadata aggregate every hour.

  The discovery interface relies primarily on mdui:DisplayName.
  To fall back on md:OrganizationDisplayName if mdui:DisplayName
  is missing from IdP metadata, add legacyOrgNames="true" to the
  MetadataProvider element as shown below.
-->
<MetadataProvider type="XML"
    url="http://md.incommon.org/InCommon/InCommon-metadata-idp-only.xml"
    backingFilePath="InCommon-metadata-idp-only.xml"
    maxRefreshDelay="3600"
    legacyOrgNames="true">

  <!--
    To bootstrap the trust fabric of the federation, each relying party
    obtains and configures an authentic copy of the federation operator's
    Metadata Signing Certificate (https://spaces.at.internet2.edu/x/moHFAg).

    Fetch the InCommon Metadata Signing Certificate and check its integrity:

    $ /usr/bin/curl -s https://ds.incommon.org/certs/inc-md-cert.pem \
        | /usr/bin/tee inc-md-cert.pem \
        | /usr/bin/openssl x509 -sha1 -fingerprint -noout
    SHA1 Fingerprint=7D:B4:BB:28:D3:D5:C8:52:E0:80:B3:62:43:2A:AF:34:B2:A6:0E:DD

    Verify the signature on the root element of the metadata aggregate
    (i.e., the EntitiesDescriptor element) using the trusted Metadata
    Signing Certificate.

    A large metadata file can cause a significant increase in startup
    time at the SP. This is due to the time it takes to verify the
    signature on the metadata, which is known to increase exponentially
    as the size of the metadata file increases. To disable signature
    verification at startup time only, add verifyBackup="false" to the
    MetadataFilter element below.
  -->
  <MetadataFilter type="Signature" certificate="inc-md-cert.pem"/>

  <!--
    Require a validUntil XML attribute on the EntitiesDescriptor element
    and make sure its value is no more than 14 days into the future
  -->
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1209600"/>
  <!--
    Consume all IdP metadata in the aggregate. TIP: If the SP supports
    SAML2 Web Browser SSO only, the md:AttributeAuthorityDescriptor
    elements in IdP metadata can be ignored.
  -->
  <MetadataFilter type="EntityRoleWhiteList">
    <RetainedRole>md:IDPSSODescriptor</RetainedRole>
    <RetainedRole>md:AttributeAuthorityDescriptor</RetainedRole>
  </MetadataFilter>

  <!--
    Hide all IdPs with the hide-from-discovery entity attribute.
    This filter has no effect if your app has no discovery interface.
    Note: Hiding an IdP from the discovery interface does NOT prevent
    the SP from accepting an assertion from the IdP.
  -->
  <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
      attributeName="http://macedir.org/entity-category"
      attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      attributeValue="http://refeds.org/category/hide-from-discovery"/>

</MetadataProvider>
```

See the List of IdP Display Names in InCommon Metadata to preview the IdPs that will appear on the discovery interface.

Slow network connection?

If you routinely experience network issues while refreshing InCommon metadata, try increasing the timeout on the SP's metadata refresh process. For example, the following child element of the `<MetadataProvider>` parent element sets the transport timeout to 120 seconds:

```
<TransportOption provider="CURL" option="13">120</TransportOption>
```

See the NativeSPTransportOption topic in the Shibboleth wiki for more details.

For More Information

- https://wiki.shibboleth.net/confluence/display/IDP30/HTTPMetadataProviders
- https://wiki.shibboleth.net/confluence/display/IDP30/SignatureValidationFilter
- https://wiki.shibboleth.net/confluence/display/IDP30/RequiredValidUntilFilter
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPMetadataProvider
- https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider
- https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPTransportOption
- https://wiki.shibboleth.net/confluence/display/EDS10