prefetch-entity-with-shib

You may wish to pre-fetch one or more entities to help mitigate any risk that the MDQ service is down. For example, if your SP primarily only interacts with one IdP in the federation, you could pre-fetch that IdP's metadata and fall back on MDQ for any other IdPs that may occasionally be used. Provided below are examples for configuring both a Shibboleth SP and a Shibboleth IdP to fetch some metadata.

For an added layer of local caching of per-entity metadata, you may wish to deploy one or more instances of the MDQ Signing Container (this is the same container that InCommon uses as the basis for this service). Configuration of that container is outside the scope of this documentation. If you choose to deploy a local MDQ service, please be aware that:

1. Unless your local deployment of the signing container is at least as available as the commercial CDN that InCommon uses for the MDQ service, you may introduce an availability problem for your metadata clients.
2. The signing container will generate its own key and re-sign InCommon metadata using that key. If you deploy multiple instances of the container, you should configure them to all use the same signing key. You would then need to configure your metadata clients to use your local MDQ service and verify the signature on metadata using it's signing key rather than InCommon's

Shibboleth SP Example

```
<!-- Pre-fetches metadata for the Internet2 IdP -->
<MetadataProvider type="XML" validate="true"
                  uri="https://mdq.incommon.org/entities/urn:mace:incommon:
internet2.edu"
                  backingFilePath="internet2-idp.xml" reloadInterval="3600"
>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1209600"/>
  <MetadataFilter type="Signature" certificate="inc-md-cert-mdq.pem"/>
</MetadataProvider>

<!-- InCommon Per-Entity Metadata Distribution Service -->
<MetadataProvider type="Dynamic" ignoreTransport="true">
  <Subst>https://mdq.incommon.org/entities/$entityID>
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="1209600"/>
  <MetadataFilter type="Signature" certificate="inc-md-cert-mdq.pem"/>
</MetadataProvider>
```


The Shibboleth SP reads metadata in the order that the providers are listed in the configuration file. You should put your pre-fetched entities ***before*** the dynamic metadata provider. In the above example, the SP will try to refresh the Internet2 IdP's metadata every hour and fall back to MDQ if any other entity's metadata is required.

Shibboleth IdP Example

Related content

- Configure other software
- Configure Shibboleth service provider
- Locating the production metadata
- Migrating to the MDQ Service
- Metadata signing key for the Production environment
- Prefetch an entity with Shibboleth
- Introducing per-entity metadata service
- Metadata Distribution Service Documentation
- Metadata Service
- Configure Shibboleth identity provider

Get help

Can't find what you are looking for?

help Ask the community

```
<!-- Pre-fetch metadata for ACME research org SP with an entity id of
https://42.acme.org/shibboleth -->
<MetadataProvider id="acme-research-sp" xsi:type="
FileBackedHTTPMetadataProvider"
            metadataURL="https://mdq.incommon.org/entities/https:%2F%2F42.
acme.org%2Fshibboleth"
            backingFile="%{idp.home}/metadata/acmd-research-sp.xml"
            maxRefreshDelay="PT1H">
  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
                  certificateFile="%{idp.home}/credentials/inc-md-cert-mdq.
pem" />
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"
/>
</MetadataProvider>

<!-- InCommon Per-Entity Metadata Distribution Service -->
<MetadataProvider id="incommon" xsi:type="DynamicHTTPMetadataProvider">

  <!-- Verify the signature on the root element (i.e., the
EntityDescriptor element) -->
  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
                  certificateFile="%{idp.home}/credentials/inc-md-cert-mdq.
pem" />

  <!-- Require a validUntil XML attribute no more than 14 days into the
future -->
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"
/>

  <!-- The MetadataQueryProtocol element specifies the base URL for the
query protocol -->
  <MetadataQueryProtocol>https://mdq.incommon.org/>
</MetadataProvider>
```

⚠ Like the Shibboleth SP configuration, the Shibboleth IdP looks up SP metadata from MetadataProviders in the order that the providers are listed in the configuration file. You should put your pre-fetched entities ***before*** the MDQ provider so that the IdP favors the prefetched copy over MDQ.