Protect Against Failed Metadata Processes

Contribute to this Wiki Page!

Log into the Spaces wiki and add a comment or suggestion to this wiki page! Send questions to the metadata-support mailing list.

Protect Against Failed Metadata Processes

Contents

Shibboleth IdP

All Shibboleth IdP deployers in the InCommon Federation are strongly advised to take the following precautions to protect themselves against possible failed metadata processes:

1. Allocate at least 1500MB of heap space in the JVM
2. Enable DEBUG-level logging on the following Java classes:
   V2: org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider
   V3: org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver

See the sections below for details.

Heap Allocation in the JVM

As of February 18, 2016, *the Shibboleth Project recommends at least 1500MB of heap space* for deployments that rely on metadata files larger than 25MB. This recommendation applies to both Shibboleth IdP V3 and Shibboleth IdP V2:

- https://wiki.shibboleth.net/confluence/display/IDP30/Jetty93
- https://wiki.shibboleth.net/confluence/display/IDP30/Jetty92
- https://wiki.shibboleth.net/confluence/display/IDP30/ApacheTomcat8
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdpGlassfishPrepare
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPApacheTomcatPrepare
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPJetty7Prepare
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPJetty9Prepare

The InCommon metadata aggregate is large and growing!

Currently the InCommon metadata aggregate is ~32MB (and growing) so *Shibboleth IdP deployers in the InCommon Federation should plan to reconfigure their Java container* as recommended by the Shibboleth Project.

Actually, we have reason to believe that metadata refresh failures are occurring with metadata files smaller than 25MB. Over the last few months, Shibboleth IdP deployers have reported numerous failed metadata processes. In the system log, it appears as though a refresh is attempted but no new metadata is found so the IdP continues to rely on the original metadata. This eventually results in expired metadata and failed user logins. The reasons for these failures are not entirely understood since a known logging issue is preventing the root cause from being logged (see the next section for a workaround to this issue). Strong evidence suggests that insufficient memory is the cause of these failures.

Allocate sufficient heap space in the JVM

As a precaution, it is recommended that deployers **allocate at least 1500MB of heap space in the JVM** as soon as possible. Do this for all your Shibboleth IdP deployments, in both test and production, for both V3 and V2.

For some Shibboleth IdP deployments, even that may not be enough. The following advice was overheard on the Shibboleth mailing list:

> *Use a 64-bit OS, hand it 3G or more, and stop wasting valuable person time trying to save money on RAM.*

Please take this issue **very** seriously!

Working Around a Known Logging Issue

Since a metadata refresh process thread reportedly fails without logging an exception, the Shibboleth Project team investigated the issue:

- Shib IdP V2: https://issues.shibboleth.net/jira/browse/JOST-243 (closed)
- Shib IdP V3: https://issues.shibboleth.net/jira/browse/OSJ-125 (closed)

Apparently the JVM is running out of memory but the error message is not being logged. There is a workaround, however. The failure can be observed in logs when DEBUG mode logging is enabled on the relevant Java class.

Work around a known logging issue

InCommon strongly recommends that all Shibboleth IdP deployers **implement the following simple workarounds immediately**, even if you are unable to upgrade the heap in the JVM at this time. Without these workarounds in place, you are running blind.

To work around this issue in Shibboleth IdP V2, add the following DEBUG logger to /opt/shibboleth-idp/conf/logging.xml:

Shibboleth IdP V2 workaround to JOST-243

```
<!-- the following logger works around issue https://issues.shibboleth.net/jira/browse/JOST-243 -->
<logger name="org.opensaml.saml2.metadata.provider.AbstractReloadingMetadataProvider" level="DEBUG"/>
```

To work around this issue in Shibboleth IdP V3, add the following DEBUG logger to /opt/shibboleth-idp/conf/logback.xml:

Shibboleth IdP V3 workaround to OSJ-125

```
<!-- the following logger works around issue https://issues.shibboleth.net/jira/browse/OSJ-125 -->
<logger name="org.opensaml.saml.metadata.resolver.impl.AbstractReloadingMetadataResolver" level="DEBUG"/>
```

Note: The logging issue will be fixed in Shibboleth IdP V2.4.5 and Shibboleth IdP V3.2.0, respectively.

SimpleSAMLphp

All simpleSAMLphp deployers in the InCommon Federation are strongly encouraged to upgrade to simpleSAMLphp v1.13.2 (or later). Previous versions of simpleSAMLphp are known to have performance issues when processing large metadata files. See the simpleSAMLphp mailing list archives for details regarding this performance issue.