Service Provider Virtualization

Running multiple SPs on a single host

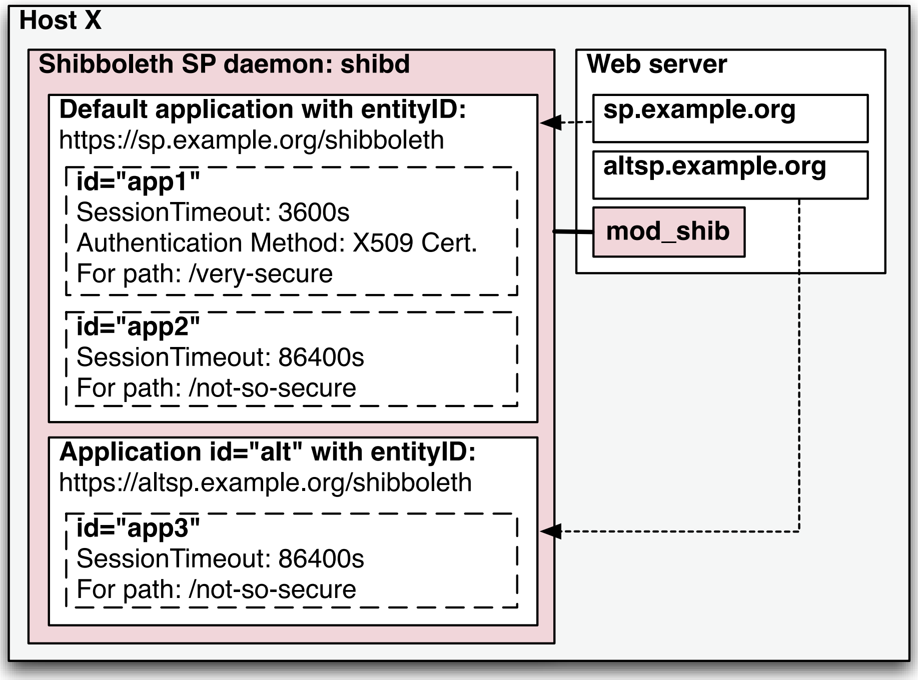
SWITCHaai Team
aai@switch.ch

Physical vs. logical SP

A single physical SP can host any number of logical SPs

- A logical SP can then include any number of “applications”
- Applications can be configured on a per-path or per-virtual-host basis
- Web virtual hosting is often related but is also independent
- Applications can inherit or override default configuration settings on a piecemeal basis

Multiple applications and domains on a single host



Host X

Shibboleth SP daemon: shibd

Default application with entityID:
https://sp.example.org/shibboleth

id="app1"
SessionTimeout: 3600s
Authentication Method: X509 Cert.
For path: /very-secure

id="app2"
SessionTimeout: 86400s
For path: /not-so-secure

Application id="alt" with entityID:
https://altsp.example.org/shibboleth

id="app3"
SessionTimeout: 86400s
For path: /not-so-secure

Web server

sp.example.org

altsp.example.org

mod_shib

shibboleth2.xml configuration

Add an **`ApplicationOverride`** element for each logical SP, and specify its own **`CredentialResolver`**:

```
<ApplicationDefaults id="default" policyId="default" ... >
  ...
  <ApplicationOverride id="altsp"
        entityID="https://altsp#.example.org/shibboleth">
    <CredentialResolver type="File"
        key="/etc/shibboleth/altsp-key.pem"
        certificate="/etc/shibboleth/altsp-cert.pem"/>
  </ApplicationOverride>
</ApplicationDefaults>
```

Note: when adding a customized **`Sessions`** element to the **`ApplicationOverride`**, be sure to spell out *all* its attributes. Inheritance from **`ApplicationDefaults`** is disabled as soon as a **`Sessions`** element is present.

Apache httpd configuration

Define an additional **`VirtualHost`** for the logical SP, and map it to the respective **`ApplicationOverride`** from shibboleth2.xml:

```
<VirtualHost *:443>
  ServerName altsp#.example.org:443
  ...

  <Location />
    ShibRequestSetting applicationId altsp
  </Location>

</VirtualHost>
```

IIS Site Mapping

In shibboleth2.xml, add a **`<Host>`** element for the logical SP (with the **`name`** attribute matching the IIS site name):

```
<RequestMapper type="Native"
  <RequestMap>
    <Host name="sp#.example.org">
      <Path name="secure" authType="shibboleth"
            requireSession="true"/>
    </Host>
    <Host name="altsp#.example.org" applicationId="altsp">
      <Path name="secure" authType="shibboleth"
            requireSession="true"/>
    </Host>
  </RequestMap>
</RequestMapper>
```

Recommendations

- use separate Apache `VirtualHosts` / IIS sites to run multiple, but distinct AAI-protected resources on a single host (avoid path-based separation of applications)
- define separate entity IDs for each resource, and create key pairs (self-signed certificates) for each of them
- register and manage each resource / logical SP in the AAI RR as a separate entity with its respective attribute requirements
- Further reading:
  https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPApplicationOverride