Authentication

SWITCH
Serving Swiss Universities

Notes:

Terms: Authentication Mechanism

- A concrete mechanism used to authenticate a user.
- Shibboleth 2 currently supports REMOTE_USER, user/pass against LDAP & Kerberos, and IP address based mechanisms.

Notes:

Terms: Authentication Method

- An identifier that a relying party may use to stipulate how authentication should be performed.
- Authentication method identifiers correspond to a prescription of how authentication is done (even if the details are only in someone's head).

Notes:

Terms: Login Handler

- An IdP component that correlates all supported authentication methods with currently configured authentication mechanisms.
- A login handler may map more than one authentication method to the same authentication mechanism.

Notes:

Terms: Session

- State information about the user, currently active authentication methods, and services to which they are signed into.
- A user's IdP session is created the first time they authenticate but may outlive the lifetime of all authentication methods.

Notes:

Authentication: Goals

- Configure UsernamePassword login handler to authenticate against LDAP.

Notes:

Login Handler: Configuration

- Login handlers are configured in handler.xml
- `<LoginHandler>` defines a login handler
- Every login handler definition has a `xsi:type` attribute that defines the type of the handler.
- Each type has its own set of configuration options.

 https://spaces.internet2.edu/display/SHIB2/IdPUserAuthn

Notes:

Login Handler: Configuration

- Each `<LoginHandler>` must contain at least one `<AuthenticationMethod>` which indicates what authentication method the login handler provides.

Notes:

Login Handler: UsernamePassword

- Login handler that prompts for a username/password and validates against a JAAS module (LDAP & Kerberos 5 currently supported)
- Type attribute value: `UsernamePassword`
- Configuration attributes:
  - `jaasConfigurationLocation` path to the JAAS configuration file

Notes:

Login Handler: UsernamePassword

- Edit the login.config

1. Uncomment the LDAP login modules
2. Configure it like this:

```
edu.vt.middleware.ldap.jaas.LdapLoginModule
  required
      host=”127.0.0.1”
      port=“10389”
      base="ou=people,dc=example,dc=org"
      userField="uid";
```

Notes:

Login Handler: UsernamePassword

- Edit handler.xml

1. Comment out RemoteUser handler
2. Uncomment UsernamePassword handler

- Turn on debug logging for the LDAP login module by adding the following logger to logging.xml

```
<logger name="edu.vt.middleware.ldap">
   <level value="DEBUG" />
</logger>
```


Notes:

LoginHandler: UsernamePassword

1. Restart Tomcat
2. Access
   https://sp#.example.org/cgi-bin/attribute-viewer
3. Select your IdP from the list
4. Use `student1/password` as the username/password

Notes:

LoginHandler: UsernamePassword

- The login page presented to the user is /opt/installfest/distro/identityprovider/resources/webpages/login.jsp
- You may define more than one UsernamePassword login handler, with different authentication methods. For example one that work with LDAP and another that works with Kerberos
- You may define more than one LDAP host so that if one is down another is used.

Notes:

Login Handler: Authentication Duration

- Each authentication mechanism supports an activity timeout
- After this timeout expires the mechanism is considered inactive for that user.
- If the user attempts to access a new service provider that requires that authentication mechanism they must re-authenticate.

Notes:

Login Handler: Authentication Duration

- It is configured by the `authenticationDuration` attribute on the `<LoginHandler>`
- Its value is the number of minutes of inactivity and its default value is 30.

Notes:

Forced Authentication

- SAML 2 allows a service provider to force authentication of the user, even if the user has an existing session.
- Only works with mechanisms that can re-authenticate a user.
- RemoteUser does not support forced authentication.
- The service provider will receive an error if the IdP can not support forced authentication

Notes:

Authentication Method Selection

- An SP may provide a list of acceptable methods
- The IdP then checks to see if any active mechanism provides any of those methods, if so, single sign on occurs
- Otherwise the IdP picks supported, but not yet active, method and uses that.

Notes: