APSSimpleUserServiceAuthServiceProvider

User Guide

Version: 0.9.2

Author: Tommy Svensson

Copyright © 2013 Natusoft AB

Table of Contents

1 APSAuthService

This is a very simple little service that only does authentication of users. This service is currently used by the APS administration web (/apsadminweb) and APSExtProtocolHTTPTransportProvider for remote calls to services over http.

The idea behind this service is that it should be easy to provide an implementation of this that uses whatever authentication scheme you want/need. If you have an LDAP server you want to authenticate against for example, provide an implementation that looks up and authenticates the user against the LDAP server.

See this a little bit like an authentication plugin.

The APS web applications that use this only uses password authentication.

1.1 APSSimpleUserServiceAuthServiceProvider

This provides an APSAuthService that uses the APSSimpleUserService to authenticate users. It only supports password authentication. If you don't have your own implementation of APSAuthService then you can deploy this one along with APSSimpleUserService, and probably APSUserAdminWeb.

1.2 API

public *interface* **APSAuthService<Credential>** [se.natusoft.osgi.aps.api.auth.user] {

This is intended to be used as a wrapper to other means of authentication. Things in APS that needs authentication uses this service.

Implementations can lookup the user in an LDAP for example, or use some other user service.

APS supplies an *APSSimpleUserServiceAuthServiceProvider* that uses the *APSSimpleUserService* to authenticate. It is provided in its own bundle.

Properties authUser(String userId, Credential credentials, AuthMethod authMethod) throws APSAuthMethodNotSupportedException

This authenticates a user. A Properties object is returned on successful authentication. null is returned on failure. The Properties object returned contains misc information about the user. It can contain anything or nothing at all. There can be no assumptions about its contents!

Returns

> *User properties on success, null on failure.*

Parameters

> *userId* - *The id of the user to authenticate.*
>
> *credentials* - *What this is depends on the value of AuthMethod. It is up to the service implementation to resolve this.*
>
> *authMethod* - *This hints at how to interpret the credentials.*

Throws

APSAuthMethodNotSupportedException *- If the specified authMethod is not supported by the implementation.*

Properties authUser(String userId, Credential credentials, AuthMethod authMethod, String role) throws APSAuthMethodNotSupportedException

This authenticates a user. A Properties object is returned on successful authentication. *null* is returned on failure. The Properties object returned contains misc information about the user. It can contain anything or nothing at all. There can be no assumptions about its contents!

Returns

User properties on success, null on failure.

Parameters

userId *- The id of the user to authenticate.*

credentials *- What this is depends on the value of AuthMethod. It is up to the service implementation to resolve this.*

authMethod *- This hints at how to interpret the credentials.*

role *- The specified user must have this role for authentication to succeed. Please note that the APS admin webs will pass "apsadmin" for the role. The implementation might need to translate this to another role.*

Throws

APSAuthMethodNotSupportedException *- If the specified authMethod is not supported by the implementation.*

AuthMethod[] getSupportedAuthMethods()

Returns an array of the AuthMethods supported by the implementation.

public *static enum* **AuthMethod** [se.natusoft.osgi.aps.api.auth.user] {

This hints at how to use the credentials.

NONE

Only userid is required.

PASSWORD

toString() on the credentials object should return a password.

KEY

The credential object is a key of some sort.

CERTIFICATE

The credential object is a certificate of some sort.

DIGEST

The credential object is a digest password.

SSO

The credential object contains information for participating in a single sign on.

}
