Security

Security Options

Securing your repository is achieved through many activities and not the result of a single feature. Attending to the physical security of the servers and good systems administration practices are a necessary first step. It is recommended that you prepare a security policy to determine the requirements, processes, and practices appropriate for your repository. Using your security policy, you choose which of Fedora's many options are right for your needs.

Quick Start Guide to Securing Your Repository

Here is a quick start guide that describes what you will need to do to configure your Fedora repository. It is recommended that you start with the new installer and one of the base security configurations it creates, and become familiar with the new installation and default security features. Then you can go back and experiment with customizing various aspects of your repository configuration and policies.

1. Select a base security configuration by running Fedora installer jar
2. Optionally customize `fedora.fcfg` for your repository
3. Choose basic security, the XACML Policy Engine, or the new Fedora Security Layer (FeSL)
4. Optionally customize XACML policies (repository-wide and object-specific policies)
5. Optionally customize fedora-users.xml for your repository and users
6. Optionally customize web.xml to use servlet filters for authentication and user attributes
7. Start the fedora server

- Remember that beSecurity has been turned off

Introduction to Fedora Servlet security filters

We here assume that you have already installed Fedora, in either quick or custom varieties. This document gives advice on using Fedora's servlet security filters and its surrogate feature. These filters authenticate Fedora users and/or provide user attributes to use in XACML authorization.

Fedora's servlet security filters are configured in the web deployment descriptor file (web.xml), typically in Fedora's webapp directory in whatever servlet container (e.g., Tomcat) you've deployed Fedora in. Section "Specifying Filter Configuration" in The Essentials of Filters discusses the format of specifying filters and filter-mappings and gives more information on the format of the servlet filter section of web.xml. (That section does not have an anchored location to link to directly.) It may be helpful to use the Fedora web.xml as guide while reading this document.

The Fedora installer will have configured several servlet filters in the correct order. Leave these in the order given, with the filter elements grouped first, and then the grouped filter-mapping elements following as a second group. Within either filter or filter-mapping unit, the filter definitions are ordered: SetupFilter, XmlUserfileFilter, (LdapFilterForAttributes), (LdapFilterForGroups), EnforceAuthnFilter, FinalizeFilter. The filters in parenthesis are optional, and won't be installed by default. Again, retain this order and if you add a filter, use the place indicated.

The filter-mappings of the EnforceAuthnFilter determine which Fedora urls require user authentication. The installer will set up these various mappings either for api-m alone or for both api-m and api-a urls/servlets. You can customize web.xml for this, likely by adding or deleting mappings for this filter, if you need and know.

Parameter settings are specific to a servlet filter, and are given below for the Fedora servlet security filters. Here is the format which the specification takes in web.xml:

```
<filter>
    <filter-name>LdapFilterForAttributes</filter-name>
    <filter-class>fedora.server.security.servletfilters.ldap.FilterLdap</filter-class>
    <init-param>
        <param-name>authenticate</param-name>
        <param-value>false</param-value>
        . . .
    </init-param>
</filter>
```

Use this format to define in web.xml the parameter settings you need.

General Parameters

The following parameters are useful for XmlUserfileFilter, LdapFilterForAttributes, and LdapFilterForGroups.

parameter	use	default	note
authenticate	whether the current filter should attempt to authenticate the user	true	if a previous filter has already authenticated the user, this filter doesn't try also for the current request. a value of "false" still permits associated-filters from providing user attributes

associated-filters	comma-separated list of previous filters, of any number including none. if any of these listed filters have authenticated the current user, then this filter will provide attributes for the user if it can.	current filter	if this parm is specified, the current filter must be explicitly named, i.e., it's no longer implicitly in the list
lookup-success-timeout-unit	how long to cache a successful lookup (whether for authentication or attribute/group lookup) – the *units* themselves	minute	
lookup-success-timeout-duration	how long to cache a successful lookup (whether for authentication or attribute/group lookup) – the *number* of units	10	
authn-failure-timeout-unit	how long to cache user not found (whether for authentication or attribute/group lookup) – the *units* themselves	second	
authn-failure-timeout-duration	how long to cache user not found (whether for authentication or attribute/group lookup) – the *number* of units	1	
lookup-exception-timeout-unit	how long to cache a problematic lookup (whether for authentication or attribute/group lookup) – the *units* themselves	second	
lookup-exception-timeout-duration	how long to cache a problematic lookup (whether for authentication or attribute/group lookup) – the *number* of units	1	

Parameters for LDAP servlet filter for user attributes

The following parameters are useful for either LdapFilterForAttributes or LdapFilterForGroups. The example values are chosen for LdapFilterForAttributes. If you are setting up this filter, use "LdapFilterForAttributes" as filter-name, "fedora.server.security.servletfilters.ldap.FilterLdap" as filter-class, and choose values from the parameters below which fit your Ldap directory configuration for reading user *attributes*. You can also use parameters for either/both Ldap authentication/binding and/or the surrogate feature, as explained elsewhere in this document. You may need to talk to your directory administrator to find out these settings.

parameter	use	example
url	internet address of directory server	ldap://ldap.virginia.edu:389/
search-base	ldap-style specification where in directory to base user search	o=University of Virginia,c=US
search-filter	ldap-style specification how to conduct user search	(uid={0})
id-attribute	directory attribute which is user id	uid
attributes	comma-separated list of directory attributes to use as user's xacml subject attributes	mailAlternateAddress,eduPersonAffiliation

Parameters to use LDAP servlet filter for user group memberships

The following parameters are useful for LdapFilterForGroups and have example values chosen for LdapFilterForGroups. If you are setting up this filter, use "LdapFilterForGroups" as filter-name, "fedora.server.security.servletfilters.ldap.FilterLdap" as filter-class, and choose values for the parameters below which fit your Ldap directory configuration for reading *group* memberships. This will be more specific to your directory than for reading user attributes. You can also use parameters for either/both Ldap authentication/binding and/or the surrogate feature, as explained elsewhere in this document. You may need to talk to your directory administrator to find out these settings. Some directories will store no group memberships, or store them in a way for which this servlet filter isn't configurable.

parameter	use	example
url	internet address of directory server	ldap://pitchfork.itc.virginia.edu:389/
search-base	ldap-style specification where in directory to base user search	ou=Groups,o=University of Virginia, c=US
search-filter	ldap-style specification how to conduct user search	(memberUid={0})
id-attribute	directory attribute which is user id	uid
attributes	comma-separated list of directory attributes to use as user's xacml subject attributes	cn
attributes-common-name	return all attribute values under this name; this override prevents using the awkward "cn" as an XACML subject attribute	groups

Parameters for Authentication and Binding with LDAP

The following parameters are useful for either LdapFilterForAttributes or LdapFilterForGroups, and are used with other values given elsewhere in this document. You must choose values from the parameters below which fit your Ldap directory configuration for binding to the directory. You may need to talk to your directory administrator to find out these settings.

parameter	use	example	note

security-authentication	specification of how to bind to directory server	simple	if specified, a directory bind will occur. so neither an anonymous connect nor a field-compare authentication will occur. if security-principal and security-credentials are specified, they are used to bind the connection. if they are not not specified, a bind is attempted with the user's credentials, and success determines user authentication, if authenticate is also specified
security-principal	privileged (non-user) id with which to bind to directory server	site-specific; get from your directory administrator	
security-credentials	privileged password with which to bind to directory server	site-specific; get from your directory administrator	
password-attribute	directory attribute which is user password. if given, marks that user password will be compared to the directory to authenticate.	uid	

Obviously, some combinations of these values are incompatible, and yet others necessary to achieve certain aims.

Parameters for Surrogate Feature

The surrogate feature supports end-user authentication by a Fedora client or web server front-end. The surrogate user is represented in the request directly (in the usual header) and is authenticated by Fedora as usual. A From: header holds the identity of the represented virtual user.

parameter	use	example	note
surrogate-attribute	name of attribute which a user authenticated by this or an earlier filter must have to become a surrogate user. Any value of the attribute is acceptable.	SURROGATE	
surrogate-associated-filters	comma-separated list of previous filters, of any number including none. if any of these listed filters have authenticated a surrogate user and so there is a virtual user, then this filter will provide attributes for the virtual user if it can.		if this parm is specified, the current filter must be explicitly named, i.e., it's not implicitly in the list.

Authorization via XACML

Fedora 2.0 hardcoded minimal authorization constraints, beyond those provided by specifications in Tomcat's web.xml file. Fedora now exposes these to customization by encoding them in the XACML standard. A complete description can be found in the documentation for the Fedora Authorization with XACML Policy Enforcement.

Default Repository Policies

Fedora ships with a set of default repository-wide XACML policies that approximate the minimal security level provided by Fedora. This set of repository-wide policies includes the following policies:

Custom Policies

Note that the default repository policies enforce a minimal level security (e.g., API-A is totally unrestricted). If you need a more customized level of access control what is provided by the default, you will need to add additional repository-wide policies or individual object-specific policies to customize your access environment. Refer to the Fedora XACML Policy Writing Guide document for more information about how to construct policies for your repository.