Apache Module mod_dav

Description:	Distributed Authoring and Versioning (WebDAV[1]) functionality
Status:	Extension
Module Identifier:	dav_module
Source File:	mod_dav.c

Summary

This module provides class 1 and class 2 WebDAV [2] ('Web-based Distributed Authoring and Versioning') functionality for Apache. This extension to the HTTP protocol allows creating, moving, copying, and deleting resources and collections on a remote web server.

Topics

Directives

See also

- DavLockDB
- LimitXMLRequestBody
- WebDAV Resources[2]

Enabling WebDAV

To enable mod_dav, add the following to a container in your httpd.conf file:

```
Dav On
```

This enables the DAV file system provider, which is implemented by the mod_dav_fs module. Therefore that module has to be compiled into the server or has to be loaded at runtime using the LoadModule directive.

In order to make it work you have to specify a web-server writable filename for the DAV lock database by adding the following to the global section in your httpd.conf file:

```
DavLockDB /tmp/DavLock
```

You may wish to add a <Limit> clause inside the <Location> directive to limit access to DAV-enabled locations. If you want to set the maximum amount of bytes that a DAV client can send at one request, you have to use the LimitXMLRequestBody directive. The "normal" LimitRequestBody directive has no effect on DAV requests.

Full Example

```
DavLockDB /tmp/DavLock

<Location /foo>
```

```
  Dav On

  AuthType Basic
  AuthName DAV
  AuthUserFile user.passwd

  <LimitExcept GET HEAD OPTIONS>
    require user admin
  </LimitExcept>
</Location>
```

Security

The use of HTTP Basic Authentication is not recommended. You should use at least HTTP Digest Authentication, which is provided by the mod_auth_digest module. Nearly all WebDAV clients support this authentication method. Of course, Basic Authentication over an SSL[3] enabled connection is secure, too.

Dav Directive

Description:	Enable WebDAV HTTP methods
Syntax:	`Dav On|Off|`*`provider-name`*
Default:	`Dav Off`
Context:	directory
Status:	Extension
Module:	mod_dav

Use the `Dav` directive to enable the WebDAV HTTP methods for the given container:

```
<Location /foo>
  Dav On
</Location>
```

The value `On` is actually an alias for the default provider `filesystem` which is served by the `mod_dav_fs` module. Note, that once you have DAV enabled for some location, it *cannot* be disabled for sublocations. For a complete configuration example have a look at the section above.

Do not enable WebDAV until you have secured your server. Otherwise everyone will be able to distribute files on your system.

DavDepthInfinity Directive

Description:	Allow PROPFIND, Depth: Infinity requests
Syntax:	`DavDepthInfinity on|off`
Default:	`DavDepthInfinity off`
Context:	server config, virtual host, directory
Status:	Extension
Module:	mod_dav

Use the DavDepthInfinity directive to allow the processing of PROPFIND requests containing the header 'Depth: Infinity'. Because this type of request could constitute a denial-of-service attack, by default it is not allowed.

DavMinTimeout Directive

Description:	Minimum amount of time the server holds a lock on a DAV resource
Syntax:	DavMinTimeout *seconds*
Default:	DavMinTimeout 0
Context:	server config, virtual host, directory
Status:	Extension
Module:	mod_dav

When a client requests a DAV resource lock, it can also specify a time when the lock will be automatically removed by the server. This value is only a request, and the server can ignore it or inform the client of an arbitrary value.

Use the DavMinTimeout directive to specify, in seconds, the minimum lock timeout to return to a client. Microsoft Web Folders defaults to a timeout of 120 seconds; the DavMinTimeout can override this to a higher value (like 600 seconds) to reduce the chance of the client losing the lock due to network latency.

Example

```
<Location /MSWord>
  DavMinTimeout 600
</Location>
```

URI References

[1] http://www.webdav.org/
[2] http://www.webdav.org
[3] http://httpd.apache.org/docs-2.1/ssl/