Apache Module mod_ldap

Description:	LDAP connection pooling and result caching services for use by other LDAP modules
Status:	Experimental
Module Identifier:	ldap_module
Source File:	util_ldap.c
Compatibility:	Available in version 2.0.41 and later

Summary

This module was created to improve the performance of websites relying on backend connections to LDAP servers. In addition to the functions provided by the standard LDAP libraries, this module adds an LDAP connection pool and an LDAP shared memory cache.

To enable this module, LDAP support must be compiled into apr-util. This is achieved by adding the `--with-ldap` flag to the `./configure` script when building Apache.

Topics

Directives

Example Configuration

The following is an example configuration that uses `mod_ldap` to increase the performance of HTTP Basic authentication provided by `mod_auth_ldap`.

```
# Enable the LDAP connection pool and shared
# memory cache. Enable the LDAP cache status
# handler. Requires that mod_ldap and mod_auth_ldap
# be loaded. Change the "yourdomain.example.com" to
# match your domain.

LDAPSharedCacheSize 200000
LDAPCacheEntries 1024
LDAPCacheTTL 600
LDAPOpCacheEntries 1024
LDAPOpCacheTTL 600

<Location /ldap-status>
  SetHandler ldap-status
  Order deny,allow
  Deny from all
  Allow from yourdomain.example.com
  AuthLDAPEnabled on
  AuthLDAPURL ldap://127.0.0.1/dc=example,dc=com?uid?one
  AuthLDAPAuthoritative on
  require valid-user
</Location>
```

LDAP Connection Pool

LDAP connections are pooled from request to request. This allows the LDAP server to remain connected and bound ready for the next request, without the need to unbind/connect/rebind. The performance advantages are similar to the effect of HTTP keepalives.

On a busy server it is possible that many requests will try and access the same LDAP server connection simultaneously. Where an LDAP connection is in use, Apache will create a new connection alongside the original one. This ensures that the connection pool does not become a bottleneck.

There is no need to manually enable connection pooling in the Apache configuration. Any module using this module for access to LDAP services will share the connection pool.

LDAP Cache

For improved performance, `mod_ldap` uses an aggressive caching strategy to minimize the number of times that the LDAP server must be contacted. Caching can easily double or triple the throughput of Apache when it is serving pages protected with mod_auth_ldap. In addition, the load on the LDAP server will be significantly decreased.

`mod_ldap` supports two types of LDAP caching during the search/bind phase with a *search/bind cache* and during the compare phase with two *operation caches*. Each LDAP URL that is used by the server has its own set of these three caches.

The Search/Bind Cache

The process of doing a search and then a bind is the most time-consuming aspect of LDAP operation, especially if the directory is large. The search/bind cache is used to cache all searches that resulted in successful binds. Negative results (*i.e.*, unsuccessful searches, or searches that did not result in a successful bind) are not cached. The rationale behind this decision is that connections with invalid credentials are only a tiny percentage of the total number of connections, so by not caching invalid credentials, the size of the cache is reduced.

`mod_ldap` stores the username, the DN retrieved, the password used to bind, and the time of the bind in the cache. Whenever a new connection is initiated with the same username, `mod_ldap` compares the password of the new connection with the password in the cache. If the passwords match, and if the cached entry is not too old, `mod_ldap` bypasses the search/bind phase.

The search and bind cache is controlled with the `LDAPCacheEntries` and `LDAPCacheTTL` directives.

Operation Caches

During attribute and distinguished name comparison functions, `mod_ldap` uses two operation caches to cache the compare operations. The first compare cache is used to cache the results of compares done to test for LDAP group membership. The second compare cache is used to cache the results of comparisons done between distinguished names.

The behavior of both of these caches is controlled with the `LDAPOpCacheEntries` and `LDAPOpCacheTTL` directives.

Monitoring the Cache

`mod_ldap` has a content handler that allows administrators to monitor the cache performance. The name of the content handler is `ldap-status`, so the following directives could be used to access the mod_ldap cache information:

```
<Location /server/cache-info>
  SetHandler ldap-status
</Location>
```

By fetching the URL http://servername/cache-info, the administrator can get a status report of every cache that is used by mod_ldap cache. Note that if Apache does not support shared memory, then each httpd instance has its own cache, so reloading the URL will result in different information each time, depending on which httpd instance processes the request.

LDAPCacheEntries Directive

Description:	Maximum number of entires in the primary LDAP cache
Syntax:	LDAPCacheEntries *number*
Default:	LDAPCacheEntries 1024
Context:	server config
Status:	Experimental
Module:	mod_ldap

Specifies the maximum size of the primary LDAP cache. This cache contains successful search/binds. Set it to 0 to turn off search/bind caching. The default size is 1024 cached searches.

LDAPCacheTTL Directive

Description:	Time that cached items remain valid
Syntax:	LDAPCacheTTL *seconds*
Default:	LDAPCacheTTL 600
Context:	server config
Status:	Experimental
Module:	mod_ldap

Specifies the time (in seconds) that an item in the search/bind cache remains valid. The default is 600 seconds (10 minutes).

LDAPCertDBPath Directive

Description:	Directory containing certificates for SSL support
Syntax:	LDAPCertDBPath *directory-path*
Context:	server config
Status:	Experimental
Module:	mod_ldap

This directive is only valid if Apache has been linked against the Netscape/iPlanet Directory SDK.

It specifies in which directory mod_ldap should look for the certificate authorities database for SSL support. There should be a file named cert7.db in that directory.

LDAPOpCacheEntries Directive

Description:	Number of entries used to cache LDAP compare operations
Syntax:	`LDAPOpCacheEntries` *`number`*
Default:	`LDAPOpCacheEntries 1024`
Context:	server config
Status:	Experimental
Module:	mod_ldap

This specifies the number of entries `mod_ldap` will use to cache LDAP compare operations. The default is 1024 entries. Setting it to 0 disables operation caching.

LDAPOpCacheTTL Directive

Description:	Time that entries in the operation cache remain valid
Syntax:	`LDAPOpCacheTTL` *`seconds`*
Default:	`LDAPOpCacheTTL 600`
Context:	server config
Status:	Experimental
Module:	mod_ldap

Specifies the time (in seconds) that entries in the operation cache remain valid. The default is 600 seconds.

LDAPSharedCacheSize Directive

Description:	Size in bytes of the shared-memory cache
Syntax:	`LDAPSharedCacheSize` *`bytes`*
Default:	`LDAPSharedCacheSize 102400`
Context:	server config
Status:	Experimental
Module:	mod_ldap

Specifies the number of bytes to specify for the shared memory cache. The default is 100kb.