kvspb / **nginx-auth-ldap**

LDAP authentication module for nginx

127 commits **1** branch **1** release **27** contributors

kvspb committed on **GitHub** Merge pull request #157 from i-rinat/remove-item-from-waiting-request... Latest commit b809421 2 days ago

LICENSE	Verify certificate CN/SAN	a year ago
README.md	add referral option	4 months ago
config	Update config	5 months ago
example.conf	replacing tabs with spaces to fix example.conf formating	2 years ago
ngx_http_auth_ldap_module.c	remove timedout request ctx's from waiting_requests queue	2 months ago

README.md

LDAP Authentication module for nginx

LDAP module for nginx which supports authentication against multiple LDAP servers.

How to install

FreeBSD

```
cd /usr/ports/www/nginx && make config install clean
```

Check HTTP_AUTH_LDAP options

```
[*] HTTP_AUTH_LDAP        3rd party http_auth_ldap module
```

Linux

```
cd ~ && git clone https://github.com/kvspb/nginx-auth-ldap.git
```

in nginx source folder

```
./configure --add-module=path_to_http_auth_ldap_module
make install
```

Example configuration

Define list of your LDAP servers with required user/group requirements:

```
http {
  ldap_server test1 {
    url ldap://192.168.0.1:3268/DC=test,DC=local?sAMAccountName?sub?(objectClass=person);
    binddn "TEST\\LDAPUSER";
    binddn_passwd LDAPPASSWORD;
    group_attribute uniquemember;
    group_attribute_is_dn on;
    require valid_user;
  }

  ldap_server test2 {
    url ldap://192.168.0.2:3268/DC=test,DC=local?sAMAccountName?sub?(objectClass=person);
    binddn "TEST\\LDAPUSER";
    binddn_passwd LDAPPASSWORD;
    group_attribute uniquemember;
    group_attribute_is_dn on;
    require valid_user;
  }
}
```

And add required servers in correct order into your location/server directive:

```
server {
    listen       8000;
    server_name  localhost;

    auth_ldap "Forbidden";
    auth_ldap_servers test1;
    auth_ldap_servers test2;
```

```
        location / {
            root   html;
            index  index.html index.htm;
        }

    }
```

Available config parameters

url

expected value: string

Available URL schemes: ldap://, ldaps://

binddn

expected value: string

binddn_passwd

expected value: string

group_attribute

expected value: string

group_attribute_is_dn

expected value: on or off, default off

require

expected value: valid_user, user, group

satisfy

expected value: all, any

connections

expected value: a number greater than 0

ssl_check_cert

expected value: on or off, default off

Verify the remote certificate for LDAPs connections. If disabled, any remote certificate will be accepted which exposes you to possible man-in-the-middle attacks. Note that the server's certificate will need to be signed by a proper CA trusted by your system if this is enabled. See below how to trust CAs without installing them system-wide.

This options needs OpenSSL >= 1.0.2; it is unavailable if compiled with older versions.

ssl_ca_file

expected value: file path

Trust the CA certificate in this file (see ssl_check_cert above).

ssl_ca_dir

expected value: directory path

Trust all CA certificates in this directory (see ssl_check_cert above).

Note that you need to provide hash-based symlinks in the directory for this to work; you'll basically need to run OpenSSL's c_rehash command in this directory.

referral

expected value: on, off

LDAP library default is on. This option disables usage of referral messages from LDAP server. Usefull for authenticating against read only AD server without access to read write.