

---

## Apache authentication and authorisation against eDir and AD using LDAP for “Neanderthals”

Lawrence Kearney  
Enterprise and Workgroup Service Analyst  
Georgia Regents University

[lawrence.kearney@earthlink.net](mailto:lawrence.kearney@earthlink.net)  
<http://www.lawrencekearney.com>

- Apache “Neanderthal “ identification and socialisation
- General discussion about Apache deployments and operations
- Tips and best practices for large and enterprise class environments
- Securing and optimising Apache servers is a different discussion
- Discussion will focus on the basics of securing and optimising communications between clients and identity stores

### Apache “Prefork” vs “Worker” Multi-Processing Module (MPM)

**Prefork:** Non-threaded children processes, less conservative resource consumption but isolates faults

Required for compatibility with older or third party modules that don’t support threading

**Worker:** Threaded children and more efficient resource consumption use, but does not isolate faults

The default for Apache on SLES is to use the Prefork MPM

## Base modules

“Hardwired” modules improve performance when:

- Hardware and operating system platforms are known
- Web server configuration will be static

Viewing the modules built into the Apache server:

```
darkvixen163:/home/admin # httpd2 -l
Compiled in modules:
  core.c
  prefork.c
  http_core.c
  mod_so.c
```

## Loaded modules

Additional modules provide server flexibility when:

- Hardware and operating system platforms vary
- Web server configuration is not static

Viewing the modules loaded with the Apache server:

```
darkvixen163:/home/admin # a2enmod -l
actions alias auth_basic authn_file authz_host authz_groupfile authz_defa
ult authz_user authn_dbm autoindex cgi dir env expires include log_config
mime negotiation setenvif ssl suexec userdir php5 mod_ldap mod_authnz_ld
ap rewrite
```

### Listing, enabling and disabling modules

```
a2enmod -l  
a2enmod <module_package_name>  
a2dismod <module_package_name>
```

for example: **a2enmod ldap**

On the suse platform, “active” modules are stored in file used by “sysconfig”

**/etc/sysconfig/apache2:** contains the module list sysconfig uses to build the loadmodule.conf file

**/etc/apache2/sysconfig.d/loadmodule.conf:** the file Apache reads at startup to load them

- Use a modular approach to web site and web server configuration
- Envision and document authentication workflows in the planning stages of your implementations
- Seek support from peers and experts when hurdles are encountered in planning and implementation phases

Do draw on their professional and personal empathy 😊

Identity driven access to web services demands a minimum set of standards be met when providing that access:

Common expectations include:

- Real time data
- Performance
- Security



We do so with credentials, context and other stuff, electronically

- Identity credentials
- Identity credentials + directory data
- Identity credentials + directory data + host data

**Recommended extracurricular viewing:**

Keynote, O'Reilly OpenSource Convention

**Identity 2.0**

Dick Hardt, Founder and CEO Sxip Identity

<http://www.youtube.com/watch?v=RrpajcAgR1E>

In Apache module ease:

- `mod_auth_basic`
- `mod_auth_basic + (mod_ldap/mod_authnz_ldap)`
- `mod_auth_basic + (mod_ldap/mod_authnz_ldap) + mod_authz_host`

So we enable these modules,

```
a2enmod mod_auth_basic  
a2enmod mod_ldap  
a2enmod mod_authnz_ldap  
a2enmod mod_authz_host
```

### **mod\_auth\_basic**

Provides a user lookup service for the Apache server

### **mod\_ldap**

Provides core LDAP library stuff like LDAP directive awareness and can be used to implement and optimise connectivity to LDAP back ends

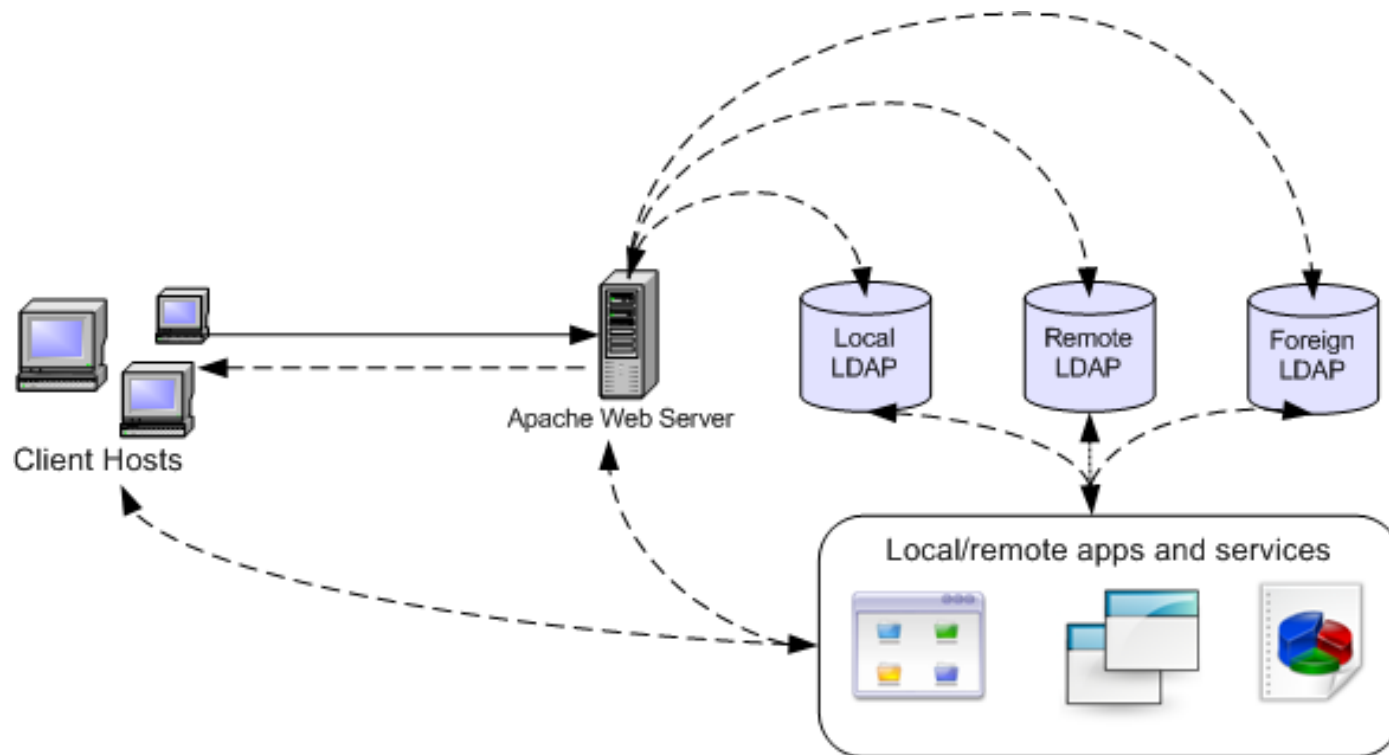
### **mod\_authnz\_ldap**

Provides LDAP authentication “and” authorisation services

### **mod\_authz\_host**

Provides authorisation and access control based on hostname, network address or host criteria

## Determining what's expected ...



To consider when configuring Apache for LDAP access:

- Directory access
  - Redundant or pooled LDAP servers
  - Non-secure or secure communication (mod\_ssl)
- Object and attribute rights
  - Anonymous access using the eDir [Public] object rights
  - Anonymous access using AD or AD LDS configurations
  - Authenticated proxy user configurations
- Optimising performance and security
  - Directory server indexing
  - LDAP search filters and policies
  - Result cache TTL settings

### eDirectory directive example

#### **Provided by mod\_ldap:**

```
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/certs/darkvixen160.crt  
LDAPTrustedMode SSL  
LDAPCacheTTL 300  
LDAPOpCacheTTL 300
```

#### **Provided by mod\_authnz\_ldap:**

```
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub"
```

- \*\* Multiple LDAP servers can be used in the "AuthLDAPUrl" directive
- \*\* LDAP cache instances are specific to each AuthLDAPUrl directives

### Active Directory directive example

#### **Provided by mod\_ldap:**

```
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/certs/darkvixen160.crt  
LDAPTrustedMode SSL  
LDAPCacheTTL 300  
LDAPOpCacheTTL 300
```

#### **Provided by mod\_authnz\_ldap:**

```
AuthLDAPUrl "ldaps://192.168.2.160/DC=dvc,DC=darkvixen,DC=com?cn?sub"
```

You should always verify your configuration:

**`/var/log/apache2/error_log`**

```
LDAPTrustedGlobalCert CA_DER /etc/apache2/certs/darkvixen160_ldap_ssl.der  
LDAPTrustedMode TLS
```

```
[info] APR LDAP: Built with OpenLDAP LDAP SDK
```

```
[info] LDAP: SSL support unavailable: LDAP: The OpenLDAP SDK only understands the  
PEM (BASE64) file type.
```

**or:**

```
LDAPTrustedGlobalCert CA_BASE_64 /etc/apache2/certs/darkvixen160_ldap_ssl.crt  
LDAPTrustedMode SSL
```

```
[info] APR LDAP: Built with OpenLDAP LDAP SDK
```

```
[info] LDAP: SSL support available
```



You should always verify your configuration:

DSTRACE using iMonitor

```
LDAP: New TLS connection 0x9d8855e0 from 192.168.2.163:50366, monitor = 0x17b,  
index = 2  
LDAP: Monitor 0x17b initiating TLS handshake on connection 0x9d8855e0  
LDAP: DoTLShandshake on connection 0x9d8855e0  
LDAP: Completed TLS handshake on connection 0x9d8855e0
```

You should always verify your configuration:

Using “ldapsearch”

```
LDAPTLS_CACERT=/etc/apache2/certs/darkvixen160_ldap_ssl.crt ldapsearch -ZZ -H  
ldap://192.168.2.160 -b "dc=dvc,dc=darkvixen,dc=com" "sAMAccountName=ldaptest" -x  
-D "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com" -W
```

LDAPTLS\_CACERT= Used to override any certificate specified in the ldap.conf file

\*\* TLS\_CACERT directive may be required in the /etc/openldap/ldap.conf

### Apache HTTP service considerations:

#### Credential submission

Clients are authorised for credential submission

Credentials will be accepted by the Apache server securely

#### Content delivery

Server security requirements (SSLCipherSuite)

Content security requirements (SSLRequire)

How will that security be enforced (mod\_rewrite)

You should always verify your configuration:

Be sure an HTTPS connection is established before sending credentials:

**Prompted for credentials:**

```
Darkvixen163:~ # netstat -atn | grep :443
```

```
tcp    0    0 0.0.0.0:443      0.0.0.0:*        LISTEN
```

**Prompted for credentials:**

```
darkvixen163:~ # netstat -atn | grep ":443"
```

```
tcp    0    0 0.0.0.0:443      0.0.0.0:*        LISTEN
```

```
tcp    0    0 192.168.2.163:443  192.168.2.18:1255  ESTABLISHED
```

or:

**Prompted for credentials:**

```
C:\Users\Administrator>netstat -atn | find ":443"
```

```
tcp    0.0.0.0:443      0.0.0.0:0        LISTENING
```

```
tcp    192.168.2.163:443  192.168.2.18:49823  ESTABLISHED
```

## Standard configuration example

```
AuthType Basic                                (mod_auth_basic)
AuthName "DarkVixen protected content"
AuthBasicProvider ldap
AuthzLDAPAuthoritative On
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub" (mod_authnz_ldap)
Require valid-user                            (core)
```

\*\* Using the “ldap” authentication provider invokes “mod\_authnz\_ldap”

\*\* AuthzLDAPAuthoritative defaults to on, but is included to bring its use to your attention, we’ll discuss it.

The configuration file used: ldap-user.conf

```
AuthType Basic
AuthName "DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub"
Require ldap-attribute objectClass=inetOrgperson
```

\*\* Reduces module and library interoperation

## The configuration file used: ldap-user.conf

```
AuthType Basic
AuthName "DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldap://192.168.2.160/DC=dvc,DC=darkvixen,DC=com?cn?sub" STARTTLS
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
AuthLDAPBindPassword "Windows2008"
Require ldap-attribute objectClass=Person
```

- \*\* Anonymous connections to AD, ADAM or AD LDS are not permitted by default
- \*\* **startTLS** commands are supported for Windows 2003 and better

 However, there is a problem. It doesn't really work ...

The search operation fails and Apache tells you so, sort of

## **Server error!**

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there was an error in a CGI script.

If you think this is a server error, please contact the [webmaster](#).

## **Error 500**

The cause for the error is rooted in how mod\_ldap and openLDAP handle LDAP referrals



### **openLDAP:**

Libraries don't support referral and rebind when simple binds are used (referral chasing)

Considered a security feature that prevents plain text credentials from being sent to multiple sources by automated referrals

Other bind types may support referral chasing

### **mod\_ldap:**

Does not support referral chasing for simple binds

If we can prevent referrals from being sent

```
AuthType Basic
AuthName "DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldap://192.168.2.160/CN=Users,DC=dvc,DC=darkvixen,DC=com?cn?sub" STARTTLS
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
AuthLDAPBindPassword "Windows2008"
Require ldap-attribute objectClass=Person
```

- ✔ Setting your search base below the domain root helps, sort of ...

So, who referred you ?

**LDAP Server:** LDAP Server - DARKVIXEN160.SERVERS.SVS.DVC

General  
 Information | Connections | Searches | Events | Tracing | Referrals

**Default Referral URL**

e.g. ldap://ldap.itd.umich.edu:389

**Conditions Which Return Default Referral**

A base DN is on an unavailable server  
 A base DN does not exist  
 A search entry is on an unavailable server

**Referral Options**

For eDirectory Searches:

For Other eDirectory Operations:

Secure chain

**Multi-valued String Editor**

Attribute: subRefs

Value to add:

Add

Values:

CN=Configuration,DC=dvc,DC=darkvixen,DC=com  
 DC=DomainDnsZones,DC=dvc,DC=darkvixen,DC=c  
 DC=ForestDnsZones,DC=dvc,DC=darkvixen,DC=co

Remove

OK Cancel

## Active Directory referrals:

The screenshot shows the Softerra LDAP Browser 4.5 interface. The left pane displays the directory tree for 'DARKVIXEN160 (AD)'. The main pane shows a list of objects with columns for Name, Value, and Type. Three entries are highlighted with red boxes:

Name	Value	Type
Idaps://ForestDnsZones.dvc.darkvixen.com:636	DC=ForestDnsZones,DC=dvc,DC=darkvix...	LDAP Referral
Idaps://DomainDnsZones.dvc.darkvixen.com:636	DC=DomainDnsZones,DC=dvc,DC=darkvix...	LDAP Referral
Idaps://dvc.darkvixen.com:636	CN=Configuration,DC=dvc,DC=darkvixen,...	LDAP Referral

The Output pane at the bottom shows several error messages, with two highlighted in red boxes:

- The host name 'ForestDnsZones.dvc.darkvixen.com' could not be resolved to its address.
- The host name 'DomainDnsZones.dvc.darkvixen.com' could not be resolved to its address.

## Active Directory referrals:

### Using ldapsearch

```
# search result  
search: 3  
result: 0 Success
```

```
# numResponses: 5  
# numEntries: 1  
# numReferences: 3
```

```
# search reference  
ref: ldap://ForestDnsZones.dvc.darkvixen.com/DC=ForestDnsZones,DC=dvc,DC=darkvixen,DC=com  
ref: ldap://DomainDnsZones.dvc.darkvixen.com/DC=DomainDnsZones,DC=dvc,DC=darkvixen,DC=com  
ref: ldap://dvc.darkvixen.com/CN=Configuration,DC=dvc,DC=darkvixen,DC=com
```

With Apache, the end result is still ...

## Server error!

The server encountered an internal error and was unable to complete your request. Either the server is overloaded or there was an error in a CGI script.

If you think this is a server error, please contact the [webmaster](#).

## Error 500

## Managing referrals with Active Directory for Domain Services (AD DS)

### **Less practical:**

- Produce a search that results in the return of a single entry
- Locate all target entries in a specific branch of the directory tree
- Disable referrals for openLDAP on the Apache host

### **More realistic:**

- Implement `mod_authn_sasl` for Apache instances
- Implement Active Directory Lightweight Directory Services (AD LDS)
- Upgrade to Apache v2.4
- Utilise the Active Directory Global Catalog service

Managing referrals with Active Directory for Domain Services (AD DS)

Implement mod\_auth\_sasl for Apache instances

Determine SASL methods available at your LDAP service:

```
ldapsearch -H ldaps://192.168.2.160 -b "" -x -s base -LLL supportedSASLMechanisms
```

```
supportedSASLMechanisms: GSSAPI
```

```
supportedSASLMechanisms: GSS-SPNEGO
```

```
supportedSASLMechanisms: EXTERNAL
```

```
supportedSASLMechanisms: DIGEST-MD5
```



Managing referrals with Active Directory for Domain Services (AD DS)

Implement Active Directory Lightweight Directory Services (AD LDS)

*Formerly Active Directory Application Mode (ADAM)*

- LDAP directory compliant
- Domain services or domain controllers not required
- Multiple instances per server with independent schemas
- Independent of the AD DS information store
- AD LDS instances can share information store data

Managing referrals with Active Directory for Domain Services (AD DS)

Upgrade to Apache v2.4

New directives have been added for mod\_ldap

**LDAPReferrals** *On/Off*

On: Referral chasing is enabled and credentials are reused on re-bind operations to referred servers

Off: Referrals are ignored

**LDAPReferralHopLimit** *number*

## Managing referrals with Active Directory for Domain Services (AD DS)

### Utilise the Active Directory Global Catalog service

- LDAP friendly
  - Must be located on a domain controller
  - Offers an aggregate view of entries in a multiple domain forest
  - Contains a subset of entries and attributes
  - Offer secure and non-secure ports (3268 and 3269)
- \*\* Local and domain groups are not replicated to the Global Catalog
- \*\* Some attributes may need to be added to the Global Catalog

## Back to the configuration files ldap-user.conf

```
AuthType Basic
AuthName "DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldap://192.168.2.160:3268/DC=dvc,DC=darkvixen,DC=com?cn?sub" STARTTLS
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
AuthLDAPBindPassword "Windows2008"
Require ldap-attribute objectClass=Person
```



No referrals are returned and the LDAP search is successful

## The configuration file used: ldap-group.conf

```
AuthType Basic
AuthName "More DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub?((objectClass=inetOrgPerson)(objectClass=groupOfNames))"
AuthLDAPBindDN "cn=APACHE,ou=PROXIES,o=CORP"
AuthLDAPBindPassword "novell"
Require ldap-group cn=IS_G,ou=IS,ou=INFOTECH,o=DVC
```

\*\* Filtering the object classes you search against improves LDAP service efficiency

## The configuration file used: ldap-group.conf

```
AuthType Basic
AuthName "More DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160:3269/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub?
(|(objectClass=person)(objectClass=group))"
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
AuthLDAPBindPassword "Windows2008"
Require ldap-group CN=IS_G,OU=IS,OU=INFOTECH,DC=dvc,DC=darkvixen,DC=com
```

\*\* sAMAccountName or userprincipalName are often better choices to search against

\*\* Local and domain groups are not replicated to the Global Catalog, Universal groups are

## The configuration file used: ldap-filter.conf

```
AuthType Basic
AuthName "Even more DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub?(|(objectClass=inetOrgPerson)(objectClass=groupOfNames))"
AuthLDAPBindDN "cn=APACHE,ou=PROXIES,o=CORP"
AuthLDAPBindPassword "novell"
Require ldap-filter &(groupMembership=cn=FSA_G,ou=MCG,o=DVC)(employeeStatus=Active)
```

## The configuration files used: ldap-filter.conf

```
AuthType Basic
AuthName "Even more DarkVixen protected content"
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160:3269/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub?
(|(objectClass=person)(objectClass=group))"
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
AuthLDAPBindPassword "Windows2008"
Require ldap-filter &(memberof=CN=FSA_G,OU=MCG,DC=dvc,DC=darkvixen,DC=com)(employeeStatus=Active)
```

\*\* Custom attributes will need to be added to the Global Catalog if used



## Search cache visibility

## Turning on the ldap-status handler

```
<Location /ldap-status>
```

```
    SetHandler ldap-status
```

```
    Order deny,allow
```

```
    Deny from all
```

```
    Allow from localhost 127.0.0.1 192.168.2
```

```
</Location>
```

Cache Name	Entries	Avg. Chain Len.	Hits	Ins/Rem	Purges	Avg Purge Time
<a href="#">LDAP URL Cache</a>	1 (0% full)	1.0	0/1	0%	1/0 (none)	0ms
<a href="#">ldap://darkvixen160win.dvc.darkvixen.com:3268/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub (Searches)</a>	0 (0% full)	0.0	0/1	0%	0/0 (none)	0ms
<a href="#">ldap://darkvixen160win.dvc.darkvixen.com:3268/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub (Compares)</a>	0 (0% full)	0.0	0/0	100%	0/0 (none)	0ms
<a href="#">ldap://darkvixen160win.dvc.darkvixen.com:3268/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub (DNCompares)</a>	0 (0% full)	0.0	0/0	100%	0/0 (none)	0ms

As always, the Apache documentation

**<http://httpd.apache.org>**

For and SSL certificate tools and troubleshooting

**<http://www.sslshopper.com>**

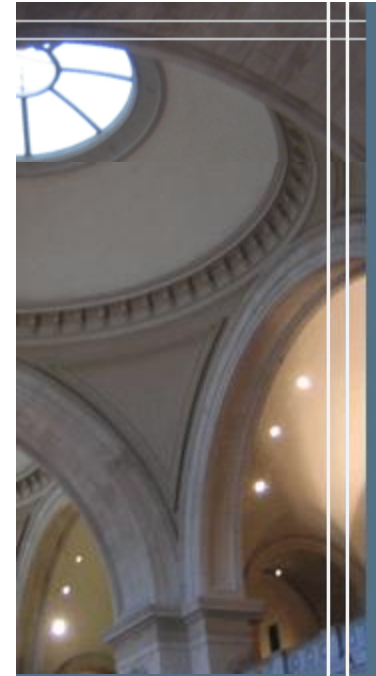
For troubleshooting and explaining LDAP service responses and error codes

**<http://ldapwiki.willeke.com>**

Full, commented conf file examples can be acquired from me, if you ask

**[lawrence.kearney@earthlink.net](mailto:lawrence.kearney@earthlink.net)**

# Question and Answer



Thank you for your attendance