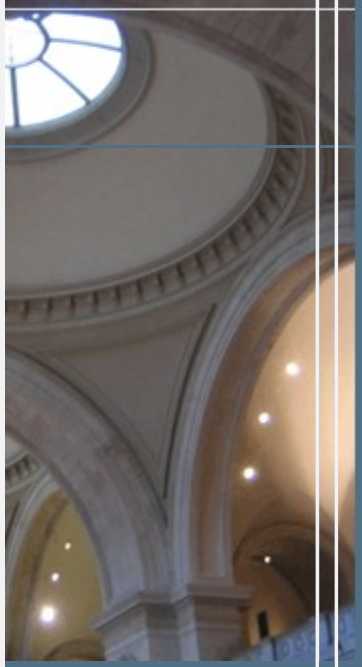


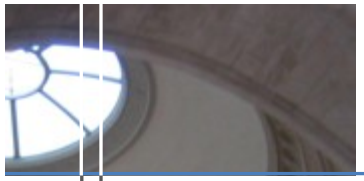
Technology Transfer Partners

Apache LDAP Configuration

using Novell Edirectory® and Microsoft Active Directory® for the Neanderthal

Lawrence Kearney
Advisory Board Member and Representative
for Higher Education in the Americas

lawrence.kearney@earthlink.net
http://www.lawrencekearney.com



Proposed Agenda

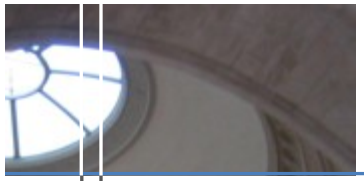
Apache “Neanderthal “ identification and socialisation

Apache deployment models

LDAP deployment models

Clients and identity store communication

Best practise tips for large environments



A Common Occurrence

Server Admin: “Can the users access the web page”

Web Content Admin: “They are prompted to login”

Server Admin: “Are the user logins successful”

Web Content Admin: “Yes, but the page isn't served”

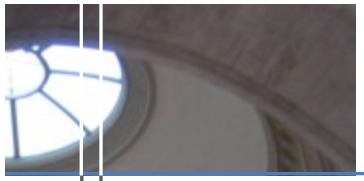
500 Internal Server Error

Sorry, something went wrong.

A team of highly trained monkeys has been dispatched to deal with this situation.

If you see them, show them this information:

```
Icwv71bPUtoDgK_T9k9nrDj6YgkIttJtqvVTS84dtVUbHOtVbPoSJyuBJX94
T0Z9jII4Yfk3R0k4eJBmfusikcSemgFjqdmsj1tVsGYgLC0StDIyTRYRug6q
D8h3PZYgkcyVy-xZ_1hPi9-JbBPJrHzSWBEEJPY6ftkqtELPJqDhRQhhahHk
NmQ9F-J61ypca3TJO8PPTPVGelMslLr4MpFJSDS5P86IjdC2F9xeOS1z3CP5
4o7xUENwE6hnvKgPs8IBc8v-_3CjeUbos32gJ8q6sBK_GooKJZvZk6Zc0bwf
dy2aCs1VLpUisKE7XRzPpDe8MMpD2k-SdYricsTbbdsAPEsnUVSoLuE97Hxb
kSLyezrz1EHGdv_8Szr7e9LDxgV3T8Xhh_RJR88J5_22-pHH6pG1zkxn8vV8
x2h7S-JIsycbqc6HQHlHZdeeI1HNI4-Bfp3NQsoNidaDsuXtZtIkO9dIijFs
TJPhjhZmTqNtiHUt-NYepG-TMnsLc1rGVa8VnymdXqSDZb3sukysM53zwzjj
nzgdjwctPMWyNt_xJymvfJpHbcjGjuUg_qhBqEZoIQLRZw5G4Cmf5QM-Bq76
HxFf3nzYHPWb425VNv6Vaq_IB7bm1292_RVrb3gJ6NWNom9UZCkooiVt9k2n
```



The real issue ?

The page isn't there

The credentials are incorrect

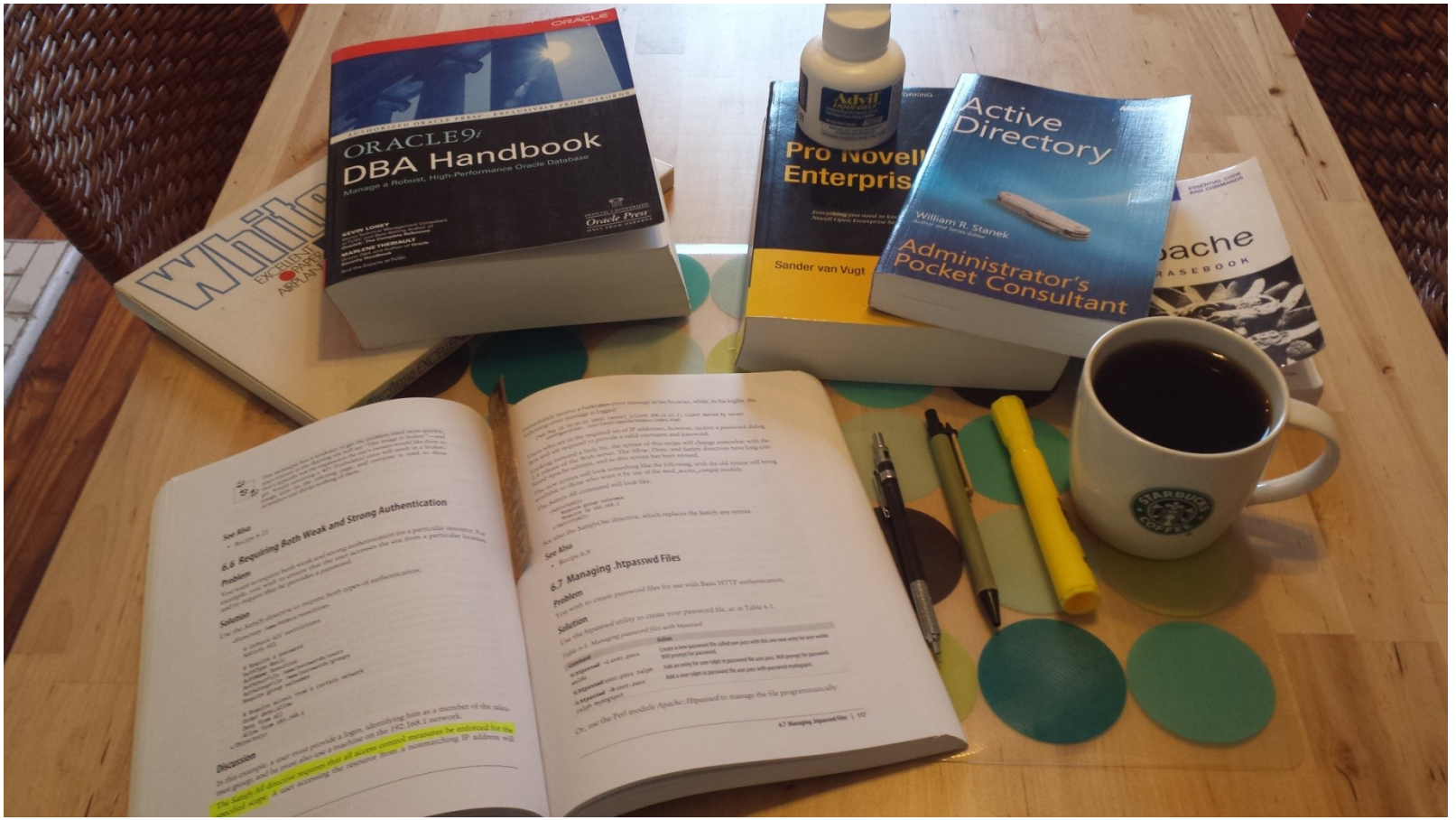
The application won't accept the credentials

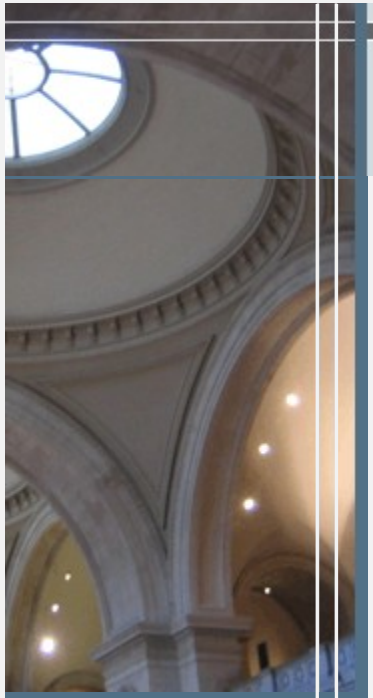
The user shouldn't be able to access the page

The LDAP configuration is incorrect

The LDAP service is experiencing issues

Someone ends up doing this …





Server Stuff We Should Know

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

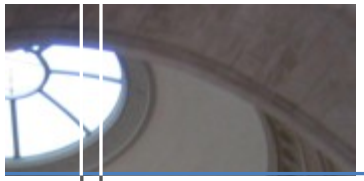
Base modules

“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
```



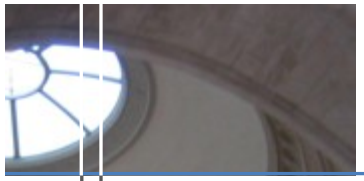
Loaded modules

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
```



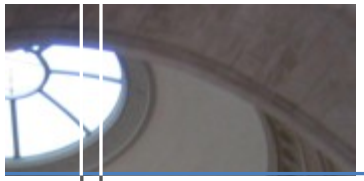
Listing, enabling and disabling modules

a2enmod –l

a2enmod **<module_package_name>**

a2dismod **<module_package_name>**

For example: a2enmod **ldap**



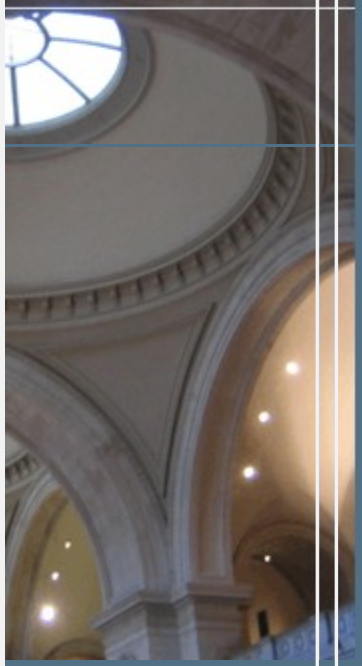
Tips …

Use a modular approach to web server configuration

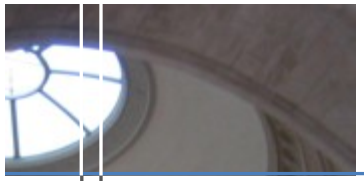
Document authentication workflows

Seek support from peers and experts

Do draw on their professional and personal empathy □



Concepts and Design Matter



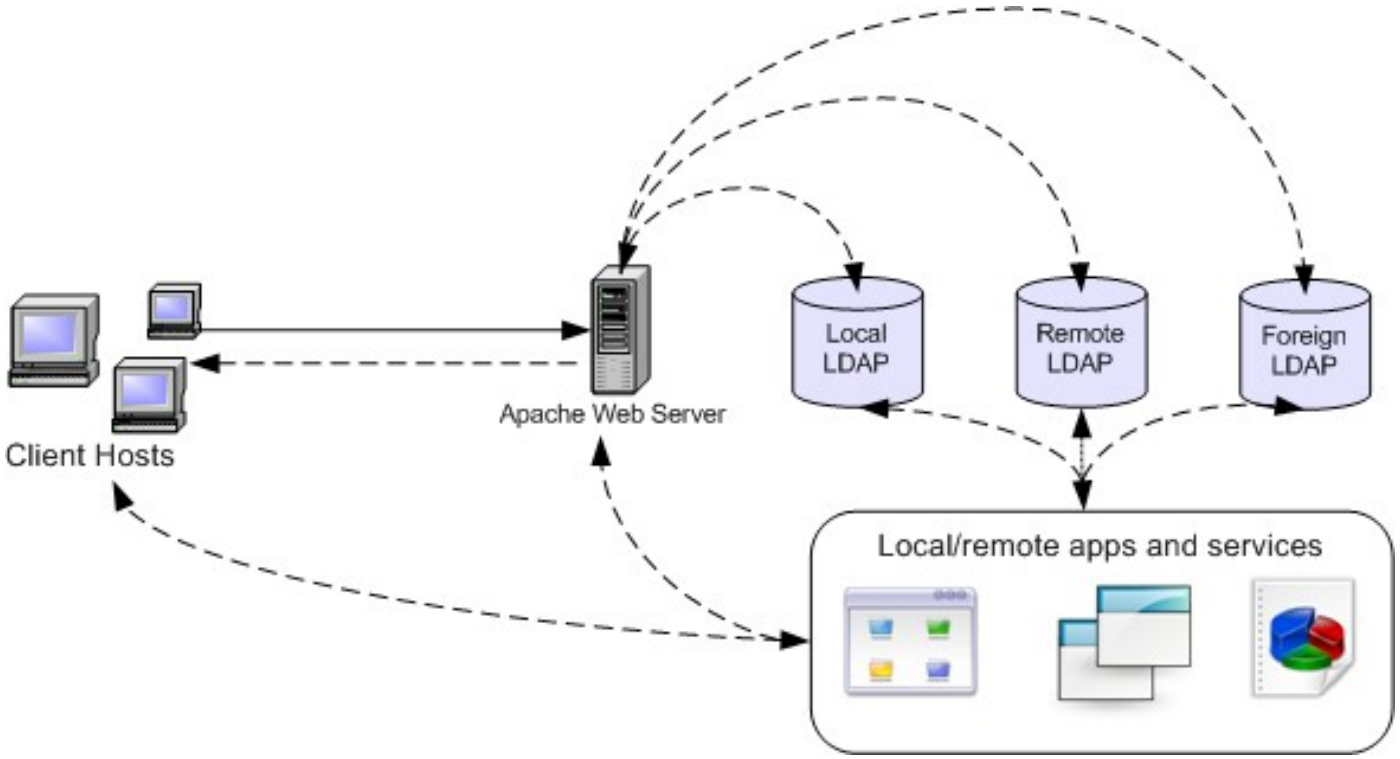
Identity based access benefits from standards

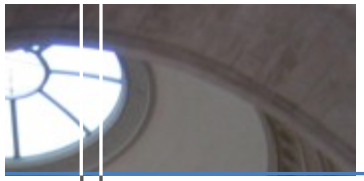
Real time data

Performance

Security

Determining what's expected …



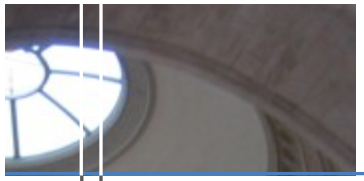


We do so with **credentials**, electronically

Identity credentials

Identity credentials + directory data

Identity credentials + directory data + host data

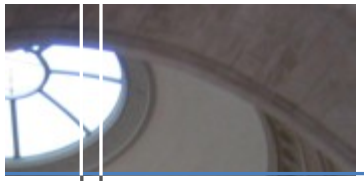


In Apache module “ease”:

mod_auth_basic

mod_auth_basic + (mod_ldap/mod_authnz_ldap)

mod_auth_basic + (mod_authnz_ldap) + mod_authz_host

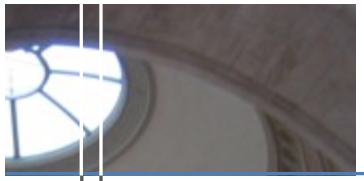


mod_auth_basic: Provides a user lookup service for Apache

mod_ldap: Provides core LDAP library, LDAP aware directive stuff and LDAP back end management

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



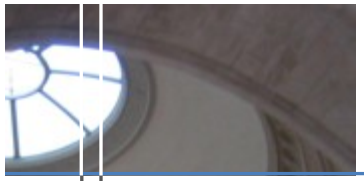
When configuring Apache for LDAP access:

Directory access

- Redundant or pooled LDAP servers
- Non-secure or secure communication (mod_ssl)

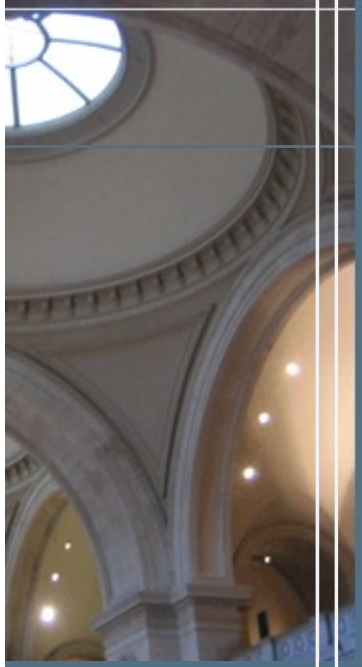
Object and attribute rights

- 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



Securing HTTP

Apache HTTP service considerations:

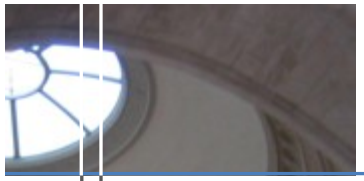
Credential submission

Clients are authorised for credential submission

Credentials will be accepted securely

Content delivery

Server security requirements	(SSLCipherSuite directives)
Content security requirements	(SSLRequire directives)
How will that security be enforced	(mod_rewrite directives)



Be sure an HTTPS connection is established before sending credentials:

Ready for credentials:

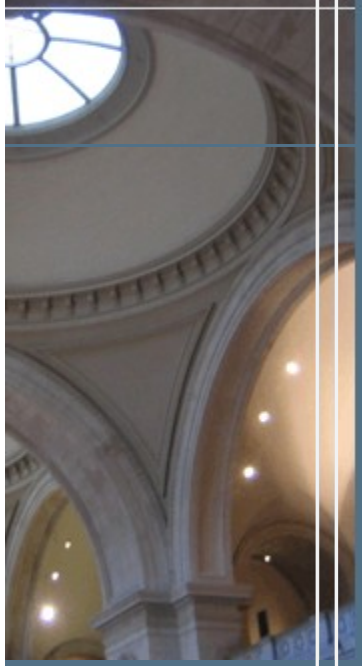
```
darkvixen163:~ # netstat -atn | grep :443
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
```

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
```

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
```



Configuring LDAP

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“

Always verify your configuration:

Using the following directives:

LDAPTrustedGlobalCert CA_DER /etc/apache2/certs/**darkvixen160_ldap_ssl.der**
LDAPTrustedMode **SSL**

Checking the /var/log/apache2/error_log:

[info] APR LDAP: Built with OpenLDAP LDAP SDK
[info] LDAP: **SSL support unavailable: LDAP:** The OpenLDAP SDK only understands the PEM (BASE64) file type

Using the following directives:

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

Checking the /var/log/apache2/error_log:

[info] APR LDAP: Built with OpenLDAP LDAP SDK
[info] **LDAP: SSL support available**

Always verify your configuration:

DSTRACE using iMonitor

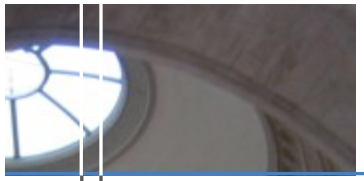
LDAP: **New TLS connection 0x9d8855e0 from 192.168.2.163:50366**
LDAP: Monitor 0x17b initiating TLS handshake on connection 0x9d8855e0
LDAP: DoTLSHandshake on connection 0x9d8855e0
LDAP: **Completed TLS handshake on connection 0x9d8855e0**

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
```

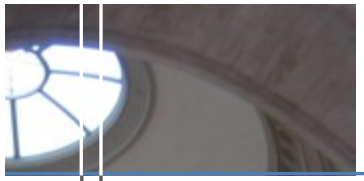
“**LDAPTLS_CACERT**=“ Used to override any certificate specified in the **ldap.conf** file



Why are there two configurations?

/etc/ldap.conf

/etc/openldap/ldap.conf

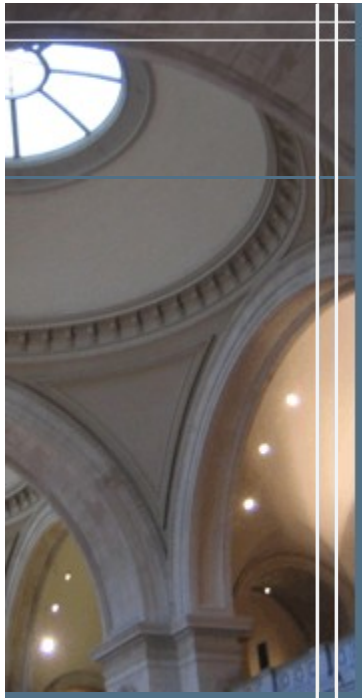


Standard configuration example

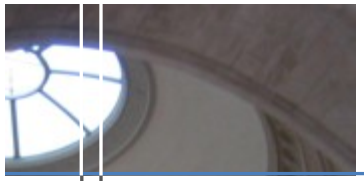
AuthType Basic (mod_auth_basic)
AuthName "DarkVixen protected content“
AuthBasicProvider **ldap**
AuthzLDAPAuthoritative On
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub“ (mod_authnz_ldap)
Require valid-user (core)

** 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.



More LDAP Configurations



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

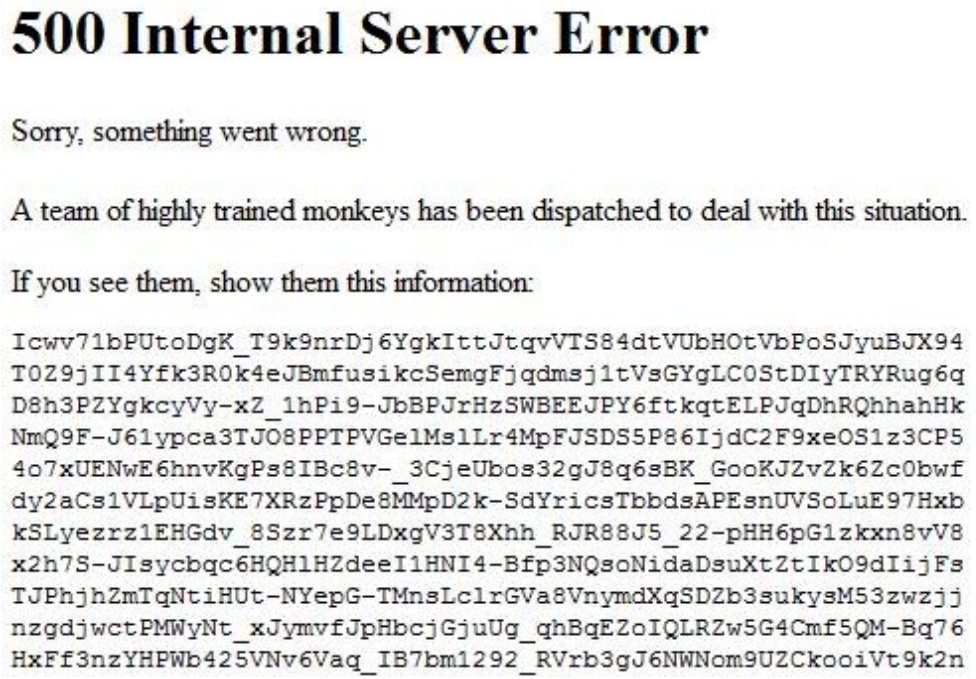
Configuration file used: ldap-user.conf

```
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



500 Internal Server Error

Sorry, something went wrong.

A team of highly trained monkeys has been dispatched to deal with this situation.

If you see them, show them this information:

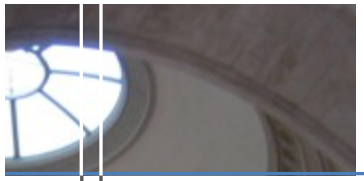
```
Icwv71bPUtoDgK_T9k9nrDj6YgkIttJtqvVTS84dtVUbHOtVbPoSJyuBJX94
T0Z9jII4Yfk3R0k4eJBmfusikcSemgFjqdmsj1tVsGYgLC0StDIyTRYRug6q
D8h3PZYgkcyVy-xZ_1hPi9-JbBPJrHzSWBEEJPY6ftkqtELPJqDhRQhhahHk
NmQ9F-J61ypca3TJO8PPTPVGelMslLr4MpFJSDS5P86IjdC2F9xeOS1z3CP5
4o7xUENwE6hnvKgPs8IBc8v-_3CjeUbos32gJ8q6sBK_GooKJZvZk6Zc0bwf
dy2aCs1VLpUisKE7XRzPpDe8MMpD2k-SdYricsTbbdsAPEsnUVSoLuE97Hxb
kSLyezrz1EHGdv_8Szr7e9LDxgV3T8Xhh_RJR88J5_22-pHH6pG1zkxn8vV8
x2h7S-JIsycbqc6HQHlHZdeeI1HNI4-Bfp3NQsoNidaDsuXtZtIkO9dIijFs
TJPhjhZmTqNtiHUt-NYepG-TMnsLclrGVa8VnymdXqSDZb3sukysM53zwzjj
nzgdjwctPMWyNt_xJymvfJpHbcjGjuUg_qhBqEZoIQLRZw5G4Cmf5QM-Bq76
HxFf3nzYHPWb425VNv6Vaq_IB7bm1292_RVrb3gJ6NWNom9UZCkooiVt9k2n
```

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

mod_ldap: Does not support referral chasing for simple binds

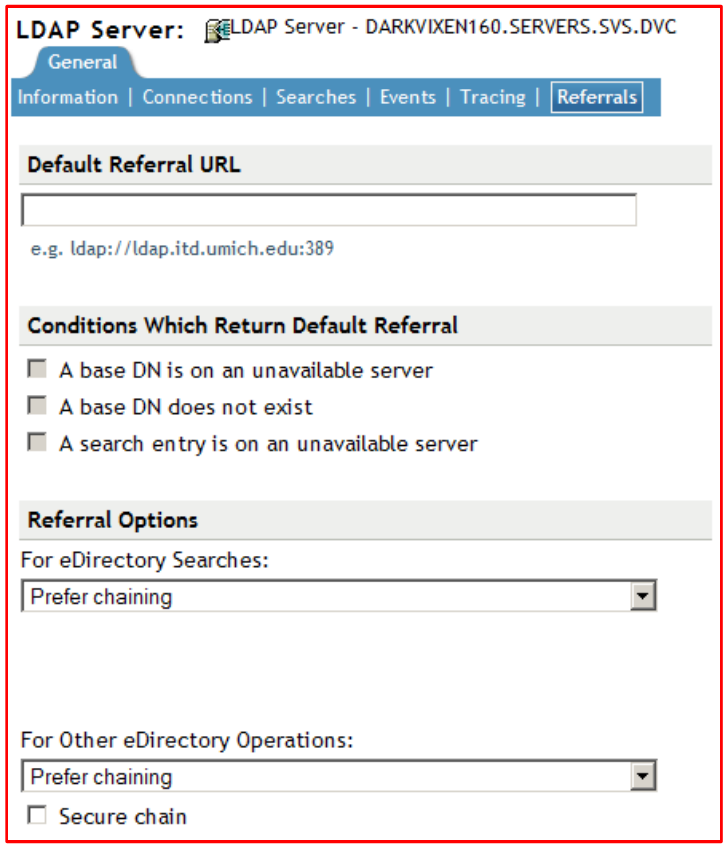


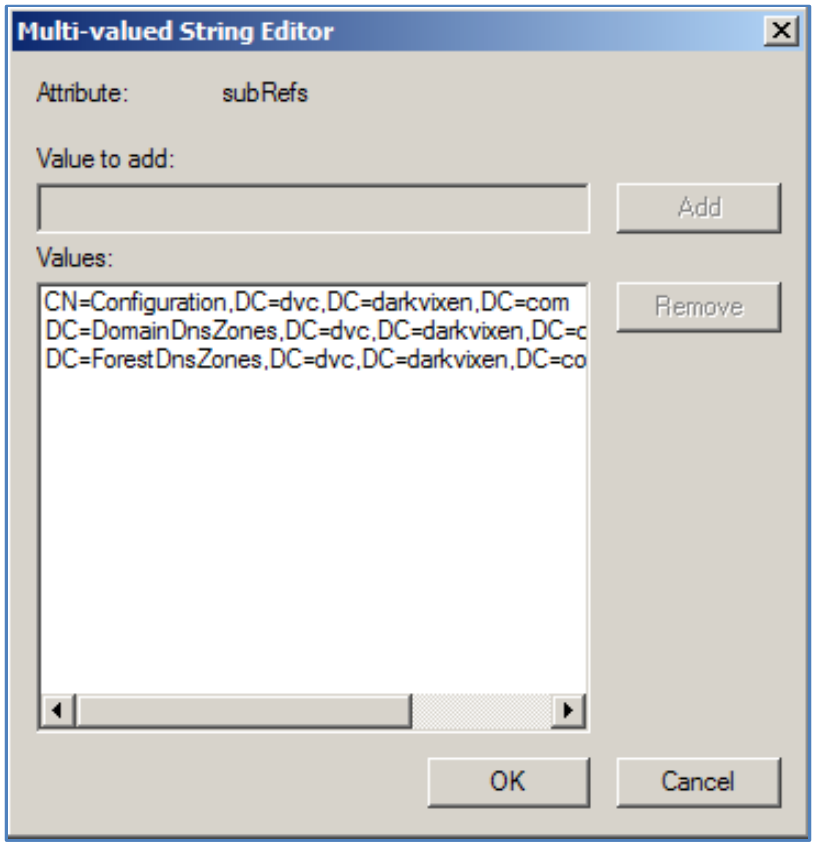
If we can prevent referrals from being sent

```
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
```

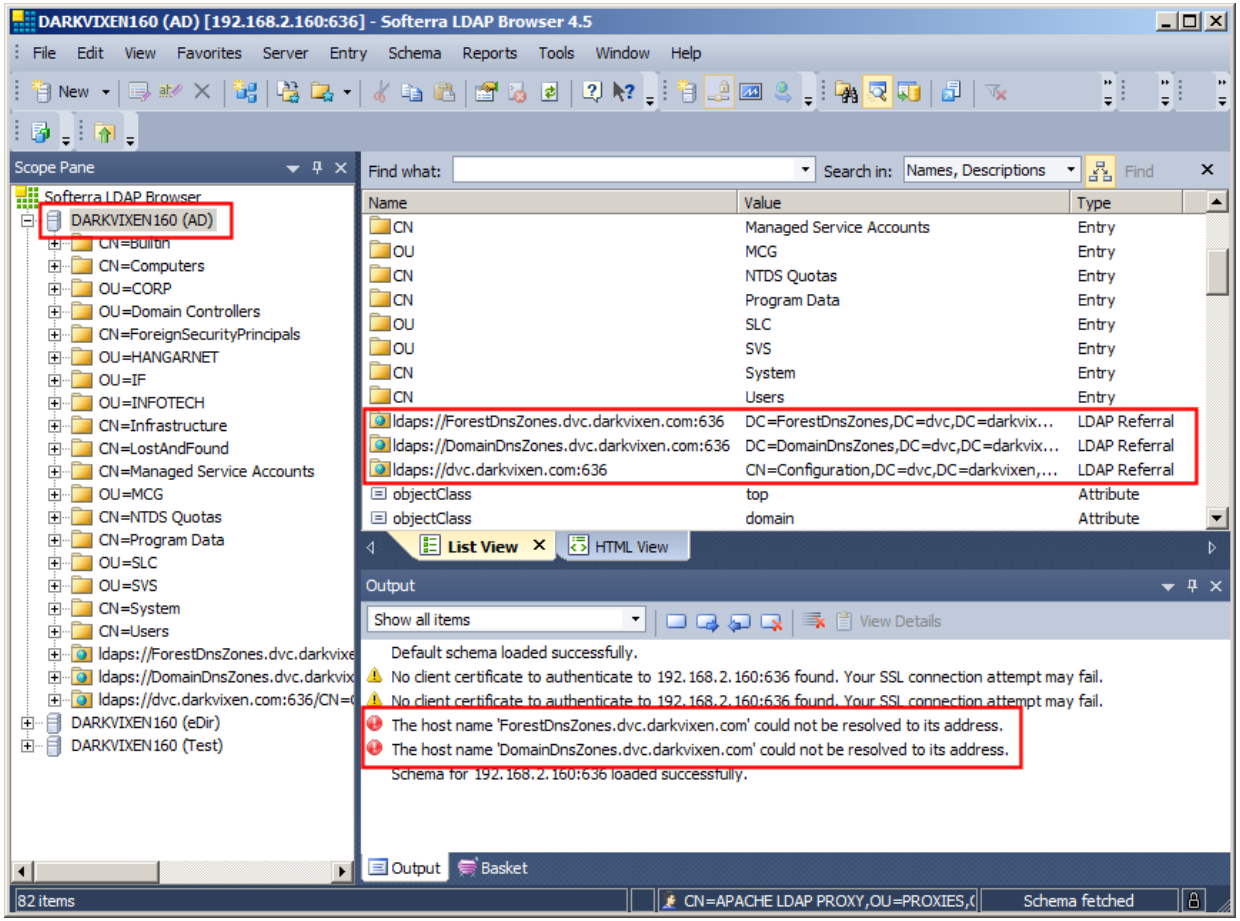
- Setting your search base below the domain root helps, sort of …

So, who referred you ?





Active Directory referrals:



Active Directory referrals:

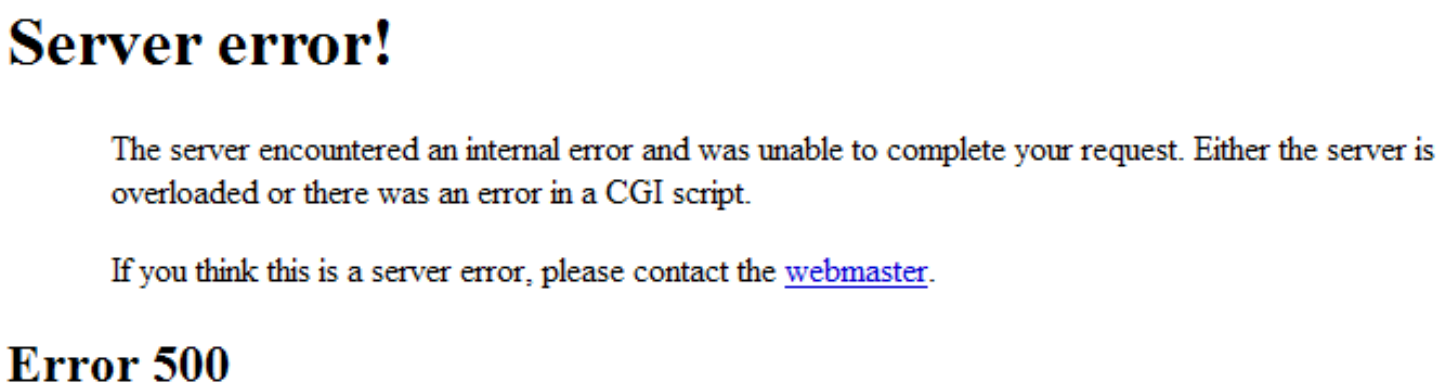
Using ldapsearch

```
# 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

With Apache, the end result is still …

500 Internal Server Error

Sorry, something went wrong.

A team of highly trained monkeys has been dispatched to deal with this situation.

If you see them, show them this information:

```
Icwv71bPUtoDgK_T9k9nrDj6YgkIttJtqvVTS84dtVUbHOtVbPoSJyuBJX94
T0Z9jII4Yfk3R0k4eJBmfusikcSemgFjqdmsj1tVsGYgLC0StDIyTRYRug6q
D8h3PZYgkcyVy-xZ_1hPi9-JbBPJrHzSWBEEJPY6ftkqtELPJqDhRQhhahHk
NmQ9F-J61ypca3TJO8PPTPVGelMslLr4MpFJSDS5P86IjdC2F9xeOS1z3CP5
4o7xUENwE6hnvKgPs8IBc8v-_3CjeUbos32gJ8q6sBK_GooKJZvZk6Zc0bwf
dy2aCs1VLpUisKE7XRzPpDe8MMpD2k-SdYricsTbbdsAPEsnUVSoLuE97Hxb
kSLyezrz1EHGdv_8Szr7e9LDxgV3T8Xhh_RJR88J5_22-pHH6pG1zkxn8vV8
x2h7S-JIsycbqc6HQHlHZdeeI1HNI4-Bfp3NQsoNidaDsuXtZtIkO9dIijFs
TJPhjhZmTqNtiHUt-NYepG-TMnsLclrGVa8VnymdXqSDZb3sukysM53zwzjj
nzgdjwctPMWyNt_xJymvfJpHbcjGjuUg_qhBqEZoIQLRZw5G4Cmf5QM-Bq76
HxFf3nzYHPWb425VNv6Vaq_IB7bm1292_RVrb3gJ6NWNom9UZCkooiVt9k2n
```

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_authn_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

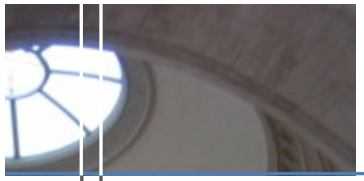
```
AuthType Basic
AuthName “More DarkVixen protected content“
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160:3269/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub?
(|(objectClass=person)(objectClass=group))"
AuthLDAPBindDN "CN=APACHE LDAP
PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"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

** sAMAccountName or userprincipleName 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

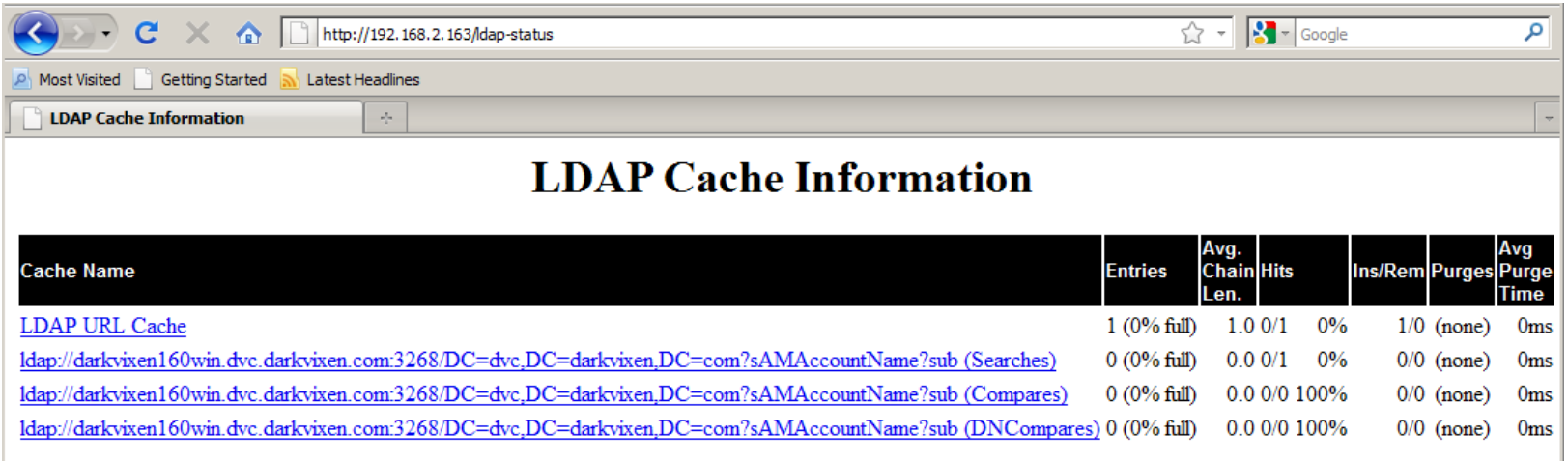
AuthType Basic
AuthName “Even more DarkVixen protected content“
AuthBasicProvider ldap
AuthLDAPUrl "ldaps://192.168.2.160:3269/DC=dvc,DC=darkvixen,DC=com?sAMAccountName?sub?(|(objectClass=person)(objectClass=group))"
AuthLDAPBindDN "CN=APACHE LDAP PROXY,OU=PROXIES,OU=CORP,DC=dvc,DC=darkvixen,DC=com"
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

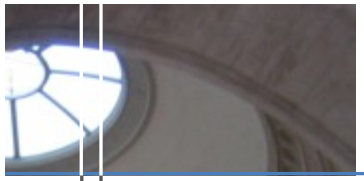
Turning on the ldap-status handler

```
<Location /ldap-status>
    SetHandler ldap-status
    Order deny,allow
    Deny from all
    Allow from localhost 127.0.0.1 192.168.2
</Location>
```



LDAP Cache Information

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



Additional info and tools

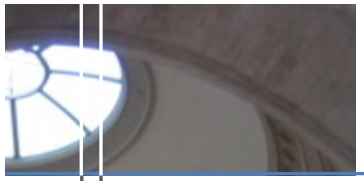
As always, the Apache documentation
http://httpd.apache.org

For and SSL certificate tools and troubleshooting
http://www.sslshopper.com

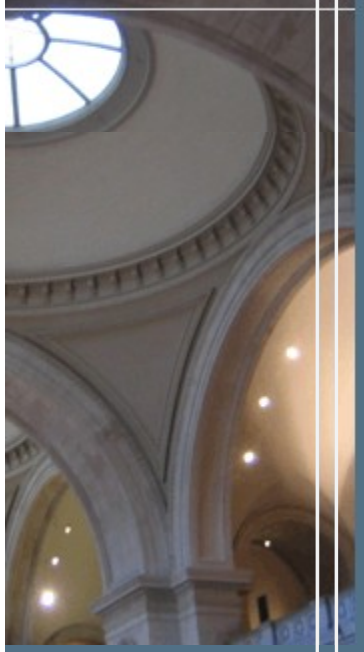
For troubleshooting and explaining LDAP service responses and error codes
http://ldapwiki.willeke.com

Full, commented conf file examples can be acquired from me, if you ask
lawrence.kearney@earthlink.net

Keynote, O'Reilly OpenSource Convention: **Identity 2.0**
Dick Hardt, Founder and CEO Sxip Identity
http://www.youtube.com/watch?v=RrpajcAgR1E



Question and Answer



Thank you for your attendance