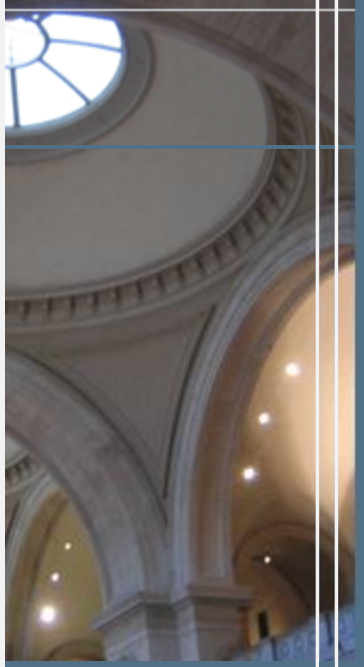
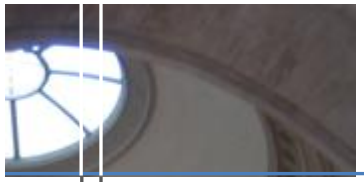


Apache authentication and authorization against eDir using LDAP for “Neanderthals”

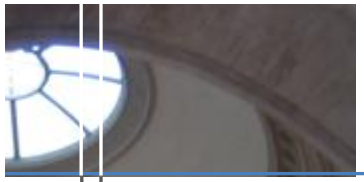
Lawrence Kearney
Enterprise and Workgroup Service Analyst
Georgia Health Sciences University

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



Session Agenda

- Apache “Neanderthal “ identification and socialization
- General discussion about Apache deployments and operations
- Tips and best practices for large and enterprise class environments
- Securing and optimizing Apache servers is a different discussion
- This discussion will focus on the basics of securing and optimizing 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

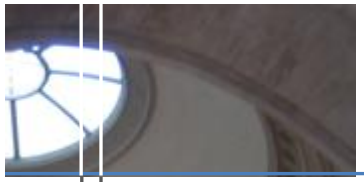
Base modules

“Hardwired” modules improve performance when:

- Hardware and operating system platforms are known
- Web server configuration scope is fixed

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
```



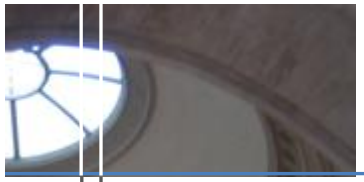
Loaded modules

Additional modules improve flexibility when:

- Hardware and operating system platforms vary
- Web server configuration scope is not fixed
- Server complexity may increase

Viewing the other that 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 other modules

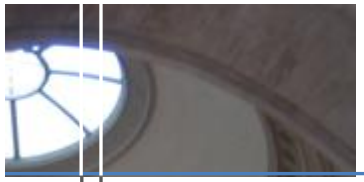
a2enmod -l
a2enmod <module_package_name>
a2dismod <module_package_name>

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

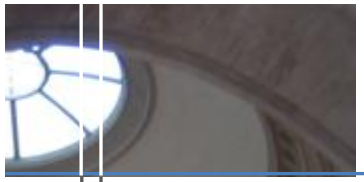
/etc/apache2/sysconfig.d/loadmodule.conf: the file Apache reads at startup to load them



Tips to begin with

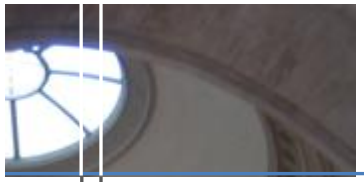
- Install and use the Apache manual
- Use a modular approach to web site and web server configuration
- Envision and document how you want your implementations to work in their planning stages
- Seek support from peers and experts when hurdles are encountered in planning and implementation phases

  (Do draw on their professional and personal empathy)



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

- Real time data expectations
- Performance expectations
- Security expectations

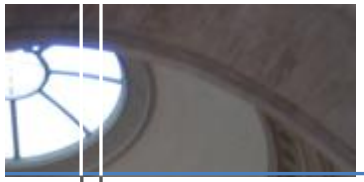


We do so with credentials, context and stuff, electronically

- 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

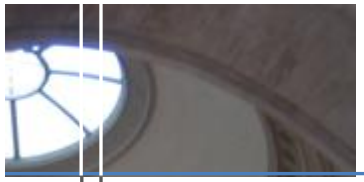


In Apache module ease:

- 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



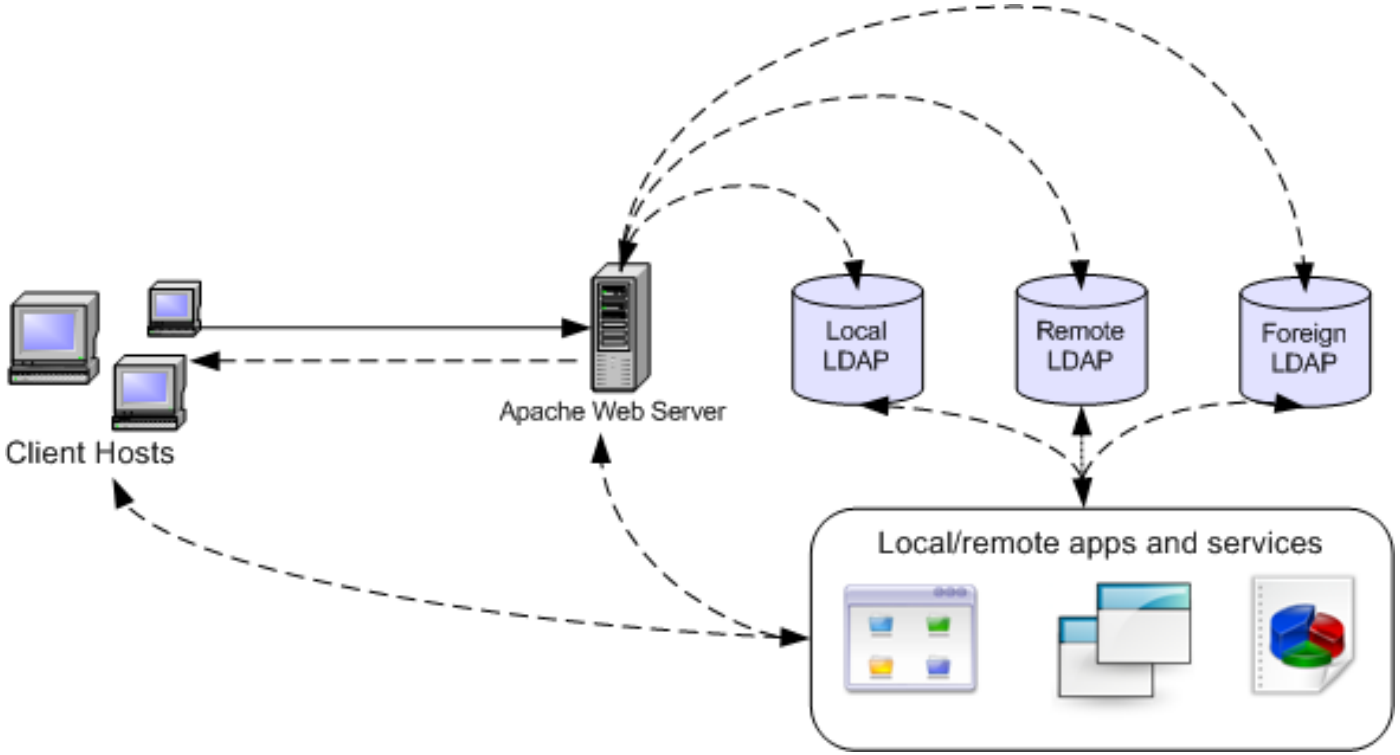
mod_auth_basic:
Provides a user lookup service for the Apache server

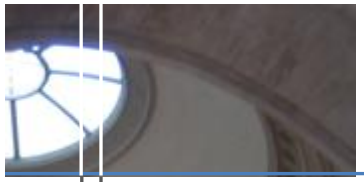
mod_ldap:
Provides core LDAP library stuff , LDAP directive awareness and can be used to optimize connectivity to LDAP back ends

mod_authnz_ldap:
Provides authentication “and” authorization services

mod_authz_host:
Provides authorization and access control based on hostname, network address or host criteria

Determining what's expected …

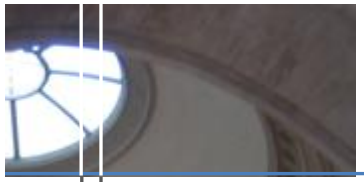




The order of things … LDAP access

To consider when configuring Apache for LDAP access:

- Directory access
  - Network address(es) of LDAP Servers
  - Non-secure or secure communication (mod_ssl)
- Object and attribute rights
  - Authenticated proxy user configuration
  - Unauthenticated anonymous access using the [Public] object
- Optimizing performance and security
  - Directory server indexing
  - LDAP search filters
  - Result cache TTL settings



The order of things … LDAPS access

Directive example

Provided by mod_ldap:

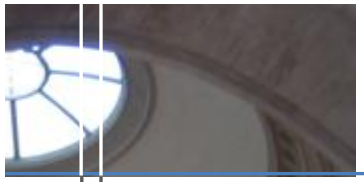
LDAPTrustedGlobalCert CA_BASE64 /etc/apache2/certs/darkvixen160.crt
LDAPTrustedMode **SSL**
LDAPOpCacheTTL 300

Provided by mod_authnz_ldap:

AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub“
AuthLDAPBindDN "cn=APACHE_LDAP_PROXY,ou=PROXIES,o=CORP“
AuthLDAPBindPassword "novell“

** Multiple LDAP servers can be used in the “AuthLDAPUrl” directive

For the suse platform:
Can be placed in the “default-server.conf” to apply globally



The order of things … LDAPS access

You should always verify your configuration:

/var/log/apache2/error_log

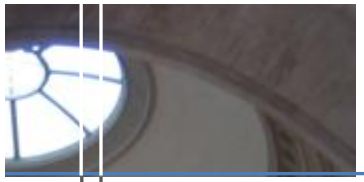
LDAPTrustedGlobalCert CA_DER /etc/apache2/certs/**darkvixen160_ldap_ssl.de**r
LDAPTrustedMode TLS

[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**

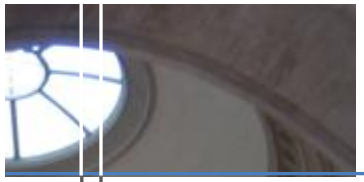


The order of things … LDAPS access

You should always verify your configuration:

DSTRACE using iMonitor

LDAP: New TLS connection 0x9d8855e0 from 192.168.2.122:50366, 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



The order of things … HTTP access

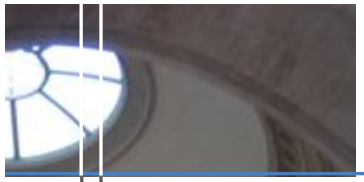
Apache HTTP service considerations:

Credential submission

- Credentials will be accepted by the Apache server (mod_ssl)
- Which clients are being evaluated for access
- How are clients being authorized for access

Content delivery

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



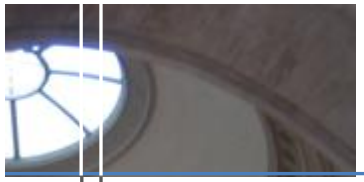
The order of things … HTTP access

Configuration of Apache HTTPS servers is a well documented process (we'll discuss and demonstrate an example if time allows)

Directive example

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

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



You should always verify your configuration:

Be sure an HTTPS connection is established before sending credentials:

Prompted for credentials:

```
darkvixen163:/etc/apache2/authnz # netstat -atn | grep :443
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
```

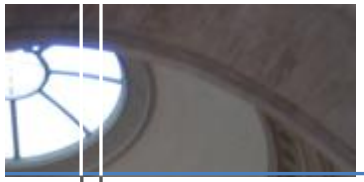
After giving credentials:

```
darkvixen163:/etc/apache2/authnz # 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       192.168.2.18:1119       ESTABLISHED
```

or:

Prompted for credentials:

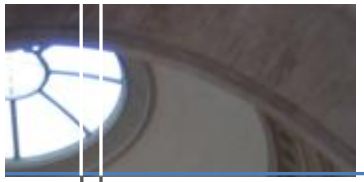
```
darkvixen163:/etc/apache2/conf.d # netstat -atn | grep :443
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp        0      0 192.168.2.163:443       192.168.2.18:1255       ESTABLISHED
```



The configuration files used: ldap-user.conf

```
AuthType Basic                                          (mod_auth_basic)
AuthName "DarkVixen protected content“
AuthBasicProvider ldap
AuthzLDAPAuthoritative On                               (mod_authnz_ldap)
AuthLDAPUrl "ldaps://192.168.2.160/o=dvc?cn?sub"
AuthLDAPBindDN "cn=APACHE,ou=PROXIES,o=CORP“
AuthLDAPBindPassword "novell“
Require ldap-attribute objectClass=inetOrgperson
```

** Using the “ldap” authentication provider invokes “mod_authnz_ldap”



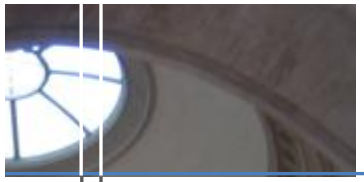
The configuration files used: ldap-group.conf

AuthType Basic (mod_auth_basic)
AuthName “More DarkVixen protected content“
AuthBasicProvider ldap
AuthzLDAPAuthoritative On (mod_authnz_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 you search against improves LDAP service efficiency



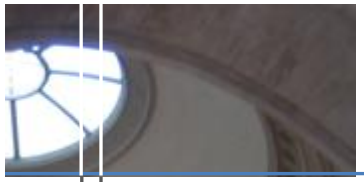
The configuration files used: ldap-filter.conf

AuthType Basic (mod_auth_basic)
AuthName “Even more DarkVixen protected content“
AuthBasicProvider ldap
AuthzLDAPAuthoritative On (mod_authnz_ldap)

AuthLDAPUrl
"ldaps://192.168.2.160/o=dvc?cn?sub?(|(objectClass=inetOrgPerson)(objectClass=group OfNames))“

AuthLDAPBindDN "cn=APACHE,ou=PROXIES,o=CORP“
AuthLDAPBindPassword "novell“

Require ldap-filter &(groupMembership=cn=FSA_G,ou=MCG,o=DVC)(employeeStatus=Active)



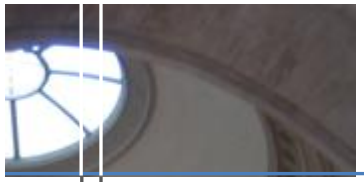
Additional info and tools

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

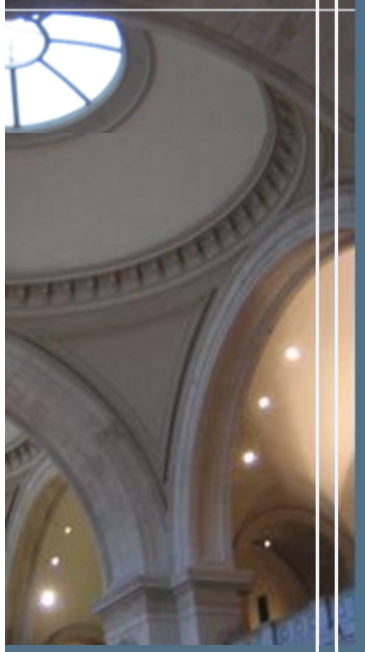
For and SSL certificate tools and troubleshooting
http://www.sslshopper.com

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



Question and Answer



Apache authentication and authorization against eDir using LDAP for “Neanderthals”

Thank you for your time and attendance