Apache LDAP Configuration
using Novell Edirectory® and Microsoft Active Directory®
for the Neanderthal

Lawrence Kearney
Advisor for Higher Education in the Americas
Technology Transfer Partners (TTP)
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”
Swing and a Miss

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_T9k9nrDj6YgkIttJtqvVTS84dtVUbH0tVbPoSJyUBjX94T0Z9jII4Yfk3R0k4eJBmfusikcSemgFjqdmsj1tVsGYgLCOStDIyTRYRug6qD8h3PZYgkcyVy-xZ_1hPi9-JbBPjrHzSWBEEJPy6ftqELPJqDhRQhhahHkNmQ9F-J61ypca3TJO8PPTVPVGe1Ms1Lr4MpfJSDS5P86IjdC2F9xeOS1z3CP5407xUENwE6hnvKgPs8IBc8v-_3CjeUbos32gJ8q6sBK_GooKJZvZk6Zc0bwfdy2aCs1VLPuISKE7XRzPpDE8MMpD2k-SdYricsTbbdsAPEsnUVSoLuE97Hxbk5LyezrzlEHGdv_8Szr7e9LDxgV3T8Xhh_RJR88J5_22-pHH6pG1zkn8vV8x2h7S-JIsycbqc6HQR1Hzdee1fHNI4-Bfp3NQsoNidaDsuXtZtIkO9dIljjFsTJPJh2mTqNTiHUt-NYepG-7MnsLclrGv8NymdXqsDZb3sukySM53zwjzjnzgdjwctPMWyNt_xJymvfJpHbcjGjuUg_qhBqEzoIQLRZw5G4Cmf5QM-Bq76HxFf3nzYHPWb425VNVv6Vaq_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
Another Common Occurrence

“Someone” ends up doing this ...
Chapter 1: Server Stuff We Should Know
Apache the Application

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
Speaking of Modules

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
Speaking of Modules

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_default authz_user authn_dbm autoindex cgi dir env expires include log_config mime negotiation setenvif ssl suexec userdir php5 mod_ldap mod_authnz_ldap ap rewrite
Speaking of Modules

Listing, enabling and disabling modules

Listing:  a2enmod -l
Enabling:  a2enmod <module_package_name>
Disabling:  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
Chapter 2: Concepts and Design Matter
Web Services in Our Day to Day

Identity based access benefits from standards

Real time data
Performance
Security
Understanding the Moving Parts

Determining what’s expected …
When We Say Who We Are ...

We do so with credentials, electronically

Identity credentials
Identity credentials + directory data
Identity credentials + directory data + host data
When We Say Who We Are ...

In Apache module “ease”:

mod_auth_basic
mod_auth_basic + (mod_ldap/mod_authnz_ldap)
mod_auth_basic + (mod_authnz_ldap) + mod_authz_host
LDAP Module Run Down

**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
The Order of Things

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
The Order of Things, Continued

Optimising performance and security

- Directory server indexing
- LDAP search filters and policies
- Result cache TTL settings
Chapter 3: Securing HTTP
HTTPS Access

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)
HTTPS Access

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
Chapter 4: Configuring LDAP
LDAP Access

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
LDAP Access

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"
LDAP Access

Always verify your configuration:

Using the following directives:

```bash
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
```
LDAP Access

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
LDAP Access

Always verify your configuration:

DSTRACE using Novell 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
LDAP Access

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
LDAP Access

Why are there two configurations?

/etc/ldap.conf
/etc/openldap/ldap.conf
Authenticating and Barely Authorising

Standard configuration example

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

** 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.
Chapter 5: More LDAP Configurations
Technical Demo Info

“Modular” server configuration

/etc

| __ ../apache2  (httpd.conf, default-server.conf)
| __ ../certs   (ldap and http certificates)
| __ ../conf.d  (sitex.conf, rewrite.conf, ssl.conf)
| __ ../authnz.d (ldapx.conf)

** Many allow directives for conf file “includes” by URL
Technical Example and Demo

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 inter operation
Technical Example and Demo

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 inter operation
Technical Example and Demo

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 ...
Technical Issue

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:

The cause for the error is rooted in how mod_ldap and openLDAP handle LDAP referrals
Technical Discussion

**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
Technical Discussion

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 ...
Technical Discussion

So, who referred you?
Technical Discussion

Active Directory referrals
Technical Discussion

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
Technical Discussion

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_T9k9nrDj6YgkIttJtqvVTS84dtVUbH0tVbPoSJyuBjXy94
TOZ9jII4Yfk3R0k4eJBMfusikcSemyGfjQdmajj1TsGYgLC0StDIyTRyRug6q
D8h3PZGykcyVv-xZ_1hPj9-JbBPJrHzSBEEJFY6ftkqtELFJqDhRQhahHk
NmQ9F-J61ypca3TJo8PPTPVGelMs1Lr4MpfJ5DS5P86IjdC2F9xe0S1z3CP5
407xUENwe6hnyKgPs8IBc8v__3CjeUbos32gJ8q6sBK_GooKJZv2k62C0bzwf
dy2aCslVLPui5KE7XRzPpDe8MMpD2k-SdYricsTbbdsAPEsnUVsOLuE97Hxb
kSLyezzr1EHGdv_8Szr7e9L9xvgV3T8Xh_LRo8J5_22-pHH6pG1zkxn8vV8
x2h75-JIsycbqc6HQH1HZdee11HNI4-Bfp3NQsoRidaDsuXtZtIk90i1jFs
TPJphjZmTqNtiHUt-NYepG-TMnsLclRGa8VnymdQxSD2b3sukysM53zwzjj
nzgjwctPWWyNt_xJymvfUpHbcjGjuUg_qhBqEzoIQLR2w5G4Cmf5QM-Bq76
HxfF3nzYHPWb425Vnv6Vaq_IB7bml392_RVrb3gJ6NWNom9UZCkoo1Vt9k2n
```
Technical Discussion

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
Technical Discussion

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
Technical Discussion

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
Technical Discussion

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*
Technical Discussion

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
Technical Example and Demo

Back to the configuration file 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
Technical Example and Demo

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=groupName))“
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
Technical Example and Demo

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
Technical Example and Demo

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)
Technical Example and Demo

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
Additional Info and Tools

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>
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.
Unpublished Work of SUSE. All Rights Reserved.
This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

General Disclaimer
This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.