Introdução ao LDAP via OpenLDAP

Alexandre Cavalcante Alencar
GNU/Linux and FOSS Specialist
COBIT, ITIL, Scrum, LPI, MCP
GNU/Linux User #260571 GNUPG 0x77EA9FF8
http://www.alexandrealencar.net
http://blog.alexandrealencar.net
http://www.alexandrealencar.com
http://www.servicosdeti.com.br
Fortaleza CE Brazil

O que são diretórios

- Serviços de diretórios são otimizados para leitura
- Modelo distribuído de armazenamento de informações
- Pode extender os tipos de informações armazenáveis
- Capacidade avançada de buscas
- Replicação sem perda
- Exemplo: Domain Name System (DNS)

Lightweight Directory Access Protocol

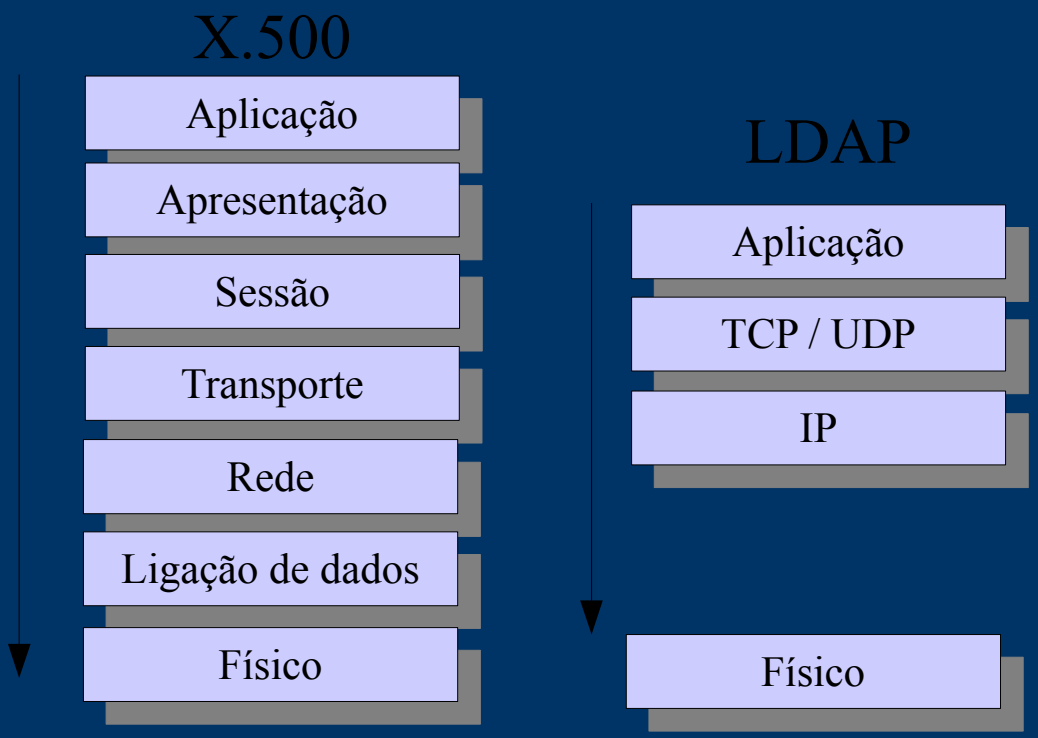
- Consolidação e centralização das informações
  - Credenciais, contatos, etc
- Acesso via diferentes aplicações
  - PAM, Postfix, Evolution, Firefox, Apache, etc
- Interoperabilidade* entre fornecedores
  - OpenLDAP.org, Active Directory, NDS, SunONE, etc
- Segurança e gerenciamento facilitados
  - Informações coerentes, atualizadas, replicação de informações para todos os sistemas com confiabilidade

O que é LDAP? (1)

- Lightweight
  - Comparado ao X.500 (Heavyweight) – Stack OSI
  - Apenas o overhead da camada TCP/IP
  - Pequeno conjunto de nove operações
- Directory
  - Otimizado para muita leitura e pouca escrita
  - LDAP é apenas um protocolo
- Access Protocol
  - Procotolo cliente/servidor baseado em mensagens

O que é LDAP? (2)

- Por quê o LDAP é considerado um protocolo de acesso a diretórios leve?



Modelos do LDAP

- Modelo Informacional
  - Estruturas e modelos de dados para criar o diretório
  - Definições de armazenamento, comparação, etc
- Modelo de Nomes
  - DIT, RDN, DN
- Modelo Funcional
  - Protocolo LDAP, operações (autenticação, leituras etc)
- Modelo de Segurança
  - Autenticação e autorização (controle de acesso)

LDIF

- LDAP Interchange Format – RFC2849
- Arquivo de texto plano
- Entradas separadas por linhas em branco
- Mapeamento de atributos e valores
- Diretivas de como o parser deve se comportar
- Importação de novos dados no diretório
- Backup do diretório
- Intercâmbio de dados

{Relative} Distinguised Names

- Uma DN armazena o caminho completo do objeto
- Uma RDN armazena o caminho relativo do objeto

DN: CN=Alexandre,DC=alexandrealencar,DC=com
CN: Alexandre
ObjectClass: person
OU: IT

O que é um atributo?

- Similar a variáves e seus tipos de dados
- Atributos são usados para armazenar valores
- Atributos podem conter múltiplos valores
- Informações de armazenamento e gerenciamento
- Sintaxe dos atributos – RFC's 2252 e 2256

Autenticação

- Codificação ({CRYPT},{MD5},{SHA},{SSHA})
- Mecanismos
  - Anonymous Authentication
    - DN com usuário e senha vazios
  - Simple Authentication
    - DN com usuário e senha em em texto plano
  - Simple Authentication over SSL/TLS
    - DN com usuário e senha em em texto plano sob SSL/TLS
  - Simple Authentication and Security Layer (SASL)
    - Negociação do mecanismo de autenticação e layer de segurança entre o cliente e servidor.
    - KRBv4, GSSAPI, S/Key, External, Digest-MD5

Diretórios Distribuídos

- Performance
  - Aplicações, grandes diretórios, deficiência em links
- Localização Geográfica
  - Partes do diretório são usadas apenas em uma região
- Descentralização da Administração
  - Delegação de controle

OpenLDAP

- POSIX Threads (Sistema Operacional/Biblioteca)
- Biblioteca SSL/TLS (OpenSSL)
- Biblioteca de banco de dados (Berkeley DB)
- SASL

OpenLDAP /etc/ldap/sladp.conf (1)

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema

schemacheck     on

pidfile         /var/run/slapd/slapd.pid

argsfile        /var/run/slapd.args

loglevel        0

modulepath      /usr/lib/ldap
moduleload      back_bdb

backend         bdb
checkpoint      512 30
```

OpenLDAP /etc/ldap/sladp.conf (2)

```
database        bdb
suffix          "dc=alexandrealencar,dc=com"
rootdn          "cn=Manager,dc=alexandrealencar,dc=com"
rootpw          {SSHA}QzZL1t9csWpSnwdgDPsK3h/XIYVSQ0ws

directory       "/var/lib/ldap"
mode            0600

index           objectClass                     eq
index           cn,uid                          pres,eq
index           uidNumber,gidNumber             eq

lastmod         on
cachesize       2000
replogfile      /var/lib/ldap/replog
```

OpenLDAP /etc/ldap/sladp.conf (3)

```
access to attrs=userPassword
        by dn="cn=Manager,dc=alexandrealencar,dc=com" write
        by anonymous auth
        by self write
        by * none

access to dn.base="" by * read

access to *
        by dn="cn=Manager,dc=alexandrealencar,dc=com" write
        by * read
```

Schemas

- *core.schema* – Base de qualquer diretório
- *inetorgperson.schema* – Informaçõões de contato
- *misc.schema* – Roteamento de correio no Sendmail
- *nis.schema* – Objetos de integração NIS + LDAP
- *openldap.schema* – Objetos do OpenLDAP
- *corba.schema* – Objetos CORBA RFC2714
- *cosine.schema* – COSINE e X.500 RFC1274
- *java.schema* – Objetos Java RFC2713

Access Control Lists (ACL's)

- Quem tem acesso ao quê?
  - * qualquer usuário conectado
  - *self* a DN do usuário atualmente conectado
  - *anonymous* usuários não autenticados
  - *users* conexões de usuários autenticados
  - *expressão regular* uma DN ou identidade SASL

Entradas Iniciais do Diretório (1)

```
# Name Space
dn: dc=alexandrealencar,dc=com
dc: alexandrealencar.com
objectClass: top
objectClass: domain

dn: ou=IT,dc=alexandrealencar,dc=com
ou: IT
objectClass: top
objectClass: organizationalUnit
```

Entradas Iniciais do Diretório (2)

dn: ou=Sales,dc=52ct,dc=eb,dc=mil,dc=br
ou: Sales
objectclass: organizationalUnit

dn: cn=Alexandre Alencar,ou=IT,dc=alexandrealencar,dc=com
cn: Alexandre Alencar
sn: Alencar
mail: alexandre@alexandrealencar.com
objectclass: inetOrgPerson

Entradas Iniciais do Diretório (3)

dn: cn=Sales Person,ou=Sales,dc=alexandrealencar,dc=com
cn: Sales Person
sn: Sales
telephoneNumber: +55 85 99953302
mobile: +55 85 99953302
mail: sales@alexandrealencar.com
labeledURI: http://www.alexandrealencar.com
objectclass: inetOrgPerson

Inserção dos Objetos Iniciais

- Para inserir os objetos iniciais:
  - /etc/init.d/slapd stop
  - slapadd -v -l 52ct.ldif
- Para iniciar o *daemon* do diretório:
  - /etc/init.d/slapd start
- Para pesquisar o diretório
  - ldapsearch -x -b “dc=alexandrealencar,dc=com” “objectClass=*”
- Explicações do *ldapsearch*
  - *-x* autenticação simples (não usar SASL)
  - *-b* base do diretório (onde iniciar a pesquisa)
  - *(objectClass)* filtro de busca (todos os tipos de objetos)

Operações via LDIF

- Executando mudanças nos objetos do diretório
  - *add* – Adiciona proprieadaes a um objeto
  - *delete* – Delete propriedades de um obejto
  - *modify* – Modifica propriedades de um objeto
  - *modrdn* – Modifica a RDN de um objeto
  - *moddn* – Modifica a DN de um objeto

```
dn: cn=Alexandre Alencar,ou=IT,dc=alexandrealencar,dc=com
changetype: modify
delete: mail
mail: alexandre@alexandrealencar.com
```

Ferramentas Gráficas

- GQ
  - Cliente GTK+, GPL, LDAPv3, SASL
- Java LDAP Browser/Editor
  - LDAPv2, LDAPv3, Multi-plataforma
- Softerra LDAP Browser
  - LDAPv2, LDAPv3, SSL (LDAPv3), Windows
- PHP LDAP Admin
  - Web, UID automático, i18n, 10 idiomas (pt-BR)

Replicação

- Implementar uma slave consistem em:
  - Parar o servidor *master*
  - Habilitar a replicação do *slapd.conf* do *master*
  - Copiar a base do *master* para o *slave*
  - Configurar o *slapd.conf* do *slave*
  - Iniciar o *daemon slapd* do *slave*
  - Iniciar o *daemon slapd* do *master*
  - Iniciar o *daemon slurpd* do *slave*

É sempre mais seguro exportar o diretório para um arquivo LDIF no servidor Master e importar este no Slave.

Replicação – Configurações Master

replica host=ldap2.alexandrealencar.com
suffix=”dc=alexandrealencar,dc=com”
binddn=”cn=replica,dc=alexandrealencar,dc=com”
credentials=ponha aqui uma senha bem estranha
bindmethod=simple
tls=yes

Replicação – Configurações Slave

- Exportando o diretório no servidor *master*
  - */etc/init.d/slapd stop*
  - *slapcat -b "dc=alexandrealencar,dc=com" -l dir.ldif*
- Importando o diretório no servidor *slave*
  - */etc/init.d/slapd stop*
  - *slapadd -l dir.ldif*

updatedn "cn=replica,dc=alexandrealencar,dc=com"

updateref ldap://ldap1.alexandrealencar.com

Autenticação do GNU/Linux (1)

- Propriedades necessárias nos objetos
  - posixAccount, shadowAccount
  - cn, uid
  - uidNumber,gidNumber,homeDirectory
  - userPassword,gecos,loginShell,description
- Relacionamento entre posixAccount e passwd

username:password:uid:gid:gecos:home:shell

uid:userPassword:uidNumber:gidNumber:gecos:homeDiretory:loginShell

Autenticação do GNU/Linux (2)

- /etc/fstab -> ou=Mounts
- /etc/hosts -> ou=Hosts
- /etc/{passwd,shadow} -> ou=People
- /etc/group -> ou=Group
- /etc/protocols -> ou=Protocols
- /etc/rpc -> ou=Rpc
- /etc/services -> ou=Services
- /etc/networks -> ou=Networks
- netgroups -> ou=Netgroups

É necessário criar as ou's People, Group

Autenticação do GNU/Linux (3)

- /etc/ldap.conf
  - *Arquivo compatilhado entre o pam_ldap e nss_ldap, contém informações gerais sobre o diretório*
  - *Definições de como o PAM deve se comportar quando da autenticação no diretório*
  - *Definições de como o NSS deve se comportar quando da busca de informações no diretório*
- /etc/nsswitch.conf
  - *Define se o sistema deverá consultar informações em arquivos locais, em serviços de rede (LDAP, NIS) ou em ambos. Como deve se comportar em caso de falhas em algum dos meios de infromações, etc.*

Autenticação do GNU/Linux (4)

- /etc/pam.d/common-auth

account sufficient pam_ldap.so
account required pam_unix.so try_first_pass

- /etc/pam.d/common-passwd

password sufficient pam_ldap.so md5
password sufficient pam_unix.so md5 try_first_pass

/etc/pam.d/common-account

account sufficient pam_ldap.so
account required pam_unix.so try_first_pass

- /etc/pam.d/common-session

session sufficient pam_ldap.so
session required pam_mkhomedir.so skel=/etc/skel umask=0022
session required pam_unix.so

Autenticação do GNU/Linux (5)

- /etc/nssswitch.conf

```
passwd:         compat ldap
group:          compat ldap
shadow:         compat ldap
```

- É necessário instalar e executar o daemon NSCD (GNU Naming Service Cache Daemon) para agilizar as pesquisas no serviço de diretório

Postfix MTA e LDAP (1)

- Suporte a LDAP no Postfix
  - O Postfix pode usar um diretório LDAP como fonte para qualquer uma de suas tabelas: aliases(5), virtual(5), canonical(5), etc
  - Permite manter as informações do sistema de correio em um serviço de rede integrado com controle de acesso
  - O controle das contas pode ser realizado de forma centralizada, servindo para diversos sistemas sem ter que manter uma cópia local em cada sistema e replicar as as alterações manualmente

Postfix MTA e LDAP (2)

- Exemplo - Tabela de Aliases (ldapaliases.cf)

server_host = localhost
search_base = dc=alexandrealencar,dc=com
scope = sub
query_filter = (uid=%s)
result_attribute = mail

- Configuração do Postfix (master.cf)

alias_maps = ldap:/etc/postfix/ldapaliases.cf, ...)

- O Posfix irá incluir o diretório LDAP em suas buscas quando chegarem novas mensagens ao servidor e o endereço não estiver na tabela padrão

OpenLDAP Usando TLS (1)

- Os servidores e clientes OpenLDAP suportam TLS para prover integridade e confidencialidade das informações e suporte ao mecanismo SASL EXTERNAL
- Os servidores e clientes usam certificados X.509
- A DN do certificado deve ser igual ao hostname do servidor (hostname -f)
- A DN do certificado do cliente pode ser igual à DN do cliente, desta forma, o método SASL EXTERNAL usará esta informação para autenticar o cliente junto ao servidor

OpenLDAP Usando TLS (2)

- Para que o TLS seja implementado, no mínimo estes requisitos precisam ser atendidos
  - Servidores
    - Certificado da CA
    - Certificado do Servidor
  - Clientes
    - Certificado da CA
- Na maioria dos casos, os certificados são emitidos pela mesma CA, de forma que os servidores e clientes precisam estar configurado apenas para o certificado da CA emissora

OpenLDAP Usando TLS (3)

- Configuração do Servidor
  - TLSCACertificateFile
    - Especifica o nome do arquivo que contém os certificados (PEM) das CA's nas quais o slapd irá confiar. É necessário que este arquivo contenha o certificado da CA que emitiu o certificado do servidor
  - TLSCACertificatePath
    - Informa o caminho onde o slapd pode encontrar os arquivos contendo os certificados individuais de cada CA confiável. O utilitário c_rehash deve ser utilizado para criar links simbólicos dos hash's dos certificados para os nomes dos arquivos em disco

OpenLDAP Usando TLS (4)

- TLSCertificateFile
  - Informa o nome do arquivo que contém o certificado a ser utilizado pelo servidor slapd
- TLSCertificateKeyFile
  - Informa o nome do arquivo que contém a chave privada do certificado do servidor slapd. A chave não pode estar encriptada, visto que o OpenLDAP ainda não suporta chaves encriptadas
- TLSCipherSuite
  - Define quais cifras serão usadas e sua ordem. Para maiores detalhes, consultar openssl ciphers -v ALL

OpenLDAP Usando TLS (5)

- TLSRandFile
  - Especifica uma fonte de semente para uso nas operações de cifragem das informações (apenas quando /dev/urandom não está disponível)
- TLSVerifyClient
  - Define que tipo de checagem deve ser feita nas conexões efetuadas pelos clientes em uma sessão TLS. Os possíveis valores são:
    - never (nunca perguntar por um certificado ao cliente)
    - allow (perguntar por um certificado, mas não é obrigatório ter um)
    - try (perguntar por um certificado, se for fornecido e não for válido, terminar a sessão, do contrário, continuar a sessão normalmente)
    - demand (um certificado válido deve ser fornecido ou a sessão é terminada)

OpenLDAP Usando TLS (5)

- Configuração do Cliente
  - Os parâmetros de configuração do cliente são basicamente os mesmos do servidor, podem ser configurados de forma global. A configuração global é sobrescrita através do arquivo .ldaprc do usuário
  - A operação LDAP Start TLS é usada para iniciar a negociação TLS. Todas as ferramentas OpenLDAP suportam as flags -Z e -ZZ para indicar o uso de TLS. A primeira solicita TLS, mas continua se não obtiver sucesso, a segunda pára a comunicação, caso um canal TLS não seja estabelecido entre o servidor e o cliente

OpenLDAP Usando TLS (6)

- TLS_CACERT
  - É equivalente à TLSCACertificateFile
- TLS_CACERTDIR
  - É equivalente à TLSCACertificatePath
- TLS_CERT
  - Especifica o arquivo que contém o certificado a ser usado nas conexões, deve existir apenas no arquivo .ldaprc
- TLS_KEY
  - Especifica o arquivo que contém a chave privada do certificado, obedece as mesmas restrições de TLSCertificateKeyFile e só deve constar em .ldaprc

OpenLDAP Usando TLS (7)

  - TLS_RANDFILE
    - Equivalente a TLSRandFile
  - TLS_REQCERT
    - Equivalente a TLSVerifyClient
    - A configuração padrão para o cliente é demand ao contrário do servidor (never)
- No arquivo de configuração do OpenSSL é necessário constar a opção abaixo
  - unique_subject = no

Cyrus POP/IMAP e LDAP

- O imapd.conf deve conter as linhas
  - sasl_pwcheck_method: saslauthd
  - sasl_passwd_chech: saslauthd
- O arquivo saslauthd.conf deve conter as linhas
  - ldap_servers: ldap://<fqdn do servidor>
  - ldap_base_dn: <base do diretório>
  - ldap_auth_method: bind
  - ldap_bind_dn: <credencial de acesso ao diretório>
  - ldap_bind_pw: <senha do diretório>
  - ldap_filter: (uid=%u)
  - ldap_use_sasl: no
  - ldap_search_base: <onde a pesquisa deve começar>

Apache e LDAP

- É necessário que o módulo auth_ldap.so esteja instalado e carregado no Apache
- Existe um outro módulo LDAP para o Apache chamado mod_authz_ldap.so

```
...
<Directory /var/www/html>
 Options Indexes FollowSymlinks Multiviews
 AuthType Basic
 AuthName "Autenticação via LDAP"
 AuthLDAPURL ldap://ldap/dc=alexandrealencar,dc=com?uid?sub
 AuthLDAPStartTLS on
 AllowOverride AuthConfig
 Require valid-user
</Directory>
...
```

ProFTPD e LDAP

- É necessário que o ProFTPD tenha o módulo mod_ldap habiltado.
- As informações (contas, senhas, etc) serão obtidas no diretório via LDAP

```
LDAPServer localhost
LDAPDNInfo uid=proftpd,dc=alexandrealencar,dc=com senha
LDAPDoAuth on “dc=alexandrealencar,dc=com”
```

Squid e LDAP

- Configuração para autenticação dos usuários do Proxy via LDAP

```
...
auth_param basic program /usr/lib/squid/ldap_auth -b
    dc=alexandrealencar,dc=com -h ldap.alexandrealencar.com -f
    "(&(ObjectClass=posixAccount)(uid=%s))"
auth_param basic realm Autenticação do Proxy Squid
auth_param basic children 30
auth_param basic credentialsttl 2 hours
...
acl usuarios_auth_ldap proxy_auth REQUIRED
...
```

DNS e LDAP

- Existem diversas implementações de DNS em LDAP, dentre elas, um add-on para o BIND
- Ldapdns é um servidor DNS que publica as informações de hosts armazenadas em um diretório via LDAP
- Microsoft Active Directory / DNS
- PowerDNS
  - (http://www.powerdns.com/products/powerdns/

Solucionando problemas

- Análise dos logs
- Ferramentas de linha de comando
- Debug
- Diagnóstico da rede
- Revisão dos arquivos de configuração

Melhorias de performance (1)

- Índices os atributos e objetos mais utilizados (cn, uid, uidNumer, gidNumber)
- Otimizar o sistema operacional, desativando serviços desnecessários
- Otimizar o disco para leituras (um disco para sistema operacional, um para armazenar o diretório)
- Desativar log excessivo (loglevel 0 e LOCAL4.* -/var/log/ldap.log no syslog)

Melhorias de performance (2)

- O slapd sincroniza o DB a cada alteração (segurança), mas em um slave é desnecessário, visto que isto torna o sistema mais lento.
- Setar a opção na configuração do DB
  - DbcacheNoWsync

Backup e restauração

- Backup dos arquivos BDB
  - Nem sempre compatível entre sistemas diferentes
- Dump do diretório para LDIF
  - Formato padronizado
  - Texto plano
  - Compatível entre plataformas
  - Compatível entre fornecedores (restrito apenas pelos esquemas utilizados)
  - Fácil de manipular
  - Precisa ser mantido em segurança

Samba e LDAP