

# LDAP

(Lightweight Directory Access Protocol)

Diego Minichiello, Mateus Azor, Paulo Nunes

# O que é LDAP?

É um protocolo aberto, livre de fornecedor e padrão de indústria, que fornece meios de acessar e manter serviços de informação de diretório distribuído sobre um IP. O LDAP reduz os recursos do sistema requeridos, incluindo apenas um subconjunto funcional do DAP (Directory Access Protocol) X.500 original.

X.500 é uma série de padrões para redes de computador abordando serviço de diretório. Sendo eles:

- DAP (Directory Access Protocol)
- DSP (Directory System Protocol)
- DISP (Directory Information Shadowing Protocol)
- DOP (Directory Operational Bindings Management Protocol)

# *Lightweight DAP*

Acessar um diretório do X.500 requer o DAP (Directory Access Protocol). No entanto, o DAP requer grandes quantidades de recursos do sistema e mecanismos de suporte para manejar a complexidade do protocolo. O LDAP foi introduzido para reduzir essa necessidade.

O LDAP, um protocolo com base em cliente e servidor, pode tratar alguns dos recursos pesados exigidos pelos clientes DAP. Um servidor LDAP pode apenas retornar resultados ou erros ao cliente, que requerem pouco do cliente.

# Funcionamento

Um cliente começa uma sessão de LDAP ligando-se a um servidor LDAP, normalmente pela porta padrão 389 (TCP). Este envia requisições para o servidor, o qual devolve respostas. As operações básicas são:

Bind (Autenticação), Search (Procurar Entradas), Compare (Testar Valores De Entradas), Add (Adicionar Entrada), Delete (Apagar Entrada), Modify (Modificar Entrada), Modify DN (Mover/Renomear Entrada), StartTLS (Proteger Conexão Com TLS), Abandon (Abortar Requisição) e Unbind (Fechar Conexão).

Com algumas exceções o cliente não precisa esperar uma resposta antes de enviar a próxima requisição e o servidor pode enviar as respostas em qualquer ordem.



# Estrutura

Uma entrada consiste de um conjunto de atributos. Um atributo possui um nome e um ou mais valores. Cada entrada possui um identificador único: Distinguished Name (DN). Ele consiste de seu Relative Distinguished Name (RDN), seguido pelo DN da entrada pai. Pense no DN como o caminho completo de um arquivo e o RDN como seu nome de arquivo relativo em sua pasta pai, por exemplo:

DN -> /root/user/file.txt

RDN -> file.txt

# Instalação - Parte 1

Atualize o sistema.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo apt update  
Hit:1 http://vn.archive.ubuntu.com/ubuntu jammy InRelease  
Hit:2 http://vn.archive.ubuntu.com/ubuntu jammy-updates InRelease  
Hit:3 http://vn.archive.ubuntu.com/ubuntu jammy-backports InRelease  
Hit:4 http://security.ubuntu.com/ubuntu jammy-security InRelease  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
7 packages can be upgraded. Run 'apt list --upgradable' to see them.  
hg@server-1:~$
```

# Instalação - Parte 2

Descubra o nome/endereço do sistema bem como seu IP.

```
hg@server-1:~$ hostname
server-1
hg@server-1:~$ hostname -f
server-1.hg.local
hg@server-1:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.15  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::b8f3:b6e7:98c5:6676  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:a1:9d:36  txqueuelen 1000  (Ethernet)
    RX packets 166793  bytes 230333180 (230.3 MB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 64887  bytes 5502476 (5.5 MB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 599  bytes 122820 (122.8 KB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 599  bytes 122820 (122.8 KB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

hg@server-1:~$
```

# Instalação - Parte 3

Instale o Apache Web Server.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo apt install apache2 php php-cgi libapache2-mod-php php-mbstring php-common php  
-pear -y
```



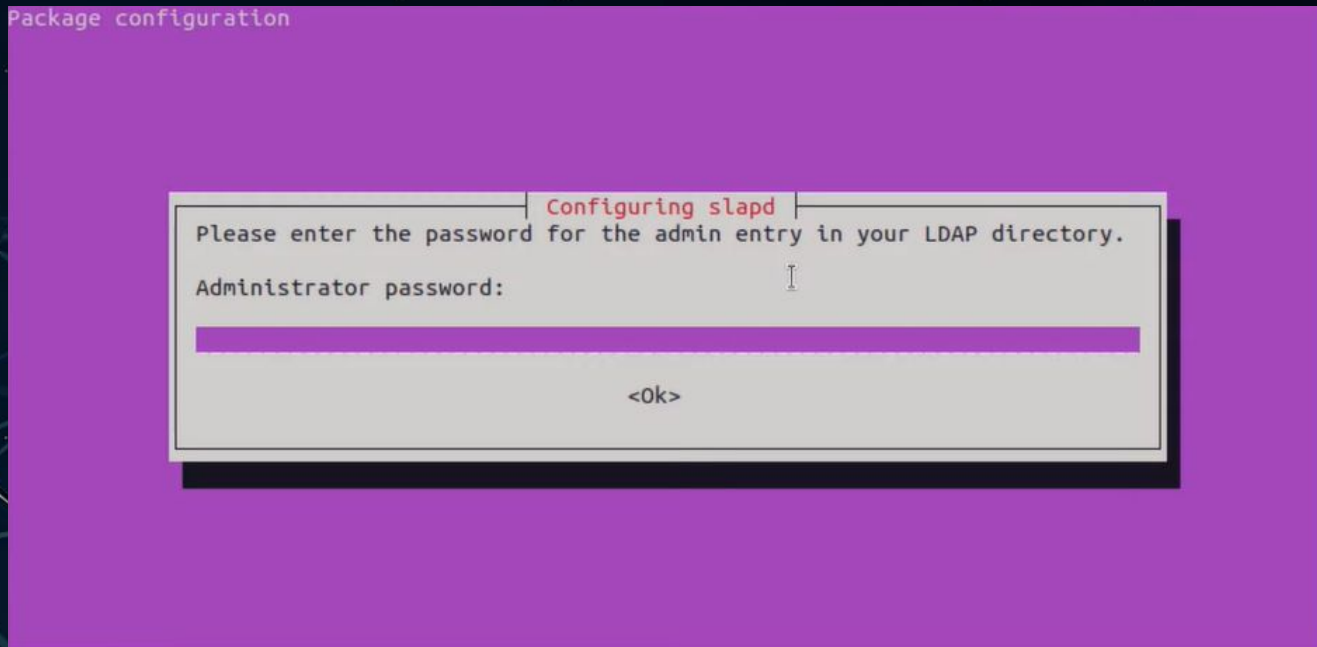
# Instalação - Parte 4.1

Instale o OpenLDAP Server.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo apt install slapd ldap-utils -y
```

# Instalação - Parte 4.2

Defina a senha de administrador do OpenLDAP.



# Instalação - Parte 4.3

Verifique a instalação.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo slapcat  
dn: dc=hg,dc=local  
objectClass: top  
objectClass: dcObject  
objectClass: organization  
o: hg.local  
dc: hg  
structuralObjectClass: organization  
entryUUID: 8bf7691a-3243-103d-80de-2904d8e04414  
creatorsName: cn=admin,dc=hg,dc=local  
createTimestamp: 20230127040514Z  
entryCSN: 20230127040514.679441Z#000000#000#000000  
modifiersName: cn=admin,dc=hg,dc=local  
modifyTimestamp: 20230127040514Z  
  
hg@server-1:~$
```

# Instalação - Parte 5.1

Instale o LAM (LDAP Account Manager).

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo apt install ldap-account-manager -y
```



# Instalação - Parte 5.2

Ative a extensão PHP-CGI.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo a2enconf php*-cgi  
Enabling conf php8.1-cgi.  
To activate the new configuration, you need to run:  
    systemctl reload apache2  
hg@server-1:~$
```

# Instalação - Parte 5.3

Reinicie o serviço Apache e ative a execução ao inicializar (boot).

```
hg@server-1:~$ sudo systemctl restart apache2
hg@server-1:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-instal
tall.
Executing: /lib/systemd/systemd-sysv-install enable apache2
hg@server-1:~$
```

# Instalação - Parte 5.4

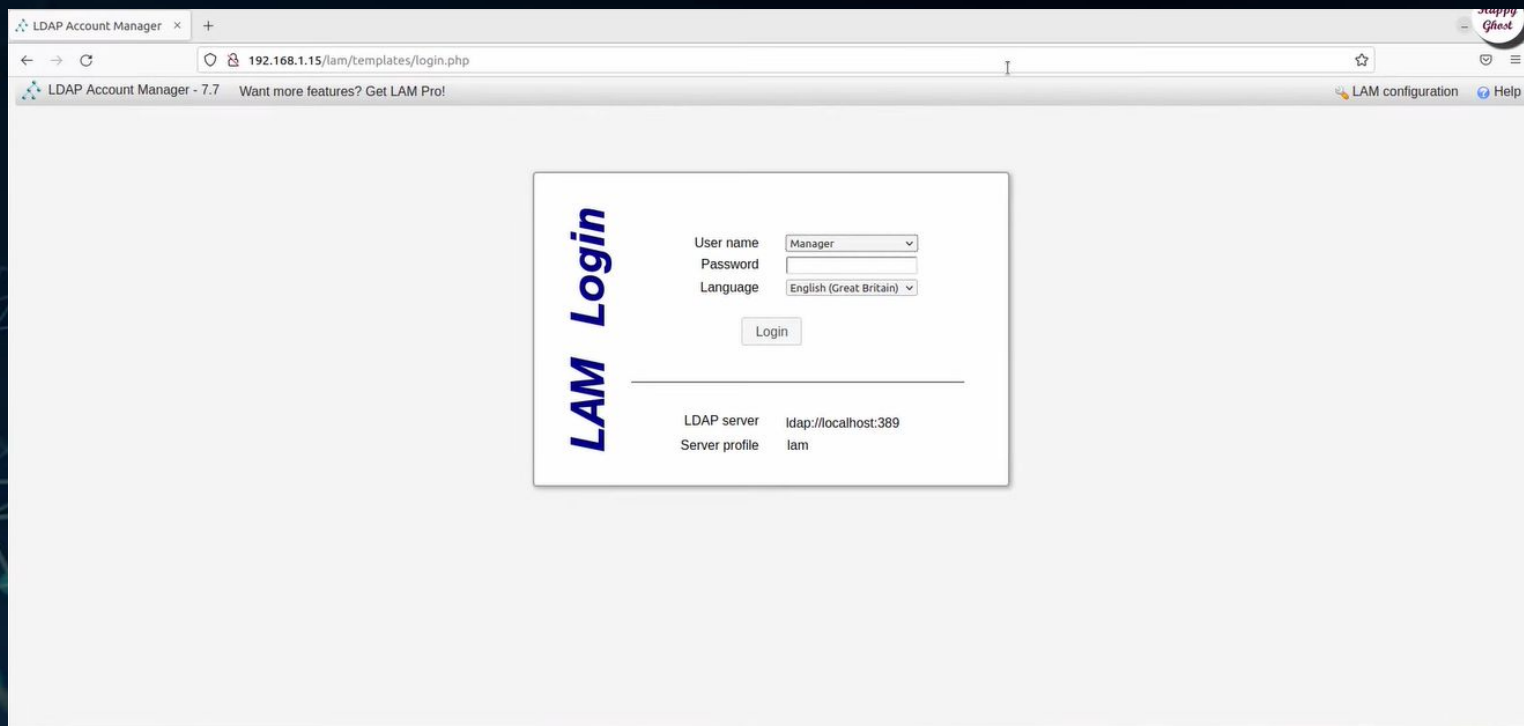
Confirme que o Apache está rodando.

```
hg@server-1:~$ sudo systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2023-01-27 11:07:24 +07; 27s ago
     Docs: https://httpd.apache.org/docs/2.4/
 Main PID: 19143 (apache2)
    Tasks: 6 (limit: 2247)
   Memory: 14.3M
      CPU: 73ms
   CGroup: /system.slice/apache2.service
           └─19143 /usr/sbin/apache2 -k start
             └─19144 /usr/sbin/apache2 -k start
               └─19145 /usr/sbin/apache2 -k start
                 └─19146 /usr/sbin/apache2 -k start
                   └─19147 /usr/sbin/apache2 -k start
                     └─19148 /usr/sbin/apache2 -k start

Thg 1 27 11:07:24 server-1 systemd[1]: Starting The Apache HTTP Server...
Thg 1 27 11:07:24 server-1 systemd[1]: Started The Apache HTTP Server.
hg@server-1:~$
```

# Instalação - Parte 6.1

Acesse *http://[ip do servidor]/lam*.



The screenshot shows a web browser window with the title "LDAP Account Manager - 7.7" and a URL bar showing "192.168.1.15/lam/templates/login.php". The page content is a login form for LAM. On the left, the text "LAM Login" is displayed vertically in blue. The form includes fields for "User name" (a dropdown menu with "Manager" selected), "Password" (a text input field), and "Language" (a dropdown menu with "English (Great Britain)" selected). Below these fields is a "Login" button. At the bottom of the form, the "LDAP server" is listed as "ldap://localhost:389" and the "Server profile" is listed as "lam". The browser's address bar also shows "LDAP Account Manager - 7.7" and "Want more features? Get LAM Pro!". The browser's status bar at the bottom shows "LAM configuration" and "Help".

LDAP Account Manager - 7.7 Want more features? Get LAM Pro!

LDAP server ldap://localhost:389  
Server profile lam



# Instalação - Parte 6.2

Vá para “LAM configuration” em seguida “Edit server profiles”.



Edit general settings



Edit server profiles

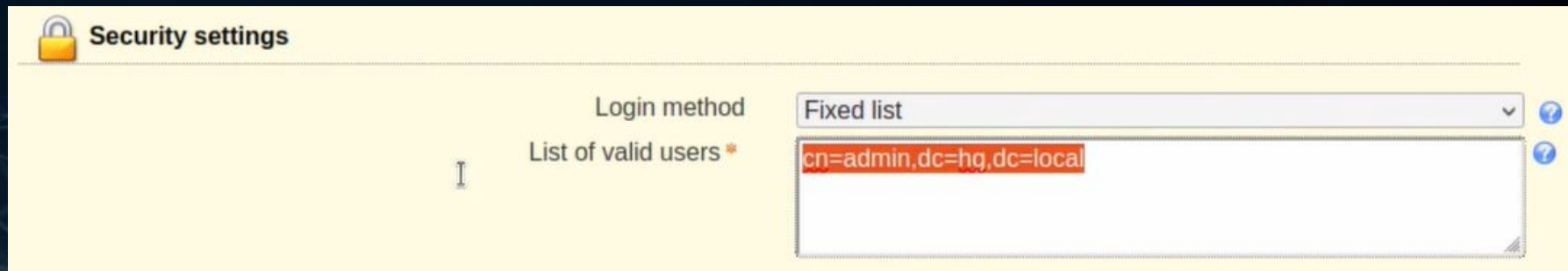


Import and export configuration

Senha padrão: “lam”.

# Instalação - Parte 6.3

Em “Security settings” preencha seu usuário.



The screenshot shows a window titled "Security settings" with a yellow background and a lock icon. It contains two main sections: "Login method" and "List of valid users". The "Login method" dropdown is set to "Fixed list". The "List of valid users" field, which has a red star icon next to it, contains the text "cn=admin,dc=hq,dc=local". There are also two question mark icons on the right side of the window.

Security settings

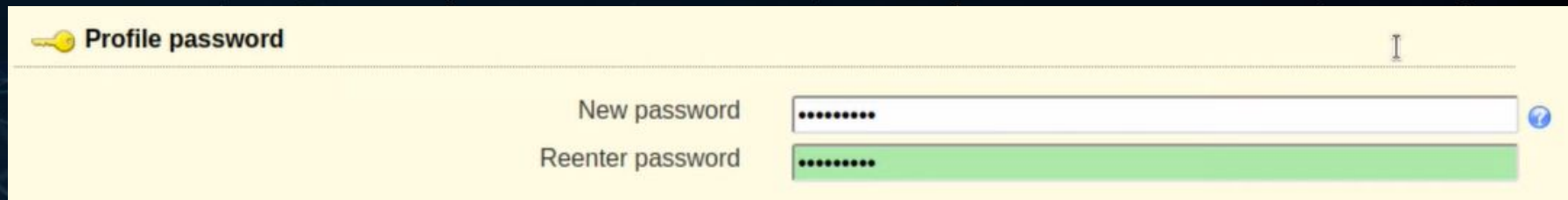
Login method: Fixed list

List of valid users ✱: cn=admin,dc=hq,dc=local

Criado na parte 4.2/4.3.

# Instalação - Parte 6.4

Em “Profile password” redefine a senha padrão.

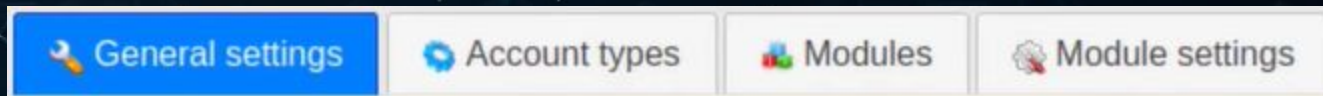


The screenshot shows a configuration window titled "Profile password" with a yellow key icon. It contains two password input fields. The first field, labeled "New password", is white and contains seven dots. The second field, labeled "Reenter password", is green and also contains seven dots. A blue question mark icon is located to the right of the "New password" field. The window has a yellow background and a thin border.

Lembre de salvar as novas configurações.

# Instalação - Parte 7.1

Em “Edit server profiles” acesse a aba “Account types”.





# Instalação - Parte 7.2

Em “Active account types” crie um departamento e grupo.

The screenshot shows the 'Active account types' configuration window. It has two main sections: 'Users' and 'Groups'. Each section has a title bar with a user/group icon, a title, and a dropdown arrow and a red 'X' icon. Below each title bar are several input fields and a checkbox.

**Users**

- LDAP suffix:
- List attributes:
- Custom label:
- Additional LDAP filter:
- Hidden: ☐

**Groups**

- LDAP suffix:
- List attributes:
- Custom label:
- Additional LDAP filter:
- Hidden: ☐

Lembre de salvar as novas configurações.

# Instalação - Parte 7.3

Após salvar e efetuar o login novamente, aceite a criação.

The following suffixes are missing in LDAP. LAM can create them for you.

You can setup the LDAP suffixes for all account types in your LAM server profile on tab "Account types".

ou=Department,dc=hg,dc=local

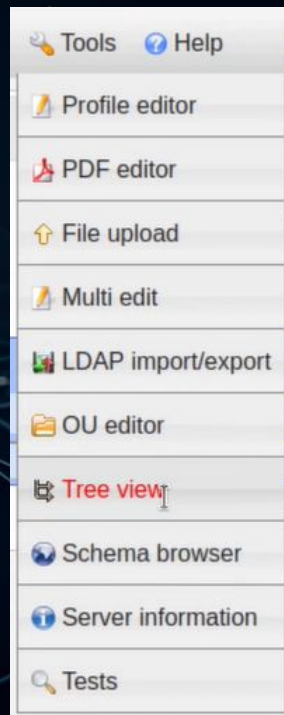
ou=Group,dc=hg,dc=local

Create

Cancel

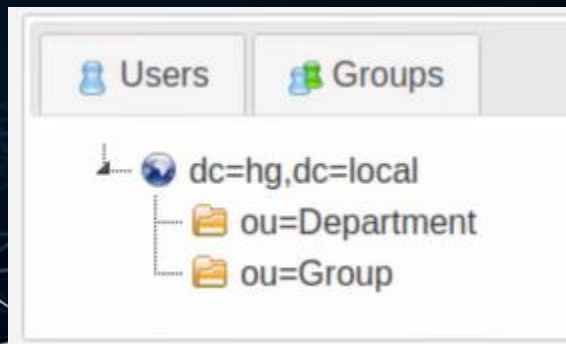
# Instalação - Parte 7.4

Após criar, vá em “Tools” e acesse “Tree view”.



# Instalação - Parte 7.5

Verifique se o departamento e grupo foram criados corretamente.





# Instalação - Parte 8.1

Verifique o estado de seu firewall.

```
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$  
hg@server-1:~$ sudo ufw status  
Status: inactive
```

# Instalação - Parte 8.2

Caso esteja inativo, ative o firewall.

```
hg@server-1:~$ sudo ufw enable  
Firewall is active and enabled on system startup
```

# Instalação - Parte 8.3

Libere as portas 80 (http), 443 (https) e 389 (LDAP) no firewall.

```
hg@server-1:~$ sudo ufw allow 80
Rule added
hg@server-1:~$ sudo ufw allow 443
Rule added
hg@server-1:~$ sudo ufw allow 389
Rule added
```

# Instalação - Parte 8.4

Verifique se as portas foram liberadas.

```
hg@server-1:~$ sudo ufw status  
Status: active
```

To	Action	From
--	-----	----
80	ALLOW	Anywhere
443	ALLOW	Anywhere
389	ALLOW	Anywhere

```
hg@server-1:~$
```

# LDAP

(Lightweight Directory Access Protocol)

**Obrigado Por Assistir!!!**



# Referências

HAPPYGHOST. LDAP - How to Install and Configure OpenLDAP Server on Ubuntu/Debian. Disponível em: <[https://www.youtube.com/watch?v=LzRK\\_8zwqxY](https://www.youtube.com/watch?v=LzRK_8zwqxY)>. Acesso em: 14 abr. 2024.

MULLER Mateus. SERVIDOR LINUX #5 - O que é LDAP? OpenLDAP? AUTENTICAÇÃO com LDAP?. Disponível em: <<https://www.youtube.com/watch?v=l8BwMIPRMF8>>. Acesso em: 14 abr. 2024.

YUNUS, M. Online LDAP test server. Disponível em: <<https://www.forumsys.com/2022/05/10/online-ldap-test-server/>>. Acesso em: 14 abr. 2024.

Basic LDAP concepts. Disponível em: <<https://ldap.com/basic-ldap-concepts/>>. Acesso em: 15 abr. 2024.