[Network] Tìm hiểu LDAP, cấu hình xác thực SSH với LDAP

May 29, 2017

13397

[Chia sẻ Facebook](http://www.facebook.com/sharer.php?u=https%3A%2F%2Ftechtalk.vn%2Fnetwork-tim-hieu-ldap-cau-hinh-xac-thuc-ssh-voi-ldap.html" \t "_new)

[Tweet](https://twitter.com/intent/tweet?text=%5BNetwork%5D+T%C3%ACm+hi%E1%BB%83u+LDAP%2C+c%E1%BA%A5u+h%C3%ACnh+x%C3%A1c+th%E1%BB%B1c+SSH+v%E1%BB%9Bi+LDAP&url=https%3A%2F%2Ftechtalk.vn%2Fnetwork-tim-hieu-ldap-cau-hinh-xac-thuc-ssh-voi-ldap.html&via=Tech+Talk" \t "_new)



**I. GIỚI THIỆU**

**1. LDAP là gì**

LDAP là chữ viết tắt của Lightweight Directory Access Protocol. LDAP phát triển dựa trên chuẩn X500. Đây là chuẩn cho dịch vụ thư mục (Directory Service – DS) chạy trên nền tảng OSI.

LDAP được coi là lightweight vì LDAP sử dụng gói tin overhead thấp, được xác định chính xác trên lớp TCP của danh sách giao thức TCP/IP (các dịch vụ hướng kết nối) còn X500 là heavyweight vì là lớp giao thức ứng dụng, chứa nhiều header hơn (các header của các layer tầng thấp hơn)

[Những việc làm hấp dẫn](https://topdev.vn/)

* [](https://topdev.vn/partners/detail-jobs/20-ky-su-phat-trien-phan-mem-webmobile-3-2010567/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=20+K%E1%BB%B9+S%C6%B0+Ph%C3%A1t+Tri%E1%BB%83n+Ph%E1%BA%A7n+M%E1%BB%81m+Web%2FMobile&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D)

**[20 Kỹ Sư Phát Triển Phần Mềm Web/Mobile](https://topdev.vn/partners/detail-jobs/20-ky-su-phat-trien-phan-mem-webmobile-3-2010567/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=20+K%E1%BB%B9+S%C6%B0+Ph%C3%A1t+Tri%E1%BB%83n+Ph%E1%BA%A7n+M%E1%BB%81m+Web%2FMobile&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "20 Kỹ Sư Phát Triển Phần Mềm Web/Mobile" \t "_blank)**

**[VIETTEL BUSINESS SOLUTIONS](https://topdev.vn/partners/detail-jobs/20-ky-su-phat-trien-phan-mem-webmobile-3-2010567/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=20+K%E1%BB%B9+S%C6%B0+Ph%C3%A1t+Tri%E1%BB%83n+Ph%E1%BA%A7n+M%E1%BB%81m+Web%2FMobile&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "20 Kỹ Sư Phát Triển Phần Mềm Web/Mobile" \t "_blank)***[HCM800 - 2,000 USD](https://topdev.vn/partners/detail-jobs/20-ky-su-phat-trien-phan-mem-webmobile-3-2010567/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=20+K%E1%BB%B9+S%C6%B0+Ph%C3%A1t+Tri%E1%BB%83n+Ph%E1%BA%A7n+M%E1%BB%81m+Web%2FMobile&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "20 Kỹ Sư Phát Triển Phần Mềm Web/Mobile" \t "_blank)*

[WebMobileJavaJava CoreiOS](https://topdev.vn/partners/detail-jobs/20-ky-su-phat-trien-phan-mem-webmobile-3-2010567/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=20+K%E1%BB%B9+S%C6%B0+Ph%C3%A1t+Tri%E1%BB%83n+Ph%E1%BA%A7n+M%E1%BB%81m+Web%2FMobile&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "20 Kỹ Sư Phát Triển Phần Mềm Web/Mobile" \t "_blank)

* [](https://topdev.vn/partners/detail-jobs/remote-senior-front-end-developer-5-15186/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BRemote%5D+Senior+Front-End+Developer&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D)

**[[Remote] Senior Front-End Developer](https://topdev.vn/partners/detail-jobs/remote-senior-front-end-developer-5-15186/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BRemote%5D+Senior+Front-End+Developer&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[Remote] Senior Front-End Developer" \t "_blank)**

**[TopDev's Client](https://topdev.vn/partners/detail-jobs/remote-senior-front-end-developer-5-15186/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BRemote%5D+Senior+Front-End+Developer&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[Remote] Senior Front-End Developer" \t "_blank)***[HCMNegotiable](https://topdev.vn/partners/detail-jobs/remote-senior-front-end-developer-5-15186/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BRemote%5D+Senior+Front-End+Developer&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[Remote] Senior Front-End Developer" \t "_blank)*

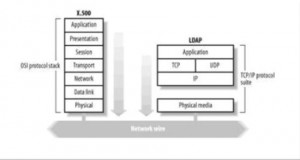
[JavaScriptCSSHTMLFront-End](https://topdev.vn/partners/detail-jobs/remote-senior-front-end-developer-5-15186/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BRemote%5D+Senior+Front-End+Developer&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[Remote] Senior Front-End Developer" \t "_blank)

* [](https://topdev.vn/partners/detail-jobs/hn-platform-embedded-software-engineer-set-top-box-product-2-15151/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BHN%5D+Platform+Embedded+Software+Engineer+%28Set-top+Box+Product%29&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D)

**[[HN] Platform Embedded Software Engineer (Set-top Box Product)](https://topdev.vn/partners/detail-jobs/hn-platform-embedded-software-engineer-set-top-box-product-2-15151/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BHN%5D+Platform+Embedded+Software+Engineer+%28Set-top+Box+Product%29&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[HN] Platform Embedded Software Engineer (Set-top Box Product)" \t "_blank)**

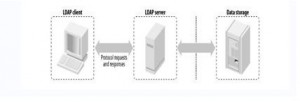
**[HUMAX VINA CO.,LTD](https://topdev.vn/partners/detail-jobs/hn-platform-embedded-software-engineer-set-top-box-product-2-15151/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BHN%5D+Platform+Embedded+Software+Engineer+%28Set-top+Box+Product%29&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[HN] Platform Embedded Software Engineer (Set-top Box Product)" \t "_blank)***[HN800 - 1,400 USD](https://topdev.vn/partners/detail-jobs/hn-platform-embedded-software-engineer-set-top-box-product-2-15151/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BHN%5D+Platform+Embedded+Software+Engineer+%28Set-top+Box+Product%29&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[HN] Platform Embedded Software Engineer (Set-top Box Product)" \t "_blank)*

[EmbeddedC++AndroidLinuxEmbedded Linux](https://topdev.vn/partners/detail-jobs/hn-platform-embedded-software-engineer-set-top-box-product-2-15151/?utm_source=techtalk.vn&utm_medium=jrec&utm_term=%5BHN%5D+Platform+Embedded+Software+Engineer+%28Set-top+Box+Product%29&token=ZKSuE%2BDgRSAzEOBNUcWfv9XiWteBtt6KdNdNI11aNYUzfyjT2VC0ZXq97IPeU9i0ITF9vI9NA30ibg73TVnifg%3D%3D" \o "[HN] Platform Embedded Software Engineer (Set-top Box Product)" \t "_blank)



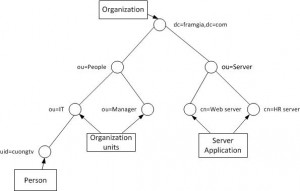
**X.500 thông qua mô hình OSI – LDAP thông qua TCP/IP**

LDAP chỉ là giao thức, không hỗ trợ xử lý như cơ sở dữ liệu. Mà nó cần một nơi lưu trữ backend và xử lý dữ liệu tại đó. Vì vậy mà LDAP client kết nối tới LDAP server theo mô hình sau:



\*\*Mối quan hệ giữa LDAP client, LDAP server và nơi chứa dữ liệu \*\*

LDAP là giao thức truy cập vì vậy nó theo mô hình dạng cây (Directory Information Tree). LDAP là giao thức truy cập dạng client/server.

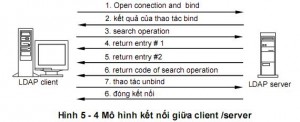


**Thư mục dạng cây của LDAP**

**2. Phương thức hoạt động của LDAP**

LDAP hoạt động theo mô hình client-server. Một hoặc nhiều LDAP server chứa thông tin về cây thư mục (Directory Information Tree – DIT). Client kết nối đến server và gửi yêu cầu. Server phản hồi bằng chính nó hoặc trỏ tới LDAP server khác để client lấy thông tin. Trình tự khi có kết nối với LDAP:

* Connect (kết nối với LDAP): client mở kết nối tới LDAP server
* Bind (kiểu kết nối: nặc danh hoặc đăng nhập xác thực): client gửi thông tin xác thực
* Search (tìm kiếm): client gửi yêu cầu tìm kiếm
* Interpret search (xử lý tìm kiếm): server thực hiện xử lý tìm kiếm
* Result (kết quả): server trả lại kết quả cho client
* Unbind: client gửi yêu cầu đóng kết nối tới server
* Close connection (đóng kết nối): đóng kết nối từ server



**Tiến trình hoạt động trao đổi LDAP client/server**

**3. Database backend của LDAP**

Slapd là một “LDAP directory server” có thể chạy trên nhiều platform khác nhau. Bạn có thể sử dụng nó để cung cấp những dịch vụ của riêng mình. Những tính năng mà slapd cung cấp:

* LDAPv3: slapd hỗ trợ LDAP cả IPv4, IPv6 và Unix IPC.
* Simple Authentication and Security Layer: slapd hỗ trợ mạnh mẽ chứng thực và bảo mật dữ liệu dịch vụ bằng SASL
* Transport Layer Security: slapd hỗ trợ sử dụng TLS hay SSL.

2 database mà SLAPD sử dụng để lưu trữ dữ liệu hiện tại là bdb và hdb. BDB sử dụng Oracle Berkeley DB để lưu trữ dữ liệu. Nó được đề nghị sử dụng làm database backend chính cho SLAPD thông thường. HDB là cũng tương tự như BDB nhưng nó sử dụng database phân cấp nên hỗ trợ cơ sỡ dữ liệu dạng cây. HDB thường được mặc định cấu hình trong SLAPD hiện nay.

**4. Lưu trữ thông tin của LDAP**

Ldif (LDAP Data Interchange Format) là một chuẩn định dang file text lưu trữ thông tin cấu hình LDAP và nội dung thư mục. File LDIF thường dùng để import dữ liệu mới vào trong directory hoặc thay đổi dữ liệu đã có. Dữ liệu trong file LDIF phải tuân theo quy luật có trong schema của LDAP.

Schema là loại dữ liệu được định nghĩa từ trước. Mọi thành phần được thêm vào hoặc thay đổi trong directory của bạn sẽ được kiểm tra lại trong schema để đảm bảo chính xác.

4.1. Cấu trúc tập tin LDIF

* Thông thường file LDIF sẽ có mẫu sau:
* Mỗi tập entry khác nhau được phân cách bởi dòng trắng
* “tên thuộc tính: giá trị”
* Một tập chỉ dẫn cú pháp để làm sao xử lý thông tin
* Những yêu cầu khi khai báo LDIF:
* Lời chú thích được gõ sau dấu # trong 1 dòng
* Thuộc tính được liệt kê bên trái dấu “:” và giá trị được biểu diễn bên phải.
* Thuộc tính dn định nghĩa duy nhất cho một DN xác định trong entry đó.

Ví dụ: thông tin của OU, people, các thư mục bên trong Distinguished Name framgia.com Thông tin LDAP thể hiện theo dạng cây o: framgia.com

*OU: PEOPLE*



|  |  |
| --- | --- |
| 1  2  3 | └── ou: IT |



|  |  |
| --- | --- |
| 1  2  3 | └──uid: cuongtv |

*OU: SERVER*

**File LDIF lưu thông tin: ——————————————————————–**

dn: o=framgia.com

objectclass: top

objectclass: organization

o: framgia.com

dn: ou=People,o=framgia.com

objectclass: organizationalUnit

ou: People

dn: ou=Server, o=framgia.com

objectclass: organizationalUnit

ou: Server

dn: ou=IT, ou=People, o=framgia.com

objectclass: organizationalUnit

ou: IT

dn: cn=cuongtv, ou=IT, ou=People, o=framgia.com

objectclass: top

objectclass: organizationalPerson

cn: cuongtv

sn: tran

givenname: cuong

uid: cuongtv

ou: IT

**4.2. Entry là gì**

Một entry là tập hợp của các thuộc tính, từng thuộc tính này mô tả một nét đặt trưng tiêu biểu của một đối tượng. Một entry bao gồm nhiều dòng

* DN : distinguished name – là tên của entry thư mục, tất cả được viết trên một dòng.
* Sau đó lần lượt là các thuộc tính của entry, thuộc tính dùng để lưu giữ dữ liệu. Mỗi thuộc tính trên một dòng theo định dạng là “kiểu thuộc tính : giá trị thuộc tính”.

**Một số các thuộc tính cơ bản trong file Ldif:**

| **STT** | **Tên** | **Mô tả** |
| --- | --- | --- |
| 1 | dn | Distinguished Name : tên gọi phân biệt |
| 2 | c | country – 2 kí tự viết tắt tên của một nước |
| 3 | o | organization – tổ chức |
| 4 | ou | organization unit – đơn vị tổ chức |
| 5 | objectClass | Mỗi giá trị objectClass hoạt động như một khuôn mẫu cho các dữ liệu được lưu giữ trong một entry. Nó định nghĩa một bộ các thuộc tính phải được trình bày trong entry (Ví dụ: entry này có giá trị của thuộc tính objectClass là eperson, mà trong eperson có quy định cần có các thuộc tính là tên, email, uid ,…thì entry này sẽ có các thuộc tính đó) |
| 6 | givenName | Tên |
| 7 | uid | id người dùng |
| 8 | cn | common name – tên thường gọi |
| 9 | telephoneNumber | số điện thoại |
| 10 | sn | surname – họ |
| 11 | userPassword | mật khẩu người dùng |
| 12 | mail | địa chỉ email |
| 13 | facsimileTelephoneNumber | số phách |
| 14 | createTimestamp | thời gian tạo ra entry này |
| 15 | creatorsName | tên người tạo ra entry này |
| 16 | pwdChangedTime | thời gian thay đổi mật khẩu |
| 17 | entryUUID | id của entry |

**II. Mô hình LDAP**

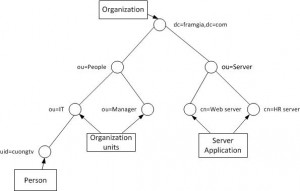
LDAP chia ra 4 mô hình:

* Mô hình LDAP information – xác định cấu trúc và đặc điểm của thông tin trong thư mục.
* Mô hình LDAP Naming – xác định cách các thông tin được tham chiếu và tổ chức.
* Mô hình LDAP Functional – định nghĩa cách mà bạn truy cập và cập nhật thông tin trong thư mục của bạn.
* Mô hình LDAP Security – định nghĩa ra cách thông tin trong thư mục của bạn được bảo vệ tránh các truy cập không được phép.

**1. Mô hình thông tin Ldap (LDAP information model)**

**Khái niệm**

* Mô hình LDAP Information định nghĩa ra các kiểu dữ liệu và các thành phần thông tin cơ bản mà bạn có thể chứa trong thư mục. Hay nó mô tả cách xây dựng ra các khối dữ liệu mà chúng ta có thể sử dụng để tạo ra thư mục.



**Mô hình thông tin Ldap**

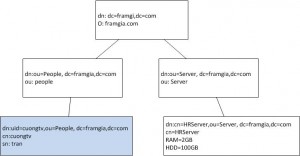
**2. Mô hình đặt tên Ldap (LDAP naming model)**

**Khái niệm**

* Mô hình LDAP Naming định nghĩa ra cách để chúng ta có thể sắp xếp và tham chiếu đến dữ liệu của mình.
* Hay mô hình này mô tả cách sắp xếp các entry vào một cấu trúc có logic, và mô hình LDAP Naming chỉ ra cách để chúng ta có thể tham chiếu đến bất kỳ một entry thư mục nào nằm trong cấu trúc đó.
* Mô hình LDAP Naming cho phép chúng ta có thể đặt dữ liệu vào thư mục theo cách mà chúng ta có thể dễ dàng quản lý nhất.

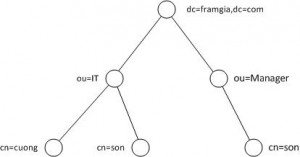
**Cách sắp xếp dữ liệu**

* Ví dụ như chúng ta có thể tạo ra một container chứa tất cả các entry mô tả người trong một tổ chức(o), và một container chứa tất cả các group của bạn, hoặc bạn có thể thiết kế entry theo mô hình phân cấp theo cấu trúc tổ chức của bạn. Việc thiết kế tốt cần phải có những nghiên cứu thoả đáng.
* Ta có thể thấy rằng entry trong thư mục có thể đồng thời là tập tin và là thư mục.



**Một phần thư mục LDAP với các entry chứa thông tin**

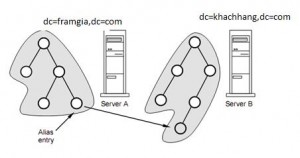
* Giống như đường dẫn của hệ thống tập tin, tên của một entry LDAP được hình thành bằng cách nối tất cả các tên của từng entry cấp trên (cha) cho đến khi trở lên root.
* Như hình trên ta thấy node có màu đậm sẽ có tên là uid=cuongtv, ou=people, dc=framgia, dc=com, nếu chúng ta đi từ trái sang phải thì chúng ta có thể quay ngược lại đỉnh của cây, chúng ta thấy rằng các thành phần riêng lẽ của cây được phân cách bởi dấu “,”.
* Với bất kỳ một DN, thành phần trái nhất được gọi là relative distingguished name (RDN), như đã nói DN là tên duy nhất cho mỗi entry trên thư mục, do đó các entry có cùng cha thì RDN cũng phải phân biệt.



* Ví dụ như hình trên, mặc dù hai entry có cùng RDN cn=son nhưng hai entry ở hai nhánh khác nhau.

**Bí danh (Aliases) – cách tham chiếu đến dữ liệu**

* Những entry bí danh (Aliases entry) trong thư mục LDAP cho phép một entry chỉ đến một entry khác.
* Để tạo ra một alias entry trong thư mục trước tiên bạn phải tạo ra một entry với tên thuộc tính là aliasedOjecctName với giá trị thuộc tính là DN của entry mà chúng ta muốn alias entry này chỉ đến.
* Hình dưới đây cho ta thấy được một aliases entry trỏ đến một entry thật sự.\



**LDAP với Alias entry**

* Nhưng không phải tất cả các LDAP Directory Server đều hổ trợ Aliases. Bởi vì một alias entry có thể chỉ đến bất kỳ một entry nào, kể cả các entry LDAP server khác. Và việc tìm kiếm khi gặp phải một bí danh có thể phải thực hiện tìm kiếm trên một cây thư mục khác nằm trên các server khác, do đó làm tăng chi phi cho việc tìm kiếm, đó là lý do chính mà các phần mềm không hổ trợ alias.

**3. Mô hình chức năng Ldap (LDAP function model)**

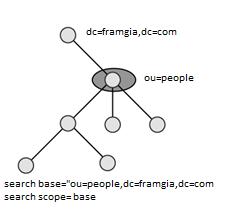
**Khái niệm**

* Đây là mô hình mô tả các thao tác cho phép chúng ta có thể thao tác trên thư mục.
* Mô hình LDAP Functional chứa một tập các thao tác chia thành 3 nhóm:
  + Thao tác thẩm tra (interrogation) cho phép bạn có thể search trên thư mục và nhận dữ liệu từ thư mục.
  + Thao tác cập nhật (update): add, delete, rename và thay đổi các entry thư mục.
  + Thao tác xác thực và điều khiển (authentiaction and control) cho phép client xác định mình đến chỗ thư mục và điều kiển các hoạt động của phiên kết nối.
  + Với version 3 giao thức LDAP ngoài 3 nhóm thao tác trên, còn có thao tác LDAP extended, thao tác này cho phép nghi thức LDAP sau này có thể mở rộng một cách có tổ chức.

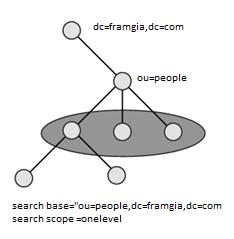
**Mô tả các thao tác**

**3.1. Thao tác thẩm tra (LDAP Interrogation)**

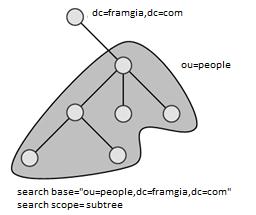
* Cho phép client có thể tìm và nhận lại thông tin từ thư mục.
* Thao tác tìm kiếm (LDAP search operation) yêu cầu 8 tham số (Ví dụ: search (“ou=people,dc=framgia,dc=com”,”base”,”derefInsearching”,10,60,attrOnly=true,Filter,ArrayAttribute)
* **Tham số đầu tiên** là đối tượng cơ sở mà các thao tác tìm kiếm thực hiện trên đó, tham số này là DN chỉ đến đỉnh của cây mà chúng ta muốn tìm.
* **Tham số thứ hai** là phạm vi cho việc tìm kiếm, chúng ta có 3 phạm vi thực hiện tìm kiếm:
  + Phạm vi “base” chỉ ra rằng bạn muốn tìm ngay tại đối tượng cơ sở.
  + Phạm vi “onelevel” thao tác tìm kiếm diễn ra tại cấp dưới (con trực tiếp của đối tượng cơ sở)
  + Phạm vi “subtree” thao tác này thực hiện tìm hết trên cây mà đối tượng cơ sở là đỉnh.



**Thao tác tìm kiếm với phạm vi base**



**Thao tác tìm kiếm với phạm vi onelevel**



\*\* Thao tác tìm kiếm với phạm vi subtree \*\*

* **Tham số thứ ba** derefAliases , cho server biết rằng liệu bí danh aliases có bị bỏ qua hay không khi thực hiện tìm kiếm, có 4 giá trị mà derefAliases có thể nhận được:”nerverDerefAliases” – thực hiện tìm kiếm và không bỏ qua bí danh (aliases) trong lúc thực hiện tìm kiếm và áp dụng với cả đối tượng cơ sở.

“derefInsearching” – bỏ qua các aliases trong trong các entry cấp dưới của đối tượng cơ sở, và không quan tâm đến thuộc tính của đối tượng cơ sở.

“derefFindingBaseObject” – tìm kiếm sẽ bỏ qua các aliases của đối tượng cơ sở, và không quan tâm đến thuộc tính của các entry thấp hơn đối tượng cơ sở.

“derefAlways” – bỏ qua cả hai nếu việc tìm kiếm thấy đối tượng cơ sở hay là các entry cấp thấp là các entry aliases.

* **Tham số thứ bốn** cho server biết có tối đa bao nhiêu entry kết quả được trả về.
* **Tham số thứ năm** qui định thời gian tối đa cho việc thực hiện tìm kiếm.
* **Tham số thứ sáu**: attrOnly – là tham số kiểu bool, nếu được thiết lập là true, thì server chỉ gởi các kiểu thuộc tính của entry cho client, nhưng sever không gởi giá trị của các thuộc tính đi
* **Tham số thứ bảy** là bộ lọc tìm kiếm (search filter) đây là một biểu thức mô tả các loại entry sẽ được giữ lại.
* **Tham số thứ tám**: danh sách các thuộc tính được giữ lại với mỗi entry.

3.2. Thao tác cập nhật (update)

Chúng ta có 4 thao tác cập nhật đó là add, delete, rename (modify DN), và modify

* Add: tạo ra một entry mới với tên DN và danh sách các thuộc tính truyền vào, khi thực hiện add một entry mới vào thư mục phải thoả các điều kiện sau :
  + Entry là nút cha của entry mới phải tồn tại
  + Chưa tồn tại một entry nào có cùng tên DN với entry mới trên thư mục
* Delete: thao tác xóa chỉ cần truyền vào tên của entry cần xóa và thực hiện thao tác nếu:
  + Entry tồn tại
  + Entry bị xóa không có entry con bên trong
* Rename: sử dụng để đổi tên hay di chuyển các entry trong thư mục
* Update: cập nhật với tham số DN và tập hợp các thay đổi được áp dụng nếu:
  + Entry với DN phải tồn tại
  + Tất cả thuộc tính thay đổi đều thành công
  + Các thao tác cập nhật phải là các thao tác được phép

**3.3. Thao tác xác thực và điều khiển (authentiaction and control)**

Thao tác xác thực gồm: thao tác bind và unbind:

* Bind : cho phép client tự xác định được mình với thư mục, thao tác này cung cấp sự xác nhận và xác thực chứng thưc
* Unbind : cho phép client huỷ bỏ phân đoạn làm việc hiện hành

Thao tác điều kiển chỉ có abandon:

* Abandon : cho phép client chỉ ra các thao tác mà kết quả client không còn quan tâm đến nữa.

**3.4. Các thao tác mở rộng**

Ngoài 9 thao tác cơ bản, LDAP version 3 được thiết kế mở rộng thông qua 3 thao tác :

* Thao tác mở rộng LDAP (LDAP extended operations)
  + Đây là một thao tác mới. Trong tương lai nếu cần một thao tác mới, thì thao tác này có thể định nghĩa và trở thành chuẩn mà không yêu cầu ta phải xây dựng lại các thành phần cốt lõi của LDAP.
  + Ví dụ một thao tác mở rộng là StarTLS, nghĩa là báo cho sever rằng client muốn sử dụng transport layer security (TLS) để mã hoá và tuỳ chọn cách xác thực khi kết nối.
* LDAP control
  + Là những phần của thông tin kèm theo cùng với các thao tác LDAP, thay đổi hành vi của thao tác trên cùng một đối tượng.
* Xác thực đơn giản và tầng bảo mật (Simple Authentication and Security Layer – SASL)
  + Là một mô hình hổ trợ cho nhiều phương thức xác thực.
  + Bằng cách sử dụng mô hình SASL để thực hiện chứng thực, LDAP có thể dễ dàng thích nghi với các phương thức xác thực mới khác.
  + SASL còn hổ trợ một mô hình cho client và server có thể kết nối trên hệ thống bảo mật diễn ra ở các tầng thấp (dẫn đến độ an toàn cao).

**4. Mô hình bảo mật Ldap (LDAP Security model)**

Vấn đề cuối cùng trong các mô hình LDAP là việc bảo vệ thông tin trong thư mục khỏi các truy cập không được phép. Khi thực hiện thao tác bind dưới một tên DN hay một người vô danh (anonymous) thì với mỗi user có một số quyền thao tác trên thư mục entry. Và những quyền nào được entry chấp nhận tất cả những điều trên gọi là truy cập điều khiển (access control). Hiện nay LDAP chưa định nghĩa ra một mô hình Access Control, các điều kiện truy cập này được thiết lập bởi các nhà quản trị hệ thống bằng các server software.

**III. Chứng thực trong LDAP**

* Việc xác thực trong một thư mục LDAP là một điều cần thiết và không thể thiếu. Quá trình xác thực được sử dụng để thiết lập quyền của khách hàng cho mỗi lần sử dụng.
* Tất cả các công việc như tìm kiếm, truy vấn, vv… được sự kiểm soát bởi các mức uỷ quyền của người được xác thực.
* Khi xác nhận một người dùng của LDAP cần tên người dùng được xác định như là một DN (ví dụ cn = cuongtv,o = it,dc = framgia,dc = com) và mật khẩu tương ứng với DN đó.

**Một số phương thức xác thực người dùng**

* Xác thực người dùng nặc danh (Anonymous Authentication)
  + Xác thực người dùng nặc danh là một xử lý ràng buộc đăng nhập vào thư mục với một tên đăng nhập và mật khẩu là rỗng. Cách đăng nhập này rất thông dụng và đuợc thường xuyên sử dụng đối với ứng dụng client.
* Xác thực nguời dùng đơn giản (Simple Authtication)
  + Đối với xác thực nguời dùng đơn giản, tên đăng nhập trong DN được gửi kèm cùng với một mật khẩu dưới dạng clear text tới máy chủ LDAP.
  + Máy chủ sẽ so sánh mật khẩu với giá trị thuộc tính userPassword hoặc với những giá trị thuộc tính đã được định nghĩa truớc trong entry cho DN đó.
  + Nếu mật khẩu được lưu dưới dạng bị băm (mã hoá), máy chủ sẽ sử dụng hàm băm tương ứng để biến đối mật khẩu đưa vào và so sánh giá trị đó với giá trị mật khẩu đã mã hoá từ trước.
  + Nếu cả hai mật khẩu trùng nhau, việc xác thực client sẽ thành công.
* Xác thực đơn giản qua SSL/TLS
  + LDAP sẽ mã hóa trước khi thực hiện bất cứ hoạt động kết nối nào. Do đó, tất cả thông tin người dùng sẽ được đảm bảo (ít nhất là trong session đó)

**IV. Cài đặt và cấu hình LDAP trên Ubuntu 12.04**

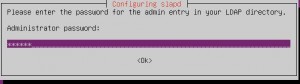
**1. Cài đặt và cấu hình LDAP**

Trên server ubuntu, ta thực hiện cài đặt các gói package sau:

\*\*apt-get update \*\*

**apt-get install slapd ldap-utils**

Trong quá trình cài đặt, hệ thống sẽ yêu cầu điền password admin cho LDAP



Sau khi cài xong, thực hiện câu lệnh sau để cấu hình lại LDAP:

**sudo dpkg-reconfigure slapd**

và thực hiện cấu hình:

* Omit OpenLDAP server configuration? **No**
* DNS domain name? **test.com**
* Organization name? **test**
* Administrator password?
* Database backend? **HDB**
* Database removed when slapd is purged? **No**
* Move old database? **Yes**
* Allow LDAPv2? **No**

**2. Thêm thuộc tính với LDIF**

Tạo file LDIF chứa thông tin cần tạo: ———————————————————

dn: ou=people,dc=test,dc=com

objectClass: organizationalUnit

ou: people

dn: ou=group,dc=test,dc=com

objectClass: organizationalUnit

ou: group

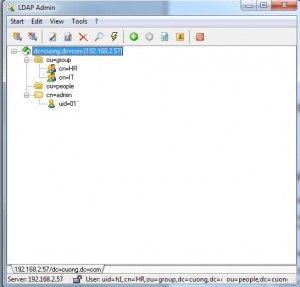
* Add entry mới vào LDAP bằng câu lệnh:

**ldapadd -x -D cn=admin,dc=test,dc=com -W -f <file.ldif>**

* Kiểm tra lại các entry có trong SLAPD bằng:

**slapcat**

**3. Chỉnh sửa LDAP với ldapadmin**

Trên windows, ta có thể sử dụng phần mềm LDAPAdmin: <http://www.ldapadmin.org/download/index.html>. Với phần mềm này, ta có thể tạo mới, chỉnh sửa hoặc xóa các Entry ngay trên giao diện  


**4. Kết nối client tới server (login ssh bằng account LDAP)**

Trên client, cài đặt các gói package sau: **apt-get install libpam-ldap nscd** và thiết lập các thành phần:

* LDAP server Uniform Resource Identifier: [**ldap://LDAP-server-IP-Address**](ldap://LDAP-server-IP-Address)
* Distinguished name of the search base: **“dc=test,dc=com”**
* LDAP version to use: **3**
* Make local root Database admin: **Yes**
* Does the LDAP database require login? **No**
* LDAP account for root: **“cn=admin,dc=test,dc=com”**
* LDAP root account password: **Your-LDAP-root-password**

Nếu config nhầm, ta có thể thực hiện cấu hình lại bằng câu lệnh:

**sudo dpkg-reconfigure ldap-auth-config**

Cấu hình file **/etc/nsswitch.conf**: thay đổi các dòng:

passwd: ldap compat

group: ldap compat

shadow: ldap compat

Và sửa lại file PAM config. PAM là module xác thực để hệ thống kết nối tới các ứng dụng yêu cầu xác thực. Ta sửa các file: **/etc/pam.d/common-session, common-account, common-auth** và **common-password**

account required pam\_unix.so

account sufficient pam\_ldap.so

account required pam\_permit.so

auth required pam\_permit.so

auth optional pam\_cap.so

auth sufficient pam\_unix.so

auth sufficient pam\_ldap.so use\_first\_pass

password required pam\_permit.so

password optional pam\_gnome\_keyring.so

password sufficient pam\_unix.so nullok md5 shadow use\_authtok

password sufficient pam\_ldap.so try\_first\_pass

session required pam\_permit.so

session optional pam\_umask.so

session optional pam\_ck\_connector.so nox11

session required pam\_mkhomedir.so skel=/etc/skel umask=0022

session required pam\_unix.so

session optional pam\_ldap.so