CUAC与Microsoft AD集成

目录

简介

本文档介绍轻量级目录访问协议(LDAP)在Cisco Unified Attendant Console(CUAC)和Microsoft Active Directory(AD)之间的工作方式，以及用于集成两个系统的过程。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM
- CUAC
- LDAP
- AD

使用的组件

本文档中的信息基于CUAC版本10.x。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

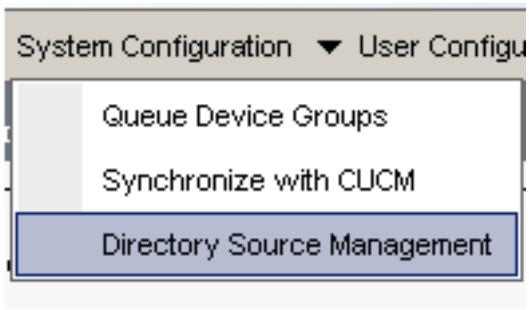
在早期的CUAC版本中，服务器通过预定义的查询和过滤器直接从Cisco Unified Communications Manager(CUCM)获取用户。使用CUAC高级版(CUACPE)，管理员可以直接从AD集成和导入用户。这为管理员提供了实施属性和过滤器的灵活性，这些属性和过滤器由他们自己选择和要求。

注意：CUACPE现已替换为版本10及更高版本的CUAC高级版。

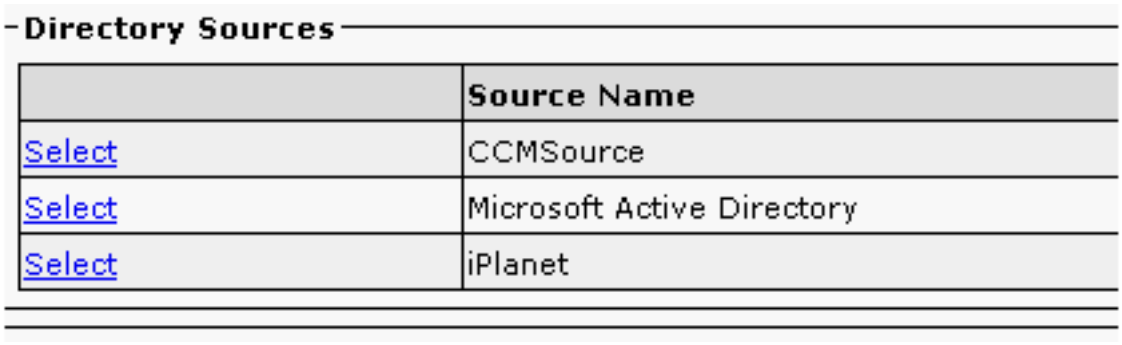
将AD与CUAC集成并从AD导入用户

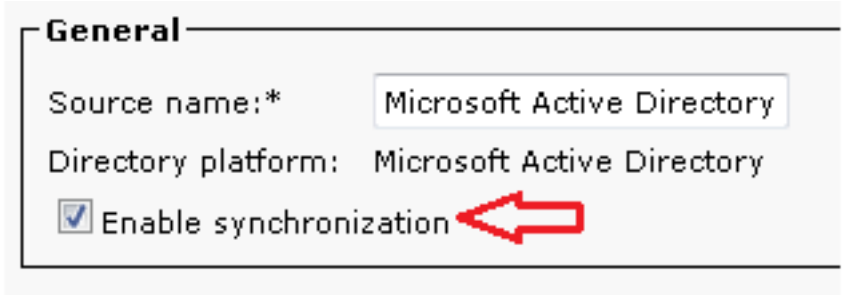
要将CUAC与AD集成并从AD导入用户，请完成以下步骤：

1. 在CUAC上启用AD的目录同步。

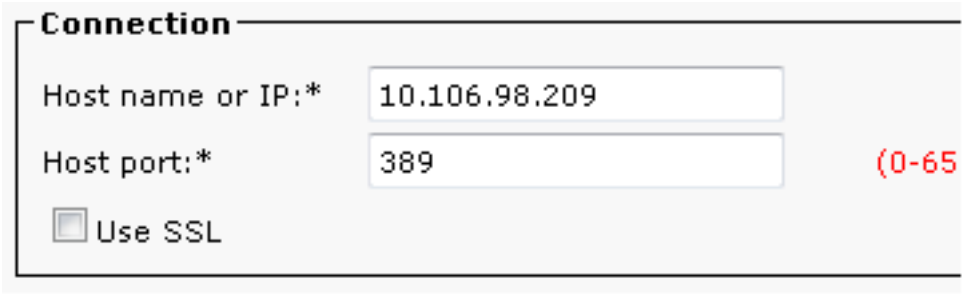


2. 选择**Microsoft Active Directory**并选中启**用同步**复选框：

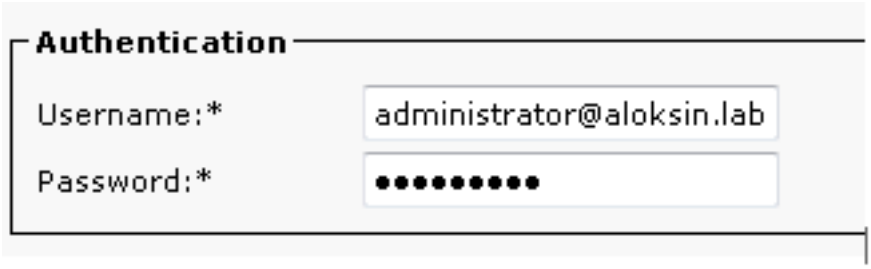




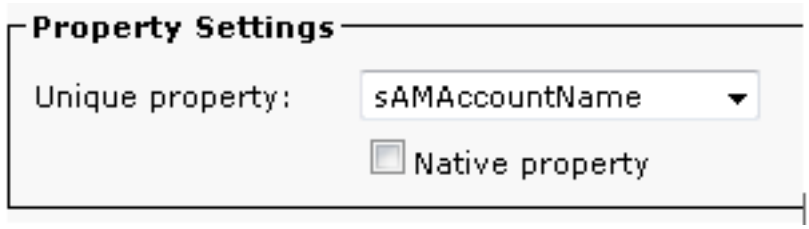
3. 输入Active Directory服务器的配置详细信息：



在本例中，**administrator@aloksin.lab**用于身份验证：



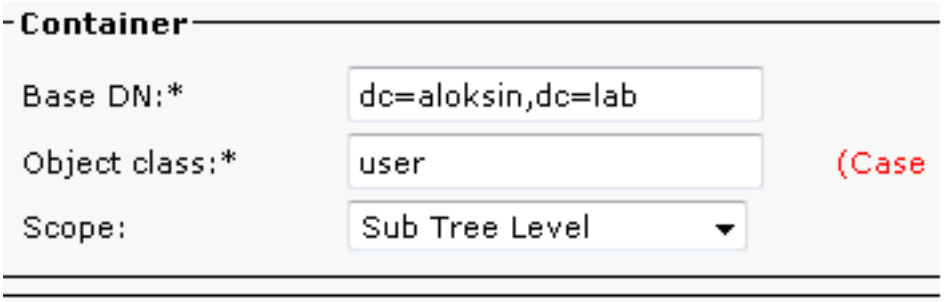
4. 在“属性设置”部分，输入“唯一”属性的配置详细信息，在输入其他详细信息并单击“保存”后，该属性将**显示**。



注意：这是AD中每个条目的唯一值。如果存在重复值，CUAC只提取一个条目。

5. 在“容器”部分，输入基本DN的配置详细信息，即AD中的用户搜索范围。

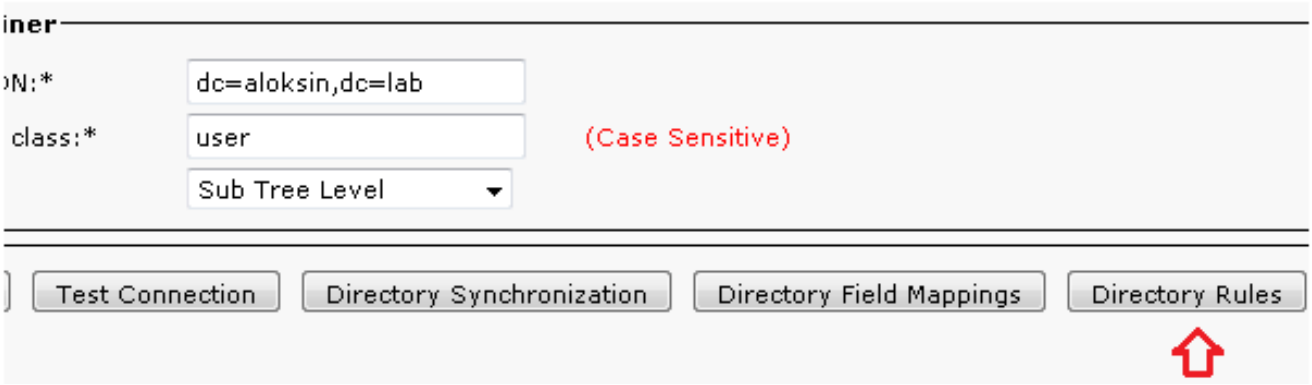
AD使用*Object class*字段来确定请求的搜索范围。默认情况下，它设置为*contact*，这意味着AD在请求的搜索*库*中查找联系人（而非用户）。要在CUAC上导入用户，请将Object类设置更改为**user**:



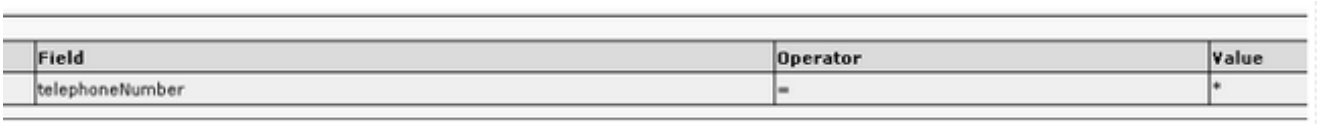
6. 保存设置，单击**目录字段映射**，并配置要为任何用户导入的所有属性。以下是本示例中使用的配置：

Source Fields	Destination Fields	Defaul
telephoneNumber	Extension	
mail	Email	
givenName	First Name	
sn	Last Name	

7. 导航至“目录”源页，然后单击“目录**规则**”:



8. 单击**Add New**并创建规则。添加目录规则时，默认情况下会显示规则过滤器。



注意：无需更改规则过滤器。它会导入所有配置了电话号码的用户。

9. 要配置与AD的自动同步，请单击“目录同步”**选项**卡。

10. 配置现已完成。导航至**Engineering > Service Management**并重新启动LDAP插件以手动启动同步。

CUAC和AD之间的LDAP功能

LDAP进程摘要

以下是CUAC和AD之间的LDAP流程摘要：

1. 两台服务器（CUAC和AD）之间建立了TCP会话。

2. CUAC向AD发送BIND请求，并通过在“身份验证”设置中配置的用户进行身份验证。

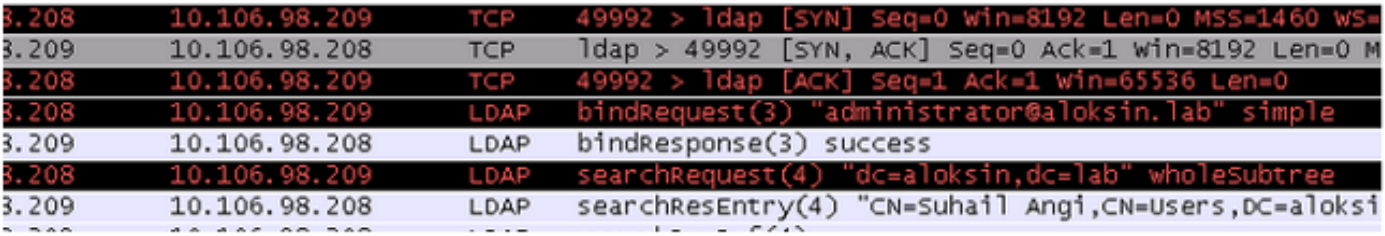
3. AD成功对用户进行身份验证后，会向CUACPE发送BIND Success通知。

4. CUAC向AD发送SEARCH请求，AD包含搜索范围信息、搜索过滤器和任何已过滤用户的属性。

5. AD扫描搜索库中所请求的对象（在“对象类”设置中配置）。它过滤与SEARCH请求消息中详细描述的条件（过滤器）匹配的对象。

6. AD使用搜索结果响应CUAC。

下面是嗅探器捕获，其中说明了以下步骤：



LDAP进程详细信息

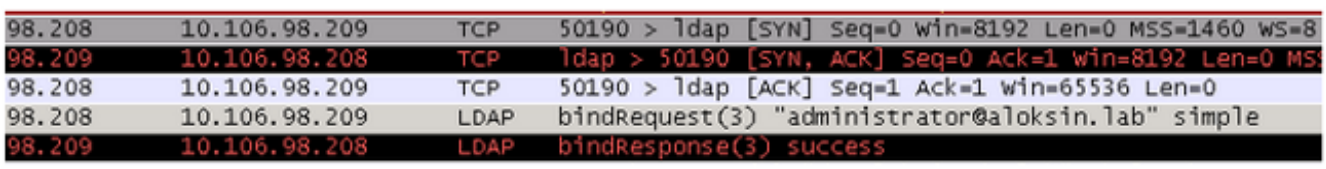
完成CUAC上的配置并重新启动LDAP插件后，CUAC服务器会与AD建立TCP会话。

然后，CUAC发送BIND请求以向AD服务器进行身份验证。如果身份验证成功，AD会向CUAC发送BIND Success响应。这样，两台服务器都尝试在端口389上设置会话，以便同步用户及其信息。

以下是服务器上定义可分辨名称的配置，用于在BIND事务中进行身份验证：

数据包捕获中会显示以下消息：

- 以下是TCP握手，后跟BIND请求：



- 以下是BIND请求的扩展：

```
Lightweight Directory Access Protocol
  LDAPMessage bindRequest(3) "administrator@aloksin.lab" simple
      messageID: 3
    protocolOp: bindRequest (0)
      bindRequest
          version: 3
          name: administrator@aloksin.lab
        authentication: simple (0)
            simple: 6331736330313233 21
[Response To: 81]
```

- 以下是BIND响应的扩展，表示用户(本例中为**管理员**)的身份验证成功：

```
Lightweight Directory Access Protocol
  LDAPMessage bindResponse(3) success
      messageID: 3
    protocolOp: bindResponse (1)
      bindResponse
          resultCode: success (0)
          matchedDN:
          errorMessage:
      [Response To: 80]
      [Time: 0.002077000 seconds]
```

成功绑定后，服务器向AD发送SEARCH请求以导入用户。此SEARCH请求包含AD使用的过滤器和属性。然后，AD在定义的搜索库（如SEARCH请求消息中所详述）中搜索用户，该搜索库满足过滤器和属性验证中的条件。

以下是CUCM发送的SEARCH请求示例：

```
Lightweight Directory Access Protocol
    LDAPMessage searchRequest(2) "dc=aloksin,dc=lab" wholeSubtree
        messageID: 2
        protocolOp: searchRequest (3)
            searchRequest
                baseObject: dc=aloksin,dc=lab
                scope: wholeSubtree (2)
                derefAliases: derefAlways (3)
                sizeLimit: 0
                timeLimit: 0
                typesOnly: False
                Filter: (&(&(objectclass=user)(!(objectclass=Computer)))
(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
                    filter: and (0)
                        and: (&(&(objectclass=user)(!(objectclass=Computer)))
(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
                            and: 3 items
                                Filter: (objectclass=user)
                                    and item: equalityMatch (3)
                                        equalityMatch
                                            attributeDesc: objectclass
                                            assertionValue: user
                                Filter: (!(objectclass=Computer))
                                    and item: not (2)
                                        Filter: (objectclass=Computer)
```

```
                                        not: equalityMatch (3)
                                            equalityMatch
                                                attributeDesc: objectclass
                                                assertionValue: Computer
                                Filter: (!(UserAccountControl:1.2.840.113556.1.4.
803:=2))
                                    and item: not (2)
                                        Filter: (UserAccountControl:1.2.840.113556
.1.4.803:=2)
                                            not: extensibleMatch (9)
                                                extensibleMatch UserAccountControl
                                                    matchingRule: 1.2.840.113556.
1.4.803
                                                    type: UserAccountControl
                                                    matchValue: 2
                                                    dnAttributes: False
            attributes: 15 items
                AttributeDescription: objectguid
                AttributeDescription: samaccountname
                AttributeDescription: givenname
                AttributeDescription: middlename
                AttributeDescription: sn
                AttributeDescription: manager
                AttributeDescription: department
                AttributeDescription: telephonenumber
                AttributeDescription: mail
                AttributeDescription: title
                AttributeDescription: homephone
                AttributeDescription: mobile
                AttributeDescription: pager
                AttributeDescription: msrtcsip-primaryuseraddress
                AttributeDescription: msrtcsip-primaryuseraddress
        [Response In: 103]
        controls: 1 item
            Control
                controlType: 1.2.840.113556.1.4.319 (pagedResultsControl)
                criticality: True
                SearchControlValue
                    size: 250
                    cookie: <MISSING>
```

当AD收到来自CUCM的此请求时，它会在baseObject:**dc=aloksin，dc=lab**，满足滤波器。任何不符合过滤器详细要求的用户都会被排除。AD使用所有已过滤的用户响应CUCM并发送所请求属性的值。

> **注意**：无法导入对象。仅导入用户。这是因为在SEARCH请求消息中发送的过滤器包括**objectclass=user**。因此，AD仅搜索用户，而不搜索联系人。默认情况下，CUCM具有所有这些映射和过滤器。

默认情况下，CUAC未配置；没有配置映射详细信息以导入用户的属性，因此必须手动输入这些详细信息。要创建这些映射，请导航至**系统配置>目录源管理> Active Directory >目录字段映射**。

允许管理员根据自己的要求映射字段。示例如下：

Directory Source

Microsoft Active Directory

Field Mappings

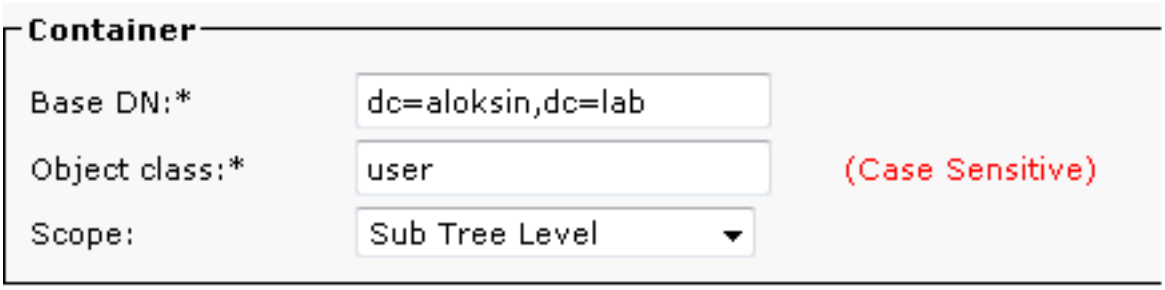
		Source Fields	Destination Fields	Default Value
	Select	telephoneNumber	Extension	
	Select	mail	Email	
	Select	givenName	First Name	
	Select	sn	Last Name	

“源字段”(Source Field)信息将在“搜索请求”(SEARCH request)消息中发送到AD。当AD发送SEARCH响应消息时，这些值存储在CUACPE的目标字段中。

请注意，CUAC默认将“对象类”设置为“联系人”。如果使用此默认设置，则会显示发送到AD的过滤器，如下所示：

```
Filter: (&(&(objectclass=contact)(  ............
```

使用此过滤器，AD从不将任何用户返回到CUACPE，因为它在搜索库中搜索*联系人*，而不是搜索*用户*。因此，必须将对象类更改为**用户**:



到目前为止，CUAC上已配置了以下设置：

- 连接详细信息
- 身份验证（绑定的可分辨用户）
- 容器设置
- 目录映射

在本示例中，Unique属性配置为**sAMAccountName**。如果在CUAC上重新启动LDAP插件并检查SEARCH请求消息，则它不包含除ObjectClass=user以外的任何**属性或过滤器**:

```
Lightweight Directory Access Protocol
   LDAPMessage searchRequest(224) "dc=aloksin,dc=lab" wholeSubtree
       messageID: 224
       protocolOp: searchRequest (3)
           searchRequest
               baseObject: dc=aloksin,dc=lab
               scope: wholeSubtree (2)
               derefAliases: neverDerefAliases (0)
               sizeLimit: 1
               timeLimit: 0
               typesOnly: True
               Filter: (ObjectClass=user)
                   filter: equalityMatch (3)
                       equalityMatch
                           attributeDesc: ObjectClass
                           assertionValue: user
               attributes: 0 items
       [Response In: 43]
```

请注意，此处缺少目录规则。要将联系人与AD同步，必须创建规则。默认情况下，未配置目录规则。一旦创建了过滤器，就已存在过滤器。无需更改过滤器，因为您必须导入所有具有电话号码的用户。

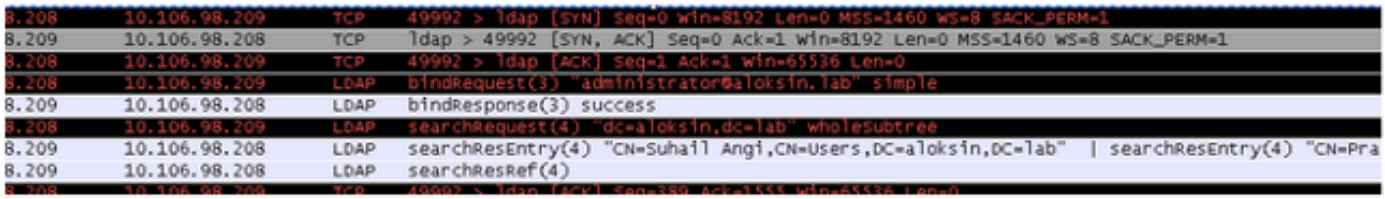
Field	Operator	Val
telephoneNumber	=	*

重新启动LDAP插件以启动与AD的同步并导入用户。以下是来自CUAC的搜索请求：

```
Lightweight Directory Access Protocol
   LDAPMessage searchRequest(4) "dc=aloksin,dc=lab" wholeSubtree
       messageID: 4
       protocolOp: searchRequest (3)
           searchRequest
               baseObject: dc=aloksin,dc=lab
               scope: wholeSubtree (2)
                derefAliases: neverDerefAliases (0)
                sizeLimit: 0
                timeLimit: 15
                typesOnly: False
                Filter: (&(&(objectclass=user)(telephoneNumber=*))
(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
                    filter: and (0)
                        and: (&(&(objectclass=user)(telephoneNumber=*))
(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
                            and: 3 items
                                Filter: (objectclass=user)
                                    and item: equalityMatch (3)
                                        equalityMatch
                                            attributeDesc: objectclass
                                            assertionValue: user
                                Filter: (telephoneNumber=*)
                                    and item: present (7)
                                        present: telephoneNumber
                                Filter: (!(UserAccountControl:1.2.840.113556.
1.4.803:=2))
                                    and item: not (2)
                                        Filter: (UserAccountControl:1.2.840.113556.
1.4.803:=2)
                                            not: extensibleMatch (9)
                                                extensibleMatch UserAccountControl
                                                    matchingRule: 1.2.840.113556.1.
4.803
                                                    type: UserAccountControl
                                                    matchValue: 2
                                                    dnAttributes: False
               attributes: 10 items
                    AttributeDescription: TELEPHONENUMBER
                    AttributeDescription: MAIL
                    AttributeDescription: GIVENNAME
                    AttributeDescription: SN
                    AttributeDescription: sAMAccountName
                    AttributeDescription: ObjectClass
                    AttributeDescription: whenCreated
                    AttributeDescription: whenChanged
                    AttributeDescription: uSNCreated
                    AttributeDescription: uSNChanged
       [Response In: 11405]
       controls: 1 item
           Control
```

```
            controlType: 1.2.840.113556.1.4.319 (pagedResultsControl)
            SearchControlValue
                size: 500
                cookie: <MISSING>
```

如果AD找到与SEARCH请求消息中详细描述的条件匹配的用户，则它会发送包*含用户*信息的SearchResEntry消息。



以下是SearchResEntry消息：

```
Lightweight Directory Access Protocol
   LDAPMessage searchResEntry(4) "CN=Suhail Angi,CN=Users,DC=aloksin,DC=lab" [4 results]
       messageID: 4
       protocolOp: searchResEntry (4)
           searchResEntry
               objectName: CN=Suhail Angi,CN=Users,DC=aloksin,DC=lab
               attributes: 9 items
                   PartialAttributeList item objectClass
                       type: objectClass
                       vals: 4 items
                           top
                           person
                           organizationalPerson
                           user
                   PartialAttributeList item sn
                       type: sn
                       vals: 1 item
                           Angi
                   PartialAttributeList item telephoneNumber
                       type: telephoneNumber
                       vals: 1 item
                           1002
                   PartialAttributeList item givenName
                       type: givenName
                       vals: 1 item
                           Suhail
                   PartialAttributeList item whenCreated
                       type: whenCreated
                       vals: 1 item
                           20131222000850.0Z
                   PartialAttributeList item whenChanged
                       type: whenChanged
                       vals: 1 item
                           20131222023413.0Z
                   PartialAttributeList item uSNCreated
                       type: uSNCreated
                       vals: 1 item
                           12802
                   PartialAttributeList item uSNChanged
                       type: uSNChanged
                       vals: 1 item
                           12843
                   PartialAttributeList item sAMAccountName
                       type: sAMAccountName
                       vals: 1 item
```

```
                        sangi
        [Response To: 11404]
        [Time: 0.001565000 seconds]
Lightweight Directory Access Protocol
   LDAPMessage searchResEntry(4) "CN=Pragathi NS,CN=Users,DC=aloksin,DC=lab" [5 results]
        messageID: 4
        protocolOp: searchResEntry (4)
            searchResEntry
                objectName: CN=Pragathi NS,CN=Users,DC=aloksin,DC=lab
                attributes: 9 items
                    PartialAttributeList item objectClass
                        type: objectClass
                        vals: 4 items
                            top
                            person
                            organizationalPerson
                            user
                    PartialAttributeList item sn
                        type: sn
                        vals: 1 item
                            NS
                    PartialAttributeList item telephoneNumber
                        type: telephoneNumber
                        vals: 1 item
                            1000
                           .......
                           ....{message truncated}..........
                           .....
```

注意：响应中没有MAIL，即使请求了此属性。这是因为AD上的用户未配置邮件ID。

CUAC收到这些值后，会将其存储在结构化查询语言(SQL)表中。然后，您可以登录到控制台，控制台从CUACPE服务器上的此SQL表获取用户列表。