CUAC與Microsoft AD整合

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[將AD與CUAC整合並從AD匯入使用者](#)
[CUAC和AD之間的LDAP功能](#)
[LDAP進程摘要](#)
[LDAP進程詳細資訊](#)

簡介

本檔案將說明輕量型目錄存取通訊協定(LDAP)在Cisco Unified Attendant Console(CUAC)和Microsoft Active Directory(AD)之間運作的方式，以及整合兩個系統時使用的程式。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM
- CUAC
- LDAP
- AD

採用元件

本檔案中的資訊是根據CUAC 10.x版。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

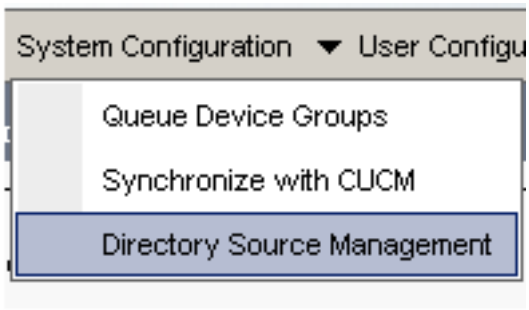
在早期的CUAC版本中，伺服器通過預定義的查詢和過濾器直接從Cisco Unified Communications Manager(CUCM)獲取使用者。通過CUAC高級版(CUACPE)，管理員可以直接從AD整合和匯入使用者。這樣，管理員就可以靈活地實施他們自己選擇和要求的屬性和過濾器。

附註：CUACPE現在已被版本10及更高版本的CUAC高級版取代。

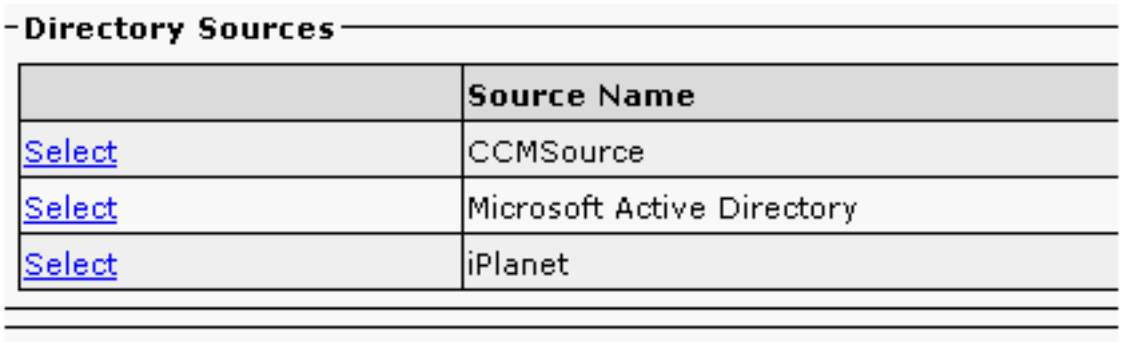
將AD與CUAC整合並從AD匯入使用者

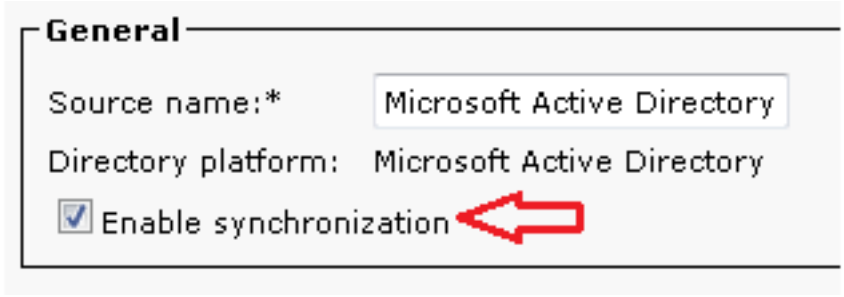
完成以下步驟，以便將CUAC與AD整合並從AD匯入使用者：

1. 在CUAC上為AD啟用目錄同步。

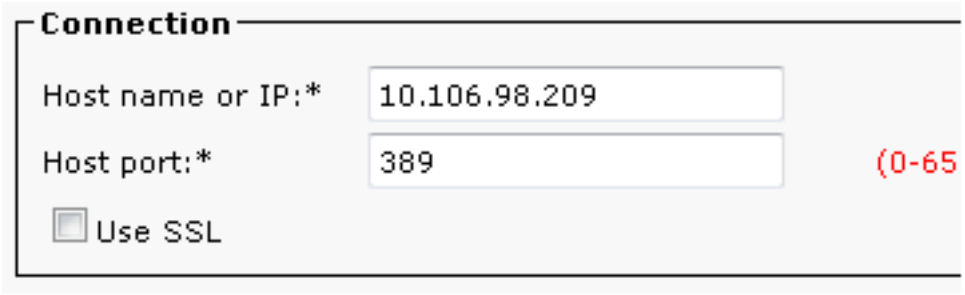


2. 選擇**Microsoft Active Directory**並選中**Enable synchronization**覈取方塊：

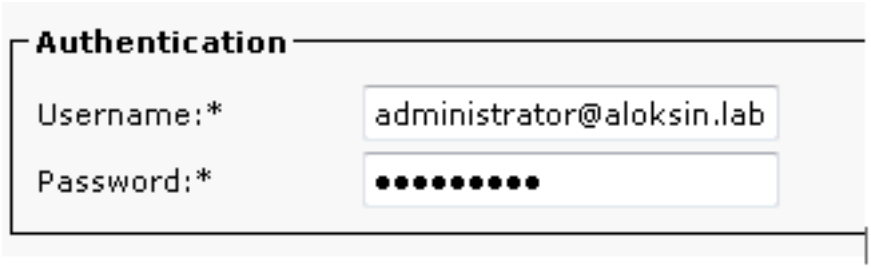




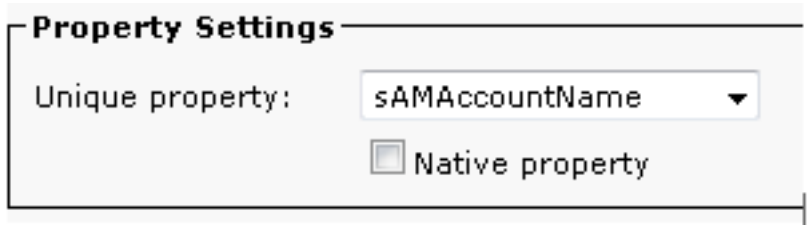
3. 輸入Active Directory伺服器的配置詳細資訊：



在本示例中，**administrator@aloksin.lab**用於身份驗證：



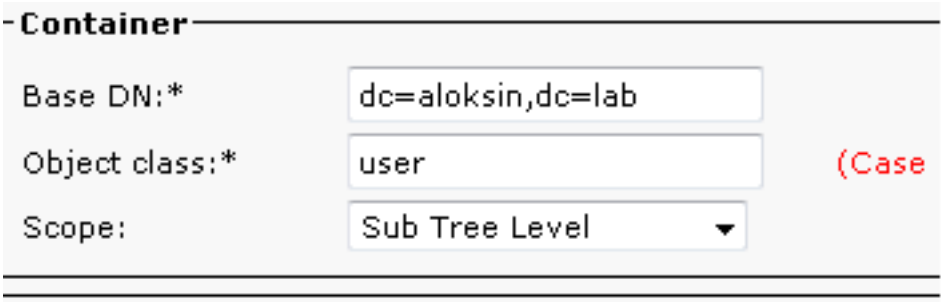
4. 在「屬性設定」部分中，輸入「唯一屬性」的配置詳細資訊，當您輸入其他詳細資訊並按一下**儲存**後，就會出現該屬性。



附註：這是AD中每個條目的唯一值。如果有重複值，則CUAC僅提取一個條目。

5. 在Container部分，輸入基礎DN的配置詳細資訊，該基礎是AD中的使用者搜尋範圍。

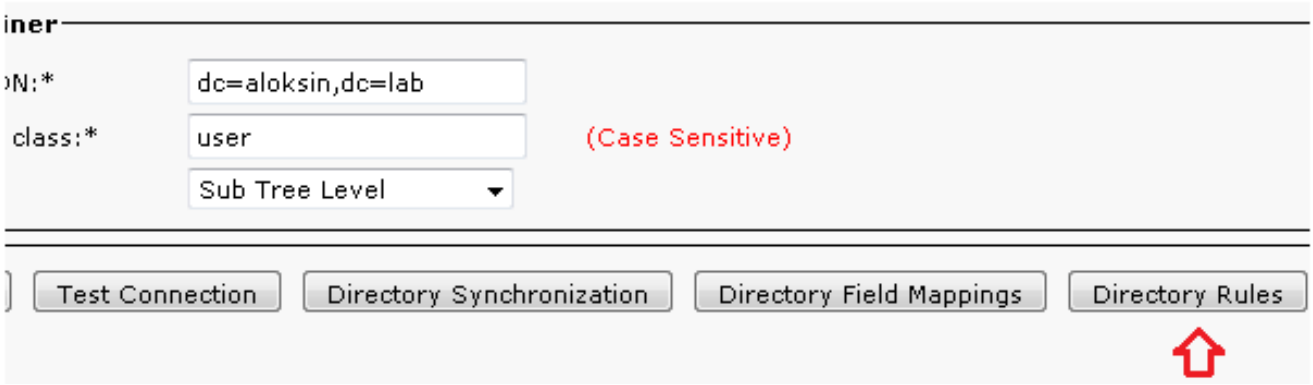
AD使用*Object class*欄位來確定請求的搜尋範圍。預設情況下，設定為*contact*，這表示AD在請求的搜尋庫中查詢*contact*（非使用者）。若要在CUAC上導入使用者，請將Object類設定更改為**user**:



6. 儲存設定，按一下**目錄欄位對映**，然後配置您要為任何使用者匯入的所有屬性。本示例中使用的配置如下：

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

7. 導航到「目錄」源頁，然後按一下**目錄規則**:



8. 按一下**Add New**並建立規則。新增目錄規則時，預設情況下將顯示規則過濾器。

	Field	Operator	Value
	telephoneNumber	=	*

附註：無需更改規則過濾器。它匯入已配置電話號碼的所有使用者。

9. 若要配置與AD的自動同步，請按一下**Directory Synchronization**頁籤。

10. 配置現在已完成。導航到**工程>服務管理**，然後重新啟動LDAP外掛以手動啟動同步。

CUAC和AD之間的LDAP功能

LDAP進程摘要

以下是CUAC和AD之間的LDAP進程的摘要：

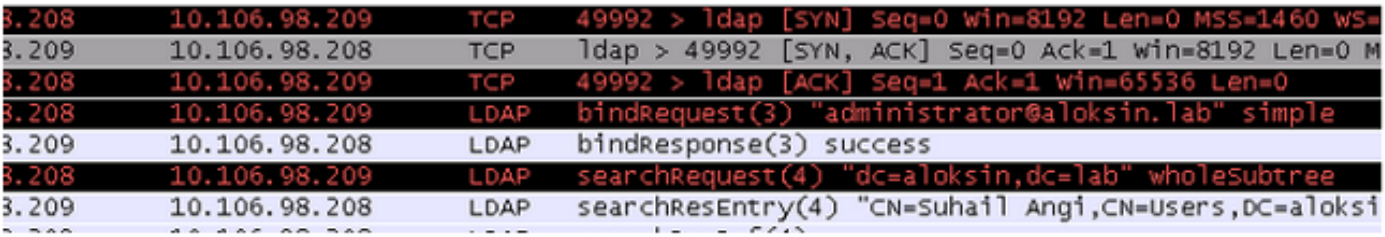
1. 兩台伺服器（CUAC和AD）之間已建立TCP作業階段。
2. CUAC向AD傳送BIND請求，並通過在身份驗證設定中配置的使用者進行身份驗證。
3. AD成功驗證使用者後，會向CUACPE傳送繫結成功通知。

4. CUAC向AD傳送SEARCH請求，AD具有搜尋範圍資訊、搜尋過濾器和任何已過濾使用者的屬性。

5. AD掃描搜尋庫中請求的對象（在「對象類」設定中配置）。它過濾掉與SEARCH請求消息中詳細列出的條件（過濾器）匹配的對象。

6. AD使用搜尋結果響應CUAC。

以下是說明這些步驟的監聽器擷取：

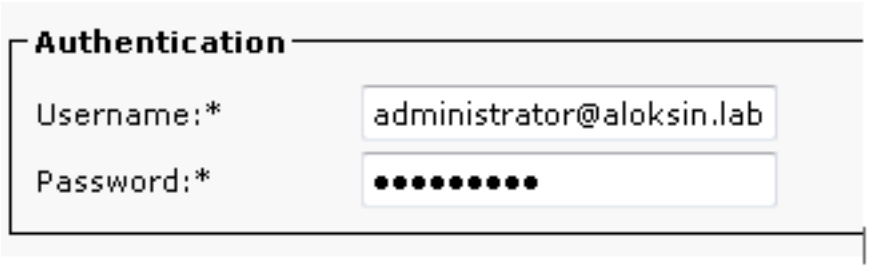


LDAP進程詳細資訊

完成CUAC上的配置並重新啟動LDAP外掛後，CUAC伺服器會與AD建立TCP會話。

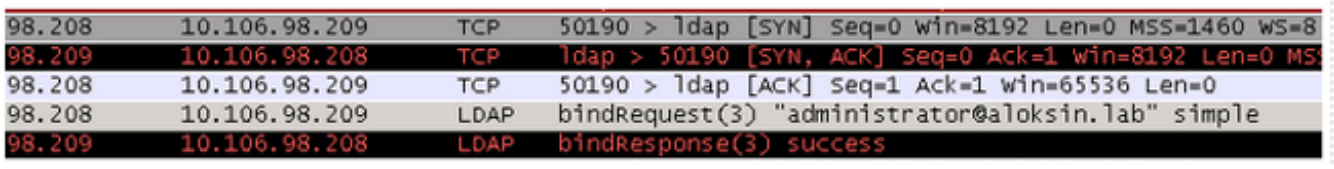
CUAC然後傳送BIND請求以便向AD伺服器進行身份驗證。如果驗證成功，AD會向CUAC傳送BIND Success響應。這樣，兩台伺服器都會嘗試在埠389上設定會話，以同步使用者及其資訊。

以下是伺服器上用於定義BIND事務中身份驗證的可分辨名稱的配置：

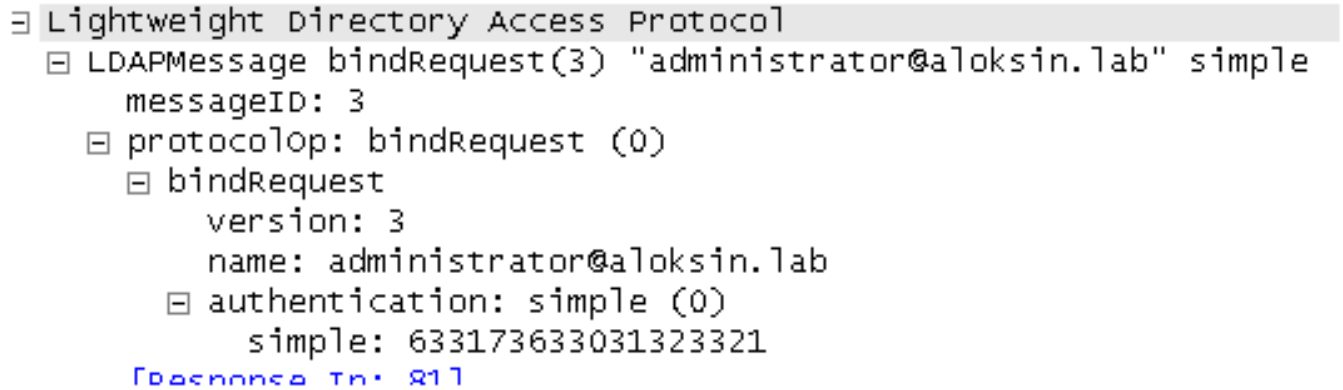


這些訊息會顯示在封包擷取中：

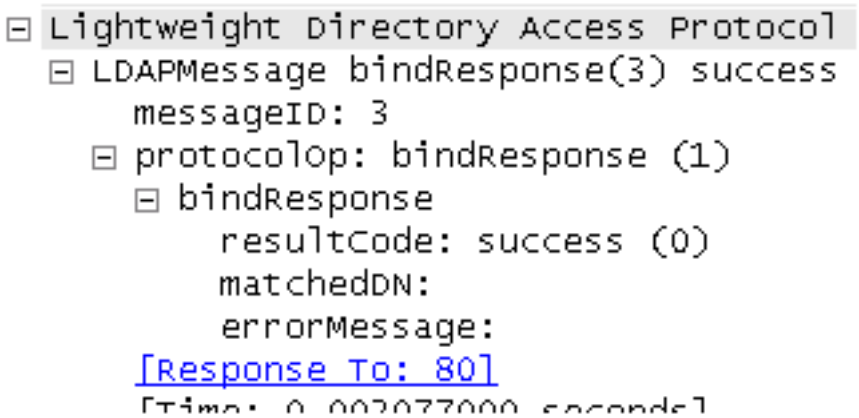
- 以下是TCP握手，然後是BIND請求：



- 以下是BIND請求的擴展：



- 以下是BIND響應的擴展，指示使用者(在本例中為**administrator**)身份驗證成功：



成功繫結後，伺服器會向AD傳送SEARCH請求以匯入使用者。此SEARCH請求包含AD使用的過濾器和屬性。然後，AD在定義的搜尋庫（如在SEARCH請求消息中詳述）內搜尋使用者，其滿足過濾器和屬性驗證中的標準。

以下是CUCM傳送的SEARCH請求示例：

```
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>
```

當AD從CUCM收到此請求時，它會在baseObject中搜尋**使用者：dc=aloksin，dc=lab，**滿足濾波條件。任何不符合篩選器所詳細要求的使用者都會被排除在外。AD用所有過濾的使用者響應CUCM並傳送請求的屬性的值。

> **附註**：無法匯入對象。僅匯入*使用者*。這是因為在SEARCH請求消息中傳送的過濾器包括**objectclass=user**。因此，AD僅搜尋使用者，而非聯絡人。預設情況下，CUCM具有所有這些對映和一個過濾器。

預設情況下未配置CUAC;沒有為使用者匯入屬性配置對映詳細資訊，因此您必須手動輸入這些詳細資訊。要建立這些對映，請導航到**系統配置>目錄源管理> Active Directory >目錄欄位對映**。

管理員可以根據自己的要求對映欄位。以下是範例：

Directory Source

Microsoft Active Directory

Field Mappings

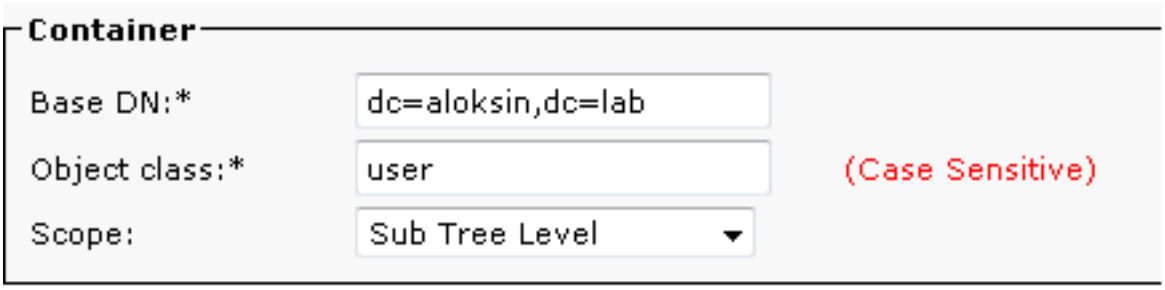
		Source Fields	Destination Fields	Default Value
☐	Select	telephoneNumber	Extension	
☐	Select	mail	Email	
☐	Select	givenName	First Name	
☐	Select	sn	Last Name	

在SEARCH請求消息中向AD傳送源欄位資訊。當AD傳送SEARCH響應消息時，這些值將儲存在CUACPE上的目標欄位中。

請注意，CUAC預設將Object Class設定為*contacts*。如果使用此預設設定，則傳送到AD的過濾器將顯示如下：

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

使用此過濾器，AD不會將任何使用者返回到CUACPE，因為它在搜尋庫*中搜*索聯絡人，而不是*使用者*。因此，必須將對象類更改為**user**:



到目前為止，已在CUAC上配置以下設定：

- 連線詳細資訊
- 身份驗證（用於繫結的可分辨使用者）
- 容器設定
- 目錄對映

在本示例中，Unique屬性配置為**sAMAccountName**。如果您在CUAC上重新啟動LDAP外掛並檢查SEARCH請求消息，則除了**ObjectClass=user**之外，該外掛不包含任何屬性或**篩選器：**

```
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]
```

請注意，此處缺少目錄規則。若要將聯絡人與AD同步，必須建立規則。預設情況下，沒有配置目錄規則。一旦建立了一個篩選器，就會出現該篩選器。無需更改篩選器，因為必須匯入具有電話號碼的所有使用者。

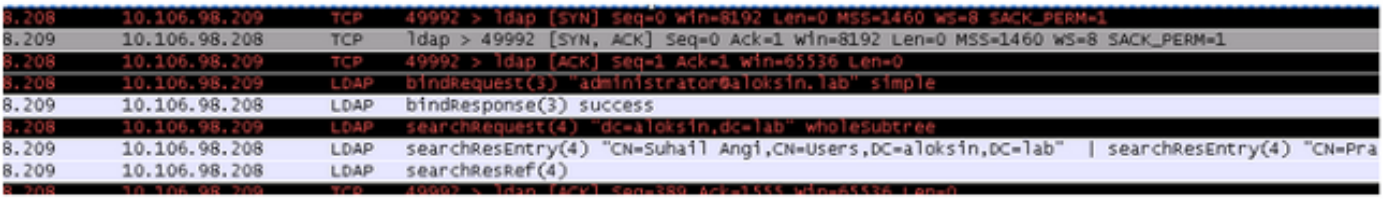
Field	Operator	Val
telephoneNumber	=	*

重新啟動LDAP外掛以啟動與AD的同步並匯入使用者。以下是來自CUAC的SEARCH請求：

```
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找到與SEARCH請求消息中詳述的條件相匹配的使用者，則會傳送包含使用者資訊的*SearchResEntry*消息。



以下是SearchResEntry訊息：

```
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}..........
                          .....
```

附註：響應中沒有郵件，即使已請求此屬性。這是因為未為AD上的使用者配置郵件ID。

CUAC收到這些值後，會將這些值儲存在結構化查詢語言(SQL)表中。然後，您可以登入到控制檯，控制檯從CUACPE伺服器上的此SQL表中提取使用者清單。