Microsoft AD と CUAC の統合

内容

概要

このドキュメントでは、Lightweight Directory Access Protocol(LDAP)がCisco Unified Attendant Console(CUAC)とMicrosoft Active Directory(AD)の間で動作する方法、および2つのシステムを統合するために使用する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- CUCM
- CUAC
- [LDAP]
- [AD]

使用するコンポーネント

このドキュメントの情報は、CUACバージョン10.xに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

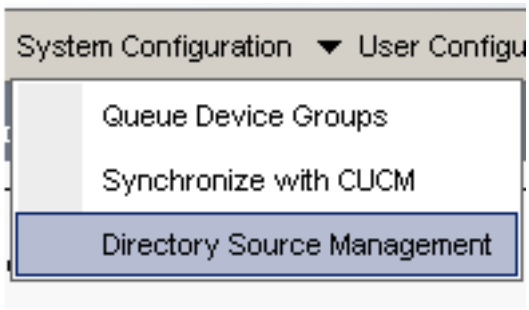
以前のバージョンのCUACでは、サーバは事前定義されたクエリーとフィルタを介してCisco Unified Communications Manager(CUCM)からユーザを直接取得します。CUAC Premium Edition(CUACPE)を使用すると、管理者はADからユーザを直接統合およびインポートできます。これにより、管理者は独自の選択と要件の属性とフィルタを柔軟に実装できます。

注：CUACPEは、バージョン10以降のCUAC Advanced Editionに置き換えられました。

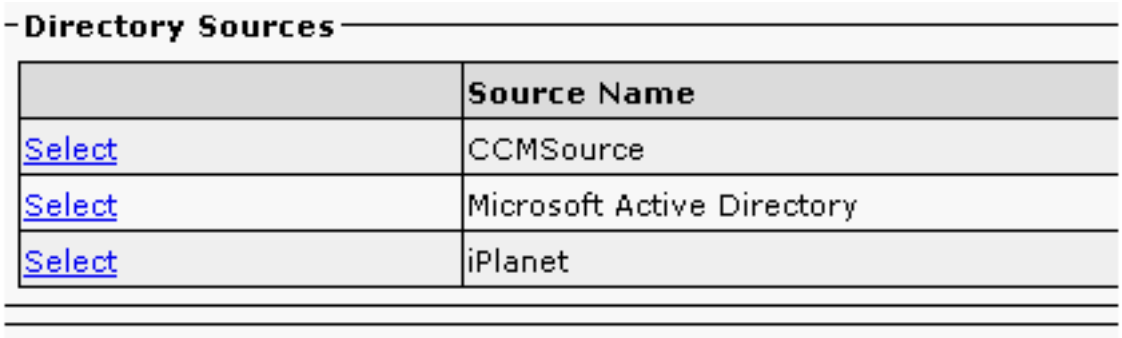
ADとCUACの統合およびADからのユーザのインポート

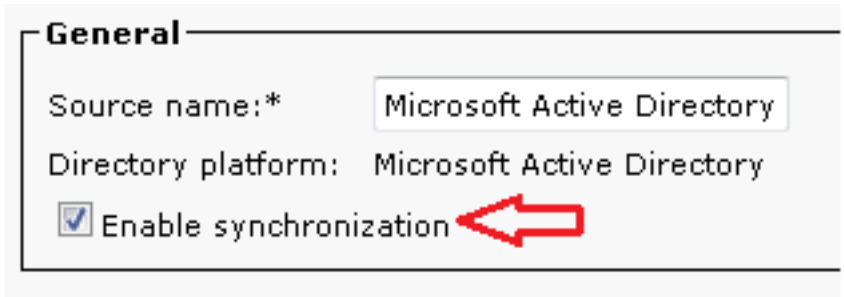
CUACをADと統合し、ADからユーザをインポートするには、次の手順を実行します。

1. CUACでADのディレクトリ同期を有効にします。

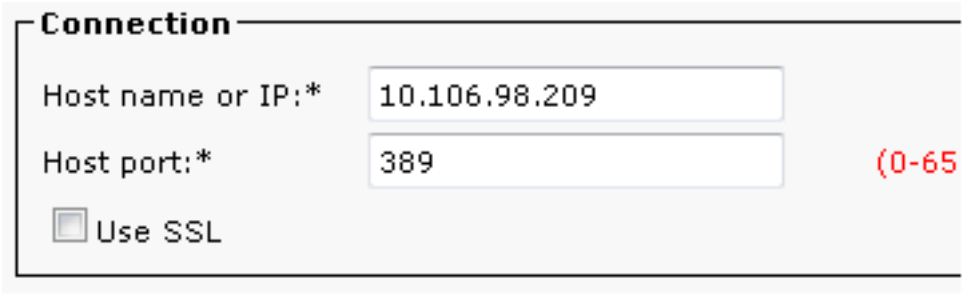


2. [Microsoft Active Directory]を選択し、[同期を有効にする]チェックボックスをオンにします。

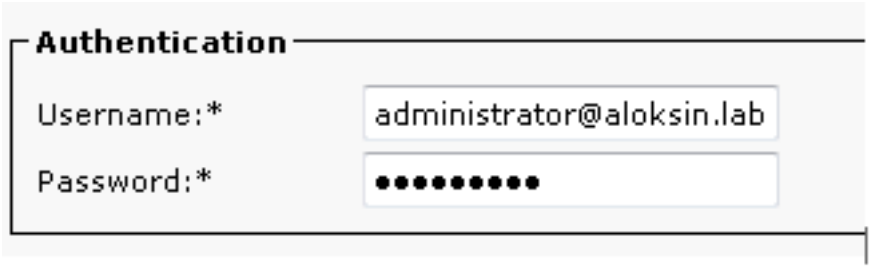




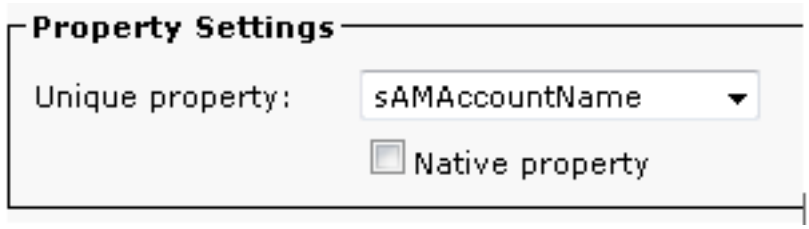
3. Active Directoryサーバの設定の詳細を入力します。



この例では、administrator@aloksin.labが認証に使用されます。



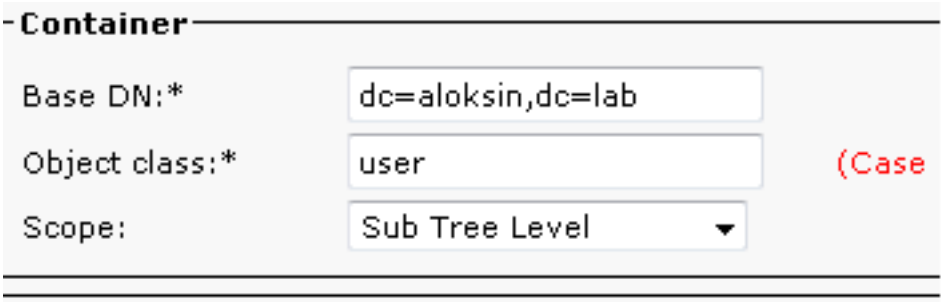
4. [プロパティの設定]セクションで、[固有]プロパティの設定の詳細を入力します。この詳細は、他の詳細を入力して[保存]をクリックします。



注：これは、ADの各エントリに固有の値です。重複する値がある場合、CUACは1つのエントリのみを取得します。

5. [Container]セクションで、ベースDNの設定の詳細を入力します。これは、ADのユーザ検索スコープです。

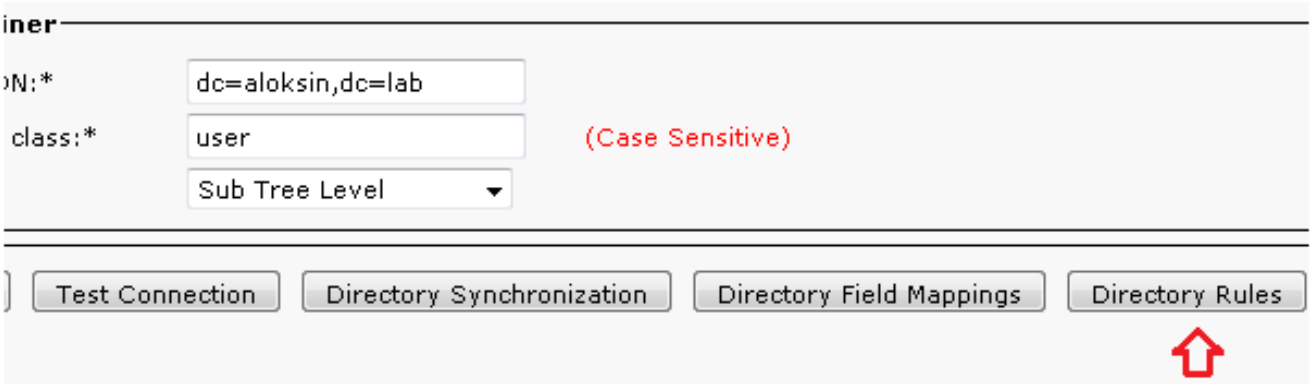
Object classフィールドは、要求された検索範囲を決定するためにADによって使用されます。デフォルトではcontactに設定されています。これは、ADが要求された検索ベースで連絡先（ユーザではない）を検索することを意味します。CUACでユーザをインポートするには、Objectクラスの設定をuserに変更します。



6. 設定を保存し、[Directory Field Mappings]をクリックして、任意のユーザーにインポートするすべての属性を設定します。この例で使用する設定は次のとおりです。

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

7. ディレクトリ・ソース・ページに移動し、「ディレクトリ・ルール」をクリックします。



8. [新しい追加]をクリックし、ルールを作成します。ディレクトリルールを追加すると、デフォルトでルールフィルタが表示されます。

Field	Operator	Value
telephoneNumber	=	*

注：ルールフィルタを変更する必要はありません。電話番号が設定されているすべてのユーザがインポートされます。

9. ADとの自動同期を設定するには、[Directory Synchronization]タブをクリックします。

10. 設定はこれで完了しました。[Engineering] > [Service Management]に移動し、LDAPプラグインを再起動して、手動で同期を開始します。

CUACとAD間のLDAP機能

LDAPプロセスの概要

CUACとADの間のLDAPプロセスの要約を次に示します。

1. 2台のサーバ（CUACとAD）間でTCPセッションが確立されます。

2. CUACはADにバインド要求を送信し、認証設定で設定されたユーザを介して認証します。

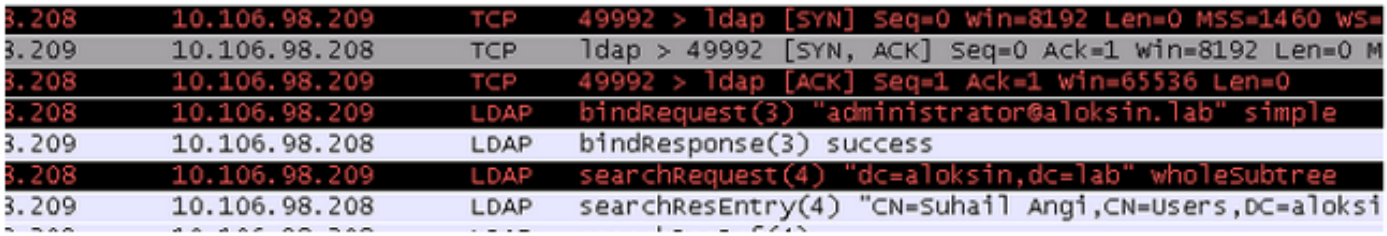
3. ADがユーザの認証に成功すると、CUACPEにBIND Success通知を送信します。

4. CUACはADにSEARCH要求を送信します。ADには、検索範囲の情報、検索のフィルタ、フィルタリングされたユーザの属性が含まれます。

5. ADは、検索ベースで要求されたオブジェクト（オブジェクトクラス設定で設定）をスキャンします。SEARCH要求メッセージで詳細に指定された条件（フィルタ）に一致するオブジェクトを除外します。

6. ADは検索結果をCUACに返します。

次の手順を示すスニファキャプチャを次に示します。

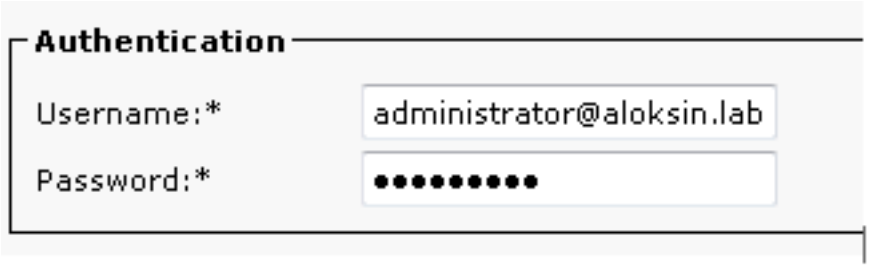


LDAPプロセスの詳細

CUACの設定が完了し、LDAPプラグインが再起動すると、CUACサーバはADとのTCPセッションをセットアップします。

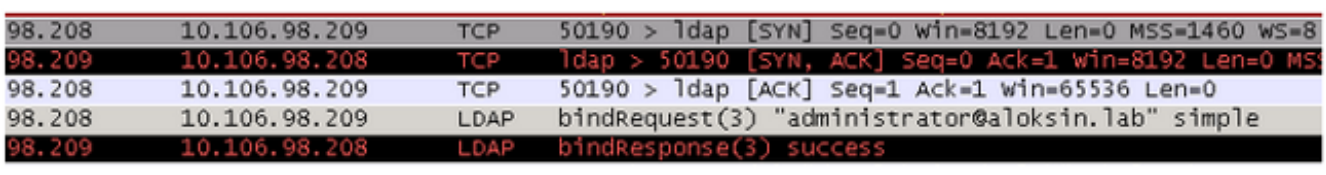
次に、CUACはADサーバで認証するためにバインド要求を送信します。認証が成功すると、ADはCUACにBIND Success応答を送信します。これにより、両方のサーバがユーザとその情報を同期するために、ポート389にセッションをセットアップしようとします。

BINDトランザクションの認証に使用される識別名(DN)を定義するサーバの設定を次に示します。

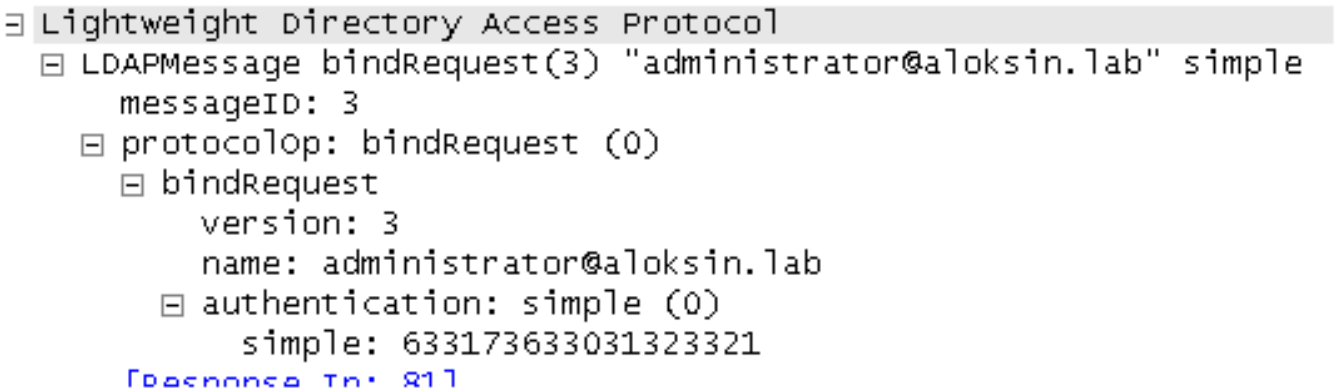


次のメッセージがパケットキャプチャに表示されます。

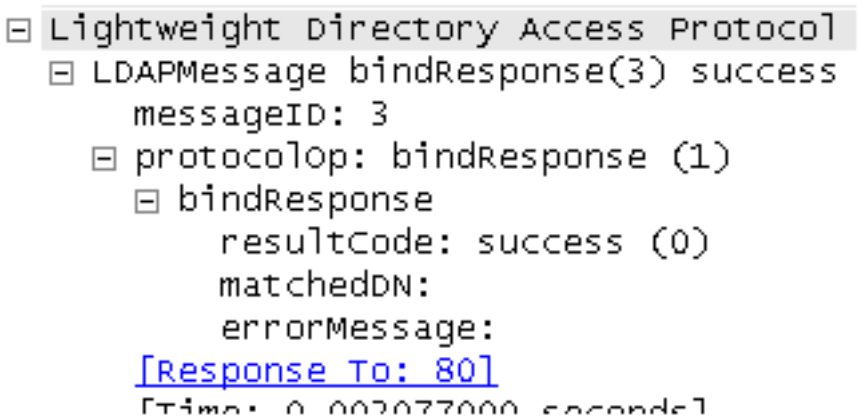
- 次にTCPハンドシェイクとバインド要求を示します。



- 次に、バインド要求の拡張を示します。



- 次に、BIND応答の拡張を示します。これは、ユーザ(この例ではadministrator)の正常な認証を示します。



バインドが成功すると、サーバはユーザをインポートするためにADにSEARCH要求を送信します。このSEARCH要求には、ADで使用されるフィルタと属性が含まれます。次に、ADは定義された検索ベース内で（SEARCH要求メッセージで詳細に説明されているように）ユーザを検索し、フィルタと属性検証の基準を満たします。

CUCMによって送信されるSEARCH要求の例を次に示します。

```
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>
```

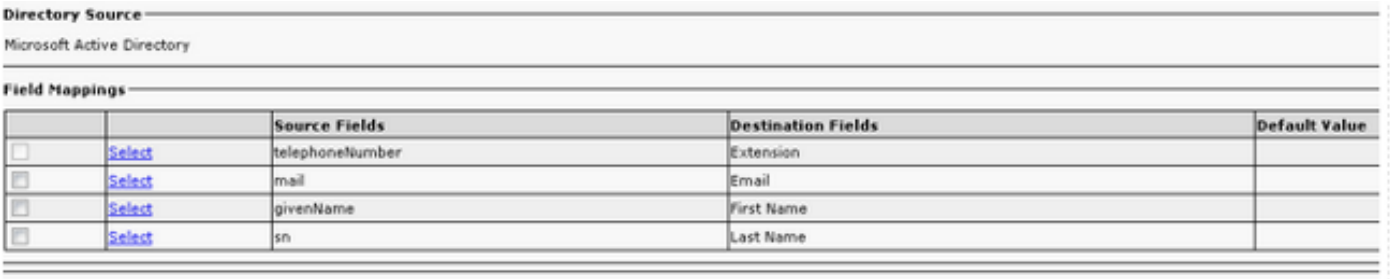
ADは、CUCMからこの要求を受信すると、baseObject内のユーザを検索します。dc=aloksin,dc=lab,フィルタを満たす。フィルタで詳細に指定された要件を満たしていないユーザは除外されます。ADは、フィルタリングされたすべてのユーザでCUCMに応答し、要求された属性の値を送信します。

> **注**：オブジェクトをインポートできません。ユーザーのみがインポートされます。これは、SEARCH要求メッセージで送信されるフィルタにobjectclass=userが含まれているためです。したがって、ADはユーザのみを検索し、連絡先は検索しません。CUCMには、これらのマッピングとデフォルトのフィルタがすべて含まれています。

CUACはデフォルトでは設定されていません。ユーザの属性をインポートするために設定されたマッピング詳細がないため、これらの詳細を手動で入力する必要があります。これらのマッピングを作成するには、[System Configuration] > [Directory Source Management] > [Active Directory]

> [Directory Field Mapping]に移動します。

管理者は、各自の要件に従ってフィールドをマッピングできます。以下が一例です。



Directory Source

Microsoft Active Directory

Field Mappings

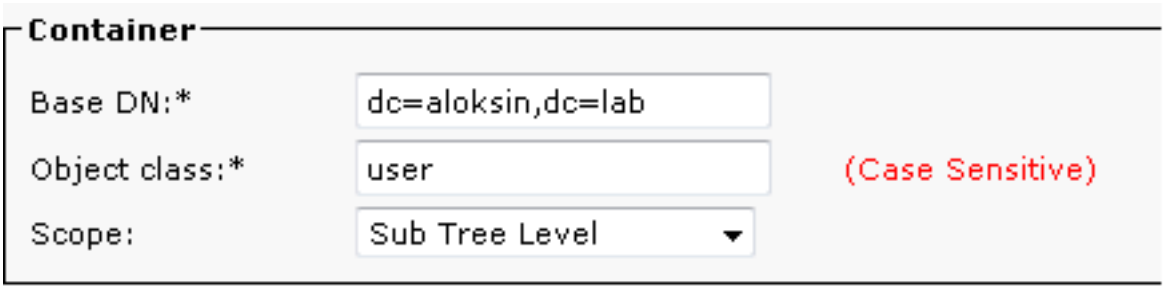
		Source Fields	Destination Fields	Default Value
☐	Select	telephoneNumber	Extension	
☐	Select	mail	Email	
☐	Select	givenName	First Name	
☐	Select	sn	Last Name	

ソースフィールド情報は、SEARCH要求メッセージでADに送信されます。ADがSEARCH応答メッセージを送信すると、これらの値はCUACPEの宛先フィールドに格納されます。

CUACでは、デフォルトで[オブジェクトクラス]が[接触]に設定されていることに注意してください。このデフォルト設定を使用すると、ADに送信されるフィルタが次のように表示されます。

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

このフィルタを使用すると、ADはユーザをCUACPEに返しません。これは、ユーザではなく検索ベースで連絡先を検索するためですからです。このため、[オブジェクトクラス]を[ユーザ]に変更する必要**があります**。



Container

Base DN:* dc=aloksin,dc=lab

Object class:* user (Case Sensitive)

Scope: Sub Tree Level

ここまでは、CUACで次の設定が行われています。

- 接続の詳細
- 認証（バインディング用の識別ユーザ）
- コンテナの設定
- ディレクトリマッピング

この例では、 Uniqueプロパティは**sAMAccountNameとして設定されています**。CUACでLDAPプラグインを再起動し、SEARCH要求メッセージを確認すると、**ObjectClass=user**以外の属性またはフィルタは含まれ**ません**。

```
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]
```

ここではディレクトリ規則が欠落していることに注意してください。連絡先をADと同期するには、ルールを作成する必要があります。デフォルトでは、ディレクトリルールは設定されていません。作成されたフィルタは既に存在します。電話番号を持つすべてのユーザーをインポートする必要があるため、フィルタを変更する必要はありません。

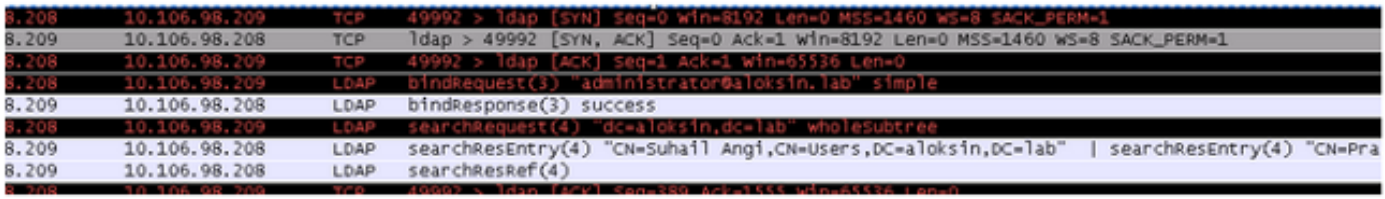
Field	Operator	Val
telephoneNumber	=	*

ADとの同期を開始し、ユーザをインポートするには、LDAPプラグインを再起動します。CUACからのSEARCH要求を次に示します。

```
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>
```

ADがSEARCH要求メッセージに詳細な条件を満たすユーザーを検出すると、そのユーザー情報を含むSearchResEntryメッセージを送信します。



SearchResEntryメッセージは次のとおりです。

```
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：この属性が要求されていても、応答にMAILはありません。これは、ADのユーザに対してメールIDが設定されていないためです。

これらの値がCUACによって受信されると、CUACは構造化クエリ言語(SQL)テーブルに格納します。その後、コンソールにログインし、コンソールがCUACPEサーバ上のこのSQLテーブルからユーザリストを取得します。