CUAC-integratie met Microsoft AD

Inhoud

[Inleiding](#)
[Voorwaarden](#)
[Vereisten](#)
[Gebruikte componenten](#)
[Achtergrondinformatie](#)
[AD met CUAC integreren en gebruikers importeren uit AD](#)
[LDAP-functies tussen CUAC en AD](#)
[LDAP-processamenvatting](#)
[LDAP-procesdetails](#)

Inleiding

Dit document beschrijft de manier waarop Lichtgewicht Directory Access Protocol (LDAP) werkt tussen de Cisco Unified Attendant Console (CUAC) en de Microsoft Active Directory (AD) en de procedures die worden gebruikt om de twee systemen te integreren.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- CUCM
- CUAC
- LDAP
- AD

Gebruikte componenten

De informatie in dit document is gebaseerd op CUAC versie 10.x.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

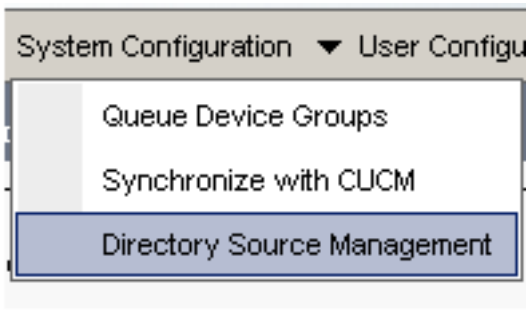
In vroegere CUAC-versies, verkrijgt de server gebruikers rechtstreeks van Cisco Unified Communications Manager (CUCM) via vooraf gedefinieerde vragen en filters. Met de CUAC Premium Edition (CUACPE) mogen beheerders gebruikers rechtstreeks vanuit de AD integreren en importeren. Dit biedt beheerders flexibiliteit voor de implementatie van eigenschappen en filters van hun eigen keuze en vereisten.

> **Opmerking:** CUACPE is nu vervangen door CUAC Advanced Edition voor versies 10 en hoger.

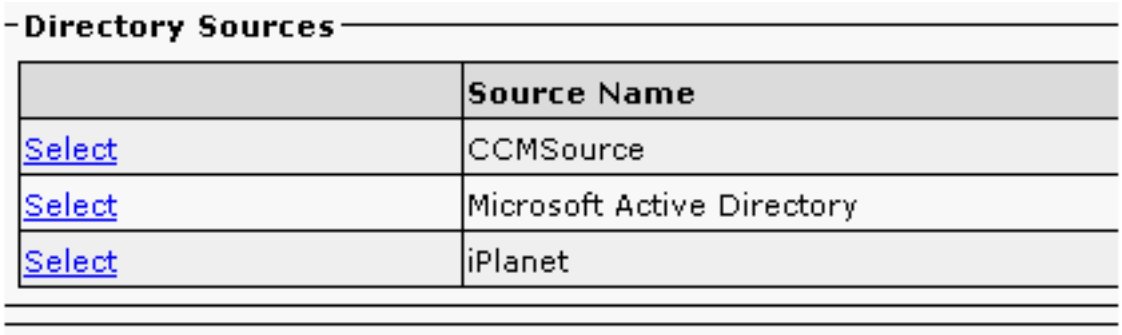
AD met CUAC integreren en gebruikers importeren uit AD

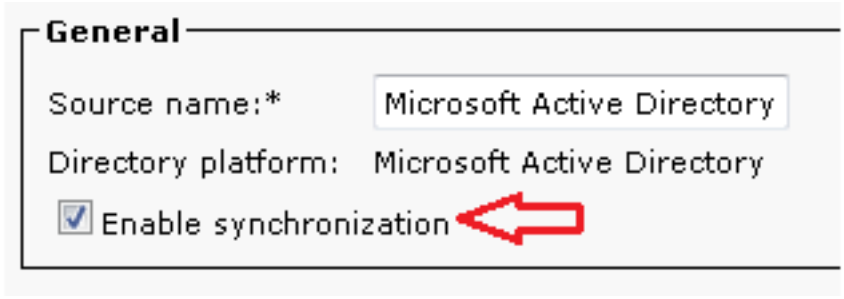
Voltooi deze stappen om de CUAC te integreren met de AD en om gebruikers te importeren uit de AD:

1. Synchronisatie van map voor AD in de CUAC inschakelen.

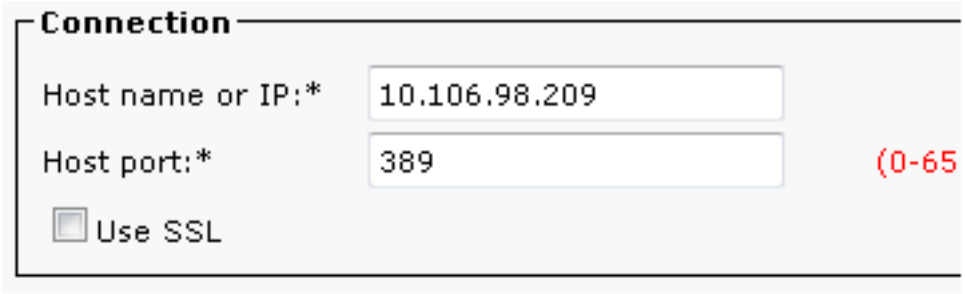


2. Selecteer **Microsoft Active Directory** en controleer het dialoogvenster **synchroniseren** inschakelen:

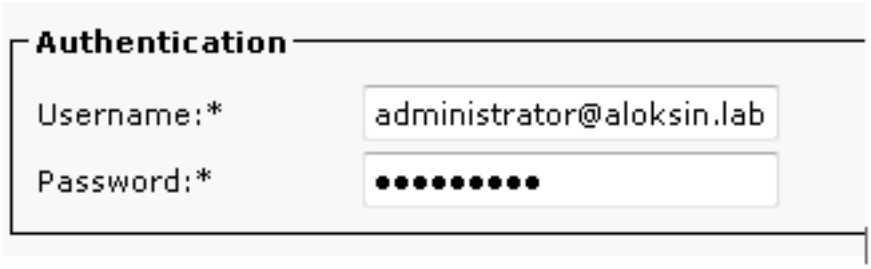




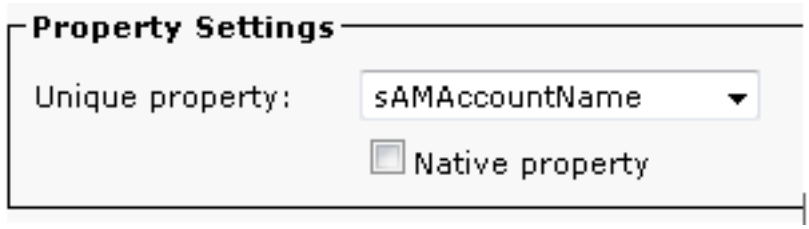
3. Voer de configuratiegegevens in voor de Active Directory Server in:



Bijvoorbeeld, **administrator@aloksin.lab** wordt gebruikt voor authenticatie:



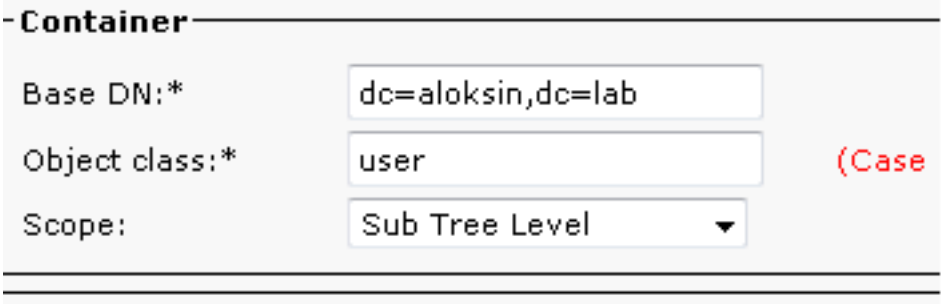
4. Typ in het gedeelte Eigenschap Settings de configuratiegegevens voor de unieke eigenschap, die weergegeven wordt zodra u de andere details hebt ingevoerd en op **Opslaan** klikt.



Opmerking: Dit is een unieke waarde voor elke vermelding in het AD. Als er dubbele waarden zijn, trekt CUAC slechts één ingang in.

5. In de sectie van de container, voer de configuratiedetails voor Base DN in, wat het gebruikerszoekbereik in de AD is.

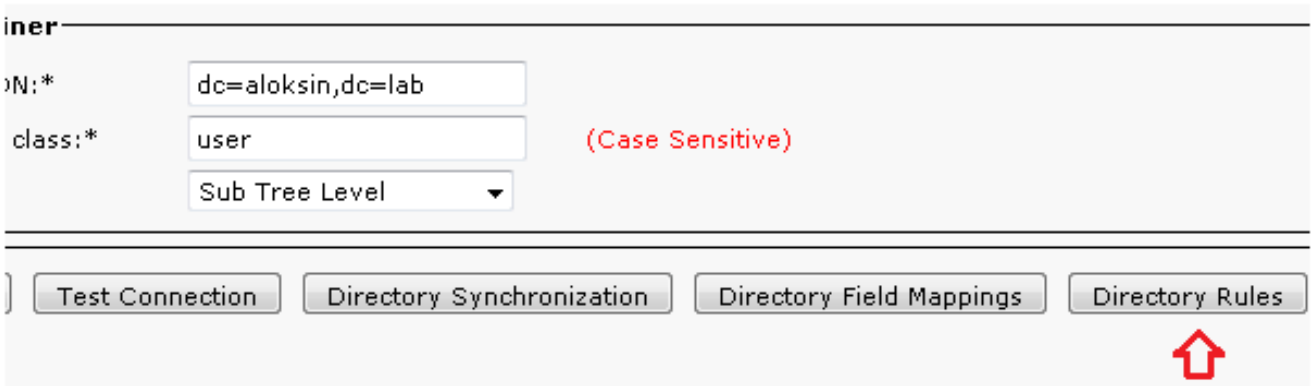
   Het veld *Objectklasse* wordt door de AD gebruikt om het gevraagde zoekbereik te bepalen. Standaard wordt het ingesteld op *contact*, wat betekent dat de AD *contacten* (niet gebruikers) in de gevraagde zoekbasis zoekt. Als u *gebruikers* in de CUAC wilt importeren, wijzigt u de instelling Objectklasse in **gebruiker**:



6. Sla de instellingen op, klik op **Directory Field mapping** en stel alle eigenschappen in die u voor een willekeurige gebruiker wilt importeren. Dit is de configuratie die in dit voorbeeld wordt gebruikt:

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

7. navigeren naar de bronpagina van de map en klik op **directory Regels**:



8. Klik op **Nieuw toevoegen** en maak een regel. Wanneer u een directory regel toevoegt, verschijnt standaard een regelfilter.

	Field	Operator	Value
	telephoneNumber	=	*

Opmerking: Het regelfilter hoeft niet te worden gewijzigd. Het importeert alle gebruikers die een telefoonnummer hebben ingesteld.

9. Om auto-sync met de AD te configureren klikt u op het tabblad **Map synchroniseren**.

10. De configuratie is nu voltooid. Navigeer naar **Engineering > Service Management** en start de LDAP plug-in opnieuw om de sync handmatig te starten.

LDAP-functies tussen CUAC en AD

LDAP-processamenvatting

Hier volgt een samenvatting van het proces van LDAP tussen de CUAC en de AD:

1. Er wordt een TCP-sessie ingesteld tussen de twee servers (CUAC en AD).

2. CUAC stuurt een BIND-aanvraag naar de AD en authenticeert deze via de gebruiker die ingesteld is in de verificatie-instellingen.

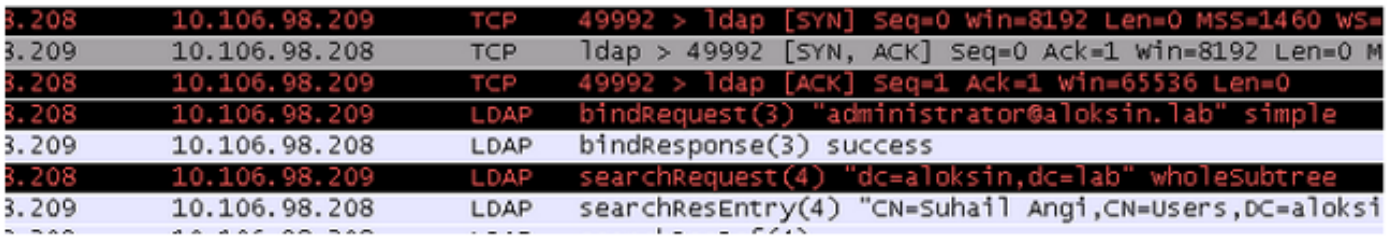
3. Zodra de AD met succes de gebruiker authentiek heeft verklaard, stuurt het een bericht van het BIND Succes aan CUACPE.

4. De CUAC stuurt een ZOEKaanvraag naar de AD met de informatie over de zoekscope, filters voor de zoekfunctie en eigenschappen voor een gefilterde gebruiker.

5. De AD scans voor het gevraagde object (ingesteld in de instellingen van de klasse van object) in de zoekbasis. Het filtreert voorwerpen uit die overeenkomen met de criteria (filter) die in het ZOEKEN-verzoekbericht worden beschreven.

6. Het AD reageert op de CUAC met de zoekresultaten.

Hier volgt een fragment van de sluipschutter die deze stappen illustreert:

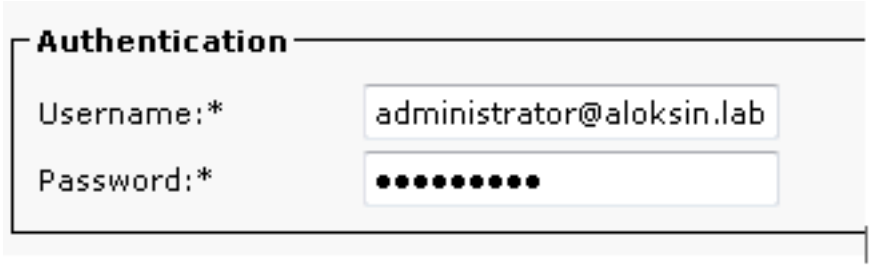


LDAP-procesdetails

Nadat de configuratie op CUAC is voltooid en de LDAP-stekker opnieuw wordt gestart, stelt de CUAC-server een TCP-sessie met de AD in.

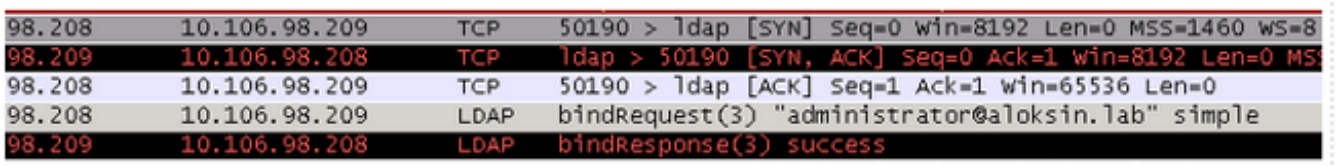
De CUAC stuurt vervolgens een BIND-aanvraag om zich te kunnen authentiseren met de AD-server. Als de authenticatie succesvol is, stuurt de AD een BIND Success antwoord op de CUAC. Met dit resultaat proberen beide servers een sessie op poort 389 op te zetten om gebruikers en hun informatie te synchroniseren.

Hier is de configuratie op de server die de Gedifferentieerde naam definieert, die gebruikt wordt voor authenticatie in de BIND-transactie:

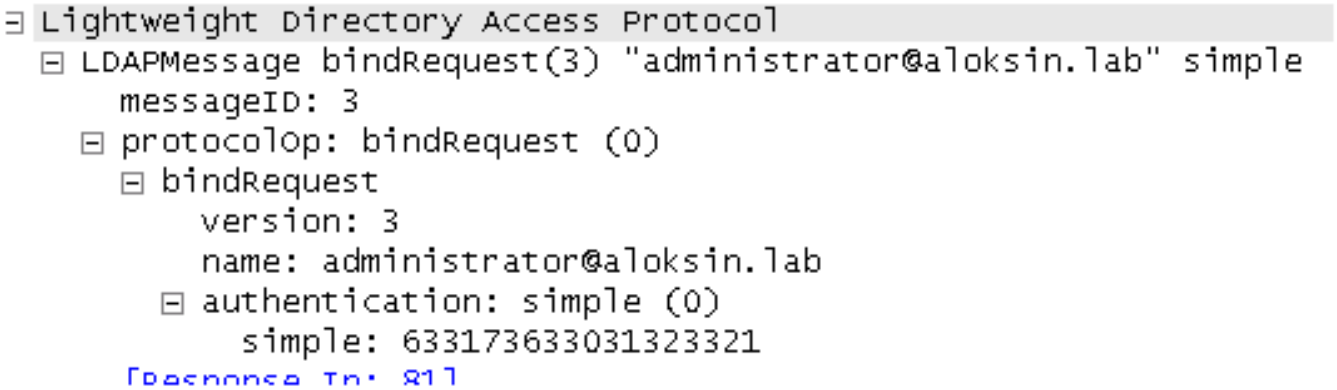


Deze berichten verschijnen in het pakket met daarin de volgende gegevens:

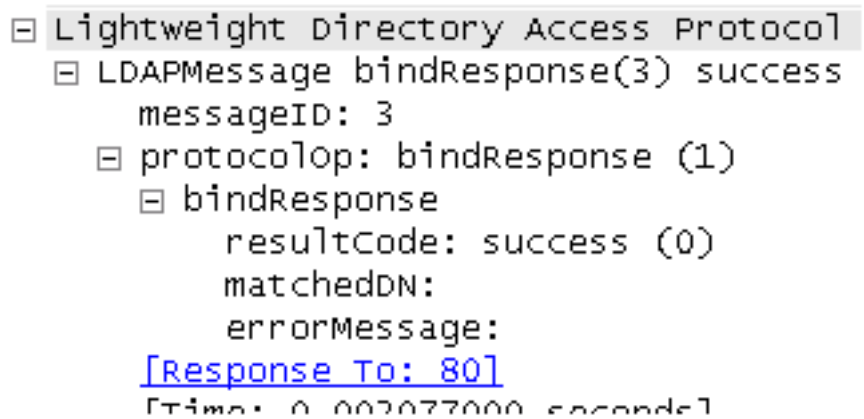
- Hier is de TCP handdruk, gevolgd door de BIND aanvraag:



- Hier is de uitbreiding van het "BIND"-verzoek:



- Hier is de expansie van de BIND respons, wat op succesvolle authenticatie van de gebruiker (**beheerder** in dit voorbeeld) wijst:



Op een succesvolle verbinding stuurt de server een ZOEKverzoek naar de AD om gebruikers te importeren. Dit ZOEKverzoek bevat het filter en de eigenschappen die door de AD worden gebruikt. De AD zoekt vervolgens naar gebruikers binnen de gedefinieerde zoekbasis (zoals beschreven in het zoekbericht) die voldoet aan de criteria in het filter en de eigenschappen verificatie.

Hier is een voorbeeld van het ZOEKverzoek dat door CUCM wordt verzonden:

```
Lightweight Directory Access Protocol
    LDAPMessage searchRequest(2) "dc=aloksin,dc=lab" wholeSubtree
        messageID: 2
        protocolOp: searchRequest (3)
            searchRequest
                baseObject: dc=aloksin,dc=lab
```

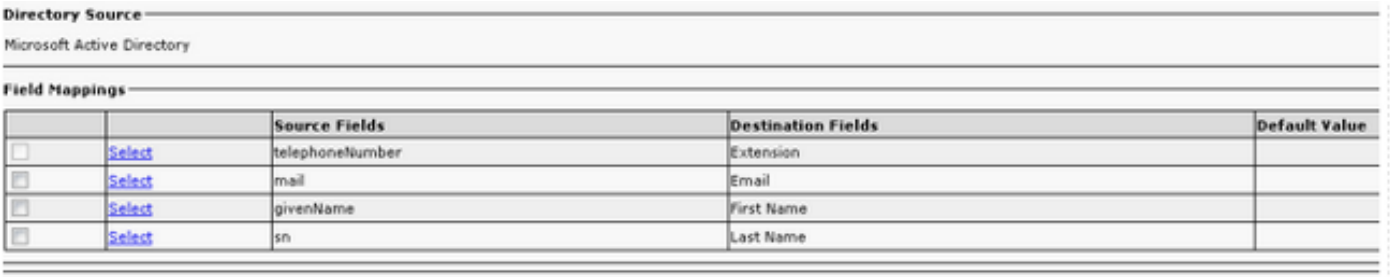
```
            scope: wholeSubtree (2)
             derefAliases: derefAlways (3)
             sizeLimit: 0
             timeLimit: 0
             typesOnly: False
             Filter: (&(&(objectclass=user)(!(objectclass=Computer)))
(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
                  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>
```

Wanneer de AD dit verzoek van CUCM ontvangt, zoekt het naar gebruikers in **baseObject: dc=aloksin, dc=lab**, dat voldoet aan het filter. Elke gebruiker die niet voldoet aan de eisen die door het filter in detail worden beschreven, wordt uitgesloten. Het AD reageert op het CUCM met alle gefilterde gebruikers en verstuurt de waarden voor de gevraagde eigenschappen.

Opmerking: Objecten kunnen niet worden geïmporteerd. Alleen *gebruikers* worden geïmporteerd. Dit komt doordat het filter dat in het ZOEKaanvraagbericht wordt verstuurd, **objectief class=user** bevat. Daarom zoekt de AD alleen naar gebruikers en geen contacten. CUCM heeft al deze afbeeldingen en een filter standaard.

De CUAC wordt standaard niet ingesteld. er zijn geen mapping-details ingesteld om eigenschappen voor gebruikers te importeren, dus u moet deze details handmatig invoeren. Om deze toewijzingen te maken, navigeer dan naar **System Configuration > Directory Source Management > Active Directory > Directory Field mapping**.

Administrateurs mogen velden volgens hun eigen eisen in kaart brengen. Hierna volgt een voorbeeld:

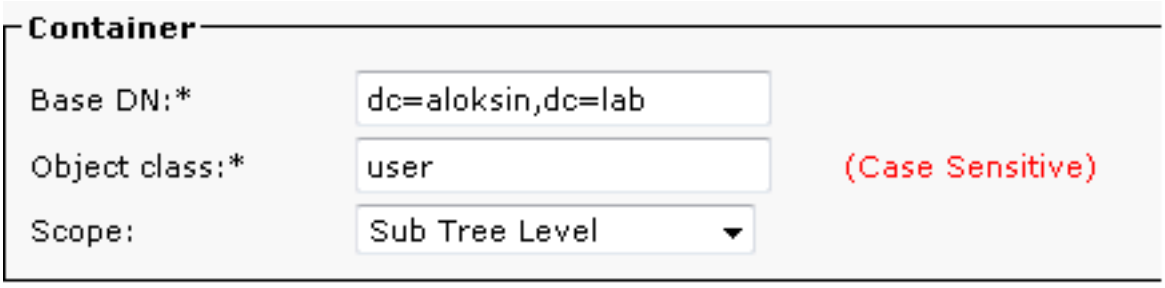


De informatie van het Bron Gebied wordt naar de AD in het ZOEKaanvraagbericht verzonden. Wanneer de AD het ZOEKresponsbericht verstuurt, worden deze waarden opgeslagen in de Doelvelden op de CUACPE.

Merk op dat de CUAC standaard de Object Class heeft ingesteld op *contacten*. Als deze standaardinstelling wordt gebruikt, wordt het filter dat naar de AD wordt verzonden weergegeven zoals hieronder wordt weergegeven:

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

Met dit filter retourneert de AD nooit gebruikers naar CUACPE, omdat het zoekt naar *contacten* in de zoekbasis, niet naar *gebruikers*. Om deze reden moet u Objectklasse in **gebruiker** wijzigen:



Tot dit punt zijn deze instellingen in de CUAC uitgevoerd:

- Verbonden informatie
- Verificatie (onderscheiden gebruiker voor binding)
- containerinstellingen
- Map-omzetting

In dit voorbeeld, wordt het unieke bezit gevormd als **sAMAAccountName**. Als u de LDAP plug-in in de CUAC opnieuw start en het ZOEKaanvraagbericht controleert, bevat het geen eigenschappen of filter behalve de **ObjectClass=user**:

```
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]
```

Merk op dat de Directory regel hier ontbreekt. Om de contacten met de AD te synchroniseren moet u een regel maken. Standaard is er geen directory regel ingesteld. Zodra er een is gemaakt, is er al een filter. Het filter hoeft niet te worden gewijzigd, omdat u alle gebruikers met een telefoonnummer moet importeren.

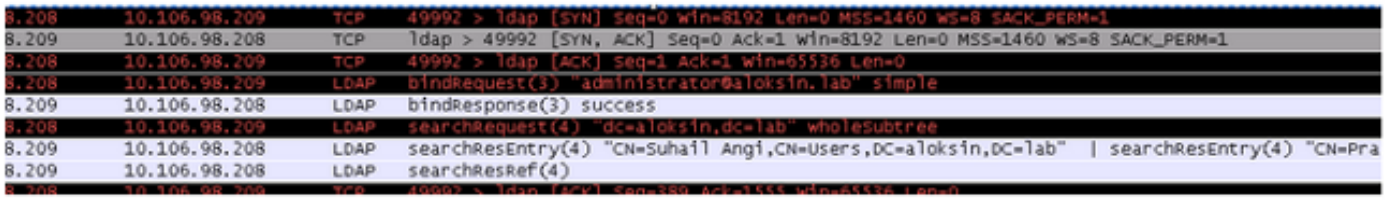
Field	Operator	Val
telephoneNumber	=	*

Start de LDAP-stekker opnieuw om een sync met de AD te starten en de gebruikers te importeren. Dit is het ZOEKverzoek van de CUAC:

```
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>
```

Als de AD gebruikers vindt die aan de criteria voldoen die in het ZOEKEN om bericht worden uiteengezet, dan verstuurt het een bericht van de *SearchResEntry* dat de gebruikersinformatie bevat.



Dit is het bericht SearchResEntry:

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

Opmerking: Het antwoord bevat geen MAIL, hoewel om deze eigenschap wordt verzocht. Dit komt doordat de MAIL-ID niet voor gebruikers op de AD is ingesteld.

Zodra deze waarden door de CUAC worden ontvangen, slaat het deze op in de tabel Structured Search Query (SQL). U kunt dan in de console loggen, en de console haalt de gebruikerslijst van deze SQL tabel op CUACPE server op.