Integración de CUAC con Microsoft AD

Contenido

Introducción

Este documento describe el funcionamiento del protocolo ligero de acceso a directorios (LDAP) entre Cisco Unified Attendant Console (CUAC) y Microsoft Active Directory (AD) y los procedimientos que se utilizan para integrar los dos sistemas.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CUCM
- CUAC
- LDAP
- AD

Componentes Utilizados

La información en este documento se basa en la versión 10.x de CUAC.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

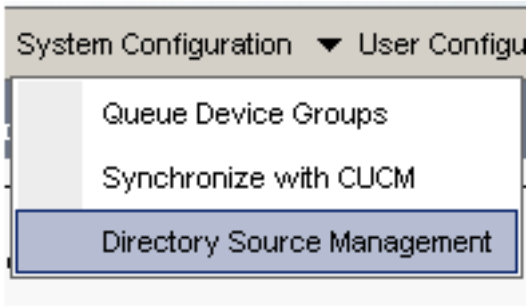
En versiones anteriores de CUAC, el servidor obtiene usuarios directamente de Cisco Unified Communications Manager (CUCM) mediante consultas y filtros predefinidos. Con CUAC Premium Edition (CUACPE), los administradores pueden integrar e importar usuarios directamente desde AD. Esto proporciona flexibilidad a los administradores para la implementación de atributos y filtros de su propia elección y requisitos.

> **Nota:** El CUACPE se ha reemplazado por el CUAC Advanced Edition para las versiones 10 y posteriores.

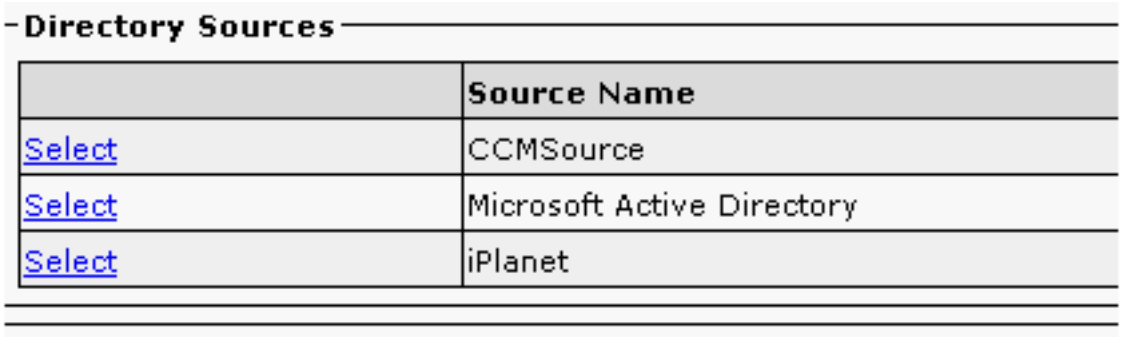
Integración de AD con CUAC e importación de usuarios de AD

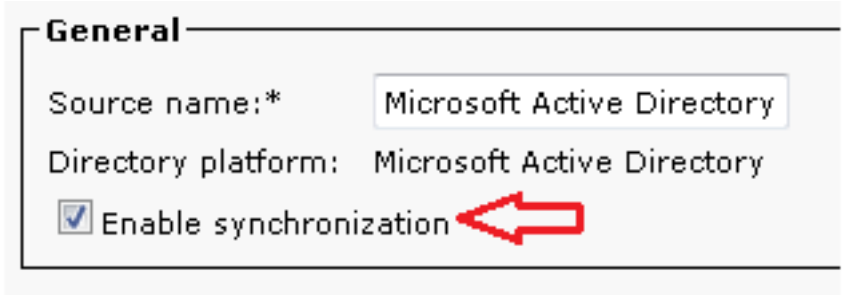
Complete estos pasos para integrar el CUAC con el AD e importar usuarios de AD:

1. Habilite la Sincronización del Directorio para AD en el CUAC.

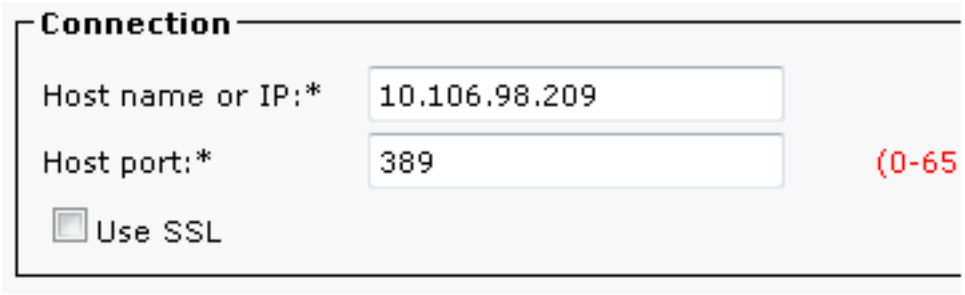


2. Seleccione **Microsoft Active Directory** y marque la casilla de verificación **Habilitar sincronización**:

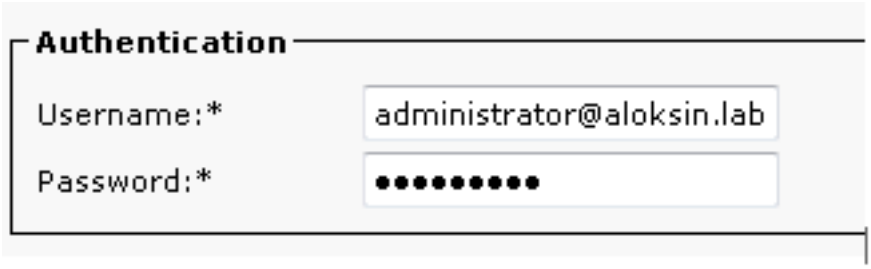




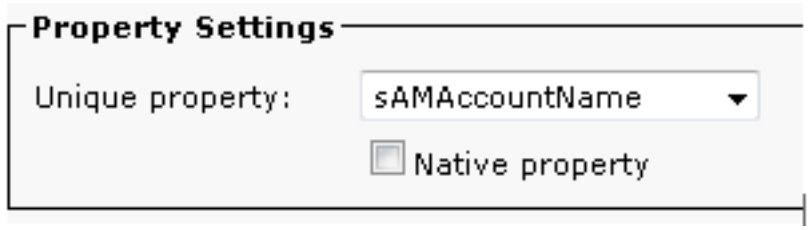
3. Introduzca los detalles de configuración para el servidor de Active Directory:



Para este ejemplo, **administrator@aloksin.lab** se utiliza para la autenticación:



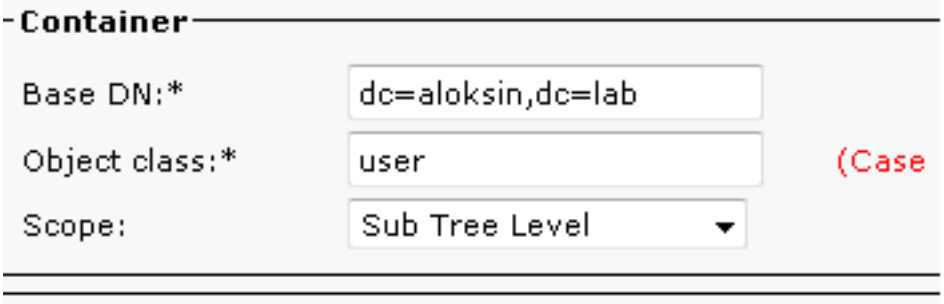
4. En la sección Configuración de propiedades, introduzca los detalles de configuración de la propiedad Única, que aparece una vez que introduzca los demás detalles y haga clic en **Guardar**.



Nota: Este es un valor único para cada entrada en AD. Si hay valores duplicados, el CUAC sólo extrae una entrada.

5. En la sección Contenedor, introduzca los detalles de configuración del DN base, que es el ámbito de búsqueda del usuario en el AD.

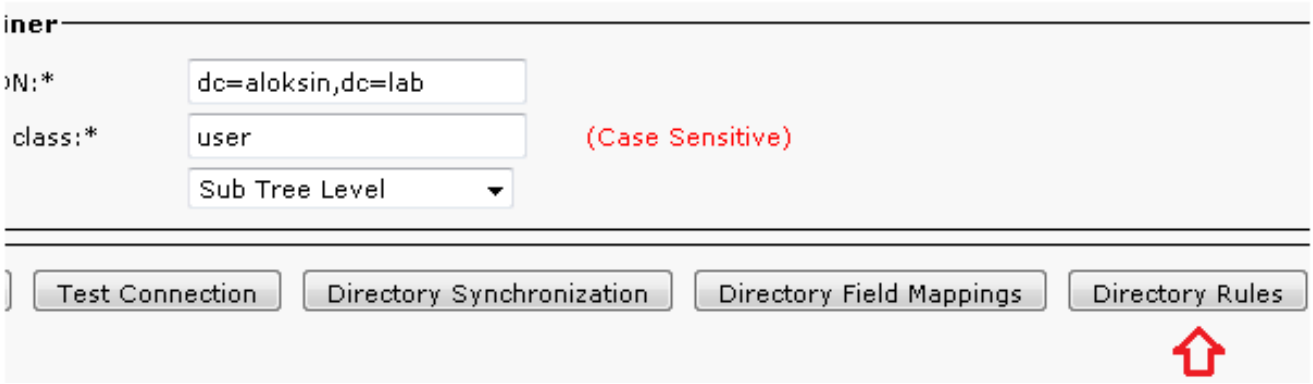
El campo *Clase Object* es utilizado por AD para determinar el ámbito de búsqueda solicitado. De forma predeterminada, se establece en *contacto*, lo que significa que AD busca *contactos* (no usuarios) en la base de búsqueda solicitada. Para importar *usuarios* en el CUAC, cambie la configuración de clase Object a **usuario**:



6. Guarde los parámetros, haga clic en **Asignaciones de campos de directorio** y configure todos los atributos que desea importar para cualquier usuario. Esta es la configuración que se utiliza en este ejemplo:

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

7. Navegue hasta la página de origen de Directorio y haga clic en **Reglas de Directorio**:



8. Haga clic en **Agregar nuevo** y cree una regla. Cuando agrega una regla de directorio, aparece de forma predeterminada un filtro de regla.

	Field	Operator	Value
	telephoneNumber	=	*

Nota: No es necesario cambiar el filtro de reglas. Importa todos los usuarios que tienen un número de teléfono configurado.

9. Para configurar la sincronización automática con AD, haga clic en la pestaña **Sincronización de directorio**.

10. La configuración ha finalizado. Navegue hasta **Ingeniería > Administración de servicio** y reinicie el plugin LDAP para iniciar la sincronización manualmente.

Funcionalidad LDAP entre CUAC y AD

Resumen del proceso LDAP

Aquí hay un resumen del proceso LDAP entre el CUAC y el AD:

1. Se establece una sesión TCP entre los dos servidores (CUAC y AD).

2. El CUAC envía una solicitud BIND al AD y se autentica a través del usuario configurado en la configuración de autenticación.

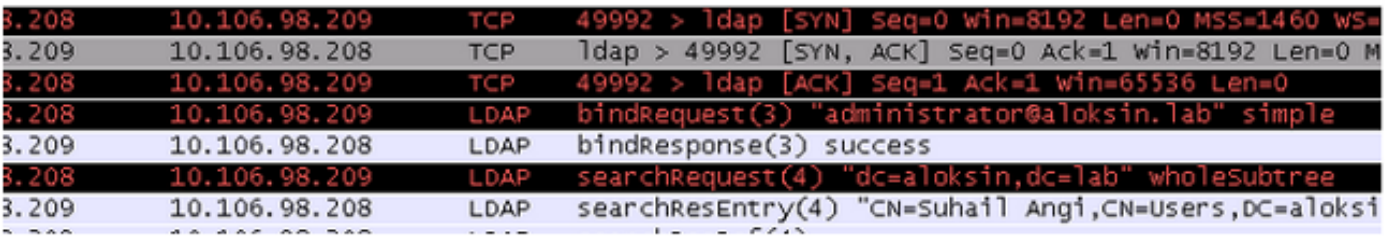
3. Una vez que AD autentica correctamente al usuario, envía una notificación BIND Success al CUACPE.

4. El CUAC envía una solicitud SEARCH al AD, que tiene la información de alcance de búsqueda, los filtros para la búsqueda y los atributos para cualquier usuario filtrado.

5. AD busca el objeto solicitado (configurado en la configuración de clase de objeto) en la base de búsqueda. Filtra los objetos que coinciden con los criterios (filtro) detallados en el mensaje de solicitud SEARCH.

6. El AD responde al CUAC con los resultados de la búsqueda.

Esta es una captura de sabueso que ilustra estos pasos:

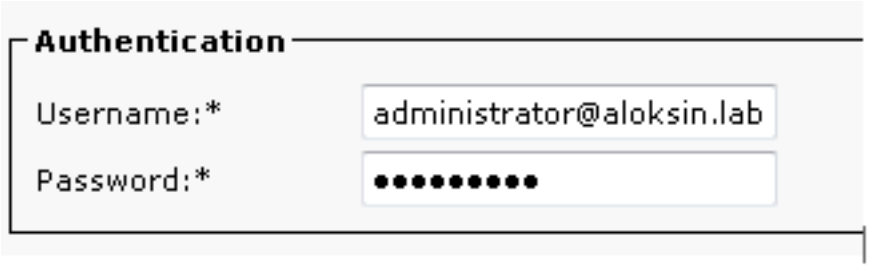


Detalles del proceso LDAP

Una vez que se completa la configuración en el CUAC y se reinicia el complemento LDAP, el servidor CUAC configura una sesión TCP con el AD.

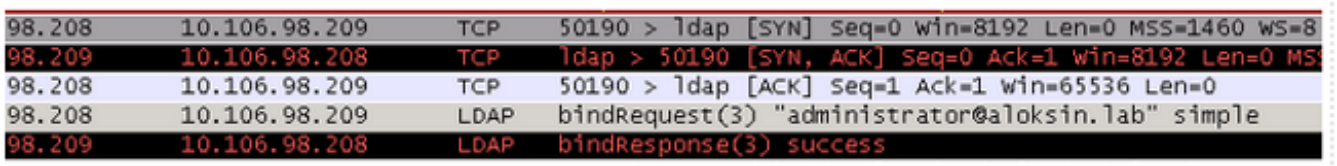
El CUAC entonces envía una solicitud BIND para autenticarse con el servidor AD. Si la autenticación es exitosa, el AD envía una respuesta BIND Success al CUAC. Con esto, ambos servidores intentan configurar una sesión en el puerto 389 para sincronizar a los usuarios y su información.

Esta es la configuración en el servidor que define el nombre distinguido, que se utiliza para la autenticación en la transacción BIND:

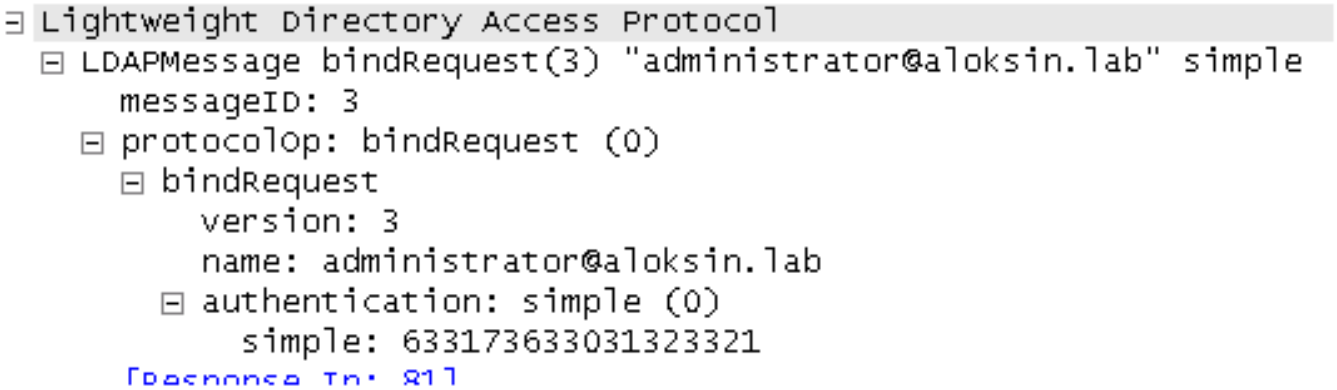


Estos mensajes aparecen en las capturas de paquetes:

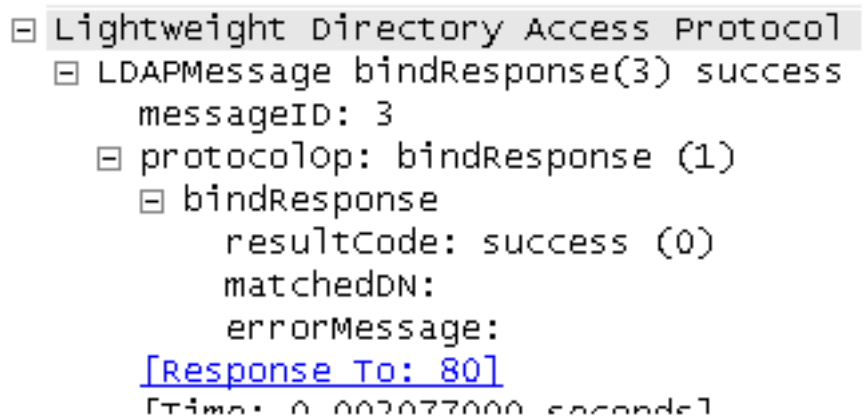
- A continuación se muestra el intercambio de señales TCP, seguido de la solicitud BIND:



- Esta es la expansión de la solicitud BIND:



- Esta es la expansión de la respuesta BIND, que indica una autenticación exitosa del usuario (**administrador** en este ejemplo):



Cuando un enlace se realiza correctamente, el servidor envía una solicitud SEARCH a AD para importar usuarios. Esta solicitud de BÚSQUEDA contiene el filtro y los atributos que utiliza el AD. A continuación, AD busca usuarios dentro de la base de búsqueda definida (como se detalla en el mensaje de solicitud SEARCH), que cumplen los criterios del filtro y la verificación de atributos.

A continuación se muestra un ejemplo de la solicitud SEARCH enviada por CUCM:

```
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>
```

Cuando AD recibe esta solicitud de CUCM, busca usuarios en **baseObject: dc=aloksin,dc=lab**, que satisface el filtro. Se excluye a cualquier usuario que no cumpla los requisitos detallados por el filtro. AD responde a CUCM con todos los usuarios filtrados y envía los valores para los atributos solicitados.

Nota: No se pueden importar objetos. Sólo *se* importan *los usuarios*. Esto se debe a que el filtro que se envía en el mensaje de solicitud SEARCH incluye **objectclass=user**. Por lo tanto, el AD sólo busca usuarios, no contactos. CUCM tiene todas estas asignaciones y un filtro de forma predeterminada.

El CUAC no está configurado de forma predeterminada; no hay detalles de asignación configurados para importar atributos para los usuarios, por lo que debe ingresar estos detalles manualmente. Para crear estas asignaciones, navegue hasta **Configuración del sistema > Administración de orígenes de directorio > Active Directory > Asignación de campos de directorio**.

Los administradores pueden asignar los campos según sus propios requisitos. Aquí tiene un ejemplo:

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	

La información del campo de origen se envía al AD en el mensaje de solicitud SEARCH. Cuando AD envía el mensaje de respuesta SEARCH, estos valores se almacenan en los campos de destino en el CUACPE.

Tenga en cuenta que el CUAC de forma predeterminada tiene la clase Object establecida en *contactos*. Si se utiliza esta configuración predeterminada, el filtro que se envía a AD aparece como se muestra aquí:

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

Con este filtro, el AD nunca devuelve ningún usuario al CUACPE, ya que busca *contactos* en la base de búsqueda, no *usuarios*. Por esta razón, debe cambiar la clase Object a **usuario**:

Container

Base DN:* dc=aloksin,dc=lab

Object class:* user (Case Sensitive)

Scope: Sub Tree Level

Hasta este punto, estos parámetros se han configurado en el CUAC:

- Detalles de las conexiones
- Autenticación (usuario distinguido para enlace)
- Configuración del contenedor
- Asignación de directorios

En este ejemplo, la propiedad Unique se configura como **sAMAccountName**. Si reinicia el complemento LDAP en el CUAC y marca el mensaje de solicitud SEARCH, no contiene ningún atributo o filtro excepto **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]
```

Tenga en cuenta que la regla Directorio falta aquí. Para sincronizar los contactos con el AD, debe crear una regla. De forma predeterminada, no hay ninguna regla de directorio configurada. Tan pronto como se crea uno, ya hay un filtro presente. No es necesario cambiar el filtro, ya que debe importar todos los usuarios que tengan un número de teléfono.

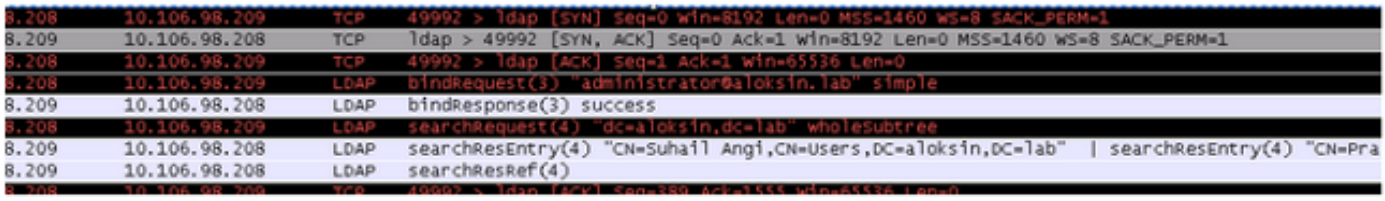
Field	Operator	Val
telephoneNumber	=	*

Reinicie el complemento LDAP para iniciar una sincronización con el AD e importar los usuarios. Esta es la solicitud de BÚSQUEDA del 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>
```

Si AD encuentra usuarios que coinciden con los criterios detallados en el mensaje de solicitud SEARCH, envía un mensaje *SearchResEntry* que contiene la información del usuario.



Este es el mensaje 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}..........
                           .....
```

Nota: No hay MAIL en la respuesta, aunque se solicite este atributo. Esto se debe a que la ID DE CORREO no se configuró para los usuarios en el AD.

Una vez que el CUAC recibe estos valores, los almacena en la tabla Lenguaje de consulta estructurado (SQL). A continuación, puede iniciar sesión en la consola y ésta obtiene la lista de usuarios de esta tabla SQL en el servidor CUACPE.