Microsoft AD と CUAC の統合

目次

概要

この資料は 2 つのシステムを統合ために使用される Lightweight Directory Access Protocol （LDAP）が Cisco Unified Attendant Console （CUAC）の間でおよび Microsoft Active Directory （AD）および手順はたらく方法を記述したものです。

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

この文書に記載されている情報は CUAC バージョン 10.x に基づいています。

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たものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

以前の CUAC バージョンでは、サーバは済みクエリおよびフィルターで Cisco Unified Communications Manager（CUCM）からのユーザを直接得ます。 CUAC 優れた版（CUACPE）によって、管理者は AD からユーザを直接統合、インポートすることができます。これは属性の実装および自身の選択および必要条件のフィルター用の管理者に柔軟性を与えます。

注: CUACPE はバージョン 10 および それ 以降のための CUAC によって進められる版と今取り替えられてしまいました。

AD を CUAC と統合、AD からユーザをインポートして下さい

CUAC を AD と統合、AD からユーザをインポートするためにこれらのステップを完了して下さい:

1. CUAC の AD のためのディレクトリ同期を有効に して下さい。

2. **アクティブ ディレクトリを**『Microsoft』 を選択 し、**イネーブル 同期** チェックボックスをチェックして下さい:

3. アクティブディレクトリサーバのためのコンフィギュレーションの詳細を入力して下さい:

   この例に関しては、**administrator@aloksin.lab は**認証のために使用されます:

4. プロパティ設定では入力し、他の詳細を一度『SAVE』 をクリック する現われる一意のプロパティのためのコンフィギュレーションの詳細を区分して下さい、入力して下さい。

   注: これは AD の各エントリの固有の値です。 重複する値がある場合、CUAC は 1 つのエントリだけ引っ張ります。
5. コンテナー セクションでは、ベース DN のためのコンフィギュレーションの詳細を入力して下さい、AD のユーザ の 検索 スコープである。

   オブジェクト クラス クラス フィールドは AD によって要求された検索スコープを判別するために使用されます。 デフォルトで、*連絡すること*を設定 しますつまり AD が要求された

検索ベースの*連絡先*（ないユーザ）を探すことを意味します。 CUAC のユーザをインポートするために、設定 する **ユーザ**にオブジェクト クラスを変更して下さい:

6. 設定を保存し、**フィールド マッピングを**『Directory』 をクリック し、あらゆるユーザ向けにインポートすることを望む属性すべてを設定して下さい。 設定はここにありますこの例で使用される:

7. Source ページ ディレクトリにナビゲート し、**ルールを**『Directory』 をクリック して下さい:

8. ルールを『Add New』 をクリック し、作成して下さい。 ディレクトリ ルールを追加するとき、ルール フィルタはデフォルトで現われます。

   注: ルール フィルタを変更する必要がありません。 それは電話番号を設定してもらうユーザ全員をインポートします。
9. auto-sync を AD で設定するために、**ディレクトリ同期**タブをクリックして下さい。

10. 設定はこれで完了しました。 **> サービス管理は設計**にナビゲート し、同期化を手動で開始するために LDAP プラグインを再起動します。

CUAC と AD 間の LDAP 機能性

LDAP プロセス 要約

CUAC と AD 間の LDAP プロセスの要約はここにあります:

1. TCP セッションは 2 つのサーバの間で設定されます（CUAC および AD）。

2. CUAC は AD に BIND 要求を送信 し、認証設定で設定されるユーザによって認証します。

3. AD がユーザの認証に成功すれば、CUACPE に BIND 成功通知を送信 します。

4. CUAC は検索スコープ 情報が、検索用のフィルタあり、あらゆるフィルタ処理された ユーザ向けに帰因する AD に検索要求を送信 します。

5. AD は検索ベースの要求されたオブジェクトのために（オブジェクト クラス設定で設定される）スキャンします。 それは検索要求 メッセージで詳述された条件（フィルタ）を満たし

たオブジェクトをフィルタ・アウトします。

6. AD は検索結果を用いる CUAC に応答します。

これらのステップを説明するスニファー キャプチャはここにあります:

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れば、CUAC サーバは AD の TCP セッションを設定します。

CUAC は AD サーバと認証するためにそれから BIND 要求を送信 します。 認証が正常である場合、AD は CUAC への BIND 成功応答を返します。 これによって、サーバは両方ともユーザおよび情報を同期するためにポート 389 のセッションを設定するように試みます。

サーバの設定はここにあります BIND トランザクションで認証のために使用される識別名を定義する、:

パケットキャプチャにこれらのメッセージが現れます:

- BIND 要求に先行している TCP ハンドシェイクはここにあります:

- BIND 要求の展開はここにあります:

- ユーザ（この例の**管理者**）の認証の成功を示す BIND 応答の展開はここにあります、:

正常なバインドに、サーバは AD にユーザをインポートするために検索要求を送信 します。 この検索要求は AD によって使用する属性およびフィルタが含まれています。 AD はフィルタおよび属性確認の基準を達成する定義された検索ベース内のユーザをそれから（検索要求 メッセージで説明されているように）捜します。

CUCM によって送信 される 検索要求の例はここにあります:

```
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 からこの要求を受け取るとき、baseObject のユーザを捜します: dc=aloksin、フィルタを満たす dc=lab。 フィルタによって詳述される必要条件を満たさないどのユーザでも省かれます。 AD はフィルタ処理された ユーザ全員の CUCM に応答し、要求された属性の値を送信 します。

> **注:** オブジェクトはインポートすることができません。 *ユーザだけ*インポートされます。 検索要求 メッセージで送信 されるこれはフィルタが objectclass=user が含まれているという理由によります。 それ故に、AD はユーザをだけ、ない連絡先捜します。 CUCM にこれらのマッピングおよびフィルタすべてがデフォルトであります。

CUAC はデフォルトで設定されません; マッピングが詳述しますユーザ向けの属性をインポートするために設定されてありません従ってこれらの詳細を手動で入力して下さい。 これらのマッピ

ングを、ナビゲート **システム構成 > ディレクトリ ソース管理 > アクティブ ディレクトリ > Directory フィールド マッピング**に作成するため。

管理者は自身の要件ごとの Map フィールドに許可されます。 次に例を示します。

Source フィールド 情報は検索要求 メッセージの AD に送信 されます。 AD が検索応答メッセージを送信 するとき、これらの値は CUACPE で宛先 フィールドで保存されます。

CUAC にデフォルトで*連絡先*に設定 されるオブジェクト クラスがあることに注目して下さい。 AD に送信 されるこのデフォルト設定が使用される場合、フィルタはここに示されているように現われます:

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

このフィルタによって、AD は CUACPE に決して検索ベースの*連絡先*を捜すのでユーザを、ないユーザ戻しません。 従って、**ユーザ**にオブジェクト クラスを変更して下さい:

このポイントまで、これらの設定は CUAC で行われました:

- 接続詳細
- 認証 (結合のための顕著なユーザ)
- コンテナー設定
- ディレクトリ マッピング すること

この例では、一意のプロパティは **sAMAccountName** で設定されます。 CUAC で差込式 LDAP を再起動し、検索要求 メッセージをチェックする場合、**ObjectClass=user** を除く属性かフィルタが含まれていません:

```
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]
```

ディレクトリ ルールがここに抜けていることに注目して下さい。 連絡先を AD と同期するために、ルールを作成して下さい。 デフォルトで、設定されるディレクトリ ルールがありません。 1 つが作成されるとすぐ、フィルタは既にあっています。 電話番号を持っているユーザの import all なるようにフィルタを変更する必要がありません。

AD の同期化を始め、ユーザをインポートするために LDAP プラグインを再起動して下さい。 CUAC からの検索要求はここにあります:

```
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 が検索要求 メッセージで詳述された条件を満たしたユーザを見つければユーザ情報が含まれている *SearchResEntry* メッセージを送信 します。

SearchResEntry メッセージはここにあります:

```
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: このアトリビュートが要求されるのに、応答にメールがありません。 これはメール ID が AD のユーザ向けに設定されなかったという理由によります。

これらの値が CUAC によって受け取られれば、構造化照会言語（SQL）表でそれらを保存します。 それからコンソールにログイン することができコンソールは CUACPE サーバのこの SQL 表からのユーザー一覧を取出します。