Интеграция CUAC с Microsoft AD

Содержание

Введение

Этот документ описывает путь, которым Протокол LDAP работает между консолью оператора Cisco Unified Attendant Console (CUAC) и Microsoft Active Directory (AD) и процедуры, которые используются для интеграции этих двух систем.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- CUCM
- CUAC
- LDAP
- AD

Используемые компоненты

Сведения в этом документе основываются на Версии 10 CUAC. x.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

В более ранних версиях CUAC сервер получает пользователей непосредственно из Cisco Unified Communications Manager (CUCM) через предопределенные запросы и фильтры. С CUAC Premium Выпуск (CUACPE), администраторам разрешают интегрировать и импортировать пользователей непосредственно из AD. Это предоставляет гибкость администраторам для реализации атрибутов и фильтров их собственного выбора и требований.

> **Примечание:** CUACPE был теперь заменен CUAC Усовершенствованный Выпуск для Версий 10 и позже.

Интегрируйте AD с CUAC и импортируйте пользователей из AD

Выполните эти шаги, чтобы интегрировать CUAC с AD и импортировать пользователей из AD:

1. Включите синхронизацию каталога для AD на CUAC.

2. Выберите **Microsoft Active Directory** и проверьте **Разрешать флажок synchronization**:

3. Введите элементы конфигурации для Сервера Active Directory:

   Для данного примера **administrator@aloksin.lab** используется для аутентификации:

4. В разделе Параметров настройки Свойства введите элементы конфигурации для свойства Unique, которое появляется, как только вы вводите другие подробные данные и нажимаете **Save**.

   Примечание: Это - уникальное значение для каждой записи в AD. Если существуют двойные значения, CUAC вытягивает только одну запись.
5. В Контейнерном разделе введите элементы конфигурации для Основного DN, который является областью поиска пользователей в AD.

Поле *Класса объекта* используется AD для определения запрошенной поисковой области. По умолчанию это собирается *связаться*, что означает, что AD ищет *контакты* (не пользователи) в запрошенном поисковом ядре. Для импорта *пользователей* на CUAC измените настройки Класса объекта **пользователю**:

6. Сохраните настройки, нажмите **сопоставления Directory Field** и настройте все атрибуты, которые требуется импортировать для любого пользователя. Вот конфигурация, которая используется в данном примере:

7. Перейдите к исходной странице Каталога и нажмите **Directory Rules**:

8. **Нажмите Add New** и создайте правило. Когда вы добавляете правило каталога, фильтр правила появляется по умолчанию.

   Примечание: Нет никакой потребности изменить фильтр правила. Это импортирует всех пользователей, которым настроили номер телефона.
9. Для настройки auto-sync с AD нажмите вкладку **Directory Synchronization**.

10. Настройка завершена. Перейдите к **Разработке> управление службами** и перезапустите плагин LDAP для начала синхронизования вручную.

Функциональность LDAP между CUAC и AD

Сводка процесса LDAP

Вот сводка процесса LDAP между CUAC и AD:

1. Сеанс TCP установлен между этими двумя серверами (CUAC и AD).

2. CUAC отправляет запрос BIND к AD и аутентифицируется через пользователя, который настроен в Настройках аутентификации.

3. Как только AD успешно аутентифицирует пользователя, он передает уведомление Успеха BIND CUACPE.

4. CUAC передает Запрос на поиск к AD, который имеет поисковые сведения об области, фильтры для поиска, и приписывает для любого фильтрованного пользователя.

5. AD просматривает для запрашиваемого объекта (настроенный в параметрах настройки Класса объекта) в поисковом ядре. Это отфильтровывает объекты, которые совпадают с критериями (фильтр), детализированный в сообщении Запроса на поиск.

6. AD отвечает на CUAC с результатами поиска.

Вот перехват анализатора, который иллюстрирует эти шаги:

Сведения о процессе LDAP

Как только конфигурация на CUAC завершена, и плагин LDAP перезапущен, настройки сервера CUAC сеанс TCP с AD.

CUAC тогда отправляет запрос BIND для аутентификации с AD сервером. Если аутентификация успешна, AD передает ответ Успеха BIND на CUAC. С этим оба сервера пытаются установить сеанс на порту 389 чтобы синхронизированным пользователям и их информации.

Вот конфигурация на сервере, который определяет Составное имя, которое используется для аутентификации в транзакции BIND:

Эти сообщения появляются в захватах пакета:

- Вот квитирование TCP - подключения, придерживавшееся запросом BIND:

- Вот расширение запроса BIND:

- Вот расширение ответа BIND, который указывает на успешную аутентификацию пользователя (**администратор** в данном примере):

На успешное связывают, сервер передает Запрос на поиск к AD для импорта пользователей. Этот Запрос на поиск содержит фильтр и атрибуты, которые используются AD. AD тогда ищет пользователей в определенном поисковом ядре (как детализировано в сообщении Запроса на поиск), который выполняет критерии в фильтре и проверке атрибутов.

Вот пример Запроса на поиск, который передается 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>
```

Когда AD получает этот запрос от CUCM, это ищет пользователей в **baseObject: dc=aloksin, dc=lab**, который удовлетворяет фильтр. Любой пользователь, который не выполняет требования, которые подробно изложены фильтром, не учтен. AD отвечает на CUCM со всеми фильтрованными пользователями и передает значения за запрошенными атрибутами.

Примечание: Объекты не могут быть импортированы. Только *пользователи* импортированы. Это вызвано тем, что фильтр, который передается в сообщении Запроса на поиск, включает **objectclass=user**. Следовательно, AD ищет только пользователей, не контакты. CUCM имеет все эти сопоставления и фильтр по умолчанию.

CUAC не настроен по умолчанию; нет никаких подробных данных сопоставления, настроенных для импорта атрибутов для пользователей, таким образом, необходимо ввести эти подробные данные вручную. Для создания этих сопоставлений перейдите к **Конфигурации системы> Управление ресурсами Каталога> Active Directory> Полевое Сопоставление Каталога**.

Администраторам разрешают сопоставить поля на их собственные требования. Например:

Исходная информация о Поле передается AD в сообщении Запроса на поиск. Когда AD передает ПОИСКОВОЕ ответное сообщение, эти значения сохранены в Полях Назначение на CUACPE.

Обратите внимание на то, что CUAC по умолчанию установили Класс объекта в *контакты*. Если эта настройка по умолчанию используется, фильтр, который передается AD, появляется как показано здесь:

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

С этим фильтром AD никогда не возвращает пользователей к CUACPE, так как это ищет *контакты* в поисковом ядре, не *пользователей*. Поэтому необходимо изменить Класс объекта на **пользователя**:

До этой точки эти параметры настройки были настроены на CUAC:

- Подробные данные соединений
- Аутентификация (отличенный пользователь для привязки)
- Контейнерные параметры настройки
- Сопоставление каталога

В данном примере свойство Unique настроено как **sAMAccountName**. Если вы перезапускаете плагин LDAP на CUAC и проверяете сообщение Запроса на поиск, это не содержит атрибутов или фильтра кроме **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]
```

Обратите внимание на то, что правило Каталога отсутствует здесь. Для синхронизации контактов с AD необходимо создать правило. По умолчанию нет никакого настроенного правила Каталога. Как только каждый создан, фильтр уже присутствует. Нет никакой потребности изменить фильтр, поскольку вы должны import all пользователей, которые имеют номер телефона.

Перезапустите плагин LDAP, чтобы инициировать синхронизование с AD и импортировать пользователей. Вот Запрос на поиск от 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>
```

Если AD находит пользователей, которые совпадают с критериями, детализированными в сообщении Запроса на поиск, то это передает сообщение *SearchResEntry*, которое содержит сведения о пользователе.

Вот сообщение 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}.........
           .....
```

Примечание: В ответе нет никакой ПОЧТЫ, даже при том, что запрашивают этот атрибут. Это вызвано тем, что ПОЧТОВЫЙ ID не был настроен для пользователей на AD.

Как только эти значения получены CUAC, он хранит их в таблице StructuredQuery Language (SQL) (язык структурированных запросов). Можно тогда войти в консоль, и консоль выбирает пользовательский список от этой таблицы SQL на сервере CUACPE.