Настройте ISE для интеграции с сервером LDAP

Содержание

Введение

Этот документ описывает, как настроить платформу Cisco Identity Services Engine (ISE) для интеграции с Протоколом доступа к каталогу облегченного Cisco (LDAP) сервер.

> **Примечание:** Этот документ допустим для настроек, которые используют LDAP в качестве внешнего идентификационного источника для проверки подлинности и авторизация ISE.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Информационный этот документ основывается на этих версиях программного и

аппаратного обеспечения:

- Версия 1.3 Cisco ISE с исправлением 2
- Версия 7 x64 Microsoft Windows с OpenLDAP установлена
- Контроллер беспроводной локальной сети Cisco (WLC) версия 8.0.100.0
- Версия 3.1 AnyConnect Cisco для Microsoft Windows
- Access Manager сети Cisco редактор профиля

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

Эти методы аутентификации поддерживаются с LDAP:

- Расширяемый протокол аутентификации Г¦¦ Карта с переменым паролем Общего назначения (EAP-GTC)
- Transport Layer Security Расширяемого протокола аутентификации (EAP-TLS) Г¦¦
- Защищенный Transport Layer Security Расширяемого протокола аутентификации (TLS PEAP) Г¦¦

Настройка

В этом разделе описывается настроить сетевые устройства и интегрировать ISE с Сервером LDAP.

Схема сети

В этом примере конфигурации оконечная точка использует беспроводной адаптер для соединения с беспроводной сетью. Беспроводная локальная сеть (WLAN) на WLC настроена для аутентификации пользователей через ISE. На ISE LDAP настроен как внешнее хранилище идентификаторов.

Этот образ иллюстрирует топологию сети, которая используется:

Настройте OpenLDAP

Установка OpenLDAP для Microsoft Windows завершена через GUI, и это прямо.

Расположение по умолчанию является **C:> OpenLDAP**. После установки необходимо видеть этот каталог:

Примите во внимание два каталога в особенности:

- **ClientTools Γ¦¦** Этот каталог включает ряд двоичных файлов, которые используются для редактирования базы данных LDAP.

- **ldifdata Γ¦¦** Это - местоположение, в котором необходимо хранить файлы с объектами LDAP.

Добавьте эту структуру к базе данных LDAP:

В соответствии с *Корневым каталогом*, необходимо настроить два Подразделения (OU). OU *OU=groups* должен иметь одну дочернюю группу (**cn=domainusers** в данном примере). OU *OU=people* определяет две учетных записи пользователя, которые принадлежат *cn=domainusers* группе.

Для начальной загрузки базы данных необходимо создать *ldif* файл сначала. Ранее упомянутая структура была создана от этого файла:

```
dn: ou=groups,dc=maxcrc,dc=com
changetype: add
ou: groups
description: All groups in organisation
objectclass: organizationalunit

dn: ou=people,dc=maxcrc,dc=com
changetype: add
ou: people
description: All people in organisation
objectclass: organizationalunit

dn: uid=john.doe,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: john.doe
givenName: John
sn: Doe
cn: John Doe
mail: john.doe@example.com
userPassword: password

dn: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
uid: jan.kowalski
givenName: Jan
sn: Kowalski
cn: Jan Kowalski
mail: jan.kowalski@example.com
userPassword: password

dn: cn=domainusers,ou=groups,dc=maxcrc,dc=com
```

```
changetype: add
objectClass: top
objectClass: posixGroup
gidNumber: 678
memberUid: uid=john.doe,ou=people,dc=maxcrc,dc=com
memberUid: uid=jan.kowalski,ou=people,dc=maxcrc,dc=com
```

Для добавления объектов к базе данных LDAP можно использовать **ldapmodify** двоичные файлы:

```
C:\OpenLDAP\ClientTools>ldapmodify.exe -a -x -h localhost -p 389 -D "cn=Manager,
dc=maxcrc,dc=com" -w secret -f C:\OpenLDAP\ldifdata\test.ldif
ldap_connect_to_host: TCP localhost:389
ldap_new_socket: 496
ldap_prepare_socket: 496
ldap_connect_to_host: Trying ::1 389
ldap_pvt_connect: fd: 496 tm: -1 async: 0
attempting to connect:
connect success
adding new entry "ou=groups,dc=maxcrc,dc=com"

adding new entry "ou=people,dc=maxcrc,dc=com"

adding new entry "uid=john.doe,ou=people,dc=maxcrc,dc=com"

adding new entry "uid=jan.kowalski,ou=people,dc=maxcrc,dc=com"

adding new entry "cn=domainusers,ou=groups,dc=maxcrc,dc=com"
```

Интегрируйте OpenLDAP с ISE

Используйте информацию, которая предоставлена в образах всюду по этому разделу для настройки LDAP как внешнего хранилища идентификаторов на ISE.

Можно настроить эти атрибуты от *Вкладки Общие*:

- **Подчиненный Objectclass Г¦** Это поле соответствует классу объекта учетных записей пользователя в *ldif* файле. Согласно Конфигурации LDAP, можно использовать один из четырех классов здесь:

  Вершина

  Человек

  Оргэнизэйшнэлперсон

  Инеторгперсон

- Г¦ **Атрибута Имени субъекта** Это - атрибут, который получен LDAP, когда ISE запрашивает, включено ли определенное имя пользователя в базу данных. В этом сценарии необходимо использовать **john.doe** или **jan.kowalski** как имя пользователя на оконечной точке.

- **Сгруппируйтесь Objectclass** Г¦ Это поле соответствует классу объекта для группы в *ldif* файле. В этом сценарии класс объекта для *cn=domainusers* группы является **posixGroup**.

- Г¦ **Атрибута Карты группы**, который определяет Этот атрибут, как пользователи сопоставлены с группами. Под *cn=domainusers* группой в *ldif* файле вы видите два атрибута *memberUid*, которые соответствуют пользователям.

ISE также предлагает некоторые предварительно сконфигурированные схемы (Microsoft Active Directory, Sun, Novell):

После установки правильного IP-адреса и названия административного домена можно *Протестировать, Связывают* с сервером. На этом этапе вы не должны получать предметы или группы, потому что еще не настроены поисковые ядра.

В следующей вкладке можно настроить Предмет/Базу поиска группы. Это - *точка соединения* для ISE к LDAP. Вы в состоянии получить только предметы и группы, которые являются потомками вашей точки присоединения. В этом сценарии получены предметы от *OU=people* и группы от *OU=groups*:

От вкладки *Groups* можно импортировать группы из LDAP на ISE:

Настройте WLC

Используйте информацию, которая предоставлена в этих образах для настройки WLC для аутентификации 802.1x:

Настройте EAP-GTC

Один из поддерживаемых методов аутентификации для LDAP является EAP-GTC. Это доступно в AnyConnect Cisco, но необходимо установить менеджера Доступа к сети Профайла Редактор для настройки профиля правильно. Необходимо также отредактировать Конфигурацию менеджера Доступа к сети, которая по умолчанию расположена здесь:

C :> ProgramData> Cisco> защищенный мобильный клиент Cisco AnyConnect Secure Mobility> Менеджер Доступа к сети> система> configuration.xml файл

Используйте информацию, которая предоставлена в этих образах для настройки EAP-GTC на оконечной точке:

Используйте информацию, которая предоставлена в этих образах для изменения политики проверки подлинности и авторизация по ISE:

После применения конфигурации, должна существовать возможность для соединения с сетью:

Проверка

Для проверки LDAP и конфигураций ISE, должна существовать возможность для получения

предметов и групп с тестовым подключением к серверу:

Эти образы иллюстрируют типовой отчёт из ISE:

Устранение неполадок

В этом разделе описываются некоторые распространенные ошибки, с которыми встречаются с этой конфигурацией и как устранить неполадки их:

- После установки OpenLDAP вы могли бы встретиться с ошибкой указать, что отсутствует **gssapi.dll**. Для устранения ошибки необходимо перезапустить Microsoft Windows

- Не могло бы быть возможно отредактировать *configuration.xml* файл для AnyConnect Cisco непосредственно. Сохраните свою новую конфигурацию в другом местоположении и затем используйте его для замены старого файла.

- В опознавательном отчёте вы могли бы видеть это сообщение об ошибках: **`Authentication method is not supported by any applicable identity store`**Это сообщение об ошибках указывает, что метод, который вы выбрали, не поддерживается LDAP. Гарантируйте, что *Протокол аутентификации* в том же отчёте показывает один из поддерживаемых методов (EAP-GTC, EAP-TLS или TLS PEAP).

- В опознавательном отчёте вы могли бы заметить, что предмет не был найден в идентификационном хранилище. Это означает, что имя пользователя из отчёта не совпадает *с Атрибутом Имени субъекта* ни для какого пользователя в базе данных LDAP. В этом сценарии значение было установлено в **uid** для этого атрибута, что означает, что ISE смотрит на значения *uid* для пользователя LDAP, когда это пытается найти соответствие.

- Предметы и группы не могли бы быть получены правильно во время *связывания с* тестом *сервера*. Наиболее вероятная причина этой проблемы является некорректной конфигурацией для поисковых ядер. Помните, что иерархия LDAP должна быть задана от листа к root, и *система цифрового управления* (может состоять из множественных слов).

  Совет: Для устранения проблем Аутентификации eap на стороне WLC обратитесь к Аутентификации eap с Контроллерами беспроводной локальной сети (WLC) Документ Cisco Примера конфигурации.