Пример конфигурации проверки подлинности LDAP для центрального UCS

Содержание

Введение

Этот документ предоставляет пример конфигурации для аутентификации Протокола LDAP для системы Cisco UCS Центральный (UCS). Процедуры используют UCS Центральный графический пользовательский интерфейс (GUI), домен в качестве примера bglucs.com и пример имени пользователя testuser.

В версии 1.0 UCS Центральное программное обеспечение LDAP является единственным поддерживаемым протоколом удаленной аутентификации. Версия 1.0 имеет очень ограниченную поддержку удаленной аутентификации и Конфигурацию LDAP для UCS, Центрального самого. Однако можно использовать UCS, Центральный для настройки всех опций для Менеджера UCS домены, которыми управляет Центральный UCS.

Ограничения UCS Центральная удаленная аутентификация включают:

- RADIUS и TACACS не поддерживаются.
- Сопоставление состава группы LDAP для присвоения роли и группы поставщика LDAP для контроллеров составного домена не поддерживаются.
- LDAP использует только атрибут CiscoAVPair или любой неиспользованный атрибут для передачи роли. Роль прошла, одна из предопределенных ролей в UCS Центральная локальная база данных.
- Домены/протоколы несколько серверов проверок подлинности не поддерживаются.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Центральный UCS развернут.
- Microsoft Active Directory развернута.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- UCS центральная версия 1.0
- Microsoft Active Directory

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.

Условные обозначения

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Соберите информацию

Этот раздел суммирует необходимую информацию для сбора перед началом конфигурации.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Свяжите пользовательские подробные данные

Свяжите пользователя, может быть любой пользователь LDAP в домене, у которого есть доступ для чтения к домену; связывать пользователь требуется для Конфигурации LDAP. Центральное использование UCS имя пользователя и пароль связывать пользователя,

чтобы подключить и сделать запрос Active Directory (AD) для проверки подлинности пользователя и т.д. Данный пример использует Учетную запись администратора в качестве связывать пользователя.

Эта процедура описывает, как администратор LDAP может использовать Редактора Интерфейсов сервиса Active Directory (ADSI) для обнаружения DN.

1. Откройте редактора ADSI.
2. Найдите связывать пользователя. Пользователь находится в том же пути как в AD.
3. Щелкните правой кнопкой мыши пользователя и выберите **Properties**.
4. В Диалоговом окне со свойствами дважды нажмите **distinguishedName**.
5. Скопируйте DN с Поля значения.
6. Нажмите **Cancel** для закрытия всех окон.

Для получения пароля для связывать пользователя свяжитесь с AD администратором.

Основные подробные данные DN

Основной DN является DN подразделения (OU) или контейнера, где начинается поиск пользовательских и пользовательских подробных данных. Можно использовать DN OU, созданного в AD для UCS или Центрального UCS. Однако можно найти более простым использовать DN для самого доменного root.

Эта процедура описывает, как администратор LDAP может использовать Редактора ADSI для обнаружения Основного DN.

1. Откройте редактора ADSI.
2. Найдите, что OU или контейнер используются в качестве основного DN.
3. Щелкните правой кнопкой мыши OU или контейнер, и выберите **Properties**.
4. В Диалоговом окне со свойствами дважды нажмите **distinguishedName**.
5. Скопируйте DN с поля значения и обратите внимание на любые другие подробные данные, в которых вы нуждаетесь.
6. Нажмите **Cancel** для закрытия всех окон.

Подробные данные поставщика

Поставщик играет ключевую роль в проверке подлинности LDAP и авторизацию в Центральном UCS. Поставщик является одним из AD серверов, что UCS Центральные запросы, чтобы искать и аутентифицировать пользователя и для получения пользовательских подробных данных, таких как информация о роли. Обязательно соберите имя хоста или IP-адрес сервера AD Поставщика.

Свойство фильтра

Поле фильтра или свойство используются для поиска AD базы данных. Идентификатор пользователя, введенный во вход в систему, пасуется назад к AD и сравнивается с фильтром.

Можно использовать sAMAccountName= $userid в качестве значения фильтра. sAMAccountName является атрибутом в AD и имеет то же значение как AD идентификатор пользователя, который используется для регистрации к UCS в Центральный GUI.

Добавьте и настройте атрибуты

Этот раздел суммирует необходимую информацию, чтобы добавить атрибут CiscoAVPair (при необходимости) и обновить атрибут CiscoAVPair или другой, предопределенный атрибут перед началом Конфигурации LDAP.

Поле атрибута задает AD атрибут (под свойством пользователя), который пасует назад роль, которая будет назначена на пользователя. В Выпуске 1.0a UCS Центральное программное обеспечение или настраиваемый атрибут CiscoAVPair или любой другой неиспользованный атрибут в AD могут быть унифицированы для передачи этой роли.

Примечание: Используйте инструмент Command Lookup (только для зарегистрированных пользователей) для того, чтобы получить более подробную информацию о командах, использованных в этом разделе.

Добавьте атрибут CiscoAVPair

Для добавления нового атрибута к домену разверните схему домена и добавьте атрибут к классу (который, в данном примере, пользователь).

Эта процедура описывает, как развернуть схему на сервере Windows AD и добавить атрибут CiscoAVPair.

1. Войдите к AD серверу.
2. Нажмите **Start> Run**, введите **mmc** и нажмите **Enter** для открытия пустой консоли Консоли управления Microsoft (MMC).
3. В MMC нажмите **File>, Add/Remove Snap - в> Добавляет**.
4. В Добавлении Автономного Моментального снимка - в диалоговом окне, выберите **Active Directory Schema** и **нажмите Add**.
5. В MMC разверните **Схему Active Directory**, щелкните правой кнопкой мыши **Атрибуты** и выберите **Create Attribute**.Диалоговое окно Create New Attribute появляется
6. Создайте атрибут под названием CiscoAVPair в сервисе удаленной аутентификации.В Общем имени и Полях имени Показа LDAP, введите **CiscoAVPair**.В Уникальных 500 полях Object ID войдите **1.3.6.1.4.1.9.287247.1**.В Поле описания введите **роль UCS и локаль**.В поле Syntax выберите **Unicode String** от выпадающего списка.Нажмите **OK**, чтобы сохранить атрибут и закрыть диалоговое окно.Как только атрибут добавлен к схеме, это должно быть сопоставленный или включенный в класс пользователя. Это позволяет вам редактировать свойство пользователя и задавать значение роль, которую передадут.
7. В том же MMC, используемом для AD расширения схемы, разверните **Классы**, щелкните правой кнопкой мыши **пользователя** и выберите **Properties**.
8. В диалоговом окне свойств пользователя нажмите вкладку **Attributes** и **нажмите Add**.
9. В диалоговом окне Select Schema Object нажмите **CiscoAVPair** и нажмите **OK**.
10. В диалоговом окне свойств пользователя нажмите **Apply**.
11. Щелкните правой кнопкой мыши **Схему Active Directory** и выберите **Reload the Schema** для включения новых изменений.
12. Если необходимо, используйте Редактора ADSI для обновления схемы. Щелкните правой кнопкой мыши **Локальный узел** и выберите **Update Schema Now**.

Обновите атрибут CiscoAVPair

Эта процедура описывает, как обновить атрибут CiscoAVPair. Синтаксисом является `shell:roles="<role>"`.

1. В диалоговом окне Edit ADSI найдите пользователя, который должен обратиться к Центральному UCS.
2. Щелкните правой кнопкой мыши пользователя и выберите **Properties**.
3. В Диалоговом окне со свойствами нажмите вкладку **Attribute Editor**, нажмите **CiscoAVPair** и нажмите **Edit**.
4. В Многозначном диалоговом окне String Editor введите значение **shell:roles = "admin"** в поле Values и нажмите **OK**.
5. Нажмите **OK**, чтобы сохранить изменения и закрыть Диалоговое окно со свойствами.

Обновите предопределенный атрибут

Эта процедура описывает, как обновить предопределенный атрибут, где роль является одной из предопределенных ролей пользователя в Центральном UCS. Данный пример использует *компанию* атрибута для передачи роли. Синтаксисом является `shell:roles="<role>"`.

1. В диалоговом окне Edit ADSI найдите пользователя, который должен обратиться к Центральному UCS.
2. Щелкните правой кнопкой мыши пользователя и выберите **Properties**.
3. В Диалоговом окне со свойствами нажмите вкладку **Attribute Editor**, нажмите **компанию** и нажмите **Edit**.
4. В диалоговом окне String Attribute Editor введите значение **shell:roles = "admin"** в Поле значения и нажмите **OK**.
5. Нажмите **OK**, чтобы сохранить изменения и закрыть Диалоговое окно со свойствами.

Настройте проверку подлинности LDAP на центральном UCS

Конфигурация LDAP в Центральном UCS завершена под операционным менеджментом.

1. Войдите к UCS, Центральному под локальной учетной записью.
2. Нажмите **Operations Management**, разверните **Группы доменов** и нажмите**> Security Operational Policies**.
3. Для настройки проверки подлинности LDAP сделайте эти шаги:Настройте поставщика LDAP.Настройте группу поставщика LDAP (не доступный в Выпуске 1.0a).Измените правило встроенной аутентификации.

Настройте поставщика LDAP

1. Нажмите **LDAP**, щелкните правой кнопкой мыши **Поставщиков** и выберите **Create LDAP Provider**.
2. В диалоговом окне Create LDAP Provider добавьте эти подробные данные, которые были собраны ранее.Имя хоста или IP поставщикаСвяжите DNОсновной DNФильтрАтрибут (или CiscoAVPair или предопределенный атрибут, такой как

компанияПароль (пароль пользователя, используемого в связывать DN)
3. Нажмите **OK**, чтобы сохранить конфигурацию и закрыть диалоговое окно.

Примечание: Никакое другое значение не должно модифицироваться на этом экране. Правила группы LDAP не поддерживаются для Централизованной аутентификации UCS в этом выпуске.

Configure LDAP Provider Group

Примечание: В Выпуске 1.0a не поддерживаются группы поставщика. Эта процедура описывает, как настроить фиктивную группу поставщика для использования в конфигурации позже.

1. Нажмите **LDAP**, щелкните правой кнопкой мыши **Provider Group** и выберите **Create LDAP Provider Group**.
2. В диалоговом окне Create LDAP Provider Group введите имя для группы в Поле имени.
3. Из списка доступных поставщиков слева, выберите поставщика и нажмите большее, чем символ (**>**), чтобы переместить того поставщика к Назначенным Поставщикам справа.
4. Нажмите **OK**, чтобы сохранить изменения и закрыть экран.

Измените правило встроенной аутентификации

Выпуск 1.0a не поддерживает домены несколько серверов проверок подлинности как в Менеджере UCS. Для обхождения этого необходимо модифицировать правило встроенной аутентификации.

Собственная аутентификация имеет опцию для изменения аутентификации для входов в систему по умолчанию или регистрационных имен консоли. Так как составные домены не поддерживаются, можно использовать или локальную учетную запись или учетную запись LDAP, но не обоих. Измените значение именованной области (Realm) для использования или локальный или LDAP как источник аутентификации.

1. Нажмите **Authentication**, щелкните правой кнопкой мыши **Собственную Аутентификацию** и выберите **Properties**.
2. Определите, хотите ли вы Проверку подлинности по умолчанию, Консольную Аутентификацию или обоих. Используйте Проверку подлинности по умолчанию для GUI и интерфейса командной строки (CLI). Используйте Консольную Аутентификацию для представления основанной на ядре виртуальной машины (KVM) виртуальной машины (VM).
3. Выберите **ldap** из выпадающего списка именованной области (Realm). Значение именованной области (Realm) определяет или локальный, или LDAP является источником аутентификации.
4. Нажмите **OK** для закрытия страницы.
5. На странице Policies нажмите **Save** при необходимости для сохранения изменений.

Примечание: Не выходите из своего текущего сеанса или модифицируйте консольную аутентификацию, пока вы не проверяете, что проверка подлинности LDAP работает правильно. Консольная аутентификация предоставляет способ вернуться к предыдущей конфигурации. См. Сверять раздел.

Проверка

Эта процедура описывает, как протестировать проверку подлинности LDAP.

1. Откройте новый сеанс в Центральном UCS, и введите имя пользователя и пароль. Вы не должны включать домен или символ перед именем пользователя. Данный пример использует testucs в качестве пользователя от домена.
2. Если вы видите UCS Центральная информационная панель, проверка подлинности LDAP успешна. Пользователь отображен внизу страницы.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация