ISE административный портальный доступ с AD примером конфигурации учетных данных

Содержание

Введение

Этот документ описывает пример конфигурации для использования Microsoft Active Directory (AD) как внешнее хранилище идентификаторов для административного доступа к платформе Cisco Identity Services Engine (ISE) GUI управления.

Предварительные условия

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Конфигурация версий Cisco ISE 1.1.x или позже
- Microsoft AD

Используемый Componenets

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

- Версия 1.1 Cisco ISE. x
- Выпуск 2 Windows Server 2008 года

Сведения, представленные в этом документе, были получены от устройств, работающих в

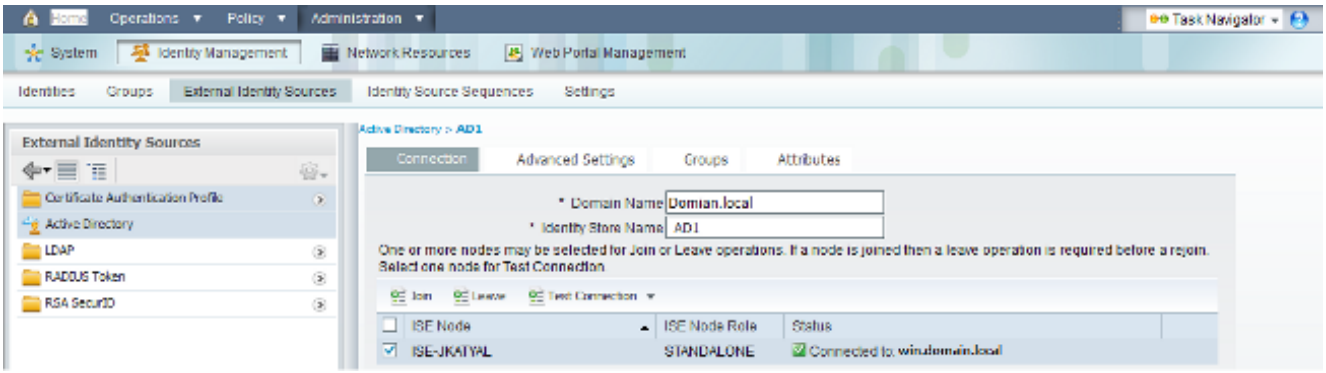
специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Настройка

Используйте этот раздел для настройки для использования Microsoft AD как внешнее хранилище идентификаторов для административного доступа к GUI управления Cisco ISE.

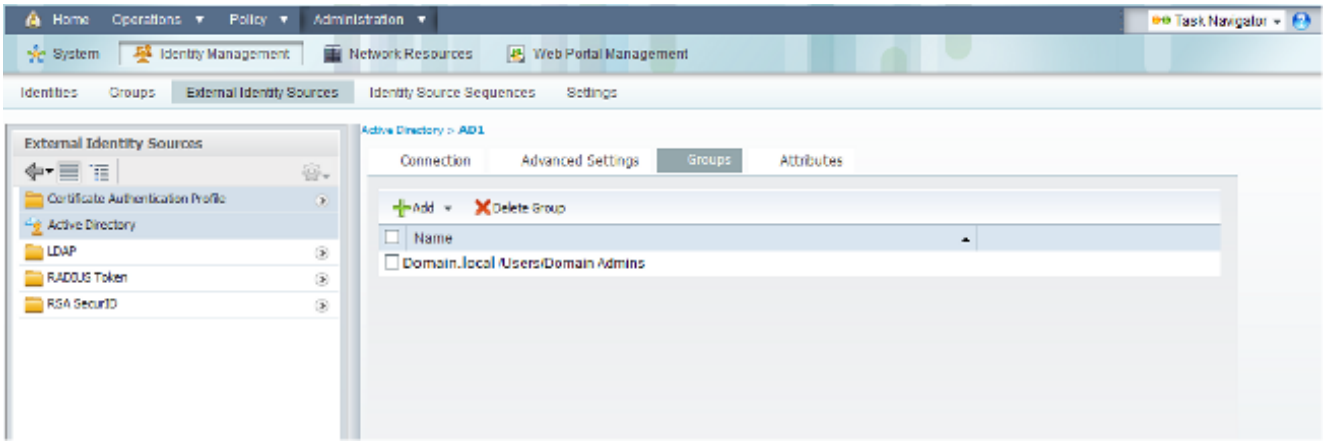
Соедините ISE с AD

1. Перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники> Active Directory**.
2. Введите AD Название магазина Доменного имени и Идентичности и нажмите **Join**.
3. Введите учетные данные AD учетной записи, которая может добавить и внести изменения в компьютерные объекты и нажать **Save Configuration**.



Выберите Directory Groups

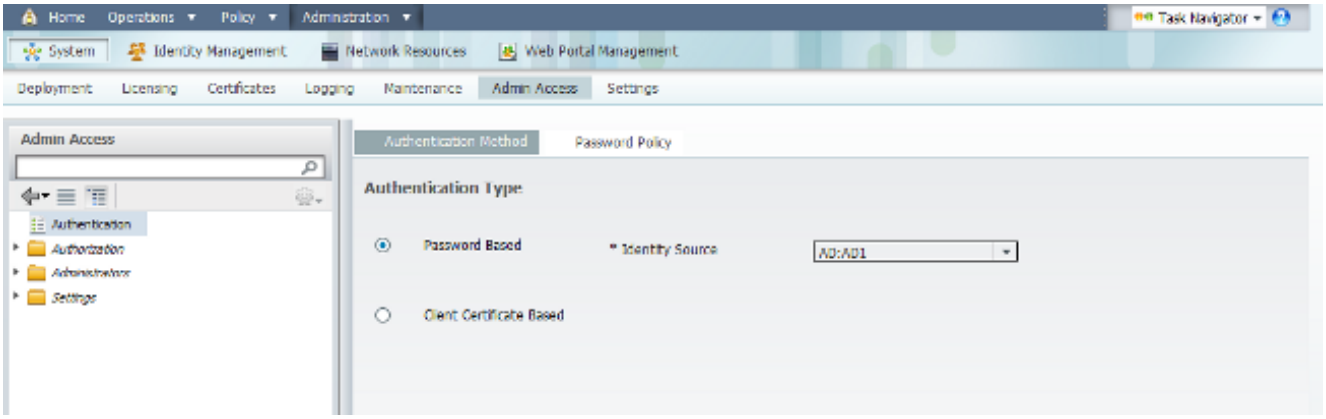
1. Перейдите к **администрированию> Управление идентификацией> Внешние Идентификационные Источники> Active Directory>, Группы> Добавляют>, Выбирают Каталог формы групп**.
2. Импортируйте по крайней мере одну AD Group, которой принадлежит ваш администратор.



Включите административный доступ для AD

Выполните эти шаги чтобы к основанной на enable password аутентификации для AD:

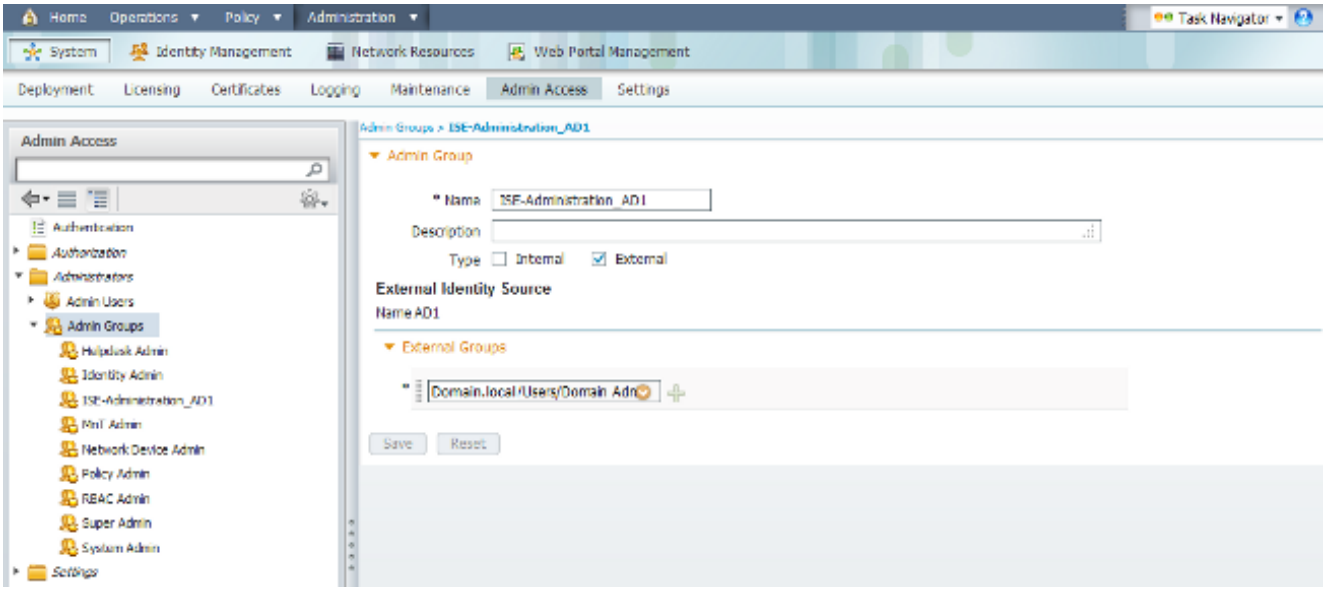
1. Перейдите к **администрированию> Система> Доступ администратора> Аутентификация**.
2. От **вкладки Authentication Method** выберите опцию **Password Based**.
3. Выберите **AD** от **Идентификационного Исходного** раскрывающегося меню.
4. **Нажмите кнопку Save Changes (Сохранить изменения).**



Настройте Admin Group к сопоставлению AD Group

Определите Admin Group Cisco ISE и сопоставьте его с AD группой. Это позволяет авторизации определить разрешения Роли базирующегося управления доступом (RBAC) для администратора на основе состава группы в AD.

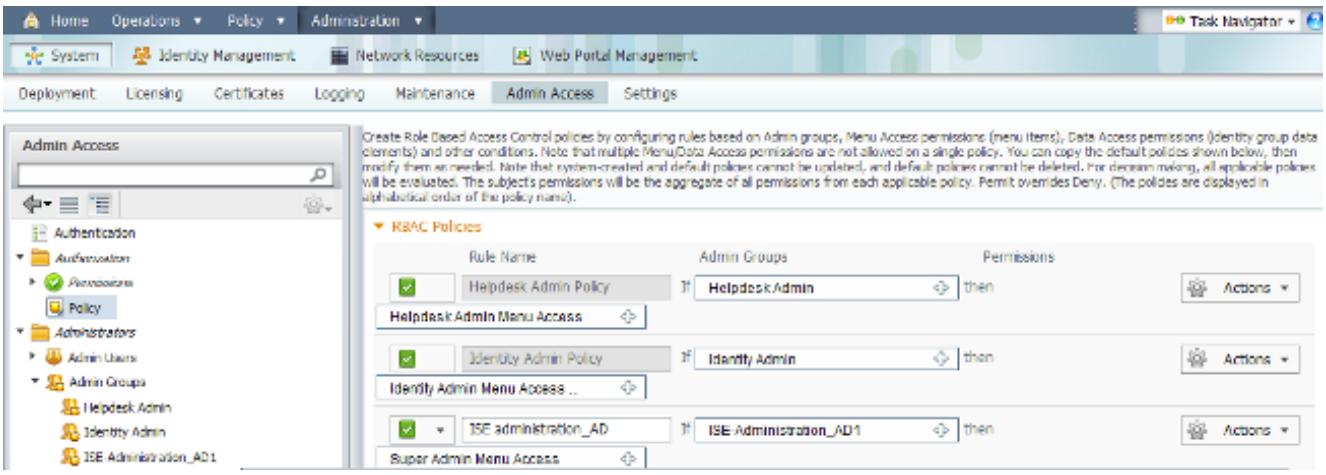
1. Перейдите к **администрированию> Система> Доступ администратора> Администраторы> Admin Group**.
2. **Нажмите Add** в заголовке таблицы для просмотра новой области конфигурации Admin Group.
3. Введите имя для новой Административной группы.
4. В поле Type установите флажок **Внешней проверки**.
5. От раскрывающегося меню **Внешних групп** выберите AD группу, с которой вы хотите, чтобы этот Admin Group сопоставил, как определено в Выбрать разделе Directory Groups.
6. **Нажмите кнопку Save Changes (Сохранить изменения).**



Набор разрешения RBAC для Admin Group

Выполните эти шаги для присвоения разрешений RBAC на Admin Group, созданных в предыдущем разделе:

1. Перейдите к **администрированию> Система> Доступ администратора> Авторизация> Политика**.
2. От раскрывающегося меню **Действий** справа, выберите **Insert New Policy Below** для добавления новой политики.
3. Создайте новое правило под названием **ISE_administration_AD**, сопоставьте его с Admin Group, определенным в Разрешать Административном доступе для AD раздела, и назначьте его разрешения.**Примечание:** В данном примере назначен Admin Group под названием **супер Admin**, который эквивалентен стандартной учетной записи администратора.
4. Нажмите **Save Changes**, и подтверждение сохраненных изменений отображено в нижнем правом углу GUI.



ISE доступа с AD учетными данными

Выполните эти шаги для доступа к ISE с AD учетными данными:

1. Выйдите из административного GUI.
2. Выберите **AD1** от **Идентификационного Исходного** раскрывающегося меню.
3. Введите имя пользователя и пароль от AD базы данных и войдите.

Примечание: Настройки по умолчанию ISE внутреннему пользователю хранят, если AD недостижим, или используемые учетные данные учетной записи не существуют в AD. Это упрощает быстрый журнал в том, если вы используете внутреннее хранилище, в то время как AD настроен для административного доступа.

Проверка

Чтобы подтвердить, что ваша конфигурация работает должным образом, проверьте проверенное имя пользователя в верхнем правом углу GUI ISE.

Устранение неполадок

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

Дополнительные сведения

- Руководство пользователя платформы Cisco Identity Services Engine, выпуск 1.1 - управляющий Indentities и доступом администратора
- Cisco Systems – техническая поддержка и документация