Добавление ролей в AxelNAC

Создание новой роли

Роли в AxelNAC можно создать в разделе **Конфигурация → Политики и контроль доступа → Роли** . На этой странице можно также ограничить количество устройств, которые могут регистрировать пользователи, имеющие определенные роли.

Разберем создание роли на примере роли сотрудника и роли АРМ. Для этого в разделе**Конфигурация → Политики и контроль доступа → Роли** нажмите **Новая роль** и укажите следующую информацию:

- **Имя:** Employee;
- **Описание:** Роль, используемая для сотрудников;
- **Максимальное число узлов на пользователя:** 2.

В данном примере мы разрешаем иметь одному пользователю сразу два зарегистрированных узла, т.к. сотрудник может иметь необходимость доступа к сети с нескольких устройств.

Выполните эти действия для другой роли:

- **Имя:** Domain_machine;
- **Описание:** Роль для АРМ, принадлежащих организации;
- **Максимальное число узлов на пользователя:** 1.

В данном примере мы разрешаем иметь одному пользователю лишь один зарегистрированный узел, т.к. эта роль назначается конкретному устройству.

Далее разберем пример использования этих двух ролей: Employee и Domain_machine. Сотрудниками и их доменным машинам с помощью Active Directory (по протоколу LDAP) будут назначены роли.

Использование роли Employee

Для того настроить назначение сотрудникам роли Employee, выполните следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** и нажмите **Новый внутренний источник**, после чего в выпадающем списке выберите **Active Directory**.

Шаг 2. В открывшемся окне заполните поля следующим образом:

- **Имя:** ad1;
- **Описание:** Active Directory для сотрудников;
- **Хост:** 192.168.1.2:389 (в поле **SSL/TLS** выберите значение **Нет**);
- **Базовое DN:** CN=Users, DC=acme, DC=local;
- **Диапазон:** Subtree;
- **Атрибут имени пользователя:** sAMAccountName;
- **Привязать DN:** CN=Administrator, CN=Users, DC=acme, DC=local;
- **Пароль:** acme123.

Пользователь, указываемый в поле **Привязать DN** должен обладать правами на просмотр домена.

Шаг 3. В поле **Правила аутентификации** нажмите **Добавить правило**, и заполните основные поля:

- **Статус:** Включено;
- **Имя:** Employee;
- **Описание:** Правило для всех сотрудников.

Не ставьте никаких условий, т.к. в примере мы рассматриваем универсальное правило.

Шаг 4. Нажмите **Добавить действие** и укажите следующие параметры:

- **Роль** — Employee;
- **Срок предоставления доступа** — 7 дней.

Шаг 5. Сохраните новый источник аутентификации, нажав **Создать**.

Шаг 6. Протестируйте подключение. При использовании этого источника аутентификации каждому пользователю, чье имя совпадает с именем в источнике (определяется с помощью sAMAccountName), будет выдаваться роль Employee с продолжительностью доступа 7 дней.

Использование роли Domain_machine

Если нужно разграничить аутентификацию пользователей и машин с помощью Active Directory, то один из способов сделать это — создать отдельный источник аутентификации для машин. Для этого необходимо выполнить следующие действия:

Шаг 1. Перейдите в раздел **Конфигурация → Политики и контроль доступа → Источники аутентификации** и нажмите **Новый внутренний источник**, после чего в выпадающем списке выберите **Active Directory**.

Шаг 2. В открывшемся окне заполните поля следующим образом:

- **Имя:** ad2;
- **Описание:** Active Directory для доменных машин;
- **Хост:** 192.168.1.2:389 (в поле **SSL/TLS** выберите значение **Нет**);
- **Базовый DN:** CN=Computers, DC=acme, DC=local;
- **Диапазон:** One-level;
- **Атрибут имени пользователя:** servicePrincipalName;
- **Привязать DN:** CN=Administrator, CN=Users, DC=acme, DC=local;
- **Пароль:** acme123.

Пользователь, указываемый в поле **Привязать DN** должен обладать правами на просмотр домена.

Шаг 3. В поле **Правила аутентификации** нажмите **Добавить правило**, и заполните основные поля:

- **Статус:** Включено;
- **Имя:** Machine;
- **Описание:** Правило для всех АРМ.

Не ставьте никаких условий, т.к. в примере мы рассматриваем универсальное правило.

Шаг 4. Нажмите **Добавить действие** и укажите следующие параметры:

- **Роль** — Corporate_machine;
- **Срок предоставления доступа** — 7 дней.

При такой конфигурации сотрудники могут подключать только доменных машины, но не личные устройства.

Шаг 5. Сохраните новый источник аутентификации, нажав **Создать**.

- Если правило определено как универсальное, то оно всегда будет работать, если атрибут имени пользователя совпадет с запрашиваемым. Это относится к источникам Active Directory, LDAP и Apache Htpasswd. Kerberos и RADIUS будут действовать универсально в любом случае.
- Если в источнике аутентификации нужно использовать другие LDAP-атрибуты, добавьте их в разделе **Конфигурация → Настройки системы → Основные настройки → Расширенные → Пользовательские атрибуты LDAP**. После этого они будут доступны в правилах, которые определил администратор.

ID статьи: 946
Последнее обновление: 3 июл., 2024
Обновлено от: Михалева А.
Ревизия: 3
База знаний AxelNAC -> Документация -> Система контроля доступа к сети «AxelNAC». Версия 2.1.0 -> AxelNAC. Руководство администратора -> Управление доступом к сети на основе ролей -> Добавление ролей в AxelNAC
https://docs.axel.pro/entry/946/