ALD Pro

ИНСТРУКЦИИ

УПРАВЛЕНИЕ ЗОНАМИ ОТВЕТСТВЕННОСТИ ПРИ АДМИНИСТРИРОВАНИИ

Версия 2.4.1

Содержание

Аннотация

Назначение документа: Особенности распределения зон ответственности при администрировании в крупных организациях, делегирование полномочий по подразделениям, распределение зон ответственности при администрировании через группы безопасности, понятие типов администраторов и возможностей по администрированию, настройка пользовательских типов администраторов.

Введение

Разграничение зон ответственности администраторов позволяет определять полномочия и/или зоны ответственности пользователей (администраторов ALD Pro), что обеспечивает удобство и информационную безопасность.

В ALD Pro реализованы следующие инструменты разграничения зон ответственности администраторов:

Пользовательские роли - создание пользовательских типов администратора, назначение их на пользователей и группы пользователей.

Назначение типа администратора - определение полномочий администраторов в соответствии с назначенным типом

Политики повышения возможностей по администрированию (SUDO) - возможность запрещать и разрешать определённым пользователям или группам выполнение конкретного набора программ, а также разрешить выполнение определённых программ без необходимости ввода своего пароля

Политики доступа к узлу (HBAC) - определение правил для настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов

Назначение типов администратора

3.1. Модель ALD Pro для типа администратора

Модель ALD Pro для типа администратора включает следующие сущности:

- **Разрешение** - право на выполнение операции/действия.
- **Возможности по администрированию** - “тематический” набор разрешений. Например, для управления группами пользователей необходимы разрешения на создание, удаление, редактирование группы пользователей. Эти три действия можно объединить в возможности по администрированию на управление группами пользователей. Аналогично можно создать возможности по администрированию на управление группами компьютеров.
- **Тип администратора** - набор возможностей по администрированию. Например, для выделенного типа, участники которой будут управлять только группами пользователей и группами компьютеров, можно назначить два вида возможностей (одна на управление группами пользователей, вторая - на управление группами компьютеров) вместо назначения множества разрешений на операции с группами, которые надо выбрать из большого общего списка разрешений.

Примечание: Любые возможности при администрировании запрещают создание и работу с следующими пользователями и группами пользователей:

Пользователи:

```
'root', 'daemon', 'bin', 'sys', 'sync', 'games', 'man', 'lp', 'mail', 'news',
↪ 'uucp', 'proxy', 'www-data', 'backup', 'list', 'irc', 'gnats', 'nobody',
↪'systemd-timesync', 'systemd-network', 'systemd-resolve', '_apt',
↪'messagebus', 'sshd', 'systemd-coredump', '_chrony', 'postgres',
↪'opendnssec', 'zabbix', '_rpc', 'statd', 'redis', 'sssd', 'custodia',
↪'dirsrv', 'bind', 'gluster', 'pkiuser', 'kdcproxy', 'ipaapi'
```

Группы пользователей:

```
'root', 'daemon', 'bin', 'sys', 'adm', 'tty', 'disk', 'lp', 'mail', 'news',
↪'uucp', 'man', 'proxy', 'kmem', 'dialout', 'fax', 'voice', 'cdrom', 'floppy
↪', 'tape', 'sudo', 'audio', 'dip', 'www-data', 'backup', 'operator', 'list',
↪ 'irc', 'src', 'gnats', 'shadow', 'utmp', 'video', 'sasl', 'plugdev',
↪'staff', 'games', 'users', 'nogroup', 'systemd-journal', 'systemd-timesync',
↪ 'systemd-network', 'systemd-resolve', 'crontab', 'input', 'kvm', 'render',
↪ 'netdev', 'messagebus', 'ssh', 'astra-admin', 'astra-console', 'systemd-
↪coredump', 'softhsm', '_chrony', 'ssl-cert', 'postgres', 'opendnssec',
↪'zabbix', 'redis', 'rdma', 'sssd', 'custodia', 'dirsrv', 'bind', 'gluster',
↪ 'sambashare', 'winbindd_priv', 'pkiuser', 'kdcproxy', 'ipaapi'
```

Функция назначения типа администратора предназначена для предоставления списка разрешений, т.е. действий, доступных обладателю конкретного типа администратора. Набор разрешений логически объединен в возможности. Конкретный вид возможности позволяет управлять только заданной группой параметров.

По умолчанию наборы возможностей разграничены между следующими типами:

- предустановленная роль главного администратора;
- роли для администрирования подразделов портала управления;
- роль на чтение всего портала;
- роль регионального администратора.

У пользователей есть возможность создать свои типы администраторов с требуемыми наборами возможностей.

Список доступных опций для каждого типа содержится в разделе **Управление доменом — Роли и права доступа — Типы администратора в системе — Таблица соответствий «Возможность (Доступный раздел/подраздел) - Роль администратора»**

В ALD Pro реализован механизм суммирования типов, т.е. при назначении пользователю нескольких типов все доступные возможности и разрешения суммируются.

Учетная запись, которой не присвоен ни один системный тип, имеет доступ только к Личному кабинету и не может использовать другие функции Системы.

Тип главного администратора по умолчанию назначен учетной записи admin.

Кроме типов администратора в разделе представлены базовые типы FreeIPA:

- ALDPRO - CIFS server

- ALDPRO - Organization units
- ALDPRO - Organizational Units Service Account
- ALDPRO - RuPost Service Integrations
- ALDPRO - SaltStack Administrators
- ALDPRO - Service Role
- ALDPRO - Trusts Service Account
- Enrollment Administrator
- helpdesk
- Security Architect
- User Administrator

Примечание: При назначении пользователю типа администратора для работы с порталом ALD Pro рекомендуется использовать типы, созданные пользователем, и типы с префиксом ALDPRO: предустановленный и пользовательские. Использование базовых типов FreeIPA без префекса ALDPRO не рекомендуется.

Для просмотра списка функций (возможностей при администрировании) доступных для конкретного типа администратора необходимо выбрать наименование необходимого типа, после чего, справа в связанной таблице отобразится перечень возможностей администратора (список разделов, подразделов ALD Pro, доступных для данного типа).

Управление типами администратора

Управление типами администратора доступно:

- из карточки **роли администратора**;
- из **карточки пользователя**.

Управление типами администратора из карточки роли осуществляется в разделе **Управление доменом — Роли и права доступа — вкладка Роли в системе - карточка Роли**. На вкладке в списке **Выбранные пользователи** приведен список пользователей, наделенных данным типом администратора. Доступна опция настройки данного списка.

Управление типами администратора из карточки пользователя осуществляется в разделе **Пользователи и компьютеры — Пользователи — карточка Пользователя — вкладка Роли**. На вкладке задаются типы, которыми будет наделена учетная запись пользователя.

Политики повышения возможностей при администрировании (SUDO)

Команда sudo (Substitute User and do, дословно «подменить пользователя и выполнить») предоставляет возможность пользователям выполнять команды от имени суперпользователя root, либо других пользователей. Правила, используемые sudo для принятия решения о предоставлении доступа, находятся в файле `/etc/sudoers` (для редактирования файла можно использовать специальный редактор `visudo`, запускаемый из командной строки без параметров, в том числе без указания пути к файлу); язык их написания и примеры использования подробно изложены в `man sudoers`.

В большинстве случаев грамотная настройка sudo делает небезопасную работу от имени суперпользователя ненужной. Все действия оказываются выполнимы из-под аккаунта пользователя, которому разрешено использовать sudo без ограничений. Имеется возможность запрещать и разрешать определённым пользователям или группам выполнение конкретного набора программ, а также разрешить выполнение определённых программ без необходимости ввода своего пароля.

ALD Pro позволяет настраивать правила разрешения и запрета на использование sudo для пользователей и групп пользователей. В правилах могут задаваться:

- Пользователи (группы пользователей), к которым применяются правила;
- Команды (группы команд), которые можно (нельзя) выполнять этим пользователям с применением sudo;
- Компьютеры (группы компьютеров), на которых применяется правило;
- Опции команды sudo, использующиеся при применении правила.

При инициализации контроллера (реплики) FreeIPA или при вводе клиента в домен FreeIPA система автоматически конфигурируется так, чтобы команда sudo использовала доменную службу sssd как источник данных о разрешениях использования sudo. Эта конфигурация задается в файле `/etc/nsswitch.conf`:

```
sudoers: files sss
```

где:

files — использовать данные из локального файла `/etc/sudoers`; sss — использовать данные, предоставленные службой `sssd`.

Служба `sssd`, в свою очередь, настроена таким образом, чтобы получать данные по правилам `sudo` от доменной службы каталогов (LDAP). Подробная информация по работе команды sudo приведена в справочной системе `man sudo`, `man sudoers`.

Примечание: Правила sudo не могут применяться к встроенной доменной группе хостов ipaserver, т.к. эта группа не имеет свойства `mepmanagedentry`, следовательно, не имеет в `objectclass` запись `mepOriginEntry`, что необходимо для идентификации группы. Это является особенностью схемы в FreeIPA.

Служба `sssd` выполняет кеширование данных с периодом обновления по умолчанию 5400 секунд. Для немедленного применения правил sudo необходимо очистить кеш, выполнив на клиентской машине следующие команды:

```
sudo systemctl stop sssd
sudo rm /var/lib/sss/db/*
sudo systemctl start sssd
```

Или воспользоваться инструментом `sssctl`, входящим в пакет `sssd-tools`:

```
sudo sssctl cache-remove
```

5.1. Команды sudo

В разделе Групповые политики — Политики повышения привилегий — вкладка Команды Sudo перечислены зарегистрированные команды Sudo, которые могут быть затронуты при создании правил Sudo. Регистрация команд Sudo осуществляется вручную.

5.1.1. Регистрация команды для использования в правилах sudo

Команды, которые будут далее использоваться в правилах sudo (т.е. которые далее могут выполняться от имени sudo указанными в правилах пользователями) должны быть зарегистрированы. Зарегистрировать можно любую команду, имеющуюся в системе, на

которой будет применяться правило. Для регистрации:

1. Перейти в раздел Групповые политики — Политики повышения привилегий — вкладка Команды Sudo;
2. Кликнуть кнопку “+ Новая команда”;
3. В появившемся окне карточки команды Sudo:
    - Указать полный путь расположения команды, которая должна выполняться от имени sudo (например, текстовый редактор `nano`, имеющий полный путь `/usr/bin/nano`);
    - Узнать полный путь расположения команды можно командой `which`, например `which nano`

Примечание: Пути расположения команд стандартны и обычно зависят от системы, однако в случае нестандартных системе может понадобиться получить пути на той машине, на которой будет применяться правило.

- Опционально указать описание команды в произвольной форме.

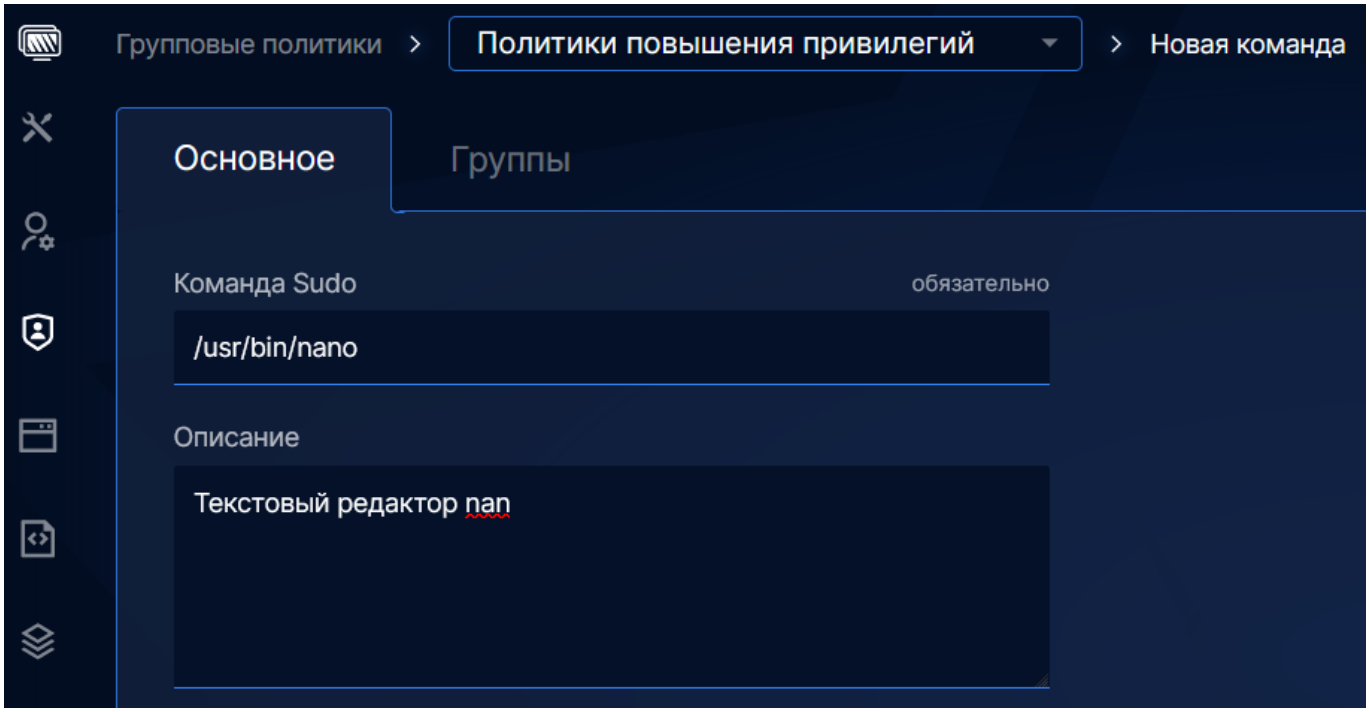

Рисунок 5.1 – Новая команда sudo

- Для сохранения и редактирования вкладки Группы нажать “Сохранить”. В результате указанная команда будет добавлена в список зарегистрированных команд. Далее эту

команду можно будет использовать в правилах sudo.

- Во вкладке **Группы** опционально настроить список групп команд sudo, в которые должны быть включена вновь добавленная команда.

5.2. Группы команд Sudo

В разделе **Групповые политики — Политики повышения привилегий — вкладка Группы команд Sudo** для удобства администратора возможно объединять несколько команд Sudo в группу.

Для создания новой группы команд Sudo необходимо нажать на кнопку **+ Новая группа**, будет выполнен переход в карточку новой группы. В карточке заполнить обязательное поле **Имя группы** и нажать кнопку **Сохранить**. Новая группа служб успешно создана, после чего доступен просмотр и настройка данной группы из ее карточки. Карточка группы содержит вкладки:

- **Основное** - отображается информация о группе команд Sudo: ее название и описание. Для редактирования доступно описание группы.
- **Команды** - осуществляется добавление команд Sudo в состав данной группы команд Sudo.

Для добавления команд Sudo в состав данной группы необходимо в списке **Все команды** отметить требуемые записи и перенести их в список **Выбранные команды**.

5.3. Создание правила sudo

Для создания нового правила sudo:

1. Перейти в раздел **Групповые политики — Политики повышения привилегий — вкладка Правила Sudo**.
2. Кликнуть кнопку **+ Новое правило**, будет выполнен переход в карточку нового правила.
3. В карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**. Остальные вкладки станут доступны после сохранения правила.

5.3.1. Настройка параметров правила sudo

Настройка правила sudo осуществляется во вкладках:

- **Параметры** — параметры для команды sudo. Например, наиболее распространенная опция - не запрашивать пароль у пользователя при использовании команды sudo (опция “!authenticate”). Если в правиле указать эту опцию, то указанные в правиле команды можно будет выполнять через sudo без ввода пароля, если опция не используется - то потребуется ввести пароль пользователя, выполняющего команду. Полный список поддерживаемых параметров см. в справочной системе: man sudoers
- **Пользователи** — список пользователей и групп пользователей, которым разрешено применять sudo в соответствии с правилом. Можно разрешить применять правило всем пользователям (группам пользователей);
- **Компьютеры** — список узлов в домене, на которых применяется правило. Можно разрешить применять правило на всех узлах;
- **Команды Sudo** — команды, к которым применяется данное правило. Возможно “Разрешить” или “Запретить” выполнение команды или группы команд (порядок объединения команд в группы см. далее), также возможно разрешить выполнять все команды;
- **Запуск от имени** — от имени какого пользователя или группы пользователей (не root-пользователя) может быть выполнена команда. При добавлении группы пользователей в “Группы пользователей запуска от имени” для выполнения команды могут использоваться идентификаторы пользователей (UID) членов этой группы. При добавлении в “Группы запуска от имени” для выполнения команды могут использоваться GID этой группы.

После внесения изменений в правило следует убедиться, что все изменения сохранены (кнопка **Сохранить** в начале формы) и нажать эту кнопку для сохранения изменений если она доступна.

5.4. Удаление или отключение правила

Для удаления или отключения правила:

1. Выбрать из списка правило, которое необходимо отключить или удалить;
2. Для отключения правила нажать кнопку **Отключить**, для удаления — **Удалить**.

Политики доступа к узлу (HBAC)

HBAC (Host-based access control) — набор правил для настройки доступа пользователей или групп пользователей к определенным хостам с использованием определенных сервисов. Например:

- ограничение доступа по ssh к контроллеру домена определенной локации только для группы администраторов этой локации;
- разрешение использовать только определенную службу для доступа определенным пользователям на определенных хостах.

Примечание:

- Правила предоставляют только разрешения доступа. Правила запрета доступа настроить невозможно.
- В домене ALD Pro по умолчанию установлено правило `allow_all`, которое после настройки и проверки своих правил следует отключить.
- FreeIPA хранит основную группу пользователя в виде числового значения атрибута gidNumber. В связи с этим, правила HBAC могут ссылаться только на дополнительные группы пользователя, но не на его основную группу.

6.1. Службы HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Службы HBAC** перечислены службы и программы, которые могут быть затронуты при создании правил HBAC. Например, `ftp, sshd, su, login`.

Администратор имеет возможность добавить любые необходимые службы.

6.2. Группы служб HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Группы служб HBAC** для удобства администратора возможно объединять несколько служб HBAC в группу.

Для создания новой группы служб необходимо нажать на кнопку **+ Новая группа**, будет выполнен переход в карточку новой группы. В карточке заполнить обязательное поле **Имя группы** и нажать кнопку **Сохранить**. Новая группа служб успешно создана, после чего доступен просмотр и настройка данной группы из ее карточки. Карточка группы содержит вкладки:

Основное - отображается информация о группе служб: ее название и описание. Для редактирования доступно описание группы.

Службы - осуществляется добавление служб HBAC в состав данной группы служб.

Для добавления служб HBAC в состав данной группы необходимо в списке **Все службы** отметить требуемые записи и перенести их в список **Выбранные службы**.

6.3. Добавление правила HBAC

В разделе **Групповые политики — Политики доступа к узлу — вкладка Правила HBAC** нажать кнопку **+ Новое правило**, откроется окно, в котором необходимо указать имя правила и нажать кнопку **Сохранить**. Новое правило успешно создано, после чего доступен просмотр и настройка данного правила из его карточки. Карточка правила содержит вкладки:

Основное - содержит информацию о правиле (название и описание) и опцию включения/отключения правила.

Пользователи - осуществляется настройка списка пользователей и/или групп пользователей, на которых будет применяться данное правило.

Компьютеры - осуществляется настройка списка рабочих станций и/или групп рабочих станций, на которые будет применяться данное правило.

Службы HBAC - осуществляется настройка списка служб и/или групп служб, использование которых будет регулироваться данным правилом.

Допускается указывать совместно пользователей и группы пользователей, компьютеры и группы компьютеров, службы и группы служб. При этом, если в группе находится только один элемент, и эта группа уже добавлена, то добавить этот элемент отдельно невозможно.

6.4. Отключение и удаление правила

Для отключения правила HBAC необходимо перейти в карточку правила и выбрать **Выключено**.

Удаление правила HBAC доступно как из карточки правила так и из общего списка правил.

Для удаления правила HBAC из карточки необходимо перейти в карточку правила, кликнуть кнопку **Удалить правило** и подтвердить удаление.

Для удаления правила из списка необходимо перейти к списку правил, отметить чек-боксом правило (несколько правил) на удаление и кликнуть кнопку **Удалить**.