

Инструкция по управлению зонами ответственности при администрировании

ALD Pro

Exported on 08/11/2023

Table of Contents

1	Введение	4
2	Делегирование прав на подразделение.....	5
2.1	Отображение делегирований после обновления Системы	5
2.1.1	Соответствие возможностей администрирования у делегирования и типов администраторов при преобразовании.....	5
3	Назначение типа администратора.....	7
3.1	Модель ALD Pro для типа администратора.....	7
3.2	Управление типами администратора.....	8
4	Политики повышения возможностей при администрировании (SUDO). 9	
4.1	Команды sudo	10
4.1.1	Регистрация команды для использования в правилах sudo	10
4.2	Группы команд Sudo	11
4.3	Создание правила sudo.....	11
4.4	Настройка параметров правила sudo.....	12
4.5	Удаление или отключение правила.....	12
5	Политики доступа к узлу (НВАС)	13
5.1	Службы НВАС	13
5.2	Группы служб НВАС	13
5.3	Добавление правила НВАС.....	13
5.4	Отключение и удаление правила.....	14

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](#)(see page 4)
- [Делегирование прав на подразделение](#)(see page 5)
 - [Отображение делегирований после обновления Системы](#)(see page 5)
- [Назначение типа администратора](#)(see page 7)
 - [Модель ALD Pro для типа администратора](#)(see page 7)
 - [Управление типами администратора](#)(see page 8)
- [Политики повышения возможностей при администрировании \(SUDO\)](#)(see page 9)
 - [Команды sudo](#)(see page 10)
 - [Группы команд Sudo](#)(see page 11)
 - [Создание правила sudo](#)(see page 11)
 - [Настройка параметров правила sudo](#)(see page 12)
 - [Удаление или отключение правила](#)(see page 12)
- [Политики доступа к узлу \(HBAC\)](#)(see page 13)
 - [Службы HBAC](#)(see page 13)
 - [Группы служб HBAC](#)(see page 13)
 - [Добавление правила HBAC](#)(see page 13)
 - [Отключение и удаление правила](#)(see page 14)

1 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:

- **Делегирование прав на подразделение** - определение полномочий администраторов по управлению объектами ALD Pro в рамках подразделения
- **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 (НВАС)** - определение правил для настройки доступа пользователей или групп пользователей к определённым хостам с использованием определённых сервисов

2 Делегирование прав на подразделение

Начиная с версии 2.0.0 ПК "ALD Pro" функционал делегирования перестает быть самостоятельным и входит в состав функционала зон ответственности при делегировании.

После обновления Системы до версии 2.0.0 все ранее созданные делегирования будут сохранены и преобразованы в типы администратора.

ВАЖНО

Все пользователи с делегированными зонами ответственности при делегировании продолжают работать в штатном режиме.

2.1 Отображение делегирований после обновления Системы

Преобразование делегирований в типы администратора происходит автоматически, без участия пользователя.

В таблице типов администратора (**Роли и права доступа->Роли в системе**) появляются пользовательские типы администратора с названием, описанием, пользователями, группами пользователей и возможностями администрирования, которые были заданы при создании делегирования.

2.1.1 Соответствие возможностей администрирования у делегирования и типов администраторов при преобразовании

Возможности администрирования у делегирований и типов администратора задавались разными способами.

В таблице представлено преобразование возможностей при администрировании у делегирований в возможности у типов администратора.

Возможности делегирования	Возможности типа администратора
Пользователи - Чтение	Users - Read, Organization units - Read
Пользователи - Добавление	Users - Add, User groups - Modify, Users - Read
Пользователи - Изменение	Users - Modify, Users - Set organization unit, Users - Read
Пользователи - Удаление	Users - Read trash, Users - Move to trash, Users - Read
Подразделения - Чтение	Organization units - Read
Подразделения - Добавление	Organization units - Add, Organization units - Read
Подразделения - Изменение	Organization units - Modify, Organization units - Read

Возможности делегирования	Возможности типа администратора
Подразделения - Удаление	Organization units - Delete, Organization units - Read
Группы пользователей - Чтение	User groups - Read, Organization units - Read
Группы пользователей - Добавление	User groups - Add, User groups - Read
Группы пользователей - Изменение	User groups - Set organization unit, User groups - Set group membership, User groups - Modify, User groups - Read
Группы пользователей - Удаление	User groups - Delete, User groups - Read
Компьютеры - чтение	Computers - Read, Organization units - Read, DNS Entries - Read, IPA Servers - Read, Sites - Read, Subsystems - Read, Computers - Remote access
Компьютеры - Добавление	-
Компьютеры - Изменение	Computers - Set organization unit, Computers - Modify, Computers - Read, Organization units - Read, DNS Entries - Read
Компьютеры - Удаление	Computers - Delete, Computers - Read, Organization units - Read, DNS Entries - Read
Группы компьютеров - Чтение	Computer groups - Read, Organization units - Read
Группы компьютеров - Добавление	Computer groups - Add, Computer groups - Read
Группы компьютеров - Изменение	Computer groups - Set organization unit, Computer groups - Set group membership, Computer groups - Modify, Computer groups - Read
Группы компьютеров - Удаление	Computer groups - Delete, Computer groups - Read

ВАЖНО

Users - Read trash, Users - Move to trash - новые возможности при администрировании, что позволяет расширить удаление пользователей в делегировании.

3 Назначение типа 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 две вида возможности (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.

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

Наборы возможностей жестко разграничены (без возможности настройки) между тремя типами:

- главный администратор
- системный администратор
- администратор информационной безопасности.

Список доступных опций для каждого типа содержится во встроенном **Справочном центре ALD Pro** в разделе **Управление доменом — Роли и права доступа — Роли в системе — Таблица соответствий «Привилегия (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 присвоена ни один системный тип не имеет доступа к функциям Системы.

Тип главного администратора по умолчанию назначена учетной записи `admin`.

Кроме типов администратора в разделе представлены базовые типы FreeIPA:

- CIFS server;
- Enrollment Administrator;
- Organization units;
- RuPost Service Integrations;
- Saltstack Administrators;
- Security Architect;
- Service Role;
- User Administrator;
- helpdesk.

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).

3.2 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**. 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 Назначенные роли**. На вкладке задаются типы, которыми будет наделена учетная запись пользователя.

4 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`.

ВАЖНО:

Правила `sudo` не могут применяться к встроенной доменной группе хостов `ipaserver`, т.к. эта группа не имеет свойства `mermanagedentry`, следовательно, не имеет в `objectclass` запись `merOriginEntry`, 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
```

4.1 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.

4.1.1 Регистрация команды для использования в правилах sudo

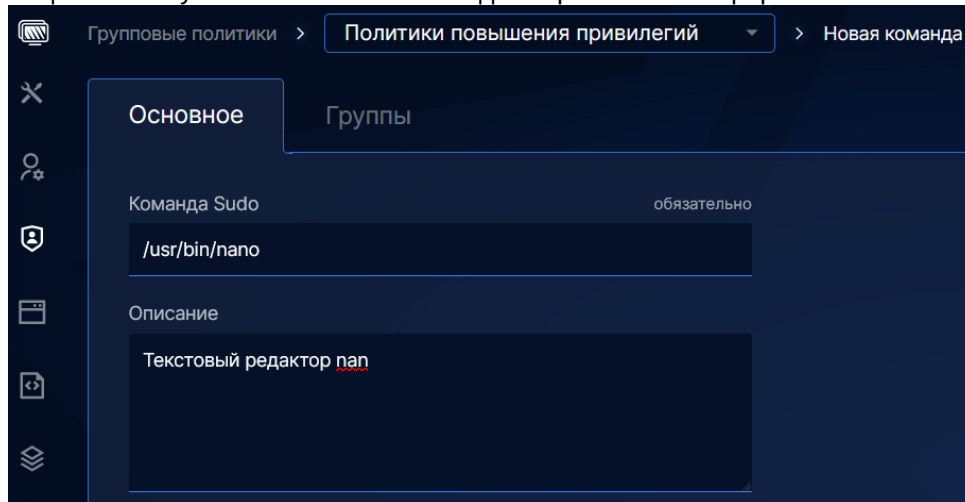
Команды, которые будут далее использоваться в правилах sudo (т.е. которые далее могут выполняться от имени sudo указанными в правилах пользователями) должны быть зарегистрированы. Зарегистрировать можно любую команду, имеющуюся в системе, на которой будет применяться правило. Для регистрации:

1. Перейти в раздел **Групповые политики — Политики повышения привилегий — вкладка Команды Sudo**
2. Кликнуть кнопку "+ Новая команда";
3. Выбрать в выпадающем меню "Sudo" пункт "Команды Sudo" и нажать "Добавить";
4. 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
```

пути расположения команд стандартны и не обычно зависят от системы, однако в случае нестандартных систем может потребоваться получить пути на той машине, на которой будет применяться правило.

- Опционально указать описание команды в произвольной форме.



- 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 команда sudo, в которые должны быть включена вновь добавленная команда

4.2 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 на карточку новой группы. На 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**.

4.3 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 на карточку нового правила
3. На карточке на вкладке **Основное** заполнить обязательное поле **Имя правила**. Остальные вкладки станут доступны после сохранения правила.

4.4 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 потребуются 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.

4.5 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".

5 Политики доступа к узлу (НВАС)

НВАС (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.

ВАЖНО:

- 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 НВАС могут ссылаться только на дополнительные группы пользователя, но не на его основную группу.

5.1 Службы НВАС

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

Администратор имеет возможность добавить любые необходимые службы.

5.2 Группы служб НВАС

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

Для создания новой группы служб необходимо нажать на кнопку **+ Новая группа**, будет выполнен переход на карточку новой группы. На 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 НВАС в состав данной группы служб.

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

5.3 Добавление правила НВАС

В разделе **Групповые политики — Политики доступа к узлу — вкладка Правила НВАС** 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 НВАС** - 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.

5.4 Отключение и удаление правила

Для отключения правила НВАС необходимо перейти в карточку правила и выбрать "Выключено".

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

Для удаления правила НВАС 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**.