

Руководство по установке

Granulex Recovery для ALD Pro/FreelPA v2.5.0

Последнее обновление: январь 2026

Введение

Настоящий документ является руководством по установке программного обеспечения Granulex Recovery, содержит перечень минимальных системных требований, описание процесса установки и первоначальной настройки.

Подготовка к установке

Для корректной установки, настройки и работы продукта Granulex Recovery обеспечьте соответствие системным требованиям.

Системные требования

Для установки продукта Granulex Recovery требуется сервер с соответствующими аппаратными и программными характеристиками.

ВАЖНО! Сервер Granulex Recovery, компьютер и учетная запись пользователя (оператора) должны входить в состав домена ALD Pro/FreelPA.

Требования к аппаратному обеспечению

Минимальные требования, предъявляемые к аппаратному обеспечению сервера, на который устанавливается продукт Granulex Recovery, в зависимости от **общего** количества объектов в каталоге:

Наименование	до 100 000	до 300 000	до 1 200 000	более 1 200 000
Архитектура	x64	x64	x64	x64
Количество ядер и частота ЦП (CPU)	2 x 3.6 ГГц	2 x 3.6 ГГц	2 x 3.6 ГГц	2 x 3.6 ГГц
Объем оперативной памяти (RAM)	4 Гб	8 Гб	16 Гб	24 Гб
Объем жесткого диска	20 Гб	40 Гб	80 Гб	120 Гб

ВНИМАНИЕ: Общее количество объектов в каталоге НЕ РАВНО количеству учётных записей пользователей.

Определить **примерное** общее количество объектов в каталоге по количеству учётных записей пользователей можно по формулам ниже:

- для каталога ALDPro: ("Количество учётных записей пользователей" * 3 + "Количество учётных записей компьютеров" + "Количество групп") * Коэффициент 1.2

- для каталога FreeIPA: ("Количество учётных записей пользователей" * 2 + "Количество учётных записей компьютеров" + "Количество групп") * Коэффициент 1.2

Для точного определения можно воспользоваться командой:

```
ldapsearch -h dc01.granulex.test -x -D uid=admin,cn=users,cn=accounts,dc=granulex,dc=test -W -b "dc=granulex,dc=test" "(objectclass=*)" dn | grep -c "^dn:"
```

Вывод команды:

```
$ ldapsearch -h dc01.granulex.test -x -D uid=admin,cn=users,cn=accounts,dc=granulex,dc=test -W -b "dc=granulex,dc=test" "(objectclass=*)" dn | grep -c "^dn:"
Enter LDAP Password:
2865
```

Требования к программному обеспечению

Корректная установка и работа продукта Granulex Recovery обеспечивается при использовании следующих программных компонентов:

Наименование	Значение
ОС	Astra Linux Special Edition 1.7.4 или выше
Уровень защищённости	Максимальный (режим «Смоленск»)
Мандатный контроль целостности (МКЦ)	Включён
Веб-браузер	Mozilla Firefox версии 114 или выше
Службы каталога LDAP	389 Directory Server в составе пакетов: FreeIPA (входит в дистрибутив ОС) или ALD Pro версии 2.1 или выше

Права доступа и полномочия

Необходимые права доступа и полномочия для установки продукта

Права доступа на сервере

Для установки продукта Granulex Recovery необходимо зайти на сервер с доменной учётной записью. Эта учетная запись должна обладать правами на использование `sudo` для запуска команд при установке пакета Granulex Recovery.

Права доступа в каталоге ALD Pro/FreeIPA

В процессе первоначальной установки продукта или его полной переустановки в каталоге ALD Pro/FreeIPA создаются необходимые служебные объекты. Для корректного создания этих объектов мастер установки запрашивает имя и пароль администратора домена ALD Pro/FreeIPA (учётную запись, входящую в группу *admins*).

Примечание: Запрашиваемые учётные данные используются **только** в момент установки продукта, **только** для выполнения операций создания объектов. Эти данные нигде не сохраняются и в дальнейшем не используются.

Убедитесь, что пользователь, устанавливающий продукт, обладает необходимыми и достаточными правами в каталоге на выполнение операций создания объектов:

Наименование объекта	Тип	Назначение
<i>granulex_backup_svc</i>	Пользователь	Служебный пользователь для создания автоматических резервных копий LDAP-каталога по расписанию. <i>Примечание: имя учётной записи, отличное от значения по умолчанию, может быть задано во время установки продукта.</i>
<i>granulex_backup</i>	Группа	Служебная группа, в которую входит служебный пользователь <i>granulex_backup_svc</i> . Используется для назначения необходимых прав доступа к объектам каталога для данного служебного пользователя.
<i>HTTP/server.example.com@EXAMPLE.COM</i>	Служба	Служба HTTP. Используется сервером Apache2 для Kerberos-аутентификации подключающихся к нему конечных пользователей продукта.
<i>granulex_backup_operators</i>	Группа	Служебная группа для операторов резервного копирования.

Примечание: Имя служебного пользователя *granulex_backup_svc*, имя служебной группы *granulex_backup* и имя группы операторов резервного копирования *granulex_backup_operators* могут быть заданы во время установки продукта. Приведённые значения являются значениями по умолчанию.

Необходимые права доступа и полномочия для работы с продуктом

В таблице ниже приведены операции чтения и записи, необходимые для выполнения основных операций Granulex Recovery:

Наименование операции	Действие
Резервное копирование	Чтение из каталога LDAP, запись данных на диск

Наименование операции	Действие
Сравнение	Чтение данных с диска и из каталога LDAP
Восстановление	Чтение данных с диска и запись в каталог LDAP

Для корректного выполнения данных операций в продукте Granulex Recovery реализован механизм разграничения прав доступа на основе членства в группах ALD Pro/FreelPA. Убедитесь, что учётные записи конечных пользователей продукта являются членами соответствующих групп:

Операция	Наименование группы
Создание резервных копий каталога вручную	<i>admins</i> или <i>granulex_backup_operators</i>
Сравнение резервной копии с каталогом	<i>admins</i> или <i>granulex_backup_operators</i>
Восстановление объектов и атрибутов в каталоге	<i>admins</i>
Создание резервных копий каталога автоматически, по расписанию	<i>granulex_backup</i>

Получение установочного пакета

Установочный пакет программного продукта Granulex Recovery доступен для скачивания на сайте <https://granulex.ru>.

Получение файла лицензионного ключа

Программное обеспечение Granulex Recovery является коммерческой разработкой ООО «МД Информационные Системы», распространяется на условиях лицензионного соглашения и требует наличия и установки файла действующего лицензионного ключа (далее «Лицензия»).

Для получения файла лицензионного ключа обратитесь к представителю отдела продаж компании «МД Информационные Системы» или компании-партнёра. Необходимые контактные данные для связи указаны на сайте <https://granulex.ru>.

Установка продукта

Требования перед началом установки

1. Убедитесь, что компьютер является членом домена (установлен доменный клиент)

ВНИМАНИЕ! Компьютер должен входить в состав домена!

2. Убедитесь, что в системе включён режим мандатного контроля целостности (МКЦ). Для этого выполните команду:

```
sudo astra-mic-control status
```

Ожидаемый вывод команды:

```
$ sudo astra-mic-control status
АКТИВНО
```

3. Убедитесь, что в системе установлен максимальный уровень защищённости (режим «Смоленск»). Для этого выполните команду:

```
sudo astra-modeswitch get
```

Ожидаемый вывод команды:

```
$ sudo astra-modeswitch get
2
```

4. Синхронизируйте время:

```
ntpdate -u pool.ntp.org
```

Вы можете использовать любой другой сервер времени.

5. Войдите в систему под доменной учетной записью, которая будет использоваться для установки продукта с **высоким уровнем целостности** (63). Для проверки разрешённых уровней целостности у учётной записи введите команду:

```
sudo pdpl-user admin
```

Ожидаемый вывод команды:

```
$ sudo pdpl-user admin
минимальная метка: Уровень_0:Низкий:Нет:0x0
0:0:0x0:0x0
максимальная метка: Уровень_0:Высокий:Нет:0x0
0:63:0x0:0x0
```

6. Убедитесь, что учётная запись пользователя, которая будет использоваться для установки продукта является членом доменной группы *admins*
7. Проверьте наличие установленных мандатных уровней конфиденциальности (минимальный и максимальный) у учётной записи. Для проверки введите команду:

```
ipa user-show admin --all | grep x-ald-user-mac
```

Если вывод команды отсутствует, то значения атрибутов «x-ald-user-mac» не заданы и их необходимо задать командой:

```
ipa user-mod admin --macmin 0 --macmax 0
```

8. При установке продукта на Astra Linux Special Edition 1.8.x необходимо установить параметр `use_fully_qualified_names` (использовать полные имена пользователей вида `username@EXAMPLE.COM` при аутентификации в системе) в значение `False` в файле `/etc/sss/sss.conf`. Это требование связано с особенностями работы модуля `mod_auth_gssapi` в составе веб-сервера Apache с включённым режимом `Astra mode`; при установленном значении `True` системная функция `getpwnam(имя_пользователя)` отрабатывает некорректно и выдаёт ошибку `user not found`. В результате, веб-сервер Apache не может корректно использовать аутентификационные данные пользователя и выполнять запросы от его имени. Пример установки параметра в файле `/etc/sss/sss.conf`:

```
use_fully_qualified_names = False
```

Установка необходимых пакетов

Перед установкой пакета Granulex Recovery выполните следующие действия:

1 Обновите базу репозитория пакетов при помощи команды:

```
sudo apt update
```

Рекомендуем использовать **frozen**-репозиторий текущей версии операционной системы для установки всех необходимых пакетов.

2 Установите пакет веб-сервера Apache2 и дополнительные модули:

```
sudo apt install -y apache2 libapache2-mod-auth-gssapi libapache2-mod-wsgi-py3
```

Для проверки установленной версии пакета `apache2` воспользуйтесь командой:

```
/usr/sbin/apache2 -v
```

Вывод команды:

```
$ /usr/sbin/apache2 -v
Server version: Apache/2.4.52 (AstraLinux)
Server built:   2023-06-13T09:18:32
```

3 Установите следующие библиотеки и утилиты:

```
sudo apt install -y python*-venv memcached dialog whiptail
```

Запуск программы установки продукта

Для установки пакета Granulex Recovery из репозитория выполните команду:

```
sudo apt install granulex
```

Если пакет получен на переносном носителе, то для его установки выполните команду:

```
sudo dpkg -i granulex_x.x.x-xxx_amd64.deb
```

Далее следуйте инструкциям мастера установки.

Мастер установки

Шаг 1

Необходимо ввести имя учетной записи администратора ALD Pro/FreelPA.

[Шаг 1 из 12] Аутентификация

Пожалуйста, введите имя учётной записи администратора домена ALD Pro/FreelPA.

Эта учётная запись будет использована только в процессе текущей установки продукта и НЕ будет сохранена где-либо для дальнейшего применения.

Имя учётной записи администратора ALD Pro/FreelPA: _____

Шаг 2

Необходимо ввести пароль учетной записи администратора ALD Pro/FreelPA.

[Шаг 2 из 12] Аутентификация

Пароль учётной записи администратора ALD Pro/FreelPA: _____

Шаг 3

Необходимо ввести имя учетной записи HTTP-сервера Apache2.

[Шаг 3 из 12] Настройка HTTP-сервера Apache2

Granulex Recovery требует наличия HTTP-сервера Apache2. Пожалуйста, задайте имя локальной учётной записи, от которой будет выполняться процесс HTTP-сервера (по умолчанию: www-data). Если пользователь с таким именем не существует, он будет создан.

Имя учётной записи HTTP-сервера Apache2: www-data

Шаг 4

Необходимо ввести имя группы HTTP-сервера Apache2.

Настройка HTTP-сервера Apache2

Учётная запись, от которой выполняется процесс HTTP-сервер Apache2 должна быть членом локальной группы на этом сервере. Пожалуйста, задайте имя локальной группы, в которую будет добавлена учётная запись HTTP-сервера (по умолчанию: www-data). Если группа с таким именем не существует, она будет создана.

Имя группы HTTP-сервера Apache2: www-data

Шаг 5

Необходимо ввести порт HTTP-сервера Apache2.

Настройка HTTP-сервера Apache2

Укажите номер порта, по которому будет доступен сервис Granulex Recovery (по умолчанию: 80).

Порт HTTP-сервера Apache2: 80

Шаг 6

Необходимо ввести путь к папке с логами HTTP-сервера Apache2.

Настройка HTTP-сервера Apache2

Укажите папку, в которой будут храниться логи HTTP-сервера Apache2 (по умолчанию: /var/log/apache2).

Путь к папке с логами HTTP-сервера Apache2: /var/log/apache2

Шаг 7

Необходимо ввести путь к папке запуска HTTP-сервера Apache2.

Настройка HTTP-сервера Apache2

Укажите папку запуска HTTP-сервера Apache2 (по умолчанию: /var/run/apache2).

Путь к папке запуска HTTP-сервера Apache2: /var/run/apache2

Шаг 8

Необходимо ввести имя учётной записи сервиса HTTP.

Настройка HTTP-сервера Apache2

Укажите имя учётной записи HTTP-сервиса Apache2 в домене ALD Pro/FreeIPA (формат: HTTP/servername.example.com). Если сервисная учётная запись с таким именем в домене не существует, она будет создана. Данная сервисная учётная запись будет использоваться HTTP-сервером Apache2 для аутентификации подключающихся к нему пользователей посредством стандартного механизма Kerberos.

Имя учётной записи сервиса HTTP: _____

Шаг 9

Необходимо ввести путь к папке резервных копий.

Резервное копирование

Укажите папку, в которой будут храниться резервные копии LDAP-каталога, создаваемые Granulex Recovery (по умолчанию: /var/opt/granulex/backup).

Путь к папке резервных копий: /var/opt/granulex/backup

Шаг 10

Необходимо ввести имя группы операторов резервного копирования.

Резервное копирование

Задайте имя группы операторов резервного копирования (по умолчанию: granulex_backup_operators). Если группа с таким именем в домене не существует, она будет создана. Данная группа должна обладать правами на "чтение всех объектов" и "чтение всех атрибутов" в каталоге ALD Pro/FreeIPA. Члены этой группы будут иметь возможность создавать резервные копии каталога (по требованию), настраивать расписания автоматического резервного копирования, проводить операции сравнения данных в выбранной резервной копии с текущими данными в каталоге, формировать детальные отчеты по результатам сравнения, просматривать журнал событий.

Имя группы операторов: granulex_backup_operators

Шаг 11

Необходимо ввести имя служебного пользователя для операций автоматического резервного копирования.

Резервное копирование

Задайте имя служебного пользователя, который будет использоваться для автоматического создания резервных копий LDAP-каталога (по умолчанию: granulex_backup_svc). Если учётная запись с таким именем в домене не существует, она будет создана. Данная учётная запись будет использоваться, когда вы настроите расписание автоматического резервного копирования (после установки продукта). Подробное описание процесса настройки автоматического резервного копирования приведено в «Руководстве пользователя».

Имя пользователя: granulex_backup_svc

Шаг 12

Необходимо ввести имя группы для служебного пользователя, который будет использоваться для операций автоматического резервного копирования.

Резервное копирование

Задайте имя группы, в которую будет добавлен служебный пользователь для операций автоматического резервного копирования (по умолчанию: granulex_backup). Если группа с таким именем в домене не существует, она будет создана. Данная группа должна обладать правами на «чтение всех объектов» и «чтение всех атрибутов» в каталоге ALD Pro/FreeIPA.

Имя группы: `granulex_backup`

Подготовка продукта к работе

Назначение необходимых прав доступа

ВНИМАНИЕ! Действия по назначению необходимых прав доступа, описанные ниже, являются обязательными! В противном случае, резервные копии, создаваемые по расписанию, а также создаваемые операторами резервного копирования вручную будут неполными.

Служебный пользователь `granulex_backup_svc` (используется для создания резервных копий каталога по расписанию), а также операторы резервного копирования (члены группы `granulex_backup_operators`) должны обладать правами на чтение всех объектов и всех атрибутов каталога. Для выдачи этих прав следуйте инструкциям ниже.

Права доступа для создания резервных копий каталога по расписанию

Для выдачи прав доступа на чтение всех объектов и всех атрибутов каталога служебному пользователю `granulex_backup_svc` воспользуйтесь встроенным механизмом разграничения и контроля доступа в каталоге ALD Pro/FreelPA - Access Control Instructions (aci).

Примечание: В примере ниже значение атрибута `aci` разбито на несколько строк для удобства отображения. В LDIF-файле это значение должно быть записано как одна непрерывная строка без переносов.

Примечание: В примерах и командах ниже используйте имя домена и имя контроллера домена, актуальные для вашей среды.

1. Создайте текстовый файл следующего содержания:

```
dn: dc=granulex,dc=test
changetype: modify
add: aci
aci: (targetattr = "*")(target = "ldap:///dc=granulex,dc=test")(version 3.0; aci
"Allow granulex_backup group read all objects and all attributes in the
directory"; allow (search, read) groupdn =
"ldap:///cn=granulex_backup,cn=groups,cn=accounts,dc=granulex,dc=test");)
```

2. Сохраните файл на диске. Например, с именем `granulex_backup_add_aci.ldif`

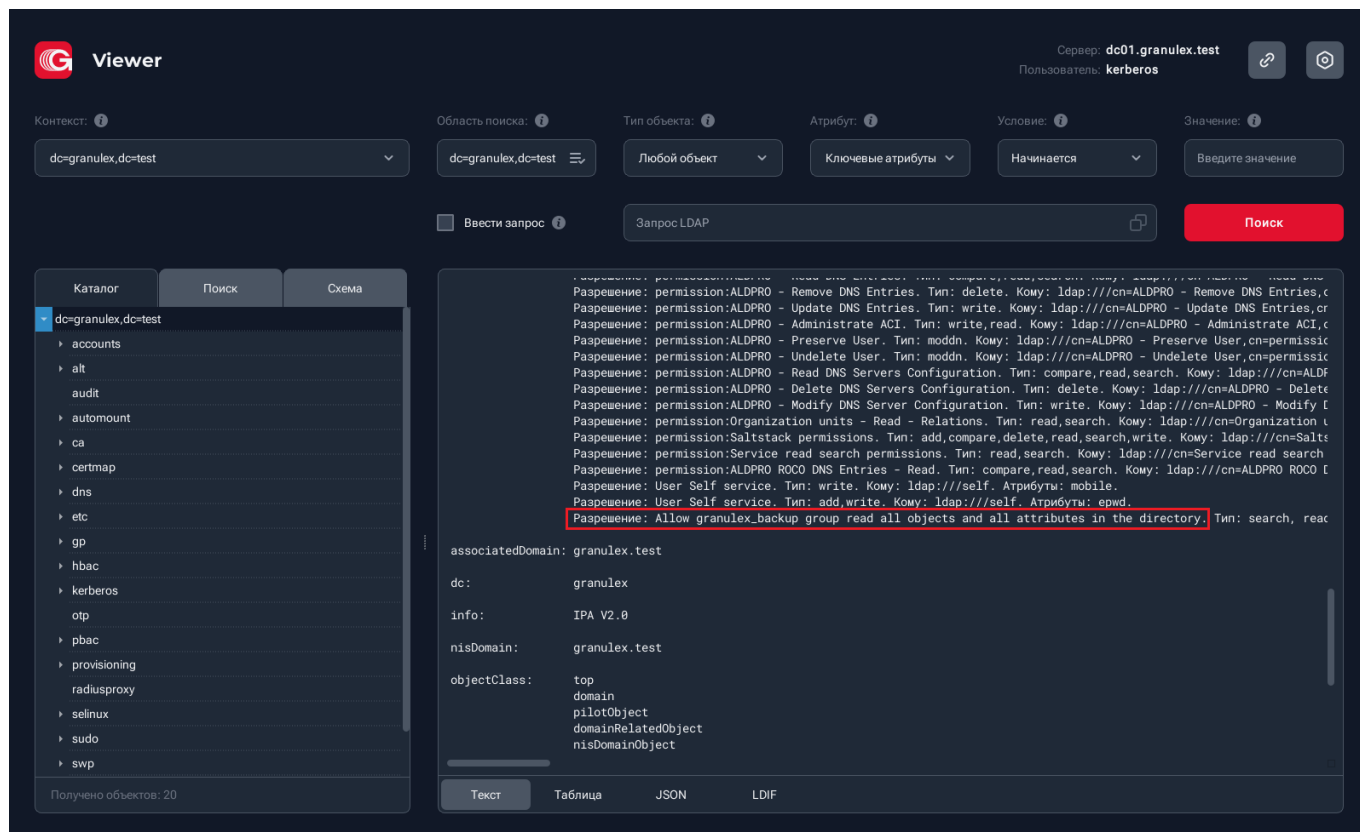
3. Откройте окно терминала и выполните команду:

```
ldapadd -h dc-01.granulex.test -f granulex_backup_add_aci.ldif
```

В результате выполнения этой команды в атрибут `aci` объекта «домен» (самый верхний уровень в иерархии раздела каталога, в котором хранятся данные пользователей - domain naming context) будет добавлена инструкция, наделяющая группу `granulex_backup` необходимыми правами доступа. Проверить добавление нужного значения можно при помощи команды:

```
ldapsearch -h dc-01.granulex.test dc=granulex aci
```

Либо воспользоваться графической утилитой для просмотра данных каталога. Например, Granulex Viewer:



Права доступа для операторов резервного копирования

Для выдачи прав доступа на чтение всех объектов и всех атрибутов каталога членам группы *granulex_backup_operators* (операторы резервного копирования) воспользуйтесь встроенным механизмом разграничения и контроля доступа в каталоге ALD Pro/FreeIPA - Access Control Instructions (aci).

Примечание: В примере ниже значение атрибута **aci** разбито на несколько строк для удобства отображения. В LDIF-файле это значение должно быть записано как одна непрерывная строка без переносов.

Примечание: В примерах и командах ниже используйте имя домена и имя контроллера домена, актуальные для вашей среды.

1. Создайте текстовый файл следующего содержания:

```
dn: dc=granulex,dc=test
changetype: modify
add: aci
aci: (targetattr = "*")(target = "ldap:///dc=granulex,dc=test")(version 3.0; aci
"Allow granulex_backup_operators group read all objects and all attributes in the
directory"; allow (search, read) groupdn =
"ldap:///cn=granulex_backup_operators,cn=groups,cn=accounts,dc=granulex,dc=test";)
```

2. Сохраните файл на диске. Например, с именем **granulex_backup_operators_add_aci.ldif**

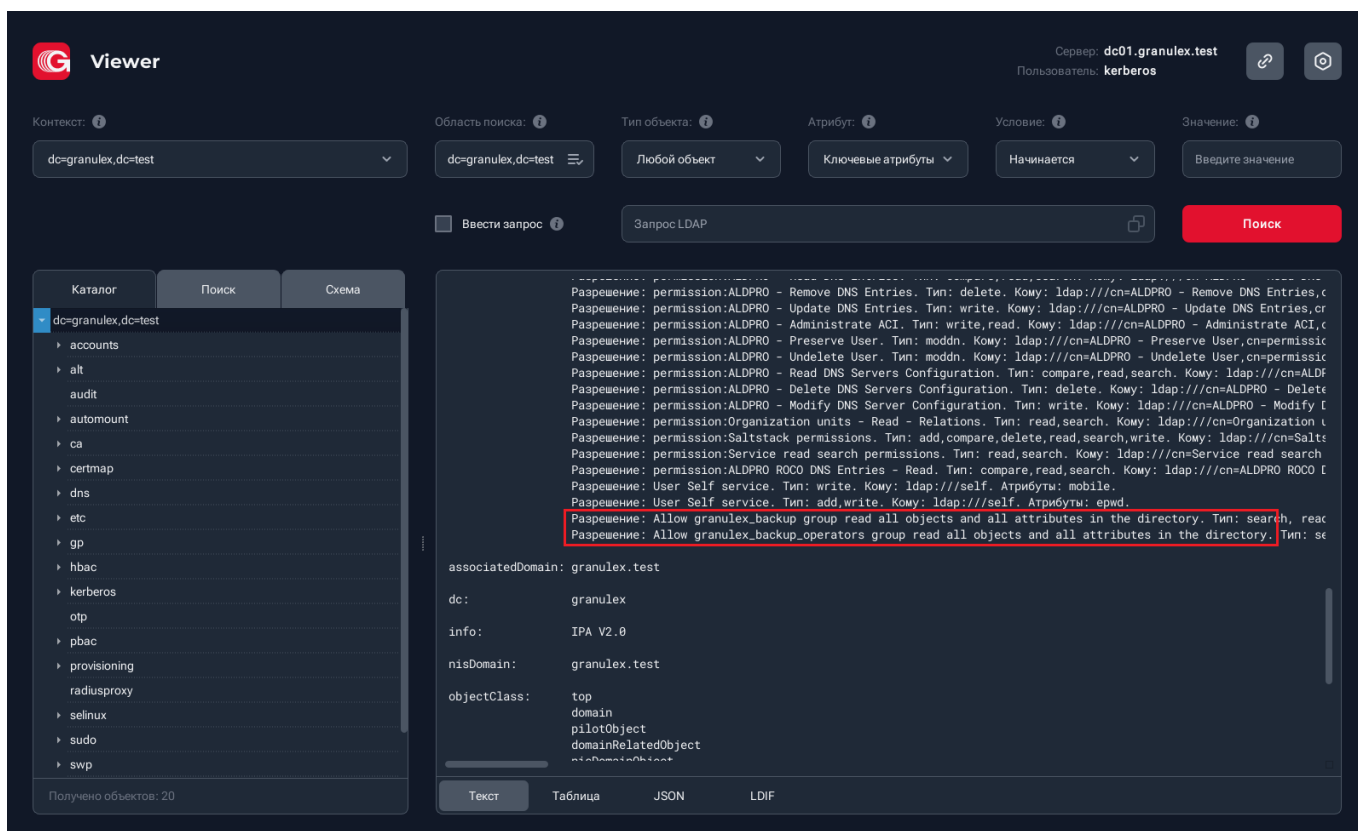
3. Откройте окно терминала и выполните команду:

```
ldapadd -h dc-01.granulex.test -f granulex_backup_operators_add aci.ldif
```

В результате выполнения этой команды в атрибут `aci` объекта «домен» (самый верхний уровень в иерархии раздела каталога, в котором хранятся данные пользователей - domain naming context) будет добавлена инструкция, наделяющая группу `granulex_backup_operators` необходимыми правами доступа. Проверить добавление нужного значения можно при помощи команды:

```
ldapsearch -h dc-01.granulex.test dc=granulex aci
```

Либо воспользоваться графической утилитой для просмотра данных каталога. Например, Granulex Viewer:

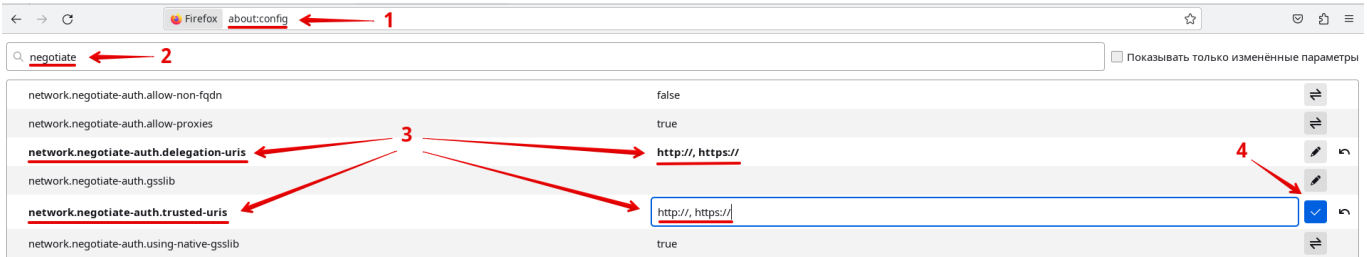


Настройка Kerberos-аутентификации в браузере

Работа с продуктом Granulex Recovery осуществляется из графического интерфейса, который доступен из интернет-браузера (Mozilla Firefox).

Перед началом работы необходимо настроить Kerberos-аутентификацию пользователя в браузере. Для этого выполните следующие шаги:

1. В адресной строке браузера введите: `about:config`
2. В строке поиска введите `negotiate`
3. В открывшемся списке параметров в полях `network.negotiate-auth.delegation-uris` и `network.negotiate-auth.trusted-uris` введите через запятую значения: `http://`, `https://`
4. Сохраните настройки, нажав галочку справа от строки



Альтернативный способ настройки указанных выше параметров - из командной строки. Скопируйте и вставьте команду целиком:

```
sudo tee /usr/lib/firefox/browser/defaults/preferences/prefs.js <<EOF
pref("network.negotiate-auth.trusted-uris","https://, http://");
pref("network.negotiate-auth.delegation-uris","https://, http://");
EOF
```

Вход в Granulex Recovery

Для входа в Granulex Recovery выполните следующие действия:

1. Убедитесь, что вы вошли в систему с доменной учётной записью (аутентифицированы в службе каталогов ALD Pro/FreeIPA)
2. Откройте браузер Mozilla Firefox
3. В адресной строке браузера введите адрес сервера, на который был установлен продукт Granulex Recovery (пример: <http://server1.granulex.test/>)
4. Если установка продукта и первоначальная настройка проведена успешно, откроется главная страница Granulex Recovery



ВНИМАНИЕ! После установки продукта сервер Granulex Recovery доступен по незащищённому протоколу HTTP. Для настройки защищённого взаимодействия с сервером по протоколу HTTPS, следуйте инструкциям, приведённым в Приложении 1 данного документа.

Установка файла лицензионного ключа

Для установки файла лицензионного ключа выполните следующие действия:

1. В графическом интерфейсе продукта откройте меню настроек и выберите **Информация о лицензии**
2. В открывшемся окне нажмите **Обновить лицензию**. Откроется системный диалог поиска и выбора файла
3. Выберите папку, в которой находится файл лицензии (.lic), выберите файл и нажмите **Открыть**. Лицензия будет загружена на сервер
4. Если проверка лицензии и ее установка прошла успешно, продукт готов к работе

Обновление продукта

Для обновления пакета Granulex Recovery из репозитория выполните команду:

```
sudo apt install granulex
```

Если пакет получен на переносном носителе, то для его установки выполните команду:

```
sudo dpkg -i granulex_x.x.x-xxx_amd64.deb
```

Далее следуйте инструкциям мастера установки.

Приложение 1. Настройка защищённого взаимодействия с сервером Granulex Recovery по протоколу HTTPS

Для работы с сервером Granulex Recovery по защищённому протоколу HTTPS, выполните шаги, приведённые ниже.

Шаг 1. Создание сертификата

Для работы по защищённому протоколу HTTPS необходим сертификат, который нужно установить на сервер с Granulex Recovery. Этот сертификат будет использоваться при установке защищённого соединения между клиентом (браузером пользователя) и сервером Granulex Recovery.

При установке и использовании Granulex Recovery в продуктивной среде сертификат для сервера, на который будет устанавливаться продукт должен быть выпущен и подписан доверенным центром сертификации (собственным, установленным в компании либо коммерческим).

При использовании Granulex Recovery в тестовой среде можно создать и использовать самоподписанный сертификат. Для этого создания самоподписанного сертификата выполните следующие шаги:

На сервере Granulex Recovery, откройте терминал и выполните команду и перейдите в папку установки веб-сервера Apache2:

```
cd /etc/apache2
```

Создайте папку для сертификатов и перейдите в нее:

```
mkdir ssl ; cd ssl
```

Сгенерируйте сертификат:

```
openssl req -new -x509 -days 365 -nodes -out cert.pem -keyout key.pem -subj  
"/C=RU/ST=MSK/L=MSK/O=Global Security/OU=IT Department/CN=srv1.granulex.test"
```

Где:

- `srv1.granulex.test` - полное доменное имя (FQDN - fully-qualified domain name) сервера, для которого выпускается сертификат
- в данном примере создаются открытый и закрытый ключи сроком действия 1 год (365 дней); значения параметра `subj` могут быть любыми в рамках тестирования.

Добавьте сертификат в доверенные. Для этого выполните команды:

```
sudo cp cert.pem /usr/local/share/ca-certificates/  
sudo update-ca-certificates -v
```

Шаг 2. Установка модуля SSL для веб-сервера Apache2

Проверьте, установлен ли модуль `ssl` веб-сервера Apache2:

```
apachectl -M | grep ssl
```

Если в выводе команды присутствует строка `ssl_module (shared)` - модуль установлен, перейдите к Шагу 3 данной инструкции. В противном случае, установите модуль `ssl`:

```
a2enmod ssl
```

Перезапустите сервис веб-сервера Apache 2, чтобы применить настройки:

```
systemctl restart apache2
```

Шаг 3. Настройка виртуальной директории веб-сервера Apache2

Откройте конфигурационный файл веб-сайта (виртуальной директории) Granulex Recovery в текстовом редакторе. Например:

```
nano /etc/apache2/sites-enabled/001-granulex.conf
```

В конец файла (после закрывающего тега `</VirtualHost>` для порта 80) добавьте параметры конфигурации для порта 443.

ВНИМАНИЕ! Текущие параметры конфигурации для порта 80 удалять не нужно! В итоговом файле должны присутствовать обе конфигурации.

```
Listen 0.0.0.0:443  
  
<VirtualHost *:443>
```

```
ServerName srv1.granulex.test
WSGIScriptAlias /granulex/api /opt/granulex/granulex_web_api/granulex.wsgi
WSGIApplicationGroup %{GLOBAL}
DocumentRoot /opt/granulex/granulex_web_ui/
SSLEngine on
SSLCertificateFile /etc/apache2/ssl/cert.crt
SSLCertificateKeyFile /etc/apache2/ssl/key.pem
#SSLCertificateChainFile ssl/cert.ca-bundle

<Directory />
AllowOverride All
RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/index.html$
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} !\.
(css|gif|ico|jpg|js|png|swf|txt|svg|woff|ttf|eot)$
    RewriteRule . index.html [L]
AuthType GSSAPI
AuthName "granulex-recovery"
GssapiCredStore keytab:/etc/apache2/http.keytab
GssapiDelegCcacheEnvVar KRB5CCNAME
GssapiDelegCcacheDir /tmp
require valid-user
RequestHeader set MYMACLABEL "%m:%c"

</Directory>
</VirtualHost>
```

Где:

- **ServerName** - полное доменное имя (FQDN - fully-qualified domain name) сервера, на котором установлен продукт Granulex Recovery
- **SSLCertificateFile** и **SSLCertificateKeyFile** - пути к файлам ключей, которые были сгенерированы на Шаге 1
- **SSLCertificateChainFile** - путь до цепочки сертификатов (при необходимости, если используется не самоподписанный сертификат)

Проверьте корректность настроек:

```
apachectl configtest
```

В случае вывода **Syntax OK** - примените новую конфигурацию к сервису Apache2:

```
apachectl graceful
```

Шаг 4. Проверка работоспособности защищённого соединения

На клиентской рабочей машине откройте браузер и перейдите на сайт Granulex Recovery, используя защищённый протокол: в адресной строке браузера введите **https://srv1.granulex.test**.

При использовании самоподписанного сертификата на сервере Granulex Recovery, в окне браузера высветится предупреждение о том, что проверка цифровой подписи сертификата не может быть пройдена и передача данных с этого сервера не безопасна. Сделайте исключение и подтвердите намерение открыть сайт.

Если защищённое соединение установлено успешно, в браузере отобразится графический интерфейс Granulex Recovery. В этом случае, перейдите к Шагу 5. В противном случае, проверьте правильность заданных ранее параметров в конфигурационных файлах и исследуйте лог-файлы веб-сервера Apache2 в каталоге `/var/log/apache2` на наличие ошибок.

Шаг 5. Настройка автоматического перенаправления для порта 80(http) на порт 443(https)

Для автоматического перенаправления запросов, отправляемых по незащищённому протоколу на порт 80(http) и установку защищённого соединения, настройте перенаправление запросов на порт 443(https). Для этого:

Откройте конфигурационный файл веб-сайта (виртуальной директории) Granulex Recovery в текстовом редакторе. Например:

```
nano /etc/apache2/sites-enabled/001-granulex.conf
```

Замените параметры конфигурации для порта 80(http) на следующие:

```
Listen 0.0.0.0:80
<VirtualHost *:80>
    ServerName srv1.granulex.test
    RewriteEngine On
    RewriteRule ^ https://srv1.granulex.test%{REQUEST_URI} [R=301,L]
</VirtualHost>
```

Итоговый файл конфигурации должен выглядеть так:

```
Listen 0.0.0.0:80
<VirtualHost *:80>
    ServerName srv1.granulex.test
    RewriteEngine On
    RewriteRule ^ https://srv1.granulex.test%{REQUEST_URI} [R=301,L]
</VirtualHost>

Listen 0.0.0.0:443
<VirtualHost *:443>
    ServerName srv1.aldpro.tst
    WSGIScriptAlias /granulex/api /opt/granulex/granulex_web_api/granulex.wsgi
    WSGIApplicationGroup %{GLOBAL}
    DocumentRoot /opt/granulex/granulex_web_ui/
    SSLEngine on
    SSLCertificateFile /etc/apache2/ssl/cert.crt
    SSLCertificateKeyFile /etc/apache2/ssl/key.pem
    #SSLCertificateChainFile ssl/cert.ca-bundle
```

```
<Directory />
AllowOverride All
RewriteEngine On
    RewriteCond %{REQUEST_URI} !^/index.html$
    RewriteCond %{REQUEST_FILENAME} !-f
    RewriteCond %{REQUEST_FILENAME} !-d
    RewriteCond %{REQUEST_URI} !\.
(css|gif|ico|jpg|js|png|swf|txt|svg|woff|ttf|eot)$
    RewriteRule . index.html [L]
AuthType GSSAPI
AuthName "granulex-recovery"
GssapiCredStore keytab:/etc/apache2/http.keytab
GssapiDelegCcacheEnvVar KRB5CCNAME
GssapiDelegCcacheDir /tmp
require valid-user
RequestHeader set MYMACLABEL "%m:%c"

</Directory>
</VirtualHost>
```

Установите модуль `rewrite` веб-сервера Apache2:

```
a2enmod rewrite
```

Примените новую конфигурацию веб-сервера Apache2:

```
systemctl restart apache2
```

Для проверки работы автоматического перенаправления, откройте веб-сайт Granulex Recovery, используя незащищённый протокол: в адресной строке браузера введите <http://srv1.granulex.test>. Если перенаправление работает, соединение с сайтом автоматически установится по защищённому протоколу; в адресной строке браузера <http> автоматически сменится на <https>.