



Введение	3
Системные Требования Ошибка! Закладка не опред	целена.
Архитектура и операционная система	3
ПК (клиентская часть)	4
Веб-браузеры	4
Требования к установке	5
Включение SSL	5
Расположение директории данных Ошибка! Закладка не опред	целена.
Выбор базы данных	5
Процесс установки	5
Подготовка виртуальных машин	5
Подготовка сервисов Kubernetes, S3, Базы данных	7
Шаг 1 - Развёртывание кластера Kubernetes при помощи Kubespray	7
Шаг 2 - Установка и настройка необходимых компонентов (PostgreSQL/Redis/MinioS3)	8
Установка программного обеспечения Astra Disk и OnlyOffice	9
Шаг 1. Установка Astra Disk	9
Шаг 2 - Настройка OnlyOffice	11
Подключение службы каталогов LDAP к Astra Disk	12
Конфигурация сервера	13
Вкладка «Пользователи»	15
Вкладка «Учетные данные»	16
Вкладка «Группы»	17
Вкладка «Дополнительно»	18
Настройки подключения	18
Настройки каталога	19
Специальные атрибуты	21
Атрибуты профиля пользователя	22
Вкладка «Эксперт»	24
Проверка работоспособности программного обеспечения Astra Disk	25
Вход в систему Astra Disk	25
Программа и методика испытаний работы функционала Astra Disk	27
Проверка работы с пользователями и группами LDAP в ПО Astra Disk	31



Введение

Добро пожаловать в Руководство по администрированию сервера Astra Disk. Данное руководство предназначено для системных администраторов, которым требуется установить и администрировать сервер Astra Disk.

Системные Требования

Для обеспечения максимальной производительности, стабильности и функциональности ниже представлены рекомендации по запуску Astra Disk.

Платформа	Рекомендации		
Операционная система (64-bit)	 Astra Linux 1.7 Astra Linux 1.8 Debian совместимые системы Red Hat совместимые системы CentOS 		
База Данных	 Tantor Minio S3 MySQL Oracle Database PostgreSQL SQLite 		
Веб-сервер	nginx		
PHP Runtime	8.18.2 (recommended)8.3		

Архитектура и операционная система

В качестве основного хранилища Астра Диск поддерживает только S3.

Рекомендуемая инфраструктура: S3 хранилище, LDAP, Система управления базами данных и база данных. Далее поднимается 2 пода кластера кубернетиса и nginx балансировщик. Рекомендованная инфраструктура для пилотной установки указана на



рис.1. Отказоустойчивая архитектура прорабатывается отдельно под конкретную установку.

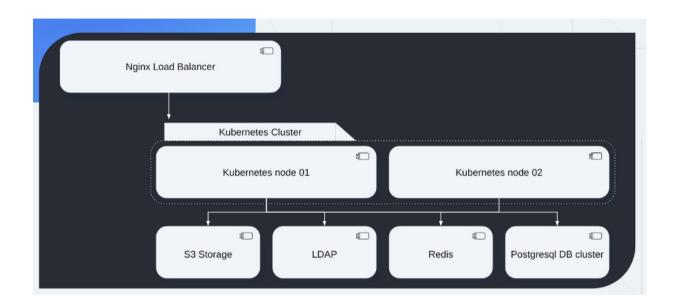


Рисунок 1. Архитектура для пилотного разверывания

Минимальные рекоммендованные ресурсы указаны в Таблице.

п/п	Название сервера (ВМ)	Кол-во ядер	ОЗУ	Дисковое пространство
1	k8s-master	4	4 ГБ	50 ГБ
2	k8s-node01	4	8 ГБ	70 ГБ
3	k8s-node02	4	8 ГБ	70 ГБ
4	Minio-s3+registry	4	4 ГБ	70 ГБ
5	PostgreSQL-db+redis	4	4 ГБ	70 ГБ

Таблица 1. Ресурсы для установки Astra Disk

ПК (клиентская часть)

- Astra Linux SE 1.7/1.8
- Windows 10+/
- macOS Lion (10.14)+ (только 64-бит)
- Linux (только 64-бит)

Веб-браузеры

Для наилучшей работы с веб-интерфейсом Astra Disk, рекомендуется использовать последнюю поддерживаемую версию браузера из следующего списка, либо браузера, основанного на них:



- Microsoft Edge
- Mozilla Firefox
- Google Chrome/Chromium
- Apple Safari

Требования к установке

Docker v.24+ или k8s v1.22+, ansible v.2.15+, python3

Включение SSL

Вы можете использовать Astra Disk через обычный HTTP, но мы рекомендуем использовать SSL/TLS для шифрования всего трафика на вашем сервере и защиты логинов и данных пользователей во время передачи.

Выбор базы данных

Для базового тестирования Astra Disk возможно использование SQLite, но рекомендуется использовать одну из следующих баз данных: Tantor DB, MySQL, MariaDB, Oracle 11g и Postgresql. Ваша база данных должна быть установлена перед запуском установочного скрипта.

Данные доступа к базе данных прописываются в inventory-файле hosts.yml.

ASTRADISK DB DBNAME: имя базы данных

ASTRADISK DB HOSTNAME: адрес сервера

ASTRADISK_DB_USER: имя пользователя

ASTRADISK DB PASSWORD: пароль

Учетная запись пользователя БД должна иметь права для создания и изменения таблиц внутри базы данных.

Процесс установки

Подготовка виртуальных машин

Подготовлено 5 виртуальных машин:



```
ansible_password = "vagrant"
ansible user = "vagrant"
vm_hostname = tolist([
 "k8smaster",
 "k8snode1",
 "k8snode2",
 "minios3",
 "postgresql",
1)
vm_ip = [
 "10.177.77.82",
 "10.177.77.81",
 "10.177.77.110",
 "10.177.77.111",
 "10.177.77.112",
1
vm name = [
 "Astra Disk k8smaster",
 "Astra Disk_k8snode1",
 "Astra Disk k8snode2",
 "Astra Disk minios3",
 "Astra Disk postgresql",
]
```

После произведенных действий получаем виртуальные машины с ір-адресами, указанными в Таблице 2.

п/п	Название сервера (ВМ)	ір-адрес	Описание
1	Astra Disk_k8smaster	10.177.77.82	k8s-master
2	Astra Disk_k8snode1	10.177.77.81	k8s-node01
3	Astra Disk_k8snode2	10.177.77.110	k8s-node02
4	Astra Disk_minios3	10.177.77.111	Minio-s3+registry
5	Astra Disk_postgresql	10.177.77.112	PostgreSQL-db+redis

Таблица 2. Ір-адресация ВМ

Выше указанные ВМ представлены в единой конфигурации:

OC Astra Linux SE 1.8.1 (Уровень защищенности Орел), 50ГБ, ОЗУ - 5ГБ (без swap), CPU-1,VCPU-2. Все виртуальные машины должны иметь выход в сеть интернет.

Также необходимо было пробросит ssh-ключ с узла minios3 на все остальные BM.



Подготовка сервисов Kubernetes, S3, Базы данных

Шаг 1 - Развёртывание кластера Kubernetes при помощи Kubespray

```
Ha узле minios3 необходимо произвести следующие команды
sudo apt install python3-venv python3-pip git
git clone -b v2.24.1 https://github.com/kubernetes-sigs/kubespray.git
cd kubespray/
python3 -m venv ~/venv
source ~/venv/bin/activate
pip install -r requirements.txt
Далее произвести действия:
1.
       vim inventory/inventory-step1.yml
2.
       all:
3.
        hosts:
4.
         edu1-ks8m:
5.
          ansible_host: 10.177.77.82
6.
          ip: 10.177.77.82
7.
          access_ip: 10.177.77.82
8.
         edu1-ks8n01:
9.
          ansible_host: 10.177.77.81
10.
          ip: 10.177.77.81
11.
          access_ip: 10.177.77.81
12.
         edu1-ks8n02:
13.
          ansible_host: 10.177.77.110
14.
          ip: 10.177.77.110
15.
          access ip: 10.177.77.110
16.
        children:
17.
         kube control plane:
18.
          hosts:
19.
           edu1-ks8m:
20.
         kube_node:
21.
          hosts:
22.
           edu1-ks8n01:
23.
           edu1-ks8n02:
24.
         etcd:
25.
          hosts:
26.
           edu1-ks8m:
27.
           edu1-ks8n01:
28.
           edu1-ks8n02:
29.
         k8s cluster:
          children:
30.
```



```
31.
           kube control plane:
32.
           kube node:
33.
         calico rr:
34.
           hosts: {}
ansible-playbook --become -e "ansible_distribution='Ubuntu'" -e "ansible_os_family='Debian'" -i
inventory/inventory-step1.yml cluster.yml
```

Шаг 2 - Установка и настройка необходимых компонентов (PostgreSQL/Redis/MinioS3)

```
Ha узле minios3
Загружаем архив:
astradisk-step2.tar.gz
Копируем с хоста на узел minios3
scp astradisk-step2.tar.qz vagrant@10.177.77.111:~/
source ~/venv/bin/activate
tar -xf astradisk-step2.tar.az
ansible-playbook astradisk-step2/main.yml
Переходим в браузере по ссылке - http://10.177.77.111:9001/ (Astra Disk_minios3)
Логин: sysadmin
Пароль:v4K2YM3ekDGkRpVt
Далее создаем корзину (bucket):
storage1
```

- - Перейдите в раздел Buckets.
 - Нажмите на Create Bucket + и введите желаемое имя (например, storage1). •
 - Включите параметр Versioning, переключив его в состояние On.

Создаем User:

Логин: user Пароль:12345678

- Перейдите в раздел identity.
- Нажмите на Create user + и введите желаемое имя (user).
- Так же указать пароль (123456768)
- Включите параметр readwrite.

Ha узле postgresql вводим команду: sudo vim /etc/redis/redis.conf

```
# Приводим к виду
bind 0.0.0.0
# В конец конфигурационного файла добавляем строку
       protected-mode no
      sudo service redis-server restart
      sudo service redis-server status
```

На узле k8smaster вводим команды:



```
sudo -i
python3 -m venv /venv
source /venv/bin/activate
pip install kubernetes
curl -fsSL -o get_helm.sh https://raw.githubusercontent.com/helm/helm/main/scripts/get-helm-3
chmod 700 get_helm.sh
./get_helm.sh
```

Установка программного обеспечения Astra Disk и OnlyOffice

Шаг 1. Установка Astra Disk

Ha узле minios3 производим действия:

- 1) Загружаем архив: astradisk-step3.tar.gz
- 2) Копируем с хоста на узел minios3 scp astradisk-step3.tar.qz vagrant@10.177.77.111:~/

```
tar -xf astradisk-step3.tar.gz cd astradisk-step3
```

nano inventory/inventory

Откроется файл со следующим содержимым:

```
all:
children:
  astradisk:
  hosts:
    astradisk-host:
    ansible host: 10.177.77.82
    ansible user: vagrant
  vars:
    ASTRADISK VERSION: "v1.6"
    NEXTCLOUD REPO: "cr.yandex/crp2utr5mdr1cv944f79/astradisk 1.6"
    NEXTCLOUD TAG: latest
    NEXTCLOUD USER: "admin"
    NEXTCLOUD NGINX ENABLED: "true"
    NEXTCLOUD IS DEV: "DISABLED"
    NEXTCLOUD_LDAP_TEST: "DISABLED"
    NEXTCLOUD_LDAP_PROD: "DISABLED"
    NEXTCLOUD SETUP ACTION: "INSTALL"
```



```
NEXTCLOUD_INSTACE_ID: "instace disk asdgd1"
   NEXTCLOUD CHART NAME: "nextcloud"
   NEXTCLOUD DATA EXISTINGCLAIM: "ext-edu1-astradisk-data"
   NEXTCLOUD DATA STORAGESIZE: "5Gi"
   NEXTCLOUD DB DBNAME: "test db"
   NEXTCLOUD DB HOSTNAME: "10.177.77.112"
   NEXTCLOUD REDIS HOST: "10.177.77.112"
   NEXTCLOUD DB USER: "test user"
   NEXTCLOUD EXISTINGCLAIM: "ext-edu1-astradisk"
   NEXTCLOUD HOST: "sup-52034.disk.astralinux.ru"
   NEXTCLOUD LDAP LOGIN:
"uid=nextcloud,cn=sysaccounts,cn=etc,dc=astralinux,dc=ru"
   NEXTCLOUD LDAP TEST HOST: "0.0.0.0"
   NEXTCLOUD LDAP TEST LOGIN: "cn=admin,dc=example,dc=com"
   NEXTCLOUD NAME: "ext-edu1-astradisk"
   NEXTCLOUD NAMESPACE: "ext-edu1-astradisk"
   NEXTCLOUD NODEPORT: "30108"
   NEXTCLOUD ONLYOFFICE HOST: "https://sup-52034-office.disk.astralinux.ru/"
   NEXTCLOUD S3 BUCKET: "storage1"
   NEXTCLOUD S3 HOSTNAME: "10.177.77.111"
   NEXTCLOUD S3 PORT: 9000
   NEXTCLOUD S3 USE SSL: "false"
   NEXTCLOUD S3 USEPATH STYLE: "true"
   NEXTCLOUD SERVICE TYPE: "NodePort"
   NEXTCLOUD STORAGECLASS: "longhorn"
   NEXTCLOUD STORAGESIZE: "5Gi"
   NEXTCLOUD VARTON LDAP LOGIN: "nextcloud"
   NEXTCLOUD CONFIG PASSWORDSALT: "k6bk+aAYa5E4Uj20eS61goS9dZ6UpC"
   NEXTCLOUD CONFIG SECRET:
"N6sdrFTueFmFoP4fyn7lFDHkmlDriuYj8pb2fVtFpSD/ERUI"
   ASTRADISK REPO USER: "json key"
   ASTRADISK REPO TOKEN: 'TOKEN HERE'
   NEXTCLOUD DB PASSWORD: "12345678"
   NEXTCLOUD LDAP TEST PASSWORD: "123456"
   NEXTCLOUD ONLYOFFICE JWT TOKEN: "p123456"
   NEXTCLOUD PASSWORD: "lah1gu9Shoj"
   NEXTCLOUD REDIS PASSWORD: ""
   NEXTCLOUD S3 KEY: "user"
   NEXTCLOUD S3 SECRET: "12345678"
```

BMecto TOKEN HERE вставить токен, полученный для данной инсталляции.



Проверяем, что в файле ір адреса соответствуют.

ansible-playbook -e "ansible_python_interpreter=/venv/bin/python" -e "hosts=astradisk-host" -i inventory/inventory deploy-ext.yml sudo -i

- 1. kubectl get ns
- NAME STATUS AGE
- default Active 28h
- 4. ext-edu1-astradisk Active 27h
- 5. kube-node-lease Active 28h
- 6. kube-public Active 28h
- 7. kube-system Active 28h
- 8. longhorn-system Active 27h
- 9. onlyoffice-pilot Active 26h
- 10. kubectl -n ext-edu1-astradisk get pods
- 11. NAME READY STATUS RESTARTS AGE
- 12. ext-edu1-astradisk-nextcloud-559b55cdbc-w7qj6 2/2 Running 0 27h

Просмотр логов:

kubectl -n ext-edu1-astradisk logs ext-edu1-astradisk-nextcloud-559b55cdbc-w7qj6 -f Подключаемся к контейнеру и выполняем

- kubectl -n ext-edu1-astradisk exec -it ext-edu1-astradisk-nextcloud-559b55cdbc-w7qj6 bash
- 2. rm -rf apps/onlyoffice
- 3. sudo -E -u www-data ./occ app:install -g onlyoffice
- 4. sudo -E -u www-data ./occ app:disable -q serverinfo
- 5. cat data/ext-edu1-astradisk-nextcloud-559b55cdbc-w7qj6.log
- 6. exit

Переходим в web: https://sup-52034.disk.astralinux.ru/login (домен выдается под конкретную инсталляции). Без домена не удастся получиться доступ к web-интерфейсу, необходим https-протокол

Логин: sysadmin Пароль: lah1gu9Shoj

Шаг 2 - Настройка OnlyOffice

1) На узле k8smaster производим следующие действия:

Загружаем архив: onlyoffice.tar.gz Копируем с хоста на узел k8smaster: scp astradisk-step3.tar.gz vagrant@10.177.77.82:~/



tar -xf onlyoffice.tar.gzcd onlyoffice/cat readme.txt sudo kubectl create ns onlyoffice-pilot sudo kubectl apply -f secret.yml sudo kubectl apply -f deploy.yml

vim deploy.yml # Приводим к виду image: cr.yandex/crp2utr5mdr1cv944f79/onlyoffice_8.0.1 sudo kubectl -n onlyoffice-pilot get pods sudo kubectl -n onlyoffice-pilot describe pod onlyoffice-web-7d76d89b6d-pm5rd sudo kubectl -n onlyoffice-pilot logs -f onlyoffice-web-7d76d89b6d-pm5rd

Подключение службы каталогов LDAP к Astra Disk

В состав Astra Disk входит плагин LDAP, позволяющий пользователям и группам LDAP отображаться в списке пользователей и групп Astra Disk. Эти пользователи будут проходить аутентификацию в Astra Disk с помощью своих учётных данных LDAP, поэтому вам не придётся создавать для них отдельные локальные учётные записи пользователей Astra Disk. Вы сможете управлять членством в группах Astra Disk, квотами и разрешениями на совместное использование файлов и папок через LDAP.

Плагин LDAP поддерживает:

- 1. Поддержка группы LDAP;
- 2. Общий доступ к файлам с пользователями и группами Astra Disk;
- 3. Автоматическое определение атрибутов LDAP, таких как базовый DN, электронная почта и номер порта LDAP-сервера;

Для подключения контроллеров домена LDAP необходимо под учетной записью администратора (login: sysadmin), которая создается автоматически и установке Astra Disk, перейти во вкладку «Параметры сервера» (рис 2).



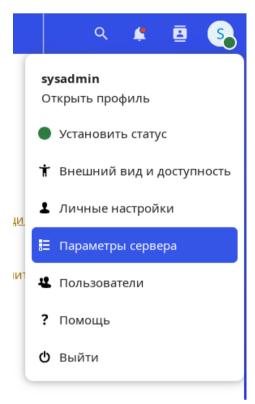


Рисунок 2. Вкладка «Параметры сервера»

Раздел меню «Параметры сервера» - «LDAP/AD интеграция» состоит из четырёх вкладок (рис.3). Для доступа к другим вкладкам необходимо правильно заполнить первую вкладку («Сервер»). Если конфигурация выполнена правильно, загорается зелёный индикатор. Наведите курсор на поля, чтобы увидеть всплывающие подсказки.

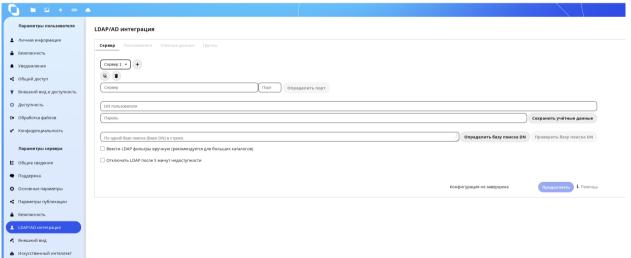


Рисунок 3. Раздел меню «LDAP/AD интеграция»

Конфигурация сервера

Настройте один или несколько серверов LDAP. Нажмите кнопку Удалить конфигурацию, чтобы удалить текущую конфигурацию (рис.4).



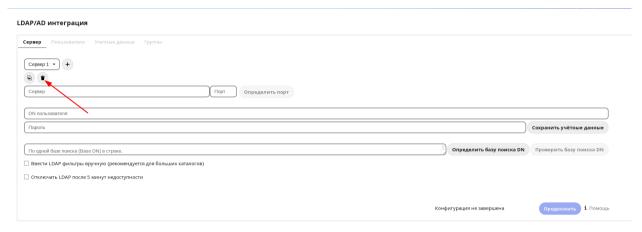


Рис.4. Удалить текущую конфигурацию

Сервер

Имя хоста или IP-адрес сервера LDAP. Это также может быть URI ldaps://. Если вы введете номер порта, это ускорит поиск сервера.

Примеры:

- directory.my-company.com
- Idaps://directory.my-company.com
- directory.my-company.com:9876

Порт

Порт, по которому осуществляется подключение к серверу LDAP. Это поле отключено в начале новой конфигурации. Если сервер LDAP работает на стандартном порту, он будет обнаружен автоматически. Если вы используете нестандартный порт, Astra Disk попытается его обнаружить. Если это не удастся, вам нужно будет ввести номер порта вручную. Пример:

389

DN пользователя

Имя в формате DN пользователя, у которого есть разрешения на поиск в каталоге LDAP. Оставьте поле пустым для анонимного доступа. Мы рекомендуем использовать для этого специального системного пользователя LDAP.

Пример:

uid=astradisksystemuser,cn=sysusers,dc=my-company,dc=com

Пароль

Пароль для пользователя, указанного выше или оставьте пустое поле для анонимного доступа.

Базовый DN (Base DN)

Базовый DN LDAP, по которому можно получить доступ ко всем пользователям и группам. Вы можете ввести несколько базовых DN, по одному в строке. (Базовые DN для пользователей и групп можно задать на вкладке «Дополнительно».) Это поле обязательно для заполнения. Astra Disk пытается определить базовый DN на основе указанного DN пользователя или хоста, и если Astra Disk не может его определить, вы должны ввести его вручную.

Пример:

• dc=my-company,dc=com



Пример заполненной конфигурации сервера можно посмотреть на рис.5. Также зеленый индикатор свидетельствует о корректном подключении.

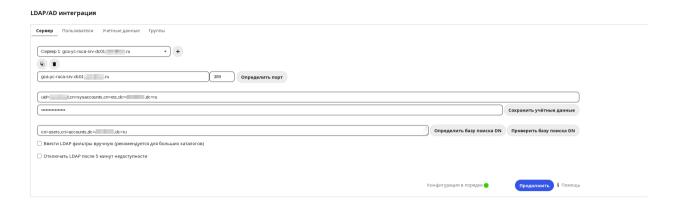


Рис.5. Пример заполненной конфигурации сервера

Вкладка «Пользователи»

Используйте вкладку «Пользователи», чтобы контролировать, какие пользователи LDAP указаны в качестве пользователей Astra Disk на сервере Astra Disk. Чтобы контролировать, какие пользователи LDAP могут входить на ваш сервер Astra Disk, используйте вкладку Атрибуты входа. Те пользователи LDAP, у которых есть доступ, но которые не указаны в качестве пользователей (если таковые имеются), будут скрытыми пользователями. При желании вы можете пропустить поля формы и ввести необработанный фильтр LDAP. Пример заполненной вкладки «Пользователи» можно посмотреть на рис.6. Также зеленый индикатор свидетельствует о корректном заполнении.



Рис.6. Вкладка "Пользователи"

Только эти классы объектов

Astra Disk определит классы объектов, которые доступны для пользовательских объектов в вашей службе каталогов. Astra Disk автоматически выберет класс объектов, который возвращает наибольшее количество пользователей. Вы можете выбрать несколько классов объектов.

Только из этих групп

Если ваш сервер LDAP поддерживает member-of-overlay фильтры LDAP, вы можете указать, что в списках пользователей в Astra Diskмогут отображаться только пользователи из одной или



нескольких определенных групп. По умолчанию значение не выбрано. Вы можете выбрать несколько групп.

Если ваш сервер LDAP не поддерживает *member-of-overlay* фильтры LDAP, поле ввода будет отключено со стороны администратора службы каталогов.

Изменить запрос LDAP

При нажатии на этот текст переключается режим фильтрации, и вы можете вручную ввести или отредактировать фильтр LDAP напрямую.

Пример:

(&(objectClass=inetOrgPerson)(memberOf=cn=astradiskusers,ou=группы,dc=пример,dc=com))

Проверить настройки и пересчитать пользователей

Это индикатор, который показывает, сколько пользователей будет в списке Astra Disk. Число обновляется автоматически после любых изменений (рис.7).



Рис. 7. Проверка настройки и пересчитать пользователей

Вкладка «Учетные данные»

Настройки на вкладке «Учетные данные» определяют, какие LDAP пользователи могут входить в систему Astra Disk и по какому атрибуту или атрибутам сопоставляется введенное имя пользователя (например, LDAP/AD имя пользователя, адрес электронной почты). Вы можете выбрать несколько сведений о пользователях (рис.8). (При желании вы можете пропустить поля формы и ввести необработанный LDAP фильтр.)

Вы можете изменить настройки пользовательского фильтра на вкладке «Пользователи», используя необработанный фильтр LDAP.



Рис.8. Вкладка «Учетные данные»

LDAP/AD Имя пользователя

Если это значение отмечено, значение для входа будет сравниваться с именем пользователя в каталоге LDAP.

LDAP/AD Адрес электронной почты



Если это значение отмечено, то значение имени пользователя будет сравниваться с адресом электронной почты в каталоге LDAP, а именно с атрибутами mailPrimaryAddress и mail.

Другие Атрибуты

Это поле с несколькими вариантами выбора позволяет выбрать другие атрибуты для сравнения. Список генерируется автоматически на основе атрибутов объекта пользователя на вашем сервере LDAP.

Изменить запрос LDAP

При нажатии на этот текст переключается режим фильтрации, и вы можете вручную ввести или отредактировать фильтр LDAP.

Заполнитель %uid заменяется именем пользователя, введённым при входе в систему. *Примеры:*

- только имя пользователя:
 (&(objectClass=inetOrgPerson)(memberOf=cn=nextcloudusers,ou=группы,dc=пример,dc=com)(uid=%uid)
- имя пользователя или адрес электронной почты: ((&(objectClass=inetOrgPerson)(memberOf=cn=nextcloudusers,ou=groups,dc=example,dc=com)(|(uid=%uid)(mail=%uid)))

Вкладка «Группы»

По умолчанию в Astra Disk не будет доступно ни одной группы LDAP. Настройки на вкладке «Группы» определяют, какие группы будут доступны в Astra Disk. Вы также можете ввести необработанный фильтр LDAP (рис.9).



Рисунок 9. Вкладка «Группы»

Только эти классы объектов

Astra Disk определит классы объектов, которые обычно доступны для групповых объектов на вашем сервере LDAP. Astra Disk будет перечислять только те классы объектов, которые возвращают хотя бы один групповой объект. Вы можете выбрать несколько классов объектов. Типичным классом объектов является «группа» или «posixGroup».

Только из этих групп

Astra Disk создаст список доступных групп, найденных на вашем сервере LDAP. Затем вы выбираете группу или группы, которые получат доступ к вашему серверу Astra Disk.

Изменить запрос LDAP

При нажатии на этот текст переключается режим фильтрации, и вы можете напрямую ввести необработанный фильтр LDAP.

Пример:

- Объектный класс=группа
- Объектный класс=posixGroup



Проверить настройки и пересчитать группы

Это индикатор, который показывает, сколько пользователей будет в списке Astra Disk. Число обновляется автоматически после любых изменений.

Вкладка «Дополнительно»

Раздел LDAP «Дополнительно» содержит параметры, которые не нужны для рабочего подключения. Здесь можно отключить текущую конфигурацию, настроить реплицируемые хосты и различные параметры для повышения производительности.

Расширенные настройки состоят из четырех частей (рис.10):

- Настройки подключения
- Настройки каталога
- Специальные Атрибуты
- Атрибуты профиля пользователей

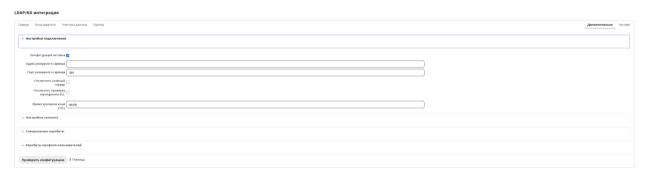


Рисунок 10. Вкладка Дополнительно

Настройки подключения

Конфигурация Активна

Включает или отключает текущую конфигурацию. По умолчанию она отключена. Когда Astra Disk успешно выполняет тестовое подключение, она автоматически включается.

Адрес резервного сервера

Если у вас есть резервный сервер LDAP, введите здесь настройки подключения. Тогда Astra Disk будет автоматически подключаться к резервному серверу, если основной сервер не будет доступен. Резервный сервер должен быть репликой основного сервера, чтобы идентификаторы объектов совпадали.

Пример:

directory2.my-company.com

Порт резервного сервера

Порт подключения резервного LDAP-сервера. Если порт не указан, а указан только хост, то будет использоваться основной порт (как указано выше).

Пример:

• 389

Отключить Главный Сервер

Вы можете вручную отключить основной сервер и Astra Disk будет подключаться только к резервному серверу. Это полезно при запланированных простоях.



Отключите проверку сертификата SSL

Отключает проверку SSL-сертификата. Используется только для тестирования.

Время хранения кэша

Кэш используется для предотвращения ненужного трафика LDAP, например для кэширования имён пользователей, чтобы их не приходилось искать на каждой странице, и для ускорения загрузки страницы «Пользователи». При сохранении конфигурации кэш очищается. Время указывается в секундах.

Настройки каталога

Заполненные поля вкладки можно увидеть на рис.11.

Поле отображаемого имени пользователя

Атрибут, который должен использоваться в качестве отображаемого имени в Astra Disk. *Пример: DisplayName*

Вторичное поле отображаемого имени пользователя

Дополнительный второй атрибут, отображаемый в скобках после имени, например, с помощью атрибута mail отображается как Molly Foo (molly@example.com).

Базовое Дерева Пользователей

Базовый DN LDAP, по которому можно получить доступ ко всем пользователям. Это должен быть полный DN, независимо от того, что вы ввели в качестве базового DN в настройках. Вы можете указать несколько базовых деревьев, по одному в каждой строке.

Пример:

cn=programmers,dc=my-company,dc=com cn=designers,dc=my-company,dc=com

Атрибуты поиска пользователя

Эти атрибуты используются при поиске пользователей, например, в диалоговом окне общего доступа. Атрибут отображаемого имени пользователя используется по умолчанию. Вы можете указать несколько атрибутов, по одному в строке.

Если атрибут недоступен для объекта пользователя, пользователь не будет отображаться в списке и не сможет войти в систему. Это также влияет на атрибут отображаемого имени. Если вы переопределяете значение по умолчанию, вы должны указать атрибут отображаемого имени здесь.

Пример: displayName mail



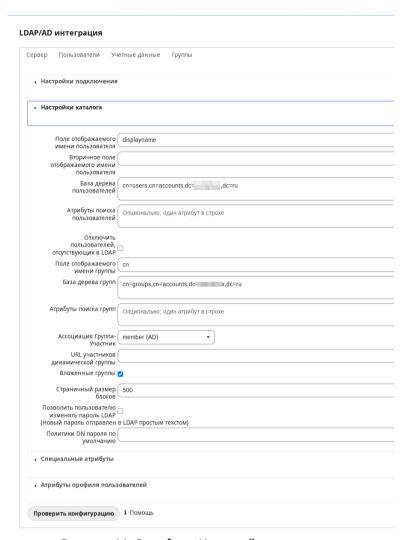


Рисунок 11. Вкладка «Настройки каталога»

Отключить пользователей, отсутствующих в LDAP

Если эта функция включена, пользователи, отсутствующие в LDAP, как если бы они были отключены в Astra Disk. Это означает, например, что общие папки этих пользователей больше не будут работать.

Поле Отображаемого имени группы

Атрибут, который следует использовать в качестве имени группы Astra Disk. В Astra Disk допускается ограниченный набор символов (a-zA-Z0-9.-_@). После присвоения имени группы его нельзя изменить.

Пример: сп

База дерева групп

Базовый DN LDAP, по которому можно получить доступ ко всем группам. Это должен быть полный DN, независимо от того, что вы ввели в качестве базового DN в настройках. Вы можете указать несколько базовых деревьев, по одному в каждой строке.

Пример:

- cn=barcelona,dc=my-company,dc=com
- cn=madrid,dc=my-company,dc=com

Атрибуты поиска групп

Эти атрибуты используются при поиске групп, например, в диалоговом окне общего доступа. По умолчанию используется атрибут отображаемого имени группы, указанный выше. Можно указать несколько атрибутов, по одному в каждой строке.



Если вы измените значение по умолчанию, атрибут отображаемого имени группы не будет учитываться, если вы не укажете его отдельно.

Пример:

Пример:

- cn
- description

Ассоциация Группа-участник

Атрибут, который используется для обозначения принадлежности к группе, то есть атрибут, используемый группами LDAP для обозначения своих пользователей. Astra Disk автоматически определяет значение. Вам следует менять его только в том случае, если у вас есть веская причина и вы знаете, что делаете.

uniquemember

Вложенные группы

Включите извлечение членов группы из подгрупп.

Политика DN паролей по умолчанию

Для использования этой функции требуется OpenLDAP с политикой ppolicy. DN политики паролей по умолчанию будет использоваться для обработки истечения срока действия пароля при отсутствии политики паролей для конкретного пользователя. Обработка истечения срока действия пароля включает следующее:

- Когда срок действия пароля LDAP подходит к концу, отобразите для пользователя предупреждающее сообщение с указанием количества дней, оставшихся до истечения срока действия. Предупреждения об истечении срока действия пароля отображаются в приложении уведомлений для Astra Disk.
- Предложите пользователям LDAP с просроченными паролями сбросить их во время входа в систему при условии, что доступно достаточное количество льготных входов в систему.

Оставьте этот параметр пустым, чтобы отключить обработку истечения срока действия пароля. Чтобы функция обработки истечения срока действия пароля работала, необходимо включить LDAP-пароли для каждого пользователя, а на LDAP-сервере должен работать OpenLDAP с соответствующим образом настроенным модулем ppolicy. Пример:

cn=default,ou=policies,dc=my-company,dc=com

Специальные атрибуты

Вкладка Специальные атрибуты указана на рис.12.



LDAP/AD интеграция Сервер Пользователи Учетные данные Группы Настройки подключения Настройки каталога ▼ Специальные атрибуты Поле квоты Квота по умолчанию Поле адреса email mail Правило именования домашнего каталога пользователя Поле-заполнитель "\$home" Атрибуты профиля пользователей Проверить конфигурацию і Помощь

Рисунок 12. Вкладка «Специальные атрибуты»

Поле Квоты

Astra Disk может считывать атрибут LDAP и устанавливать пользовательскую квоту в соответствии с его значением. Укажите здесь атрибут, и он вернёт значения, понятные человеку, например «2 ГБ».

Пример:

AstradiskQuota

Квота по умолчанию

Указывает квоту по умолчанию для пользователей LDAP, для которых не задана квота в поле «Квота» выше.

Пример:

15 Γ Ε

Атрибуты профиля пользователя

Вкладка Атрибуты профиля пользователя указана на рис.13.



DAP/AD интеграция	
Сервер Пользователи Уче	етные данные Группы
 Настройки подключения 	
, Настройки каталога	
 Специальные атрибуты 	
 Атрибуты профиля польз 	ователей
Поле телефона	
Поле web-сайта	
Поле адреса	
Поле Twitter	
Поле Федерации	
Поле организации	
Поле роли	
Поле заголовка	
Поле биографии (
Проверить конфигурацию	і Помощь

Рисунок 13. Вкладка «Атрибуты профиля пользователей»

После настройки этих атрибутов данные профиля пользователя будут перезаписаны соответствующими данными из LDAP. Контрольная сумма данных из LDAP будет сохранена в настройках пользователя user_ldap, lastProfileChecksum и обновление профиля будет пропущено, если данные из LDAP не изменятся. Если memcache.distributed включено в config.php, то контрольная сумма будет кэшироваться, и проверка будет пропущена, если кэшированное значение существует (срок действия истекает через ldapCacheTTL секунд).

Поле адреса

Атрибут LDAP, содержащий адрес пользователя. Именованное местоположение на странице профиля пользователя. Nextcloud требует однострочное значение, например city, country или somewhere under the loving sun. Многострочный формат почтового адреса будет переформатирован, разделитель в виде знака доллара будет заменен на запятую + пробел.

Пример: Почтовый адрес Пример: localityName



Вкладка «Эксперт»

В разделе «Эксперт» можно настроить дополнительные параметры в соответствии с вашими потребностями. Перед началом использования LDAP авторизации следует проверить конфигурацию (рис.14).



Рисунок 14. Вкладка «Эксперт»

Внутреннее Имя пользователя

Внутреннее имя пользователя — это идентификатор в Astra Disk для пользователей LDAP. По умолчанию оно будет создано на основе атрибута UUID. Атрибут UUID гарантирует, что имя пользователя уникально и что символы не нужно преобразовывать. Допустимы только следующие символы: [a-zA-Z0-9_.@-]. Другие символы заменяются их эквивалентами в ASCII или просто пропускаются.

Серверная часть LDAP гарантирует отсутствие дублирующихся внутренних имён пользователей в Astra Disk, то есть проверяет все другие серверные части пользователей (включая локальных пользователей Astra Disk). При возникновении коллизий к полученному значению добавляется случайное число (от 1000 до 9999). Например, если существует имя «Иван», следующее имя пользователя может быть «Иван_1337».

Внутреннее имя пользователя — это имя домашней папки пользователя по умолчанию в Astra Disk. Оно также является частью удалённых URL-адресов, например, для всех служб *DAV. Вы можете изменить все это с помощью параметра «Внутреннее имя пользователя». Оставьте его пустым для использования по умолчанию. Изменения затронут только недавно добавленных пользователей LDAP.

При настройке этого параметра имейте в виду, что имя пользователя в Astra Disk считается неизменным и не может быть изменено впоследствии. Это может вызвать проблемы при использовании атрибута, который может измениться, например, адреса электронной почты пользователя, который будет изменён при смене имени. Пример:

uid

Переопределить нахождение UUID

По умолчанию Astra Disk автоматически определяет атрибут UUID. Атрибут UUID используется для уникальной идентификации пользователей и групп LDAP. Внутреннее имя пользователя будет создано на основе UUID, если не указано иное.

Вы можете изменить настройки и указать атрибут по своему выбору. Убедитесь, что выбранный вами атрибут можно получить как для пользователей, так и для групп, и что он уникален. Оставьте поле пустым, чтобы использовать настройки по умолчанию. Изменения будут действовать только для пользователей и групп, LDAP которых были сопоставлены недавно. Они также будут действовать при изменении DN пользователя или группы, если старый UUID был кэширован, что приведёт к созданию нового пользователя. Поэтому настройку следует применить до того, как Nextcloud будет использоваться в рабочей среде, и очистить привязки (см. раздел *User and Group Mapping* ниже).

Пример:



cn

Соответствия Имя-Пользователь LDAP

Astra Disk использует имена пользователей в качестве ключей для хранения и назначения данных. Для точной идентификации и распознавания пользователей каждый пользователь LDAP будет иметь внутреннее имя пользователя в Astra Disk. Для этого требуется сопоставление имени пользователя Astra Disk с пользователем LDAP. Созданное имя пользователя сопоставляется с UUID пользователя LDAP. Кроме того, DN также кэшируется для сокращения взаимодействия с LDAP, но не используется для идентификации. Если DN изменится, Astra Disk обнаружит это изменение, проверив значение UUID.

То же самое справедливо и для групп.

Внутреннее имя Astra Disk используется во всех разделах Astra Disk. При очистке сопоставлений везде останутся неуправляемые связи. Никогда не очищайте сопоставления в рабочей среде, только на тестовом или экспериментальном сервере.

Проверка конфигурации

Кнопка «Проверить конфигурацию» проверяет значения, указанные в данный момент в полях ввода. Перед проверкой не нужно сохранять данные. При нажатии на кнопку Astra Disk попытается подключиться к серверу Astra Disk, используя настройки, указанные в данный момент в полях ввода (рис.15). Если подключение не удастся, вы увидите желтое предупреждение с сообщением об ошибке «Конфигурация неверна. Пожалуйста, ознакомьтесь с журналами ошибок для получения более подробной информации».

Когда тест конфигурации завершится успешно, сохраните настройки и проверьте, правильно ли отображаются пользователи и группы на странице «Пользователи».



Рисунок 15. Результат проверки конфигурации

Проверка работоспособности программного обеспечения Astra Disk

Вход в систему Astra Disk

Для проверки работоспособности программного обеспечения Astra Disk, развёрнутого в Бресте необходимо перейти по доменному адресу, указанного в Шаге 1 Установки программного обеспечения Astra Disk и OnlyOffice данной инструкции, в качестве примера: https://sup-52034.disk.astralinux.ru/login

Перед пользователями откроется страница авторизации (рис.16).



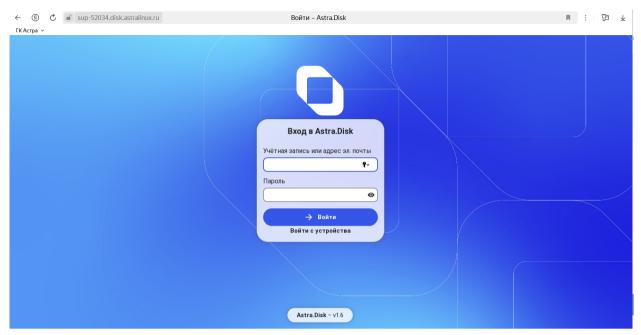


Рисунок 16. Страница авторизации Astra Disk

Далее вводим логин и пароль, указанные в Шаге 1 Установки программного обеспечения Astra Disk и OnlyOffice данной инструкции

Логин: sysadmin Пароль: lah1gu9Shoj

Далее откроется рабочее пространство пользователя (рис.17).

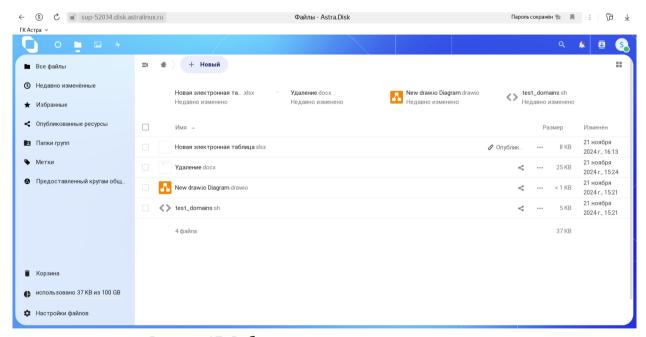


Рисунок 17. Рабочее пространство пользователя.



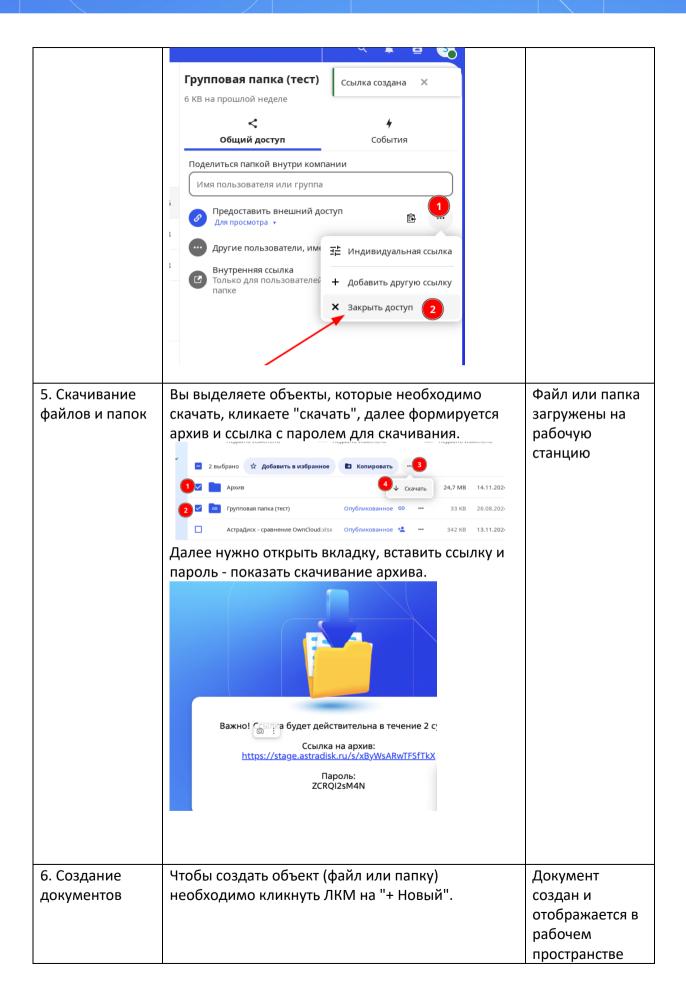
Программа и методика испытаний работы функционала Astra Disk

Номер и название	Описание	Результат
1. Загрузка файлов и папок	Чтобы загрузить файл вы можете воспользоваться кнопкой "Новый" - "Загрузка файлов". И в открывшемся окне указать необходимые документы или же воспользоваться дроп-зоной, которая появляется, когда вы переносите файл в интерфейс Астра Диска (можно что-то загрузить с рабочего стола в дроп зону)	Файл загружен
2. Поделиться файлом/ папкой	Вы можете перейти в раздел работы с доступами к файлам и папкам из рабочего пространства, нажав на значок или в открывшейся вкладке можно управлять ограничениями на доступы, можно указывать имена пользователей или групп из каталога LDAP. Вы можете разрешить или запретить: чтение запись создание удаление публикация скачивание установить срок публикации Для применения настроек необходимо кликнуть" сохранить общий доступ".	Пользователям, с которыми поделились файлом или папкой стала доступна папка или файл с учетом указанных ограничений.

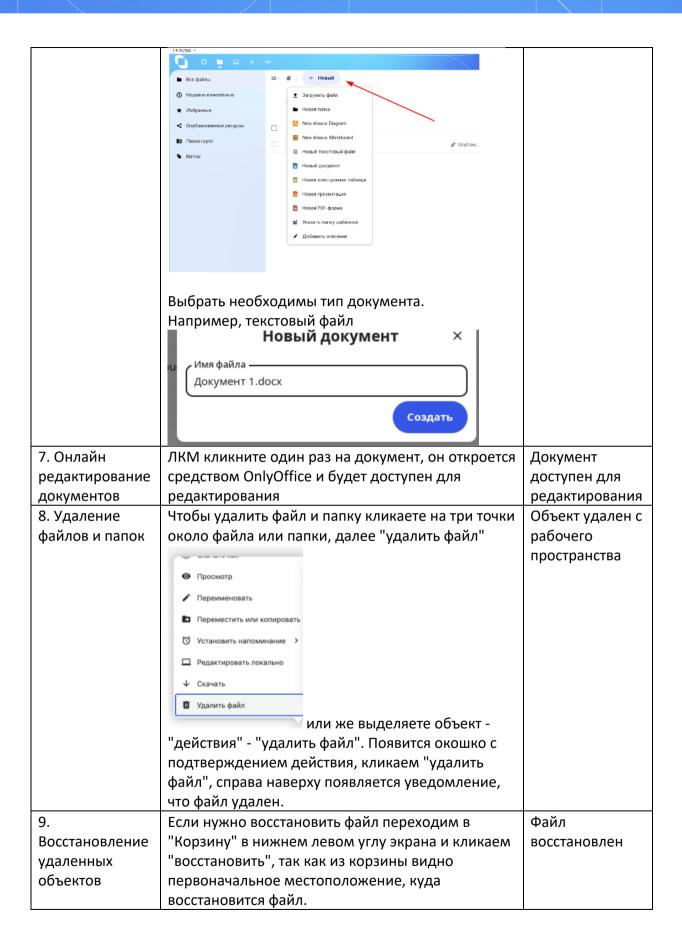


3. Создание	Вы можете перейти в раздел работы с доступами	Внешний доступ
ссылок с	к файлам и папкам из рабочего пространства,	предоставлен.
внешним	_	
доступом	+2	
	,	
	нажав на значок или . В	
	открывшейся вкладке выбрать «предоставить	
	внешний доступ».	
	Групповая папка (тест)	
	6 КВ на прошлой неделе	
	< ∳ Общий доступ События	
	Поделиться папкой внутри компании Имя пользователя или группа	
	Предоставить внешний доступ	
	∙ Оругие пользователи, имеющие доступ • Оправления общие доступ • Оправ	
	Внутренняя ссылка Только для пользователей с доступом к этой папке	
	Halike	
	Вы можете разрешить или запретить:	
	• чтение	
	• запись	
	• создание	
	• удаление	
	• публикация	
	• скачивание	
	• установить срок публикации	
	Для применения настроек необходимо	
	кликнуть"сохранить общий доступ".	
4. Удаление	Вы можете перейти в раздел работы с доступами	Внешняя ссылка
ссылок с	к файлам и папкам из рабочего пространства,	недоступна
внешним	_	
доступом	م بـ •	
	нажав на значок или . В	
	нажав на значок или . В открывшейся вкладке выбрать «Закрыть доступ».	
	открывшейся вкладке выорать «закрыть доступ».	

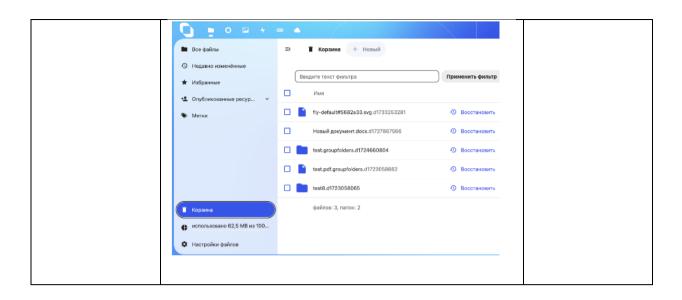












Проверка работы с пользователями и группами LDAP в ПО Astra Disk

Номер теста	Описание	Результат
Номер теста Тест 1 - Авторизация	Описание Попытка входа на странице авторизации выполнена успешно. Необходимо ввести логин и пароль, кликнуть кнопку «войти»	Войти – Astra.Disk Вход в Astra.Disk Учётная запись или адрес эл. почты птапикhina
		Пароль ———————————————————————————————————
Тест 2 –	Выдача прав на файл	Права на файл выданы успешно. Можно проверить
Управление правами на файл (пользователю)	пользователю. Необходимо перейти «Открыть подробности», ввести логин доменного пользователя, «сохранить общий ресурс».	выдачу прав, авторизовавшись под доменным пользователем, кому были выданы права.



		Control Contro
		Conformment prop. Insent Text doping pdf Marrie Married Marr
		Hosan PDF-dopma.pdf
		Версии О <mark>бщий дес</mark> туп Собиния Подальное филоков ступри компини
		See Suppos Copycion See See See See See See See See See Se
		Michael Applicat Captions Annual Applicat Captions Michael Captions Michael Captions Michael Captions Michael Captions Michael Captions Michael Captions
		© POUTS INSERING
	_	
Тест 3 –	Выдача прав на папку	Права на папку выданы успешно. Можно
Управление правами на папку	пользователю. Необходимо перейти	проверить выдачу прав, авторизовавшись под доменным пользователем, кому были выданы
(пользователю)	«Открыть	права.
(11071b30ba1c71l0)	подробности», ввести	права.
	логин доменного	
	пользователя LDAP,	
	«сохранить общий ́	© © 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
	ресурс».	⊕ Header on Conference □ 2 months ↑ Info@mente □ 1 Moder on the conference ■ Moder on the conference ■ 1 Moder on the conference □ 1 Moder on the conference ■ 1 Moder on the conference □ 2 Moder on the conference □ 1 Moder on the conference □ 2 Moder on the conference □ 2 Moder on the conference □ 3 Moder on the conference □ 2 Moder on the conference □ 3 Moder on the conference □ 3 Moder on the conference □ 3 Moder on the conference □ 3 Moder on the conference □ 3 Moder on the conference □ 3 Moder on the conference □ 4 Moder on the conference □ 3 Moder on the conference □ 4 Moder on the conference □ 4 Moder on the conference □ 5 Moder on the conference □ 4 Moder on the conference □ 5 Moder on the conference □ 4 Moder on the conference □ 6 Moder on the conference □ 4 Moder on the conference □ 6 Moder on the conference □ 4 Moder on the conference □ 6 Moder on the conference □ 4 Moder on the conference □ 7 Moder on the conference □ 4 Moder on the conference □ 7 Moder on the conference □ 4 Moder on the conference
		■ Hassa POF-Sports (OF 1998 1997 1998 1998 1999 (1999 1999 1999 1999 199
		Areas Coppens Annual Coppens
		A AND A GIVEN AND A STATE OF THE AND A STATE OF T
		A. ARECHIQUE AND
Тест 4 -	Выдача прав на файл	Права на файл выданы успешно. Можно проверить
Управление	группе	выдачу прав, авторизовавшись под доменным
правами на файл	пользователей.	пользователем – участником выбранной группы,
(группа пользователей)	Необходимо перейти «Открыть	которой были выданы права.
The state of the s	подробности», ввести	S to plates S to to below + New S
	название группы	Pagano paredemore
	LDAP, «сохранить	
	общий ресурс».	House Put-dopped poil 1010 Z rounge abusing O
		ократи в общения по
		19 squarefood white corner 4 19 squarefood white corner 4
		3 speedstand within on 4
		1 spention finder o 4
		Toposos
Тест 5 -	Выдача прав на папку	Права на папку выданы успешно. Можно
Управление	группе	проверить выдачу прав, авторизовавшись под
правами на папку	пользователей.	доменным пользователем – участником
(группа	Необходимо перейти	выбранной группы, которой были выданы права.
пользователей)	«Открыть подробности», ввести	<u> </u>
	название группы	To the State of the Control of the C
	LDAP, «сохранить	# Endpartment
	общий ресурс».	Specification of the specific
		3 agreendatud schalacry 4. Signification of the control 4.
		5 signification of fair ro 4.
		S tag-rendals of field or a
	<u> </u>	



Тест 6 – Поиск Поиск сотрудников в Поиск работает корректно. пользователей в адресной книге адресной книге можно осуществить кликнув в верхнем Поиск контактов правом углу на значок Поиск контакта... sysadmin В открывшемся sysadmin@localhost.lo... окне можно Александр Усков произвести поиск auskov@astralinux.ru сотрудника по Александр Чудскаев achudskaev@astralinu... логину/электронной Александра Ващенко почте/ имени. AB avashchenko@astralin... ая PDF-Алексей Осипов AO 2 месяца aosipov@astralinux.ru

Ð