

Руководство
администратора

Atlansys WhiteCloud



Atlansys White Cloud

Руководство администратора

ООО «Программные системы Атлансис»

Версия 4.0

Информация, касающаяся описания продукта в данном руководстве, может быть изменена без предварительного уведомления. Все утверждения, информация и рекомендации в настоящем руководстве полагаются корректными, но приведены без гарантий любого рода, явных или подразумеваемых. Пользователи должны принять на себя полную ответственность за их применение. Лицензия на программное обеспечение изложена в документации, поставляющейся вместе с продуктом, а также включена в настоящее руководство. Если по каким-либо причинам вы не можете найти текста лицензионного соглашения, свяжитесь с представителем ООО «Программные системы Атлансис» для получения ее копии.

Компания ООО «Программные системы Атлансис» не несет ответственности за любой косвенный, специальный или побочный ущерб, включая, без ограничений, упущенную прибыль, убыток или повреждение данных, вытекающие из использования или невозможности использования данного руководства, даже если ООО «Программные системы Атлансис», ее поставщики, партнеры или дистрибьюторы были заранее извещены о возможности такого ущерба.

Copyright © ООО «Программные системы Атлансис», 2012-2021

Содержание

Введение	v
1. Назначение документа	v
2. Сведения о продукте	v
1. Техническая поддержка.....	1
2. Сервис защищенных хранилищ Atlansys White Cloud.....	2
3. Общие сведения	3
3.1. Комплектность поставки	3
3.1.1. Программное обеспечение, необходимое для функционирования	3
3.1.2. Сервер. Системные требования.....	3
3.1.3. Клиент. Системные требования.	3
4. Установка Atlansys White Cloud	5
4.1. Установка сервера.....	5
4.2. Запуск сервера.....	5
4.3. Установка web-интерфейса	6
5. Настройки Atlansys White Cloud.....	7
5.1. Настройки службы	7
6. Настройки доступа	9
6.1. Настройки групп пользователей	9
6.2. Настройки пользователей	9
6.2.1. Импорт пользователей из LDAP-каталога.....	10
6.3. Настройки общих папок.....	12
7. Система восстановления ключей	14
7.1. Введение.....	14
7.2. Настройка мастер-сертификата группы.....	14
7.3. Восстановление ключей.....	14
8. Журнал событий	16

Список иллюстраций

6.1. Группы пользователей.....	9
6.2. Список пользователей.....	10
6.3. LDAP авторизация.....	10
6.4. Импорт пользователей.....	11
6.5. Импорт групп пользователей.....	11
6.6. Добавление пользователя.....	12
6.7. Общие папки.....	12
6.8. Добавление общей папки.....	13
6.9. Дерево пользователей.....	13
7.1. Создание группы.....	14
7.2. Изменение пароля.....	15
7.3. Изменение сертификата.....	15
8.1. Журнал событий.....	16

Введение

1. Назначение документа

Данное руководство администратора содержит сведения по установке, настройке и эксплуатации Atlansys White Cloud и предназначено для конечных администраторов системы.

2. Сведения о продукте

Программный продукт Atlansys White Cloud предназначен для работы с веб-сервисом Atlansys White Cloud, который предоставляет пользователям личное защищенное хранилище данных.

Дополнительные сведения об использовании данного продукта и последние версии документации можно получить на сайтах компании www.atlansys.ru, www.atlansys.tech.

Глава 1. Техническая поддержка

Техническая поддержка данного продукта осуществляется в рамках правил, опубликованных на сайтах www.atlansys.ru, www.atlansys.tech. Обратиться в службу технической поддержки можно по телефонам, указанным на сайте, либо по электронной почте по адресу <support@atlansys.ru>. Для получения оперативного ответа при запросе в службу технической поддержке будьте готовы предоставить следующую информацию:

- Фамилию, имя, отчество контактного лица, адрес электронной почты, номер телефона.
- Полное наименование продукта.
- Версия продукта (отображается в диалоге «О программе»).
- Лицензионный ключ, либо серийный номер продукта.
- Версия операционной системы, описание конфигурации компьютера.
- Краткое описание возникшей проблемы и действий, которые к ней привели.
- По возможности, снимки экрана при возникновении ошибки, код ошибки, лог-сообщения, которые предшествовали ошибке.
- При возникновении ошибок в сторонних программах, связанных с использованием данного продукта, наименование и номера версий этих программ.



Важно

Никогда не сообщайте кому-бы то ни было пароли и другую конфиденциальную информацию. Служба технической поддержки не запрашивает каких-либо паролей, ключей и ПИН-кодов.

Глава 2. Сервис защищенных хранилищ Atlansys White Cloud

Сервис Atlansys White Cloud предоставляет пользователям личные защищенные хранилища данных, доступ к информации в которых отсутствует даже у администраторов сервиса. Все пользовательские данные в хранилище шифруются одним из нескольких криптостойких алгоритмов, который можно выбрать на этапе создания хранилища. Доступ к хранилищу осуществляется как при помощи веб-интерфейса (подробности можно узнать на сайтах компании www.atlansys.ru, www.atlansys.tech), так и при помощи программного клиента для Windows.

Глава 3. Общие сведения

3.1. Комплектность поставки

3.1.1. Программное обеспечение, необходимое для функционирования

Atlansys White Cloud поставляется в трех файлах:

- Atlansys-White-Cloud-Server-(version).(revision). zip – архив, содержащий серверную часть СХД;
- Atlansys-White-Cloud-Administrator-Console.zip – архив, содержащий управляющий модуль для доступа к настройке серверной части;
- Atlansys_Cloud_Client-(version).(revision)-setup-x(platform).msi – инсталлятор программного клиента для ОС Windows.

3.1.2. Сервер. Системные требования.

Для функционирования серверной части необходимо следующее программное обеспечение:

- ОС семейства Linux (в настоящее время поддерживается Ubuntu Server версии 14 и выше и Alt Linux версии 6.0 и выше);
- Сервер баз данных MySQL версии 5 или выше.

Для функционирования веб-интерфейса необходимо наличие:

- ОС семейства Linux (в настоящее время поддерживается Ubuntu Server версии 14 и выше и Alt Linux версии 6.0 и выше);
- Веб-сервер Apache 2.2;
- Сервер баз данных MySQL версии 5 или выше;
- PHP версии 5 или выше (как модуль Apache).

Для функционирования веб-интерфейса требуется любой компьютер, на котором может работать современный веб-браузер.

Для функционирования сервера необходимы следующие минимальные системные требования:

- IBM PC совместимый с процессором архитектуры x64 и операционной системой ALT Linux;
- Процессор Intel Pentium IV с частотой не менее 2ГГц (рекомендуется использовать серверные многоядерные процессоры);
- ОЗУ не менее 2ГБ (рекомендуется не менее 16ГБ);
- Свободное место на жестком диске не менее 500МБ (для размещения хранилищ пользователей свободное место следует рассчитывать отдельно, исходя из потребностей).

3.1.3. Клиент. Системные требования.

Для функционирования программного клиента необходимо наличие:

- ОС Windows XP, Vista, 7, 8, 8.1, 10 (32 или 64);

Для функционирования клиента необходимы следующие минимальные системные требования:

- IBM PC совместимый с процессором архитектуры x32 или x64 и операционной системой Windows;
- Процессор Intel Pentium IV с частотой не менее 1,8ГГц;
- ОЗУ не менее 1ГБ;
- Свободное место на жестком диске не менее 100МБ.
- Видеопамять не менее 64МБ.

Глава 4. Установка Atlansys White Cloud

4.1. Установка сервера



Важно

Что следует помнить перед установкой ПО Atlansys White Cloud:

- Сервер должен быть настроен в конфигурации LAMP (Linux, Apache, MySQL, PHP).
- Необходимо обладать правами Администратора операционной системы.
- Необходимо знать логин и пароль Администратора СУБД.

Для установки сервера в систему необходимо распаковать tar файл с дистрибутивом сервера во временный каталог, перейти в этот каталог и выполнить команду **sudo ./install.sh**

В процессе установки необходимо ответить на несколько вопросов.

1. **Enter type authentication for Atlansys White Cloud (ldap or db) [db]:** Тип авторизации: ldap или db. Параметр определяет, будет ли использоваться ldap-сервер для импорта учетных записей.
2. **Enter MySQL host [localhost]:** Адрес сервера, где установлена база данных MySQL (здесь и далее в квадратных скобках приведены значения по умолчанию).
3. **Enter MySQL superuser name [root]:** Имя суперпользователя MySQL.
4. **Enter MySQL root password:** Пароль суперпользователя MySQL.
5. **Enter MySQL user name for database 'cloud' [cloud]:** Имя пользователя для базы данных WhiteCloud.
6. **Enter MySQL user password:** Пароль пользователя базы данных.

Если был выбран тип авторизации "ldap" будут заданы еще несколько дополнительных вопросов.

1. **Enter LDAP host [192.168.1.1]:** Адрес LDAP-сервера, где хранится информация о сертификатах пользователей.
2. **Enter LDAP port [389]:** Порт для подключения к LDAP-серверу.
3. **Enter LDAP user [anonymous]:** Имя пользователя для подключения к LDAP-серверу.
4. **Enter LDAP user password:** Пароль для подключения к LDAP-серверу. Может быть пустым. Если установка пройдет успешно, то в конце появится надпись "Installation successfully complete".

В результате выполнения этой команды сервер будет установлен в каталог `/var/whitecloud` со следующими подкаталогами:

- bin – в нем располагается исполняемый файл сервера;
- etc – в нем располагается конфигурационный файл сервера;
- storage – в нем располагаются пользовательские файлы и каталоги.

4.2. Запуск сервера

Запуск сервера осуществляется автоматически при загрузке операционной системы.

Для запуска сервера вручную необходимо выполнить команду:

```
sudo service acd start
```

Для остановки сервера необходимо выполнить команду:

```
sudo service acd stop
```

Для проверки правильности запуска сервера необходимо выполнить команду:

```
"sudo service acd status" или "ps aux | grep acd"
```

В случае, если сервер запущен, будет выведено сообщение:

```
"acd is running" или две строчки: /var/whitecloud/bin/acd  
grep acd
```

В противном случае появится сообщение:

```
acd is stopped или одна строчка: /var/whitecloud/bin/acd
```

4.3. Установка web-интерфейса

Установка web-интерфейса осуществляется автоматически в процессе установки сервера.

Глава 5. Настройки Atlansys White Cloud

5.1. Настройки службы

Настройки службы расположены в файле `/var/whitecloud/etc/acd.conf`

```
[main]
storage_path=/mnt/whitecloud_disk/storage
storage_group_name=awc      #имя      группы
threads_count=10
db_host=localhost          #имя сервера СУБД
db_port=                   #порт сервера СУБД
db_name=cloud              #имя базы данных
db_user=cloud              #имя пользователя для подключения к базе данных
db_password=cloud         #пароль пользователя для подключения к базе данных

[auth_plugins]
names=auth_db              #имя модуля аутентификации пользователей

[auth_db]                  #настройки модуля для внутренней аутентификации пользователей
file=/var/whitecloud/modules/auth/libdb.so #путь к модулю администратора
host=localhost            #имя сервера СУБД
port=                     #порт сервера СУБД
db_name=cloud             #имя базы данных
user=cloud                #имя пользователя для подключения к базе данных
password=cloud            #пароль пользователя для подключения к базе данных

[auth_ldap]                #настройки модуля для аутентификации пользователей через LDAP
file=/var/whitecloud/modules/auth/libldap.so #путь к модулю
address=192.168.1.126     #адрес LDAP сервера
port=389                  #порт LDAP сервера
admin=anonymous           #логин для доступа к LDAP серверу
password=                  #пароль для доступа к LDAP серверу
search_base="C=RU"        #корневой адрес для поиска учетных записей в LDAP-каталоге
user_id_field_name=cn     #название поля, по которому идет поиск учетных записей в LDAP-
каталоге certs_field_name=userCertificate #название поля, в котором хранится сертификат
пользователя
[logger]
mode_db=0                 #журнал событий писать в БД
local_db_log_level=5     #уровень событий для записи в журнал
db_host=localhost        #имя сервера СУБД
db_port=                 #порт сервера СУБД
db_name=cloud            #имя базы данных
db_user=cloud            #имя пользователя для подключения к базе данных
db_password=cloud        #пароль пользователя для подключения к базе данных
mode_syslog=0            #журнал событий писать в SYSLOG
address_syslog=          #IP адрес SYSLOG сервера
syslog_level=5           #уровень событий для записи в журнал
syslog_port=             #порт SYSLOG сервера
```

`main/storage_path` - путь к хранилищу файлов на сервере.

`main/storage_group_name` - имя группы владельца хранилища файлов на сервере.

`main/threads_count` - количество одновременно выполняемых задач в службе сервера хранилищ.

`main/db_*` - параметры подключения службы сервера хранилищ к СУБД.

`auth_plugins/names` - имя секции, используемой для аутентификации. Возможные значения: `auth_db` - аутентификация с использованием СУБД, `auth_ldap` - с использованием LDAP.

Секция `auth_db` используется для подключения к системе аутентификации с помощью СУБД. В `auth_db/file` - указывается путь к файлу модуля аутентификации. `Host`, `port`, `db_name`, `user` и `password` параметры подключения к СУБД.

Секция `auth_ldap` используется для подключения к системе аутентификации с помощью LDAP. В `auth_ldap/file` - указывается путь к файлу модуля аутентификации. `Address` и `port` - адрес и порт LDAP сервера.

В секции `logger` содержатся настройки записи в журнал. Журнал может писаться в два вида хранилищ: в БД и в Syslog-сервер.

1. Параметр `logger/mode_db` служит для включения(1)/выключения(0) записи в журнал БД. `Logger/db_*` - параметры подключения к СУБД при записи журнала в БД. Параметр `logger/local_db_log_level` может иметь значение от 0 до 7 и устанавливает уровень детализации журнала.
2. Параметр `logger/mode_syslog` служит для включения(1)/выключения(0) записи в журнал Syslog. Параметр `logger/syslog_level` может иметь значение от 0 до 7 и устанавливает уровень детализации журнала.

Уровни регистрируемых ошибок в журнале:

1. `Emergency` - критический сбой
2. `Alert` - тревога
3. `Critical` - критическая ошибка
4. `Error` - ошибка
5. `Warning` - предупреждение
6. `Notice` - уведомление
7. `Info` - информация
8. `Debug` - сообщения для отладки

Для применения настроек сервера необходимо выполнить команду

`sudo service acd restart`

Глава 6. Настройки доступа

6.1. Настройки групп пользователей

Вкладка «Группы» предназначена для управления группами пользователей и реализует следующие функции:

- добавление/импорт группы пользователей;
- редактирование параметров группы пользователей;
- удаление группы пользователей;

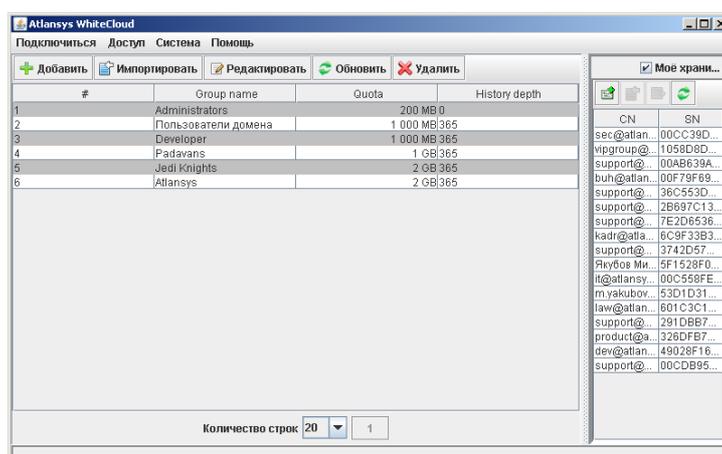


Рисунок 6.1. Группы пользователей

Группа пользователей обладает следующими параметрами:

- «Имя группы» - имя группы;
- «Квота» - общий размер пользовательского пространства;
- «История» - критерии ведения истории файла;
- «Default» - группа по умолчанию (по умолчанию создаваемые пользователи попадают в эту группу);
- «Роль» - роль группы (значения: «Administrator» - группа администраторов, «User» - пользовательские группы). Роль группы используется только для ограничения доступа к настройкам системы:
 - «Administrator» - имеет доступ к функциям управления пользователями, группами пользователей, просмотр всего журнала событий, просмотр и изменение настроек системы.
 - «User» - имеет полный доступ к своему хранилищу данных и может просматривать только свой журнал событий.

6.2. Настройки пользователей

Вкладка «Пользователи» предназначена для управления пользователями и реализует следующие функции:

- добавление/импорт пользователя;
- редактирование пользователя;
- удаление пользователя;

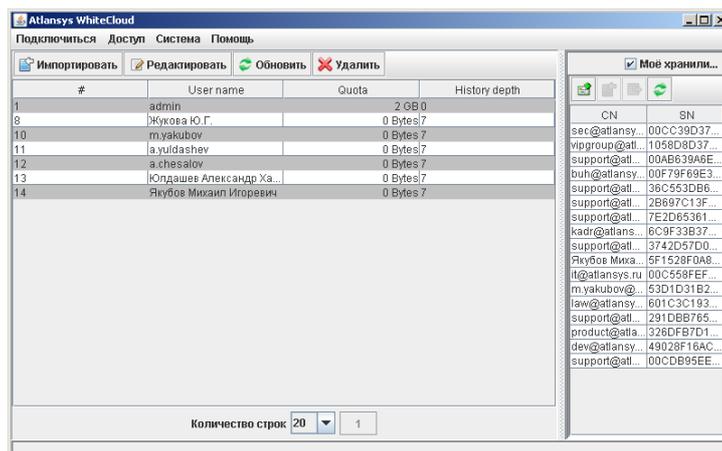


Рисунок 6.2. Список пользователей

Пользователь обладает следующими параметрами:

- «Имя пользователя» - имя пользователя;
- «Пароль» - пароль пользователя;
- «Сертификат» - личный сертификат пользователя;
- «Группы пользователя» - группы, в которые пользователь входит;
- «Квота» - общий размер пользовательского пространства;
- «История» - критерии ведения истории файла.

6.2.1. Импорт пользователей/групп пользователей из LDAP-каталога

Для операций по импорту учетных записей требуется подключение к LDAP серверу. Для подключения нужно в главном меню консоли администратора выбрать раздел Подключиться > LDAP. Затем нужно ввести следующие данные:

- Адрес – IP/URL адрес LDAP сервера
- Логин и пароль – учетные данные для входа. При анонимном доступе можно не заполнять либо указать anonymous без пароля.
- Домен – внутренний DN нужной ветки LDAP-каталога. Например OU = Исполнительный аппарат, O = ПАО «РОССЕТИ», C = RU

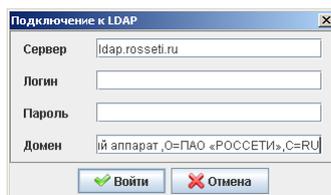


Рисунок 6.3. LDAP авторизация

Для импорта учетной записи из LDAP каталога нужно нажать на панели инструментов кнопку Импортировать. Будет отображен список найденных учетных записей в LDAP каталоге. Напротив нужной учетной записи нужно нажать кнопку Импортировать. Аналогично для групп пользователей

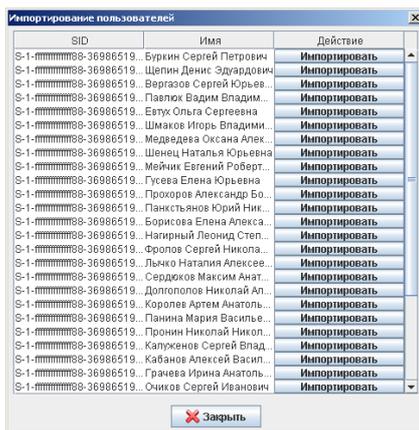


Рисунок 6.4. Импорт пользователей

После этого будут запрашиваться закрытые ключи установленных в системе сертификатов. При необходимости может потребоваться ввести несколько раз ПИН код. Далее открывается окно редактирования настроек пользователя. Здесь нужно выбрать группы, в которые требуется включить пользователя, а также его сертификат. Для завершения импорта нужно нажать кнопку Сохранить и ввести необходимое количество раз ПИН-код для мастер-сертификатов выбранных групп, если требуется.

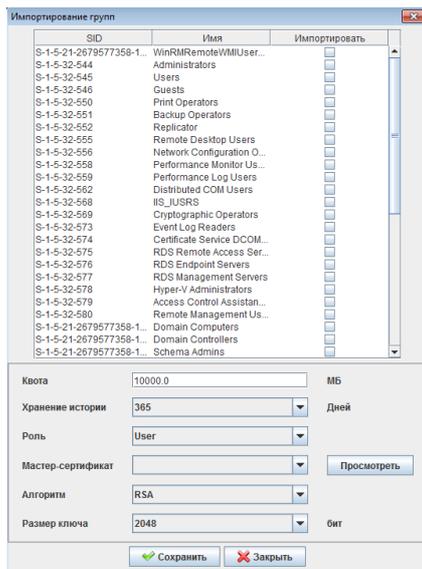


Рисунок 6.5. Импорт групп пользователей

При импорте групп необходимо будет задать «Квоту» выбрать Роль группы "USER"/"Administrator" и мастер-сертификат с закрытым ключом, установленный в системе сертификатов. При необходимости может потребоваться ввести несколько раз ПИН код. При импорте групп пользователей из LDAP-каталога в базу данных WhiteCloud необходимо, чтобы имя учетных записей совпадало с sAMAccountName при авторизации по логину и паролю. По умолчанию при импорте пользователей пароль присваивается для всех учетных записей один и тот же: 12345678. При авторизации пользователя на клиенте для Windows пользователь вводит свой доменный пароль, если все правильно ввел выйдет окно с вводом старого пароля, таким образом, надо ввести в окне: 12345678 и пароль доменного пользователя применится к учетной записи в нашей базе данных.

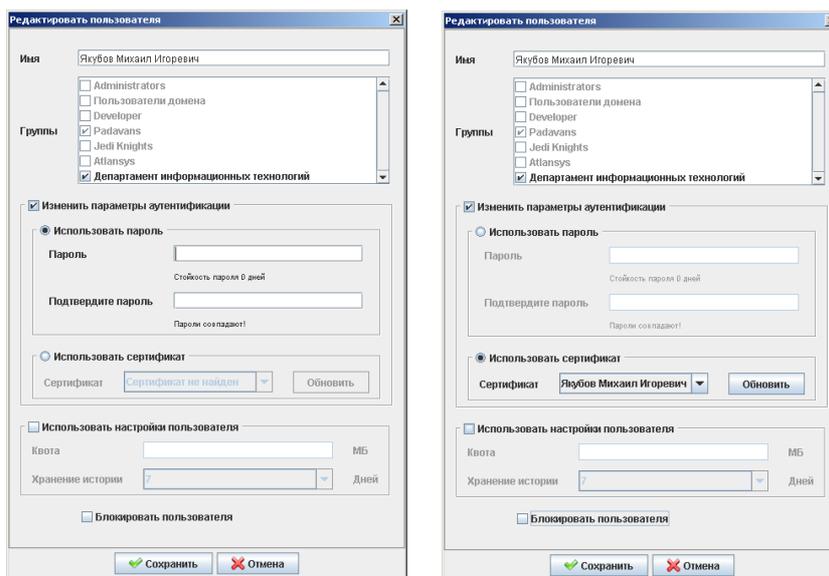


Рисунок 6.6. Добавление пользователя

В случае, если при добавлении/импорте пользователя выбран тип авторизации по паролю, необходимо вместо выбора сертификата ввести пароль пользователя в соответствующие поля.

6.3. Настройки общих папок

Вкладка «Общие папки» предназначена для управления общими папками пользователей и реализует следующие функции:

- добавление общих папок;
- редактирование параметров доступа к содержимому общих папок;

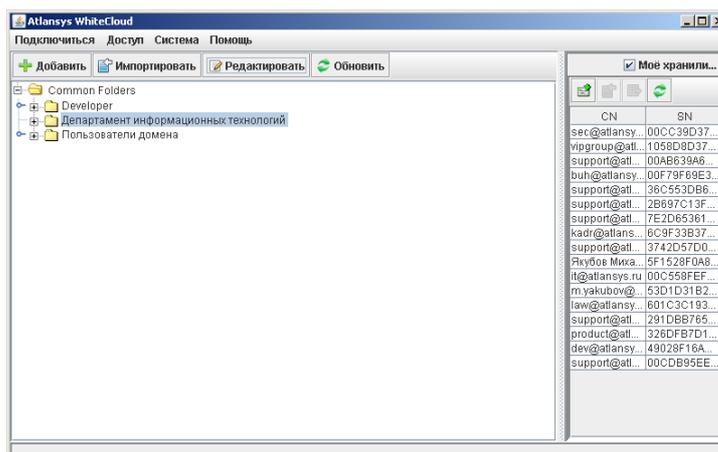


Рисунок 6.7. Общие папки

Для добавления общих папок нужно в главном меню консоли администратора выбрать раздел Доступ > Общие папки.

Далее нужно выбрать корневую директорию и на панели инструментов нажать кнопку Добавить.

Далее вводится имя папки, задаются права на доступ к ней для разных групп, после чего нужно нажать кнопку Сохранить, чтобы применить изменения, сделанные на сервере.

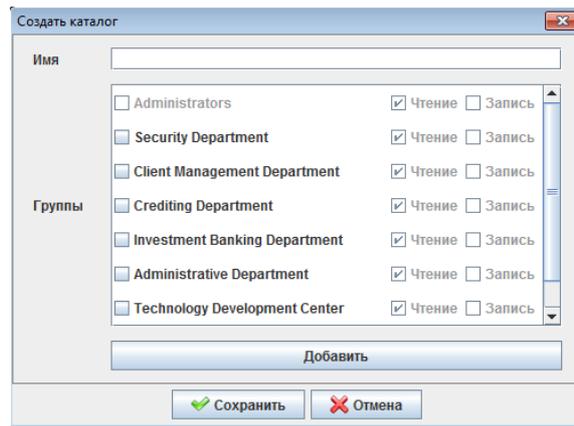


Рисунок 6.8. Добавление общей папки

При добавлении Общих папок можно выполнить импорт групп из LDAP-каталога, которые будут участвовать в распределении доступа к этой Общей папке.

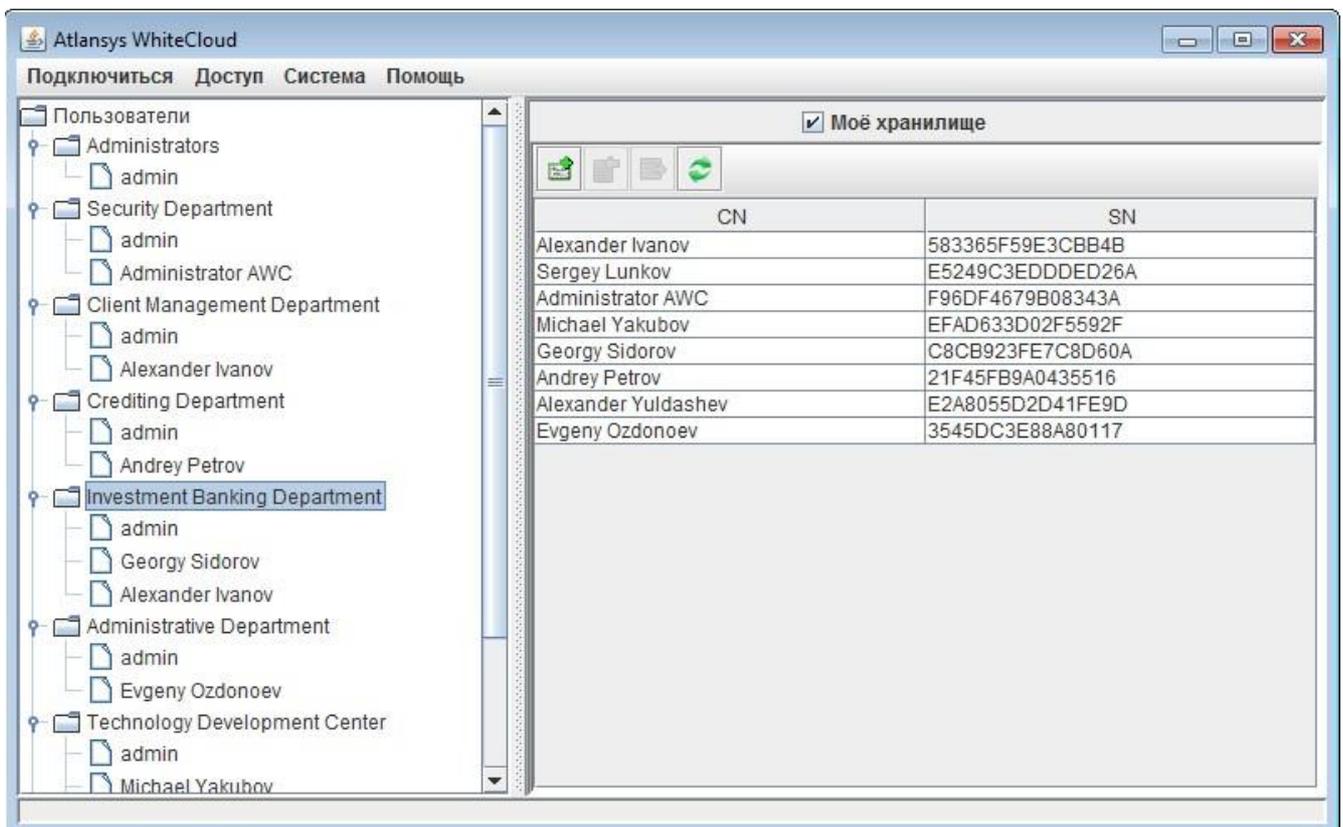


Рисунок 6.9. Дерево пользователей

При просмотре дерева пользователей можно одним кликом на учетной записи/группе зайти в свойства и выполнить редактирование выбранного объекта.

Глава 7. Система восстановления ключей

7.1. Введение

Процедура восстановления ключей применяется в случае невозможности получения доступа пользователя к своему хранилищу данных, в случае утраты пароля, либо сертификата с закрытым ключом.

7.2. Настройка мастер-сертификата группы

Для каждой группы пользователей создается свой уникальный мастер-ключ для восстановления доступа.

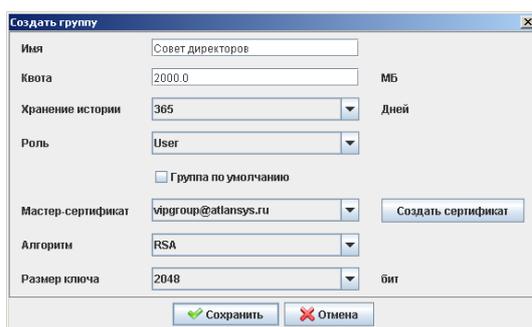


Рисунок 7.1. Создание группы

Мастер-сертификат группы используется при добавлении новых пользователей и редактировании параметров аутентификации каждого пользователя.



Важно

Утеря мастер-сертификата делает систему восстановления ключей неработоспособной.

7.3. Восстановление ключей

Для восстановления доступа пользователя, перейдите во вкладку "Пользователи". Найдите в списке нужного пользователя и нажмите кнопку "Редактировать".

The screenshot shows a dialog box titled "Редактировать пользователя" (Edit User). The "Имя" (Name) field contains "Якубов Михаил Игоревич". Under "Группы" (Groups), several options are listed, with "Департамент информационных технологий" (IT Department) selected. The "Изменить параметры аутентификации" (Change authentication parameters) section is checked, and the "Использовать пароль" (Use password) radio button is selected. The "Пароль" (Password) and "Подтвердите пароль" (Confirm password) fields are empty. The "Использовать сертификат" (Use certificate) option is not selected, and the "Использовать настройки пользователя" (Use user settings) option is also not selected. At the bottom, there are "Сохранить" (Save) and "Отмена" (Cancel) buttons.

Рисунок 7.2. Изменение пароля

This screenshot is similar to the previous one, but the "Использовать сертификат" (Use certificate) radio button is now selected. The "Сертификат" (Certificate) dropdown menu now displays "Якубов Михаил Игоревич". The "Использовать пароль" option is now unselected. All other elements, including the name, groups, and user settings, remain the same as in the previous screenshot.

Рисунок 7.3. Изменение сертификата

В появившемся окне редактирования выберите пункт "Изменить параметры аутентификации" и укажите новый пароль/сертификат пользователя. Затем нажмите кнопку "Сохранить".

Глава 8. Журнал событий

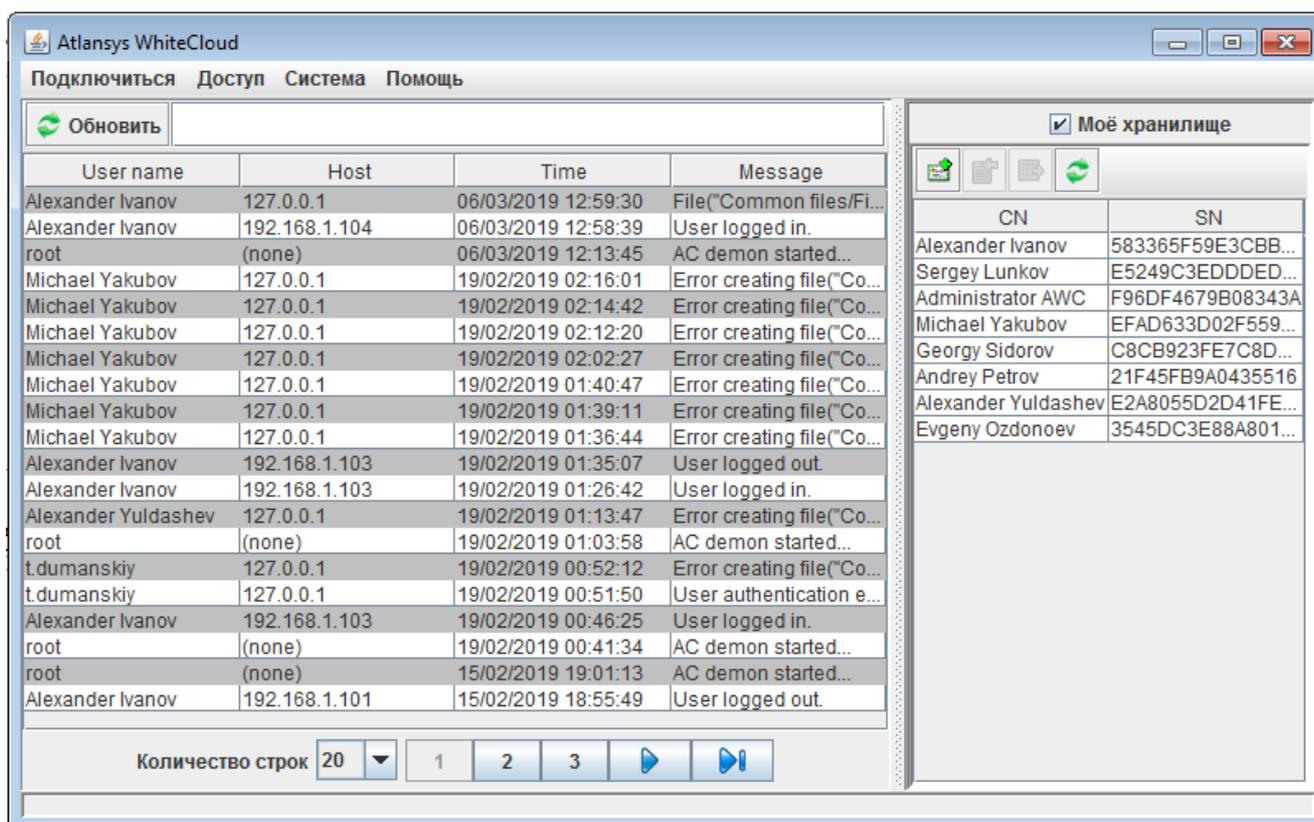
При просмотре журнала событий в поиске можно задать имя пользователя/событие/дату, и система осуществить фильтр по данным критериям.

Также есть возможность экспорта событий на сервер SYSLOG. Для этого необходимо в конфигурационном файле `acd.conf` в секции выставить режим записи событий не в локальную базу данных.

[logger]

`mode_db = 0` #журнал событий писать в БД `mode_syslog = 1` #журнал событий писать в SYSLOG

`address_syslog = ip-address/domain_name` #адрес SYSLOG сервера `syslog_level = 5` #уровень событий для записи в журнал SYSLOG-сервера `syslog_port =` #порт SYSLOG сервера



The screenshot shows the Atansys WhiteCloud interface. The main window displays a table of events with columns for User name, Host, Time, and Message. The table contains 20 rows of log entries. Below the table, there is a control bar with a dropdown menu for the number of rows (set to 20) and navigation buttons. To the right of the event log, there is a sidebar titled 'Моё хранилище' (My storage) which contains a table of users with columns for CN and SN.

User name	Host	Time	Message
Alexander Ivanov	127.0.0.1	06/03/2019 12:59:30	File("Common files/Fi...
Alexander Ivanov	192.168.1.104	06/03/2019 12:58:39	User logged in.
root	(none)	06/03/2019 12:13:45	AC demon started...
Michael Yakubov	127.0.0.1	19/02/2019 02:16:01	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 02:14:42	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 02:12:20	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 02:02:27	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 01:40:47	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 01:39:11	Error creating file("Co...
Michael Yakubov	127.0.0.1	19/02/2019 01:36:44	Error creating file("Co...
Alexander Ivanov	192.168.1.103	19/02/2019 01:35:07	User logged out.
Alexander Ivanov	192.168.1.103	19/02/2019 01:26:42	User logged in.
Alexander Yuldashev	127.0.0.1	19/02/2019 01:13:47	Error creating file("Co...
root	(none)	19/02/2019 01:03:58	AC demon started...
t.dumanskiy	127.0.0.1	19/02/2019 00:52:12	Error creating file("Co...
t.dumanskiy	127.0.0.1	19/02/2019 00:51:50	User authentication e...
Alexander Ivanov	192.168.1.103	19/02/2019 00:46:25	User logged in.
root	(none)	19/02/2019 00:41:34	AC demon started...
root	(none)	15/02/2019 19:01:13	AC demon started...
Alexander Ivanov	192.168.1.101	15/02/2019 18:55:49	User logged out.

CN	SN
Alexander Ivanov	583365F59E3CBB...
Sergey Lunkov	E5249C3EDDED...
Administrator AWC	F96DF4679B08343A
Michael Yakubov	EFAD633D02F559...
Georgy Sidorov	C8CB923FE7C8D...
Andrey Petrov	21F45FB9A0435516
Alexander Yuldashev	E2A8055D2D41FE...
Evgeny Ozdonoev	3545DC3E88A801...

Рисунок 8.1. Журнал событий