

Настройка синхронизации

Данный модуль предназначен для настройки соединения с доменом в сети, по средствам сетевого протокола kerberos или ldap.

Kerberos

ООО "Организация" > Настройки авторизации

Kerberos

LDAP

Имя компьютера *

test

Имя домена *

test.ru

При изменении имени компьютера и домена будет изменено имя системы в модуле Система

DNS-имя контроллера домена *

AD.test.ru

Keytab файл



Для создания кейтаба необходимо выполнить следующие действия в контроллере домена:

1. Создать пользователя test с бессрочным паролем
2. Выполнить от имени администратора в командной строке:

```
ktpass -princ HTTP/test.test.ru@TEST.RU -mapuser "test" -pass "Aa123456" -crypto All -ptype KRB5_NT_PRINCIPAL -out C:\ics_01.keytab
```

-princ HTTP/test.test.ru@TEST.RU - имя принципала службы (SPN)
-mapuser "test" - пользователь
-pass "Aa123456" - пароль

Сохранить

Обновить

Для подключения к контроллеру домена по сетевому протоколу kerberos необходимо заполнить все имеющиеся поля:

Поле «Имя компьютера». Задаёт hostname.

Поле «Имя домена». Задаёт имя домена, в котором ИКС будет как пользователь.

Поле «DNS-имя контроллера домена». Указывается соответствующее имя.

Поле «Keytab файл». Предназначено для загрузки Keytab файла.

Рассмотрим пример создания Keytab файла, предположим, что имя компьютера - Test, а имя домена - test.ru. Тогда для создания Keytab файла необходимо выполнить следующие действия на контроллере домена:

- Создать пользователя **Test** с бессрчным паролем, имя не должно содержать кириллических символов
- Выполнить от имени администратора в командной строке

```
ktpass -princ HTTP/Test.test.ru@TEST.RU -mapuser «Test» -pass «Aa123456» -crypto All -ptype KRB5_NT_PRINCIPAL -out C:\ics_01.keytab
```

где

-princ HTTP/Test.test.ru@TEST.RU - имя принципала службы (SPN)

-mapuser «Test» - пользователь созданный в контроллере домена

-pass «Aa123456» - пароль созданного пользователя

-out C:\ics_01.keytab - путь где создавать Keytab файл с указанием его имени

В случае удачной настройки, ИКС сообщит соответствующую информацию (А-запись, PTR-запись, Попытка авторизации должны иметь статус - ок). В случае неудачной попытки, ИКС выдаст рекомендации по их устранению. Также стоит отметить, что при подключении по протоколу kerberos имя ситемы будет изменено на *имя.домен*.

LDAP

Данные полей синхронизируется с формой импорта из [LDAP/AD](#). При заполнении настроек, обязательными полями являются: «Контроллер домена» - указывается IP-адрес, «Домен» - указывается имя домена, «Логин» и «Пароль» пользователя из домена (не обязательно администратора). При корректном заполнении всех необходимых полей и нажатии кнопки «Сохранить», служба синхронизации будет запущена, в ином случае настройки не будут сохранены.

В случае необходимости установки зашифрованного канала между LDAP-сервером и «ИКС» необходимо установить флаг «Secure LDAP» и выбрать сертификат из модуля [сертификатов](#) «ИКС». Стоит отметить, что данный сертификат должен быть установлен на LDAP-сервере. При создании сертификата на «ИКС» стоит выбрать в поле «Тип сертификата» - «Конечный сертификат», а в поле «Шаблон» - «Сервер».

ООО "Организация" > LDAP

Kerberos LDAP

У вас настроена синхронизация пользователей с LDAP-сервером. Для импорта пользователей с другого LDAP-сервера необходимо удалить синхронизированных пользователей

Контроллер домена *

Домен *

☐ Secure LDAP

Сертификат *

Логин *

Пароль *

From:

<https://doc-old.a-real.ru/> - Документация

Permanent link:

<https://doc-old.a-real.ru/doku.php?id=ics70:kerberos&rev=1592057810>

Last update: 2020/06/13 17:16

