РУКОВОДСТВО ПО УСТАНОВКЕ

CTI SSO

Версия: 1.0

СОДЕРЖАНИЕ

1

ВВЕДЕНИЕ

1. ВВЕДЕНИЕ

В данном документе описывается установка и настройка CTI SSO - специализированного программного обеспечения, разработанного на основе свободно распространяемой платформы Gluu Server 4.2.

1.1. Назначение

CTI SSO 1.0 разработан на основе Gluu Server 4.2 и предназначен для организации единой точки доступа в информационные системы организации (сквозная аутентификация и авторизации пользователей в едином информационном пространстве).
Позволяет реализовать следующие механизмы:

- единый вход пользователя в информационное пространство организации;
- мобильная аутентификация пользователей;
- управление доступом к API информационных систем;
- двухфакторная аутентификация пользователей;
- идентификация пользователей и управление доступом к информационным системам;
- удостоверение личности пользователя.

Взаимодействие пользователя осуществляется через веб-интерфейс.

1.2. Соглашения и условные обозначения

СОГЛАШЕНИЯ В ДОКУМЕНТЕ

Внимание!
Указывает на обязательное для исполнения или следования действие, или информацию.

Примечание
Указывает на необязательное, но желательное для исполнения или следования действие, или информацию.

УСЛОВНЫЕ ОБОЗНАЧЕНИЯ В ДОКУМЕНТЕ

- Названия элементов интерфейса (названия пунктов меню, кнопок и прочее) выделены **полужирным** шрифтом (например, **Начать работу**);
- Взаимоотношения между двумя фрагментами текста, при котором можно осуществлять быстрый переход от одного фрагмента к другому, помечен стилем гиперссылки (например, ссылка);
- Текстовая составляющая модальных окон помечена таким текстом;
- Элементы кода, переменные, программные составляющие выделены `таким шрифтом`.

2

Подготовительные операции

2. Подготовительные операции

Этот раздел содержит инструкции по подготовке виртуальной машины к развертыванию одноузлового сервера CTI SSO. Как только сервер будет готов, установите CTI SSO на одну из поддерживаемых операционных систем.

2.1. Требования к оборудованию

Минимальные требования:

Количество процессоров	Оперативная память	Объём диска	Тип процессора
2	4GB	40 GB	64бит

Дополнительно:

- При установке дополнительных компонентов (например, oxAuth, oxytrust и LDAP) рекомендуется использовать машину с объемом оперативной памяти не менее 8 ГБ.
- CTISSO должен быть развернут на сервере или виртуальной машине со статическим IP-адресом. Статический IP-адрес должен быть разрешён в имя хоста компьютера. Этого можно достигнуть путем добавления записи на DNS-сервер или в /etc/hosts.
- При локальной настройке виртуальной машины рекомендуется использовать VMPlayer (не VirtualBox!!).

2.2. Операционные системы

Развертывание CTI SSO возможно на сервере или виртуальной машине под одной из следующих поддерживаемых операционных систем:

- Докер
- Ubuntu 16, 18
- CentOS 7.x
- RHEL 7.x
- Debian 8, 9

2.3. Порты

Следующие порты по умолчанию открыты для доступа в интернет.

НОМЕР ПОРТА	ПРОТОКОЛ	ПРИМЕЧАНИЕ
80	tcp	Переадресуется на 443
443	tcp	apache2/httpd
22	tcp	ssh

ПРИМЕЧАНИЕ

Список внутренних портов, используемых серверными компонентами CTI SSO (например, oxAuth, oxytrust и т. д.), см. В руководстве по эксплуатации.

Чтобы проверить состояние этих портов в Ubuntu, используйте следующие команды (другие ОС имеют аналогичные команды):

```
ufw status verbose
```

По умолчанию ufw запрещает входящие и разрешает исходящие сообщения. Чтобы установить настройки по умолчанию:

```
ufw default deny incoming
ufw default allow outgoing
ufw reset
```

Если по какой-либо причине порты закрыты, разрешите подключение по:

```
ufw allow <порт>
```

Порты 443, 80 и 22 должны быть доступны.

2.4. Файл дескрипторов (ФД)

CTI SSO сервер требует настроить файл дескрипторов.
Выполните следующие действия или изучите, как это сделать на вашей платформе Linux.

- Добавьте следующие строки в файл /etc/security/limits.conf.

```
* soft nofile 65535
* hard nofile 262144
```

- Добавьте следующую строку в файл /etc/pam.d/login, если её в нём нет.

```
session required pam_limits.so
```

- Увеличьте размер FD до 65535. Ограничение указывается в /proc/sys/fs/file-max.

Рекомендуется проверить размер FD, прежде чем увеличивать его. Если этот размер настроен и превышает значение по умолчанию, мы рекомендуем использовать более высокий. Размер FD можно найти с помощью следующей команды.

```
# cat /proc/sys/fs/file-max
```

Обратите внимание, что команда может варьироваться в зависимости от используемой операционной системы.

```
echo 65535 > /proc/sys/fs/file-max**
```

Используйте команду ulimit, чтобы установить предел FD на жесткий предел, указанный в файле /etc/security/limits.conf.

```
ulimit -n 65535
```

Примечание

ПРИМЕЧАНИЕ
CentOS по умолчанию не будет принимать больше максимального значения по умолчанию-65535. При выполнении приведенной выше команды может возникнуть ошибка.

- Перезагрузите систему

2.5. IP-адрес

Сервер или виртуальная машина должны быть развернуты на статическом IP - адресе. Облачные серверы уже должны иметь этот набор. При установке сервера CTI SSO убедитесь, что сервер имеет статический IP-адрес.

2.5.1. CentOS

Создайте файл с именем `/etc/sysconfig/network-scripts/ifcfg-eth0`, содержащий следующую информацию:

```
DEVICE=eth0

BOOTPROTO=none

ONBOOT=yes

PREFIX=24

IPADDR=192.168.2.203 <replace with your IP>
```

Перезагрузите сетевую службу:

system ctl restart network

2.5.2. Другие операционные системы

Откройте файл vi /etc/network/interfaces с помощью любого редактора
Ниже приведена конфигурация сети. Обратите внимание, что iface ens33 inet указан как dhcp.

```
#This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).
source /etc/network/interfaces.d/*
# The loopback network interface
auto lo
iface lo inet loopback
# The primary network interface
auto ens33
iface ens33 inet dhcp
```

Закомментируйте строку, содержащую dhcp, добавив # перед ней и добавьте значения для адреса, маски сети, сети, широковещательной передачи, шлюза и dns-серверов имен сети, как показано в примере ниже:

```
#This file describes the network interfaces available on your system
#and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens33
#iface ens33 inet dhcp
iface ens33 inet static
    # This value is an example
    address 192.168.1.10
    # This value is an example
    netmask 255.255.255.0
    # This value is an example
    network 192.168.1.0 #
    # This value is an example
    broadcast 192.168.1.255
    # This value is an example
    gateway 192.168.1.1
# This value is an example
dns-nameservers 8.8.8.8 8.8.4.4 # This value is an example
```

Перезагрузите сетевую службу:

```
service networking restart
```

или перезапустите сервер.

```
/etc/init.d/networking restart
```

2.6. Полное доменное имя (FQDN)

CTI SSO должен быть развернут на полном доменном имени (FQDN), например https://my-ctisso.server.com. Localhost не поддерживается.
В Linux отредактируйте файлы hosts и добавьте в них соответствующий IP-адрес и полное доменное имя. Например:
vi /etc/hosts
Если IP-адрес был 192.168.1.1, а полное доменное имя было test.ctisso.org добавьте все файлы hosts: 192.168.1.1 test.ctisso.org
Файлы Windows hosts находится по адресу C:\Windows\System32\drivers\etc\hosts

3

Установка

3. Установка

3.1. Docker

Этот раздел содержит инструкции по развертыванию CTI SSO на одном узле виртуальной машины с помощью Docker.
Требуется:
Скачать исполняемый файл pyctisso-compose.pyz:

```
wget  https://github.com/ctissoFederation/community-edition-containers/releases/download/v1.2.5/pyCTISSO-compose.pyz \
   && chmod +x pyctisso-compose.pyz
```

ПРИМЕЧАНИЕ

pyctisso-compose.pyz требует Python 3.6+ (и пакет python3-distutils, если используется Ubuntu/Debian).

Выполните следующую команду, чтобы создать манифесты для развертывания:

```
./pyctisso-compose.pyz init./pyctisso-compose.pyz init
```

Будут сгенерированы файлы аналогичны приведенному ниже примеру

```
tree
.
├── couchbase.crt
├── couchbase_password
├── docker-compose.yml
├── gcp_kms_creds.json
├── gcp_kms_stanza.hcl
├── jackrabbit_admin_password
├── job.persistence.yml
├── svc.casa.yml
├── svc.cr_rotate.yml
├── svc.fido2.yml
├── svc.jackrabbit.yml
├── svc.ldap.yml
├── svc.oxauth.yml
├── svc.oxd_server.yml
├── svc.oxpassport.yml
├── svc.oxshibboleth.yml
├── svc.oxtrust.yml
├── svc.radius.yml
├── svc.redis.yml
├── svc.scim.yml
├── svc.vault_autounseal.yml
├── vault_ctisso_policy.hcl
├── vault_role_id.txt
└── vault_secret_id.txt
```

3.2. Ubuntu

Пакеты для установки на Linux-сервер доступны для Ubuntu 20.x, 18.04.x. Следуйте инструкциям ниже.

3.2.1. Предусловие

1. Выполнены все условия, описанные в разделе «Подготовительные операции»
2. Для Ubuntu 18 или 20: репозиторий Universe должен быть доступен.

3.2.2. Установка пакетов

CTI SSO создаст свою файловую систему под /root/ и будет установлен под /opt. Размер файла и минимальные требования остаются такими же, как и у хоста.
1. Для Ubuntu 20.x выполните следующие команды:

```
echo "deb https://repo.ctisso.org/ubuntu/ focal main" > /etc/apt/sources.list.d/ctisso-repo.list
curl https://repo.ctisso.org/ubuntu/ctisso-apt.key | apt-key add -
apt update
apt install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
apt-mark hold ctisso-server
```

2. Для Ubuntu 18.04.x выполните следующие команды:

```
echo "deb https://repo.ctisso.org/ubuntu/ bionic main" > /etc/apt/sources.list.d/ctisso-repo.list
curl https://repo.ctisso.org/ubuntu/ctisso-apt.key | apt-key add -
apt update
apt install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
apt-mark hold ctisso-server
```

3.2.3. Запуск сервера и вход в систему

CTI SSO представляет собой chroot контейнер, который должен быть запущен.

Для Ubuntu 20.x (18.04.x) выполните следующие команды:

```
/sbin/ctisso-serverd enable
/sbin/ctisso-serverd start
/sbin/ctisso-serverd login
```

3.2.4. Запуск скрипта установки

Настройка завершается запуском сценария установки из контейнера chroot. Это создает сертификаты и отображает файлы конфигурации. Запустите сценарий с помощью следующих команд:

```
cd /install/community-edition-setup
./setup.py
```

3.2.5. Вход в систему через браузер

Подождите в общей сложности около 10 минут, пока сервер перезагрузится и завершит свою конфигурацию. По истечении этого срока войдите в систему через веб-браузер. Имя пользователя будет admin, а ваш пароль-ldap_password, предоставленный вами во время установки.

ПРИМЕЧАНИЕ

Если страница входа в систему не отображается, убедитесь, что порт 443 открыт в виртуальной машине. Если он не открыт, откройте порт 443 и снова попытайтесь связаться с хостом в браузере.

3.2.6. Отключение репозитория

Чтобы предотвратить непроизвольную перезапись текущего развернутого экземпляра (в случае обнаружения более новой версии того же пакета во время регулярных обновлений ОС), отключите ранее добавленные репозитории CTI SSO после первоначальной установки.

3.3. Debian

Пакеты для установки на Linux-сервер доступны для Debian 9 и 10. Следуйте инструкциям ниже.

3.3.1. Предусловие

1. Выполнены все условия, описанные в разделе «Подготовительные операции»
2. Перед добавлением ctisso-repo.list убедитесь, что пакет Debian apt-transport-https уже установлен. В противном случае установка может быть затруднена.

3.3.2. Установка пакетов

CTI SSO создаст свою файловую систему под /root/ и будет установлен под /opt. Размер файла и минимальные требования остаются такими же, как и у хоста.
1. Для Debian 10 (Buster) выполните следующие команды:

```
echo "deb https://repo.ctisso.org/debian/ buster-stable main" > /etc/apt/sources.list.d/ctisso-repo.list
# curl https://repo.ctisso.org/debian/ctisso-apt.key | apt-key add -
apt update
apt install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
apt-mark hold ctisso-server
```

2. Для Debian 9 (Stretch) выполните следующие команды:

```
echo "deb https://repo.ctisso.org/debian/ stretch-stable main" > /etc/apt/sources.list.d/ctisso-repo.list
# curl https://repo.ctisso.org/debian/ctisso-apt.key | apt-key add -
apt update
apt install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
apt-mark hold ctisso-server
```

3.3.3. Запуск сервера и вход в систему

CTI SSO представляет собой chroot контейнер, который должен быть запущен.

Выполните следующие команды:

```
/sbin/ctisso-serverd enable
/sbin/ctisso-serverd start
/sbin/ctisso-serverd login
```

3.3.4. Запуск скрипта установки

Настройка завершается запуском сценария установки из контейнера chroot. Это создает сертификаты и отображает файлы конфигурации. Запустите сценарий с помощью следующих команд:

```
cd /install/community-edition-setup
```

./setup.py

3.3.5. Вход в систему через браузер

Подождите в общей сложности около 10 минут, пока сервер перезагрузится и завершит свою конфигурацию. По истечении этого срока войдите в систему через веб-браузер. Имя пользователя будет admin, а ваш пароль-ldap_password, предоставленный вами во время установки.

ПРИМЕЧАНИЕ

Если страница входа в систему не отображается, убедитесь, что порт 443 открыт в виртуальной машине. Если он не открыт, откройте порт 443 и снова попытайтесь связаться с хостом в браузере.

3.3.6. Отключение репозитория

Чтобы предотвратить непроизвольную перезапись текущего развернутого экземпляра (в случае обнаружения более новой версии того же пакета во время регулярных обновлений ОС), отключите ранее добавленные репозитории CTI SSO после первоначальной установки.

3.4. RHEL

Пакеты для установки на Linux-сервер доступны для RHEL 7 и 8. Следуйте инструкциям ниже.

3.4.1. Предусловие

1. Выполнены все условия, описанные в разделе «Подготовительные операции»
2. Для SELinux должны быть даны права на /etc/selinux/config.

3.4.2. Установка пакетов

CTI SSO создаст свою файловую систему под /root/ и будет установлен под /opt. Размер файла и минимальные требования остаются такими же, как и у хоста.
1. Для RHEL 8 выполните следующие команды:

```
get https://repo.ctisso.org/rhel/ctisso-rhel8.repo -O /etc/yum.repos.d/ctisso.repo
wget https://repo.ctisso.org/rhel/RPM-GPG-KEY-ctisso -O /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
yum clean all
yum install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
yum versionlock ctisso-server
```

2. Для RHEL 7 выполните следующие команды:

```
wget https://repo.ctisso.org/rhel/ctisso-rhel7.repo -O /etc/yum.repos.d/ctisso.repo
wget https://repo.ctisso.org/rhel/RPM-GPG-KEY-ctisso -O /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
yum clean all
yum install ctisso-server
```

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

```
yum versionlock ctisso-server
```

3.4.3. Запуск сервера и вход в систему

CTI SSO представляет собой chroot контейнер, который должен быть запущен.
Выполните следующие команды:

/sbin/ctisso-serverd enable
/sbin/ctisso-serverd start
/sbin/ctisso-serverd login

3.4.4. Запуск скрипта установки

Настройка завершается запуском сценария установки из контейнера chroot. Это создает сертификаты и отображает файлы конфигурации. Запустите сценарий с помощью следующих команд:
cd /install/community-edition-setup
./setup.py

3.4.5. Вход в систему через браузер

Подождите в общей сложности около 10 минут, пока сервер перезагрузится и завершит свою конфигурацию. По истечении этого срока войдите в систему через веб-браузер. Имя пользователя будет admin, а ваш пароль-ldap_password, предоставленный вами во время установки.

ПРИМЕЧАНИЕ
Если страница входа в систему не отображается, убедитесь, что порт 443 открыт в виртуальной машине. Если он не открыт, откройте порт 443 и снова попытайтесь связаться с хостом в браузере.

3.4.6. Отключение репозитория

Чтобы предотвратить непроизвольную перезапись текущего развернутого экземпляра (в случае обнаружения более новой версии того же пакета во время регулярных обновлений ОС), отключите ранее добавленные репозитории CTI SSO после первоначальной установки.

3.5. CentOS

Пакеты для установки на Linux-сервер доступны для CentOS 8 и 7. Следуйте инструкциям ниже.

3.5.1. Предусловие

1. Выполнены все условия, описанные в разделе «Подготовительные операции»
2. Для SELinux должны быть даны права на /etc/selinux/config.

3.5.2. Установка пакетов

CTI SSO создаст свою файловую систему под /root/ и будет установлен под /opt. Размер файла и минимальные требования остаются такими же, как и у хоста.
1. Для CentOS 8 выполните следующие команды:
echo "deb https://repo.ctisso.org/debian/ buster-stable main" > /etc/apt/sources.list.d/ctisso-repo.list
curl https://repo.ctisso.org/debian/ctisso-apt.key | apt-key add -
apt update
apt install ctisso-server

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:
yum versionlock ctisso-server
2. Для CentOS 7 выполните следующие команды:
wget https://repo.ctisso.org/centos/ctisso-centos7.repo -O /etc/yum.repos.d/ctisso.repo
wget https://repo.ctisso.org/centos/RPM-GPG-KEY-ctisso -O /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
rpm --import /etc/pki/rpm-gpg/RPM-GPG-KEY-ctisso
yum clean all

yum install ctisso-server

После установки пакет необходимо исключить из автоматического обновления с помощью следующей команды:

yum versionlock ctisso-server

3.5.3. Запуск сервера и вход в систему

CTI SSO представляет собой chroot контейнер, который должен быть запущен.
Выполните следующие команды:

/sbin/ctisso-serverd enable
/sbin/ctisso-serverd start
/sbin/ctisso-serverd login

3.5.4. Запуск скрипта установки

Настройка завершается запуском сценария установки из контейнера chroot. Это создает сертификаты и отображает файлы конфигурации. Запустите сценарий с помощью следующих команд:

cd /install/community-edition-setup
./setup.py

3.5.5. Вход в систему через браузер

Подождите в общей сложности около 10 минут, пока сервер перезагрузится и завершит свою конфигурацию. По истечении этого срока войдите в систему через веб-браузер. Имя пользователя будет admin, а ваш пароль-ldap_password, предоставленный вами во время установки.

ПРИМЕЧАНИЕ

Если страница входа в систему не отображается, убедитесь, что порт 443 открыт в виртуальной машине. Если он не открыт, откройте порт 443 и снова попытайтесь связаться с хостом в браузере.

3.5.6. Отключение репозитория

Чтобы предотвратить непроизвольную перезапись текущего развернутого экземпляра (в случае обнаружения более новой версии того же пакета во время регулярных обновлений ОС), отключите ранее добавленные репозитории CTI SSO после первоначальной установки.

3.6. Настройка решения

3.6.1. Настройка с использованием TUI

После установки запуск setup.py по умолчанию запустит Setup TUI. TUI шаг за шагом проведет процесс настройки.

1. Появится предупреждение, если свободное место на диске меньше рекомендованных 40 ГБ.

2. TUI определит, какая операционная система, тип инициализации и версия Apache, которая установлена в настоящее время на сервере.

3. На третьем экране будет собрана основная информация для создания сертификатов.

4. Затем выберите, какие службы следует установить для этого развертывания.

5. Затем выберите механизм сохранения. Выберите WrenDS, LDAP, который можно установить локально или удаленно, или Couchbase, облачную NoSQL базу данных предприятия.

6. Просмотрите сводный экран, на котором представлен обзор выбранных в процессе настройки параметров.

3.6.2. Настройка с использованием командной строки

Если TUI недоступен в вашей среде, он переключается на командную строку. Если вы хотите использовать командную строку, выполните с аргументом -c:

```
/install/setup.py -c
```

Сценарий установки вызовет приглашение предоставить информацию для сертификата, а также IP-адрес и имя хоста для сервера CTI SSO. Нажмите Enter, чтобы принять значения по умолчанию.

Подробная информация о доступных параметрах настройки указана в следующей таблице:

Вариант настройки	Описание
Ввести IP-адрес	Используется главным образом Apache httpd для директивы Listen. Используйте IP-адрес, назначенный одному из сетевых интерфейсов этого сервера (использование адресов, назначенных интерфейсам обратной связи, не поддерживается)
Ввести имя хоста	Полное доменное имя с выходом в Интернет, которое используется для создания сертификатов и метаданных. Не используйте IP-адрес или localhost.

Ввести свой город или местность	Используется для создания сертификатов X.509.
Ввести двухбуквенный код штата или провинции	Используется для создания сертификатов X.509.
Ввести двухбуквенный код страны	Используется для создания сертификатов X.509.
Ввести название организации	Используется для создания сертификатов X.509.
Ввести адрес электронной почты технической поддержки в вашей организации	Используется для создания сертификатов X.509.
Необязательно: ввести пароль для oxTrust и суперпользователя LDAP	спользуется в качестве пароля диспетчера каталогов LDAP и для пользователя-администратора по умолчанию для oxTrust
Установить сервер авторизации oxAuth OAuth2	Обязательно. Включает в себя реализации провайдера OpenID Connect (OP) и сервера авторизации UMA (AS)
Установить интерфейса администратора oxTrust	Это панель администратора сервера CTI SSO
Требуется установка внутреннего сервера БД	Устанавливает OpenDJ, используемый для хранения информации о пользователе и данных конфигурации
Установить веб-сервер Apache 2	Обязательно
Установить Shibboleth SAML IDP	Необязательно. Устанавливайте только в том случае, если требуется поставщик удостоверений SAML (IDP)
Установить oxAuth RP	Необязательно. Тестовый клиент OpenID Connect: полезно для тестовых сред
Установить паспорт	Необязательно. Установите, если вы хотите поддерживать внешний IDP, например, чтобы предлагать пользователям вход через социальные сети
Установить Gluu Radius	Устанавливает Radius-сервер

По завершении сценарий установки покажет выбранные варианты и запросит подтверждение. Если все в порядке, выберите Y, чтобы завершить установку.

Через 5-10 минут появится следующее сообщение об успешном выполнении:

«Установка сервера прошла успешно! В браузере укажите [имя хоста].»
Войдите в систему, используя имя пользователя admin и пароль из приглашения сценария установки, например hIE3vzf0hMdD, или введенный в процессе установки пароль.
Чтобы избежать проблем с настройкой, обратите внимание на следующее:

IP-адрес: не используйте localhost ни в качестве IP-адреса, ни в качестве имени хоста.

Имя хоста:
Обязательно внимательно выбирайте имя хоста. Изменить имя хоста после установки - непростая задача.
Используйте настоящее имя хоста - этим всегда можно управлять с помощью записей файла хоста, если добавление записи DNS слишком сложно для тестирования.
Для кластерных развертываний используйте имя хоста кластера, который будет использоваться приложениями, подключающимися к CTI SSO.

ВНИМАНИЕ!
Используйте полное доменное имя (полное доменное имя) в качестве имени хоста и воздержитесь от использования 127.0.0.1 в качестве IP-адреса или использования частного IP-адреса не поддерживается и не рекомендуется.

Запустите сценарий установки только один раз. Выполнение команды дважды приведет к поломке экземпляра.

Если разрешаемый DNS-хост не используется, его необходимо добавить к имени хоста файла hosts операционной системы на сервере, на котором запущен браузер.

ВНИМАНИЕ!

Удалите или зашифруйте файл `setup.properties.last`, поскольку он содержит пароли в открытом виде для LDAP, пользователя admin, хранилищ ключей и соли 3DES

Ошибки можно найти в файле setup_errors.log, а подробные пошаговые инструкции по установке можно найти в файле setup.log в папке / install .

Сценарий установки может использоваться для настройки сервера CTI SSO и добавления начальных данных для запуска oxAuth и oxTrust. Если в этой папке находится файл setup.properties, эти свойства будут автоматически использоваться вместо интерактивной настройки.

ПАРАМЕТРЫ КОМАНДНОЙ СТРОКИ СЦЕНАРИЯ

Администратор может использовать следующие параметры командной строки для включения дополнительных компонентов:

-c - переход в командную строку;
-r - установить oxAuth RP;
-p - установить паспорт;
-d - указать каталог, в котором находится установка, по умолчанию - '.';
-f - указать файл setup.properties;
-h - вызвать эту подсказку;
-n - отключение интерактивного запроса перед началом установки. Запустить с -f;
-N - отключение httpd-сервера Apache;
-s - установить Shibboleth IDP;
-u - обновить файл hosts с IP-адресом / именем хоста;
-w - получить заголовочные war-файлы;
-t - данные нагрузочного теста;
-x - загрузить тестовые данные и выйти;
-stm - включить режим тестирования Scim;
-properties-password - указать пароль для декодирования setup.properties.last.enc;
–import-ldif = custom-ldif-dir - отображать шаблоны ldif из custom-ldif-dir и импортировать их в LDAP;
–listen_all_interfaces - разрешить серверу LDAP прослушивать все серверные интерфейсы. Это необходимо для кластерных установок для репликации между серверами LDAP. Если не включено, сервер LDAP слушает только localhost;
— allow-pre-Release-features - включить параметры для установки экспериментальных функций, которые еще официально не поддерживаются;
–remote-ldap - разрешать использовать удаленный сервер LDAP;
–install-local-opendj - установить локальный LDAP-сервер OpenDJ;
–remote-couchbase - разрешить использовать удаленный сервер Couchbase;
–no-data - не импортировать данные в базу данных, используемую для кластеризации;
–no-oxauth - не устанавливать сервер авторизации oxAuth OAuth2;
–no-oxtrust - не устанавливать интерфейс администратора oxTrust;
–install-gluu-radius - установить интерфейс администратора oxTrust;
-ip-address - используется главным образом Apache httpd для директивы Listen;
-host-name - полное доменное имя с выходом в Интернет, которое используется для создания сертификатов и метаданных;
-org-name - поле названия организации, используемое для генерации сертификатов X.509;
-email - адрес электронной почты для поддержки в вашей организации, используемый для создания сертификатов X.509;
-city - поле города, используемое для генерации сертификатов X.509;
-state - поле штата, используемое для генерации сертификатов X.509;
-country - двухбуквенный код страны, используемые для создания сертификатов X.509;

-oxtrust-admin-password - пароль, используемый для администратора, создаваемого по умолчанию в oxTrust;
-ldap-admin-password **- пароль диспетчера каталога LDAP.**
-application-max-ram - устанавливает максимальное значение RAM, которое будет использоваться приложением;
-properties-password - закодированный пароль к файлу setup.properties;
–install-casa - установить Casa;
–install-oxd - установить сервер Oxd;
–install-scim - установить Scim Server;
–install-fido2 - установить Fido2;
-couchbase-bucket-prefix - установить префикс для ковшей на диване;
–generate-oxd-certificate - сгенерировать сертификат для oxd на основе имени хоста;
–load-passwords - загрузить пароль из setup.properties.

Пример команды:

```
# ./setup.py -ps
```

Эта команда установит CTI SSO с Passport и Shibboleth IDP.

Примечание

ПРИМЕЧАНИЕ

setup.py сохранит зашифрованный файл свойств с именем setup.properties.last.enc. Пароль для доступа такой же, как и пароль администратора oxTrust. Сохраните этот пароль, чтобы использовать этот файл для будущих установок. Чтобы повторно использовать файл, его необходимо расшифровать с помощью следующей команды:

```
openssl enc -d -aes-256-cbc -in setup.properties.last.enc -out setup.properties.last
```

При появлении запроса введите пароль администратора oxTrust.

117218, г. Москва, ул. Кржижановского, д. 29, корпус 1 (5-й этаж)
Телефон:
+7.495.784.73.13
+7.495. 784.73.11 - техническая поддержка
8.800.550.43.57 - многоканальный телефон
E-mail: support@cti.ru
Web: www.cti.ru