Руководство по установке и настройке

Листов 16

2024

Содержание

Перечень сокращений

АРМ	–	автоматизированное рабочее место
ИБ	–	информационная безопасность
ИС	–	информационная система
ОС	–	операционная система
ПО	–	программное обеспечение
СКЗИ	–	средство криптографической защиты информации
УЦ	–	удостоверяющий центр

Перечень терминов

Авторизация	–	предоставление субъекту доступа прав доступа, а также предоставление доступа в соответствии с установленными правилами управления доступом
Блокирование	–	действие, в результате которого прекращается предоставление доступа заблокированному субъекту
Браузер	–	программа для поиска и просмотра информации из вычислительной сети
Виртуальная машина	–	программная среда, которая внутри одной программной и (или) аппаратной системы эмулирует работу другой программной и/или аппаратной системы.
Временное блокирование	–	действие, в результате которого прекращается предоставление доступа заблокированному субъекту на определённый промежуток времени (перевод в разблокированное состояние проводится автоматически)
Двухфакторная аутентификация	–	аутентификация, при выполнении которой используется два различных фактора аутентификации
Доступ	–	получение одной стороной информационного взаимодействия возможности использования ресурсов другой стороны информационного взаимодействия
Идентификация	–	действия по присвоению субъектам и объектам доступа идентификаторов и/или по сравнению предъявляемого идентификатора с перечнем присвоенных идентификаторов
Интегрированная ИС	–	ИС, авторизация в которой проводится с помощью учётной записи X-IDBox
Информационная система	–	совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
Парольная политика	–	минимальные требования к характеристикам паролей
Пользователь	–	физическое лицо, первичная идентификация которого выполнена в конкретной среде функционирования
Правила разграничения доступа	–	правила, регламентирующие условия доступа субъектов доступа к объектам доступа в автоматизированной информационной системе

Профиль учётной записи	–	совокупность данных о пользователе и назначенные ему роли в организации, для доступа к ИС которой используется учётная запись
Разблокирование	–	восстановление предоставленного доступа субъекту
Ресурс	–	объект системы, к которому может быть предоставлен доступ
Ролевая политика	–	совокупность профилей учётных записей и назначенных им ролей
Роль	–	предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой
Список разрешенных УЦ	–	перечень УЦ, сертификаты, выданные которыми, могут быть использованы в X-IDBox
Удостоверяющий центр	–	юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом от 06.04.2011 № 63-ФЗ
Управление доступом	–	ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа
Учётная запись	–	совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа к его личным данным и настройкам в X-IDBox и интегрированных ИС
Электронная подпись	–	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

1. Общие сведения

1.1. Назначение и функции X-IDBox

X-IDBox представляет собой систему идентификации, аутентификации и разграничения доступа, имеющую встроенный механизм управления доступом.

X-IDBox обеспечивает процедуру единого входа во все ИС, интегрированные с X-IDBox, что позволяет выполнять переход между ИС без повторной аутентификации. Для каждой ИС возможна настройка способов аутентификации.

X-IDBox предоставляет следующие функциональные возможности:

1) Управление учётными записями пользователей (для всех ИС, интегрированных с X-IDBox, поддерживается единый каталог пользователей):

– регистрация пользователей, включая самостоятельную регистрацию пользователей;

– загрузка списка пользователей из файла;

– загрузка изменения ролей пользователей из файла;

– редактирование личных данных пользователей;

– блокирование (в том числе и временное) и разблокирование учётных записей пользователей;

– уведомление пользователей об операциях по управлению доступом.

2) Управление профилями учётных записей пользователей:

– добавление профилей к учётной записи пользователей;

– загрузка профилей из файла;

– редактирование сведений о профилях;

– управление доступом к интегрированным ИС путем назначения и (или) снятия ролей;

– управление доступом к X-IDBox путем назначения и (или) снятия ролей;

– блокирование (в том числе и временное) и разблокирование профилей.

3) Управление ролями:

– изменение параметров ролей;

– загрузка ролей доступа из файла;

– экспорт перечня ролей;

4) Обеспечение юридической значимости операций в системе путем подписания заявок, формируемых для каждого выполняемого действия в системе.

5) Просмотр списка организаций.

6) Управление списком разрешённых УЦ: добавление и удаление УЦ из списка.

7) Управление парольными политиками.

8) Управление параметрами блокирования учётных записей пользователей.

9) Управление параметрами двухфакторной аутентификации.

10) Управление шаблонами уведомлений: создание, изменение и удаление шаблонов.

1.2. Функциональные роли

В X-IDBox в соответствии с имеющимися зонами ответственности предусмотрены следующие функциональные роли:

– Пользователь;

– Системный администратор;

– Администратор ИБ;

– Менеджер информационной системы;

– Менеджер учётных записей.

Каждая учётная запись наделена определёнными правами в соответствии со своей ролью, подробный перечень прав приведен в Руководстве пользователя.

Одной учётной записи может быть назначено несколько ролей в X-IDBox (обязательно включая роль Пользователя). При этом Менеджер информационной системы может (должен) управлять только одной ИС. Все операции, доступные Менеджеру информационной системы, связаны именно с управляемой ИС.

Роль Пользователя присваивается автоматически при регистрации учётной записи и не подлежит отзыву, а также изменению срока действия. Операции, доступные Пользователю, выполняются им только по отношению к своей собственной учётной записи.

Назначать и отзывать роли в X-IDBox, а также изменять сроки их действия может только Системный администратор. Также Системный администратор может выполнять регистрацию пользователей, блокирование и разблокирование учётных записей, управление профилями, шаблонами уведомлений.

Управление ролями в ИС, интегрированных с X-IDBox, доступно Менеджеру учётных записей. Также ему доступно управление учётными записями и профилями учётных записей.

Администратору ИБ доступно блокирование и разблокирована учётных записей пользователей и профилей учётных записей, управление списком разрешённых УЦ и настройками безопасности.

2. Условия применения

2.1. Требования к серверной части

Для корректного функционирования сервисов X-IDBox необходим сервер или виртуальная машина под управлением операционной системы ОС Linux, входящие в реестр отечественного ПО с характеристиками не хуже:

– CPU – Core 4;

– RAM – 16 ГБ;

– HDD – 200 ГБ.

2.2. Требования к АРМ пользователя

Для корректной работы X-IDBox на АРМ пользователя необходима установка и настройка СКЗИ и веб-браузера.

X-IDBox поддерживает совместимость со следующими браузерами:

1) Браузеры на основе ядра Chromium 96.0.4664.110 или выше, в частности:

– Google Chrome версии 97.0.4692.71 или выше;

– Яндекс.Браузер версии 21.11.4.727 или выше.

Для работы X-IDBox необходимо СКЗИ «КриптоПро CSP» версии 4.0 или выше, а вместе с ним – «КриптоПро ЭЦП Browser plug-in» версии 2.0.

Подробное описание подготовки АРМ пользователя к работе с X-IDBox приведено в Руководстве пользователя.

3. Установка системы

3.1. Подготовка к установке

Перед началом установки X-IDBox:

1) Выполните установку ОС Linux на сервер (виртуальную машину) согласно официальной документации. Рекомендуется использовать вариант установки «minimal».

2) Настройте сетевые интерфейсы в соответствии с требованиями вашей инфраструктуры и установите обновления.

3) Установите Docker CE в соответствии с официальной документацией (https://docs.docker.com/engine/install/) для выбранного вами дистрибутива Linux.

4) Установите docker-compose в соответствии с официальной документацией (https://docs.docker.com/compose/install/) для выбранного вами дистрибутива Linux.

5) Проверьте работу docker выполнив команду:

```
docker run hello-world
```

3.2. Установка X-IDBox

Для установки X-IDBox:

1) Скопируйте дистрибутив X-IDBox в локальную папку на сервере (виртуальной машине).

2) Разрешите выполнение bash-скриптов дистрибутива, в папке с дистрибутивом выполнив команду:

```
chmod +x *.sh
```

3) Установите стороннее ПО, необходимое для работы системы (PostgreSQL, Redis), выполнив скрипт:

```
./run-external-services.sh.
```

4) Проверьте, что контейнеры с указанными сервисами успешно развернулись и запустились, выполнив команду:

```
docker ps
```

5) Установите X-IDBox, выполнив скрипт:

```
./run-x-idbox-services.sh
```

6) Проверьте, что контейнеры с сервисами системы развернулись и запустились, выполнив команду:

```
docker ps
```

7) В скрипте «politics-x_idbox.sql» в папке «sql» укажите имя сервера (<your_server_address>), на котором будет размещаться X-IDBox.

8) Выполните скрипты из папки «sql» на базе данных «x-idbox-postgres».

9) Если на сервере включен межсетевой экран (firewall), разрешите входящие соединения по портам 80, 443/TCP.

В результате установки веб-интерфейс системы будет доступен по адресу сервера (http://<your_server_address>/signin).

Адрес электронной почты и пароль стартового пользователя указаны в файле «usr-x_idbox.sql».

3.3. Добавление ИС X-IDBox при первом запуске

Добавление ИС X-IDBox при первом запуске:

1) Создайте ИС в БД одним из способов:

– выполните запрос на создание ИС в database-service вида:

```
POST
http://<your_server_address>:8080/database/api/v1/information/system

Content-Type: application/json
{
    "techName": "xidbox",
    "name": "ИС XIDBox",
    "shortName": "XIDBox",
    "availableAuthenticationTypes": [
        {
            "type": "LOGIN",
            "factor": "FIRST",
            "host": "authz_<your_server_address>"
        }
```

```
    ]
}
```

– выполните запросы непосредственно в БД. Добавьте данные об ИС:

```
insert
into x_id_box.information_system(tech_name, name,
short_name)
values ('xidbox', 'ИС XIDBox', 'XIDBox');
```

далее выполните запрос по добавлению разрешенных способов входа:

```
insert
into x_id_box.information_system_setting(info_syste
m_id, available_authentication_type, factor, host)
values (<идентификатор ИС>, 'LOGIN', 'FIRST',
'authz_<your_server_address>')
```

где `info_system_id` – идентификатор нужной ИС X-IDBox,

`host` – хост ИС X-IDBox,

`available_authentication_type` – способ аутентификации,

`factor` – фактор.

> Возможные сочетания `available_authentication_type` и `factor` (LOGIN | CERT) & FIRST или CODE_FROM_EMAIL & SECOND,
>
> где LOGIN – необходим вход по логину/адресу электронной почты, CERT – необходим вход по сертификату,
>
> CODE_FROM_EMAIL – необходимо ввести код из сообщения почты,
>
> FIRST – первый фактор,
>
> SECOND – второй фактор.

2) Загрузите ролевую политику:

– выполните запрос:

```
POST
http://<your_server_address>:8093/backend/api/v1/ro
le/politics/parse
Content-Type: application/json

{
  "content": "*текст ролевой политики без блока
APPROVAL RULE BLOCK*"
```

```
}
```

– полученный ответ передайте в API, выполнив команду:

```
POST http://<your_server_address>:8093/backend/api/v1/role/politics
Content-Type: application/json
```

3) Загрузите организацию, выполнив запрос:

```
POST http://localhost:8095/organization/api/v1/organizations
```

В запросе можно передавать от 1 до n организаций.

4) Добавьте пользователя:

– Выполните запрос:

```
INSERT INTO x_id_box.usr (first_name, last_name, login, email, count_error_auth_attempt, state, is_blocked, reg_date)
VALUES ('{Имя пользователя}', '{Фамилия пользователя}', '{логин}', '{рабочая почта}', 0, 'ACTIVE', false, now());
```

– Через веб-интерфейс (http://<your_server_address>/signin) выполните сброс пароля.

– Перейдите по ссылке из письма, полученного на электронную почту, указанную в файле «usr-x_idbox.sql».

– Выполните sql-запрос на добавление профиля пользователя вида:

```
INSERT INTO x_id_box.user_profile (user_id, organization_id, is_blocked, state, work_email, work_email_verified, registration_date)
VALUES ({id_пользователя}, {id_организации}, false, 'ACTIVE', 'email@infosec.ru', now(), now());
```

– Назначьте для созданного профиля роли «Пользователь» и «Системный администратор» запросами вида:

```
INSERT INTO x_id_box.user_profile_role (user_profile_id, role_id, actual_start_date)
VALUES ({id_профиля}, {id_роли}, now());
```

– Войдите в систему через веб-интерфейс (http://<your_server_address>/signin).

– Подтвердите согласие на обработку персональных данных.

– Зарегистрируйте нужных пользователей и назначьте им советующие профили и роли.

4. Подключение информационной системы

Для подключения ИС:

1) Создайте ИС в БД одним из способов:

– выполните запрос на создание ИС в database-service вида:

```
POST
http://<your_server_address>:8080/database/api/v1/information/system

Content-Type: application/json
{
    "techName": "xidbox",
    "name": "ИС XIDBox",
    "shortName": "XIDBox",
    "availableAuthenticationTypes": [
        {
            "type": "LOGIN",
            "factor": "FIRST",
            "host": "authz_<your_server_address>"
        }
    ]
}
```

– выполните запросы непосредственно в БД. Добавьте данные об ИС:

```
insert
into x_id_box.information_system(tech_name, name, short_name)
values ('xidbox', 'ИС XIDBox', 'XIDBox');
```

далее выполните запрос по добавлению разрешенных способов входа:

```
insert
into x_id_box.information_system_setting(info_system_id, available_authentication_type, factor, host)
values (1052, 'LOGIN', 'FIRST',
'authz_<your_server_address>')
```

где `info_system_id` – идентификатор нужной ИС,

`host` – хост ИС,

`available_authentication_type` – способ аутентификации,

`factor` – фактор.

Возможные
сочетания `available_authentication_type` и `factor` (LOGIN | CERT) & FIRST или CODE_FROM_EMAIL & SECOND,

где LOGIN – необходим вход по логину/адресу электронной почты, CERT – необходим вход по сертификату,

CODE_FROM_EMAIL – необходимо ввести код из сообщения почты,

FIRST – первый фактор,

SECOND – второй фактор.

2) Сформируйте ролевую политику подключаемой ИС.

3) Выполните создание пользователя.

4) Зайдите под учётной записью с ролью «Менеджер учётных записей», зарегистрируйте пользователя или используйте существующего и назначьте ему роль «Менеджер информационной системы», указав подключаемую ИС как управляемую.

5) Зайдите под учётной записью, которой была назначена роль «Менеджера информационной системы».

6) Выполните загрузку ролей доступа подключаемой ИС из файла.

7) При необходимости добавьте в файл «nginx.conf» паттерн с названием хоста подключаемой ИС – необходим для отображения страницы входа X-IDBOX и аутентификации на хосте ИС, а также для проверок запросов при авторизации.