|  |  |
| --- | --- |
|  |  |
| ПРОГРАММНЫЙ КОМПЛЕКС «U-CONNECT» | |
| Версия 1.0 | |
| Руководство администратора U-Connect | |
| Редакция от 26.04.2021 года | |
| Всего страниц: | |
|  |  |

**СОДЕРЖАНИЕ**

[1. Общие положения 3](#_Toc82182723)

[1.1. Обзор программного продукта 3](#_Toc82182724)

[1.2. Документация 4](#_Toc82182725)

[1.3. Термины и сокращения 4](#_Toc82182726)

[1.4. Уровень подготовки пользователей 5](#_Toc82182727)

[2. Общее описание ПК «U-Connect» 5](#_Toc82182728)

[2.1. Структура системы 5](#_Toc82182729)

[2.2. Компоненты с открытым исходным кодом 6](#_Toc82182730)

[2.3. Системные требования 6](#_Toc82182731)

[3. Установка и настройка 7](#_Toc82182732)

[3.1. Порядок действий 7](#_Toc82182733)

[3.2. Установка сервера 7](#_Toc82182734)

[3.3. Интеграция с 1С:ITIL 8](#_Toc82182735)

[3.4. Заполнение справочников 8](#_Toc82182736)

[3.5. Распространение агентов 9](#_Toc82182737)

[3.5.1. Общая информация 9](#_Toc82182738)

[3.5.2. Формирование ссылки на скачивание агента 10](#_Toc82182739)

[3.5.3. Создание и модификация пакетов 10](#_Toc82182740)

[3.6. Установка виртуальной машины 12](#_Toc82182741)

[4. Функционирование системы 13](#_Toc82182742)

[5. Проверка работоспособности 14](#_Toc82182743)

[5.1. Подготовка 14](#_Toc82182744)

[5.2. Проверка работоспособности агента 14](#_Toc82182745)

[5.3. Проверка инвентаризации 16](#_Toc82182746)

[5.4. Проверка мониторинга 27](#_Toc82182747)

[6. Эксплуатация 29](#_Toc82182748)

[6.1. Безопасность 29](#_Toc82182749)

[6.2. Резервное копирование 31](#_Toc82182750)

# Общие положения

## Обзор программного продукта

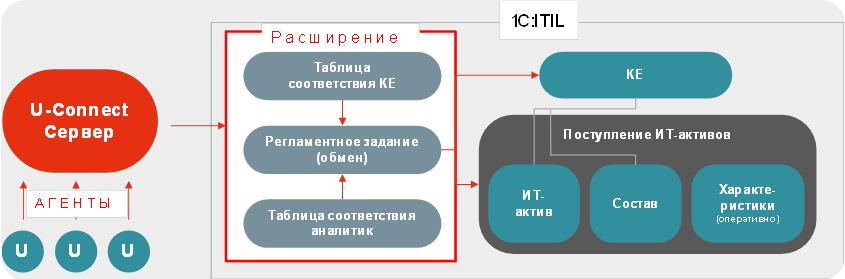
Программный комплекс «U-Connect» предназначен для использования сотрудниками подразделений информационных технологий в целях повышения оперативности и эффективности управления ИТ-инфраструктурой, включая серверы (физические и виртуальные), рабочие станции, маршрутизаторы, принтеры и сканеры, другое оборудование и сервисы.

Решение состоит из расширения 1С:ITIL, сервера сбора данных U-Connect, и агентов U-Connect для 1С:ITIL устанавливаемых на конечные устройства.

Сервер U-Connect является центром сбора и актуализации хранимых данных, содержит инструменты настройки скриптов для настройки логики работы программного комплекса.

Агенты U-Connect предназначены для сбора информации с рабочих станций и серверов (конечных устройств) об их компонентах. Для этой цели они устанавливаются на конечные устройства и соединяются с сервером по каналу, защищенному сертификатом безопасности. Агенты могут устанавливаться на компьютеры под управлением Windows 7-10, Windows Server 2012 и выше, а также на Linux (Debian, CentOS, RedHat). Информацию, получаемую от агентов, разделяют на две группы: информация из аудитов – статическая информация о компоненте; информация мониторинга телеметрии – динамическая информация, отражающая текущее состояние компонента.

Расширение 1C:ITIL выступает в качестве пользовательского интерфейса для программного комплекса, обеспечивает обработку и управление жизненным циклом объектов учета, информация о которых получена с помощью агентов. Передача данных между 1С:ITIL и серверной частью U-Connect происходит через программный интерфейс передачей JSON файлов.



## Документация

Настоящий документ содержит описание основных функциональных характеристик, порядка установки и первоначальной настройки программного комплекса «U-Connect», способа проверки его работоспособности, а также действий по его администрированию в процессе эксплуатации.

Дополнительную информацию можно получить в следующих документах:

* Руководство пользователя U-Connect
* Описание программного интерфейса (API)

Контакты технической поддержки размещены на сайте [u-connect.ru](https://u-connect.ru/).

## Термины и сокращения

В документе используются следующие термины и сокращения.

|  |  |
| --- | --- |
| **Термин/сокращение** | **Описание** |
| HTTP | Незащищённый протокол передачи данных между участниками информационного обмена |
| HTTPS | Защищённый протокол передачи данных между участниками информационного обмена |
| SSO | (Single sign-on) - Технология единого входа, при использовании которой пользователь переходит из одного раздела портала в другой, либо из одной системы в другую, не связанную с первой системой, без повторной аутентификации |
| Агент | Программный модуль, реализующий функции управления, сбора статистической информации и удалённого доступа к компьютеру |
| Агентская задача | Внутренняя структура данных, используемая для передачи информации, конфигурации, команд и их результатов |
| База данных | Организованная структура, предназначенная для хранения, изменения и обработки взаимосвязанной информации |
| Внутренняя структура данных | Любой объект информации, передающийся между участниками информационного обмена Программного комплекса «U-Connect» |
| Клиентская часть | Графический интерфейс по визуализации, созданию и изменению Внутренних структур данных, Агентских задач и Конфигурационных единиц |
| Конфигурационная единица | Внутренняя структура данных, предназначенная для изменения свойств, порядка и принципов работы участников информационного обмена Программного комплекса «U-Connect» |
| Сервер | Всеобъемлющее определение всех управляющих или участвующих в обмене модулей Программного комплекса «U-Connect» |

## Уровень подготовки пользователей

Программный комплекс «U-Connect» предназначен для применения следующими категориями пользователей:

* Администратор U-Connect
* Пользователь U-Connect

**Администратор U-Connect**

Администратор U-Connect устанавливает, настраивает и администрирует программный комплекс «U-Connect». Для этого он должен обладать следующими знаниями и умениями:

* Администрирование виртуальных сред
* Администрирование ОС Linux на уровне не ниже LPIC-2
* Знание стеков протокола TCP/IP
* Знание и умение администрирования СУБД PostgreSQL

**Пользователь U-Connect**

Пользователь U-Connect работает в пользовательском интерфейсе расширения U-Connect для 1С:ITIL. Пользователь запрашивает и обрабатывает данные аудита и телеметрии. Для этого он должен обладать следующими знаниями и умениями:

● Знание и умение работы с 1С:ITIL

● Администрирование персональных компьютеров

# Общее описание ПК «U-Connect»

## Структура системы

Программный комплекс «U-Connect» состоит из:

* Сервера U-Connect, устанавливаемого на виртуальную машину или физический компьютер, и управляющего работой U-Connect. Сервер U-Connect работает под управлением операционной системы Linux.
* Программных агентов U-Connect, устанавливаемых на управляемых компьютерах и работающих под управлением сервера. Пакеты установки программных агентов генерируются сервером U-Connect. Программные агенты U-Connect могут функционировать под управлением операционных систем MS Windows и Linux.

Данные компоненты осуществляют обмен данными посредством API U-Connect. Кроме того, API U-Connect используется для управления сервером U-Connect.

Программный комплекс «U-Connect» интегрируется с системой управления ИТ-процессами «1С:ITIL» (средства интеграции поставляются отдельно). Кроме того, посредством API программный комплекс «U-Connect» может быть интегрирован с любой другой информационной системой.

## Компоненты с открытым исходным кодом

Программный комплекс «U-Connect» использует следующие компоненты с открытым исходным кодом.

|  |  |
| --- | --- |
| **Наименование** | **Лицензия** |
| 7zip | LGPL |
| Apache Guacamole | Apache license 2.0 |
| Apache Kafka | Apache license 2.0 |
| boost 1.76 | Собственная, похожая на BSD/MIT |
| Docker 3 | Apache license 2.0 |
| Docker Compose | Apache license 2.0 |
| Faust | BSD 3-clause |
| Keycloak 12.0.2 | Apache license 2.0 |
| MinIO | GNU Affero General Public License v3.0 |
| Nchan | BSD 2-clause |
| Nginx 1.18 | BSD 2-clause |
| PostgreSQL 14 | PostgreSQL License |
| Python 3.9 | Python Software Foundation License |
| Qt | LGPL v3 |
| Redis Community Edition | BSD 3-clause |
| TightVNC 2.8.59 | GPL v2 |

## Системные требования

Минимальные требования к серверу U-Connect при условии развертывания до 1000 агентов:

* Процессор: 2,8 Ghz
* Ядер: не менее 6
* ОЗУ: 8 Gb
* Дисковый объём: 250 Гб

При росте общей нагрузки (количество агентов, количество конфигурационных единиц, интенсивность информационного обмена) требования к аппаратному обеспечению сервера U-Connect пропорционально увеличиваются.

# Установка и настройка

## Порядок действий

Поставка программного комплекса U-Connect возможна различными способами. Основной способ установки с помощью систем контейнеризации (Docker). Такой способ позволяет быстро обновлять элементы инфраструктуры и поддержать высокую работоспособность системы. Альтернативным способом поставки является распространения серверной части с помощью преднастроенной виртуальной машины. Такой способ проще в развертывании, но сложнее в эксплуатации.

Для установки U-Connect необходимо последовательно выполнить следующую последовательность шагов:

* Установка сервера U-Connect
* Интеграция с 1С:ITIL
* Заполнение справочников U-Connect
* Распространение и установка агентов U-Connect на управляемые компьютеры

Более подробно эти действия описаны ниже.

## Установка сервера

Дистрибутив представляет собой набор Docker-файлов с сервером U-Connect. Перед началом установки необходимо убедиться в наличии установленных утилит Docker и Docker Compose.

Далее необходимо выполнить следующие действия:

1. Сгенерировать сертификат администратора.
2. Установить докер-файлы, запустив bash файл распаковки.
3. Назначить IP адрес
4. Сгенерировать ключи
5. Сделать запись DNS типа A в DNS зоне для сервера на IP адрес, через который агенты из внешней сети будут соединяться с сервером
6. Внести созданное имя в настройки сервера U-Connect

После этого сервер U-Connect готов к работе.

## Интеграция с 1С:ITIL

Интеграция с 1С:ITIL происходит путем установки предоставляемой конфигурации 1С стандартными средствами программы. При этом обмен данными и управление программным комплексом U-Connect происходит через набор API. Вследствие этого остается возможность управления программным комплексом U-Connect в обход интерфейса 1С:ITIL при действительном сертификате безопасности. Такой сценарий использования системы может быть полезен при эксплуатации и администрировании системы для прямого доступа к возможностям сервера U-Connect.

## Заполнение справочников

После установки сервера рекомендуется заполнить перечисленные ниже справочники, используемые для группировки конфигурационных единиц. Если этот шаг будет пропущен, группировка конфигурационных единиц по этим признакам будет недоступна.

Справочники к заполнению:

* Справочник организаций
* Справочник подразделений
* Справочник мест размещения (локаций)

Заполнять справочники можно любым из следующих способов:

* С помощью API, описанного в документе «U-Connect. Описание программного интерфейса».
* Посредством графического интерфейса 1С:ITIL.

**Справочник организаций**

Справочник организаций представляет собой перечень организаций, обслуживаемых данным сервером U-Connect для 1С:ITIL. Каждая организация может содержать подразделения. Используемые организацией конфигурационные единицы могут располагаться в различных локациях (местах размещения).

**Справочник подразделений**

Справочник подразделений представляет собой иерархический перечень подразделений той или иной организации. Каждая конфигурационная единица может быть отнесена к одному подразделению.

**Справочник мест размещения (локаций)**

Справочник локаций представляет собой иерархический перечень мест размещения конфигурационных единиц. Под локацией понимаются площадки размещения, здания, части зданий, этажи, комнаты и т.п. Каждая конфигурационная единица может быть отнесена к одной локации.

## Распространение агентов

Дистрибутивы (пакеты установки) агентов формируются сервером U-Connect. Для распространения агентов по управляемым компьютерам необходимо выполнить следующие шаги:

* Создание пакета(-ов) установки агента
* Формирование ссылки для скачивания пакета
* Установка пакета на управляемых компьютерах

Первые два шага можно выполнить любым из следующих способов:

* С помощью API, описанного в документе «U-Connect. Описание программного интерфейса».
* Посредством графического интерфейса 1С:ITIL (подробно описано в руководстве пользователя).

**Создание пакета**

Пакет установки агента – это его дистрибутив с внедренными в него первоначальными параметрами конфигурации, которые, помимо технических параметров, также содержат идентификаторы подразделения и локации, к которым относится компьютер. Таким образом, создав пакеты установки для каждого сочетания подразделения и локации, можно избежать ручной классификации конфигурационных единиц, соответствующих компьютерам с установленными агентами.

**Установка пакета на управляемых компьютерах**

Важно: Разрядность операционной системы и права пользователя, осуществляющего установку, должны сочетаться, соответственно, с разрядностью агента и типом установки, указанными при формировании ссылки.

ИТ-специалист передает пакет установки агента пользователям посредством электронной почты в виде вложения или ссылки для скачивания, через общую сетевую папку или на носителе информации. Затем пользователь самостоятельно устанавливает агент на свой компьютер.

## Общая информация

Установочный дистрибутив агента скачивается посредством специализированного запроса к API по URL.

В системе доступно два типа установочных пакетов:

1. Системные - устанавливается в виде службы Windows или демон в Linux
2. Пользовательские - устанавливаются в директорию пользователя и не требуют прав администратора компьютера

В установочные пакеты в качестве параметров при создании могут быть переданы аналитики, к которым агент будет привязан во время установки. В настоящее время доступны две аналитики:

* Департамент
* Размещение

## Формирование ссылки на скачивание агента

Для формирования ссылки на скачивание можно воспользоваться примером

https:/<ServerIP>/api/v1/packages/<PacketID>/agent?agent\_type=<PacketType>

Где:

* <ServerIP> - адрес сервера. Может быть как IP адрес, так и имя ресурса
* <PacketID> - GUID пакета
* <PacketType> - тип пакета
* UAgentSystemInstall - системный
* UAgentUserInstall - пользовательский

## Создание и модификация пакетов

URL для работы с пакетами установки агента https://<ServerIP>/api/v1/packages.

Доступные методы и примеры использования методов по работе с пакетами:

* Получить список установочных пакетов:  
  *curl -X 'GET' '*[*https://<ServerIP>/api/v1/packages?limit=100&offset=0*](about:blank)*' -H 'accept: application/json'*
* Создать пакет:  
  *curl -X 'POST' \*  
   *'https://<ServerIP>/api/v1/packages' \*  
  *-H 'accept: application/json' \*  
  *-H 'Content-Type: application/json' \*  
  *-d '{*  
  *"name": "TEST121",*  
  *"location\_id": "<Location GUID>",*  
  *"department\_id": "<Department GUID>",*  
  *"config": {*  
  *"mainSettings": {*  
  *"urlPostCsrAndReceiveClientCert": https://<ServerIP>/api/v1/agents/register*  
   *},*  
  *"remote\_server": {*  
  *"address": https://<ServerIP>/,*  
  *"wsaddress": "wss://<ServerIP>/sub"*  
  *},*  
  *"remoteAccess": {*  
  *"enabled": false,*  
  *"globalAddress": "<ServerIP>",*  
  *"globalPort": "4444",*  
  *"localPort": "6001"*  
  *},*  
  *"sentry": {*  
  *"enabled": false,*  
  *"httpLogPath": https://<ID>@<LogServerIP>/2*  
  *},*  
  *"log": {*  
  *"logtype": "trace"*  
  *}*  
  *}*  
  *}'*
* Изменить пакет:  
  *curl -X 'PUT' \*  
  *'https://<ServerIP>/api/v1/packages/<Package GUID>' \*  
  *-H 'accept: application/json' \*  
  *-H 'Content-Type: application/json' \*  
  *-d '{*  
  *"name": "TEST122",*  
  *"location\_id": "<Location GUID>",*  
  *"department\_id": "<Department GUID>",*  
  *"config": {*  
  *"mainSettings": {*  
  *"urlPostCsrAndReceiveClientCert": https://<ServerIP>/api/v1/agents/register*  
   *},*  
  *"remote\_server": {*  
  *"address": https://<ServerIP>/,*  
  *"wsaddress": "wss://<ServerIP>/sub"*  
  *},*  
  *"remoteAccess": {*  
  *"enabled": false,*  
  *"globalAddress": "<ServerIP>",*  
  *"globalPort": "4444",*  
  *"localPort": "6001"*  
  *},*  
  *"sentry": {*  
  *"enabled": false,*  
  *"httpLogPath": https://<ID>@<LogServerIP>/2*  
  *},*  
  *"log": {*  
  *"logtype": "trace"*  
  *}*  
  *}*  
  *}'*
* Удалить пакет  
  curl -X 'DELETE' \  
  'https://*<ServerIP>*/api/v1/packages/*<PackageGUID>*' \  
  -H 'accept: \*/\*'
* Получить ссылку на скачивание пакета
  + Системного  
    *curl -X 'GET' \*  
     *'https://<ServerIP>/api/v1/packages/<PackageGUID>/agent?agent\_type=UAgentSystemInstall' \*  
     *-H 'accept: application/json'*
  + Пользовательского  
    *curl -X 'GET' \*  
     *'https://<ServerIP>/api/v1/packages/<PackageGUID>/agent?agent\_type=UAgentUserInstall' \*  
     *-H 'accept: application/json'*

## Установка виртуальной машины

При установке программного комплекса, поставляемого в виде виртуальной машины, необходимо провести следующие действия.

Архив для поставки содержит образ машины, а также сертификат безопасности и файл с паролями для установки сертификата.

Файл виртуальный машины, предлагаемый к поставке, предназначен для импорта в гипервизор Hyper-V. При этом в настройках гипервизора для стабильной работы системы следует выделить не менее 8 ГБ оперативной памяти. В качестве дополнительных системных требований следует отметить необходимость выделения не менее 6 ядер с частотой не менее 2,8 ГГц. Виртуальная машина займет 9 Гб дискового пространства.

В качестве сетевой карты для виртуальной машины необходимо выбрать физическую карту, установленную на хосте. Для использования функциональности системы в настройках виртуальный машины должен быть подключен сетевой мост и включена раздача IP-адресов по DHCP в сети.

После запуска сервера, произвести вход на сам сервер по идентификационным данным.

После входа необходимо посмотреть полученный ip-адрес (например, командой: hostname –I, необходимый адрес будет первым в списке)

После этого сменить директорию cd ~/deploy/u\_backend и отредактировать файл docker-compose.yml следующим образом:

1. Найти раздел

 u\_backend:

   extra\_hosts:

     - "rc-serv1.u-back.lcl:192.168.133.108"

2. Сменить ip-адрес 19.168.133.108 на адрес, который сервер получил по dhcp.

3. Сменить директорию cd ../guacamole\_keycloak и выполнить команду: sudo docker-compose up -d && docker-compose ps. Все контейнеры должны иметь статус «up».

4. Сменить директорию cd ../u\_backend  и запустить docker-compose  командой sudo docker-compose up -d && docker-compose ps. Все контейнеры должны иметь статус «up».

Для машины, с которой планируется подключение к серверу, необходимо провести следующие действия:

1. На компьютере, с которого планируется подключение, необходимо установить сертификат, скачанный вместе с образом машины. Запустить его и установить в личное хранилище сертификатов, используя пароль от сертификата, который записан в файле pass.txt.

2. В файле hosts добавить запись your\_ip\_address\_server serv1.u-back.lcl, где your\_ip\_address\_server - это Ip-адрес, который сервер получил по dhcp.

3. Проверить подключение к API U-Connect через Swagger по адресу https://serv1.u-back.lcl/api/v1/docs.

# Функционирование системы

Сразу после установки агент U-Connect автоматически регистрируется на сервере U-Connect, проводит инвентаризацию компьютера и пересылает ее результаты на сервер.

В дальнейшем агент:

* С определенной периодичностью проводит аудит изменений в конфигурации компьютера и в случае изменений отправляет новые данные на сервер.
* С определенной частотой определяет параметры утилизации процессора, оперативной памяти и логических дисков (телеметрия) и отправляет эту информацию на сервер.
* Ожидает от сервера команд на удаленное подключение и при ее поступлении запускает соответствующий сервис.

Сервер U-Connect:

* Принимает от агентов и сохраняет в своей базе данных результаты инвентаризации конфигурационных единиц и ее изменений, а также данные телеметрии.
* Ожидает поступления по API команды на удаленное подключение к определенному компьютеру, отсылает на установленный на нем агент соответствующую команду и организует подключение к удаленному рабочему столу.

# Проверка работоспособности

## Подготовка

Действия по проверке работоспособности должны проводиться после установки и настройки системы, как это описано в разделе 3 «Установка и настройка».

Для проверки работоспособности системы можно использовать Swagger или иное средство, позволяющее непосредственно работать с REST API. Описание API U-Connect содержится в документе «U-Connect. Описание программного интерфейса (API)».

## Проверка работоспособности агента

***Установка агента***

***Действие:***

Для начала работы с программным комплексом U-Connect необходимо установить установочный пакет агента ucagent\_0.4.85-1\_amd64.deb на тестовую машину. При поставке в составе единичной машины агент на неё предустановлен и операцию установки агента нужно пропустить.

Для проверки правильности установки агента необходимо открыть папку /usr/local/ucagent/.

***Ожидаемый результат:***

На машине сформированы следующие папки:

agentServer:

bin/

etc/ucAgent.conf

lib/

var/log/ucAgent/main

var/ucAgent/certificates/syslog + cacert.cem + clientCert.cem + clientPrivateKey.pem + csrx509

var/ucAgent/plugins

***Проверка сертификата доступа***

***Действие:***

После проверки наличия указанных папок следует открыть файл, содержащий логи агента, расположенный в папке /usr/local/ucagent/var/log/ucAgent/main - самый первый файл по времени создания – после каждой остановки/запуска агента формируется новый файл лога.

Для обеспечения безопасности системы у каждого агента есть сертификат доступа. В рамках проверки работоспособности агента необходимо проверить присвоение uid-ов и формирование сертификата:

***Ожидаемый результат:***

machineUniqueId: 'c1df4224-9fd5-5acd-a224-282a8d9d5bc8'

'-----BEGIN CERTIFICATE-----

MIIEUjCCAjqgAwIBAgIUXDQrv+3yFzTjwwBE6a3Wle0PHBowDQYJKoZIhvcNAQEL

BQAwWTELMAkGA1UEBhMCUlUxDTALBgNVBAgMBFRlc3QxDTALBgNVBAcMBFRlc3Qx

ETAPBgNVBAoMCFUtc3lzdGVtMRkwFwYDVQQDDBBkZXYudS1jb25uZWN0LnJ1MB4X

DTIxMDgxODA4MDU1OVoXDTIyMDgxODA4MDU1OVowbTELMAkGA1UEBhMCUlUxDTAL

BgNVBAgMBFRlc3QxDTALBgNVBAcMBFRlc3QxETAPBgNVBAoMCFUtc3lzdGVtMS0w

KwYDVQQDDCQ5Y2UyZDcwNi0yY2U4LTQwYWQtYjA2ZS01MTI5NTdjOTJlOGIwggEi

MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCU5eA0k8+DyYxzIg4LnIhIRg65

r9npcbjXbYZfeL2JAQsg8/1OSs3nAlK9MVspUF7Psr870CM1CST5jk6oZVC5Qn3f

FwDkgcPyY/QzzTLHk8oDKji/CUjWYdXbRkBaVLyVLtGI2YRA3y9ya0bNds89sSQm

FQltBURy8bTdhsOijLy3Np4iKYmHb4n1B4eAT4ZfZleP78/19tk14Sv9iNriY+NF

ESHI8oLiKsVvN4ZNB60Hb5rBtf+LXqHdh6WgoXiAEeZNXtp81sGVTXkejZdf4UfS

xxrhhwLP8JvfC9JwrWotWH3/COXewCRTYxOCCwC6JP2HQuB6zAhFaeFSM47HAgMB

AAEwDQYJKoZIhvcNAQELBQADggIBADWecyrj5bS4mXih82qGiAwq8B2G4DP1GTmw

VlPGCKyr1cY6sb2fI/n0wRwTjjU65b9ahQ8A8EIG/SXQGXhOCsqvZXlpKSQorc2g

gllQ0fXbn0VktbCJ6wGFBnnnaK0aXIPBND1idGULHVoraIOuhPexuAa3i06+7zff

fpE2rtegmuxAeyhGZz9AWLYSvl0S0e04NZ8pIBgVkW54eIS8u/j/WOrMaEiAXtDT

K0qSnQOqVASbzO3edRe/Iz5gOXbRXzNc0Lgfz1m4IooJupx2F50U+C3A1tmDPSZU

DX148ptdltp5ecV6llja/+rtcDpbNCAP9bhFhtlXfq9E3nDcGw2b7FX/7KXrcu0G

1bg+dLRnt8PsORmHfW50rV8/u/mx/KwEa0QRisVWrm83gBcCH0gqrA1yQ0wDPQRI

+7jUwCLZkkxBdrCtxfWH/IbNI0VJoEg9umGRGxk5SNKlQ91odI/YVu+C/joID0aK

JmYWMt4Fdv9uIjswJT10m6Dm5EQHi3N/h9nZmRRsTh2G6IvkywF5qIFCQ8uctnL7

+ncY8l4d3pKW7PKeYtMysvKKJ0Su0H/kAQdeK5ZneYHNzZOxsWy+scmdi2QovS/l

nu8+y09LQK79V5cj8hZHGqqz0PIUsdu3KmtIda/F0M0QRdRmfleXlpHhSS92AK8L

16wYvjDH

-----END CERTIFICATE-----'

CN is: '9ce2d706-2ce8-40ad-b06e-512957c92e8b'

***Запрос перечня агентов на сервере***

***Действие:***

Для завершения проверки работоспособности агента рекомендуется сделать запрос перечня существующих агентов на сервере. Для этого формируем cURL запрос вида:

curl -X 'GET' \

'https://192.168.133.108/api/v1/agents?limit=100&offset=0'

***Ожидаемый результат:***

Получаем ответа типа

{

"limit": 100,

"offset": 0,

"count": 5,

"total": 1,

"items": [

{

"created\_at": "2021-04-29T06:51:58.616535+00:00",

"updated\_at": "2021-04-29T06:51:58.616565+00:00",

"id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"version": 0,

"guac\_id": 320,

"group\_id": null,

"online": false,

"host\_name": "Kirills-MacBook-Pro.local",

"node\_id": null

}

Подробное описание ответа см. п.2.1 U-Connect. API v20210818

## Проверка инвентаризации

***Первичная инвентаризация***

***Действие:***

При регистрации агента он проводит первичную инвентаризацию компонентов системы. Для проверки результатов необходимо проверить результаты задач, запускаемых при регистрации

***Ожидаемый результат:***

Перечень оприходованных КЕ полностью совпадает с данными с самого компьютера и заполняется в API вида:

*driveDeviceAudit*

data: '{

"data": {

"currentHash": "string",

"isHashChanged": true,

"isMatchingMode": false,

"result": [

{

"mountPoint": "string",

"serialNumber": "значение",

"totalSize": "объём в байтах",

"type": "string"

},

]

},

"result": "Success"

}'

*gpuDeviceAudit*

data: '{

"data": {

"currentHash": " string ",

"isHashChanged": true,

"isMatchingMode": false,

"result": [

{

"name": " string ",

"note": " string "

}

]

},

"result": "Success"

}'

*cpuDeviceAudit*

data: '{

"data": {

"currentHash": " string ",

"isHashChanged": true,

"isMatchingMode": false,

"result": [

{

"name": " string ",

"note": " string ",

"numCpu": "значение"

}

]

},

"result": "Success"

}'

*softAudit*

data: '{

"data": {

"currentHash": " string ",

"isHashChanged": true,

"isMatchingMode": false,

"result": [

{

"exePath": " string ",

"installedDt": "дата в формате ГГГГММДД",

"name": " string ",

"note": " string ",

"version": "значение"

},

]

},

"result": "Success"

}'

*networkDeviceAudit*

data: '{

"data": {

"currentHash": " string ",

"isHashChanged": true,

"isMatchingMode": false,

"result": [

{

"dhcp4Enabled": false,

"dhcp6Enabled": false,

"humanReadableName": "lo",

"ipAddresses": [

{

"broadcast": "ххх.ххх.ххх.ххх",

"ip": " ххх.ххх.ххх.ххх ",

"netmask": " ххх.ххх.ххх.ххх ",

"prefixLength": значение

},

{

"broadcast": "",

"ip": " ххх.ххх.ххх.ххх",

"netmask": "ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff",

"prefixLength": значение

}

],

"ipv4Dns": [

"",

""

],

"ipv4Gateway": [

""

],

"ipv6Dns": [

"",

""

],

"ipv6Gateway": [

""

],

"macAddress": "00:00:00:00:00:00",

"name": "lo",

"type": 1

},

*baseSystemAudit*

data: '{

"data": {

"currentHash": " string",

"isHashChanged": true,

"isMatchingMode": false,

"result": {

"OSFamily": " string ",

"buildAbi": " string ",

"buildCpuArchitecture": " string ",

"cpu": [

{

"name": " string ",

"note": " string ",

"numCpu": "значение"

}

],

"currentCpuArchitecture": " string ",

"drives": [

{

"mountPoint": " string ",

"serialNumber": "значение",

"totalSize": "значение в байтах",

"type": " string "

},

],

"kernelType": " string ",

"kernelVersion": значение",

"machineHostName": " string ",

"machineUniqueId": " string ",

"machineUniqueIdReal": " string ",

"prettyProductName": " string ",

"productType": " string ",

"productVersion": " string ",

"totalRam": "значение в байтах",

"username": " string "

}

},

"result": "Success"

}'

***Действие:***

Полученные при первичном аудите данные загружаются на сервер U-Connect. После чего они доступны для запроса через стандартные API программного комплекса. Проверка данных рабочим станциям (endpoint) производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&agent\_id=ae3b282e-ab3c-444b-9cb3-b52e0d957c14', где ae3b282e-ab3c-444b-9cb3-b52e0d957c14 - id агента, получить который можно командой curl -X 'GET' \

'https://192.168.133.108/api/v1/agents?limit=100&offset=0'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818)

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"parent\_id": null,

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": true,

"detected\_at\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"user\_defined\_name": "SRV10904",

"agent\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"ci\_type\_id": null,

"ci\_class": "endpoint",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"is\_portable": false,

"virtualization": null,

"os": {

"family": "windows",

"version": "server2012r2",

"name": "Windows Server 2012 R2 Version 6.3 (Build 9600)"

},

"host\_name": "SRV10904",

"chassis\_type": null,

"summary\_info": null,

"vsm\_info": {

"host\_address": "192.168.133.22",

"name": "hyperV",

"version": ""

},

"host\_info": null,

"last\_reboot\_time": null,

"last\_seen": null,

"username": "SYSTEM"

}

}

]

}

***Проверка результатов инвентаризации***

***Действие:***

Проверка данных по входящим жёстким дискам производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&parent\_id=c1df4224-9fd5-5acd-a224-282a8d9d5bc8&ci\_class=storage', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818), необходимо сравнить полученные данные с установленным аппаратным обеспечением

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "77ee18da-277b-49bb-af00-10c697b5ce18",

"parent\_id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": false,

"detected\_at\_id": "b97a715c-bb37-4a85-984f-d539197b96af",

"user\_defined\_name": null,

"agent\_id": null,

"ci\_type\_id": null,

"ci\_class": "storage",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"size": 156918345728,

"type": "NTFS",

"mount\_point": "C:/",

"serial\_number": ""

}

},

***Действие:***

Проверка данных по входящему ПО производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&parent\_id=c1df4224-9fd5-5acd-a224-282a8d9d5bc8&ci\_class=software', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818), необходимо сравнить полученные данные с установленным программным обеспечением

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "9743d688-b66d-4393-946f-51b713b94375",

"parent\_id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": false,

"detected\_at\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"user\_defined\_name": null,

"agent\_id": null,

"ci\_type\_id": null,

"ci\_class": "software",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"name": "7-Zip 18.05 (x64)",

"version": "18.05",

"exe\_path": "C:\\Program Files\\7-Zip\\",

"installed\_dt": "",

"note": ""

}

},

***Действие:***

Проверка данных по входящим видеокартам производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&parent\_id=c1df4224-9fd5-5acd-a224-282a8d9d5bc8&ci\_class=gpu', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818), необходимо сравнить полученные данные с установленным аппаратным обеспечением

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "531b4ea2-b539-413c-98ca-90608aa1250a",

"parent\_id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": false,

"detected\_at\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"user\_defined\_name": null,

"agent\_id": null,

"ci\_type\_id": null,

"ci\_class": "gpu",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"name": "Microsoft Basic Display Adapter",

"version": null,

"exe\_path": null,

"installed\_dt": null,

"note": "Microsoft Basic Display Adapter"

}

}

]

}

***Действие:***

Проверка данных по входящим процессорам производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&parent\_id=c1df4224-9fd5-5acd-a224-282a8d9d5bc8&ci\_class=cpu', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818)

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "c530561a-e2b6-42cc-a11e-c8720756b3ef",

"parent\_id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": false,

"detected\_at\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"user\_defined\_name": null,

"agent\_id": null,

"ci\_type\_id": null,

"ci\_class": "cpu",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"name": "AMD Phenom(tm) II X6 1100T Processor",

"cores": 6,

"architecture": "x86\_64",

"note": "AMD64 Family 16 Model 10 Stepping 0"

}

}

]

}

Подробное описание ответа см. п.3.3 U-Connect. API v20210818

***Действие:***

Проверка данных по входящим сетевым устройствам производится командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/ci/detail?limit=100&offset=0&parent\_id=c1df4224-9fd5-5acd-a224-282a8d9d5bc8&ci\_class=network\_interface', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.3.3 U-Connect. API v20210818)

{

"limit": 10,

"offset": 0,

"count": 0,

"total": 0,

"items": [

{

"id": "02d887f3-29f1-43ef-b8bb-11092df08f12",

"parent\_id": "c1df4224-9fd5-5acd-a224-282a8d9d5bc8",

"ci\_name": null,

"system\_name": null,

"serial\_number": null,

"inv\_number": null,

"manufacturer\_id": null,

"verified": false,

"vsm\_host\_machine": false,

"detected\_at\_id": "9ce2d706-2ce8-40ad-b06e-512957c92e8b",

"user\_defined\_name": null,

"agent\_id": null,

"ci\_type\_id": null,

"ci\_class": "network\_interface",

"location\_id": "19411a72-9547-4143-9d0e-d001e91fa869",

"department\_id": "a2c5b5aa-3b38-48c1-8aeb-d10e74c51a87",

"detail": {

"human\_readable\_name": "vEthernet (ext133)",

"ip\_addresses": [

{

"broadcast": "192.168.133.255",

"defaultGateway": null,

"dhcpEnabled": null,

"dnsServer": null,

"ip": "192.168.133.22",

"netmask": "255.255.255.0",

"prefixLength": 24

}

]

## Проверка мониторинга

***Мониторинг утилизации ресурсов***

***Действие:***

Мониторинга утилизации ресурсов системы рабочей станции запускается автоматически через фиксированные промежутки времени.

***Ожидаемый результат:***

Результат отображается в логах агента в формате:

BaseSystemMonitoring

data: '{

"data": {

"cpuLoad": [

"значение в %"

],

"drives": [

{

"freeSize": "значение в байтах",

"mountPoint": "string",

"serialNumber": "значение",

"totalSize": " значение в байтах ",

"uuid": string "

},

],

"freeRam": "значение в байтах",

"localAddress": "ххх.ххх.ххх.ххх",

"onlineUsers": [

"string"

],

"totalRam": " значение в байтах "

},

"result": "Success"

}'

***Запрос данных мониторинга***

***Действие:***

Данные мониторинга посредством API передаются на сервер U-Connect. На сервере данные телеметрии можно запросить командой:

curl -X 'GET' \

'https://192.168.133.108/api/v1/telemetry?uid=c1df4224-9fd5-5acd-a224-282a8d9d5bc8', где c1df4224-9fd5-5acd-a224-282a8d9d5bc8 - id машины, на которую установлен агент, получить который можно командой curl -X 'GET' \ 'https://192.168.133.108/api/v1/ci?limit=100&offset=0&ci\_class=endpoint'

***Ожидаемый результат:***

Получаем ответа типа (подробное описание ответа см. п.10.1 U-Connect. API v20210818)

{

"base": {

"cpu\_load": [

"45"

],

"drives": [

{

"size": 156918345728,

"type": null,

"mount\_point": "C:/",

"serial\_number": "1847389967",

"path": ""

},

{

"size": 842915639296,

"type": null,

"mount\_point": "D:/",

"serial\_number": "4276187719",

"path": ""

},

{

"size": 3000457228288,

"type": null,

"mount\_point": "E:/",

"serial\_number": "919323690",

"path": ""

}

],

"local\_address": "192.168.133.22",

"free\_ram": 2984068,

"total\_ram": 16514144,

"state": null

},

"by\_vsm": null,

"vsm\_info": null

# Эксплуатация

## Безопасность

Объектами защиты структуры, попадающими в область применения ПК «U-Connect» и, соответственно, в сферу контроля встроенной системы защиты, являются объекты, к которым администратором безопасности разрешен удаленный доступ с использованием ПК «U-Connect»:

1. персональные компьютеры и серверы (далее – сетевые станции),
2. информационные ресурсы, представленные в виде объектов файловых систем сетевых станций (тома, папки, файлы, реестры),
3. программное обеспечение, размещенное на сетевых станциях,
4. иные объекты, доступ к которым возможен из операционной среды сетевой станции (например, объекты баз данных, к которым пользователю открыт доступ с сетевой станции).

При этом необходимыми условиями для осуществления удаленного доступа к указанным выше объектам (условиями попадания объектов защиты в сферу контроля ПК «U-Connect») являются:

1. предоставление доступа (средствами системы защиты информации (СЗИ)) к объектам защиты для пользователя, осуществляющего свою деятельность на сетевой станции;
2. инсталляция клиентской части ПК «U-Connect» на сетевой станции заказчика;
3. разрешение (средствами СЗИ и в соответствии с правилами разграничения доступа) удаленного доступа с сетевой станции Оператора ПК «U-Connect» к сетевой станции;
4. регистрация сетевой станции и сетевой станции Оператора ПК «U-Connect» в ПК «U-Connect»;
5. разрешение (средствами встроенной системы защиты ПК «U-Connect» и в соответствии с правилами разграничения доступа ПК «U-Connect») удаленного доступа с сетевой станции Оператора ПК «U-Connect» к сетевой станции;
6. определение сотрудником прав (из тех, что предоставлены ему в соответствии с матрицей доступа), которые могут быть делегированы Оператору ПК «U-Connect» при удаленном доступе его к сетевой станции;

Схема включения ПК «U-Connect» в программно-аппаратный комплекс заказчика выбирается оператором в зависимости от задач, которые планируется решать с использованием ПК «U-Connect». Обязательным условием применения ПК «U-Connect» в системе заказчика является размещение серверной части ПК «U-Connect» в защищенном сегменте вычислительной сети. Оператором системы при этом определяется ряд организационных мероприятий, предваряющих применение ПК «U-Connect» в составе программно-аппаратного комплекса, таких как:

1. ввод в действие разрешительных документов, позволяющих и регламентирующих доступ к защищаемым ресурсам Операторов ПК «U-Connect» (соглашение о неразглашении информации Оператором ПК «U-Connect», корректировка матрицы доступа, правил межсетевого экранирования и т.д.);
2. при размещении сетевых станций ПК «U-Connect» за пределами контролируемой зоны – организация защищенного канала передачи данных между сетевыми станциями ПК «U-Connect» и необходимыми (требующих обслуживания в ПК «U-Connect») сетевыми станциями;
3. регистрация выделенных для взаимодействия сетевых станций в ПК «U-Connect» с соблюдением требований политик подключения, установленных политикой безопасности;
4. регистрация учетных данных Операторов ПК «U-Connect»;
5. активация учетных записей пользователей ПК «U-Connect» и назначение им прав доступа.

При внедрении ПК «U-Connect» оператор должен пересмотреть и при необходимости скорректировать модель угроз безопасности информации и модель нарушителя на предмет оценки актуальности угроз, связанных с особенностями удаленного доступа к защищаемым ресурсам при использовании ПК «U-Connect»

Защита от несанкционированного доступа к информации в ПК «U-Connect» обеспечивается встроенным средством защиты информации. Встроенное средство защиты является составной частью ПК «U-Connect» и предназначено для защиты информации от несанкционированного доступа исключительно в ПК «U-Connect». Соответственно, сферой ответственности встроенного средства защиты является защита информации от несанкционированного доступа в контуре ПК «U-Connect», включающем:

1. сервер ПК «U-Connect»;
2. сервер базы данных управления конфигурациями (CMDB);
3. Агент U-Connect
4. клиентская часть ПК «U-Connect», установленная на сетевых станциях операторов и клиентов ПК «U-Connect».

Защита от несанкционированного доступа к информации на сетевых станциях сотрудников, подключенных к ПК «U-Connect», а также защита каналов связи, выходящих за пределы контролируемой зоны, защита периметра сети и защита сегмента вычислительной сети, в которой размещается серверная часть ПК «U-Connect», осуществляется средствами системы защиты информации заказчика.

## Резервное копирование

При эксплуатации программного комплекса U-Connect рекомендуется делать регулярное резервное копирование следующих компонентов инфраструктуры:

* Создание копии конфигурационных файлов комплекса
* Создание резервных копий базы данных postgres средствами самой базы данных (согласно документации к postgres версии 13)

Резервное копирование баз данных и конфигурационных файлов рекомендуется проводить планово не реже одного раза в неделю в рамках регулярного обслуживания программного комплекса. Внеплановое копирование рекомендуется проводить до обновления компонентов системы, а также до технических работ на серверах, на которых установлен программный комплекс.