Изображение выглядит как Графика, логотип, Шрифт, текст

Автоматически созданное описание



Программа для ЭВМ «Система управления конфигурациями «Атом.Порт: Целевой релиз»

**Руководство системного администратора**

Листов: 29

Дата: 18.09.2023

Версия: 1.0

Аннотация

В настоящем документе приведено руководство системного администратора по установке и настройке программы для ЭВМ Система управления конфигурациями «Атом.Порт: Целевой релиз» (далее – Программа).

В разделе «Общие сведения о программе» указаны назначение и функции Программы, сведения о технических и программных средствах, обеспечивающих выполнение Программы.

В разделе «Структура программы» приведены сведения о структуре программы, ее составных компонентах и модулях.

В разделе «Настройка программы» приведено описание действий по настройке Программы на условиях конкретного применения.

В разделе «Проверка программы» приведено описание способов проверки, позволяющих дать общее заключение о работоспособности Программы.

Структура и оформление настоящего документа соответствует ГОСТ 19.503-79.

Примечание. В связи с постоянным развитием Программы элементы интерфейса и значения ее фактических параметров могут отличаться от документированных.

Содержание

[1 Общие сведения о программе 4](#_Toc145951299)

[1.1 Назначение программы 4](#_Toc145951300)

[1.2 Условия применения 5](#_Toc145951301)

[1.2.1 Описание типовой инфраструктуры миграции 5](#_Toc145951302)

[1.2.2 Требования к серверу Программы «Атом.Порт» 6](#_Toc145951303)

[1.2.3 Требования к рабочим станциям 7](#_Toc145951304)

[1.2.4 Требования к сетевой инфраструктуре 7](#_Toc145951305)

[1.2.4.1 Общие требования 7](#_Toc145951306)

[1.2.4.2 Настройка сервера DHCP 8](#_Toc145951307)

[1.2.4.3 Настройка антивирусных систем и систем предотвращения вторжений 9](#_Toc145951308)

[1.2.4.3.1 Пример настройки исключений антивирусных продуктов Dr.WEB 9](#_Toc145951309)

[1.2.4.3.2 Пример настройки исключений антивирусных продуктов Касперского 11](#_Toc145951310)

[2 Структура программы 13](#_Toc145951311)

[3 Настройка программы 15](#_Toc145951312)

[3.1 Установка серверных компонентов Программы 15](#_Toc145951313)

[3.1.1 Установка сервера на виртуальную машину 15](#_Toc145951314)

[3.2 Установка клиентских компонентов Программы 17](#_Toc145951315)

[3.2.1 Установка клиента с помощью пакетного файла 17](#_Toc145951316)

[3.2.2 Установка клиента в интерактивном режиме 18](#_Toc145951317)

[3.2.3 Установка клиента с помощью групповых политик Microsoft AD 21](#_Toc145951318)

[4 Проверка программы 26](#_Toc145951319)

[4.1 Мониторинг работы серверных компонентов Программы 26](#_Toc145951320)

[4.1.1 Системные процессы 26](#_Toc145951321)

[4.1.2 Проверка работоспособности Программы при помощи файлов журналов 27](#_Toc145951322)

[4.2 Мониторинг работы клиента Программы 28](#_Toc145951323)

[4.2.1 Мониторинг работы клиента в ОС Windows 28](#_Toc145951324)

[4.2.2 Мониторинг работы клиента в ОС Linux 29](#_Toc145951325)

[4.2.3 Проверка работоспособности АРМ Администратора Программы 29](#_Toc145951326)

# Общие сведения о программе

## Назначение программы

Программа для ЭВМ «Система управления конфигурациями «Атом.Порт» (далее — Программа) — это программный комплекс, предназначенный для централизованного управления программными конфигурациями рабочих станций на базе операционных систем семейств GNU/Linux и Microsoft Windows.

Программа предназначена для управления инфраструктурой рабочих мест государственных и коммерческих средних предприятий.

Программа предназначена для осуществления следующих видов деятельности по автоматизации:

1. Инвентаризация автоматизированных рабочих мест (далее – АРМ) пользователей, включающая сбор, хранение и обработка данных о рабочих станциях (далее – РС);
2. Мониторинг состояния рабочих станций;
3. Конфигурирование рабочих станций и групп рабочих станций, в том числе миграция рабочих станций пользователей на отечественное ПО;
4. Управление конфигурациями гибридной инфраструктуры рабочих станций.

Программа позволяет осуществлять следующие операции:

1. Получать актуальную и подробную информацию о действующем парке вычислительной техники предприятия.
2. Осуществлять автоматизированный процесс миграции рабочих станций пользователей на отечественное ПО:

2.1. миграция с созданием виртуальной машины;

2.2. миграция без создания виртуальной машины;

2.3. миграция с двойной загрузкой.

1. Управлять гибридной инфраструктурой по окончании процесса миграции:

3.1. устанавливать ПО,

3.2. добавлять сертификаты,

3.3. управлять локальными пользователями,

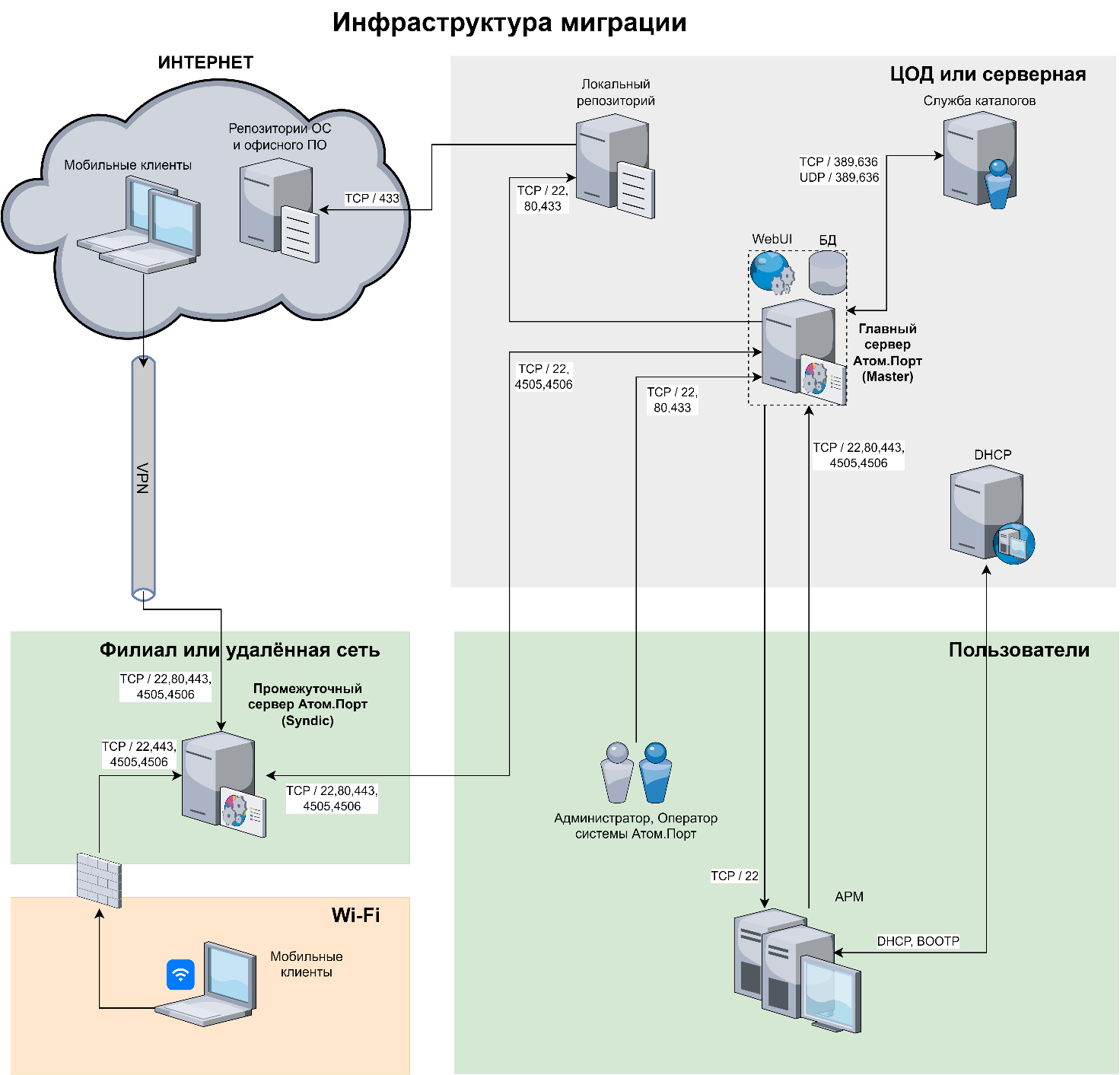
3.4. подключать печатно-копировальное оборудование.

## Условия применения

### Описание типовой инфраструктуры миграции

На рисунке Рисунок 1 представлена схема типовой инфраструктуры миграции для локальной вычислительной сети предприятия с доступом в Интернет, имеющей в своём составе доверенные пользовательские сети и недоверенные сегменты (беспроводную сеть Wi-Fi и пр.).

На схеме указаны номера портов TCP и UDP, используемых сетевыми службами компонентов Программы.



**Рисунок 1 – Схема типовой инфраструктуры миграции**

### Требования к серверу Программы «Атом.Порт»

Требования к аппаратному обеспечению сервера Программы «Атом.Порт» приведены в таблице Таблица 1.

**Таблица 1 – Требования к аппаратному обеспечению сервера**

| **№** | **Параметр** | **Минимальное значение** | **Рекомендуемое значение** |
| --- | --- | --- | --- |
|  | Архитектура процессора | x86\_64 | x86\_64 |
|  | Тактовая частота процессора, ГГц | 1.8 | не менее 2 |
|  | Количество ядер процессора, шт. | 4 | 8 |
|  | Объем оперативной памяти, ГБ | 8 | 16 |
|  | Доступное свободное место на накопителе на жестких магнитных дисках или твердотельном накопителе, Гбайт | 50 | 200 |
|  | Пропускная способность сетевого интерфейса, Мбит/с | 100 | 1000 |

Для хранения резервных копий пользовательских данных и образов дисков с ОС Windows необходимо наличие дополнительного раздела достаточной ёмкости на локальном диске сервера или в автономном хранилище с доступом по протоколу SSH.

Для сетевого интерфейса сервера должен быть выделен один IP-адрес в локальной сети.

Для установки программного обеспечения на сервер используются образы:

1. Образ ПО Сlonezilla – свободного программного обеспечения для клонирования дисков, с помощью которого выполняется развёртывание серверных компонентов ПО Программы.

Образ размещён по ссылке:

**https://clonezilla.org/downloads/download.php?branch=stable**

Для скачивания необходимо выбрать формат **iso**.

1. Образ диска с Программой (формат **iso**).

Образ размещён по ссылке:

**https://cloud.charon.su/s/dLDMf2BcYKooogi**

Порядок установки серверных компонентов ПО Программы описан в разделе 3.1 настоящей инструкции.

### Требования к рабочим станциям

Требования к аппаратному обеспечению рабочих станций приведены в таблице Таблица 2.

**Таблица 2 – Требования к аппаратному обеспечению рабочих станций**

| **№** | **Параметр** | **Без создания**  **виртуальной машины** | | **С созданием**  **виртуальной машины** | |
| --- | --- | --- | --- | --- | --- |
| **Минимальное значение** | **Рекомендуемое значение** | **Минимальное значение** | **Рекомендуемое значение** |
|  | Архитектура процессора | x86\_64 | x86\_64 | x86\_64 | x86\_64 |
|  | Тактовая частота процессора, ГГц | 1.2 | 1.2 | 1.8 | 2 |
|  | Количество ядер процессора, шт. | 2 | 2 | 4 | 4 |
|  | Объем оперативной памяти, ГБ | 2 | 4 | 8 | 8 |
|  | Доступное свободное место на накопителе на жестких магнитных дисках или твердотельном накопителе, Гбайт | 20 | 50 | 100 | 200 |
|  | Операционная система | Windows 7 / 8 / 8.1 / 10 | Windows 7 / 8 / 8.1 / 10 | Windows 7 / 8 / 8.1 / 10 | Windows 7 / 8 / 8.1 / 10 |

В BIOS рабочих станций должен быть отключён режим загрузки Secure Boot.

В BIOS рабочих станций должна быть включена виртуализация (Virtualization, VT-x, AMD-V, SVM, Vanderpool, Intel VT-d, AMD IOMMU).

На рабочих станциях не должно быть шифрованных, сжатых и динамических томов.

Порядок установки Программы на рабочие станции и порядок настройки антивирусного ПО описаны в разделе 3.2 настоящей инструкции.

### Требования к сетевой инфраструктуре

#### Общие требования

Для ввода рабочей станции в домен после перевода на использование отечественной ОС необходимо наличие сетевой доступности контроллеров домена.

Должно отсутствовать клиентское оборудование, подключённое к рабочей станции в режиме моста (например, IP-телефоны).

Сетевые коммутаторы должны позволять использование нескольких клиентских MAC-адресов на одном физическом интерфейсе.

Для обеспечения работоспособности функции отслеживания онлайн-статуса рабочей станции при организации сетевого взаимодействия между сервером и рабочей станцией не должно применяться преобразование сетевых адресов (NAT).

Для выполнения работ по миграции и обслуживанию к серверу управления миграцией должен быть организован внешний доступ при помощи технологии VPN. Доступ может быть организован средствами сервера управления миграцией в случае согласования соответствующих разрешающих правил сетевого доступа.

Ключевое влияние на скорость процессов миграции оказывает скорость обмена данными между рабочей станцией, с одной стороны, и сервером управления миграцией и файловым хранилищем – с другой стороны.

Основными факторами, определяющими скорость обмена, являются:

* пропускная способность дисковых подсистем рабочих станций, сервера управления миграцией и хранилища;
* пропускная способность сегментов сети между рабочей станцией и сервером управления миграцией, рабочей станцией и файловым хранилищем, включая сетевые интерфейсы сервера, хранилища и рабочей станции, а также всё коммутационное оборудование, образующее соответствующий сегмент сети.

В качестве правила расчёта необходимой пропускной способности следует принять, что 100 Мбит/c пропускной способности необходимо на каждые три рабочие станции, одновременно участвующие в процессах миграции.

#### Настройка сервера DHCP

Для рабочих станций, получающих сетевые параметры по протоколу DHCP, необходимо выполнение следующих условий:

* рабочие станции, переводимые на отечественную ОС, должны быть объединены в один широковещательный домен для обеспечения корректного функционирования сервисов, предоставляемых сервером управления миграцией;
* в случае распределения рабочих станций, переводимых на отечественную ОС, и сервера управления миграцией по разным широковещательным доменам, на коммутационном оборудовании Заказчика должна быть настроена пересылка широковещательных UDP-пакетов, в том числе, пересылка DHCP-запросов (Relay Option 82 по стандарту RFC 3046);
* пул IP-адресов сервера DHCP должен быть достаточным для выдачи всем рабочим станциям и создаваемым виртуальным машинам.

#### Настройка антивирусных систем и систем предотвращения вторжений

Имена и полные пути файлов, номера портов TCP и UDP, используемых компонентами Программы, должны быть добавлены в списки исключений систем защиты информации от несанкционированного доступа и антивирусных систем, используемых на рабочих станциях.

##### Пример настройки исключений антивирусных продуктов Dr.WEB

1. Открыть **«Dr.WEB →Центр безопасности → Превентивная защита →Поведенческий анализ»**, перейти на вкладку **«Доступ приложений»**.

Добавить новое правило: указать приложение **„C:\Program Files\Salt Project\Salt\bin\python.exe “**, отметить флажок **«Разрешить»** для объекта **«Файл HOSTS»**, нажать **«ОК»** (Рисунок 2).

Изображение выглядит как текст, снимок экрана, число, Параллельный

Автоматически созданное описание

**Рисунок 2 – Добавление правила для приложения python.exe**

1. Добавить новое правило: указать приложение **„C:\salt\opt\grub2\grub-install.exe“**, отметить флажок **«Разрешать»** для объекта **«Низкоуровневый доступ к диску»**, нажать **«ОК»** (Рисунок 3).

Изображение выглядит как текст, снимок экрана, число, Параллельный

Автоматически созданное описание

**Рисунок 3 – Добавление правила для приложения grub-install.exe**

1. В окне правил поведенческого анализа отображаются добавленные правила (Рисунок 4).

Изображение выглядит как текст, снимок экрана, Шрифт, программное обеспечение

Автоматически созданное описание

**Рисунок 4 – Правила доступа приложений**

##### Пример настройки исключений антивирусных продуктов Касперского

1. Открыть **«Kaspersky →Настройка → Угрозы и исключения → Настроить исключения»**.

Добавить новое правило: в поле **«Файл или папка»** указать **„C:\Program Files\Salt Project\Salt\bin\python.exe “**, отметить в компонентах защиты **«Предотвращение вторжений»**, статус **«Активно»**, нажать **«ОК»** (Рисунок 5).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

**Рисунок 5 – Добавление исключения для приложения python.exe**

1. Добавить новое правило: в поле **«Файл или папка»** указать **„C:\salt\opt\grub2\grub-install.exe“**, отметить в компонентах защиты **«Предотвращение вторжений»**, статус **«Активно»**, нажать **«ОК»** (Рисунок 6).

Изображение выглядит как текст, снимок экрана, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

**Рисунок 6 – Добавление исключения для приложения grub-install.exe**

1. В окне исключений отображаются добавленные исключения (Рисунок 7).

Изображение выглядит как снимок экрана, текст, программное обеспечение, Мультимедийное программное обеспечение

Автоматически созданное описание

**Рисунок 7 – Добавленные исключения**

# Структура программы

Структура Программы и схема взаимодействия компонентов представлены на рисунке Рисунок 8.

Изображение выглядит как текст, диаграмма, снимок экрана, Параллельный

Автоматически созданное описание

**Рисунок 8 – Структура Программы**

Службы и их функции, подготавливаемые в ходе установки ПО перечислены в таблице Таблица 3.

**Таблица 3 – Службы и их назначение**

| Имя службы | Назначение | Примечание |
| --- | --- | --- |
| celery | Распределённая асинхронная очередь задач | Обеспечивает запуск заданий синхронно и асинхронно, по расписанию, вложенные задания и т.д. |
| runner.py | Запуск команд SaltStack |  |
| sniffer.py | Отслеживание событий SaltStack |  |
| nginx | Веб-сервер | Публикует пользовательский интерфейс, обеспечивает взаимодействие с командной строкой администратора миньона на рабочей станции. |
| uvicorn | Асинхронный сервер приложений |  |
| redis | Сервер Redis | Резидентная система управления базами данных класса NoSQL с открытым исходным кодом, работающая со структурами данных типа «ключ — значение». Используется для реализации брокера сообщений модуля Celery |
| salt-master | Сервер SaltStack | Система управления конфигурацией, включающая серверный компонент salt-master и клиенты salt-minion |
| postgresql | СУБД PostgreSQL |  |

# Настройка программы

## Установка серверных компонентов Программы

### Установка сервера на виртуальную машину

1. Подключить образ ПО Clonezilla к виртуальной машине.
2. Подключить образ диска сервера Программы к виртуальной машине для обеспечения доступа к нему из ПО Clonezilla.
3. Выполнить загрузку виртуальной машины с использованием образа ПО Clonezilla.
4. Выбрать язык — **русский**.
5. Оставить раскладку по умолчанию — **US**.
6. В диалоговом окне выбрать пункт:

**Enter\_shell — Войти в командную строку**

1. В командной строке ввести команду:

$ sudo blkid -L ATOMPORT



**Рисунок 9 – Монтирование диска с данными**

1. В выводе команды будет указано устройство, на котором находится образ Программы. В данном примере это /dev/sr1. Далее ввести команду подключения устройства:

$ sudo mount /dev/sr1 /home/partimag/

(см. Рисунок 9).

1. Ввести команду:

$ exit

1. Выбрать пункт:

**Start\_Clonezilla — Запуск Clonezilla**

1. Выбрать пункт:

**device-image — работать с дисками или разделами, используя образы**

1. Выбрать пункт:

**skip — использовать существующий /home/partimag...**

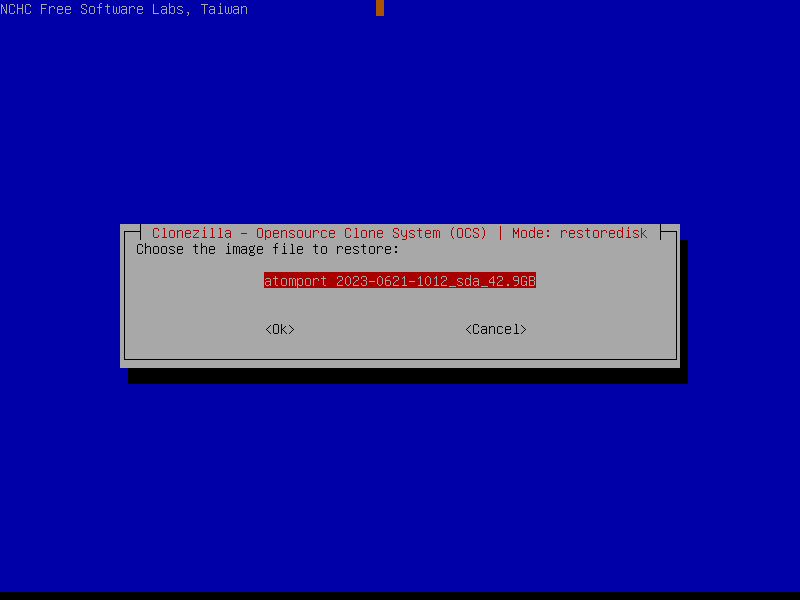
1. Нажать**“Enter”** для продолжения…
2. Выбрать пункт:

**Expert — экспертный уровень…**

1. Выбрать пункт:

**restore\_disk — Восстановить\_образ\_на\_локальный\_диск**

1. Выбрать образ диска сервера **atomport**



**Рисунок 10 – Выбор образа для установки**

1. Выбрать целевой диск — диск, на который будут установлены серверные компоненты Программы.
2. На 1-м экране («Установка дополнительных параметров»), ничего не меняя, нажать **“<OK>”**.
3. На 2-м экране («Установка дополнительных параметров») выбрать пункт:

**-k1 Создать таблицу разделов пропорционально**

1. Выбрать пункт:

**-scr Нет, пропустить проверку до восстановления**

1. Выбрать пункт:

**-p choose…**

1. Нажать **“Enter”** для продолжения.
2. На запрос внести изменения и продолжить ввести **“Y”** и нажать **“Enter”**.
3. Ждать завершения процесса.
4. Нажать **“Enter”** для продолжения.
5. Выбрать пункт:

**reboot — Перезагрузка**

1. После загрузки Программы необходимо указать актуальные значения IP-адресов сервера, шлюза по умолчанию и сервера DNS в файлах:

/etc/network/interfaces, /etc/resolv.conf согласно инструкции:

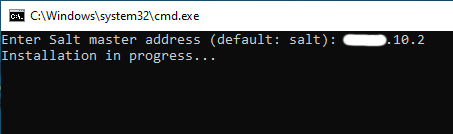
**https://wiki.astralinux.ru/pages/viewpage.action?pageId=3277370#id-НастройкасетевыхподключенийвAstraLinux-Сетевыеинтерфейсывстатичныхсетях**

## Установка клиентских компонентов Программы

### Установка клиента с помощью пакетного файла

1. Для установки клиентских компонентов Программы в «тихом» режиме запустить файл install.bat, который запустит инсталлятор клиента, соответствующий разрядности ОС.

На запрос **„Enter Salt master address (default: salt):“** ввести выделенный IP‑адрес сервера.



**Рисунок 11 – Запуск инсталлятора клиента Программы**

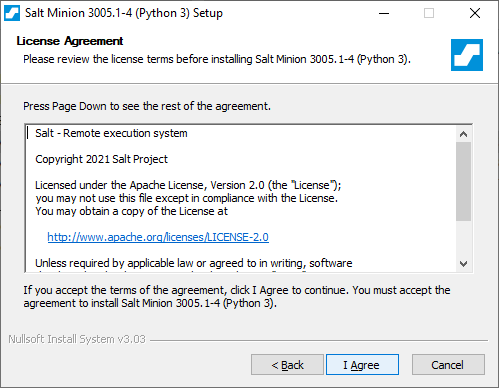
### Установка клиента в интерактивном режиме

1. Для установки клиента Программы в интерактивном режиме запустить **exe**‑файл инсталлятора, соответствующий разрядности ОС, без указания параметров запуска.
2. Нажать **“Next >”** в стартовом окне инсталлятора (Рисунок 12)



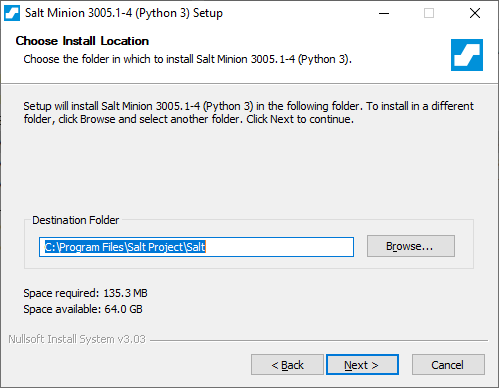
**Рисунок 12 – Стартовое окно инсталлятора службы salt-minion**

1. Нажать **“I Agree”** в окне лицензионного соглашения (Рисунок 13).



**Рисунок 13 – Окно лицензионного соглашения**

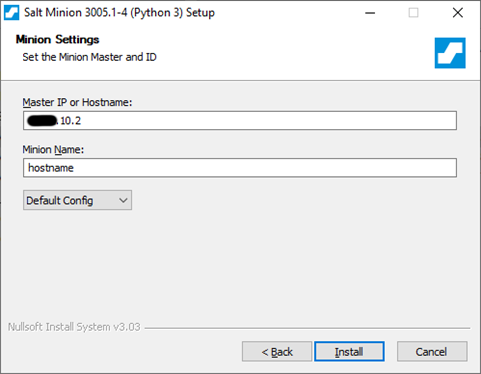
1. Указать путь к папке инсталляции клиента (Рисунок 14).



**Рисунок 14 – Окно установки папки назначения**

1. В окне установки параметров службы salt-minion в первом поле указать выделенный IP‑адрес сервера, значения **Minion Name: hostname** и **Default config** оставить без изменения (Рисунок 15).

Нажать **“Install”** и дождаться окончания процесса установки клиента.



**Рисунок 15 – Окно установки параметров службы salt-minion**

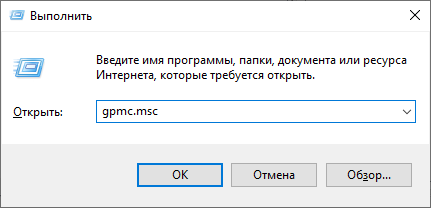
1. Нажать **“Finish”** в окне завершения установки службы salt-minion (Рисунок 16).



**Рисунок 16 – Окно завершения установки службы salt-minion**

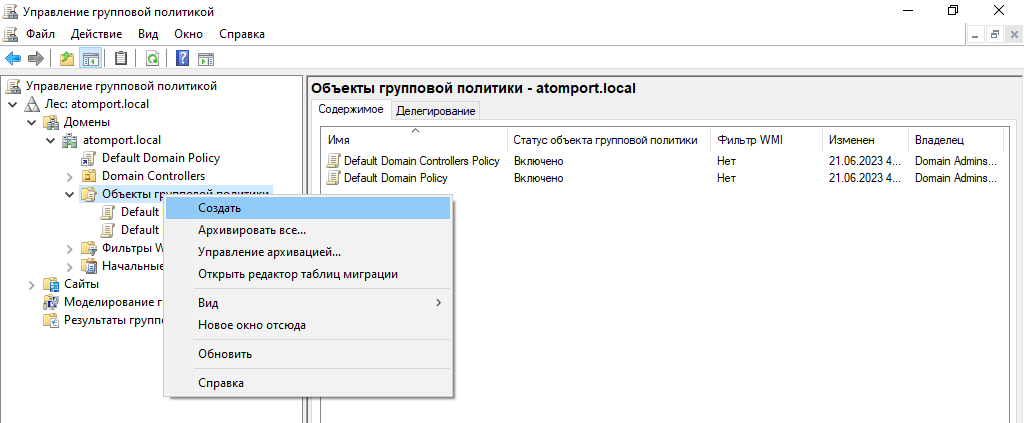
### Установка клиента с помощью групповых политик Microsoft AD

1. В меню **«Пуск»** выбрать пункт **«Администрирование / Управление групповой политикой»** либо выбрать пункт **«Выполнить»** (Рисунок 17).



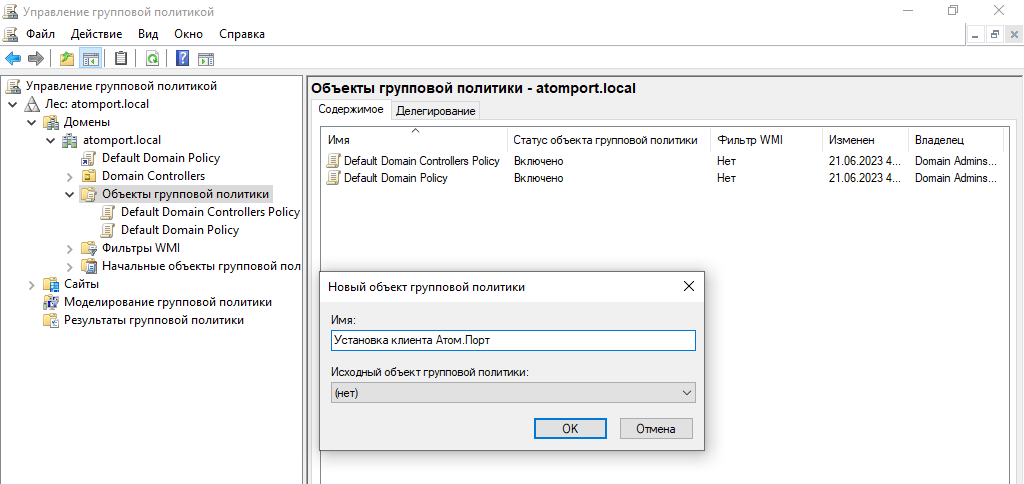
**Рисунок 17 – Запуск оснастки управления групповой политикой**

1. В дереве объектов домена кликнуть правой кнопкой мыши на узле **«Объекты групповой политики»**, выбрать пункт **«Создать»** (Рисунок 18).



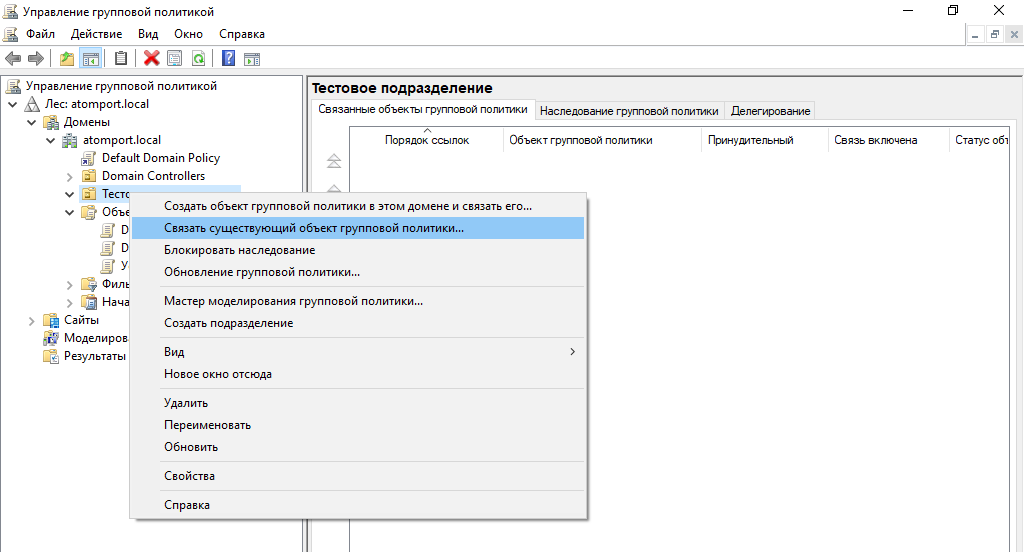
**Рисунок 18 – Создание объекта групповой политики**

1. В диалоговом окне ввести наименование нового объекта групповой политики и нажать **«ОК»**. В данном примере объект групповой политики называется **«Установка клиента Атом.Порт»** (Рисунок 19).



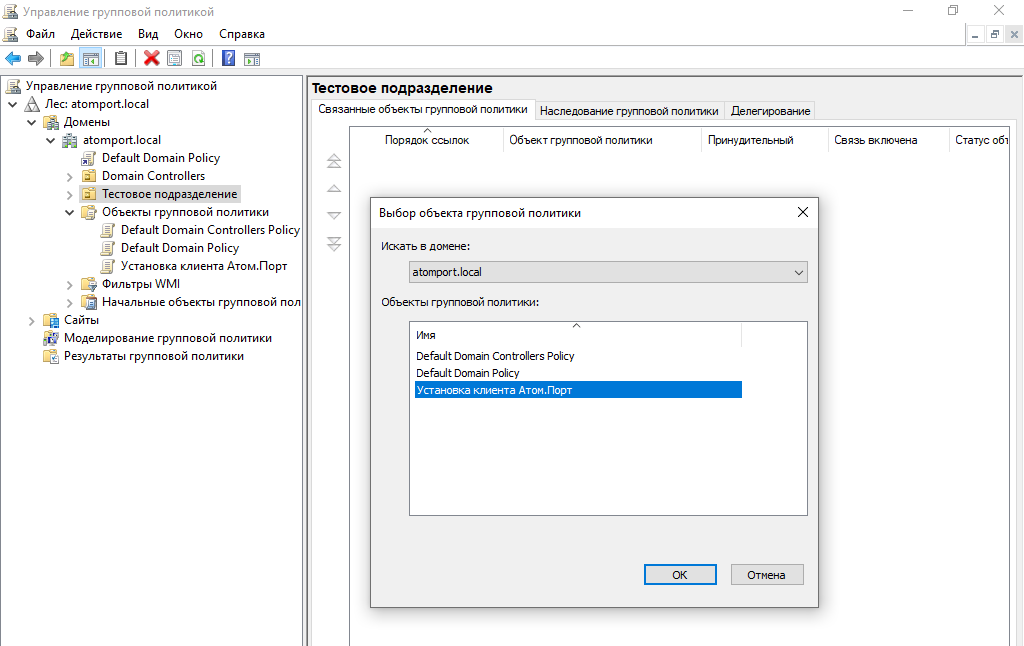
**Рисунок 19 – Ввод наименования нового объекта групповой политики**

1. В дереве объектов домена кликнуть правой кнопкой мыши на нужном Organizational Unit (в данном примере – **«Тестовое подразделение»**), выбрать пункт **«Связать существующий объект групповой политики»** (Рисунок 20).



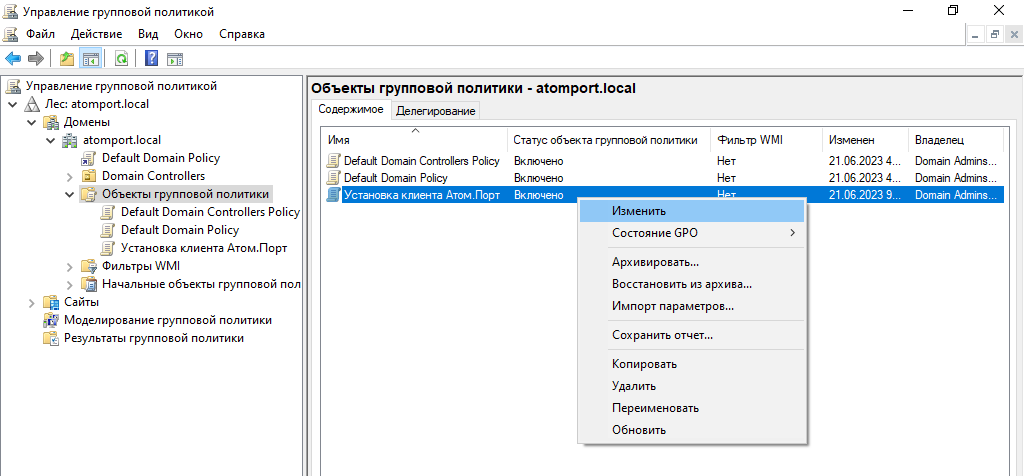
**Рисунок 20 – Создание связи Organizational Unit с объектом групповой политики**

1. В окне выбора объекта групповой политики выбрать объект **«Установка клиента Атом.Порт»**.



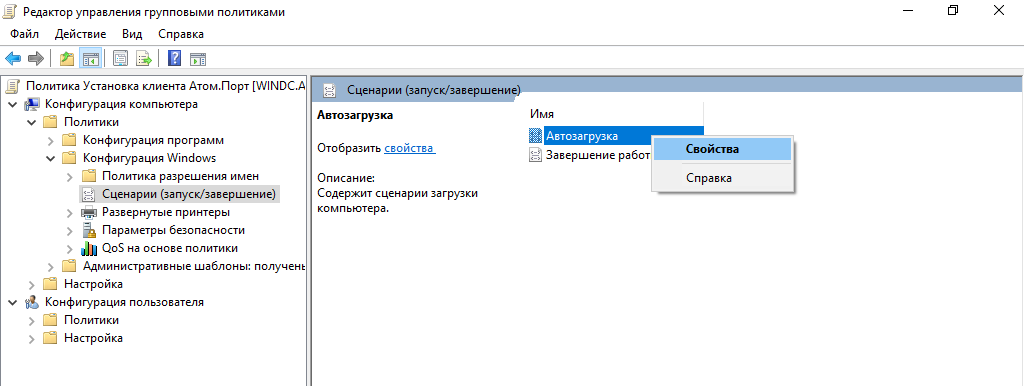
**Рисунок 21 – Выбор объекта групповой политики для связи с Organizational Unit**

1. В списке объектов групповой политики домена кликнуть правой кнопкой мыши на объекте **«Установка клиента Атом.Порт»**, выбрать пункт **«изменить»** (Рисунок 22).



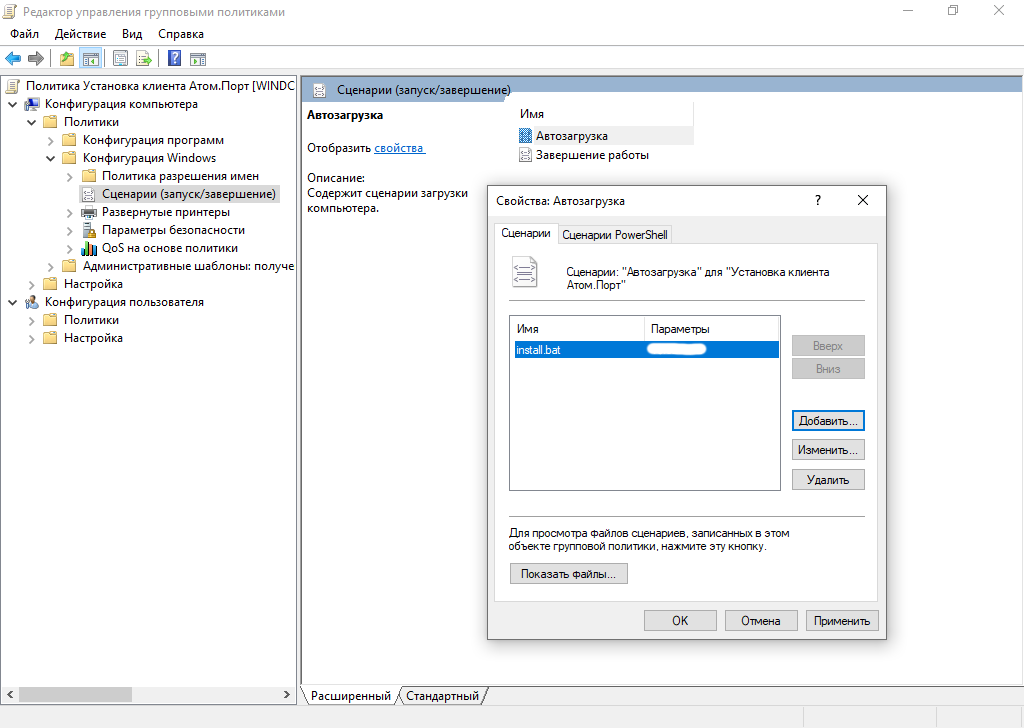
**Рисунок 22 – Изменение объекта групповой политики**

1. В открывшемся окне редактора управления групповыми политиками в узле **«Конфигурация компьютера»**, **«Конфигурация Windows»** выбрать пункт **«Сценарии»** (Рисунок 23).
2. В окне со списком сценариев кликнуть правой кнопкой мыши на сценарии **«Автозагрузка»**, выбрать пункт **«Свойства»** (Рисунок 23).



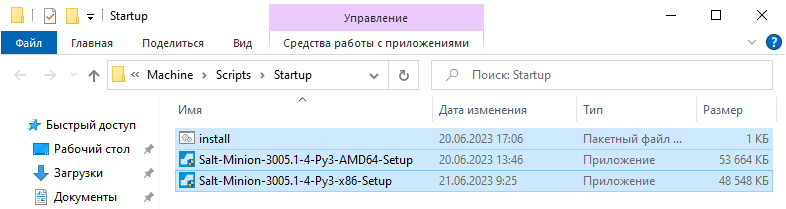
**Рисунок 23 – Изменение свойств сценария автозагрузки**

1. В открывшемся окне свойств сценария автозагрузки на вкладке **«Сценарии»** нажать кнопку **«Показать файлы»** (Рисунок 24).



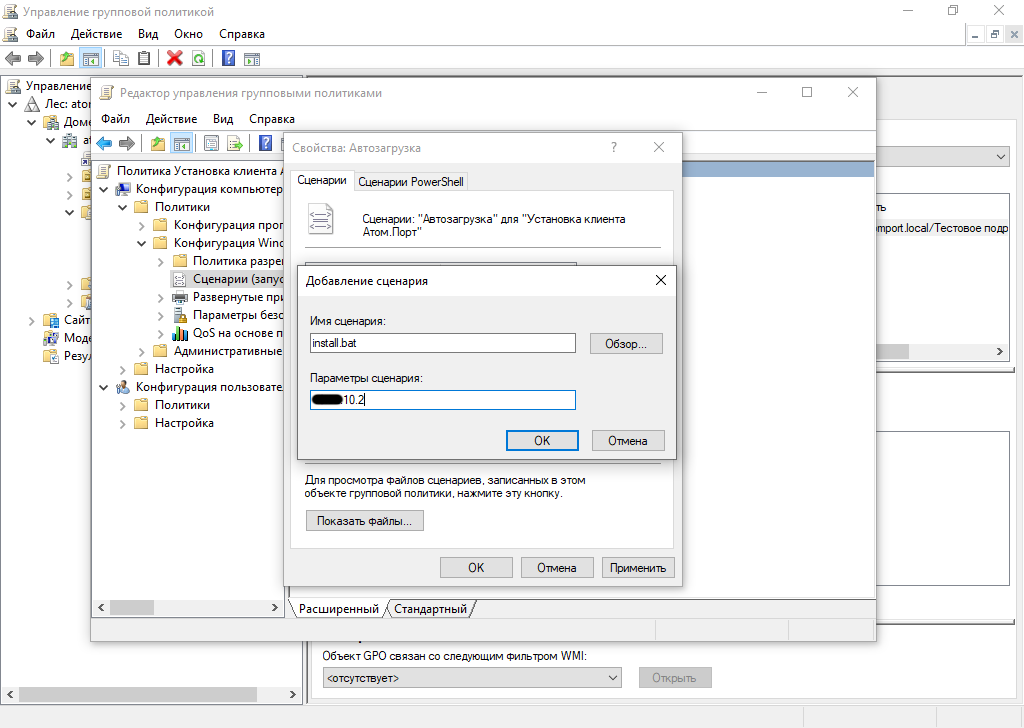
**Рисунок 24 – Свойства сценария автозагрузки**

1. В папку сценария автозагрузки, открывшуюся в проводнике Windows, скопировать файл install.bat и **exe**‑файлы инсталляторов для ОС Windows 32- и 64-разрядной архитектуры (Рисунок 25).



**Рисунок 25 – Копирование файлов в папку сценария автозагрузки**

1. Закрыть проводник и нажать кнопку **«Добавить»** на вкладке **«Сценарии»** окна свойств сценария автозагрузки (Рисунок 24).
2. Ввести имя **install.bat** и значение параметра – выделенный IP-адрес сервера и нажать **«ОК»** (Рисунок 26).



**Рисунок 26 – Ввод параметров сценария автозагрузки**

# Проверка программы

## Мониторинг работы серверных компонентов Программы

### Системные процессы

Ядро Программы функционирует в виде множества процессов, осуществляющих получение, обработку и хранение данных от АРМ и пользователей Программы, управление конфигурациями АРМ и взаимодействие между функциональными модулями Программы.

Проверить состояние процессов ядра Программы можно с помощью команды:

# systemctl list-units –all \

charon-\*.service \

postgresql.service \

nginx.service \

salt-\*.service \

redis-server.service

Пример вывода:

UNIT LOAD ACTIVE SUB DESCRIPTION

charon-celery-beat.service loaded active running Charon system Celery beat scheduler

charon-celery-flower.service loaded active running Flower Celery Service

charon-celery-worker@default.service loaded active running Charon system Celery default worker

charon-celery-worker@process.service loaded active running Charon system Celery process worker

charon-process-rule-runner.service loaded active running Charon system process rule runner

charon-process-runner.service loaded active running Charon system process runner

charon-remote-access-watcher.service loaded active running Charon system VNC watcher

charon-sniffer.service loaded active running Charon system bus sniffer

charon-uvicorn.service loaded active running Charon async backend

nginx.service loaded active running A high performance web server and a reverse proxy server

postgresql.service loaded active exited PostgreSQL RDBMS

redis-server.service loaded active running Advanced key-value store

salt-master.service loaded active running The Salt Master Server

salt-minion.service loaded active running The Salt Minion

LOAD = Reflects whether the unit definition was properly loaded.

ACTIVE = The high-level unit activation state, i.e. generalization of SUB.

SUB = The low-level unit activation state, values depend on unit type.

14 loaded units listed.

To show all installed unit files use 'systemctl list-unit-files'.

Проверить доступность клиентов Программы можно с помощью команды:

salt '\*' test.ping.

В выводе команды должны отображаться результаты вида:

<id клиента>:

True

для всех подключённых клиентов.

### Проверка работоспособности Программы при помощи файлов журналов

В таблице Таблица 4 представлен перечень процессов и исполняемых файлов серверных компонентов Программы с указанием формируемых ими файлов журналов.

**Таблица 4 – Серверные компоненты Программы**

| **№** | **Имя службы** | **Назначение** | **Файлы журналов** |
| --- | --- | --- | --- |
|  | charon-celery-beat  charon-celery-flower  charon-celery-worker | Сервер асинхронной очереди задач | /var/log/syslog  # journalctl -u charon-celery\*.service |
|  | charon-process-rule-runner  charon-process-runner | Запуск команд SaltStack | /var/log/syslog  # journalctl -u charon-process\*.service  /var/log/charon/charon\_runner.log  /var/log/charon/charon\_rule\_runner.log |
|  | charon-remote-access-watcher |  | # journalctl -u charon-remote-access-watcher.service  /var/log/charon/remote\_access\_watcher.log |
|  | iperf3 |  | /var/log/iperf3.log |
|  | nginx | Веб-сервер | /var/log/nginx/access.log  /var/log/nginx/error.log |
|  | postgres | Сервер СУБД PostgreSQL | /var/log/postgresql/postgresql-14-atomport.log |
|  | pypiserver |  | /var/log/pypiserver.log |
|  | redis-server |  | /var/log/redis/redis-server.log |
|  | salt-master | Сервер системы управления конфигурацией SaltStack | /var/log/salt/master |
|  | salt-minion |  | /var/log/salt/minion |
|  | sniffer | Прослушивание событий SaltStack | /var/log/syslog  # journalctl -u charon-sniffer.service  /var/log/charon/charon\_sniffer.log |
|  | uvicorn | ASGI-сервер | /var/log/syslog  # journalctl -u charon-uvicorn.service |
|  | charon | Создание учётных записей пользователей, загрузка описаний автопроцессов | /var/log/charon/charon\_core.log |
|  | python3 | Интерпретатор CPython для запуска Python-программ | Стандартный каталог |

В файлах журналов не должно быть сообщений о повторяющихся приоритетных ошибках (уровень **«ERROR»** и выше).

## Мониторинг работы клиента Программы

### Мониторинг работы клиента в ОС Windows

Для выявления проблем в работе клиентских компонентов Программы в ОС Linux необходимо:

* убедиться, что клиент Программы установлен – в списке установленных программ должна присутствовать запись **salt minion**;
* убедиться, что клиент Программы запущен – при выполнении в командной строке команды sc query salt-minion должно отобразиться состояние «RUNNING». Пример вывода:

Имя\_службы: salt-minion

Тип : 10 WIN32\_OWN\_PROCESS

Состояние : 4 RUNNING

(STOPPABLE, NOT\_PAUSABLE, ACCEPTS\_SHUTDOWN)

Код\_выхода\_Win32 : 0 (0x0)

Код\_выхода\_службы : 0 (0x0)

Контрольная\_точка : 0x0

Ожидание : 0x0

* убедиться, что есть связь с сервером:
* При выполнении команды ping <IP-адрес сервера Атом.Порт> должно выводиться сообщение об отсутствии потерь пакетов (0% потерь)
* При выполнении команды salt-call test.ping должен выдаваться ответ:

local:

True

* В выводе команды netstat -an | findstr 450 должна присутствовать строка:

<IP-адрес сервера Атом.Порт>:4505 ESTABLESHED

либо

<IP-адрес сервера Атом.Порт>:4506 ESTABLESHED

* убедиться, что архитектура системы и клиента совпадают, для этого запустить:

C:\Program Files\Salt Project\Salt\bin\python.exe.

На экране в 64-разрядных системах должна появиться строка, содержащая текст:

64 bit (AMD64).

### Мониторинг работы клиента в ОС Linux

В таблице Таблица 5 представлен перечень процессов и утилит, выполняемых на АРМ, с указанием формируемых ими файлов журналов.

**Таблица 5 – Процессы, выполняемые на АРМ**

| **№** | **Имя процесса**  **(исполняемого файла)** | **Назначение** | **Файлы журналов** |
| --- | --- | --- | --- |
|  | salt-minion | Служба клиента SaltStack | /var/log/salt/minion |

В файлах журналов не должно быть сообщений о повторяющихся приоритетных ошибках (уровень **«ERROR»** и выше).

### Проверка работоспособности АРМ Администратора Программы

Для проверки работоспособности АРМ администратора Программы необходимо:

* Очистить локальное хранилище браузера и открыть в браузере веб-интерфейс Программы. Должна открыться страница входа в Программу.
* На первый запрос сервер должен вернуть код **«200»**.
* Сообщения, свидетельствующие о проблемах в работе Программы, можно увидеть в консоли отладки JavaScript (в «инструментах разработчика» браузера).