УТВЕРЖДЕН
ЧОГА.300317.32-01-ЛУ

СИСТЕМА УПРАВЛЕНИЯ КОНФИГУРАЦИЯМИ АТОМ.ПОРТ

Руководство системного администратора

ЧОГА.300317.32-01

Листов 17

2021

Инв. № подл.	Подпись и дата	Взам. инв. №	Инв. № дубл.	Подпись и дата

АННОТАЦИЯ

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

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

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

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

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

Структура и оформление настоящего документа соответствует ГОСТ 19.503-79.

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

СОДЕРЖАНИЕ

1. ОБЩИЕ СВЕДЕНИЯ О ПРОГРАММЕ

1.1. Общие сведения

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

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

Система 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.

1.2. Возможности Системы

Система 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.
3. 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.

1.3. Область применения

Система может быть использована государственными и коммерческими средними предприятиями в первую очередь для решения таких задач, как инвентаризация ПО, миграция на отечественное ПО, управление гибридной инфраструктурой рабочими станциями на отечественном ПО.

1.4. Условия применения

1. Система может быть установлена как на выделенный сервер, так и на виртуальную машину под управлением совместимого дистрибутива GNU/Linux.
2. Системе требуется один высокоскоростной сетевой интерфейс. Должен предоставляться сетевой адрес, корректно настроенный DNS-сервер и шлюз с доступом к сети Интернет.
3. Системе должно быть предоставлено достаточное дисковое хранилище, подключенное непосредственно к Серверу, либо предоставляемое по одному из поддерживаемых сетевых протоколов.
4. Сетевой интерфейс Системы должен быть доступен для рабочих станций. Для работоспособности всех функций Системы, сетевые интерфейсы рабочих станций также должны быть доступны для Системы. Сетевой экран должен позволять подключения к ряду предопределённых портов.
5. Система активно взаимодействует с управляемыми рабочими станциями с использованием нескольких сетевых протоколов и должна быть добавлена в разрешающий список системы предотвращения вторжений.

2. СТРУКТУРА ПРОГРАММЫ

Компоненты Системы построены по модульному принципу.

Выделяются следующие основные компоненты:

1. Ядро Системы обеспечивает подключение к рабочим станциям, хранение и обработку данных и взаимодействие модулей Системы.
2. Интерфейс пользователя представляет собой веб-интерфейс, оформленный в виде одностраничного приложения (SPA).
3. Подсистема развёртывания обеспечивает наиболее сложные сценарии конфигурирования рабочих станций, связанные с заменой операционной системы.

Система включает в себя следующие модули:

1. модуль инвентаризации;
2. модуль резервного копирования;
3. модуль конфигураций;
4. модуль управления конфигурациями;
5. модуль интерактивного удалённого управления;
6. модуль создания отчётов;
7. модуль отслеживания подключений.

Структура продукта и схема взаимодействия составных частей представлены на рисунке Рисунок 1.

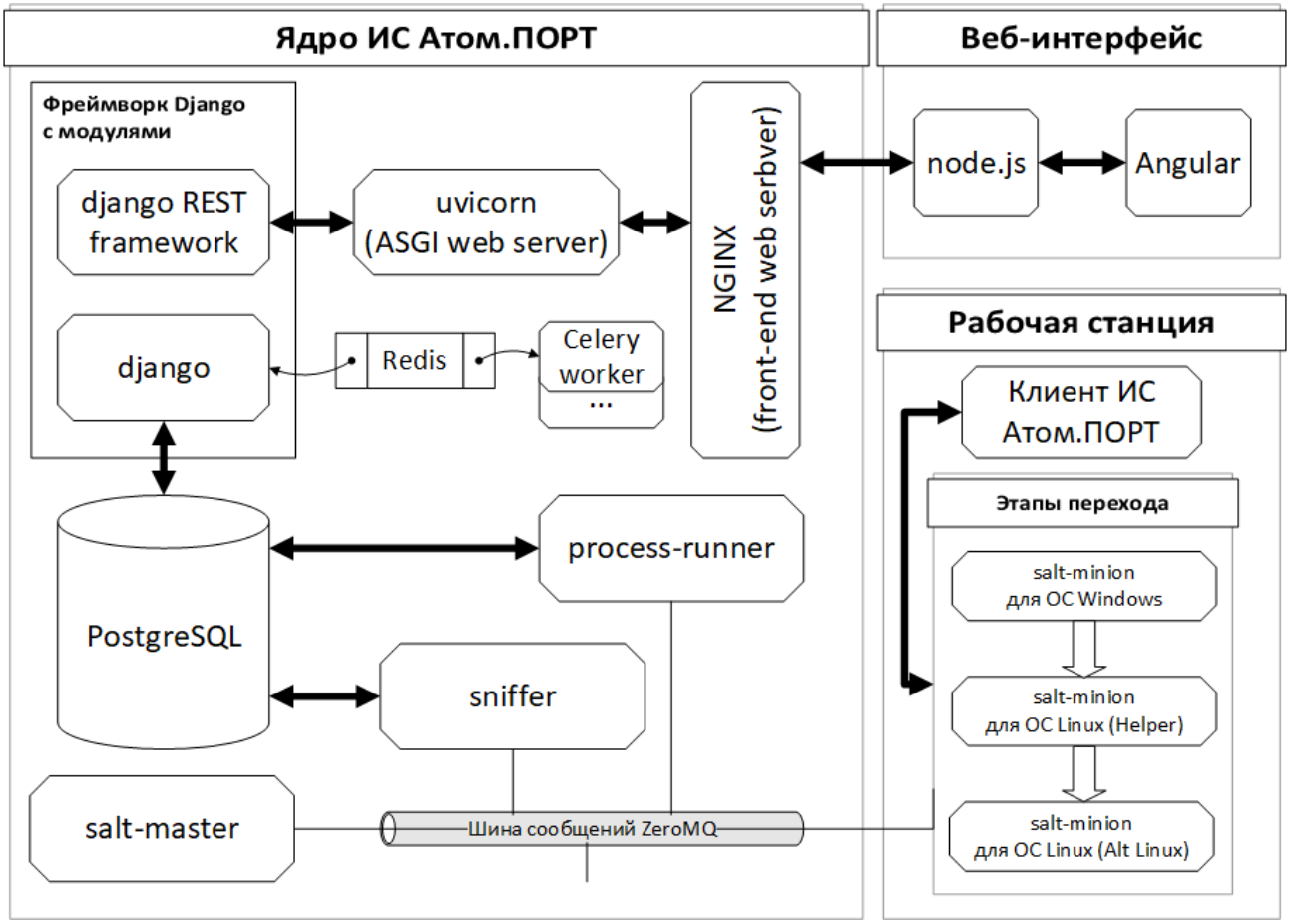

Рисунок 1

Основные компоненты продукта:

- Python — динамический язык программирования, представленный интерпретатором CPython и инфраструктурой модулей;
- SaltStack — система управления конфигурацией, включающая серверный компонент salt-master и клиенты salt-minion;
- PostgreSQL — система управления базами данных;
- 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;
- Celery — асинхронная очередь задач.

Службы и их функции, подготавливаемые в ходе установки ПО перечислены в таблице Таблица 1

Таблица 1 Службы и их назначение

Имя службы	Назначение	Примечание
celery	Распределённая очередь заданий	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.
gunicorn	Сервер приложений	
redis	Сервер Redis	
salt-master	Сервер SaltStack	
postmaster	СУБД PostgreSQL	

Взаимодействие оператора с Системой происходит через веб-интерфейс, разработанный на открытой платформе Angular. Оператору предоставлен необходимый инструментарий для настройки и организации интерфейса под свои нужды и предпочтения. Внешний вид интерфейса приведён на рисунке Рисунок 2.

Система 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:
   - миграция с созданием виртуальной машины;
   - миграция без создания виртуальной машины;
   - миграция с двойной загрузкой.
3. Управлять гибридной инфраструктурой по окончании процесса миграции:
   - устанавливать ПО,
   - добавлять сертификаты,
   - управлять локальными пользователями,

– подключать печатно-копировальное оборудование.

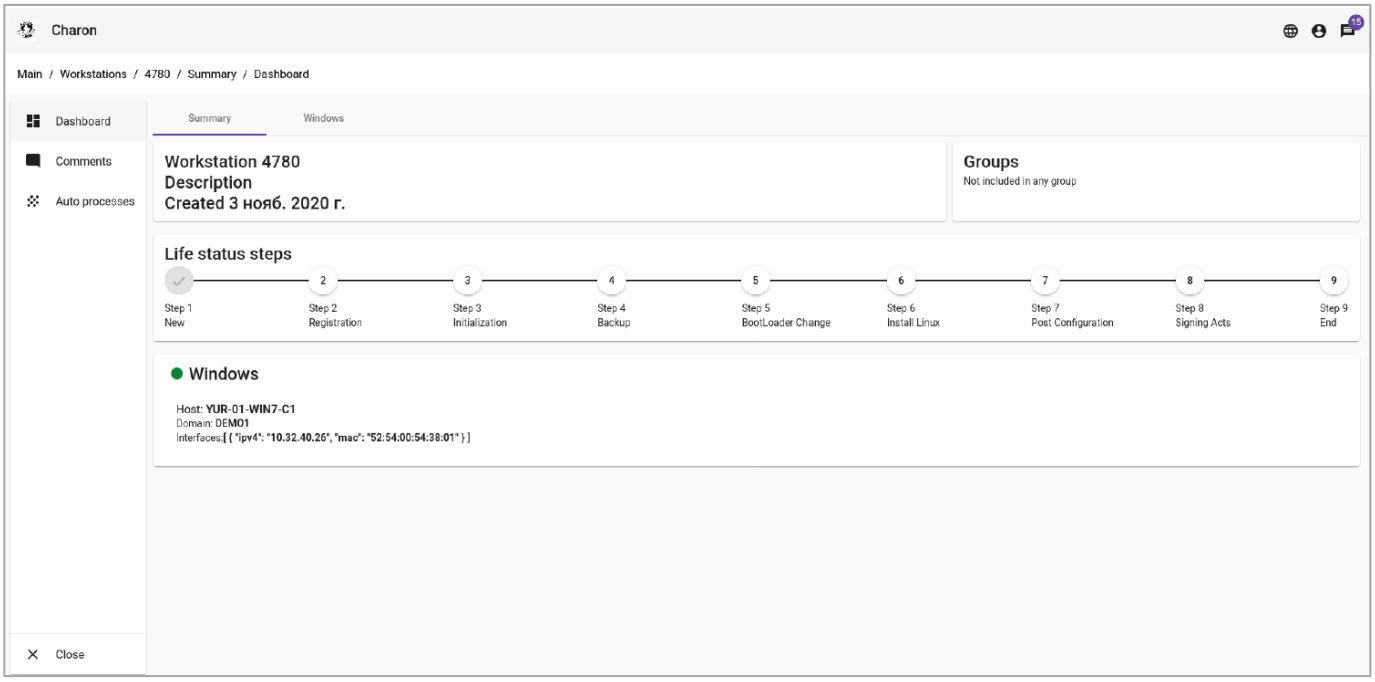

Рисунок 2

3. НАСТРОЙКА ПРОГРАММЫ

3.1. Настройки серверной инфраструктуры

Для перевода АРМ с используемой ОС Windows на ОС Astra Linux развёртывается серверная инфраструктура на виртуальных вычислительных ресурсах VMware.

Серверная инфраструктура предназначена для автоматизированной обработки запросов ТР и хранения данных в необходимом для функционирования ТР объёме.

Минимальные требования к серверу инфраструктуры до 100 рабочих мест:

- ЦП архитектуры x86-64 4 ядра 2 ГГц;
- ОЗУ 4 ГБ;
- Дисковое пространство 80 ГБ;
- Сетевой интерфейс 100 Мбит/сек.

Требования для объёма от 100 до 2000 АРМ:

- ЦП архитектуры x86-64 8 ядер 2 ГГц;
- ОЗУ 8 ГБ;
- Дисковое пространство 80 ГБ;
- Сетевой интерфейс 200 Мбит/сек/

На сервере может быть установлен любой совместимый дистрибутив GNU/Linux.

До начала миграции должны быть разрешены следующие сетевые взаимодействия:

- рабочие станции должны иметь доступ к серверу с использованием TCP портов 22(SSH), 4505, 4506;
- с АРМ оператора Системы должны быть доступны TCP порты сервера 22(SSH), 80(HTTP), 443(HTTPS);
- на рабочих станциях должны быть доступны с АРМ оператора Системы обеспечивающие удалённое управление TCP-порты 22(SSH), 5900, 5901, 3389(RDP) и UDP-порт 3389(RDP).

Рекомендуется обеспечить внешний доступ к серверу с использованием технологии VPN с открытием необходимых для этого сетевых взаимодействий.

Сервер и АРМ должны находиться в одном сетевом сегменте, трансляции адресов (NAT) при сетевом взаимодействии между ними происходить не должно.

В случае создания резервных копий и образов дисков на удалённом хранилище, необходимо предусмотреть дополнительное локальное хранилище на сервере Системы, либо автономное файловое хранилище с доступом по протоколу SSH. Для одновременной миграции с созданием виртуальной машины каждых десяти АРМ рекомендуется хранилище от 1 ТБ. В случае

необходимости ввода рабочих станций в домен после процесса миграции, необходимо наличие доступного рабочим станциям контроллера домена.

Применение сценария, предполагающего создание виртуальной машины с сетевым интерфейсом в режиме моста, дополнительно требует обеспечить наличие доступного рабочим станциям DHCP-сервера с пулом адресов, достаточным по размерам для выдачи рабочим станциям (хостовым машинам) и гостевым виртуальным машинам, развёрнутым на них.

При планировании миграции следует учитывать, что ключевое влияние на скорость и успешность процессов миграции влияет скорость обмена данными рабочих станций с сервером и файловым хранилищем. Основными факторами, ограничивающими эту скорость, являются:

- Пропускная способность дисковых подсистем рабочих станций, сервера и хранилища;
- Пропускная способность сегментов сети между рабочей станцией и сервером, рабочей станцией и хранилищем, включая сетевые интерфейсы сервера, хранилища и рабочей станции, а также всё коммутационное оборудование, образующее сегмент сети, в котором они размещены.

Общее правило, обеспечивающее приемлемую скорость миграции, заключается в том, что на каждые три рабочие станции, одновременно участвующие в процессе миграции, должно приходиться не менее 100 Мбит/с пропускной способности сети.

3.2. Аппаратное обеспечение АРМ

Для функционирования ПО необходима следующая минимальная конфигурация оборудования АРМ, таблица 1.

Таблица 1.

№	Параметр	Рекомендуемое значение	
		Без виртуализации	**С виртуализацией**
1.	Процессор, архитектура	x86_64	x86_64
2.	Процессор, тактовая частота, ГГц, не менее	1.2	2
3.	Объем оперативной памяти, ГБ, не менее	4	8
4.	Накопитель на жестких магнитных дисках (свободное доступное место) ГБ, не менее	50	100
5.	Процессор, количество ядер, не менее	2	4

Материнская плата АРМ при миграции с применением виртуализации должна поддерживать технологию виртуализации. АРМ должен иметь возможность локального или сетевого подключения к печатающему устройству. Колонки, сканер, видеокамера могут подключаться по необходимости.

АРМ должен иметь сетевое подключение к серверной инфраструктуре, описанной в пункте 3.1 настоящего документа.

3.3. Установка программного обеспечения

Для установки программного обеспечения на сервер используется модуль CharonSandboxCreator. Его развёртывание и установка ПО осуществляются с выполнением следующих операций:

1. Установить и настроить ПО виртуализации QEMU/KVM:

```
sudo apt install -y libvirt-clients libvirt-daemon-system
sudo usermod -aG libvirt $(whoami)
newgrp libvirt
```

При настройке виртуализации необходимо дать доступ к подготовленным образам дисков машин. Каждый директорий в пути к хранилищу образов должен быть доступен на чтение и запуск (o+rx).

2. Установить зависимости:

```
sudo apt install -y libvirt-dev python3-pip python3-venv git
```

3. Создать клон репозитория и назначить директорий проекта текущим:

```
git clone https://dev.charon.su/developers/sandbox_creator.git
cd sandbox_creator
```

4. Установить пакет в виртуальное окружение:

```
python3 -m venv env
```

5. Активировать созданное виртуальное окружение:

```
source ./env/bin/activate
```

6. Для предотвращения ошибок при сборке пакета libvirt-python следует установить пакет wheel:

```
pip3 install wheel
```

7. Задать режим «редактирование» устанавливаемого модуля:

```
pip3 install -e
```

Необходимо заметить, что при повторных запусках оболочки виртуальное окружение должно быть активировано для каждой оболочки индивидуально:

```
source ./env/bin/activate
```

Для запуска модуля SandboxCreator следует использовать консольную команду следующего синтаксиса:

```
sandbox_creator [--config FILE] [--download] [--prod] [--debug] [--
help] [--stages STAGES ...]
```

где:

--config: задаёт конфигурационный файл FILE, который может переопределять параметры конфигурации по умолчанию;

--download: требует скачать образы виртуальных машин, если они не будут обнаружены локально;

--prod: инициирует производственную сборку песочницы;

--debug: осуществляет вывод подробных сообщений;

--stages: позволят выбрать этапы процесса развёртывания, по умолчанию — все. Могут быть указаны следующие этапы:

download - загрузка образов виртуальных машин;

deploy - развёртывание виртуальных машин и клиентов;

deploy:install_server -установка сервера;

migrate запуск миграции;

browser_test - тестовые операции.

Например, при установке Charon на предварительно установленную ОС Linux необходимо в конфигурационном файле задать параметр `charon_address`, указав в его значении ip-адрес хоста, а затем запустить програму командой:

```
sandbox_creator --config FILE --stages deploy:install_server
```

Пример содержимого конфигурационного файла:

```
# Имя сервера (будет установлено)
sandbox_name: charon_tmp
# Сетевой адрес подготовленной машины
charon_address: 192.168.0.2
# Данные суперпользователя на подготовленной машине
charon_ssh_username: 'root'
# После установки root можно отключить
charon_ssh_password: 'password'
# Обнулённый список тестовых миньонов
minions: []
```

3.4. Настройка клиентской части

В домене Windows клиентская часть развёртывается с помощью групповых политик. Доменные групповые политики позволяют установить программное обеспечение путём рассылки программного обеспечения компьютеру-члену домена, входящему в группу рассылки. После назначения рассылки ПО оно устанавливается на всех входящих в группу компьютерах при следующем за рассылкой старте компьютера. Если задача рассылки ПО назначена компьютеру, то оно устанавливается независимо от того, какой пользователь авторизовался на компьютере при запуске. Назначение и настройка задачи рассылки программного обеспечения осуществляется с помощью ММС консоли управления групповыми политиками. Запуск консоли продемонстрирован на рисунке Рисунок 3.

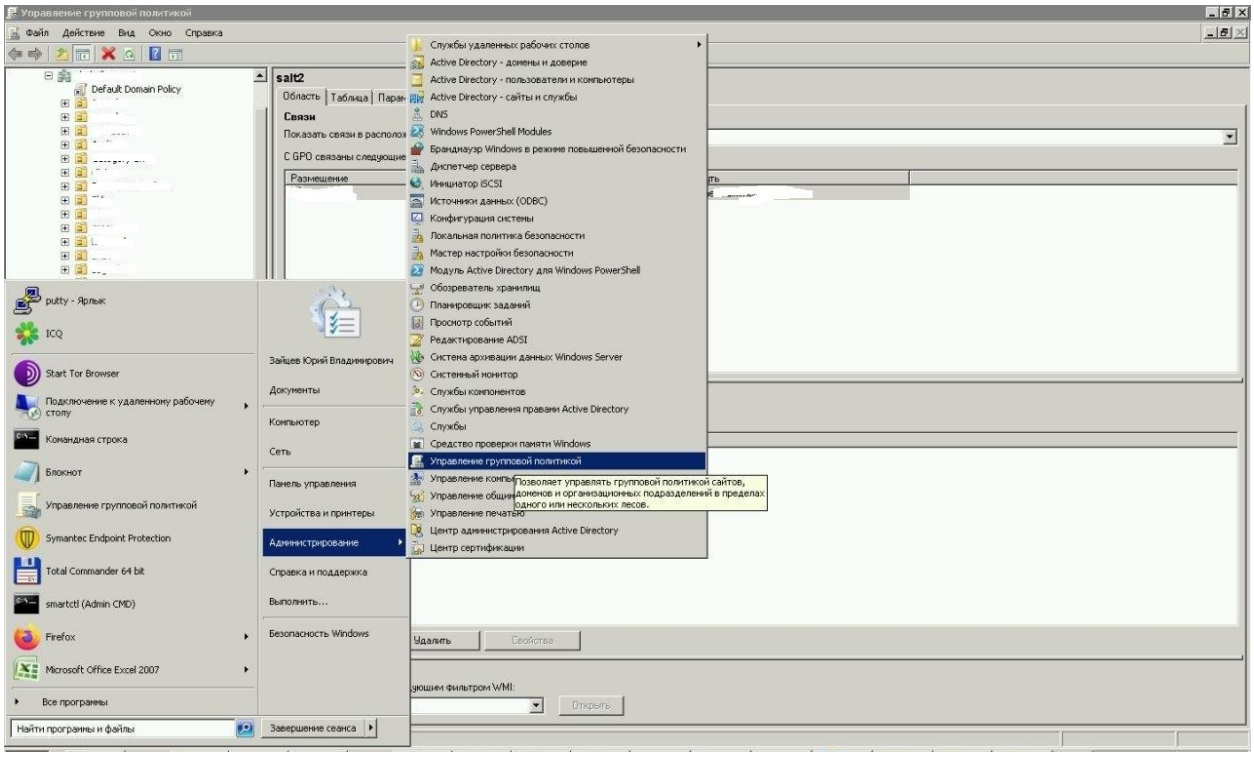
Управление групповой политикой
Файл Действие Вид Окно Справка
Default Domain Policy
salt2
Область Таблица
Связи
Размещение
Службы удаленных рабочих столов
Active Directory - домены и доверие
Active Directory - пользователи и компьютеры
Active Directory - сайты и службы
DNS
Windows PowerShell Modules
Брандмауэр Windows в режиме повышенной безопасности
Диспетчер сервера
Инициатор iSCSI
Источники данных (ODBC)
Конфигурация системы
Локальная политика безопасности
Мастер настройки безопасности
Модуль Active Directory для Windows PowerShell
Обозреватель хранилищ
Планировщик заданий
Просмотр событий
Редактирование ADSI
Система архивации данных Windows Server
Системный монитор
Службы компонентов
Службы управления правами Active Directory
Службы
Средство проверки памяти Windows
Управление групповой политикой
Управление компьютерами
Управление общими папками
Управление печатью
Центр администрирования Active Directory
Центр сертификации
Позволяет управлять групповой политикой сайтов, доменов и организационных подразделений в пределах одного или нескольких лесов.
putty - Ярлык
ICQ
Start Tor Browser
Подключение к удаленному рабочему столу
Командная строка
Блокнот
Управление групповой политикой
Symantec Endpoint Protection
Total Commander 64 bit
smartctl (Admin CMD)
Firefox
Microsoft Office Excel 2007
Все программы
Найти программы и файлы
Завершение сеанса
Зайцев Юрий Владимирович
Документы
Компьютер
Сеть
Панель управления
Устройства и принтеры
Администрирование
Справка и поддержка
Выполнить...
Безопасность Windows
Удалить
Свойства
Открыть

Рисунок 3

4. ПРОВЕРКА ПРОГРАММЫ

По завершении установки необходимо убедиться, что операция прошла корректно. Для этого необходимо запустить команду

```
sandbox_creator --help
```

Если программа работает корректно, будет выведена краткая встроенная справка:

```
usage: sandbox_creator [-h] [--config CONFIG] [--debug] [--disable-
progress-bar] [--download] [--fail-on-minion-error] [--prod] [--
stages [STAGES ...]] [--snapshots] [--truncate-images]

create vm...

optional arguments:
  -h, --help            show this help message and exit
  --config CONFIG       point to overriding config file
  --debug               be verbose
  --disable-progress-bar
                        do not show animated progress bars
  --download            enable download stage: overwrite images from
cloud
  --fail-on-minion-error
                        stop and exit instantly on minion setup or
migration
  --prod                every service will be installed with
production configuration
  --stages [STAGES ...]
                        run only specified stages (download, deploy,
deploy:install_server, migrate, browser_test)
  --snapshots           Create snapshots of virtual machines for
major stages
  --truncate-images     Delete files from image directories which is
not mentioned in config
```

Командой, представленной ниже (вводится одной строкой), можно получить информацию о состоянии служб, обеспечивающих нормальную работу решения:

```
systemctl list-units --all gunicorn.service sniffer.service
process_runner.service 'celery-*' salt-master.service redis.service
postgresql.service nginx.service
```

В ответной выдаче команды все перечисленные компоненты должны быть загружены (“**Loaded**”) и активны (“**Active**”).

Проверка доступности клиентов производится командой

```
salt '*' test.ping
```

В ответной выдаче должны быть представлены идентификаторы всех активных клиентов с признаком наличия связи “**True**”.

ПЕРЕЧЕНЬ ПРИНЯТЫХ СОКРАЩЕНИЙ

АРМ	Автоматизированное рабочее место
ГОСТ	Государственный стандарт России
ОЗУ	Оперативное запоминающее устройство
ОС	Операционная система
ПК	Персональный компьютер
ПО	Программное обеспечение
РС	Рабочая станция
Система	Программа для ЭВМ “Система управления конфигурациями «Атом.Порт»”
ЦП	Центральный процессор

Лист регистрации изменений									
Номера листов (страниц)					Всего листов (страниц) в докум.	№ документа	Входящий № сопроводит. докум. и дата	Подп.	Дата
Изм.	измененных	замененных	новых	аннулированных					