ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«РусБИТех-Астра»

ПРОГРАММНЫЙ КОМПЛЕКС
«ASTRA CONFIGURATION MANAGER»

ВЕРСИЯ 1.0.0 STANDARD

Руководство администратора.
Инструкция по развертыванию и обновлению

(Листов - 94)

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

ACM	-	Astra Configuration Manager
Агент, Агент системы управления, Агент ACM	-	Программный модуль, компонент системы управления ACM, устанавливаемый на компьютер для удаленного управления компьютером со стороны системы управления ACM.
Возможность	-	Разрешение для выполнения операции или набора операций (запись, добавление, удаление и т.д.) с объектами или атрибутами объекта, к которым эти операции применяются.
Директория	-	Логический объект системы ACM для объединения записей компьютеров и/или записей пользователей и применения профилей управления, назначения прав доступа. Директории могут образовывать иерархическую структуру с n-уровнями вложенности. Одна запись компьютера может одновременно находиться только в одной директории.
Домен	-	Область, которая является единицей административной автономии в сети, в составе вышестоящей по иерархии такой области.
Набор возможностей	-	Логический объект системы ACM, представляющий собой преднастроенный (предустановленный системой или настроенный вручную администратором) набор разрешений или операций в системе ACM, который может быть назначен на УЗ пользователя в системе ACM.
Обнаружение ПО	-	Внутренний процесс системы ACM, обработка собранных с компьютеров инвентарных данных и создание связей между управляемым компьютером и ПО на основе имеющихся правил обработки инвентарных данных.
ОС	-	Операционная система.
ПО	-	Программное обеспечение.

Правило обнаружения ПО	-	Логический объект АСМ, правило, включающее тип ПО, способ идентификации ПО, версию ПО и условия, позволяющие определить ПО в системе АСМ.
Профиль установки ОС	-	Управляющий объект АСМ, определяющий комбинацию настроек для автоматизации установки и конфигурирования ОС с использованием системы АСМ.
ПУА	-	Платформа управления агентами - программный модуль в составе АСМ, предназначенный для организации использования технологии Saltstack при управлении компьютером системой АСМ.
Репозиторий	-	Серверная роль системы управления АСМ, предназначенная для хранения пакетов программного обеспечения, а также других файлов и данных, и предоставления доступа со стороны управляемых компьютеров при установке/обновлении ПО и/или установке ОС.
Родительская директория	-	Логический объект системы АСМ, директория, содержащая другие директории. Родительская директория также может содержать записи компьютеров.
Сегмент	-	Логическая единица АСМ, объединяющая серверы управления и подключенные к ним управляемые компьютеры, предназначенная для выделения группы управления в целях оптимизации сетевого трафика и/или снижения нагрузки на управляющие серверы АСМ.
Структура управления	-	Древовидная (иерархическая) структура директорий, внутренний объект системы АСМ.
СЦ	-	Справочный центр системы АСМ.
УЗ	-	Учетная запись.
Управляемый (целевой) компьютер	-	Компьютер, на который установлен агент АСМ, подключенный к системе АСМ, доступный для применения к нему профилей и инструментов удаленного управления.

ALD Pro	-	Программный комплекс на базе ОС Astra Linux для централизованного управления объектами домена организаций различного масштаба.
DHCP	-	Dynamic Host Configuration Protocol - протокол прикладного уровня, позволяющий сетевым устройствам автоматически получать IP адрес и другие параметры, необходимые для работы в сети TCP/IP.
Preseed скрипт	-	Скрипт, содержащий ответы на вопросы и автоматизирующий процесс установки ОС Astra Linux. Является составным компонентом Профиля установки ОС в системе АСМ.
Postinstall скрипт	-	Скрипт, содержащий команды для выполнения непосредственно после установки ОС и позволяющий автоматизировать установку и применение некоторых параметров конфигурации ОС Astra Linux. Является составным компонентом Профиля установки ОС в системе АСМ.
Saltstack	-	Система управления конфигурациями и удалённого выполнения операций.
UEFI	-	Unified Extensible Firmware Interface - низкоуровневое программное обеспечение, предназначенное для инициализации и управления оборудованием компьютера.

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Обозначение и наименование

Наименование программы — «ASTRA CONFIGURATION MANAGER».

Сокращенное наименование программы — ACM, Система, Система ACM.

1.2 Языки программирования

Текст системы ACM написан на следующих языках:

- Python;
- JavaScript.

1.3 Область применения

Областью применения ACM является автоматизация деятельности системных администраторов в рамках эксплуатации ИТ-инфраструктуры на базе ОС Astra Linux.

Средой функционирования ACM является ОС Astra Linux. ACM интегрировано с комплексом средств защиты информации ОС Astra Linux, является прикладным программным обеспечением и не реализует самостоятельно функции защиты информации.

1.4 Требования к квалификации администратора

Администратор выполняет действия по развертыванию и вводу в эксплуатацию ACM.

На администратора возлагается выполнение следующих функций:

- подготовка технических средств;
- установка и конфигурирование системных программных средств.

Для выполнения возложенных функций администратор должен обладать:

- навыками администрирования ОС Astra Linux;
- навыками развертывания ИТ-инфраструктуры;
- навыками администрирования общего и специального программного обеспечения.

1.5 Функциональное назначение

Система ACM предназначена для централизованного управления компьютерами под управлением ОС Astra Linux и использования в организациях различного масштаба.

Система АСМ версии 1.0.0 Standard выполняет следующие функции:

№ п/п	Описание функций
1.	**Управление инфраструктурой Системы:** - создание, редактирование и удаление сегментов управления АСМ; - создание, редактирование и удаление серверов агентов.
2.	**Управление пользователями и их возможностями:** - ведение списка пользователей; - разграничение возможностей пользователей; - управление наборами возможностей пользователей.
3.	**Управление организационной структурой (директориями) компьютеров:** - создание, редактирование и удаление подразделений (директорий) компьютеров; - ведение списка подразделений (директорий) компьютеров; - возможность настройки организационной структуры подразделений (директорий) компьютеров в иерархическом виде; - возможность управления составом компьютеров в директории.
4.	**Управление компьютерами:** - установка агента и подключение управляемого компьютера к системе; - создание, редактирование и удаление записей компьютеров; - ведение списка компьютеров; - возможность экспорта отчета по списку компьютеров в файл; - возможность экспорта отчета по инвентарным данным компьютера в файл.
5.	**Аппаратная инвентаризация:** - возможность сбора инвентарных данных об аппаратной части управляемых компьютеров; - возможность просмотра собранных сведений об аппаратной части управляемых компьютеров.
6.	**Инвентаризация установленного ПО:** - возможность сбора инвентарных данных по программной части

№ п/п	Описание функций
	управляемых компьютеров; - управление правилами выявления ПО на управляемых компьютерах; - возможность просмотра собранных сведений о программной части управляемых компьютеров; - возможность просмотра собранных сведений о пакетах ПО на управляемых компьютерах.
7.	**Учет лицензий:** - выполнение учета лицензий ОС Astra Linux на основе собранных инвентарных данных с управляемых.
8.	**Установка ОС на новом компьютере (bare-metal):** - подготовка и настройка сервера установки ОС по сети; - управление параметрами установки ОС по сети на новом компьютере; - управление скриптами установки, используемыми образами; - выполнение установки ОС по сети.
9.	**Управление пользовательской сессией в веб-браузере:** - возможность входа в Систему через веб-интерфейс; - завершение текущей сессии в веб-интерфейсе Системы; - управление цветовой схемой веб-интерфейса Системы.
10.	**Справочный центр:** - наличие встроенного в Систему справочного центра на русском языке; - возможность доступа к справочному центру из любого компонента Системы.

2 ОПИСАНИЕ АРХИТЕКТУРЫ

АСМ имеет клиент-серверную архитектуру и состоит из следующих компонентов:

- Серверная часть — предназначена для установки на серверное оборудование;
- Клиентская часть — реализована в виде агента, устанавливаемого на все управляемые компьютеры. Агент обеспечивает получение и применение данных централизованного управления, а также сбор и передачу информации о состоянии компьютера и событиях на нем;
- Портал управления — предоставляет пользователю графический веб-интерфейс для доступа к данным и управления системой АСМ, доступный в браузере.

В данном разделе описана архитектура АСМ и приведены возможные конфигурации системы.

2.1 Типовые конфигурации

	Основной сегмент АСМ		Удаленный сегмент АСМ		Количество подключаемых компьютеров клиентов
	Кол-во серверов (физических или виртуальных)	**Выделенные серверы с указанием функциональных ролей АСМ**	**Кол-во серверов (физических или виртуальных)**	**Выделенные серверы с указанием функциональных ролей АСМ**	
Конфигурация минимальная	1	Основной сервер АСМ	Удаленный сегмент не устанавливается		до 500 компьютеров клиентов
Конфигурация распределенная с одним сегментом	3	Основной сервер АСМ, Сервер БД, Сервер брокера АСМ	2 или 1 *	Сервер управления агентами АСМ, *Сервер установки ОС АСМ**	до 1000 компьютеров клиентов
Конфигурация распределенная с двумя и более сегментами	3	Основной сервер АСМ, Сервер БД, Сервер брокера АСМ	2 или 1 *	Сервер управления агентами АСМ, *Сервер установки ОС АСМ**	до 1000 х Количество удаленных сегментов АСМ

** сервер установки ОС не обязателен, если в сегменте не планируется установка ОС по сети*

2.2 Функциональные серверы АСМ

Для возможности сценариев развертывания АСМ с разным набором функций в составе серверной части АСМ выделены функциональные (серверные) роли, необходимые для реализации той или иной функции АСМ:

№ пп	Название серверной роли	Набор сервисов АСМ	Назначение
1	Основной сервер АСМ	- API-шлюз (api-gateway); - сервис портала управления АСМ; - сервис аутентификации и авторизации (acm-auth-service); - сервис управления конфигурациями (acm-configuration-service); - сервис управления инфраструктурой АСМ (acm-infrastructure-service)	Обязательный компонент, обеспечивает выполнение следующих функций: - координация всех функциональных процессов АСМ, - работа с записями компьютеров, - работа со структурой управления (директории), - работа с профилями управления и их назначение на структуру управления, - работа портала управления, - управление входом/выходом пользователей на портал управления и назначения возможностей, - управление, хранение и предоставление доступа ко всем инвентарным данным, собранным с компьютеров клиентов, - обнаружение ПО, - учет лицензий.
2	Север БД	СУБД PostgreSQL и БД основного сервера АСМ: - БД сервиса acm-auth-service - БД сервиса acm-configuration-service; - БД сервиса acm-infrastructure-service.	Обязательный компонент, обеспечивает хранение и управление данных Основного сервера АСМ
3	Сервер брокера	Брокер сообщений RabbitMQ	Обязательный компонент, обеспечивает взаимодействие

№ пп	Название серверной роли	Набор сервисов АСМ	Назначение
	АСМ		серверных компонент (основного сервера АСМ, сервера управления агентами, сервера установки ОС) АСМ
4	Сервер управления агентами АСМ	- Сервис управления агентами (acm-agent-service); - СУБД PostgreSQL с БД agent-service - GIT-сервер - Брокер сообщений RabbitMQ	Требуется для подключения к АСМ управляемых компьютеров. Обязательный компонент в составе «Сегмента АСМ».
5	ПУА (платформа управления агентами)	- Сервис amp-runner - Salt-master	Обеспечивает выполнение управляющих функций на управляемых компьютерах
6	Сервер репозиториев	Центральный сервер репозиториев в основном сегменте: - репозитории ОС Astra Linux для установки ОС по сети. Дополнительный сервер в удаленном сегменте АСМ: - nginx; - репозитории ОС Astra Linux для установки ОС по сети.	Обязателен для развертывания для реализации функций: - управление ПО; - установка и переустановка ОС; - управление конфигурацией компьютера. Обеспечивает хранение и предоставление управляемым компьютерам пакетов ПО и файлов, необходимых для установки/обновления ПО, установки/обновления ОС или других функций управления, требующих пакеты/файлы.
7	Сервер установки ОС АСМ	- Сервис установки ОС по сети (acm-osdeployment-service); - PXE-сервер; - TFTP-сервер; - DHCP-сервис.	Обязателен для развертывания для реализации функций: - установка и переустановка ОС. Обеспечивает выполнение функций установки\ переустановки ОС на управляемых компьютерах по PXE

2.3 Конфигурация минимальная

2.3.1 Общие сведения о конфигурации

Данная конфигурация представляет собой минимальную установку ACM. Рекомендуется использовать конфигурацию в следующих случаях:

- для тестирования и проверки функциональности системы ACM (стендирование, пилотные проекты);
- для обслуживания малого парка компьютеров.
- Сценарий предполагает:
- подключение до 500 управляемых компьютеров;
- использование простой сетевой конфигурации, когда сервер и подключаемые компьютеры клиенты находятся в одной локальной сети.
- отсутствие требований и необходимости использовать решения по отказоустойчивости системы ACM;

Данная конфигурация позволяет реализовать все функции управления ACM Standard v1.0.0, приведенные в разделе « 1.5 Функциональное назначение».

2.3.2 Схема компонент

В минимальной конфигурации все серверные роли ACM устанавливаются на одном физическом или виртуальном сервере. Перечень устанавливаемых серверных ролей приведен в разделе « 2.2 Функциональные серверы ACM».

Схема размещения функциональных серверов представлена на рисунке ниже (Рисунок 1).

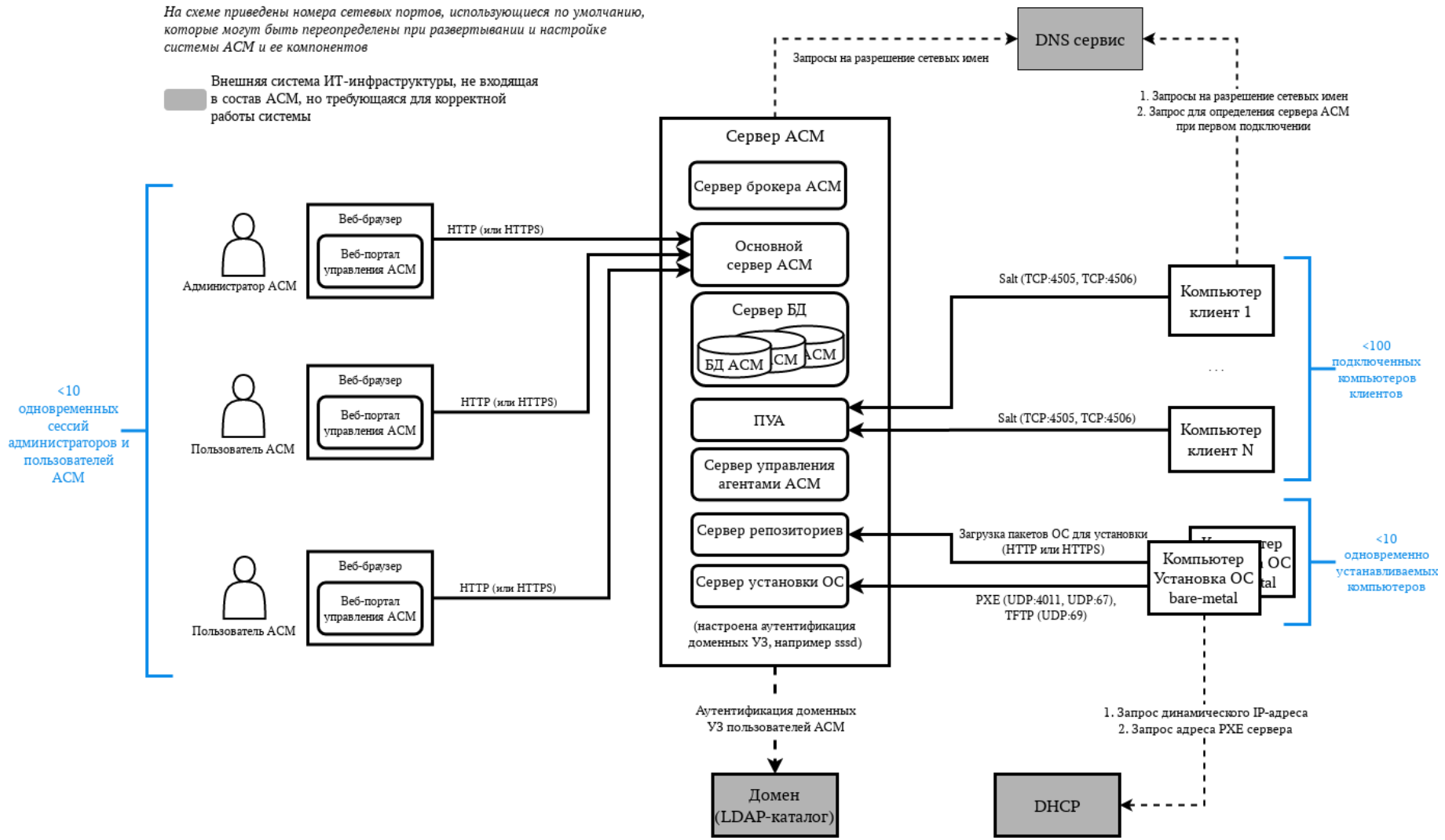

Рисунок 1. Схема компонент для минимальной конфигурации АСМ

2.4 Конфигурация распределенная с одним сегментом

2.4.1 Общие сведения о конфигурации

Конфигурация размещения компонентов АСМ для обслуживания до 1000 компьютеров клиентов с учетом отказоустойчивой схемы хранения данных АСМ. Рекомендуется использовать конфигурацию в следующих случаях:

- использование системы АСМ для обслуживания небольшого парка компьютеров (до 1000 компьютеров клиентов);

Сценарий предполагает:

- развертывание компонентов хранения и передачи данных (СУБД PostgreSQL и Брокер сообщений RabbitMQ) в кластерной конфигурации для обеспечения отказоустойчивости;
- использование в инфраструктуре без сложной распределенной структуры сети (все серверы и компьютеры в одной локальной сети с надежными быстрыми каналами связи, с возможностью сетевого доступа).

Данная конфигурация позволяет реализовать все функции управления ACM Standard v1.0.0, приведенные в разделе « 1.5 Функциональное назначение».

2.4.2 Схема компонент

В данной конфигурации рекомендуется использовать выделенные серверы (физические или виртуальные) для функциональных серверов:

- Сервер АСМ (для размещения функциональных серверов АСМ «Основной сервер АСМ» и «Центральный сервер репозиториев АСМ»);
- Сервер БД (для размещение БД «Основного сервера АСМ»);
- Сервер брокера АСМ (для размещения необходимых компонент «Сервера брокера АСМ»);
- Сервер управления агентами АСМ (для размещения функциональных серверов «Сервер управления агентами АСМ» и «ПУА»);
- Сервер установки ОС АСМ (для размещения функциональных серверов «Сервер установки ОС АСМ» и «Сервер репозиториев»).

Использование выделенных серверов требуется для повышения производительности и организации отказоустойчивых кластеров для «Сервера БД» (используется кластер СУБД PostgreSQL) и «Сервера брокера» (используется кластер RabbitMQ).

Схема размещения функциональных серверов представлена на рисунке ниже (Рисунок 2).

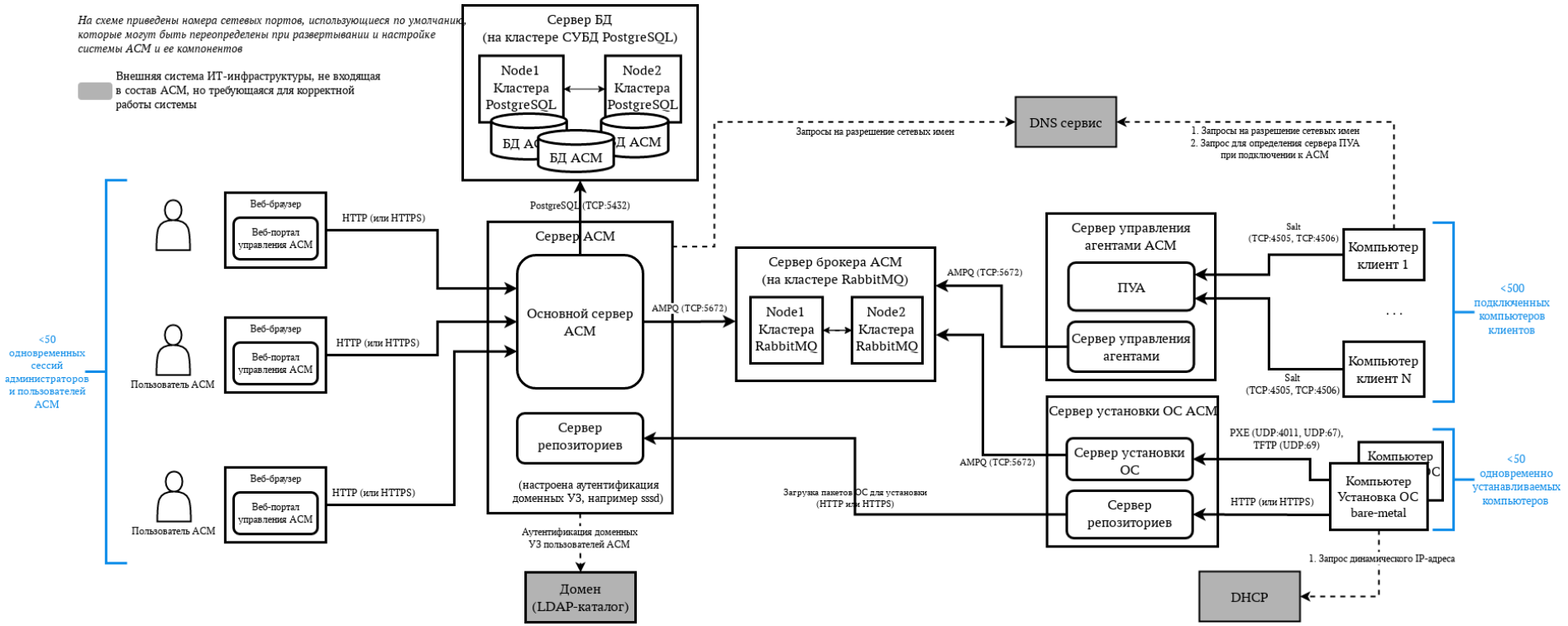

Рисунок 2. Схема компонент для распределенной конфигурации с одним сегментом АСМ

2.5 Конфигурация распределенная с двумя и более сегментами

2.5.1 Общие сведения о конфигурации

Схема установки АСМ в распределенной сетевой инфраструктуре с большим количеством клиентов:

- для подключения к АСМ региональных офисов с ненадежными/слабыми каналами связи;
- для развертывания в фрагментированной сети (когда есть отдельные фрагменты сети с ограниченным доступом);
- для подключения большого количества компьютеров клиентов (2000+).

Сценарий предполагает:

- подключение 2000 + управляемых компьютеров;

Данная конфигурация позволяет реализовать все функции управления ACM Standard v1.0.0, приведенные в разделе « 1.5 Функциональное назначение».

Для больших распределенных инфраструктур есть следующие рекомендации по выделению серверов АСМ:

- Для больших инфраструктур (с количеством компьютеров клиентов > 1000) рекомендуется выделение сервера БД на отдельный сервер. Для повышения отказоустойчивости может использоваться кластер СУБД PostgreSQL из нескольких нод.
- Для больших инфраструктур (с количеством компьютеров клиентов > 1000), в которых используется функция установки ОС по сети, рекомендуется выделение центрального сервера репозиториев на отдельный сервер.
- Для больших инфраструктур (с количеством функциональных серверов АСМ > 3 и количеством подключаемых компьютеров клиентов > 2000) рекомендуется выделение сервера брокера АСМ на отдельный сервер. Для повышения отказоустойчивости может использоваться кластер RabbitMQ из нескольких нод.

Требуется выделение отдельного сегмента АСМ при подключении компьютеров клиентов, находящихся в выделенном фрагменте сети (например, в региональном офисе, подключенном слабыми и ненадежными каналами связи).

В таком сегменте должны быть расположены:

1. Один «Сервер управления агентами АСМ».
2. «Сервер ПУА». Из расчета 1 сервер ПУА на каждые 500 компьютеров-клиентов. Если количество компьютеров-клиентов менее 500, то «Сервер управления агентами АСМ» и «Сервер ПУА» могут быть установлены на одном сервере (физическом или виртуальном).

При необходимости установки ОС по сети на компьютеры клиенты в выделенном фрагменте сети требуется установка сервера установки ОС АСМ. Количество серверов установки ОС в сегменте АСМ может быть любым и определяется:

1. Количеством одновременно устанавливаемых компьютеров клиентов. Рекомендуется не более 50 одновременно устанавливаемых компьютеров клиентов на один «Сервер установки ОС».
2. Особенностями сетевого доступа со стороны устанавливаемых компьютеров клиентов к Серверу установки ОС. Рекомендуется выделение отдельного сервера установки ОС в широковещательный домен (подсеть), содержащий устанавливаемые компьютеры клиенты. В разделе « 4.6.4 Установка сервера репозиториев и сервера установки ОС» приведено описание настройки сервера установки ОС для нескольких широковещательных доменов (подсетей).

Для входа пользователя на портал управления АСМ с доменной УЗ требуется использование УЗ из домена (LDAP-каталога), к которому подключен «Основной сервер АСМ».

2.5.2 Схема компонент

Требуется выделение отдельного сегмента АСМ в следующих случаях:

- при подключении компьютеров клиентов, находящихся в выделенном фрагменте сети.
- при подключении более 2000 компьютеров клиентов.

В таком сегменте должны быть расположены:

- Один «Сервер управления агентами АСМ», расположенный на выделенном сервере (выделенный сервер требуется для обеспечения необходимой производительности).
- Количество «Серверов ПУА» должно соответствовать формуле: один выделенный сервер ПУА на каждые 500 компьютеров клиентов.

На схеме (Рисунок 3) представлен вариант размещения компонент АСМ при выделении сегмента АСМ для подключения компьютеров клиентов, находящихся в фрагменте сети с ограниченным сетевым доступом. На схеме (Рисунок 4) представлен вариант размещения компонент АСМ при выделении сегмента АСМ для подключения большого количества компьютеров клиентов.

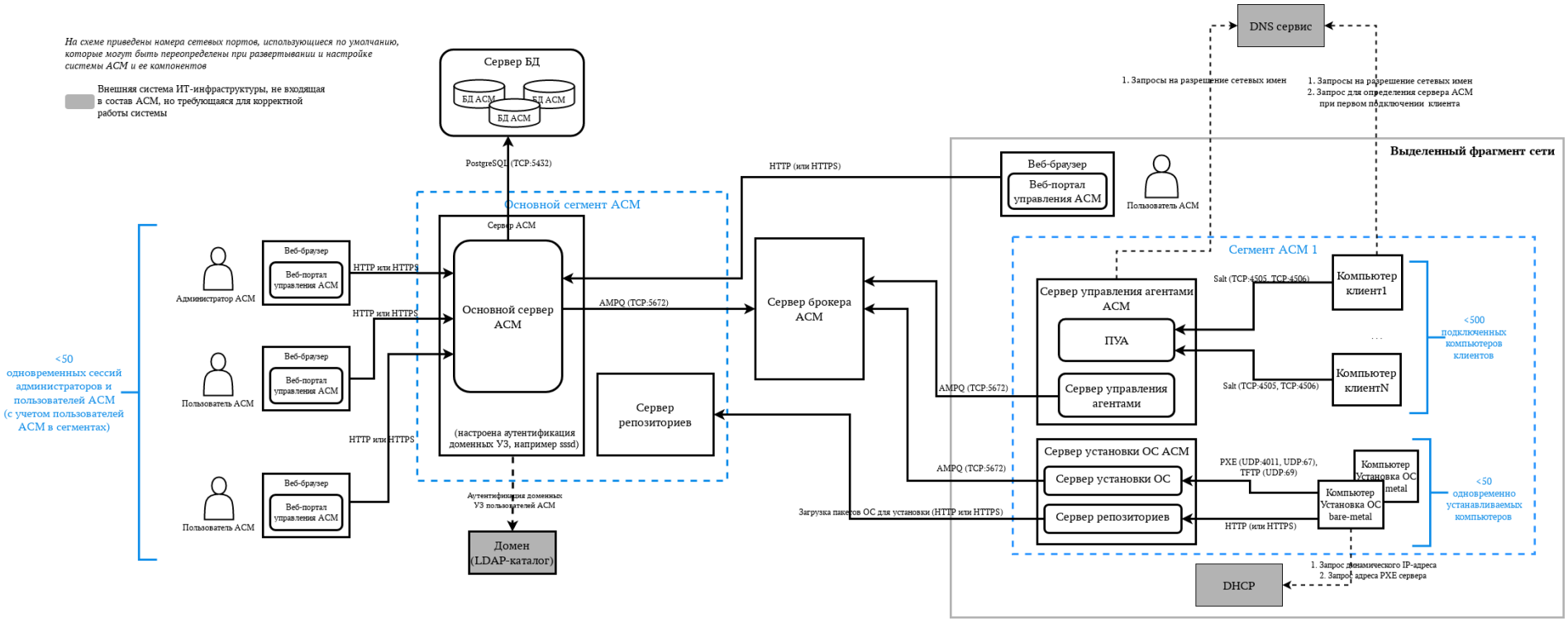

Рисунок 3. Схема компонент для распределенной конфигурации с двумя и более сегментами ACM

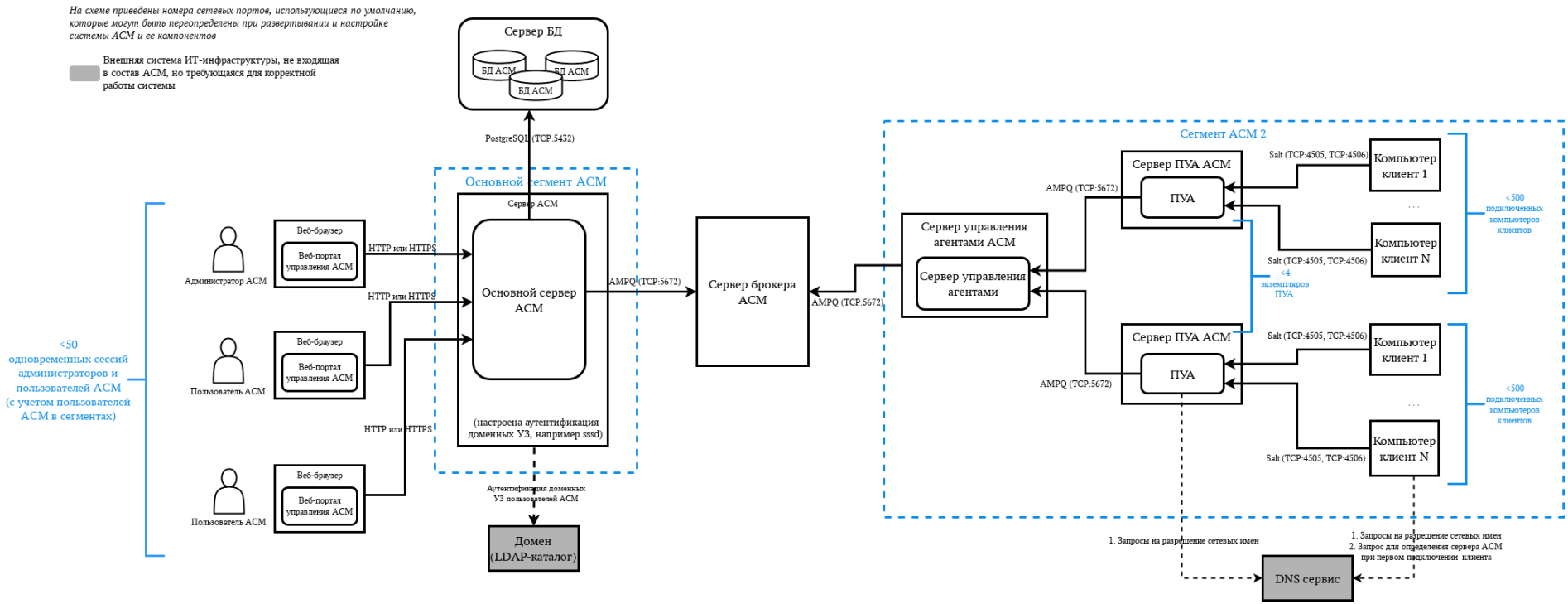

Рисунок 4. Схема компонент для распределенной конфигурации с двумя и более сегментами АСМ и выделенными серверами ПУА

3 УСЛОВИЯ ПРИМЕНЕНИЯ

Для функционирования Системы необходим состав программно-аппаратных средств с характеристиками и программным обеспечением, описанным далее.

3.1 Требования к программному обеспечению

Для установки функциональных серверов АСМ требуется ОС Astra Linux v1.7.5.

ОС Astra Linux функционирует на минимальном уровне защищенности (базовый «Орел»).

3.2 Требования к сетевой инфраструктуре и таблица сетевых взаимодействий компонентов

Ниже приведены общие требования к сетевой инфраструктуре, которые актуальны для всех конфигураций.

- Сетевые интерфейсы серверов (на которых функционируют серверные компоненты АСМ) настроены с постоянными IPv4 адресами. Рекомендуется использовать статические адреса, так как это позволяет исключить потенциальные проблемы, связанные с назначением адреса DHCP сервером;
- Серверы (на которых функционируют серверные компоненты АСМ) имеют заданное имя сетевое имя, отличное от других серверов АСМ;
- Настроен DNS-сервер, который разрешает сетевые имена всех серверов АСМ в корректный IP адрес;
- Пропускная способность канала для взаимодействия серверных компонент АСМ не менее 100 Мб/с;
- На серверах АСМ выключен встроенный firewall, или настроено разрешение сетевого доступа, согласно приведенным далее таблицам сетевого взаимодействия компонентов АСМ.

Примечание: Необходимо, чтобы доменное имя Salt разрешалось DNS сервером в IP адрес сервера, на котором развернут сервер ПУА.

Для корректной работы Системы необходимо обеспечить сетевой доступ для взаимодействия компонент в соответствии с требованиями, приведенными в таблице. В таблице приведены протоколы и номера сетевых портов, использующиеся по умолчанию. Некоторые номера сетевых портов и протоколы могут быть изменены администратором при установке и настройке системы.

3.2.1 Сводная таблица сетевых взаимодействий АСМ для всех конфигураций

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
1	Веб-портал управления АСМ	Основной сервер АСМ	HTTP (TCP:8080) или HTTPS (TCP:443)	не менее 1 Гбит/с	Взаимодействие администратора/пользователя АСМ и системы АСМ
2	Компьютер-клиент	Сервер ПУА АСМ	Salt (TCP:4505, TCP:4506)	не менее 100 Мбит/с	Взаимодействие агента АСМ на управляемом компьютере (клиенте) и ПУА.
3	Компьютер-клиент	Сервер установки ОС АСМ	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера репозитория: получение пакетов при первичной (bare-metal) установке ОС
4	Компьютер-клиент	Сервер установки ОС АСМ	PXE (UDP:4011, UDP:67), TFTP (UDP:69)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера установки ОС: получение параметров установки ОС при первичной (bare-metal) установке ОС
5	Основной сервер АСМ	Сервер БД (СУБД PostgreSQL)	SQL (TCP:5432)	не менее 1 Гбит/с	Взаимодействие серверных компонент основного сервера АСМ и базы данных
6	Основной сервер АСМ	Сервер брокера АСМ	AMPQ (TCP:5672,TCP:15672)	не менее 1 Гбит/с	Внутреннее взаимодействие серверных компонент системы АСМ
7	Сервер установки ОС АСМ	Сервер брокера АСМ	AMPQ (TCP:5672)	не менее 10 Мбит/с	Взаимодействие сервера установки ОС и системы АСМ
8	Сервер	Сервер брокера	AMPQ	не менее	Взаимодействие сервера

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
	управления агентами АСМ	АСМ	(TCP:5672,TCP:15672)	10 Мбит/с	управления агентами и системы АСМ
9	Сервер установки ОС АСМ	Сервер репозиториев (основной сегмент АСМ)	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 10 Мбит/с	Загрузка пакетов устанавливаемых ОС с сервера репозиториев (в основном сегменте) на сервер установки ОС
10	Сервер ПУА АСМ	Сервер управления агентами АСМ	AMPQ (TCP:5672)	не менее 1 Гбит/с	Взаимодействие ПУА и сервера управления агентами: получение заданий
11	Сервер ПУА АСМ	Сервер управления агентами АСМ	SSH (TCP:22)	не менее 1 Гбит/с	Взаимодействие ПУА и сервера управления агентами: получение артефактов для выполнения управляющих воздействий на компьютерах клиентах

3.2.2 **Таблица сетевых взаимодействий для минимальной конфигурации АСМ**

Для корректной работы Системы АСМ в минимальной конфигурации (подробнее описание приведено в разделе «Конфигурация минимальная») необходимо обеспечить сетевой доступ для взаимодействия компонент в соответствии с требованиями, приведенными в таблице. В таблице приведены протоколы и номера сетевых портов, использующиеся по умолчанию. Некоторые номера сетевых портов и протоколы могут быть изменены администратором при установке и настройке системы.

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
1	Веб-портал управления АСМ	Сервер АСМ	HTTP (TCP:8080) или HTTPS (TCP:443)	не менее 1 Гбит/с	Взаимодействие администратора/пользователя АСМ и системы АСМ
2	Компьютер-клиент	Сервер АСМ	Salt (TCP:4505, TCP:4506)	не менее 100 Мбит/с	Взаимодействие агента АСМ на управляемом компьютере (клиенте) и ПУА.
3	Компьютер-клиент	Сервер АСМ	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера репозитория: получение пакетов при первичной (bare-metal) установке ОС
4	Компьютер-клиент	Сервер АСМ	PXE (UDP:4011, UDP:67), TFTP (UDP:69)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера установки ОС: получение параметров установки ОС при первичной (bare-metal) установке ОС

3.2.3 **Таблица сетевых взаимодействий для конфигурации распределенной с одним сегментом**

Для корректной работы Системы АСМ в распределенной конфигурации с одним сегментом (подробнее описание приведено в разделе «Конфигурация распределенная с одним сегментом») необходимо обеспечить сетевой доступ для взаимодействия компонент в соответствии с требованиями, приведенными в таблице. В таблице приведены протоколы и номера сетевых портов, использующиеся по умолчанию. Некоторые номера сетевых портов и протоколы могут быть изменены администратором при установке и настройке системы.

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
1	Веб-портал управления АСМ	Сервер АСМ	HTTP (TCP:8080) или HTTPS (TCP:443)	не менее 1 Гбит/с	Взаимодействие администратора/пользователя АСМ и системы АСМ
2	Компьютер-клиент	Сервер управления агентами АСМ	Salt (TCP:4505, TCP:4506)	не менее 100 Мбит/с	Взаимодействие агента АСМ на управляемом компьютере (клиенте) и ПУА.
3	Компьютер-клиент	Сервер установки ОС АСМ	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера репозитория: получение пакетов при первичной (bare-metal) установке ОС
4	Компьютер-клиент	Сервер установки ОС АСМ	PXE (UDP:4011, UDP:67), TFTP (UDP:69)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера установки ОС: получение параметров установки ОС при первичной (bare-metal) установке ОС
5	Сервер АСМ	Сервер БД (СУБД PostgreSQL)	SQL (TCP:5432)	не менее 1 Гбит/с	Взаимодействие серверных компонент основного сервера АСМ и базы данных
6	Сервер АСМ	Сервер брокера АСМ	AMPQ (TCP:5672,TCP:15672)	не менее 1 Гбит/с	Внутреннее взаимодействие серверных компонент системы АСМ
7	Сервер установки ОС АСМ	Сервер брокера АСМ	AMPQ (TCP:5672)	не менее 10 Мбит/с	Взаимодействие сервера установки ОС и системы АСМ
8	Сервер управления агентами АСМ	Сервер брокера АСМ	AMPQ (TCP:5672,TCP:15672)	не менее 10 Мбит/с	Взаимодействие сервера управления агентами и системы АСМ
9	Сервер	Сервер АСМ	HTTP (TCP:80)	не менее	Загрузка пакетов

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
	установки ОС АСМ		или HTTPS (TCP:443)	10 Мбит/с	устанавливаемых ОС с сервера репозиториев на сервер установки ОС

3.2.4 Таблица сетевых взаимодействий для конфигурации распределенной с двумя и более сегментами

Для корректной работы Системы АСМ в распределенной конфигурации с двумя и более сегментами (подробнее описание приведено в разделе «Конфигурация распределенная с двумя и более сегментами») необходимо обеспечить сетевой доступ для взаимодействия компонент в соответствии с требованиями, приведенными в таблице. В таблице приведены протоколы и номера сетевых портов, использующиеся по умолчанию. Некоторые номера сетевых портов и протоколы могут быть изменены администратором при установке и настройке системы.

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
1	Веб-портал управления АСМ	Сервер АСМ	HTTP (TCP:8080) или HTTPS (TCP:443)	не менее 1 Гбит/с	Взаимодействие администратора/пользователя АСМ и системы АСМ
2	Компьютер-клиент	Сервер ПУА АСМ	Salt (TCP:4505, TCP:4506)	не менее 100 Мбит/с	Взаимодействие агента АСМ на управляемом компьютере (клиенте) и ПУА.
3	Компьютер-клиент	Сервер установки ОС АСМ	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера репозитория: получение пакетов при

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
					первичной (bare-metal) установке ОС
4	Компьютер-клиент	Сервер установки ОС АСМ	PXE (UDP:4011, UDP:67), TFTP (UDP:69)	не менее 100 Мбит/с	Взаимодействие компьютера (клиента) и сервера установки ОС: получение параметров установки ОС при первичной (bare-metal) установке ОС
5	Сервер АСМ	Сервер БД (СУБД PostgreSQL)	SQL (TCP:5432)	не менее 1 Гбит/с	Взаимодействие серверных компонент основного сервера АСМ и базы данных
6	Сервер АСМ	Сервер брокера АСМ	AMPQ (TCP:5672,TCP:15672)	не менее 1 Гбит/с	Внутреннее взаимодействие серверных компонент системы АСМ
7	Сервер установки ОС	Сервер брокера АСМ	AMPQ (TCP:5672)	не менее 10 Мбит/с	Взаимодействие сервера установки ОС и системы АСМ
8	Сервер управления агентами	Сервер брокера АСМ	AMPQ (TCP:5672,TCP:15672)	не менее 10 Мбит/с	Взаимодействие сервера управления агентами и системы АСМ
9	Сервер установки ОС АСМ	Сервер репозиториев (основной сегмент АСМ)	HTTP (TCP:80) или HTTPS (TCP:443)	не менее 10 Мбит/с	Загрузка пакетов устанавливаемых ОС с сервера репозиториев (в основном сегменте) на сервер установки ОС
10	Сервер ПУА АСМ	Сервер управления агентами	AMPQ (TCP:5672)	не менее 1 Гбит/с	Взаимодействие ПУА и сервера управления агентами: получение заданий
11	Сервер ПУА АСМ	Сервер управления агентами АСМ	SSH (TCP:22)	не менее 1 Гбит/с	Взаимодействие ПУА и сервера управления агентами: получение

№	Адрес источника	Адрес назначения	Протокол уровня приложения (Транспортный протокол:Сетевой порт)	Требования к пропускной способности канала связи	Комментарий
					артефактов для выполнения управляющих воздействий на компьютерах клиентах

3.3 Аппаратные требования

3.3.1 Конфигурация минимальная

Требования к сетевому адаптеру — скорость не менее 1 ГБ/с.

3.3.1.1 Аппаратные требования к основному серверу

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

3.3.2 Конфигурация распределенная с одним сегментом

Требования к сетевому адаптеру — скорость не менее 1 ГБ/с.

3.3.2.1 Аппаратный требования к основному серверу

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

3.3.2.2 Аппаратные требования к серверу БД

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

Примечание: Если используется отказоустойчивый кластер СУБД PostgreSQL, обратитесь к рекомендациям производителя кластерного решения PostgreSQL по требованиям к программному и аппаратному обеспечению узлов кластера.

3.3.2.3 Аппаратные требования к серверу управления агентами

Требования	Рекомендуемые
Процессор	3 ГГц
Количество ядер	4 шт.
Оперативная память	8 Гб
Дисковое пространство	80 Гб

3.3.2.4 Аппаратные требования к серверу репозиториев и серверу установки ОС

Требования	Рекомендуемые
Процессор	3 ГГц
Количество ядер	4 шт.
Оперативная память	8 Гб
Дисковое пространство	100 Гб

Примечание: рекомендуемый размер дискового пространства зависит от количества используемых при установке ОС репозиториев.

3.3.2.5 Аппаратные требования к серверу брокера

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

3.3.3 **Конфигурация распределенная с двумя и более сегментами**

Требования к сетевому адаптеру — скорость не менее 1 ГБ/с.

3.3.3.1 Аппаратные требования к основному серверу

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

3.3.3.2 Аппаратные требования к серверу БД

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

Примечание: Если используется отказоустойчивый кластер СУБД PostgreSQL, обратитесь к рекомендациям производителя кластерного решения PostgreSQL по требованиям к программному и аппаратному обеспечению узлов кластера.

3.3.3.3 Аппаратные требования к серверу управления агентами

Требования	Рекомендуемые
Процессор	3 ГГц
Количество ядер	4 шт.
Оперативная память	8 Гб
Дисковое пространство	80 Гб

3.3.3.4 Аппаратные требования к серверу ПУА

Требования	Рекомендуемые
Процессор	3 ГГц
Количество ядер	4 шт.
Оперативная память	8 Гб
Дисковое пространство	80 Гб

3.3.3.5 Аппаратные требования к серверу репозиториев и серверу установки ОС

Требования	Рекомендуемые
Процессор	3 ГГц
Количество ядер	4 шт.
Оперативная память	8 Гб
Дисковое пространство	100 Гб

Примечание: рекомендуемый размер дискового пространства зависит от количества используемых при установке ОС репозиториев.

3.3.3.6 Аппаратные требования к серверу брокера

Требования	Рекомендуемые
Процессор	2 ГГц
Количество ядер	2 шт.
Оперативная память	4 Гб
Дисковое пространство	50 Гб

4 РАЗВЕРТЫВАНИЕ АСМ

4.1 Установка и настройка Системы

В данном разделе приведено описание действий по установке и настройке системы АСМ, для различных конфигураций.

4.2 Описание скриптов установки acm-bootstrap

Для установки серверных компонентов системы АСМ используются заранее подготовленные скрипты установки (bootstrap скрипты), обеспечивающие автоматизацию по установке и настройке необходимых компонент АСМ. Используется несколько различных скриптов установки для покрытия различных вариантов конфигураций АСМ.

Скрипты установки предоставляются в составе пакета acm-bootstrap, входящего в репозиторий дистрибутивов системы АСМ. При установке пакета acm-bootstrap в каталоге /opt/acm/acm-bootstrap создаются необходимые скрипты для установки всех сервисов системы и файлы конфигурации.

Для передачи настраиваемых значений в скрипты установки используется конфигурационный файл с переменными env (acm-bootstrap/env). Переменные в конфигурационном файле сгруппированы в зависимости от необходимости их изменения для выполнения корректной установки системы:

1) Переменные, сгруппированные под тегом

```
### Variables that MUST be set
```

должны быть обязательно указаны администратором для корректной установки и работы системы.

2) Переменные, сгруппированные под тегом

```
### Variables that MUST be changed
```

должны быть обязательно изменены администратором для корректной установки и работы системы.

3) Переменные, сгруппированные под тегом

```
### Variables that CAN BE changed
```

опционально могут быть изменены администратором для корректной работы системы.

Подробное описание используемых в env файле переменных приведено в «Приложение. Параметры переменных конфигурационного env файла».

4.3 Установка основного сервера АСМ

4.3.1 Подготовка сервера

Необходимо подготовить сервер (физический или виртуальный), соответствующий требованиям:

– требования к аппаратным характеристикам сервера приведены в разделе « 3.3 Аппаратные требования» (необходимо выбрать соответствующую конфигурацию → раздел «Требования к аппаратным характеристикам серверов»);

– требования к ОС и составу ПО на сервере приведены в разделе «Ошибка: источник перекрёстной ссылки не найден Ошибка: источник перекрёстной ссылки не найден»;

– требования по сетевому доступу должны соответствовать разделу « 3.2 Требования к сетевой инфраструктуре и таблица сетевых взаимодействий компонентов».

4.3.2 Развертывание основного сервера АСМ

Для установки основного сервера АСМ администратору необходимо выполнить следующие действия на сервере:

1) Подключить репозитории Astra Linux 1.7.5 в список используемых репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки:

```
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base 1.7_x86-64 main non-free contrib

deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-extended 1.7_x86-64 main contrib non-free
```

2) Скопировать на сервер файл iso с дистрибутивами АСМ.

3) Смонтировать iso образ дистрибутивов АСМ, выполнив в терминале команду, где <*ACM iso*> - полный путь до к iso файлу:

```
sudo mkdir -p /mnt/acm/frozen/1.x/ && sudo mount -o loop <ACM iso> /mnt/acm/frozen/1.x/
```

4) Подключить репозиторий АСМ, выполнив в терминале команду:

```
echo "deb file:/mnt/acm/frozen/1.x/ 1.0.0 main" | sudo tee -a
```

```
/etc/apt/sources.list
```

5) Обновить список репозиториев и пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

6) Установить пакет acm-bootstrap, выполнив в терминале команду:

```
sudo apt install -y acm-bootstrap
```

7) Отредактировать файл с переменными /opt/acm/acm-bootstrap/env, значение переменных приведено в « 4.2 Описание скриптов установки acm-bootstrap». Для установки «Основного сервера АСМ» для минимальной конфигурации используются все переменные, указанные в файле env, пример конфигурационного файла env приведен в «Приложение. Переменные файла env при установке основного сервера АСМ».

Примечание: в конфигурационном файле env в переменной BUILT_ACCOUNT требуется указать имя учетной записи, которая будет использоваться как предустановленный администратор системы АСМ. Может быть указана локальная учетная запись ОС Astra Linux сервера, на котором производится установка «Основного сервера АСМ» (например, BUILT_ACCOUNT="admin"). Если сервер включен в домен и используется аутентификация на базе доменных УЗ, может быть указана доменная УЗ (например, BUILT_ACCOUNT="admin@domain.name"). Обратите внимание, что учетные записи являются регистрозависимыми (т. е. «Admin» и «admin» - это разные учетные записи). Изменить учетную запись предустановленного администратора АСМ после установки системы невозможно. Убедитесь, что указанная учетная запись существует и под ней корректно выполняется вход на сервер, на котором выполняется установка «Основного сервера АСМ».

8) Запустить установку и загрузку репозиториев ОС Astra Linux 1.7.5, требующихся для настройки функции установки ОС в АСМ, выполнив в терминале команду:

```
sudo /opt/acm/acm-bootstrap/bootstrap-centralrepo.sh
```

Примечание: загрузка репозиториев осуществляется с сетевого ресурса

https://dl.astralinux.ru/astra/, для успешного выполнения требуется доступ с сервера в сеть Интернет. Операция подготовки репозиториев может занять некоторое время. Размещение загруженных репозиториев производится в файловой системе сервера, на котором выполняется установка, в каталог, указанный в конфигурационном файле env в переменной MIRROR_DIR. Убедитесь, что в разделе, где расположен каталог, есть не менее 30 Гб свободного пространства.

9) Запустить установку основного сервера АСМ:

```
sudo /opt/acm/acm-bootstrap/bootstrap-acm.sh
```

10) Открыть интерфейс портала АСМ по адресу http://<ACM_IP>:8080, где <*ACM_IP*> - адрес хоста, на котором выполнена установка основного сервера АСМ.

11) Выполнить вход на портал управления АСМ по адресу http://<ACM_IP>:8080, используя учетную запись (доменную или локальную), имя входа которой было указано в конфигурационном файле /opt/acm/acm-bootstrap/env, использовавшемся при установке Основного сервера АСМ.

4.3.3 Настройка аутентификации по доменным УЗ

Для корректной работы аутентификации пользователей на портале управления АСМ по доменным учетным записям необходимо:

1) Добавить сервер, на котором установлен «Основной сервер АСМ» в домен, который будет использоваться для аутентификации и настроить аутентификацию по доменным учетным записям пользователей в ОС Astra Linux. Инструкцию по включению сервера в домен смотрите в документации соответствующего домена (службы каталога LDAP).

2) Убедиться, что на сервере, на котором установлен «Основной сервер АСМ», в конфигурационном файле /etc/sssd/sssd.conf в разделе [domain/имя домена] присутствуют следующие строки (если необходимо, добавить строки в файл):

```
cache_credentials = True

use_fully_quallified_names = True
```

3) После изменения конфигурационного файла перезагрузить сервер, на

котором установлен «Основной сервер АСМ».

4.4 Установка сервера управления агентами АСМ

По умолчанию в составе основного сервера АСМ производится установка серверной роли «сервер управления агентами» и подключение к предустановленному «Основному сегменту» системы АСМ. Данный сервер управления агентами предназначен для обслуживания компьютеров клиентов, подключаемых непосредственно к основному серверу АСМ в случае небольших инсталляций с ограниченным количеством управляемых компьютеров. Установка и настройка дополнительного сервера управления агентами АСМ необходима при выделении дополнительного сегмента АСМ в следующих случаях:

– Требуется создание дополнительного сегмента с подключением к системе АСМ более 1000 компьютеров клиентов.

– Требуется подключить к системе АСМ компьютеры клиенты, расположенные в сегменте сети с ограниченным сетевым доступом (слабые или ненадежные каналы связи или ограничение сетевого доступа в целях ИБ).

4.4.1 Подготовка сервера

Необходимо подготовить сервер (физический или виртуальный), соответствующий требованиям:

– требования к аппаратным характеристикам сервера приведены в разделе « 3.3 Аппаратные требования» (необходимо выбрать соответствующую конфигурацию → раздел «Требования к аппаратным характеристикам серверов»);

– требования к ОС и составу ПО на сервере приведены в разделе «Ошибка: источник перекрёстной ссылки не найден Ошибка: источник перекрёстной ссылки не найден»;

– требования по сетевому доступу должны соответствовать разделу « 3.2 Требования к сетевой инфраструктуре и таблица сетевых взаимодействий компонентов».

4.4.2 Создание сегмента

Для создания сегмента необходимо:

1) Создать сегмент АСМ в разделе «Управление системой» → «Сегменты управления» портала управления АСМ. Подробнее шаги по созданию сегмента приведены в документе «Руководство оператора».

2) Скопировать UID созданного сегмента на карточке сегмента на портале управления АСМ.

4.4.3 Развертывание Сервера управления агентами

Примечание: Версия ОС Astra Linux, подключаемых компьютеров клиентов не может быть выше, чем версия сервера.

1) Подключить репозитории Astra Linux 1.7.5 в список используемых репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки:

```
deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base
1.7_x86-64 main non-free contrib

deb http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-
extended 1.7_x86-64 main contrib non-free
```

2) Подключить репозиторий ACM, выполнив в терминале команду, где <*ACM repo IP*> - IP адрес основного сервера ACM, развернутого согласно раздела « 4.3.2 Развертывание основного сервера ACM»:

```
echo "deb http://<ACM repo IP>/acm/frozen/1.x/ 1.0.0 main" | sudo tee -a
/etc/apt/sources.list
```

3) Обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

4) Установить пакет acm-bootstrap, выполнив команду:

```
sudo apt install -y acm-bootstrap
```

5) Отредактировать файл с переменными /opt/acm/acm-bootstrap/env, подробнее в разделе « 4.2 Описание скриптов установки acm-bootstrap», состав переменных и примеры значений переменных приведено в «Приложение. Переменные файла env при установке сервера управления агентами ACM».

6) Запустить установку сервера управления агентами ACM, выполнив команду, здесь вместо <*UID сегмента*> подставить идентификатор сегмента ACM, созданного в разделе « 4.4.2 Создание сегмента», вместо <*адрес центрального сервера очередей*> подставить IP адрес основного сервера ACM, развернутого согласно раздела « 4.3.2 Развертывание основного сервера ACM»:

```
sudo /opt/acm/acm-bootstrap/bootstrap-agent.sh <UID сегмента> <адрес
```

```
центрального сервера очередей>
```

4.5 Установка ПУА

Примечание: Версия ОС Astra Linux подключаемых компьютеров клиентов не может быть выше, чем версия сервера.

Необходимо, чтобы доменное имя Salt разрешалось DNS сервисом в IP адрес, на котором развернут сервер ПУА.

Необходимость выделения отдельного сервера (физического или виртуального) для компонента ПУА либо размещение ПУА на одном сервере с сервером управления агентов АСМ определяется используемой конфигурацией развертывания и прогнозируемым количеством компьютеров клиентов.

При использовании выделенного сервера (физического или виртуального) для компонента ПУА необходимо подготовить сервер, соответствующий требованиям:

– требования к аппаратным характеристикам сервера приведены в разделе « 3.3 Аппаратные требования» (необходимо выбрать соответствующую конфигурацию → раздел «Требования к аппаратным характеристикам серверов»);

– требования к ОС и составу ПО на сервере приведены в разделе «Ошибка: источник перекрёстной ссылки не найден Ошибка: источник перекрёстной ссылки не найден»;

– требования по сетевому доступу должны соответствовать разделу « 3.2 Требования к сетевой инфраструктуре и таблица сетевых взаимодействий компонентов».

Перед развертыванием сервера ПУА должен быть развернут сервер управления агентами, к которому будет подключаться развернутый компонент ПУА. Описание действий по развертыванию сервера управления агентами приведено в разделе « 4.4 Установка сервера управления агентами АСМ».

4.5.1 Установка ПУА на сервере управления агентами

Примечание: Установка ПУА производится после установки в сети сервера управления агентами.

Для установки ПУА на том же сервере, что и компонент «Сервер управления агентами АСМ», администратору необходимо выполнить следующие действия на сервере:

1) Подключить репозитории Astra Linux 1.7.5 в список используемых

репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки:

```
deb   http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base
1.7_x86-64 main non-free contrib

deb      http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-
extended 1.7_x86-64 main contrib non-free
```

2) Подключить репозиторий АСМ, выполнив в терминале команду, где <*ACM repo IP*> - IP адрес основного сервера АСМ, развернутого согласно раздела « 4.3.2 Развертывание основного сервера АСМ»:

```
echo "deb http://<ACM repo IP>/acm/frozen/1.x/ 1.0.0 main" | sudo tee -a
/etc/apt/sources.list
```

3) Обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

4) Установить пакет acm-bootstrap, выполнив команду:

```
sudo apt install -y acm-bootstrap
```

5) Отредактировать файл с переменными /opt/acm/acm-bootstrap/env, значение переменных приведено в « 4.2 Описание скриптов установки acm-bootstrap», пример файла в «Приложение. Переменные файла env при установке ПУА».

6) Запустить установку сервера ПУА АСМ, выполнив команду, вместо <*адрес сервера управления агентами*> указать IP адрес сервера управления агентами АСМ, развернутого согласно раздела « 4.4.3 Развертывание Сервера управления агентами»:

```
sudo /opt/acm/acm-bootstrap/bootstrap-amp.sh <адрес сервера управления агентами>
```

4.5.2 Установка ПУА на отдельном сервере

Примечание: Установка ПУА производится после установки в сети сервера управления агентами.

Для установки ПУА на выделенном сервере (физическом или виртуальном) администратору необходимо выполнить следующие действия на сервере:

1) Подключить репозитории Astra Linux 1.7.5 в список используемых репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки:

```
deb   http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base 1.7_x86-64 main non-free contrib

deb      http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-extended 1.7_x86-64 main contrib non-free
```

2) Подключить репозиторий ACM, выполнив в терминале команду, где <*ACM repo IP*> - IP адрес основного сервера ACM, развернутого согласно раздела « 4.3.2 Развертывание основного сервера ACM»:

```
echo "deb http://<ACM repo IP>/acm/frozen/1.x/ 1.0.0 main" | sudo tee -a /etc/apt/sources.list
```

3) Обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

4) Установить пакет acm-bootstrap, выполнив команду:

```
sudo apt install -y acm-bootstrap
```

5) Отредактировать файл с переменными /opt/acm/acm-bootstrap/env, значение переменных приведено в «Приложение. Переменные файла env при установке основного сервера ACM».

6) Скопировать rsa ключи /home/${GIT_USER}/.ssh/git_id_rsa* с сервера управления агентами ACM, к которому будет подключен разворачиваемый ПУА, в директорию /root/.ssh/

7) Запустить установку сервера ПУА ACM, выполнив команду, вместо <*адрес сервера управления агентами*> указать IP адрес сервера управления агентами ACM, развернутого согласно раздела « 4.4.3 Развертывание Сервера управления агентами»:

```
sudo /opt/acm/acm-bootstrap/bootstrap-amp-db.sh <адрес сервера управления агентами>
```

4.6 Установка сервера установки ОС по сети

4.6.1 Требования к настройке DHCP

Для корректной работы сервера установки ОС АСМ должны быть выполнены следующие требования к инфраструктуре:

1) В инфраструктуре должен быть предварительно настроен DHCP сервер (не входит в состав АСМ), который выдает IP адреса клиентам. Данный DHCP сервер не должен отдавать DHCP опции для PXE: 66 (next server) и 67 (boot file). Эти опции всегда отдаются сервером установки ОС по сети АСМ.

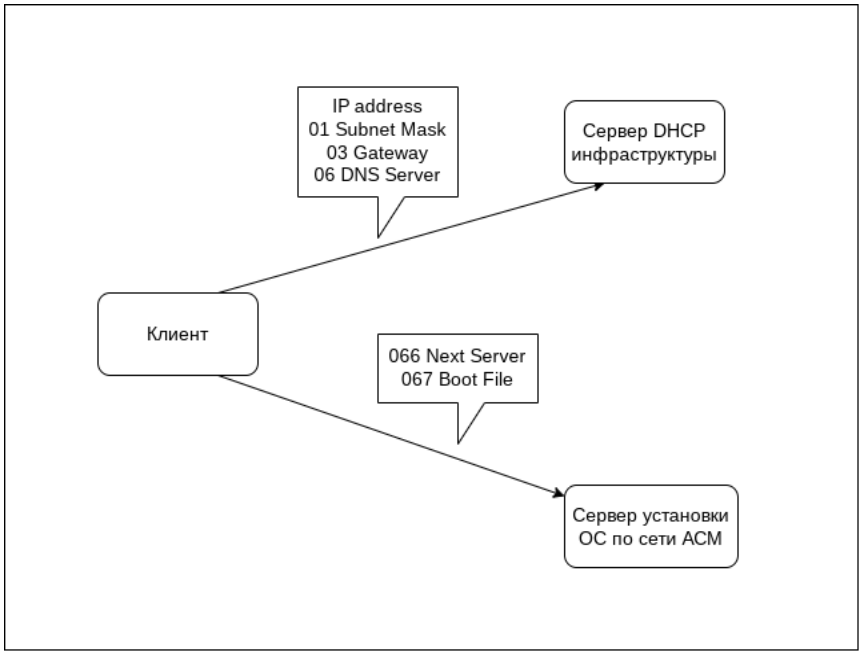

Рис. 5. Схема получения данных при установке ОС

Примечание: Рекомендуется не устанавливать сервер установки ОС по сети и инфраструктурный DHCP сервер на одном физическом или виртуальном сервере. Если у вас есть отдельная группа, которая отвечает за сетевую инфраструктуру и сетевые службы, уведомите об этом и включите эту команду в период оценки и тестирования. Например, установка сервиса isc-dhcp-server (в роли инфраструктурного DHCP сервера) на сервер установки ОС по сети может вызвать бесконечный цикл запроса IP адреса на одном из этапов установки ОС по сети.

Примечание: Сервер установки ОС по сети поддерживает загрузку BIOS (Legacy) и UEFI клиентов. Для них сервер автоматически прописывает соответствующий загрузочный файл в опцию 067 (boot_file).

2) Сетевая инфраструктура должна быть настроена таким образом, чтобы DHCP запросы клиентов приходили как на инфраструктурный DHCP сервер, так и на сервер установки ОС АСМ.

Возможны два случая:

– Сервер установки ОС по сети и клиенты находятся в одном широковещательном домене (подсети). В данном случае каких-то дополнительных настроек на уровне сети не требуется.

– Сервер установки ОС по сети и клиенты находятся в разных широковещательных доменах (подсетях). В данном случае без дополнительной настройки на уровне сети широковещательный DHCP запрос от клиента не будет покидать широковещательный домен и не достигнет сервера установки ОС по сети АСМ.

Требуется настроить на сетевом оборудовании, обрабатывающем сетевой трафик клиентов, функцию DHCP Relay Agent (IP helper), указывающий на сервер установки ОС по сети. Данную настройку требуется выполнить для каждой подсети, где находятся клиенты DHCP. DHCP Relay Agent (IP Helper) конвертирует широковещательный DHCP запрос в персональный, который отправляется на IP адрес сервера установки ОС по сети.

3) В текущей реализации сервера установки ОС по сети АСМ невозможно задать уникальные и предопределенные имена компьютеров при установке ОС. Для задания таких имен необходимо настроить резервации на инфраструктурном сервере DHCP.

4.6.2 Описание работы DHCP при PXE загрузке

Ключевые участники:

– Клиент – компьютер, который необходимо загрузить по сети;

– DHCP сервер – сервер, который выдает клиентам настройки сети (IP адрес, маска подсети, шлюз, DNS сервер, DNS домен и т.д.);

– PXE сервер – сервер установки ОС АСМ, который выдает клиентам настройки PXE (адрес сервера PXE, загрузочный файл), а также необходимые загрузочные файлы.

Процесс загрузки

Шаг 1 – Клиент отправляет широковещательное сообщение DHCPDISCOVER.

Шаг 2 – DHCP сервер, а также PXE сервер получают сообщение клиента и отвечают сообщением DHCPOFFER. DHCP сервер в своем сообщении включает опции настройки сети (IP адрес, маска подсети, шлюз, DNS сервер, DNS домен и т.д.). PXE сервер в своем сообщении включает только опции PXE (адрес сервера PXE, загрузочный файл).

Шаг 3 – Клиент после получения сообщений DHCPOFFER отправляет

сообщения DHCPREQUEST, которые содержат набор полученных опций. Каждому серверу отправляется только полученный от него набор опций.

Примечание: при получении конфликтных сообщений DHCPOFFER поведение клиента может быть недетерминированным. В большинстве реализаций клиентов будет выбран первый поступивший ответ из конфликтных.

Шаг 4 – DHCP сервер, а также PXE сервер после получения DHCPREQUEST, отправляют сообщение DHCPACK, подтверждая клиенту правильность всех опций.

Шаг 5 – Клиент обращается к серверу, указанному в опции 066 (next_server) и скачивает файл, относительный путь к которому указан в опции 067 (boot_file). Скачанный файл используется клиентом как загрузчик и ему передается управление.

4.6.3 Подготовка сервера

Примечание: далее описаны действия по установке дополнительного сервера установки ОС. По умолчанию при развертывании «Основного сервера АСМ» на нем устанавливается сервис установки ОС по сети, подключенный к «Основному сегменту АСМ». Для установки дополнительного сервера установки ОС в системе АСМ должен быть создан хотя бы один дополнительный «Сегмент АСМ», в котором развернуты Сервер управления агентами и ПУА.

Примечание: Если планируется устанавливать более одного экземпляра "Сервера установки ОС" АСМ, то рекомендуется обеспечить нахождение этих серверов в разных широковещательных доменах. В противном случае обслуживание компьютеров клиентов при установке ОС по сети тем или иным сервером становится негарантируемым и непредсказуемым. По этой же причине не рекомендуется размещать "Сервер установки ОС" АСМ в одном широковещательном домене с другими серверами, предоставляющими функцию загрузки устройств по сети (PXE).

Для установки и настройки сервиса репозиториев и сервера установки ОС необходимо подготовить сервер (физический или виртуальный), соответствующий требованиям:

– требования к аппаратным характеристикам сервера приведены в разделе « 3.3 Аппаратные требования» (необходимо выбрать соответствующую конфигурацию → раздел «Требования к аппаратным характеристикам серверов»);

– требования к ОС и составу ПО на сервере приведены в разделе «Ошибка: источник перекрёстной ссылки не найден Ошибка: источник перекрёстной ссылки не найден»;

– требования по сетевому доступу должны соответствовать разделу « 3.2 Требования к сетевой инфраструктуре и таблица сетевых взаимодействий компонентов».

4.6.4 Установка сервера репозиториев и сервера установки ОС

Сервер репозиториев и сервер установки ОС необходимы для настройки в АСМ функции установки ОС по сети. Если эта функция использоваться не будет, то сервер репозиториев и сервер установки ОС можно не устанавливать.

Для обеспечения корректной работы сервер установки ОС и сервис репозиториев должны быть установлены на одном сервере (физическом или виртуальном).

Для установки сервера репозиториев и сервера установки ОС необходимо выполнить следующие действия:

1) Подключить репозитории Astra Linux 1.7.5 в список используемых репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки:

```
deb   http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-base 1.7_x86-64 main non-free contrib

deb      http://download.astralinux.ru/astra/frozen/1.7_x86-64/1.7.5/repository-extended 1.7_x86-64 main contrib non-free
```

2) Подключить репозиторий АСМ, выполнив в терминале команду, где <*ACM repo IP*> - IP адрес основного сервера АСМ, развернутого согласно раздела « 4.3.2 Развертывание основного сервера АСМ»:

```
echo "deb http://<ACM repo IP>/acm/frozen/1.x/ 1.0.0 main" | sudo tee -a /etc/apt/sources.list
```

3) Обновить пакеты, выполнив в терминале команду:

```
sudo apt update && sudo apt dist-upgrade -y
```

4) Установить пакет acm-bootstrap, выполнив команду:

```
sudo apt install -y acm-bootstrap
```

5) Отредактировать файл с переменными /opt/acm/acm-bootstrap/env, значение переменных приведено в « 4.2 Описание скриптов установки acm-bootstrap», пример файла в «Приложение. Переменные файла env при установке сервера установки ОС и сервера репозиториев».

6) Запустить установку сервера установки ОС АСМ, выполнив команду, здесь вместо <*UID сегмента*> подставить идентификатор сегмента АСМ, созданного в разделе « 4.4.2 Создание сегмента», вместо <*адрес сервера брокера АСМ*> подставить IP адрес основного сервера АСМ, развернутого согласно раздела « 4.3.2 Развертывание основного сервера АСМ»:

```
sudo /opt/acm/acm-bootstrap/bootstrap-os.sh <UID сегмента> <адрес центрального сервера очередей>
```

7) Запустить установку и скачивание репозиториев с центрального сервера репозиториев АСМ, выполнив команду, где вместо <*адрес центрального сервера репозиториев*> указать IP адрес основного сервера АСМ, развернутого согласно раздела « 4.3.2 Развертывание основного сервера АСМ»:

```
sudo /opt/acm/acm-bootstrap/bootstrap-repo-segment.sh <адрес центрального сервера репозиториев>
```

Примечание: загрузка репозиториев осуществляется с Основного сервера АСМ. Операция загрузки и подготовки репозиториев может занять некоторое время. Размещение загруженных репозиториев производится в файловой системе сервера, на котором выполняется установка, в каталог, указанный в конфигурационном файле env в переменной FILES_DIR. Убедитесь, что в разделе, где расположен каталог, есть не менее 30 Гб свободного пространства.

4.7 Порядок проверки работоспособности

В браузере перейти по адресу:

```
http://<IP-адрес или FQDN сервера АСМ>:8080
```

Отобразится страница входа на портал. На странице входа указать учетные данные — имя входа и пароль — учетной записи (локальной или доменной), которая была указана как предустановленная учетная запись с правами

администратора при установке Основного сервера АСМ, и нажать кнопку «Вход» или клавишу Enter.

Примечание: имя входа учетной записи, используемой системой АСМ в качестве предустановленной УЗ с правами администратора, указывается в конфигурационном файле /opt/acm-bootstrap/env в переменной ***BUILT_ACCOUNT*** *при установке «Основного сервера АСМ». Обратите внимание, что имя учетной записи является регистрозависимым (т. е. «Admin» и «admin» - это разные учетные записи).*

После успешного входа отобразится главная страница веб-портала управления АСМ.

4.8 Настройка и подключение компьютеров клиентов

Добавление компьютера клиента АСМ осуществляется после развертывания основного сервера согласно раздела « 4.3.2 Развертывание основного сервера АСМ».

Необходимо убедиться, что каждый клиент имеет уникальное сетевое имя хоста (hostname), поскольку сетевое имя хоста используется в качестве идентификатора машины.

Для подключения компьютера к системе АСМ необходимо выполнить следующие действия:

1) Подключить репозитории Astra Linux 1.7.5 в список используемых репозиториев. Убедиться, что файл /etc/apt/sources.list содержит следующие строки, вместо <ACM repo IP> указать IP адрес основного сервера АСМ, развернутого согласно « 4.3.2 Развертывание основного сервера АСМ» или IP адрес сервера установки ОС по сети, развернутого согласно разделу « 4.6.4 Установка сервера репозиториев и сервера установки ОС». Выбор используемого сервера производится в зависимости от наличия дополнительного «Сервера установки ОС» и сетевой доступности сервера для подключаемого компьютера клиента:

```
deb http://<ACM repo IP>/astra/frozen/1.7_x86-64/1.7.5/repository-base 1.7_x86-64 main non-free contrib

deb http://<ACM repo IP>/astra/frozen/1.7_x86-64/1.7.5/repository-extended 1.7_x86-64 main contrib non-free

deb http://<ACM repo IP>/acm/frozen/1.x/ 1.0.0 main
```

2) Установить необходимые пакеты:

```
apt update && apt install acm-salt-minion hwinfo
```

4.9 Проверка статуса компьютера клиента

Выполнить вход на портал управления ACM, указав логин и пароль пользователя.

На главной странице портала управления ACM выполнить переход к разделу «Объекты управления» → «Компьютеры». Компьютер, подключенный к ACM согласно раздела « 4.8 Настройка и подключение компьютеров клиентов», отображается в общем списке компьютеров.

5 РАБОТА С СИСТЕМОЙ АСМ

5.1 Управление системой

5.1.1 Сегменты управления

Сегмент АСМ — логическая сущность, которая объединяет управляемые компьютеры (клиенты) и серверы АСМ (сервер агентов) и обеспечивает подключение управляемых компьютеров к ближайшим серверам АСМ для оптимизации использования сетевых подключений.

Границы сегмента АСМ определяются сервером управления агентов: все управляемые компьютеры, подключенные к определенному серверу управления агентов, попадают в сегмент АСМ, к которому относится данный сервер управления агентов. Каждый Сервер управления агентов должен относиться к отдельному сегменту АСМ, не поддерживается подключение 2-х и более активных серверов управления агентами в одном сегменте АСМ.

Основной сегмент АСМ — это первый сегмент, который автоматически создается при установке системы и предназначен для размещения основного репозитория и экземпляра сервиса агентов. При развертывании экземпляр сервиса агентов всегда связывается с основным сегментом. Основной сегмент АСМ не может быть изменен или удален пользователем. Основной сегмент АСМ может содержать, а может и не содержать подключенные управляемые компьютеры.

Создание дополнительного сегмента может потребоваться в следующих случаях:

– Требуется подключить к системе АСМ более 1000 компьютеров клиентов (рекомендуется в один сегмент включать не более 1000 компьютеров).

– Требуется подключить к системе АСМ компьютеры клиенты, расположенные в сегменте сети с ограниченным сетевым доступом (слабые или ненадежные каналы связи или ограничение сетевого доступа в целях ИБ).

После создания записи сегмента необходимо развернуть и настроить сервер управления агентами и указать идентификатор созданного сегмента. Подробнее про установку сервера управления агентами и привязку к сегменту см. в разделе « 4.4 Установка сервера управления агентами АСМ».

Если в сегменте требуется функция первичной установки ОС, то необходимо развернуть в новом сегменте сервер репозиториев и сервер установки ОС, подробнее в разделе « 4.6.4 Установка сервера репозиториев и сервера установки ОС».

При подключении компьютеров в новом сегменте следует выполнить установку клиента АСМ и в конфигурационном файле настройки клиента указать IP адрес сервера управления агентами соответствующего сегмента (подробнее в разделе « 4.8 Настройка и подключение компьютеров клиентов»).

Удаление сегмента возможно, только если к сегменту не привязан ни один сервер.

Возможности пользователя, назначенные на сегменты, распространяются также на серверы. Подробное описание возможностей по управлению Сегментами и действий, которые они предоставляют пользователю, приведено в разделе «Сегменты и серверы».

Подробно операции с сегментами (просмотр, создание, редактирование, удаление) описаны в документе «Руководство оператора».

5.1.2 Серверы АСМ

Сервер АСМ — логическая сущность в системе АСМ, обозначающая экземпляр соответствующего функционального сервиса/сервера, развернутого на сетевом узле (хосте). Развертывание сервиса (сервера) в системе АСМ производится вручную администратором. Добавление сервера в систему АСМ происходит в момент развертывания сервиса. В интерфейсе системы добавление сервера недоступно.

В АСМ версии 1.0.0 Standard в интерфейсе доступен для просмотра функциональный сервер АСМ Сервер агентов — сервер с экземпляром сервиса АСМ, обеспечивающий управление компьютерами клиентами. В одном сегменте может быть развернут только один активный сервер агентов.

Возможности пользователя, назначенные на сегменты, распространяются также на серверы. Подробное описание возможностей по управлению Сегментами и действий, которые они предоставляют пользователю, приведено в разделе «Сегменты и серверы».

Подробно операции с сегментами (просмотр, редактирование, удаление) описаны в документе «Руководство оператора».

5.1.3 Разграничение возможностей

5.1.3.1 Общие сведения о разграничении возможностей в АСМ

Для входа и работы в портале управления АСМ используются учетные записи пользователей. Для входа на портал пользователю необходимо указать имя входа (login) и пароль доменной учетной записи или локальной учетной записи ОС Astra Linux сервера АСМ. Для входа с помощью доменной УЗ пользователю

необходимо ввести имя пользователя с учетом полного доменного суффикса, например user@domain.name. При использовании короткого имени входа, без указания домена (например admin) система АСМ будет использовать для аутентификации локальные УЗ ОС Astra Linux «Основного сервера АСМ».

При первом успешном входе пользователя на портал управления в системе АСМ создается внутренняя учетная запись пользователя, сопоставленная по имени входа (login) с внешней учетной записью (доменной или локальной учетной записи ОС Astra Linux сервера АСМ).

Для определения разрешенных для пользователя операций с объектами АСМ используются «возможности», назначенные на учетную запись пользователя. Возможности определяют, какие операции (чтение, создание, изменение, удаление и т. д.) пользователь может выполнять и с какими именно объектами системы АСМ (директориями, профилями управления, программным обеспечением, образами ОС и т.д.).

В процессе установки системы АСМ создается предустановленная учетная запись со всеми доступными возможностями. Данная учетная запись предназначена для первого входа в систему АСМ и первичной настройки системы. Предустановленная запись не может быть удалена или изменена посредством обычных функций для работы с учетными записями пользователей. Кроме предустановленных УЗ пользователей, в системе АСМ предусмотрены добавленные УЗ, которые по умолчанию не имеют назначенных возможностей (возможности назначает пользователь).

Возможности могут быть назначены непосредственно на учетную запись пользователя или получены при назначении на учетную запись пользователя набора возможностей.

Набор возможностей представляет собой внутренний логический объект системы АСМ и позволяет заранее настроить нужное сочетание возможностей к объектам АСМ для последующего назначения и применения к учетным записям пользователей. На учетную запись пользователя может быть назначено любое количество наборов возможностей. Система АСМ предусматривает некоторое количество предустановленных и преднастроенных наборов возможностей, также администратор системы АСМ может создавать и настраивать любые нужные ему дополнительные наборы возможностей в графическом интерфейсе портала управления. Администратор системы АСМ может назначать или снимать назначение наборов возможностей на учетную запись пользователя в графическом интерфейсе портала управления АСМ.

Итоговые возможности пользователя рассчитываются как результат сложения возможностей, назначенных непосредственно на учетную запись пользователя, и всех наборов возможностей, назначенных на учетную запись пользователя.

Изменение возможностей пользователя применяется при работе с графическим порталом управления сразу же и не требует повторного входа пользователя в систему.

Для удобства настройки возможности настраиваются для определенных категорий объектов системы АСМ (например, возможности для объектов категории «директория», «обнаруживаемое ПО», «профиль первичной установки ОС» и т. д.). При этом могут быть настроены общие возможности для всех экземпляров определенной категории (например, возможность «чтение» для всех директорий), так и возможности для определенного экземпляра (например, возможность «чтение» для определенной директории «Компьютеры офиса А», дающая доступ только к этой директории). Общие возможности распространяются как на существующие в системе, так и создаваемые в дальнейшем объекты этой категории. Подробнее возможности для разных категорий объектов приведены в « 5.1.3.2 Описание возможностей для категорий объектов в АСМ».

В системе АСМ не предусмотрена настройка возможностей непосредственно на записи компьютеров, вместо этого используются возможности, назначенные на директорию, в которой находится запись компьютера.

5.1.3.2 Описание возможностей для категорий объектов в АСМ

Директории и компьютеры

Примечание: Возможности, назначенные на директории, распространяются также на записи компьютеров, входящие в директорию. Возможности на уровне отдельных записей компьютеров в системе АСМ не предусмотрены.

№	Объект	Возможность	Что дает Возможность
1	Директории и компьютеры	Создание	Позволяет создать объект «Директория». На уровне портала управления данная Возможность дает доступ к кнопке «+ Новая директория» и карточке создания новой директории. При создании директории пользователю необходимо выбрать «Родительскую директорию» - либо вариант «Без директории» (для создания корневой директории), либо любую директорию, на которую у

№	Объект	Возможность	Что дает Возможность
			пользователя есть возможность. «Редактировать». После успешного создания директории пользователь-создатель автоматически получает Возможности «Чтение», «Редактирование», «Удаление» к созданной директории. Позволяет создать новую запись компьютера. На уровне портала управления данная Возможность дает доступ к кнопке «+ Новый компьютер». При создании записи компьютера пользователю необходимо выбрать «Родительскую директорию» - любую директорию, на которую у пользователя есть возможность «Редактировать». После создания запись компьютера наследует все возможности, назначенные на выбранную родительскую директорию. Возможность «Создание» может быть назначена только в разделе «Общие возможности».
2	Директории и компьютеры	Чтение	Позволяет просматривать директорию в дереве «Структуры управления» и в списках директорий. Также дает возможность просмотра всех родительских директорий для отображения иерархической структуры дерева директорий. Позволяет перейти на карточку директории и посмотреть значение всех полей директории, а также список компьютеров, входящих в состав директории. Дает возможность «Чтение» на все записи компьютеров, входящих в состав директории: - просмотр записей компьютеров в списке «Компьютеры»;

№	Объект	Возможность	Что дает Возможность
			- включение записи компьютера в сформированный csv отчет по списку компьютеров; - просмотр карточки компьютера и всех данных по компьютеру.
3	Директории и компьютеры	Изменение	Позволяет изменить значение параметров директории: «Название», «Комментарий». Позволяет изменять родительскую директорию (выбор только из числа директорий, на которые так же есть Возможность «Редактирование»). Позволяет создание дочерних директорий. Позволяет изменять состав компьютеров: - удалять компьютеры из состава директории (при этом удаленные из состава директории компьютеры будут автоматически помещены системой АСМ в «Директория по умолчанию», если у пользователя нет возможностей на «Директория по умолчанию», он потеряет доступ к записям компьютеров); - добавлять компьютеры в состав директории (при добавлении компьютера в состав директории требуется дополнительно возможность «Редактирование» на исходную директорию добавляемого компьютера). Дает возможность «Редактирование» для всех записей компьютеров, находящихся в составе директории (например, изменение поля «Комментарий», изменение директории компьютера, но только на ту директорию, на которую у пользователя также есть возможность «Редактирование»). *Примечание: при предоставлении*

№	Объект	Возможность	Что дает Возможность
			возможности «Редактирование» система АСМ автоматически добавляет возможность «Чтение».
4	Директории и компьютеры	Удаление	Позволяет удалять директорию. При удалении директории все компьютеры, входящие в состав удаляемой директории, не удаляются из системы, а переносятся системой в директорию «Директория по умолчанию» (если у пользователя нет возможностей на «Директория по умолчанию», то он потеряет доступ к записям компьютеров). Дает возможность «Удаление» для всех записей компьютеров, входящих в состав директории - пользователь может удалить любую запись компьютера, входящую в директорию (если нет других ограничений системы, например статус агента «Активен» для данной записи компьютера). *Примечание: при предоставлении возможности «Удаление» система АСМ автоматически добавляет возможность «Чтение».*

Сегменты и серверы

Примечание: В АСМ версии 1.0.0 Standard возможности, назначенные для сегментов, распространяются также на серверы АСМ, подключенные в данном сегменте.

№	Объект	Возможность	Что дает Возможность
1	Сегмент (сервер)	Создание	Позволяет создать объект «Сегмент». На уровне портала управления данная Возможность дает доступ к кнопке «+ Новый сегмент» и карточке создания нового сегмента. При создании сегмента, пользователь-

№	Объект	Возможность	Что дает Возможность
			создатель автоматически получает Возможности «Чтение», «Изменение», «Удаление» к созданному сегменту. Возможность «Создание» может быть назначена только в разделе «Общие возможности».
2	Сегмент (сервер)	Чтение	Позволяет просматривать сегмент в списке сегментов. Позволяет перейти на карточку сегмента и посмотреть свойства сегмента, скопировать значение «Уникального идентификатора» сегмента. Позволяет просматривать серверы АСМ, подключенные к данному сегменту, в списке серверов. Позволяет перейти на карточку сервера АСМ, подключенного к данному сегменту, и посмотреть информацию о сервере АСМ.
3	Сегмент (сервер)	Изменение	Позволяет изменить параметры сегмента: «Название», «Комментарий». Позволяет изменить параметры сервера АСМ, подключенного к сегменту: поле «Комментарий». *Примечание: при предоставлении возможности «Изменение» система АСМ автоматически добавляет возможность «Чтение».*
4	Сегмент (сервер)	Удаление	Позволяет удалить сегмент (если нет других ограничений системы, например наличие подключенных к сегменту серверов, или сегмент является предустановленным «Основным сегментом»). Позволяет удалить сервер АСМ, подключенный к сегменту. *Примечание: при предоставлении*

№	Объект	Возможность	Что дает Возможность
			возможности «Удаление» система АСМ автоматически добавляет возможность «Чтение».

Наборы Возможностей и пользователи

№	Объект	Возможность	Что дает Возможность
1	Наборы Возможностей и пользователи	Разрешить операции с УЗ пользователей, набором возможностей и предоставлением возможностей	Предоставляет пользователю все возможности для УЗ пользователей (просмотр, изменение параметров, назначение наборов возможностей, управление предоставленными пользователю возможностями, удаление УЗ пользователя) и наборов возможностей (создание, просмотр, изменение, управление предоставленными возможностями, назначение на УЗ пользователей, удаление набора).

Лицензии ПО

Примечание: Для категории объектов «Лицензии» можно назначить только общие возможности для всех объектов, не предусмотрено назначение возможностей на отдельные типы лицензий.

№	Объект	Возможность	Что дает Возможность
1	Лицензии ПО	Чтение	Позволяет просматривать список лицензий, добавленных в учет. Позволяет просматривать карточку лицензии, параметры лицензии и список компьютеров, соответствующих лицензии такого типа.
2	Лицензии ПО	Изменение	Позволяет добавлять лицензии в учет и удалять лицензии из учета. Позволяет изменить количество имеющихся лицензий такого типа на карточке лицензии. *Примечание: при предоставлении возможности «Изменение» система АСМ*

№	Объект	Возможность	Что дает Возможность
			автоматически добавляет возможность «Чтение».

Обнаружение ПО

№	Объект	Возможность	Что дает Возможность
1	Обнаруживаемое ПО	Создание	Позволяет создать объект «Обнаруживаемое ПО». На уровне портала управления данная Возможность дает доступ к кнопке «+ Новое ПО» и карточке для создания нового обнаруживаемого ПО. При создании Обнаруживаемого ПО пользователь-создатель автоматически получает Возможности «Чтение», «Изменение», «Удаление». Возможность «Создание» может быть назначена только в разделе «Общие возможности».
2	Обнаруживаемое ПО	Чтение	Позволяет просматривать обнаруживаемое ПО в списке «Обнаружение ПО». Позволяет перейти на карточку «Обнаруживаемого ПО» и посмотреть основные параметры и значения объекта, посмотреть назначенные правила обнаружения ПО и их параметры. *Примечание: Возможность «Чтение» не распространяется на просмотр инвентарных данных компьютера - список обнаруженного ПО на вкладке «Инвентаризация» карточки компьютера будет доступен пользователю, имеющему возможность «Чтение» к записи компьютера и не имеющему никаких возможностей к объектам «Обнаружение ПО».*
3	Обнаруживаемое ПО	Изменение	Позволяет изменить объект «Обнаруживаемое ПО»:

№	Объект	Возможность	Что дает Возможность
			- изменить данные в основных параметрах (название, версия, производитель, тип ПО, комментарий и т.п.); - изменить правила обнаружения, связанные с данным объектом «Обнаруживаемое ПО» - добавить новые правила, изменить условия существующих правил, удалить правила обнаружения ПО. *Примечание: при предоставлении возможности «Изменение» система АСМ автоматически добавляет возможность «Чтение».*
4	Обнаруживаемое ПО	Удаление	Позволяет удалить объект «Обнаруживаемое ПО». *Примечание: при предоставлении возможности «Удаление» система АСМ автоматически добавляет возможность «Чтение».*

Профиль установки ОС

№	Объект	Возможность	Что дает Возможность
1	Профиль установки ОС	Создание	Позволяет создать объект «Профиль установки ОС». На уровне портала управления данная Возможность дает доступ к кнопке «+ Новый профиль» и карточке для создания нового профиля установки ОС. При создании Профиля установки ОС пользователь-создатель автоматически получает Возможности «Чтение», «Изменение», «Удаление» к созданному профилю установки ОС. Возможность «Создание» может быть назначена только в разделе «Общие возможности».
2	Профиль	Чтение	Позволяет просматривать профиль

№	Объект	Возможность	Что дает Возможность
	установки ОС		установки ОС в списке профилей. Позволяет перейти на карточку профиля установки ОС и посмотреть свойства и параметры, параметры Preseed и Postinstall, установленные для профиля.
3	Профиль установки ОС	Изменение	Позволяет изменить значение параметров профиля установки ОС: «Название», «Комментарий», «Preseed», «Postinstall». Позволяет изменить статус профиля - включать, выключать (при условии соблюдения других ограничений и требований по работе с профилями установки ОС). Позволяет назначить профиль установки ОС профилем по умолчанию (при условии соблюдения других ограничений и требований по работе с профилями установки ОС). *Примечание: при предоставлении возможности «Изменение» система АСМ автоматически добавляет возможность «Чтение».*
4	Профиль установки ОС	Удаление	Позволяет удалить объект «Профиль установки ОС» (при условии соблюдения других требований и ограничений системы: например удаление разрешено только для профилей в состоянии «выключено»). *Примечание: при предоставлении возможности «Удаление» система АСМ автоматически добавляет возможность «Чтение».*

Отчеты

№	Объект	Возможность	Что дает Возможность
1	Отчеты	Разрешить формирование и просмотр отчетов	Позволяет пользователю сформировать и загрузить отчет (csv) по списку компьютеров и по данным инвентаризации отдельного компьютера. *Примечание: в отчет csv попадут только те записи компьютеров, на которые у пользователя есть возможность «Чтение».*

5.1.3.3 Пользователи АСМ

В процессе установки системы АСМ создается предустановленная учетная запись со всеми возможностями. Данная учетная запись предназначена для первого входа в систему АСМ и первичной настройки системы. Предустановленная запись не может быть удалена или изменена посредством обычных функций для работы с учетными записями пользователей.

Примечание: не допускается назначение наборов возможностей для встроенной учетной записи пользователя.

Для повышения безопасности эксплуатации и администрирования системы АСМ нужно создать записи пользователей с типом «Добавленная». Добавленная учетная запись пользователя создается автоматически системой АСМ при первом успешном входе на портал управления с доменной УЗ или локальной УЗ ОС Astra Linux сервера АСМ. Для входа с помощью доменной УЗ пользователю необходимо ввести имя пользователя с учетом полного доменного суффикса, например user@domain.name.

Примечание: при использовании короткого имени входа, без указания домена (например admin) система АСМ будет использовать для аутентификации локальные УЗ ОС Astra Linux Основного сервера АСМ.

Данные пользователя, представленные на вкладке «Основное» карточки пользователя, не синхронизируются с внешними системами и хранятся исключительно в системе АСМ. Для идентификации используется имя входа учетной записи.

Только что созданная добавленная учетная запись пользователя не обладает набором возможностей по умолчанию. После первого успешного входа и создания добавленной учетной записи пользователя требуется настроить необходимые возможности для учетной записи: либо назначив на запись имеющиеся наборы

возможностей, либо настроив возможности непосредственно в параметрах самой учетной записи пользователя.

Для упрощения администрирования системы рекомендуется использовать наборы возможностей вместо назначения возможностей непосредственно на учетную запись пользователя.

Возможности в системе АСМ могут распространяться как на категорию объектов в целом, так и на единичный экземпляр объекта. Установка или снятие возможности в панели «Общие возможности» не приводит к установке или снятию аналогичной возможности в панели «Возможности для экземпляров категории объектов», но учитывается независимо от них при проверке прав доступа.

При просмотре объектов в АСМ производится отображение только тех объектов, к которым пользователь, устанавливающий возможности, имеет возможность «Чтение». Поэтому важно назначить для администратора, выполняющего назначение возможностей другим пользователям, соответствующие возможности на чтение объектов в системе АСМ.

Возможности назначенного на пользователя набора возможностей и отдельные возможности, назначенные на пользователя на вкладке «Возможности», существуют как независимые друг от друга наборы возможностей. Если пользователь имеет назначенный набор возможностей и дополнительные возможности, выданные на вкладке «Возможности», с точки зрения взаимодействия с объектами управления системы эти возможности суммируются.

Подробное описание возможностей по управлению пользователями и действий, которые они предоставляют пользователю, приведено в разделе «Наборы Возможностей и пользователи».

В АСМ существуют записи пользователей, не подлежащие удалению. К ним относятся:

– предустановленная запись пользователя, указанная в процессе установки системы;

– собственная учетная запись пользователя, под которым выполнен вход на портал управления.

Подробно операции с пользователями (просмотр, создание, редактирование, удаление) описаны в документе «Руководство оператора».

5.1.3.4 Наборы возможностей

Набор возможностей — это предустановленный или выбранный администратором набор возможных операций в системе АСМ, назначаемый пользователям. Наборы возможностей созданы для быстрого назначения возможностей на

большое количество пользователей.

При установке системы АСМ автоматически создаются встроенные наборы возможностей, предназначенные для упрощения настройки системы. Встроенные наборы возможностей не могут быть удалены или изменены вручную посредством обычных функций для работы с наборами возможностей. Использование встроенных наборов возможностей остается на усмотрение администратора системы АСМ — если данные наборы не подходят или не удобны, можно создать и использовать собственные добавленные наборы возможностей, назначив им необходимые сочетания возможностей.

Встроенные наборы возможностей:

– Главный администратор;
– Пользователь отчетов.

Набор возможностей «Главный администратор» имеет возможности на создание, чтение, редактирование и удаление ко всем объектам управления системы и всем директориям системы.

Набор возможностей «Пользователь отчетов» имеет возможности на чтение ко всем ко всем объектам управления системы и всем директориям системы.

Примечание: указанное название создаваемого набора возможностей не должно совпадать с уже существующими в системе наборами возможностей.

Если (добавленный) набор возможностей назначен на УЗ пользователей, то пользователь не может удалить такой набор возможностей. Сначала необходимо снять назначение набора со всех УЗ пользователей. Встроенный набор возможностей удалить из системы невозможно.

Подробное описание возможностей по управлению наборами возможностей и действий, которые они предоставляют пользователю, приведено в разделе «Наборы Возможностей и пользователи».

Подробно операции с наборами возможностей (создание, просмотр, редактирование, удаление) описаны в документе «Руководство оператора».

5.2 Объекты управления

5.2.1 Структура управления

Структура управления — древовидная (иерархическая) структура директорий. Директория — это внутренний объект системы АСМ, позволяющий группировать записи компьютеров для настройки и выполнения действий по управлению.

Кроме того, директория предназначена для назначения возможностей пользователя системы АСМ для выполнения действий с записями компьютеров, вхо-

дящих в её состав. Назначение возможностей непосредственно на запись компьютера в системе АСМ не предусмотрены, возможности назначаются на директории. Возможности пользователя, назначенные на структуры управления, распространяются также на компьютеры. Подробное описание возможностей по управлению Структурами управления и действий, которые они предоставляют пользователю, приведено в разделе «Директории и компьютеры».

Запись компьютера обязательно должна входить в состав какой-либо директории. Запись компьютера может в один момент времени находиться только в одной директории: при переносе записи компьютера в другую директорию, запись компьютера удаляется из предыдущей директории.

В АСМ версии 1.0.0 Standard при первом доступе к разделу «Структура управления» после установки системы данный раздел сразу содержит «Директорию по умолчанию». «Директория по умолчанию» является предустановленной системной директорией и создается автоматически при установке системы АСМ.

Системная директория «Директория по умолчанию» не может быть удалена или изменена вручную пользователем АСМ. Но пользователь может добавлять и удалять компьютеры в составе «Директории по умолчанию», назначать возможности, так же, как на любую другую директорию, созданную вручную.

Системная директория «Директория по умолчанию» не может являться родительской или дочерней для любой другой созданной вручную директории.

Новые записи компьютеров, созданные в системе АСМ, по умолчанию попадают в состав системной директории «Директория по умолчанию», если не была явно указана другая родительская директория при создании записи компьютера.

Если директория имеет дочерние директории, то удаление такой директории запрещено.

Подробно операции с директориями (просмотр, создание, редактирование, удаление) описаны в документе «Руководство оператора».

5.2.2 Компьютеры

Идентификация записей компьютеров в системе АСМ осуществляется на основании сетевого имени компьютера.

Запись компьютера может быть добавлена автоматически при установке агента и подключении компьютера к системе управления АСМ. Также запись компьютера может быть создана вручную администратором с помощью интерфейса портала управления.

Добавление записи компьютера в систему АСМ вручную не приводит к ав-

томатической установке программного модуля агента и подключению компьютера к системе АСМ.

Назначение возможностей непосредственно на запись компьютера в системе АСМ не предусмотрены, возможности назначаются на директорию и распространяются на все записи компьютеров, которые входят в эту директорию. Подробное описание возможностей по управлению Структурами управления и действий, которые они предоставляют пользователю, приведено в разделе «Директории и компьютеры».

Наличие программного модуля агента и подключение компьютера к системе АСМ можно проверить по значению «Статус агента»:

– Статус агента «Активен» означает, что на компьютере установлен программный модуль агент, компьютер подключен к системе АСМ.

– Статус агента «Недоступен» означает, что на компьютере был установлен программный модуль агент, однако была потеряна связь с сервером АСМ в течении установленного в настройках сервера периода времени.

– Статус агента «Неизвестно» означает, что на компьютере либо не был установлен программный модуль агента (например, запись компьютера была добавлена в систему вручную), либо агент потерял связь с сервером АСМ в течение установленного в настройках сервера периода времени.

В системе АСМ можно удалить только записи компьютеров, статус агента которых в значении «Неизвестно». Если статус агента находится в значении «Активен» или «Недоступен», то удалить запись такого компьютера нельзя.

Подробно операции с компьютерами (просмотр, создание, редактирование, удаление) описаны в документе «Руководство оператора».

5.3 Инвентаризация

5.3.1 Обнаружение ПО

Обнаружение ПО — это обработка собранных с компьютеров инвентарных данных и создание связей между управляемым компьютером и ПО на основе имеющихся правил обработки инвентарных данных. Правила обработки создаются пользователем системы АСМ с использованием графического интерфейса портала управления: администратор указывает, какое именно ПО нужно обнаруживать: название ПО, версию ПО, тип ПО из предустановленного списка и критерии — на основании каких пакетов ПО система АСМ должна сделать вывод о наличии данного ПО на компьютере. Процесс обнаружения ПО запускается в системе АСМ автоматически в случае создания или изменения правил обнаружения ПО или в случае изменения инвентарных данных, собранных с управляемых

компьютеров. В результате работы обнаружения ПО на основе собранных в системе АСМ инвентарных данных формируется актуальный список ПО, установленного на компьютере. Актуальный список обнаруженного ПО можно увидеть на карточке компьютера в разделе «Инвентаризация» в категории «Программное обеспечение».

Создание, удаление, редактирование правил обнаружения ПО выполняется пользователем системы АСМ, обладающим соответствующими возможностями. Подробное описание возможностей по управлению Обнаружением ПО и действий, которые они предоставляют пользователю, приведено в разделе «Обнаружение ПО».

Подробно операции с Обнаружением ПО (просмотр, создание, редактирование, удаление) описаны в документе «Руководство оператора».

5.3.2 Лицензии ПО

В АСМ версии 1.0.0 Standard представлена функция учета лицензий только для ОС Astra Linux.

Для каждой добавленной в учет версии лицензии ОС Astra Linux система АСМ на основе собранных инвентарных данных произведет расчет количества компьютеров, которым соответствует эта версия и представит список компьютеров.

Пользователь АСМ может также указать количество лицензий ОС Astra Linux той или иной версии, имеющееся у организации — для автоматического расчета недостатка или остатков по использованию лицензий.

Подробное описание возможностей по управлению Лицензиями ПО и действий, которые они предоставляют пользователю, приведено в разделе «Лицензии ПО».

Подробно операции с лицензиями (просмотр, добавление, редактирование, удаление) описаны в документе «Руководство оператора».

5.4 Управление установкой ОС

5.4.1 Процесс настройки первичной (bare-metal) установки ОС в АСМ

Примечание: В АСМ версии 1.0.0 Standard поддерживается установка версий ОС Astra Linux 1.7.x.

Функция первичной (bare-metal) установки ОС по сети на компьютеры клиенты выполняется в следующем порядке:

1) Администратору необходимо установить и настроить «Сервер установки ОС АСМ» для выполнения функции. Сервер установки ОС по сети обеспечивает

непосредственное взаимодействие с целевым компьютером, управление процессом установки ОС, предоставление пакетов устанавливаемой ОС. Требуется обеспечить быстрое и надежное подключение по сети между сервером установки ОС и компьютерами, на которых будет выполняться установка ОС по сети. Если есть удаленные региональные офисы с ненадежными каналами связи или выделенные сегменты сети с ограниченным доступом, в которых требуется функция установки ОС по сети, рекомендуется развернуть в них выделенные серверы установки ОС.

Примечание: В системе АСМ может быть установлено любое количество серверов установки ОС по сети. Допускается установка нескольких серверов установки ОС по сети в одном сегменте АСМ. Допускается отсутствие сервера установки ОС по сети в сегменте АСМ.

В АСМ версии 1.0.0 Standard установка, настройка и управление сервером установки ОС АСМ осуществляется администратором вручную в соответствии с представленными инструкциями и требованиями. Сервер установки ОС по сети не создается в системе АСМ в качестве логического объекта и не представлен в портале управления АСМ в качестве управляемого объекта.

Важно: для корректной работы функции установки ОС по сети в сетевой инфраструктуре должен быть настроен и доступен для компьютеров клиентов сервис DHCP (сервис динамической адресации).

Описание действий по установке и настройке всех необходимых компонент (в том числе требования по настройке инфраструктурных сервисов) приведены в разделе « 5.4 Управление установкой ОС».

2) Администратору необходимо подготовить установочные пакеты устанавливаемой ОС Astra Linux. Требуются основной (base) репозиторий для установки ОС Astra Linux и расширенный (extended) репозиторий для установки дополнительных пакетов ПО и системных компонент. Для этого требуется скопировать необходимые репозитории, предоставляемые вендором, и разместить их в центральном репозитории АСМ. Далее необходимо убедиться, что выполнилась синхронизация репозиториев и добавленные каталоги были скопированы на все серверы установки ОС АСМ.

3) Администратору АСМ требуется настроить с помощью портала управления АСМ профиль первичной установки ОС. Профиль первичной установки ОС представляет собой управляющий объект системы АСМ и позволяет настроить:

– параметры Preseed — содержит описание конфигурации устанавливаемой системы, использующееся мастером установки ОС Astra

Linux, например, параметры разбиения дискового пространства, создание УЗ пользователя, выбор часового пояса и локализации устанавливаемой ОС и т.д.

– параметры Postinstall — содержит скрипт для первичной настройки установленной ОС, например, может содержать установку необходимого ПО, включение и запуск системных сервисов, установку значения переменных, копирование необходимых файлов конфигурации и т.п.

Может быть настроено любое необходимое количество профилей первичной установки ОС. Описание действий по созданию и настройке профиля первичной установки ОС приведено в разделе « 5.4.3 Профили установки ОС (первичная установка ОС)». При настройке параметров Preseed профиля первичной установки ОС потребуется указать путь к каталогу репозитория, подготовленному на шаге 2. Описание параметров Preseed и требований по его настройке приведено в разделе « 5.4.4 Настройка Preseed». Настройка параметров Preseed является обязательной для корректной работы профиля первичной установки ОС. Настройка параметров Postinstall является обязательной для корректной работы профиля первичной установки ОС. Рекомендации по настройке Postinstall приведены в разделе « 5.4.5 Настройка Postinstall».

По умолчанию профиль первичной установки создается в состоянии «Выключено». После того, как все параметры профиля настроены, и профиль готов для загрузки на серверы установки ОС, администратор должен «Включить» профиль (на карточке профиля портала управления). После включения информация о настройках профиля первичной установки ОС передается на все серверы установки ОС АСМ и он может быть использован для установки ОС на компьютеры клиенты.

На сервер установки ОС АСМ передаются только профили в состоянии «Включено». Профили в состоянии «Выключено» присутствуют в системе АСМ и доступны для изменения со стороны администратора, но на серверы установки ОС не передаются.

4) Настройка профиля по умолчанию. Может быть подготовлено и включено любое необходимое количество профилей первичной установки ОС. При наличии в системе более одного профиля первичной установки ОС в состоянии «Включено», администратор может указать в настройках, какой из профилей будет использоваться по умолчанию. Данный профиль будет использоваться на компьютере клиенте, если администратор не выбрал вручную любой другой из предлагаемых профилей в течение определенного времени таймаута (по умолчанию 50 сек.).

После этого сервер установки ОС считается подготовленным и настроенным для выполнения первичной (bare-metal) установки ОС по сети на обратившееся компьютеры клиенты.

5.4.2 Процесс первичной установки ОС на компьютер клиент в АСМ

Процесс первичной (bare-metal) установки ОС на компьютеры клиенты выглядит следующим образом:

На компьютере клиенте в настройках BIOS (или UEFI) должен быть установлен параметр загрузки устройства по сети (PXE).

После включения компьютер клиент:

1. получает от сервера DHCP динамический IP адрес и другие параметры сетевого подключения;
2. получает от сервера АСМ параметры для первоначальной загрузки по сети.

   Примечание: в п. 2 используется инфраструктурный сервер DHCP, который должен быть настроен и доступен для компьютера клиента. DHCP сервер не входит в состав компонент АСМ.

Если в системе АСМ было создано несколько профилей первичной установки ОС в состоянии «Включено», то на компьютере клиенте отображается текстовое меню для выбора нужного варианта. По умолчанию по истечению таймаута (указанного в конфигурационном файле сервера установки ОС) производится выбор варианта установки, указанного по умолчанию.

Производится установка ОС на компьютер клиент в соответствии с параметрами, настроенными в профиле первичной установки. При этом используются пакеты ПО, размещенные на сервере установки ОС и указанные в настройках Preseed профиля первичной установки ОС.

5.4.3 Профили установки ОС (первичная установка ОС)

Профиль первичной установки ОС — это логический объект, позволяющий настроить параметры установки ОС: используемые пакеты образа ОС Astra Linux 1.7.x, параметры Preseed и Postinstall, определяющие параметры установки и первичной настройки устанавливаемой ОС.

Профиль первичной установки ОС может быть в состоянии:

– «Включено» — профиль распространяется и применяется системой АСМ на развернутых серверах установки ОС АСМ, предлагается как один из вариантов для использования в процессе установки ОС на компьютеры клиенты.

– «Выключено» — профиль в таком состоянии удаляется из настроек серверов установки ОС АСМ и не используется в процессе установки ОС на компьютеры клиенты. При этом профиль остается в системе АСМ и может использоваться в дальнейшем. В основном состояние «Выключено» предназначено для редактирования параметров профилей или временного отключения профиля из списка используемых.

Настройка профилей первичной установки ОС осуществляется в графическом интерфейсе портала управления АСМ. Однако есть ряд действий, которые администратору требуется выполнить перед созданием или настройкой профиля первичной установки ОС:

– опубликовать необходимые пакеты устанавливаемой версии ОС Astra Linux 1.7.x на сервисе репозиториев;

– подготовить и проверить настройки Preseed и Postinstall для указания в настройках профиля первичной установки ОС.

Для перевода профиля в состояние "Включено" параметр Preseed является обязательным для заполнения.

Создание, удаление, редактирование профилей первичной установки ОС выполняется пользователем системы АСМ, обладающим соответствующими возможностями. Подробное описание возможностей по управлению Профилями первичной установки ОС и действий, которые они предоставляют пользователю, приведено в разделе «Профиль установки ОС».

Подробно операции с профилями (создание, просмотр, редактирование, удаление) описаны в документе «Руководство оператора».

5.4.4 Настройка Preseed

В системе АСМ при первичной установке ОС Astra Linux по сети используется preseeding – метод частичной автоматизации установки операционной системы, который позволяет заранее указать ответы на вопросы, задаваемые при установке, и автоматически сконфигурировать часть настроек при установке ОС.

Файл Preseed — разновидность конфигурационного файла, содержащего параметры, необходимые для автоматической установки ОС.

Примечание: Команда `d-i preseed/late_command` *зарезервирована системой АСМ и не может быть использована в пользовательском Preseed (любой пользовательский* `d-i preseed/late_command` *не будет выполнен). Команды, которые пользователь планирует поместить в* `d-i preseed/late_command`*, необходимо прописать в скрипте Postinstall.*

В скрипте Preseed могут быть использованы переменные. Переменные для Preseed настраиваются в конфигурационном файле сервиса установки ОС. На данный момент доступна следующая переменная:

${osdeploy_ip} — содержит адрес сервера установки ОС (сервера репозиториев) в виде IP адреса или доменного имени. Переменная обязательна к использованию в команде d-i mirror/http/hostname string ${osdeploy_ip}.

Все остальные параметры Preseed файла (Настройка языка, Настройка разбиения диска, Добавление пользователя по умолчанию и т.д.) могут быть изменены в соответствии с требованиями к структуре файла ответов Preseed и рекомендациями вендора.

Для подготовки файла Preseed можно использовать описание по установке ОС Astra Linux v1.7 и v1.6 с использованием файла Preseed, которое доступно в Справочном центре Astra Linux.

5.4.5 Настройка Postinstall

В системе АСМ при первичной установке ОС Astra Linux по сети используется файл Postinstall – скрипт первичной настройки, выполняющийся однократно сразу же после установки ОС. Может быть указан bash скрипт, выполняющий нужные команды и действия.

На вкладке Postinstall может быть указан скрипт, выполняющий первичную настройку ОС после установки. Например, такой скрипт может содержать команды для:

- подключения необходимых репозиториев;
- установки ПО и пакетов ПО;
- включения и запуска необходимых системных компонент и сервисов;
- заполнения конфигурационных файлов и установки необходимых значений системных переменных.

Примечание: Система АСМ автоматически добавляет в Postinstall файл действия по установке программного модуля агента АСМ и подключению агента к серверу АСМ, дополнительных действий от пользователя по установке этих компонентов не требуется. Данные действия выполняются даже в том случае, когда Postinstall в профиле не был заполнен.

В скрипте Postinstall могут быть использованы переменные. Переменные для Postinstall настраиваются в конфигурационном файле сервиса установки ОС. На данный момент доступна следующая переменная:

${osdeploy_ip} — содержит адрес сервера установки ОС (сервера репозиториев) в виде IP адреса или доменного имени.

6 ДИАГНОСТИКА ОШИБОК И СПОСОБЫ РАЗРЕШЕНИЯ

6.1 Возможные ошибки при работе с веб порталом управления АСМ

В таблице ниже приведены возможные сообщения об ошибках, которые могут появляться при работе с веб порталом управления АСМ.

Тип ошибки	Описание ошибки	Вероятные сценарии возникновения ошибки и рекомендации по устранению
400 Bad Request Неверный запрос	Используется в операциях удаления записей. Операция завершается с данным кодом при невыполнении условий для удаления записи (попытка удалить запись, имеющую связанные записи в БД) или объект управления по умолчанию.	Ошибки с таким статусом могут возникать в случае: 1. Попытка удаления предустановленного (или встроенного) объекта, удаление которого запрещено системой. Например, попытка удалить предустановленный «Основной сегмент» или предустановленный набор возможностей «Главный администратор». Предустановленные (или встроенные) объекты предназначены для обеспечения корректной работы системы АСМ и не могут быть удалены пользователем. 2. Попытка удаления объекта, имеющего связи с другими зависящими от него объектами. Необходимо уточнить, не связан ли объект управления, который пользователь пытается удалить, с другими объектами. Необходимо удалить все связи со сторонними объектами управления и повторно удалить объект. Например, сегмент не может быть удален, если к нему привязаны функциональные серверы.
401 Unauthorized Неавторизованный запрос	Используется во всех операциях. Операция завершается с данным кодом при условии отсутствия или истечения срока жизни токена входа в систему.	Ошибки с таким статусом могут возникать в случае нарушения входа пользователя в систему. При получении ошибки с таким статусом рекомендуется завершить текущую сессию (выйти из текущей сессии) и заново выполнить вход в систему.
403 Forbidden	Используется во всех	Ошибки с таким статусом могут

Тип ошибки	Описание ошибки	Вероятные сценарии возникновения ошибки и рекомендации по устранению
Нарушение прав доступа	операциях. Операция завершается с данным кодом при отсутствии возможностей к объектам управления или операциям с объектами.	возникать, если у пользователя недостаточно возможностей для выполнения действия. Например, пользователь пытается внести изменения в объект, на который у него нет возможности «Изменение». Для устранения ошибки рекомендуется проверить наличие у пользователя возможности на действия и объект, которые вызвали ошибку. Предоставить дополнительные возможности на нужные действия и объект можно на странице «Управление системой» > «Разграничение возможностей».
404 Not Found Данные не найдены	Используется в операциях получения записи объекта. Операция завершается с данным кодом при невыполнении условий для поиска записи (*отсутствие записи*).	Ошибка с таким статусом возникает, если при работе с графическим порталом управления указан адрес несуществующего ресурса. Для устранения ошибки необходимо вернуться на главную страницу портала управления и попробовать повторить переход в нужный раздел или к нужному объекту системы АСМ.
409 Conflict Конфликт данных	Используется в операциях создания и обновления записей. Операция завершается с данным кодом при условии выполнения ожидаемого сценария создания записи с параметрами уже существующей записи, либо редактирования параметров существующей записи до схожих параметров другой существующей записи.	Ошибка с таким статусом может возникать в случае: 1. Попытка создать объект, название которого совпадает с уже имеющимся в системе объектом. Например, при попытке создать директорию с именем уже существующей директории 2. Попытка изменить название объекта и совпадения названия с уже существующим объектом. Необходимо убедиться, что вводимые параметры для создаваемого или редактируемого объекта не дублируют данные уже существующего объекта такого типа, и выбрать другое название в случае совпадения.

Тип ошибки	Описание ошибки	Вероятные сценарии возникновения ошибки и рекомендации по устранению
412 Precondition Failed Предварительное условие не выполнено	Используется в операциях изменения записей. Операция завершается с данным кодом при попытке параллельного одновременного изменения одной и той же записи.	Ошибка с таким статусом может возникать при попытке сохранить изменения какого-либо объекта (например, сохранить измененный комментарий на карточке директории), если параметры объекта были изменены в другой сессии портала управления другим пользователем системы. Необходимо обновить (F5) карточку редактируемого объекта, чтобы загрузились изменения, внесенные в другой сессии портала управления, и повторить изменение параметров.
422 Unprocessable Content Валидация не пройдена	Используется во всех операциях. Операция завершается с данным кодом при условии ошибки валидации значений параметров и наличия значений в параметрах.	Ошибка с таким статусом может возникать в случае: 1. Попытка создать объект, указав значения параметров, не удовлетворяющие требованиям системы. Например, при попытке создать директорию с названием, содержащим специальный символ %. 2. Попытка изменить объект, указав значения параметров, не удовлетворяющие требованиям системы. Необходимо убедиться, что при вводе данных указаны все необходимые данные и эти данные корректны (например, к обязательным полям могут предъявляться дополнительные требования по заполнению: наличие или отсутствие определенных символов, раскладки клавиатуры и т. д.).
429 Too Many Requests Превышен лимит запросов	Используется в операциях получения записи объекта. Операция завершается с данным кодом при получении множественных запросов на генерацию отчетов	Необходимо однократно нажать на кнопку «Выгрузить отчет» и дождаться завершения формирования и выгрузки файла отчета.

Тип ошибки	Описание ошибки	Вероятные сценарии возникновения ошибки и рекомендации по устранению
	(пользователь за краткий промежуток времени многократно нажимает на кнопку «Выгрузить отчет»).	
500 Internal Server Error Внутренняя ошибка или непредвиденное исключение	Используется во всех операциях. Операция завершается с данным кодом при отказе сервисов в работе или возникновении новой, не описанной выше ошибки.	Необходимо убедиться, что: 1. Задействованные сервисы активны и работают корректно. 2. В случае, если ошибка не вызвана нарушением работы сервисов, рекомендуется обратиться в техническую поддержку.

6.2 Регистрационные сообщения серверных компонент

Серверные компоненты ACM представлены набором сервисов в зависимости от функциональной роли.

Каждый сервис ACM создает файл с регистрационными сообщениями в каталоге /var/log/unit-acm/, имя файла соответствует названию сервиса, например acm-configuration-service.log. Исключением является сервис ПУА (amp-runner), который создает файл логов в /var/log/amp/default.log.

При создании регистрационных сообщений создается два файла:

1) <*название_сервиса*>.log, содержащий информационные сообщения о работе сервиса;

2) <*название_сервиса*> _err.log, содержащий сообщения об ошибках.

Уровень логирования определяется значением переменной LOG_LEVEL в конфигурационном файле /opt/<название_сервиса_ACM>/dev.env. Значения переменной представлены в таблице ниже:

Значение переменной	Описание
Debug (10)	Самый низкий уровень логирования, предназначенный для отладочных сообщений, для вывода диагностической информации о приложении.
Info (20)	Уровень предназначен для вывода данных о фрагментах кода, работающих так, как ожидается.

Значение переменной	**Описание**
Debug (10)	Самый низкий уровень логирования, предназначенный для отладочных сообщений, для вывода диагностической информации о приложении.
Warning (30)	Уровень логирования предусматривает вывод предупреждений, применяется для записи сведений о событиях, на которые требуется обратить внимание. Такие события вполне могут привести к проблемам при работе приложения. Если явно не задать уровень логирования — по умолчанию используется именно warning.
Error (40)	Уровень логирования предусматривает вывод сведений об ошибках — о том, что часть приложения работает не так как ожидается, о том, что программа не смогла правильно выполниться.
Critical (50)	Уровень используется для вывода сведений об очень серьёзных ошибках, наличие которых угрожает нормальному функционированию всего приложения. Если не исправить такую ошибку — приложение прекратит работу.

Сервис ПУА (amp-runner) по умолчанию использует уровень логирования ERROR и не предполагает ручной настройки уровня логирования администратором.

В случае проблем с серверными компонентами рекомендуется передать файлы с регистрационными сообщениями сервисов в техническую поддержку и далее следовать указаниям специалистов технической поддержки.

Регистрационные сообщения инфраструктурных компонент (СУБД PostgreSQL, брокер сообщений RabbitMQ и т.д.) доступны в соответствии с настройками этих инфраструктурных компонент.

ПРИЛОЖЕНИЕ. ПАРАМЕТРЫ ПЕРЕМЕННЫХ КОНФИГУРАЦИОННОГО ENV ФАЙЛА

Переменные сервера установки ОС

export PXE_INTERFACE=""

Необходимо указать наименование сетевого интерфейса сервера установки ОС АСМ, с которого будет производиться установка ОС.

export PXE_SUBNET=""

Необходимо указать адрес подсети, с которой работает DHCP сервер, без указания маски.

export OSDEPLOY_IP=""

Необходимо указать IP адрес сервера, на котором будет развернут Сервер установки ОС.

Пароли для подключения к объектам инфраструктуры

export DB_PASSWORD="password"

Необходимо задать пароль УЗ для подключения к СУБД PostgreSQL системы АСМ (имя используемой УЗ указывается в переменной **DB_USER**). Если установка СУБД PostgreSQL производится bootstrap скриптом АСМ, то УЗ пользователя с указанным именем и паролем будет создана в процессе установки СУБД PostgreSQL. Если установка СУБД PostgreSQL производится другим способом, то администратору необходимо создать УЗ пользователя с указанным именем и паролем.

export RMQ_PASSWORD="password"

Необходимо задать пароль УЗ для подключения к сервису брокера RabbitMQ системы АСМ (имя используемой УЗ указывается в переменной **RMQ_USER**). Если установка брокера RabbitMQ производится bootstrap скриптом АСМ, то УЗ пользователя с указанным именем и паролем будет создана в процессе установки RabbitMQ. Если установка RabbitMQ производится другим способом, то администратору необходимо создать УЗ пользователя RabbitMQ с указанным именем и паролем.

export REDIS_PASSWORD="password"

Необходимо задать пароль УЗ для подключения к сервису БД Redis системы АСМ (имя используемой УЗ указывается в переменной **REDIS_USER**). Установка Redis производится bootstrap скриптом АСМ, в процессе установки производится также создание и настройка УЗ с указанным именем и паролем.

Значения отладки

```
# Debug vars

export DEBUG="0"
export DB_ECHO="0"
```

Значения уровня логирования отладочных сообщений. После установки для каждого конкретного сервиса значение можно поменять значения в файле /etc/<service_name>/prod_config.ini и выполнить перезапуск сервиса с помощью команды systemctl restart <service_name>.

Инфраструктурные переменные

```
# Infrastructure vars

export DB_HOST="localhost"
```

Необходимо указать IP адрес сервера СУБД PostgeSQL, который будет использоваться для размещения БД «Основного сервера АСМ». Если основной сервер АСМ и БД расположены на одном сервере, вносить изменения не нужно.

```
export DB_PORT="5432"
```

Необходимо указать номер сетевого порта (TCP) для подключения к СУБД PostgreSQL.

```
export DB_USER="acmastra"
```

Необходимо указать наименование (логин) УЗ СУБД PostgreSQL для подключения к СУБД PostgreSQL системы АСМ. Если установка СУБД PostgreSQL производится bootstrap скриптом АСМ, то УЗ пользователя с указанным именем и паролем будет создана в процессе установки СУБД PostgreSQL. Если установка СУБД PostgreSQL производится другим способом, то администратору необходимо создать УЗ пользователя с указанным именем и паролем и наделить УЗ ролью «CREATE_DB».

```
export RMQ_HOST="localhost"
```

Необходимо указать IP адрес сервера брокера сообщений RabbitMQ. Если основной сервер АСМ и сервис брокера расположены на одном сервере, вносить изменения не нужно.

```
export RMQ_PORT="5672"
```

Необходимо указать номер сетевого порта (TCP) для подключения серверных компонент АСМ (для обмена данными) к серверу брокера RabbitMQ.

```
export RMQ_PORT_API="15672"
```

Необходимо указать номер сетевого порта (TCP) для подключения серверных компонент АСМ (для управления) к серверу брокера RabbitMQ.

export RMQ_USER="acmastra"

Необходимо указать наименование (логин) УЗ, под которой система АСМ будет подключаться для работы с брокером сообщений RabbitMQ. Если установка брокера RabbitMQ производится bootstrap скриптом АСМ, то УЗ пользователя с указанным именем и паролем будет создана в процессе установки RabbitMQ. Если установка брокера RabbitMQ производится другим способом, то администратору необходимо создать УЗ пользователя с указанным именем и паролем и наделить УЗ ролью «Администратор».

export REDIS_HOST="localhost"

Необходимо указать IP адрес сервера БД Redis. Если основной сервер АСМ и БД Redis расположены на одном сервере, вносить изменения не нужно.

export REDIS_PORT="6379"

Необходимо указать номер сетевого порта (TCP) для подключения серверных компонент АСМ к серверу БД Redis.

export REDIS_USER="acmastra"

Необходимо указать наименование (логин) УЗ, под которой система АСМ будет подключаться для работы с БД Redis. Установка Redis производится bootstrap скриптом АСМ, в процессе установки производится также создание и настройка УЗ с указанным именем и паролем.

export GIT_HOST="localhost"

Необходимо указать IP адрес сервера репозиториев GIT. Рекомендуется размещать GIT на том же хосте, что и сервер управления агентами.

export GIT_PORT="22"

Необходимо указать порт SSH для подключения ПУА к серверу GIT.

export GIT_USER="acm-git"

Необходимо указать наименование (логин) УЗ, которая будет использоваться сервером ПУА для подключения по SSH к серверу GIT. Указанная УЗ будет создана в процессе развертывания системы АСМ в ОС Astra Linux на сервере размещения GIT сервера.

export GIT_KEY="/home/${GIT_USER}/.ssh/git_id_rsa"

Путь размещение ключа, используемого сервером ПУА для подключения по SSH к серверу GIT. Данный ключ автоматически генерируется при установке системы АСМ.

export AUTH_PRIVATE_KEY_PATH="/etc/acm-auth-service/auth_id_rsa"

Путь размещения ключа, используемого сервисом acm-auth-service. Данный ключ автоматически генерируется при установке системы АСМ.

Переменные сервиса авторизации

```
# Auth-service vars

export BUILT_ACCOUNT="admin"
```

Необходимо указать название (логин) для предустановленной УЗ с правами Главного администратора для проведения первоначальной настройки системы. Возможно указание уже настроенной в домене полной доменной записи. Если УЗ не существует, ее необходимо предварительно создать вручную (в случае локальной УЗ), либо в домене (в случае доменной УЗ).

```
export SEGMENT_UID="b479771e-7be8-4eeb-b622-fae85f1ca7b6"
```

Переменная содержит уникальный идентификатор, используемый для создания предустановленного сегмента «Основной сегмент» при установке «Основного сервера АСМ». Во избежание ошибок рекомендуется не вносить изменения в данный параметр.

Переменные сервиса конфигурации

```
# Configuration-service vars

export REPORT_STORAGE_PATH="/opt/acm/acm-configuration-service-data"
```

Каталог хранения выгружаемых данных (например, отчетов) на основном сервере АСМ.

Переменные сервиса репозиториев

```
 # Repo vars

export MIRROR_DIR="/srv/repo"
```

Каталог для хранения репозиториев.

```
export REPO_DIR="${MIRROR_DIR}/mirror/dl.astralinux.ru"
```

Каталог для хранения репозиториев Astra Linux и АСМ, использующихся при установке ОС по сети и для установки агента АСМ на подключаемые компьютеры клиенты.

```
export ACM_REPO_DIR="${REPO_DIR}/acm/"
```

Каталог для хранения репозиториев АСМ.

```
export ASTRA_REPO_DIR="${REPO_DIR}/astra/"
```

Каталог для хранения репозиториев Astra Linux.

```
export TFTP_PATH="/srv/tftp"
```

Каталог для хранения данных, используемых Сервером установки ОС (загрузчик PXE и файл меню для загрузчика).

export FILES_DIR="/srv/files"

Каталог для хранения данных, используемых Сервером установки ОС.

Переменные установки ОС

 # OSdeployment-service vars

export DB_PATH="/opt/acm/acm-osdeployment-service-data/db/database.db"

Каталог внутренней БД (SQlite) сервиса установки ОС.

export ACM_REPO_PATH_BASE="/astra/frozen/1.7_x86-64/1.7.5/repository-base/"

Каталог для хранения репозитория Astra Linux v 1.7.5 base.

export ACM_REPO_PATH_EXTENDED="/astra/frozen/1.7_x86-64/1.7.5/repository-extended/"

Каталог для хранения репозитория Astra Linux v 1.7.5 extended.

export ACM_REPO_PATH_ACM="/acm/frozen/1.x/"

Каталог для хранения репозитория ACM v 1.0.0 Standard

export STORAGE_PXE_CONF_PATH="${TFTP_PATH}/pxelinux.cfg/default"

Каталог для хранения данных сервера PXE (файл меню для загрузчика).

export STORAGE_PROFILES_DIR_PATH="/srv"

Каталог для хранения данных профилей первичной установки ОС.

export STORAGE_GRUB_CONF_PATH="${TFTP_PATH}/debian-installer/amd64/grub/grub.cfg"

Каталог для хранения данных загрузчика grub, используемого для UEFI.

export STORAGE_URL="http://${OSDEPLOY_IP}"

Переменная сервиса установки ОС ACM, содержащая адрес размещения preseed файлов профилей первичной установки.

export PROFILES_DIR="${STORAGE_PROFILES_DIR_PATH}/profiles/"

Переменная сервиса установки ОС ACM, содержащая каталог размещения данных профилей первичной установки.

ПРИЛОЖЕНИЕ. ПЕРЕМЕННЫЕ ФАЙЛА ENV ПРИ УСТАНОВКЕ ОСНОВНОГО СЕРВЕРА ACM

Пример значений переменных конфигурационного файла env для развертывания основного сервера ACM.

```
### Variables that MUST be set
export PXE_INTERFACE="eth0"
export PXE_SUBNET="10.0.14.0"
export OSDEPLOY_IP="10.0.14.1"
###


### Variables that MUST be changed
export DB_PASSWORD="password"
export RMQ_PASSWORD="password"
export REDIS_PASSWORD="password"
###


### Variables that CAN BE changed
# Debug vars
export DEBUG="0"
export DB_ECHO="0"


# Infrastructure vars
export DB_HOST="localhost"
export DB_PORT="5432"
export DB_USER="acmastra"
export RMQ_HOST="localhost"
export RMQ_PORT="5672"
export RMQ_PORT_API="15672"
export RMQ_USER="acmastra"
export REDIS_HOST="localhost"
export REDIS_PORT="6379"
export REDIS_USER="acmastra"
export GIT_HOST="localhost"
export GIT_PORT="22"
export GIT_USER="acm-git"
export GIT_KEY="/home/${GIT_USER}/.ssh/git_id_rsa"
export AUTH_PRIVATE_KEY_PATH="/etc/acm-auth-service/auth_id_rsa"


# Auth-service vars
export BUILT_ACCOUNT="astra"
export SEGMENT_UID="b479771e-7be8-4eeb-b622-fae85f1ca7b6"


# Configuration-service vars
```

```
export REPORT_STORAGE_PATH="/opt/acm/acm-configuration-service-data"


# Repo vars
export MIRROR_DIR="/srv/repo"
export REPO_DIR="${MIRROR_DIR}/mirror/dl.astralinux.ru"
export ACM_REPO_DIR="${REPO_DIR}/acm/"
export ASTRA_REPO_DIR="${REPO_DIR}/astra/"
export TFTP_PATH="/srv/tftp"
export FILES_DIR="/srv/files/"


# OSdeployment-service vars
export DB_PATH="/opt/acm/acm-osdeployment-service-data/db/database.db"
export ACM_REPO_PATH_BASE="/astra/frozen/1.7_x86-64/1.7.5/repository-base/"
export         ACM_REPO_PATH_EXTENDED="/astra/frozen/1.7_x86-64/1.7.5/repository-
extended/"
export ACM_REPO_PATH_ACM="/acm/frozen/1.x/"
export STORAGE_PXE_CONF_PATH="${TFTP_PATH}/pxelinux.cfg/default"
export STORAGE_PROFILES_DIR_PATH="/srv"
export
STORAGE_GRUB_CONF_PATH="${TFTP_PATH}/debian-installer/amd64/grub/grub.cfg"
export STORAGE_URL="http://${OSDEPLOY_IP}"
export PROFILES_DIR="${STORAGE_PROFILES_DIR_PATH}/profiles/"
###
```

ПРИЛОЖЕНИЕ. ПЕРЕМЕННЫЕ ФАЙЛА ENV ПРИ УСТАНОВКЕ СЕРВЕРА УПРАВЛЕНИЯ АГЕНТАМИ ACM

Пример значений переменных конфигурационного файла env для развертывания сервера управления агентами ACM.

```
### Variables that MUST be changed
export DB_PASSWORD="password"
export RMQ_PASSWORD="password"
###


### Variables that CAN BE changed
# Debug vars
export DEBUG="0"
export DB_ECHO="0"


# Infrastructure vars
export DB_HOST="localhost"
export DB_PORT="5432"
export DB_USER="acmastra"
export RMQ_HOST="localhost"
export RMQ_PORT="5672"
export RMQ_PORT_API="15672"
export RMQ_USER="acmastra"
export GIT_HOST="localhost"
export GIT_PORT="22"
export GIT_USER="acm-git"
export GIT_KEY="/home/${GIT_USER}/.ssh/git_id_rsa"
export AUTH_PRIVATE_KEY_PATH="/etc/acm-auth-service/auth_id_rsa"
```

ПРИЛОЖЕНИЕ. ПЕРЕМЕННЫЕ ФАЙЛА ENV ПРИ УСТАНОВКЕ ПУА

Пример значений переменных конфигурационного файла env для развертывания сервера ПУА АСМ.

```
### Variables that MUST be changed
export DB_PASSWORD="password"
export RMQ_PASSWORD="password"
###

### Variables that CAN BE changed
# Debug vars
export DEBUG="0"
export DB_ECHO="0"

# Infrastructure vars
export DB_HOST="localhost"
export DB_PORT="5432"
export DB_USER="acmastra"
export RMQ_HOST="localhost"
export RMQ_PORT="5672"
export RMQ_PORT_API="15672"
export RMQ_USER="acmastra"
export GIT_HOST="localhost"
export GIT_PORT="22"
export GIT_USER="acm-git"
export GIT_KEY="/home/${GIT_USER}/.ssh/git_id_rsa"
export AUTH_PRIVATE_KEY_PATH="/etc/acm-auth-service/auth_id_rsa"
```

ПРИЛОЖЕНИЕ. ПЕРЕМЕННЫЕ ФАЙЛА ENV ПРИ УСТАНОВКЕ СЕРВЕРА УСТАНОВКИ ОС И СЕРВЕРА РЕПОЗИТОРИЕВ

Пример значений переменных конфигурационного файла env для развертывания сервера установки ОС АСМ.

```
### Variables that MUST be set
export PXE_INTERFACE="eth0"
export PXE_SUBNET="10.0.14.0"
export OSDEPLOY_IP="10.0.14.1"
###


### Variables that MUST be changed
export RMQ_PASSWORD="password"
###


### Variables that CAN BE changed
# Debug vars
export DEBUG="0"
export DB_ECHO="0"


# Infrastructure vars
export RMQ_HOST="localhost"
export RMQ_PORT="5672"
export RMQ_PORT_API="15672"
export RMQ_USER="acmastra"


# Repo vars
export MIRROR_DIR="/srv/repo"
export REPO_DIR="${MIRROR_DIR}/mirror/dl.astralinux.ru"
export ACM_REPO_DIR="${REPO_DIR}/acm/"
export ASTRA_REPO_DIR="${REPO_DIR}/astra/"
export TFTP_PATH="/srv/tftp"
export FILES_DIR="/srv/files/"


# OSdeployment-service vars
export DB_PATH="/opt/acm/acm-osdeployment-service-data/db/database.db"
export ACM_REPO_PATH_BASE="/astra/frozen/1.7_x86-64/1.7.5/repository-base/"
export         ACM_REPO_PATH_EXTENDED="/astra/frozen/1.7_x86-64/1.7.5/repository-
extended/"
export ACM_REPO_PATH_ACM="/acm/frozen/1.x/"
export STORAGE_PXE_CONF_PATH="${TFTP_PATH}/pxelinux.cfg/default"
export STORAGE_PROFILES_DIR_PATH="/srv"
export
STORAGE_GRUB_CONF_PATH="${TFTP_PATH}/debian-installer/amd64/grub/grub.cfg"
```

```
export STORAGE_URL="http://${OSDEPLOY_IP}"
export PROFILES_DIR="${STORAGE_PROFILES_DIR_PATH}/profiles/"
###
```

ПРИЛОЖЕНИЕ. ПРИМЕР ФАЙЛА PRESEED

Ниже представлен пример файла Preseed для использования в системе АСМ:

```
# Сетевой репозиторий для установки
d-i mirror/protocol string http
d-i mirror/country string manual
#необходимо использовать переменную ${osdeploy_ip}
d-i mirror/http/hostname string ${osdeploy_ip}
#необходимо указать путь к репозиторию с пакетами устанавливаемой ОС Astra Linux
d-i mirror/http/directory string /astra/frozen/1.7_x86-64/1.7.5/repository-base/

# Настройки языка
d-i mirror/country string manual
d-i debian-installer/locale string ru_RU
d-i debian-installer/locale select ru_RU.UTF-8
d-i debian-installer/language string ru
d-i debian-installer/country string RU
d-i debian-installer/keymap string ru

# Настройки клавиатуры
d-i console-tools/archs select at
d-i console-keymaps-at/keymap select ru
d-i console-setup/toggle string Ctrl+Shift
d-i console-setup/layoutcode string ru
d-i keyboard-configuration/toggle select Ctrl+Shift
d-i keyboard-configuration/layoutcode string ru
d-i keyboard-configuration/xkb-keymap select ru
d-i languagechooser/language-name-fb select Russian
d-i countrychooser/country-name select Russia

# Настройки сетевого интерфейса
d-i netcfg/choose_interface select auto
# Выбор компонент репозитория
d-i apt-setup/non-free boolean true
d-i apt-setup/contrib boolean true
d-i apt-setup/services-select none

# Select which update services to use; define the mirrors to be used.
# Values shown below are the normal defaults.
#d-i apt-setup/services-select multiselect security, updates
#d-i apt-setup/security_host string security.debian.org

# By default the installer requires that repositories be authenticated
# using a known gpg key. This setting can be used to disable that
# authentication. Warning: Insecure, not recommended.
```

```
#d-i debian-installer/allow_unauthenticated boolean true

# Uncomment this to add multiarch configuration for i386
#d-i apt-setup/multiarch string i386

# Настройка часов и синхронизации времени
d-i clock-setup/utc boolean true
d-i time/zone string Europe/Moscow
d-i clock-setup/ntp boolean false

# 7. Disk partitioning
# scheme:
# gpt
# part1: BIOS GRUB partition, 1MiB
# part2: EFI partition, 500 MiB
# part3: swap partition, 4 GiB
# part4: / partition, 50 GiB
# part5: /home partition, remaining disk space
#
d-i partman-auto/method string regular
d-i partman-efi/non_efi_system boolean true
d-i partman-partitioning/choose_label    select    gpt
d-i partman-partitioning/default_label string gpt
d-i partman-lvm/device_remove_lvm boolean true
d-i partman-md/device_remove_md boolean true
d-i partman-lvm/confirm boolean false
d-i         partman-auto/expert_recipe         string         myroot         ::
\
    1 1 1 free                                                  \
        $iflabel{ gpt }                                             \
        $reusemethod{ }                                             \
        method{ biosgrub } .                                         \
                                                        \
        524 524 524 fat32                                             \
        $reusemethod{ }                                          \
        method{ efi }                                              \
        format{ } .                                              \
                                                        \
    4295 4295 4295 linux-swap                                         \
        $reusemethod{ }                                          \
        method{ swap }                                             \
        format{ } .                                              \
                                                        \
    53688 53688 53688 ext4                                              \
            method{  format  }  format{  }  use_filesystem{  }  filesystem{  ext4  }
mountpoint{ /    } .        \
                                                        \
```

```
    10240 20480 -1 ext4                                                 \
             method{  format  }  format{  }  use_filesystem{  }  filesystem{  ext4  }
mountpoint{ /home    } .
d-i partman-auto/choose_recipe select myroot


d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true


d-i partman-md/confirm boolean true
d-i partman-partitioning/confirm_write_new_label boolean true
d-i partman/choose_partition select finish
d-i partman/confirm boolean true
d-i partman/confirm_nooverwrite boolean true


d-i base-installer/kernel/image string linux-image-generic


#d-i passwd/make-user boolean true


# Учетная запись и пароль пользователя
#d-i passwd/user-fullname string astra
#d-i passwd/username string astra
#d-i passwd/user-password password 12345678
#d-i passwd/user-password-again password 12345678
#d-i passwd/root-login boolean true
#d-i passwd/root-password-crypted password $1$U2VxNOjA$p0mKUrsMLoh69RmhIN2dy0


d-i passwd/make-user boolean true
d-i passwd/user-fullname string user
d-i passwd/username string acm
d-i passwd/user-password password 12345678
d-i passwd/user-password-again password 12345678
#d-i passwd/user-password-crypted password $1$U2VxNOjA$p0mKUrsMLoh69RmhIN2dy0
d-i debian-installer/allow_unauthenticated string true


# Выбор ПО для установки
tasksel tasksel/first multiselect Base packages, SSH server
tasksel tasksel/astra-feat-setup multiselect
d-i pkgsel/include string wget qemu-guest-agent


# Выбор уровня защищенности ОС
#d-i astra-additional-setup/os-check select Maximum security level Smolensk
d-i astra-additional-setup/os-check select Base security level Orel
```

```
# Выбор параметров ОС
#d-i   astra-additional-setup/additional-settings-smolensk   multiselect   Enable Mandatory Integrity Control, Enable Mandatory Access Control, Disable ptrace capability
d-i astra-additional-setup/additional-settings-orel multiselect Disable ptrace capability


tripwire tripwire/use-localkey boolean false
tripwire tripwire/use-sitekey boolean false
tripwire tripwire/installed note ok
portsentry portsentry/warn_no_block note ok
astra-license astra-license/license boolean true
krb5-config krb5-config/kerberos_servers string
libnss-ldapd libnss-ldapd/ldap-base string
libnss-ldapd libnss-ldapd/ldap-uris string
libnss-ldapd libnss-ldapd/nsswitch multiselect services
ald-client ald-client/make_config boolean false
ald-client ald-client/manual_configure false
astra-feat-setup astra-feat-setup/feat multiselect kiosk mode false
astra-feat-setup astra-feat-setup/feat multiselect Служба ALD false
d-i console-cyrillic/switch select "Клавиша Menu"
d-i console-cyrillic/toggle select Control+Shift
d-i samba-common/dhcp boolean false
d-i samba-common/workgroup string testgroup1
popularity-contest popularity-contest/participate boolean false
d-i grub-installer/only_debian boolean true
d-i grub-installer/with_other_os boolean true


# Пароль загрузчика grub
d-i grub-installer/password password 12345678
d-i grub-installer/password-again password 12345678
grub-installer grub-installer/password-mismatch error


# Не показывать последнее сообщение о том, что установка завершена.
d-i finish-install/reboot_in_progress note
d-i finish-install/exit/poweroff boolean true
```