Министерство образования и молодежной политики Свердловской области государственное автономное профессиональное

образовательное учреждение Свердловской области

«Уральский радиотехнический колледж им. А.С. Попова»

Специальность 09.02.06

Сетевое и системное администрирование

ОТЧЕТ

О выполнении индивидуального задания за период производственной практики на предприятии АО «КОНСИСТ-ОС»

Выполнил:

Обучающийся Т.И. Куваев

Группы Са-401

Проверено:

Руководитель практики на предприятии

\_\_\_\_\_\_\_\_\_\_ М.А. Мокшанцев

Должность: главный специалист отдела

аналитики и архитектуры государственной

единой облачной платформы и

государственной информационной системы

Руководитель практики от колледжа

\_\_\_\_\_\_\_\_\_\_ Д.Л. Боровиков

Оценка \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Екатеринбург, 2025 г.

Информация о предприятии

Сегодня АО «КОНСИСТ-ОС» является внутренним интегратором и центром компетенций в области информационных технологий, информационной безопасности, проектного управления, а также центром цифровых технологий индустрии 4.0 и оператором всех центров обработки данных дивизиона «Электроэнергетический», в том числе крупнейшего ЦОД в РФ и Европе – ЦОД «Калининский».

Основу компании составляют высококвалифицированные специалисты – выпускники ведущих ВУЗов страны: МГУ, МИФИ, МЭИ, МАИ, МИЭМ и базовых ВУЗов Министерства обороны. Сотрудники АО «КОНСИСТ-ОС» имеют многолетний опыт работы в атомной энергетике и оборонной промышленности, в том числе в области коммуникаций и технического обеспечения всех видов связи.

АО «КОНСИСТ-ОС» оказывает услуги по техническому обслуживанию и обеспечению работоспособности средств диспетчерского и технологического управления, кабельной сети и многоканальных телекоммуникационных систем, основных и вспомогательных подсистем и сервисов корпоративной информационной системы атомных станций.

В настоящее время АО «КОНСИСТ-ОС» предоставляет ИТ-сервисы АО «Концерн Росэнергоатом» по следующим направлениям:

* + оказание услуг по технической поддержке пользователей;
  + сопровождение и техническое обслуживание информационных корпоративных систем центрального аппарата Концерна и локальных систем филиалов;
  + сопровождение инфраструктурных информационных систем;
  + сопровождение и техническое обслуживание мультимедийных систем;
  + сопровождение и техническое обслуживание инженерных систем;
  + управление ИТ-активами;
  + управление проектами в области ИТ;
  + оказание услуг по обеспечению информационной безопасности;
  + предоставление услуг связи.

Я буду проходить производственную практику на должности специалиста отдела аналитики и архитектуры государственной единой облачной платформы и государственной информационной системы.

Ход производственной практики

03.03 Прошёл инструктаж по технике безопасности, ознакомился с персоналом и заданием на производственную практику – настройкой сетевой части инфраструктуры, развертыванием инфраструктурных сервисов и сервисов, необходимых для осуществления рабочих функций в виртуальной инфраструктуре.

10.03 Приступил к развертыванию виртуальных машин по схеме, представленной на рисунке 1. В качестве основного ПО для развертывания инфраструктуры использовал GNS3, в качестве гипервизора – QEMU.

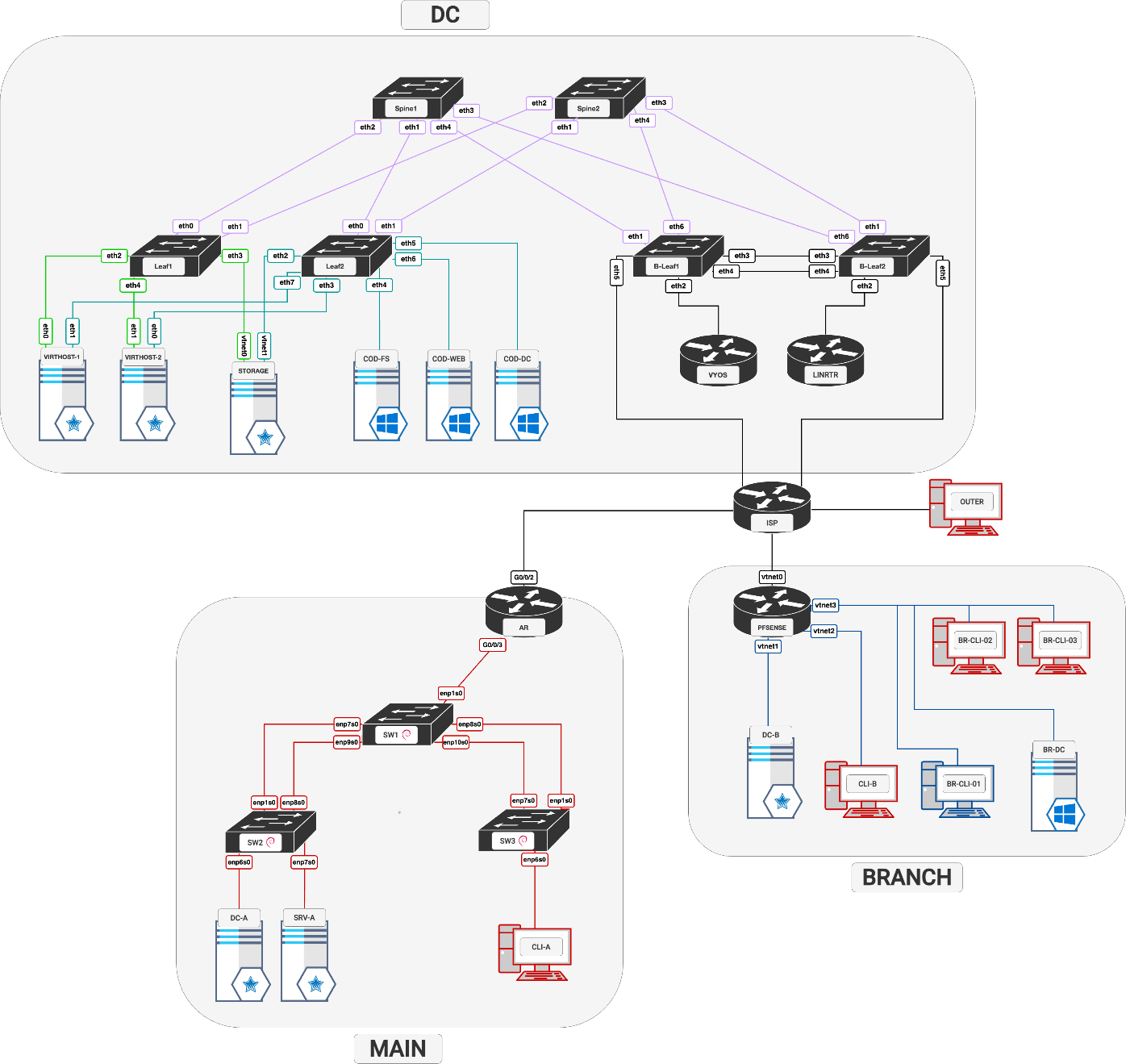


Рисунок 1 – Схема физических подключений машин в инфраструктуре

Установил операционные системы Windows Server 2025, Windows 10, Astra Linux Special Edition 1.7 и 1.8. В качестве ОС для сетевых устройств использовал Huawei и UserGate в ЦОД. Развернул все виртуальные машины и проверил работоспособность сетевых соединений и всех машин в целом.

11.03 Для вложенных гипервизоров установил на сервера отечественную систему виртуализации ZVirt, без полного развертывания менеджера виртуальных машин и сервера хранения данных.

zVirt позволяет управлять всей виртуальной инфраструктурой - хостами, виртуальными машинами, сетями, хранилищами и пользователями - с помощью централизованного графического интерфейса пользователя или REST API.

Схема работы кластера и состав системы виртуализации представлен на рисунке 2.

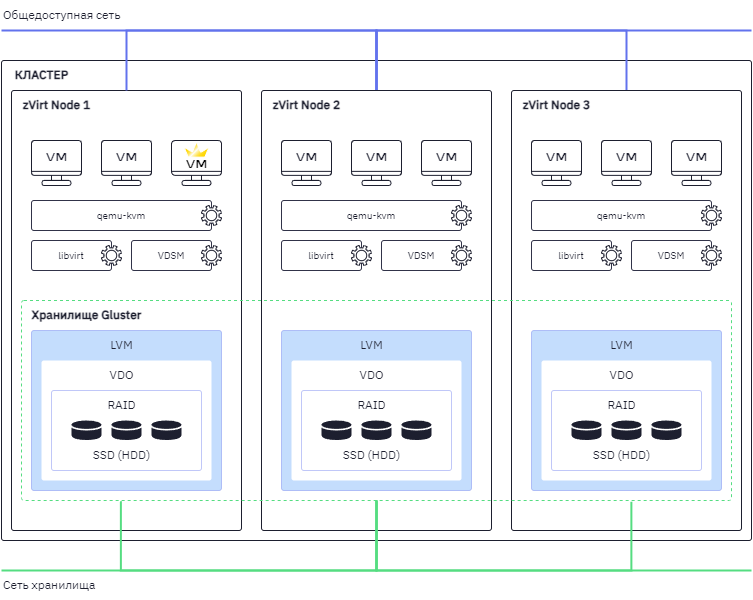


Рисунок 2 – Схема кластера из серверов с ZVirt

12.03 Приступил к развертыванию CХД, чтобы развернуть менеджер управления на одном из хостов виртуализации.

Среда виртуализации zVirt может быть развернута как в архитектуре Hosted Engine, так и в архитектуре Standalone. В архитектуре Hosted Engine менеджер управления работает как виртуальная машина на специализированных хостах в той же среде, которой он управляет. Также требуется одного хранилище, доступное для всех хостов в кластере, которые будет использоваться для хранения данных менеджера.

После развертывания менеджера создал кластер из двух серверов и добавил тома в центр данных, тем самым закончив настройку ZVirt, внешний вид которого представлен на рисунке 3.

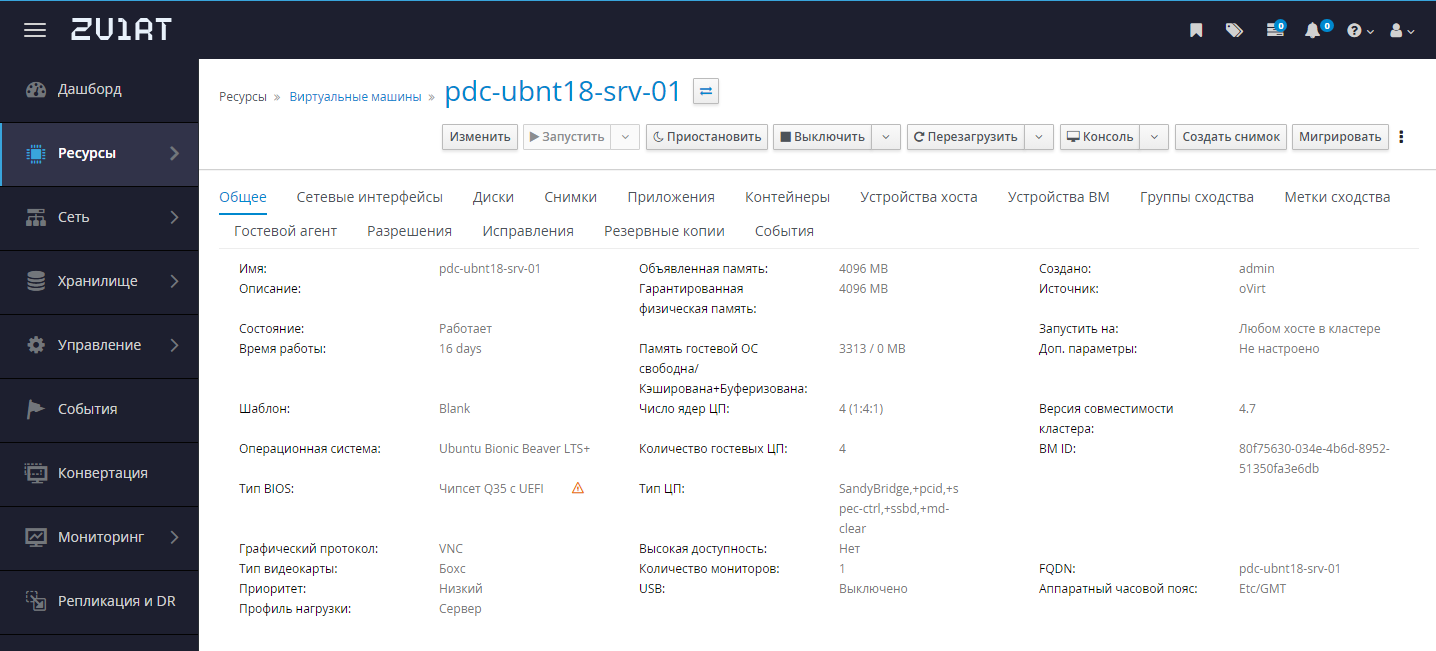


Рисунок 3 – Внешний вид панели менеджера управления

14.03 Ознакомился с более подробными требованиями, представленными к сетевой части инфраструктуры. L3-схема, по которой производилась настройка представлена на рисунке 4. На коммутаторах развернул агрегированные каналы с использованием LACP, настроил балансировку трафика. На агрегации настроил транки, разрешая только необходимые VLAN.

Для подключения офисов к ЦОД настроил GRE-туннели между роутерами в ЦОД и шлюзами в офисах, предварительно защитил их с помощью IPSec. Динамическую маршрутизацию обеспечил через протокол OSPF, запущенный поверх туннелей. За счет этого была обеспечена сквозная связность между офисами и ЦОД, заодно гарантируя безопасность внутренних данных.

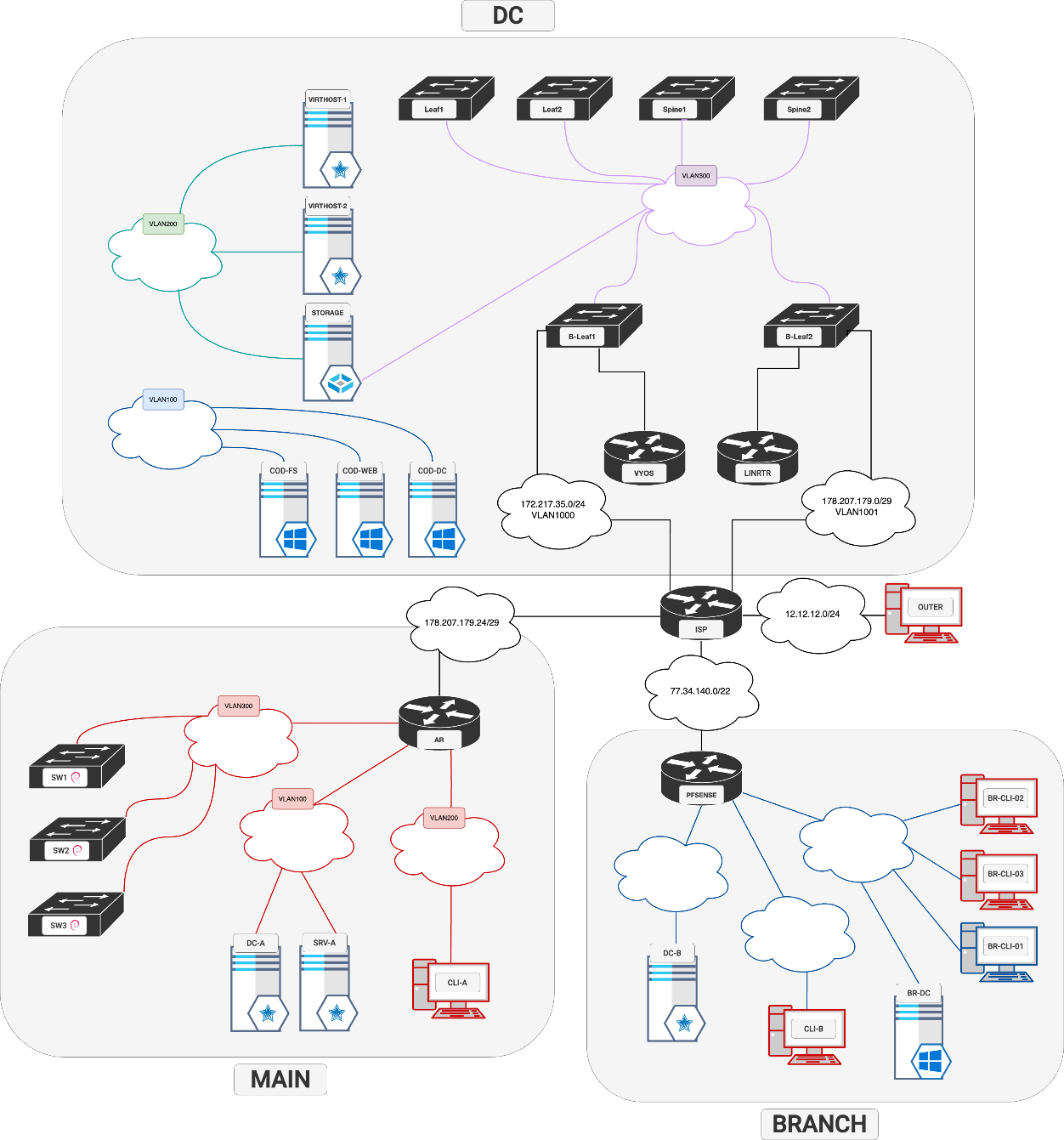


Рисунок 4 – L3-схема всей инфраструктуры

14.03 Приступил к настройке VXLAN-Фабрики в ЦОД, начав с underlay-сети обеспечив связность между Spine и Leaf коммутаторами. Для этого агрегировал физические интерфейсы с использованием протокола LACP, настроил адресацию третьего уровня с 31 маской, исходя из требований. Создал виртуальные dummy-интерфейсы: один для идентификации маршрутизатора и управления BGP-сессиями, второй — в качестве источника туннелей VXLAN, третий — для выделенного управления в отдельном VRF. Маршрутизация в underlay-сети реализована через OSPF point-to-point, из-за отсутствия возможности использования широковещательного трафика. Также при установлении соседей была реализована аутентификация. Самая простая реализация технологии VXLAN-туннелей представлена на рисунке 5.

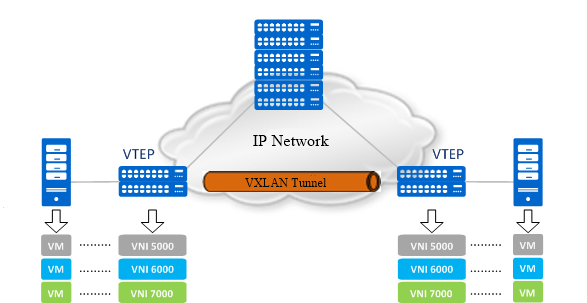


Рисунок 5 – Простейший пример реализации VXLAN-туннелей

17.03 На этапе построения overlay-сети развернул EVPN/VXLAN, настроив eBGP между spine и leaf коммутаторами. Spine-устройства выступают в роли рефлекторов маршрутов, что упрощает обмен EVPN-префиксами между нижестоящими коммутаторами. Каждый leaf-коммутатор сконфигурирован как VTEP с использованием виртуального интерфейса для инкапсуляции VXLAN-трафика. Для передачи кадров второго уровня назначены уникальные идентификаторы VNI, привязанные к VLAN, а для межсегментной маршрутизации внутри VRF добавлены отдельные L3VNI. Чтобы обеспечить распределённую работу шлюзов, настроил SAG с одинаковыми SVI-адресами на всех leaf-коммутаторах.

19.03 Настроил контроллеры домена на базе ALD PRO в обоих офисах, с двусторонним доверием между доменами офисов, обеспечив кросс-аутентификацию пользователей и автоматическую взаимную выдачу kerberos-билетов. Реализованы группы безопасности с ограничением доступа: одна блокирует вход в систему, другая — консольные сессии. Для администраторов автоматически создаются ярлыки веб-интерфейсов, а профили пользователей хранятся на выделенном сервере с синхронизацией между офисами через NFSv4. Один из шагов развертывания ALD PRO показан на рисунке 6.

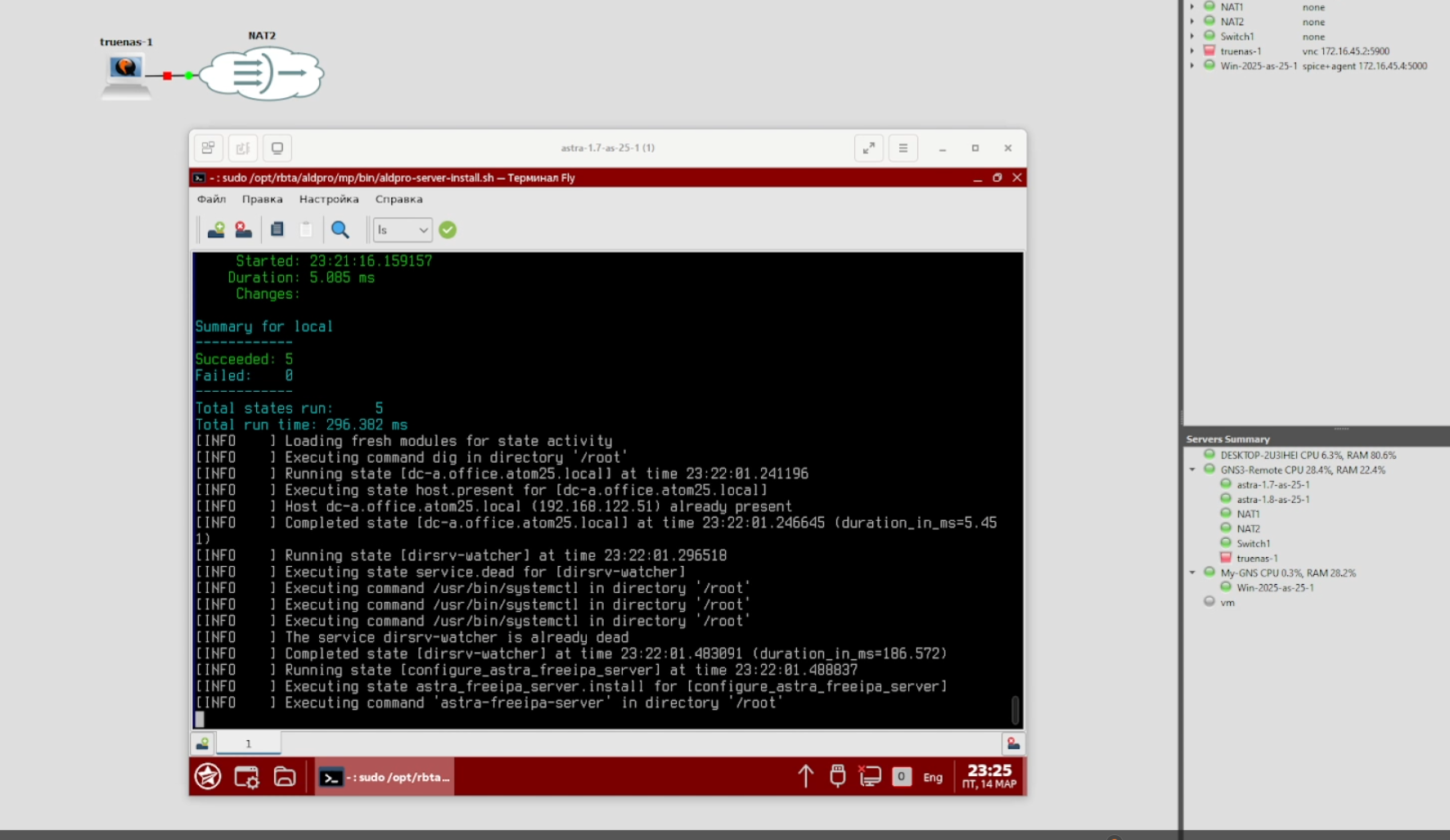


Рисунок 6 – Процесс развертывания ALD PRO

21.03 Развернул домен с созданием дополнительного сайта, настроил репликацию между узлами и динамическое распределение IP-адресов. Организовал OU для автоматического размещения устройств, ограничив ввод компьютеров в домен специальными группами администраторов. На контроллере домена внедрил LAPS для управления паролями локальных учётных записей, исключив несанкционированный доступ.

24.03 Были настроены групповые политики для централизованного контроля безопасности и доступа: внедрены строгие парольные требования, автоматизация аудита событий входа и блокировки учётных записей. По итогу политики обеспечивают автоматическое применение LAPS для управления локальными администраторами, а также интеграцию с ALD Pro для синхронизации прав доступа между доменами.

26.03 Настроил корневой ЦС с длительным сроком действия сертификатов и частым обновлением списков отзыва (CRL). Для распространения информации о сертификатах был развернут внутренний веб-сайт, где опубликованы ссылки на CRL и точки распространения сертификатов (AIA). Корневой сертификат был автоматически доверен всем устройствам домена через групповые политики. Созданы шаблоны: для веб-серверов (с экспортируемыми ключами) и административного доступа (с ручной выдачей уполномоченным группам).

31.03 Реализовано двустороннее доверие между доменами офисов к родительскому домену в ЦОД средствами Kerberos. Интеграция ALD Pro с Windows-инфраструктурой позволила централизованно управлять правами доступа и группами, синхронизируя политики безопасности между системами. Для защиты запросов между КД настроено шифрование данных по TLS, а аудит операций в междоменной среде фиксирует все попытки несанкционированного доступа. Один из шагов настройки показан на рисунке 7.

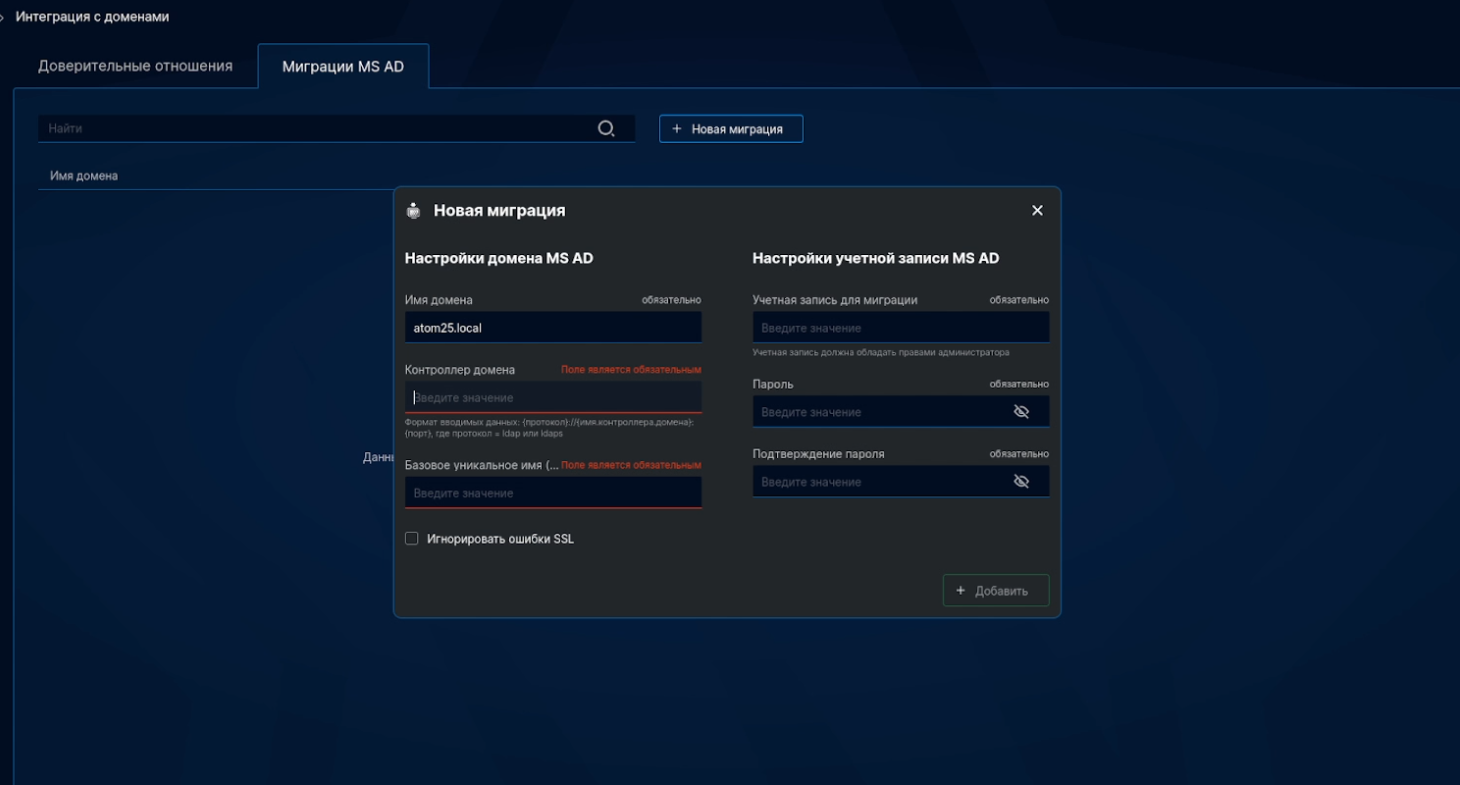


Рисунок 7 – Процесс миграции пользователей из Windows-домена для ДДО

02.04 Приступил к настройке DFS, опубликовал ресурсы с различными правами доступа для разных групп безопасности. Созданы домашние каталоги пользователей с автоматическим подключением и изоляцией доступа. Для каждого профиля установлена жёсткая квота в 300 МБ, ограничивающая объём хранимых данных. В итоге windows-инфраструктура обеспечивает баланс между доступностью ресурсов, защитой данных и соблюдением корпоративных политик.

04.04 Развернул корпоративный репозиторий с GPG-ключом, обеспечив безопасное подключение клиентов. Настроил автоматическое доверие к репозиторию, исключив предупреждения при обновлении пакетов. Установил необходимый пакет на один из клиентов, а на другом ограничился подключением репозитория без установки.

07.04 Развернул почтовый сервер с поддержкой TLS, обеспечил аутентификацию через доменные учётные данные, также настроил интеграцию с Kerberos.

09.04 Установил и настроил корпоративный прокси-сервер с ограничением доступа к запрещенным ресурсам только для клиентов филиала через Firefox. Также были созданы ACL: разрешён доступ к внутренним ресурсам, заблокированы, а для служебных веб-сервисов добавлена HTTP-аутентификация с локальной базой пользователей.

11.04 Развернул СУБД, создав пользователей с ограниченными правами доступа к конкретным базам данных. Для суперпользователя назначил полные привилегии, остальным аккаунтам предоставил доступ только к необходимым ресурсам. Пароли всех пользователей соответствуют заданным требованиям.

14.04 Развернул службу Zabbix на виртуальной машине в ZVirt, обеспечив мониторинг сетевых устройств через SNMP с использованием стандартных шаблонов. Для серверов на базе Linux настроен сбор метрик через Zabbix Agent, включая отслеживание процессорной нагрузки и использования памяти. Создал дашбордыс графиками времени ответа по ICMP, а также для визуализации утилизации ресурсов. Также был настроен базовый функционал автообнаружения хостов.

18.04 Приступил к реализации дипломного проекта по теме «Разработка макета IT-инфраструктуры современной компании», сосредоточившись на теоретическом разделе. Разработал рабочий вариант структуры работы, систематизировав тематические блоки для аналитических глав и сформулировав ключевые аспекты для анализа. Сформировал список базовых материалов: методические пособия по вопросам проектирования сетей и инфраструктурных сервисов, а также нормативно-технические материалы российских разработчиков программно-аппаратных комплексов. Дополнительно выделил направления для изучения практико-ориентированных аспектов в рамках выбранной тематики.

21.04 Продолжил развитие теоретической главы, акцентируя внимание на анализе методологий проектирования инфраструктуры, включая исследование кейсов российских экспертов в области корпоративных IT-решений. В рамках работы провел сравнительный анализ подходов к организации технологических слоев — от сетевой архитектуры до систем хранения данных. На данном этапе сфокусировался на поиске оптимального формата подачи материала, а именно продумывал логику разделения обзора технологического стека на этапы, чтобы отразить взаимосвязь инструментов и прочих технологий на разных стадиях создания инфраструктуры.

23.04 Продолжил изучение источников и начал систематизировать информацию. Приступил к написанию раздела 1.1. После начал раздел 1.2, где описал базовые типы инфраструктур, особенности и прочие нюансы, так как тема довольна обширная. После приступил к описанию составляющих компонентов IT-инфраструктуры (аппаратная, сетевая, программная). Обдумывал, как теорию связать с практикой, чтобы плавно перейти к описанию реальных задач, которые будут решаться в проекте.

25.04 Продолжил написание раздела 1.2, где поверхностно, чтобы не заполнять диплом излишней информацией, описал протоколы и решения, которые используются при проектировании или в процессе эксплуатации инфраструктуры. Приступил к написанию раздела 1.3, начал с описания традиционной инфраструктуры и особенностей при ее эксплуатации и внедрении. В предпоследнюю очередь начал детальное рассмотрение облачных инфраструктур, произвел детальное сравнение каждой и описал процесс, которого стоит придерживаться при выборе облачной инфраструктуры. Завершил раздел рассмотрением и описанием сетевой архитектуры, ее типов и решений, когда и в каком месте каждая из описанных может применяться, после произвел небольшое сравнение.

27.04 Приступил к разделу 1.4 «Безопасность IT-инфраструктуры». Первым делом написал небольшое введение по тому, что это и зачем инфраструктура должна находиться в безопасности. Приступил к описанию основных угроз и мер защиты по их устранению. После привел лучшие практики по использованию некоторых инструментов обеспечения информационной безопасности. После взялся за изучение законодательной базы, которая отвечает за безопасность информации.

30.04 Завершил написание раздела «Безопасность IT-инфраструктуры» и приступил к изучению и описанию представленных требований к будущему макету.

02.05 После долгого согласования требований приступил к написанию раздела 1.5 и анализу того, что будет реализовано в практической части дипломного проекта.

04.05 Приступил к выбору лабораторной среды, в которой будет реализован макет, исходя из требований описанных в прошлом разделе и анализа проблем, которые могут возникнуть при развертывании и настройке инфраструктуры.

06.05 После анализа и тестирования всех инструментов начал написание последнего раздела в теоретической части. Описал детальное сравнение всех инструментов, приложил изображения с момента тестирования каждого. Выбрал лабораторную среду и описал, почему проект будет реализован именно в ней.

08.05 Приступил к практической части. Начал раздел 2.1 «Определение ПО, сервисов и производителей, подходящих под требования», в котором по каждому пункту требований подобрал подходящих производителей и аргументировал свой выбор. Представил итоговую конфигурацию стенда дипломного проекта.

10.05 Начал раздел 2.2 «Планирование и подготовка к реализации будущей инфраструктуры», в котором описал процесс проектирования сетевой инфраструктуры и применения лучших практик.

12.05 Завершил практику, оформил все записи и подготовил отчет о проделанной работе. Подготовил документы для сдачи отчета и получения отзыва.

Заключение

В результате прохождения производственной практики на предприятии АО «КОНСИСТ-ОС» я ознакомился с должностью специалиста отдела аналитики и архитектуры государственной единой облачной платформы и государственной информационной системы, изучил актуальное отечественное ПО, методы и подходы к проектированию сетей и инфраструктурных сервисов,

Полученный опыт на предприятии поможет мне как личностно, так и профессионально развиваться в сфере администрирования инфраструктуры и в сфере ее проектирования и развертывания.