

Домен и управление инфраструктурой

Практический взгляд на выбор платформы, hybrid mode и подготовку проекта

Виталий Попов

Департамент Реализации Инфраструктурных Проектов



О чём поговорим

Фокус не на чек-листе функций, а на реальном пути перехода

1. Развилка рынка

Почему выбор чаще всего сводится к FreeIPA- и Samba-подходу

2. Что изменилось за последний год

Продукты развиваются, и архитектурные ограничения рынка уже не те, что год назад

3. Где подводные камни

Hybrid mode, совместимость, политики, service accounts и day-2 эксплуатация

4. Что нужно для успешной миграции

Аудит, целевая архитектура, пилот, автоматизация и управляемая этапность

5. Кейсы

Большой ландшафт, выбор кандидатов и зависимость от конфигурационного контура

Почему это не «замена домена»

Для enterprise-среды меняется не только каталог, а контур управления и доверенная модель

Что реально перестраивается

- идентичность пользователей и устройств
- модель делегирования и администрирования
- политики и конфигурации рабочих мест
- интеграции с почтой, PKI и прикладными ИС
- сайты, подсети, DNS, DHCP, NTP

Что это меняет в эксплуатации

- операционную модель команд сопровождения
- процедуры change / rollback
- наблюдаемость и аудит изменений
- длительный hybrid mode
- стоимость сопровождения

Ключевой риск: смотреть на проект как на поиск «аналога AD», а не как на смену платформенных допущений.

Рынок действительно разделился на два лагеря

На практике большинство проектов крутится вокруг FreeIPA- и Samba-подхода, плюс есть независимые кандидаты

FreeIPA-подход

- сильнее в Linux-first сценариях
- доверительные отношения с AD и сосуществование
- обычно требует отдельного слоя управления конфигурациями
- хорош при линуксовом фокусе и зрелой автоматизации



Samba-подход

- AD-подобная логика и объектная модель
- хорошо ложится на mixed Windows / Linux среды
- цена вопроса — сложность coexistence
- политики для Linux обычно требуют доп. инструментария



Независимые кандидаты

- собственные ядра и свой путь эволюции
- могут закрывать отдельные боли лучше open-source базы
- но важно проверять зрелость экосистемы и интеграций
- выбор почти всегда требует предметного пилота



Вывод: спор обычно уже не «что каталог вообще выбрать?», а «какая архитектурная ставка лучше переживёт ваш hybrid mode».

Что изменилось по материалам вендоров

По свежим публикациям видно: рынок стал зрелее именно в сценариях миграции, coexistence и управления

Альт Домен

- решение на базе Samba для смешанной Windows / Linux среды
- интеграция с MS AD без изменения структуры домена; постепенный переход заявлен как штатный сценарий
- поддержка схем домена 2012 / 2012 R2 / 2016 / 2019
- собственные Linux-инструменты ADMS, GPUI, GPUUpdate и GPResult для GPO-подобного управления и диагностики



RED ADM

- в актуальных обновлениях добавлены ADMT migration и поддержка Microsoft Exchange
- появились SID History, SID Filtering и задокументированный API
- добавлены миграция DHCP из Windows Server, проверки SELinux и совместимости уровней домена
- продукт усиливается уже не только как каталог, а как migration toolkit



ALD Pro 3.2.0

- в документации 3.2.0 как актуальной версии описаны hidden replica, глобальный каталог и модуль синхронизации
- документированы диагностика интеграции с MS AD, ошибки синхронизации и репликация FreeIPA
- явно оформлены контуры групповых политик, HBAC, sudo, автоматизации и журналирования
- в домен заводятся Astra Linux 1.7/1.8, Альт и РЕД ОС - это важно для mixed-инфраструктур

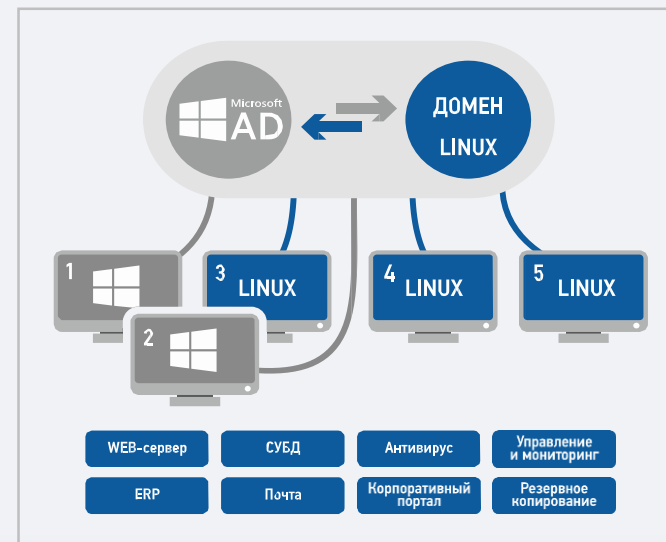


Вывод: свежие материалы уже позволяют обсуждать не абстрактный “аналог AD”, а конкретные сценарии — coexistence с MS AD, групповые политики, trust / sync, Exchange, DHCP и day-2 управление.

Как выглядит реальный контур миграции

Цели проекта:

- Импортзамещение базовых инфраструктурных сервисов и служб
- Внедрение автоматизированного управления базовыми инфраструктурными сервисами и службами
- Внедрение автоматизированного управления АРМ пользователей
- Обеспечение необходимого и достаточного уровня информационной безопасности



500

ИТ отдел

10

Филиалов

12K

АРМ

20K

ПЯ

85

ИС

112

ПО

400

Серверов

500

GPO

ОБСЛЕДОВАНИЕ

6 месяцев

ПРОЕКТИРОВАНИЕ

3 месяца

ПМИ(ПСИ)

4 месяца

МЕТОДИКА И
МИГРАЦИЯ

6 месяцев

ОПЭ и ТП

6 месяцев

С таким масштабом подводные камни почти всегда лежат в периферии проекта: прикладные интеграции, service accounts, почта, PKI, нестандартные политики, филиальная сеть и профиль сопровождения.

Где обычно находятся подводные камни

Проблемы редко в самом каталоге — чаще в связях вокруг него

Почта

- Exchange / coexistence
- почтовые атрибуты
- адресные книги и делегирование

Приложения и ИБ

- Kerberos / SPN
- hardcoded зависимости
- service accounts

Политики

- разрыв между GPO и Linux
- скрипты vs policy engine
- дрейф конфигурации

Сеть и сайты

- DNS/DHCP/NTP
- сайты и подсети
- межфилиальные задержки

Эксплуатация

- rollback
- аудит изменений
- обучение и ownership

Самая дорогая ошибка — поздно обнаружить зависимости, из-за которых приходится держать старый домен заметно дольше запланированного.

Самый сложный этап — не cutover, а hybrid mode

Именно сосуществование обычно рождает больше всего дорогих вопросов

Старый контур

MS AD

исторические политики

почтовые связи

интеграции

операционные привычки



- authoritative source по объектам
- правила синхронизации атрибутов
- границы ответственности команд
- условия выхода из coexistence

Новый контур

новая модель каталога

конфигурации

новые точки консолидации

новые средства автоматизации

Если этот этап недоописан, проект легко превращается во «временную архитектуру», которая живёт годами.

Что необходимо для успешной миграции

Хорошая миграция — это не только выбор платформы, а последовательность подготовительных решений

1. Аудит

приложений, домена, сервисов, политик, service accounts, GPO, филиалов

2. Целевая архитектура

каталог, DNS/DHCP/NTP, PKI, sites/subnets, CM, почта

3. Пилот

проверка реальных пользовательских и прикладных сценариев

4. Конфигурационное управление

массовые настройки, inventory, drift control, rollback

5. Пошаговая миграция

этапность, метрики, ownership, контроль рисков

6. Эксплуатационная модель

операции, мониторинг, аудит, обучение и поддержка

Если хотя бы один блок из этого списка провисает, проект чаще всего зависает либо на пилоте, либо в затянувшемся hybrid mode.

Автоматизация нужна, но она не серебряная пуля

Инструменты конфигурационного управления ускоряют проект, но не заменяют архитектурную работу

Что реально даёт автоматизация

- массовые изменения без ручной рутины
- единый контур для Windows / Linux
- доставка конфигураций и ПО
- повторяемость и контроль волн миграции

Чего она не решает сама

- неразобранные зависимости приложений
- архитектурную неопределённость
- ownership и процессы сопровождения
- ошибки выбора target state

Правильная роль инструмента: force multiplier для уже спроектированной миграции.

Кейс 1

Модернизация ИТ-инфраструктуры крупной распределительной энергетической компании

Масштабный ландшафт, миграция рабочих мест и базовых сервисов | 11 месяцев

Исходные вводные

- требование уйти на российское ПО
- план: 7 000 сотрудников за год
- нужно перевести не только АРМ, но и базовые сервисы

Что делали

- обучение персонала и прототипирование
- клонирование текущих образов и развёртывание мини-модели среды
- перевод базовых инфраструктурных сервисов
- собственный инструментарий для ускорения миграции

Что этот кейс показывает

- доменная миграция быстро становится инфраструктурной программой проектов
- без прототипа и дополнительного инструментария темп не держится
- скорость достигается не одним продуктом, а правильной сборкой контура

Выбор каталога через демостенды, а не через маркетинговые обещания

двухэтапный подход

Ситуация

Заказчик рассматривал замену базовых инфраструктурных сервисов, включая службу каталогов, систему мгновенных сообщений и управление конфигурациями.

Подход

- для каждой категории были собраны демостенды на площадке заказчика
- по результатам тестов был подготовлен отчёт с плюсами и минусами решений
- второй этап — уже внедрение выбранного стека в боевую инфраструктуру

Вывод

Связка FreeIPA / Samba / независимые кандидаты почти никогда не должна выбираться только по презентациям. Слишком многое становится видно только на демостенде: интеграции, модели управления, поведение в coexistence и удобство эксплуатационных операций.

Опыт, он приходит с «опытом»

Работы завершены в срок, не более чем 6 месяцев с даты подписания договора на выполнение работ.

3.5.2. Надёжность решений.

Процент инцидентов, связанных с внедряемыми решениями, составляет не более 2% от общего количества ИТ-инцидентов Заказчика.

3.5.3. Удовлетворение клиентских ожиданий.

Устранены все замечания конечных потребителей внедряемых решений, предоставленные Заказчиком по результатам проведённых ПМИ (работники и технический персонал АО РНПК).

3.5.4. Достижение ключевых параметров по совместимости.

Количество служебных и бизнес информационных систем и сервисов Заказчика успешно интегрировано с новой ЕСК на 97%.

КПО успешно развернуто на 97% АРМ Заказчика.

Итоги обследования

- 30 информационных систем
- Из них 15 Microsoft
- Эксплуатация не обучена

Критерии ТЗ недостижимы

Как я бы формулировал критерии выбора сегодня

Не по количеству галочек в матрице, а по тому, что важнее для вашего перехода

Критерий	FreeIPA-подход	Samba-подход	Независимые кандидаты
Mixed Windows / Linux	средне	сильнее	зависит от конкретного вендора
Нужен AD-подобный UX	скорее нет	ближе к ожиданиям	очень по-разному
Linux-first и зрелая автоматизация	сильнее	возможно, но не всегда оптимально	зависит от экосистемы
Сложные интеграции и долгий coexistence	проверять отдельно	проверять отдельно	обязателен пилот
Риск быстрого устаревания оценки	средний	средний	выше из-за темпа эволюции

Итоговый выбор всё равно делается только после стенда / пилота на актуальных версиях решений.

Практические рекомендации перед стартом проекта

Что лучше сделать до выбора платформы и до запуска пилота

1. Зафиксировать список критичных интеграций и владельцев систем
2. Отдельно описать сценарии hybrid mode и критерии выхода из coexistence
3. Проверить почтовые, PKI и service-account зависимости раньше, чем кажется нужным
4. Рассматривать каталог и управление конфигурациями как единый контур
5. Делать пилот на актуальных релизах и с реальными прикладными сценариями
6. Сразу проектировать «эксплуатацию»: мониторинг, аудит, rollback, ownership

Успешная миграция домена — это не выбор
«правильного продукта»,
а грамотное прохождение пути
от аудита до эксплуатации.

