А. М. Охохонин, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732, 004.722

ОРГАНИЗАЦИЯ БЕЗОПАСНОЙ МИГРАЦИИ КОНТРОЛЛЕРА ДОМЕНА КОМПЬЮТЕРНОЙ СЕТИ ПРЕДПРИЯТИЯ СРЕДСТВАМИ ОТЕЧЕСТВЕННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Аннотация. В данной статье проанализированы отечественные программные решения для управления службой каталога и рассмотрены угрозы информационной безопасности, которые могут возникнуть во время миграции контроллера домена организации. Результатом исследования стал алгоритм безопасной миграции контроллера домена в компьютерной сети компании.

Ключевые слова: алгоритм миграции контроллера домена, угрозы информационной безопасности, LDAP, Astra Linux, Ald Pro, автоматизация.

Введение. В связи со сложившейся в мире ситуацией противостояния, многие зарубежные компании, чье программное обеспечение широко использовалось в российских компаниях, прекращают свою деятельность на территории Российской Федерации. Это грозит невозможностью использовать программное обеспечение, на которое российские компании полагались десятилетиями, что, в свою очередь, ставит под угрозу современные бизнес-процессы, зависящие от сетевой инфраструктуры организации.

Контроллер домена — центральный сервис в современных компьютерных сетях. Windows Server — флагманский программный продукт компании Microsoft, на котором работают большинство компаний в мире.

Миграция контроллера домена Microsoft — трудоемкий процесс, и допущенные в ней ошибки могут привести к появлению уязвимостей в IT-инфраструктуре организации. В то же время инструкции, направленные на помощь в этом процессе, как правило, описывают только отдельные шаги и не всегда учитывают проблемы информационной безопасности.

На отечественном рынке существует несколько решений для управления службой каталога. В процессе миграции в каждом отдельно взятом решении есть свои тонкости, а потому во время его реализации могут возникнуть ошибки, уникальные именно для него.

В проанализированных нами статьях были представлены сценарии миграции доменных инфраструктур [1], особенности выбора программных решений для развертывания доменной инфраструктуры [2], а также особенности и проблемы различных решений для централизованного управления компьютерной сетью [3-5]. В данном исследовании были определены проблемы информационной безопасности, связанные с миграцией контроллера домена на отечественное программное обеспечение, при этом особое внимание уделялось вопросам автоматизации процесса миграции.

Проблема исследования. Для того чтобы разработать алгоритм безопасной миграции контроллера домена, были поставлены следующие задачи:

1. Проанализировать современные отечественные и открытые программные решения для организации служб каталогов и провести сравнительный анализ их функциональных возможностей;

2. Выявить актуальные угрозы информационной безопасности для компании, возникающие в результате миграции;

3. Разработать и задокументировать алгоритм поэтапной безопасной миграции контроллера домена Active Directory в выбранное программное решение;

4. Разработать набор скриптов, обеспечивающий частичную автоматизацию алгоритма безопасной миграции.

Материалы и методы. Методами исследования являются анализ, изучение, моделирование. Апробация проводилась на виртуальных образах сетевого оборудования с использованием системы оркестрации GNS3 версии 2.2.6, для чего использовались IOU-образы маршрутизаторов и коммутаторов Cisco. С целью виртуализации оконечных устройств использовался программный гипервизор VirtualBox версии 6.1.48.

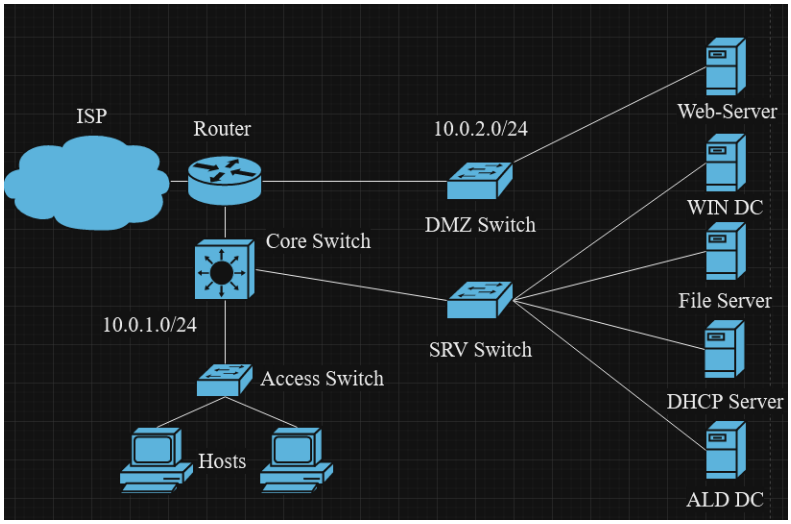

Рис. 1. Виртуальный стенд в среде GNS3

Результаты. В настоящее время существует несколько отечественных программных решений для управления службой каталога. В данной работе были рассмотрены ALD Pro, Атом.Домен и РЕД АДМ, наряду с классическими открытыми решениями FreeIPA, Samba AD, и проведен сравнительно-сопоставительный анализ их функциональных возможностей (табл. 1).

Таблица 1

Сравнение программного обеспечения для управления службой каталога

Функциональная возможность	*ALD Pro*	*Атом. Домен*	*РЕД АДМ*	*Free IPA*	*Samba AD*
Поддержка системы поддоменов	+	+	-	+	-
Широкий спектр работы с различными операционными системами	-	+	-	+	+
Инструменты для миграции из Active Directory	+	+	+	-	-
Независимость развития продукта от зарубежных продуктов	+	-	+	-	-
Специализированная разработка конкретной защищенной отечественной операционной системы	+	-	+	-	-

Для дальнейшей работы было выбрано решение ALD Pro от компании «РусБИТех-Астра». Это программное решение получает частые обновления, в которых добавляют недостающие функции; имеет широкие возможности для администрирования клиентских станций с операционной системой Astra Linux и инструменты для плавной и безопасной миграции из Microsoft Active Directory, а также поддерживает поддомены, что подходит для решения задач многих организации.

В ходе миграции контроллера домена могут быть допущены ошибки, которые в дальнейшем приведут к инцидентам информационной безопасности. Речь идет, например, об использовании незашифрованного протокола LDAP в процессе миграции. В этом случае контроллеры домена обмениваются информацией (в том числе логинами и паролями) в открытом виде (рис. 2), и злоумышленник, имеющий доступ к сетевой среде, сможет их перехватить. Один из способов этого избежать — использование протокола LDAPs, который шифрует сообщения LDAP с помощью сертификатов криптографического протокола SSL, что обеспечивает безопасность при взаимодействии контроллеров домена в процессе миграции.

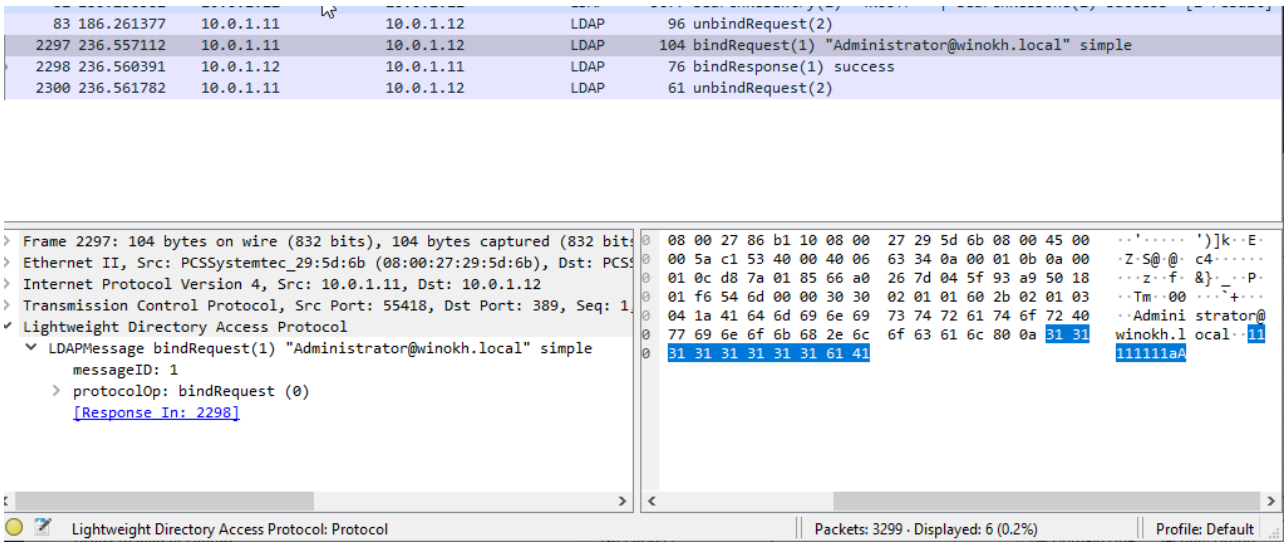

Рис. 2. Пример открытого сообщения LDAP

С целью предотвращения подобных инцидентов был разработан подробный алгоритм миграции контроллера домена, который учитывает все найденные актуальные угрозы, и сводит к минимуму вероятность их успешной реализации.

Алгоритм состоит из следующих этапов:

1. Предварительный этап (резервное копирование, информирование пользователей);
2. Первичное внедрение (установка и настройка первого контроллера домена, подготовка к миграции, миграция учетных записей, групп, организационных подразделений, генерация и распространение одноразовых паролей пользователей);
3. Гибридный этап (сосуществование двух доменов, миграция некоторых рабочих станций, настройка вспомогательных серверов в новом домене);
4. Завершающий этап (окончательный перенос доменной инфраструктуры в новый домен, миграция оставшихся рабочих станций на Astra Linux, вывод из эксплуатации контроллеров домена Active Directory).

На каждом этапе учтены проанализированные угрозы информационной безопасности, что позволяет минимизировать их реализацию.

Также были разработаны скрипты, автоматизирующие решение некоторых задач, которые возникают при миграции:

1. Первичная установка и настройка сервера контроллера домена ALD Pro;
2. Добавление нового сервера в уже развернутый домен ALD Pro;
3. Добавление нового клиента в домен ALD Pro;
4. Генерация безопасных одноразовых паролей для пользователей ALD Pro.

Для реализации автоматической миграции был разработан bash-скрипт, выполняющий первичную установку и настройку контроллера домена ALD Pro на базе Astra Linux Special Edition 1.7.4, работающей в максимальном режиме безопасности «Смоленск». Эта задача в текущем виде требует настройки сетевых интерфейсов и репозиториев, службы разрешения имен, установки пакетов и базовой конфигурации контроллера домена. Все эти действия выполняются вручную, и поэтому вероятны ошибки, которые приведут к некорректной работе и инцидентам безопасности. Используя скрипт, администратор указывает параметры, и вся настройка выполняется автоматически. Скрипт выполняет следующие действия:

1. Устанавливает указанное пользователем имя контроллера домена.
2. Настраивает статическую IP-адресацию.
3. Отключает службу NetworkManager.
4. Настраивает разрешение локального имени в файле /etc/hosts.
5. Подключает репозитории Astra Linux и ALD Pro.
6. Обновляет необходимые пакеты.
7. Устанавливает пакеты ALD Pro (включая глобальный каталог и модуль синхронизации).
8. Устанавливает локальный адрес в качестве DNS сервера.
9. Запускает встроенный скрипт ALD Pro для повышения привилегий сервера до контроллера домена.

Скрипты для добавления машин в домен выполняются около 30 минут, и исключают примерно 6-10 минут ручной настройки на каждой машине (без учета возможных ошибок). Скрипт для генерации и смены паролей необходим, так как миграция паролей пользователей из Active Directory в ALD Pro версии 2.1.0 не поддерживается. Он позволяет автоматически сгенерировать и назначить безопасные одноразовые пароли для пользователей. На смену пароля одного пользователя скрипт тратит примерно 0,5 секунды (из-за встроенной в команду ipa user-mod задержки). Исходя из того, что с аналогичной задачей администратор справится за 15 секунд, можно заключить что при смене паролей 10 000 пользователей скрипт сэкономит примерно 40 часов рабочего времени.

Заключение. В результате исследования было проведено сравнение отечественных программных решений для управления службой каталога и разработан алгоритм безопасной миграции, с учетом угроз, которые могут возникнуть в процессе миграции. Также была смоделирована компьютерная сеть компании в современной среде виртуализации, где алгоритм прошел успешную апробацию. Разработанный набор bash-скриптов оптимизирует процесс миграции и обеспечивает частичную автоматизацию алгоритма безопасной миграции.

СПИСОК ЛИТЕРАТУРЫ

1. Синельников Е. Сценарии миграции доменных инфраструктур / Е. Синельников // Объединенная конференция «СПО: от обучения до разработки»: сборник тезисов конференции, Переславль-Залесский, 19–22 мая 2022 года. — Москва: ООО «МАКС Пресс», 2022. — С. 187-191. — EDN BULGXF. URL: https://elibrary.ru/item.asp?id=48603367 (дата обращения: 28.03.2024).
2. Ильенко В.О. Обоснование выбора средств развертывания доменной инфраструктуры телекоммуникационной системы на базе отечественного системного и прикладного программного обеспечения / В.О. Ильенко // III научно-педагогические чтения молодых ученых имени профессора С.В. Познышева: сборник материалов Всероссийской научно-практической конференции курсантов и студентов, Воронеж, 19 апреля 2023 года. — Воронеж: ФКОУ ВО Воронежский институт ФСИН России, 2023. — С. 53-55. — EDN LEWLRL. — URL: https://elibrary.ru/item.asp?id=60047288 (дата обращения: 28.03.2024).
3. Яремчук С. Проект FreeIPA. Централизованное управление сетью / С. Яремчук // Системный администратор. — 2011. — № 5 (102). — С. 40-46. — EDN RFVGDH. — URL: https://www.elibrary.ru/item.asp?id=20464151 (дата обращения: 28.03.2024).
4. Ильенко В.О. Анализ возможности практического применения программного комплекса ALD pro для централизованного управления / В.О. Ильенко, А.С. Кравченко // Актуальные проблемы деятельности подразделений УИС: сборник материалов Всероссийской научно-практической конференции, Воронеж, 20 октября 2022 года. — Воронеж: Издательско-полиграфический центр «Научная книга», 2022. — С. 90-92. — EDN JHVNLV. URL: https://elibrary.ru/item.asp?id=50055600. (дата обращения: 28.03.2024).
5. Ландышева О.Н. Проблемы импортозамещения централизованной системы аутентификации пользователей информационной системы для малого авиапредприятия / О.Н. Ландышева, В.А. Ландышев // Гражданская авиация: прошлое, настоящее, будущее: материалы всероссийской научно-практической конференции, посвященной празднованию 100-летия гражданской авиации России (Авиатранс-2023), Ростов-на-Дону, 20 октября 2023 года. — Ростов-на-Дону: Общество с ограниченной ответственностью «ДГТУ-ПРИНТ», Московский государственный технический университет гражданской авиации, 2023. — С. 129-133. — EDN PCXAYK. URL: https://www.elibrary.ru/item.asp?id=59742689. (дата обращения: 28.03.2024).