ДОВЕРЕННАЯ ДОМЕННАЯ ИНФРАСТРУКТУРА

ИМПОРТОЗАМЕЩЕНИЕ В ДЕЙСТВИИ

Денис ПОЛУШИН
менеджер продукта Aladdin Enterprise CA, компания Аладдин

Евгений ПАУТОВ
директор департамента разработки средств управления ГК «Астра»

Большинство компаний используют в качестве системы управления доменом решения от Microsoft. Ввиду ухода из России иностранного вендора заказчикам нужен работоспособный сценарий импортозамещения, который бы позволил им перевести корпоративную инфраструктуру на отечественные решения, выстроив на их основе безопасную доверенную ИТ-среду. Это серьезная и масштабная задача, которая требует комплексного подхода, и она может быть решена путем интеграции совместимых продуктов. Приведем пример совместной работы таких компонентов.

Первый из них — система централизованного управления службой каталогов ALD Pro от ГК «Астра». Она позиционируется разработчиками как полноценная замена Microsoft Active Directory. Второй компонент — корпоративный центр сертификации, разработанный российской компанией Аладдин. Это решение Aladdin Enterprise CA, призванное заменить службу Microsoft Certificate Services. Третий участник интеграции — Aladdin SecurLogon — клиентское приложение, которое реализует двухфакторную аутентификацию в среде Linux.

Расскажем подробнее о продуктах и о том, как они взаимодействуют друг с другом. ALD Pro существует на рынке уже более года и внесен в реестр отечественного ПО Минцифры. Он позволяет построить доменную инфраструктуру под Linux, причем с использованием не только Astra Linux, но и других дистрибутивов, и управлять ее объектами: компьютерами, учетными записями пользователей и серверами. Когда разработчики из ГК «Астра» создавали это решение, они думали в первую очередь про администраторов систем от Microsoft, которые мигрируют на Linux и не имеют достаточных компетенций для работе с этой ОС. Написание скриптов, работа в терминале и другие тривиальные для администратора-линуксоида действия вызывают у них затруднения. Поэтому ALD Pro спроектировали таким образом, что вся работа ведется в графическом интерфейсе, как это сделано в MS Active Directory.

Важным аспектом при работе с доменом является управление организационной структурой. Существуют Open Source-проекты для Linux, такие как служба каталогов FreeIPA. Однако там отсутствует возможность завести подразделения в виде структуры, иерархии, а имеется лишь «плоский» справочник. Эта недостающая возможность реализована в ALD Pro. Поддержка организационной структуры позволяет более эффективно настраивать полномочия администраторов, а также предоставляет больше возможностей для работы с групповыми политиками, чтобы они корректно распределялись по подразделениям.

Из последних нововведений в ALD Pro можно отметить поддержку глобального каталога, появление двусторонних доверительных отношений и синхронизации объектов. Пользователям очень важна гетерогенная работа в нескольких доменах, поскольку импортозамещение происходит не одномоментно: это долгий процесс, который может занимать не один год. Соответственно, администратору и пользователям, которые находятся в домене, нужно иметь возможность работы в гетерогенной среде.

Ранее продукт обладал только базовой функциональностью. Можно было настроить контролеры доменов, в целом развернуть службу каталога в своей инфраструктуре, завести туда компьютеры, учетные записи пользователей, настроить оргструктуру и работать с групповыми политиками, а также устанавливать ОС и ПО по сети.

В результате был сделан инструмент, который в автоматическом режиме синхронизирует все учетные записи между двумя доменами. Пользователи,

которые перешли на Linux, должны иметь доступ ко всем ресурсам, которые развернуты на Microsoft Windows. Миграция ресурсов — это процесс еще более длительный, поэтому разработчики реализовали функции глобального каталога и двусторонних доверительных отношений.

Ранее доверительные отношения также существовали, однако они были односторонними. ALD Pro доверял ресурсам Active Directory, а последняя не допускала учетные записи ALD Pro в свой домен, и в этом году в системе появилась возможность настройки полноценного двунаправленного доступа между доменами.

Также совместно с компанией Аладдин в этом году в ALD Pro было реализовано совместное решение для двухфакторной аутентификации в домене с использованием токенов JaCarta.

Как работает этот механизм? Внутри корпоративной инфраструктуры используются сертификаты, которые могут выдаваться как внешним, так и внутренним пользователям для аутентификации, подключения через VPN, документооборота и т.д. Сертификаты есть не только у пользователей, но и у серверов, сервисов, устройств. Компания Аладдин предоставляет корпоративный центр сертификации, Aladdin Enterprise CA. Решение предназначено для внедрения строгой аутентификации, создания по-настоящему доверенной инфраструктуры, обеспечения устройств и объектов сертификатами и корпоративными электронными подписями. Продукт зарегистрирован в реестре отечественного ПО.

В числе ключевых особенностей Aladdin Enterprise CA можно упомянуть ориентацию на пользователей Microsoft Certificate Services, поддержку миграции с решения Microsoft, совместимость с российскими операционными системами, включая Astra Linux, а также с доменами Active Directory и ALD Pro. Также важны наличие и поддержка всего необходимого функционала для организации PKI-инфраструктуры: иерархия, настройка точек доступа CRL DP, AIA, DeltaCRL, OCSP и т.д.

Поддерживаются алгоритмы шифрования RSA и ECDSA. В ближайших планах разработчиков — добавление поддержки алгоритмов ГОСТ. Имеется ролевая модель полномочий, возможность уведомления пользователя, различные способы выпуска сертификатов. Доступен API для подключения внешних систем.

Можно создать пароль длиной до 63 символов, скрытый от пользователя и недоступный, который нельзя записать на бумажке и приклеить на монитор

Клиентское решение Aladdin SecurLogon также служит важным элементом в построении инфраструктуры для двухфакторной аутентификации. Оно необходимо для настройки двухфакторной аутентификации, хотя, конечно, он обладает и другими функциями. К примеру, в инфраструктуре для пользователей он позволяет применять определенные политики в части обеспечения строгости и надежности пароля. Так, можно создать пароль длиной до 63 символов, скрытый от пользователя и недоступный, который нельзя записать на бумажке и приклеить на монитор, что обычно бывает со сложными паролями. От пользователя будет требоваться вход в систему только по токену. Есть и средства для группового администрирования, групповое развертывание и удаленная настройка с рабочего места администратора, защита удаленных соединений по RDP или SSH и др. Это мощный клиентский компонент, который можно применять для настройки аутентификации по сертификату, хотя его возможности гораздо шире.

Что дает интеграция ALD Pro и продуктов компании Аладдин? Пользователь получает токен JaCarta вместе с ключевой парой, сгенерированной удостоверяющим центром Aladdin Enterprise CA. С его помощью происходит двухфакторная аутентификация. Благодаря использованию Aladdin Enterprise CA стало возможным развернуть корпоративную PKI-инфраструктуру в среде Linux и управлять пользовательскими ключами и сертификатами. Подобная автоматизация особенно заметна и эффективна, когда речь идет о сотнях и тысячах пользователей, которых необходимо обеспечить токенами.

Второе приложение, Aladdin SecurLogon, предоставляет удобный графический интерфейс, с помощью которого можно аутентифицироваться в системе, используя двухфакторную аутентификацию.

Важным моментом в применении решений, позволяющих использовать двухфакторную аутентификацию внутри защищенной доменной инфраструктуры, является тот факт, что она значительно повышает сохранность и безопасность учетных данных пользователей домена. Это возможно благодаря совместной работе продуктов ALD Pro и Аладдин.

Aladdin Enterprise CA подключается к каталогу ALD Pro, получает сведения об учетных записях пользователей и их свойствах, позволяет выпустить для них сертификаты и опубликовать их на контроллере домена в ALD Pro. Таким образом все пользователи домена имеют свои сертификаты для входа в домен, что повышает уровень информационной безопасности.

ALD Pro контролирует, чтобы информация об ИТ-ландшафте не стала доступна злоумышленникам, и они не смогли спланировать и совершить атаку. Ролевая модель и механизмы разграничения доступа в ALD Pro позволяют защитить от посторонних глаз множество объектов инфраструктуры: компьютеры, серверы и учетные записи пользователей. А злоумышленника, не обладающего сертификатом, контроллер домена просто не пропустит на этапе аутентификации.