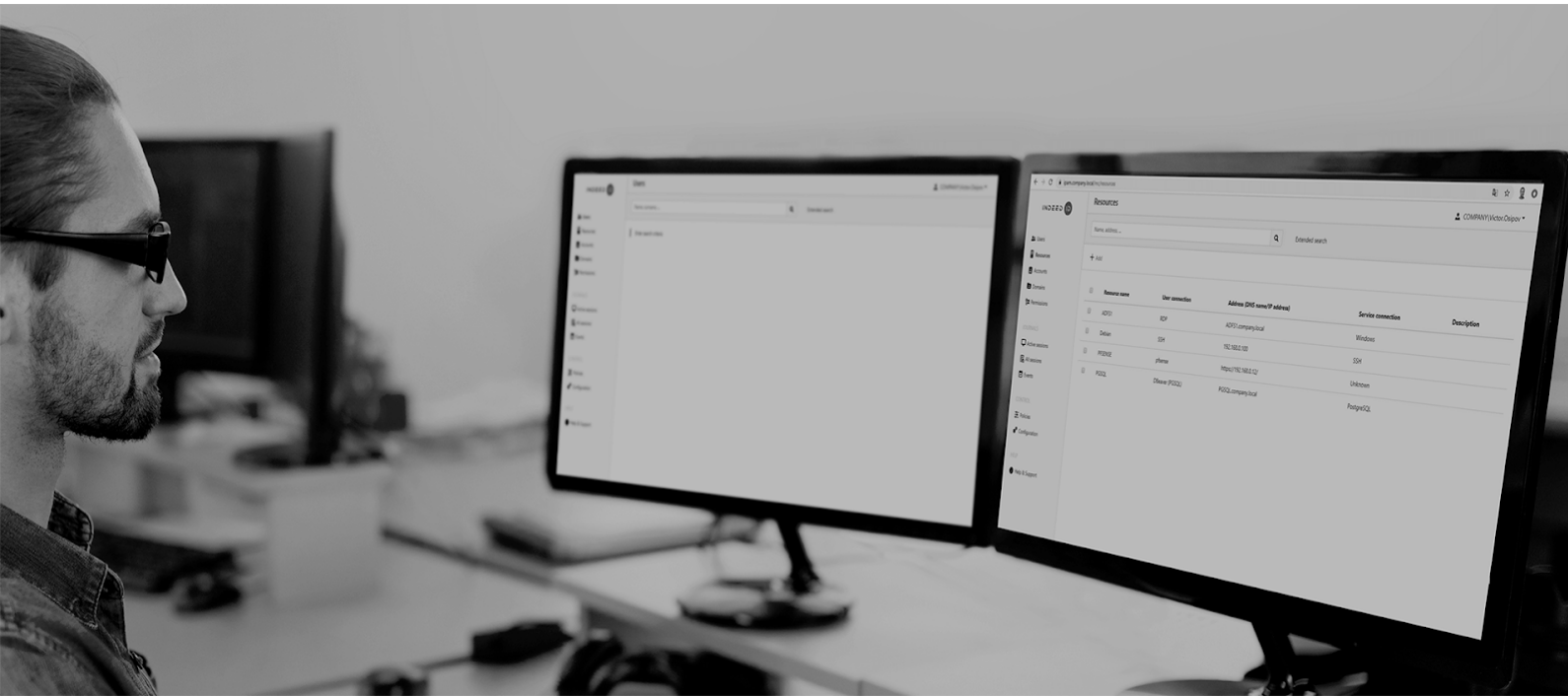
INDEED ID

WHITE PAPER

INDEED PRIVILEGED ACCESS MANAGER

Управление доступом привилегированных пользователей к ИТ-системам компании



Содержание

Привилегированный доступ - угроза безопасности

Постоянное наращивание и усложнение IT-инфраструктуры компаний делает управление привилегированным доступом одной из важнейших задач информационной безопасности. Увеличивающееся количество информационных систем и разнообразие сценариев доступа к ним затрудняют решение этой задачи. Получив данные административной учетной записи (УЗ), злоумышленник может нанести предприятию намного более серьезный ущерб, чем в случае компрометации учетных данных рядового сотрудника. Административные учетные записи могут быть использованы для отключения защиты, остановки работы информационных систем и доступа к конфиденциальной информации. Защитить привилегированный доступ сложнее, решение этой проблемы невозможно с использованием общих подходов к защите учетных данных и требует применения специализированных решений.

Привилегированные пользователи

Иметь повышенные права доступа к важной информации и критичным функциям программного обеспечения и оборудования могут различные категории как штатных, так и внешних сотрудников компании.

Администраторы информационных систем

Каждое устройство и каждое прикладное или системное программное обеспечение имеют свои административные учетные записи. Это самая очевидная группа сотрудников привилегированного доступа, примерами таких сотрудников являются:

- Администраторы Active Directory
- Администраторы сетевого оборудования
- Администраторы баз данных
- Администраторы серверов (Windows, Unix/Linux)
- Администраторы VDI

Бизнес-пользователи

Несмотря на то, что бизнес-пользователи не обладают административным доступом, они могут иметь широкие полномочия в рамках отдельно взятых информационных систем. Например, они могут иметь возможность выполнять денежные переводы, управлять производственным процессом и получать доступ к данным, которые являются коммерческой тайной.

Подрядчики и партнеры

Сотрудники подрядчиков, как правило, выполняют сопровождение специализированных программных и аппаратных комплексов. Это могут быть сотрудники вендора или интегратора. Обычно такие пользователи имеют удаленный доступ в инфраструктуру предприятия, что дополнительно осложняет контроль их работы.

Служебные учетные записи

Служебные учетные записи используются для автоматизации процессов. От их имени работают различные службы и демоны, скрипты и другое программное обеспечение. Про такие учетные записи легко забыть, т.к. сотрудники не используют их в явном виде каждый день. Это создает дополнительные трудности и риски.

Управление привилегированным доступом

Для успешного решения проблемы управления и защиты привилегированного доступа необходимо обеспечить выполнение следующих задач:

- Централизованное управление доступом сотрудников к контролируемым ресурсам.
- Предотвращение бесконтрольного использования привилегированных учетных записей, обнаружение и взятие их под контроль. Хранение паролей в секрете, регулярная проверка и смена паролей на случайные значения.
- Сокращение количества привилегированных учетных записей, необходимых для управления информационными системами предприятия. Регистрация в журнале доступа попыток использования привилегированных учетных записей, с указанием какой сотрудник, когда и к какой учетной записи получал доступ.
- Обеспечение мультифакторной аутентификации сотрудников при доступе к привилегированным учетным записям.
- Реализация механизмов расследования инцидентов и восстановления картины случившегося.

Продукт Indeed Privileged Access Manager (Indeed PAM) представляет собой систему управления доступом с использованием привилегированных учетных записей. Ниже описано, как Indeed PAM решает перечисленные задачи.

Централизованное управление доступом

Indeed PAM хранит информацию обо всех привилегированных учетных записях и выданных разрешениях на их использование. Разрешения в Indeed PAM являются основным механизмом предоставления привилегированного доступа сотрудникам. Разрешение определяет следующие параметры доступа:

- кто имеет доступ — какие пользователи или группы пользователей;
- куда — какие сервера, оборудование и приложения будут доступны для работы;
- с какими правами — какая учетная запись будет использоваться для подключения;
- на каких условиях выдается доступ — на какое время и с каким графиком, по каким протоколам.

Рисунок 1. Параметры разрешения на доступ

Разрешения выдаются централизованно администратором в консоли управления Indeed PAM. Разрешение может быть приостановлено для временного прекращения доступа или отозвано, если доступ более не требуется. Indeed PAM поддерживает интеграцию с системами класса Service/Help

Desk. Такая интеграция позволяет использовать процесс согласования доступа в привычной для сотрудников системе и автоматически выдавать и отзывать разрешения в Indeed PAM в рамках данного рабочего процесса. Для этих целей Indeed PAM предлагает два механизма взаимодействия: утилита командной строки и программный web-интерфейс (API).

Механизм разрешений дополняет еще один инструмент контроля доступа — политики Indeed PAM. Политики определяют общие параметры доступа, такие как:

- разрешенные и запрещенные команды в ssh-сессиях
- требуется ли одобрение администратора PAM на открытие привилегированной сессии
- доступные локальные ресурсы пользовательского ПК на удаленном ресурсе (диски, буфер обмена и др.)
- необходимость сброса пароля привилегированной учетной записи после завершения сессии
- эксклюзивное использование привилегированной учетной записи (невозможность открытия двух сессий под одной учетной записью)
- максимальная продолжительность привилегированной сессии.

Контроль использования привилегированных учетных записей

Для контроля за использованием привилегированных учетных записей Indeed PAM реализует четыре механизма:

- Обнаружение привилегированных учетных записей
- Хранение учетных данных
- Ротация паролей и SSH ключей
- Безопасное использование учетных данных

Обнаружение учетных записей

Indeed PAM включает механизм Account Discovery, который реализует функции регулярного поиска новых учетных записей на подключенных ресурсах и доменах. Частота поиска настраивается и может отличаться для разных групп ресурсов. Когда система находит новую учетную запись, которая еще не зарегистрирована в PAM, информация о ней заносится в общий репозиторий. Кроме того, в журнал записывается соответствующее событие, на которое администратор может получить почтовое уведомление, чтобы более оперативно принять решение об использовании новой учетной записи. Indeed PAM поддерживает поиск учетных записей на следующих типах ресурсов:

- Windows PC и сервера[1]
- *nix системы
- СУБД (MS SQL, MySQL, PostgreSQL, Oracle DB)
- Active Directory.

Хранение учетных данных

Indeed PAM выступает в роли централизованного репозитория привилегированных учетных данных, доступ к которым предоставляется только при наличии действующего разрешения. Без такого разрешения даже администратор PAM не имеет прав на просмотр паролей и SSH ключей.

Кроме хранения Indeed PAM выполняет регулярную проверку паролей и SSH ключей, чтобы убедиться, что в системе хранятся актуальные учетные данные. Если будет обнаружено несовпадение,

[1] В текущей версии выполняется поиск локальных учетных записей, в будущих версиях появится возможность искать служебные учетные записи, от имени которых запускаются службы и запланированные задания.

администратор получит соответствующее уведомление.

Ротация паролей и SSH ключей

Чтобы обеспечить безопасность паролей и SSH ключей, Indeed PAM выполняет их смену на случайные по заданному расписанию. Для соблюдения политик безопасности компании можно настроить параметры сложности генерируемого пароля.

Все предыдущие значения паролей и SSH ключей также сохраняются в PAM в истории паролей. Это дает возможность “откатить” пароль или ключ на любой требуемый момент в прошлом. Данная функция необходима, когда целевой ресурс восстанавливается из резервной копии, и нужно использовать учетные данные, актуальные на момент создания резервной копии.

Безопасное использование привилегированных учетных данных

Внедряя Indeed PAM, компании могут отказаться от использования сотрудниками привилегированных учетных данных в явном виде. Администраторам серверов, сетевого оборудования, Active Directory и прикладных систем больше не требуется владеть административными учетными данными, эту задачу для них решает PAM. Сотрудник подключается к PAM с помощью своей пользовательской учетной записи, а на целевом ресурсе ему открывается сессия под учетной записью, обладающей нужным набором прав. Такой подход позволяет предотвратить бесконтрольное использование привилегированных учетных записей, когда сотрудники могут хранить их в небезопасном месте (в файлах на рабочем столе или сетевом диске, на стикерах и т.п.) или умышленно передать пароли третьим лицам.

Для наиболее важных привилегированных учетных записей Indeed PAM позволяет включить режим эксклюзивного использования. В этом режиме от имени привилегированной учетной записи возможно открыть только одну сессию. Это позволяет избежать проблем, связанных с одновременным внесением изменений в администрируемые системы.

Single Sign-On

Indeed PAM позволяет открывать сессии с прозрачной для пользователей передачей учетных данных на целевой ресурс не только для классических протоколов удаленного доступа, таких как RDP, SSH или Telnet. В состав системы входит специализированный SSO агент (Single Sign-On агент), который обеспечивает автоматическую подстановку учетных данных в формы web- и desktop-приложений. Используя агент, Indeed PAM может предоставлять прозрачный доступ к web-интерфейсам администрирования сетевого оборудования, “толстым” клиентам СУБД и другим приложениям.

Application to Application Password Management[2]

Учетные записи с расширенными полномочиями используются не только сотрудниками. Многие средства автоматизации (приложения, скрипты и др.) применяют служебные записи для реализации своих функций. Чтобы избежать хранения паролей в скриптах и конфигурационных файлах, Indeed PAM предлагает программный интерфейс (API) для получения актуальных служебных учетных данных. Все операции получения паролей будут зафиксированы в журнале PAM, а пароли изменены на новое случайное значение через заданный интервал времени.

Сокращение количества привилегированных учетных записей

Механизм Account Discovery оперативно обнаруживает учетные записи, про которые могли забыть администраторы и сотрудники ИБ (например, временные учетные записи, которые вовремя не

[2] Функция Application to Application Password Management будет реализована в 2021 году.

удалили и не заблокировали). Такая регулярная “инвентаризация” позволяет содержать парк привилегированных учетных записей в актуальном состоянии, не делая его избыточным. В свою очередь это уменьшает площадь потенциальной атаки злоумышленников и повышает информационную защищенность компании.

Используя PAM, компании могут отказаться от создания персональных учетных записей для администраторов, еще больше сократив число привилегированных УЗ. Indeed PAM фиксирует все события доступа на контролируемые ресурсы, в которых указываются:

- сотрудник, получивший доступ
- ресурс, к которому был осуществлен доступ
- учетная запись, от имени которой был произведен доступ
- дата и время доступа
- продолжительность сессии
- используемый протокол доступа.

Таким образом, даже при использовании обезличенных учетных записей для доступа к ресурсам (administrator, root и т.п.), в PAM останется информация о том, кто именно из сотрудников выполнял работы.

Мультифакторная аутентификация

Когда сотрудники получают привилегированный доступ, важно применять надежные способы аутентификации, чтобы гарантировать, что доступ имеют только легитимные пользователи. Indeed PAM “из коробки” поддерживает двухфакторную аутентификацию пользователей в режиме пароль + OTP (One-Time Password). Одноразовый пароль генерируется пользователем в приложении на смартфоне.

Компании, использующие штатные возможности ОС Windows для аутентификации пользователей с помощью смарт-карт и цифровых сертификатов, смогут применять данной подход и для аутентификации в Indeed PAM.

Расследование инцидентов

При осуществлении привилегированного доступа всегда есть риск нарушить работу информационных систем или получить нежелаемое поведение. Также при выполнении работ подрядчиками не всегда есть уверенность в том, что работы выполнены корректно и в полном объеме. В таких ситуациях важно иметь возможность выяснить, какие именно изменения вносились в работу систем и кто производил работы.

Indeed PAM позволяет выполнять фиксацию действий пользователей в следующих форматах:

- Видеозапись — запись всего экрана монитора. Система позволяет настроить параметры видеозаписи, такие как: качество изображения, разрешение и частота кадров.
- Скриншоты — периодическое снятие снимков экрана. Данная функция может быть полезна для экономии дискового пространства и записи некритичных сессий.
- Текстовая запись — текстовый лог сессии. Для SSH сессий записывается весь пользовательский ввод/вывод, для RDP сессий фиксируются запускаемые процессы, заголовки активных окон и пользовательский ввод.

Администраторы PAM имеют возможность просматривать сессии как в режиме реального времени, так и уже после их завершения. В ходе просмотра активной сессии администратор может ее

разорвать, если обнаружит подозрительное поведение.

Материалы сессии (видео, скриншоты, текстовый лог) могут быть выгружены для просмотра и анализа в сторонних инструментах.

Indeed Privileged Access Manager

Состав Indeed Privileged Access Manager

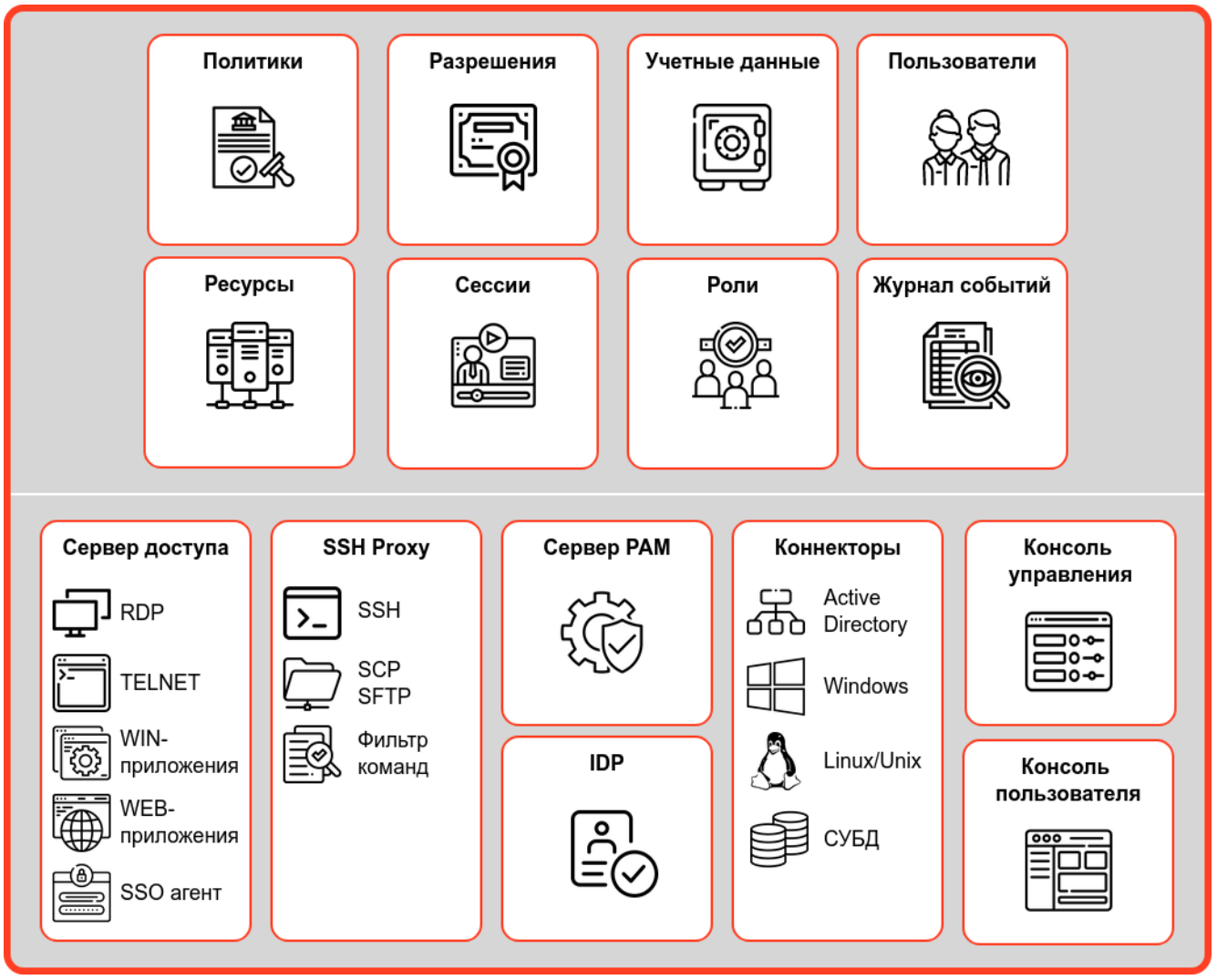


Рисунок 2. Структура Indeed Privileged Access Manager

Indeed PAM состоит из следующих логических и функциональных модулей.

Политики и разрешения

Политики и разрешения определяют параметры привилегированного доступа:

- кому предоставлен доступ
- к каким учетным записям предоставлен доступ
- к каким ресурсам (серверам и оборудованию) предоставлен доступ
- на какое время (постоянно/временно, в рабочие часы или в любое время)
- какую запись сессий нужно производить (видео и текстовую запись, только текстовую, скриншоты и т.п.)
- какие локальные ресурсы (диски, смарт-карты) будут доступны пользователю в удаленной

сессии
- разрешено ли пользователю просматривать пароль привилегированной учетной записи

Централизованные политики сокращают затраты на администрирование системы и делают параметры и права доступа прозрачными для специалистов информационной безопасности и аудиторов. Подробнее политики и разрешения рассматриваются в разделе “Централизованное управление доступом”.

Учетные данные

Учетные данные, необходимые для доступа (логины, пароли, SSH-ключи), хранятся в хранилище, к которому имеет доступ только сервер Indeed PAM. Хранение и передача данных к/от сервера производятся в зашифрованном виде с применением стойких алгоритмов шифрования. Доступ к хранилищу ограничен и возможен только для сервера PAM, для реализации этого подхода применяется специальная процедура по “запечатыванию” сервера - hardening сервера базы данных.

Пользователи

Пользователи PAM — сотрудники, которые получают привилегированный доступ через систему PAM. В качестве каталога пользователей Indeed PAM использует службу Active Directory. Пользовательские учетные записи применяются для доступа к консоли пользователя, серверу доступа, SSH Proxy и консоли управления.

Ресурсы

Ресурс в Indeed PAM — это объект, к которому предоставляется доступ. В большинстве случаев это windows- и linux-сервера. Кроме этого, ресурсом может быть отдельное приложение, например, для управления СУБД или web-конфигуратор маршрутизатора.

Сессии

Все сеансы привилегированного доступа записываются и сохраняются в архиве Indeed PAM. В архиве сессий записи хранятся в зашифрованном виде, получить к ним доступ возможно только обладая соответствующими полномочиями в рамках системы PAM. Записи ведутся в следующих форматах:

- Текстовая запись ведется всегда и фиксирует такие данные:
    - полный ввод и вывод консоли в SSH подключениях;
    - все запускаемые процессы, открываемые окна и клавиатурный ввод для RDP подключений.
- Видеозапись производится как для RDP, так и для SSH подключений. Видеозапись не обязательна, ее включение выполняется администратором PAM с помощью механизма политик. Качество видео настраивается и может быть разным для различных учетных записей. Например, сеансы администраторов домена могут записываться с максимальным качеством, а сеансы операторов — со сжатием.
- Снятие снимков экрана также производится как для RDP, так и для SSH подключений. Сохранение снимков экрана не обязательно, его включение выполняется администратором PAM с помощью механизма политик. Частота снятия и качество снимков экрана задаются в политиках.

Просмотр активных сессий доступен в режиме реального времени с возможностью разрыва сессии администратором PAM.

Роли

Роли определяют полномочия при работе в консоли управления Indeed PAM. По умолчанию в системе имеется три роли:

- Администратор — имеет полный доступ ко всем функциям и настройкам PAM.
- Оператор — имеет полномочия на выдачу и отзыв разрешений.
- Инспектор — имеет доступ на чтение.

Набор привилегий для каждой роли может быть изменен и адаптирован под нужды организации. Кроме этого, можно создавать собственные роли для более тонкого разграничения полномочий.

Журнал событий

Журнал событий хранится на выделенном сервере Indeed PAM. Такие события включают в себя всю активность администраторов и пользователей PAM. Журнал фиксирует, кто и какие параметры системы изменял и кто под какими учетными данными выполнял подключение к целевым ресурсам.

Для удобства интеграции в SEIM и своевременного реагирования на инциденты, события могут доставляться по протоколу syslog на сторонний журнальный сервер.

Сервер доступа

Сервер доступа реализует централизованную модель получения привилегированного доступа. Сначала сотрудник выполняет подключение к серверу доступа, на котором проверяются его права и выполняется двухфакторная аутентификация, после чего ему открывается сессия на целевом ресурсе.

Сервер доступа работает на базе сервера удаленных рабочих столов Microsoft RDS (Remote Desktop Services), на котором установлены компоненты Indeed PAM. Когда пользователь подключается к серверу доступа, в качестве оболочки рабочего стола запускается специализированное приложение Indeed PAM, которое выполняет следующие функции:

- проверяет права доступа пользователя — разрешено ли ему получать доступ под запрашиваемой учетной записью на запрашиваемый целевой ресурс;
- производит аутентификацию пользователя — перед открытием сессии пользователь обязан предоставить второй фактор аутентификации;
- ведет видеозапись сессии и снятие снимков экрана.

Для открытия сессий в целевые системы и приложения на сервере доступа применяются следующее клиентское ПО:

- RDP-клиент Microsoft (mstsc) для доступа на Windows сервера;
- Браузер для доступа в web-приложения;
- Клиент PuTTY для доступа по протоколам SSH и Telnet;
- Специализированное клиентское ПО для доступа в различные информационные системы с использованием проприетарных протоколов (“толстый” клиент).

SSH Proxy

SSH Proxy является альтернативным вариантом получения доступа через Indeed PAM в Linux/Unix системы. Данный метод обладает следующими преимуществами:

- не требуется использование Microsoft RDS;
- возможно использование любого SSH-клиента;

- SSH-клиент работает локально на рабочей станции сотрудника.

SSH Proxy выполняет аналогичные функции, что и сервер доступа:

- проверяет права доступа пользователя;
- производит аутентификацию пользователя;
- ведет текстовую запись сессии (фиксируется полный ввод/вывод ssh).

При использовании SSH Proxy пользователь инициирует подключение со своего рабочего места с помощью привычного для него SSH-клиента. В качестве сервера подключения сотрудник указывает адрес SSH Proxy. При подключении к прокси у пользователя также запрашивается второй фактор аутентификации, после чего открывается сессия на целевой ресурс.

Фильтр команд

Для SSH сессий администратор PAM имеет возможность определить команды, разрешенные или запрещенные для выполнения на определенных целевых ресурсах (список ресурсов определяется областью действия политики). Фильтр команд можно настроить для работы в одном из двух режимов:

- Разрешено все, что не запрещено. В этом случае администратор определяет те команды, которые должны быть запрещены для запуска.
- Запрещено все, что не разрешено. Более строгий фильтр, в котором администратор явно указывает те команды, которые разрешены для запуска, все остальные команды блокируются.

Для описания команд используется механизм регулярных выражений. На ввод запрещенной команды могут быть заданы следующие типы реакций:

- прервать сессию
- прервать выполнение команды.

SFTP и SCP[3]

Помимо доступа по SSH протоколу, SSH Proxy позволяет подключаться к целевым ресурсам по протоколам SFTP и SCP. Подключение в этом случае выполняется аналогично SSH: в качестве сервера подключения сотрудник указывает адрес SSH Proxy. При подключении к прокси у пользователя также запрашивается второй фактор аутентификации, после чего открывается сессия на целевой ресурс.

При использовании протоколов SFTP и SCP SSH Proxy создает текстовый лог сессии, в котором фиксируются файловые операции, выполняемые пользователем.

Сервер PAM

Сервер PAM является центральным модулем системы Indeed PAM и обеспечивает обмен данными и функционирование остальных модулей. Основными задачами, которые решает сервер, являются:

- Обеспечение централизованного управления всеми данными системы (пользователи, ресурсы, учетные данные, разрешения, политики и пр.).
- Шифрование критичных данных в базе данных PAM (привилегированные учетные данные и пр.).
- Выполнение задач по расписанию (поиск учетных записей, ротация паролей и пр.).
- Предоставление API для интеграции со сторонними системами.

[3] Функции работы с протоколами SFTP и SCP будут реализованы в 2021 году.

Identity Provider (IDP)

Модуль Identity Provider (IDP) обеспечивает двухфакторную аутентификацию пользователей при доступе ко всем компонентам системы. Первым фактором аутентификации является доменный пароль пользователя, вторым — одноразовый пароль (OTP), генерируемый в приложении на смартфоне.

При первом входе в консоль управления или консоль пользователя сотруднику предлагается зарегистрировать приложение для генерации OTP. После успешной регистрации сотруднику предоставляется доступ в систему.

Помимо пользователей, IDP отвечает за аутентификацию приложений, использующих API сервера PAM.

Коннекторы

Коннекторы обеспечивают выполнение ряда функций по управлению привилегированными учетными записями:

- Периодический поиск новых привилегированных учетных записей на целевых ресурсах. Данная мера позволяет защититься от недобросовестного администратора, который создал себе учетную запись для работы в обход системы PAM.
- Периодическая проверка паролей и SSH-ключей привилегированных учетных записей. Данная функция позволяет убедиться, что в хранилище PAM содержатся актуальные учетные данные и недобросовестный администратор не выполнил сброс пароля учетной записи для использования ее в обход PAM.
- Периодическая смена паролей и SSH-ключей. Indeed PAM генерирует случайные сложные пароли и SSH-ключи для контролируемых привилегированных учетных данных, защищая их от несанкционированного доступа.
- Сброс пароля учетной записи после показа его пользователю. Администратор PAM может разрешить сотрудникам просматривать пароль привилегированной учетной записи в тех случаях, когда необходимо явное использование пароля. После того, как сотрудник получит пароль, через заданный промежуток времени Indeed PAM сбросит пароль в новое случайное значение.

Indeed PAM включает коннекторы для следующих целевых систем:

- коннектор к Active Directory;
- коннектор к Windows и Windows Server;
- SSH-коннектор для подключения к Linux/Unix системам на базе различных дистрибутивов;
- коннектор к СУБД (MS SQL, Oracle, PostgreSQL и др.).

Консоль управления

Консоль управления предоставляет интерфейс для настройки и аудита работы системы и выполнена в виде web-приложения. Используя консоль, администратор предоставляет пользователям доступ к учетным данным и ресурсам, настраивает политики доступа и просматривает журналы событий и записи привилегированных сессий. Также консоль позволяет администраторам PAM просматривать активные привилегированные сессии в реальном времени и при необходимости прекращать сеанс работы сотрудника. Доступ в консоль управления выполняется с помощью двухфакторной

аутентификации.

Консоль пользователя

Консоль пользователя выполнена в виде web-приложения. В консоли доступны все выданные сотруднику разрешения, имеется возможность поиска по адресу или имени ресурса, протоколу подключения или имени учетной записи. Найдя нужный ресурс для подключения, пользователь скачивает RDP-файл с необходимыми параметрами. Этот файл можно сохранить и переиспользовать снова, нет необходимости скачивать каждый раз новый файл. Для SSH-ресурсов есть возможность скопировать в буфер обмена строку подключения для использования в произвольном SSH-клиенте.

В консоли пользователь также может просмотреть привилегированные учетные данные, на которые ему были выданы разрешения. Доступ в консоль выполняется с помощью двухфакторной аутентификации.

Основные характеристики Indeed PAM

Протоколы доступа	RDP SSH HTTP(s) Telnet SFTP SCP Любой протокол через публикацию клиента
Поддерживаемые типы учетных данных	Логин + пароль SSH-ключ
Поиск привилегированных учетных записей и управление паролем	Windows Linux Active Directory СУБД (MS SQL, PostgreSQL, My SQL, Oracle и др.)
Поддерживаемые каталоги пользователей	Active Directory
Технологии двухфакторной аутентификации	Пароль + TOTP (программный генератор)
Поддерживаемые типы записи сессий	Текстовый лог Видеозапись Снимки экрана
Технологии удаленного доступа	Microsoft RDS SSH Proxy

О компании Индид

Компания «Индид» (indeed-id.ru) – российский разработчик программных комплексов в области информационной безопасности. За 10 лет компания самостоятельно разработала 4 программных комплекса для повышения уровня информационной безопасности и корпоративного использования в компаниях разных отраслей экономики. Результат внедрения продуктов компании не ограничивается решением отдельных задач информационной безопасности. Программные комплексы обеспечивают выполнение требований регуляторов и реализацию соответствия нормативным документам (ГОСТ,

ФСТЭК и др.), а также включены в Реестр отечественного ПО, что имеет важное значение для реализации требований программы импортозамещения в РФ. ПО внедрено на территории РФ и стран СНГ во многих компаниях разных отраслей экономики, а также в странах Европы и Азии.