INDEED ID

White Paper

Indeed Privileged Access Manager

Управление доступом к привилегированным учетным записям


www.indeed-id.ru

Содержание

Привилегированный доступ - угроза безопасности

Постоянное наращивание и усложнение IT-инфраструктуры компаний делает управление привилегированными учетными записями 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, 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

Бизнес-пользователи хоть и не обладают административным доступом, но 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 коммерческой тайне.

Подрядчики и партнеры

Сотрудники подрядчиков, как правило, выполняют сопровождение специализированных программных и аппаратных комплексов. Это могут быть, например, 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 различной 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 по управлению ими.

Indeed Privileged Access Manager

Продукт Indeed Privileged Access Manager (Indeed PAM) “с нуля” разрабатывается как система управления доступом с использованием привилегированных учетных записей. В основе продукта лежит многолетний опыт компании Индид по созданию продуктов в области информационной безопасности. Основные решаемые задачи этого продукта следующие:

- Регистрация попыток использования привилегированных учетных записей в журнале доступа, с указанием какой сотрудник, когда и к какой учетной записи получал доступ
- Ведение видео и текстовой записи привилегированных сессий с возможностью просмотра архива сессий
- Обеспечение мультифакторной аутентификации сотрудников при доступе к привилегированным учетным записям
- Хранение паролей привилегированных учетных записей в секрете от сотрудников, регулярная смена паролей на случайные значения.

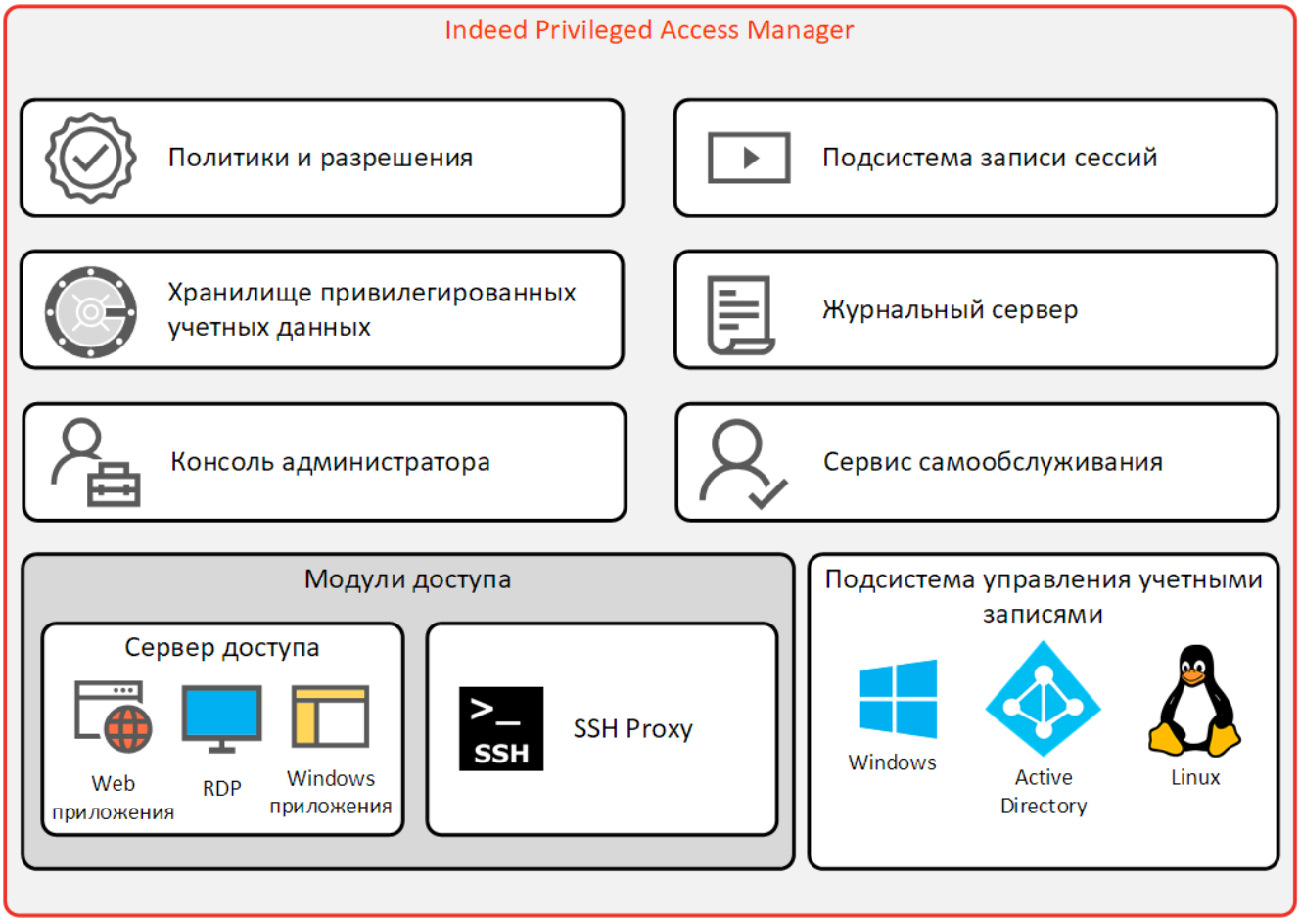

Рисунок 1. Структура Indeed Privileged Access Manager

Indeed PAM состоит из следующих функциональных и логических 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.

Хранилище привилегированных учетных данных

Учетные данные, необходимые для доступа (логины, пароли, SSH-ключ) хранятся в хранилище, к которому имеет доступ только сервер Indeed PAM. Хранение и передача данных к/от сервера производится 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.

Подсистема записи сессий

Все сеансы привилегированного доступа записываются в обязательном порядке и сохраняются в архиве Indeed PAM. В архиве 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 задается в политиках.

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

Журнальный сервер

Журнальный сервер является выделенным сервисом по сбору событий 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.

Консоль администратора

Консоль администратора предоставляет интерфейс для настройки, управления и аудита работы системы и выполнена в виде web-приложения. Используя консоль, администратор предоставляет пользователям доступ к учетным данным, 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 администратора выполняется с помощью двухфакторной аутентификации.

Сервисы самообслуживания

Для получения привилегированного доступа сотрудники используют два инструмента:

- Консоль пользователя, выполненная в виде web-приложения. В консоли пользователя сотрудники просматривают доступные им учетные записи и ресурсы, а также запускают привилегированные сессии.
- Приложение на сервере доступе. С использованием этого приложения сотрудники получают доступ минуя консоль пользователя. В этом случае сотрудник подключается напрямую к серверу доступа, где ему предлагается выбрать разрешенное подключение.

В обоих случаях доступ сотрудников защищен двухфакторной аутентификацией с помощью OTP (One-Time Password).

Модули доступа

Модули доступа предоставляют механизмы открытия и записи привилегированных сессий.

Сервер доступа

Сервер доступа реализует централизованную модель получения привилегированного доступа. Сотрудник сначала выполняет подключение к серверу доступа, на котором проверяются его права и выполняется аутентификация по второму фактору, после чего, сотруднику открывается сессия на целевом ресурсе.

Сервер доступа работает на базе сервера удаленных рабочих столов Microsoft RDS (Remote Desktop Services), на котором установлено приложение Indeed PAM. Данное приложение 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;
- SSH-клиент PuTTY для доступа на Linux/Unix системы;
- 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 те же функции, что и сервер доступа:

- проверяет права доступа пользователя;
- производит аутентификацию пользователя;
- ведет видеозапись сессии и снятие снимков экрана.

При использование 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.

Подсистема управления учетными записями

При использовании систем класса PAM офицерам информационной безопасности важно понимать, что в инфраструктуре компании нет неучтенных привилегированных записей и доступ к ним контролируется и протоколируется. В рамках Indeed PAM эту задачу решает подсистема управления учетными записями. Подсистема выполняет следующие функции:

- 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 сотрудники 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.

Для выполнения указанных функций в состав подсистемы управления учетными записями входят модули подключения (коннекторы) для целевых систем:

- коннектор к Active Directory;
- коннектор к Windows и Windows Server;
- SSH-коннектор для подключения к Linux/Unix системам на базе различных дистрибутивов.

Основные характеристики Indeed PAM

Протоколы доступа	RDP SSH HTTP(s)
Поддерживаемые типы учетных данных	Имя пользователя + пароль SSH-ключи
Поиск привилегированных учетных записей и управление паролем	Windows Linux Active Directory
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 является российским разработчиком программного обеспечения под маркой Indeed Identity. Разрабатываемые нами программные комплексы предназначены для управления доступом сотрудников к информационным ресурсам компании, контроля доступа привилегированных пользователей, а также управлению инфраструктурой открытых ключей и жизненным циклом смарт-карт и USB-ключей. Продукты компании используются в ведущих компаниях России и СНГ в различных отраслях: финансовой, производстве, нефтегазовой, ритейле и телекоммуникационной. Офисы компании расположены в Санкт-Петербурге, Москве, Великом Новгороде и Вильнюсе.

Чтобы получить дополнительную информации о продуктах компании, задать интересующие вопросы и получить консультацию посетите сайт www.indeed-id.ru.