Безопасность

Резервные учётные записи

Решения класса Privileged Access Management - это ряд технических, программных и организационных мер, которые защищают привилегированные учётные записи от несанкционированного использования.

Один из механизмов защиты Indeed PAM это изоляция паролей учётных записей доступа в БД Indeed PAM Core, их шифрование и изменение по расписанию или требованию на случайные или пользовательские значения.

БД и сервис Indeed PAM Core критические элементы, повреждение БД или отказ сервиса приведет к потере доступа к ресурсам, так как пароли учётных записей доступа неизвестны конечным пользователям и администраторам.

Рекомендуется для каждого ресурса выделить резервную учётную запись с правами локального администратора (ОС Windows) или с правами на выполнение команды SUDO (ОС *nix). Мера позволит восстановить доступ к ресурсам в случае выхода из строя БД Indeed PAM Core или самого сервиса. Для этих целей назначьте уполномоченного сотрудника, который будет отвечать за сохранность резервных учётных записей и паролей.

Доступ к Indeed PAM

Для обеспечения безопасности компонентов Indeed PAM рекомендуется выполнять установку в соответствии с размещением 2, в этом случае на одном сервере будут установлены компоненты:

- Indeed PAM Core
- Indeed PAM IdP
- Indeed PAM Management Console
- Indeed PAM User Console
- Indeed Log Server
- Indeed Pam EventLog
- Microsoft SQL Server или PostgreSQL, PostgreSQL Pro

Расположение ключевых компонентов Indeed PAM и хранилища данных на одном сервере позволяет снизить риски неправомерного доступа к ним. Для корректной работы потребуется открыть следующие порты:

Протокол	Порт	Описание
Входящие и исходящие		

TCP/UDP	53	DNS
TCP/UDP	389/636	LDAP/SSL
TCP	3268/3269	Microsoft Global Catalog/SSL
TCP/UDP	88	Kerberos
TCP/UDP	464	Kerberos
Входящие		
TCP	80/443	Indeed PAM Core/SSL Indeed PAM Management Console/SSL Indeed PAM User Console/SSL Indeed PAM IdP/SSL Indeed Log Server/SSL