Диаграмма развертывания Sherpa Process Discovery

СИСТЕМНЫЕ ТРЕБОВАНИЯ

Sherpa Process Discovery Server:

8 vCore 32 Гб КАМ

SSD 300 Гб свободного места

Linux с поддержкой Docker 18+ (совместимость проверена с RedHat, Debian, Ubuntu, CentOS)

Ресурсы указаны из расчёта 10 одновременно подключенных и

активных Process Discovery Agent. Объем жесткого диска указан из расчёта сбора и хранения сырых и обработанных данных для 10 пользователей в течение 14 дней (стандартные рамки эксперимента).

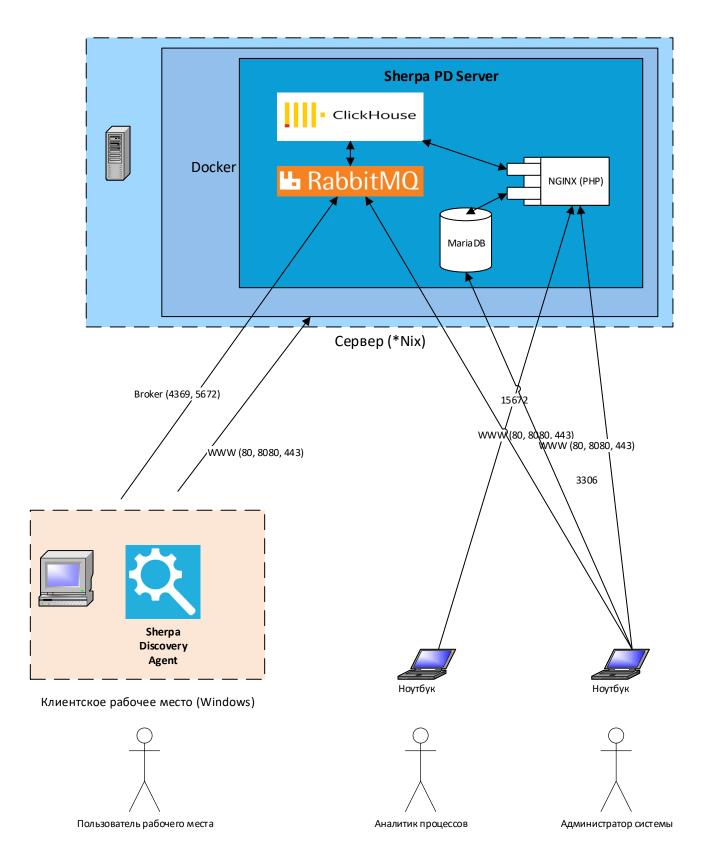
Sherpa Process Discovery Agent:

2 vCore 2 Гб RAM SSD / HDD 10 Гб свободного места Windows 7 – Windows 10 или Windows Server 2012 – 2022

.NET Framework 4.8+

При работе пользователей через RDS или Citrix данные требования применяются к каждой пользовательской учетной записи на терминальном сервере,

при этом Process Discovery Agent должен быть установлен в учётной записи удаленного пользователя. При использовании мигрирующих профилей пользователей Process Discovery Agent должен быть установлен внутри папок мигрирующего профиля, а групповыми политиками должен быть предусмотрен автозапуск исполняемого файла Process Discovery Agent при логине пользователя.



ОПИСАНИЕ:

Схема описывает верхнеуровневую реализацию функционала, который использует возможности искусственного интеллекта для выявления бизнес-процессов, наиболее подходящих по заданным критериям для последующей роботизации. Сбор всей необходимой информации по работе пользователей, ее обработка и анализ производятся в фоновом режиме, без отвлечения персонала от основной деятельности. Анализируются действия отдельных пользователей на детальном уровне, по конкретным шагам (кликам, переходам и др).

Тип собираемых данных - снимок экрана/метаданные для каждого действия пользовател (скриншот для каждого действия пользователя). Подробные метаданные, соответствующие каждому скриншоту, включают в себя:

- Имя приложения
- Имя пользователя
- Тип события (например, колесо мыши, щелчок левой кнопкой мыши)
- Положение мыши (например, х: 933, у:637)
- Отметка времени

Обеспечивается контроль над тем, какие бизнес-приложения следует отслеживать, используя списки, определяющие приложения для мониторинга. Любые приложения, не одобренные для обнаружения по соображениям безопасности или другим причинам, могут быть исключены из списка приложений для включения или добавлены в список приложений для исключения.

По запросу может быть применена маскировка собираемой текстовой информации по заданному списку регулярных выражений.

Диаграмма развертывания:

Все компоненты Sherpa Process Discovery устанавливается локально в сети Банка, без связи с внешними серверами или службами SaaS.

Все данные сохраняются во внутреннем хранилище сервера обнаружения и не передаются и не экспортируются за пределы сервера, автоматически или вручную. По умолчанию развертывание Process Discovery Server осуществляется с помощью Docker-контейнера. Развертывание Sherpa Discovery Agents на рабочих местах пользователей осуществляется вручную с помощью exe-инсталлятора либо автоматически с помощью msi-инсталлятора, с помощью мexaнизмa GPO.

Последовательность шагов процесса:

(1) Sherpa Discovery Agents установленные на рабочих столах сотрудников, собирают поведенческие данные о пользователе, процессах и приложениях, и отправляют на Sherpa Discovery Server для анализа.

(2) Sherpa Process Discovery Server использует данные, собранные Sherpa Discovery Agents для выявления регулярно повторяющихся сходных последовательностей действий пользователя, и представляет результат работы через веб-интерфейс, доступный для просмотра через веб-браузер на рабочем месте бизнес-аналитика. Sherpa Discovery Server включает в себя реляционную базу данных (по умолчанию - Maria DB), колоночную базу данных (по умолчанию - ClickHouse) и брокер сообщений (по умолчанию - RabbitMQ), в которых хранятся и обрабатываются все данные, собранные Discovery Agents. Собранные данные передаются почти сразу в базы данных приложений и остаются на клиентской машине в течение короткого времени.

(3) Бизнес аналитик (сотрудник Отдела технологических решений) с помощью веб-интерфейса Sherpa Discovery Server получает доступ к собранным данным в виде таблиц, списков, диаграмм, а также получает возможность выгрузки отчётов по выявленным бизнес-процессам.

Конфигурация сети:

Конфигурация портов и сетевые протоколы Sherpa Process Discovery могут быть настроены для поддержки всех общих требований брандмауэра. Конфигурация порта по умолчанию выглядит следующим образом:

- *Discovery Agents, исходящие на Discovery Server: 5672 (или 5671 при использовании TLS)
- *Discovery Agents, входящие с Discovery Server: динамические
- *Связь с базой данных: 3306 и 1433-настраивается
- *Доступ пользователя к веб-интерфейсу Sherpa Process Discovery Server: 80 или 443

Для взаимодействия с веб сервером используется https, опционально возможно http.

Sherpa Process Discovery поддерживает защищенную связь (с использованием протокола TLS 1.2) между Discovery Agents и Discovery Server. При установке с помощью TLS клиент должен предоставить необходимые сертификаты, разместив их по пути /opt/app/config/certs/, переименовав их в orchestrator.crt и orchestrator.key.

Механизмы аутентификации

Аутентификация Discovery Agents в Discovery Server осуществляется с помощью Bearer Token, передаваемого в заголовке запросов. Bearer Token сопоставляется с уникальным GUID каждого экземпляра Discovery Agent. Для аутентификации пользователей веб-интерфейса Discovery Server применяется авторизация с помощью пары логин-пароль. При повторном входе используется сессионная кука, имеющая ограниченный срок жизни.

Логирование

Для логирования используется компонент Monolog. События аудита и системные ошибки сохраняются в выделенную таблицу базы данных.