скаут

Система автоматизации регламентных проверок

Требования к развертыванию и окружению

Версия СКАУТ 1.2.1 от 20.10.2020

Отдел продаж

Тел.: +7 (495) 787 43 43
E-mail: sales@interfax.ru

Оглавление

Введение

Данный документ содержит информацию о минимальных требованиях к развертыванию и окружению системы автоматизации регламентных проверок контрагентов «Интерфакс-СКАУТ».

Приведенные требования соответствуют коробочной версии системы, поставляемой клиентам в порядке «как есть». В случае, если предполагаются какие-либо доработки «Интерфакс-СКАУТ» (например, доработка или расширение перечня функций и бизнес-процессов) реализуемых «Интерфакс-СКАУТ», приведенные требования могут измениться.

1 Требования к развертыванию

1.1 Административные работы (установка системы и ее обновлений)

Для целей работ по установке обновлений в автоматическом режиме и её обслуживанию в ручном режиме должна быть доступна учетная запись ОС используемых хостов системы SCOUT с правами локального администратора (далее "УЗ системного администратора"). Если используется учетная запись Active Directory, то ее использование где-либо, кроме как на выделенных хостах может быть заблокировано.

Также для целей работ по обслуживанию и изменению необходимых настроек MS SQL Server должна быть доступна учетная запись, входящая в серверную роль sysadmin. Это может быть как УЗ системного администратора, так и отдельная учетная запись встроенной подсистемы аутентификации MS SQL Server (далее по тексту она также называется "УЗ системного администратора").

1.2 Работа системы

Для запуска системы SCOUT в качестве службы Windows должна быть предоставлена учетная запись с правами на запуск в качестве службы (далее "УЗ системы"). В случае использования для входа в системы пользователей из Active Directory данная учетная запись должна иметь права на обращение к контроллеру домена Active Directory с целью проверки наличия пользователя и корректности его пароля, а также определения групп пользователя. Если используется учетная запись Active Directory, то ее использование где-либо, кроме как на выделенных хостах может быть заблокировано.

УЗ системы должна иметь право на вход MS SQL Server. Доступ от ее имени (помимо доступа в MS SQL Server) требуется только со стороны сервера приложения на сетевые ресурсы сервера СУБД по протоколу SMB (используется для работы модуля MS SQL Server FILESTREAM)

1.3 HTTPS/SSL сертификат для доступа к веб-сайту системы

Для корректной работы системы обязательно требуется правильно сконфигурированный веб-сервер, который должен иметь возможность работать по протоколу http2 с корректным SSL-сертификатом. Сертификат должен быть выпущен на доменное имя

системы, с которого предполагается давать доступ конечным пользователям системы. Например, если пользователи должны попадать в систему по адресу https://scout.company.ru, то для имени scout.company.ru должен быть выдан SSL-сертификат, который на рабочих станциях пользователей будет распознаваться браузером, как полностью валидный.

Важные условия:

1. Issued to: имя сервера, например *scout.company.ru*, или **.company.ru*.
2. OID: Server Authentication (1.3.6.1.5.5.7.3.1).
3. Формат сертификата: PEM (ASCII файлы, закодированные по схеме Base64, начинающиеся с -----BEGIN CERTIFICATE----- и -----BEGIN PRIVATE KEY-----).
4. Наличие приватного ключа обязательно.

2 Требования к окружению

2.1 Требования к программно-техническому обеспечению продуктивного стенда

Назначение	Требования к программному обеспечению	Требования к аппаратному обеспечению
Сервер приложений (back-end)	1. Microsoft Windows Server 2019 Standard EN x64 (min build 1809) с установленными последними обновлениями и паролем администратора (для установки обновлений силами АО "Интерфакс"). 2. .NET Framework 4.6.1. 3. .NET Core Runtime 2.2. 4. Установленный модуль SQL Server в PowerShell. 5. Microsoft® Command Line Utilities for SQL Server. 6. Microsoft® ODBC Driver for SQL Server.	1. CPU ≥ 4 ядер, каждое ≥ 2 ГГц. 2. RAM ≥ 16 ГБ. 3. Disk: 3.1. OS Disk ≥ 10 ГБ. 3.2. DATA Disc не требуется. 4. DR (если требуется) — резервное копирование каталога компонентов приложения. 5. Сетевое подключение ≥ 1 ГБ/с.
Сервер СУБД	1. Microsoft SQL Server 2019 Standard EN с установленными последними обновлениями и известным доступом к стандартной учетной записи администратора SA (для установки обновлений силами АО "Интерфакс"). 1.1. Каталог данных должен быть расположен в корне SSD-диска. Например, X :\SQLServerData. 1.2. Каталог бэкапов должен быть расположен в корне HDD-диска. Например X:\SQLServerBackups.	1. CPU ≥ 8 ядер, каждое ≥ 2 ГГц. 2. RAM ≥ 24 ГБ. 3. Disk: 3.1. OS Disk не требуется. 3.2. DATA Disc: 3.2.1. HDD ≥ 2 ТБ свободного места. 3.2.2. SSD ≥ 200 ГБ свободного места. 4. DR (если требуется) — резервное копирование БД / журнала транзакций БД. 5. Сетевое подключение ≥ 1 ГБ/с.

Назначение	Требования к программному обеспечению	Требования к аппаратному обеспечению
	2. Для развертывания и настройки Системы должен быть обеспечен внешний доступ по протоколу RDP. 3. Включенный FILESTREAM и уровень доступа FILESTREAM - полный 4. Включенный Full-Text Search.	
Интеграционный прокси-сервер (при размещении в DMZ компонент требуется для доступа к сервисам в сети Интернет)	1. Microsoft Windows Server 2019 Standard EN x64 (min build 1809) с установленными последними обновлениями и паролем администратора (для установки обновлений силами АО "Интерфакс"). 2. .NET Framework 4.6.1. 3. .NET Core Runtime 2.2. 4. Установленный модуль SQL Server в PowerShell. 5. Microsoft® Command Line Utilities for SQL Server. 6. Microsoft® ODBC Driver for SQL Server.	1. CPU ≥ 2 ядер, каждое ≥ 2 ГГц. 2. RAM ≥ 2 ГБ. 3. Disk: 3.1. OS Disk ≥ 1 ГБ. 3.2. DATA Disc не требуется. 4. DR не требуется. 5. Сетевое подключение ≥ 1 ГБ/с.
Сервер backup	1. Microsoft Windows Server 2019 Standard EN x64 (min build 1809) с установленными последними обновлениями и паролем администратора. 2. Microsoft SQL Server 2019 Standard EN с установленными последними обновлениями и известным доступом к стандартной учетной записи администратора SA (для установки обновлений силами АО "Интерфакс").	1. CPU ≥ 2-х ядер, ≥ 2 ГГц. 2. RAM ≥ 4 ГБ. 3. HDD ≥ 2 ТБ свободного места. 4. Сетевое подключение ≥ 1 ГБ/с.

Для развертывания требуется выполнить настройки сети:

1. Для сервера бэк-энда доступные порты извне на данный компьютер для доступа к системе (в том сегменте сети, где требуется пользоваться системой):
   1.1. 80/tcp. Используется внутри сети клиента для доступа к системе с рабочих станций пользователей по протоколу http. На порту расположен веб-сервер, на который будут обращаться браузеры конечных пользователей по установленному доменному имени системы.
   1.2. 443/tcp. Используется для доступа к системе по протоколу https.
2. Для сервера СУБД для доступа к БД (с хоста сервера приложений требуется доступ к файлам сервере СУБД по протоколу SMB 3.0):
   2.1. 1433/tcp.
   2.2. 445/tcp.
   2.3. 445/udp.
3. Для серверов бекэнда и СУБД:
   3.1. 3389/ tcp.

Входящих соединений от внешних сервисов не требуется. Схема взаимодействия серверов приведена на рисунке 1.

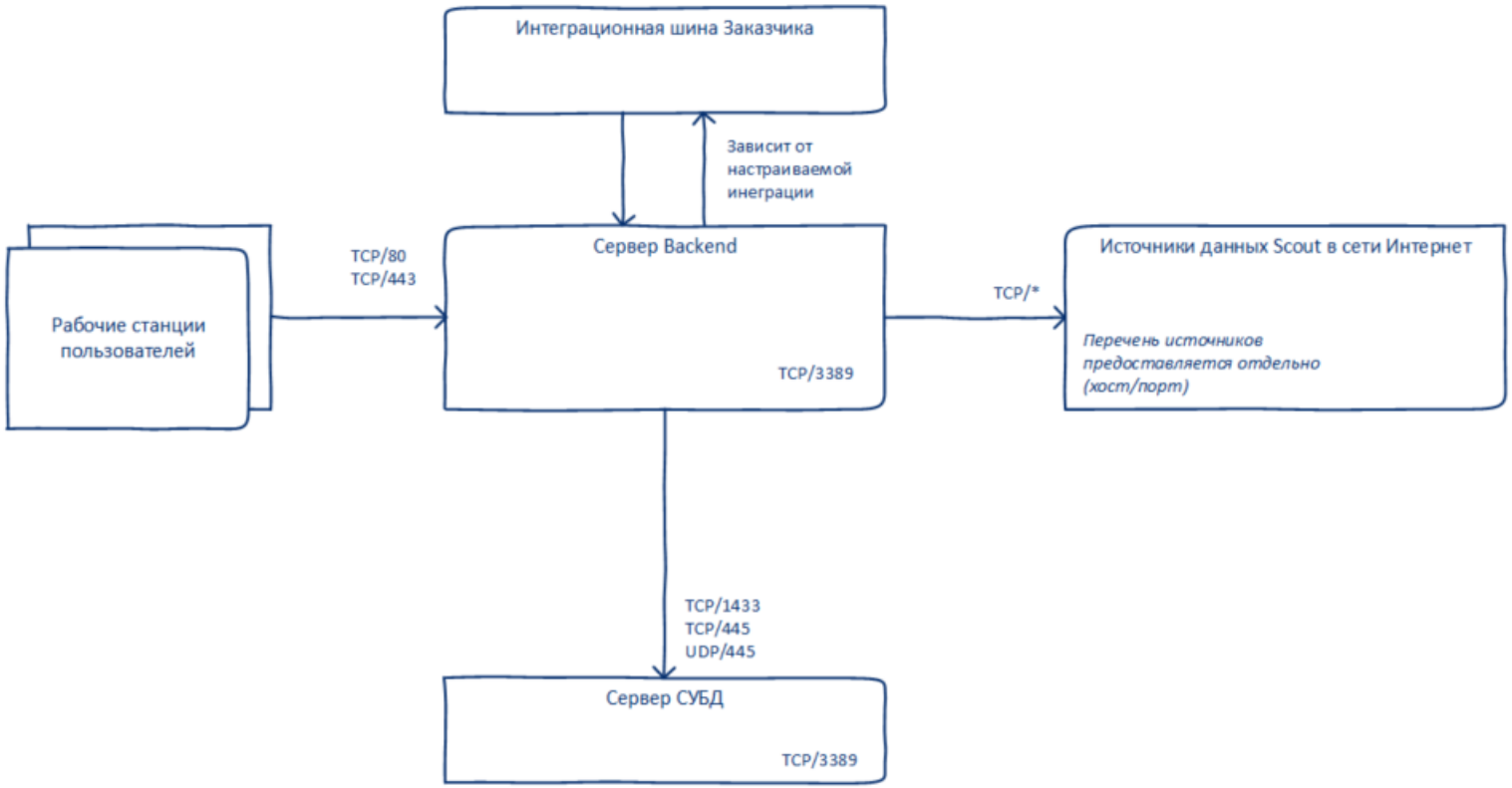

Рисунок 1 – Схема взаимодействия серверов

2.2 Требования к программно-техническому обеспечению тестового стенда

Назначение	Требования к программному обеспечению	Требования к аппаратному обеспечению
Сервер (back-end + СУБД)	1. Microsoft Windows Server 2019 Standard EN x64 с установленными последними обновлениями и паролем администратора (для установки обновлений силами АО "Интерфакс"). 2. Microsoft SQL Server 2019 Standard EN с установленными последними обновлениями и известным доступом к стандартной учетной записи администратора SA (для установки обновлений силами АО "Интерфакс"). 2.1. Каталог данных должен быть расположен в корне SSD-диска. Например, X :\SQLServerData. 2.2. Каталог бэкапов должен быть расположен в корне HDD-диска. Например X:\SQLServerBackups. 3. .NET Framework 4.6.1. 4. Для развертывания и настройки Системы должен быть обеспечен внешний доступ по протоколу RDP. При необходимости возможно указать перечень IP-адресов, с которых будет осуществляться доступ к тестовой машине 5. Доступный порт 80 извне на данный компьютер для доступа к системе (в том сегменте сети, где требуется пользоваться системой).	1. CPU ≥ 4-х ядер, каждое ≥ 2 ГГц. 2. RAM ≥ 4 ГБ. 3. Disk: 3.1. OS Disk ≥ 10 ГБ. 3.2. DATA Disc ≥ 100 ГБ свободного места. 4. DR не требуется.

Входящих соединений от внешних сервисов не требуется. Схема взаимодействия серверов приведена на рисунке 2.

Рисунок 2 – Схема взаимодействия серверов

2.3 Требования к программно-техническому обеспечению рабочих станций пользователей

Назначение	Требования к программному обеспечению	Требования к аппаратному обеспечению
Сервер (back-end + СУБД)	1. Любая из поддерживаемых производителем операционных систем: 1.1. Microsoft: Windows 10 и современнее. Допускается (но не рекомендуется) использование Windows 8.1. 1.2. Apple: OS X 10.11 (El Capitan) и современнее. 1.3. Linux: 64-битные версии Ubuntu 14.04+, Debian 8+, openSUSE 13.3+ или Fedora Linux 24+. 2. Любой из поддерживаемых производителем браузеров с установленными последними обновлениями: 2.1. Google Chrome, версия 75 и современнее. 2.2. Yandex Browser, версия 18 и современнее. 2.3. Safari, версия 12 и современнее. 2.4. Firefox, версия 67 и современнее. 2.5. Opera, версия 60 и современнее. 2.6. Microsoft Edge, версия 44 и современнее.	1. CPU ≥ 2-х ядер, ≥ 1,5 ГГц. 2. RAM ≥ 2 ГБ. 3. Видеокарта. 4. Монитор с разрешением не ниже 1280 x 768. 5. Клавиатура, мышь. 6. Сетевая карта Ethernet не менее 100 Мбит/с и/или Wi-Fi стандарта не ниже 802.11g.

2.4 Доступ и учетные данные

Необходимо обеспечение следующих условий:

1. Круглосуточный защищенный удаленный доступ (к внутреннему сегменту сети Заказчика, в котором находятся серверы) посредством VPN для специалистов «Интерфакс» (минимум 5 учетных записей) к информационной системе для целей установки системы, дистанционного мониторинга и оперативного решения проблем.

2. Для обеспечения полноценной диагностики системы со стороны «Интерфакс» – круглосуточный защищенный удаленный доступ (к внутреннему сегменту сети Заказчика, в котором находятся серверы) посредством VPN для автоматизированного сбора журналов, содержащих технические сведения о работе системы (ошибки, предупреждения, внутренние сообщения системы о важных этапах своего функционирования и т.п. (минимум 1 учетная запись).
3. Должна быть возможность подключаться к серверам посредством RDP.
4. На тестовом сервере и на продуктивном сервере приложений должен быть пользователь (учетная запись), от имени которого выполняется запуск компонентов систем. Данный пользователь должен обладать следующими правами/возможностями:
   4.1. вход в качестве службы;
   4.2. файловый доступ на чтение к каталогам расположения компонентов системы;
   4.3. файловый доступ за запись в каталоги расположения журналов (если настроено);
   4.4. иметь имя входа (логин) на SQL Server, где расположена БД системы. Также это имя входа должно быть привязано к пользователю БД системы с правами db_owner.
5. Учетная запись электронной почты, для отправки уведомлений из системы и реквизиты доступа к почтовому серверу.