Описание функциональных характеристик

Продукта Platform V SOWA

(Код продукта SWA)

Версия релиза № 2.6.0

Дата релиза 16.09.22

ОГЛАВЛЕНИЕ

Описание функциональных характеристик

Термины и обозначения

Термин	Полное обозначение	Определение
АВПО	Антивирусное Программное обеспечение	СПО, предназначенное для проверки объектов на факт наличия в них вирусов, троянов, закладок и другого вредоносного содержимого.
АС	Автоматизированная система	Комплекс сервисов и средств автоматизации бизнес-процессов.
Балансировка	-	Метод распределения заданий между несколькими сетевыми устройствами (серверами) с целью оптимизации использования ресурсов, сокращения времени обслуживания запросов, а также обеспечения отказоустойчивости.
Валидация	-	Проверка на соответствие какого-либо документа, сообщения с данными определенному заданному формату, а также проверка на синтаксическую корректность документа или файла.

ЖЦ	Жизненный Цикл программного обеспечения	Период времени, который начинается с момента принятия решения о необходимости создания программного продукта и заканчивается в момент его полного изъятия из эксплуатации.
ИШ	Интеграционный шлюз	Обеспечивает взаимодействие уровня система – система с произвольным контрагентом и должен поддерживать максимальное количество форматов внешнего взаимодействия наиболее безопасным способом.
ИР	Информационный ресурс	Единица учета сервисов в ITIL-процессах в Банке.
КТС	Комплекс Технических Средств	Аппаратные средства, такие как: сервера, маршрутизаторы, процессора, память, диски и др.
КЭ	Конструктивный элемент	Единица учета любых ресурсов в ITIL-процессах в Банке.
Маршрутизация	-	(от англ. Routing) процесс определения маршрута данных в сетях связи.

МО	Менеджер очередей	СПО, отвечающее за управление очередями сообщений и прием вывозов от прикладных программ.
ОС	Операционная система	Комплекс программ, обеспечивающий управление аппаратными средствами компьютера, организующий работу с файлами и выполнение прикладных программ, осуществляющий ввод и вывод данных. На сегодняшний день, операционная система — это первый и основной набор программ, загружающийся в компьютер.
ОЗУ	Оперативное запоминающее устройство	Компонент, который позволяет компьютеру кратковременно хранить данные и осуществлять быстрый доступ к ним.
ППО	Прикладное Программное Обеспечение	Профиль прикладного программного обеспечения (ППО), функциями которого являются обработка запросов от клиентов и передача их далее системам-получателям, а также направление полученных от систем сообщений в ответ.

Профиль	-	(от англ. Profile) это коллекция артефактов, необходимых для описания поведения и SLA сервисов пользователя, и предназначенная для их изоляции, группировки и дистрибуции.
Релиз	-	Версия ППО или СПО, которая может быть использована для решения любого рода задач в какой-либо среде.
Релиз Dev	-	Релиз, находящийся в разработке, проходящий наполнение доработками. По умолчанию не рекомендован для промышленного использования.
Релиз Hotfix	-	Поставка, содержащая срочные изменения или исправления к релизам, находящимся в промышленной эксплуатации.
Релиз Release Candidate	-	Кандидат в релизы с устоявшимся набором доработок, прошедший стадии Функционального и Нагрузочного тестирования.

СПО	Системное Программное Обеспечение	В контексте данной документации подразумевается ПО, осуществляющее служебную функцию, позволяющую запускать практические задачи.
Схема валидации	-	Документ, описывающий структуру других документов, таких как XML/JSON/YAML/GraphQL документы.
ТТ	Технические Требования	Перечень количественных и качественных требований, предъявляемых к КТС и необходимых для создания и/или работы АС.
УЗ	Учетная Запись	
УЦ	Удостоверяющий Центр	Организация или АС, занимающаяся выпуском и подписанием сертификатов или ключей.
Шлюз	Шлюз	АС или СПО для сопряжения компьютерных сетей и сервисов.
Шлюз безопасности	-	ШПУ, осуществляющий фильтрацию и валидацию передаваемого контента по определенным правилам.

Шлюз безопасности АС	-	Обеспечивает взаимодействие модулей одной системы Банка, размещенных во внешней и внутренней сети. Как правило, используется для организации клиентского доступа (сотрудник, клиент) к функциональности конкретной системы Банка.
Шлюз Открытого API	-	Обеспечивает взаимодействие уровня система – система с произвольными контрагентами, позволяя управлять подключениями к API сразу нескольких приложений, поддерживающими спецификацию OpenAPI и реализацию требований безопасности по защите периметра Банка.
ШПУ	Шлюз Прикладного уровня	Шлюз, реализующий функции сопряжения на уровне приложений. L7 по модели OSI.
Bitbucket	-	Серверная система контроля версий на основе GIT.

DevOps	-	Методология активного взаимодействия специалистов по разработке со специалистами по информационно-технологическому обслуживанию и взаимная интеграция их рабочих процессов друг в друга для обеспечения качества продукта.
DLP	Data Leakage Prevention или Data Loss Protection	СПО или АС, обеспечивающее детектирование и/или блокировку передачи информации в случае содержания в ней секретной информации. Необходимо для предотвращения утечек информации различного рода.
EDA	Event-Driven Architecture	Архитектура, управляемая событиями, является шаблоном архитектуры программного обеспечения, позволяющим создание, определение, потребление и реакцию на события.

GC	Garbage Collector	Специальный процесс, называемый сборщиком мусора, периодически освобождает память, удаляя объекты, которые уже не будут востребованы приложением.
GIT	-	Распределенная система управления версиями. Необходима для коллективной работы над различными версиями исходного кода (или других артефактов).
GraphQL SDL	GraphQL Schema Definition Language	Язык описания GraphQL сервисов согласно спецификации GraphQL SDL.
ICAP	Internet Content Adaptation Protocol	Протокол для расширения прокси-серверов. В Банке используется для интеграции с различными АВПО и DLP системами.
IPA	Integrational Protocol Adapter	Java-адаптер, обеспечивающий протокольные преобразования.
ITIL	IT Infrastructure Library	Руководство по управлению услугами информационных технологий. Лежит в основе процесса управления различными информационными технологиями и технологическими ресурсами в Банке.

Jenkins	-	СПО, обеспечивающее возможность имплементации техник DevOps.
JSON	JavaScript Object Notation	Стандарт описания объектов в JavaScript. Предназначен для формализации сложноструктурированных данных в понятном для машин и людей виде. Наиболее часто используется в Web-технологиях.
Kafka	-	Менеджер очередей нового поколения с открытым исходным кодом.
Nexus	-	Система управления репозиториями. Изначально для хранения различных версий Java-библиотек.
MQ	-	Проприетарный менеджер очередей от компании IBM.
PR	Pull Request	Механизм и практика внесения изменений в исходный код посредством заведения специального объекта Pull Request, изменения в котором валидируются и верифицируются людьми и различного рода автоматизированными системами.

SIEM	Security Infrastructure And Event Management	АС для управления инфраструктурой средств киберзащиты и управления событиями, поступающими с этих средств.
Snapshot	Snapshot профиля	Полноценный слепок профиля в формате yaml, получаемый в результате конфигурирования профиля (выполнения команды sowa-config --config). Если содержание профиля разделено на несколько файлов (используется include), вся структура соберется в единый блок, а в случае использования средо-зависимых переменных в профиле, они заменятся на значения соответствующих параметров из файла list_value (выполнения команды sowa-config -e path_to_list_value/list_value --config).
SOWA	Sber Own Web Application Firewall	Шлюз прикладного уровня, разработанный на базе Open Source (т.е. открытого программного обеспечения), предназначенный для фильтрации и валидации контента.

Syslog	-	Простой протокол передачи текстовых сообщений. Используется для отправки различного рода сообщений в системы мониторинга.
SSL	Secure Socket Layer	Криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
TLS	Transport Socket Layer	Протокол защиты транспортного уровня, обеспечивающий защищенную передачу данных между узлами в сети Интернет, использует асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.

XML	eXtensible Markup Language	Человекочитаемый и расширяемый язык разметки информации. Предназначен для формализации сложноструктурированных данных в понятном для машин виде. Пришел из мира Enterprise приложений.
XSL	XML Stylesheet Language	Язык для форматирования или преобразования XML-документов.
YAML	Yet Another Markup Language	Человекочитаемый и расширяемый язык разметки информации. Предназначен для формализации сложноструктурированных данных в понятном для машин виде. Является надмножеством JSON, но предназначен для описания сущностей.
WS	WebSocket	Независимый веб-протокол, который позволяет создавать интерактивное соединение между сервером и клиентом (браузером) и обмениваться сообщениями в реальном времени. В отличие от HTTP, веб-сокеты позволяют работать с двунаправленным потоком данных.
WSS	WebSocket Secure	Протокол WebSocket над HTTPS.

Назначение сервиса

Цель создания

Продукт Platform V SOWA (Sber OWn Application firewall) - это шлюз прикладного уровня, который разработан на замену IBM DataPower. Данный инструмент разработан на базе OpenSource (Nginx + OpenResty + ModSecurity) и представляет собой шлюз между клиентами и Backend, предназначенный для фильтрации, маршрутизации и модификации проходящих через него сообщений. Он блокирует нелегитимные обращения к службам или сервисам — то есть не дает фронтальным компонентам иметь прямой доступ к внутренним сервисам организации.

Описание основных функций

Описание основных функций:

Название функции	Потребители функции	Аргументы функции	Результат
Маршрутизация	Потребители сервиса	Url входящего запроса; конфигурация сервиса	Входящий запрос перенаправлен на внешний сервис в соответствии с параметрами конфигурации.
Валидация входящего сообщения	Потребители сервиса	Параметры запроса; параметры конфигурации	В случае соответствия параметров запроса заданным политикам безопасности в параметрах конфигурации осуществляется валидация входящего сообщения и запрос передается далее на внешний сервис.

Валидация исходящего сообщения	Потребители сервиса	Параметры ответа; конфигурация сервиса	В случае соответствия параметров ответа заданным политикам безопасности в параметрах конфигурации осуществляется валидация исходящего сообщения и ответ передается далее потребителю.
Преобразование сообщений	Потребители сервиса	Параметры конфигураций; параметры сообщений	Сообщение преобразовано к требуемому виду для последующей валидации.
Преобразование протоколов	Потребители сервиса	Параметры конфигурации; параметры сообщений	Сообщение готово для передачи в соответствующем протоколе.
Конфигурирование	Потребители сервиса	Параметры конфигурации	Набор конфигурационных примитивов.
Аудит/Мониторинг/Журналирование	Сотрудник сопровождения и/или кибербезопасности/администраторы	-	Логи аудита конфигурирования и трассировки запросов, показатели текущего состояния профиля.

Сценарии использования

Определение ролей "владелец сервиса", "эксперт кибербезопасности", "администратор системы" и "специалист сопровождения" указано в разделе "Термины и обозначения". Указанный набор ролей является рекомендованным и в общем случае роли могут совмещаться.

Основные

Определение конфигурации:

1. Владелец сервиса задает параметры конфигурации для прикладного сервиса с учетом функциональных требований, а также требований безопасности, которые могут быть сформулированных экспертом кибербезопасности при наличии данной роли в организации. Рекомендуется участие роли "эксперт кибербезопасности" в процессе подготовки конфигурации для прикладного сервиса.
2. Владелец сервиса контролирует актуальность текущей конфигурации и вносит изменения по мере необходимости.

Описание параметров фильтрации:

1. Владелец сервиса задает правила фильтрации передаваемых сообщений. Рекомендуется участие роли "эксперт кибербезопасности" в процессе подготовки правил фильтрации для прикладного сервиса.
2. Владелец сервиса контролирует функционирование правил безопасности и модифицирует их по согласованию с экспертами кибербезопасности, при наличии данной роли в организации.

Описание схем валидации:

1. Владелец сервиса задает схемы валидации для структурированных передаваемых данных в соответствии функциональными требованиями к сервису, а также с учетом требований безопасности при наличии таковых. Рекомендуется участие роли "эксперт кибербезопасности" в процессе подготовки схем валидации для структурированных данных, пердаваемых сервисом.
2. Владелец сервиса вносит изменения в схемы валидации при изменении функциональных требований к сервису или требований безопасности.

Квотирование:

1. Владелец сервиса задает параметры частоты и размеры сообщений исходя из функциональных требований, а также с учетом требований безопасности при наличии таковых. Рекомендуется участие роли "эксперт кибербезопасности" в процессе описания параметров квотирования.
2. Владелец сервиса вносит параметры частоты и размеров сообщений при изменении функциональных требований к сервису или требований безопасности.

Определение требований безопасности:

Рекомендуется наличие на предприятии роли эксперт кибербезопасности. Эксперт кибербезопасности определяет требования безопасности к конфигурации прикладного сервиса на основании имеющихся корпоративных стандартов, правил и норм, а также лучших практик в области защиты информации.

Контроль соблюдения требований кибербезопасности:

Рекомендуется наличие на предприятии роли эксперт кибербезопасности. Эксперт кибербезопасности на основании анализа конфигурации принимает решение о соответствии ее требованиям безопасности и при необходимости выдвигает требования к изменению конфигурации.

Контроль функционирования на системном уровне:

1. Администратор системы, исследуя показания системного мониторинга и системных журналов, оценивает стабильность функционирования продукта в рамках текущей конфигурации.
2. В случае отклонений принимает необходимые корректирующие действия.
3. Обновляет системное ПО.

Анализ системных журналов:

1. Администратор анализирует системные журналы операционной системы в случае выявления отклонений поведения продукта.
2. Администратор превентивно анализирует системные журналы для предотвращения критических сбоев.

Установка обновлений системного программного обеспечения продукта:

1. Администратор, в соответствии с заданной релизной политикой, своевременно обновляет СПО.
2. Администратор определяет план обновления СПО.

Мониторинг системных метрик:

1. Администратор анализирует метрики с использованием централизованных средств с целью оценки поведения продукта.
2. Администратор определяет триггеры на изменения системных метрик в целях предупреждения и оперативного срабатывания на потенциально некорректное поведение продукта или среды функционирования продукта.

Анализ журналов событий и ошибок сервисов:

1. Администратор анализирует журналы событий и ошибок сервисов в случае выявления отклонений поведения продукта.
2. Администратор консолидирует данные об ошибках и передает их владельцу сервиса для принятия мер по исправлению ошибок.
3. Владелец сервиса на основании полученных данных передает информацию для обработки владельцам смежных сервисов, либо команде разработки для исправления ошибок, либо специалистам Кибербезопасности для анализа проблемы.

Альтернативные

Контроль функционирования на прикладном уровне:

1. Специалист сопровождения осуществляет мониторинг журналов прикладных событий и сопоставляя с поведением, заданным в конфигурации оценивает корректность функционирования конфигурации сервиса на прикладном уровне.
2. При необходимости внесения изменений специалист сопровождения уведомляет владельца сервиса.
3. Специалист сопровождения вносит изменения конфигурации.

Обеспечение стабильности сервиса в случае некорректного квотирования:

1. Специалист сопровождения, основываясь на события аудита и журнал мониторинга, фиксирует заполнение памяти сервиса и сообщает об этом владельцу сервиса.
2. Владелец сервиса увеличивает средозависимые квоты.

Исключительные

Восстановление в случае сбоев:

1. Администратор анализирует причины отклонений от нормального поведения.
2. Определяет необходимые корректирующие воздействия.
3. Выполняет штатные операции по восстановлению.

Обеспечение стабильности сервиса при непредвиденных нагрузках:

1. Специалист сопровождения уведомляет владельца сервиса о случившемся факте переполнения памяти.
2. Владелец сервиса увеличивает квоту.

Обеспечение защиты в случае появления новых угроз:

1. Эксперт кибербезопасности получает данные об уязвимости, информирует об этом специалиста соровождения.
2. Специалист сопровождения вносит необходимые изменения.