

Руководство по настройке интеграции

«МОЙОФИС ЧАСТНОЕ ОБЛАКО 2» С ВНЕШНИМИ SIEM-СИСТЕМАМИ
В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«МОЙОФИС ЧАСТНОЕ ОБЛАКО 2»
В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ**

**РУКОВОДСТВО ПО НАСТРОЙКЕ ИНТЕГРАЦИИ
С ВНЕШНИМИ SIEM-СИСТЕМАМИ**

2.8G

На 12 листах

**Москва
2024**

МойОфис

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

1 Общие сведения	6
1.1 Назначение	6
1.2 Системные требования	6
2 Настройка работы	7
2.1 Архитектура решения для СО	8
2.2 Архитектура решения для PGS	9
3 Настройка SIEM-системы	10
4 Регистрируемые события системы	11

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В настоящем документе используются следующие сокращения с соответствующими расшифровками (см. Таблицу 1).

Таблица 1 — Сокращения и расшифровки

Сокращение, термин	Расшифровка и определение
CO	CloudOffice, Система редактирования и совместной работы в составе «МойОфис Частное Облако 2» в варианте исполнения ГОСТ
PGS	Pythagoras, Система хранения данных в составе «МойОфис Частное Облако 2» в варианте исполнения ГОСТ
ОС	Операционная система
ПО	Программное обеспечение
Тенант	Логический объект, включающий в себя совокупность вычислительных ресурсов, репозиторий и пользователей
KUMA	Kaspersky Unified Monitoring and Analysis Platform — SIEM-система для централизованного сбора, ускоренного анализа и корреляции событий безопасности из различных источников данных

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Совместная работа «МойОфис Частное Облако 2» в варианте исполнения ГОСТ версии 2.8G с внешними SIEM-системами позволяет передавать во внешние SIEM-системы события безопасности, фиксируемые в «МойОфис Частное Облако 2» в варианте исполнения ГОСТ, в формате SEF по протоколу syslog для их дальнейшего хранения и анализа средствами внешней системы.

Регистрация событий безопасности обеспечена в соответствии с требованиями приказов ФСТЭК России № 17, 21, 31, 239.

1.2 Системные требования

Перечень требований к программному и аппаратному обеспечению ПО МойОфис приведен в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Системные требования».

2 НАСТРОЙКА РАБОТЫ

Для совместной работы «МойОфис Частное Облако 2» в варианте исполнения ГОСТ и внешней SIEM-системы необходимо включить и настроить функцию в административной панели (подробно см. в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по администрированию»).

Архитектура решения совместной работы Системы редактирования и совместной работы (CO), Системы хранения данных» (PGS) и внешней SIEM-системы представлена на рисунке 1.

Сервис аудита (Audit Service) является единой точкой входа событий аудита для Системы редактирования и совместной работы (CO) и Системы хранения данных (PGS).

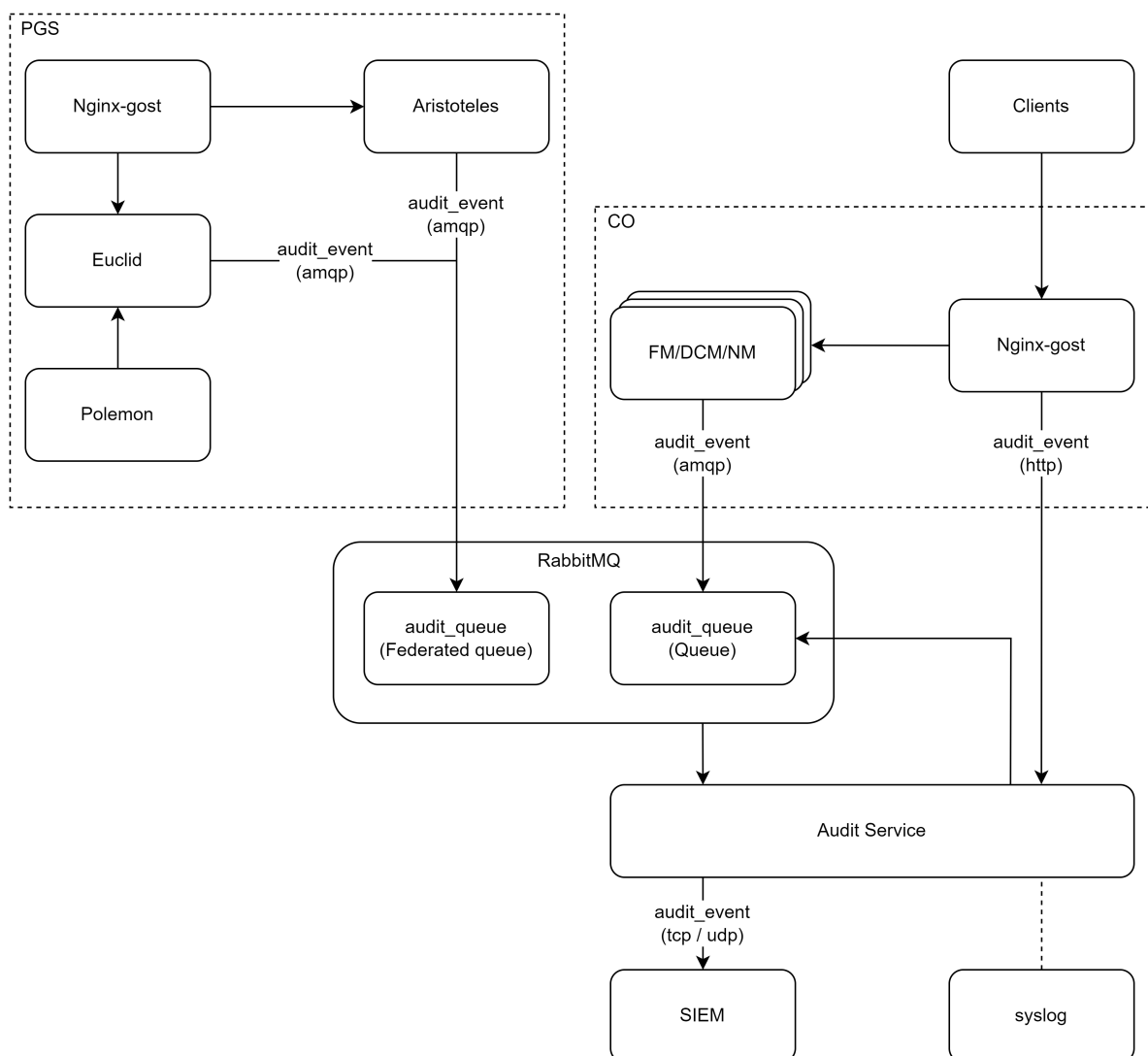


Рисунок 1 — Схема сбора и передачи событий

2.1 Архитектура решения для СО

Клиентские запросы (Clients) инициализируют создание событий в модулях Nginx, FM (File Manager), NM (Notification Manager) и DCM (Document Collaboration manager). После инициализации события отправляются через RabbitMQ (брокер сообщений, audit_queue) в Audit Service, который их записывает в SIEM-систему (KUMA) или в syslog в CEF-формате.

Для каждого события записывается модуль и хост, в котором оно было создано (пример для модуля FM: `<140>1 2024-03-24T09:33:40.467Z server.example.com co.core.fm ...`). Все модули имеют единую точку обработки и отправки сообщений. Исходя из данных клиентского запроса, заполняются все поля сообщения, указанные в документе «Перечень регистрируемых событий». Для получения актуальных данных о тенанте модуль отправляет запрос в PGS («Система хранения данных»).

События представляют собой сообщения CEF-формата.

`<co_server>/api/v1/audit (POST)` – место сбора `/api/v1/audit` для отправки событий CefEvent в Audit Service со стороны СО, полученных от Nginx.

Пример сообщения CEF-формата:

```
Raw <140>1 2023-03-28T14:01:37.047Z alice.office.ru co.core.fm - - - CEF:0|
MyOffice|Optional[MyOffice Private Cloud]|2.8|301899|Download an Object|0|
msg=Unknown Error outcome=failure dvc=0.0.0.0
externalId=e9b0738b87831ae0edb7cc79455caf10 start=2023-03-28T14:01:31.671927Z
fileId=1c74e733-ab39-44d7-a9eb-b5867863db7f fname=photo1771018324.jpeg
fileCreateTime=2023-01-25T10:43:56Z cs5=pgs8491350672 fileModificationTime=2023-
03-28T14:01:31.667793Z src=10.100.56.79 suser=alexandr.smirnov@office.ru
filePath=/media/photo1771018324.jpeg suid=03f34f8e44f14a7b971f5c16068485bd
fileType=image/jpeg
```

Пример события, полученного Kaspersky Unified Monitoring and Analysis Platform (KUMA):

```
TenantName : Main
Timestamp : Mar 28, 2024 17:01:37.052
Name : Download an Object
StartTime : Mar 28, 2024 17:01:31.671
Message : Unknown Error
DeviceAddress : 0.0.0.0
DeviceEventClassID : 301899
DeviceFacility : 17
DeviceHostName : server.example.com
DeviceProcessName : co.core.fm
DeviceProduct : Optional[MyOffice Private Cloud]
DeviceReceiptTime : Mar 28, 2023 17:01:37.047
DeviceVendor : MyOffice
DeviceVersion : 2.8
SourceAddress : 10.100.1.1
SourceUserID : 03f34f8e44f14a7b971f5c16068485bd
SourceUserName : ivan.ivanov@office.ru
DeviceCustomString5 : pgs84913506721
Service : Service
EventOutcome : failure
```



```
ExternalID : e9b0738b87831ae0edb7cc79455caf10
FileCreateTime : Jan 25, 2024 13:43:56.000
FileID : 1c74e733-ab39-44d7-a9eb-b5867863db7f
FileModificationTime : Mar 28, 2024 17:01:31.667
FileName : photo1771018324.jpeg
FilePath : /media/photo1771018324.jpeg
FileType : image/jpeg
Priority : Low
Severity : 0
Type: Base
```

2.2 Архитектура решения для PGS

Функциональная возможность аудита в PGS реализована внутри сервисов PGS – Aristoteles и Euclid, обрабатывающих HTTP-запросы от CO и Polemon (компоненты «МойОфис Частное Облако 2» в варианте исполнения ГОСТ) с требованием отправки события. Сервисы запрашивают у компонента PGS Aristoteles настройки аудита с адресом SIEM-системы, далее генерируют событие в формате CEF и по полученному адресу посылают сообщение. События содержат информацию о пользователях и группах пользователей, действиях администратора, публичных ссылках и объектах файловой системы.

Более подробно с архитектурными особенностями можно ознакомиться в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Архитектура».

Локальный файл журнала событий расположен в следующей директории:

```
/var/log/pgs/<env>.<default_domain>/epicure/access.log
```

Пример сообщений CEF-формата:

1. Без чувствительных данных

```
<140>1 2024-03-29T15:10:29.199Z localhost Euclid - - - CEF:0|MyOffice|MyOffice
Private Cloud|2.8|100100|Create a User|1|msg=User Created Successfully
outcome=success dst=10.160.1.1 externalId=cidaevhkuczj1z start=2024-03-29-15-06-
39.451268 cs5=pgs59628 suser=admin@server.example.com src=10.5.156.199
duser=auth2@server.example.com suid=5677bddd-97f4-457f-976c-75b72a7d06eb
```

2. С чувствительными данными (где параметр cs5 — информация о тенанте)

```
<140>1 2024-03-29T14:59:41.657Z localhost Euclid - - - CEF:0|MyOffice|MyOffice
Private Cloud|2.8|100100|Create a User|1|msg=User Created Successfully
outcome=success dst=10.160.1.1 externalId=zjtkzcvbaupxtzk start=2024-03-29-14-55-
51.845147 cs5=pgs59628 filePermission=default,admin
suser=admin@server.example.com src=10.5.156.199 duser=auth2@server.example.com
suid=5677bddd-97f4-457f-976c-75b72a7d06eb
```

3 НАСТРОЙКА SIEM-СИСТЕМЫ

Для настройки работы с «МойОфис Частное Облако 2» в варианте исполнения ГОСТ на стороне SIEM-системы необходимо установить соответствие между регистрируемыми событиями и их параметрами. Перечень регистрируемых в «МойОфис Частное Облако 2» в варианте исполнения ГОСТ событий и их параметров представлен в документе «Перечень регистрируемых событий».

4 РЕГИСТРИРУЕМЫЕ СОБЫТИЯ СИСТЕМЫ

Перечень регистрируемых событий системы приведен в документе «Перечень регистрируемых событий».

Регистрируемые события подразделяются на следующие классы:

- User – все действия, связанные с пользователями, такие как создание, удаление, изменение прав пользователя, авторизация, блокировка и т.п.;
- Group – действия, связанные с группами пользователей, такие как создание, удаление, изменение состава группы и т.п.;
- Document – действия, связанные с файлами в системе, такие как создание, удаление, изменение содержимого, изменение прав доступа к файлу и т.п.;
- Folder – действия, связанные с папками, такие как создание, открытие, загрузка папки, изменение прав доступа и т.п.;
- Links – действия, связанные с публичными и внутренними ссылками, такие как создание, блокировка, удаление ссылки и т.п.;
- Administrator – действия администратора, такие как создание, удаление, переименование общей папки или смена ее владельца, восстановление объектов, разрешение или запрет создания публичных ссылок, включение или выключение автоверсионирования, настройка глубины и частоты сохранения версий, настройка тенанта и т.п.

Регистрируемые события классифицируются по уровню важности (Severity). Описание уровней важности регистрируемых событий приведено в таблице 2.

Таблица 2 – Уровни важности события

Уровень важности	Приоритет	Описание
0	Critical	Критичные события, являются прямыми индикаторами атаки
1	High	События высокой важности, при множественных повторениях или в совокупности с другими событиями являются индикаторами атаки
2	Medium	События средней важности, необходимы для восстановления последовательности действий в процессе
3	Low	События низкой важности, напрямую не свидетельствующие об атаке. Являются обогащающими событиями для расследования инцидента
4	Informational	Информационные события, используемые для обогащения данных
5	Unknown	События, возникающие при неизвестной ошибке

Поля событий, отмеченные в документе «Перечень регистрируемых событий» символом *, несут угрозу раскрытия данных. Процедура включения и исключения чувствительных данных в сообщениях описана в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство администратора» и в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по настройке».

ID события имеет четкую структуру построения:

- первые две цифры – класс события;
- вторые две цифры – подкласс события;
- последние две цифры – уникальный идентификатор события в подклассе.