«Инфомаксимум»

(Общество с ограниченной ответственностью)

Система «Proceset»

Руководство администратора информационной безопасности

2026 г.

Оглавление

Администратор безопасности

Раздел предназначен для специалистов по информационной безопасности.

В разделе приведены инструкции по аудиту действий пользователей и мониторингу состояния системы, а также описание журналов безопасности и реализованных в системе Proceset мер защиты.

Описание механизма аудита

Выявление неправомерных действий

Для выявления неправомерных действий в системе необходимо использовать инструмент логирования событий. Журнал событий безопасности *security.log* по умолчанию располагается:

- На Windows — в каталоге *C:\ProgramData\Infomaximum\logs* (локальный диск может отличаться)
- На Linux — в контейнере */var/log/infomaximum*

Для выявления неправомерных действий необходимо использовать журнал безопасности и описание процесса выявления неправомерных действий.

Неправомерные действия с описанием

Входы в систему с разными ID пользователя с одной рабочей станции в короткие интервалы времени (интервал устанавливается экспертами)

1. Вход 1 (действие 1):

- Тип события: *logon*
- Дополнительный параметр типа события: *success*
- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Поле: *Время события*

2. Вход 2 (действие 2):

- Тип события: *logon*
- Дополнительный параметр типа события: *success*
- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Поле: *Время события*

Если параметры ID объекта отличаются, а *remote_address* имеют одинаковое значение, то Время события 1 — Время события 2 = интервал входа с одной рабочей станции (интервал сравнивается с установленным параметром).

Вход с одним и тем же ID пользователя с разных рабочих станций в короткие интервалы времени (интервал устанавливается экспертами)

1. Вход 1 (действие 1):

- Тип события: *logon*
- Дополнительный параметр типа события: *success*
- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Поле: *Время события*

2. Вход 2 (действие 2):

- Тип события: *logon*
- Дополнительный параметр типа события: *success*

- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Поле: *Время события*

Если ID имеют одинаковое значение, а значения remote_address отличаются, то Время события 1 — Время события 2 = интервал входа с одной рабочей станции (интервал сравнивается с установленным параметром).

Большое количество неудачных входов в систему с одним ID с разных терминалов

- Тип события: *logon*
- Дополнительный параметр типа события: *invalid_logon*
- Объект: *id*
- Адрес рабочей станции: *remote_address*

Или

- Тип события: *logon*
- Дополнительный параметр типа события: *invalid_logon_and_max_logon_attempts_exceed*
- Объект: *id*
- Адрес рабочей станции: *remote_address*,

Где *remote_address* имеют разные значения в каждой попытке входа.

Большое количество неудачных входов в систему с разными ID с одного терминала

- Тип события: *logon*
- Дополнительный параметр типа события: *invalid_logon*
- Объект: *id*
- Адрес рабочей станции: *remote_address*

Или:

- Тип события: *logon*
- Дополнительный параметр типа события: *invalid_logon_and_max_logon_attempts_exceed*
- Объект: *id*
- Адрес рабочей станции: *remote_address*,

Где *remote_address* имеют одинаковое значение в каждой попытке входа.

Попытка входа в систему с заблокированной учётной записью

- Тип события: *logon*
- Дополнительный параметр типа события: *disabled_logon*
- Объект: *id*

Отключение логирования

Для конфигурирования логов используется файл *logback.xml*, расположенный:

- На Windows — в каталоге *C:\ProgramData\Infomaximum*
- На Linux — в контейнере */var/lib/infomaximum*

Также есть вариант с подменой конфигурации через механизм инициализации системы логирования.

Подробный порядок и загрузки файла конфигурации описан: https://logback.qos.ch/manual/configuration.html.

Совет.

- Необходимо отслеживать изменение: на Windows — в папке *C:\ProgramData\Infomaximum*, на Linux — в контейнере */var/lib/infomaximum*.
- Необходимо отслеживать изменение: на Windows — в папке *C:\Program Files\Infomaximum*, на Linux — в контейнере */usr/sbin/infomaximum*.
- Необходимо отслеживать изменения службы.

Удаление/очистка логов

Удаление и очистка логов не может осуществляться через веб-интерфейс. Логирование данного неправомерного действия не осуществляется.

Доступ к удалению/очистке логов регламентируется на уровне файловой системы в рамках политики Windows.

Добавление нового ID пользователя в систему и его удаление (блокировка) в короткий промежуток времени (короткий промежуток времени устанавливается экспертами)

Субъект (тот, кто производит действие):

- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Сотрудник: *employee_id*
- Действие 1 (тип события): *create* (создание)
- Действие 2 (тип события): *remove* (удаление)
- Действие 3 (тип события): *change_enabled_logon*
- Дополнительный параметр действия 3: — *false* (отключение разрешения на авторизацию, блокировка)
- Поле: *Время события* (для каждого действия)

Объект (над кем производят действие):

- Объект: *id*
- Объект: *employee*

Если ID объекта (добавляемого сотрудника) имеет одинаковое значение при всех действиях:

- Время события действия *remove* — Время события действия *create* = интервал времени между созданием и удалением сотрудника

Или:

- Время события действия *change_enabled_logon* (доп. параметр: — *false*) — Время события действия *create* = интервал времени между созданием и блокировкой сотрудника

Назначение новых прав/членства в группе пользователю и их последующая отмена в короткий интервал времени (интервал устанавливается экспертами)

Субъект (тот, кто производит действие):

- Объект: id
- Адрес рабочей станции: remote_address
- Сотрудник: employee_id
- Действие 1 (Тип объекта): adding_access_role (добавление сотруднику РД) • Действие 2 (Тип объекта):
- removing_access_role (удаление у сотрудника РД в группе «Административные» роли)
- Дополнительный параметр у всех типов объектов (всех действий):
  - access_role_id (id роли доступа)
  - access_role_name (имя роли доступа)
- Поле: Время события (для каждого действия)

Объект (над кем производят действие):

- Объект: id, employee, login

Если *ID* и *Login* объекта (над кем производят действие) имеет одинаковое значение при всех действиях и назначаемая и отменяемая РД имеет одинаковое значение *access_role_id*, то Время события действия *removing_access_role* — Время события действия *adding_access_role* = интервал времени между назначением новых прав и их последующая отмена.

Изменение парольной политики АС

Любое изменение из 6 типов событий (действий) является изменением парольной политики АС для объекта.

1. Действие 1 (Тип объекта): *change_complex_password*. Включение/выключение контроля сложности пароля.

2. Действие 2 (Тип объекта): *change_min_password_length*. Изменение минимальной длины пароля.

3. Действие 3 (Тип объекта): *password_expiration_date*. Включение/выключение срока действия пароля.

4. Действие 4 (Тип объекта): *change_password_expiration_time*. Изменение срока действия пароля.

5. Действие 5 (Тип объекта): *limit_login_attempts*. Включение/выключение ограничить попытки входа.

6. Действие 6 (Тип объекта): *change_max_invalid_logon_count*. Изменение лимита на неуспешные попытки входа.

Отслеживаемые параметры объекта:

- Объект: *id*
- Адрес рабочей станции: *remote_address*
- Сотрудник: *employee_id*, *login*

Мониторинг состояния системы

Работоспособность системы

Для контроля работоспособности системы:

- Для ручной проверки выполните вход в веб-интерфейс системы по URL-адресу сервера, на котором система развернута (*http(s)://{адрес_сервера}:{порт}/*)
- Для автоматической проверки отправьте GraphQL-запрос вида: *{server{status}}*. Вы можете ознакомиться с инструкцией по выполнению GraphQL-запросов в разделе Работа с GraphQL
- Отслеживайте события типа ERROR в журнале работы системы *main.log*:
  - На ОС Windows — в каталоге *C:\ProgramData\Infomaximum\logs*
  - На ОС Linux — в контейнере */var/log/infomaximum*

Рекомендации по контролю целостности

Для контроля целостности системы рекомендуется отслеживать:

На ОС Windows

- Контрольные суммы файлов в каталоге — *C:\Program Files\Infomaximum*
- Обновление конфигурационных файлов в каталоге — *C:\ProgramData\Infomaximum\config*
- Файл для шифрования файловых баз данных Proceset — *C:\ProgramData\Infomaximum\secret_key\secret_key*
- Команду запуска службы — Infomaximum
- Контрольную сумму файла *logback.xml* в каталоге — *C:\ProgramData\Infomaximum*
- Настройки системы в ветке реестра —
- *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Infomaximum*
- Файл сертификата и закрытого ключа x.509 — путь прописывается в конфигурационном файле *C:\ProgramData\Infomaximum\config\com.infomaximum.subsystem.frontend.json*
- События журнала безопасности с объектом «system» (target@729368) в логе — *C:\ProgramData\Infomaximum\logs\security.log*

На ОС Linux

- Контрольные суммы файлов в каталоге — */usr/sbin/infomaximum*
- Обновление конфигурационных файлов в каталоге — */var/lib/infomaximum/config/*
- Файл для шифрования файловых баз данных Proceset — */var/lib/infomaximum/secret_key/secret_key*
- Команду запуска службы — Infomaximum
- Контрольную сумму файла *logback.xml* в каталоге — */var/lib/infomaximum*
- Файл сертификата и закрытого ключа x.509 — по умолчанию файл и пароль расположены в каталогах
- */run/secrets/infomaximum_app_https_certificate* и
- */run/secrets/infomaximum_app_https_certificate_password*
- События журнала безопасности с объектом «system» (target@729368) в логе — */var/log/infomaximum/security.log*

В СУБД ClickHouse

- Контрольные суммы файлов в каталоге — */usr/bin/clickhouse/*
- Каталог с чувствительными данными — */run/secrets/*

Дополнительные меры по ограничению доступа

Ниже представлены файлы и каталоги приложения, для которых могут потребоваться дополнительные меры по ограничению доступа:

- Рабочий каталог:
  - На ОС Windows — *C:\ProgramData\Infomaximum*
  - На ОС Linux — */var/lib/infomaximum/* В СУБД ClickHouse — */var/lib/clickhouse/*
- Каталог с файловыми базами данных:
  - На ОС Windows — *C:\ProgramData\Infomaximum\databases*
  - На ОС Linux — */var/lib/infomaximum/databases/*
- Файловые базы данных с ключевыми метаданными:
  - На ОС Windows — *C:\ProgramData\Infomaximum\databases\main*
  - На ОС Linux — */var/lib/infomaximum/databases/main/*
- Каталог, в котором хранятся логи, в том числе логи аудита:
  - На ОС Windows — *C:\ProgramData\Infomaximum\logs*
  - На ОС Linux — */var/log/infomaximum/*
  - В СУБД ClickHouse — */var/log/clickhouse-server/*
- Каталог конфигурационных файлов:
  - В СУБД ClickHouse — */etc/clickhouse-server/*

Реализованные защитные меры ИБ в системе

Аутентификация пользователей в системе

Аутентификация пользователей может осуществляться несколькими способами:

1. С помощью логина и пароля, заданных в системе. При входе пользователя происходит сравнение хеша введенного им пароля (для указанного логина) с хешем пароля, сохраненным в базе данных. При первом входе в систему сотруднику необходимо задать собственный пароль.

2. Посредством интеграции Active Directory.

3. С использованием протокола SAML.

4. С использованием протокола Kerberos.

5. С использованием протокола OpenID.

Перечень объектов защиты системы

Перечень защищаемых объектов представлен ниже.

- Журналы безопасности, хранящиеся в логах:
  - На Windows — в каталоге C:\ProgramData\Infomaximum\logs
  - На Linux — в контейнере /var/log/infomaximum
- Аутентификационная информация пользователей, хранящаяся в базе:
  - На Windows — в каталоге C:\ProgramData\Infomaximum\database
  - На Linux — в контейнере /var/lib/infomaximum/data/databases
- Файлы настроек, хранящиеся в базе:
  - На Windows — в каталоге C:\ProgramData\Infomaximum\database
  - На Linux — в контейнере /var/lib/infomaximum/data/databases
- Права доступа, хранящиеся в базе:
  - На Windows — в каталоге C:\ProgramData\Infomaximum\database
  - На Linux — в контейнере /var/lib/infomaximum/data/databases
- Механизмы настройки прав и аудита, хранящиеся в базе:
  - На Windows — в каталоге C:\ProgramData\Infomaximum\database
  - На Linux — в контейнере /var/lib/infomaximum/data/databases
- Исполняемые файлы, хранящиеся в каталоге:
  - На Windows — C:\Program Files\Infomaximum
  - На Linux — /usr/sbin/infomaximum/
- Элементы интерфейса для веб, хранящиеся в каталоге:
  - На Windows — C:\Program Files\Infomaximum
  - На Linux — /usr/sbin/infomaximum/

Необходима защита на уровне операционной системы следующих каталогов:

- C:\Program Files\Infomaximum
- C:\ProgramData\Infomaximum
- Docker service: infomaximum-clickhouse
- Docker volume: infomaximum-clickhouse

Проверка безопасности пароля пользователей

Параметры паролей пользователей для встроенной аутентификации можно настроить через веб-интерфейс системы: «Настройки»/«Аутентификация»/«Название аутентификации».

Сложный пароль

Проверка безопасности пароля пользователей включает в себя следующие ограничения на установку/изменение пароля в системе:

- Прописные буквы английского алфавита от A до Z
- Строчные буквы английского алфавита от a до z
- Десятичные цифры (от 0 до 9)
- Неалфавитные символы (например, !, $, #, %)
- Длина пароля
- Запрет на повторное использование уже использованных паролей

Проверка соблюдения этих требований выполняется при изменении или создании паролей. Проверка на содержание в пароле символов из e-mail отсутствует.

Минимальная длина пароля

Настройка минимальной длины пароля доступна только в случае, если включен параметр *«Сложный пароль»*. Параметр указывает минимально допустимое количество символов при создании/изменении пароля. Допустимые значения: от 8 до 15 символов.

Если параметр *«Сложный пароль»* находится в состоянии **«Выкл.»**, то минимальное количество символов по умолчанию — 4. Просмотр настройки параметров доступен также через веб-интерфейс по указанному выше адресу.

Срок действия пароля

Параметр *«Срок действия пароля (дней)»* указывает срок действия пароля с момента его задания/изменения. Возможное значение параметра — от 1 до 1000 дней. После того, как срок действия завершился, пользователю предлагается задать новый пароль. Пока пользователь не задаст новый пароль, доступ в систему будет ограничен. Чтобы сделать срок действия пароля без ограничений, оставьте параметр незаполненным.

Если параметр *«Сложный пароль»* находится в состоянии **«Выкл.»**, то пользователь при вводе нового пароля может использовать предыдущие, за исключением последнего заданного пароля.

Если срок действия пароля не истек, но сотрудник поменял пароль на тот же, который установлен у него в данный момент, то счетчик срока действия пароля не обнуляется. Если пользователь поменял пароль на другой (хотя срок действия пароля не закончился), счетчик срока действия обнуляется и отсчет идет согласно заданному параметру.

Шифрование паролей

Для шифрования паролей в системе используется алгоритм: AES-256. AES — симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит).

При инициализации системы создается 256-битный ключ, который по умолчанию хранится:

- На Windows — в каталоге C:\ProgramData\Infomaximum\secret_key. Путь берется из конфигурационного файла subsystem.core.json, который находится в C:\ProgramData\Infomaximum\config\com.infomaximum
- На Linux — в контейнере /var/lib/infomaximum/data/secret_key

Ключ используется для шифрования/дешифрования хранимых паролей.

Алгоритм шифрования пароля AES-256 используется:

- при интеграции с Active Directory
- соединении с БД ClickHouse
- создании подключений в пространстве

Для паролей от доверенных сертификатов и их хранилища также предусмотрено шифрование:

1. В качестве аргументов --password и --secret_key_path укажите пароль и путь к ключу шифрования secret_key.

2. В файле com.infomaximum.subsystem.frontend.json замените параметры ssl_cert_store_password и trust_store_password на зашифрованные версии encrypted_ssl_cert_store_password и encrypted_trust_store_password соответственно.

3. Замените указанные пароли в параметрах на полученные в консоли значения.

После сохранения изменений пароли будут храниться в зашифрованном виде.

Хеширование паролей пользователей

На сервер не отправляется введенный пользователем пароль в исходном виде. Хеширование пароля происходит с помощью алгоритма SHA256.

Сервер получает хеш пароля и использует повторно хеш-функцию, а также функцию, формирующую секретный ключ по стандарту PBKDF2 (PBKDF2WithHmacSHA512). Сервер сохраняет в базе 2 значения в виде секретного ключа: Соль + Хеш (от присланного хеша пароля). Просмотр настройки параметров доступен также через веб-интерфейс по указанному выше адресу.

Количество попыток входа

Параметр *«Кол-во попыток входа»* позволяет ограничить количество попыток входа в систему. Допустимое значение параметра *«Кол-во попыток входа»* — от 1 до 100. Параметр отвечает за количество попыток входа, которые пользователь может совершить в системе. Попытка входа — когда пользователь верно указал логин, но неправильно ввел пароль и нажал **Войти**.

Если попытки достигают заданного параметра, пользователь блокируется. Этому пользователю ограничивается вход в систему. Чтобы не ограничивать количество попыток входа, оставьте параметр незаполненным.

Период, после которого попытки входа пользователя обнуляются, по умолчанию составляет 10 минут. То есть, если между попытками ввода учетных данных не более 10 минут, то они считаются последовательными, как 1,2,3,4 и т.д., и по заданному значению *«Кол-во попыток входа»* аккаунт блокируется. Как только проходит 10 минут, счетчик сбрасывается.

Изменение периода возможно посредством конфигурационного файла только на Windows. Чтобы изменить период, после которого происходит обнуление попыток входа:

1. Перейдите по пути: C:\ProgramData\Infomaximum\config.

2. Откройте файл конфигурации: *infomaximum.subsystem.core.json*.

3. Измените значение параметра: *reset_count_invalid_logon_duration* (значение можно указать в днях, часах, минутах и секундах).

Срок жизни ссылки на восстановление пароля

Если пользователь забыл пароль, то его можно восстановить через почту. Письмо будет отправлено, если настроен сервер исходящей почты в системе Proceset. В письме указывается ссылка, после перехода по которой пользователь может создать новый пароль согласно настройкам парольной политики. По умолчанию параметр *«Срок жизни ссылки для восстановления пароля»* имеет значение 1 день (24 часа). Изменение параметра через веб-интерфейс недоступно. Изменение периода возможно через конфигурационный файл только на Windows.

Чтобы изменить период:

1. Откройте папку: C:\ProgramData\Infomaximum\config.

2. Откройте файл конфигурации: *com.infomaximum.subsystem.core.json*.

3. Измените параметр *restorelink_timeout* (значение можно указать в днях, часах, минутах и секундах).

Время жизни неактивной сессии

По умолчанию период жизни неактивной сессии для каждого пользователя – 1 неделя (7 дней). Изменение параметра через веб-интерфейс недоступно. Изменение периода возможно через конфигурационный файл только на Windows.

Чтобы изменить период:

1. Откройте папку: C:\ProgramData\Infomaximum\config.

2. Откройте файл конфигурации: *com.infomaximum.subsystem.fronted.json*.

3. Измените параметр: *session_timeout* (значение можно указать в днях, часах, минутах и секундах).

4. Перезапустите службу *«infomaximum»*.

Идентификация, аутентификация субъектов и объектов доступа

Для всех пользователей и программных процессов осуществляется идентификация, аутентификация и авторизация. Пользователю, не прошедшему аутентификацию, не предоставляется доступ в систему. В системе существуют механизмы управления учетными записями пользователей: создание, активация, блокирование, предоставление и изменение прав и т.д.

Для управления компонентами системы требуется собственная авторизация. При этом выполняются следующие требования:

- При входе осуществляется идентификация и проверка подлинности субъектов доступа
- Пароль-хеш и идентификаторы передаются исключительно по сети и хранятся в зашифрованном виде
- Отсутствует возможность изменить пароль методом замены объекта, хранящего зашифрованный пароль
- Реализована возможность установления минимальной длины (не менее 8 символов) и срока действия пароля (парольная политика)
- Реализована возможность установления уровня сложности пароля (парольная политика)
- Реализована возможность установления запрета на повторное использование одного и того же пароля (парольная политика)
- Пользователю предоставляется право самостоятельно изменять свой пароль
- Отсутствует доступ администраторов системы к паролю пользователя
- Осуществляется контроль и подсчет попыток входа в систему (успешный или неуспешный, т.е. несанкционированный)
- Система уведомляет пользователя о превышении количества неудачных попыток входа. После превышения заданного количества неудачных попыток входа доступ не предоставляется. Также при предъявлении правильного пароля пользователь не информируется о вводе правильного пароля
- Система позволяет производить блокировку сеанса по запросу субъекта

Блокировка пользователей системы

Блокирование пользователей возможно осуществить следующими способами:

1. Через веб-интерфейс: «Настройки»/«Сотрудники»/«Профиль сотрудника». Удалите активные аутентификации во вкладке *«Доступ»* в параметре *«Аутентификация»* у нужного сотрудника.

2. Через массовое назначение. У пользователей, которым нужно ограничить доступ, через функцию *«массовое назначение»* выберите *«Аутентификация»* и отключите активные аутентификации. Сохраните изменения.

3. С использованием GraphQL-запроса для блокировки из внешней АС. Отправьте следующий запрос:

```
mutation {
   employee {
      set_authentication(target_employee_ids:[id],
       authentication_ids:[])
   }
}
```

Где id — идентификатор пользователя.

Инструкция по выполнению GraphQL-запросов представлена в соответствующем разделе.

После блокировки пользователя происходит его оперативное отключение от системы, текущий сеанс блокируется. При каждом новом входе в систему необходимо ввести данные для авторизации.

Блокировка пользователей из внешней системы

Для автоматической выгрузки пользователей из внешней системы необходимо наличие созданного Ключа API с определенными правами доступа. Для блокировки пользователей системы из внешней АС выполните следующие запросы:

<http://127.0.0.1:8010/graphql?query={employee{employees{id,login}}}&api_key=826ac84312a0481ea57cc160fd1b59dc>

Где 127.0.0.1:8010 — это адрес сервера, 826ac84312a0481ea57cc160fd1b59dc — Ключ API.

С помощью следующего запроса можно определить ID пользователя в системе:

<http://localhost:8093/graphql?query=mutation{employee{set_authentication(target_employee_ids:[id], authentication_ids:[])}}&api_key=fd7dbbf252fd43daad15628989d5eb0a>

Где localhost:8093 – это адрес сервера, fd7dbbf252fd43daad15628989d5eb0a — Ключ API, id — уникальный ID конкретного пользователя.

После определения ID выполните блокировку сотрудника.

Журналы безопасности

К перечню журналов безопасности относятся журнал событий безопасности системы и журналы безопасности на уровне ОС.

Журнал событий безопасности системы *security.log* по умолчанию располагается:

- На Windows — в каталоге *C:\Program Data\Infomaximum\logs*
- На Linux — в контейнере */var/log/infomaximum*

Логирование событий осуществляется в формате, основанном на спецификации RFC 5424 (The Syslog Protocol). Для временных меток используется формат RFC 3339.

Подробное описание формата представлено в спецификации RFC 5424:

Оригинальный документ (IETF)

Русский перевод

Формат временных меток описан в спецификации RFC 3339.

Используется EnterpriseId 729368, не зарегистрированный в IANA.

События записываются на уровне отдельных нод:

- Если агент автоматизации установлен на одной ноде с Proceset, все события записываются в общий файл логов
- Если агент автоматизации установлен на отдельной ноде, события Proceset и агента автоматизации фиксируются в отдельных файлах логов на своих нодах

Размер журналов безопасности системы

Предположительный размер файлов лога системы вычисляется по формуле:

Память в год = Количество сотрудников*1 Мб.

Файл *logback.xml* позволяет настраивать ротацию логов. Логи безопасности по умолчанию хранятся 3 года. Если период недостаточен, необходимо изменить файл конфигурации.

Описание журналов безопасности

Формат записи:

```
37<1> <time> <hostname> infomaximum <pid> <MSGID> [meta sequenceId=""][system@729368 version.core="1.0.0" version.proceset="1.0.0"][source@729368 ...][event@729368 ...][target@729368 ...]
```

Пример записи в журнале безопасности:

```
<37>1~2019-03-26T16:07:06+03:00~infomaximum61~infomaximum~9160~update~[metasequenceId="80"]~[system@729368 version.platform="1.0.0" version.proceset="1.0.0"]~[source@729368 sessionHash="3915d830623a26b61a044d1ad9c1bebb6e61705a969559e1c5f436d2210aabcc" id="1" type="employee" login="admin" remoteAddress="10.0.75.1"]~[event@729368 old_first_name="Денис" old_email=petr@gmail.com new_first_name="Владимир" new_email="email@gmail.com"]~[target@729368 module="platform" id="2" type="employee" login="vpetrov"]
```

Спецификация полей журнала безопасности

№	Описание	Комментарий	Зарезервированное значение
1	Приоритет	Все сообщения идут с одним приоритетом: 4*8+5	37
2	Версия syslog		1
3	HOSTNAME	Имя сервера, если определить не удалось или имя не соответствует требованиям RFC 5424, то "-"	
4	Имя процесса	Нарушение спецификации. Спецификация требует указать имя приложения (java), но это не обеспечивает уникальность продукта	infomaximum
5	ID процесса (PID)	Если pid определить не удалось, то '-'	
6	MSGID события	Уникальный идентификатор события, основан на *«инкрементирующем значении»*. Строковое значение типа события	

Соответствие видов событий журнала

Информация о событии в терминах СЗИ	Элемент в строке в журнале безопасности	Примечание
Уникальный номер строки о событии ИБ	[meta sequenceId="80"]	Значение meta sequenceId является уникальным номером строки о событии
Название АС-источника информации о событии	[source@729368 … type="employee"…]	Значение type в source является типом источника события. Подробнее в таблице Блоки записи в журнале безопасности
Версия источника информации о событии	[system@729368 version.platform= "1.0.0"]	Значение version.platform является информацией об источнике события. Подробнее в таблице Блоки записи в журнале безопасности
Системное имя (логин) пользователя-инициатора события	[source@729368 … id="1" type="employee" login="admin"…]	Значение id="1", "login="admin" является информацией о пользователе-инициаторе, а именно: login – логин, id – порядковый номер пользователя. Подробнее в таблице Блоки записи в журнале безопасности
IP-адрес хоста-источника события	[source@729368… remoteAddress="10.0.75.1"]	Значение remoteAddress является IP-адресом хоста-источника события Важно: В лог-файле корректно отображается IP пользователя только при стандартном запуске Docker. В rootless-режиме IP подменяется. При проксировании через Nginx реальный IP сохраняется в remote_proxy, а не в remote_address
Системное имя (логин) пользователя получателя	[target@729368 …id="1" type="employee" login="admin"]	Значения в target id="1" type="employee" login="admin" являются информацией о пользователе-получателе, где: id – порядковый номер пользователя login – логин пользователя type – тип получателя

Информация о событии в терминах СЗИ	Элемент в строке в журнале безопасности	Примечание
Системный идентификатор сообщения о событии	update	Идентификатором-сообщением о событии может быть значение <MSGID> Подробнее в таблицах со структурированными данными для каждого модуля
Системное время источника события	2019-03-26T16:07:06+03:00	Время источника события фиксируется в строке под <time> Формат даты: yyyy-MM-ddTHH:mm:ssZ
Текст сообщения в максимально подробном виде, включая старые и новые значения измененных свойств	[event@729368 old_first_name="Денис" old_email=petr@gmail.com new_first_name="Владимир" new_email="email@gmail.com]	old_first_name – старое значение имени old_email – старое значение электронного адреса new_first_name – новое значение имени new_email – новое значение электронной почты
Полное имя процесса(службы) результат (успех/отказ)		Результат (успех/отказ) фиксируется не для всех событий в системе

Блоки записи в журнале безопасности

Поле	Описание
Meta	
sequenceId	Идентификатор события, основан на *«инкременте»*
Система: system@729368	
version.platform	Версия ядра
Источник: source@729368	
system	Внутреннее действие системы
remote_address remote_proxy	Запросы без авторизации. Тип источника: «anonymous». remoteAddress – удаленный адрес, с которого пришел запрос remoteProxy – адрес прокси-сервера
remoteAddress remoteProxy id sessionHash login	Запрос пользователя. Тип источника: «employee». remoteAddress – удаленный адрес, с которого пришел запрос remoteProxy – адрес прокси-сервера id – идентификатор пользователя sessionHash – SHA256 от строкового значения сессии login – логин пользователя
subtype remote_address remote_proxy id name login_AD domain_name	Запрос ключа API. Тип источника: «api_key». subtype ="AD" – тип авторизации через ключ API посредством политик AD certificate – тип авторизации через ключ API посредством клиентской аутентификации (сертификатов безопасности) none – тип авторизации только через ключ API remote_address – удаленный адрес, с которого пришел запрос remote_proxy – адрес прокси-сервера id – идентификатор ключа API name – название ключа API login_AD – логин пользователя в AD (появляется только в том случае, если есть интеграция с AD)

Поле	Описание
	domain_name – доменное имя (появляется только в том случае, если есть интеграция с AD)
Объект, над которым произведено действие: target@729368	

Ротация журнала безопасности

Все журналирование системы основано на компоненте Logback (https://logback.qos.ch).

По умолчанию в системе применяется файл конфигурации logback.xml, расположенный:

- На Windows — в каталоге C:\ProgramData\Infomaximum
- На Linux — в контейнере /var/lib/infomaximum

Также в системе возможны варианты с переопределением файла конфигурации, при этом используется механизм приоритизации загрузки файла конфигурации.

Подробно о формате файла конфигурации, а также о приоритетах загрузки файлов конфигурации можно посмотреть в документации:

https://logback.qos.ch/manual/configuration.html .

По умолчанию в системе включена ротация логов, для журнала безопасности применяются следующие правила: файл журнала безопасности упаковывается в архив и переименовывается в соответствии с шаблоном ("security.%d{yyyy-MM-dd}.%i.log.gz") при следующих условиях:

- Наступили следующие сутки
- Журнал лога превысил размер в 50 Мб

По умолчанию файлы журнала безопасности хранятся 3 года. По истечении этого времени старые журналы безопасности удаляются. Параметры, которые отвечают за ротацию логов, настраиваются в файле logback.xml.

Горячее обновление конфигурации

В системе по умолчанию предусмотрен механизм «горячего» обновления конфигурации. За это отвечают параметры «scan» и «scanPeriod». Сканирование происходит каждые 30 секунд. Этот механизм позволяет временно изменять правила логирования, вплоть до полного его отключения (<configuration scan="true" scanPeriod="30 seconds">).

Docker-контейнеры

Образы контейнера ClickHouse

Компания *«Инфомаксимум»* не добавляет неиспользуемые библиотеки или пакеты.

Образы контейнеров, контейнеры, параметры запуска контейнера, конфигурационные файлы контейнеров не хранят критичную информацию (пароли в файлах, hard-coded пароли, ключи, логины). Логины и хеш паролей приходят через Docker Secrets.

Образ контейнера был подписан компанией *«Инфомаксимум»*.

Логирование ClickHouse

Контейнер с ClickHouse записывает логи в отдельный volume: infomaximumclickhouse-log. Для просмотра логов подключите и запустите контейнер с необходимым volume, например:

```
docker run -it --rm -v=infomaximum-clickhouselog:/ mnt/volume ubuntu bash
```

Внутри контейнера выполните:

```
tail -n 200 -f /mnt/volume/clickhouseserver.log
```

Логи хост машины не кастомизируются и располагаются по умолчанию в /var/log/….

Работа Docker Secrets

Применение секретов позволяет не передавать пароли и приватные ключи в открытом виде (в docker-контейнеры).

В настоящий момент через секреты передаются следующие значения:

- логин для подключения к clickhouse
- хеш-пароля для подключения к clickhouse
- сертификат (для https)
- приватный ключ (для https)
- Diffie Hellman ключ (для https)

Доступ к секретам предоставляется в момент создания сервиса и впоследствии не может быть изменен. Чтобы внести изменения, удалите сервис и создайте его повторно.

Все секреты хранятся в зашифрованном в виде в Docker Swarm.

При запуске контейнера Docker Swarm монтирует секреты в виде файлов в каталог /run/secrets/….

Разворачивание ClickHouse в Docker-контейнере

Разворачивание происходит в соответствии с установкой БД ClickHouse.

Взаимная аутентификация между сервером приложений и ClickHouse

Взаимодействие осуществляется по HTTPS-протоколу.

При подключении к ClickHouse сервер приложения осуществляет аутентификацию ClickHouse по серверному сертификату, который ранее был настроен в docker-контейнере. ClickHouse осуществляет аутентификацию сервера приложения по связке логин + пароль. Пароль хранится во встроенной файловой базе данных в зашифрованном виде.

Логин и пароль передается в Post-запросе.

Пример запроса к БД, полученный посредством программы Wireshark:

```
Hypertext Transfer Protocol
POST /?extremes=0&database=default&user=writeUser&password=write&compress=1
HTTP/1.1\r\n
[Expert Info (Chat/Sequence): POST /?
extremes=0&database=default&user=writeUser&password=write&compress=1 HTTP/1.1\r\
n]
[POST /?extremes=0&database=default&user=writeUser&password=write&compress=1
HTTP/1.1\r\n]
[Severity level: Chat]
[Group: Sequence]
Request Method: POST
Request URI: /?
extremes=0&database=default&user=writeUser&password=write&compress=1
Request URI Path: /
Request URI Query:
extremes=0&database=default&user=writeUser&password=write&compress=1
Request URI Query Parameter: extremes=0
Request URI Query Parameter: database=default
Request URI Query Parameter: user=writeUser
Request URI Query Parameter: password=write
Request URI Query Parameter: compress=1
Request Version: HTTP/1.1
Content-Length: 62\r\n
Content-Type: text/plain; charset=UTF-8\r\n
Host: 192.168.88.15:8888\r\n
Connection: Keep-Alive\r\n
User-Agent: Apache-HttpClient/4.5.2 (Java/11.0.4)\r\n
\r\n
[Full request URI: http://192.168.88.15:8888/?
extremes=0&database=default&user=writeUser&password=write&compress=1]
File Data: 62 bytes
Line-based text data: text/plain (1 lines)
select currentDatabase() FORMAT TabSeparatedWithNamesAndTypes;
```

Пользователи в ClickHouse имеют минимальные права и выполняют исключительно SQL-запросы. Применимо ограничение настроек для конкретного пользователя. Невозможно устанавливать настройки ClickHouse посредством SQL-запросов.

Настройки безопасности изменяются только на сервере в файлах «/etc/clickhouse-server/config.xml» и «/etc/clickhouse-server/users.xml».

Если у пользователя нет физического доступа к серверу ClickHouse, то невозможно поменять настройки сервера. Более подробное описание безопасности представлено: https://clickhouse.yandex/docs/ru/operations/settings/.