

Журнал событий системы MITIGATOR

Формат записи syslog

Оглавление

Формат записи журнала событий в syslog	3
Пример записи события:	3
Пример записи события с расширенным набором полей:	3
Поля записи журнала	4
Типы событий.....	6
Расширение набора полей записи события	13

Формат записи журнала событий в syslog

Каждая запись журнала событий MITIGATOR состоит из префикса «backend BIFIT Mitigator[]» и содержательной части, описывающей событие. Содержательная часть имеет формат JSON и включает три обязательных поля и ряд необязательных, состав которых зависит от типа события. Все возможные поля описаны в таблице «Поля записи журнала событий».

Для ряда событий предусмотрено расширение формата описания. Для таких событий в записи журнала будет присутствовать поле «custom», содержащее JSON объект со специфичным для события набором полей. Перечень таких типов событий и состав полей приведены в таблице «Расширение набора полей записи события».

Все типы событий системы MITIGATOR перечислены в таблице «Типы событий».

Пример записи события:

```
Aug 27 14:54:31 backend BIFIT Mitigator[1]:{"instance_id":1,"instance_name":  
"Mitigator0", "created_at":"2019-08-29T11:54:31.976847Z","type_id": "auth_login",  
"type":"Logged in","user_id":1,"user_login":"admin",  
"firstname":"System","surname":"Administrator", "user_ip":"192.168.5.6",  
"user_role":"System administrator"}
```

Пример записи события с расширенным набором полей:

```
Aug 27 14:58:31 backend BIFIT Mitigator[1]:{"instance_id":1,"instance_name":  
"Mitigator0", "created_at":"2019-09-03T17:50:14.968337Z", "type_id":  
"autodetect_alert_up", "type":"Трафик поднялся выше порога", "user_id":3,  
"user_id":3, "firstname":"Autodetection", "surname":"System", "custom":{"autodetect_al  
ert_alert":true, "autodetect_alert_created_at":"2019-09-  
03T20:50:14.968200927+03:00", "autodetect_alert_flow":"status.input.pps",  
"autodetect_alert_policy_id":15, "autodetect_alert_policy_name":"poiskoviki  
google", "autodetect_alert_threshold":"0.00", "autodetect_alert_value":"1.00"}}
```

Поля записи журнала

Поле	Тип	Назначение	Комментарии
instance_id	uint	Идентификатор экземпляра	
instance_name	string	Имя экземпляра	
created_at	time	Время фиксации события	Время на сервере MITIGATOR по UTC. Обязательное поле.
type_id	string	Идентификатор типа события	Обязательное поле.
type	string	Название типа события	Обязательное поле.
user_id	uint	Идентификатор пользователя, совершившего действие	Информация о пользователе присутствует для событий, которые возникают в результате действий пользователя. Действия системы автодетектирования фиксируются с идентификатором пользователя «3».
user_login	string	Логин пользователя	
firstname	string	Имя пользователя	Для действий системы автодетектирования указывается значение «Autodetection».
surname	string	Фамилия пользователя	Для действий системы автодетектирования указывается значение «System».
user_ip	string	IP-адрес устройства, с которого выполнен вход	
user_role	string	Роль пользователя в системе	
user_group	string	Название группы пользователя	Присутствует только для групповых пользователей.
policy_id	uint	Идентификатор политики защиты	
policy_name	string	Название политики защиты	
is_ipv6	boolean	Признак IPv6 политики защиты	
element	string	Название контрмеры	
element_id	uint	Идентификатор контрмеры	
handler	string	Измененный параметр	В следующих версиях поле будет упразднено. Измененные параметры и значения будут записываться в поле custom.

value	string	Новое значение параметра	В следующих версиях поле будет упразднено. Измененные параметры и значения будут записываться в поле custom.
custom	string	Расширенная информация о событии	Массив пар "ключ": "значение". Набор полей зависит от типа события. Присутствует не для всех типов.

Значение типа time передаются в формате Internet Date/Time согласно RFC 3339 с точностью до микросекунды.

Пример: 2019-08-24T11:54:48.780948Z

Типы событий

Служебный идентификатор типа события	Название типа события
Политики защиты	
autodetect_off	Отключено автодетектирование
autodetect_on	Включено автодетектирование
automitigation_off	Автоматическое включение защиты запрещено
automitigation_on	Автоматическое включение защиты разрешено
policy_add	Создана политика защиты
policy_delete	Удалена политика защиты
policy_edit	Изменены параметры политики защиты
policy_rename	Название политики изменено
policy_on	Включена политика
policy_off	Отключена политика
policy_monitor_mode	Изменение тестового режима работы контрмеры
isn_settings	Изменены параметры синхронизации сессии
isn_servers	Установлены IP-адреса серверов с синхронизацией
Управление политиками по syslog	
attack_on	Включена политика защиты по сигналу syslog
attack_off	Отключена политика защиты по сигналу syslog
attack_start	По syslog получен сигнал включения политики защиты
attack_stop	По syslog получен сигнал отключения политики защиты
syslog_create	Создан syslog сервер
syslog_update	Обновлены настройки syslog сервера
syslog_delete	Удален syslog сервер
syslog_on	Включен удаленный сислог
syslog_off	Выключен удаленный сислог
Правила маршрутизации	
rules_update_common	Обновлены групповые правила маршрутизации
rules_update_post	Обновлены Пост-правила маршрутизации
rules_update_pre	Обновлены Пред-правила маршрутизации
Лицензирование	
autodetect_license_threshold_crossed_up	Входящий трафик поднялся выше лицензионной полосы
autodetect_license_threshold_crossed_down	Входящий трафик опустился ниже лицензионной полосы
license_bandwidth_limit_expired	Время действия лицензионных лимитов закончилось
license_server_disconnected	Соединение с сервером лицензирования разорвано
license_server_connected	Соединение с сервером лицензирования установлено
license_token_update	Обновлен лицензионный ключ
license_set_limit	Лицензионная полоса изменена

license_upload_limit	Загружен лицензионный файл
license_server_failed	Произошла ошибка на стороне сервера лицензирования
license_tariff_expiring	Время действия тарифа подходит к концу
license_tariff_expired	Время действия тарифа истекло
support_expired	Время действия сервисного контракта истекло
license_token_delete	Удалён лицензионный ключ
license_change	Изменён режим лицензирования
license_dynamic_limit	Лицензионная полоса изменена динамически
Системные события	
mitigation_on	Включена система защиты
mitigation_off	Отключена система защиты
router_ext_on	Установлено соединение с внешним роутером
router_ext_off	Разорвано соединение с внешним роутером
router_int_on	Установлено соединение с внутренним роутером
router_int_off	Разорвано соединение с внутренним роутером
port_up	Включен сетевой порт
port_down	Отключен сетевой порт
backend_start	Запущен Backend
backend_stop	Остановлен Backend
click_start	Запущен MITIGATOR
click_stop	Обработчик пакетов остановлен
log_level_set	Изменён уровень логирования
waf_add	WAF добавлен
waf_edit	WAF изменён
waf_delete	WAF удалён
softstart_started	Применён «Мягкий старт»
softstart_aborted	«Мягкий старт» прерван пользователем
softstart_finished	Закончен «Мягкий старт»
dns_not_available	DNS-сервер недоступен
host_not_available	Ошибка разрешения доменного имени
resolver_settings_update	Изменены параметры опроса DNS-сервера
incident_on	Начало инцидента
incident_off	Завершение инцидента
incident_comment	Отредактирован комментарий инцидента
scan	Зафиксирован сброс трафика
multi_conflict	Возник конфликт лидерства экземпляров
accesslog_alert	Получено оповещение от анализатора логов
accesslog_rules	Изменены правила анализа логов
isn_key_delete	Удален секретный ключ для ISN
isn_key_set	Установлен секретный ключ для ISN

Пользователи	
auth_login	Вошел в систему
failed_auth_login	Неудачная попытка входа в систему
auth_logout	Вышел из системы
group_create	Создана группа
group_update	Обновлена группа
group_delete	Удалена группа
user_create	Создана учетная запись пользователя
user_update	Изменена учетная запись пользователя
user_delete	Удалена учетная запись пользователя
group_user_create	Создана учетная запись группового пользователя
group_user_update	Изменена учетная запись группового пользователя
group_user_delete	Удалена учетная запись группового пользователя
role_create	Создана роль
role_delete	Удалена роль
role_update	Изменена роль
group_role_create	Создана групповая роль
group_role_delete	Удалена групповая роль
group_role_update	Изменена групповая роль
notification_update	Обновлена подписка на уведомления
BGP	
bgp_neighbor_add	Добавлен BGP-сосед
bgp_neighbor_update	Изменены параметры BGP-соседа
bgp_neighbor_delete	Удален BGP-сосед
bgp_config_change	Изменены параметры BGP-соединения
bgp_idle	Разорвано BGP-соединение
bgp_established	Установлено BGP-соединение
bgp_community_add	Создан список комьюнити для анонса
bgp_community_update	Обновлён список комьюнити для анонса
bgp_community_delete	Удалён список комьюнити для анонса
bgp_flowspec_add	Создан список флоуспек-правил для анонса
bgp_flowspecs_update	Обновлен список FlowSpec-правил
bgp_flowspec_delete	Удалён список флоуспек-правил для анонса
bgp_prefixes_add	Создан список сетей для анонса
bgp_prefixes_update	Обновлён список сетей для анонса
bgp_prefixes_delete	Удалён список сетей для анонса
bgp_announce	Отправка BGP-анонса
bgp_policy_edit	Изменены параметры политики анонса
bgp_announce_on	Включено анонсирование префиксов политики по BGP
bgp_announce_off	Выключено анонсирование префиксов политики по BGP

bgp_prefixlist_settings_change	Изменены настройки префикслистов
Настройка системы	
geolite2_update	Загружена база данных стран
mail_update	Обновлены настройки почтового сервера
deploy_set	Изменен способ интеграции в сеть
bypass_mode	Установлен режим работы bypass
vestochka_update	Обновлены настройки Весточки
deploy_mssp	Переключен выключатель GRE MSSP
logo_delete	Удален логотип
logo_update	Обновлен логотип
deploy_settings	Изменена схема деплоя
connreqtable_reset	Сброшена таблица отслеживаемых соединений и запросов для всех политик
telegram_update	Обновлены настройки Telegram
external_auth_settings	Параметры внешней аутентификации изменены
accesslog_config	Изменен адрес анализатора логов
background_update	Обновлен фон страницы входа
background_delete	Удален фон страницы входа
sflow_v4_switch_enable	Включена отправка sFlow IPv4
sflow_v4_switch_disable	Отключена отправка sFlow IPv4
sflow_v4_update	Изменены параметры sFlow IPv4
sflow_v6_switch_enable	Включена отправка sFlow IPv6
sflow_v6_switch_disable	Отключена отправка sFlow IPv6
sflow_v6_update	Изменены параметры sFlow IPv6
statistic_settings	Изменены параметры отправки статистики
syslog_notifications_update	Обновлены настройки уведомлений по Syslog
syslog_tbl	Изменился список временно заблокированных IP-адресов
Изменение настроек контрмер	
acl_write	Обновлены правила фильтрации
ipset_remove	Удалены значения из списка IP-адресов
ipset_add	Добавлены значения в список IP-адресов
ipset_reset	Сброшен список IP-адресов
ipset_update	Обновлен список IP-адресов
ipset_settings	Обновлены параметры прогрессивной блокировки
config_change	Изменены параметры контрмеры
switch_on	Включена контрмера
switch_off	Отключена контрмера
geolite2_action	Задан тип действия над трафиком
geolite2_selections	Задан список стран
prefix_limiter_delete	Удалены значения

prefix_limiter_reset	Список ограничений очищен
prefix_limiter_set	Добавлены значения
prefix_limiter_updated	Обновлены значения
prefix_limiter_reset_drops	Сброшены счетчики
prefix_limiter_reset_drops_stats	Сброшена статистика
prefix_limiter_drops_trigger	Отослано уведомление
tls_training_started	Запущено обучение
tls_training_finished	Обучение окончено
tls_training_aborted	Обучение прервано пользователем
tls_training_failed	Обучение завершено с ошибкой
tls_prot_database	Загружена база правил
training_reset	Удалены результаты обучения
learning_start	Запущено обучение
learning_reset	Сброшена статистика обучения
autodetect_alert_up	Трафик поднялся выше порога
autodetect_alert_down	Трафик опустился ниже порога
autodetect_timing_policy_update	Обновлены тайминги автодетекта для политики
autodetect_cm_update	Обновлены переменные
autodetect_cm_delete	Удалены переменные
autodetect_reset	Сброшены данные
autodetect_timing_update	Обновлены тайминги автодетекта
iptable_reset	Сброшена таблица аутентифицированных IP-адресов
conntable_reset	Сброшена таблица отслеживаемых соединений
ipall_reset	Сброшена таблица аутентифицированных IP-адресов для всех политик
reqtable_reset	Сброшена таблица отслеживаемых запросов
session_reset	Сброшена таблица сессий
add_by_tuple	Добавлен IP-адрес по параметрам пакета
scan_detected	Обнаружено сканирование
pcap_start	Запущен захват пакетов
pcap_stop	Остановлен захват пакетов
autopcap_settings	Изменены настройки автозахвата пакетов
autopcap_start	Запущен автозахват пакетов
autopcap_stop	Остановлен автозахват пакетов
pcap_failed	Захват пакетов завершен с ошибкой
autopcap_failed	Автозахват пакетов завершен с ошибкой
packet_capture_send	Результаты захвата отправлены на email
bpf_program_upload	Программа загружена
bpf_program_delete	Программа удалена
table_add	Добавлено значение в таблицу
table_delete	Удалено значение из таблицы

table_reset	Очищена таблица
fingerprint_wl_add	Загружен белый список отпечатков
fingerprint_wl_delete	Удален белый список отпечатков
fingerprint_bl_add	Загружен черный список отпечатков
fingerprint_bl_delete	Удален черный список отпечатков
fingerprint_allow_add	Загружен список разрешенных отпечатков
fingerprint_allow_delete	Удален список разрешенных отпечатков
fingerprint_autobl_delete	Автоматически собранный черный список удален
fingerprint_autoallow_delete	Автоматически собранный список разрешенных удален
fingerprint_auto_delete	Удален список автоматически собранных отпечатков
fingerprint_collection_attack	Запущен сбор выборки атаки
fingerprint_collection_start	Запущен сбор отпечатков
fingerprint_collection_stop	Остановлен сбор отпечатков
fingerprint_collection_finished	Закончен сбор отпечатков
config_auto_change	Автоматически изменены настройки контрмеры
rts_start	Запущена генерация сигнатур
rts_stop	Остановлена генерация сигнатур
rts_reference_start	Запущен захват эталонного дампа
rts_reference_stop	Остановлен захват эталонного дампа
rts_reference_delete	Эталонный дамп удалён
rts_reference_add	Эталонный дамп добавлен
learning_on	Включено обучение
learning_off	Отключено обучение
hpa_enabled	Адресная защита начата
learning_list_clear	Очищена таблица обучения
config_auto_change	Автоматически изменены настройки контрмеры
Облачная сигнализация «Тип 1»	
type1_objects_add	Добавлен объект мониторинга соседа
type1_objects_update	Обновлён объект мониторинга соседа
type1_objects_delete	Удалён объект мониторинга соседа
type1_neighbor_add	Создан новый сосед
type1_neighbor_update	Обновлён сосед
type1_neighbor_delete	Удалён сосед
type1_alert_on	Отправлен алерт
type1_alert_off	Снят алерт
type1_alert_off_recv	Alert остановлен в системе
Облачная сигнализация «Периметр»	
perimeter_switch_on	Включено подключение к Периметру
perimeter_switch_off	Отключено подключение к Периметру
perimeter_add	Создан новый объект Периметр

perimeter_update	Изменены настройки объекта Периметр
perimeter_delete	Удален объект Периметр
perimeter_wl	В Периметр передан белый список
perimeter_bl	В Периметр передан черный список
perimeter_mitigation_start	В Периметр отправлен запрос митигации
perimeter_mitigation_stop	В Периметр отправлен запрос остановки митигации
perimeter_mitigation_start_recv	Митигация запущена в Периметре
perimeter_mitigation_stop_recv	Митигация остановлена в Периметре
Управление сигнатурами регулярных выражений	
rex_aliases_delete	Удалены наборы правил
rex_aliases_update	Обновлены наборы правил
rex_reset	Сброшены настройки
rex_templates_delete	Удалены шаблоны
rex_templates_update	Обновлены шаблоны
rex_versions_update	Обновлены версии
Экземпляры	
leader_order_set	Задан порядок выбора экземпляра-лидера
instance_change	Настройки экземпляра изменены
click_out_of_sync	Рассинхронизация настроек клика
leader_giveup	Экземпляр прекратил лидировать

Расширение набора полей записи события

Событие/Поле	Тип	Описание
autodetect_alert_up		Трафик поднялся выше порога (срабатывание системы автодетектирования при пересечении порога вверх)
autodetect_alert_created_at	time	Время события
autodetect_alert_alert_true	boolean	Превышение
autodetect_alert_flow	string	Параметр автодетектирования
autodetect_alert_threshold	float	Заданный порог срабатывания
autodetect_alert_value	float	Зафиксированное значение
autodetect_alert_down		Трафик опустился ниже порога (срабатывание системы автодетектирования при пересечении порога вниз)
autodetect_alert_created_at	time	Время события
autodetect_alert_alert_false	boolean	Понижение
autodetect_alert_flow	string	Параметр автодетектирования
autodetect_alert_threshold	float	Заданный порог срабатывания
autodetect_alert_value	float	Зафиксированное значение
switch_on		Включена контрмера (срабатывание при пересечении порога вверх)
autodetect_predicate	string	Предикат
autodetect_threshold_name	string	Название порога
autodetect_threshold_value	string	Значение порога
autodetect_metric_value	string	Наблюдаемое значение
switch_off		Отключена контрмера (срабатывание при пересечении порога вниз)
		Те же поля, что для switch_on
packet_capture_send		Результаты захвата отправлены на email
files	array[string,]	Список фалов захвата с указанием размера каждого.
prefix_limiter_drops_trigger		Отослано уведомление (отправка уведомления о срабатывании ограничений DLIM)
Drops	array[object,]	Список зафиксированных срабатываний ограничений. Для каждого сработавшего ограничения в записи будет присутствовать JSON объект с набором приведенных ниже полей.
drops_prefix	string	IP-адрес получателя
drops_limit_packets	uint	Ограничение в пакетах в секунду
drops_limit_bits	uint	Ограничение в битах в секунду
drops_triggered_packets	boolean	Активно ограничение в пакетах
drops_triggered_bits	boolean	Активно ограничение в битах
drops_active_time	time	Общая продолжительность работы ограничений
drops_last_time	time	Время последнего срабатывания ограничения
drops_first_time	time	Время первого срабатывания ограничения
drops_packets	uint	Число срабатываний ограничения в пакетах

drops_bytes	uint	Число срабатываний ограничения в битах
drops_total	uint	Общее число срабатываний ограничений
user_create		Создана учетная запись пользователя
id	uint	Идентификатор пользователя
firstname	string	Имя
patronymic	string	Отчество
surname	string	Фамилия
username	string	Логин
blocked	boolean	Заблокирован
email	string	Email
max_attach_size	uint	Максимальный размер письма и вложений
language	string	Язык
password	string	Пароль
phone	string	Телефон
position	string	Должность
role_id	uint	Идентификатор роли
telegram_id	string	Telegram ID
telegram_size	uint	Максимальный размер письма и вложений
token_ttl	uint	Время бездействия пользовательской сессии
group_user_create		Создана учетная запись группового пользователя
		Те же поля, что для user_create
user_group_id	uint	Идентификатор группы
user_group	string	Название группы
user_update		Изменена учетная запись пользователя
id	uint	Идентификатор пользователя
firstname	string	Имя
patronymic	string	Отчество
surname	string	Фамилия
username	string	Логин
blocked	boolean	Заблокирован
email	string	Email
max_attach_size	uint	Максимальный размер письма и вложений
language	string	Язык
password	string	Пароль
phone	string	Телефон
position	string	Должность
telegram_id	string	Telegram ID
telegram_size	uint	Максимальный размер письма и вложений
token_ttl	uint	Время бездействия пользовательской сессии
old_firstname	string	Имя предыдущее (поле присутствует только если произошло изменение значения)

old_surname	string	Фамилия предыдущая (поле присутствует только если произошло изменение значения)
old_patronymic	string	Отчество предыдущее (поле присутствует только если произошло изменение значения)
old_username	string	Логин предыдущее (поле присутствует только если произошло изменение значения)
role_id	uint	Идентификатор роли (поле присутствует только если произошло изменение значения)
group_user_update		Изменена учетная запись группового пользователя
		Те же поля, что для user_update
user_group_id	uint	Идентификатор группы
user_group	string	Название группы
user_delete		Удалена учетная запись пользователя
id	uint	Идентификатор пользователя
firstname	string	Имя
patronymic	string	Отчество
surname	string	Фамилия
username	string	Логин
group_user_delete		Удалена учетная запись группового пользователя
		Те же поля, что для user_delete
user_group_id	uint	Идентификатор группы
user_group	string	Название группы
role_create, group_role_create, role_delete, group_role_delete		Создана роль Создана групповая роль Удалена роль Удалена групповая роль
role_name	string	Название роли
role_update, group_role_update		Изменена роль Изменена групповая роль
role_name	string	Название роли
old_role_name	string	Название роли предыдущее
license_dynamic_limit		Лицензионная полоса изменена динамически
enable	boolean	Использовать динамическое распределение
up_threshold	uint	Порог повышения
down_threshold	uint	Порог понижения
hold_duration	uint	Время удержания
min_bandwidth	uint	Минимум используемой полосы
max_bandwidth	uint	Максимум используемой полосы
previous_limit	uint	Предыдущее значение полосы
current_limit	uint	Новое значение полосы
incident_on		Начало инцидента
incident_id	uint	ID инцидента

incident_started_at	time	Время начала
incident_max_input_pps	uint	Максимальная скорость входящего трафика в пакетах
incident_max_input_bps	uint	Максимальная скорость входящего трафика в байтах
incident_max_drop_pps	uint	Максимальная скорость сброшенного трафика в пакетах
incident_max_drop_bps	uint	Максимальная скорость сброшенного трафика в байтах
incident_max_pass_pps	uint	Максимальная скорость прошедшего трафика в пакетах
incident_max_pass_bps	uint	Максимальная скорость прошедшего трафика в байтах
incident_off		Завершение инцидента
incident_type	string	Тип
incident_countermeasures	string	Контрмеры
incident_finished_at	time	Время завершения
incident_duration	uint	Длительность
softstart_started		Применён «Мягкий старт»
learning_period	uint	Длительность режима «Мягкий старт»
bgp_established, bgp_idle		Установлено BGP-соединение Разорвано BGP-соединение
bgp_neighbor_name	string	Имя
bgp_neighbor_address	string	IP-адрес
bgp_as	uint	Номер AS
instance_id	uint	Идентификатор экземпляра
instance_name	string	Название экземпляра
policy_monitor_mode		Изменение тестового режима работы контрмеры
policy_id	uint	Идентификатор настроек
monitor_mode	boolean	Тестовый режим работы контрмеры
scan_detected		Обнаружено сканирование
scanner_ip	string	IP сканера
scanner_first_time	time	Первое обнаружение
scanner_last_time	time	Последнее обнаружение
instance_id	uint	Идентификатор экземпляра
instance_name	string	Название экземпляра
as_number	string	Номер AS
as_name	string	Название AS
country	string	Страна
city	string	Город
accesslog_alert		Получено оповещение от анализатора логов
ips	string	IP-адреса
external_auth_settings		Параметры внешней аутентификации изменены
user_login_tag	string	Логин пользователя
user_ip_tag	string	IP-адрес пользователя
error	string	Ошибка

click_out_of_sync		Рассинхронизация настроек клика
request	string	Запрос
method	string	HTTP method
error	string	Ошибка
config_change		Изменены параметры контрмеры
game_version	uint	Версия протокола
perimeter_switch_on, perimeter_switch_off, perimeter_update		Включено подключение к Периметру Отключено подключение к Периметру Изменены настройки объекта Периметр
perimeter_id	uint	Идентификатор Периметра
perimeter_name	string	Название Периметра
rts_start		Запущена генерация сигнатур
rts_settings_id	uint	Идентификатор настроек RTS
rts_settings_apply	boolean	Применить полученные правила