

Table of Contents

Table of Contents	1
Журналы и отчёты	2
Журнал событий	3
Экспорт журналов	4
Режим расширенного поиска	7
Описание форматов журналов	9

Журнал событий

Documentation: ☒

Product: UGMC

Version: 7.x

В журнале отображены события, связанные с изменением настроек UGMC, а также все события авторизации в консоли, старта, выключения, перезагрузки сервера и т.п.

Для удобства поиска необходимых событий записи могут быть отфильтрованы по различным критериям, например, диапазон дат, компонент, важность, тип события.

В UserGate Management Center также представлен режим расширенного поиска для формирования сложных фильтров с использованием специального языка запросов, синтаксис которого рассмотрен далее в разделе [Режим расширенного поиска](#).

После выбора необходимых параметров настроенный фильтр можно сохранить, нажав кнопку **Сохранить как**. Список сохранённых фильтров можно будет увидеть во вкладке **Популярные фильтры**.

Администратор может сам выбрать столбцы, которые будут отражены в журнале. Для этого необходимо навести указатель мыши на название любого столбца, нажать на появившуюся справа от названия столбца стрелку, выбрать **Столбцы** и в появившемся контекстном меню выбрать необходимые параметры.

С помощью кнопки **Экспортировать в CSV** администратор может скачать отфильтрованные данные журнала в csv-файл для дальнейшего анализа.

Нажатие на кнопку **Показать** выведет окно с подробным описанием события.

Documentation: ☒
Product: UGMC
Version: 7.x

Функция экспорта журналов UserGate позволяет выгружать информацию на внешние серверы для последующего анализа или для обработки в системах SIEM (Security information and event management).

Поддерживается отправка журналов на серверы SSH (SFTP), FTP и Syslog. Отправка на серверы SSH и FTP проводится по указанному в конфигурации расписанию или разово (кнопка **Послать разово**). Отправка на серверы Syslog происходит сразу же при добавлении записи в журнал.

Для отправки журналов необходимо в режиме администратора устройства создать правила экспорта журналов в разделе **Журналы и отчеты → Экспорт журналов**.

ПримечаниеНастройки экспорта журналов не являются кластерными. Если UGMC работает в кластерной конфигурации, правила экспорта журналов создаются отдельно на каждом узле.

При создании конфигурации требуется указать следующие параметры:

Наименование	Описание
Название правила	Название правила экспорта журналов.
Описание	Оptionальное поле для описания правила.
Журналы для экспорта	Выбор файлов журналов, которые необходимо экспортировать: - Журнал событий. Для каждого из журналов возможно указать синтаксис выгрузки: - CEF — Common Event Format (ArcSight). - JSON — JSON format. @CEE: JSON — CEE Log Syntax (CLS) Encoding JSON. Обратитесь к документации на используемую у вас систему SIEM для выбора необходимого формата выгрузки журналов. Подробное описание форматов журналов читайте в приложении Описание форматов журналов.
Тип сервера	SSH (SFTP), FTP, Syslog.
Адрес сервера	IP-адрес или доменное имя сервера.
Транспорт	Только для типа серверов Syslog — TCP или UDP.
Порт	Порт сервера, на который следует отправлять данные.
Протокол	Только для типа серверов Syslog — RFC5424 или BSD syslog RFC 3164. Выберите протокол, совместимый с используемой у вас системой SIEM.
Критичность	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: Тревога: состояние, требующее незамедлительного вмешательства. Критическая: состояние, требующее незамедлительного вмешательства либо предупреждающее о сбое в системе. Ошибки: в системе возникли ошибки. Предупреждения: предупреждения о возможном возникновении ошибок, если не будут предприняты никакие действия. Уведомительная: события, которые относятся к необычному поведению системы, но не являются ошибками. Информативная: информационные сообщения.

Наименование	Описание
Facility	Только для типа серверов Syslog. Необязательное поле, проконсультируйтесь с документацией на используемую у вас систему SIEM. Возможны следующие значения: • Сообщения пользовательские. • Системный сервис. • Безопасность/авторизация. • Аудит. • Тревога. • Local 0. • Local 1. • Local 2. • Local 3. • Local 4. • Local 5. • Local 6. • Local 7.
Имя хоста	Только для типа серверов Syslog. Уникальное имя хоста, идентифицирующее сервер, отправляющий данные на сервер syslog, в формате Fully Qualified Domain Name (FQDN).
App-Name	Только для типа серверов Syslog. Уникальное имя приложения, которое отправляет данные на сервер syslog.
Логин	Имя учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Пароль	Пароль учетной записи для подключения к удаленному серверу. Не применяется к методу отправки Syslog.
Путь на сервере	Каталог на сервере для копирования файлов журналов. Не применяется к методу отправки Syslog. В кластерной конфигурации UGMC при экспорте журналов с разных узлов кластера необходимо указывать разные каталоги на сервере для каждого узла UGMC, поскольку имена файлов журналов на каждом узле идентичны.
Расписание	Выбор расписания для отправки логов. Не применяется к методу отправки Syslog. Возможны варианты: • Ежедневно. • Еженедельно. • Ежемесячно • Каждые ... часов. • Каждые ... минут. • Задать вручную. При задании вручную необходимо использовать crontab-подобный формат, при котором строка выглядит как шесть полей, разделенных пробелами. Поля задают время в следующем виде: (минуты: 0-59) (часы: 0-23) (дни месяца: 1-31) (месяц: 1-12) (день недели: 0-6, 0-воскресенье). Каждое из первых пяти полей может быть задано следующим образом: • Звездочка (*) — обозначает весь диапазон (от первого до последнего). • Дефис (-) — обозначает диапазон чисел. Например, "5-7" будет означать 5,6 и 7. • Списки. Это числа (или диапазоны), разделенные запятыми. Например, "1,5,10,11" или "1-11,19-23". • Звездочка или диапазон с шагом. Используется для пропусков в диапазонах. Шаг указывается после косой черты. Например, "2-10/2" будет значить "2,4,6,8,10", а выражение "*" / 2 в поле "часы" будет означать "каждые два часа".

Наименование	Описание
Управление журналами	Управление временными файлами журналов, подготавливаемых для отправки на удаленные серверы ssh и ftp. При отправке журналов на сервера ssh и ftp UserGate сохраняет данные для отправки во временных файлах в кодировке UTF-8. Журналы за предыдущие дни (по количеству дней ротации) хранятся в виде архивов, журнал за текущий день не архивирован. По указанному расписанию все созданные для отправки файлы копируются на удаленный сервер, при этом файлы не очищаются и не удаляются. Данная настройка позволяет указать период ротации временных файлов (в днях) или удалить любой из временных файлов вручную. Ротация файлов происходит один раз в сутки.

Примечание Возможно сохранение журнала администратором вручную непосредственно из веб-консоли. При этом данные сохраняются только в формате CSV.

Режим расширенного поиска

Documentation: ☒

Product: UGMC

Version: 7.x

Объем данных, регистрируемых в журналах, как правило, значителен, поэтому в стандартном режиме просмотра отображается лишь часть доступных полей. Для быстрого доступа к необходимой информации в UserGate MC предусмотрены средства поиска и фильтрации журналов. Поиск может выполняться как в простом, так и в расширенном режиме.

В режиме простого поиска фильтрация записей осуществляется с помощью графического интерфейса. Настройка условий поиска выполняется в удобной форме и не требует знания специальных команд или синтаксиса.

Для создания более сложных условий отбора предназначен режим расширенного поиска, использующий специализированный язык запросов. В этом режиме доступны поля журналов, которые не отображаются и не могут использоваться в стандартном режиме поиска. Запросы формируются с использованием имен полей, их значений, ключевых слов и логических операторов. Значения, содержащие пробелы, необходимо заключать в одинарные (' ') или двойные (" ") кавычки. Для значений без пробелов кавычки не требуются. Для объединения и группировки нескольких условий в запросе можно использовать круглые скобки.

Ключевые слова отделяются пробелами и могут быть следующими:

Ключевые поля	Значение
AND или and	Логическое «И», требует выполнение всех условий, заданных в запросе
OR или or	Логическое «ИЛИ», требует выполнение одного из условий запроса

Операторы определяют условия фильтра и могут быть следующими:

Оператор	Значение
=	Равно — требует полного совпадения значения поля с указанным значением. Пример: ip = 172.16.31.1. Будут отображены все записи журнала, в которых поле ip будет точно соответствовать значению 172.16.31.1
!=	Не равно — значение поля не должно совпадать с указанным значением. Пример: ip != 172.16.31. Будут отображены все записи журнала, в которых поле ip не будет равно значению 172.16.31.1
<=	Меньше либо равно — значение поля должно быть меньше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date <= '2019-03-28T20:59:59' AND statusCode = 303
>=	Больше либо равно — значение поля должно быть больше или равно указанному в запросе значению. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date >= "2019-03-13T21:00:00" AND statusCode = 200
<	Меньше — значение поля должно быть меньше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: date < '2019-03-28T20:59:59' AND statusCode = 404
>	Больше — значение поля должно быть больше указанного в запросе значения. Оператор применим для полей, поддерживающих сравнение. Например, поля даты, portSource, portDest, statusCode и т. п. Пример: (statusCode > 200 AND statusCode < 300) OR (statusCode = 404)
IN	Позволяет указать в запросе несколько значений поля. Список значений необходимо заключать в круглые скобки. Пример: category IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category')

Оператор	Значение
NOT IN	Позволяет указать в запросе несколько значений поля. Будут отображены записи, в которых значение поля не совпадает ни с одним из указанных. Список значений необходимо заключать в круглые скобки. Пример: category NOT IN (botnets, compromised, 'illegal software', 'phishing and fraud', 'reputation high risk', 'unknown category')
~	Содержит — позволяет указать подстроку, которая должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser ~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
!~	Не содержит — позволяет указать подстроку, которая не должна присутствовать в значении выбранного поля. Поиск выполняется без учета регистра. Пример: browser !~ "Mozilla/5.0". Оператор применяется только к полям, содержащим строковые значения
MATCH	Поиск по полю с помощью регулярного выражения. Будут показаны только те записи, в которых значение поля соответствует заданному шаблону. Пример: details MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details найдется слово «NAT»
NOT MATCH	Поиск записей, в которых значение поля не совпадает с заданным регулярным выражением. Будут показаны только те записи, в которых значение поля не соответствует заданному шаблону. Пример: details NOT MATCH NAT — будут отфильтрованы все записи журнала, в которых в проверяемом поле details не найдется слово «NAT»

При формировании запроса в режиме расширенного поиска UserGate MC предлагает варианты названий полей, допустимых операторов и возможных значений. Это упрощает создание сложных поисковых выражений и снижает вероятность ошибок при вводе. Набор доступных полей и перечень допустимых значений зависят от типа просматриваемого журнала.

При переходе из режима простого поиска в режим расширенного поиска UserGate MC автоматически преобразует заданные параметры фильтрации в строку запроса, соответствующую условиям, указанным в базовом режиме. Вы можете продолжить формирование строки поиска с использованием расширенных возможностей языка запросов без необходимости повторного ввода критериев отбора.

Documentation: ☒
Product: UGMC
Version: 7.x

Формат журнала событий

CEF

Тип поля	Название поля	Описание	Пример значения
CEF заголовок	CEF:Version	Версия CEF.	CEF:0
	Device Vendor	Производитель продукта.	UserGate
	Device Product	Тип продукта.	NGFW
	Device Version	Версия продукта.	7
	Source	Тип журнала.	events
	Origin	Модуль, в котором произошло событие.	admin_console
	Severity	Важность события.	Может принимать значения: • 0 — информационные. • 6 — предупреждения. • 8 — ошибки. • 10 — критичные.
CEF [расширение]	rt	Время, когда было получено событие: миллисекунды с 1 января 1970 года.	1652344423822
	deviceExternalId	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einsonstal
	suser	Имя пользователя.	Administrator (Admin)
	cat	Компонент, в котором произошло событие.	console_auth
	act	Тип события.	administrator_login
	src	IPv4-адрес источника.	192.168.117.254
	cs1Label	Поле используется для указания деталей события.	Attributes
	cs1	Детали события в формате JSON.	{"login":"ex_admin","realm_id":"31d8fcb6-e51d-4e3f-b799-181d31a45b06"}

JSON

Название поля	Описание	Пример значения
user	Имя пользователя.	Admin

Название поля	Описание	Пример значения
timestamp	Время получения события в формате: уууу-mm-ddThh:mm:ssZ.	2022-05-12T08:11:46.15869Z
ip_address	IPv4-адрес источника события.	192.168.174.134
node	Имя, которое однозначно идентифицирует устройство, генерирующее это событие.	mc_core@einsonstal
attributes	Детали события в формате JSON.	{"rule":{"logrotate":12,"attributes":{"timezone":"Asia/Novosibirsk"},"id":"66f9de9f-d698-4bec-b3b0-ba65b46d3608","name":"Example log export ftp"}
event_type	Тип события.	logexport_rule_updated
event_severity	Важность события.	info (информационные), warning (предупреждения), error (ошибки), critical (критичные).
event_origin	Модуль, в котором произошло событие.	core
event_component	Компонент, в котором произошло событие.	console_auth

