



MAKVES

Руководство администратора

www.makves.ru

Оглавление

О платформе Makves.....	3
Об инцидентах информационной безопасности	3
Об анализе объектов корпоративной сети	4
Аппаратно-программные требования.....	5
Аппаратные требования	5
Программные требования.....	5
Развертывание платформы Makves в корпоративной сети	6
Интерфейс веб-консоли.....	8
Инциденты информационной безопасности	10
Регистрация инцидентов	10
Управление зарегистрированными инцидентами.....	11
Настройки инцидентов	14
О статусах инцидентов.....	14
О категориях инцидентов	15
О сценариях реагирования.....	16
О метках	17
О полях	19
О скриптах	19
Объекты.....	21
Получение данных	21
Экспорт пользователей, групп и компьютеров из Active Directory...	21
Сбор данных о файлах в папке.....	23
Сбор событий из журналов событий (Event Log) с удаленных рабочих компьютеров	25

Экспорт списка почтовых ящиков из Microsoft Exchange	28
Анализ пользователей и групп.....	28
Анализ компьютеров	29
Анализ файлов.....	30
Анализ почтовых ящиков.....	31
Анализ событий	31
Учетные записи и уведомления.....	33

О платформе Makves

Уважаемый пользователь!

Вы читаете руководство администратора платформы реагирования на инциденты информационной безопасности Makves (далее платформа Makves).

Платформа Makves – это инструмент для сбора и анализа информации об инцидентах информационной безопасности (ИБ). Платформа состоит из веб-консоли, программной части и базы данных.

В этом руководстве вы найдете ответы на вопросы о разворачивании платформы Makves, об интерфейсе веб-консоли, о регистрации и обработке инцидентов ИБ, о возможностях анализа данных, которая предоставляет платформа, и о средствах уведомления об инцидентах ИБ.

Об инцидентах информационной безопасности

Инциденты ИБ – это любые инциденты в корпоративной сети, которые прямо или косвенно влияют на безопасность инфраструктуры компании (например, несанкционированный доступ на периферийные устройства, компрометация учетных данных пользователя, неработоспособность оборудования или заражение зловредным ПО). Зачастую количество инцидентов настолько велико, что обработка потока данных требует значительных ресурсов и больше не может быть выполнена без применения специализированных решений.

Платформа Makves предназначена для фиксации, категоризации и обработки инцидентов ИБ. С помощью платформы Makves вы можете назначать инцидентам ИБ статусы решения, сотрудников, ответственных за решение инцидента и инспекторов, которые могут отслеживать как скорость, так и качество решения инцидентов ИБ. Кроме того, платформа Makves позволяет внедрять автоматизацию ответов на инциденты безопасности с помощью скриптов.

Об анализе объектов корпоративной сети

Администрирование корпоративных сетей, даже небольших, является непростой задачей. Необходимость постоянного анализа состояния объектов корпоративной инфраструктуры, таких как компьютеры, почтовые ящики, пользователи и события приводит к естественному выводу о необходимости автоматизированного решения для обработки и анализа потока данных.

Платформа Makves предоставляет интерфейс, в котором вы можете обрабатывать и анализировать не только количественные и качественные показатели объектов корпоративной инфраструктуры. С помощью платформы вы можете анализировать и оценивать риски для пар объектов, например, пользователи и файлы, пользователи и почтовые ящики.

Аппаратно-программные требования

Аппаратные требования

- Процессор Intel Core i5
- Оперативная память (ОЗУ): 8 GB
- Свободное место на жестком диске: 10 GB

Программные требования

Поддерживаемые операционные системы:

- Windows 10
- Windows Server 2016
- Windows Server 2019
- OS X 10.9 – 10.11
- macOS 10.14 и выше
- Ubuntu 16 LTS (Xenial Xerus)
- Ubuntu 18 LTS (Bionic Beaver)

Дополнительное программное обеспечение:

- Браузер Chrome.
- Для операционных систем Windows:
 - a. Docker Desktop 18 или выше для Windows 10, Docker Enterprise для Windows Server.
 - b. Система управления базами данных (СУБД) PostgreSQL (при установке из MSI-файла).
- Для операционных систем macOS: Docker 18.*.
- Для операционных систем Linux:
 - a. Docker 18.*.
 - b. docker-compose 3.6 или выше.

Внимание! Для работы платформы Makves требуется доступ в интернет.

Развертывание платформы Makves в корпоративной сети

Платформа Makves может быть установлена на устройства под управлением операционных систем Windows, macOS, Linux.

Установка с помощью Docker Desktop на Windows

1. Загрузите и установите программу Docker Desktop для Windows.

Внимание! При установке следует выбрать режим Linux-контейнеров.

2. Создайте рабочую папку (например, C:\Users\Admin\Documents\IRP).
3. Скопируйте в нее файл docker-compose.yml.
4. Откройте командную строку от имени администратора, перейдите в рабочую папку (`cd C://Users/Documents/IRP`) и выполните следующие команды:
 - a. `docker-compose pull` для загрузки последней версии платформы Makves.
 - b. `docker-compose up` для запуска платформы Makves.

После запуска веб-консоль будет доступна по адресу <http://localhost:8000>. По умолчанию для входа в веб-консоль используются имя пользователя и пароль admin/admin.

Установка с помощью Docker на macOS

1. Загрузите и установите программу Docker для macOS.
2. Создайте рабочую папку (например, /Users/Admin/Documents/IRP).
3. Скопируйте в нее файл docker-compose.yml.
4. В командной строке перейдите в рабочую папку (`cd /Users/Admin/Documents/IRP`) и выполните следующие команды:

- c. `docker-compose pull` для загрузки последней версии платформы Makves.
- d. `docker-compose up` для запуска платформы Makves.

После запуска веб-консоль будет доступна по адресу <http://localhost:8000>. По умолчанию для входа в веб-консоль используются имя пользователя и пароль `admin/admin`.

Установка на Windows из MSI-файла

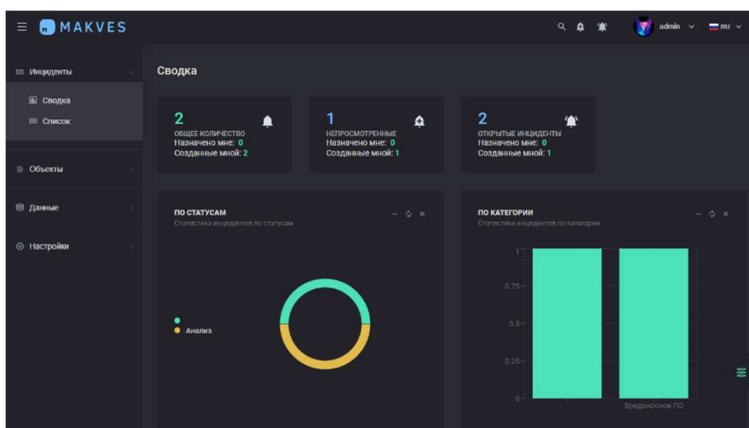
Внимание! На компьютере должна быть установлена СУБД PostgreSQL.

1. Двойным щелчком мыши запустите файл `makves.msi` и установите программу.
2. Создайте пустую базу данных в СУБД PostgreSQL.
3. Измените настройки подключения к СУБД PostgreSQL в конфигурационном файле в папке установки программы.
4. Зарегистрируйте `makves_` как сервис с помощью команды `makves install`.
5. Запустите службу `makves`.

Интерфейс веб-консоли


Интерфейс веб-консоли (см. Изображение 1) состоит из следующих элементов:

- **Основное меню.** Плавающее меню, которое содержит основные разделы веб-консоли. Может быть свернуто или перемещено в панель инструментов. По умолчанию расположено в левой части экрана.
- **Рабочая область.** Область, изменяющаяся в зависимости от выбранного раздела. В рабочей области могут отображаться сводка зарегистрированных инцидентов и добавленных объектах, окна регистрации новых инцидентов и добавления объектов и другие инструменты. Рабочая область занимает большую часть экрана.
- **Панель инструментов.** Панель, которая содержит дополнительные инструменты для управления инцидентами и объектами, включая поиск, оповещение о новых и назначенных инцидентах, а также средства переключения учетных записей и языка системы. Панель расположена в верхней части экрана.
- **Панель управления видом консоли.** Панель содержит инструменты управления основным меню и темой веб-консоли.




Изображение 1 Интерфейс

Изменение положения основного меню

1. Нажмите на кнопку  в левом нижнем углу.
2. Выполните одно из следующих действий:
 - a. Переведите переключатель **Свернутое меню** в положение ВКЛ или ВЫКЛ, чтобы свернуть или развернуть основное меню.
 - b. Переведите переключатель **Меню сверху** в положении ВКЛ или ВЫКЛ, чтобы переместить основное меню в верхнюю часть экрана или вернуть меню в левую часть экрана.

*Внимание! Если переключатель **Меню сверху** включен, основное меню нельзя свернуть.*

Переход на светлую тему

1. Нажмите на кнопку  в левом нижнем углу.
2. Переведите переключатель **Темная тема** в состояние ВЫКЛ.

Инциденты информационной безопасности

Этот раздел содержит информацию о том, как регистрировать инциденты ИБ в веб-консоли и управлять зарегистрированными инцидентами. Кроме того, в этом разделе содержится информация о создании категорий, статусов, сценариев реагирования и меток для инцидентов.

Регистрация инцидентов

Вы можете регистрировать инциденты вручную или импортировать из существующей базы данных инцидентов, используя запросы REST API.

Регистрация инцидента

3. В боковом меню выберите пункт **Инциденты > Список**.
4. В правом верхнем углу рабочей области нажмите на кнопку **Зарегистрировать**.
Откроется окно, в котором вы можете зарегистрировать новый инцидент.
5. В выпадающем меню **Категория** выберите категорию инцидента.
6. В выпадающем меню **Сценарий** выберите сценарий реагирования на инцидент.
7. В выпадающем меню **Приоритет** выберите приоритет инцидента.
8. В выпадающем меню **Статус** выберите статус инцидента.
9. В выпадающем меню **Ответственный** выберите лицо, ответственное за решение инцидента.
10. В поле **Тема** введите краткую информацию об инциденте.
11. В поле **Описание** введите подробную информацию об инциденте.
12. Нажмите на кнопку **Создать**.

Инцидент будет зарегистрирован в базе данных.

Импорт инцидентов из базы данных

Вы можете использовать запрос со следующим синтаксисом:

```
POST /incident/ HTTP/1.1
Host: localhost:8000
Content-Type: application/json
Authorization: Basic YWRtaW46YWRtaW4=
cache-control: no-cache
Postman-Token: 66c89571-101d-4247-b3b1-2d50e43b6d0b
{
  "assignee": "test_admin@gmail.com",
  "body": "<p>Текст</p>",
  "category": "8",
  "playbook": "0",
  "priority": "3",
  "state": "3",
  "title": "Вирус"
```

Управление зарегистрированными инцидентами

В этом разделе дается информация о том, как просматривать сводные данные о зарегистрированных инцидентах, а также о том, как изменять параметры, просматривать историю и добавлять комментарии в зарегистрированные инциденты.

Просмотр сводной информации об инцидентах

В боковом меню выберите пункт **Инциденты > Сводка**.

Откроется окно с краткой информацией об инцидентах, зарегистрированных в базе данных.

В этом окне вы сможете найти следующие данные об инцидентах:

- Общее количество инцидентов в системе.
- Количество инцидентов, решение которых назначено текущей учетной записи.
- Количество инцидентов, созданных с текущей учетной записи.
- Общее количество инцидентов, которые не были рассмотрены текущей учетной записью.
- Количество нерассмотренных инцидентов, решение которых назначено текущей учетной записи.
- Количество не просмотренных инцидентов, созданных с текущей учетной записи.
- Общее количество открытых инцидентов.
- Количество открытых инцидентов, решение которых назначено текущей учетной записи.
- Количество открытых инцидентов, созданных с текущей учетной записи.
- Графики по статусам, категориям, меткам, приоритету и лицам, ответственным за решение, для всех инцидентов, зарегистрированных в базе данных.

Просмотр инцидентов в виде списка

1. В боковом меню выберите пункт **Инциденты > Список**.

Откроется список инцидентов, имеющихся в базе данных.

2. Выполните следующие действия:


- Нажмите на кнопку **Назначено мне**, чтобы просмотреть все инциденты, назначенные текущей учетной записи.
- Нажмите на кнопку **Создано мной**, чтобы просмотреть все инциденты, созданные текущей учетной записью.
- Нажмите на кнопку **Открытые**, чтобы просмотреть все открытые инциденты.
- В раскрывающемся **Важность** выберите один из типов приоритета, чтобы просмотреть все инциденты, которые относятся к этому типу.


- В раскрывающемся списке **Статус** выберите одно из состояний инцидента, чтобы просмотреть все инциденты, которые относятся к этому состоянию.
- В раскрывающемся списке **Метка** выберите одну из меток, чтобы просмотреть все инциденты, которые помечены этой меткой.

Просмотр инцидентов в виде таблицы

1. В боковом меню выберите пункт **Инциденты > Список**.

Откроется список инцидентов, имеющихся в базе данных.

2. В верхнем правом углу нажмите на кнопку .

Кнопка изменится на  и список инцидентов будет отображен в виде таблицы. Чтобы вернуться к виду по умолчанию, нажмите на кнопку еще раз.

Просмотр и изменение информации об инциденте

1. В боковом меню выберите пункт **Инциденты > Список**.

Откроется список инцидентов, имеющихся в базе данных.

2. Нажмите на инцидент в списке.

Откроется окно изменения инцидента.

3. Выполните следующие действия:

- Перейдите на закладку **Описание**, чтобы просмотреть или изменить информацию об инциденте, предоставленную лицом, зарегистрировавшим инцидент.
- Перейдите на закладку **Комментарий**, чтобы просмотреть комментарии лиц, ответственных за решение инцидента, или добавить свой комментарий.
- Перейдите на закладку **Активность**, чтобы просмотреть историю работы с инцидентом.
- Перейдите на закладку **Файлы**, чтобы добавить или загрузить файлы, прикрепленные к инциденту.

- Перейдите на закладку **Объекты**, чтобы добавить пользователя, компьютер, файл или событие, связанные с инцидентом.
- Перейдите на закладку **Инструкции**, чтобы ознакомиться с действиями, которые необходимо выполнить для решения инцидента.

Настройки инцидентов

В комплекте поставки платформы Makves присутствует файл settings.json с настройками по умолчанию. При первоначальном развертывании платформы рекомендуется загрузить настройки по умолчанию из этого файла.

Загрузка файла settings.json с настройками по умолчанию

1. В боковом меню выберите пункт **Данные > Загрузка**.
2. Выполните одно из следующих действий:
 - Перетащите файл settings.json в поле **Загрузить файлы с данными**.
 - Нажмите на кнопку **Загрузить** и выберите файл settings.json.

Настройки по умолчанию будут применены.

О статусах инцидентов

Статусы инцидентов предназначены для отслеживания текущего этапа работ по разрешению инцидента. Вы можете добавлять свои статусы, чтобы детализировать процесс, и фильтровать инциденты по текущему состоянию. Например, вы можете добавить статусы *Зарегистрирован*, *В работе*, *Работа завершена*.

Создание статусов инцидентов

1. В боковом меню выберите пункт **Настройки > Инциденты > Статусы**.
Откроется список статусов, которые можно присвоить инциденту. По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.
Откроется окно, в котором вы можете добавить детали нового статуса.

3. Выполните следующие действия:

- с. В поле **Имя** введите название статуса.
- d. В поле **Описание** добавьте описание статуса.
- e. В списке **Цвет** выберите цвет, который будет соответствовать статусу.
- f. Установите флажок **Конец обработки**, если этот статус означает, что инцидент закрыт.

4. Нажмите на кнопку **Создать**.

Статус будет добавлен в список статусов, а также станет доступен при создании и изменении инцидентов.

Изменение статуса инцидента

1. В боковом меню выберите пункт **Инциденты > Список**.
Откроется список инцидентов, имеющихся в базе данных.
2. Нажмите на инцидент в списке.
Откроется окно изменения инцидента.
3. В списке **Статус** выберите статус, который вы хотите установить инциденту.

О категориях инцидентов

Категории инцидентов служат для разделения группы инцидентов по общему признаку.

Добавление категорий инцидентов

1. В боковом меню выберите пункт **Настройки > Инциденты > Категории**.
Откроется список категорий, которые можно присвоить инциденту.
По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.

Откроется окно, в котором вы можете добавить детали новой категории.

3. Выполните следующие действия:

- a. В поле **Имя** введите название категории.
- b. В поле **Описание** добавьте краткую информацию о категории.
- c. В списке **Приоритет по умолчанию** выберите приоритет, который будет автоматически присваиваться инциденту при выборе категории.
- d. В списке **Ответственный по умолчанию** выберите лицо, ответственное за решение инцидента, которое будет автоматически назначено при выборе категории.
- e. В поле **Инструкции** добавьте список действий, который нужно выполнить ответственному лицу для решения инцидента. При необходимости использовать язык гипертекстовой разметки установите флажок **Редактировать как HTML**.

4. Нажмите на кнопку **Создать**.

Категория будет добавлена в список категорий, а также станет доступна при создании и изменении инцидентов.

О сценариях реагирования

Сценарии реагирования – это набор инструкций, которые должен выполнить ответственный за решение инцидента.

Вы можете создавать сценарии реагирования и назначать их инцидентам.

Создание сценария реагирования

1. В боковом меню выберите пункт **Настройки > Инциденты > Сценарии реагирования**.

Откроется список сценариев реагирования на инциденты. По умолчанию список пуст.

2. В правом верхнем углу рабочей области нажмите на кнопку **Создать**.

Откроется окно, в котором вы можете добавить детали нового сценария.

3. Выполните следующие действия:

- a. В поле **Имя** введите название сценария реагирования.
- b. В поле **Описание** добавьте краткую информацию о сценарии реагирования.
- c. В списке **Действие** выберите действие, которое необходимо выполнить в сценарии реагирования.
- d. В списке **Поля** выберите поля, которые соответствуют сценарию реагирования.
- e. В списке **Для категории** выберите категорию, при выборе которой сценарий реагирования будет автоматически назначен инциденту.
- f. В поле **Инструкции** добавьте информацию о действиях, которые необходимо выполнить для решения инцидента. При необходимости использовать язык гипертекстовой разметки установите флажок **Редактировать как HTML**.

4. Нажмите на кнопку **Создать**.

Сценарий реагирования будет добавлен в список сценариев, а также станет доступен при изменении существующих инцидентов.

О метках

Для дифференциации зарегистрированных инцидентов вы можете добавлять *метки*. Метки – это дополнительный инструмент для быстрого добавления и получения информации об инциденте. Метки выглядят как разноцветные области с поясняющим текстом и отображаются в списке инцидентов.

Вы можете создать набор меток (например, *Под контролем СИБ*, *Под контролем генерального директора*) разных цветов.



Создание меток

1. В боковом меню выберите пункт **Настройки > Метки**.
Откроется список меток. По умолчанию список пуст.
2. Нажмите на кнопку **Создать**.
Откроется окно, в котором вы можете добавить детали новой метки.
3. В поле **Имя** введите название новой метки.
4. В поле **Описание** добавьте информацию о метке.
5. В списке **Цвет** выберите цвет метки.
6. Нажмите на кнопку **Создать**.

Метка будет добавлена в список меток, а также станет доступна при изменении инцидентов.

Вы можете добавлять метки существующим инцидентам.

Добавление меток для инцидента

1. В боковом меню выберите пункт **Инциденты > Список**.
2. Нажмите на инцидент в списке.
Откроется окно изменения инцидента.
3. Нажмите на кнопку **Установить метки** .
Откроется диалоговое окно со список меток.
4. Установите флажок рядом с нужными метками.
5. Закройте диалоговое окно нажатием на любую часть рабочей области.
6. Чтобы добавить или удалить метки, в окне изменения инцидента нажмите на кнопку  и установите/снимите флажки рядом с имеющимися метками.

Добавленные метки отображаются в списке инцидентов.

О полях

Вы можете добавлять поля, которые необходимо заполнить при выполнении инструкций сценария реагирования.

Добавление поля

1. В боковом меню выберите пункт **Настройки > Поля**.
Откроется окно со списком полей.
2. Нажмите на кнопку **Создать**.
Откроется окно, в котором вы можете добавить новый скрипт.
3. В поле **Имя** укажите название поля.
4. В поле **Описание** добавьте подробную информацию о поле.
5. В поле **Ключ** укажите значение, которое будет использовано при формировании запросов.
6. В раскрывающемся списке **Тип** выберите один из доступных форматов полей.
7. Вы можете указать текстовый (**Строка**) или числовой (**Число**) формат.

Поля, имеющиеся в базе данных, становятся доступны при создании сценария реагирования.

О скриптах

Вы можете добавлять скрипты, которые будут автоматически выполняться при решении инцидентов. Платформа Makves позволяет выполнять скрипты, написанные на Javascript, Python, Bash, PowerShell.

Добавление скрипта

1. В боковом меню выберите пункт **Настройки > Скрипты**.
Откроется окно со списком скриптов.
2. Нажмите на кнопку **Создать**.
Откроется окно, в котором вы можете добавить новый скрипт.

3. Выполните следующие действия:
4. В поле **Имя** укажите название скрипта.
5. В поле **Описание** добавьте подробную информацию о скрипте.
6. В раскрывающемся списке **Язык скрипта** выберите синтаксис кода скрипта.
7. В раскрывающемся списке **Применяется для** выберите объект, при появлении которого применяется скрипт.

Вы можете добавить скрипты для следующих объектов: пользователь, компьютер, группа, файл или событие.

8. В поле **Содержание** добавьте код скрипта.

Объекты

Платформа Makves позволяет анализировать данные о пользователях, файлах компьютерах и событиях в корпоративной сети.

Получение данных

Данные, которые требуется загрузить в базу данных платформы Makves для дальнейшего анализа, могут быть загружены в виде файлов JSON или в виде файлов журналов в формате EVTХ.

Добавление файлов JSON или EVTХ в базу данных

1. В боковом меню выберите пункт **Данные > Загрузка**.
2. Выполните одно из следующих действий:
 - Перетащите файл с данными в поле **Загрузить файлы с данными**.
 - Нажмите на кнопку **Загрузить** и выберите нужный файл.

Данные будут загружены в базу данных платформы Makves.

Для сбора данных требуется использовать скрипты Microsoft PowerShell, предоставляемые компанией Makves.

Экспорт пользователей, групп и компьютеров из Active Directory

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

Внимание! Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1

Пример запуска команды:

```
powershell.exe -ExecutionPolicy Bypass -Command ".\export-ad.ps1" -base DC=acme``,DC=local -server dc.acme.local -outfilename export-ad
```

Параметры		
Название параметра	Обязателен	Назначение
base	Да	Корневое подразделение (Organizational unit) в Active Directory, из которого будут экспортированы данные о пользователях, группах и компьютерах.
server	Да	Имя контроллера домена.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
outfilename	Да	Файл, в который будут записаны полученные данные.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права на чтение данных из Active Directory.

Сбор данных о файлах в папке

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

Внимание! Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1

Пример запуска команды без выделения текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-  
folder.ps1" -folder "c:\\work\\test" -outfilename folder_test
```

Пример запуска команды с выделением текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-  
folder.ps1" -folder "c:\\work\\test" -outfilename folder_test -  
extract
```

Пример запуска команды для сбора данных обо всех папках общего доступа с компьютеров, зарегистрированных в указанном подразделении (OU) без выделения текста:

```
powershell.exe -ExecutionPolicy Bypass -Command "./explore-  
folder.ps1" -base DC=acme``,DC=local -server dc.acme.local -  
outfilename folder_test
```


Параметры		
Название параметра	Обязателен	Назначение
folder	Да	Локальная или сетевая папка для сбора данных.
base	Нет	Корневое подразделение (Organizational unit) в Active Directory для получения списка компьютеров, с которых будут собраны файлы.
server	Нет	Имя контроллера домена для получения списка компьютеров, с которых будут собраны файлы.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
outfilename	Да	Файл, в который будут записаны полученные данные.
extract	Нет	Извлечение текста из файлов DOC, DOCX, XLS, XSLX.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права на чтение инспектируемых файлов и папок и на чтение данных из Active Directory.

Сбор событий из журналов событий (Event Log) с удаленных рабочих компьютеров

Требования для использования:

- Windows 7 или более поздние версии.
- Windows Server 2012 или более поздние версии.
- Windows PowerShell 5 или более поздние версии.
- Remote Server Administration Tools для соответствующей версии ОС.

Внимание! Рекомендуется использовать Windows 10.1803 x64 или более поздние версии, Windows Server 2019 и Windows PowerShell 5.1

Пример запуска команды для сбора всех типов событий с компьютера dc.acme.local

powershell.exe -ExecutionPolicy Bypass -Command "./export-events.ps1" -Computers dc.acme.local

Пример запуска команды для сбора событий типа Logon с компьютера dc.acme.local

powershell.exe -ExecutionPolicy Bypass -Command "./export-events.ps1" -Computers dc.acme.local -Target Logon

Параметры		
Название параметра	Обязателен	Назначение
computers	Да	Список компьютеров, с которых будут собраны записи журналов событий.
target	Да	Типы собираемых событий.
outfilename	Нет	Файл, в который будут записаны полученные данные.
user	Нет	Пользователь, от чьего имени выполняется запрос.
pwd	Нет	Пароль пользователя, от чьего имени выполняется запрос.
fwd	Нет	Имя журнала, использованного при форвардинге.
start	Нет	Временная точка, начиная с которой собираются события. Формат: ууууММддННммсс
count	Да	Количество собираемых событий. По умолчанию собирается 3000 событий.

Типы событий	
Название параметра	Тип
All	Все возможные типы событий.
Logon	События, возникающие при попытке аутентификации.

Service	События, возникающие при управлении службами.
User	События, возникающие при управлении учетными данными пользователей.
Computer	События, возникающие при управлении учетными данными компьютеров.
Clean	События, возникающие при очистке журналов.
File	События, возникающие при обращении пользователей к файлам.
MSSQL	События, возникающие при работе Microsoft SQL Server.
RAS	События, возникающие при удаленном подключении пользователей.
USB	События, возникающие при работе с USB-устройствами.
Sysmon	События, возникающие при функционировании System Monitor.
TS	События, возникающие при работе Windows Terminal Services.

Если параметр user не задан, после запуска команды появится окно с запросом учетных данных для доступа к контроллеру домена. Для корректной работы команды пользователь, чьи учетные данные используются при выполнении запроса, должен иметь права чтения журналов событий Event Log.

Экспорт списка почтовых ящиков из Microsoft Exchange

Требования для использования:

Запуск команды следует осуществлять из Windows PowerShell ISE с включенным Exchange Management Shell.

Пример запуска команды для экспорта списка почтовых ящиков

```
".\export_mb_folders.ps1" -outfile mailboxes
```

Параметры		
Название параметра	Обязателен	Назначение
outfile	Да	Файл, в который будут записаны полученные данные.

Анализ пользователей и групп

Вы можете просмотреть информацию о пользователях, собранную с помощью скрипта export-ad.ps1, выбрав пункт бокового меню **Объекты > Пользователи**.

В верхней части рабочей области представлена сводная информация об общем количестве пользователей, включая отключенных и неактивных, о количестве групп пользователей и возможных рисках, которые обнаружены в результате анализа.

В нижней части рабочей области представлен список пользователей в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Аватар** – фотография пользователя.
- **Имя** – идентификатор пользователя в домене.
- **Домен** – название домена, с которого получена информация о пользователе.
- **Email** – почтовый адрес пользователя.

- **Риск-фактор** – информация о потенциальных рисках, которые платформа Makves обнаружила при анализе пользователя.
- **Телефон** – контактный номер телефона.
- **Аккаунт** – имя пользователя учетной записи, которое закреплено за пользователем в домене.
- **Принципал** – уникальное имя пользователя для аутентификации в домене.
- **NT-имя** – имя пользователя в NT-домене.
- **Последний логон** – время последнего входа пользователя в учетную запись.
- **Количество входов** – сколько раз пользователь входил в учетную запись.

Анализ компьютеров

Вы можете просмотреть информацию о компьютерах, собранную с помощью скрипта export-ad.ps1, выбрав пункт бокового меню **Объекты > Компьютеры**.

В верхней части рабочей области представлена сводная информация об общем количестве компьютеров, включая отключенные и неактивные, о количестве групп компьютеров и возможных рисках, которые обнаружены в результате анализа.

В нижней части рабочей области представлен список компьютеров в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Домен** – название домен, к которому принадлежит компьютер.
- **Имя** – имя компьютера в домене.
- **Операционная система** – операционная система, установленная на компьютере.
- **Версия ОС** – версия операционной системы, установленной на компьютере.
- **Риск-фактор** – информация о потенциальных рисках, которые платформа Makves обнаружила при анализе компьютера.

- **Количество общих файлов** – количество файлов, к которым разрешен сетевой доступ.
- **Размер общих файлов** – общий размер всех файлов, к которым разрешен сетевой доступ.
- **Количество входов** – количество входов в учетные записи компьютера.
- **Количество вводов неверного пароля** – количество попыток ввести неверный пароль при входе в учетные записи компьютера.

Анализ файлов

Вы можете просмотреть информацию о файлах, собранную с помощью скрипта export-ad.ps1, выбрав пункт бокового меню **Объекты > Файлы**.

В верхней части рабочей области представлена сводная информация об общем количестве и размере файлов, о количестве файлов дубликатов и информация о файлах, регулируемых стандартом.

В нижней части рабочей области представлен список файлов в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Тип** – тип файла.
- **Компьютер** – компьютер, на котором расположен файл.
- **Каталог** – папка, в которой расположен файл.
- **Имя** – имя файла.
- **Время изменения** – время последнего изменения файла.
- **Время доступа** – время последней обращения к файлу.
- **Тип документа** – формат файла.
- **Размер** – размер файла.
- **Риск-фактор** - информация о потенциальных рисках, которые платформа Makves обнаружила при анализе файла.
- **Регулируется стандартом**
- **Дубликаты** – количество копий файлов.

Анализ почтовых ящиков

Вы можете просмотреть информацию о пользователях, собранную с помощью скрипта `export-mb-folders.ps1`, выбрав пункт бокового меню **Объекты > Почтовые ящики**.

В верхней части рабочей области представлена сводная информация об общем количестве почтовых ящиков в домене, о количестве папок, заведенных пользователя, а также информация о количестве и размере элементов в почтовых ящиках.

В нижней части рабочей области представлен список почтовых ящиков в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Имя** – имя пользователя, которое используется в почтовом адресе.
- **Alias** – псевдоним пользователя.
- **Имя сервера** – название сервера, на котором используется имя пользователя.
- **Количество папок** – количество папок в почтовом ящике.
- **Количество элементов** – количество элементов в почтовом ящике.
- **Размер** – общий размер всех элементов в почтовом ящике.

Анализ событий

Вы можете просмотреть информацию о пользователях, собранную с помощью скрипта `export-events.ps1`, выбрав пункт бокового меню **Объекты > События**.

В верхней части рабочей области представлена сводная информация об общем количестве событий.

В нижней части рабочей области представлен список файлов в виде таблицы.

В столбцах таблицы вы можете найти следующую информацию:

- **Время** – время регистрации события в журнале событий.
- **Категория** – категория события в журнале событий.
- **ID-события** – уникальный номер события.

- **Действие** – действие, которое было выполнено во время события.
- **Компьютер** – название компьютера, на котором произошло событие.
- **Пользователь** – пользователь, на чьей учетной записи произошло событие.
- **Домен** – домен, в котором произошло событие.

Учетные записи и уведомления

В веб-консоли предусмотрено автоматическое уведомление учетных записей, ответственных за решение инцидента, а также учетных записей, назначенных наблюдателями инцидентов.

Добавление учетных записей ответственных лиц в платформу Makves

1. В боковом меню выберите пункт **Настройки > Аккаунты**.

Откроется список учетных записей ответственных лиц.

2. Нажмите на кнопку **Создать**.

Откроется окно, в котором вы можете добавить новую учетную запись.

3. Выполните следующие действия:

- a. В поле **Имя** укажите имя учетной записи.
- b. В поле **Полной имя** укажите полное имя ответственного лица.
- c. В поле **Аватар** нажмите на кнопку **Выберите файл** и выберите изображение, которое будет отображаться для этой учетной записи.
- d. В поле **Описание** добавьте информацию об ответственном лице.
- e. В поле **Почта** укажите адрес электронной почты ответственного лица.
- f. В поле **Пароль** укажите пароль учетной записи.
- g. В поле **Подтвердить** укажите пароль учетной записи еще раз.
- h. Установите флажок **Права администратор**, если требуется предоставить учетной записи права администратора.
- i. Установите флажок **Права инспектора**, если требуется предоставить учетной записи права инспектора.

Учетные записи с правами администратора и инспектора могут изменять настройки платформы и добавлять объекты.

Добавление ответственного лица при создании инцидента

1. В боковом меню выберите пункт **Инциденты > Список**.

Откроется окно со списком инцидентов.

2. Нажмите на кнопку **Зарегистрировать**.

Откроется окно создания инцидента.

3. В раскрывающемся списке **Ответственный** выберите учетную запись лица, ответственного за решение инцидента.

4. Заполните остальные поля и нажмите на кнопку **Создать**.

Лицу, назначенному ответственным за решение инцидента, будет отправлено уведомление о новом инциденте.

Добавление наблюдателя

1. В боковом меню выберите пункт **Инциденты > Список**.

Откроется окно со списком инцидентов.

2. Нажмите на инцидент в списке.

Откроется окно создания инцидента.

3. В раскрывающемся списке **Наблюдатели не установлены** выберите учетную запись, которая будет наблюдателем.

Лицу, назначенному наблюдателем инцидента, будет отправлено уведомление о новом инциденте.

+7 (495) 150-54-06
support@makves.ru
www.makves.ru