Title

Управление инцидентами

Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

Пройти сертификационный экзамен

Все инциденты в **InfiMONITOR NEXT** формируются в соответствии с правилами, в которых описаны условия, при выполнении которых инциденты должны создаваться.

Инциденты

Важность

Важность инцидента помогает сетевым инженерам точно приоритизировать проблемы, выявляемые системой мониторинга в работе беспроводной сети. Чем выше приоритет, тем важнее решение соответствующей проблемы. Всего в **InfiMONITOR NEXT** предусмотрено 3 уровня важности:

- **Высокая** - инциденты, указывающие на критические проблемы, приводящие к нарушению функционирования беспроводной сети.
- **Средняя** - инциденты, указывающие на проблемы, которые не имеют критического влияния на функционирование беспроводной сети, но требу ющие внимания сетевых инженеров.
- **Низкая** - информационные сообщения, требующие внимания сетевых инженеров, но не оказывающие влияния на функционирование беспроводной сети.

Приоритет определяется в правиле формирования инцидента и будет устанавливаться на все инциденты, создаваемые в соответствии с этим правилом.

Жизненный цикл

Жизненный цикл инцидента включает в себя несколько этапов, описанных в таблице.

Этап	Статус инцидента	Описание
Выполнение условия правила		Если условие правила однократно выполнилось, то запускается процедура подтверждения инцидента. До ее завершения инцидент не будет сформирован.
Подтверждение инцидента		Проверяется выполнение условия правила в течение времени подтверждения. Если условие выполняется на протяжении всего времени, то будет сформирован инцидент. Если хотя бы один раз условие не было выполнено, то инцидент считается неподтвержденным и его жизненный цикл завершается.
Формирование инцидента	Открытый	Сформированный инцидент может быть назначен ответственному лицу, в этом случае выполняется переход на этап обработки. Если ответственный не назначен, то проверяется выполнение условия формирования инцидента на основе данных регулярного опроса: при однократном невыполнении условия срабатывания выполняется переход к этапу подтверждения разрешения инцидента.
Обработка инцидента	В работе	Ответственный за обработку выполняет работу по устранению причин возникновения инцидента. Проверяется выполнение условия формирования инцидента на основе данных регулярного опроса: при однократном невыполнении условия срабатывания выполняется переход к этапу подтверждения разрешения инцидента.

Подтверждение разрешения инцидента	Открытый / В работе	Проверяется выполнение условия правила в течение времени подтверждения. Если условие не выполняется в течение времени подтверждения, то осуществляется переход к этапу закрытия инцидента. В противном случае выполняется переход к этапу формирования или обработки, в зависимости от того, назначен ли ответственный.
Закрытие инцидента	Разрешен	Данный этап является конечным, инцидент считается разрешенным.

Статус "**Разрешен**" является конечным и означает, что инцидент был закрыт. Если условия возникновения инцидента снова выполнятся, то будет создан новый инцидент.

Область видимости

Инцидент будет доступен пользователю системы мониторинга только в том случае, если устройство, в отношении которого он возник, находится в области видимости этого пользователя.

Правила

Структура

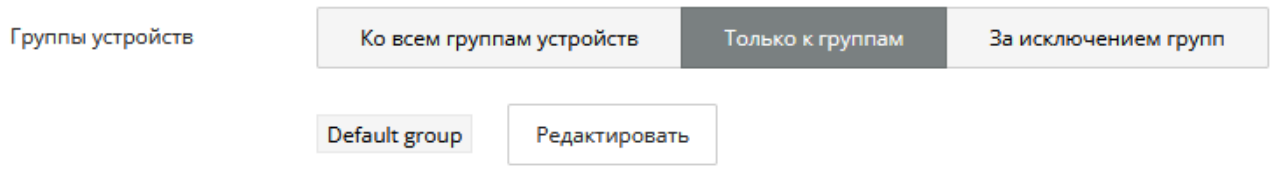
Каждое правило имеет следующую структуру:

- **Название** - произвольное имя правила.
- **Важность инцидента** - важность, которая будет назначена созданному инциденту:
- **Описание** - произвольное описание, которое позволит впоследствии быстрее понять суть возникшего инцидента.
- **Группы устройств** - группы устройств, в отношении которых будет действовать данное правило.
- **Условия возникновения инцидента**.
  - **условие срабатывания:** одно или несколько условий, объединённых логическими операциями.
  - **время подтверждения:** период времени, в течение которого автоматически выполняется проверка условия срабатывания.

Группы устройств

Каждое правило содержит в себе перечень групп устройств, в отношении которых оно будет действовать. Для настройки используются следующие категории:

1. **Ко всем группам устройств** - правило будет действовать в отношении устройств всех групп.
2. **Только к группам** - правило будет действовать в отношении устройств выбранных групп.
3. **За исключением групп** - правило будет действовать в отношении устройств всех групп, кроме выбранных.



Область действия правила

Условия возникновения инцидента

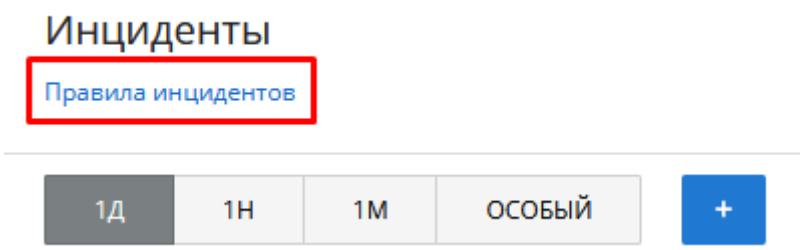
Каждое условие описывается следующими параметрами:

1. **Оконная функция** - применяется к набору значений метрик, полученных в течение указанного временного окна. Например, размер окна составляет 20 минут, в течение которых было выполнено 4 опроса, которые дали следующие результаты: "23, 52, 31, 15". Оконная функция "Max", примененная к этому набору, даст значение "52", "Min" - 15, "All" - "23, 52, 31, 15" и т.д.
2. **Метрика** - метрика, значение которой будет использовано в условии.
3. **Оператор** - оператор сравнения порогового и фактического значения метрики.
4. **Значение** - пороговое значение.

Время подтверждения - время, в течение которого ожидается подтверждение выполнения условий срабатывания правила. Если в отношении какого-то устройства выполнились условия правила, то инцидент будет сформирован только в том случае, если условие будет повторно выполняться в течение установленного времени подтверждения - на этом этапе частота опроса соответствующего устройства увеличивается до 1 раза в минуту.

Создание правила

Управление правилами формирования инцидентов осуществляется в разделе "Инциденты".



Переход в раздел управления правилами инцидентов

По умолчанию в **InfiMONITOR NEXT** добавлены два правила:

- Host down - инцидент возникнет, если сетевой узел перейдет в статус DOWN.
- Link down - инцидент возникнет, если беспроводной канал связи перейдет в статус DOWN.

Правило	Описание	Группы
Host down	This rule will fire events when host changes status to oth...	Default Group, Auto-Discovered Devices, XG, Evo
Link down	This rule will fire events when link status is not Up.	Default Group, Evo, XG, Auto-Discovered Devices

Правила инцидентов по умолчанию

Для создания нового правила нажмите кнопку "**Добавить новое правило**". В открывшейся форме в соответствии с описанной выше структурой укажите:

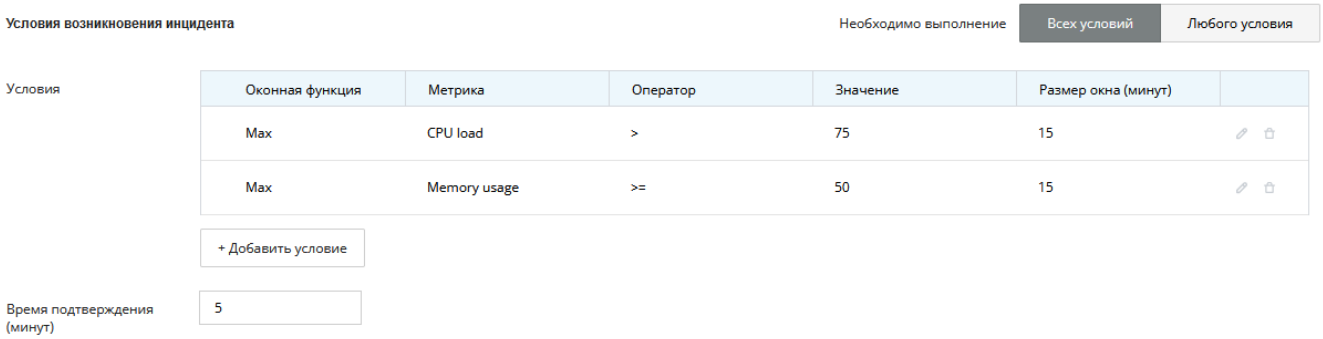
1. наименование правила;
2. важность инцидента;
3. описание;
4. область действия.

Следующим этапом является определение условий возникновения инцидента. Суть условий заключается в сравнении значения какой-либо метрики, установленного правилом, с фактическим значением, полученным в процессе опроса беспроводного устройства.

Рассмотрим пример, в котором необходимо формировать инциденты в случае, если в течение 5 минут загрузка процессора устройства превышает 75% и объём используемой оперативной памяти составляет не менее 50%. В этом примере условия будут выглядеть следующим образом:

- Поскольку количество условий в правиле больше одного, то в поле "Необходимо выполнение" нужно установить значение "Всех условий", которое соответствует логическому "И".
- Для обеих метрик будет применена оконная функция "Max" с размером окна 15 минут, что означает, что в качестве значения метрики будет взято максимальное значение, полученное в течение последних 15 минут.
- Для метрики "CPU load" используется оператор ">", а для "Memory usage" - ">=".
- Время подтверждения - 5 минут.

Title



Пример условия возникновения инцидента

Для завершения создания правила нажмите кнопку "**Сохранить**". Правило начинает действовать, начиная со следующего цикла опроса беспроводного устройства.