Title

Управление событиями

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

Пройти сертификационный экзамен

- Создание группы правил
  - Сетевые узлы
  - Правила
  - Уведомления
- Создание правил
- Срок хранения событий

Все события в **InfiMONITOR** формируются в соответствии с правилами, в которых описаны условия, при которых они должны появиться в списке событий.

На изображении представлена организация подсистемы формирования событий **InfiMONITOR**:

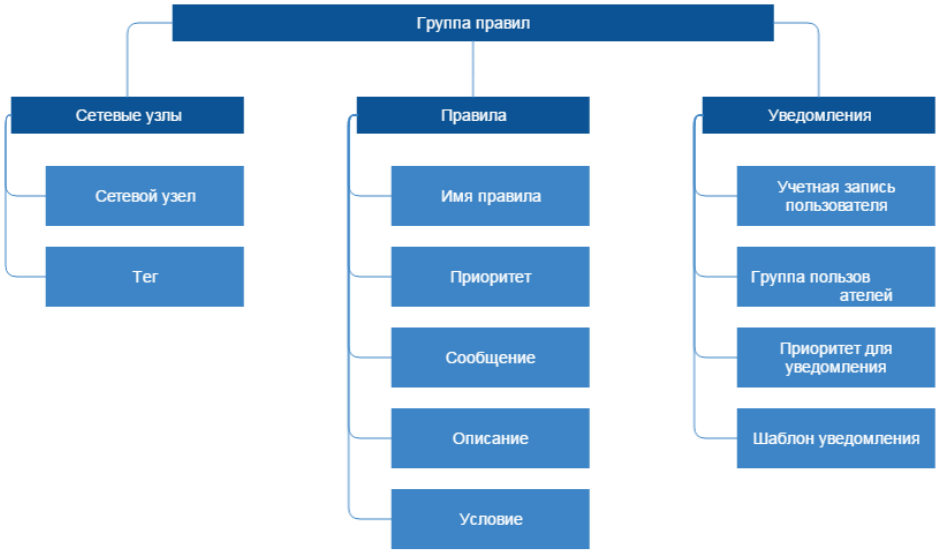

Рисунок - Принцип организации подсистемы формирования событий

Каждая группа правил включает в себя:

- **Сетевые узлы** - перечень сетевых узлов, в отношении которых необходимо формировать события
- **Правила** - перечень правил, согласно которым будут формироваться события в отношении сетевых узлов, входящих в группу правил
- **Уведомления** - правила операторов **InfiMONITOR** отправки уведомлений о событиях, которые формируются в соответствии с правилами в отношении сетевых узлов, входящих в группу правил.

Создание группы правил

Управление правилами формирования событий осуществляется в разделе "Settings" -> "Event rules" -> "Groups of rules". Для создания новой группы нажмите кнопку "**Create Group**", на экране появится форма, которая включат в себя три раздела, по умолчанию открыт раздел "Hosts"

Сетевые узлы

В разделе "Hosts" осуществляется выбор сетевых узлов, в отношении которых должны формироваться события. Этот раздел включает в себя следующие параметры:

- "*Group name*" - произвольное имя группы правил

- "*Assigned hosts*" - список выбранных сетевых узлов, которые будут добавлены в создаваемую группу правил. Для исключения узла из группы его необходимо выбрать и нажать кнопку "**Remove selected**" или перетащить с помощью курсора мыши из списка "*Assigned hosts"* в список "*Available hosts"*
- "*Available hosts*" - список всех доступных в **InfiMONITOR** сетевых узлов. Для добавления узла в группу правил его необходимо выбрать и нажать кнопку "**Assign selected**" или перетащить с помощью курсора мыши из списка "*Available hosts"* в список "*Assigned hosts"*.

ВНИМАНИЕ

Сетевые узлы могут быть добавлены как по одному, так и группой с помощью тега. Если хотя бы на один узел в разделе "Network Monitoring" -> "Hosts" был назначен хотя бы один тег, то он будет доступен в списке "*Available hosts"*. В случае, если вы желаете добавить группу сетевых узлов за исключением некоторых из них, то такие узлы могут быть помещены в список исключений. Для этого соответствующие узлы необходимо найти и выделить в списке "*Available hosts*", а затем нажать кнопку "**Exclude selected**". Таким образом, события будут формироваться в отношении всех сетевых узлов с выбранным тегом, но не будут для тех, что были добавлены в исключения.

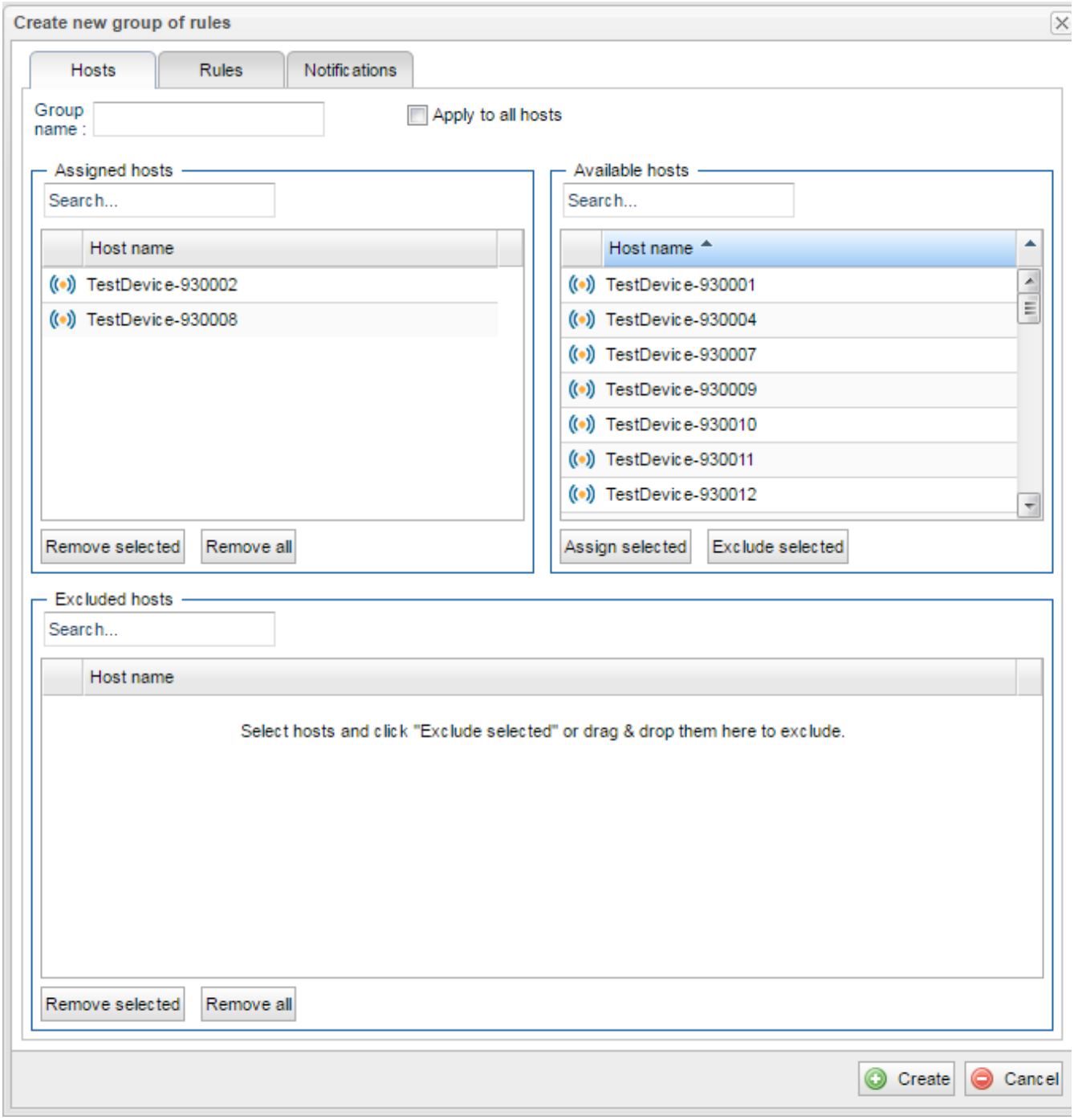

Рисунок - Добавление устройств в группу правил

Правила

После выбора сетевых узлов необходимо выбрать правила, в которых указаны условия, по которым должны формироваться события. Эти правила будут применяться только к тем узлам, которые были добавлены в группу правил. Перейдите в раздел "Rules", который включает в себя следующие параметры:

- "*Assigned rules*"- список выбранных правил, которые будут добавлены в создаваемую группу правил. Для исключения правила из группы его необходимо выбрать и нажать кнопку "**Remove selected**" или перетащить с помощью курсора мыши из списка "*Assigned rules"* в список "*Available rules"*
- "*Available rules*" - список всех доступных в **InfiMONITOR** правил. Для добавления правила в группу правил его необходимо выбрать и нажать кнопку "**Assign selected**" или перетащить с помощью курсора мыши из списка "*Available rules"* в список "*Assigned rules"*.

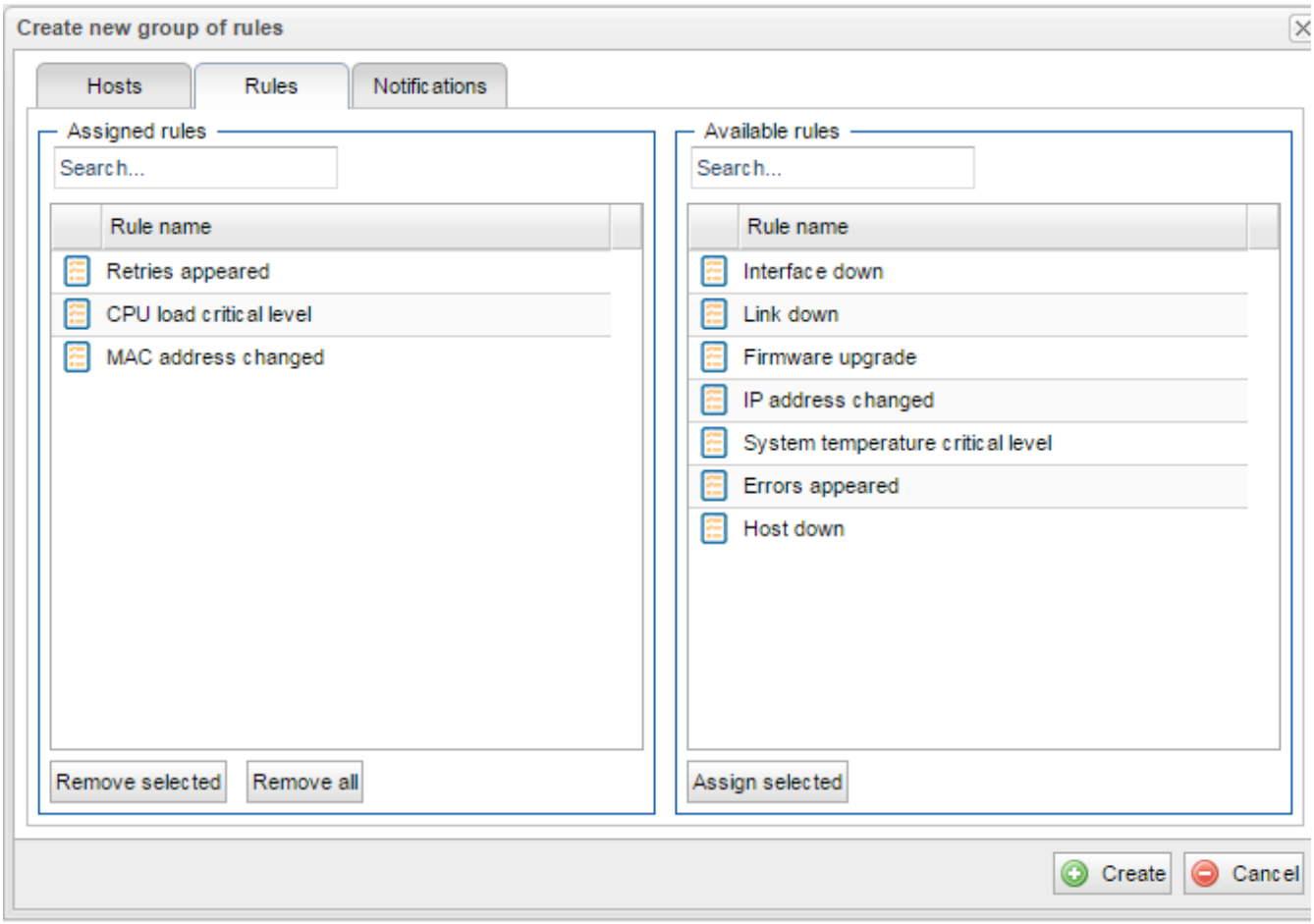

Рисунок - Добавление правил в группу правил

Уведомления

После выбора сетевых узлов и правил необходимо определить, какие операторы **InfiMONITOR** должны получать уведомления о формировании событий на email. Перейдите в раздел "Notifications", который включает в себя следующие параметры:

- "*Assigned users*"- список выбранных учетных записей пользователей и групп, которым будут отправлять уведомления. Для исключения пользователя из группы его необходимо выбрать и нажать кнопку "**Remove selected**" или перетащить с помощью курсора мыши из списка "*Assigned users"* в список "*Available users"*
- "*Available users*" - список всех доступных в **InfiMONITOR** учетных записей пользователей и групп. Для добавления пользователя в группу правил его необходимо выбрать и нажать кнопку "**Assign selected**" или перетащить с помощью курсора мыши из списка "*Available users"* в список "*Assigned users"*
- "*Send notifications*" - активация/деактивация отправки уведомлений выбранным пользователям

- "*Severity*" - минимальный приоритет события, при котором должно отправляться уведомление. Таким образом, если установлен приоритет "*Warning*", то пользователи будут получать уведомления о событиях с приоритетом "*Warning*" и "*Critical*". Если у события будет приоритет "*Info*", то уведомление отправлено не будет
- "*Subject*" - тема письма с уведомлением. В тексте могут быть использованы переменные, вместо которых будут подставляться действительные значения соответствующих параметров события. Полный перечень возможных переменных можно получить, нажав на знак вопроса, расположенный рядом с полем
- "*Body*" - текст уведомления. В тексте могут быть использованы переменные, вместо которых будут подставляться действительные значения соответствующих параметров события. Полный перечень возможных переменных можно получить, нажав на знак вопроса, расположенный рядом с полем.

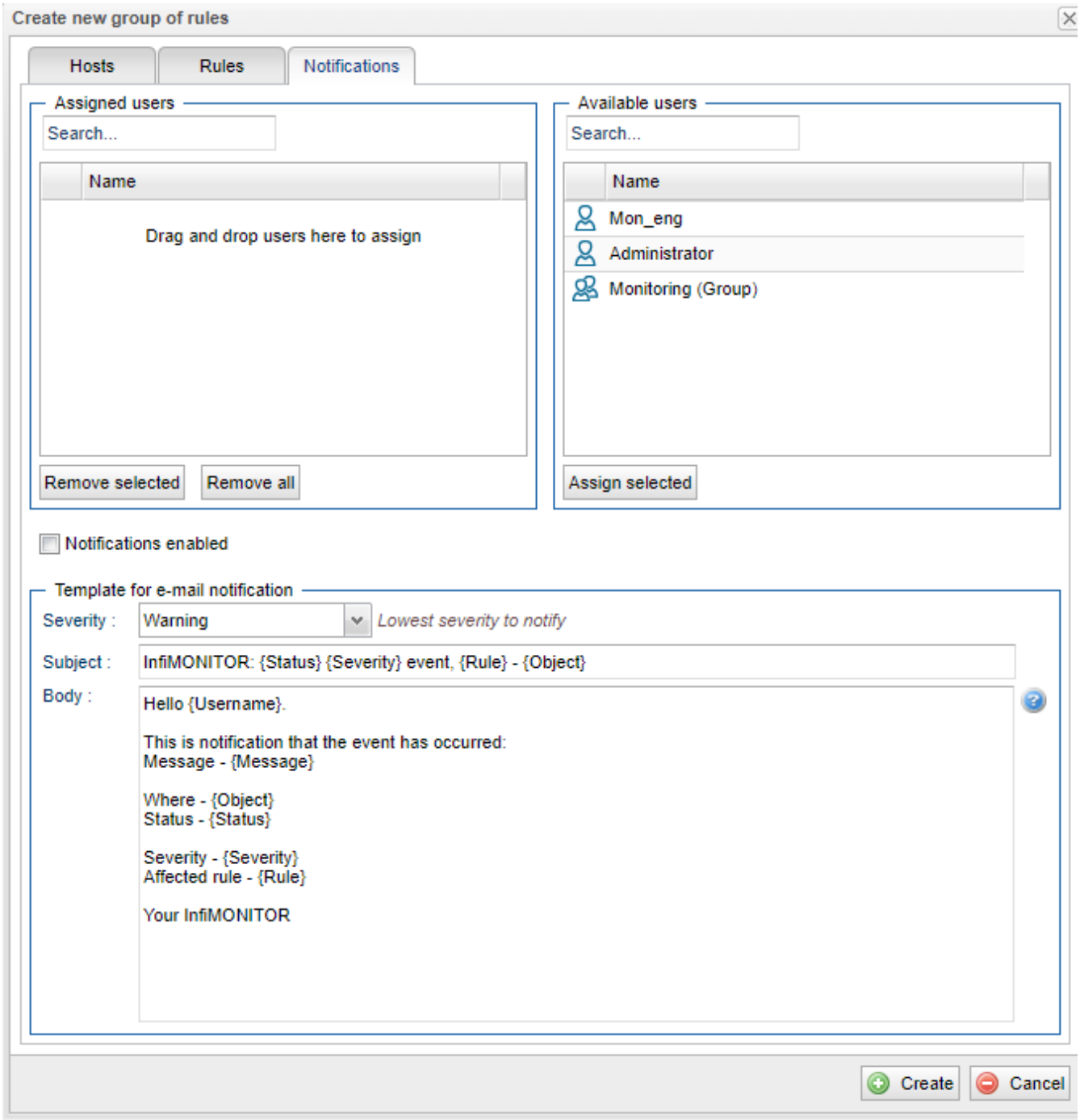

Рисунок - Управление уведомлениями в группе правил

Нажмите кнопку "**Create**" для завершения процесса создания группы правил.

Создание правил

Правило - ключевой компонент подсистемы формирования событий, они служат основанием для принятия решения о том, должно ли быть сформировано событие или нет. Управление правилами осуществляется в разделе "Settings" -> "Event rules" -> "Rules".

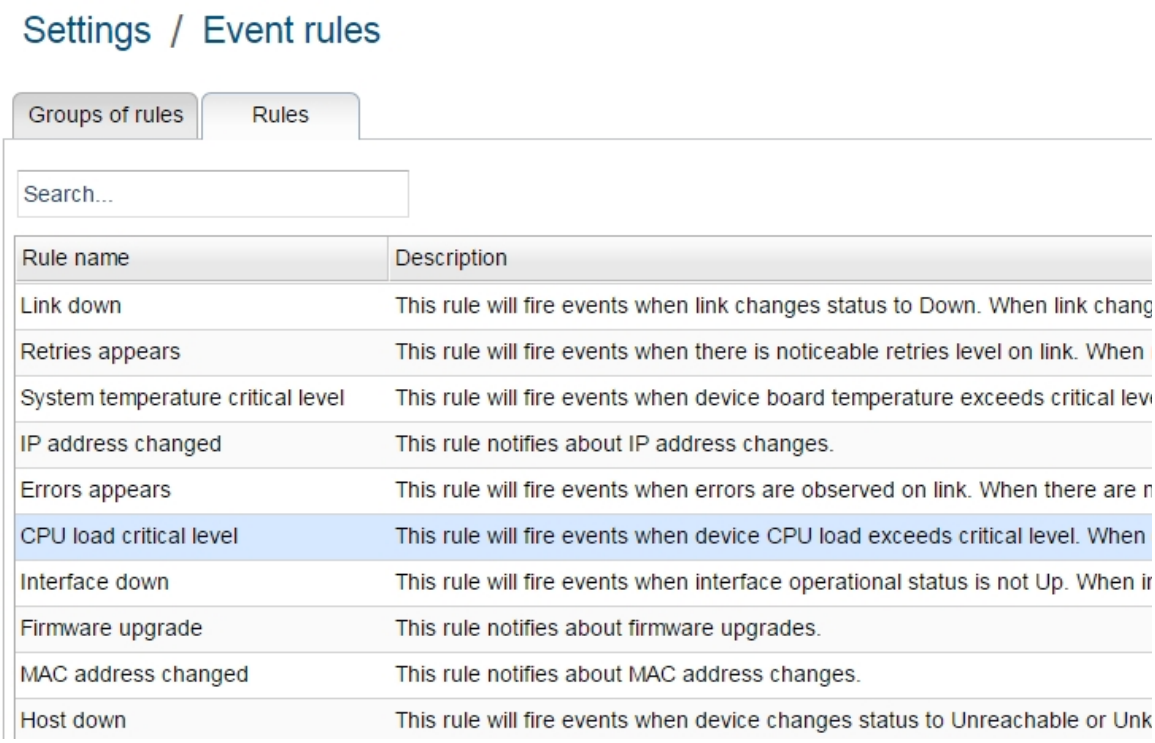

Рисунок - Перечень правил формирования событий

Для создания нового правила нажмите кнопку "**Create rule**", на экране появится форма, содержащая два раздела:

- "Settings" - общие параметры правила
- "Condition" - условие формирования события.

По умолчанию открыт раздел "Settings", содержащий следующие поля:

- "*Rule name*" - произвольное имя правила
- "*Severity*" - приоритет, который будет назначен событию, сформированному согласно этому правилу
- "*Message*" - сообщение, которое будет указано в событии, сформированном согласно этому правилу. В тексте могут быть использованы переменные, вместо которых будут подставляться действительные значения соответствующих параметров события. Полный перечень возможных переменных можно получить, нажав на знак вопроса, расположенный рядом с полем
- "*Description*" - произвольное описание правила
- "*May* be *resolved automatically*" - флаг, указывающий на то, может ли быть событию, сформированному правилом, автоматически изменен статус на "*Resolved"* в случае, когда причины его формирования были устранены. Такой флаг имеет смысл устанавливать у обратимых событий, например, потеря связи с сетевым узлом. Когда связь восстановится, то, если флаг установлен, событию будет автоматически установлен статус "*Resolved"*. Однако в том случае, когда речь идет о необратимых последствиях, то данный флаг не имеет смысла. Например, если речь идет о событии об изменении версии программного обеспечения узла, которое носит сугубо уведомительный характер.

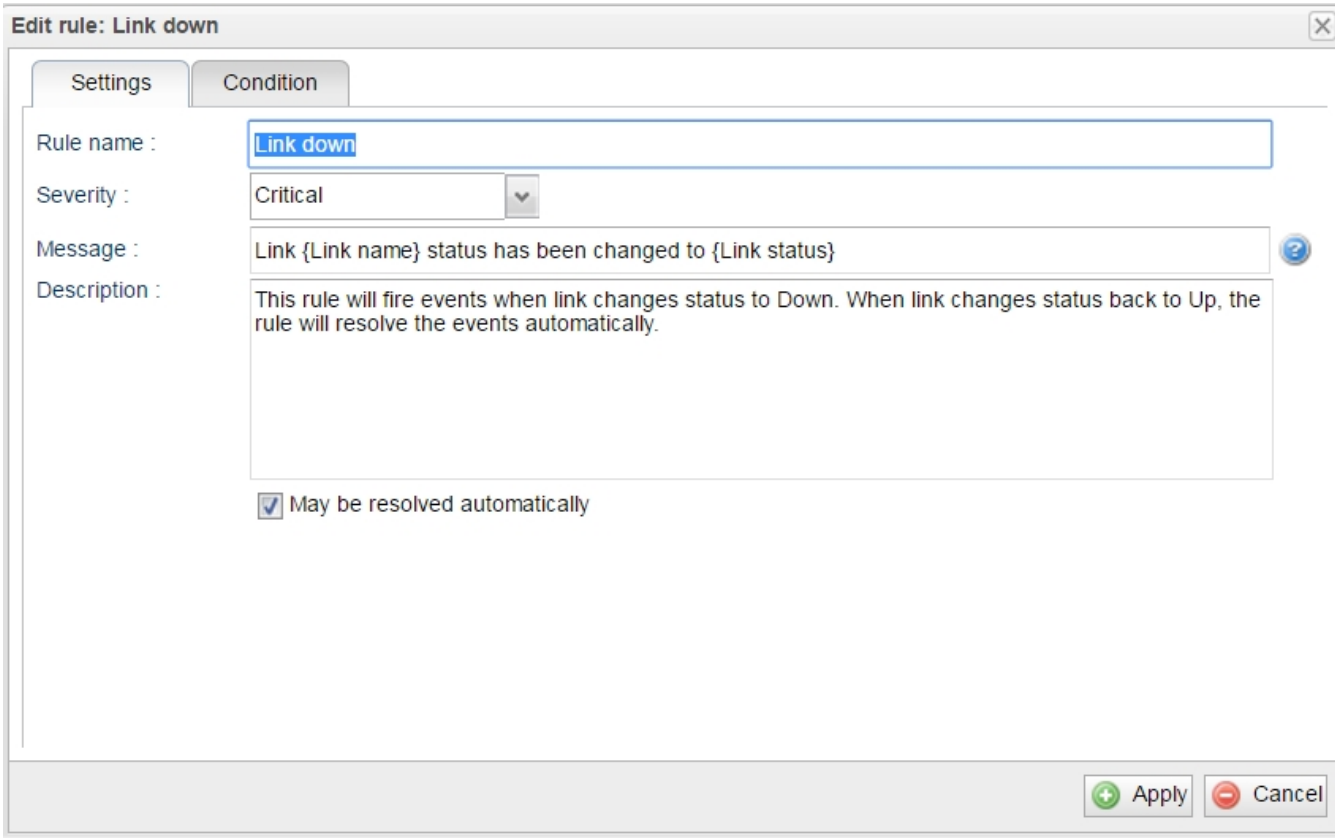

Рисунок - Основные параметры правила формирования событий

В разделе "Condition" указывается условие, при выполнении которого будет сформировано событие. Условие состоит из трех компонентов:

- "Логический оператор" - операторы "*and*", "*or*" и "*not*" указывают на тип сравнения параметров, указанных в условии. Логические операторы могут быть вложенными друг в друга:
  - "*And*" - означает, что условие будет выполнено, если результатом операций сравнения всех параметров будет истина
  - "*Or*" - означает, что условие будет выполнено, если результатом операций сравнения одного любого параметра будет истина
  - "*Not*" - означает, что условие будет выполнено, если результатом операций сравнения всех параметров будет ложь
- "Параметр" - параметр сетевого узла или беспроводного канала связи, к значениям которых применяется оператор сравнения
- "Оператор сравнения" - операторы "*empty*", "*not empty*", "*equals*", "*not equal*", "*changed*", "*not changed*", "*greater than*", "*greater than or equal to*", "*less than*", "*less than or equal to*" указывают на тип сравнения значений параметров:
  - "*empty*" - результатом выполнения оператора будет истина, если значение параметра будет пустым, иначе - ложь
  - "*not empty*" - результатом выполнения оператора будет истина, если значение параметра будет не пустым, иначе - ложь
  - "*equals*" - результатом выполнения оператора будет истина, если значение параметра будет равным указанному значению, иначе - ложь
  - "*not equal*" - результатом выполнения оператора будет истина, если значение параметра не будет равным указанному значению, иначе - ложь
  - "*changed*" - результатом выполнения оператора будет истина, если значение параметра изменилось по отношению к предыдущему, иначе - ложь
  - "*not changed*" - результатом выполнения оператора будет истина, если значение параметра не изменилось по отношению к предыдущему, иначе - ложь
  - "*greater than*" - результатом выполнения оператора будет истина, если значение параметра будет больше указанного значения, иначе - ложь
  - "*greater than or equal to*"- результатом выполнения оператора будет истина, если значение параметра будет больше или равно указанному значению, иначе - ложь
  - "*less than*" - результатом выполнения оператора будет истина, если значение параметра будет меньше указанного значения, иначе - ложь
  - "*less than or equal to*" - результатом выполнения оператора будет истина, если значение параметра будет меньше или равно указанному значению, иначе - ложь.

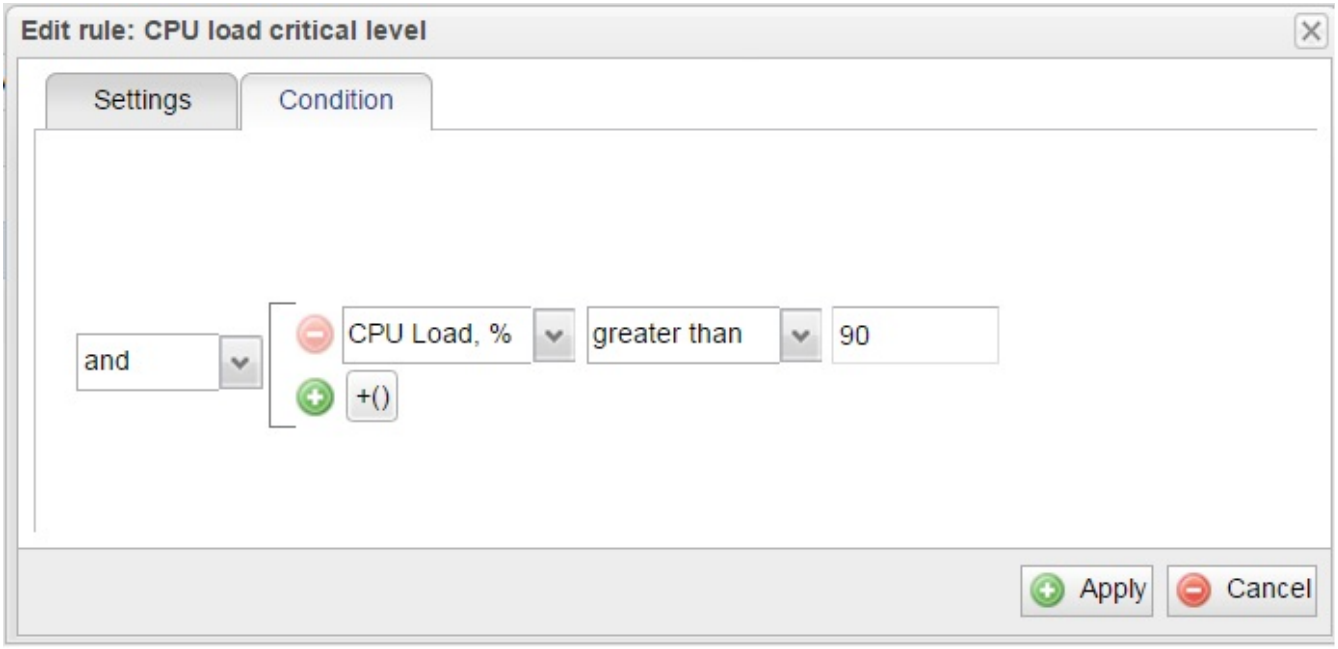

Рисунок - Условия правила формирования событий

Нажмите кнопку "**Apply**" для завершения процесса создания правила. Теперь оно может быть добавлено в группу правил.

Срок хранения событий

В целях предотвращения исчерпания дискового пространства InfiMONITOR осуществляет ежедневное автоматическое удаление событий со статусами "*Re solved*" или "*Aged*", дата возникновения которых превышает установленный срок хранения. По умолчанию, срок хранения составляет 1 месяц. В секции "Events retention" раздела "Settings" -> "System" администратор InfiMONITOR может изменить максимальный срок хранения событий вплоть до 12 месяцев.

Рисунок - Срок хранения событий