Umbrales de baja utilización en Interfaces NMIS8

Objetivo

Los clientes han solicitado soluciones que solo les alertan cuando un evento es relevante en cuanto al tiempo. Este documento proporcionará una posible solución para las alertas basadas en el tiempo.

Ejemplo:

El enrutador 'r2' tiene una interfaz que, en general, siempre debe utilizarse en más del 1%; si se utiliza menos del 1%, se supone que hay una situación que requiere que un ingeniero investigue. ¡Sin embargo! También se sabe que entre las 01:00 y las 05:00 es normal que la interfaz del enrutador caiga por debajo del 1% de utilización. Debido a esto, solo deseamos alertas de baja utilización entre las 05:00 y la 01:00.

Documentos relacionados

- Umbrales básicos y avanzados en NMIS8
- Acciones de eventos y escalamiento

Solución

Umbrales de nivel bajo NMIS

Nuestro ejemplo se basa en una utilización de bajo nivel. En base a esto, haremos la configuración necesaria en NMIS para un umbral de interfaz de bajo nivel.

Common Thresholds

Los administradores de NMIS pueden agregar umbrales modificando /usr/local/nmis8/models/Common-threshold.nmis. Observe la estructura de este archivo.
/usr/local/nmis8/models/Common-threshold.nmis

```
%hash = (
  'threshold' => {
    'name' => {
###
### Threshold configuration goes here
###
    }
  }
)
```

Este es un ejemplo de un umbral de 'LOW Interface Input Utilization'. Observe la clave 'control', así es como podemos filtrar nodos e interfaces en el nivel de umbral. Para obtener más información sobre cómo personalizar y configurar umbrales, consulte: Umbrales básicos y avanzados en NMIS8

```
'low_util_in' => {
   'event' => 'Proactive LOW Interface Input Utilization',
   'item' => 'inputUtil',
   'select' => {
     '10' => {
       'control' => '$node eq "r2"',
       'value' => {
         'fatal' => '0.1',
         'critical' => '0.4',
         'major' => '0.6',
         'minor' => '0.8',
         'warning' => '1'
       },
      },
    },
},
```

Si desea aplicarlo en general, la configuración debe ser como se muestra a continuación:

```
'low_util_in' => {
   'event' => 'Proactive LOW Interface Input Utilization',
   'item' => 'inputUtil',
   'select' => {
     'default' => {
       'value' => {
         'fatal' => '0.1',
         'critical' => '0.4',
         'major' => '0.6',
         'minor' => '0.8',
         'warning' => '1'
       },
      },
    },
},
```

Agregar un umbral a un modelo

Después de que se crea el nuevo umbral; necesitamos asociarlo con cualquier modelo que deba evaluarlo. Para este ejemplo, utilizamos el modelo de CiscoRouter. Al encontrar la sección de interfaz, notamos la clave de umbral. Simplemente podemos agregar nuestro nuevo umbral 'low_util_in' a este valor separado por comas.
/usr/local/nmis/model/Model-CiscoRouter.nmis

```
   'interface' => {
    'rrd' => {
      'interface' => {
        'indexed' => 'true',
        'threshold' => 'low_util_in,util_in,util_out',
```

Actualizar el nodo

Para que nuestra nueva configuración surta efecto, necesitamos actualizar el nodo apropiado.

```
/usr/local/nmis8/bin/nmis.pl type=collect node=r2 force=true
```

Verificar

Podemos verificar consultando el archivo var nodos. Busque nuestro nuevo umbral en este archivo; en este ejemplo /usr/local/nmis8/var/r2-node.json. Obs erve que la utilización actual de Fa1 / 0 es 1,43%, lo que es normal según nuestra configuración.
/usr/local/nmis8/var/<node>-node.json

```
"low_util_in--2" : {
   "status" : "ok",
   "value" : "1.43",
   "event" : "Proactive LOW Interface Input Utilization",
   "element" : "FastEthernet1/0",
   "index" : "2",
   "level" : "Normal",
   "type" : "interface",
   "level_select" : "10",
   "method" : "Threshold",
   "updated" : 1532738282,
   "property" : "low_util_in"
},
```

opEvents - Acciones de eventos

A continuación, debemos configurar opEvents para que solo envíen alertas entre las 05:00 y la 01:00. Para nuestro ejemplo, usaremos un servidor syslog externo como acción, pero esta acción podría ser enviar un correo electrónico, activar un script o casi cualquier cosa. Para esta maniobra toda la configuración se realiza en /usr/local/omk/conf/EventActions.nmis. Antes de continuar, revise: Acciones de eventos y escalamiento

Concepto de configuración

- Proporcione una política de escalada que solo se active entre las 05:00 y la 01:00
- Identificar y etiquetar el evento
- Activar la política de escalada basada en la etiqueta

Antes de editar /usr/local/omk/conf/EventActions.nmis, observe la estructura de este archivo. Está dividido en las siguientes secciones.

- política
- Iniciar sesión
- texto
- syslog
- mensaje
- escalar

Nuestra configuración llamará a las secciones de política y escalamiento.

Escalar política

La política de ampliación a continuación cumplirá con los requisitos de nuestro ejemplo.
/usr/local/omk/conf/EventActions.nmis

```
#### Escalate Section
 'escalate' => {
                'LOW_Events' => {
                  'name' => 'LOW_Events',
                  'IF' => {
                    priority => '>=0',
                    begin => '05:00',
                    end => '01:00',
                  },
                  '1' => 'syslog.server1()',
                },
```

Reglas de política

Agregaremos dos reglas de política.

El primero; 1.414, identificará y etiquetará el evento. En este caso, estamos indicando que cualquier nombre de evento que contenga 'LOW' debe estar sujeto a establecer la etiqueta LOW en TRUE.

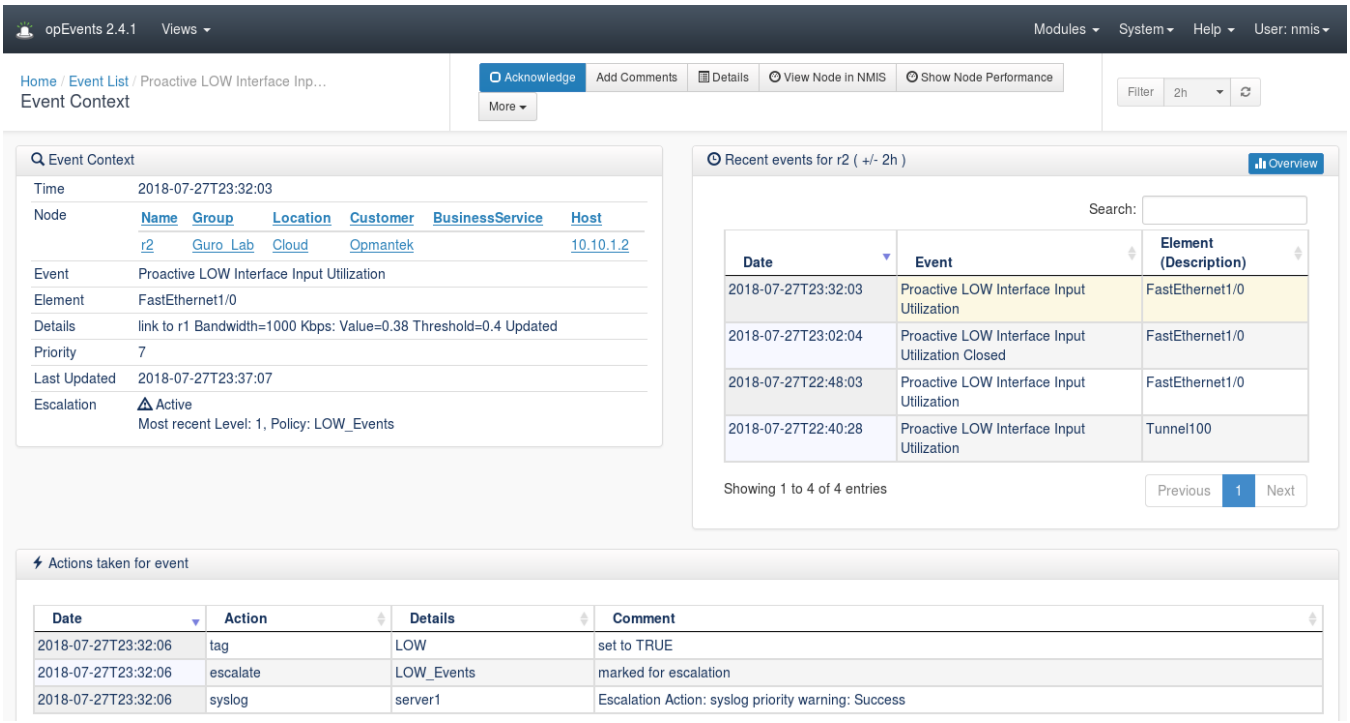
El segundo; 999, activará la política de escalamiento 'LOW_Events' previamente aprovisionada.
/usr/local/omk/conf/EventActions.nmis

```
#### Policy Section
                                '1.414' => {
                                        IF => 'event.event =~ qr{LOW}',
                                        THEN => 'tag.LOW(TRUE)',
                                        BREAK => 'false'
                                },

#--- snip ---
#
# Other policy rules will be here.
#
# We recommend the final policy rules match tags and fire things.

                                '999' => {
                                        IF => 'event.tag_LOW eq "TRUE"',
                                        THEN => 'escalate.LOW_Events()',
                                        BREAK => 'false'
                                },
```

Verificar

Ventana de escalamiento interior

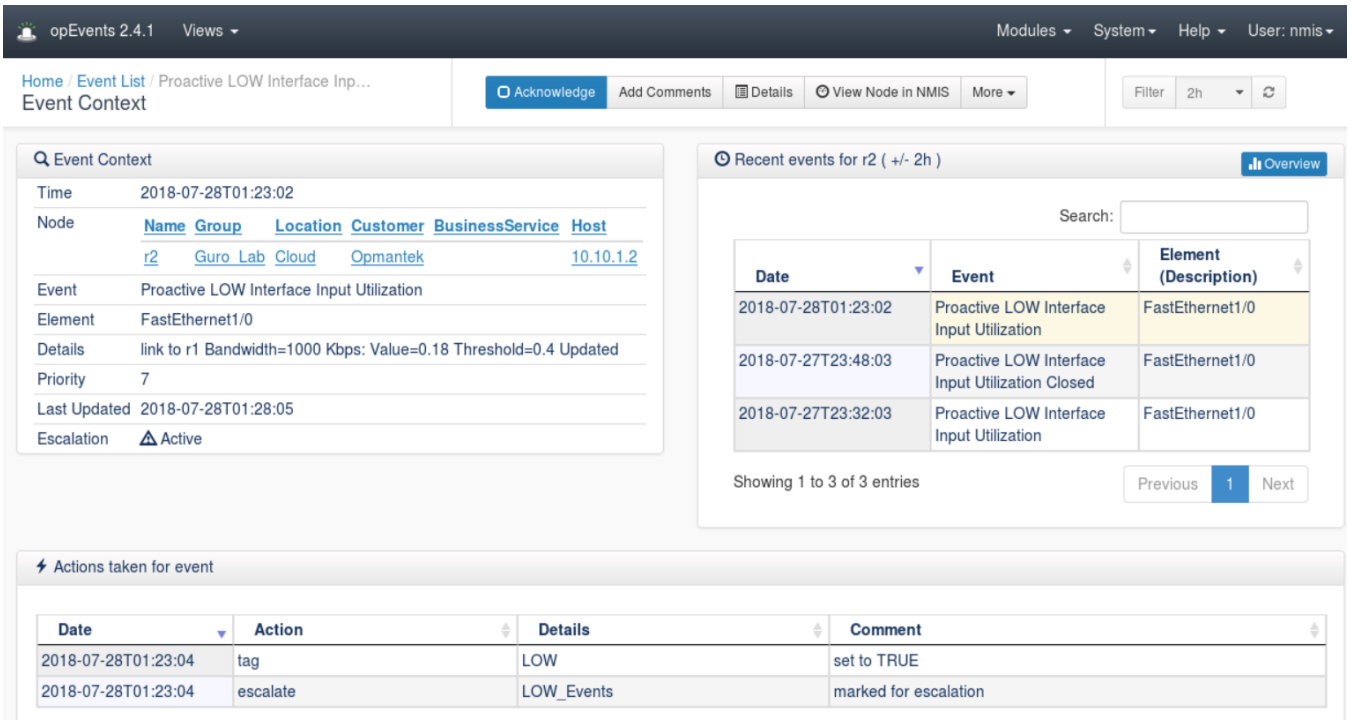
Podemos verificar la configuración observando el evento en opEvents.



Echemos un vistazo a la sección anterior "Acciones realizadas para el evento". Vemos que el evento tenía la etiqueta LOW configurada como verdadera. Note el tiempo; 23:32, estamos dentro del tiempo de la política de escalada. Debido a esto, opEvents actuó sobre la política de escalamiento y envió un mensaje de syslog al servidor1.

Ventana de escalada exterior

Ahora echemos un vistazo a un evento que ocurre fuera de la ventana de tiempo de escalada.



Note el tiempo; 01:23, estamos fuera de la ventana de escalada. Debido a esto, la acción de escalada no se activó, no se ha enviado ningún mensaje de syslog al servidor1. Si esta alerta no ha sido reconocida por un evento 'Cerrado' antes de las 05:00, la política de escalamiento enviará la alerta en ese momento. Si se confirma antes de las 05:00, no se realizará ninguna acción.