Línea Base Dinámica y Herramienta de Umbral para opCharts

- ¿Por qué necesitamos una herramienta de umbral y una línea base dinámica?
  - Tipos de métricas
  - Comparando métricas consigo mismas
  - La herramienta de umbral y línea base dinámica de opCharts
- Establecimiento de una línea base dinámica
  - Valor actual
  - Línea base de varios días
  - Línea base en un mismo día
  - Línea base delta
- Instalación de la herramienta de línea base
- Trabajar con la herramienta de línea base dinámica y umbrales
  - Opciones de configuración de línea base dinámica
    - Ejemplo de configuración de línea base dinámica el mismo día
    - Ejemplo de configuración de línea base dinámica de varios días
    - Ejemplo de configuración de línea base delta
    - Ejemplo de configuración de Delta base para paquetes de salida descartados
  - Ejecución de la herramienta de línea base
    - Opciones de línea de comando para nodo y grupo
    - Procesamiento automático usando Cron
    - Uso de group_regex y cron para procesamiento paralelo

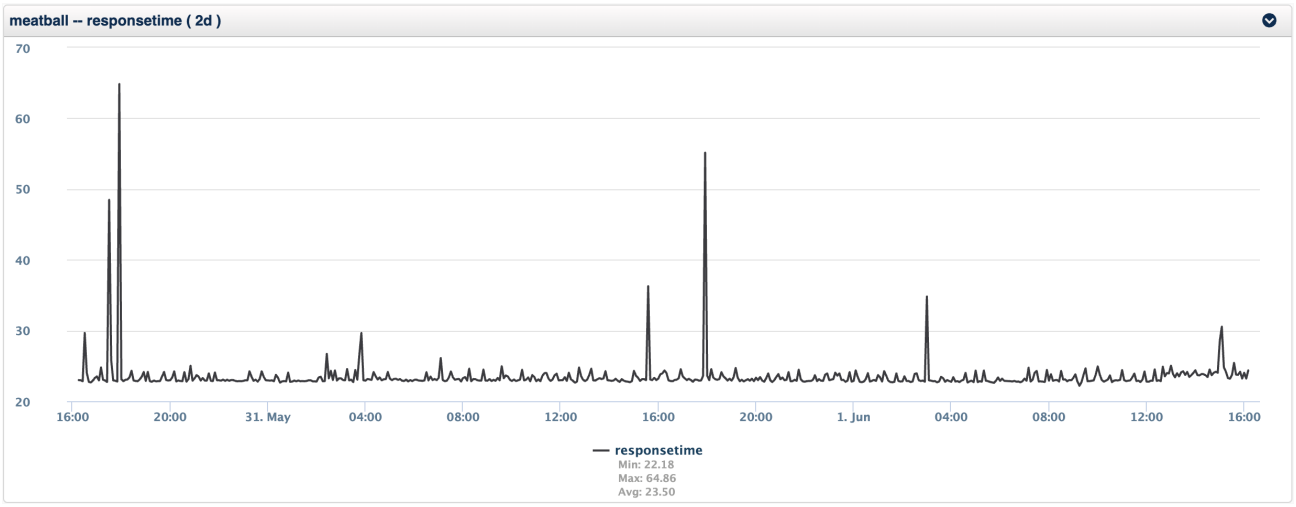
¿Por qué necesitamos una herramienta de umbral y una línea base dinámica?

La razón por la que queremos establecer una línea base y un umbral de nuestros datos, es para poder recibir alertas que nos adviertan sobre problemas en nuestro entorno, de modo que podamos actuar para resolver problemas más pequeños antes de que se vuelvan más grandes.

Tipos de métricas

Al analizar los datos en una línea del tiempo, puede identificar rápidamente una tendencia común en lo que está viendo y encontrará que algunas métricas que está monitoreando serán "estables", es decir, tendrán patrones muy repetidos y cambiarán de manera similar con el tiempo; mientras que otras métricas serán más caóticas, con un patrón difícil de identificar.

Tomemos, por ejemplo, dos métricas: el tiempo de respuesta y el número de ruta (el número de rutas en la tabla de enrutamiento). Puede ver en los gráficos a continuación que el tiempo de respuesta es más caótico con algún patrón pero realmente poca estabilidad en la métrica, mientras que la última métrica numérica es constante, sin cambios caóticos.



Comparando métricas consigo mismas

Este router ejemplo llamado "meatball", es un enrutador de oficina pequeño, con poca variación en el enrutamiento, sin embargo, un enrutador de distribución WAN sería generalmente estable, pero tendría un poco más de variabilidad. ¿Cómo podría obtener una alarma de cualquiera de estos sin configurar algunos umbrales estáticos complejos?

La respuesta es establecer una línea base de la métrica tal como está y comparar su valor actual con la línea base, este método es muy útil para valores que son muy diferentes en varios dispositivos. Aquí lo que se desea es saber cuándo cambia la métrica, por ejemplo, número de ruta, número de usuarios conectados, número de procesos que se ejecutan en Linux, tiempo de respuesta en general, pero especialmente el tiempo de respuesta de un servicio.

La herramienta de umbral y línea base dinámica de opCharts

En general, esto es lo que hace opTrend. El sofisticado modelo estadístico que crea es muy poderoso y ayuda a detectar estas tendencias con la herramienta de referencia. Hemos ampliado opTrend con algunas funciones adicionales para que pueda recibir rápidamente alertas de las métricas que son importantes para usted.

Lo que es realmente clave aquí, es que la herramienta de línea base detectará cambios hacia abajo y hacia arriba, por lo que si su tráfico se estaba reduciendo fuera de la línea base, recibiría una alerta.

Establecimiento de una línea base dinámica

Valor actual

En primer lugar, quiero calcular mi valor actual y podría usar el último valor recopilado, pero dependiendo de la estabilidad de la métrica, esto podría causar falsos positivos. Como NMIS siempre ha empleado, usar un período de umbral más grande al calcular el valor actual puede proporcionar resultados más relevantes.

Para métricas muy estables, el uso de un período de umbral pequeño no es un problema, pero para valores más caóticos, se recomienda un período más largo. Para las alertas de tiempo de respuesta, sería una buena idea usar un período de umbral de 15 minutos o más. Eso significa que hay un problema sostenido y no solo un problema de conexión a Internet. Sin embargo, con nuestro número de ruta, podríamos estar muy contentos de usar el último valor y recibir una advertencia antes.

Línea base de varios días

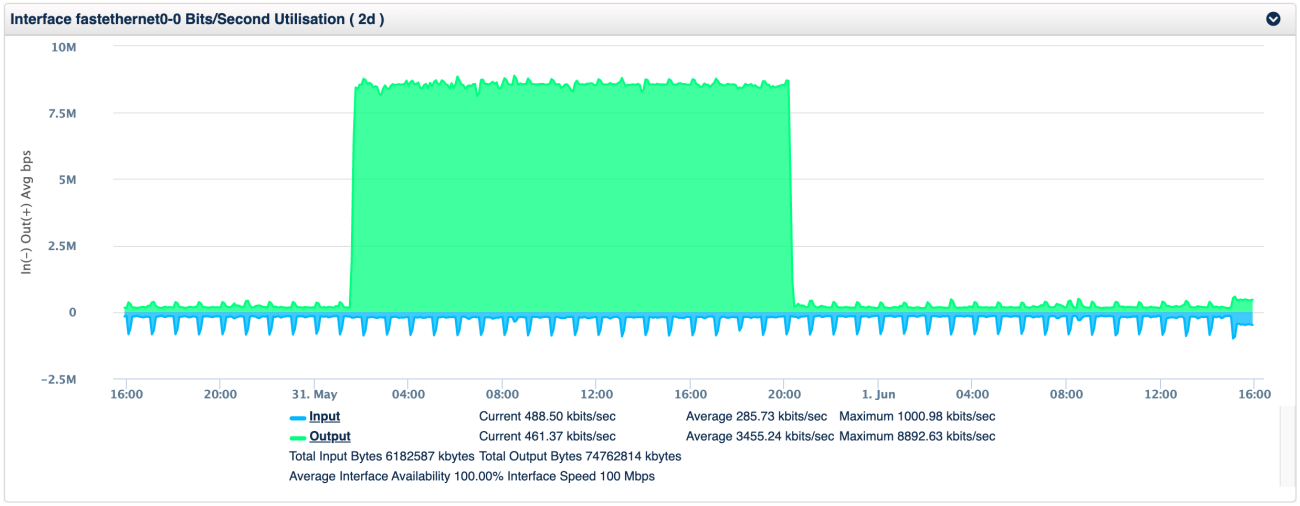
Actualmente, dos tipos de líneas de base son compatibles con la herramienta de línea base. La primera es la que podría llamarse opTrend Lite, que se basa en el trabajo de SEDS y SEDS lite de Igor Trubin , este método calcula el valor promedio para una pequeña ventana de tiempo mirando hacia atrás el número configurado de semanas, por lo que si mi línea base fue de 1 hora durante las últimas 4 semanas y el tiempo ahora es 16:40 el 1 de junio de 2020, miraría hacia atrás y reuniría lo siguiente:

- Semana 1: 15:40 a 16:40 el 25 de mayo de 2020
- Semana 2: 15:40 a 16:40 el 18 de mayo de 2020
- Semana 3: 15:40 a 16:40 el 11 de mayo de 2020
- Semana 4: 15:40 a 16:40 el 4 de mayo de 2020

Con el promedio de cada una de estas ventanas de tiempo calculado, ahora puedo construir mi línea base y comparar mi valor actual con el valor de esa línea base.

Línea base en un mismo día

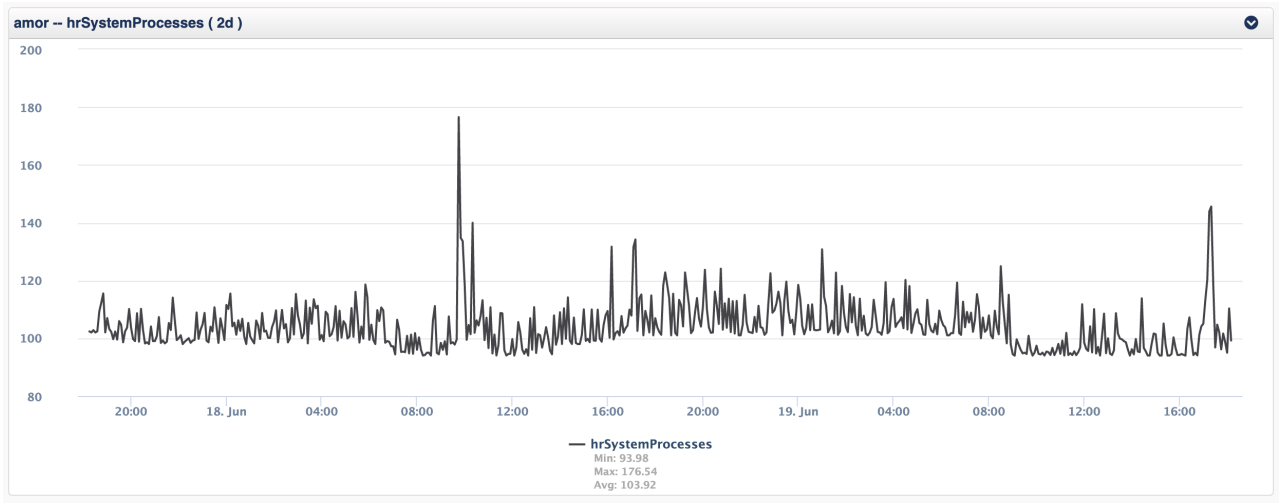
Dependiendo de la estabilidad de la métrica, puede ser preferible utilizar los datos de ese día. Por ejemplo, si su valor aumenta y disminuye, puede ser preferible utilizar solo las últimas 4 a 8 horas del día para su línea base. Tome este tráfico de interfaz como ejemplo, la tasa de entrada mientras que la tasa de salida es estable con una meseta repentina y luego es estable nuevamente.



Si este fuera un patrón semanal, la línea base de varios días sería una mejor opción, pero si esto sucede de manera más aleatoria, usar el mismo día generaría un evento inicial en aumento, entonces el evento desaparecería cuando ~ 8Mbps se volviera normal. y luego, cuando el valor volviera a bajar, se generaría otra alerta.

Línea base delta

La línea base delta solo se refiere a la cantidad de cambio en la línea base, por ejemplo, a partir de una muestra de datos de las últimas 4 horas, veríamos que el promedio de una métrica es 100, luego tomamos el valor actual, por ejemplo, el pico de 145 a continuación, y calculamos el cambio como un porcentaje, que sería un cambio del 45% que da como resultado un nivel de evento crítico.



La configuración de la línea base delta permite definir el nivel del evento en función del porcentaje de cambio, para los valores predeterminados, esto daría como resultado un Major. Puede ver la configuración en el ejemplo a continuación, esta tabla es cómo visualizar la configuración.

Cambio %	Nivel de evento resultante
10	Warning
20	Minor
30	Major
40	Critical
50	Fatal

Si el cambio es inferior al 10% el nivel será Normal, entre el 10% y el 20% Minor, por lo que hasta más del 50% se considerará Fatal.

En la práctica, este pico fue breve y utilizando el período de umbral de 15 minutos (el actual es el promedio de los últimos 15 minutos) el valor para calcular el cambio sería 136 y el cambio resultante sería del 36%, por lo que se trata de un evento importante. El período de umbral está amortiguando los picos para eliminar los cambios breves y permitirle ver los cambios que duran más.

Instalación de la herramienta de línea base

Copie el archivo Baseline-X.Y.tgz en el servidor y haga lo siguiente. La actualización será el mismo proceso.

Instalacion Baseline

```
tar xvf Baseline-X.Y.tgz
cd Baseline/
sudo ./install_baseline.sh
```

Trabajar con la herramienta de línea base dinámica y umbrales

La herramienta incluye varias opciones de configuración para que pueda ajustar el algoritmo para aprender de manera diferente según la métrica que se utilice. La herramienta viene con varias métricas ya configuradas. Es un requisito del sistema que el modelado de estadísticas se complete para la métrica que necesita para ser la línea base, así es como la API de NMIS extrae información estadística de la base de datos de rendimiento.

Opciones de configuración de línea base dinámica

La configuración de la herramienta de línea base se realiza en el archivo /usr/local/omk/conf/Baseline.nmis, la configuración predeterminada debe instalarse cuando se instala la herramienta.

Opción de configuración	Descripción	Ejemplo
baseline	Qué tipo de línea base estamos usando: "dinámica" o "delta". El valor predeterminado es dinámico, si no está definido, se usará dinámico.	delta
active	¿Está activa o no la línea base de esta métrica? Los valores son verdaderos o falsos.	true
metric	Qué punto o variable de datos NMIS equivale a un RRD DS.	RouteNumber
type	Qué sección o métrica del modelo NMIS.	RouteNumber
use_index	Para usar con ciertos tipos donde el tipo no es cómo se almacena el índice, por ejemplo, el índice para pkts_hc es interfaz, entonces cuando type=pkts_hc entonces use_index=interface. Una opción poco utilizada.	interface (cuando corresponda)
section	¿Cuál es el nombre de la sección en la información del nodo? Simplemente ejecútelo, de lo contrario, la sección debe existir.	
nodeModel	Esto es un regex que define qué modelos de NMIS deben coincidir.	CiscoRouter
event	El nombre del evento que se utilizará se establecerá de forma predeterminada en la métrica de tipo de línea base proactiva si no se proporciona ninguna.	Proactive Route Number Change
indexed	¿Esta variable está indexada o no?	false
threshold_exceeds	Se ignora si no está definido; de lo contrario, el valor TAMBIÉN debe exceder este umbral para generar un evento.	undef
threshold_period	¿Cuántos minutos se debe promediar el valor de referencia? Por ejemplo: -5 minutos es el último poll, -15 minutos sería el promedio de los últimos 15 minutos, -1 hora serían los últimos 60 minutos.	-5 minutes
multiplier	Cuántas desviaciones estándar varía la línea base.	1
weeks	La cantidad de semanas para mirar hacia atrás.	0
hours	La cantidad de horas que se incluirán en las métricas de referencia.	8
levels	La sección de levels es utilizada por el método de línea base delta para definir cuándo una cantidad de cambio desencadenará un evento y en qué nivel será ese evento.	

Ejemplo de configuración de línea base dinámica el mismo día

Así es como se vería el archivo de configuración, este ejemplo es una línea base del mismo día:

```
'RouteNumber' => {
  'active' => 'true',
  'metric' => 'RouteNumber',
  'type' => 'RouteNumber',
  'nodeModel' => 'CiscoRouter',
  'event' => 'Proactive Route Number Change',
  'indexed' => 'false',
  'threshold_exceeds' => undef,
  'threshold_period' => "-5 minutes",
  'multiplier' => 1,
  'weeks' => 0,
  'hours' => 8,
},
```

Ejemplo de configuración de línea base dinámica de varios días

Otra opción de configuración que utiliza los prefijos BGP que se intercambian con los pares BGP es del modelado systemHealth y esta es una línea base de varios días:

```
'cbgpAcceptedPrefix' => {
  'active' => 'true',
  'metric' => 'cbgpAcceptedPrefix',
  'type' => 'bgpPrefix',
  'section' => 'bgpPrefix',
  'nodeModel' => 'CircuitMonitor|CiscoRouter',
  'event' => 'Proactive BGP Peer Prefix Change',
  'indexed' => 'true',
  'multiplier' => 1,
  'weeks' => 4,
  'hours' => 1,
},
```

Ejemplo de configuración de línea base delta

Actualmente, las líneas base delta no admiten varios días, pero el valor de las horas puede ser muy grande si es necesario.

```
'hrSystemProcesses' => {
  'baseline' => 'delta',
  'active' => 'true',
  'metric' => 'hrSystemProcesses',
  'type' => 'Host_Health',
  'nodeModel' => 'net-snmp',
  'indexed' => 'false',
  'hours' => 4,
  'threshold_period' => "-15 minutes",
  'levels' => {
    'Warning' => 10,
    'Minor' => 20,
    'Major' => 30,
    'Critical' => 40,
    'Fatal' => 50
  }
},
```

Ejemplo de configuración de Delta base para paquetes de salida descartados

Actualmente, las líneas base delta no admiten varios días, pero el valor de las horas puede ser muy grande si es necesario.

```
'ifOutDiscards' => {
  'baseline' => 'delta',
  'active' => 'true',
  'metric' => 'ifOutDiscards',
  'type' => 'pkts_hc',
  'use_index' => 'interface',
  'nodeModel' => 'CiscoRouter',
  'event' => 'Proactive Output Discards (Delta)',
  'indexed' => 'true',
  'hours' => 1,
  'threshold_period' => "-15 minutes",
  'levels' => {
    'Warning' => 1,
    'Minor' => 2,
    'Major' => 3,
    'Critical' => 4,
    'Fatal' => 7
  }
},
```

Ejecución de la herramienta de línea base

Una vez instalada, la herramienta se ejecutará desde cron automáticamente, pero puede ejecutarla de forma interactiva con el siguiente comando:

```
/usr/local/omk/bin/baseline.pl act=run
```

Hay algunas opciones de depuración para ver un poco más de detalle, debug=true, debug=2 o debug=3 son los niveles actuales de verbosidad.

Se pueden agregar opciones adicionales, ejecutar la herramienta sin argumentos le indicará las opciones admitidas actualmente.

Opciones de línea de comando para nodo y grupo

Para que la herramienta solo se ejecute para un subconjunto de dispositivos, puede usar las opciones node_regex y group_regex. Estos son útiles para ejecutar la herramienta solo para un solo nodo mientras se prueban nuevas configuraciones de línea base o, en el caso de group_regex, es posible que solo necesite que la herramienta de línea base se ejecute para un subconjunto de sus dispositivos.

Ejecutando para un par de nodos usando regex:

```
/usr/local/omk/bin/baseline.exe act=run node_regex="router1|server2"
```

Corriendo para un par de grupos usando regex:

```
/usr/local/omk/bin/baseline.exe act=run group_regex="HQ|Data Center|West Coast"
```

Procesamiento automático usando Cron

La herramienta de línea base debería haber creado una configuración en el archivo /etc/cron.d/baseline, que contendrá lo siguiente:

```
#
# this cron schedule runs the baseline system every 5 minutes.
#
#
# if you DON'T want any NMIS cron mails to go to root,
# uncomment and adjust the next line
#MAILTO=prefered@domain.com
#
# m h dom month dow user command
#
# run the baseline every 5 minutes starting at 4 minutes offset from the hour.
4-59/5 * * * * root /usr/local/omk/bin/baseline.exe act=run > /usr/local/omk/log/baseline.log 2>&1
```

Uso de group_regex y cron para procesamiento paralelo

La opción de expresiones regulares grupales se puede utilizar para proporcionar procesamiento paralelo si la herramienta de línea base tarda más de 5 minutos en ejecutarse. Un ejemplo simple, sería utilizar la herramienta de referencia para todos los dispositivos centrales y de distribución en una ejecución de procesamiento y una segunda para todos los dispositivos de acceso.

```
# run the baseline every 5 minutes starting at 3 and 4 minutes offset from the hour.
3-58/5 * * * * root /usr/local/omk/bin/baseline.exe act=run group_regex="Core|Dist" > /usr/local/omk/log
/baseline1.log 2>&1
4-59/5 * * * * root /usr/local/omk/bin/baseline.exe act=run group_regex="Access" > /usr/local/omk/log/baseline2.
log 2>&1
```