

# Manual operativo para opFlow

## Descripción de opFlow

El módulo de opFlow recopila información de flujo para permitir que las organizaciones determinen cuánto de la red se está utilizando, por quién y de qué manera. Compatible con varios proveedores, entre ellos Cisco NetFlow y Juniper J-Flow. opFlow ayudará a analizar la congestión, monitorear el uso de datos altos e identificar comportamientos sospechosos.

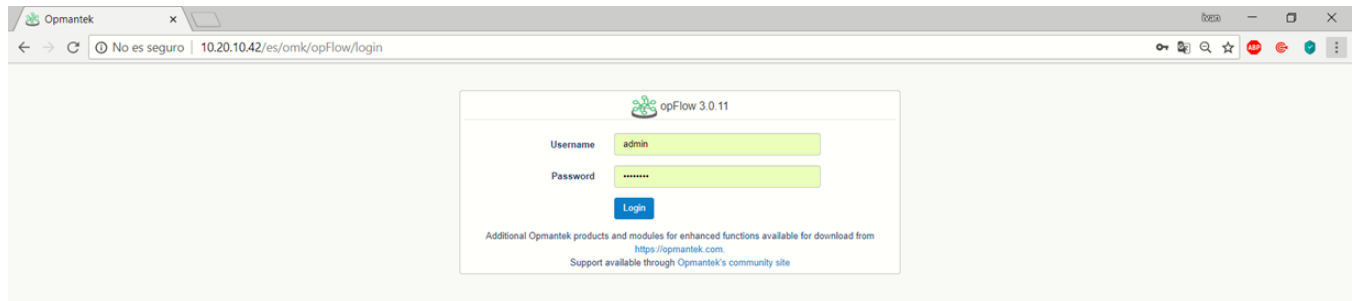
### Funcionalidades principales de opFlow

- Visión de la red: proporciona información que permite a las organizaciones determinar cuánto de la red está siendo utilizada, por quién y de qué manera.
- Identificación de cuellos de botella: rápida identificación del motivo de los cuellos de botella.
- Análisis de tráfico y seguridad: identificación rápida de patrones de tráfico inusuales.
- Planificación de la infraestructura: información clave para la planificación y el aseo de la red.
- Reducción del tiempo de inactividad: tiempo de inactividad reducido gracias a la rápida identificación del impacto de los cambios,
- Entiende el flujo de aplicaciones empresariales en la red.

## Acceso a opFlow

El acceso al portal de opFlow se deberá realizar mediante la siguiente ruta. El demonio que permite la operación del módulo es opFlow.

Link de referencia [http://IP\\_ADDRESS/es/omk/opFlow](http://IP_ADDRESS/es/omk/opFlow), tomando en cuenta que IP\_ADDRESS es la IP del servidor.

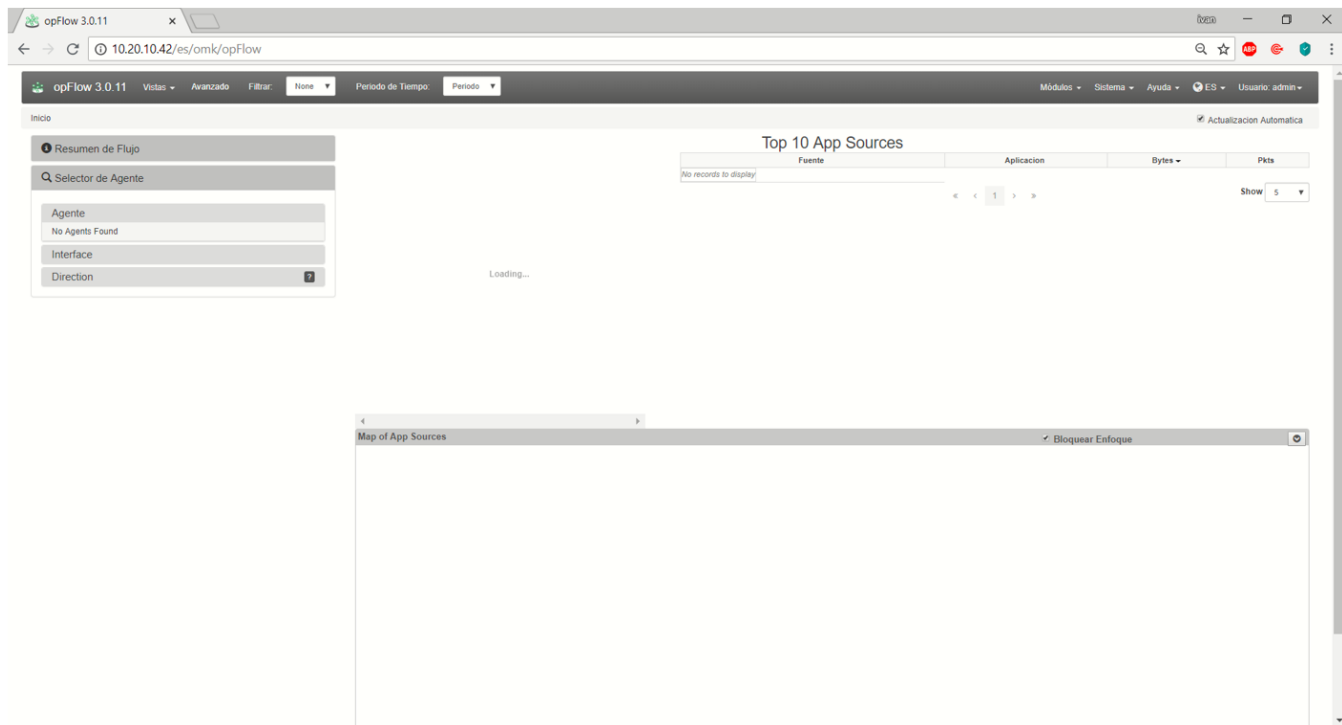


### Vista principal opFlow



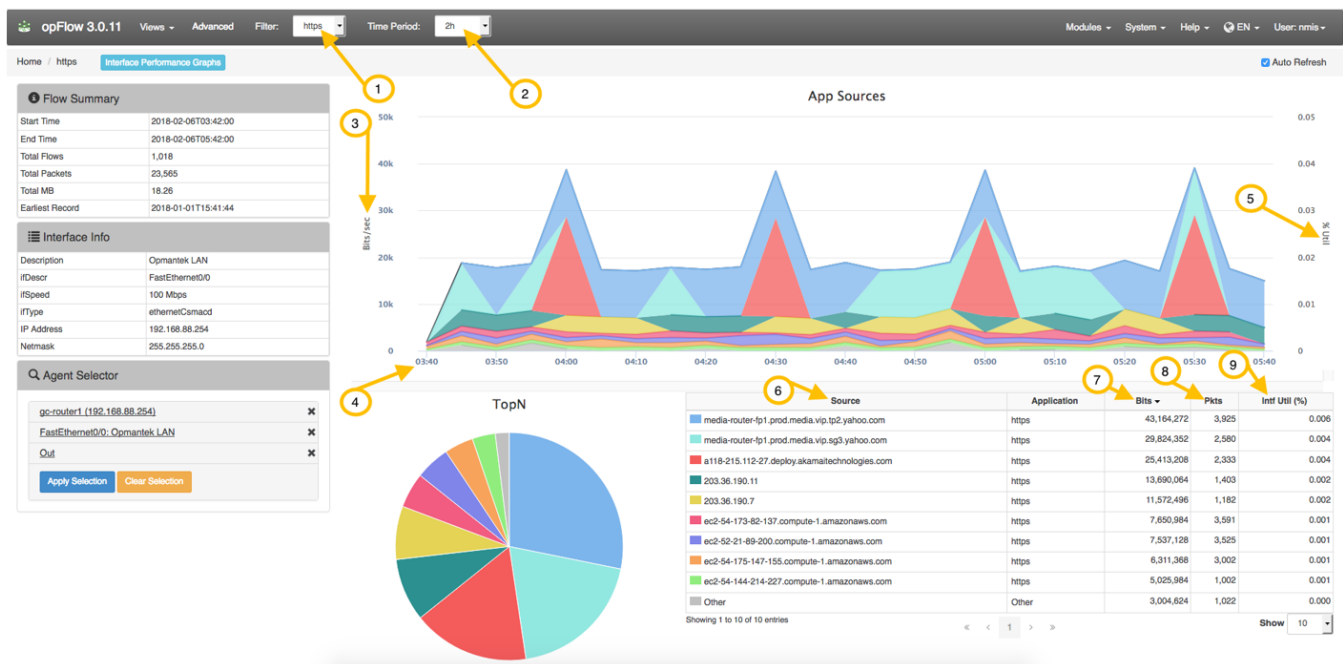
## Pantalla Principal para Visualización de flujos

Vista principal de la pantalla de opFlow, en la cual veremos el resumen de Flujo, los agentes, interfaces y dirección, También el topN de los recursos de las aplicaciones y el mapa de los recursos. Se pueden recibir flujos mediante la configuración del envío de estos hacia la IP del esclavo que se requiera. Vista sin carga de Información.



Vista de Flujo con información colectada.

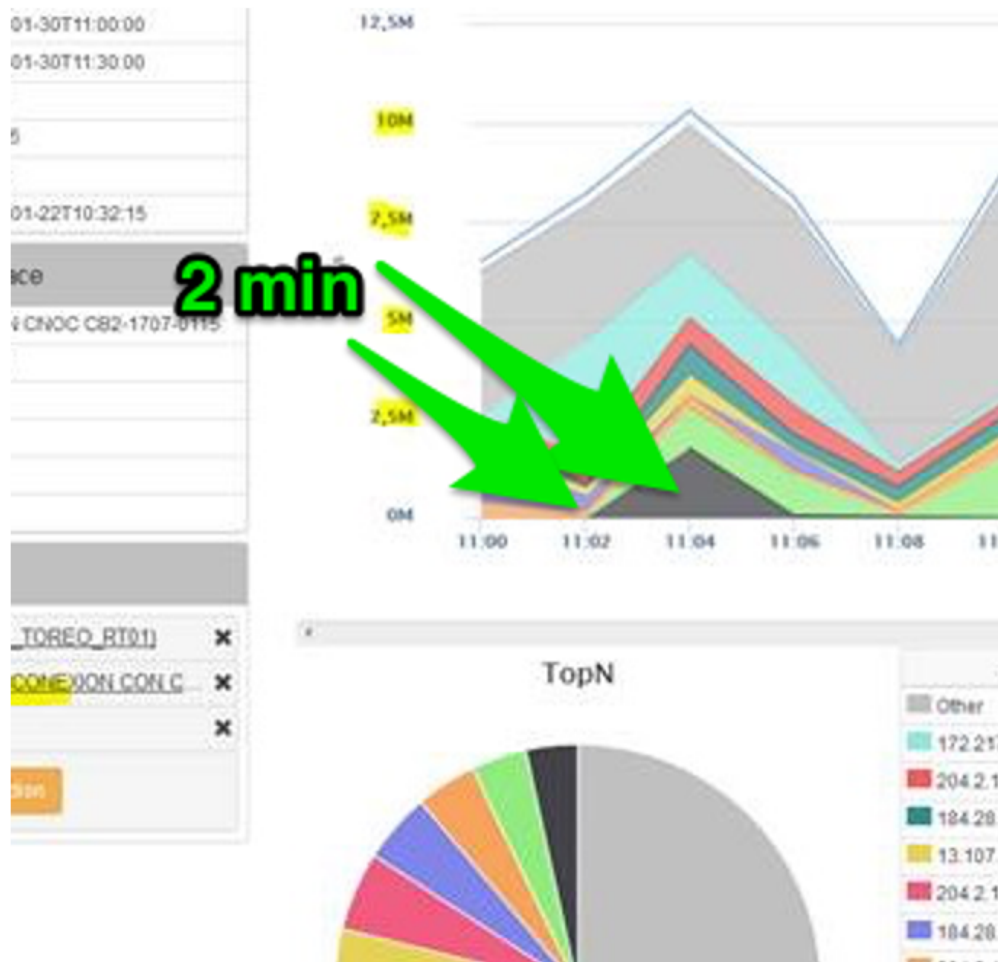
Se observan gráficamente los recursos de la aplicación, así como el TopN y el Mapa de recursos de los aplicativos, esta vista ayuda a explicar qué información se muestra en un gráfico opFlow durante un período de tiempo. Usando el siguiente ejemplo, podemos ver el resumen de flujo de un agente, en este caso se trata de un enrutador llamado gc-router1. Estamos recopilando información de flujo enviada en la interfaz llamada FastEthernet0 / 0: Opmantek LAN. Si desea ver la entrada de información de flujo, cambie esta opción a In después de seleccionar el agente y la interfaz para monitorear.



A continuación se muestra una descripción de los elementos clave para ayudar a comprender la información de opFlow.

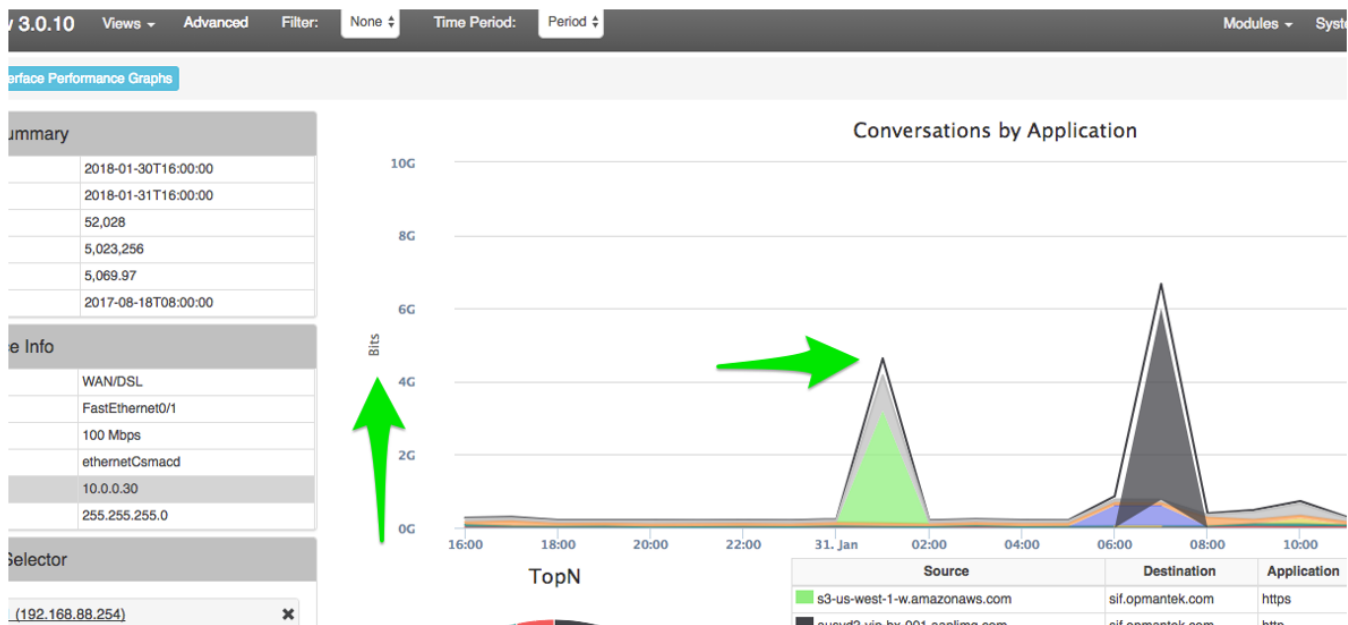
Variable	Description
(1) Filtro	Ningún filtro muestra todas las aplicaciones. La aplicación del filtro HTTPS muestra solo aplicaciones
(2) Periodo de tiempo	Seleccione el periodo de tiempo para el gráfico. (15m - 2d)
(3) Bits / Sec	Información mostrada en bits por segundo. Esto también se puede mostrar en Flujos / seg. Y en Paquetes
(4) Tiempo	Hora de inicio definida por el filtro Periodo de tiempo.
(5)% Util	Porcentaje de utilización.
(6) Fuente	La fuente de los flujos capturados.
(7) Bits	Total de bits enviados desde la fuente durante el Periodo de tiempo seleccionado.
(8) Pkts	Total de paquetes enviados desde la fuente durante el Periodo de tiempo seleccionado.
(9) Intf Util (%)	Muestra el porcentaje de utilización de interfaz de cada fuente.

Cuando la hora se muestra en la parte inferior del gráfico en la imagen de arriba (4), cada punto en el gráfico representa una cantidad de datos transferidos durante un período de tiempo. En este ejemplo anterior, el Período de tiempo se establece en 2 horas, lo que hace que la información se muestre en intervalos de 10 minutos. El período de resumen es elegido por opFlow, por lo que la cantidad de datos colocados en el gráfico es razonable (por lo general, buscamos alrededor de 42 puntos de datos por gráfico) y depende del tamaño del período total de la página. Por ejemplo, el gráfico en la imagen a continuación muestra que entre 11:02 y 11:04, se transfirieron 10 megabits. El gráfico también muestra % Util (5). Al mirar la imagen de arriba, puede ver que esos picos nunca superan el 4% de utilización.

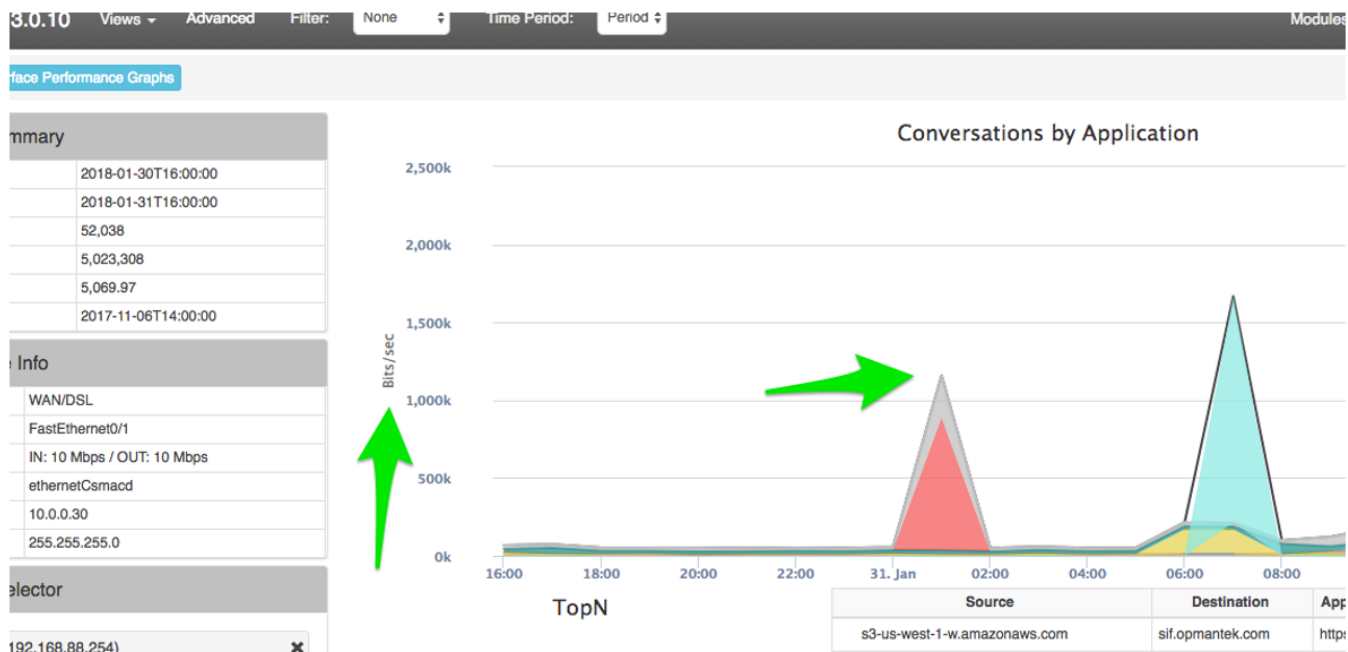


Ejemplificando la interfaz puede transferir 2 mb / s, por lo que en 2 minutos puede transferir  $(2 * 60 * 2) 240$  mb.  $10\text{mb} / 240\text{mb} = \sim .04$  o 4%. Es comprensible que esto no sea la forma en que un ingeniero de red pensaría en los datos (en la cantidad transferida). opFlow tiene una opción para mostrar el gráfico en bits / segundo en lugar de solo bits. La opción de configuración 'opflow\_gui\_graph\_over\_time\_per\_sec' => 1 cambia el gráfico.

Las siguientes imágenes muestran ejemplos de gráficos que se muestran en Bits vs. Bits/Sec para resaltar la diferencia que hace la opción de configuración opflow\_gui\_graph\_over\_time\_per\_sec. La primera imagen directamente debajo se muestra en Bits.

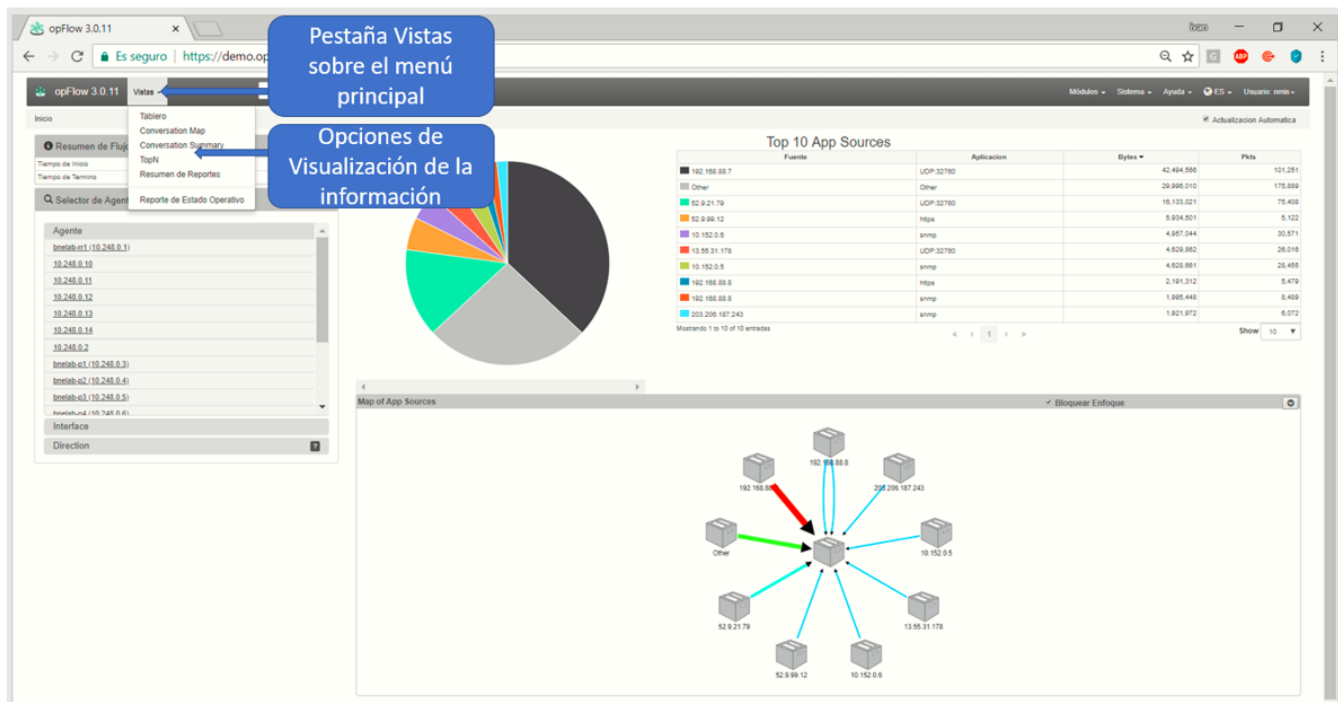


Esta segunda imagen muestra un gráfico en Bits / Sec para los mismos datos y el mismo período de tiempo. Puede ver en el cuadro de resumen a la izquierda de las imágenes de arriba y abajo que efectivamente está usando los mismos datos y los mismos Períodos de tiempo.



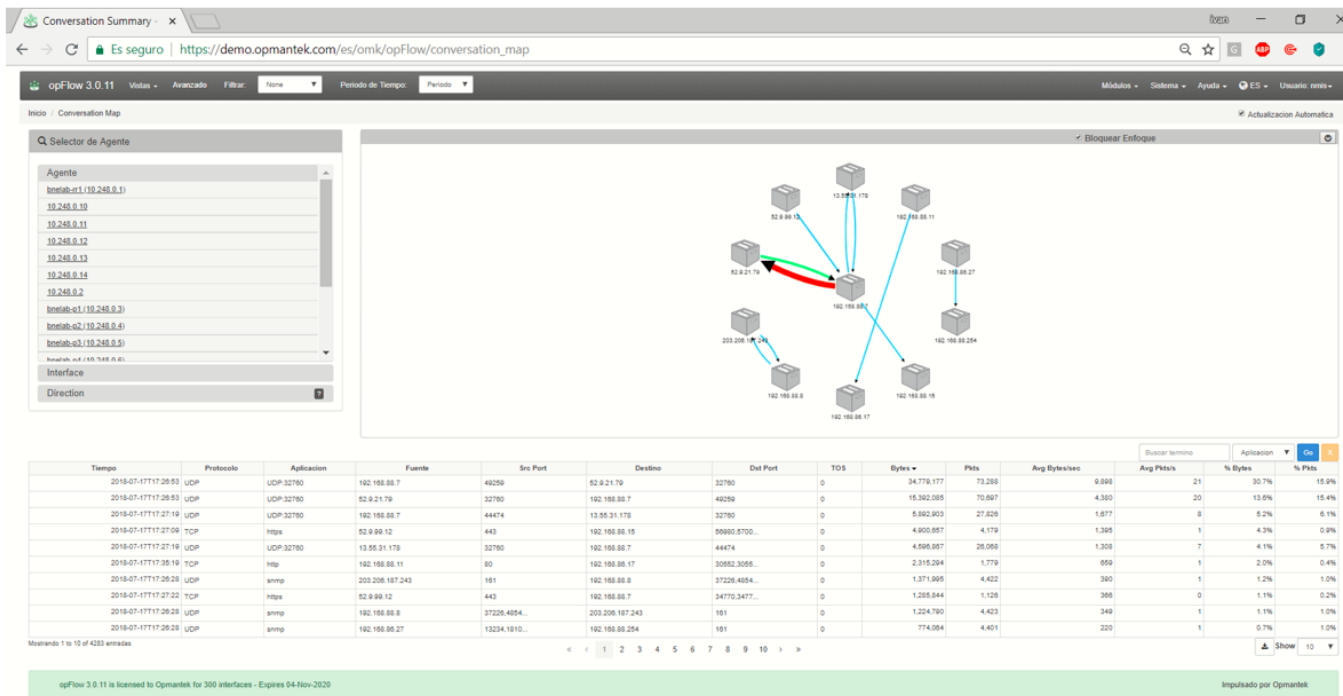
## Menú principal – Vistas

En el menú principal existe la pestaña vistas que nos muestra las distintas opciones de visualizar nuestros distintos campos y acciones sobre los nodos, interfaces, direcciones, aplicaciones, flujos promedio en Bytes y paquetes que deseamos obtener la información que es necesaria para tener control de lo que está sucediendo sobre nuestra red.



## Mapa de Conversación

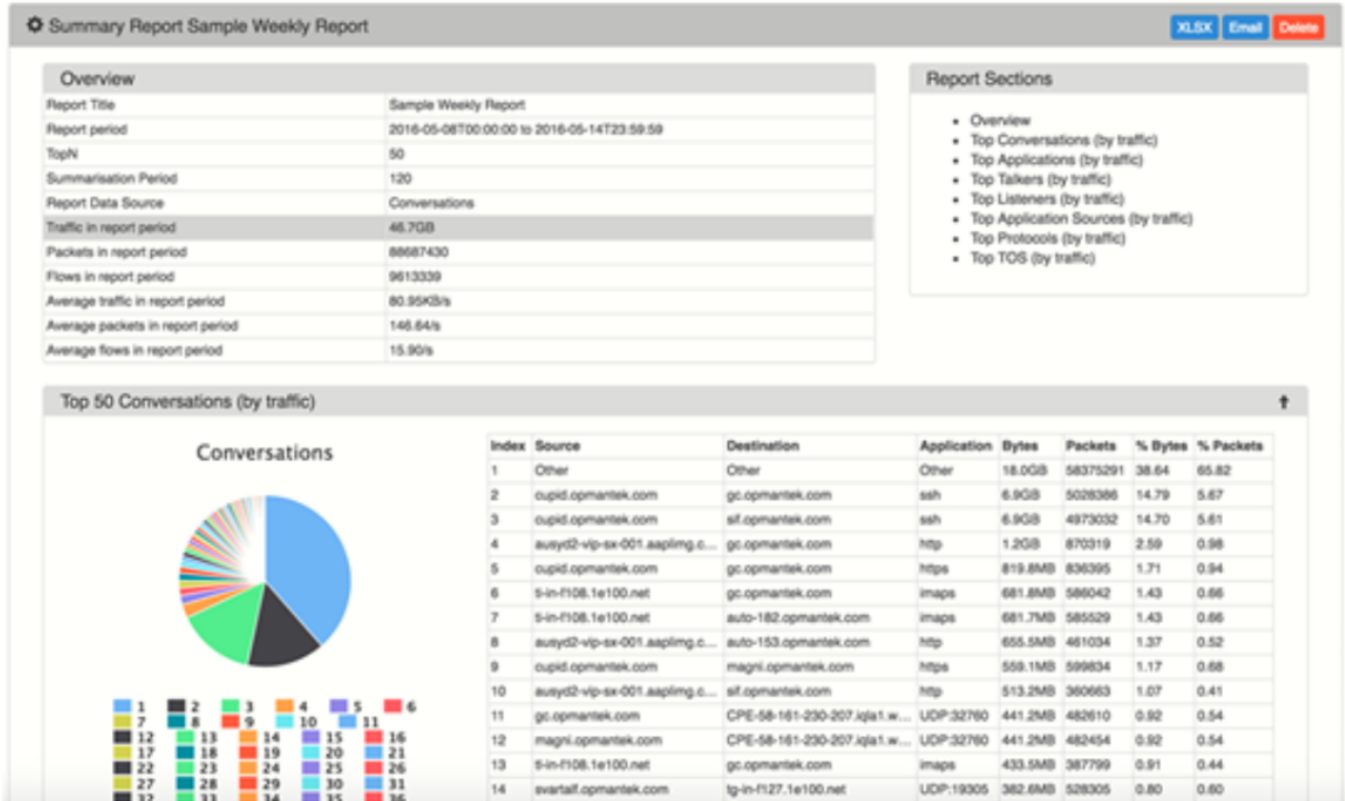
Nos muestra un mapa de nodos vecinos a la cual tienen interacción entre si los componentes y aplicaciones sobre nuestra red, mostrándonos el tiempo de conexión, protocolo utilizado, la aplicación, dirección fuente y dirección destino, tiempos de transmisión por puerto, cantidad promedio de paquetes y bytes utilizados.



## Resumen de Mapas de conversación

## Visualización de reportes

Así mismo, podemos verificar los reportes de los flujos y agregar nuevos de los dispositivos que se muestran en el portal. Ir a Generar un reporte > Views > Summary Reports > Agregar nuevo Reporte. Los reportes pueden ser exportados vía XLSX.





Advanced
×

### Specific Time

1

Dates

Enter the Start Date and Time

Enter the End Date and Time

### Time Period

2

Period

2h

### Flow Options

3

Summary Type

Application

4

Summary Field

Bytes

### Data Summarization

5

TopN

10

Cancel

Apply Selection

Variable	Descripción
(1) Fecha y hora de inicio / finalización	Seleccione la fecha y hora de inicio / finalización personalizada.
(2) Período	Seleccione el período de tiempo para el gráfico. (15m - 2d)
(3) Tipo de resumen	Tipo de información del gráfico que se muestra. (Aplicaciones, Fuentes de aplicaciones, Destinos de aplicaciones, Conversaciones por solicitud,
(4) Campo de resumen	Tipo de información del gráfico que se muestra. (Bytes, flujos, paquetes)
(5) TopN	La cantidad de elementos TopN mostrados.

## Visualización de Agentes

Son los Nodos o Equipos de los cuales se tiene conectividad establecida y recolectando información.

opFlow 3.0.11 Vistas - Avanzado Período de Tiempo: Período

Reporte de Estado Operativo

Fecha Actividad Tipo Estado Detalles

2019-07-17T19:44:47	loadCycle	completed	ok	Process 1638 done with file(s) ifmapd 201907171642
2019-07-17T19:42:48	loadCycle	completed	ok	Process 1440 done with file(s) ifmapd 201907171640
2019-07-17T19:40:48	loadCycle	completed	ok	Process 1162 done with file(s) ifmapd 201907171638
2019-07-17T19:38:41	loadCycle	completed	ok	Process 986 done with file(s) ifmapd 201907171636
2019-07-17T19:36:48	loadCycle	completed	ok	Process 635 done with file(s) ifmapd 201907171634
2019-07-17T19:34:47	loadCycle	completed	ok	Process 367 done with file(s) ifmapd 201907171632
2019-07-17T19:32:50	loadCycle	completed	ok	Process 32679 done with file(s) ifmapd 201907171630
2019-07-17T19:30:50	loadCycle	completed	ok	Process 32442 done with file(s) ifmapd 201907171628
2019-07-17T19:30:08	summaryCycle hourly	completed	ok	Process 32360 completed summary hourly (Tue Jul 17 17:00:00 2019 - Tue Jul 17 18:00:00 2019)
2019-07-17T19:28:49	loadCycle	completed	ok	Process 32196 done with file(s) ifmapd 201907171626
2019-07-17T19:26:44	loadCycle	completed	ok	Process 31995 done with file(s) ifmapd 201907171624
2019-07-17T19:24:44	loadCycle	completed	ok	Process 31707 done with file(s) ifmapd 201907171622
2019-07-17T19:22:44	loadCycle	completed	ok	Process 31573 done with file(s) ifmapd 201907171620
2019-07-17T19:20:44	loadCycle	completed	ok	Process 31372 done with file(s) ifmapd 201907171618
2019-07-17T19:18:43	loadCycle	completed	ok	Process 31137 done with file(s) ifmapd 201907171616
2019-07-17T19:16:43	loadCycle	completed	ok	Process 30987 done with file(s) ifmapd 201907171614
2019-07-17T19:14:43	loadCycle	completed	ok	Process 30867 done with file(s) ifmapd 201907171612
2019-07-17T19:12:43	loadCycle	completed	ok	Process 30265 done with file(s) ifmapd 201907171610
2019-07-17T19:10:48	loadCycle	completed	ok	Process 30072 done with file(s) ifmapd 201907171608
2019-07-17T19:08:47	loadCycle	completed	ok	Process 29749 done with file(s) ifmapd 201907171606
2019-07-17T19:06:42	loadCycle	completed	ok	Process 29549 done with file(s) ifmapd 201907171604
2019-07-17T19:04:42	loadCycle	completed	ok	Process 29317 done with file(s) ifmapd 201907171602
2019-07-17T19:02:42	loadCycle	completed	ok	Process 29169 done with file(s) ifmapd 201907171600
2019-07-17T19:00:48	loadCycle	completed	ok	Process 28807 done with file(s) ifmapd 201907171558
2019-07-17T17:58:48	loadCycle	completed	ok	Process 28395 done with file(s) ifmapd 201907171556

Mostrando 1 to 25 of 31 entradas

opFlow 3.0.11 is licensed to Opmantek for 300 interfaces - Expires 04-Nov-2020

Impulsado por Opmantek

https://demo.opmantek.com/es/omk/opFlow/agents

Pestaña sistema se encuentran las opciones de control

Agentes Custom Apps Filters

Sync Agent/Node Data

Load Time: 0.41s, Insertion Time: 0.08s, Filter Time: 0.03s, Fijos: 2126, Conversations: 370, Unique IPs: 88

Load Time: 0.32s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1193, Conversations: 453, Unique IPs: 124

Load Time: 0.85s, Insertion Time: 0.16s, Filter Time: 0.06s, Fijos: 3477, Conversations: 1214, Unique IPs: 907

Load Time: 0.85s, Insertion Time: 0.16s, Filter Time: 0.04s, Fijos: 2720, Conversations: 1117, Unique IPs: 627

Load Time: 1.85s, Insertion Time: 0.78s, Filter Time: 0.17s, Fijos: 4143, Conversations: 1947, Unique IPs: 1359

Load Time: 0.44s, Insertion Time: 0.13s, Filter Time: 0.03s, Fijos: 1636, Conversations: 882, Unique IPs: 607

Load Time: 0.31s, Insertion Time: 0.06s, Filter Time: 0.02s, Fijos: 1056, Conversations: 412, Unique IPs: 66

Summary Time: 1.05s, Aggregation Time: 0.84s, Source Conversations: 15387, Conversations: 882

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.01s, Fijos: 1007, Conversations: 381, Unique IPs: 84

Load Time: 0.31s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1034, Conversations: 408, Unique IPs: 101

Load Time: 0.52s, Insertion Time: 0.12s, Filter Time: 0.03s, Fijos: 1050, Conversations: 388, Unique IPs: 95

Load Time: 0.31s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1053, Conversations: 384, Unique IPs: 95

Load Time: 0.31s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1073, Conversations: 405, Unique IPs: 101

Load Time: 0.3s, Insertion Time: 0.06s, Filter Time: 0.02s, Fijos: 999, Conversations: 380, Unique IPs: 102

Load Time: 0.31s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1063, Conversations: 416, Unique IPs: 104

Load Time: 0.31s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1014, Conversations: 374, Unique IPs: 83

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.01s, Fijos: 1014, Conversations: 390, Unique IPs: 95

Load Time: 0.29s, Insertion Time: 0.05s, Filter Time: 0.01s, Fijos: 1042, Conversations: 384, Unique IPs: 101

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.01s, Fijos: 1051, Conversations: 390, Unique IPs: 95

Load Time: 0.32s, Insertion Time: 0.07s, Filter Time: 0.02s, Fijos: 1088, Conversations: 412, Unique IPs: 108

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.02s, Fijos: 1005, Conversations: 395, Unique IPs: 93

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.02s, Fijos: 1073, Conversations: 407, Unique IPs: 104

Load Time: 0.3s, Insertion Time: 0.05s, Filter Time: 0.01s, Fijos: 996, Conversations: 372, Unique IPs: 82

Show 25

# Visualización del nodo, IP, nombre en NMLs y la información de la ultima sincronización.

opFlow 3.0.11 Vistas - Filtro: None

Inicio / Agents

Nombre NMLs Node Name Last Info Sync

10.248.2.2	bm1ab-m1	2019-07-17T18:16:04
10.248.0.3	bm1ab-p1	2019-07-17T18:16:04
10.248.0.2		2019-07-17T18:16:04
10.248.0.4	bm1ab-p2	2019-07-17T18:16:04
10.248.0.5	bm1ab-p3	2019-07-17T18:16:04
10.248.0.7		2019-07-17T18:16:04
10.248.0.9		2019-07-17T18:16:04
10.248.0.6	bm1ab-p4	2019-07-17T18:16:04
10.248.0.11		2019-07-17T18:16:04
10.248.0.8		2019-07-17T18:16:04
10.248.0.10		2019-07-17T18:16:04
10.248.0.14		2019-07-17T18:16:04
10.248.0.12		2019-07-17T18:16:04
10.248.0.13		2019-07-17T18:16:04
192.168.88.8	bm1-server1	2019-07-17T18:16:04

Mostrando 1 to 15 of 17 entradas

opFlow 3.0.11 is licensed to Opmantek for 300 interfaces - Expires 04-Nov-2020

Impulsado por Opmantek

# Aplicativo Customizado

opFlow 3.0.11 Vistas - Filtro: None

Inicio / Custom Apps

Nombre Descripción Port Protocolo

Consolidated	Placeholder for records that were consolidated	8888	Consolidated
--------------	--	------	--------------

Mostrando 1 to 1 of 1 entradas

opFlow 3.0.11 is licensed to Opmantek for 300 interfaces - Expires 04-Nov-2020

Impulsado por Opmantek

