

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

CLASIFICACIÓN Y CONFIDENCIALIDAD

Este documento es clasificado como **“uso interno”**.

El presente documento es propiedad del grupo Keralty y está restringido a los colaboradores de la organización que cuenten con la autorización expresa para su consulta.

No se permite la reproducción total o parcial de este documento, así como su transmisión a terceros sin la autorización del responsable designado por el grupo Keralty.

LISTA DE DISTRIBUCIÓN

Este documento es de uso interno del grupo Keralty y su copia debe ser controlada y registrada de acuerdo con los procedimientos establecidos por la organización. Su distribución se debe realizar de acuerdo con la lista definida en la tabla de distribución maestra SGSI.

Todo cambio realizado a este documento debe ser controlado, documentado de acuerdo con el procedimiento de control documental y registrados en la tabla de control de cambios del presente documento.

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

TABLA DE CONTENIDO

1. OBJETIVO.....	3
2. ALCANCE.....	3
3. DEFINICIONES	3
4. CONTENIDO.	4
4.1 Arquitectura de solución de monitoreo UIM.....	4
4.2 Procedimiento de Gestión de Eventos	4
4.2.1 Caída de Equipo.....	4
4.2.2 Saturación de enlaces	5
4.2.3 Lentitud en Comunicación	13
4.2.4 Validaciones con Thousandeyes	18
4.3 Administración de los dispositivos de comunicaciones lan keralty	26
4.4 Gestión de switch keralty	26
5. CONTROL DE CAMBIOS.....	31
6. FLUJO DE APROBACIÓN.....	32

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

1. OBJETIVO.

El proceso de monitoreo y gestión de redes de Keralty es una parte de las tareas que se han generado para mitigar la no disponibilidad de las herramientas y servicios que requiere el negocio para brindar un servicio de calidad al usuario final. Estas acciones son requeridas para mantener en óptimo funcionamiento de las redes de Keralty con el fin de evitar que los incidentes menores o mayores (Caídas y saturación) que sin la respectiva gestión o análisis de causa raíz, obstaculicen el correcto funcionamiento de los servicios que se encuentran bajo la responsabilidad del área de redes y comunicaciones de Keralty en Colombia.

2. ALCANCE.

Gestionar y monitorear el inventario de switches y WLC de Keralty. Además del monitoreo de los router de los ISP que brindan servicio de comunicaciones entre sedes de los operadores Claro, Telefónica, Tigo y Sencinet en Colombia.

3. DEFINICIONES

Monitoreo: proporciona información que los administradores de redes usan para ver si una red está funcionando de manera óptima.

Gestionar: Conjunto de operaciones que se realizan para dirigir y administrar.

Incidente: cualquier interrupción en los servicios de TI de una organización que afecta cualquier elemento, desde un solo usuario o toda la empresa. De esta forma, un incidente es cualquier cosa que interrumpe la continuidad del negocio.

Tiempos de respuesta: es la cantidad total de tiempo que se tarda en responder a una solicitud de servicio

Saturación: se produce cuando la red (o parte de ella) tiene más tráfico del que puede cursar, ya que está recibiendo demasiadas solicitudes y no tiene capacidad para resolverlas todas.

Arquitectura: sistema que está compuesto por un conjunto de equipos de transmisión, programas, protocolos de comunicación y una infraestructura radioeléctrica que

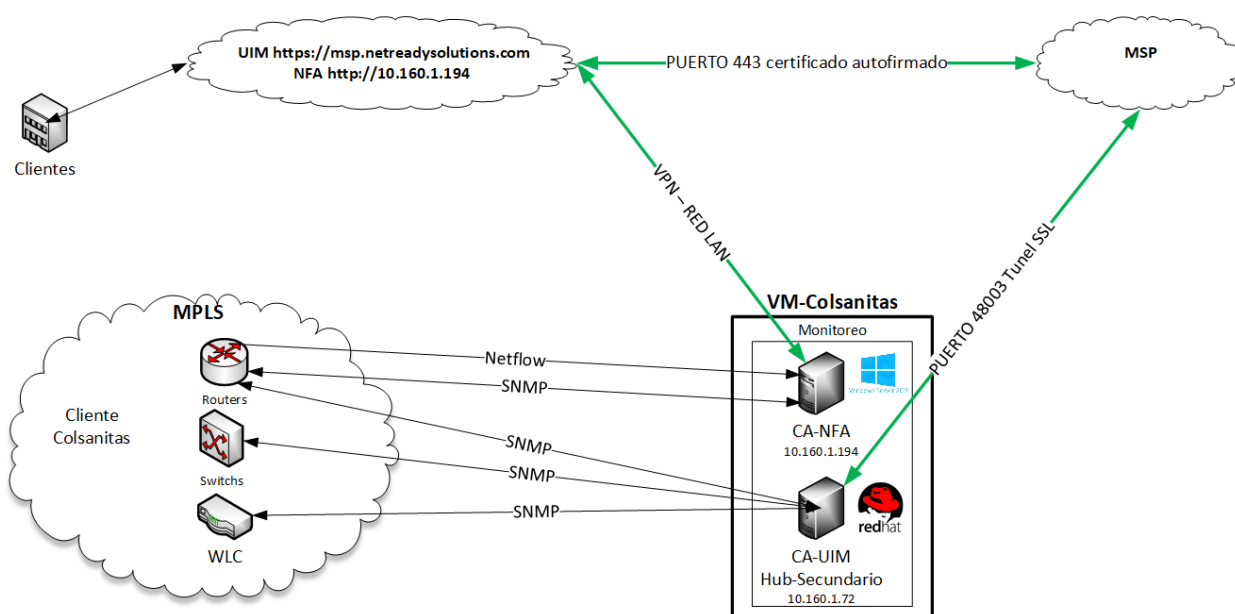
Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

posibilita la conexión y transmisión de datos a través de la red, de esta forma se logra compartir información de manera fiable y eficiente.

4. CONTENIDO.

4.1 Arquitectura de solución de monitoreo UIM

Diagrama de conexión Monitoreo de redes



4.2 Procedimiento de Gestión de Eventos

Los siguientes puntos indican los escenarios y sus procedimientos asociados, el cual debe ser realizado para la verificación y validación de una falla en la plataforma de comunicaciones.

4.2.1 Caída de Equipo


- Comprobar la vigencia de la alarma y la alcanzabilidad del dispositivo. Esto se realiza a través de un PING a la dirección IP del equipo monitoreado.

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Si la validación anterior corrobora la información de la caída, se procede a realizar el respectivo descarte de primer nivel, llamando a los funcionarios de la sede. La finalidad del primer nivel es determinar si existe una causa local que origine el incidente como por ejemplo una falla eléctrica o equipos apagados.
- Luego de realizado el contacto inicial y validado las posibles causas del incidente, se procede a redactar un correo electrónico informando de los detalles y relacionando el contacto que dio la información.
- Dependiendo de la causa del incidente el correo electrónico será informativo o de escalamiento. Si el problema es de la sede (Falla Eléctrica o problemas con la UPS), será un correo informativo. Si el problema se asume de problemas con el proveedor (por no existir una falla de energía o apagado de los equipos), se procede a copiar a los buzones de correo de CGP de su respectivo ISP en horario laboral y de Overtime de cada proveedor (Claro y Telefónica) fuera del horario laboral solicitando la revisión. Cabe aclarar que el proveedor no realizará ninguna acción si no se realiza el descarte del primer nivel.

4.2.2 Saturación de enlaces

- Se corroborará la información de los enlaces con alarma de saturación en la herramienta de monitoreo CA UIM, revisando cuál es el porcentaje de utilización. Es de resaltar que el umbral acordado reportar al cliente, es una utilización igual o superior al 90% del bandwidth de la interfaz, por un espacio de tiempo de 15 minutos continuos. Es de aclarar que este tipo de reporte por acuerdo con el cliente se genera solamente por demanda esto con el fin de darle tratamiento más especializado a la hora de tomar acciones para la sede afectada.
URL: <https://msp.netreadysolutions.com>
- Se utilizará la siguiente estructura definida para la elaboración del correo.

 martes 06/08/2019 11:38 a. m.
Héctor Briceño
RE: REPORTE LENTITUD DEL APLICATIVOS OFICINA BARRANCA

Para Soporte Colombia; Luz Mary Gamba Reyes; Robinson Rojas Duran
CC Miguel Angel Leon Garcia; Viviana Andrea Cortes Duran; Martha Argenis Rivera; Flor Angela Beltran Montanez; Edna Margarita Puerto Rubio; Genny Catalina Quintero Carrillo; Misael Arbey Conde Vargas; Antonio Jose Orduz Barrera; Robert Aza; Diego Alexander Suarez Barrera

Buen día

Señores en la revisión solicitada ayer en la tarde adjunto grafica de consumo y conversaciones de la sede con mayor consumo donde se sigue evidenciando la ip 192.168.36.36.

Conclusiones

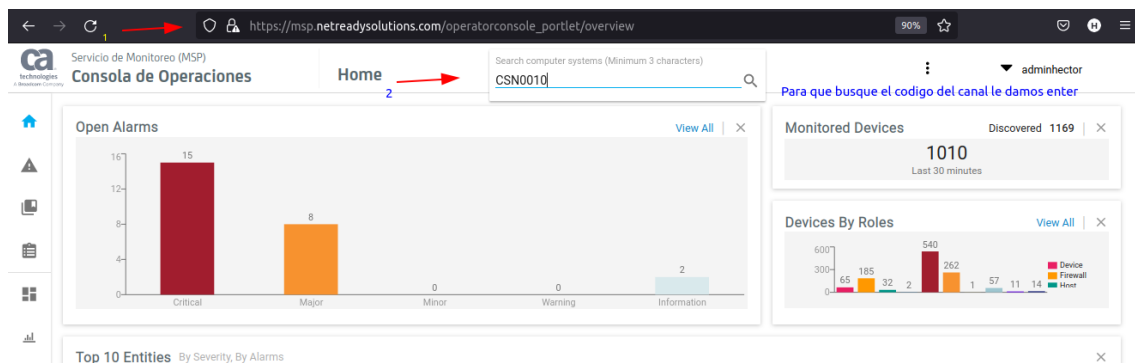
- En el detalle de la revisión se evidencian consumos a distintas sedes al host de QFlow y esto afecta el rendimiento del canal.
- No se observa según lo que se reportó en el correo adjunto baja en el consumo de la sede con el equipo apagado.
- Se sugiere realizar un cambio en la dirección ip del host para revisar el comportamiento luego del cambio.

- Se adjuntarán las gráficas de utilización de la sede relacionada. Donde se pueda diferenciar el tipo de consumo que es expresado en bits y que corresponde al ancho de banda utilizado por el canal en las últimas 24 horas para corroborar el ancho de banda del canal revisaremos el archivo de inventario de enlaces <https://docs.google.com/spreadsheets/d/1rvphF->

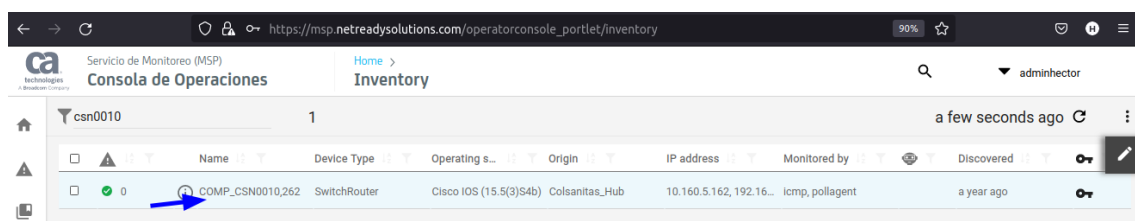
Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

OvaYPaXyqqhFiWezShyDPathYpMiCPSGUkg8/edit?pli=1#gid=1038081887
donde lo se ubica por el código o IP y sabremos el porcentaje utilizado.

- Login en herramienta de monitoreo UIM y luego buscar el código o ip del enlace con el reporte recibido.

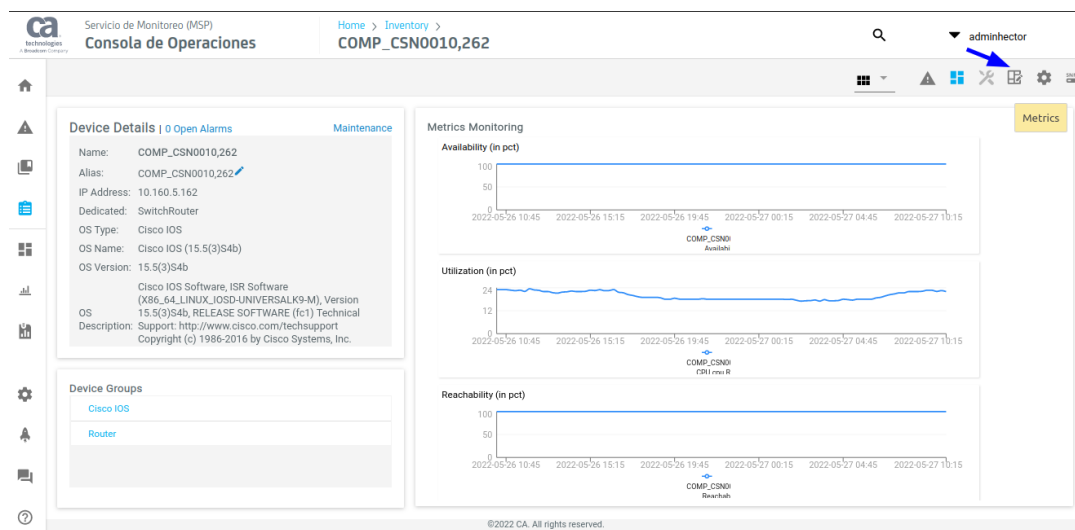


1. Al encontrar el dispositivo se da clic sobre el nombre y aparecerá la información del dispositivo.



Name	Device Type	Operating s...	Origin	IP address	Monitored by	Discovered
COMP_CSN0010,262	SwitchRouter	Cisco IOS (15.5(3)S4b)	Colsanitas_Hub	10.160.5.162, 192.16...	icmp, pollagent	a year ago

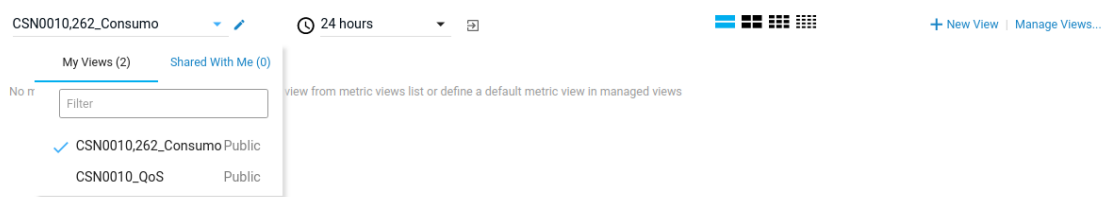
2. Posteriormente se da clic al siguiente icono para ver las vistas donde se puede observar la saturación o las gráficas de calidad de servicio.



Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

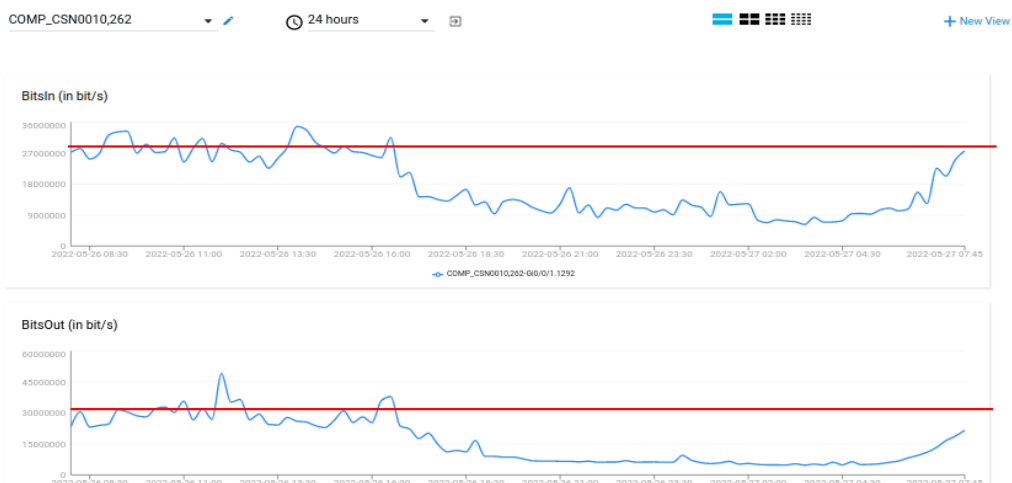
3. El sistema desplegará el siguiente cuadro para ubicar las gráficas, y allí se encuentra la gráfica de consumo y la de calidad de servicio. En modo de ejemplo a continuación se evidencia la nombrada CSN0010_Consumos

Device Metrics COMP_CSN0010,262



4. Se podrán validar las gráficas de consumo de la sede.

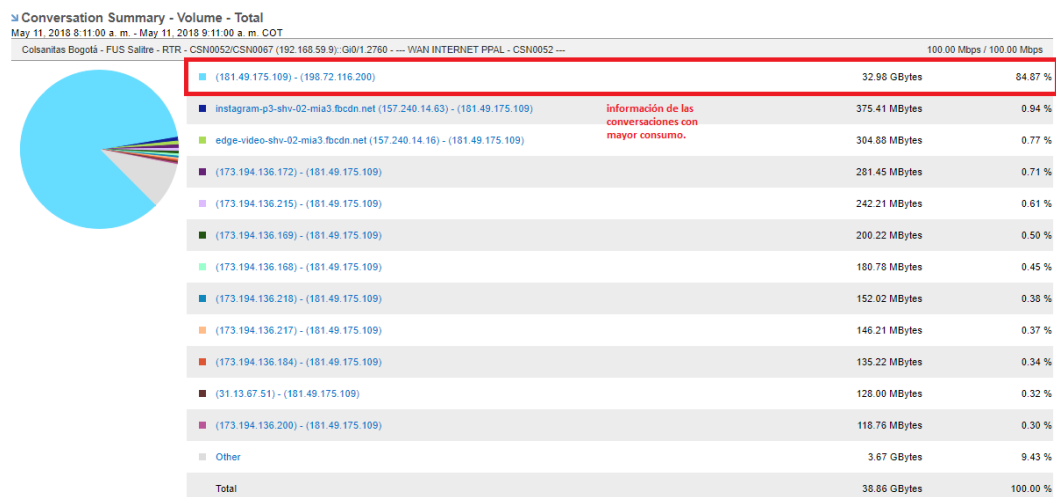
Device Metrics COMP_CSN0010,262



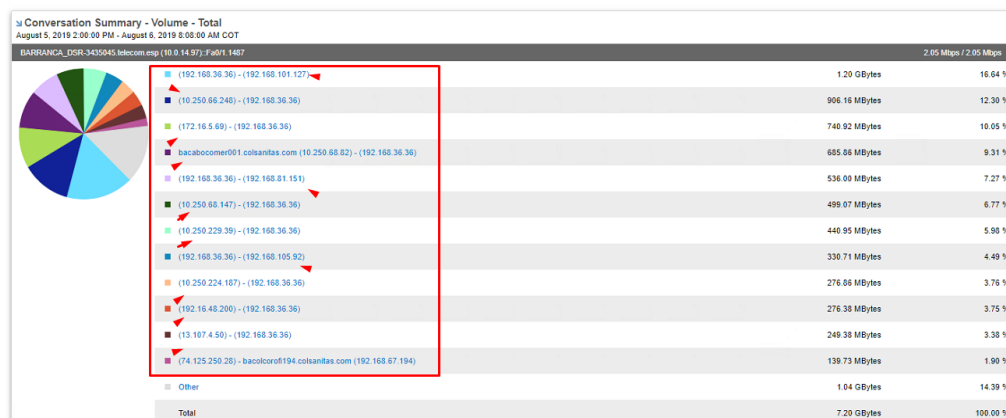
Luego que la gráfica de utilización permita identificar el horario en que ocurrió o está ocurriendo la saturación se utilizara la herramienta CA Network Flow Analysis (CA NFA) para identificar las conversaciones que están generando la saturación en el canal, se ubica el router y la interface a diagnosticar que por lo general será la que esté identificada en su descripción como “WAN” y capturar la gráfica de conversaciones como se muestra a continuación.

http://10.160.1.194

- I. Al revisar las conversaciones existen 2 tipos de situación que pueden presentarse ya que la causa de la saturación puede ser una conversación en particular como se ve en la gráfica 1
- II. La otra que se puede presentar y que es la más recurrente en Keralty son las conversaciones de varios hosts de la sede contra un host en particular grafica 2.



Grafica 1



Grafica 2

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

Host Summary - Volume - To	
August 5, 2019 2:00:00 PM - August 6, 2019 8:00:00 AM COT	
BARRANCA_USR-3435045 Intelcom.esip (10.0.14.97): Fa0/1.1487	2.05 Mbps
(192.168.36.36)	6.34 GBytes 88.27 %

Grafica 3

- En caso de ubicar información de direccionamiento IP público, se utilizan herramientas en internet como por ejemplo <https://www.whois.com/whois>, <https://network-tools.com/> o <https://talosintelligence.com/> donde se podrá ubicar la información que permita orientar el uso del tráfico. En la siguiente imagen un ejemplo de la búsqueda de información.

Seguro | <https://www.whois.com/whois/181.49.175.109>

DOMAINS HOSTING CLOUD WEBSITES EMAIL SECURITY WHOIS SUP

Whois IP 181.49.175.109 Updated 1 day ago

```
% Joint Whois - whois.lacnic.net
% This server accepts single ASN, IPv4 or IPv6 queries
% LACNIC resource: whois.lacnic.net

% Copyright LACNIC lacnic.net
% The data below is provided for information purposes
% and to assist persons in obtaining information about or
% related to AS and IP numbers registrations
% By submitting a whois query, you agree to use this data
% only for lawful purposes.
% 2018-05-09 12:09:46 (BRT -03:00)

inetnum: 181.48/13
status: allocated
aut-num: N/A
owner: ● Telmex Colombia S.A. ●
ownerid: CO-ACSA-LACNIC
responsible: Operaciones Core IP
address: CLARO FIJO COLOMBIA - Cra 68A No. 24B-10, 11111,
address: 11111 - Bogota - DC
country: CO
phone: +57 01 7480000 []
owner-c: ATI
tech-c: ATI
abuse-c: ATI
inetrev: 181.49/16
nserver: NS3.TELMEXLA.NET.CO
nsstat: 20180508 AA
nslastaa: 20180508
nserver: NS2.TELMEXLA.NET.CO
nsstat: 20180508 AA
nslastaa: 20180508
created: 20110502
changed: 20110502
```

https://www.talosintelligence.com/reputation_center/lookup?search=181.49.147.130

TALOS

Lookup data results for IP Address 181.49.147.130

IP & Domain Reputation Overview File Reputation Lookup Email & Spam Data Malware Data Reputation Support

LOCATION DATA

🇪🇸 Santiago de Cali, Colombia

OWNER DETAILS

IP ADDRESS 181.49.147.130

FW/DREV DNS MATCH No

NETWORK OWNER Telmex Colombia S.A.

REPUTATION DETAILS

EMAIL REPUTATION ● Neutral

WEB REPUTATION ● Neutral

WEB CATEGORY

	LAST DAY	LAST MONTH
SPAM LEVEL	None	None
EMAIL VOLUME	0.0	0.0
VOLUME CHANGE	0%	

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Luego de realizar las validaciones, todos los correos de saturación deben incluir los correos de las personas que solicitaron la revisión junto con el equipo de Comunicaciones de Keralty y el tercero designado para que tenga conocimiento del incidente.
- En el caso de visualizarse conversaciones asociadas a actualizaciones de OS Windows o Antivirus en horario hábil, se debe generar un correo electrónico e incluir la siguiente nota mostrada a continuación, modificando, dependiendo del tipo de servidor:

Buzón de correo de

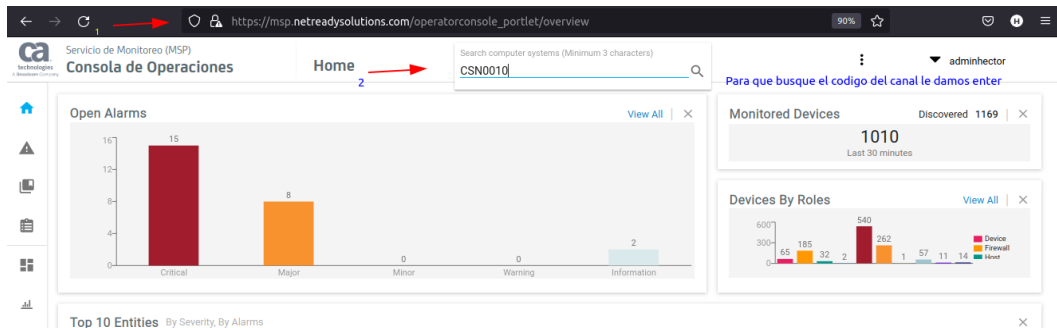
Actualizaciones de Windows, a través del líder de microinformática

Actualizaciones de Antivirus Seguridad de la información

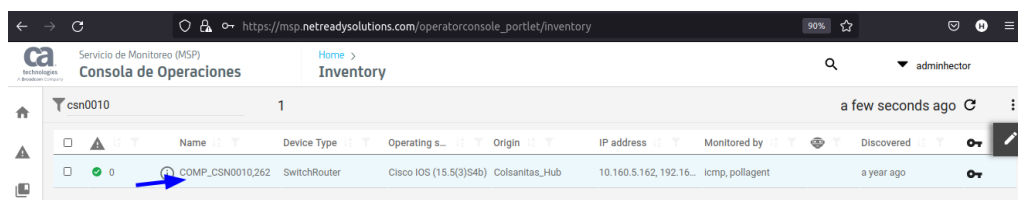
Mensaje en el Correo: @XXXXX buen día, agradecemos su amable colaboración validando los procesos de la consola de antivirus o actualizaciones de Windows de la ciudad de “Nombre de la ciudad” y para ambos casos anexar la dirección ip del host. Como se observa hay conversaciones que están realizando actualización.

- En el caso de visualizarse conversaciones asociadas a visualización de cámaras de seguridad en horario hábil, se debe generar una comunicación al área de redes y comunicaciones de Keralty que permita informar de la situación para que se tomen los correctivos pertinentes.
 - En caso de que la anterior validación no permita establecer algún motivo de la lentitud en particular de una aplicación se deberá realizar la revisión de las gráficas de calidad de servicio en caso de que el canal tenga configurado esta política con el fin de establecer si las políticas principales de aplicaciones tienen un descarte de paquetes considerables que no permitan un correcto funcionamiento de la aplicación.
- I. Esto se podrá validar ingresando al cuadro de búsqueda de la página principal de nuestra herramienta de monitoreo y colocaremos el código del canal de la sede o la IP del Router en caso de tenerla.

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

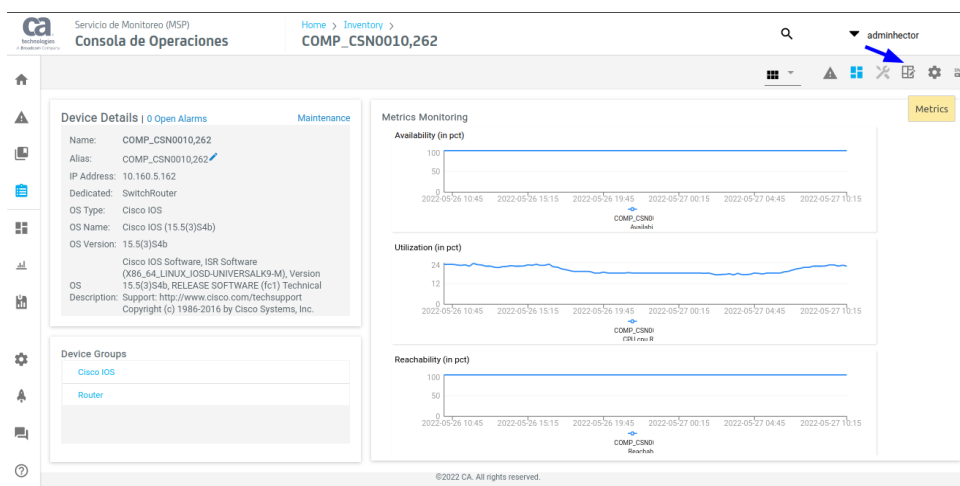


- II. Al encontrar el dispositivo se da clic sobre el nombre y aparecerá la información del dispositivo.



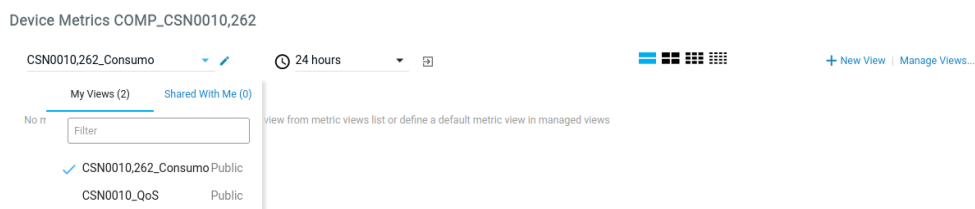
Name	Device Type	Operating s...	Origin	IP address	Monitored by	Discovered
COMP_CSN0010,262	SwitchRouter	Cisco IOS (15.5(3)S4b)	Colsanitas_Hub	10.160.5.162, 192.16...	icmp, pollagent	a year ago

- III. Posterior se da clic al siguiente icono para ver las vistas donde podemos observar la saturación o las gráficas de calidad de servicio.

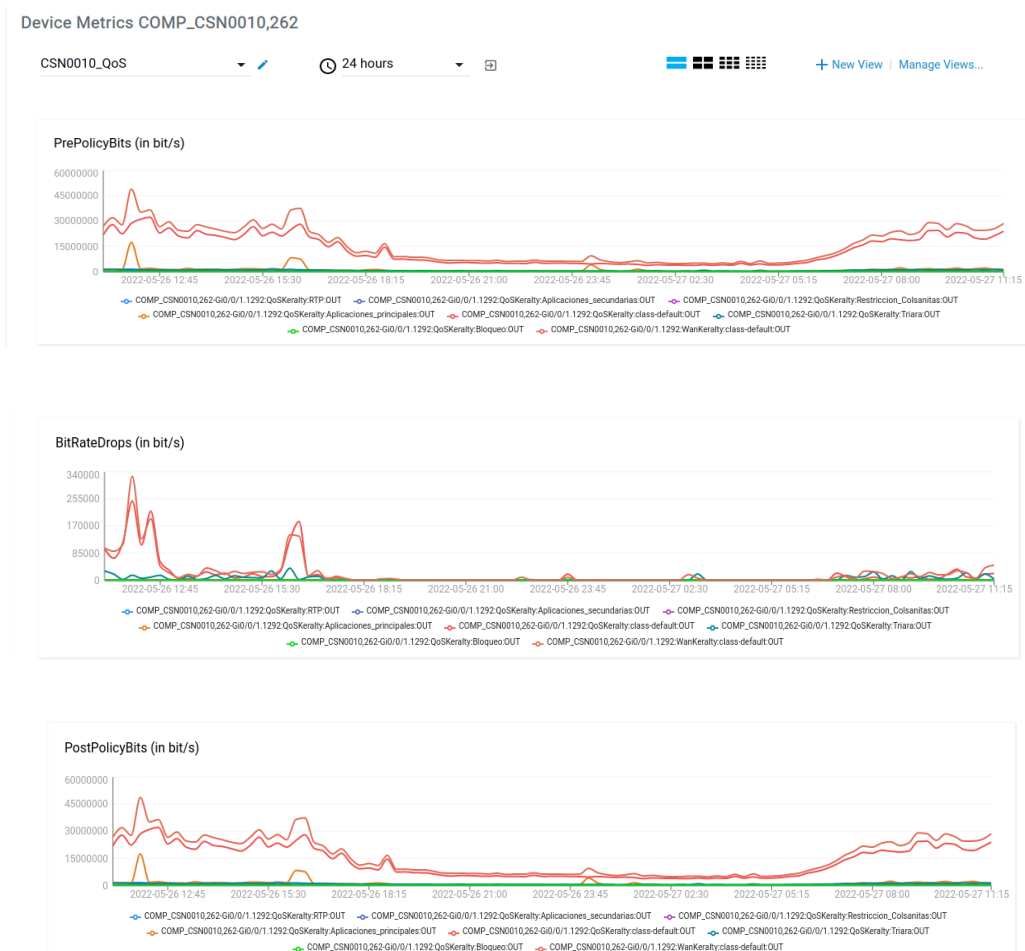


Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- IV. Aparecerá el siguiente cuadro para ubicar las gráficas, en donde se encuentra la gráfica de consumo y la de calidad de servicio. Para este ejemplo tomaremos la nombrada CSN0010_QoS

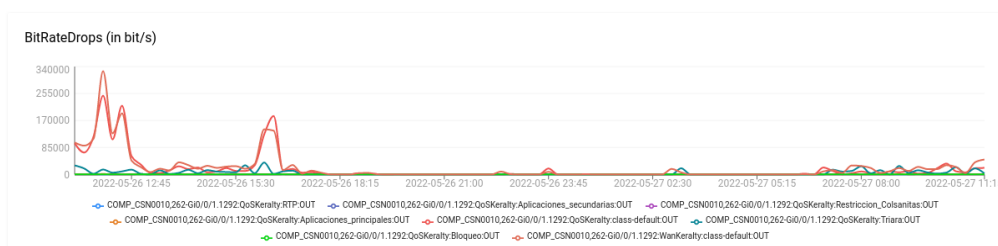


- V. En el menú desplegable se encuentran las gráficas de las métricas PrepolicyBits, Bitratedrops y PostpolicyBits.



Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

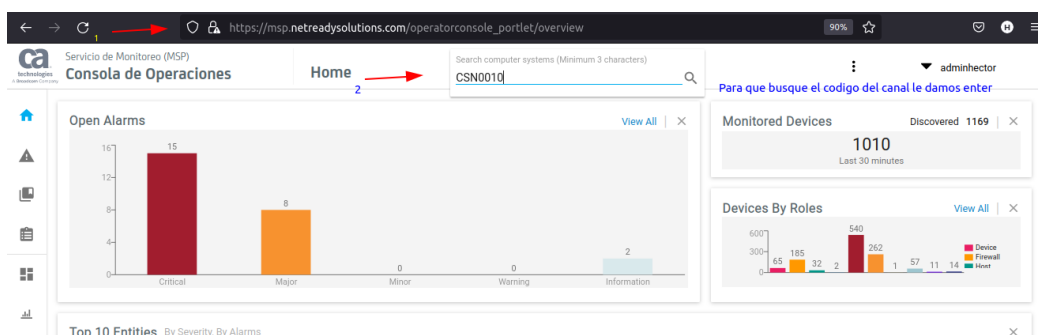
- VI. Al abrirse la página del detalle se observará primero la métrica Bitratedrops y la mayoría de los casos para las categorías Aplicaciones principales, secundarias y Triará el valor no debe ser superior a 0.



Si el valor es diferente de 0 se deberá evaluar el ancho de banda vs los consumos de cada categoría de la política y sugerir un aumento de la capacidad para evitar cuellos de botella y lentitud en la información.

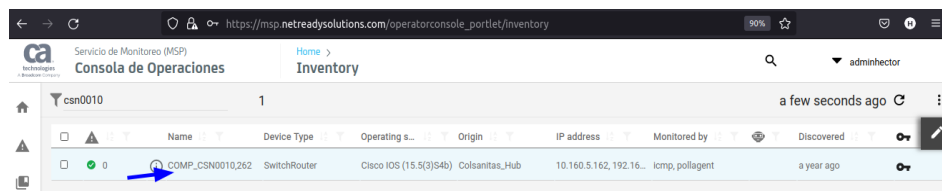
4.2.3 Lentitud en Comunicación

- Como primera medida se realizará contacto con el o los afectados, buscando determinar si el problema es de toda la sede o algo puntual del usuario. Adicionalmente es importante precisar el problema a la aplicación que reporta lentitud: Correo Electrónico, Aplicación Corporativa, Aplicación del Negocio, etc., y poder abordar el diagnóstico de una forma más efectiva.
 - En el caso de ser conocida la sede donde se origina la lentitud, se realiza una validación de la utilización, errores y descarte de paquetes del canal WAN esta se realizará con la vista del
1. Paso 1

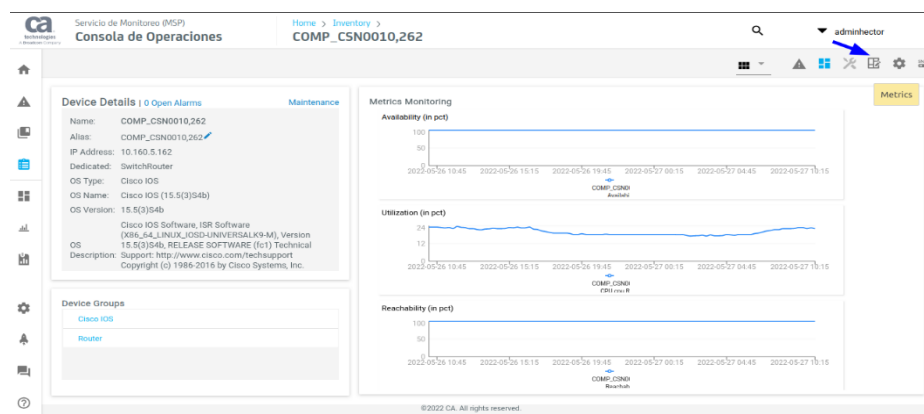


Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

2. Paso 2

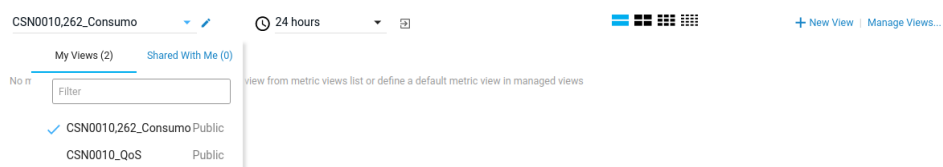


3. Paso 3



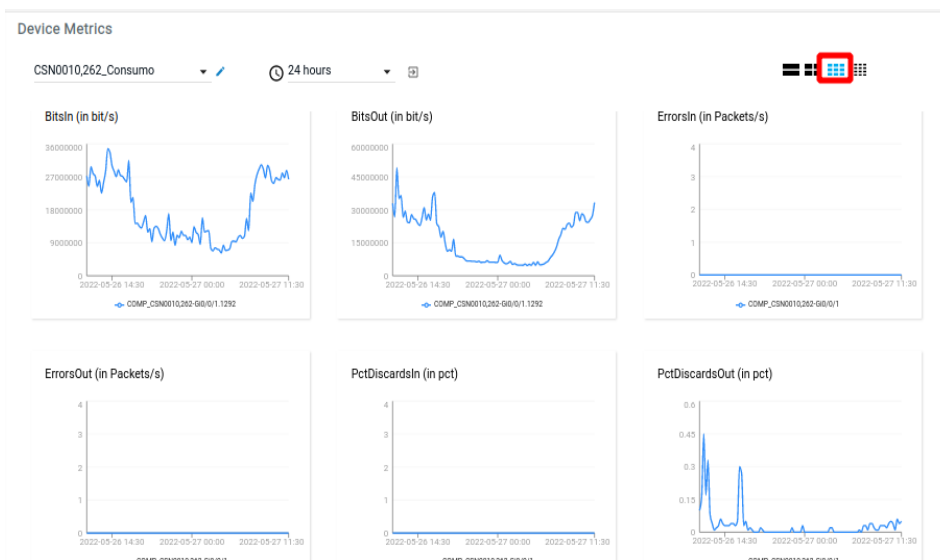
4. Paso 4 opción CSN0010,262_Consumos

Device Metrics COMP_CSN0010,262



Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

5. Vista de las gráficas de consumo junto con las gráficas de errores y descarte de paquetes.



- En caso de existir saturación, se realiza un análisis de tráfico para determinar las causas y validar si es tráfico corporativo o no corporativo. En los casos de errores y descarte de paquetes se debe generar un caso al proveedor.
- En el caso de no ser conocida la sede, se debe llamar al usuario que reporta el incidente y solicitar su dirección IP. Esta información permitirá cotejar con el inventario de direccionamiento IP Keralty o realizar una traza hacia la ip suministrada y con ayuda de la herramienta de monitoreo establecer a qué sede pertenece y conocer la sede donde se origina el incidente. Una vez conocida la localidad se procede al paso b.

```

C:\Users\adminca>tracert -d 192.168.77.53

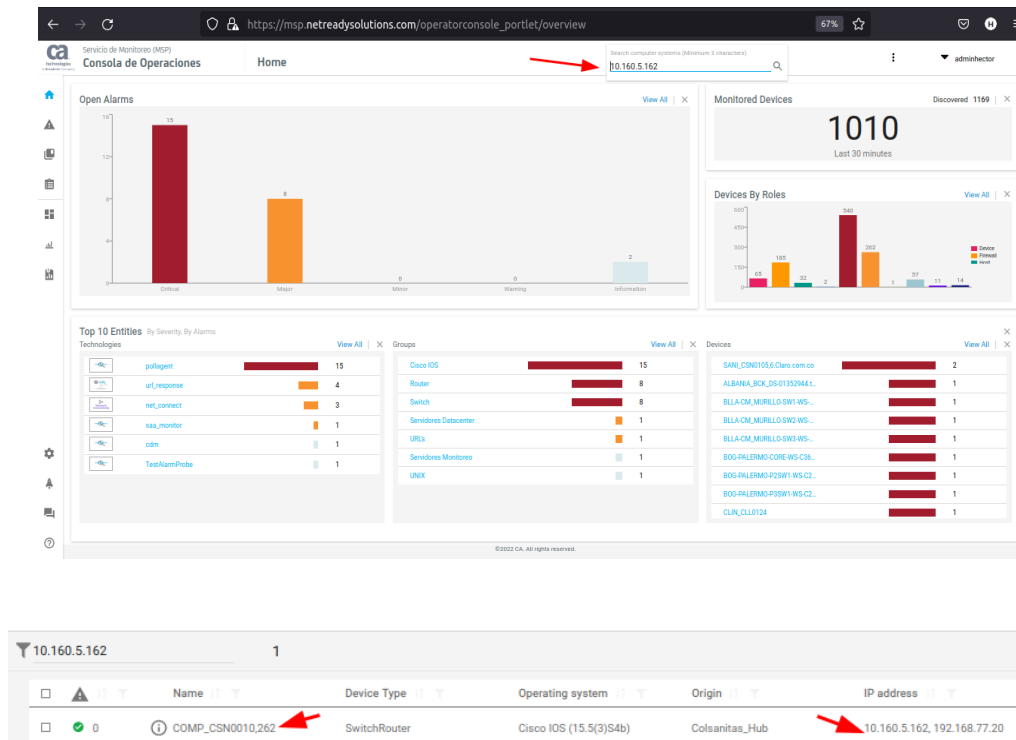
Tracing route to 192.168.77.53 over a maximum of 30 hops

  1    <1 ms    <1 ms    <1 ms    172.18.48.129
  2    <1 ms    <1 ms    <1 ms    172.22.129.187
  3    <1 ms    <1 ms    <1 ms    10.161.251.21
  4    3 ms     2 ms     3 ms     10.14.7.65
  5    3 ms     3 ms     3 ms     10.160.5.162
  6    4 ms     10 ms    8 ms     192.168.77.53

Trace complete.
  
```

Versión: 3.0	<div> <div>  </div> </div>
Fecha: 14-05-2024	
Código: SIG-TIRC-CKE-PL02	

POLÍTICA MONITOREO REDES



- En el caso que no exista saturación en el enlace WAN, se debe ubicar el puerto de red que conecta al usuario. Esta búsqueda se realiza a través del MAC Address en los switches de red. Con la dirección IP del usuario, se realiza una búsqueda en el core switch de la MAC Address (`show arp | include "dirección_ip"`). Posteriormente se realiza la búsqueda del puerto de red (`show mac address-table | include "mac-address"`).
- Se deberá realizar un ping desde el Switch donde se ubica el host, al destino y al host indicado por el usuario anteriormente con un paquete con peso superior a 1024 para establecer qué tipo de problemas se puede estar presentando o generando.

[illegible]

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Una vez ubicado el puerto de red, se valida lo siguiente.

```

CALI-TEQ-EPS-SW2-C2960X-24P-S#sho int Gi1/0/11
GigabitEthernet1/0/11 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 689c.e2fb.df8b (bia 689c.e2fb.df8b)
  MTU 1500 bytes, BW 100000 kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:18, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 76
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 30000 bits/sec, 2 packets/sec
  5 minute output rate 39000 bits/sec, 6 packets/sec
    28750985 packets input, 19746071898 bytes, 0 no buffer
    Received 167774 broadcasts (154345 multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 154345 multicast, 0 pause input
    0 input packets with dribble condition detected
  37601318 packets output, 14883242808 bytes, 0 underruns
    0 output errors, 0 collisions, 1 interface resets
    55951 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out

```

```

--- 192.168.44.93 ping statistics ---
 69 packet(s) transmitted
 54 packet(s) received
 21.73% packet loss
 round-trip min/avg/max = 8/9/19 ms

[SW_TEQUENDAMA_EPS_CALI_48P]dis int GigabitEthernet1/0/45
GigabitEthernet1/0/45 current state: UP
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 7848-595e-9084
Description: GigabitEthernet1/0/45 Interface
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
100Mbps-speed mode, full-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Broadcast MAX-ratio: 100%
Unicast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Allow jumbo frame to pass
PVID: 101
Mdi type: auto
Port link-type: hybrid
  Tagged VLAN ID : 100
  Untagged VLAN ID : 101
Port priority: 0
Last clearing of counters: Never
Peak value of input: 51013 bytes/sec, at 2019-07-22 12:05:01
Peak value of output: 230344 bytes/sec, at 2019-06-27 12:08:22
Last 300 seconds input: 25 packets/sec 5113 bytes/sec 0%
Last 300 seconds output: 33 packets/sec 8585 bytes/sec 0%
Input (total): 12033356 packets, 2408256176 bytes
  10463270 unicasts, 295684 broadcasts, 180849 multicasts, 0 pauses
Input (normal): 10939803 packets, - bytes
  10463270 unicasts, 295684 broadcasts, 180849 multicasts, 0 pauses
Input: 1093553 input errors, 0 runs, 0 giants, 0 throttles
  488058 CRC, 402598 frame, - overruns, 202897 aborts
  - ignored, - parity errors
Output (total): 28091209 packets, 8182957026 bytes
  11213662 unicasts, 8545599 broadcasts, 8331948 multicasts, 0 pauses
Output (normal): 28091209 packets, - bytes
  11213662 unicasts, 8545599 broadcasts, 8331948 multicasts, 0 pauses
Output: 0 output errors, - underruns, - buffer failures
  0 aborts, 0 deferred, 0 collisions, 0 late collisions

```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

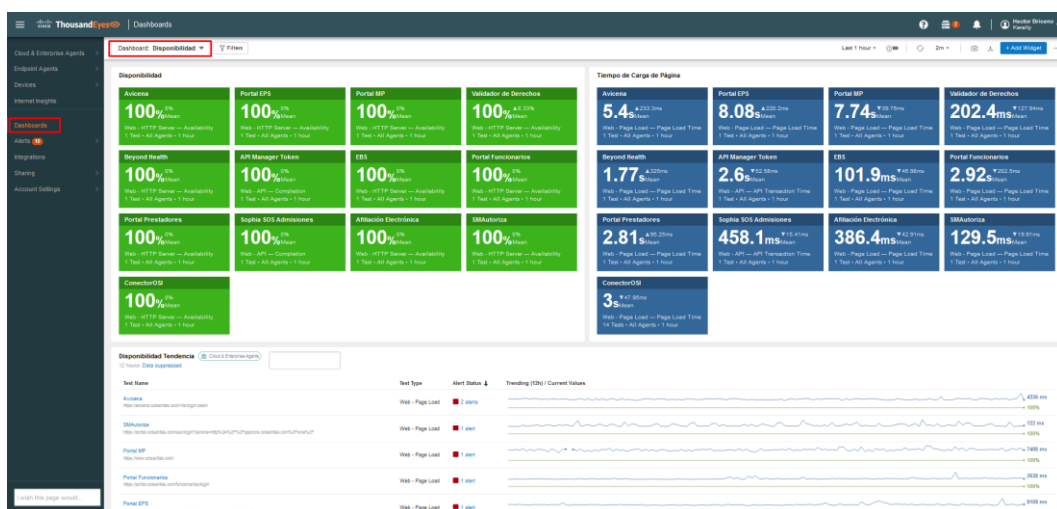
1. Estado del puerto de red (show interface).
 2. Estadísticas del puerto de red en la búsqueda de errores (show interface).
 3. Correcta configuración del puerto de acceso (show run interface).
- Se sugiere clarear las estadísticas del puerto que se revise y ver si con cada validación las cantidades mostradas aumentan. De no existir problemas en el puerto de red del usuario y el computador estar ubicado en un switches en cascada, validar los errores en los enlaces troncales entre los switches y entre Core switch y router.

4.2.4 Validaciones con Thousandeyes

Ingresar con las credenciales asignadas y validar las gráficas inicialmente en los agentes enterprise para validar si es un problema general de alguna aplicación pudiendo validar los nodos de MPLS.

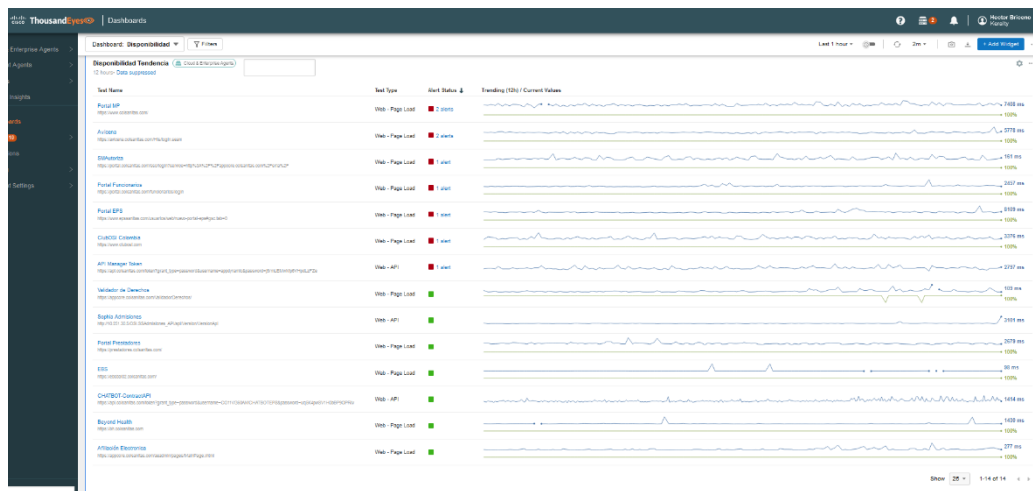
<https://app.thousandeyes.com/>

Posterior al ingreso se tiene acceso al dashboard de disponibilidad de las aplicaciones, en el menú de la izquierda se elige “Dashboard” y posterior en el menú desplegable de la derecha se elige el nombrado como “Disponibilidad”, como se observa en la imagen, el primer marco que se muestra en la parte izquierda se visualiza la disponibilidad de la aplicación y en la parte derecha el tiempo de carga de la web expresado en segundos o milisegundos sea el caso.



Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

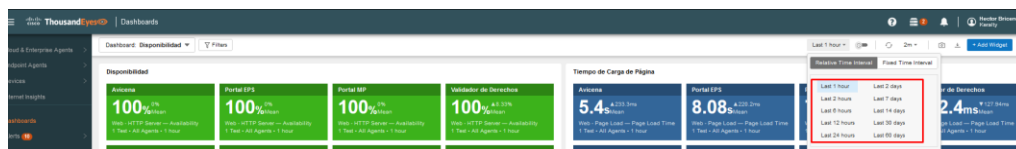
En el siguiente frame se observa el nombre de la aplicación y la URL que se testea permitiendo ver la tendencia en las últimas 12 horas con una visual general del comportamiento de esta durante ese tiempo.



Por último se cuenta con los valores de cada una de las métricas de los test que se realizan para medir con precisión la carga de la página.

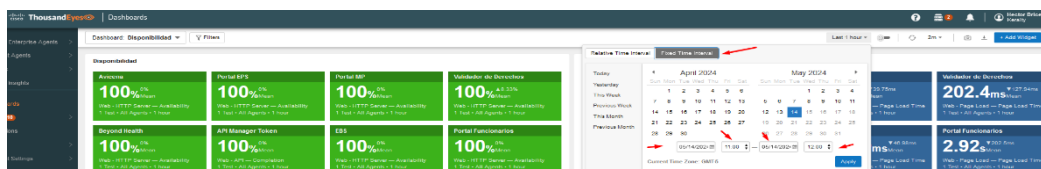


Por otra parte, en el menú de la derecha se tiene la opción de escoger que tiempo se desea visualizar, una hora como valor mínimo o últimos 60 días.

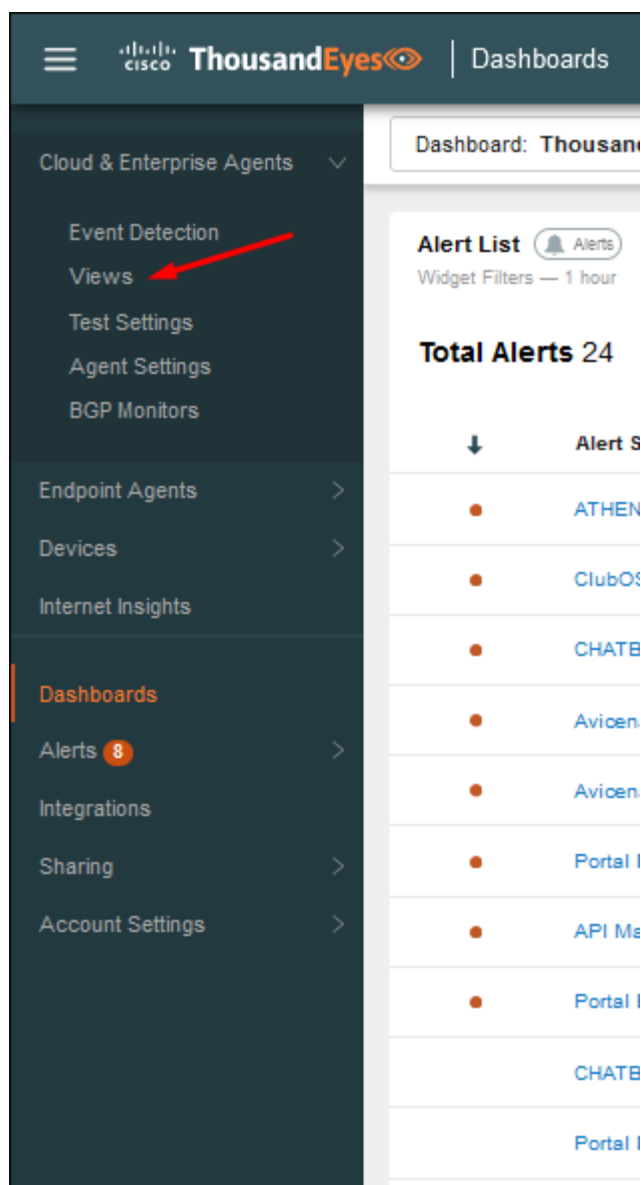


Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

Dicho menú tiene la opción de personalizar el tiempo de visualización, ingresando al menú Fixed Time Interval e ingresando los valores requeridos

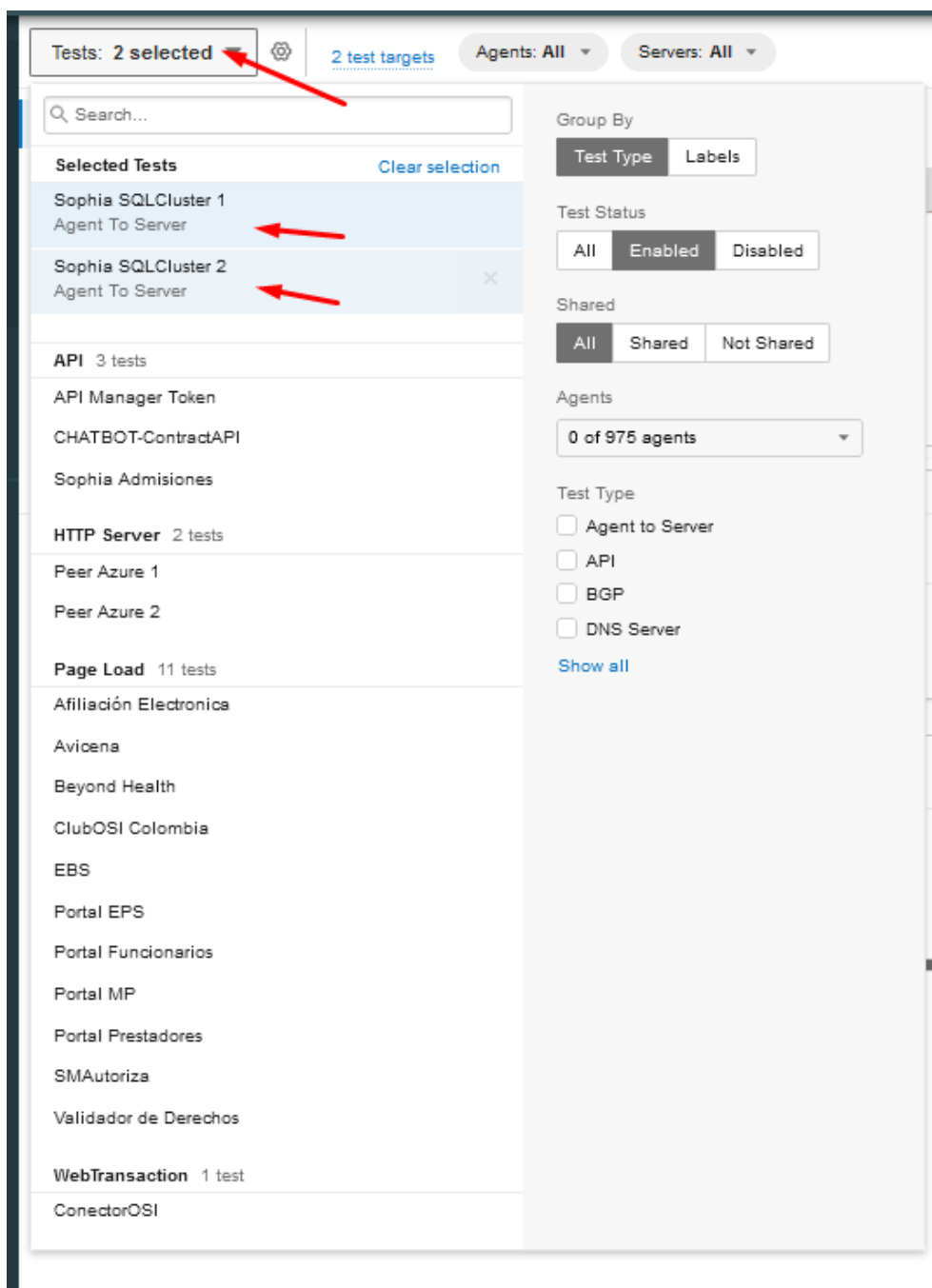


Se cuenta con otra visualización dando clic en el menú del costado izquierdo “Cloud & Enterprise Agent menú Views”, en donde en dicha visualización cuenta con mayor detalle del comportamiento en el tiempo de alguna aplicación.



Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

Dentro del módulo cargado al lado derecho se selecciona en la lista desplegable, “test” el nombre de la aplicación que queremos validar desde los servidores dedicados a los test



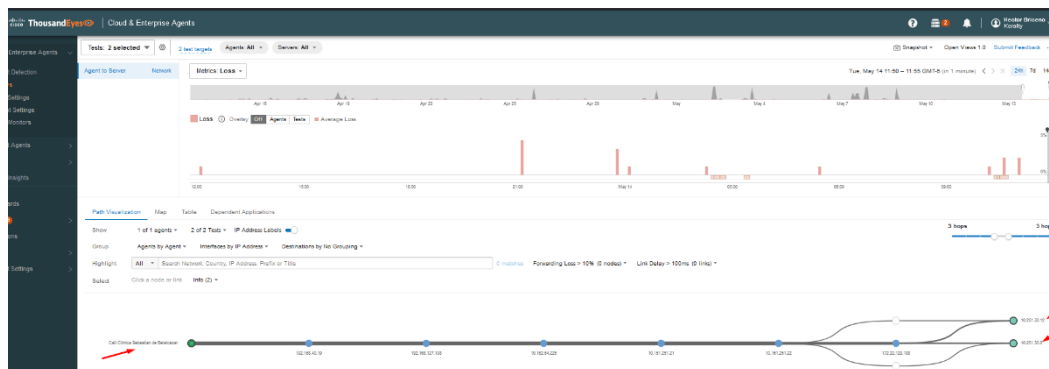
Versión: 3.0
Fecha: 14-05-2024

Código: SIG-TIRC-CKE-PL02

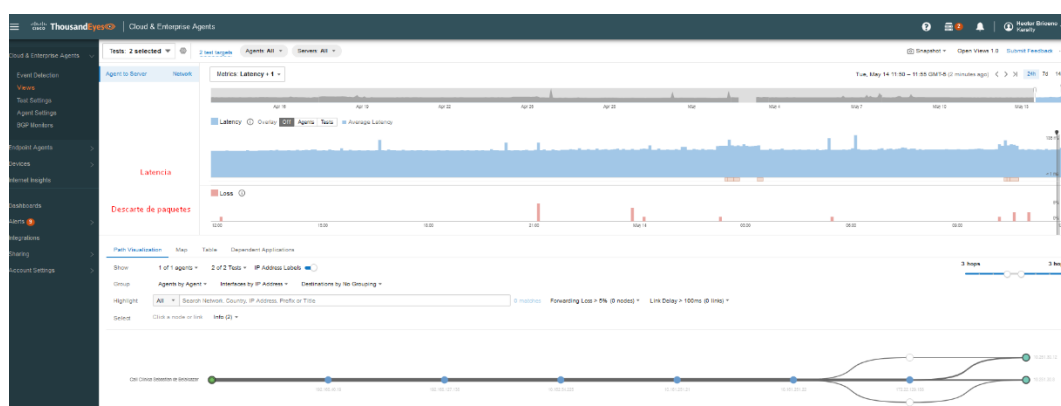
POLÍTICA MONITOREO REDES



Posterior a la carga del test, se pueden observar las métricas del servidor; como ejemplo, a continuación, se toman los test que se realizan hacia la bd de Sophia, al cargar al lado derecho se observara las métricas que se evalúan desde el servidor de la Clínica Sebastián de Belalcazar



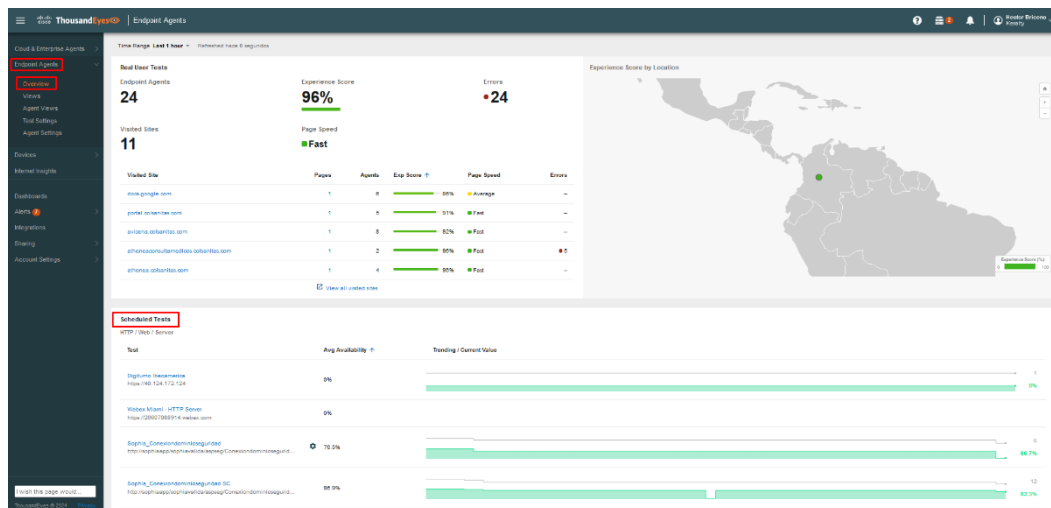
Para este test se observa la métrica de paquetes perdidos y si se observa cada nodo desde la CSB hasta el destino las direcciones finales de las bases de datos en el test que se está visualizando no se observa ningún nodo con pérdida de paquetes superior al 5%



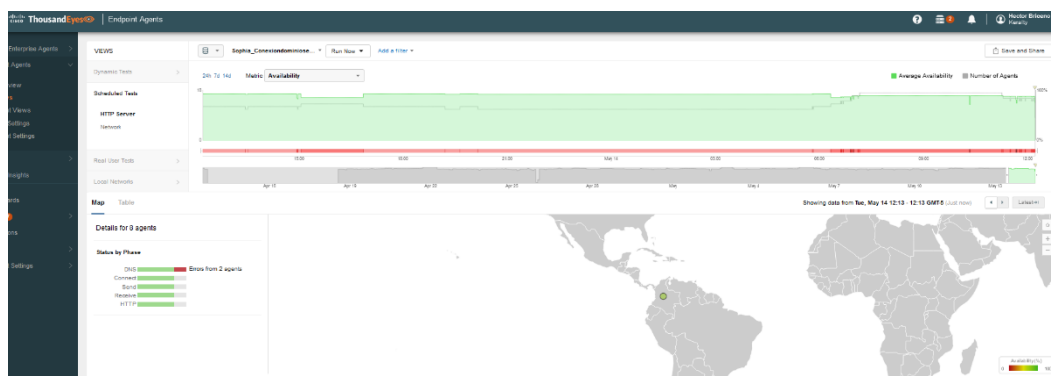
Para este caso de ejemplo, se comparan 2 métricas de paquetes perdidos y latencia de red que permite establecer si existe algún cambio en los valores normales de tránsito de los paquetes sobre la MPLS.

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

Otra opción para visualizar el comportamiento de forma más precisa es una sede la que reporta lentitud de alguna de las aplicaciones testeadas desde los computadores de algunas sedes es ingresar al módulo de endpoint agent así

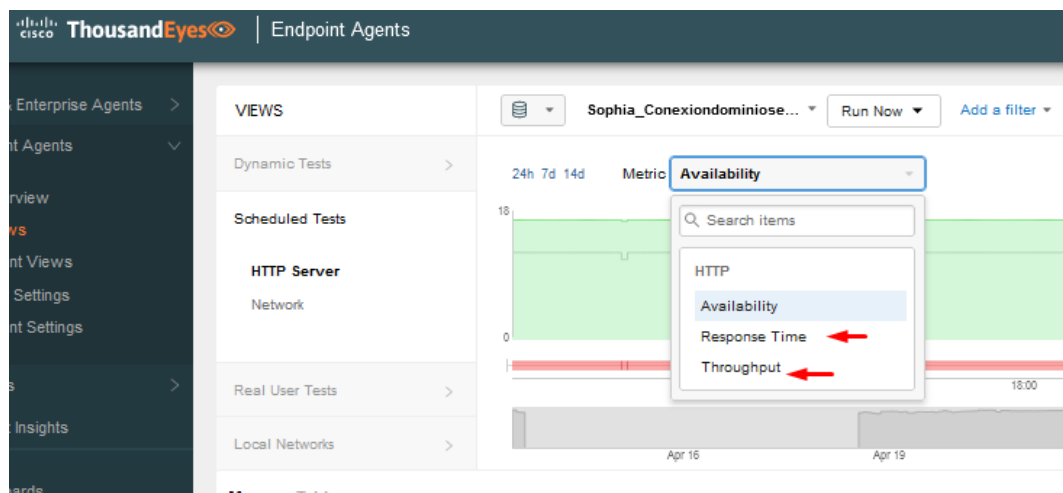


En las opciones señaladas permitirá acceder al detalle de las aplicaciones testeadas de los usuarios finales de algunas de las sedes para este caso ingresamos a los tes de Sophian conexión dominio seguridad y en la página principal de ese recurso muestra la disponibilidad de la web las últimas 24 horas

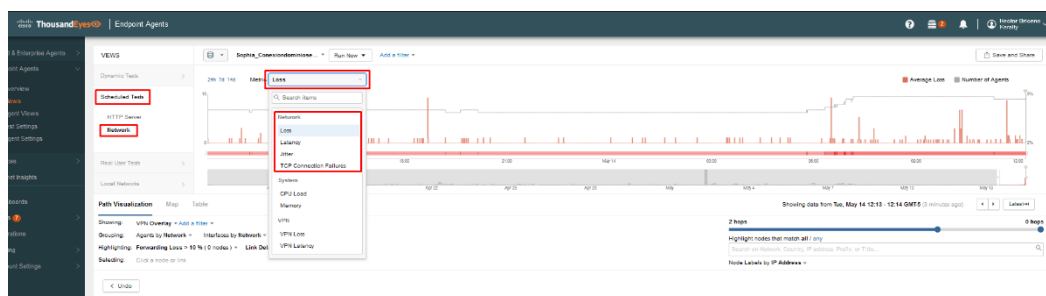


Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

En las opciones de las métricas web testeadas podremos observar otras como Tiempos de respuesta y consumo de bw de este recurso



Otra opción que permite realizar un diagnóstico más preciso es ingresar a los test de las métricas de red como se observa en la imagen siguiente para validar si algún nodo desde la sede escogida presenta valores que puedan afectar negativamente la experiencia del usuario final



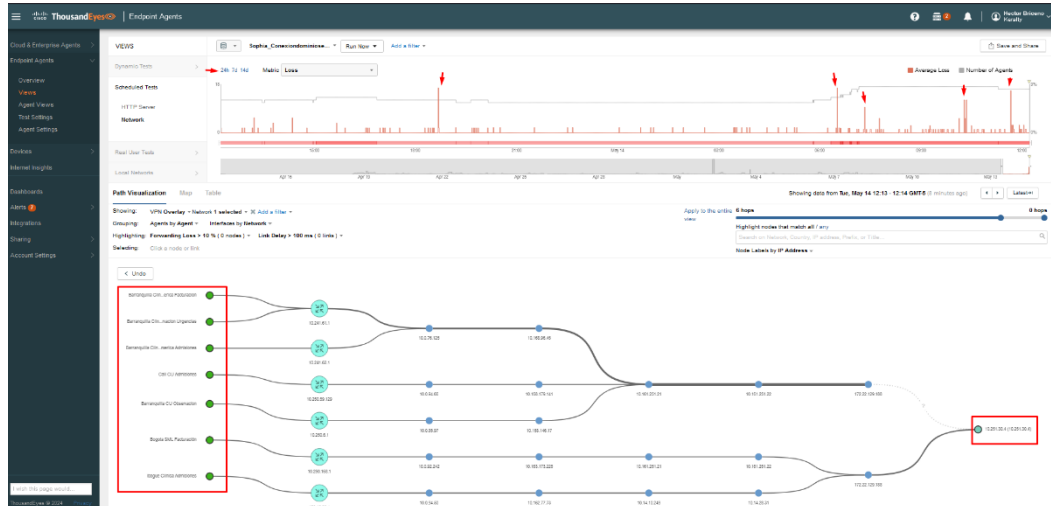
Para este ejemplo en las últimas 24 horas los test han presentado algunos valores altos en cuanto a la métrica de pérdida de paquetes de hasta el 9% pero que no se mantuvieron en el tiempo si no fueron de corta duración permitiéndonos ver los orígenes de cada una de las sedes al lado derecho y el destino al lado izquierdo para las últimas 24 horas.

Versión: 3.0

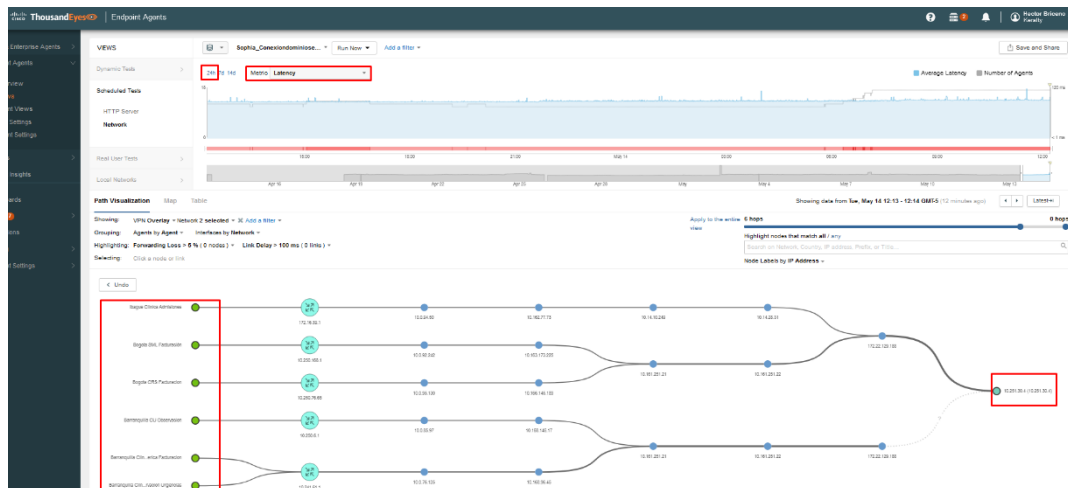
Fecha: 14-05-2024

Código: SIG-TIRC-CKE-PL02

POLÍTICA MONITOREO REDES



Esta vista nos permite validar si existe algún problema en la red puntualizando el nodo donde se pudiera presentar para así escalarlo con el proveedor para este caso que sería CLARO.



Otra métrica a tener en cuenta para el rendimiento de las aplicaciones a nivel de red es la métrica de latencia la cual nos puede indicar alguna degradación en los tiempos de respuesta del viaje de los paquetes del origen al destino.

Como se comentó en el punto anterior si alguno de los valores de los test esta por fuera del valor normal este será escalado al proveedor para que realice las validaciones respectivas.

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

4.3 Administración de los dispositivos de comunicaciones lan keralty

La gestión y administración de los dispositivos, se realiza sobre la totalidad de equipos existentes en la red LAN, y actualmente se contemplan más de 860 equipos de tipo Switch de los fabricantes Cisco y HP. Para realizar esta actividad se cuenta con acceso a estos equipos y abordar las siguientes actividades mencionadas a continuación.

- Diagnóstico para problemas que se reporten por los usuarios sobre saturación y problemas de conectividad (Se usa procedimiento 4.4 Saturación de enlaces)
- Configuraciones de los equipos de Redes LAN, como por ejemplo SNMPv3, interfaces, Redes Virtuales (VLAN) y otras configuraciones solicitadas a demanda o por problemas reportados.
- Realización de pruebas que permitan establecer causa raíz sobre los diferentes servicios de Keralty.
- Actualización del inventario.
- Ejecución de backups mensuales.

4.4 Gestión de switch keralty

- Configuración de vlan

Con la MAC suministrada por el usuario del área de soporte de sistemas de Keralty se procede a ubicar la sede donde se requiere el cambio de la vlan para que el dispositivo solicitado.

Se abre el core de la sede o el equipo principal al que se tenga acceso en la sede utilizando el usuario asignado para el ingeniero que esté realizando la labor

```
BOG-CL80_P5_CORE-WS-C3650-48PS#show mac address-table | include a24b
109      b4a3.8236.a24b      DYNAMIC      Gi1/0/37
BOG-CL80_P5_CORE-WS-C3650-48PS#sho run int Gi1/0/37
Building configuration...

Current configuration : 125 bytes
!
interface GigabitEthernet1/0/37
 description ACCESO USUARIOS
 switchport trunk native vlan 199
 switchport mode trunk
end
```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Como se observa en la imagen el puerto en el cual se ubica la MAC suministrada es un puerto troncal el cual este asignado a un switch de acceso al cual ingresaremos

```
BOG-CL80_P5_CORE-WS-C3650-48PS#show cdp neighbors Gi1/0/37 d
-----
Device ID: BOG-CL80_P3S-WS-C3750-48PC-L.colsanitas.
Entry address(es):
  IP address: 10.0.75.11
Platform: cisco WS-C3750G-48PS, Capabilities: Switch IGMP
Interface: GigabitEthernet1/0/37, Port ID (outgoing port): GigabitEthernet1/0/48
Holdtime : 155 sec

Version :
Cisco IOS Software, C3750 Software (C3750-ADVIPSERVICESK9-M), Version 12.2(40)SE, RELEA
SE SOFTWARE (fc3)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Fri 24-Aug-07 00:56 by myl

advertisement version: 2
Protocol Hello: OUI=0x000000C, Protocol ID=0x0112; payload len=27, value=00000000FFFFFF
FF010221FF0000000000000001B0DCE0080FF0000
VTP Management Domain: ''
Native VLAN: 199
Duplex: full
Management address(es):
  IP address: 10.0.75.11

Total cdp entries displayed : 1
```

- Se ingresa al switch con la información obtenida del comando anterior y se realiza nuevamente la búsqueda de la MAC.

```
BOG-CL80_P3S-WS-C3750-48PC-L#show mac address-table | include a24b
109      b4a3.8236.a24b      DYNAMIC      Gi1/0/45
```

```
BOG-CL80_P3S-WS-C3750-48PC-L#show cdp neighbors Gi1/0/45 d
-----
Device ID: BOG-CL80_P3S-WS-C2960-48PC-L.colsanita
Entry address(es):
  IP address: 10.0.75.12
Platform: cisco WS-C2960X-48FPS-L, Capabilities: Switch IGMP
Interface: GigabitEthernet1/0/45, Port ID (outgoing port): GigabitEthernet1/0/48
Holdtime : 127 sec

Version :
Cisco IOS Software, C2960X Software (C2960X-UNIVERSALK9-M), Version 15.2(2)E6, RELEASE
SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2016 by Cisco Systems, Inc.
Compiled Fri 16-Dec-16 21:27 by prod_rel_team

advertisement version: 2
Protocol Hello: OUI=0x000000C, Protocol ID=0x0112; payload len=27, value=00000000FFFFFF
FF010221FF000000000000000706BB9E07100FF0000
VTP Management Domain: ''
Native VLAN: 199
Duplex: full
Management address(es):
  IP address: 10.0.75.12
```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Se ingresa al siguiente switch que se muestra donde se encuentra la MAC y se valida si el puerto es de acceso o troncal para este caso es de acceso y solo observamos una MAC que corresponde al del dispositivo que requerimos realizar el cambio de vlan.

```
BOG-CL80_P3SW2-WS-C2960-48PC-L#show mac address-table | include a24b
109    b4a3.8236.a24b    DYNAMIC    Gi1/0/2
BOG-CL80_P3SW2-WS-C2960-48PC-L#sho run int Gi1/0/2
Building configuration...

Current configuration : 141 bytes
!
interface GigabitEthernet1/0/2
 switchport access vlan 109
 switchport mode access
 switchport voice vlan 100
 spanning-tree portfast
end

BOG-CL80_P3SW2-WS-C2960-48PC-L#sho mac ad int Gi1/0/2
Mac Address Table
-----
Vlan    Mac Address      Type        Ports
-----
109     b4a3.8236.a24b    DYNAMIC     Gi1/0/2
```

- Se ingresa en modo de configuración para hacer el cambio y asignar a la vlan requerida previa consulta de los segmentos en el switch core de la sede en caso de que este maneje la capa 3 o solicitar la información al ISP correspondiente para el suministro del listado de las vlan asignadas a la sede. posterior de realizar el cambio se ejecuta el comando #wr para guardar los cambios cuando el usuario confirme que el puerto funciona correctamente.

```
BOG-CL80_P5_CORE-WS-C3650-48PS#show ip interface brief | e una
Interface      IP-Address      OK? Method Status  Protocol
Vlan100        192.168.17.130  YES NVRAM  up      up
Vlan101        192.168.8.129   YES NVRAM  up      up
Vlan105        172.16.4.129    YES NVRAM  up      up
Vlan109        10.248.246.1    YES NVRAM  up      up
Vlan111        10.250.56.129   YES NVRAM  up      up
Vlan199        10.0.75.2       YES NVRAM  up      up

BOG-CL80_P3SW2-WS-C2960-48PC-L#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
BOG-CL80_P3SW2-WS-C2960-48PC-L(config)#int Gi1/0/2
BOG-CL80_P3SW2-WS-C2960-48PC-L(config-if)#switchport access vlan 101
```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

Configuración de puerto troncal

- Cuando se requiera conectar un switch en cascada u otro dispositivo que requiera un puerto troncalizado se deberán realizar los siguientes pasos.
- Buscar un puerto que no tenga conectado ningún dispositivo y se valida su estado

```
GigabitEthernet1/0/45  unassigned  YES unset  down  down
```

- Validar el estado procedemos a validar que tipo de configuración cuenta

```
BOG-CL80_P3SW2-WS-C2960-48PC-L#sho run int GigabitEthernet1/0/45
Building configuration...

Current configuration : 142 bytes
!
interface GigabitEthernet1/0/45
  switchport access vlan 101
  switchport mode access
  switchport voice vlan 100
  spanning-tree portfast
end
```

- Si se encuentra como puerto de acceso se debe cambiar la configuración con los siguientes comandos, ingresando en modo de configuración, borrando primero la configuración anterior y asignando la nueva configuración.

```
BOG-CL80_P3SW2-WS-C2960-48PC-L#conf t
Enter configuration commands, one per line. End with CNTL/Z.
BOG-CL80_P3SW2-WS-C2(config)#int GigabitEthernet1/0/45
BOG-CL80_P3SW2-WS-C2(config-if)#undo switchport access vlan 101
BOG-CL80_P3SW2-WS-C2(config-if)#undo switchport mode access
BOG-CL80_P3SW2-WS-C2(config-if)#undo switchport voice vlan 100
BOG-CL80_P3SW2-WS-C2(config-if)#description Troncal
BOG-CL80_P3SW2-WS-C2(config-if)#switchport trunk native vlan 199
BOG-CL80_P3SW2-WS-C2(config-if)#switchport mode trunk
```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

- Al finalizar debe quedar como se observa en la siguiente imagen y posterior a la validación del correcto funcionamiento del puerto, se guardan los cambios con la ejecución del comando #wr

```
BOG-CL80_P3SW2-WS-C2960-48PC-L#sho run int GigabitEthernet1/0/48
Building configuration...

Current configuration : 117 bytes
!
interface GigabitEthernet1/0/48
  description Troncal
  switchport trunk native vlan 199
  switchport mode trunk
end
BOG-CL80_P3SW2-WS-C2960-48PC-L#wr
```

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

5. CONTROL DE CAMBIOS.

FECHA	CAMBIO	VERSIÓN
03/10/2022	Creación del documento	1
06/10/2023	Actualización del documento	2
14/05/2024	Actualización del documento, el documento se revisa en el marco de la actualización del SGSI año 2024, se realiza inclusión de la sigla del país y la compañía en el código del documento.	3

Tabla 1 control de cambios

Versión: 3.0	POLÍTICA MONITOREO REDES	
Fecha: 14-05-2024		
Código: SIG-TIRC-CKE-PL02		

6. FLUJO DE APROBACIÓN.



ELABORÓ	REVISÓ	APROBÓ
Nombre: Héctor Iván Briceño Carranza Área/Proceso: Redes y Comunicaciones Fecha: 03/10/2022 	Nombre: Miguel Ángel León García Área/Proceso: Redes y comunicaciones Fecha: 14/05/2024 	Nombre: Javier Galván Área/Proceso: Gerencia corporativa de tecnología Fecha: 20/05/2024

Tabla 2 Flujo de aprobación

Cualquier copia impresa de este documento se considera como **COPIA NO CONTROLADA**.