

NUESTRA EMPRESA

MISIÓN

Aportamos soluciones integrales en telecomunicaciones a la dinámica corporativa de nuestros clientes, garantizando un servicio de calidad con personal altamente calificado

VISIÓN

Nos proyectamos para el año 2030 aumentando nuestro alcance en el mercado nacional a través de alianzas estratégicas en las principales ciudades del país. Visualizamos un portafolio de servicios más amplio que se adapte a los retos cambiantes que se presentan en el ámbito tecnológico, todo esto para seguir atendiendo las necesidades de nuestros clientes

VALORES CORPORATIVOS

Transparencia
Respeto
Integridad
Servicio
Calidad
Eficiencia
Compromiso

Los principales beneficios de nuestro servicio se resumen en:

Reducción de costos mediante una eficiente asignación de recursos que a futuro se puedan presentar al no requerir nueva infraestructura.

Implementación de nuevos servicios que repercuten en nuevos ingresos y oportunidades de mejora a la infraestructura de servicios actual.

Optimización y control de la infraestructura de comunicaciones, reducción de indisponibilidades y rápido retorno de la inversión realizada al obtener información de primera mano reduciendo costos operativos propios y de terceros.

RESUMEN EJECUTIVO

En la actualidad INSTITUCION UNIVERSITARIA PASCUAL BRAVO se encuentra en proceso de optimización de su infraestructura tecnológica con el fin de identificar posibles fallas y mejorar los servicios que se prestan y circulan a través de la red de área local LAN e infraestructura de servidores y aplicaciones al interior de la universidad.

Es por esto que CV-COMUNICACIONES, en calidad de distribuidor para Colombia de la marca SAVVIUS, presenta a consideración de la IUPB la presente oferta para el servicio de ANALISIS DE TRAFICO de la plataforma tecnológica y de misión crítica que busca centralizar y consolidar el monitoreo de los equipos de networking, servidores y aplicaciones, así como los servicios críticos para la universidad con el fin de garantizar y optimizar su disponibilidad e identificar proactivamente los incidentes y eventos sobre la infraestructura de TI.

La solución propuesta permitirá incrementar la productividad y eficiencia de la plataforma de red, de servidores y aplicaciones permitiendo medir el tráfico y el desempeño de los dispositivos que componen la plataforma tecnológica y de misión crítica de IUPB, detectar fallas en tiempo real, consolidar niveles de disponibilidad y SLAs sin mayores inversiones a futuro y reduciendo costos operativos a mediano y largo plazo, contando con una solución de ANALISIS DE TRAFICO versátil, que incluye herramientas altamente funcionales para conformar una plataforma de monitoreo robusta y de alto desempeño con los servicios especializados de analistas de TI dedicados a monitorear, cuantificar, solucionar y optimizar la plataforma tecnológica de IUPB.

La solución de monitoreo de la plataforma tecnológica de IUPB se encuentra enmarcada en componentes de software, hardware y servicios de personal especializado.

Los componentes de software incluyen las herramientas de monitoreo, la herramienta de registro de incidentes, las herramientas de diagnóstico y solución de fallas.

SERVICIO DE ANALISIS DE TRÁFICO DE LA PLATAFORMA TECNOLÓGICA Y DE MISIÓN CRÍTICA IUPB.

- OBJETIVO GENERAL

El objetivo de la presente oferta es brindar a IUPB una solución integral de ANALISIS DE TRAFICO monitoreo y gestión de infraestructura de TI, mediante la cual contará con una solución de gestión especializada para el análisis de trafico monitoreo constante de los dispositivos que componen la red de comunicaciones, infraestructura de servidores y aplicaciones, obteniendo información sobre el comportamiento, consumo y estadísticas en tiempo real de todos los equipos y canales que la componen, contando con los altos niveles de disponibilidad, seguridad, calidad y eficiencia que estos servicios requieren, ayudando a que mediante el servicio de monitoreo de la infraestructura tecnológica se integren todos los procesos de administración, monitoreo, consolidación y publicación de la información de cada uno de los servidores, aplicaciones y equipos de networking, incrementando la productividad y eficiencia de la plataforma tecnológica, permitiendo medir, monitorizar y optimizar el desempeño de los dispositivos, detectar fallas en tiempo real, consolidar

niveles de disponibilidad y SLAs sin mayores inversiones a futuro y reduciendo costos operativos a mediano y largo plazo, contando con un conjunto de herramientas funcional, robusto y de alto desempeño en comparación con otras soluciones del mercado.

- OBJETIVOS ESPECÍFICOS

Suministrar la solución necesaria en hardware y software de las herramientas requeridas para el despliegue del proyecto de implementación del proyecto descrito en las especificaciones técnicas.

Brindar los servicios de diseño, implementación, puesta en marcha y capacitación para solución de análisis propuestas.

Suministrar los servicios posventa remoto y es sitio (si se requieren) y con soporte de fábrica durante 1 año sobre la solución adquirida.

2. ALCANCE

2.1. Definición

El modelo del servicio que hemos diseñado, se basa en el suministro de la solución de análisis , diseño, implementación, puesta en marcha, capacitación y soporte con personal en sitio o vía remota de la plataforma de monitoreo para la infraestructura tecnológica y de misión crítica de IUPB consistente en un conjunto de herramientas de monitoreo basadas en software, las cuales recibirá información y datos de manera centralizada de todos los equipos de red, servidores y aplicaciones que componen la infraestructura de TI de IUPB así como los servicios asociados para el correcto funcionamiento de la misma.

CV-COMUNICACIONES incluye el diseño y puesta en funcionamiento de la solución, así como la capacitación y soporte sobre la misma , con acceso para IUPB de todos los servicios y recursos vía Web de la comunidad SAVVIUS con el fin de obtener capacitación, nuevas funcionalidades de la plataforma, actualizaciones y herramientas adicionales gratuitas. Este servicio estará vigente durante 1 año y posteriormente se puede renovar para contar con todos los beneficios directamente de fábrica.

CV-COMUNICACIONES ofrece el servicio de monitoreo para la plataforma tecnológica y de misión crítica de IUPB incluyendo el diseño e implementación alineados con las mejores prácticas, cumpliendo con los procedimientos y requerimientos de IUPB y proporcionando el apoyo en la definición e implementación de procesos enmarcados en las mejores prácticas ITIL para la atención y servicios generales de la infraestructura de TI.

El servicio ofrecido permitirá a IUPB contar con las facilidades (sin limitarse a estas) de:
Realizar ANALISIS DE TRAFICO y medición del desempeño de la infraestructura de control de IUPB así como de los servicios críticos que requieren un alto nivel de disponibilidad.

Contar con una solución de fácil uso y administración.

Contar con una solución fácilmente integrable a los procesos internos de soporte y gestión de tecnología.

Valor obvio “out-of-the-box” y de rápida puesta en funcionamiento de la solución en corto tiempo.

Alto nivel de robustez en todas las plataformas de software utilizadas.

Tecnología sólida con una base fuerte de servicio al cliente.

Contar con óptima calidad de los servicios de la plataforma de gestión para el monitoreo de la infraestructura de TI y los dispositivos que eventualmente integran todos los servicios de TI.

Contar con un sistema de gestión que analiza el tráfico en tiempo real y a profundidad el rendimiento de la red, servidores y aplicaciones y que no requiere la instalación de agentes, ya que la información se obtiene mediante métricas SNMP, WMI, RPC, ICMP.

Contar con una interfaz intuitiva y personalizable vía web que soporta múltiples puntos de vista por los analistas, usuarios y departamentos de IUPB para realizar consultas en cualquier momento.

Definir avanzadas de alertas para eventos correlacionados, condiciones sostenidas, y complejas combinaciones de estados de cada uno de los dispositivos y enlaces que componen la infraestructura de TI.

Asesoría en la mejora continua del servicio para detectar fallas y problemas a nivel de red, de servidores y aplicaciones con el fin de optimizar el rendimiento y desempeño de los enlaces y servicios críticos de IUPB.

Contar con una completa plataforma de ANALISIS DE TRAFICO y monitoreo de infraestructura tecnológica y servicios con la cual se podrá optimizar y controlar fallas, indisponibilidades, medición de SLAs, así como monitorear a profundidad cada uno de los dispositivos que componen la infraestructura tecnológica y de misión crítica de IUPB posibilitando su mejora y optimización.

El resumen del servicio ofrecido se presenta en la siguiente gráfica:

Los principales beneficios de nuestro servicio se resumen en:
Reducción de costos mediante una eficiente asignación de recursos que a futuro se puedan presentar al no requerir nueva infraestructura.

Implementación de nuevos servicios que repercuten en nuevos ingresos y oportunidades de mejora a la infraestructura de servicios actual.

Optimización y control de la infraestructura tecnológica y de misión crítica, reducción de indisponibilidades y rápido retorno de la inversión realizada al obtener información de primera mano reduciendo costos operativos propios y de terceros.

Centralización de procesos que mejoran la gestión de la información y la comunicación.

Soporte a la infraestructura de TI y a los servicios de manera proactiva.

2.2. ENTREGABLES

El resumen de entregables para la solución propuesta es el siguiente:

SOLUCIÓN DE ANALISIS DE TRAFICO DE INFRAESTRUCTURA TECNOLÓGICA

ÍTEM	DESCRIPCIÓN
1	OMNIPEEK LICENSE

- Escalamiento y Niveles de Servicio
- Servicio de Soporte Técnico en Sitio

El servicio de soporte técnico anual incluye:

- Soporte para solución de fallas de segundo nivel.
- Mantenimiento preventivo y correctivo de la solución a nivel de aplicación y configuración.
- Instalación de actualizaciones y parcheo de la solución.
- Acompañamiento y consultoría de nuevos servicios y ampliación del sistema.
- Las solicitudes de soporte se podrán realizar en los horarios establecidos según la modalidad contratada a través de:
- Cel: (57) – 3155892224
- E-mail: jorge.robledo@cv-comunicaciones.com

Una decisión que involucre escalar un problema a un nivel de soporte mayor dependerá de la gravedad y el nivel de prioridad del mismo. A continuación se detalla el nivel de soporte técnico en sitio ofrecido:

Los niveles de Falla y tiempo de atención son los siguientes:

GRAVEDAD	*PRIORIDAD*	*DEFINICION*	*TIEMPO DE ATENCION*
Crítica	1	Normalmente es atribuible a problemas específicos sobre la solución y que requieren asistencia directa del fábricante.	2 horas
Alta	2	Cuando la totalidad de los usuarios no pueden acceder a la plataforma de gestión y cuando se presentan problemas con el acceso al appliance, o de los servicios necesarios a nivel de sistema operativo para funcionamiento de la plataforma ó reinstalación del appliance por parte del cliente, así mismo, cuando se interrumpe el normal funcionamiento del sistema de analisis y	3-4 horas

		no es solucionado por el personal directo del cliente. En los casos mencionados se requiere desplazamiento de personal de soporte.	
Media	3	Son fallas que pueden ser solucionadas por el cliente directamente con asistencia telefónica o vía e-mail, como lo son problemas de acceso de algún usuario a la plataforma, desconfiguración parcial o reconfiguración de algún dispositivo que esta siendo monitoreado, configuración de reportes, alarmas o vistas de usuarios	5-8 horas
Baja	4	lentitud de acceso a la plataforma y no es recurrente.	12-24 horas

Estos son los niveles de servicio para reparación de fallas:

GRAVEDAD	*PRIORIDAD*	*DEFINICION*	*TIEMPO DE SOLUCION*
Crítica	1	Normalmente es atribuible a problemas específicos sobre la solución y que requieren asistencia directa en sitio.	4 horas
Alta	2	Cuando la totalidad de los usuarios no pueden acceder a la plataforma de gestión y cuando se presentan problemas con el acceso al servidor, cuando se presenta falla en las bases de datos o desconfiguración total de los dispositivos que están siendo monitorizados, se presentan fallas de sistema operativo, o de los servicios necesarios a nivel de sistema operativo para funcionamiento de la plataforma ó reinstalación del servidor por parte del cliente, así mismo, cuando se interrumpe el normal funcionamiento del sistema de gestión y no es solucionado por el personal directo	4-6 horas

		del cliente. En los casos mencionados se requiere desplazamiento de personal de soporte.	
Media	3	Son fallas que pueden ser solucionadas por el cliente directamente con asistencia telefónica o vía e-mail, como lo son problemas de acceso de algún usuario a la plataforma, desconfiguración parcial o reconfiguración de algún dispositivo que esta siendo monitoreado, configuración de reportes, alarmas o vistas de usuarios	6-8 horas
Baja	4	Lentitud de acceso a la plataforma y no es recurrente.	12-24 horas

- Tiempo máximo para solucionar requerimientos de fallas en la plataforma de gestión. El diagnóstico y solución bajo la responsabilidad de CV-COMUNICACIONES es lo referente al correcto funcionamiento de la herramienta SAVVIUS INSIGHT instalada. NO incluye suministro o revisiones del hardware, enrutadores, switches, equipos activos o servidores. No incluye la configuración o sustitución total o parcial de ningún elemento que haga parte de la solución entregada a IUPB, como son: enrutadores, switches, servidores, planta telefónica ó elementos propios del cliente como lo son aplicativos de terceros, cableado estructurado, o servicios de instalación por falla que no sea de fábrica ó inherente a la instalación, configuración ajeno a CV-COMUNICACIONES, pérdida de información por manipulación de personal externo, problemas de acceso o lentitud ocasionados por aplicativos de terceros o por fallas ocasionadas por avalanchas, terrorismo, sobrepicos de tensión del sistema eléctrico que afecten el appliance en donde se encuentra alojada la solución. El cliente es responsable por el soporte de primer nivel. TIEMPO DE REPARACIÓN DE LA FALLA: Mínimo 4 horas hábiles de forma remota.

- Tiempo máximo para solucionar requerimientos de fallas de acceso al sistema de gestión o desconfiguración de los dispositivos que se monitorizan en la plataforma de gestión. El diagnóstico y solución bajo la responsabilidad de CV-COMUNICACIONES es lo referente al correcto funcionamiento de la herramienta SAVVIUS instalada en un APPLIANCE asignado. No incluye la configuración o sustitución parcial o total, configuración de red y aplicativos adicionales. Tampoco incluye suministro o revisiones del hardware, enrutadores, switches, equipos activos o servidores. No incluye la configuración o sustitución total o parcial de ningún elemento que haga parte de la solución entregada a IUPB, como son: enrutadores, switches, servidores, planta telefónica ó elementos propios del cliente como lo son aplicativos de terceros, cableado estructurado, o servicios de instalación por falla que no sea de fábrica ó inherente a la instalación, configuración ajeno a CV-COMUNICACIONES, o por fallas ocasionadas por avalanchas, terrorismo, sobrepicos de tensión del sistema eléctrico que afecten el servidor en donde se encuentra alojada la herramienta. El cliente

es responsable por el soporte de primer nivel. TIEMPO DE REPARACIÓN DE LA FALLA: Mínimo de 4 a 6 horas hábiles de forma remota.

- Tiempo máximo para solucionar fallas de acceso o configuraciones de vistas para usuarios y que el personal de IUPB puede solucionar directamente con asistencia remota o telefónica local o directamente de fábrica. No incluye asistencia a fallas soporte a hardware, ni la sustitución total o parcial de ningún elemento que haga parte de la solución entregada a IUPB, como son: enrutadores, switches, servidores, planta telefónica ó elementos propios del cliente como lo son aplicativos de terceros, cableado estructurado, o servicios de instalación por falla que no sea de fábrica o inherente a la instalación, configuración ajeno a CV-COMUNICACIONES, pérdida de información por manipulación de personal externo, falla en el servidor que ocasione pérdida de bases de datos, o por fallas ocasionadas por avalanchas, terrorismo, sobrepicos de tensión del sistema eléctrico que afecten el APPLIANCE en donde se encuentra alojada la herramienta. El cliente es responsable por el soporte de primer nivel. TIEMPO DE REPARACIÓN DE LA FALLA: Mínimo de 6 a 8 horas de forma remota.

- Tiempo máximo para solucionar requerimientos de lentitud en el acceso al sistema de gestión. No incluye asistencia a fallas sobre soporte a hardware, ni la sustitución total o parcial de ningún elemento que haga parte de la solución entregada a IUPB, como son: enrutadores, switches, servidores, planta telefónica ó elementos propios del cliente como lo son cableado estructurado, o servicios de instalación por falla que no sea de fábrica ó inherente a la instalación, configuración ajeno a CV-COMUNICACIONES, pérdida de información por manipulación de personal externo, instalación de aplicativos de terceros, falla en el APPLIANCE SAVVIUS, o por fallas ocasionadas por avalanchas, terrorismo, sobrepicos de tensión del sistema eléctrico que afecten el servidor en donde se encuentra alojada la herramienta. El cliente es responsable por el soporte de primer nivel. TIEMPO DE REPARACIÓN DE LA FALLA: Mínimo de 12-24 horas hábiles de forma remota.

    - Niveles de Escalamiento

NIVEL DE ESCALAMIENTO	*DEFINICION*
1	Ingenieros de Soporte
2	Gerente de Proyecto
3	Ingeniero Especialista Fábrica

Mantenimiento Correctivo:

El mantenimiento correctivo es aquel que se realiza para corregir un evento o falla que ocasiona la salida del servicio de la plataforma de manera parcial o total; éste se realiza luego de generar la

solicitud vía telefónica o e-mail con un tiempo de respuesta aproximado de 3 horas, dependiendo de los permisos de ingreso y acceso al servidor en donde se encuentra instalada la plataforma.

Las actividades que se realizan incluyen el diagnóstico del evento o falla y dependiendo del mismo se realizan las siguientes actividades:

- Revisión y estado del appliance savvius
- Revisión de conectividad hacia la red.
- Corrección de errores a nivel de aplicaciones.
- Reinstalación de software.
- Reconfiguración lógica de dispositivos dentro de la plataforma y generación del informe de actividades y recepción a satisfacción de IUPB.

Medellin Septiembre 20 de 2021



Señores

Institucion Universitaria Pascual Bravo

Asunto : Entrega de licenciamiento Omnipeek Savvius

Por medio de la presente CV-COMUNICACIONES esta realizando la entrega del licenciamiento y aplicación para la utilizacion de la solucion snnifer savvius

Licencia: omnipeek_insight_92217

Validad Septiembre 20 de 2021 – Septiembre 20 de 2022

Equipo:

SAVVIUS_IST_128G_100M

SERIAL:SV201604001325

MODEL: FW-7525C-SU1



savvius Insight | Knowledge Base | Forums | Ask a Question

The user account has been added to the system. Please check your email for an activation email for your account.

Register Your Appliance

Jorge *

Robledo *

jorgerobledo@gti-servicios.com *

GTI SERVICIOS SAS *

Savvius Insight Serial Number(s). *

SV201604001325

Please enter one serial number per line



SAVVIUS GUIDE

Acerca de Savvius Insight

Savvius Insight ™ es un dispositivo compacto, de cuatro núcleos y seis puertos, que no tiene ventilador u otras partes móviles, y se ajusta fácilmente a un armario de cableado. Incluye puertos puente para supervisar la conexión a Internet de la ubicación y tres puertos adicionales para monitorear redes internas. Savvius Insight proporciona informes integrados a largo plazo y cuadros de mando basados en web para analizar y mostrar estadísticas de la red durante largos períodos. Savvius Insight también se puede utilizar para la solución de problemas de red y aplicaciones a nivel de paquete al conectarse directamente con Savvius Omnipeek. Al instalar Savvius Insight en cada oficina remota, los administradores de red pueden obtener información fácil y asequible sobre el rendimiento y la seguridad de la red y las aplicaciones en todas las ubicaciones bajo administración. Savvius Insight pone a disposición analíticas de red de clase empresarial en áreas que hasta ahora no se han satisfecho. Savvius Insight está disponible en dos configuraciones:

Casos de uso del cliente

Redes de oficina remota

En las grandes redes corporativas, Savvius Insight complementa los aparatos de supervisión más grandes de Savvius en áreas de la red con menor utilización, donde a menudo no tienen buena visibilidad. En estas situaciones, los miembros del equipo de asistencia técnica pueden utilizar Savvius Insight para el control 24x7 de la salud de las redes remotas con tableros web potentes, personalizables y fáciles de usar. Cuando se identifican problemas que requieren solución de problemas a nivel de paquete, los analistas de protocolos del equipo TAC pueden usar el software de análisis de red Savvius Omnipeek para conectarse directamente a los dispositivos y realizar la captura de paquetes y el análisis a nivel de paquete. Savvius Insight también se puede utilizar para realizar análisis de varios segmentos con dispositivos Savvius más grandes.

Proveedores de servicios gestionados (MSP)

Savvius Insight también es perfecto para los proveedores de servicios de TI administrados. Los proveedores de servicios gestionados gestionan las redes y la infraestructura de TI para los clientes, normalmente con 5-50 empleados por cliente. Savvius Insight permite a los proveedores de servicios gestionados reducir el tiempo medio de resolución (MTTR) para los clientes y aumentar su conocimiento de cuándo se están produciendo los problemas, al mismo tiempo que se reducen los costes. Para lograr esto, los proveedores de servicios administrados instalan Savvius Insight en cada ubicación del cliente. Los proveedores de servicios administrados pueden iniciar sesión en cada uno de los sistemas en cualquier momento para ver el estado actual de las redes del cliente. Los proveedores de servicios administrados también pueden definir alarmas y alertas sobre indicadores clave de rendimiento (KPI) y recibir notificaciones cada vez que se activa una alerta. Si se detecta un

problema o se recibe una alerta, el proveedor de servicios de TI puede conectarse rápidamente para ver cuál es el problema.

Savvius Insight es muy adecuado para oficinas que externalizan la administración de TI, como contadores, agentes de seguros y profesionales médicos. Tienen un administrador de TI compartido que pasa demasiado tiempo de oficina en oficina para tratar problemas típicos de red, como una red lenta o los usuarios que tienen problemas para conectarse. El administrador de TI necesita visibilidad remota en cada oficina, así como datos históricos para comparaciones cuando surjan problemas. Con Savvius Insight instalado en cada oficina, el administrador de TI puede realizar un seguimiento de todas las oficinas desde una única ubicación, utilizando las capacidades de supervisión de red integradas de Insight y Savvius Omnipeek para Savvius Insight para la solución de problemas de red. Al revisar los datos recopilados, el administrador de TI puede determinar la fuente de la mayoría de los problemas casi en tiempo real y realizar auditorías diarias rápidas para asegurar la fiabilidad general y la satisfacción del usuario en cada oficina.

Qué está incluido

Su paquete estándar Savvius Insight incluye:

• Dispositivo Savvius Insight

• Software Savvius Capture Engine preinstalado en Savvius Insight

• Guía de inicio rápido de Savvius Insight

• Adaptador y cable de alimentación de CA

• Pies de goma (4)

• Cable de la consola serie (RJ45 a DB-9)

Resumen del hardware 3

Guía del usuario de Savvius Insight

Resumen del hardware

Aquí está un resumen del hardware para el Savvius Insight:

• Procesador Quad-core 1700MHZ Intel Atom

• SSD de 128 GB

• 8 GB de RAM

• Dos puertos USB 2.0

• Puerto serie (con conexión física RJ45)

• Puerto de gestión

• Tres puertos Ethernet

• Dos puertos puente

• Adaptador de alimentación externo

Flujo de trabajo de Savvius Insight

¡Savvius Insight es simple y fácil de usar! Estos son los pasos para empezar:

1. Instale Savvius Insight. Consulte Instalación de Savvius Insight .

2. Conecte los cables a los paneles frontal y posterior de Savvius Insight. Consulte Conexión de cables a los paneles frontal y posterior.

3. Power en Savvius Insight. Consulte Inicio / cierre de Savvius Insight.

4. Configure los ajustes iniciales de Savvius Insight. Consulte Configuración inicial mediante la utilidad de configuración.

• Si está utilizando Savvius Insight para recopilar datos para el servidor de informes local incorporado, asegúrese de que Local esté seleccionado como la opción de generación de informes en la utilidad de configuración. Para obtener más información sobre el uso de Savvius Insight con un servidor de informes local, consulte Uso de Savvius Insight para informes a largo plazo.

• Si está utilizando Savvius Insight para reenviar datos de paquetes a un servidor Elasticsearch remoto, asegúrese de que Remote Elasticsearch esté seleccionado y configurado como la opción de generación de informes en la utilidad de configuración. Para obtener más información sobre el uso de Savvius Insight con un servidor remoto Elasticsearch, consulte Utilización de Savvius Insight para informes a largo plazo.

• Si está utilizando Savvius Insight para reenviar datos de paquetes a un servidor Splunk, asegúrese de que Remote Splunk esté seleccionado y configurado como la opción de generación de informes en la utilidad de configuración. Para obtener más información sobre el uso de Savvius Insight con Splunk, consulte

Guía del usuario de Savvius Insight

4 Instalación de Savvius Insight

Uso de Savvius Insight y Splunk.

5.Si utiliza Omnipeek para el software Savvius Insight para iniciar capturas de paquetes y para analizar los archivos de paquetes que se capturan y guardan en Savvius Insight, instale

el software opcional Omnipeek para Savvius Insight en un equipo con Windows. Para obtener más información sobre el uso de Omnipeek para Savvius Insight, consulte Uso de Savvius Insight y Omnipeek para Savvius Insight.

Instalación de Savvius Insight

Para instalar Savvius Insight:

1. Determinar la ubicación de dónde instalar Savvius Insight. Aquí hay algunas pautas para determinar la ubicación:

• La ubicación de instalación más común es instalar Savvius Insight en algún lugar entre su módem por cable (conexión a Internet) y la LAN. Uno de los puertos puente de Savvius Insight está conectado al módem de cable, mientras que el otro puerto de puente está conectado a la LAN.

• Necesitará configurar Savvius Insight inicialmente a través del puerto '0 MGMT' usando otra computadora. Asegúrese de tener acceso fácil a Savvius Insight para poder conectar el ordenador al puerto '0 MGMT' de Savvius Insight.

• También es posible conectar Savvius Insight con un solo cable Ethernet a un puerto de un enrutador configurado como puerto SPAN o a un TAP. Asegúrese de tener acceso fácil a estas conexiones.

2. Coloque Savvius Insight sobre una superficie plana.

PRECAUCIÓN: No coloque nada encima o directamente al lado de Savvius Insight. Cualquier obstrucción al disipador de calor ubicado en la parte superior de Savvius Insight puede causar que la unidad se sobrecaliente.

3. Pegue los pies de goma a la parte inferior de Savvius Insight.

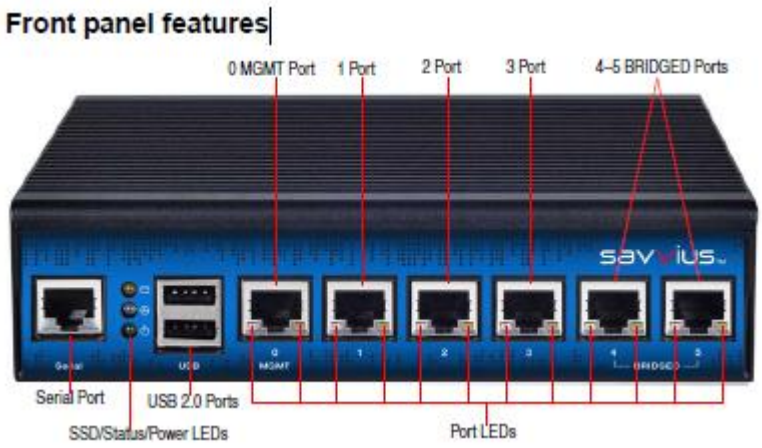
4. Conectar el adaptador de corriente atornillando el conector del adaptador a la toma de corriente en el panel posterior.

5. Conecte el otro extremo del adaptador de corriente a una toma de CA.

Conexión de los cables a los paneles frontal y posterior

A continuación se describen los cables de conexión a los paneles frontal y posterior, así como los estados de LED en Savvius Insight.

Características del panel frontal



• Puerto serie: El puerto serie le permite conectarse a otro terminal de computadora para diagnósticos avanzados o acceso de recuperación mediante el cable de consola serie RJ-45 a DB-9 incluido con Savvius Insight. El conector RJ-45 del cable de la consola está conectado al puerto serie de Savvius Insight y el conector DB-9 (macho) del cable de la consola está conectado al puerto serie DB-9 (hembra) del terminal del ordenador. Consulte Conexión a Savvius Insight a través del puerto serie en la página 17.

Nota: No todos los equipos tienen un puerto serie DB-9. Asegúrese de que el terminal de computadora que está utilizando tiene uno. Si es necesario, puede obtener e instalar un adaptador USB a COM en el terminal de la computadora.

• LED SSD / Estado / Alimentación:

• SSD: Si el LED parpadea, indica actividades de acceso a datos; De lo contrario, permanece apagado.

• Estado: Cuando el Savvius Insight se enciende por primera vez, el LED parpadea momentáneamente en verde y, a continuación, permanece apagado.

SSD / Estado / LEDs de potencia0 Puerto MGMT4-5 Puertos BRIDGED USB 2.0 Puertos1 Port2 Port3 PortSerial PortPort LEDs

• Alimentación: Si el LED está encendido indica que el sistema está encendido. Si está apagado, indica que el sistema está apagado.

• Puertos USB 2.0: Los puertos USB están reservados para futuras expansiones.

• Puerto '0 MGMT': Este puerto Ethernet es el puerto de administración que le permite configurar inicialmente Savvius Insight (consulte Configuración inicial mediante la utilidad de configuración en la página 8). Una vez que Savvius Insight esté configurado, el puerto se puede utilizar para la administración del dispositivo. Conecte un cable Ethernet estándar de su red al puerto '0 MGMT'.

• Puertos '1 - 3': Estos puertos Ethernet se utilizan para capturar paquetes desde su red. Conecte un cable Ethernet estándar de su red al puerto deseado de Savvius Insight.

• Puertos '4 - 5 BRIDGED': Estos puertos Ethernet se configuran como un puente y se utilizan cuando se desea insertar Savvius Insight en línea entre dos dispositivos de red. Esta configuración permite la captura del tráfico que fluye entre los dos nodos de la red sin necesidad de un toque. En esta implementación, los paquetes entran en Savvius Insight a través de uno de los puertos de puente y, a continuación, salen de Savvius Insight a través del puerto de puente restante. Esencialmente, cualquier tráfico que llega a un puerto de puente se copia en el otro puerto de puente. En los casos en que la alimentación se apaga o se pierde para Savvius Insight, los dos puertos de puente están conectados como si fueran un cable (‘fail to wire’), de modo que la conectividad a Internet no se pierda.

Para establecer el puente, conecte cables Ethernet estándar para que Savvius Insight se encuentre entre su módem por cable (conexión a Internet) y la LAN. Uno de los puertos Bridge de Savvius Insight está conectado al módem de cable, mientras que el otro puerto de bridge está conectado a la LAN. Ambos puertos Bridge deben estar conectados de esta manera para establecer correctamente el puente.

No conecte cada uno de los puertos de puente a la misma red enrutada IP; De lo contrario, se crea un bucle de enrutamiento y puede hacer que la red sea inoperable.

Nota: Si está utilizando Savvius Insight para reenviar datos al servidor incorporado local o a un servidor remoto Elasticsearch o Splunk, las capturas se inician automáticamente en los puertos de bridge y los datos se reenvían al servidor configurado en la utilidad de configuración. Consulte Configuración inicial mediante la utilidad de configuración.

• LEDs de puerto: Los dos LEDs en la parte inferior de los puertos 0-5 se iluminan para indicar actividad. Se ha establecido una luz LED verde y amarilla para indicar una conexión. Un LED amarillo intermitente indica las actividades de acceso a los datos.



Botón de reinicio: inserte un clip de papel y mantenga pulsado el botón de reinicio durante tres segundos para restablecer la configuración de fábrica de Savvius Insight. Usted perderá todas las configuraciones y datos guardados en Savvius Insight cuando se restablezca a sus ajustes de fábrica. Una vez que Savvius Insight se ha restablecido, deberá volver a ejecutar la utilidad de configuración como se describe en Configuración inicial mediante la utilidad de configuración.

Nota: También puede realizar un restablecimiento de fábrica desde el cuadro de diálogo Acciones.

• Botón de encendido con LED: Presione para encender o apagar el Savvius Insight. Cuando está en modo de espera, el LED se enciende en rojo; En el modo de encendido, el LED se enciende en verde; Cuando está apagado, el LED no se enciende.

Nota: También puede desactivar Savvius Insight desde el diálogo Acciones.

• Enchufe de encendido: se conecta al conector atornillable del adaptador de alimentación incluido con Savvius Insight.

Nota: Asegúrese de que el conector atornillable del adaptador de alimentación esté conectado al enchufe de encendido en Savvius Insight antes de conectar el adaptador de alimentación a una fuente de alimentación de CA.

Inicio / cierre de Savvius Insight

Para iniciar Savvius Insight, haga lo siguiente:

• Pulse el botón de encendido en el panel posterior de Savvius Insight.

Para cerrar Savvius Insight, realice una de las siguientes acciones:

• Presione brevemente el botón de encendido en el panel posterior de Savvius Insight.

• Haga clic en el enlace acciones situado en la parte superior de la utilidad de configuración para mostrar el cuadro de diálogo Acciones y, a continuación, seleccione la opción Apagado.

PRECAUCIÓN Al apagar el Savvius Insight, al presionar el botón de encendido se realiza un apagado limpio de Savvius Insight. Al mantener pulsado el botón durante varios segundos, Savvius Insight realiza un apagado inmediato, lo que provoca la pérdida de datos. Esta operación sólo se utilizará si Savvius Insight no responde.

Configuración inicial mediante la utilidad de configuración

La utilidad de configuración de Savvius Insight le permite configurar las opciones de configuración de dispositivo, red, hora y generación de informes.

Importante: Savvius Insight viene de fábrica configurado inicialmente con una dirección IP de 192.168.1.21. Para ejecutar la utilidad de configuración inicialmente, debe utilizar un cable Ethernet conectado directamente entre el puerto de administración '0 MGMT' de Savvius Insight y su PC o portátil y, a continuación, utilice una ventana del navegador en la PC o portátil para abrir la utilidad de configuración. El PC o portátil debe estar configurado para estar en la misma subred IP que Savvius Insight (consulte la página web de Savvius Insight si necesita instrucciones para configurar su computadora para que esté en la misma subred que el dispositivo).

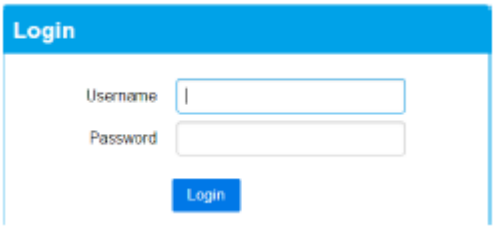
Una vez que utilice la utilidad de configuración, podrá configurar Savvius Insight en una nueva dirección IP directamente accesible a través de la red.

Para configurar inicialmente Savvius Insight mediante la utilidad de configuración:

1.Use un PC o portátil y configúrelo para una dirección IP compatible con la red 192.168.1.0/24. Esto permite que la PC o portátil se comunique con Savvius Insight, que tiene una dirección predeterminada de 192.168.1.21. (Consulte la página web de Savvius Insight si necesita instrucciones para configurar su computadora para que esté en la misma subred que Savvius Insight).

2.Conecte un cable Ethernet desde el PC o portátil al puerto '0 MGMT' de Savvius Insight.

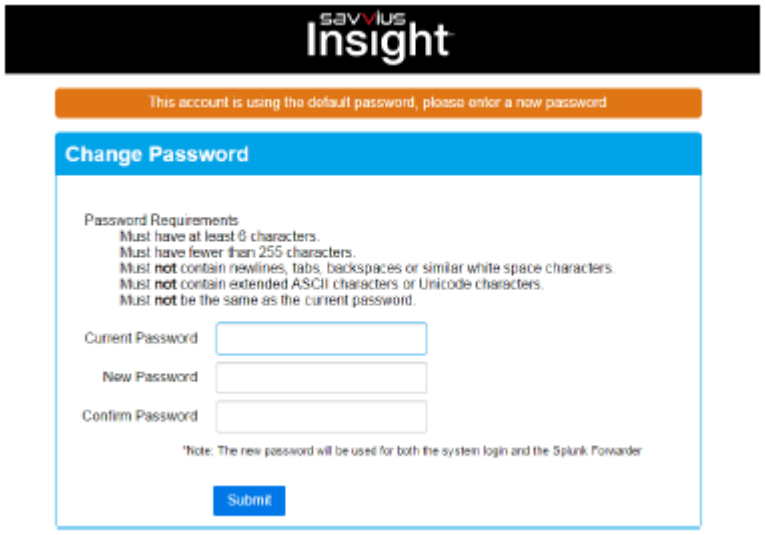
Desde una ventana del navegador en el PC o portátil, ingrese la dirección IP predeterminada de Savvius Insight de 192.168.1.21 en el cuadro URL. Aparecerá la pantalla de inicio de sesión de Savvius Insight.



• Nombre de usuario: introduzca el nombre de usuario predeterminado para Savvius Insight. El valor predeterminado es root.

• Contraseña: ingrese la contraseña de Savvius Insight. El valor predeterminado es savvius

4. Desde que inicia sesión en Savvius Insight por primera vez, se le pedirá que cambie la contraseña predeterminada antes de continuar.



• Contraseña actual: introduzca la contraseña actual de Savvius Insight. El valor predeterminado es savvius.

• Nueva contraseña: introduzca la nueva contraseña de Savvius Insight.

• Confirmar contraseña: vuelva a introducir la nueva contraseña para Savvius Insight.

Nota: La contraseña que ingresa aquí se utiliza tanto para Savvius Insight como para el reenviador Splunk. Asegúrese de anotar la contraseña que ha configurado.

También puede cambiar la contraseña de Savvius Insight en cualquier momento haciendo clic en Cambiar contraseña en la utilidad de configuración.

5.Haga clic en Enviar. Aparecerá la utilidad de configuración Savvius Insight.

6.Configure la configuración de Savvius Insight:

Importante: Una vez que haya configurado y aplicado los ajustes siguientes, ya no se utilizará la dirección predeterminada de Savvius Insight de 192.168.1.21. Para acceder de nuevo a la utilidad de configuración, debe introducir la dirección IP de Savvius Insight tal como se configura a continuación, así como la nueva contraseña introducida anteriormente.



• Portal Savvius Insight: haga clic en el vínculo insight.savvius.com para acceder a la documentación y los recursos de soporte para los propietarios de Savvius Insight. Contiene enlaces para descargar Omnipeek para el software de análisis de red Savvius Insight para Windows y la aplicación Savvius para Splunk.

• Device Name: Introduzca un nombre para Savvius Insight. Un nombre de dispositivo único permite una fácil identificación de las fuentes de datos.

• Asignación de IP: Esta configuración le permite especificar si Savvius Insight usa DHCP o configuraciones estáticas. Si DHCP está seleccionado, Savvius Insight es configurado por el servidor DHCP. Si está seleccionado estático, las configuraciones de dirección, máscara de red, puerta de enlace y DNS se pueden configurar para Savvius Insight.

Importante: Savvius Insight se puede configurar para obtener una dirección IP automáticamente desde un servidor DHCP; Sin embargo, recomendamos encarecidamente el uso de una dirección IP estática para Savvius Insight. Si se utiliza DHCP y si la dirección

cambia en una nueva concesión DHCP, el usuario debe buscar la nueva dirección IP asignada a Savvius Insight desde el servidor DHCP. Para ayudarle a buscar la dirección IP, aparece la dirección MAC de Savvius Insight si selecciona DHCP.

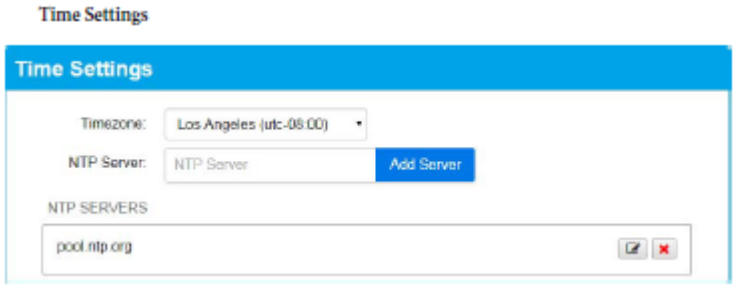
Nota: Si DHCP está seleccionado, tiene aproximadamente dos minutos para conectar Savvius Insight a su red para que el servidor DHCP asigne una dirección IP. Asegúrese de que Savvius Insight esté conectado a su red dentro del período de dos minutos desde el momento en que haga clic en Aplicar. Si reinicia Savvius Insight, el reloj de dos minutos también se restablece.

• Dirección: Esta configuración le permite especificar la dirección IP que está asignando a Savvius Insight.

• Máscara de red: Una máscara de red, combinada con la dirección IP, define la red asociada con Savvius Insight.

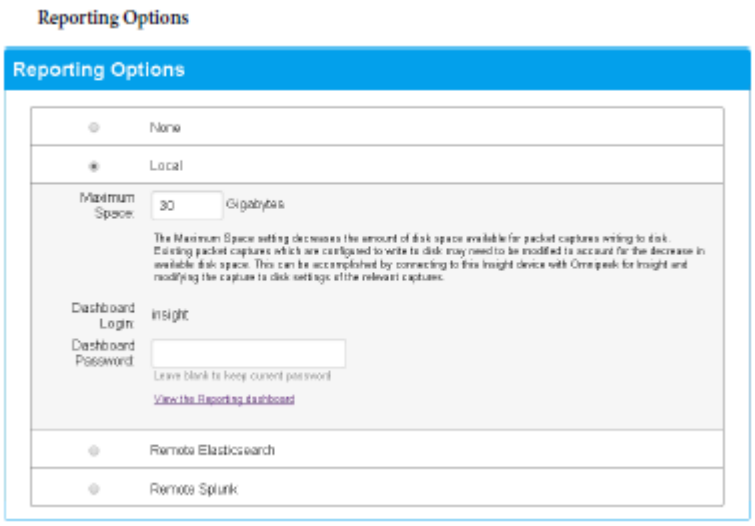
• Puerta de enlace: también conocida como 'Puerta de enlace predeterminada'. Cuando Savvius Insight no tiene una ruta IP para el destino, el paquete IP se envía a esta dirección, ya que no sabe cómo dirigirla localmente. Sólo se puede definir una única puerta de enlace predeterminada.

• DNS: Es el servidor de nombres de dominio. Un servidor de nombres de dominio traduce nombres de dominio (por ejemplo, www.savvius.com) a una dirección IP. Introduzca la dirección del servidor DNS y haga clic en Agregar servidor. Pueden definirse varios servidores de nombres DNS. También puede editar o eliminar cualquier servidor DNS definido.



• Zona horaria: la opción Zona horaria le permite especificar la ubicación física de Savvius Insight. Seleccione de la lista la ubicación más cercana a su Savvius Insight.

• Servidor NTP: El protocolo de tiempo de red (NTP) se utiliza para sincronizar los relojes de los ordenadores a través de una red. Para sincronizar el reloj Savvius Insight, puede especificar la dirección IP de un servidor NTP ubicado en la red local o en Internet. Introduzca la dirección del servidor NTP y haga clic en Agregar servidor. Pueden definirse varios servidores NTP. También puede editar o eliminar cualquier servidor NTP definido.



Ninguno: seleccione esta opción si no está recopilando estadísticas automáticamente para una de las tres opciones de informe que se muestran a continuación.

• Local: Seleccione esta opción para configurar el servidor de informes local integrado en Savvius Insight como la opción de informes que Savvius Insight reenvía automáticamente a sus estadísticas de red una vez que se aplican los valores de configuración. Consulte también Uso de Savvius Insight para informes a largo plazo en la página 18:

• Máximo espacio: introduzca la cantidad máxima de espacio en disco (en gigabytes) asignada al servidor de informes antes de eliminar los datos antiguos escritos en el disco duro para dejar espacio a los datos más recientes. Los datos más antiguos se eliminan hasta que el espacio de disco total utilizado en el servidor de informes esté por debajo de la cantidad configurada.

Nota Al configurar Espacio Máximo, tenga en cuenta que debe dejar suficiente espacio en disco disponible para otras funciones de Savvius Insight, incluidas las capturas de captura a disco.

• Ingreso de panel de control: muestra el nombre de usuario utilizado para iniciar sesión en el servidor de informes local desde un navegador web. El nombre de usuario de inicio de sesión predeterminado en el cuadro de mandos es la perspicacia. Este nombre de usuario es diferente del nombre de usuario de inicio de sesión configurado anteriormente para la utilidad de configuración.

• Contraseña de panel: introduzca una contraseña utilizada para iniciar sesión en el servidor de informes local desde un navegador web. La contraseña predeterminada del tablero es savvius. Esta contraseña es diferente de la contraseña de inicio de sesión configurada anteriormente para la utilidad de configuración.

• Remote Elasticsearch: Seleccione esta opción para configurar un servidor Elasticsearch remoto como la opción de informes que Savvius Insight reenvía automáticamente a sus estadísticas de red una vez que se aplican los valores de configuración. Consulte también Uso de Savvius Insight para informes a largo plazo en la página 18:

• Servidor: Introduzca la dirección IP del servidor Elasticsearch remoto.

• Puerto: Introduzca el puerto utilizado para comunicarse con el servidor Elasticsearch.

NotaSi Remote Elasticsearch está seleccionado como la opción de generación de informes en la utilidad de configuración, para ver los cuadros de diálogo de Savvius Insight, primero debe iniciar sesión en el servidor Elasticsearch remoto e importar el archivo de tablas Savvius Insight al servidor. Consulte Importar tableros de control de Savvius Insight al servidor remoto en la página 22.

• Remote Splunk: seleccione esta opción para configurar un servidor Splunk remoto como la opción de informes que Savvius Insight reenvía automáticamente a sus estadísticas de red una vez que se aplican los valores de configuración. Consulte también Uso de Savvius Insight y Splunk en la página 23:

• Servidor: Introduzca la dirección IP del servidor Splunk.

• Puerto: Introduzca el puerto utilizado para comunicarse con el servidor Splunk.

7. Haga clic en Aplicar para guardar y aplicar los valores de configuración a Savvius Insight.

Nota: Se perderá la conexión con Savvius Insight si ha configurado una nueva dirección estática en Configuración anterior.

8. Desconecte el cable de la computadora / portátil al puerto '0 MGMT' de Savvius Insight.

9. Conecte el '0 MGMT' a un puerto de enrutador de su red. Ahora debe ser capaz de alcanzar la dirección IP del puerto de administración de la red.

10.Reserve la configuración de red anterior de su PC o portátil y vuelva a conectarla a su red.

Acciones de Savvius Insight

El enlace de acciones en la parte superior de la utilidad de configuración muestra el cuadro de diálogo Acciones que incluye opciones para apagar, reiniciar y restablecer Savvius Insight a sus valores predeterminados de fábrica.





• Apagado: seleccione esta opción para desactivar Savvius Insight.

• Reiniciar: Seleccione esta opción para reiniciar Savvius Insight.

• Factory Reset: Seleccione esta opción para restablecer los ajustes de fábrica de Savvius Insight. Usted perderá todas las configuraciones y datos guardados en Savvius Insight cuando se restablezca a sus ajustes de fábrica. Una vez que Savvius Insight se ha restablecido, deberá volver a ejecutar la utilidad de configuración como se describe en Configuración inicial mediante la utilidad de configuración en la página 8.

Nota: También puede realizar un restablecimiento de fábrica mediante el botón Restablecer, tal como se describe en Configuración inicial mediante la utilidad de configuración.

Conexión a Savvius Insight a través del puerto serie

Utilizando el cable serie incluido conectado al puerto serie de Savvius Insight, un PC / portátil y un programa terminal de su elección, puede iniciar sesión en Savvius Insight y acceder al símbolo del sistema (root @ Insight). Esto es especialmente útil para el diagnóstico avanzado o el acceso de recuperación.

Para conectarse a Savvius Insight a través del puerto serie:

1.Conecte el cable de la consola serie incluido con Savvius Insight desde el puerto serie (DB-9) de su computadora portátil al puerto serie (RJ-45) en el panel posterior de Savvius Insight.

2. Utilizando cualquier programa de terminal serie (por ejemplo, HyperTerminal o Putty), establezca una conexión con Savvius Insight. Asegúrese de que la configuración del terminal correspondiente coincida con la configuración predeterminada de Savvius Insight:

• Tipo de terminal: [VT100 +]

Guía del usuario de Savvius Insight

18 Uso de Savvius Insight para informes a largo plazo

• Bits por segundo: [115200]

• Bits de datos: [8]

• Paridad: [Ninguno]

• Bits de parada: [1]

• Control de flujo: [Ninguno]

• Soporte de teclas combinadas VT-UTF8: [Activado]

• Modo de grabadora: [Desactivado]

• Resolución 100x31: [Activado]

3.Una vez que se ha establecido una conexión a Savvius Insight, aparece el indicador de inicio de sesión de Insight.

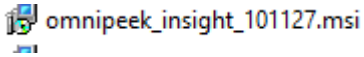
4.Ingrese en Savvius Insight ingresando el nombre de usuario y la contraseña que configuró anteriormente utilizando la utilidad de configuración. Si no configuró un nombre de usuario y una contraseña anteriormente, el valor predeterminado es:

Nombre de usuario: root

Contraseña: savvius

5.El mensaje de comando Insight (root @ Insight) aparece una vez que haya iniciado sesión.

Uso de Savvius Insight y Omnipeek para Savvius Insight



Una versión del software de Omnipeek llamada 'Omnipeek for Savvius Insight' está disponible para su descarga para los usuarios de Savvius Insight. Puede utilizar Omnipeek para el software Savvius Insight para iniciar capturas de paquetes y para analizar los archivos de paquetes que se capturan y guardan en Savvius Insight. El software Omnipeek for Savvius Insight se instala en un equipo con Windows ubicado en la misma red que Savvius Insight. Puede registrar su Savvius Insight y descargar el software Omnipeek para Savvius Insight visitando https://insight.savvius.com/omnipeek.

Nota: Si tiene instalado el software Omnipeek (versión 9.2 y superior) en una computadora, puede usar esa versión de Omnipeek para iniciar capturas y para analizar los archivos de paquetes capturados y guardados en Savvius Insight.

Estas son algunas de las maneras estratégicas de comenzar con Omnipeek para el software Savvius Insight:

• Iniciar una captura: Iniciar una captura le permite capturar y analizar datos en tiempo real y grabar datos para el análisis posterior a la captura de uno o más dispositivos Savvius Insight instalados en la red. Puede ver una captura en tiempo real o guardarla en disco (captura-a-disco) para análisis posterior. Consulte Cómo iniciar una captura en Savvius Insight.

Nota: Recomendamos limitar las instancias de capturas de captura a disco en Savvius Insight para prolongar la vida útil del SSD.

• Ver el dashboard de instrumentos de Compass y otros cuadros de mando: El panel de control de Compass es un panel interactivo de análisis forense que muestra la utilización de la red a lo largo del tiempo, incluyendo estadísticas de protocolos, nodos, flujos, VLAN y aplicaciones. Puede ver estas estadísticas desde un único archivo de captura admitido o desde varios archivos de captura (* .pkt, * .apc, * .pcap [sólo formato Libpcap], * .wcap [sólo formato Libpcap], * .cap [formato Libpcap Sólo], * .wpz y * .pcapng) agregados dentro del espacio de trabajo Compass. Además, otros cuadros de mando, como los paneles de la línea de tiempo, la red y las aplicaciones, también están disponibles para mostrar datos gráficos sobre su red resumidos en varias pantallas fáciles de leer.

• Ver los expertos: las vistas Experto proporcionan un análisis experto del tiempo de respuesta, el rendimiento y las aplicaciones de red en una vista centrada en el flujo de tráfico capturado. Las vistas de expertos también proporcionan una vista detallada de cada

transacción, anotando cualquier evento que se encuentre en cada conversación o flujo individual. Puede profundizar para seleccionar los paquetes asociados con un evento en particular o con cualquier conversación en vistas de Expertos.

• Ver los paquetes: Los paquetes, las unidades de datos transportadas en la red, son la base para todo análisis de red de nivel superior. Al solucionar problemas de red, es importante poder profundizar en los paquetes ellos mismos mirando sus decodificadores individuales así como utilizar los paquetes capturados en el almacenador intermediario como la fundación para el experto y el estadístico

Ventana principal del programa

análisis. La vista Paquetes de una ventana de captura es donde puede ver información sobre los paquetes individuales transmitidos en su red.

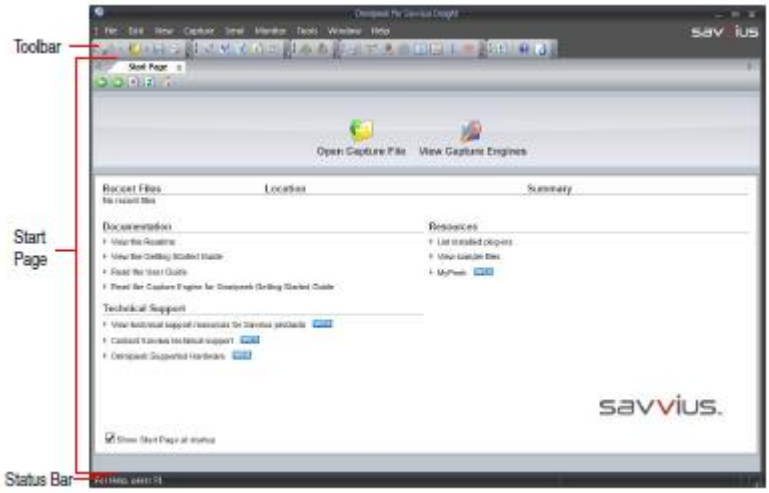
Para obtener más información sobre las características anteriores y más, consulte la Guía del usuario de Omnipeek y la ayuda en línea.

Ventana principal del programa y página de inicio

Para iniciar Omnipeek para Savvius Insight:

• En el menú Inicio, haga clic en Omnipeek para Savvius Insight.

Aparecerá la ventana principal del programa y la página de inicio. A continuación se describen las partes de la ventana principal del programa.



Barra de herramientas: Proporciona botones para las tareas de uso frecuente en Omnipeek. Para mostrar barras de herramientas diferentes o para personalizar opciones de barra de herramientas, en el menú Ver, haga clic en Barras de herramientas.

• Página de inicio: proporciona botones para abrir los archivos de captura guardados y ver la ventana de los motores de captura. Además, la página de inicio proporciona enlaces a recursos útiles, tanto locales como en línea.

ToolbarStatus BarStart Página

Guía del usuario de Savvius Insight

Uso de Savvius Insight y Omnipeek para Savvius Insight

• Barra de estado: Muestra mensajes sensibles al contexto a la izquierda y el adaptador de monitor actual a la derecha. Para alternar la visualización de la barra de estado, en el menú Ver, haga clic en Barra de estado.

Cómo iniciar una captura en Savvius Insight

Las capturas de Savvius Insight le permiten capturar y analizar datos de red en tiempo real y, opcionalmente, registrar datos para el análisis posterior a la captura. Puede iniciar capturas desde cada uno de los puertos Ethernet y desde los puertos puente de Savvius Insight. El uso de los puertos Ethernet requerirá el uso de una toma de red. Las capturas de puerto de puente deben configurarse como se describe en Características del panel frontal en la página 5.

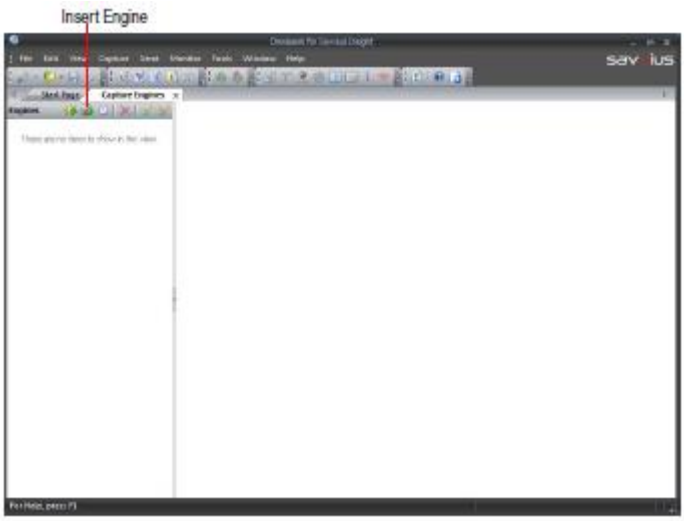
Para iniciar una captura en Savvius Insight:

1. En Omnipeek for Savvius Insight, realice una de las siguientes acciones para abrir la ventana Capture Engines:

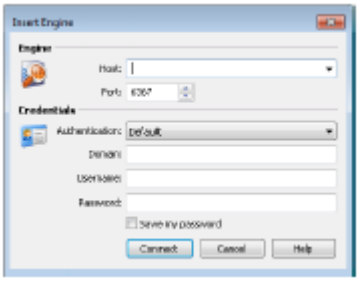
• En la página de inicio, haga clic en Ver motores de captura

En el menú Ver, haga clic en Capture Engines

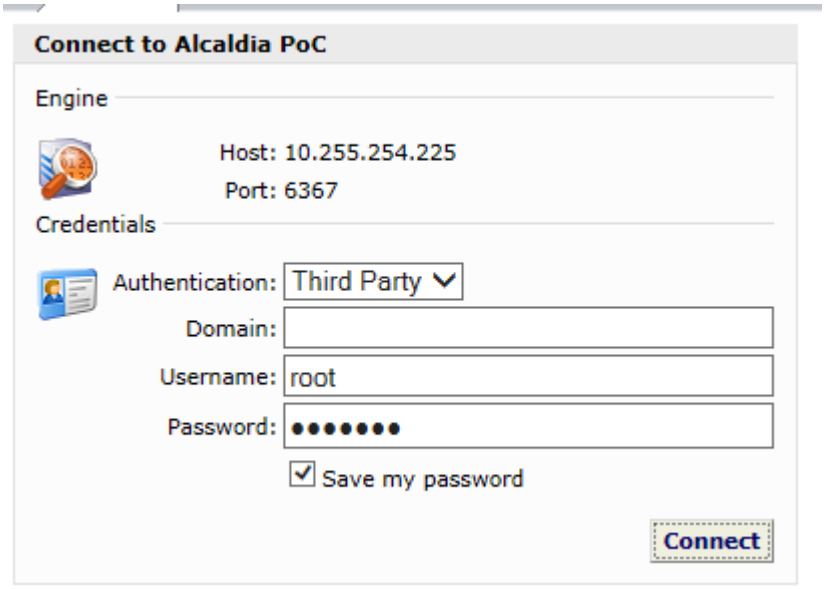
Aparecerá la ventana Motores de captura.



2. Desde la ventana Motores de captura, haga clic en **Insert Engine**. Aparecerá el cuadro de diálogo **Insert Engine**.



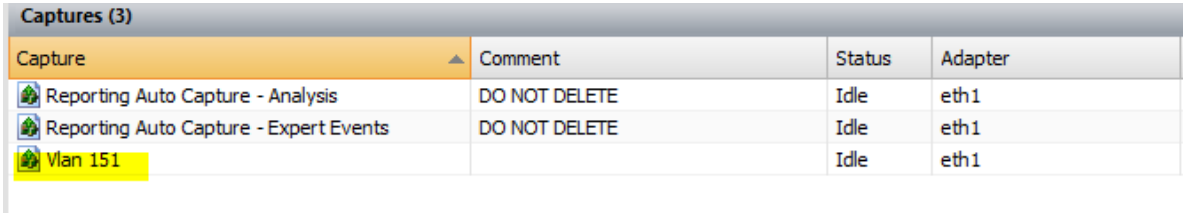
En el caso de la Pascual Bravo :



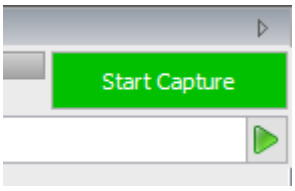
Username: root

Password: xxxxx

Dar click en view Capture :

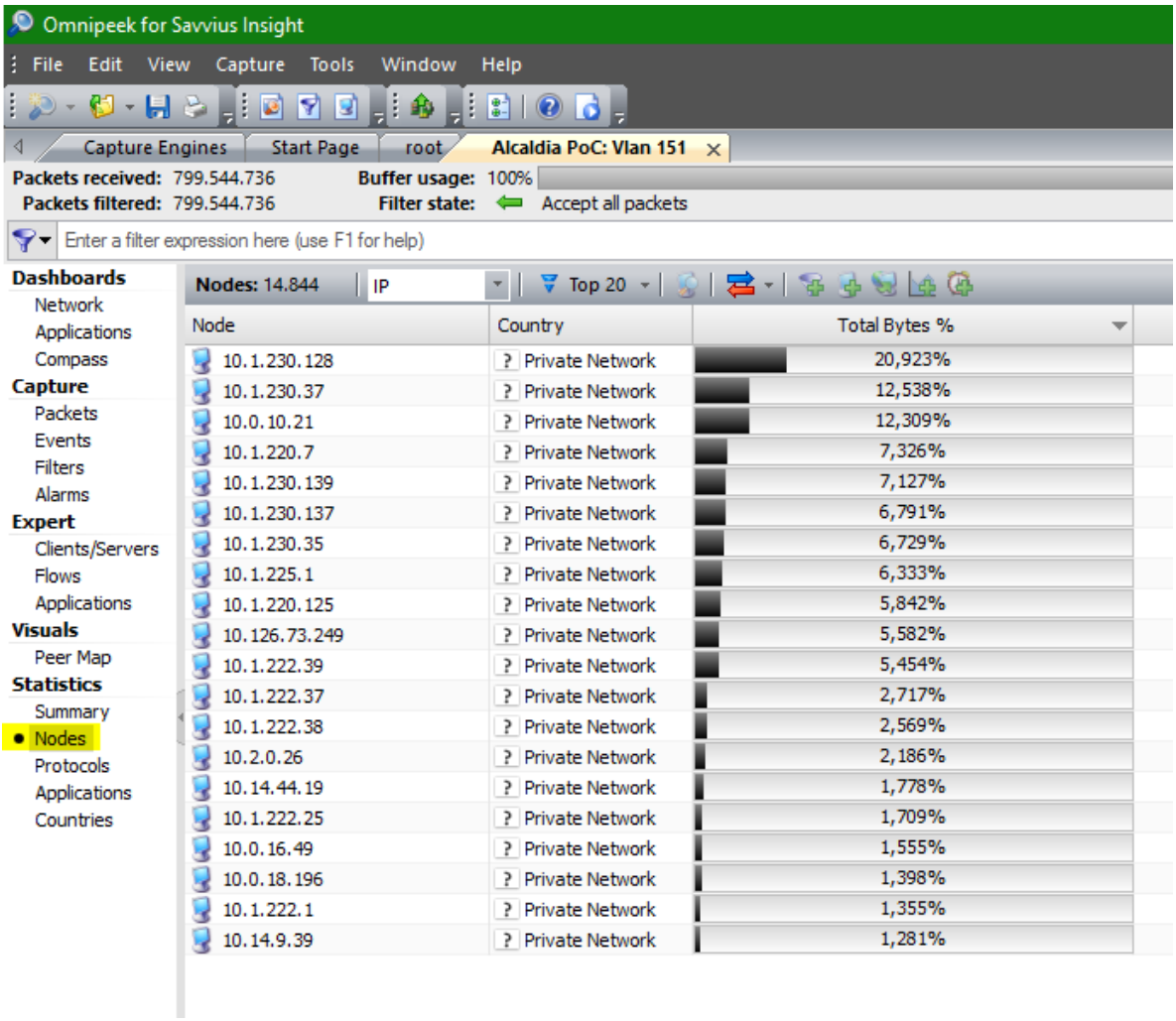


Dar doble click en Vlan 151



Debe aparecer el dashboard:

Aquí ya podemos navegar y visualizar en la solución



3.Complete el cuadro de diálogo:

• Host: Introduzca la dirección IP del Savvius Insight al que desea conectarse.

• Puerto: introduzca el puerto TCP / IP utilizado para las comunicaciones. El puerto predeterminado para el protocolo Savvius WP Omni es 6367.

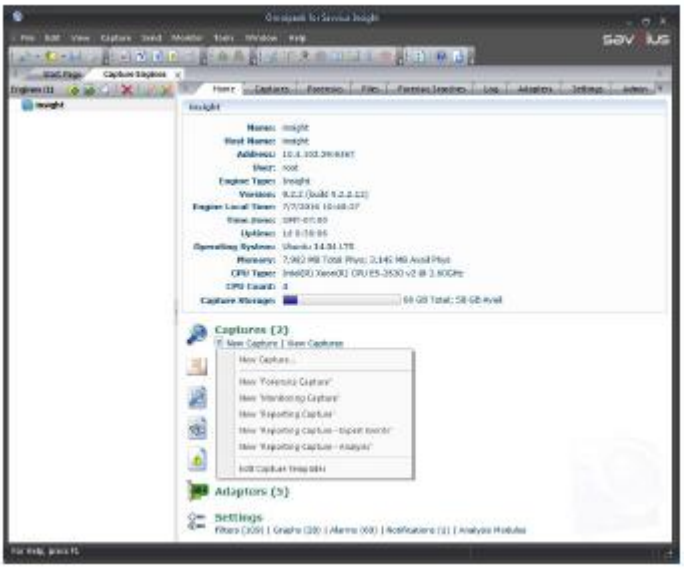
• Autenticación: seleccione Terceros para conectarse a Savvius Insight.

• Dominio: Escriba el Dominio para iniciar sesión en Savvius Insight. Si Savvius Insight no es miembro de ningún dominio, deje este campo en blanco.

• Nombre de usuario: Escriba el nombre de usuario para iniciar sesión en Savvius Insight.

• Contraseña: Escriba la Contraseña para iniciar sesión en Savvius Insight.

4.Haga clic en Conectar. Cuando se establece la conexión, aparece la pestaña Inicio de Savvius Insight.



Quisiera crear:

• New Capture ...: Esta opción le permite crear una nueva captura de Savvius Insight basada en la configuración de captura que defina.

• Nuevo "Forensics Capture": Esta opción le permite crear una nueva captura de Savvius Insight basada en una plantilla de captura forense configurada para el análisis forense después de la captura.

• Nueva "Captura de monitoreo": Esta opción le permite crear una nueva captura de Savvius Insight basada en una plantilla de captura de monitoreo configurada para ver datos de expertos y estadísticos de nivel superior en una captura continua en tiempo real.

• Nueva captura de informes: esta opción le permite crear una nueva captura de informes de Savvius Insight basada en una plantilla de captura configurada para reenviar datos a una de las opciones de informes de Savvius Insight.

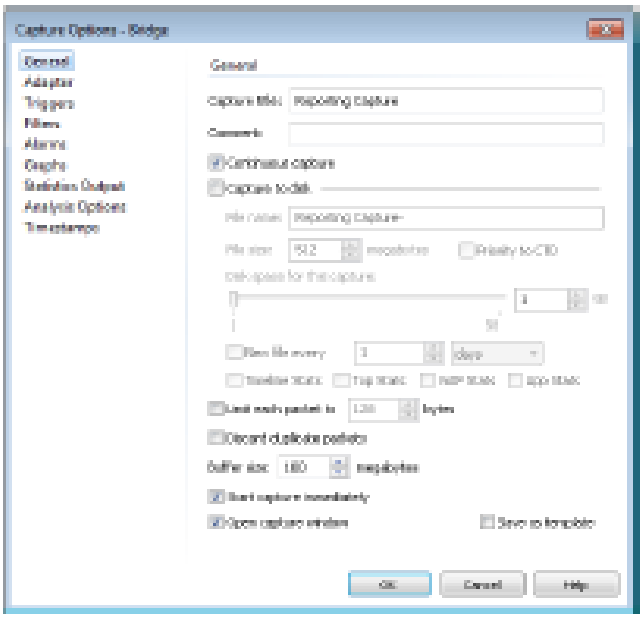
• Nueva captura de informes: eventos de expertos: esta opción le permite volver a crear una captura de informes de Savvius Insight basada en una plantilla de captura optimizada

para el análisis de expertos y configurada para reenviar datos a una de las opciones de informes de Savvius Insight. Esta cómo iniciar una captura en Savvius Insight Se utiliza normalmente junto con el "Reporting Capture - Analysis" para crear una captura de alto rendimiento para exportar datos a una de las opciones de informes. Úselo sólo para volver a crear la captura de informes predeterminada que se preconfiguró en el dispositivo.

• Nuevo "Captura de informes - Análisis": esta opción le permite volver a crear una captura de informes de Savvius Insight basada en una plantilla de captura optimizada para el análisis y configurada para reenviar datos a una de las opciones de informes de Savvius Insight. Esto se suele utilizar junto con "Reporting Capture - Expert Events" para crear una captura de alto rendimiento para exportar datos a una de las opciones de informes. Úselo sólo para volver a crear la captura de informes predeterminada que se preconfiguró en el dispositivo.

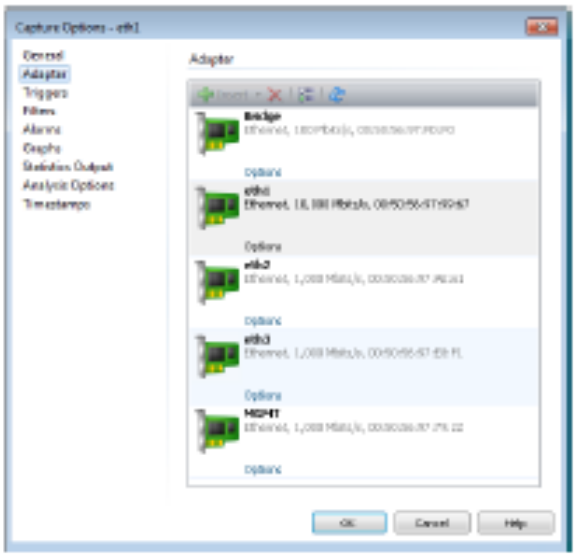
• Editar plantillas de captura: esta opción abre el cuadro de diálogo Plantillas de captura y le permite crear nuevas plantillas de captura o editar las existentes.

Nota: También puede seleccionar las opciones anteriores en la lista desplegable Insertar disponible en la ficha Capturas y en las opciones de Nueva captura disponibles en la ficha Adaptadores.



6. Configure las opciones generales. Haga clic en Ayuda en el cuadro de diálogo para ayudarle a configurar las opciones.

7. Elija un adaptador de captura Savvius Insight en Opciones del adaptador. Cada adaptador corresponde a los puertos Ethernet de Savvius Insight.



8. Haga clic en Aceptar. Aparecerá una nueva ventana de captura de Savvius Insight.



Vistas de la ventana de captura

El panel de navegación de cada ventana de captura presenta las vistas que muestran información sobre los datos de captura. Una ventana de captura de Savvius Insight puede tener las vistas enumeradas a continuación. A continuación se muestra un ejemplo de una ventana de captura de captura a disco desde un dispositivo Savvius Insight.



Cuadros de mando: Estos cuadros de mando muestran los datos gráficos de su red resumidos en varias pantallas fáciles de leer.

• Línea de tiempo: este cuadro de mandos proporciona una visión general de los principales comunicadores, los principales protocolos y la utilización de la red para el motor de captura.

• Red: Este panel proporciona una visión general de las estadísticas de la red para la captura.

• Aplicaciones: Este panel muestra estadísticas clave para las aplicaciones en la ventana de captura.

• Compás: este panel le permite ver la utilización de la red y las estadísticas principales desde un único archivo de captura compatible o desde varios archivos de captura.

• Captura: estas vistas muestran información sobre paquetes capturados en el búfer de captura.

• Paquetes: Esta vista enumera todos los paquetes colocados en el búfer de una ventana de captura (o archivo de captura). Los paneles Decode y Hex muestran el contenido del paquete seleccionado decodificado o en hexadecimal y ASCII.

• Registro: esta vista recoge los mensajes generados por eventos relacionados con la ventana de captura en particular. Estos eventos incluyen los resultados de las notificaciones generadas por los disparadores o módulos de análisis seleccionados para la ventana de captura.

• Filtros: esta vista permite activar, desactivar, añadir, editar y eliminar filtros utilizados para capturar paquetes en el búfer de la ventana de captura.

• Alarmas: esta vista permite consultar una función de estadísticas de monitor específica una vez por segundo, probando las condiciones de resolución y problema especificadas por el usuario. Al hacer coincidir cualquiera de estas pruebas, la función de alarma envía una notificación de la gravedad especificada por el usuario.

• Experto: estas vistas proporcionan un análisis experto de retardo, rendimiento y una amplia variedad de eventos de red en una vista centrada en la conversación del tráfico en una ventana de captura.

• Clientes / Servidores: Esta vista facilita el seguimiento de los eventos y su visualización en el contexto de los patrones de tráfico peer-to-peer o cliente-servidor.

• Flujos: Esta vista muestra cada flujo independientemente en una vista plana. Esta vista simplificada le permite comparar flujos entre sí, independientemente del par de nodos al que pertenezcan.

• Aplicación: Esta vista permite clasificar cada flujo por aplicación. Esta vista le permite ver quién está utilizando cada aplicación en su red y cómo se está realizando cada aplicación.

• Web: estas vistas le permiten mostrar las solicitudes y respuestas de la página web, lo que le permite realizar un seguimiento de la actividad cliente / servidor dentro de una captura. Los mismos datos web se presentan en cuatro formatos.

• Servidores: Esta vista le permite centrarse en qué servidores se están utilizando.

• Clientes: Esta vista le permite centrarse en qué clientes están utilizando qué servidores.

• Páginas: esta vista muestra una lista de páginas web con cada solicitud individual anidada debajo.

• Solicitudes: Esta vista muestra una lista plana de solicitudes HTTP individuales.

• Visuales: estas vistas muestran gráficamente el tráfico y las estadísticas de la red.

• Peer Map: Esta vista le permite visualizar el tráfico de red mostrando nodos y el tráfico entre los nodos. Las líneas indican tráfico entre dos nodos. El espesor relativo de las líneas indica el volumen de tráfico que se produce.

• Gráficos: Esta vista muestra gráficas de elementos individuales de las otras vistas de estadísticas en tiempo real. Los datos de estos gráficos también se pueden guardar como texto delimitado por tabuladores o delimitado por comas, o como XML \ HTML. En un motor de captura, esta vista debe estar habilitada en las opciones de gráficos del cuadro de diálogo Opciones de captura.

• Estadísticas: estas vistas muestran diversos datos estadísticos sobre su red.

Solución de problemas con Omnipeek para Savvius Insight

• Nodos: Esta vista muestra datos en tiempo real organizados por nodo de red. Puede elegir mostrar los nodos en una vista jerárquica anidada (direcciones lógicas anidadas debajo de su dirección física) o en una variedad de vistas tabulares planas. Haga clic con el botón secundario en el encabezado de columna para agregar o quitar varias columnas.

• Protocolos: Esta vista muestra el volumen de tráfico de red como un porcentaje del total de bytes, desglosado por protocolo y subprotocolo. Puede elegir mostrar los protocolos en una vista de Clientes / Servidores anidados o en una vista Flujos.

• Resumen: estas vistas le permiten supervisar las estadísticas clave de la red en tiempo real y guardarlas para una comparación posterior. Las estadísticas resumidas también son sumamente valiosas para comparar el rendimiento de dos redes o segmentos de red diferentes.

• Aplicaciones: estas vistas le permiten ver estadísticas básicas sobre aplicaciones para una ventana de captura.

• Países: estas vistas le permiten ver un desglose geográfico del tráfico basado en la dirección IP para una ventana de captura.

Limitar captura a disco para preservar SSD

Savvius Insight utiliza un SSD con un ciclo de trabajo que no está clasificado para captura continua en disco. Recomendamos limitar las instancias de capturas de captura a disco en Savvius Insight para extender la vida útil del SSD. Los problemas asociados con el uso continuo de captura a disco no están cubiertos por la garantía.

Solución de problemas con Omnipeek para Savvius Insight

Omnipeek for Savvius Insight se puede utilizar de muchas maneras para resolver problemas en su red. Esta sección describe cinco tareas comunes de análisis de red que puede realizar fácilmente con Omnipeek para Savvius Insight.

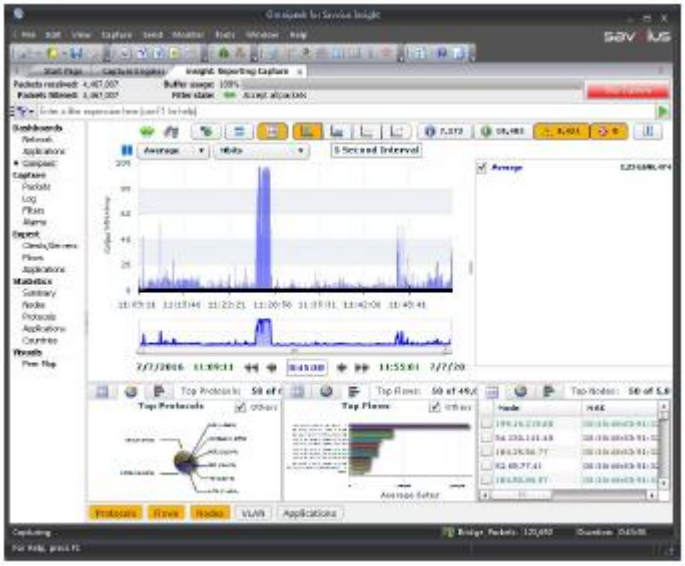
Nota: Los ejemplos siguientes se basan en un archivo de captura de captura a disco guardado en un dispositivo Savvius Insight.

¿Dónde empiezo?

El panel de control de Compass proporciona un resumen intuitivo pero detallado de toda la actividad de la red. Utilice este tablero de instrumentos como su "brújula" para encontrar qué áreas necesitan un análisis más detallado.

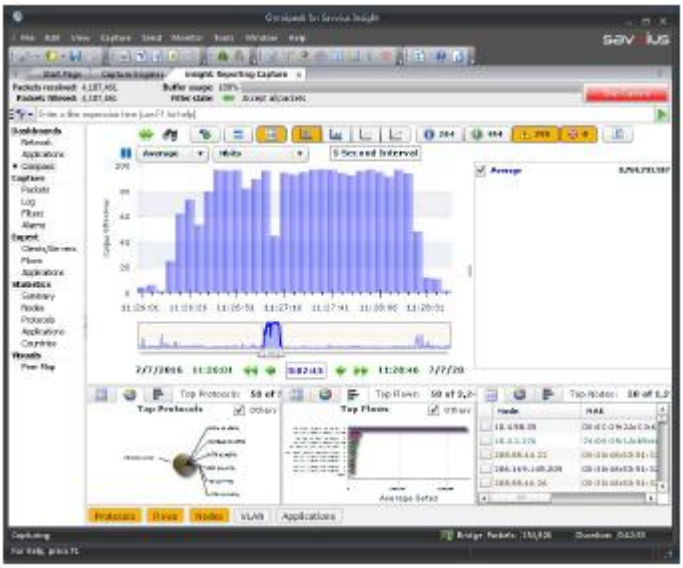
Para utilizar el panel de control de Compass:

1. Haga clic en Compass en el panel de navegación de la ventana de captura para mostrar el panel de control de Compass.



2. En el ejemplo anterior, vamos a aprender más sobre el aumento en la actividad de la red (media Mbits gráfico).

3. Coloque su cursor justo a la izquierda de la espiga, arrastre a través de la espiga, y luego dejar ir. El tablero completo de Compass, el gráfico y los paneles detallados a continuación, se actualizan automáticamente para reflejar el intervalo de tiempo que seleccionó alrededor del punto.

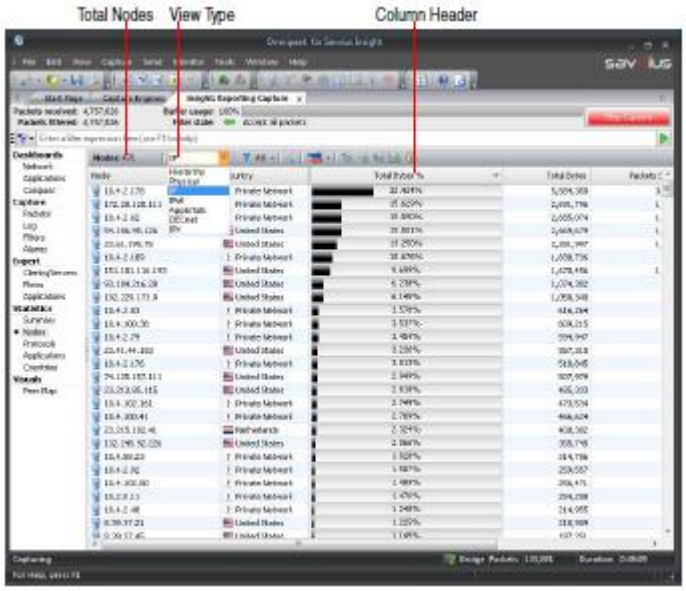


4. Note las ventanas del gráfico de estadísticas de Protocolos, flujos y nodos debajo del gráfico. Puede fijar o desencriptar ventanas de gráficos de estadísticas para Canales, WLAN, VLAN, Tarifas de datos y Aplicaciones haciendo clic en la pestaña deseada o en el icono de pin / unpin (push-pin) en la parte superior derecha de la ventana del gráfico de estadísticas.

5. Ahora tiene una visión completa de su tráfico de red para sólo el punto en la actividad. Utilice cada una de las ventanas de la tabla de estadísticas para ver rápidamente qué causó la punta y determinar si se necesita un análisis más detallado.

¿Quién usa mi red y cómo?

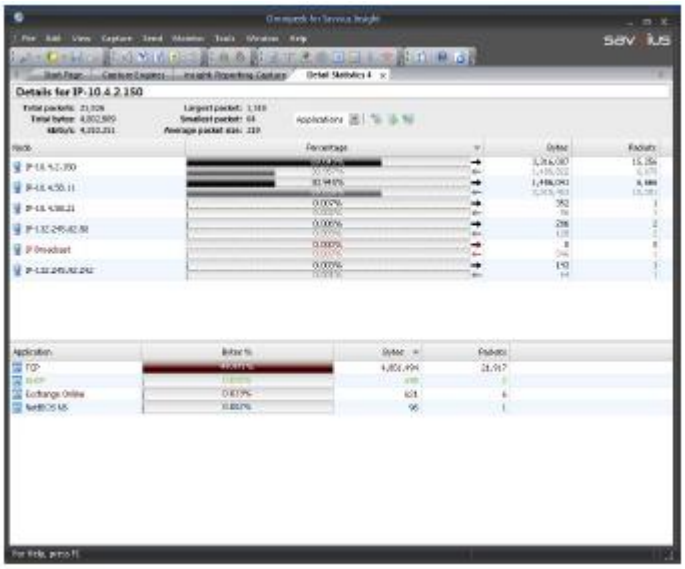
1. Haga clic en Nodos en el panel de navegación de la ventana de captura para mostrar la vista Nodos. La vista Nodos proporciona una lista de todos los nodos que han estado activos en la red desde que se inició la captura.



2. El número total de nodos se muestra en la esquina superior izquierda. Utilice el menú desplegable adyacente para elegir el tipo de datos del nodo a mostrar. "IP" es la vista más común.

3. Haga clic en un encabezado de columna para ordenar los datos por ese parámetro. Si necesita ver rápidamente a sus interlocutores principales, clasifique en las columnas "Total bytes" o "Bytes totales%". Sus locutores superiores subirán a la tapa de la lista.

4. Para ver exactamente lo que están haciendo sus principales interlocutores en la red, simplemente haga doble clic en el nodo para crear una nueva pestaña que muestre el uso general de la aplicación o protocolo para ese nodo. La vista se puede alternar entre la aplicación y el protocolo mediante el cuadro desplegable en la barra de título.



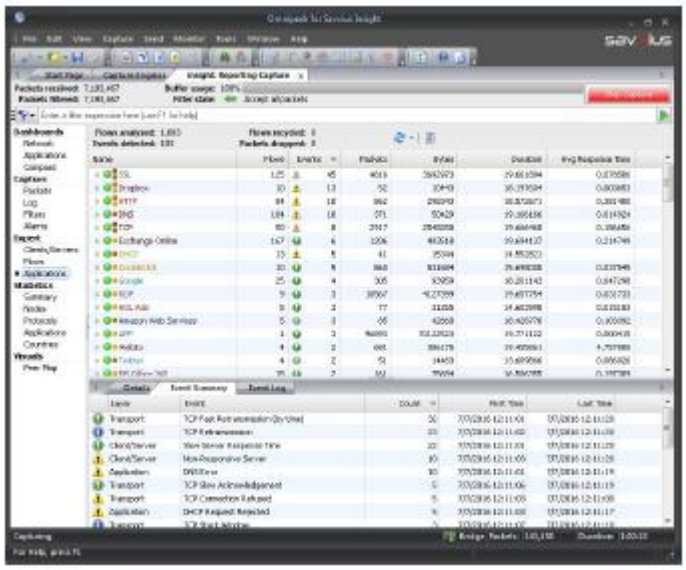
5. Usted ahora sabe quién está utilizando su red, y cómo.

¿Cómo funciona mi red?

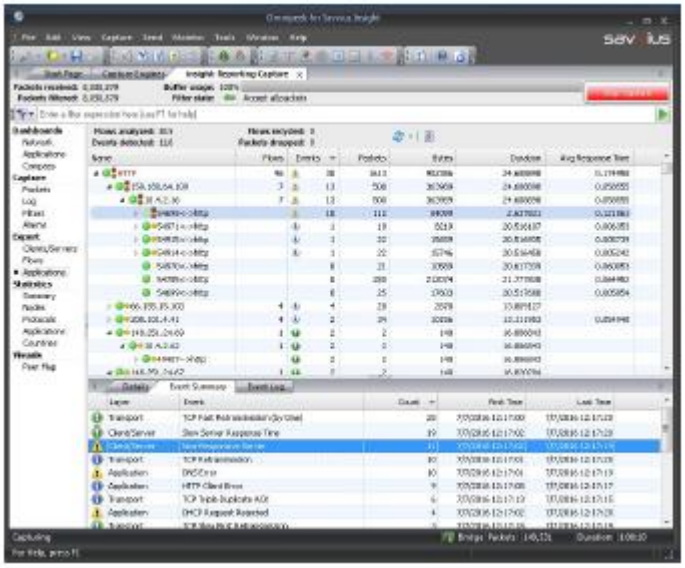
Omnipeek for Savvius Insight realiza un análisis detallado de la red (**análisis "experto"**) en segundo plano para encontrar problemas de red comunes e incluso no tan comunes. Una lista de estos posibles problemas se puede encontrar en las vistas de expertos.

Para utilizar las vistas Experto para realizar análisis de red:

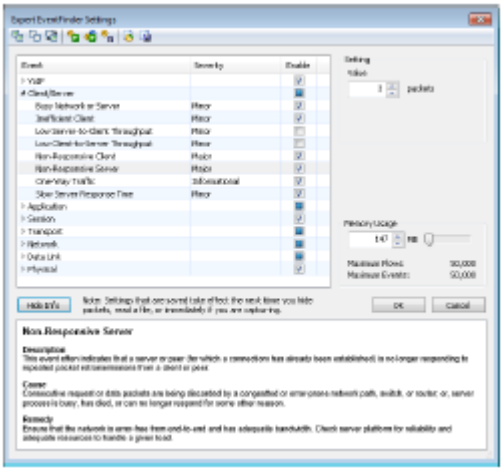
1.Haga clic en Aplicaciones en las vistas Experto del panel de navegación de la ventana de captura. La vista Aplicaciones muestra Análisis experto categorizado por aplicación.



2. Asegúrese de que la pestaña "Resumen de eventos" esté seleccionada en la ventana inferior. La pestaña "Resumen de eventos" muestra todos los problemas potenciales que se han identificado durante esta captura.



3. Para encontrar rápidamente exactamente qué aplicación y qué usuario ha sido afectado por un servidor que no responde, simplemente haga clic en ese evento. Los datos de la aplicación en la ventana superior se ampliarán automáticamente para mostrar exactamente qué aplicación, servidor y cliente se han realizado. En este caso, las tres instancias corresponden a la misma comunicación entre 10.4.2.16 y el servidor 159.180.64.109 sobre HTTP.



4. Si desea ajustar la configuración de esta función de análisis, haga clic con el botón derecho del ratón en el evento en el resumen de eventos, seleccione EventFinder Settings y ajuste los parámetros en el cuadro de diálogo que aparece. También puede ver un resumen del evento y cambiar la gravedad del evento.

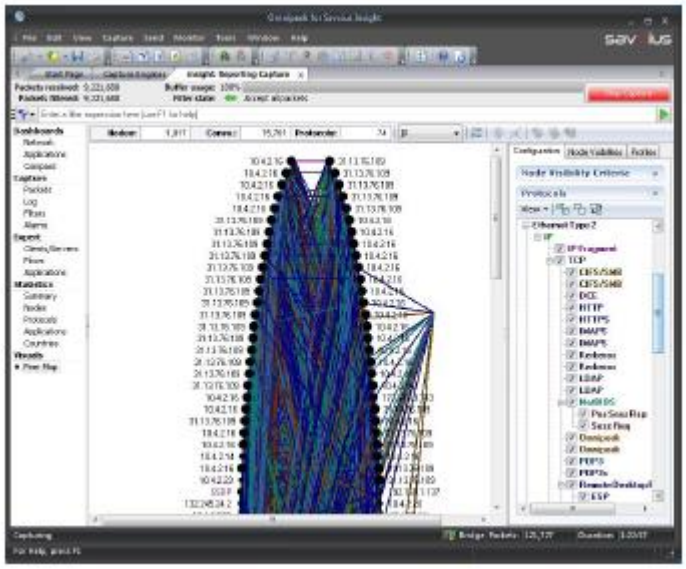
5. Con los eventos de expertos, Omnipeek para Savvius Insight observa su red para usted. Puede configurar alertas basadas en la gravedad del evento para que nunca se pierda un problema.

¿Cómo puedo obtener una sola vista de quién está hablando con quién?

Omnipeek for Savvius Insight incluye una característica llamada Peer Map que proporciona una representación visual de quién está hablando con quien en la red.

Para utilizar el mapa de pares:

1. Haga clic en Peer Map en el panel de navegación de la ventana de captura para mostrar la vista de Peer Map.



. El mapa de pares representa cada nodo de red con un punto.

A. El tamaño del punto varía con el tráfico relativo de ese nodo.

B. Las líneas que emanan de cada nodo representan cada una de sus conexiones a otros nodos de la red.

C. El espesor de la línea se escala al tráfico entre esos dos nodos en relación con todos los otros nodos.

D. El color de la línea representa los protocolos subyacentes en uso - múltiples colores significa múltiples protocolos en uso entre los nodos de la red.

3. Para aislar mejor un nodo, simplemente arrástrelo lejos de los otros para obtener una vista más clara. Cualquier reposicionamiento de nodo se mantendrá la próxima vez que abra el archivo de paquete.

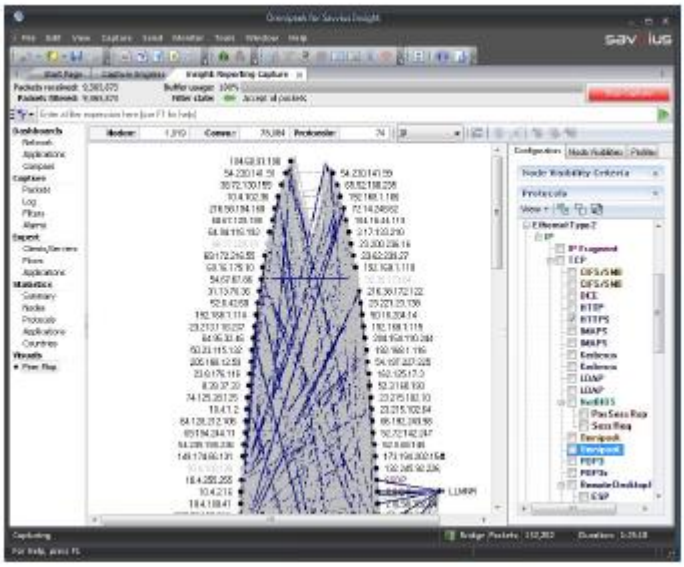
4. El panel de la derecha le permite personalizar la vista en el mapa de pares. Los elementos clave de personalización incluyen:

A. Número de nodos

¿Cómo guardo un archivo para compartirlo con otra persona?

B. Tipo de nodos

C. Protocolos en uso



Por ejemplo, si desea aislar un protocolo concreto para encontrar rápidamente sólo esas conversaciones, haga clic para desactivar todos los protocolos en el panel "Protocolos" y, a continuación, haga clic en la casilla de verificación junto al protocolo que desea aislar, en este caso, HTTPS.

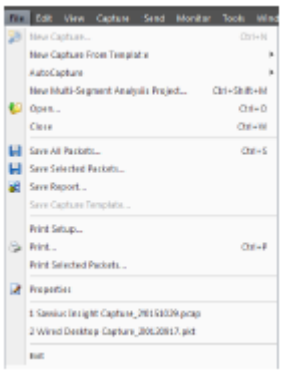
6. En sólo unos pocos clics hemos identificado rápidamente la conversación usando HTTPS que se conecta a Savvius Insight.

¿Cómo guardo un archivo para compartirlo con otra persona?

Puede haber ocasiones en las que desee compartir un archivo de paquetes con otra persona para obtener su opinión sobre un problema de red. Esto es muy fácil de hacer con Omnipeek para Savvius Insight.

Para crear un archivo de paquete:

1. En el menú Archivo, haga clic en Guardar todos los paquetes .... Esto creará un archivo que incluya todos los paquetes asociados con la ventana de captura abierta.



2.Omnipeek for Savvius Insight proporciona una amplia gama de formatos para guardar paquetes, dependiendo del uso que se pretenda del archivo guardado. Algunos ejemplos incluyen:

Formato a.Omnipeek (.pkt, .wpz): utilice este formato si está compartiendo archivos con otro usuario de Omnipeek.

B.Packet List (coma o tab delimited): utilice este formato para exportar información de paquetes a otro programa. El uso más común es importar datos en Microsoft Excel para un análisis adicional de la representación gráfica.

C.Libpcap o PcapNG - utilice uno de estos formatos si está compartiendo archivos con un

Usuario de Wireshark.



Especificaciones técnicas

Las especificaciones técnicas de Savvius Insight se enumeran a continuación:

Configuración básica del sistema

• Pre-cargado, probado y totalmente integrado con el software Savvius Capture Engine

• 8 GB de RAM

• 128 GB HD / SSD SATA

• Procesador Quad-core 1700MHZ Intel Atom

Actuación

• Análisis de red hasta 100Mbps

• Hasta cuatro capturas simultáneas

Ethernet

• Seis puertos Ethernet Gigabit 10/100/1000 integrados

• Interfaz RJ-45

I / O

• Un botón de reinicio

• Un puerto serie RJ45

• Dos puertos USB tipo A

Guía del usuario de Savvius Insight

46 Especificaciones técnicas

Proceso de dar un título

• EMC CE Clase B

• Clase B de la FCC

VCCI

• RoHS

Ambiental

• Temperatura de funcionamiento: 0 ° a 40 ° C (32 ° a 104 ° F)

• Temperatura de almacenamiento: -20 ° a 70 ° C (-4 ° a 158 ° F)

• Humedad relativa: 5% a 90% (sin condensación)

Requisitos de entrada de energía y sistema

• Adaptador de corriente AC / DC externa de 36W

• Tensión de entrada CA: 100-240 VAC

• Corriente nominal de entrada: 100 (10A) - 240V (4A)

• Frecuencia de entrada nominal: 50-60 Hz

Dimensiones y peso

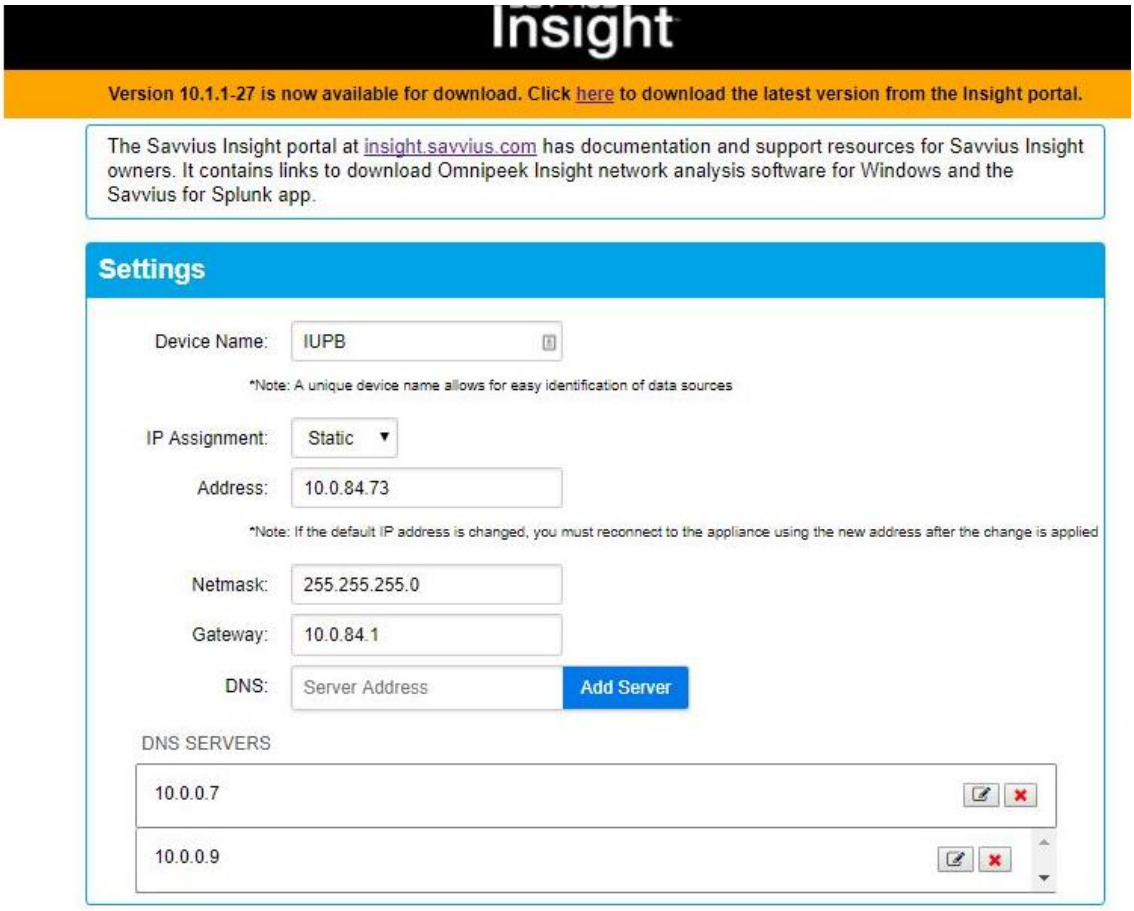
• 44 h x 177 w x 145,5 d

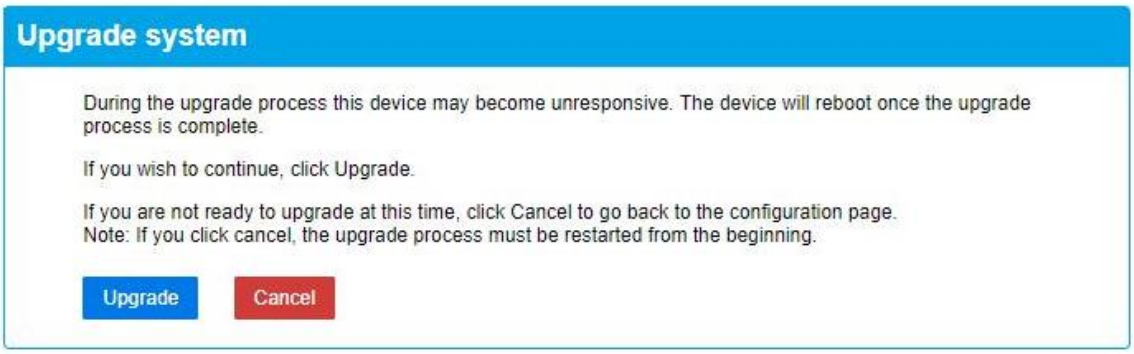
• 2,6 libras

Sistema operativo compatible

Linux

Garantía Savvius Insight/GTI





Reportes de Direcciones IP :

200.114.57.82	Colombia	13,371%	3.154.472.082
200.114.57.96	Colombia	8,982%	2.119.036.220
200.114.57.97	Colombia	7,416%	1.749.575.966
10.0.88.20	Private Network	6,816%	1.608.099.657
10.0.88.48	Private Network	6,399%	1.509.640.339
10.0.88.21	Private Network	5,445%	1.284.586.966
10.0.88.24	Private Network	5,305%	1.251.488.641
157.240.6.51	United States	5,003%	1.180.204.642
10.0.89.212	Private Network	4,818%	1.136.633.675
10.0.88.164	Private Network	4,790%	1.130.087.144
172.217.30.202	United States	4,423%	1.043.517.062
10.0.90.151	Private Network	4,140%	976.720.426
200.114.57.81	Colombia	3,621%	854.374.501
172.217.28.106	United States	3,145%	741.868.100
10.0.88.22	Private Network	3,091%	729.243.041
216.58.222.202	United States	2,868%	676.580.508
10.0.88.136	Private Network	2,828%	667.149.986
10.0.88.10	Private Network	2,734%	644.975.014
190.248.35.81	Colombia	2,617%	617.370.344
190.216.143.147	Colombia	2,244%	529.458.228
190.248.35.78	Colombia	2,220%	523.695.592
190.248.35.76	Colombia	2,205%	520.243.510
200.114.35.66	Colombia	2,130%	502.506.365
190.248.35.77	Colombia	2,026%	478.050.820
190.248.35.83	Colombia	1,985%	468.279.784
200.114.35.130	Colombia	1,926%	454.358.060
10.0.88.127	Private Network	1,858%	438.435.867
190.248.35.82	Colombia	1,614%	380.802.732
10.0.88.155	Private Network	1,576%	371.797.193
10.0.92.143	Private Network	1,538%	362.862.533
10.0.88.68	Private Network	1,483%	349.948.594

Atentamente,

Jorge Robledo Delgado
Ingeniero Preventa
Celular 3158762925
Jorge.robledo@cv-comunicaciones.com