Hoja de datos

Obtenga recolección de registros escalable hoy

HP ArcSight Connectors

Usted archiva y analiza datos de registros por una amplia gama de motivos que abarcan desde monitoreo de la seguridad hasta operaciones de TI, y desde el cumplimiento regulatorio hasta la detección de fraudes. Una capa eficaz de recolección de registros simplifica y optimiza la adición de registros en miles de dispositivos y cientos de ubicaciones. Sirve como base de administración de registros y plataformas de información de seguridad y administración de eventos (SIEM).

La recolección de registros completa y eficiente en toda la empresa va más allá de proporcionar una taxonomía común para facilitar el análisis. Con el rápido crecimiento del panorama regulatorio, se necesita recolectar un conjunto mucho más amplio de fuentes de eventos, que incluyen dispositivos físicos, de redes y seguridad, hosts, bases de datos y una gama de aplicaciones comerciales y desarrolladas internamente. Por lo tanto, la amplitud y profundidad de dispositivos compatibles en términos de recolección de archivos son primordiales.

Los diversos dispositivos, hosts y aplicaciones que generan registros abarcan cientos o incluso miles de ubicaciones físicas. Por consiguiente, las infraestructuras de recolección de registros deben escalar para responder a las necesidades de grandes redes heterogéneas distribuidas. También deben proporcionar una colección de registros protegida y confiable con calidad de auditoría, con controles de administración de tráfico, implementación y administración simples.

La tecnología HP ArcSight Connector enfrenta estos desafíos básicos a través de una poderosa capa de agregación y optimización de registros que también representa la base para su plataforma más amplia de administración de registros y SIEM.

Amplitud y profundidad de dispositivos compatibles

La biblioteca de HP ArcSight de conectores fuera de caja proporciona una recolección optimizada para más de 300 productos comerciales. Estos productos abarcan toda la variedad de tipos de fuentes generadoras de eventos, desde dispositivos de red y seguridad hasta bases de datos y aplicaciones empresariales. Además de las muchas fuentes comúnmente compatibles, la tecnología HP ArcSight Connector también admite de forma exclusiva:

- Gestión de la identidad y el control de acceso
- Prevención de fuga de datos
- Monitoreo de la actividad de la base de datos
- Mainframe
- Aplicaciones

Asimismo, el framework de HP FlexConnector brinda una interfaz impulsada por asistente para crear la lógica de recolección y contextualizar los registros de fuentes propietarias y desarrolladas internamente. Cada uno es crítico para satisfacer los casos de uso, como cumplimiento, fraude y amenazas internas.

Aspectos destacados

- Ofrece visibilidad completa con compatibilidad de recolección para cualquier fuente de evento, desde la capa física hasta la capa de la aplicación
- Ofrece facilidad de análisis a través de un formato de evento común para todas las fuentes de registros
- Crea relevancia de contenido universal con contenido precreado, independiente del proveedor

Procesamiento distribuido

Una vez recolectados, es necesario analizar los datos de registros en tiempo real e históricamente para abordar diversos casos de uso, como monitoreo de la seguridad y cumplimiento regulatorio. Típicamente, todo el procesamiento queda en la administración centralizada de registros y componentes de SIEM.

Sin embargo, HP ArcSight Connectors está diseñado para descargar eficientemente la administración de registros de HP ArcSight y las plataformas SIEM desde tareas de procesamiento central, que se ejecutan con igual eficiencia en el punto de recolección. Con este objetivo, HP ArcSight Connectors también puede realizar diversas funciones, que incluyen:

- Recolección de registros brutos junto con normalización de eventos de registros individuales, y mapeo tanto de sus valores como de sus esquemas en una taxonomía de eventos universal. Esto desempeña un papel fundamental al permitir búsquedas, información y correlación entre dispositivos.
- Categorización o clasificación adicional de eventos con un formato común, legible para los humanos, que evita que el usuario final tenga que ser experto en la lectura del producto de innumerables dispositivos de varios proveedores. La categorización también prepara a las empresas para el futuro al hacer que todo el dispositivo de contenido sea independiente, por lo que si necesita reemplazar los proveedores, todos los informes y reglas continúan funcionando con fluidez.
- Filtrado opcional de los datos que es externo al análisis y no se requiere para la retención según los requisitos regulatorios o las políticas corporativas, como alertas de estado del sistema.

Recolección de registros con calidad de auditoría

La recolección protegida y confiable de registros de auditoría es esencial para permitir la viabilidad de los datos de registros con fines legales y forenses. Sin embargo, muchas fuentes en ubicaciones remotas son solo capaces de generar registros a través de protocolos no confiables y sin protección, como el protocolo como syslog mediante User Datagram Protocol (UDP). HP ArcSight Connectors ofrece una opción de recolección localizada, fácil de implementar y administrar, para oficinas remotas, que proporciona seguridad de extremo a extremo y disponibilidad de datos de registros.

HP ArcSight Connectors ofrece caché local, por lo que en caso de pérdida de conectividad entre oficinas remotas y puntos de adición de registros centrales, no hay pérdida de datos de eventos críticos. HP ArcSight Connectors también admite failover automatizado a un HP ArcSight Logger secundario o HP ArcSight Enterprise Security Manager (ESM) en caso de que el destino primario no esté disponible.

Administración del tráfico de registros

Las oficinas remotas, como las tiendas minoristas, a menudo carecen de enlaces de red de área amplia (WAN) de alto ancho de banda a data centers. Además, es necesario priorizar el ancho de banda disponible para el tráfico de transacciones críticas para los negocios. Para enfrentar estos desafíos, HP ArcSight Connectors ofrece controles de ancho de banda pormenorizados, compresión de registros en tránsito, así como priorización y loteo de datos de registros por tiempo y gravedad.

Cumplimiento de las políticas de implementación de hardware y software

La implementación distribuida y localizada de la infraestructura de recolección de registros es fundamental para la recolección protegida y confiable de registros. Sin embargo, organizaciones como la suya luchan con los dolores de cabeza de desplegar infraestructura adicional en ubicaciones remotas. El espacio en rack a veces es limitado y los servidores existentes no pueden sobrecargarse con agentes adicionales para la recolección de registros. Asimismo, su personal de TI a veces es limitado y no puede implementar y administrar la infraestructura de recolección de registros en oficinas remotas. Para resolver estas limitaciones, HP ArcSight Connectors está disponible en una gama de dispositivos plug-and-play y como software que puede implementarse con facilidad y administrarse de forma remota. HP ArcSight Connectors ofrece una opción de recolección localizada, aunque sin agentes, que reduce el costo neto de adquisición y reduce la demora debido a la selección, adquisición y prueba del hardware.

Para ubicaciones donde no hay espacio adicional en rack disponible pero donde se dispone de ciclos de computación de reserva en servidores existentes, HP ArcSight Connectors ofrece la flexibilidad de implementaciones basados en software, mientras ofrece capacidades sólidas de gestión centralizada.

Gestión centralizada de infraestructura de recolección de registros

Hay gastos significativos asociados con las actualizaciones, los cambios de configuración y el mantenimiento general permanentes de una implementación distribuida de recolección de registros. Incluso las organizaciones mundiales con numerosas oficinas prefieren evitar gastar valiosos recursos humanos de TI en administrar otra infraestructura distribuida. Por lo tanto, no es suficiente para una solución de recolección de registros simplemente admitir una implementación distribuido. HP ArcSight Connectors ayuda a minimizar los gastos administrativos permanentes a través de soporte de diagnóstico, definición universal, definición selectiva, alteración e implementación de parámetros de recolección de registros y valores de configuración desde una interfaz centralizada basada en la Web. Las capacidades de gestión centralizada incluyen todos los conectores basados en software y dispositivos en todo el entorno.

Aspectos destacados

- Consola de gestión de seguridad centralizada para la solución de análisis de registros de HP ArcSight
- Facilidad de implementación, gestión y escalabilidad
- Administre grandes implementaciones fácilmente para permitir alta escalabilidad
- Administración de cambios simplificada a través de una única consola

HP ArcSight Management Center

Consola centralizada

Un centro de gestión de la seguridad centralizado unifica la administración, configuración y monitoreo de la solución de administración de registros HP ArcSight para grandes empresas. El HP ArcSight Management Center permite a los clientes administrar grandes implementaciones de HP ArcSight Logger(dispositivo y software), SmartConnectors, FlexConnectors, y Connector Appliance (ConApp) a través de una única vista consolidada. Management Center le permite enfocarse en sus casos de usos, transmisiones y amenazas eficazmente en oposición a gestionar una solución de administración de registros.

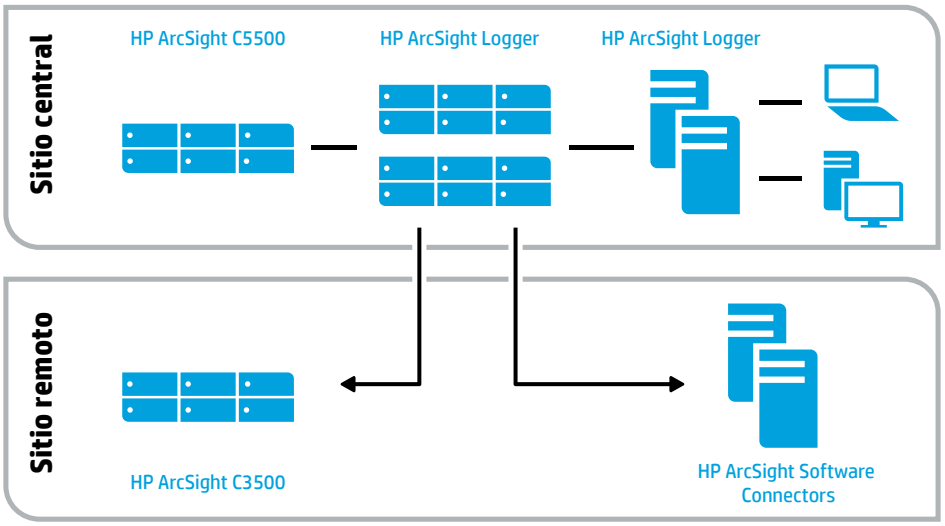
Intercambio de contenido con HP ArcExchange

HP ArcSight Connectors posibilita el intercambio de información con un simple clic del mouse. Con el recurso HP ArcExchange, los usuarios pueden descargar y cargar conectores creados a medida de Protect 724, la comunidad de usuarios en línea de HP Enterprise Security. Los conectores desarrollados y compartidos por esta comunidad permiten la recolección de datos de eventos desde aplicaciones personalizadas y avanzadas, bases de datos, dispositivos y otras fuentes. Esta capacidad, junto con compatibilidad inmediata con más de 300 productos, hace que la plataforma HP ArcSight sea la solución SIEM más amplia disponible en el mercado.

Integración de la plataforma HP ArcSight

Los requisitos de retención regulatoria, las necesidades de informes de auditoría, la resolución de problemas de operaciones de TI, los acuerdos de nivel de servicios (SLA) y el monitoreo proactivo de las amenazas de seguridad representan una continuidad en la cadena de valor de extracción de contenido e inteligencia de los datos de registros. Así, es lógico aprovechar una infraestructura de recolección común en la gama completa de necesidades de recolección y archivo de registros para una empresa, y eso es exactamente lo que ofrece HP ArcSight Connectors. Como capa de recolección de datos en la plataforma, los conectores ofrecen una infraestructura de recolección integral, sólida, escalable y fácilmente administrable que puede utilizarse en la administración de registros y los módulos SIEM, como se muestra en la figura 1. Esta es una ventaja distintiva de la plataforma integrada HP ArcSight y evita la implementación de varias infraestructuras de colección que se necesitarían si se utilizaran soluciones de varios proveedores para la administración de registros y SIEM. Este beneficio se aplica a los despliegues de tecnología de HP ArcSight Connector basada tanto en dispositivos como en software.

Figura 1. Colección de registros protegida y confiable en todos los dispositivos y ubicaciones



HP ArcSight Connector Appliance (ConApp)

Modelo	EPS máx.
C3500 (HP)	2500
C5500 (HP)	5000
Software ConApp	**SO compatible:** Red Hat Enterprise Linux v6.2, 64 bits Oracle Enterprise Linux, v6.1, 64 bits CentOS, v6.2, 64 bits **Versión de software:** Connector Appliance v6.3 o posterior **Hardware mínimo recomendado:** CPU: 1 o 2 Intel® Xeon® de cuatro núcleos o equivalente Memoria: 4–12 GB Espacio en disco: 4-12 GB
Dispositivo ConApp	**SO compatible:** Red Hat Enterprise Linux v6.2, 64 bits **Administración:** navegador web, CLI, API de servicios web **Versión de software:** Connector Appliance v6.4 P1 o posterior **CPU:** 1 procesador Intel Xeon, E5-2620 2.0 GHz, de 6 núcleos **RAM:** 32 GB, 1600 MHz de RAM **Chasis:** 1U **Almacenamiento:** 4x500 GB (1.5 TB RAID-5) **Alimentación:** 2 fuentes de alimentación de 460 W CS Platinum **Dimensiones (largo x ancho x alt.):** 27,5" x 17,1" x 1,7" **Interfaces de Ethernet:** 4 x 10/100/1000

Conclusión

HP ArcSight Connectors ofrecen registros flexibles, escalables, con calidad de auditoría de manera protegida y confiable para monitoreo de seguridad y cumplimiento. La administración centralizada de todos los conectores en todo el entorno aumenta la eficiencia operativa al hacer que la implementación y la administración sean simples. Nuestros productos se adaptan a las necesidades de los clientes al brindar conectores tanto en formatos de dispositivos de software y hardware, adaptándose de ese modo a sus necesidades y no obligándolo a adaptase a las nuestras.

Acerca de HP Enterprise Security

Somos un proveedor líder de soluciones de seguridad y cumplimiento normativo para las empresas modernas que desean mitigar el riesgo en sus entornos híbridos y defenderse de amenazas avanzadas. Basada en productos líderes del mercado de HP ArcSight, HP Fortify y HP TippingPoint, HP Security Intelligence Platform ofrece de forma exclusiva correlación avanzada, protección de la aplicación y defensa de la red para proteger la infraestructura de TI híbrida actual de amenazas cibernéticas sofisticadas.

Servicios HP Software

Los Servicios mundiales HP ESP adoptan un enfoque holístico para construir y ejecutar soluciones de seguridad y respuesta cibernética y capacidades que apoyan la gestión de amenazas cibernéticas y las necesidades de cumplimiento normativo de las empresas más grandes del mundo. Usamos una combinación de conocimiento operativo, suyo y nuestro, y metodologías comprobadas para entregar resultados rápidos y efectivos y demostrar el retorno de la inversión (ROI). Nuestras soluciones probadas impulsadas por casos de uso combinan tecnología líder del mercado con un proceso de negocios y técnico sostenible ejecutado por personas capacitadas y organizadas.

Conozca más sobre los Servicios mundiales HP ESP en hpenterprisesecurity.com.

Conozca más en
hp.com/go/SIRM

Suscríbase para obtener actualizaciones
hp.com/go/getupdated

Compartir con colegas

Calificar este documento

4AA4-1233SPL, octubre de 2014, Rev. 3