Optar-en y del permiso búsqueda avanzada orbital en su AMP para el despliegue de las puntos finales (para los clientes existentes el 8 de enero 2020)

Contenido

Cisco puso en marcha recientemente dos paquetes para el AMP para las puntos finales: Esencial y ventaja. La búsqueda avanzada orbital es una característica fundamental en el paquete de la ventaja. Todos los clientes existentes a partir de la fecha del lanzamiento (8 de enero 2020) pueden optar-en utilizarla sin cargo para el resto de su término de contrato. Este FAQ tiene más información sobre los paquetes y cómo afecta a los clientes existentes a partir de la fecha del lanzamiento.

La búsqueda avanzada orbital es una nueva capacidad avanzada en Cisco AMP para las puntos finales diseñadas para hacer la investigación de la Seguridad y la búsqueda de la amenaza simples proporcionando sobre las interrogaciones de cientos catálogos. Esto permite que usted funcione con rápidamente las interrogaciones complejas en cualquiera o todas las puntos finales. Esto también le permite ganar una visibilidad más profunda en qué sucedió en cualquier punto final en un momento dado tomando una foto de su estado actual.

Con la búsqueda avanzada orbital, usted puede hacer las tareas importantes siguientes mejor, más rápidamente:

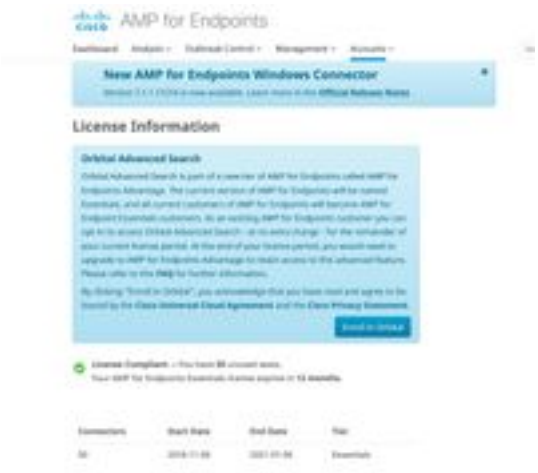
- **Caza de la amenaza**. Búsqueda para los artefactos malévolos en el tiempo real cercano para acelerar su caza para las amenazas.
- **Investigación de incidente**. Consiga a la causa raíz del incidente rápido, corrección de aceleración.
- **Operaciones TIC**. Siga simplemente la espacio de disco, la memoria, y otros artefactos de las operaciones TIC.
- **Vulnerabilidad y conformidad**. Controle rápidamente el estatus de los sistemas operativos para saber si hay cosas como las versiones y las actualizaciones de la corrección, asegurando sus puntos finales están de acuerdo con las Políticas actuales.

Este documento es guía paso a paso a recorrer usted con cómo optar-en a la nueva función y para activarla en sus puntos finales. Una guía de usuario orbital completa está disponible también. El AMP para los clientes de las puntos finales puede activar la búsqueda avanzada orbital fácilmente si sus puntos finales tienen ya un conector instalado (7.1.5 o más alto). Vea el AMP para el tema de ayuda de la consola de las puntos finales en el orbitario para la versión más actual del conector y la otra información. La búsqueda avanzada orbital se utiliza actualmente en Windows 64-bit 10 host que funcionan con la versión 1703 (actualización de los creador) o más adelante.

Una vez que usted ha completado estos pasos, vea la guía de inicio rápido para una más descripción detallada de cómo conseguir comenzado usando la búsqueda avanzada orbital.

Paso 1: Optar-en a la búsqueda avanzada orbital

Si usted no ha alistado en la búsqueda avanzada orbital beta ni ha optado previamente adentro explícitamente, usted puede hacer tan de la página de la información sobre la licencia en el AMP para la consola de las puntos finales. Optar-en a la búsqueda avanzada orbital, el registro en el AMP para las puntos finales consuela y selecciona el descenso abajo de las **cuentas > de la información sobre la licencia**. En esta página usted puede hacer clic **alista en el orbitario** para conseguir el acceso a esta capacidad.



NOTA: Usted debe ser un usuario privilegiado (admin) optar-en a la búsqueda avanzada orbital.

Paso 2: Búsqueda avanzada orbital del permiso en una política existente

Si sus puntos finales tienen ya un conector le instaló (versión 7.1.5 o posterior) entonces puede activar simplemente la búsqueda avanzada orbital en una política existente para sus puntos finales.

- Vaya al AMP para la consola de las puntos finales. En la **Administración > las directivas**, seleccione la directiva que usted quiere activar la búsqueda avanzada orbital adentro y hacer clic el **botón Edit** para abrir la **directiva del corregir** bajo *configuraciones avanzadas* seleccione el **orbitario** y verifique que la búsqueda avanzada orbital está activada. El cuadro **orbital de la búsqueda avanzada del permiso** debe ser controlado. Si no, controle el cuadro para activarlo.

A este punto cualquier conector instalado con esta directiva activará automáticamente la búsqueda avanzada orbital en esa punto final.

Paso 3: Active la búsqueda avanzada orbital en una nuevos directiva y grupo de ordenadores (opcionales)

Como se describe anteriormente, una vez que usted ha activado la búsqueda avanzada orbital en una política existente entonces toda la los conectores usando esa directiva tendrán búsqueda avanzada orbital activada y cualquier nuevos conectores que usted instale, que utilizan esa directiva, también tendrá búsqueda avanzada orbital activada. Por ejemplo, si usted hace que 1000 ordenadores en su “protejan” al grupo, simplemente la activación de la búsqueda avanzada orbital en esa directiva activará automáticamente la búsqueda avanzada orbital en esas puntos finales mientras se despliegue la versión 7.1.5 o posterior del conector.

Crear las nuevos directivas y grupos es opcional. Sin embargo, si usted quiere utilizar la búsqueda avanzada orbital en un grupo específico de puntos finales usando una nueva directiva y el grupo, después siga simplemente la Documentación del Producto para crear una nuevos directiva y/o grupo y para asegurarse de que la búsqueda avanzada orbital está activada en la directiva como se muestra arriba.

Paso 4: Explore la consola orbital

Una vez que usted ha activado la búsqueda avanzada orbital en una directiva con una versión del conector más arriba de 7.1.5 instalados en por lo menos una punto final, usted puede ahora ejecutar las interrogaciones en una punto final para recopilar la información de ella.

- Vaya a la **Administración > a los ordenadores** y localice un ordenador con la búsqueda avanzada orbital amplían el cristal y hacen clic la **interrogación orbital**. (Usted puede también tener acceso a la consola orbital yendo al **análisis > búsqueda avanzada orbital**).
- La consola orbital se carga en un nuevo navegador cuadro. Si es necesario, **clave del** tecleo **con el Cisco Security** a autenticar usando sus credenciales existentes de la consola AMP.

NOTA: Usted puede también tener acceso a la búsqueda avanzada orbital directamente en https://orbital.amp.cisco.com

- **Las puntos finales** colocan las demostraciones los ordenadores que serán preguntados. Usted puede ingresar un GUID específico o ingresar **todos** en este campo para preguntar

cada punto final en su organización que tenga búsqueda avanzada orbital activada. Si usted quisiera tomar un muestreo al azar de las puntos finales, haga clic las elipses (...) para abrir el cuadro de diálogo **al azar de las puntos finales del agregar**.

- Usted puede ingresar las declaraciones SELECTAS de la aduana en el campo **SQL**, o el tecleo **hojea el catálogo de la interrogación** para abrir el **catálogo de la interrogación**, que contiene las docenas de interrogaciones que usted pueda agregar a su interrogación. **Usted no necesita saber escribir una instrucción select SQL para utilizar el orbitario.**

- **Interrogación del** tecleo. La interrogación se funciona con contra las puntos finales especificadas, y los resultados se visualizan en el panel derecho. Usted puede corregir la interrogación y el reestreno. Usted puede descargar los resultados. Usted puede salvar la interrogación mientras que un trabajo de ser ejecutado sobre una base programada que usted pueda configurar.
- Para más información consiguiendo comenzado con la búsqueda avanzada orbital, explore el inicio rápido