Acceda y habilite la búsqueda avanzada orbital en su implementación de AMP para terminales (para clientes existentes a partir del 8 de enero de 2020)

Contenido

Cisco ha lanzado recientemente dos paquetes para AMP para terminales: Aspectos básicos y ventajas. La búsqueda avanzada orbital es una función clave del paquete Advantage. Todos los clientes existentes a partir de la fecha de lanzamiento (8 de enero de 2020) pueden suscribirse para utilizarla sin coste alguno durante el resto de su contrato. Esta FAQ tiene más información sobre los paquetes y cómo afecta a los clientes existentes en la fecha de lanzamiento.

Orbital Advanced Search es una nueva capacidad avanzada de Cisco AMP para terminales diseñada para facilitar la investigación de seguridad y la búsqueda de amenazas proporcionando más de cien consultas de catálogo. Esto le permite ejecutar rápidamente consultas complejas en cualquier o todos los terminales. Esto también le permite obtener una mayor visibilidad de lo que ha sucedido en cualquier terminal en un momento dado tomando una instantánea de su estado actual.

Con la búsqueda avanzada orbital, puede realizar las siguientes tareas importantes mejor y más rápido:

- **Caza de amenazas**. Busque artefactos maliciosos casi en tiempo real para acelerar la búsqueda de amenazas.
- **Investigación de incidentes**. Llegue rápidamente a la causa principal del incidente, acelerando la remediación.
- **Operaciones de TI**. Solo tiene que realizar un seguimiento del espacio en disco, la memoria y otros artefactos de operaciones de TI.
- **Vulnerabilidad y cumplimiento**. Compruebe rápidamente el estado de los sistemas operativos en busca de versiones y actualizaciones de parches, asegurándose de que los terminales cumplen con las políticas actuales.

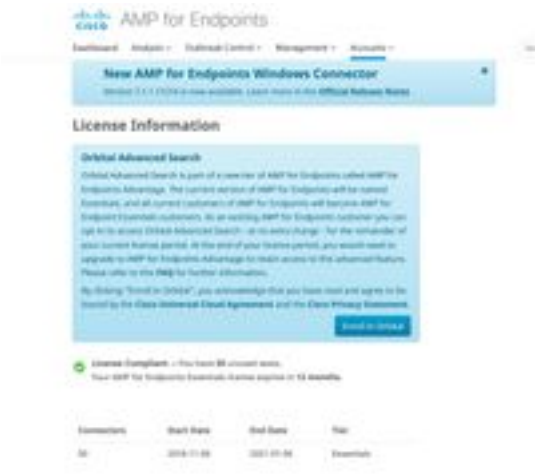
Este documento es una guía paso a paso para guiarle en cómo inscribirse en la nueva función y habilitarla en sus terminales. También se encuentra disponible una guía del usuario orbital completa. Los clientes de AMP para terminales pueden habilitar Orbital Advanced Search fácilmente si sus terminales ya tienen instalado un conector (7.1.5 o superior). Consulte el tema de Ayuda de AMP para terminales en Orbital para obtener la versión más actual del conector y otra información. La búsqueda avanzada orbital se admite actualmente en hosts de Windows 10 de 64 bits que ejecutan la versión 1703 (actualización de creadores) o posterior.

Una vez que haya completado estos pasos, consulte la guía Inicio rápido para obtener una

descripción más detallada de cómo empezar a utilizar la Búsqueda avanzada orbital.

Paso 1: Inicio de la búsqueda avanzada en orbital

Si no se ha inscrito previamente en la versión beta de Búsqueda avanzada orbital o ha optado por hacerlo explícitamente, puede hacerlo desde la página Información de licencia de la consola de AMP para terminales. Para participar en la búsqueda avanzada orbital, inicie sesión en la consola de AMP para terminales y seleccione el menú desplegable **Cuentas > Información de licencia**. En esta página puede hacer clic en **Inscribirse en orbital** para acceder a esta función.



NOTE: Debe ser un usuario con privilegios (admin) para participar en la búsqueda avanzada orbital.

Paso 2: Habilitar la búsqueda avanzada orbital en una política existente

Si los terminales ya tienen instalado un conector (versión 7.1.5 o superior), puede activar la búsqueda avanzada orbital en una política existente para los terminales.

- Vaya a la consola de AMP para terminales. En Management > Policies, seleccione la política en la que desea habilitar la Búsqueda avanzada orbital y haga clic en el botón **Edit** para abrir la **Editar política** en la **Configuración avanzada** seleccione **Orbital** y verifique que la Búsqueda avanzada orbital esté habilitada. Se debe marcar la casilla **Habilitar búsqueda avanzada orbital**. Si no es así, active la casilla para activarla.

En este momento, cualquier conector instalado con esta política activará automáticamente la búsqueda avanzada orbital en ese terminal.

Paso 3: Habilitar la búsqueda avanzada orbital en una nueva política y grupo de ordenadores (opcional)

Como se ha descrito anteriormente, una vez que haya habilitado la Búsqueda avanzada orbital en una política existente, todos los conectores que utilicen esa política tendrán activada la Búsqueda avanzada orbital y cualquier conector nuevo que instale, que utilice esa política, también tendrá activada la Búsqueda avanzada orbital. Por ejemplo, si tiene 1000 equipos en su grupo "Proteger", al activar la búsqueda avanzada orbital en esa política, se habilitará automáticamente la búsqueda avanzada orbital en esos terminales siempre y cuando se implemente la versión 7.1.5 o posterior del conector.

Crear nuevas políticas y grupos es opcional. Sin embargo, si desea utilizar la búsqueda avanzada orbital en un grupo específico de terminales mediante una nueva política y grupo, siga la documentación del producto para crear una nueva política o grupo y asegúrese de que la búsqueda avanzada orbital esté habilitada en la política como se muestra anteriormente.

Paso 4: Explore la consola orbital

Una vez que ha habilitado la Búsqueda avanzada orbital en una política con una versión de conector superior a 7.1.5 instalada en al menos un terminal, ahora puede ejecutar consultas en un terminal para recopilar información de él.

- Vaya a **Management > Computers** y busque un equipo con Orbital Advanced Search Expanda el panel y haga clic en **Orbital Query**. (También puede acceder a la consola orbital yendo a **Analysis > Orbital Advanced Search**).
- La consola orbital se carga en una nueva pestaña del navegador. Si es necesario, haga clic en **Iniciar sesión con Cisco Security** para realizar la autenticación mediante las credenciales existentes de la consola de AMP.

NOTE: También puede acceder directamente a Búsqueda avanzada orbital en https://orbital.amp.cisco.com

- El campo **Terminales** muestra los equipos que se consultarán. Puede introducir un GUID específico o **todo** en este campo para consultar todos los terminales de su organización que tengan activada la Búsqueda avanzada orbital. Si desea realizar un muestreo aleatorio de terminales, haga clic en los puntos suspensivos (...) para abrir el cuadro de diálogo **Agregar extremos aleatorios**.
- Puede introducir instrucciones SELECT personalizadas en el campo **SQL** o hacer clic en **Examinar catálogo de consultas** para abrir el **catálogo de consultas**, que contiene docenas de consultas que puede agregar a la consulta. **No es necesario saber cómo escribir una instrucción SELECT de SQL para utilizar Orbital.**

- Haga clic en **Consulta**. La consulta se ejecuta en los extremos especificados y los resultados se muestran en el panel derecho. Puede editar la consulta y volver a ejecutarla. Puede descargar los resultados. Puede guardar la consulta como un trabajo que se ejecutará de forma programada y que puede configurar.
- Para obtener más información sobre cómo empezar con la búsqueda avanzada orbital, consulte el Inicio rápido