Opt-In e Enable Orbital Advanced Search in your AMP for Endpoints Deployment (para clientes existentes a partir de 8 de janeiro de 2020)

Contents

A Cisco lançou recentemente dois pacotes para a AMP para endpoints: Essentials e Advantage. A Pesquisa avançada orbital é um recurso importante no pacote Advantage. Todos os clientes atuais a partir da data de lançamento (8 de janeiro de 2020) podem optar por usá-la gratuitamente durante o restante do período de vigência do contrato. Este FAQ tem mais informações sobre os pacotes e como eles afetam os clientes existentes a partir da data de lançamento.

A Pesquisa avançada orbital é um novo recurso avançado no Cisco AMP para endpoints projetado para simplificar a investigação de segurança e a busca de ameaças, fornecendo mais de cem consultas de catálogo. Isso permite executar consultas complexas rapidamente em qualquer ou em todos os endpoints. Isso também permite que você obtenha visibilidade mais profunda do que aconteceu em qualquer endpoint a qualquer momento, fazendo um snapshot do seu estado atual.

Com a Pesquisa avançada orbital, você pode realizar as seguintes tarefas importantes de forma melhor e mais rápida:

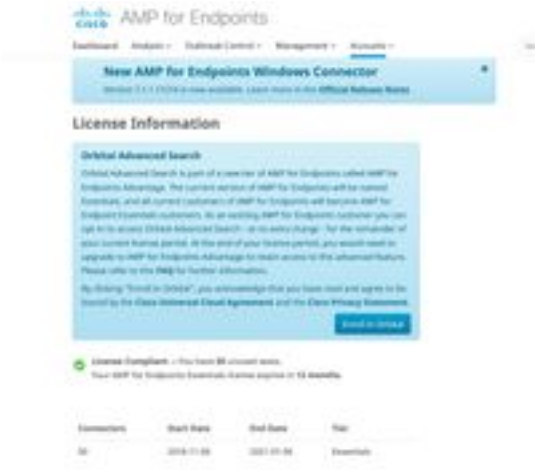
- **Caça a ameaças**. Procure artefatos mal-intencionados quase em tempo real para acelerar sua busca por ameaças.
- **Investigação de incidente**. Acelere a remediação para a raiz do incidente rapidamente.
- **Operações de TI**. Basta rastrear espaço em disco, memória e outros artefatos de operações de TI.
- **Vulnerabilidade e conformidade**. Verifique rapidamente o status dos sistemas operacionais em busca de versões e atualizações de patches, garantindo que seus endpoints estejam em conformidade com as políticas atuais.

Este documento é um guia passo a passo para mostrar como optar pelo novo recurso e ativá-lo em seus endpoints. Um Guia do Usuário Orbital completo também está disponível. Os clientes da AMP para endpoints podem habilitar a Pesquisa avançada orbital facilmente se os endpoints já tiverem um conector instalado (7.1.5 ou superior). Consulte o tópico da Ajuda do console da AMP para endpoints no Orbital para obter a versão mais recente do Connector e outras informações. A Pesquisa avançada orbital é atualmente suportada em hosts Windows 10 de 64 bits executando a versão 1703 (Atualização de criadores) ou posterior.

Depois de concluir estas etapas, consulte o guia Início rápido para obter uma descrição mais detalhada de como começar a usar a Pesquisa avançada orbital.

Passo 1: Optar pela pesquisa avançada orbital

Se você não se inscreveu anteriormente na versão beta da Pesquisa avançada orbital ou optou por participar explicitamente, você pode fazer isso na página Informações de licença no console da AMP para endpoints. Para optar pela Pesquisa avançada orbital, faça login no console da AMP para endpoints e selecione a lista suspensa **Contas > Informações de licença**. Nesta página, você pode clicar em **Inscrever-se em Orbital** para obter acesso a esse recurso.

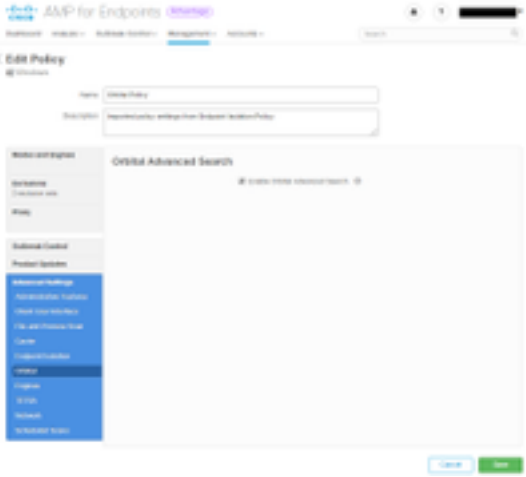


NOTE: Você deve ser um usuário privilegiado (admin) para participar da Pesquisa avançada orbital.

Passo 2: Habilitar pesquisa avançada orbital em uma política existente

Se seus endpoints já tiverem um conector instalado (versão 7.1.5 ou superior), você poderá simplesmente habilitar a Pesquisa avançada orbital em uma política existente para seus endpoints.

- Vá para o console do AMP for Endpoints. Em Gerenciamento > Políticas, selecione a política na qual deseja habilitar a Pesquisa avançada Orbital e clique no botão **Editar** para abrir a **Política de edição** em *Configurações avançadas* selecione **Orbital** e verifique se a Pesquisa avançada orbital está habilitada. A caixa **Enable Orbital Advanced Search** deve ser marcada. Caso contrário, marque a caixa para ativá-la.



Nesse ponto, todos os conectores instalados com essa política habilitarão automaticamente a Pesquisa avançada orbital nesse endpoint.

Passo 3: Habilitar pesquisa avançada orbital em uma nova política e grupo de computadores (opcional)

Como descrito acima, uma vez que a Pesquisa avançada orbital esteja habilitada em uma política existente, todos os conectores que usam essa política terão a Pesquisa avançada orbital ativada e todos os novos conectores instalados, que usam essa política, também terão a Pesquisa avançada orbital ativada. Por exemplo, se você tiver 1000 computadores no grupo "Proteger", simplesmente habilitar a Pesquisa avançada orbital nessa diretiva ativará automaticamente a Pesquisa avançada orbital nesses endpoints, desde que a versão do Connector 7.1.5 ou posterior seja implantada.

A criação de novas políticas e grupos é opcional. No entanto, se quiser usar a Pesquisa avançada orbital em um grupo específico de endpoints usando uma nova política e um novo grupo, siga a documentação do produto para criar uma nova política e/ou grupo e certifique-se de que a Pesquisa avançada orbital esteja habilitada na política, como mostrado acima.

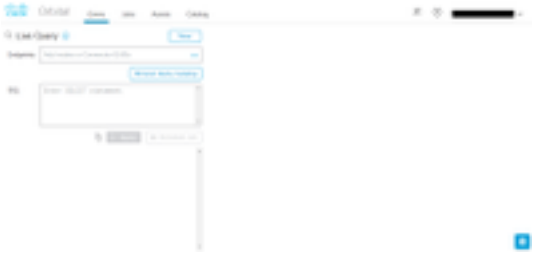
Passo 4: Explore o console orbital

Depois de habilitar a Pesquisa avançada orbital em uma política com uma versão do Connector superior a 7.1.5 instalada em pelo menos um endpoint, você poderá agora executar consultas em um endpoint para coletar informações dele.

- Vá para **Management > Computers** e localize um computador com Orbital Advanced Search Expanda o painel e clique em **Orbital Query**. (Você também pode acessar o console Orbital acessando **Analysis > Orbital Advanced Search**).
- O console Orbital é carregado em uma nova guia do navegador. Se necessário, clique em **Fazer login com o Cisco Security** para autenticar usando suas credenciais do console AMP existentes.

NOTE: Você também pode acessar a Pesquisa avançada orbital diretamente em https://orbital.amp.cisco.com

- O campo **Endpoints** mostra os computadores que serão consultados. Você pode digitar um GUID específico ou inserir **todos** neste campo para consultar cada endpoint na sua organização que tenha a Pesquisa avançada orbital habilitada. Se você quiser fazer uma amostragem aleatória de endpoints, clique nas elipses (...) para abrir a caixa de diálogo **Adicionar endpoints aleatórios**.
- Você pode inserir instruções SELECT personalizadas no campo **SQL** ou clicar em **Procurar Catálogo de Consultas** para abrir o **Catálogo de Consultas**, que contém dezenas de consultas que você pode adicionar à consulta. **Você não precisa saber como escrever uma instrução SQL SELECT para usar Orbital.**



- Clique em **Consulta**. A consulta é executada nos pontos finais especificados e os resultados

são exibidos no painel direito. Você pode editar a consulta e executá-la novamente. Você pode fazer o download dos resultados. Você pode salvar a consulta como um trabalho para ser executado em uma base agendada que você pode configurar.

- Para obter mais informações sobre como começar a pesquisa avançada orbital, explore o Início rápido