Opt-In et Enable Orbital Advanced Search dans votre déploiement AMP for Endpoints (pour les clients existants à partir du 8 janvier 2020)

Contenu

Cisco a récemment lancé deux packages pour AMP for Endpoints : Essentials and Advantage. Orbital Advanced Search est une fonctionnalité clé du package Advantage. Tous les clients existants à compter de la date de lancement (8 janvier 2020) peuvent choisir de l'utiliser gratuitement pour le reste de leur contrat. Cette FAQ contient plus d'informations sur les packages et sur leur impact sur les clients existants à la date de lancement.

La recherche avancée Orbital est une nouvelle fonctionnalité avancée de Cisco AMP for Endpoints conçue pour simplifier les enquêtes de sécurité et la recherche de menaces en fournissant plus d'une centaine de requêtes de catalogue. Cela vous permet d'exécuter rapidement des requêtes complexes sur n'importe quel ou tous les points de terminaison. Cela vous permet également d'avoir une meilleure visibilité sur ce qui s'est passé sur n'importe quel terminal à un moment donné en prenant un instantané de son état actuel.

Grâce à la fonction de recherche avancée Orbital, vous pouvez effectuer les tâches importantes suivantes de manière plus efficace et plus rapide :

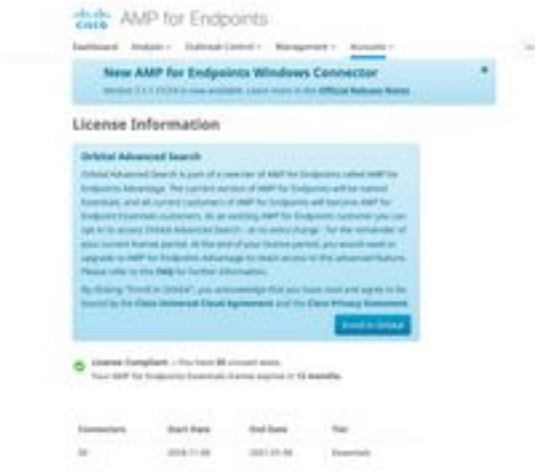
- **La chasse aux menaces**. Recherchez des artefacts malveillants en temps quasi réel pour accélérer votre recherche de menaces.
- **Enquête sur les incidents**. Accédez rapidement à la cause première de l'incident, en accélérant la résolution.
- **Opérations informatiques**. Il vous suffit de suivre l'espace disque, la mémoire et d'autres artefacts d'opérations informatiques.
- **Vulnérabilité et conformité**. Vérifiez rapidement l'état des systèmes d'exploitation pour des éléments tels que les versions et les mises à jour de correctifs, en vous assurant que vos terminaux sont conformes aux politiques actuelles.

Ce document est un guide détaillé qui vous explique comment vous inscrire à la nouvelle fonction et l'activer sur vos terminaux. Un Guide de l'utilisateur orbital complet est également disponible. Les clients d'AMP for Endpoints peuvent facilement activer la recherche avancée orbitale si vos terminaux ont déjà un connecteur installé (version 7.1.5 ou ultérieure). Reportez-vous à la rubrique d'aide de la console AMP for Endpoints sur Orbital pour obtenir la version la plus récente du connecteur et d'autres informations. La recherche avancée orbitale est actuellement prise en charge sur les hôtes Windows 10 64 bits exécutant la version 1703 (Creators Update) ou ultérieure.

Une fois ces étapes terminées, reportez-vous au guide Démarrage rapide pour obtenir une description plus détaillée de la façon de commencer à utiliser la recherche avancée Orbital.

Étape 1 : Recherche avancée Orbital

Si vous ne vous êtes pas encore inscrit à la version bêta de la recherche avancée orbitale ou que vous n'avez pas choisi explicitement, vous pouvez le faire à partir de la page Informations de licence de la console AMP for Endpoints. Pour vous inscrire à Oracle Advanced Search, connectez-vous à la console AMP for Endpoints et sélectionnez la liste déroulante **Accounts > License Information**. Sur cette page, vous pouvez cliquer sur **S'inscrire dans Orbital** pour accéder à cette fonctionnalité.

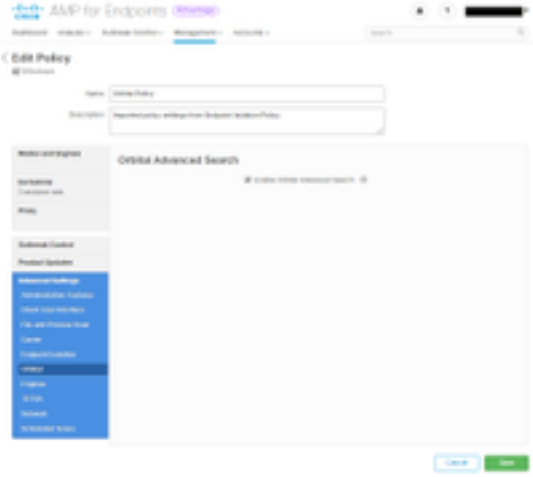


NOTE: Vous devez être un utilisateur privilégié (administrateur) pour pouvoir accéder à la recherche avancée Orbital.

Étape 2 : Activer la recherche avancée Oracle dans une stratégie existante

Si un connecteur est déjà installé sur vos terminaux (version 7.1.5 ou ultérieure), vous pouvez simplement activer la recherche avancée Orbital dans une stratégie existante pour vos terminaux.

- Accédez à la console AMP for Endpoints. Dans Management > Policies, sélectionnez la stratégie dans laquelle vous voulez activer la recherche avancée Orbital et cliquez sur le bouton **Edit** pour ouvrir la **stratégie Edit** Under *Advanced Settings* sélectionnez **Orbital** et vérifiez que la recherche avancée Orbital est activée. La case **Activer la recherche avancée orbitale** doit être cochée. Si ce n'est pas le cas, cochez cette case pour l'activer.



Àce stade, tous les connecteurs installés avec cette stratégie activeront automatiquement la recherche avancée Orbital sur ce point de terminaison.

Étape 3 : Activer la recherche avancée orbitale dans une nouvelle stratégie et un nouveau groupe d'ordinateurs (facultatif)

Comme décrit ci-dessus, une fois que vous avez activé Oracle Advanced Search dans une stratégie existante, tous les connecteurs qui utilisent cette stratégie auront activé Oracle Advanced Search et tous les nouveaux connecteurs que vous installez, qui utilisent cette stratégie, auront également activé Oracle Advanced Search. Par exemple, si vous avez 1000 ordinateurs dans votre groupe “ Protect ”, la simple activation de la recherche avancée Orbital dans cette stratégie active automatiquement la recherche avancée Orbital sur ces terminaux tant que Connector version 7.1.5 ou ultérieure est déployé.

La création de nouvelles stratégies et de nouveaux groupes est facultative. Cependant, si vous voulez utiliser la recherche avancée Orbital sur un groupe spécifique de terminaux à l'aide d'une nouvelle stratégie et d'un nouveau groupe, suivez simplement la documentation produit pour créer une nouvelle stratégie et/ou un nouveau groupe et assurez-vous que la recherche avancée Orbital est activée dans la stratégie comme indiqué ci-dessus.

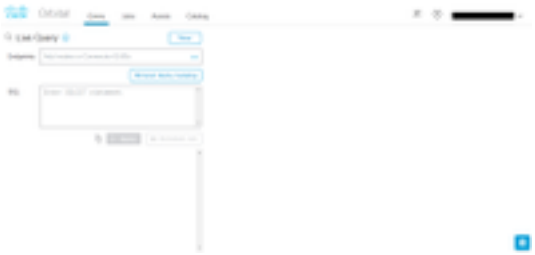
Étape 4 : Explorer la console orbitale

Une fois que vous avez activé Orbital Advanced Search dans une stratégie avec une version de connecteur supérieure à 7.1.5 installée sur au moins un point de terminaison, vous pouvez maintenant exécuter des requêtes sur un point de terminaison afin de recueillir des informations à partir de celui-ci.

- Accédez à **Management > Computers** et localisez un ordinateur avec Oracle Advanced Search. Développez le volet et cliquez sur **Orbital Query**. (Vous pouvez également accéder à la console Orbital en accédant à **Analyse > Recherche avancée Orbital**).
- La console Orbital est chargée dans un nouvel onglet de navigateur. Si nécessaire, cliquez sur **Se connecter avec Cisco Security** pour vous authentifier à l'aide de vos informations d'identification AMP Console existantes.

NOTE: Vous pouvez également accéder à la recherche avancée Orbital directement à l'adresse https://orbital.amp.cisco.com

- Le champ **Terminaux** affiche le ou les ordinateurs qui seront interrogés. Vous pouvez entrer un GUID spécifique ou **tout** entrer dans ce champ pour interroger chaque point de terminaison de votre organisation dont la recherche avancée Oracle est activée. Si vous souhaitez prélever un échantillon aléatoire de points de terminaison, cliquez sur les ellipses (...) pour ouvrir la boîte de dialogue **Ajouter des points de terminaison aléatoires**.
- Vous pouvez entrer des instructions SELECT personnalisées dans le champ **SQL**, ou cliquer sur **Parcourir le catalogue de requêtes** pour ouvrir le **catalogue de requêtes**, qui contient des dizaines de requêtes que vous pouvez ajouter à votre requête. **Vous n'avez pas besoin de savoir comment écrire une instruction SQL SELECT pour utiliser Orbital.**



- Cliquez sur **Requête**. La requête est exécutée sur les points de terminaison spécifiés et les résultats sont affichés dans le volet de droite. Vous pouvez modifier la requête et la réexécuter. Vous pouvez télécharger les résultats. Vous pouvez enregistrer la requête en tant que tâche à exécuter sur une base planifiée que vous pouvez configurer.
- Pour plus d'informations sur la recherche avancée Orbital, consultez le Guide de démarrage rapide