Guide des meilleures pratiques en matière d'offres groupées

Publié: 2024-11-03

Si vous créez un bundle qui pourrait être utile aux utilisateurs d'ExtraHop dans d'autres domaines de votre organisation, vous pouvez télécharger et partager ce bundle. Avant de partager, il est important d'inspecter chaque objet du bundle pour s'assurer que les noms et les descriptions sont informatifs et bien écrits, que les informations sensibles sont supprimées et que les dépendances de chaque objet sont incluses. Les mesures personnalisées, les détections personnalisées et les applications sont créées via des déclencheurs. Les tableaux de bord, les alertes et les requêtes d'enregistrement s'appuient souvent sur des mesures et des applications personnalisées.

Avant de commencer

- Vous devez avoir une écriture complète ou supérieure privilèges pour créer ou télécharger un bundle.
- Vous devez avoir une écriture personnelle ou supérieure privilèges pour télécharger et installer un bundle.

Avant de télécharger un bundle, nous vous recommandons de vérifier les paramètres de chacun des objets de votre bundle et d'appliquer les bonnes pratiques décrites dans chacune des sections suivantes.

- Alertes - supprimez les notifications d'alerte, notez les éventuelles dépendances entre les déclencheurs et assurez-vous que tous les champs de description sont informatifs.
- Demandes - notez toutes les dépendances entre les groupes déquipements et les alertes et assurez-vous que tous les champs de description sont informatifs.
- Tableaux de bord - notez toutes les dépendances des déclencheurs et assurez-vous que tous les champs de description sont informatifs.
- Détections personnalisées - prenez note de toutes les dépendances des déclencheurs.
- Groupes de périphériques dynamiques - supprimez tous les critères qui pourraient ne pas être pertinents dans d'autres environnements des groupes d'équipements dynamiques et assurez-vous que tous les champs de description sont informatifs.
- Requêtes d'enregistrement - notez toutes les dépendances entre les formats d'enregistrement et assurez-vous que tous les champs de description sont informatifs.
- Formats d'enregistrement - notez toutes les dépendances des déclencheurs et assurez-vous que tous les champs de description sont informatifs.
- éléments déclencheurs - assurez-vous que tous les objets dépendant du déclencheur sont définis et que les commentaires sont informatifs.

Inclure les alertes dans les bundles (accès au module NPM requis)

Les alertes sont souvent configurées avec des paramètres spécifiques à l'environnement. Par exemple, une alerte peut être configurée pour envoyer des notifications aux adresses e-mail de votre entreprise. Ces configurations doivent être supprimées des alertes avant de les inclure dans un bundle.

Vérifiez les paramètres d'alerte suivants avant d'inclure une alerte dans un bundle. Pour plus d'informations sur ces paramètres, voir Alertes.

Réglages	Remarques
Nom	Entrez un nom d'alerte descriptif et ne contenant pas d'informations sensibles.
Auteur	Entrez un auteur d'alerte adapté au grand public et ne contenant pas d'informations sensibles.

Réglages	Remarques
	Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, par exemple ExtraHop.
Métrique	Si l'alerte fait référence à une application ou à une métrique personnalisée, votre bundle doit également inclure le déclencheur qui crée l'application ou la métrique personnalisée.
Groupes de notifications par e-mail	Supprimez tous les groupes d'e-mails de ce champ. L'inclusion de groupes de notifications dans des ensembles peut entraîner l'envoi d'e-mails aux mauvais destinataires.
Adresses e-mail supplémentaires	Supprimez toutes les adresses e-mail de ce champ. L'inclusion d'adresses e-mail dans des offres groupées peut entraîner l'envoi d'e-mails aux mauvais destinataires.
Descriptif	Tapez une description de l'alerte qui fournit des informations utiles, telles que les conditions qui génèrent cette alerte, et qui ne contient aucune information sensible.
Missions	Décochez la case Attribuer à tous. Les offres groupées ne capturent pas les assignations aux adresses IP individuelles. Toutefois, si une alerte est attribuée à un groupe d'équipements, l'assignation sera capturée dans le bundle.

Inclure des applications dans des offres groupées

Les applications contiennent de multiples références à d'autres composants. Les ensembles qui incluent une application doivent également inclure tout groupe de dispositifs dynamiques personnalisés ou toute configuration d'alerte référencée par l'application.

Si vous ajoutez une application à un bundle, assurez-vous que l'application ainsi que tous les groupes d' équipements et alertes auxquels elle fait référence ne contiennent aucune information sensible, telle que des adresses IP internes ou des sous-réseaux. Vérifiez les paramètres d'application suivants avant d'inclure une application dans un bundle. Pour plus d'informations sur la modification de ces paramètres, voir Création d'une application.

Réglages	Remarques
Nom d'affichage	Entrez un nom d'application descriptif qui ne contient pas d'informations sensibles.
Identifiant de l'application	Entrez un identifiant unique et permanent adapté au grand public et ne contenant pas d'informations sensibles. Une fois l'application enregistrée, l'identifiant ne peut être ni modifié ni supprimé.
Site	Si vous créez une application sur un console, le site sélectionné n'est pas inclus lorsque vous ajoutez l'application à un bundle. Les identifiants de site sont spécifiques à votre environnement et sont

Réglages	Remarques
	automatiquement supprimés lorsqu'une application est exportée dans un bundle.
Les sources	Votre bundle doit inclure tous les groupes d'équipements dynamiques référencés par votre application. N'incluez pas les applications qui font référence à des appareils individuels.
Alertes	Si des alertes sont attribuées à une application, votre bundle doit également inclure l'alerte attribuée.

Inclure les tableaux de bord dans les bundles (accès au module NPM requis)

Les tableaux de bord constituent le moyen le plus simple d'afficher des ensembles de mesures. Toutefois, si un tableau de bord d'un bundle inclut des métriques personnalisées et des applications générées via un déclencheur, vous devez inclure ces déclencheurs dans le bundle.

Les tableaux de bord peuvent contenir des informations sensibles dans leurs métadonnées. Il est important de supprimer ces informations sensibles avant d'inclure le tableau de bord dans un bundle. Il est également conseillé de revoir votre tableau de bord pour vous assurer que chaque composant est bien étiqueté.

Vérifiez les paramètres du tableau de bord suivants avant de les inclure dans un bundle. Pour plus d'informations sur ces paramètres, voir Tableaux de bord.

Réglages	Remarques
Titre du tableau de bord	Entrez un titre de tableau de bord descriptif et ne contenant aucune information sensible.
Auteur du tableau de bord	Entrez un auteur de tableau de bord adapté au grand public et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, par exemple ExtraHop.
Description du tableau de bord	Tapez une description de tableau de bord qui fournit des informations utiles, telles que l'objectif du tableau de bord, et qui ne contient aucune information sensible.
Lien permanent du tableau de bord	Incluez des caractères aléatoires dans le permalien pour vous assurer que le permalien n' est pas déjà spécifié sur un autre système ExtraHop. Si un tableau de bord d'un bundle inclut un permalien déjà spécifié sur le système, un nouveau lien permanent sera attribué au tableau de bord du bundle lorsque le bundle sera appliqué, ce qui signifie que les liens vers ce tableau de bord depuis un autre tableau de bord ne fonctionneront pas.
Titre du widget	Tapez des titres de widgets descriptifs qui ne contiennent pas d'informations sensibles.
Sources et statistiques du widget	Si les sources ou les métriques du widget incluent des applications ou des métriques personnalisées, votre bundle doit également

Réglages	Remarques
	inclure le déclencheur qui crée ces applications ou métriques personnalisées.
Détails du widget	Supprimez toutes les configurations spécifiques à l'environnement et les informations sensibles des détails du widget. Par exemple, un widget peut être configuré pour afficher uniquement les résultats relatifs à un nom d'hôte donné.
Widgets de zone de texte	Tapez des descriptions dans des widgets de zone de texte bien rédigés et informatifs.

Inclure des détections personnalisées dans les offres groupées

Les ensembles qui incluent une détection personnalisée doivent inclure à la fois le déclencheur qui définit la détection personnalisée et le type de détection personnalisée. Assurez-vous que l'ID du type de détection personnalisé correspond à l'ID du type de détection dans la fonction CommitDetection du déclencheur.

Vérifiez les paramètres suivants avant d'inclure une détection personnalisée dans un bundle. Pour plus d'informations sur la modification de ces paramètres, voir Création d'une détection personnalisée.

Réglages	Remarques
Nom d'affichage	Entrez un nom d'affichage pour la détection personnalisée qui soit descriptif et ne contienne aucune information sensible.
ID du type de détection	Entrez la valeur d'ID du type de détection référencée dans la fonction CommitDetection du déclencheur de détection personnalisé.
Auteur	Tapez un auteur adapté au grand public et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, par exemple ExtraHop.
Technique MITRE	Sélectionnez une ou plusieurs techniques MITRE que vous souhaitez associer à la détection.

Inclure des groupes d'équipements dans les offres groupées

Les ensembles peuvent inclure des groupes d'équipements dynamiques, mais pas des groupes d'équipements statiques. Les groupes d'équipements statiques reposent sur des adresses IP statiques et il est peu probable qu'ils soient pertinents dans plusieurs environnements. Si vous incluez un groupe dynamique d'appareils dans votre bundle, assurez-vous qu'il ne contient aucune information sensible, telle que des adresses IP internes ou des sous-réseaux.

Note: Les assignations aux groupes d'équipements sont capturées dans un bundle ; toutefois, le groupe d'équipements doit également être inclus dans le bundle.

Vérifiez les paramètres de groupe d'appareils suivants avant d'inclure un groupe d'appareils dans un bundle. Pour plus d'informations sur ces paramètres, voir Création d'un groupe d'équipements dynamique.

Réglages	Remarques
Nom	Entrez un nom de groupe descriptif qui ne contient pas d'informations sensibles.

Réglages	Remarques
Auteur	Tapez un auteur adapté au grand public et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, par exemple ExtraHop.
Critères	Supprimez toutes les configurations spécifiques à l'environnement. Supprimez, par exemple, les références aux adresses IP internes ou aux sous-réseaux.

Inclure les requêtes d'enregistrement dans les bundles

Les requêtes d'enregistrement sont souvent configurées pour effectuer des recherches sur des ressources spécifiques à l'environnement, telles que des sous-réseaux ou des noms d'hôtes. Supprimez ces références internes avant de télécharger une requête d'enregistrement dans un bundle. Les requêtes d'enregistrement peuvent également faire référence à des types d'enregistrement définis dans des formats d'enregistrement personnalisés ; si une requête d'enregistrement dépend d'un format d'enregistrement personnalisé, le format d'enregistrement personnalisé doit être inclus dans le bundle.

Vérifiez les paramètres suivants avant d'inclure une requête d'enregistrement dans un bundle. Pour plus d'informations sur la modification de ces paramètres, voir Enregistrer les requêtes.

Réglages	Remarques
Type d'enregistrement	Si le type d'enregistrement est défini dans un format d'enregistrement personnalisé, votre bundle doit également inclure ce format d'enregistrement personnalisé.
Filtres	Supprimez les références aux ressources internes ou aux informations sensibles des filtres.
Nom	Entrez un nom descriptif qui ne contient pas d'informations sensibles.
Descriptif	Entrez une description de requête d'enregistrement qui fournit des informations utiles, telles que les informations capturées dans la requête, et qui ne contient aucune information sensible.

Inclure les formats d'enregistrement dans les bundles

Les formats d'enregistrement personnalisés définissent les types d'enregistrement qui peuvent être référencés dans les requêtes. Si vous incluez une requête d'enregistrement qui dépend d'un format d'enregistrement personnalisé, vous devez inclure le format d'enregistrement dans le bundle.

Si un format d'enregistrement personnalisé fait référence à un type d'enregistrement personnalisé, vous devez inclure le format d'enregistrement personnalisé et le déclencheur qui définit le type d'enregistrement personnalisé dans le bundle. Les formats d'enregistrement peuvent également contenir des informations sensibles dans leurs métadonnées.

Vérifiez les propriétés suivantes des paramètres Schema on Read d'un format d'enregistrement avant d'inclure le format d'enregistrement dans un bundle. Pour plus d'informations sur la modification de ces paramètres, voir Création d'un format dac.enregistrement personnalisé.

Propriété	Remarques
description	Tapez une description du format d'enregistrement qui fournit des informations utiles , telles que les informations affichées par le format, et qui ne contient pas d'informations sensibles.
nom	Entrez un nom descriptif qui ne contient pas d'informations sensibles.
nom_affichage	Entrez un nom d'affichage descriptif qui ne contient pas d'informations sensibles.
méta-types	Définissez le champ meta_types de manière appropriée pour éviter toute confusion. Par exemple, un horodateur ne sera pas formaté comme un horodateur sauf si le méta_type est spécifié.

Inclure les déclencheurs dans les offres groupées

Les déclencheurs sont souvent inclus dans les bundles pour créer des métriques et des applications personnalisées, qui sont souvent requises par d'autres objets du bundle tels que les tableaux de bord et les alertes. Après avoir identifié toutes les dépendances des autres objets du bundle, vous devez vous assurer d'inclure les déclencheurs associés pour prendre en charge ces objets.

Les déclencheurs peuvent être configurés pour agir sur des caractéristiques spécifiques à l'environnement ou pour révéler des informations sensibles dans les commentaires. Avant d'inclure un déclencheur dans un bundle, assurez-vous que ces configurations ont été supprimées.

Vérifiez les paramètres de déclencheur suivants avant d'inclure un déclencheur dans un bundle. Pour plus d'informations sur ces paramètres, voir éléments déclencheurs.

Réglages	Remarques
Nom	Entrez un nom descriptif qui ne contient pas d'informations sensibles.
Auteur	Entrez un auteur de déclencheur adapté au grand public et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, par exemple ExtraHop.
Descriptif	Entrez une description du déclencheur qui fournit des informations utiles, telles que les mesures créées par le déclencheur, et qui ne contient aucune information sensible.
Activer le journal de débogage	Décochez la case Activer le débogage. Assurez-vous qu'un déclencheur a été débogué avant de le partager avec d'autres personnes.
Script de déclenchement	• Définissez toutes les dépendances par rapport aux autres objets du bundle. • Supprimez toute référence à des ressources internes, telles que les noms d'hôtes ou les sous-réseaux, et supprimez les informations sensibles des commentaires.

Réglages	Remarques
	• Expliquez la fonctionnalité de chaque section du déclencheur dans les commentaires.
Options avancées	Désélectionnez le **Attribuer à tous les appareils** case à cocher. Les offres groupées ne capturent pas les assignations aux adresses IP individuelles. Toutefois, si un déclencheur est attribué à un groupe d'équipements, l'assignation sera capturée dans le bundle.