Guide des meilleures pratiques pour les offres groupées

Publié: 2023-09-19

Si vous créez une offre groupée qui pourrait être utile aux utilisateurs d'ExtraHop dans d'autres secteurs de votre organisation, vous pouvez la télécharger et la partager. Avant de partager, il est important d'inspecter chaque objet de l'ensemble pour s'assurer que les noms et les descriptions sont informatifs et bien rédigés, que les informations sensibles sont supprimées et que les dépendances de chaque objet sont incluses. Les déclencheurs permettent de créer des mesures, des détections et des applications personnalisées. Les tableaux de bord, les alertes et les requêtes d'enregistrement s'appuient souvent sur des mesures et des applications personnalisées.

Avant de télécharger une offre groupée, nous vous recommandons de revoir les paramètres de chacun des objets de votre offre groupée et d'appliquer les meilleures pratiques décrites dans chacune des sections suivantes.

- Alertes - supprimez les notifications d'alerte, notez les dépendances des déclencheurs et assurez-vous que tous les champs de description sont informatifs.
- Applications - notez toutes les dépendances des groupes d'appareils et des alertes et assurez-vous que tous les champs de description sont informatifs.
- Tableaux de bord - notez toutes les dépendances de déclenchement et assurez-vous que tous les champs de description sont informatifs.
- Détections personnalisées - notez toutes les dépendances de déclenchement.
- Groupes d'appareils dynamiques - supprimez des groupes d'appareils dynamiques tous les critères qui pourraient ne pas être pertinents dans d'autres environnements et assurez-vous que tous les champs de description sont informatifs.
- Requêtes d'enregistrement - notez toutes les dépendances de format 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.
- Déclencheurs - assurez-vous que tous les objets dépendant des déclencheurs sont définis et que les commentaires sont informatifs.

Inclusion d'alertes dans les offres groupées

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 électroniques de votre entreprise. Ces configurations doivent être supprimées des alertes avant d'inclure l'alerte dans une offre groupée.

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

Paramètres	Notes
Nom	Saisissez un nom d'alerte descriptif et ne contenant pas d'informations sensibles.
Auteur	Saisissez un auteur d'alerte approprié pour un public général et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise comme auteur, comme ExtraHop.
Métrique	Si l'alerte fait référence à une application ou à une mesure personnalisée, votre offre groupée

Paramètres	Notes
	doit également inclure le déclencheur qui crée l'application ou la mesure personnalisée.
Groupes de notification par courriel	Supprimez tous les groupes de messagerie de ce champ. L'inclusion de groupes de notification dans les offres groupées peut entraîner l'envoi d'e-mails aux mauvais destinataires.
Adresses électroniques supplémentaires	Supprimez toutes les adresses électroniques de ce champ. L'inclusion d'adresses électroniques dans les lots peut entraîner l'envoi de courriels aux mauvais destinataires.
Description	Saisissez une description de l'alerte qui fournit des informations utiles, telles que les conditions qui génèrent cette alerte, et qui ne contient pas d'informations sensibles.
Affectations	Les regroupements ne capturent pas les affectations à des adresses IP individuelles. Toutefois, si une alerte est attribuée à un groupe de périphériques, l'attribution sera capturée dans l'ensemble.

Inclure des applications dans des bundles

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

Si vous ajoutez une application à une offre groupée, assurez-vous que l'application et tous les groupes de dispositifs et alertes qu'elle référence ne contiennent pas d'informations sensibles, telles que des adresses IP internes ou des sous-réseaux. Vérifiez les paramètres d'application suivants avant d'inclure une application dans une offre groupée. Pour plus d'informations sur la modification de ces paramètres, voir Créer une application.

Paramètres	Notes
Nom d'affichage	Saisissez un nom d'application descriptif et ne contenant pas d'informations sensibles.
ID de l'application	Saisissez un identifiant unique et permanent, adapté à un public général 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 une console, le site sélectionné n'est pas inclus lorsque vous ajoutez l'application à une offre groupée. Les identifiants de site sont spécifiques à votre environnement et sont automatiquement supprimés lorsqu'une application est exportée dans un bundle.
Sources	Votre offre groupée doit inclure tous les groupes de dispositifs dynamiques référencés par votre

Paramètres	Notes
	application. N'incluez pas les applications qui font référence à des dispositifs individuels.
Alertes	Si des alertes sont attribuées à une application, votre offre groupée doit également inclure l'alerte attribuée.

Inclure des tableaux de bord dans les offres groupées

Les tableaux de bord sont le moyen le plus simple d'afficher des ensembles de mesures. Toutefois, si un tableau de bord d'une offre groupée comprend des métriques et des applications personnalisées générées par un déclencheur, vous devez inclure ce déclencheur dans l'offre groupée.

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 une liasse. Il est également conseillé de revoir votre tableau de bord pour vous assurer que chaque composant est bien étiqueté.

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

Paramètres	Notes
Titre du tableau de bord	Saisissez un titre de tableau de bord descriptif et ne contenant pas d'informations sensibles.
Auteur du tableau de bord	Saisissez un auteur de tableau de bord approprié pour un public général et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, comme ExtraHop.
Description du tableau de bord	Saisissez une description du tableau de bord qui fournit des informations utiles, telles que l'objectif du tableau de bord, et qui ne contient pas d'informations sensibles.
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'une offre groupée inclut un lien permalien déjà spécifié sur le système, le tableau de bord de l'offre groupée se verra attribuer un nouveau lien permalien lors de l'application de l'offre groupée, ce qui signifie que tout lien vers ce tableau de bord à partir d'un autre tableau de bord ne fonctionnera pas.
Titre du widget	Saisissez des titres de widgets qui sont descriptifs et ne contiennent pas d'informations sensibles.
Sources et mesures des widgets	Si les sources de widgets ou les mesures comprennent des applications ou des mesures personnalisées, votre offre groupée doit également inclure le déclencheur qui crée ces applications ou mesures personnalisées.

Paramètres	Notes
Détails du widget	Supprimez les configurations spécifiques à l'environnement et les informations sensibles des détails des widgets. Par exemple, un widget peut être configuré pour n'afficher que les résultats relatifs à un nom d'hôte donné.
Zones de texte	Tapez des descriptions bien écrites et informatives dans les zones de texte.

Inclusion de détections personnalisées dans les offres groupées

Les offres groupées qui incluent une détection personnalisée doivent inclure à la fois le déclencheur qui définit la détection personnalisée et le type de détection personnalisé. 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 une liasse. Pour plus d'informations sur la modification de ces paramètres, voir Créer une détection personnalisée.

Paramètres	Notes
Nom d'affichage	Saisissez un nom d'affichage pour la détection personnalisée qui soit descriptif et ne contienne pas d'informations sensibles.
ID du type de détection	Saisissez la valeur de l'ID du type de détection qui est référencée dans la fonction commitDetection du déclencheur de détection personnalisé.
Auteur	Saisissez un auteur approprié pour un public général et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise comme auteur, comme ExtraHop.
Technique MITRE	Sélectionnez une ou plusieurs techniques MITRE que vous souhaitez lier à la détection.

Inclusion de groupes de dispositifs dans les offres groupées

Les offres groupées peuvent inclure des groupes de dispositifs dynamiques, mais pas des groupes de dispositifs statiques. Les groupes de dispositifs statiques reposent sur des adresses IP statiques et il est peu probable qu'ils soient pertinents dans plusieurs environnements. Si vous incluez un groupe de dispositifs dynamiques dans votre offre, assurez-vous que le groupe de dispositifs ne contient pas d'informations sensibles, telles que des adresses IP internes ou des sous-réseaux.

Note: Les affectations aux groupes de dispositifs sont capturées dans une offre groupée ; cependant, le groupe de dispositifs doit également être inclus dans l'offre groupée.

Vérifiez les paramètres de groupe de dispositifs suivants avant d'inclure un groupe de dispositifs dans une offre groupée. Pour plus d'informations sur ces paramètres, voir Créer un groupe de dispositifs dynamique.

Paramètres	Notes
Nom	Saisissez un nom de groupe descriptif et ne contenant pas d'informations sensibles.

Paramètres	Notes
Auteur	Saisissez un auteur approprié pour un public général et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise comme auteur, tel que ExtraHop.
Critères	Supprimez toutes les configurations spécifiques à l'environnement. Par exemple, supprimez les références aux adresses IP internes ou aux sous-réseaux.

Inclure des requêtes d'enregistrement dans les bundles

Les requêtes d'enregistrement sont souvent configurées pour rechercher 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 une liasse. 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, ce dernier doit être inclus dans l'offre groupée.

Vérifiez les paramètres suivants avant d'inclure une requête d'enregistrement dans une liasse. Pour plus d'informations sur la modification de ces paramètres, voir Requêtes d'enregistrement.

Paramètres	Notes
Type d'enregistrement	Si le type d'enregistrement est défini dans un format d'enregistrement personnalisé, votre liasse doit également inclure ce format d'enregistrement personnalisé.
Filtres	Supprimez des filtres toute référence à des ressources internes ou à des informations sensibles.
Nom	Saisissez un nom descriptif ne contenant pas d'informations sensibles.
Description	Tapez une description de la requête d'enregistrement qui fournit des informations utiles, telles que les informations capturées dans la requête, et qui ne contient pas d'informations sensibles.

Inclure des formats d'enregistrement dans les liasses

Les formats d'enregistrement personnalisés définissent des 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 la liasse.

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 la liasse. 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 une liasse. Pour plus d'informations sur la modification de ces paramètres, voir Créer un format d'enregistrement personnalisé.

Propriété	Notes
description	Saisissez 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	Saisissez un nom descriptif qui ne contient pas d'informations sensibles.
nom_affichage	Saisissez un nom d'affichage descriptif et ne contenant pas d'informations sensibles.
meta_types	Définissez le champ meta_types de manière appropriée afin d'éviter toute confusion. Par exemple, un timestamp ne sera pas formaté comme un timestamp si le meta_type n'est pas spécifié.

Inclure des déclencheurs dans les offres groupées

Les déclencheurs sont souvent inclus dans les offres groupées pour créer des mesures et des applications personnalisées, qui sont souvent requises par d'autres objets de l'offre groupée tels que les tableaux de bord et les alertes. Après avoir identifié toutes les dépendances des autres objets de l'offre groupée, vous devez vous assurer d'inclure les déclencheurs correspondants 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 une liasse, assurez-vous que ces configurations ont été supprimées

.Vérifiez les paramètres de déclenchement suivants avant d'inclure un déclencheur dans une liasse. Pour plus d'informations sur ces paramètres, consultez Déclencheurs.

Paramètres	Notes
Nom	Saisissez un nom descriptif ne contenant pas d'informations sensibles.
Auteur	Saisissez un auteur de déclenchement approprié pour un public général et ne contenant pas d'informations sensibles. Par exemple, vous pouvez saisir le nom de votre entreprise en tant qu'auteur, comme ExtraHop.
Description	Tapez une description du déclencheur qui fournit des informations utiles, telles que les métriques créées par le déclencheur, et qui ne contient pas d'informations sensibles.
Activer le journal de débogage	Désactivez la case à cocher Activer le débogage . Assurez-vous qu'un déclencheur a été débogué avant de le partager avec d'autres personnes .
Script du déclencheur	• Définissez toutes les dépendances des autres objets de la liasse.

Paramètres	Notes
	• Supprimez toute référence à des ressources internes, telles que les noms d'hôte ou les sous-réseaux, et supprimez les informations sensibles des commentaires. • Expliquez la fonctionnalité de chaque section du déclencheur dans les commentaires.
Options avancées	Désélectionnez la case à cocher **Affecter à tous les périphériques** . Les bundles ne capturent pas les affectations à des adresses IP individuelles. Toutefois, si un déclencheur est affecté à un groupe de périphériques, l'affectation sera capturée dans l'ensemble.