Planifier un rapport de tableau de bord sur Active Directory

Publié: 2024-01-31

Active Directory est une application critique dont la surveillance et le dépannage peuvent prendre beaucoup de temps. Dans le pack ExtraHop pour Active Directory, nous avons compilé des tableaux de bord qui fournissent une vue complète de haut niveau des données Active Directory, ce qui permet de détecter facilement les problèmes potentiels.

Pour vous aider à surveiller facilement les modifications, vous pouvez planifier un rapport pour votre tableau de bord Active Directory. Un rapport de tableau de bord fournit un fichier PDF contenant les données du tableau de bord à tout destinataire d'e-mail que vous spécifiez.

Dans cette présentation, nous allons vous montrer comment télécharger et appliquer le bundle à votre système ExtraHop, et comment planifier un rapport de tableau de bord bihebdomadaire à l'intention de vos parties prenantes sur l'état de santé de votre environnement Active Directory.

Note: Vous ne pouvez planifier des rapports qu'à partir d'une console.

Prérequis

- Vous devez avoir accès à un console.
- Vous devez disposer d'un compte utilisateur auprès de privilèges d'écriture limités ou complets pour créer un tableau de bord

Récupérez le bundle ExtraHop Active Directory

Avant de pouvoir télécharger le bundle Active Directory sur votre système ExtraHop, vous devez récupérer le bundle depuis l'index des bundles de solutions ExtraHop.

1. Accédez au Page du bundle Active Directory.
2. Si vous n'êtes pas encore connecté au site Web ExtraHop, cliquez sur **S'identifier** dans le volet droit, puis spécifiez un nom d' utilisateur et un mot de passe valides.
3. Dans la section Comment obtenir ce bundle, cliquez sur le lien pour créer une demande de service afin de récupérer le bundle.

Téléchargez et appliquez le bundle Active Directory à votre système ExtraHop

Dans les étapes suivantes, vous téléchargerez et installerez le bundle que vous avez téléchargé depuis le site Web d'ExtraHop sur votre console.

1. Connectez-vous au console à travers `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur l'icône des paramètres système dans le coin supérieur droit.
3. Cliquez **Bundles**.
4. Sur le Bundles page, cliquez **Télécharger le bundle**.
5. Cliquez **Choisissez un fichier**, puis sélectionnez le fichier Active Directory .json que vous avez téléchargé dans la section précédente.
6. Dans la section Options d'installation, cochez les cases suivantes :
   a) Sélectionnez le site sur lequel vous souhaitez installer le bundle.
   b) Sélectionnez le **Appliquer les 9 devoirs inclus** case à cocher.

Cette option attribue le bundle aux sources métriques incluses dans le bundle. Dans la plupart des cas, il est préférable d'appliquer les assignations par défaut.

c) Sélectionnez le **Remplacer le contenu existant** case à cocher.

Cette option remplace tous les objets portant le même nom que les objets du bundle. Si vous souhaitez conserver des objets système existants portant le même nom , vous devez renommer ces objets pour éviter de les remplacer par les objets du bundle.

7. Cliquez **Installer**, puis cliquez sur **Terminé**. Votre bundle est installé et répertorié dans le tableau !

Configuration des déclencheurs Active Directory

Au cours des étapes suivantes, vous allez activer et configurer un déclencheur pour refléter les paramètres de verrouillage et de compte privilégié dans votre environnement Active Directory.

1. Cliquez sur l'icône des paramètres système .
2. Cliquez **DÉCLENCHEURS**.
3. Activez chaque déclencheur du bundle Active Directory v4 en effectuant les étapes suivantes.
   a) Dans le tableau, cliquez sur le nom d'un déclencheur commençant par **ANNONCE**.
   b) Effacez le **Désactiver le déclencheur** case à cocher pour activer le déclencheur.
   c) Cliquez **Enregistrer et fermer**.
4. Modifiez des champs spécifiques dans le déclencheur Kerberos pour qu'ils correspondent à vos comptes Active Directory en effectuant les étapes suivantes.
   a) Dans le tableau, cliquez sur **AD : Kerberos** puis cliquez sur **Rédacteur** onglet.
   b) Réglez le `failedLoginDisableInterval` constante pour correspondre à la valeur du `Reset account lockout counter after` définition des politiques dans votre environnement Active Directory.
   c) Réglez le `accountLockoutDuration` constante à la valeur de `Account lockout duration` définition des politiques dans votre environnement Active Directory.
   d) Ajoutez les noms complets de tous les comptes privilégiés de votre environnement dans le `priv_names` liste et toute correspondance partielle avec `priv_regex` liste. Voici des exemples de comptes privilégiés :

```
var priv_names = {'admin', 'administrator', 'root', 'ss', 'sys',
        'sysadmin, 'informix'}
```

   e) Cliquez **Enregistrer et fermer**.

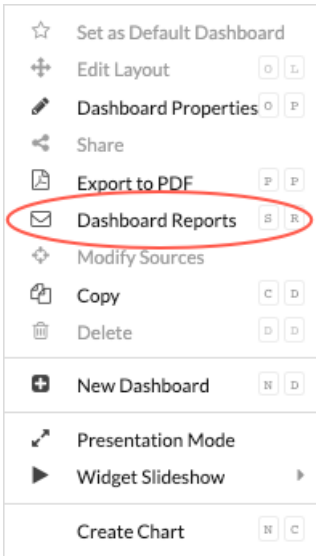
Création, planification et enregistrement d'un rapport de tableau de bord

Dans les étapes suivantes, nous allons vous montrer comment planifier un rapport de tableau de bord hebdomadaire qui sera diffusé les lundis et jeudis à 7h00. Nous vous montrerons également comment envoyer le rapport du tableau de bord à un collègue, par exemple à une personne qui gère les services d'authentification de votre entreprise.

1. Cliquez **Tableaux de bord** en haut de la page, puis cliquez sur **Présentation d'Active Directory** tableau de bord dans le volet gauche.

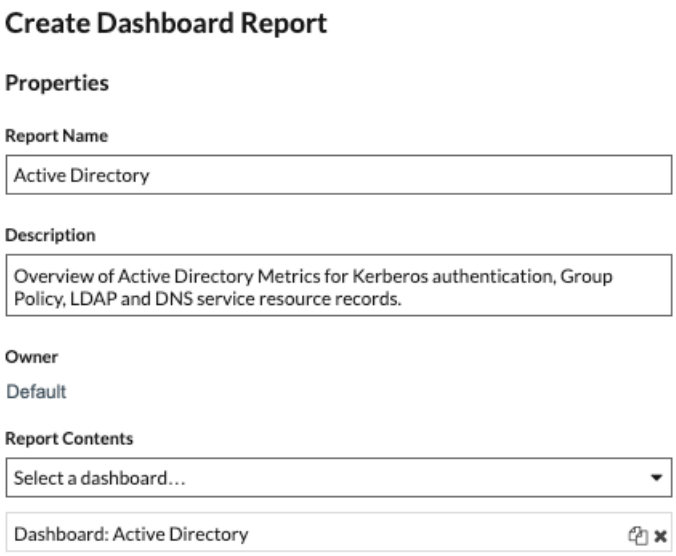
   Note: Chaque rapport ne peut être lié qu'à un seul tableau de bord. Vous pouvez sélectionner n'importe quel tableau de bord dont vous êtes propriétaire ou qui a été partagé avec vous pour créer un rapport.

2. Dans le coin supérieur droit de la page du tableau de bord, cliquez sur le menu de commandes , puis sélectionnez **Rapports du tableau de bord**.



UN Rapports du tableau de bord une page affiche tous les rapports stockés sur la console. S'il s'agit de votre premier rapport, cette page sera vide.

3. Dans le coin supérieur droit, cliquez sur **Créez**.
4. Dans le champ Nom du rapport, le nom du tableau de bord est affiché. Supprimons les informations relatives à l'hôte du site connecté du titre, comme illustré dans la figure suivante.

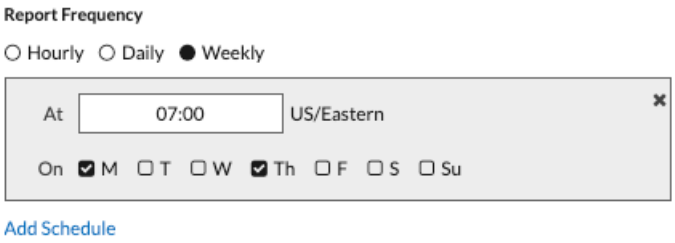


5. Passons au bas de la page pour définir le calendrier des rapports du tableau de bord. Dans la section Intervalle de temps, sélectionnez la période des données du tableau de bord que vous souhaitez afficher dans le fichier PDF du rapport. Pour cette présentation pas à pas, examinons les données des 4 derniers jours. Cliquez sur le **Dernier** champ, puis tapez 4.

Note: Pour plus d'informations sur la configuration de chaque champ, voir Création d'un rapport de tableau de bord planifié.

6. Dans la section Fréquence des rapports, définissez le calendrier de livraison des e-mails. Pour cette présentation, nous vous enverrons un rapport hebdomadaire deux jours différents à 7 h 00. Effectuez les étapes suivantes :
   a) Cliquez sur le **À** liste déroulante et sélectionnez **07h00**. Ce paramètre planifie la livraison du rapport à 7 h 00.

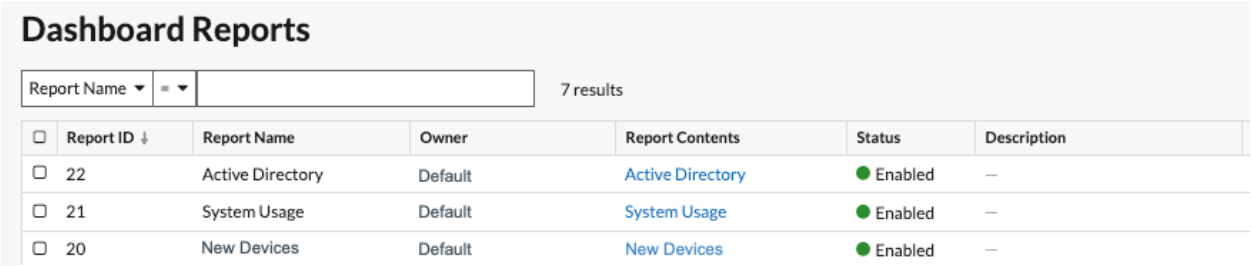
      L'heure système définie pour votre console détermine le fuseau horaire affiché lors de la configuration de votre rapport. Pour plus d'informations sur la configuration du fuseau horaire de votre système ExtraHop via les paramètres d'administration ExtraHop, voir Configurer l'heure du système.
   b) Cochez les cases à côté de M et Th pour planifier la livraison du rapport le lundi et le jeudi.



7. Pour ajouter l'adresse e-mail de votre collègue, faites défiler la page vers le bas jusqu'à la section Envoyer à. Cliquez sur le champ Adresses e-mail et saisissez l'e-mail.

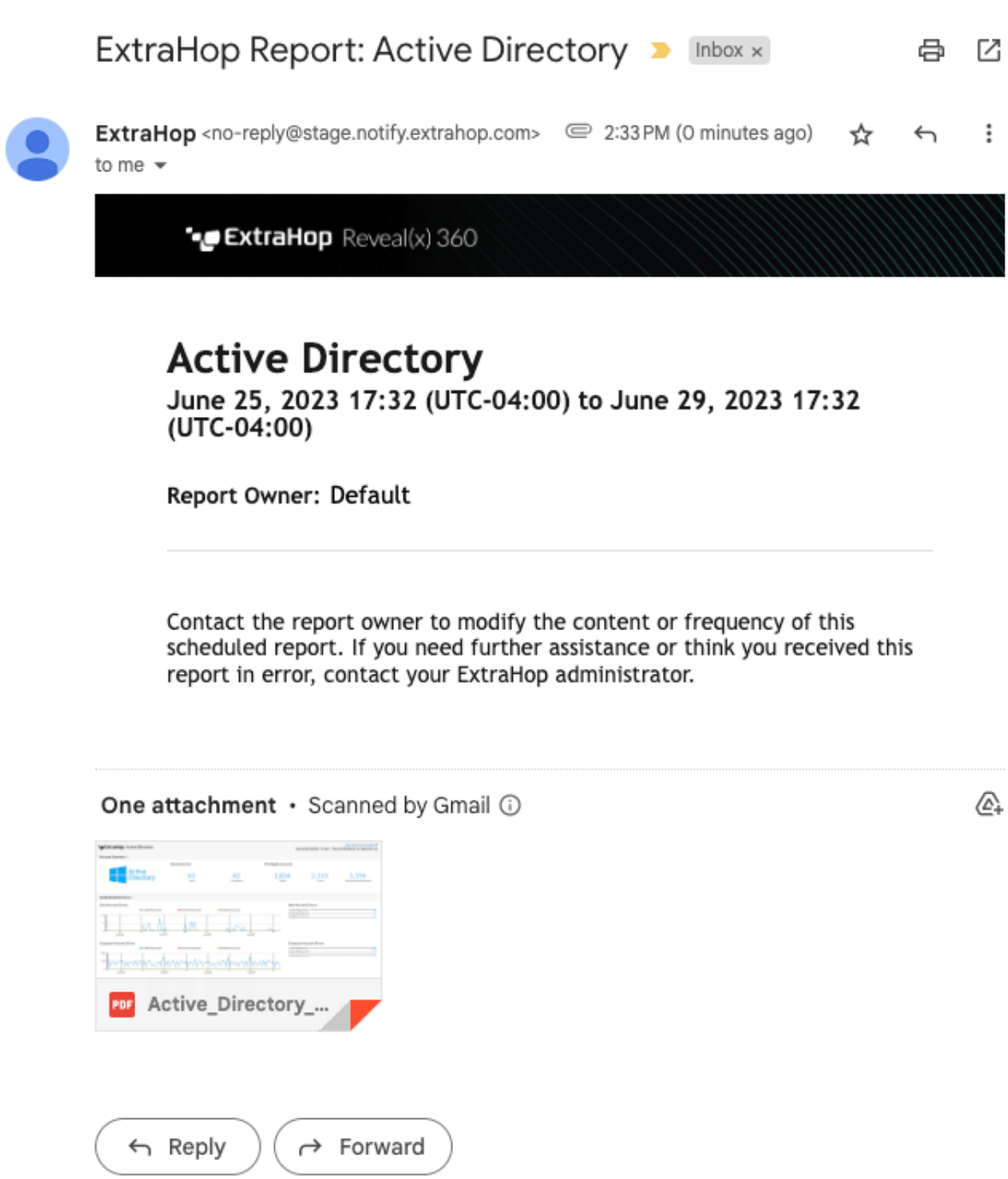
Note: Le système ExtraHop ne stocke pas les adresses e-mail des comptes utilisateurs ExtraHop. Toutefois, si votre système ExtraHop Reveal (x) Enterprise est configuré avec un groupe de messagerie, vous pouvez sélectionner un groupe de notifications à envoyer par e-mail. Reveal (x) 360 ne prend pas en charge les groupes de notifications par e-mail.

8. Optionnel : Cliquez **Envoyer maintenant** pour envoyer un e-mail de test au destinataire.
9. Cliquez **Terminé**. Le rapport de votre tableau de bord apparaît désormais sur la page Rapports du tableau de bord, comme le montre la figure suivante.



10. Dans le coin inférieur droit de la page, cliquez sur **Terminé** une nouvelle fois pour revenir à votre tableau de bord.

Votre collègue recevra un e-mail similaire à l'exemple ci-dessous avec le fichier de rapport PDF en pièce jointe.



Note: Dans le coin supérieur droit du fichier PDF, cliquez sur **Voir le rapport sur ExtraHop** lien pour accéder au tableau de bord qui a généré le rapport. Pour les utilisateurs d'ExtraHop, le lien ouvre la console et définit le tableau de bord selon l' intervalle de temps indiqué dans le rapport. Vous pouvez désormais étudier les indicateurs plus en détail à partir du tableau de bord.

Ajouter une autre adresse e-mail à un rapport enregistré

Si vous souhaitez apporter des modifications à un rapport de tableau de bord, vous pouvez y accéder à tout moment. Ajoutons l'adresse e-mail d'une nouvelle partie prenante à notre rapport Active Directory.

1. Sur la page du tableau de bord, cliquez sur le menu de commandes dans le coin supérieur droit, puis sélectionnez **Rapports du tableau de bord**.
2. Dans le **Nom du rapport** dans ce champ, cliquez sur le titre de votre rapport.
3. Faites défiler la page vers le Envoyer un e-mail section.
4. Cliquez sur le champ Adresses e-mail.
5. Tapez une virgule après la première adresse e-mail, puis saisissez la nouvelle adresse e-mail.

6. Cliquez **Enregistrer**.
7. Cliquez **Terminé** pour revenir à votre tableau de bord. Le rapport prévu pour cette procédure pas à pas est désormais mis à jour.

Prochaines étapes
Au fil du temps, vous souhaiterez peut-être suspendre la livraison du rapport en désactivation d'un rapport de tableau de bord. Vous pouvez également apporter des modifications à votre tableau de bord pour afficher différents graphiques ou données. Pour plus d' informations sur la modification d'un tableau de bord, consultez les ressources suivantes :

- Modifier la mise en page d'un tableau de bord
- Utilisation de tableaux de bord pour organiser et présenter les données (Formation en ligne)
- Modifier un graphique de tableau de bord avec l'explorateur de métriques
- Modifier un widget de zone de texte

Voici des instructions supplémentaires sur la création de tableaux de bord à partir de zéro pour surveiller les métriques du protocole :

- Surveillez les performances du site Web dans un tableau de bord (Procédure pas à pas)
- Surveiller l'état de la base de données dans un tableau de bord (Procédure pas à pas)
- Surveiller les erreurs DNS dans un tableau de bord (Procédure pas à pas)