Guide de configuration et d'administration de Reveal (x) 360

Publié: 2024-02-13

Après avoir reçu votre premier e-mail d'ExtraHop Networks, vous devez effectuer quelques procédures avant de pouvoir commencer à analyser votre trafic. Ce guide fournit des procédures pour la configuration et l'administration de base du système Reveal (x) 360.

Activez votre compte administrateur

Le privilège d'administration du système et des accès est accordé à l'adresse e-mail que vous avez fournie lors de votre inscription.

1. Ouvrez votre e-mail Welcome to ExtraHop Reveal (x) 360.
2. Cliquez sur le lien URL de votre environnement Reveal (x) 360.
3. Sur la page de connexion, entrez votre adresse e-mail et le mot de passe temporaire inclus dans l'e-mail.
4. Cliquez **Connectez-vous**.
5. Sur l'écran Modifier le mot de passe, entrez un nouveau mot de passe dans les deux champs de mot de passe , puis cliquez sur **Envoyer**.
6. Sur la page de configuration de l'authentification multifactorielle, scannez le code QR ou saisissez manuellement le code qui apparaît dans votre application d'authentification.
7. Entrez le code fourni par votre application d'authentification dans **Code** champ, puis cliquez sur **Configuration complète**.
8. Sur la page Réussite, cliquez sur **Poursuivre**.

Configurez vos règles de pare-feu

Si votre système ExtraHop est déployé dans un environnement doté d'un pare-feu, vous devez ouvrir l' accès aux services cloud ExtraHop. Pour les systèmes Reveal (x) 360 connectés à des systèmes autogérés capteurs, vous devez également ouvrir l'accès à l'ExtraHop Cloud Recordstore.

Accès ouvert aux services cloud

Pour accéder aux services cloud ExtraHop, votre capteurs doit être capable de résoudre les requêtes DNS pour*.extrahop.com et d'accéder au protocole TCP 443 (HTTPS) à partir de l'adresse IP correspondant à votre sonde licence :

- 35.161.154.247 (Portland, États-Unis)
- 54.66.242,25 (Sydney, Australie)
- 52.59.110.168 (Francfort, Allemagne)

Accès ouvert au Cloud Recordstore

Pour accéder à l'ExtraHop Cloud Recordstore, votre capteurs doit être en mesure d' accéder au protocole TCP 443 (HTTPS) sortant à ces noms de domaine complets :

- `bigquery.googleapis.com`
- `bigquerystorage.googleapis.com`
- `oauth2.googleapis.com`
- `www.googleapis.com`

- `www.mtls.googleapis.com`
- `iamcredentials.googleapis.com`

Vous pouvez également consulter les conseils publics de Google à propos de calcul des plages d'adresses IP possibles pour googleapis.com.

Outre la configuration de l'accès à ces domaines, vous devez également configurer le paramètres globaux du serveur proxy.

Ajouter et gérer des utilisateurs

1. Sur la page d'aperçu de Reveal (x) 360, cliquez sur **Réglages du système** puis cliquez sur **Toute l'administration**.
2. Cliquez **Accès utilisateur**.
3. Dans la section Utilisateurs, cliquez sur **Afficher les utilisateurs**.
4. Cliquez **Créez**.
5. Entrez l'adresse e-mail, le prénom et le nom de famille du nouvel utilisateur.
6. Dans la section Accès au système, sélectionnez l'un des privilèges suivants.

Privilège	Description
Administration du système et des accès	Créez et modifiez tous les objets et paramètres, y compris les pages d'administration, dans Reveal (x) 360.
Administration du système	Créez et modifiez des objets et des paramètres, à l'exception de l'accès utilisateur et de l'accès API sur la page d'administration.
Écriture complète	Créez et modifiez tous les objets et paramètres, à l'exception des pages d'administration.
Écriture limitée	Créez, modifiez et partagez des tableaux de bord. Créez et modifiez des règles de réglage. Créez et modifiez les règles de détection et de notification des informations sur les menaces.
Rédaction personnelle	Créez des tableaux de bord personnels et modifiez les tableaux de bord partagés avec l'utilisateur connecté.
Lecture seule complète	Afficher les objets dans le système ExtraHop.
Lecture seule restreinte	Afficher les tableaux de bord partagés avec cet utilisateur.

7. Dans la section Accès au module NDR, sélectionnez l'un des privilèges suivants.

Privilège	Description
Accès complet	Accès aux détections du réseau.
Pas d'accès	Aucun accès aux détections du réseau.

8. Dans la section Accès au module NPM, sélectionnez l'un des privilèges suivants.

Privilège	Description
Accès complet	Accès aux détections de performance.
Pas d'accès	Aucun accès aux détections de performances.

9. Dans le **Accès aux paquets et aux clés de session** section, sélectionnez l'un des privilèges suivants :

Privilège	Description
Paquets et clés de session	Recherchez et téléchargez les paquets et les clés de session associées.
Paquets uniquement	Recherchez et téléchargez des paquets.
Tranches de paquets uniquement	Recherchez et téléchargez les 64 premiers octets d'un paquet.
Pas d'accès	Aucun accès aux paquets.

10. Cliquez **Enregistrer**.
    L'utilisateur reçoit un e-mail contenant l'URL de l' environnement Reveal (x) 360 et son mot de passe temporaire. Le mot de passe temporaire expire dans 7 jours.
11. Cliquez **Terminé**.

Modifier les paramètres utilisateur

Vous pouvez modifier les niveaux de privilèges attribués, réinitialiser la configuration de l'authentification multifacteur ou supprimer l'utilisateur.

Modifier les privilèges des utilisateurs

1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Dans le volet de gauche, sélectionnez le nouveau niveau de privilège pour l'utilisateur, puis cliquez sur **Enregistrer**.

Réinitialisation de l'authentification multifacteur

1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Effacez le **Réinitialiser la configuration MFA pour cet utilisateur** .
   L'utilisateur doit configurer l'authentification multifacteur lors de sa prochaine connexion à Reveal (x) 360.

Supprimer un utilisateur

1. Dans la section Utilisateurs, cliquez sur le nom de l'utilisateur que vous souhaitez modifier.
2. Cliquez **Supprimer**.
3. Sélectionnez l'une des options suivantes :
   - **Transférez des tableaux de bord, des collections et des cartes d'activités appartenant à *<username>* à l' utilisateur suivant :** puis sélectionnez un nouvel utilisateur dans la liste déroulante.
   - **Supprimer tous les tableaux de bord, collections et cartes d'activité appartenant à *<username>***
4. Cliquez **Supprimer**.

Gérez les politiques mondiales

Les administrateurs peuvent configurer des politiques globales qui s'appliquent à tous les utilisateurs qui accèdent au système.

1. Sur la page Vue d'ensemble, cliquez sur **Réglages du système**, puis cliquez sur **Accès utilisateur**.
2. Dans la section Politiques globales, spécifiez une ou plusieurs des options suivantes.

Option	Description
Contrôle de modification des groupes d'appareils	Sélectionnez cette option pour contrôler si tous les utilisateurs disposant de droits d'écriture limités peuvent créer et modifier des groupes d'équipements. Lorsque cette règle est sélectionnée, tous les utilisateurs à écriture limitée peuvent créer des groupes

Option	Description
	d'équipements et ajouter d'autres utilisateurs à écriture limitée en tant qu'éditeurs à leurs groupes d'équipements.
Tableau de bord par défaut	Spécifiez le tableau de bord que les utilisateurs voient lorsqu'ils se connectent au système. Seuls les tableaux de bord partagés avec tous les utilisateurs peuvent être définis par défaut global. Les utilisateurs peuvent annuler ce paramètre par défaut depuis le menu de commandes de n'importe quel tableau de bord.

3. Cliquez **Enregistrer les modifications**.

Configuration d'une liste d'autorisations

Configurez une liste d'adresses IPv4 et de blocs CIDR autorisés à accéder à Reveal (x) 360.

1. Sur la page Vue d'ensemble, cliquez sur Paramètres système, puis sur **Accès utilisateur**.
2. Dans la section Liste d'autorisations, cliquez sur **Activer la liste d'autorisations**.
3. Tapez une liste séparée par des virgules des adresses IPv4 ou des blocs CIDR autorisés à accéder au système. Les adresses IPv6 ne sont pas prises en charge.
4. Cliquez **Enregistrer**. L'activation de la liste d'autorisation peut prendre plusieurs minutes.

Configurer l'heure du système

La page Heure du système affiche les paramètres d'heure système par défaut et le temps d'affichage par défaut configurés pour votre système ExtraHop.

Voici quelques considérations relatives aux paramètres d'heure du système dans Reveal (x) 360 :

- Vous devez disposer de privilèges d'administrateur système ou d'une version supérieure pour apporter des modifications.
- L'heure système par défaut est un fuseau horaire global appliqué à votre système ExtraHop.
- L'heure d'affichage par défaut pour les utilisateurs est le fuseau horaire que tous les utilisateurs voient dans le système ExtraHop, sauf si un utilisateur modifie manuellement son fuseau horaire affiché.

1. Sur la page Vue d'ensemble, cliquez sur **Réglages du système** puis cliquez sur **Heure du système**.
2. À partir du Heure système par défaut liste déroulante, sélectionnez le fuseau horaire souhaité.
3. À partir du Durée d'affichage par défaut pour les utilisateurs section, sélectionnez l'une des options suivantes :
   - Heure du navigateur
   - Heure du système
   - UTC
4. Cliquez **Enregistrer les modifications**.

Priorité du nom de l'appareil

Les appareils découverts sont automatiquement nommés en fonction de plusieurs sources de données réseau. Lorsque plusieurs noms sont trouvés pour un équipement, un ordre de priorité par défaut est appliqué. Vous pouvez modifier l'ordre de priorité.

1. Cliquez sur l'icône des paramètres système puis cliquez sur **Toute l'administration**.

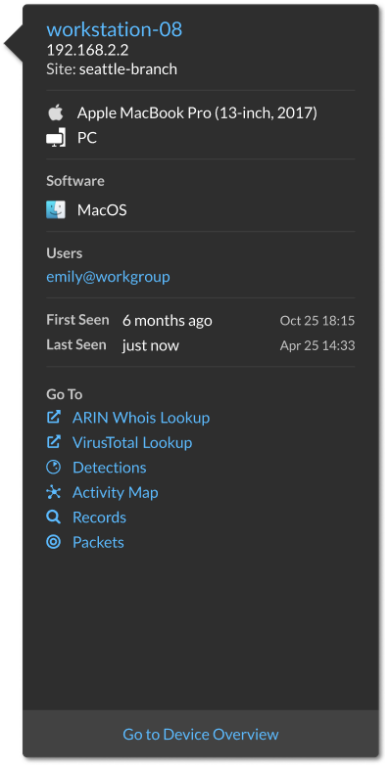
2. Dans la section Paramètres de la console, cliquez sur **Priorité du nom de l'appareil**.
3. Cliquez sur les noms des équipements et faites-les glisser pour créer un nouvel ordre de priorité.
4. Cliquez **Enregistrer**.
   Cliquez **Revenir à la valeur par défaut** pour annuler vos modifications.

Configurer les liens de recherche des points de terminaison

La recherche de point de terminaison vous permet de spécifier des outils d' adresse IP externes disponibles pour récupérer des informations sur les points de terminaison au sein du système ExtraHop. Par exemple, lorsque vous cliquez ou placez le pointeur sur une adresse IP, les liens des outils de recherche s' affichent afin que vous puissiez facilement trouver des informations sur ce point de terminaison.

Les liens de recherche suivants sont configurés par défaut et peuvent être modifiés ou supprimés :

- Recherche Whois ARIN
- Recherche VirusTotal



1. Connectez-vous à la page d'administration de Reveal (x) 360.
2. Sur la page Vue d'ensemble, cliquez sur **Réglages du système** puis cliquez sur **Toute l'administration**.
3. Dans la section Paramètres de la console, cliquez sur **Recherche d'un terminal**.
4. Dans le **Modèle d'URL** dans ce champ, saisissez l'URL de l' outil de recherche.

   L'URL doit inclure `$ip` variable, qui est remplacée par l'adresse IP du point de terminaison lors de la recherche. Par exemple, `https://search.arin.net/rdap/?query=$ip`
5. Dans le **Nom d'affichage** dans ce champ, tapez le lien du nom tel que vous souhaitez qu'il apparaisse.
6. Sélectionnez l'une des options suivantes Options d'affichage:
   - Afficher ce lien sur tous les terminaux
   - Afficher ce lien sur les points de terminaison externes
   - Afficher ce lien sur les points de terminaison internes

- Ne pas afficher ce lien

7. Cliquez **Enregistrer**.

Connecter les capteurs

Ajouter capteurs à Reveal (x) 360 pour surveiller le trafic de votre réseau.

Reveal (x) géré par ExtraHop capteurs pour AWS peut être sélectionné et déployé depuis la console Reveal (x) 360.

- Déployez les capteurs Reveal (x) 360 pour AWS

Autogéré capteurs et les packetstores peuvent également être connectés depuis la console Reveal (x) 360. Notez que si vous possédez déjà une console, vous devez la déconnecter avant de connecter votre console autogérée capteurs vers Reveal (x) 360.

- Connectez-vous à Reveal (x) 360 à partir de capteurs autogérés

Authentification multifactorielle

L'authentification multifactorielle (MFA) est une amélioration de la sécurité qui vous oblige à fournir deux types d'informations d'identification lorsque vous vous connectez à votre compte. En plus de vos informations d'identification ExtraHop, vous devez fournir des informations d'identification provenant d'une application d'authentification tierce.

Sélectionnez et téléchargez une application d'authentification sur votre équipement et générez des codes sécurisés à six chiffres lorsque vous vous connectez à votre système Reveal (x) 360.

Il existe de nombreuses applications d'authentification parmi lesquelles choisir. Les étapes suivantes sont des directives générales, mais vous devez également consulter la documentation d'aide de l'application que vous sélectionnez.

1. Choisissez un équipement, tel qu'un ordinateur ou un équipement mobile (téléphone ou tablette), sur lequel vous pouvez installer des applications.
2. Téléchargez et installez une application d'authentification sur l'équipement. Voici quelques options populaires :
   - Android et iOS : Google Authenticator, Authy
   - Windows et macOS : 1Password, OTP Manager
   - Extensions Chrome : Authenticator
3. Ouvrez un nouveau navigateur et connectez-vous à votre système ExtraHop Reveal (x) 360.
4. Suivez les instructions pour scanner ou entrez le code qui apparaît sur l'écran de configuration de l'authentification multifactorielle ExtraHop, puis entrez les informations d'identification fournies par votre application d'authentification.

Améliorez les capteurs connectés dans Reveal (x) 360

Les administrateurs peuvent mettre à niveau capteurs connectés à Reveal (x) 360.

Avant de commencer

- Votre compte utilisateur doit disposer de privilèges sur Reveal (x) 360 pour l' administration du système et des accès ou pour l'administration du système.

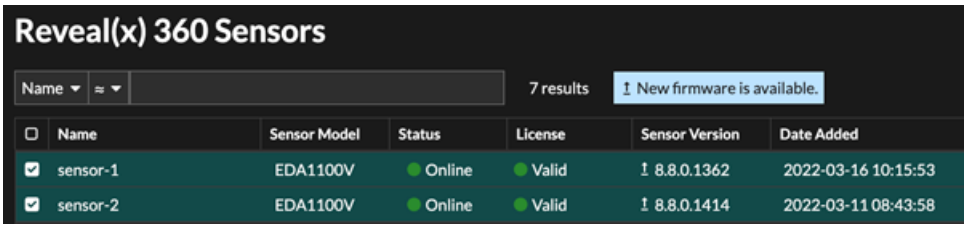
Voici quelques points à prendre en compte lors de la mise à niveau des capteurs :

- Les capteurs doivent être connectés aux services cloud ExtraHop
- Des notifications apparaissent lorsqu'une nouvelle version du microprogramme est disponible

- Vous pouvez mettre à niveau plusieurs capteurs en même temps

1. Connectez-vous à Reveal (x) 360.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Capteurs**.

   Les capteurs éligibles à la mise à niveau affichent une flèche vers le haut dans Version du capteur champ.



3. Cochez la case à côté de chaque sonde que vous souhaitez mettre à niveau.
4. Dans le Détails du capteur dans le volet, sélectionnez la version du microprogramme dans le **Micrologiciel disponible** liste déroulante.

   La liste déroulante affiche uniquement les versions compatibles avec les versions sélectionnées capteurs.

   Uniquement les sélectionnés capteurs pour lesquels une mise à niveau du microprogramme est disponible apparaissent dans capteur Volet de détails.
5. Cliquez **Installation du microprogramme**.

   Lorsque la mise à niveau est terminée, le Version du capteur le champ est mis à jour avec la nouvelle version du firmware.

Enregistrer l'ingestion et la capacité

Le tableau d'ingestion et de capacité des enregistrements sur la page d'administration principale vous permet de surveiller les niveaux d'ingestion et de capacité des enregistrements et de confirmer que la limite de capacité est optimale pour votre environnement.

La ligne rouge en pointillés sur le graphique représente la capacité d'enregistrement de votre abonnement, et les barres bleues représentent le montant d'ingestion effectué chaque jour jusqu'aux 60 derniers jours.

Tu peux créer une règle de notification du système pour vous avertir si l'espace de stockage des enregistrements est proche (supérieur à 80 %) ou supérieur (supérieur à 100 %) de votre capacité quotidienne d'ingestion d'enregistrements.

Si vous constatez que vous dépassez régulièrement la capacité qui vous est allouée, contactez votre représentant commercial ExtraHop.