Migration de modules

Publié: 2023-09-19

Le système ExtraHop propose désormais des modules distincts avec des fonctionnalités segmentées et optimisées pour les cas d'utilisation liés à la sécurité et aux performances.

Le module Network Detection and Response (NDR) fournit des flux de travail de sécurité et d'investigation, tandis que le module Network Performance Management (NPM) fournit des flux de travail liés aux opérations et aux performances. Des modules supplémentaires sont disponibles pour les systèmes de criminalistique des paquets et de détection d'intrusion. En savoir plus sur modules.

Ce guide fournit des informations sur modifications du système global, tâches administratives, ainsi que des directives sur les fonctionnalités sont disponibles pour chaque module.

Changements du système global

Le système ExtraHop met automatiquement à jour certaines fonctionnalités dans le cadre de la migration du module.

Page de connexion par défaut

Pour les utilisateurs ayant accès à NPM, la page de tableau de bord par défaut qui s'affiche après la connexion peut être spécifiée par un administrateur.

Pour les utilisateurs de NPM, la valeur par défaut tableau de bord la page qui s'affiche après la connexion peut être spécifiée globalement par un administrateur ou être défini personnellement par un utilisateur. Si aucun tableau de bord n'est spécifié, le tableau de bord Active Directory apparaît.

Les utilisateurs peuvent accéder à leur tableau de bord par défaut préféré, cliquer sur le menu de commandes dans le coin supérieur droit de la page, puis sélectionner Définir comme tableau de bord par défaut.

Règles de réglage

Le système supprimera l'option Tous les types de détection des critères de type de détection pour les règles de réglage.

Règles de réglage sont affichés en fonction des options d'accès au module spécifiées par privilèges d'utilisateur.

Les règles de réglage existantes qui contiennent les critères Tous les types de détection sont automatiquement divisées en deux règles spécifiques aux catégories de sécurité ou de performance. La règle existante est modifiée pour spécifier tous les types de détection de sécurité, et une nouvelle règle est créée pour tous les types de détection de performance. Pendant la migration, les détections masquées peuvent être associées à une nouvelle règle de réglage correspondant aux critères de détection.

Lorsque vous créez ou modifiez une règle de réglage, vous pouvez spécifier des critères de type de détection en fonction de vos privilèges d'accès au module. La liste déroulante Type de détection peut inclure des options pour tous les types de détection de sécurité ou pour tous les types de détection de performance.

Règles de notification

Les règles de notification de détection ne prennent plus en charge les critères qui s'appliquent à la fois aux détections de sécurité et de performance. Les règles de notification sont affichées en fonction des privilèges d'accès de votre module.

Règles de notification de détection qui spécifient le type d'événement de détection sont automatiquement divisés en deux règles spécifiques aux catégories de sécurité ou de performance. La

règle existante est modifiée pour spécifier le nouveau type d'événement de détection de sécurité et inclut uniquement les critères de sécurité de la règle d'origine. Une nouvelle règle est créée pour le nouveau type d'événement de détection des performances et inclut uniquement les critères de performance de la règle d'origine.

Lorsqu'une règle de notification est divisée pendant la migration, les types de détection associés à la fois à la sécurité et aux performances sont uniquement inclus dans la version de sécurité de la règle afin d'éviter les notifications dupliquées.

Les règles de notification désactivées qui contiennent à la fois des critères de sécurité et de performance ne sont pas divisées. La règle est convertie en règle de sécurité uniquement et reste désactivée.

Les actions spécifiées par les règles de notification, telles que les listes de distribution d'e-mails et les webhooks, sont incluses dans la règle NDR modifiée et dans la nouvelle règle NPM. Passez en revue ces actions pour vous assurer que les notifications de sécurité et de performance sont envoyées au bon public.

Lorsque vous créez une règle de notification, vous pouvez spécifier des types d'événements de détection de sécurité ou de détection des performances, en fonction des options d'accès au module spécifiées dans votre privilèges d'utilisateur. Après avoir sélectionné un type d'événement, vous pouvez uniquement ajouter des critères de type de détection et de catégorie associés au type d'événement sélectionné.

Tâches administratives

Les systèmes migrés permettent à tous les utilisateurs d'accéder aux modules de surveillance des performances réseau (NPM) et de détection et de réponse du réseau (NDR).

Les administrateurs doivent accorder un accès basé sur les rôles à tous les utilisateurs qui se connectent via authentification à distance (LDAP, RADIUS, SAML et TACACS+) ainsi que utilisateurs locaux.

Il existe deux ensembles de privilèges d'utilisateur qui doit être accordé :

Accès au module

Ces privilèges utilisateur déterminent les fonctionnalités auxquelles un utilisateur peut accéder. Par exemple, un utilisateur doit disposer d'un accès complet au module NDR pour voir les détections d'attaques. Voir fonctionnalités spécifiques à chaque module.

Accès au système

Ces niveaux de privilèges utilisateur déterminent le niveau de fonctionnalité des utilisateurs avec les fonctionnalités des modules. Par exemple, les utilisateurs de Full Write peuvent créer et modifier tous les objets du système.

Les sections suivantes fournissent des instructions sur la façon de mettre à jour les privilèges des utilisateurs.

Mise à jour des paramètres d'authentification à distance

Les administrateurs doivent revoir les paramètres d'authentification à distance pour les modules NDR et NPM et les mettre à jour si nécessaire.

Accès au module de détection et de réponse réseau (NDR)

Les paramètres d'authentification à distance pour l'accès au module NDR doivent être configurés sur Reveal (x) Enterprise systèmes sur lesquels la politique globale de privilèges Detections Access, désormais obsolète, n'était pas activée auparavant.

L'accès des utilisateurs au module NDR est directement hérité du paramètre de politique de privilège globale de Detections Access. Par exemple, si seuls des utilisateurs spécifiques bénéficiaient d'un accès aux détections avec accès complet au système d'écriture avant la migration, ces mêmes utilisateurs ont désormais accès au module NDR avec des privilèges complets au système d'écriture après la migration.

Accès au module de surveillance et de performance réseau (NPM)

Les paramètres d'authentification à distance pour l'accès au module NPM doivent être configurés sur les deux Révéler (x) 360 et Reveal (x) Enterprise systèmes.

Mettre à jour la configuration IdP personnalisée dans Reveal (x) 360

Mettez à jour votre configuration personnalisée de fournisseur d'identité (IdP) dans Reveal (x) 360 pour accorder des privilèges aux utilisateurs pour l'accès aux modules NDR et NPM.

Authentification à distance pour l'accès au module NDR

L'accès au module NDR est automatiquement configuré avec les paramètres précédents pour le contrôle d'accès aux détections.

Authentification à distance pour l'accès au module NPM

Vous devez mettre à jour la configuration personnalisée de votre fournisseur d'identité (IdP) pour autoriser les utilisateurs à accéder au module NPM dans Reveal (x) 360.

Ajoutez des privilèges NPM à l'application ExtraHop dans votre fournisseur d'identité

Si votre IdP n'inclut pas d'attribut de groupe pour l'application ExtraHop, vous devez ajouter un attribut utilisateur et un nom correspondant à ceux que vous allez configurer dans Reveal (x) 360.

1. Connectez-vous à votre fournisseur d'identité.
2. Ajoutez un nom et une valeur d'attribut.
3. Enregistrez la configuration.

Prochaines étapes

En savoir plus sur la configuration Okta, Google, Azure AD, ou Jumpcloud.

Ajoutez des privilèges NPM aux paramètres de votre fournisseur d'identité dans Reveal (x) 360

1. Connectez-vous au système Reveal (x) 360 avec un compte doté de privilèges d' administration du système et des accès.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Accès utilisateur**.

   Un panneau Action requise vous guidera à travers les étapes de configuration restantes. Si le panneau Action requise n'apparaît pas, vous n'avez pas besoin de mettre à jour vos paramètres IdP.
3. Entrez un nom dans le champ Nom de l'attribut.
4. Entrez un nom dans le champ Valeur d'attribut.

   Note: Le nom et la valeur de l'attribut doivent correspondre aux paramètres configurés sur votre IdP.
5. Cochez la case pour confirmer que vous êtes prêt à commencer la mise à jour.

   Important: Tous les utilisateurs seront déconnectés du système une fois que vous aurez cliqué **Mettre à jour maintenant** à l' étape suivante.
6. Cliquez **Mettre à jour maintenant**.

Mettre à jour la configuration IdP personnalisée dans Reveal (x) Enterprise

Mettez à jour la configuration personnalisée de votre fournisseur d'identité (IdP) dans Reveal (x) Enterprise pour accorder des privilèges aux utilisateurs pour l'accès aux modules NDR et NPM.

Authentification à distance pour l'accès au module NPM

Vous devez mettre à jour la configuration personnalisée de votre fournisseur d'identité (IdP) pour autoriser les utilisateurs à accéder au module NPM dans Reveal (x) Enterprise.

1. Connectez-vous à la console Reveal (x) Enterprise avec un compte doté de privilèges d'administration du système et des accès.

2. Cliquez sur l'icône des paramètres système puis cliquez sur **Toute l'administration**.
3. Dans la section Paramètres d'accès, cliquez sur **Politiques mondiales**.

   Un panneau Action requise affiche un lien permettant de consulter vos paramètres d'authentification à distance. Si le panneau Action requise n'apparaît pas, vous n'avez pas besoin de mettre à jour vos paramètres IdP.
4. Cliquez **Afficher l'authentification à distance**.
5. Sélectionnez votre méthode d'authentification dans le **Méthode d'authentification à distance** liste déroulante.
6. Procédez comme suit pour la méthode d'authentification à distance que vous avez sélectionnée :

Option	Description

LDAP	Configurez l'accès au module NPM en fonction de votre option d'attribution de privilèges.
	1. Obtenez le niveau de privilèges auprès du serveur distant :
	   1. Entrez un nom unique dans DN d'accès au module NPM champ.
	2. Les utilisateurs distants disposent d'un accès complet en écriture
	   a. Sélectionnez **Accès complet**.
	3. Les utilisateurs distants disposent d'un accès complet en lecture seule
	   a. Sélectionnez **Accès complet**.

RAYON	Configurez l'accès au module NPM en fonction de votre option d'attribution de privilèges.
	1. Les utilisateurs distants disposent d'un accès complet en écriture
	   a. Sélectionnez **Accès complet**.
	2. Les utilisateurs distants disposent d'un accès complet en lecture seule
	   a. Sélectionnez **Accès complet**.

SAML	Modifiez les paramètres du fournisseur d'identité pour ajouter un nom d'attribut et une valeur d'attribut pour l'accès au module NPM. Le nom et les valeurs de l'attribut doivent correspondre aux valeurs configurées dans votre fournisseur d'identité.

TACACS+	Configurez l'accès au module NPM en fonction de votre option d'attribution de privilèges.
	1. Obtenez le niveau de privilèges auprès du serveur distant :
	   1. Sur votre serveur TACACS+, ajoutez l'attribut personnalisé suivant :
	      Attribut : `npmfull`
	      Valeur : 1
	2. Les utilisateurs distants disposent d'un accès complet en écriture

Option	Description
	a. Sélectionnez **Accès complet**. 3. Les utilisateurs distants disposent d'un accès complet en lecture seule a. Sélectionnez **Accès complet**.

7. Retournez au Politiques mondiales page.
8. Cochez la case pour confirmer que vous êtes prêt à démarrer la mise à jour.

   Important: Tous les utilisateurs seront déconnectés du système, à l'exception du compte utilisateur configuré.
9. Cliquez **Mettre à jour maintenant**.

Authentification à distance pour l'accès au module NDR
Si le contrôle d'accès aux détections était activé sur votre système Reveal (x) Enterprise en tant que politique globale avant la migration, l'accès au module NDR est automatiquement configuré avec les paramètres précédents pour le contrôle d'accès aux détections.

Si le contrôle d'accès à la détection n'a pas été activé, vous devez mettre à jour la configuration personnalisée de votre fournisseur d'identité (IdP) pour autoriser les utilisateurs à accéder au module NDR dans Reveal (x) Enterprise.

1. Connectez-vous à la console Reveal (x) Enterprise avec un compte doté de privilèges d'administration du système et des accès.
2. Cliquez sur l'icône des paramètres système puis cliquez sur **Toute l'administration**.
3. Dans la section Paramètres d'accès, cliquez sur **Politiques mondiales**.

   Un panneau Action requise affiche un lien permettant de consulter vos paramètres d'authentification à distance. Si le panneau Action requise n'apparaît pas, vous n'avez pas besoin de mettre à jour vos paramètres IdP.
4. Cliquez **Afficher l'authentification à distance**.
5. Sélectionnez votre méthode d'authentification dans le **Méthode d'authentification à distance** liste déroulante.
6. Procédez comme suit pour la méthode d'authentification à distance que vous avez sélectionnée :

Option	Description
LDAP	Configurez l'accès au module NDR en fonction de votre option d'attribution de privilèges. 1. Obtenez le niveau de privilèges auprès du serveur distant : 1. Entrez un nom unique dans le DN d'accès au module NDR champ. 2. Les utilisateurs distants disposent d'un accès complet en écriture a. Sélectionnez **Accès complet**. 3. Les utilisateurs distants disposent d'un accès complet en lecture seule a. Sélectionnez **Accès complet**.
RAYON	Configurez l'accès au module NDR en fonction de votre option d'attribution de privilèges. 1. Les utilisateurs distants disposent d'un accès complet en écriture

Option	Description
	a. Sélectionnez **Accès complet**. 2. Les utilisateurs distants disposent d'un accès complet en lecture seule a. Sélectionnez **Accès complet**.
SAML	Modifiez les paramètres du fournisseur d'identité pour ajouter un nom d'attribut et une valeur d'attribut pour l'accès au module NDR. Le nom et les valeurs de l'attribut doivent correspondre aux valeurs configurées dans votre fournisseur d'identité.
TACACS+	Configurez l'accès au module NDR en fonction de votre option d'attribution de privilèges. 1. Obtenez le niveau de privilèges auprès du serveur distant : 1. Sur votre serveur TACACS+, ajoutez l'attribut personnalisé suivant : Attribut : `néphréal` Valeur : 1 2. Les utilisateurs distants disposent d'un accès complet en écriture a. Sélectionnez **Accès complet**. 3. Les utilisateurs distants disposent d'un accès complet en lecture seule a. Sélectionnez **Accès complet**.

7. Retournez au Politiques mondiales page.
8. Cochez la case pour confirmer que vous êtes prêt à démarrer la mise à jour.

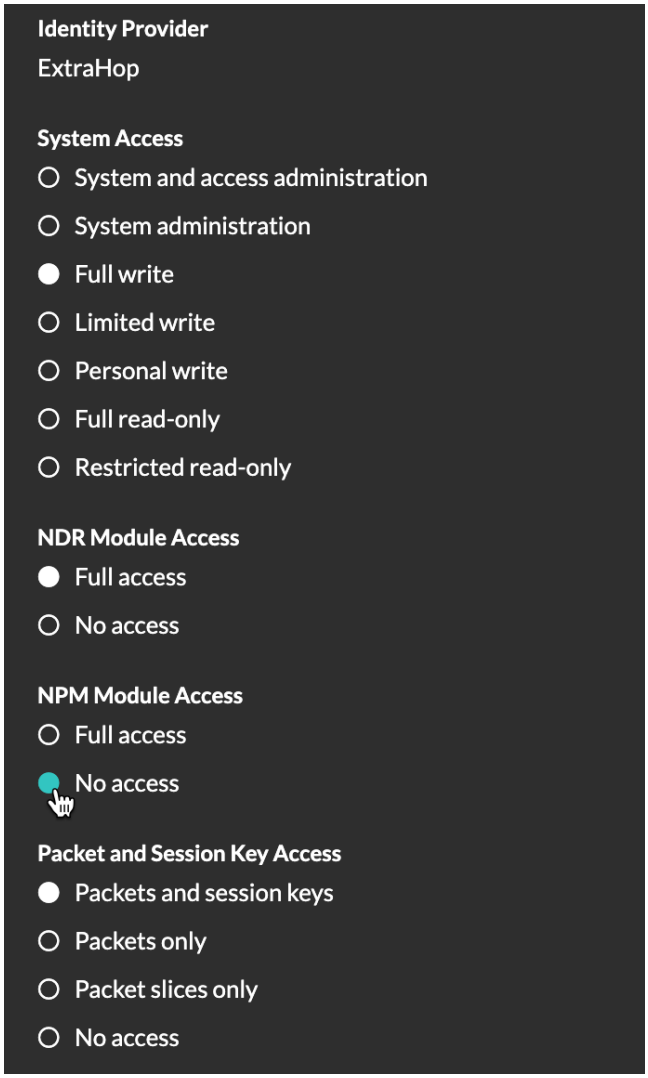
   Important: Tous les utilisateurs seront déconnectés du système, à l'exception du compte utilisateur configuré.
9. Cliquez **Mettre à jour maintenant**.

Mise à jour des paramètres utilisateur locaux

Les administrateurs doivent revoir les privilèges d'accès des utilisateurs locaux pour les modules NDR et NPM et les mettre à jour si nécessaire.

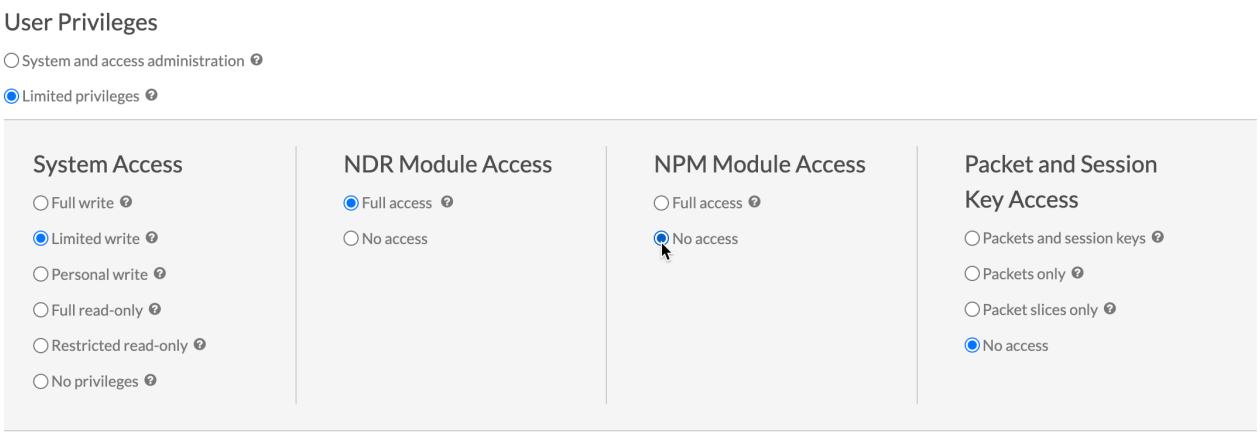
Mettre à jour les utilisateurs locaux dans Reveal (x) 360

1. Connectez-vous à Reveal (x) 360, cliquez sur l'icône des paramètres système, puis cliquez sur **Toute l'administration**.
2. Cliquez **Accès utilisateur**.
3. Dans le Utilisateurs section, cliquez **Afficher les utilisateurs**.
4. Cliquez sur un utilisateur pour afficher et modifier les privilèges d'accès.



Mettre à jour les utilisateurs locaux dans Reveal (x) Enterprise

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans le Paramètres d'accès section, cliquez **Utilisateurs**.
3. Cliquez sur un utilisateur pour afficher et modifier les privilèges d'accès.



Fonctionnalités disponibles par module

Le tableau ci-dessous présente les principales fonctionnalités disponibles par module. Les fonctionnalités non répertoriées sont disponibles dans les deux modules.

Fonctionnalité	NDR	NPM
Page d'aperçu de la sécurité	Y	N
Rapports exécutifs	Y	N
Tableaux de bord de sécurité intégrés	Y	N
Détections de sécurité	Y	N
Plan MITRE	Y	N
Enquêtes	Y	N
Réglage des règles pour les détections de sécurité	Y	N
Règles de notification pour les détections de sécurité et les briefings sur les menaces	Y	N
Briefings sur les menaces	Y	N
Renseignements sur les menaces	Y	N
Tableaux de bord personnalisés	N	Y
Tableaux de bord de performance intégrés	N	Y
Détections de performances	N	Y
Règles de réglage pour les détections de performances	N	Y
Règles de notification pour les détections de performances	N	Y
Alertes	N	Y