Configuration de l'authentification à distance via TACACS+

Publié: 2023-09-19

Le système ExtraHop prend en charge Terminal Access Controller Access-Control System Plus (TACACS+) pour l'authentification et l'autorisation à distance.

Assurez-vous que chaque utilisateur à autoriser à distance dispose du service ExtraHop configuré sur le serveur TACACS+ avant de commencer cette procédure.

1. Connectez-vous aux paramètres d'administration du système ExtraHop via `https://<extrahop-hostname-or-IP-address>/admin`.
2. Dans la section Paramètres d'accès, cliquez sur **Authentification à distance**.
3. Dans la liste déroulante Méthode d'authentification à distance, sélectionnez **TACACS+**, puis cliquez sur **Continuer**.
4. Sur la page Ajouter un serveur TACACS+, saisissez les informations suivantes :

   • Hôte **:** Le nom d'hôte ou l'adresse IP du serveur TACACS+. Assurez-vous que le DNS du système ExtraHop est correctement configuré si vous saisissez un nom d'hôte.

   • Secret **:** Secret partagé entre le système ExtraHop et le serveur TACACS+. Contactez votre administrateur TACACS+ pour obtenir le secret partagé

   Note: . Le secret ne peut pas inclure le signe numérique (#)

   .

   • Délai d'attente **:** Délai en secondes pendant lequel le système ExtraHop attend une réponse du serveur TACACS+ avant de tenter de se reconnecter.
5. Cliquez sur **Ajouter un serveur**.
6. Optionnel : Ajoutez des serveurs supplémentaires si nécessaire.
7. Cliquez sur **Enregistrer et terminer**.
8. Dans la liste déroulante Options d'attribution des autorisations, choisissez l'une des options suivantes :

   - **Obtenir le niveau de privilèges du serveur distant**

     Cette option permet aux utilisateurs distants d'obtenir des niveaux de privilèges à partir du serveur distant. Vous devez également configurer les autorisations sur le serveur TACACS+.

   - **Les utilisateurs distants ont un accès en écriture complet**

     Cette option accorde aux utilisateurs distants un accès en écriture complet au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants ont un accès en lecture seule**

     Cette option permet aux utilisateurs distants d'accéder au système ExtraHop en lecture seule. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session SSL, l'accès au module NDR et l'accès au module NPM.
9. Optionnel : Configurez l'accès aux paquets et aux clés de session. Sélectionnez l'une des options suivantes pour permettre aux utilisateurs distants de télécharger des captures de paquets et des clés de session SSL.

   - **Aucun accès**
   - **Tranches de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**

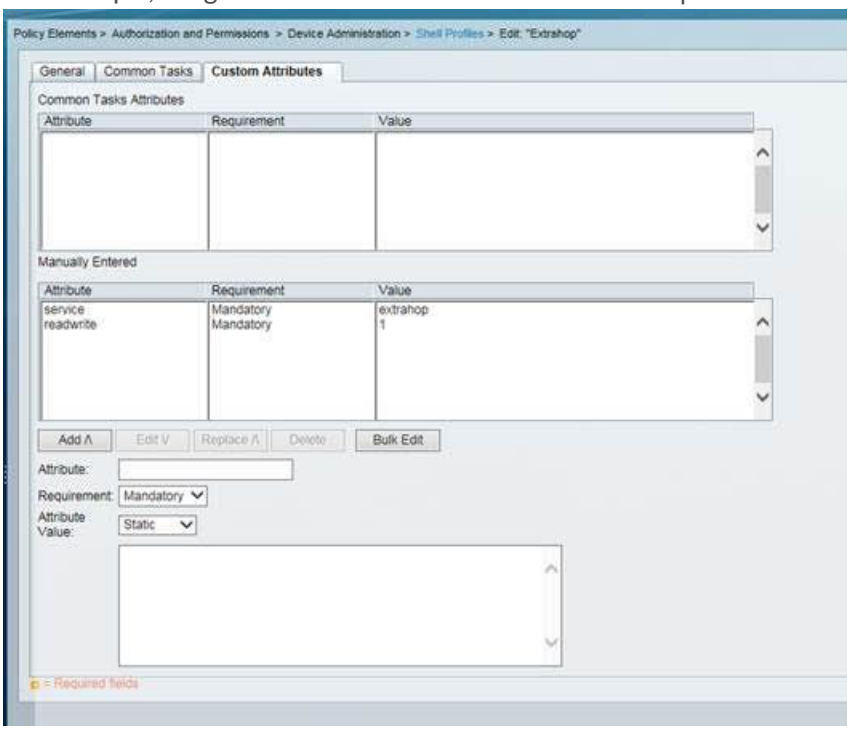
10. Optionnel : Configurez l'accès aux modules NDR et NPM.
    - **Pas d'accès**
    - **Accès complet**
11. Cliquez sur **Enregistrer et terminer**.
12. Cliquez sur **Terminer**.

Configurer le serveur TACACS

Outre la configuration de l'authentification à distance sur votre système ExtraHop, vous devez configurer votre serveur TACACS+ avec deux attributs, l'un pour le service ExtraHop et l'autre pour le niveau d'autorisation. Si vous disposez d'un packetstore ExtraHop, vous pouvez éventuellement ajouter un troisième attribut pour la capture des paquets et la journalisation des clés de session.

1. Connectez-vous à votre serveur TACACS+ et accédez au profil shell de votre configuration ExtraHop.
2. Pour le premier attribut, ajoutez `service`.
3. Pour la première valeur, ajoutez `extrahop`.
4. Pour le deuxième attribut, ajoutez le niveau de privilège, par exemple `readwrite`.
5. Pour la deuxième valeur, ajoutez `1`.

   Par exemple, la figure suivante montre l'attribut `extrahop`et un niveau de privilège de `readwrite`.



Voici un tableau des attributs de permission disponibles, des valeurs et des descriptions :

Attribut	Valeur	Valeur Description
`setup`	`1`	Créer et modifier tous les objets et paramètres du système ExtraHop et gérer l'accès des utilisateurs
`readwrite`	`1`	Créer et modifier tous les objets et paramètres du système

Attribut	Valeur	Valeur Description
		ExtraHop, à l'exception des paramètres d'administration
`limited`	`1`	Créer, modifier et partager des tableaux de bord
`readonly`	`1`	Visualiser des objets dans le système ExtraHop
`personal`	`1`	Créer des tableaux de bord personnels et modifier les tableaux de bord qui ont été partagés avec eux.
`limited_metrics`	`1`	Visualiser les tableaux de bord partagés
`ndrfull`	`1`	Afficher, accuser réception et masquer les détections de sécurité
`npmfull`	`1`	Afficher, accuser réception et masquer les détections de performances
`packetsfull`	`1`	Visualiser et télécharger des paquets stockés sur un packetstore connecté.
`packetslicesonly`	`1`	Visualiser et télécharger des tranches de paquets sur un packetstore connecté.
`packetsfullwithkeys`	`1`	Visualiser et télécharger les paquets et les clés de session associées stockés sur un packetstore connecté.

6. Optionnel : Ajoutez l'attribut suivant pour permettre aux utilisateurs d'afficher, d'accuser réception et de masquer les détections de sécurité

Attribut	Valeur
`ndrfull`	`1`

7. Optionnel : Ajoutez l'attribut suivant pour permettre aux utilisateurs d'afficher, d'accuser réception et de masquer les détections de performances qui apparaissent dans le système ExtraHop.

Attribut	Valeur
`npmfull`	`1`

8. Optionnel : Si vous disposez d'un magasin de paquets ExtraHop, ajoutez un attribut permettant aux utilisateurs de télécharger des captures de paquets ou des captures de paquets avec les clés de session associées.

Attribut	Valeur de l'attribut	Description de l'attribut
`packetslicesonly`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent visualiser et télécharger les 64 premiers octets des paquets.
`paquets complets`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent visualiser et télécharger les paquets stockés dans un magasin de paquets connecté.
`packetslicesonly`	`1`	Visualiser et télécharger des tranches de paquets sur un packetstore connecté.
`packetsfullwithkeys`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent visualiser et télécharger les paquets et les clés de session associées stockés dans un magasin de paquets connecté.