Configuration de l'authentification à distance via TACACS+

Publié: 2023-10-01

Le système ExtraHop prend en charge le 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 des 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 le Paramètres d'accès section, cliquez **Authentification à distance**.
3. À partir du méthode d'authentification à distance liste déroulante, sélectionnez **TACACS+**, puis cliquez sur **Poursuivre**.
4. Sur le Ajouter un serveur TACACS+ page, 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 entrez un nom d'hôte.

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

   - **Obtenir le niveau de privilèges auprès d'un serveur distant**

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

   - **Les utilisateurs distants disposent d'un accès complet en écriture**

     Cette option accorde aux utilisateurs distants un accès complet en écriture 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 disposent d'un accès complet en lecture seule**

     Cette option accorde aux utilisateurs distants un accès en lecture seule 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.
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.

   - **Pas d'accès**
   - **Tranches de paquets uniquement**
   - **Paquets uniquement**
   - **Paquets et clés de session**

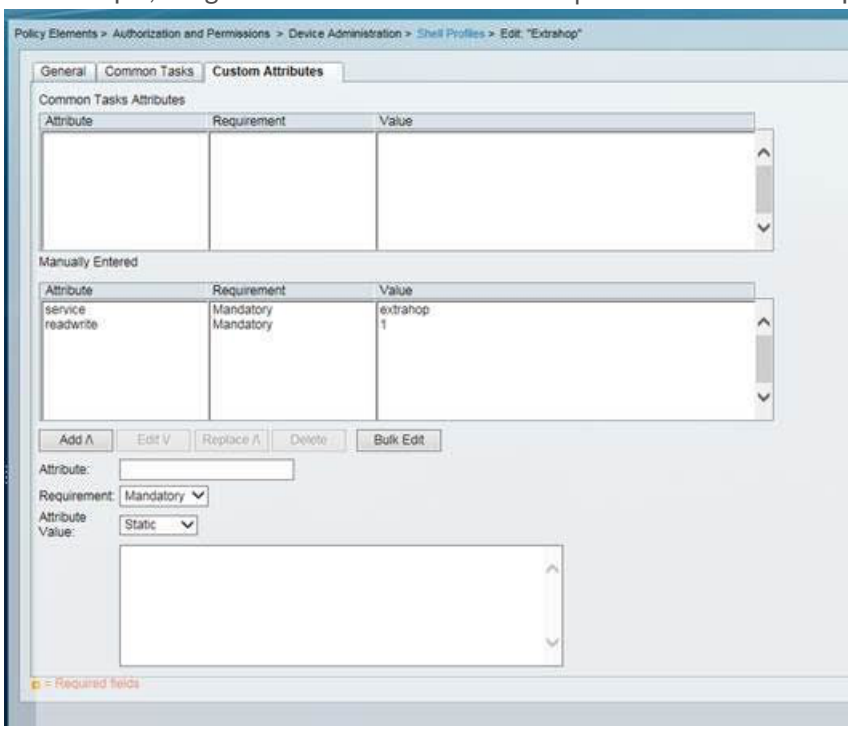
10. Optionnel : Configurez l'accès aux modules NDR et NPM.
    - **Pas d'accès**
    - **Accès complet**
11. Cliquez **Enregistrer et terminer**.
12. Cliquez **Terminé**.

Configuration du 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 avez un stockage des paquets ExtraHop, vous pouvez éventuellement ajouter un troisième attribut pour la capture des paquets et l'enregistrement des clés de session.

1. Connectez-vous à votre serveur TACACS+ et accédez au profil shell correspondant à votre configuration ExtraHop.
2. Pour le premier attribut, ajoutez `service`.
3. Pour la première valeur, ajoutez `saut supplémentaire`.
4. Pour le deuxième attribut, ajoutez le niveau de privilège, tel que `lire/écrire`.
5. Pour la deuxième valeur, ajoutez `1`.

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



Voici un tableau des attributs, des valeurs et des descriptions d'autorisation disponibles :

Attribut	Valeur	Description
`setup`	`1`	Créez et modifiez tous les objets et paramètres du système ExtraHop et gérez l'accès des utilisateurs
`readwrite`	`1`	Créez et modifiez tous les objets et paramètres du système

Attribut	Valeur	Description
		ExtraHop, à l'exception des paramètres d'administration
`limited`	`1`	Créez, modifiez et partagez des tableaux de bord
`readonly`	`1`	Afficher les objets dans le système ExtraHop
`personal`	`1`	Créez des tableaux de bord personnels pour eux-mêmes et modifiez les tableaux de bord partagés avec eux
`limited_metrics`	`1`	Afficher les tableaux de bord partagés
`ndrfull`	`1`	Afficher, confirmer et masquer les détections de sécurité
`npmfull`	`1`	Afficher, reconnaître et masquer les détections de performances
`packetsfull`	`1`	Afficher et télécharger les paquets stockés sur un magasin de paquets connecté.
`packetslicesonly`	`1`	Affichez et téléchargez des tranches de paquets sur un magasin de paquets connecté.
`packetsfullwithkeys`	`1`	Afficher et télécharger les paquets et les clés de session associées stockés dans un magasin de paquets connecté.

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

Attribut	Valeur
`nerfull`	`1`

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

Attribut	Valeur
`npmfull`	`1`

8. Optionnel : Si vous avez un magasin de paquets ExtraHop, ajoutez un attribut pour permettre aux utilisateurs de télécharger des captures de paquets ou des captures de paquets avec les clés de session associées.

Attribut	Valeur	Description
`tranches en paquets uniquement`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent

Attribut	Valeur	Description
		consulter et télécharger les 64 premiers octets de paquets.
`paquets pleins`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les paquets stockés dans un magasin de paquets connecté.
`packetslicesonly`	`1`	Affichez et téléchargez des tranches de paquets sur un magasin de paquets connecté.
`paquets remplis de clés`	`1`	Les utilisateurs, quel que soit leur niveau de privilège, peuvent consulter et télécharger les paquets et les clés de session associées stockés dans un magasin de paquets connecté.