Configuration de l'authentification à distance via LDAP

Publié: 2023-10-01

Le système ExtraHop prend en charge le protocole LDAP (Lightweight Directory Access Protocol) pour l'authentification et l'autorisation. Au lieu de stocker les informations ddevicdentification de l'utilisateur localement, vous pouvez configurer votre système ExtraHop pour authentifier les utilisateurs à distance auprès d'un serveur LDAP existant. Notez que l'authentification LDAP ExtraHop ne demande que les comptes utilisateurs ; elle ne demande aucune autre entité susceptible de se trouver dans l'annuaire LDAP.

Avant de commencer

- Cette procédure nécessite de connaître la configuration du LDAP.
- Assurez-vous que chaque utilisateur fait partie d'un groupe doté d'autorisations spécifiques sur le serveur LDAP avant de commencer cette procédure.
- Si vous souhaitez configurer des groupes LDAP imbriqués, vous devez modifier le fichier de configuration en cours d'exécution. Contacter Assistance ExtraHop pour obtenir de l'aide.

Lorsqu'un utilisateur tente de se connecter à un système ExtraHop, le système ExtraHop essaie de l' authentifier de la manière suivante :

- Tente d'authentifier l'utilisateur localement.
- Tente d'authentifier l'utilisateur via le serveur LDAP s'il n'existe pas localement et si le système ExtraHop est configuré pour l' authentification à distance avec LDAP.
- Connecte l'utilisateur au système ExtraHop s'il existe et le mot de passe est validé localement ou via LDAP. Le mot de passe LDAP n'est pas stocké localement sur le système ExtraHop. Notez que vous devez saisir le nom d'utilisateur et le mot de passe dans le format pour lequel votre serveur LDAP est configuré. Le système ExtraHop transmet uniquement les informations au serveur LDAP.
- Si l'utilisateur n'existe pas ou si un mot de passe incorrect est saisi, un message d'erreur apparaît sur la page de connexion.

> **Important:** Si vous remplacez ultérieurement l'authentification LDAP par une autre méthode d'authentification à distance, les utilisateurs, les groupes d'utilisateurs et les personnalisations associées créés par le biais de l'authentification à distance sont supprimés. Les utilisateurs locaux ne sont pas concernés.

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 **LDAP** puis cliquez sur **Poursuivre**.
4. Sur le Paramètres LDAP page, renseignez les champs d'informations du serveur suivants :
   a) Dans le Nom d'hôte dans ce champ, saisissez le nom d'hôte ou l' adresse IP du serveur LDAP. Si vous configurez un nom d'hôte, assurez-vous que l'entrée DNS du système ExtraHop est correctement configurée.
   b) Dans le Port dans ce champ, saisissez le numéro de port sur lequel le serveur LDAP écoute.
   c) À partir du Type de serveur liste déroulante, sélectionnez **Posix** ou **Active Directory**.
   d) Optionnel : Dans le Bind DN dans le champ, saisissez le DN de liaison. Le DN de liaison correspond aux informations ddevicdentification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche d'utilisateurs. Le DN de liaison doit disposer d'un accès de liste au DN de base et à toute unité d'organisation, groupe ou compte utilisateur requis pour l'authentification LDAP . Si cette valeur n'est pas définie, une liaison anonyme est effectuée. Notez que les liaisons anonymes ne sont pas activées sur tous les serveurs LDAP .

e) Optionnel : Dans le Bind Password dans le champ, saisissez le mot de passe de liaison. Le mot de passe de liaison est le mot de passe requis lors de l'authentification auprès du serveur LDAP en tant que DN de liaison spécifié ci-dessus. Si vous configurez une liaison anonyme, laissez ce champ vide. Dans certains cas, une liaison non authentifiée est possible, lorsque vous fournissez une valeur DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés .

f) À partir du Chiffrement dans la liste déroulante, sélectionnez l'une des options de chiffrement suivantes.

- **Aucune:** Cette option spécifie les sockets TCP en texte clair. Tous les mots de passe sont envoyés sur le réseau en texte clair dans ce mode.
- **LDAPS:** Cette option spécifie le protocole LDAP intégré au protocole SSL.
- **Démarrez TLS:** Cette option spécifie le protocole TLS LDAP. (Le protocole SSL est négocié avant l'envoi des mots de passe.)

g) Sélectionnez **Valider les certificats SSL** pour activer la validation des certificats. Si vous sélectionnez cette option, le certificat du point de terminaison distant est validé par rapport aux certificats racines tels que spécifiés par le gestionnaire de certificats sécurisés. Vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats sécurisés. Pour plus d'informations, voir Ajoutez un certificat fiable à votre système ExtraHop.

h) Entrez une valeur temporelle dans le Intervalle d'actualisation champ ou laissez le paramètre par défaut de 1 heure. L'intervalle d'actualisation garantit que toutes les modifications apportées à l'accès des utilisateurs ou des groupes sur le serveur LDAP sont mises à jour sur le système ExtraHop.

5. Configurez les paramètres utilisateur suivants :

a) Entrez le DN de base dans le DN de base champ. Le DN de base est le point à partir duquel un serveur recherchera des utilisateurs. Le DN de base doit contenir tous les comptes utilisateurs qui auront accès au système ExtraHop. Les utilisateurs peuvent être des membres directs du DN de base ou être imbriqués dans une UO au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Étendue de la recherche spécifiée ci-dessous.

b) Entrez un filtre de recherche dans le Filtre de recherche champ. Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des comptes utilisateurs dans l'annuaire LDAP.

Important: Le système ExtraHop ajoute automatiquement des parenthèses pour encapsuler le filtre et n'analysera pas correctement ce paramètre si vous ajoutez des parenthèses manuellement. Ajoutez vos filtres de recherche à cette étape et à l'étape 5b, comme dans l'exemple suivant :

```
cn=atlas*
|(cn=EH-*)(cn=IT-*)
```

De plus, si les noms de vos groupes incluent le caractère astérisque (*), celui-ci doit être évité en tant que `\2a`. Par exemple, si votre groupe possède un CN appelé `test*group`, tapez `cn=test\2agroup` dans le champ Filtre de recherche.

c) À partir du Étendue de la recherche dans la liste déroulante, sélectionnez l'une des options suivantes. L'étendue de la recherche indique l'étendue de la recherche dans l'annuaire lors de la recherche d'entités utilisateur.

- **Sous-arbre entier:** Cette option recherche de manière récursive sous le nom distinctif du groupe pour les utilisateurs correspondants.
- **Niveau unique:** Cette option recherche uniquement les utilisateurs qui existent dans le DN de base, pas les sous-arborescences.

6. Optionnel : Importez des groupes d'utilisateurs. Sélectionnez le **Importer des groupes d'utilisateurs depuis le serveur LDAP** case à cocher et configurez les paramètres suivants.

Note: L'importation de groupes d'utilisateurs LDAP vous permet de partager des tableaux de bord avec ces groupes. Les groupes importés apparaissent sur la page Groupe d'utilisateurs dans les paramètres d'administration.

a) Entrez le DN de base dans le DN de base champ. Le DN de base est le point à partir duquel un serveur recherchera des groupes d'utilisateurs. Le DN de base doit contenir tous les groupes d'utilisateurs qui auront accès au système ExtraHop. Les groupes d'utilisateurs peuvent être des membres directs du DN de base ou imbriqués au sein d'une UO au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour le Étendue de la recherche spécifiée ci-dessous.

b) Entrez un filtre de recherche dans le Filtre de recherche champ. Les filtres de recherche vous permettent de définir des critères de recherche lorsque vous recherchez des groupes d'utilisateurs dans l'annuaire LDAP.

Important: Pour les filtres de recherche de groupe, le système ExtraHop filtre implicitement sur objectclass=group, et objectclass=group ne doit donc pas être ajouté à ce filtre.

c) À partir du Étendue de la recherche dans la liste déroulante, sélectionnez l'une des options suivantes. L'étendue de la recherche indique l'étendue de la recherche dans l'annuaire lors de la recherche d'entités de groupes d'utilisateurs.

• **Sous-arbre entier:** Cette option recherche de manière récursive sous le DN de base pour les groupes d'utilisateurs correspondants.

• **Niveau unique:** Cette option recherche les groupes d'utilisateurs qui existent dans le DN de base ; elle ne recherche aucun sous-arbre.

7. Cliquez **Réglages du test**. Si le test réussit, un message d'état apparaît en bas de la page. Si le test échoue, cliquez sur **Afficher les détails** pour voir la liste des erreurs. Vous devez corriger toutes les erreurs avant de continuer.
8. Cliquez **Enregistrer et continuer**.

Prochaines étapes
Configuration des privilèges utilisateur pour l'authentification à distance

Configuration des privilèges utilisateur pour l'authentification à distance

Vous pouvez attribuer des privilèges d'utilisateur à des utilisateurs individuels sur votre système ExtraHop ou configurer et gérer des privilèges via votre serveur LDAP.

Lorsque vous attribuez des privilèges utilisateur via LDAP, vous devez remplir au moins un des champs de privilèges utilisateur disponibles. Ces champs nécessitent des groupes (et non des unités organisationnelles) prédéfinis sur votre serveur LDAP. Un compte utilisateur disposant d'un accès doit être membre direct d'un groupe spécifié. Les comptes d'utilisateurs qui ne sont pas membres d'un groupe spécifié ci-dessus n'y auront pas accès. Les groupes absents ne sont pas authentifiés sur le système ExtraHop.

Le système ExtraHop prend en charge les adhésions à des groupes Active Directory et POSIX. Pour Active Directory, `memberOf` est pris en charge. Pour POSIX, `memberuid`, `posixGroups`, `groupofNames`, et `groupofuniqueNames` sont pris en charge.

1. Choisissez l'une des options suivantes dans le Options d'attribution de privilèges liste déroulante :

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

Cette option attribue des privilèges via votre serveur d'authentification à distance. Vous devez remplir au moins l'un des champs de nom distinctif (DN) suivants.

• **DN d'administration du système et des accès:** Créez et modifiez tous les objets et paramètres du système ExtraHop, y compris les paramètres d'administration.

• **DN d'écriture complet:** Créez et modifiez des objets sur le système ExtraHop, sans inclure les paramètres d'administration.

• **DN d'écriture limité:** Créez, modifiez et partagez des tableaux de bord.

• **Personal Write DN:** Créez des tableaux de bord personnels et modifiez les tableaux de bord partagés avec l'utilisateur connecté.

• **DN complet en lecture seule:** Afficher les objets dans le système ExtraHop.

• **DN en lecture seule restreint:** Afficher les tableaux de bord partagés avec l'utilisateur connecté.

• **DN d'accès aux tranches de paquets:** Affichez et téléchargez les 64 premiers octets de paquets capturés via l'appliance ExtraHop Trace.

• **DN d'accès aux paquets:** Affichez et téléchargez les paquets capturés via l' appliance ExtraHop Trace.

• **DN d'accès aux clés de paquet et de session:** Affichez et téléchargez les paquets et toutes les clés de session SSL associées capturés via l'appliance ExtraHop Trace.

• **DN d'accès au module NDR:** Affichez, confirmez et masquez les détections de sécurité qui apparaissent dans le système ExtraHop.

• **DN d'accès au module NPM:** Affichez, confirmez et masquez les détections de performance qui apparaissent dans le système ExtraHop.

- **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.

2. 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**
3. Optionnel : Configurez l'accès aux modules NDR et NPM.
   - **Pas d'accès**
   - **Accès complet**
4. Cliquez **Enregistrer et terminer**.
5. Cliquez **Terminé**.