Configuration de l'authentification à distance via LDAP

Publié: 2025-03-28

Le système ExtraHop prend en charge le protocole LDAP (Lightweight Directory Access Protocol) pour l'authentification et l'autorisation. Au lieu de stocker localement les informations d_identification de l_utilisateur, 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 n' interroge aucune autre entité susceptible de figurer dans l'annuaire LDAP.

Avant de commencer

- Cette procédure nécessite de connaître la configuration du LDAP.
- Assurez-vous que chaque utilisateur appartient à un groupe d'autorisations spécifique 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 d' authentifier l'utilisateur 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 si 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 au format pour lequel votre serveur LDAP est configuré. Le système ExtraHop ne transmet les informations qu'au serveur LDAP.
- Si l'utilisateur n'existe pas ou si un mot de passe incorrect est saisi, un message d'erreur s'affiche sur la page de connexion.

> **Important:** Si vous modifiez ultérieurement l'authentification LDAP pour une autre méthode dauthentification à distance, les utilisateurs, les groupes d'utilisateurs et les personnalisations associées qui ont été 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 sur **Authentification à distance**.
3. À partir du méthode dveloppement d'authentification à distance menu déroulant, sélectionnez **LDAP** puis cliquez sur **Continuer**.
4. Dans le Nom d'hôte dans le 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.
5. Dans le Port dans le champ, saisissez le numéro de port sur lequel le serveur LDAP écoute.
6. À partir du **Type de serveur** menu déroulant, sélectionnez **Posix** ou **Active Directory**.
7. Optionnel : Dans le Lier le DN dans le champ, saisissez le DN de liaison. Le DN de liaison est constitué des informations d'identification de l'utilisateur qui vous permettent de vous authentifier auprès du serveur LDAP pour effectuer la recherche des utilisateurs. Le DN de liaison doit disposer d'un accès par liste au DN de base et à toute unité d'organisation, à tout groupe ou à tout 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.
8. Optionnel : Dans le Mot de passe de liaison 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 de DN de liaison mais aucun mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés.

9. À partir du **Chiffrement** menu déroulant, sélectionnez l'une des options de chiffrement suivantes.

   • **Aucune:** Cette option spécifie les sockets TCP en texte clair. Dans ce mode, tous les mots de passe sont envoyés sur le réseau en texte clair.

   • **LDAPS:** Cette option spécifie le protocole LDAP encapsulé dans le protocole TLS.

   • **Démarrez le protocole TLS:** Cette option spécifie le protocole TLS LDAP. (Le protocole TLS est négocié avant l'envoi de tout mot de passe.)

10. 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 racine, comme spécifié par le gestionnaire de certificats de confiance. 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.

11. Dans le Intervalle de rafraîchissement dans ce champ, saisissez une valeur de temps ou laissez le réglage 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.

12. Dans le DN de base dans le champ, saisissez le nom distinctif (DN) de base.

    Le DN de base est le point à partir duquel un serveur recherche des utilisateurs. Seuls les groupes d'utilisateurs du DN de base peuvent accéder au système ExtraHop. Les utilisateurs peuvent être membres directs du DN de base ou être imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessous.

    Important: Pour les magasins d'enregistrements et les magasins de paquets, tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au magasin de paquets disposent de privilèges administratifs. Vous pouvez restreindre davantage l'accès à l'aide du champ DN d'accès complet.

13. Dans le Filtre de recherche champ, saisissez un filtre de recherche.

    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 envelopper 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 comportent un astérisque (*), celui-ci doit être supprimé car `\2a`. Par exemple, si votre groupe possède un CN appelé `test*group`, tapez `cn=test\2agroup` dans le champ Filtre de recherche.

14. À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.

    L'étendue de recherche spécifie l'étendue de la recherche dans l'annuaire lors de la recherche d' entités utilisateur.

    • **Sous-arbre entier:** Cette option recherche de manière récursive le DN du groupe pour les utilisateurs correspondants.

    • **Niveau unique:** Cette option recherche uniquement les utilisateurs qui existent dans le DN de base, pas les sous-arbres.

15. Pour les disquaires et les magasins de paquets, dans le **Accès complet au DN** champ, saisissez un DN dans le DN de base.

    Cette option restreint davantage l'accès à l'espace de stockage des enregistrements ou au stockage des paquets au seul DN spécifié.

    Important: Tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au stockage des paquets bénéficient de privilèges administratifs.

16. Optionnel : Pour les capteurs et les consoles, sélectionnez **Importer des groupes d'utilisateurs depuis le serveur LDAP** case à cocher et configurez les paramètres suivants pour importer des groupes d'utilisateurs.

    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 Groupes d'utilisateurs dans les paramètres d'administration.

    a) Dans le DN de base dans le champ, saisissez le DN de base.

    Le DN de base est le point à partir duquel un serveur recherche 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 membres directs du DN de base ou imbriqués dans une unité d'organisation au sein du DN de base si **Sous-arbre entier** l'option est sélectionnée pour Champ de recherche spécifié ci-dessous.

    b) Dans le Filtre de recherche dans ce champ, saisissez un filtre de recherche.

    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 le objectclass=group, et objectclass=group ne doit donc pas être ajouté à ce filtre.

    c) À partir du **Champ de recherche** menu déroulant, sélectionnez l'une des options suivantes.

    L'étendue de recherche spécifie 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 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, mais pas les sous-arbres.

17. Cliquez **Paramètres 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 afficher la liste des erreurs. Vous devez corriger toutes les erreurs avant de continuer.

18. 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.

Important: Cette section s'applique uniquement aux capteurs et aux consoles. Pour les magasins d'enregistrements et les magasins de paquets, tous les utilisateurs qui peuvent accéder à l'espace de stockage des enregistrements ou au magasin de paquets disposent de privilèges administratifs.

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)

qui sont prédéfinis sur votre serveur LDAP. Un compte utilisateur avec accès doit être membre direct d'un groupe spécifié. Les comptes 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 appartenances aux 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 Options d'attribution de privilèges menu déroulant :

   - **Obtenir le niveau de privilèges à partir 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 complète:** Créez et modifiez des objets sur le système ExtraHop, à l'exception des paramètres d' administration.

     • **DN à écriture limitée:** Créez, modifiez et partagez des tableaux de bord.

     • **DN d'écriture personnel:** 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 un stockage des paquets.

     • **DN d'accès aux en-têtes de paquets:** Recherchez et téléchargez uniquement les en-têtes des paquets capturés via un stockage des paquets.

     • **DN d'accès aux paquets:** Afficher et télécharger les paquets capturés via un stockage des paquets.

     • **DN d'accès aux clés de paquets et de session:** Affichez et téléchargez les paquets et toutes les clés de session TLS associées capturées via un stockage des paquets.

     • **DN d'accès au module NDR:** Afficher, accuser réception et masquer les détections de sécurité qui apparaissent dans le système ExtraHop.

     • **DN d'accès au module NPM:** Affichez, confirmez et masquez les détections de performances 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 TLS, l'accès au module NDR et l'accès au module NPM.
   - **Les utilisateurs distants disposent d'un accès complet en lecture seule**

     Cette option permet aux utilisateurs distants d'accéder en lecture seule au système ExtraHop. En outre, vous pouvez accorder un accès supplémentaire pour les téléchargements de paquets, les clés de session TLS, 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 TLS.

   - **Pas d'accès**
   - **Tranches en sachets uniquement**
   - **En-têtes de paquets uniquement**
   - **Paquets uniquement**

- **Paquets et clés de session**

3. Optionnel : Configurez l'accès aux modules NDR et NPM (sur les capteurs et les consoles uniquement).
   - **Pas d'accès**
   - **Accès complet**
4. Cliquez **Enregistrer et terminer**.
5. Cliquez **Terminé**.