Configuration de l'authentification à distance via LDAP

Publié: 2023-09-19

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 d'identification des utilisateurs localement, vous pouvez configurer votre système ExtraHop pour qu'il authentifie les utilisateurs à distance avec un serveur LDAP existant. Notez que l'authentification LDAP d'ExtraHop n'interroge que les comptes d'utilisateurs ; elle n'interroge pas les autres entités qui pourraient se trouver dans l'annuaire LDAP.

Avant de commencer

- Cette procédure nécessite d'être familiarisé avec la configuration de LDAP.
- Assurez-vous que chaque utilisateur fait partie d'un groupe spécifique sur le serveur LDAP avant de commencer cette procédure.
- Si vous souhaitez configurer des groupes LDAP imbriqués, vous devez modifier le fichier Running Configuration. Contactez l'assistance ExtraHop pour obtenir de l'aide.

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

- Tentative d'authentification locale de l'utilisateur.
- Tente d'authentifier l'utilisateur via le serveur LDAP si l'utilisateur n'existe pas localement et si le système ExtraHop est configuré pour l'authentification à distance avec LDAP.
- Connecte l'utilisateur au système ExtraHop si l'utilisateur existe et si le mot de passe est validé localement ou par 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 ne fait que transmettre 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 qui ont été créés par le biais de l'authentification à distance sont supprimés. Les utilisateurs locaux ne sont pas affectés.

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 **LDAP**, puis cliquez sur **Continuer**.
4. Sur la page Paramètres LDAP, complétez les champs d'informations suivants sur le serveur :
   a) Dans le champ Nom d'hôte, 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 champ Port, saisissez le numéro de port sur lequel le serveur LDAP écoute.
   c) Dans la liste déroulante Type de serveur, sélectionnez **Posix** ou **Active Directory**.
   d) Optionnel : Dans le champ Bind DN (DN de liaison), saisissez le DN de liaison. Le DN de liaison est l'identifiant de l'utilisateur qui vous permet de vous authentifier auprès du serveur LDAP pour effectuer la recherche d'utilisateurs. Le DN de liaison doit avoir un accès de liste au DN de base et à tout OU, groupe ou compte d'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 champ Bind Password (Mot de passe de liaison), 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 pas de mot de passe de liaison. Consultez votre administrateur LDAP pour connaître les paramètres appropriés.

f) Dans la liste déroulante Encryption, sélectionnez l'une des options de cryptage suivantes.

- **Aucun:** Cette option spécifie des sockets TCP en texte clair. Dans ce mode, tous les mots de passe sont envoyés en clair sur le réseau.
- **LDAPS:** Cette option indique que le protocole LDAP est intégré dans le protocole SSL.
- **StartTLS:** Cette option spécifie le LDAP TLS. (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 racine spécifiés par le gestionnaire de certificats de confiance. Vous devez configurer les certificats auxquels vous souhaitez faire confiance sur la page Certificats de confiance. Pour plus d'informations, voir Ajouter un certificat de confiance à votre système ExtraHop.

h) Saisissez une valeur temporelle dans le champ Intervalle d'actualisation ou laissez le paramètre par défaut de 1 heure. L'intervalle d'actualisation garantit que toute modification apportée à l'accès d'un utilisateur ou d'un groupe sur le serveur LDAP est mise à jour sur le système ExtraHop.

5. Configurez les paramètres utilisateur suivants :

a) Saisissez le DN de base dans le champ DN de base. 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 OU au sein du DN de base si l'option **Sous-arbre entier** est sélectionnée pour l'étendue de la recherche spécifiée ci-dessous.

b) Saisissez un filtre de recherche dans le champ Filtre de recherche. Les filtres de recherche vous permettent de définir des critères de recherche lors de la recherche de comptes d'utilisateurs dans l'annuaire LDAP.

> **Important:** Le système ExtraHop ajoute automatiquement des parenthèses pour envelopper le filtre et n'analysera pas ce paramètre correctement 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-*)
> ```
>
> En outre, si les noms de vos groupes comprennent le caractère astérisque (*), l'astérisque doit être échappé sous la forme `\2a`. Par exemple, si votre groupe a un CN appelé `test*group`, tapez `cn=test\2agroup` dans le champ Filtre de recherche.

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

- **Sous-arbre entier:** Cette option recherche les utilisateurs correspondants de manière récursive sous le DN du groupe.
- **Niveau unique:** Cette option recherche les utilisateurs qui existent uniquement dans le DN de base, à l'exclusion de tout sous-arbre.

6. Optionnel : Importer des groupes d'utilisateurs. Cochez la case **Importer des groupes d'utilisateurs à partir du serveur LDAP** 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) Saisissez le DN de base dans le champ DN de base. Le DN de base est le point à partir duquel un serveur recherchera les 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 être imbriqués dans une OU du DN de base si l'option **Sous-arbre entier** est sélectionnée pour l'étendue de la recherche spécifiée ci-dessous.

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

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

c) Dans la liste déroulante Étendue de la recherche, sélectionnez l'une des options suivantes. L'étendue de la 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 récursivement sous le DN de base les groupes d'utilisateurs correspondants.
- **Niveau unique:** Cette option recherche les groupes d'utilisateurs qui existent dans le DN de base, à l'exclusion de tout sous-arbre.

7. Cliquez sur **Test Settings**. Si le test réussit, un message d'état s'affiche en bas de la page. Si le test échoue, cliquez sur **Afficher les détails** pour afficher une liste d'erreurs. Vous devez résoudre toutes les erreurs avant de continuer.
8. Cliquez sur **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 autorisations d'accès à des utilisateurs individuels sur votre système ExtraHop ou configurer et gérer des autorisations d'accès par l'intermédiaire de votre serveur LDAP.

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

Le système ExtraHop prend en charge l'appartenance aux groupes Active Directory et POSIX. Pour Active Directory, `memberOf` est pris en charge. Pour POSIX, les adresses `memberuid`, `posixGroups`, `groupofNames` et `groupofuniqueNames` sont prises en charge.

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

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

  Cette option permet d'attribuer des privilèges par l'intermédiaire de votre serveur d'authentification distant. Vous devez renseigner au moins l'un des champs de nom distinctif (DN) suivants.

  - **DN d'administration du système et des accès:** Permet de créer et de modifier tous les objets et paramètres du système ExtraHop, y compris les paramètres d'administration.
  - **DN d'écriture complet:** Créer et modifier des objets sur le système ExtraHop, à l'exception des paramètres d'administration.
  - **DN d'écriture limitée:** Créer, modifier et partager des tableaux de bord.

• **DN d'écriture personnel:** Créer des tableaux de bord personnels et modifier les tableaux de bord partagés avec l'utilisateur connecté.

• **DN en lecture seule:** Visualiser les objets du système ExtraHop.

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

• **DN d'accès aux tranches de paquets:** Visualisation et téléchargement des 64 premiers octets des paquets capturés par l'appliance ExtraHop Trace.

• **DN d'accès aux paquets:** Visualiser et télécharger les paquets capturés par l'appliance ExtraHop Trace.

• **DN d'accès aux paquets et aux clés de session:** Permet d'afficher et de télécharger les paquets et les clés de session SSL associées capturés par l'appliance ExtraHop Trace.

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

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

- **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.

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.
   - **Aucun 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 sur **Enregistrer et terminer**.
5. Cliquez sur **Terminer**.