Configuration de l'authentification à distance via SAML

Publié: 2023-09-19

Vous pouvez configurer une authentification unique (SSO) sécurisée au système ExtraHop par le biais d'un ou plusieurs fournisseurs d'identité SAML (Security Assertion Markup Language).

Lorsqu'un utilisateur se connecte à un système ExtraHop configuré en tant que fournisseur de services (SP) pour l'authentification SAML SSO, le système ExtraHop demande une autorisation au fournisseur d'identité (IdP) approprié. Le fournisseur d'identité authentifie les informations d'identification de l'utilisateur et renvoie l'autorisation de l'utilisateur au système ExtraHop. L'utilisateur peut alors accéder au système ExtraHop.

Les guides de configuration pour les fournisseurs d'identité spécifiques sont indiqués ci-dessous. Si votre fournisseur ne figure pas dans la liste, appliquez les paramètres requis par le système ExtraHop à votre fournisseur d'identité.

Les fournisseurs d'identité doivent répondre aux critères suivants :

- SAML 2.0
- Prise en charge des flux de connexion initiés par le fournisseur d'identité. Les flux de connexion initiés par l'IdP ne sont pas pris en charge.
- Prise en charge des réponses SAML signées
- Prise en charge de la liaison HTTP-Redirect

L'exemple de configuration de cette procédure permet d'accéder au système ExtraHop par le biais d'attributs de groupe.

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs d'utilisateur avec les privilèges d'accès d'écriture, de paquets et de détection appropriés.

Activer l'authentification à distance SAML

Avertissement : Si votre système est déjà configuré avec une méthode d'authentification à distance, la modification de ces paramètres supprimera tous les utilisateurs et les personnalisations associées créés par le biais de cette méthode, et les utilisateurs distants ne pourront pas accéder au système. 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. Sélectionnez **SAML** dans la liste déroulante de la méthode d'authentification à distance, puis cliquez sur **Continuer**.

- Cliquez sur **View SP Metadata (Afficher les métadonnées SP)** pour afficher l'URL de l'Assertion Consumer Service (ACS) et l'ID d'entité du système ExtraHop. Ces chaînes sont requises par votre fournisseur d'identité pour configurer l'authentification SSO. Vous pouvez également télécharger un fichier de métadonnées XML complet que vous pouvez importer dans la configuration de votre fournisseur d'identité

  Note: . Si l'URL ACS contient un nom d'hôte inaccessible, tel que le nom d'hôte par défaut du système `extrahop`, vous devez modifier l'URL lors de l'ajout de l'URL ACS à votre fournisseur d'identité et spécifier le nom de domaine complet (FQDN) du système ExtraHop

  .
- Cliquez sur **Ajouter un fournisseur d'identité** pour ajouter les informations suivantes :

• **Nom du fournisseur:** Saisissez un nom pour identifier votre fournisseur d'identité spécifique. Ce nom apparaît sur la page de connexion au système ExtraHop après le texte **Connexion avec**.

• **ID de l'entité:** Collez dans ce champ l'identifiant de l'entité fourni par votre fournisseur d'identité.

• **URL SSO:** Collez dans ce champ l'URL d'authentification unique fournie par votre fournisseur d'identité.

• **Certificat public:** Collez le certificat X.509 fourni par votre fournisseur d'identité dans ce champ.

• **Auto-provisionnement des utilisateurs:** Lorsque cette option est sélectionnée, les comptes utilisateurs ExtraHop sont automatiquement créés lorsque l'utilisateur se connecte via le fournisseur d'identité. Pour contrôler manuellement les utilisateurs autorisés à se connecter, décochez cette case et configurez manuellement les nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST. Tout nom d'utilisateur distant créé manuellement doit correspondre au nom d'utilisateur configuré sur le fournisseur d'identité.

• **Activer ce fournisseur d'identité:** Cette option est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter via ce fournisseur d'identité, décochez la case.

• **Attributs de privilèges utilisateur:** Vous devez configurer les attributs de privilège de l'utilisateur avant que les utilisateurs puissent se connecter au système ExtraHop par l'intermédiaire d'un fournisseur d'identité.

Les noms et les valeurs des attributs de privilège de l'utilisateur doivent correspondre aux noms et aux valeurs que votre fournisseur d'identité inclut dans les réponses SAML, qui sont configurées lorsque vous ajoutez l'application ExtraHop à un fournisseur. Par exemple, dans Azure AD, vous configurez des noms de demande et des valeurs de condition de demande qui doivent correspondre aux noms et valeurs des attributs de privilèges d'utilisateur dans le système ExtraHop. Pour des exemples plus détaillés, voir les rubriques suivantes :

- Configurer l'authentification unique SAML avec JumpCloud
- Configurer l'authentification unique SAML avec Google
- Configurer l'authentification unique SAML avec Okta
- Configurer l'authentification unique SAML avec Azure AD

Note: Si un utilisateur correspond à plusieurs valeurs d'attribut, il se voit accorder le privilège d'accès le plus permissif. Par exemple, si un utilisateur correspond à la fois aux valeurs d'écriture limitée et d'écriture complète, il se voit accorder les privilèges d'écriture complète. Pour plus d'informations sur les niveaux de privilèges, voir Utilisateurs et groupes d'utilisateurs.

• **Accès au module NDR:** Les attributs NDR permettent aux utilisateurs d'accéder aux fonctions NDR.

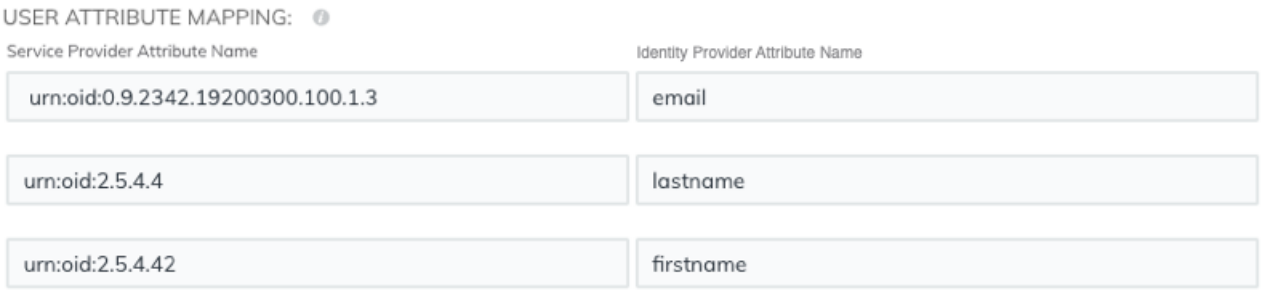
• **Accès au module NPM:** Les attributs NPM permettent aux utilisateurs d'accéder aux fonctions NPM.

• **Accès aux paquets et aux clés de session:** Les attributs de paquets et de clés de session permettent aux utilisateurs d'accéder aux paquets et aux clés de session. La configuration des attributs de paquets et de clés de session est facultative et n'est requise que lorsque vous disposez d'un magasin de paquets ExtraHop connecté.

Mappage des attributs utilisateur

Vous devez configurer l'ensemble suivant d'attributs utilisateur dans la section de mappage d'attributs d'application de votre fournisseur d'identité. Ces attributs permettent d'identifier l'utilisateur dans le système ExtraHop. Reportez-vous à la documentation de votre fournisseur d'identité pour connaître les noms de propriété corrects lors du mappage des attributs.

Nom de l'attribut ExtraHop	Nom convivial	Catégorie	Nom de l'attribut du fournisseur d'identité
`urn:oid:0.9.2342.19200300.100.1.3`	mail	Attribut standard	Adresse électronique principale
`urn:oid:2.5.4.4`	sn	Attribut standard	Nom de famille
`urn:oid:2.5.4.42`	givenName	Attribut standard	Prénom



Attributs de groupe

Le système ExtraHop prend en charge les déclarations d'attributs de groupe afin d'associer facilement les privilèges des utilisateurs à tous les membres d'un groupe spécifique. Lorsque vous configurez l'application ExtraHop sur votre fournisseur d'identité, indiquez un nom d'attribut de groupe. Ce nom est ensuite saisi dans le champ Nom de l'attribut lorsque vous configurez le fournisseur d'identité sur le système ExtraHop.

Si votre fournisseur d'identité ne prend pas en charge les déclarations d'attributs de groupe, configurez les attributs utilisateur avec les privilèges d'accès appropriés en écriture, en paquets et en détection.

Prochaines étapes

- Configurer l'authentification unique SAML avec JumpCloud
- Configurer l'authentification unique SAML avec Google
- Configurer l'authentification unique SAML avec Okta