Configurer l'authentification unique SAML avec JumpCloud

Publié: 2023-09-19

Vous pouvez configurer votre système ExtraHop pour permettre aux utilisateurs de se connecter au système via le service de gestion des identités JumpCloud.

Avant de commencer

- Vous devez être familiarisé avec l'administration de JumpCloud.
- Vous devez être familiarisé avec l'administration des systèmes ExtraHop.

Ces procédures nécessitent de copier et de coller des informations entre le système ExtraHop et JumpCloud, il est donc utile d'avoir les deux systèmes ouverts côte à côte.

Activer SAML sur le système ExtraHop

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 **SAML**.
4. Cliquez sur **Continuer**.
5. Cliquez sur **View SP Metadata (Afficher les métadonnées SP)**. Vous devrez copier l'URL ACS et l'ID d'entité pour les coller dans la configuration JumpCloud dans la procédure suivante.

Configurer les paramètres SAML dans JumpCloud

1. Connectez-vous à la console d'administration de JumpCloud via `https://console.jumpcloud.com/`.
2. Dans le volet gauche, sous Authentification de l'utilisateur, cliquez sur **SSO**.
3. Cliquez sur **Add New Application (Ajouter une nouvelle application)**.
4. Cliquez sur **Custom SAML App**.

5. Sur la page Nouveau SSO, dans la section Informations générales, tapez un nom pour identifier le système ExtraHop dans le champ Étiquette d'affichage.
6. Cliquez sur l'onglet **SSO** et configurez les champs suivants :

   • **IdP Entity ID:**

   Saisissez n'importe quelle chaîne de caractères. Cet identifiant est requis lorsque vous configurez le fournisseur d'identité sur le système ExtraHop.

   • **SP Entity ID:** Saisissez ou collez l'ID de l'entité du système ExtraHop.

   • **URL ACS:** Tapez ou collez l'URL de l'Assertion Consumer Service (ACS) du système ExtraHop.

   • **Certificat SP:** Laissez ce champ vide pour que JumpCloud génère un nouveau certificat. Vous pouvez également fournir votre propre certificat.

   • **SAMLSubject NameID:** Sélectionnez l'**email** dans la liste déroulante.

• **SAMLSubject NameID Format:** Sélectionnez **urn:oasis:names:tc:SAML:2.0:nameid-format:persistent**dans la liste déroulante.

• **Algorithme de signature:** Sélectionnez **RSA-SHA256** dans la liste déroulante.

• **État du relais par défaut:** Laissez ce champ vide.

• **URL de connexion:** Laissez ce champ vide.

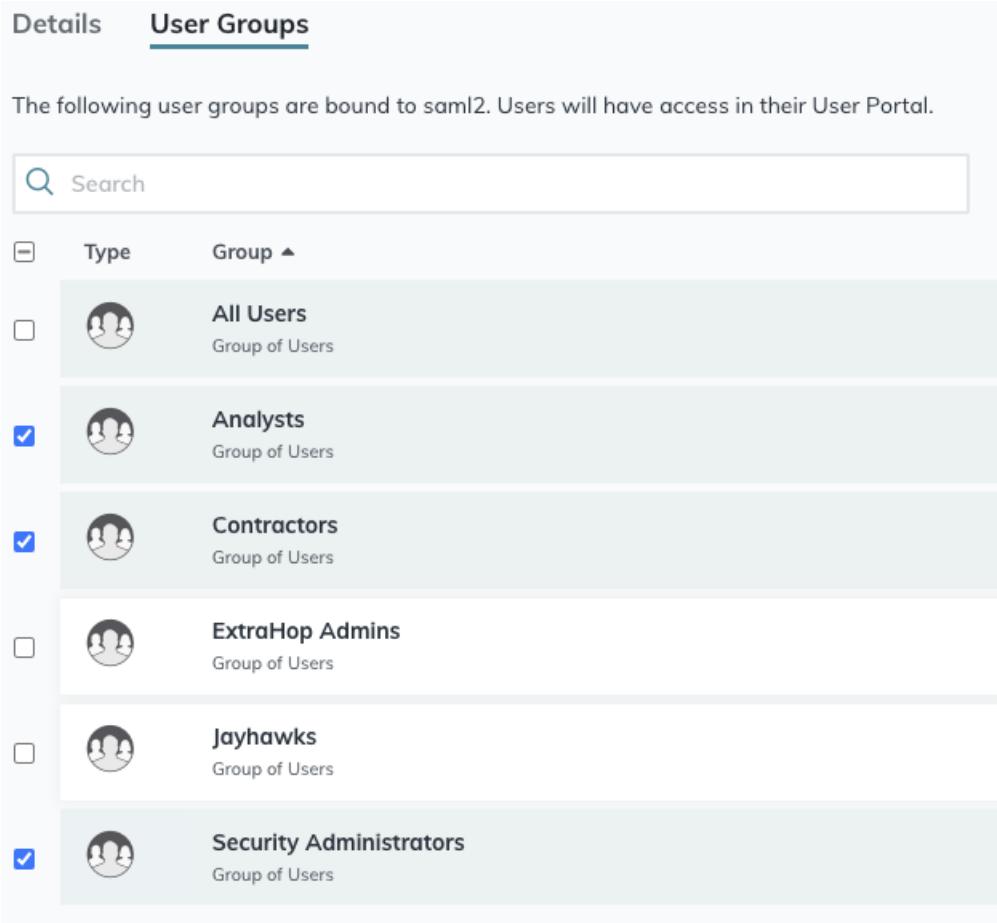
• **IdP URL:** Tapez un nom d'identification dans le champ. L'URL ressemble à l'exemple suivant : https://sso.jumpcloud.com/saml2/extrahop.

7. Dans la section User Attribute Mapping, cliquez sur **add attribute (ajouter un attribut**) et saisissez les chaînes suivantes. Ces attributs permettent d'identifier l'utilisateur dans le système ExtraHop.

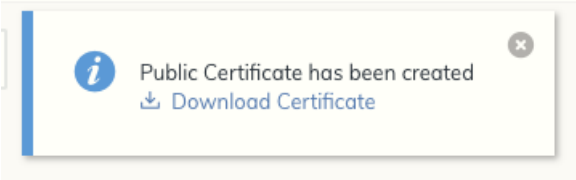
Nom d'attribut du fournisseur de services	Nom de l'attribut JumpCloud
urn:oid:0.9.2342.19200300.100.1.3	courriel
urn:oid:2.5.4.4	nom de famille
urn:oid:2.5.4.42	prénom

8. Dans la section Attributs de groupe, sélectionnez **Inclure l'attribut de groupe** et saisissez un nom dans le champ pour identifier le groupe. Vous spécifierez ce nom lorsque vous configurerez les attributs des privilèges des utilisateurs sur le système ExtraHop.

9. Cliquez sur l'onglet **Groupes d'utilisateurs**.
10. Sélectionnez tous les groupes qui doivent avoir accès au système ExtraHop. Trois groupes sont sélectionnés dans l'exemple ci-dessous.



11. Cliquez sur **Activer**.
12. Cliquez sur **Continuer** pour confirmer les nouveaux paramètres.
JumpCloud génère un certificat après la création de l'application. Cliquez sur **Télécharger le certificat** et enregistrez le fichier sur votre ordinateur.



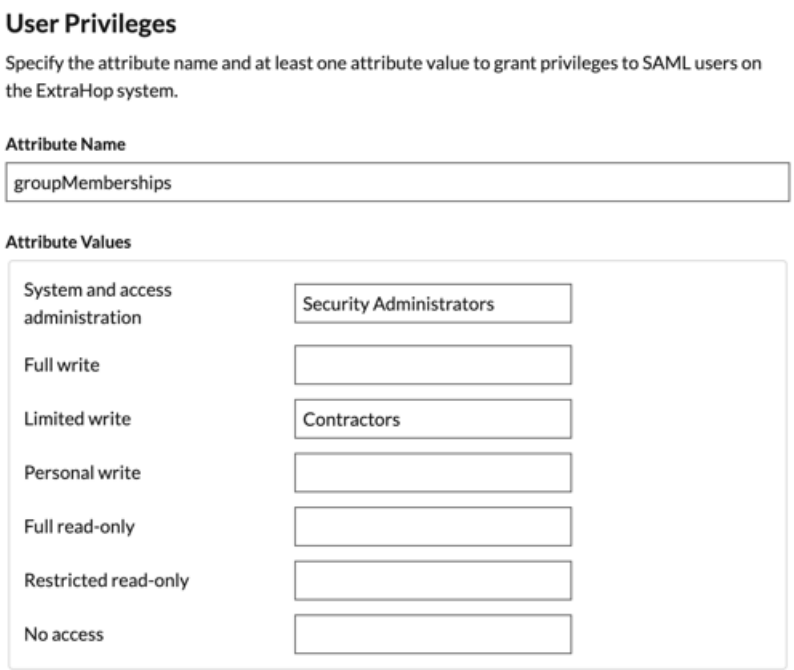
Ajouter des informations sur le fournisseur d'identité sur le système ExtraHop

1. Retournez dans les paramètres d'administration du système ExtraHop. Fermez la fenêtre des métadonnées du fournisseur de services si elle est encore ouverte, puis cliquez sur **Ajouter un fournisseur d'identité**.
2. Saisissez un nom unique dans le champ Nom du fournisseur. Ce nom apparaît sur la page de connexion du système ExtraHop.
3. Depuis JumpCloud, copiez l'ID de l'entité IdP et collez-le dans le champ ID de l'entité sur le système ExtraHop.
4. Depuis JumpCloud, copiez l'URL de l'IdP et collez-la dans le champ URL SSO du système ExtraHop.

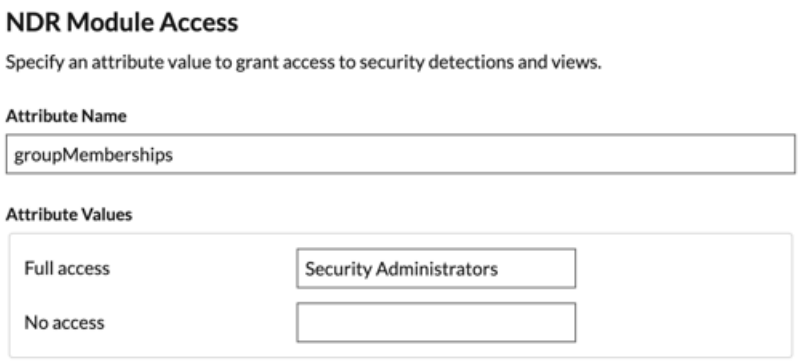
5. Ouvrez le fichier `certificate.pem` dans un éditeur de texte, copiez les données du certificat et collez-les dans le champ Certificat publicdu système ExtraHop.
6. Choisissez l'une des options suivantes pour provisionner les utilisateurs.
   - Sélectionnez Auto-provision users (Approvisionnement automatique des utilisateurs) pour créer un nouveau compte utilisateur SAML distant sur le système ExtraHop lorsque l'utilisateur se connecte pour la première fois au système.
   - Décochez la case Approvisionnement automatique des utilisateurs et configurez manuellement de nouveaux utilisateurs distants via les paramètres d'administration d'ExtraHop ou l'API REST.
7. L'option **Activer ce fournisseur d'identité** est sélectionnée par défaut et permet aux utilisateurs de se connecter au système ExtraHop. Pour empêcher les utilisateurs de se connecter, décochez la case.
8. Configurez les attributs des privilèges des utilisateurs. Vous devez configurer l'ensemble des attributs utilisateur suivants avant que les utilisateurs puissent se connecter au système ExtraHop par l'intermédiaire d'un fournisseur d'identité. Les valeurs sont définies par l'utilisateur, mais elles doivent correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne sont pas sensibles à la casse et peuvent inclure des espaces. Pour plus d'informations sur les niveaux de privilèges, voir Utilisateurs et groupes d'utilisateurs.

   Important: Vous devez spécifier le nom de l'attribut et configurer au moins une valeur d'attribut autre que **Pas d'accès** pour permettre aux utilisateurs de se connecter.

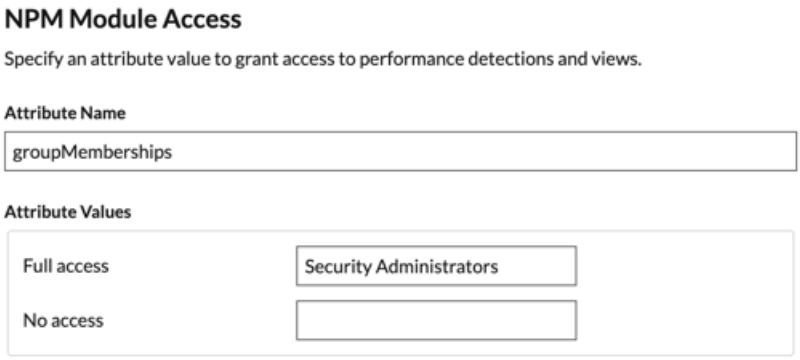
   Dans l'exemple ci-dessous, le champ Nom de l' attribut est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité et les Valeurs de l'attribut sont les noms de vos groupes d'utilisateurs. Si un utilisateur est membre de plusieurs groupes, il se voit accorder le privilège d'accès le plus permissif.



9. Configurer l'accès au module NDR.



10. Configurer l'accès au module NPM.



11. Optionnel : Configurez l'accès aux paquets et aux clés de session. Cette étape est facultative et n'est requise que lorsque vous disposez d'un packetstore connecté.

12. Cliquez sur **Save (Enregistrer)**.
13. Sauvegarder la configuration en cours d'exécution.

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez sur **Se connecter avec** *<nom du fournisseur>*.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse électronique et de votre mot de passe. Vous êtes automatiquement dirigé vers la page de présentation d'ExtraHop.