Configurer l'authentification unique SAML avec JumpCloud

Publié: 2024-07-03

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 vous obligent à copier-coller des informations entre le système ExtraHop et JumpCloud. Il est donc utile d'ouvrir chaque système côte à côte.

Activez 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. À partir du méthode dac.authentification à distance liste déroulante, sélectionnez **SAML**.
4. Cliquez **Poursuivre**.
5. Cliquez **Afficher les métadonnées SP**. Vous devrez copier l' URL ACS et l'ID d'entité pour les coller dans la configuration JumpCloud lors de la procédure suivante .

Configurer les paramètres SAML dans JumpCloud

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

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

   • **ID d'entité IdP:**

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

   • **ID de l'entité SP:** Tapez ou collez l'ID d'entité depuis le système ExtraHop.

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

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

   • **Nom du sujet SAML:** Sélectionnez **courriel** depuis la liste déroulante.

   • **Format SAML du nom/identifiant du sujet:** Sélectionnez **urn:oasis:names:tc:saml:2.0:nameid-format:persistent** depuis la liste déroulante.

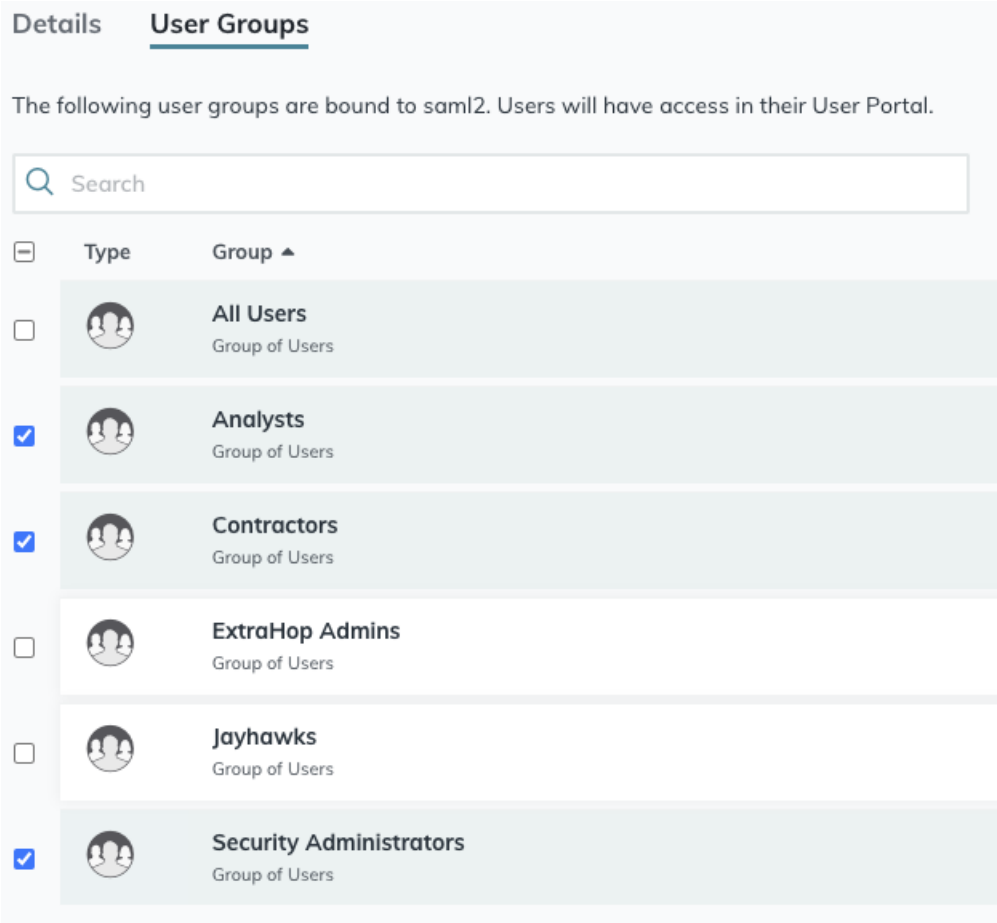
- **Algorithme de signature:** Sélectionnez **RSA-SHA255** depuis la liste déroulante.
- **État du relais par défaut:** Laissez ce champ vide.
- **URL de connexion:** Laissez ce champ vide.
- **URL de l'IdP:** Entrez un nom d'identification dans le champ. L'URL ressemble à l'exemple suivant : `https://sso.jumpcloud.com/saml2/extrahop`.

7. Dans le Mappage des attributs utilisateur section, cliquez **ajouter un attribut** et tapez les chaînes suivantes. Ces attributs identifient l'utilisateur dans l'ensemble du système ExtraHop.

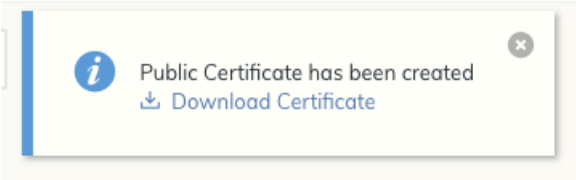
Nom de l'attribut du fournisseur de services	Nom de l'attribut JumpCloud
urn:oid:0.9.2342.19200300.100.1.3	courriel
urn:oid:2.5.4.4	nom de famille
urn:oid:2.5.4.42	prénom

8. Dans le Attributs du groupe section, sélectionnez **inclure un attribut de groupe** et saisissez un nom dans le champ pour identifier le groupe. Vous spécifierez ce nom lorsque vous configurerez les attributs de privilèges utilisateur sur le système ExtraHop.

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



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



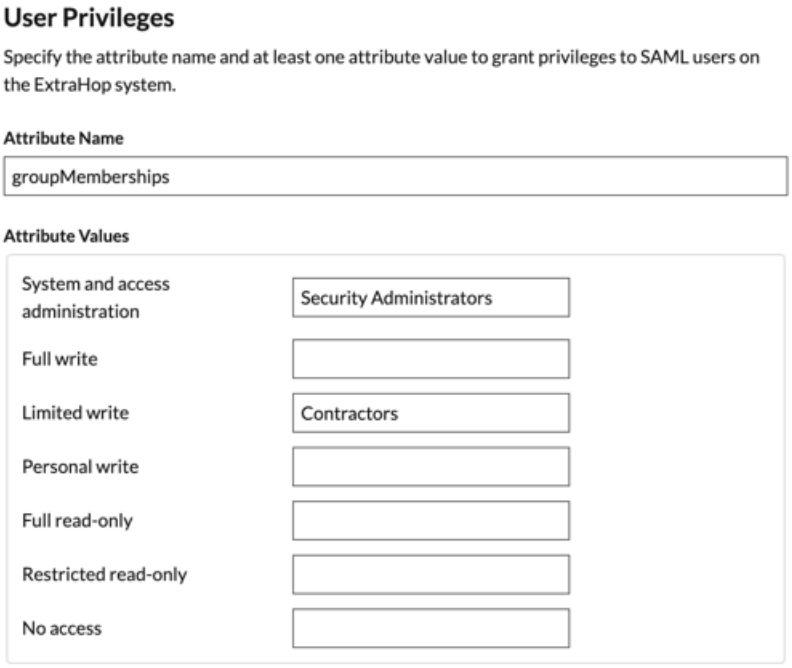
Ajouter les informations du fournisseur d'identité sur le système ExtraHop

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

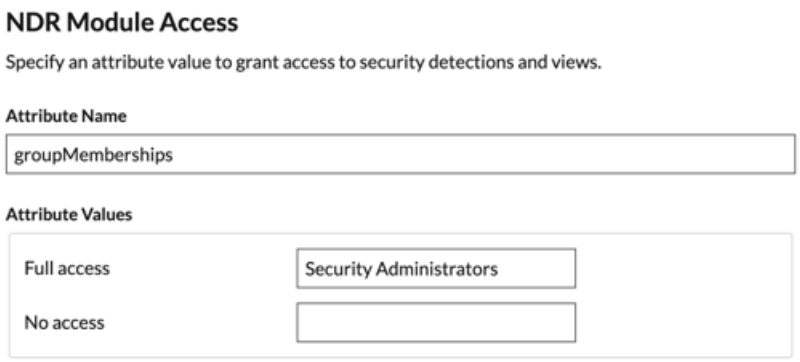
5. Ouvrez le `certificate.pem` dans un éditeur de texte, copiez les données du certificat et collez-les dans le Certificat public champ sur le système ExtraHop.
6. Choisissez la manière dont vous souhaitez approvisionner les utilisateurs à partir de l'une des options suivantes.
   - Sélectionnez Provisionner automatiquement les 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 les nouveaux utilisateurs distants via les paramètres d'administration ExtraHop ou l'API REST.
7. Le **Activer ce fournisseur d'identité** L'option 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 de privilèges utilisateur. Vous devez configurer l'ensemble d'attributs utilisateur suivant avant que les utilisateurs puissent se connecter au système ExtraHop via un fournisseur d' identité. Les valeurs peuvent être définies par l'utilisateur ; elles doivent toutefois correspondre aux noms d'attributs inclus dans la réponse SAML de votre fournisseur d'identité. Les valeurs ne distinguent pas les majuscules et minuscules 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.

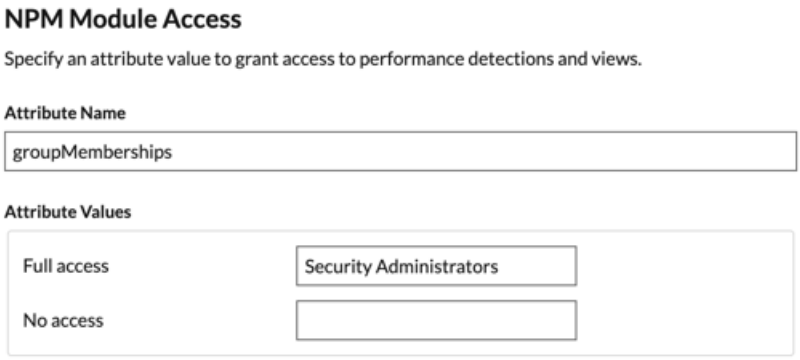
   Dans l'exemple ci-dessous, le Nom de l'attribut le champ est l'attribut de groupe configuré lors de la création de l'application ExtraHop sur le fournisseur d'identité et le Valeurs d'attribut sont les noms de vos groupes d'utilisateurs. Si un utilisateur est membre de plusieurs groupes, il bénéficie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



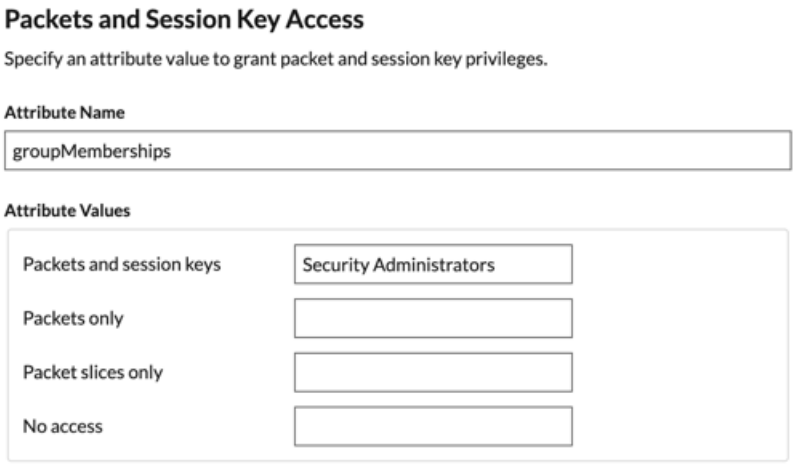
9. Configurez l'accès au module NDR.



10. Configurez 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 si vous avez un stockage des paquets connecté.



12. Cliquez **Enregistrer**.
13. Enregistrez la configuration en cours.

Connectez-vous au système ExtraHop

1. Connectez-vous au système ExtraHop via `https://<extrahop-hostname-or-IP-address>`.
2. Cliquez **Connectez-vous avec** *<provider name>*.
3. Connectez-vous à votre fournisseur à l'aide de votre adresse e-mail et de votre mot de passe. Vous êtes automatiquement dirigé vers la page d'aperçu d'ExtraHop.