Gérer les paramètres d'authentification SAML

Active IQ Unified Manager

NetApp
October 15, 2025

Sommaire

Gérer les paramètres d'authentification SAML

Après avoir configuré les paramètres d'authentification à distance, vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web d'Unified Manager.

Notez que seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance.

Exigences relatives aux fournisseurs d'identité

Lors de la configuration d'Unified Manager pour utiliser un fournisseur d'identité (IdP) pour effectuer l'authentification SAML pour tous les utilisateurs distants, vous devez connaître certains paramètres de configuration requis pour que la connexion à Unified Manager réussisse.

Vous devez saisir l'URI et les métadonnées d'Unified Manager dans le serveur IdP. Vous pouvez copier ces informations à partir de la page d'authentification SAML d'Unified Manager. Unified Manager est considéré comme le fournisseur de services (SP) dans la norme Security Assertion Markup Language (SAML).

Normes de cryptage prises en charge

- Norme de chiffrement avancée (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Fournisseurs d'identité validés

- Schibboleth
- Services de fédération Active Directory (ADFS)

Exigences de configuration ADFS

- Vous devez définir trois règles de réclamation dans l'ordre suivant qui sont requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée d'approbation de partie de confiance.

Règle de réclamation	Valeur
nom-du-compte-SAM	Nom d'identification
nom-du-compte-SAM	urn:oid:0.9.2342.19200300.100.1.1
Groupes de jetons – Nom non qualifié	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- Vous devez définir la méthode d'authentification sur « Authentification par formulaire » sinon les utilisateurs risquent de recevoir une erreur lors de la déconnexion d'Unified Manager. Suivez ces étapes :

a. Ouvrez la console de gestion ADFS.

b. Cliquez sur le dossier Stratégies d'authentification dans l'arborescence de gauche.

c. Sous Actions sur la droite, cliquez sur Modifier la politique d'authentification principale globale.

d. Définissez la méthode d'authentification intranet sur « Authentification par formulaire » au lieu de la valeur par défaut « Authentification Windows ».

- Dans certains cas, la connexion via l'IdP est rejetée lorsque le certificat de sécurité Unified Manager est signé par une autorité de certification. Il existe deux solutions de contournement pour résoudre ce problème :
  - Suivez les instructions identifiées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour la partie de confiance associée au certificat CA chaîné :

    "Désactiver la vérification de révocation par approbation de partie de confiance"

  - Demandez au serveur CA de résider dans le serveur ADFS pour signer la demande de certificat du serveur Unified Manager.

Autres exigences de configuration

- Le décalage de l'horloge d'Unified Manager est défini sur 5 minutes, de sorte que la différence de temps entre le serveur IdP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

Activer l'authentification SAML

Vous pouvez activer l'authentification SAML (Security Assertion Markup Language) afin que les utilisateurs distants soient authentifiés par un fournisseur d'identité sécurisé (IdP) avant de pouvoir accéder à l'interface utilisateur Web d'Unified Manager.

Avant de commencer

- Vous devez avoir configuré l'authentification à distance et vérifié qu'elle réussit.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle d'administrateur d'application.
- Le fournisseur d'identité (IdP) doit être pris en charge par Unified Manager et il doit être configuré.
- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès au serveur IdP.

Une fois l'authentification SAML activée à partir d'Unified Manager, les utilisateurs ne peuvent pas accéder à l'interface utilisateur graphique tant que l'IdP n'a pas été configuré avec les informations de l'hôte du serveur Unified Manager. Vous devez donc être prêt à terminer les deux parties de la connexion avant de commencer le processus de configuration. L'IdP peut être configuré avant ou après la configuration d'Unified Manager.

Seuls les utilisateurs distants auront accès à l'interface utilisateur graphique d'Unified Manager une fois l'authentification SAML activée. Les utilisateurs locaux et les utilisateurs de maintenance ne pourront pas accéder à l'interface utilisateur. Cette configuration n'a pas d'impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.

Unified Manager redémarre automatiquement une fois la configuration SAML terminée sur cette page.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Cochez la case **Activer l'authentification SAML**.

   Les champs requis pour configurer la connexion IdP s'affichent.

3. Saisissez l'URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager au serveur IdP.

   Si le serveur IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URI IdP pour remplir automatiquement le champ Métadonnées IdP.

4. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans un fichier texte XML.

   Vous pouvez configurer le serveur IdP avec ces informations à ce stade.

5. Cliquez sur **Enregistrer**.

   Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

6. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants autorisés tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification sur la page de connexion IdP au lieu de la page de connexion d'Unified Manager.

Si ce n'est pas déjà fait, accédez à votre IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.

Lorsque vous utilisez ADFS comme fournisseur d'identité, l'interface utilisateur graphique d'Unified Manager ne respecte pas le délai d'expiration ADFS et continue de fonctionner jusqu'à ce que le délai d'expiration de la session Unified Manager soit atteint. Vous pouvez modifier le délai d'expiration de la session de l'interface graphique en cliquant sur **Général** > **Paramètres des fonctionnalités** > **Délai d'inactivité**.

Modifier le fournisseur d'identité utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identité (IdP) qu'Unified Manager utilise pour authentifier les utilisateurs distants.

Avant de commencer

- Vous devez disposer de l'URL et des métadonnées de l'IdP.
- Vous devez avoir accès à l'IdP.

Le nouvel IdP peut être configuré avant ou après la configuration d'Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Saisissez le nouvel URI IdP et les métadonnées IdP requises pour connecter le serveur Unified Manager à l'IdP.

   Si l'IdP est accessible directement depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** après avoir saisi l'URL de l'IdP pour remplir automatiquement le champ Métadonnées IdP.

3. Copiez l'URI des métadonnées d'Unified Manager ou enregistrez les métadonnées dans un fichier texte XML.
4. Cliquez sur **Enregistrer la configuration**.

   Une boîte de message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouvel IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.

La prochaine fois que les utilisateurs distants autorisés tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la nouvelle page de connexion IdP au lieu de l'ancienne page de connexion IdP.

Mettre à jour les paramètres d'authentification SAML après la modification du certificat de sécurité d'Unified Manager

Toute modification du certificat de sécurité HTTPS installé sur le serveur Unified Manager nécessite la mise à jour des paramètres de configuration de l'authentification SAML. Le certificat est mis à jour si vous renommez le système hôte, attribuez une nouvelle adresse IP au système hôte ou modifiez manuellement le certificat de sécurité du système.

Une fois le certificat de sécurité modifié et le serveur Unified Manager redémarré, l'authentification SAML ne fonctionnera pas et les utilisateurs ne pourront pas accéder à l'interface graphique d'Unified Manager. Vous devez mettre à jour les paramètres d'authentification SAML sur le serveur IdP et sur le serveur Unified Manager pour réactiver l'accès à l'interface utilisateur.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Lancez l'interface utilisateur d'Unified Manager à l'aide du nom de domaine complet ou de l'adresse IP mis à jour, acceptez le certificat de serveur mis à jour dans votre navigateur et connectez-vous à l'aide des informations d'identification de l'utilisateur de maintenance.
4. Dans la page **Configuration/Authentification**, sélectionnez l'onglet **Authentification SAML** et configurez la connexion IdP.
5. Copiez l'URI des métadonnées de l'hôte Unified Manager ou enregistrez les métadonnées de l'hôte dans

un fichier texte XML.

6. Cliquez sur **Enregistrer**.

   Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

7. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.
8. Accédez à votre serveur IdP et saisissez l'URI et les métadonnées du serveur Unified Manager pour terminer la configuration.

Fournisseur d'identité	Étapes de configuration
ADFS	a. Supprimez l'entrée de confiance de la partie de confiance existante dans l'interface graphique de gestion ADFS. b. Ajoutez une nouvelle entrée de confiance de partie de confiance à l'aide de la `saml_sp_metadata.xml` à partir du serveur Unified Manager mis à jour. c. Définissez les trois règles de réclamation requises pour qu'Unified Manager analyse les réponses SAML ADFS pour cette entrée de confiance de partie de confiance. d. Redémarrez le service Windows ADFS.
Schibboleth	a. Mettez à jour le nouveau FQDN du serveur Unified Manager dans le `attribute-filter.xml` et `relying-party.xml` fichiers. b. Redémarrez le serveur Web Apache Tomcat et attendez que le port 8005 soit en ligne.

9. Connectez-vous à Unified Manager et vérifiez que l'authentification SAML fonctionne comme prévu via votre IdP.

Désactiver l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs distants via un fournisseur d'identité sécurisé (IdP) avant qu'ils puissent se connecter à l'interface utilisateur Web d'Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, effectuent l'authentification de connexion.

Après avoir désactivé l'authentification SAML, les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à l'aide de la console de maintenance Unified Manager si vous n'avez pas accès à l'interface utilisateur graphique.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **Général** > **Authentification SAML**.
2. Décochez la case **Activer l'authentification SAML**.
3. Cliquez sur **Enregistrer**.

   Une boîte de message s'affiche pour confirmer que vous souhaitez terminer la configuration et redémarrer Unified Manager.

4. Cliquez sur **Confirmer et se déconnecter** et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'Unified Manager au lieu de la page de connexion IdP.

Accédez à votre IdP et supprimez l'URI et les métadonnées du serveur Unified Manager.

Désactiver l'authentification SAML depuis la console de maintenance

Vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance lorsqu'il n'y a pas d'accès à l'interface graphique utilisateur d'Unified Manager. Cela peut se produire en cas de mauvaise configuration ou si l'IdP n'est pas accessible.

Avant de commencer

Vous devez avoir accès à la console de maintenance en tant qu'utilisateur de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, effectuent l'authentification de connexion. Les utilisateurs locaux et les utilisateurs de maintenance pourront accéder à l'interface utilisateur graphique en plus des utilisateurs distants configurés.

Vous pouvez également désactiver l'authentification SAML à partir de la page Configuration/Authentification de l'interface utilisateur.

Unified Manager redémarre automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, saisissez le numéro de l'option **Désactiver l'authentification SAML**.

   Un message s'affiche pour confirmer que vous souhaitez désactiver l'authentification SAML et redémarrer Unified Manager.

3. Tapez **y**, puis appuyez sur Entrée et Unified Manager redémarre.

La prochaine fois que les utilisateurs distants tenteront d'accéder à l'interface graphique d'Unified Manager, ils saisiront leurs informations d'identification dans la page de connexion d'Unified Manager au lieu de la page de

connexion IdP.

Si nécessaire, accédez à votre IdP et supprimez l'URL et les métadonnées du serveur Unified Manager.

Page d'authentification SAML

Vous pouvez utiliser la page Authentification SAML pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identité sécurisé (IdP) avant de pouvoir se connecter à l'interface utilisateur Web d'Unified Manager.

- Vous devez disposer du rôle d'administrateur d'application pour créer ou modifier la configuration SAML.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez sélectionner la case à cocher Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IdP**

  L'URI pour accéder à l'IdP à partir du serveur Unified Manager. Des exemples d'URI sont répertoriés ci-dessous.

  Exemple d'URI ADFS :

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  Exemple d'URI Shibboleth :

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Métadonnées IdP**

  Les métadonnées IdP au format XML.

  Si l'URL IdP est accessible depuis le serveur Unified Manager, vous pouvez cliquer sur le bouton **Récupérer les métadonnées IdP** pour remplir ce champ.

- **Système hôte (FQDN)**

  Le nom de domaine complet du système hôte Unified Manager tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI de l'hôte**

  L'URI pour accéder au système hôte Unified Manager à partir de l'IdP.

- **Métadonnées de l'hôte**

  Les métadonnées du système hôte au format XML.

Informations sur le copyright

Informations sur les marques commerciales