Gestion des paramètres d'authentification SAML

Active IQ Unified Manager 9.11

NetApp
October 16, 2025

Sommaire

Gestion des paramètres d'authentification SAML

Une fois que vous avez configuré les paramètres d'authentification à distance, vous pouvez activer l'authentification SAML afin que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant d'accéder à l'interface utilisateur Web Unified Manager.

Notez que seuls les utilisateurs distants ont accès à l'interface utilisateur graphique 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 aucun impact sur les utilisateurs qui accèdent à la console de maintenance.

Exigences du fournisseur d'identités

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

Vous devez entrer l'URI Unified Manager et les métadonnées dans le serveur IDP. Vous pouvez copier ces informations à partir de la page Unified ManagerSAML Authentication. Unified Manager est considéré comme le fournisseur de services dans la norme SAML.

Normes de chiffrement prises en charge

- Advanced Encryption Standard (AES) : AES-128 et AES-256
- Algorithme de hachage sécurisé (SHA) : SHA-1 et SHA-256

Des fournisseurs d'identité validés

- Hurlent
- ADFS (Active Directory Federation Services)

Configuration requise pour ADFS

- Vous devez définir trois règles de sinistre dans l'ordre suivant qui sont nécessaires à Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance.

Règle de réclamation	Valeur
SAM-account-name	ID nom
SAM-account-name	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 des formulaires » pour que les utilisateurs puissent recevoir une erreur lors de la déconnexion d'Unified Manager . Voici la procédure à

suivre :

a. Ouvrez la console de gestion ADFS.

b. Cliquez sur le dossier Authentication Policies dans l'arborescence de gauche.

c. Sous actions à droite, cliquez sur Modifier la stratégie d'authentification principale globale.

d. Définissez la méthode d'authentification Intranet sur « authentification des formulaires » au lieu de « authentification Windows » par défaut.

- Dans certains cas, la connexion via le PDI est rejetée lorsque le certificat de sécurité Unified Manager est signé avec une autorité de certification. Il existe deux solutions pour résoudre ce problème :
  - Suivez les instructions indiquées dans le lien pour désactiver la vérification de révocation sur le serveur ADFS pour les certificats CA chaînés associés à la partie de confiance :

    "Désactiver le contrôle de révocation par confiance de la partie utilisatrices"

  - Demandez au serveur CA de se trouver dans le serveur ADFS pour signer la demande d'autorisation de serveur Unified Manager.

Autres exigences de configuration

- L'inclinaison de l'horloge de Unified Manager est définie sur 5 minutes, la différence de temps entre le serveur IDP et le serveur Unified Manager ne peut pas dépasser 5 minutes, sinon l'authentification échouera.

Activation de l'authentification SAML

Vous pouvez activer l'authentification SAML (Security assertion Markup Language) pour que les utilisateurs distants soient authentifiés par un fournisseur d'identités sécurisé avant d'accéder à l'interface utilisateur Web d'Unified Manager.

Ce dont vous aurez besoin

- Vous devez avoir configuré l'authentification à distance et vérifié qu'elle a réussi.
- Vous devez avoir créé au moins un utilisateur distant ou un groupe distant avec le rôle Administrateur d'applications.
- Le fournisseur d'identités doit être pris en charge par Unified Manager et doit être configuré.
- Vous devez disposer de l'URL IDP et des métadonnées.
- 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 le IDP n'a pas été configuré avec les informations d'hôte du serveur Unified Manager. Vous devez donc être prêt à effectuer les deux parties de la connexion avant de lancer le processus de configuration. Le IDP peut être configuré avant ou après la configuration de Unified Manager.

Seuls les utilisateurs distants ont accès à l'interface utilisateur graphique 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 aucun impact sur les utilisateurs qui accèdent à la console de maintenance, aux commandes Unified Manager ou aux ZAPI.

Unified Manager est redémarré automatiquement après la configuration SAML de 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 sont affichés.

3. Entrez l'URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified Manager au serveur IDP.

   Si le serveur IDP est accessible directement à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **Fetch IDP Metadata** après avoir saisi l'URI IDP pour remplir automatiquement le champ IDP Metadata.

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 pour le moment.

5. Cliquez sur **Enregistrer**.

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

6. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants autorisés saisissent leurs identifiants sur la page de connexion du fournisseur intégré au lieu de la page de connexion de Unified Manager.

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

> Lorsque vous utilisez ADFS en tant que fournisseur d'identité, l'interface graphique Unified Manager ne respecte pas le délai d'attente de l'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 de fonction** > **délai d'inactivité**.

Modification du fournisseur d'identités utilisé pour l'authentification SAML

Vous pouvez modifier le fournisseur d'identités utilisé par Unified Manager pour authentifier les utilisateurs distants.

Ce dont vous aurez besoin

- Vous devez disposer de l'URL IDP et des métadonnées.
- Vous devez avoir accès au PDI.

Le nouveau IDP peut être configuré avant ou après avoir configuré Unified Manager.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **authentification SAML**.
2. Entrez le nouveau URI du IDP et les métadonnées IDP requises pour connecter le serveur Unified Manager au IDP.

   Si l'IDP est accessible directement à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** après avoir saisi l'URL IDP pour remplir automatiquement le champ métadonnées IDP.

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

   Un message s'affiche pour confirmer que vous souhaitez modifier la configuration.

5. Cliquez sur **OK**.

Accédez au nouveau IDP et entrez l'URI du serveur Unified Manager et les métadonnées pour terminer la configuration.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants autorisés saisissent leurs identifiants sur la nouvelle page de connexion IDP au lieu de l'ancienne page de connexion IDP.

Mise à jour des paramètres d'authentification SAML après une modification du certificat de sécurité 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 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**, entrez 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 Unified Manager à l'aide du FQDN 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**.

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

7. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.
8. Accédez à votre serveur IDP, puis entrez l'URI du serveur Unified Manager et les métadonnées 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 la partie de confiance à l'aide du `saml_sp_metadata.xml` À partir du serveur Unified Manager mis à jour. c. Définissez les trois règles de sinistre requises par Unified Manager pour analyser les réponses SAML ADFS pour cette entrée de confiance de tiers de confiance. d. Redémarrez le service Windows ADFS.
Hurlent	a. Mettez à jour le nouveau FQDN du serveur Unified Manager dans `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.

Désactivation de l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs distants via un fournisseur d'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager. Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification.

Une fois l'authentification SAML désactivée, 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 graphique.

Unified Manager est redémarré 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**.

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

4. Cliquez sur **confirmer et Déconnexion** et Unified Manager redémarre.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

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

Désactivation de l'authentification SAML à partir de la console de maintenance

Si vous n'avez pas accès à l'interface graphique Unified Manager, vous devrez peut-être désactiver l'authentification SAML à partir de la console de maintenance. Cela peut se produire en cas de mauvaise configuration ou si le IDP n'est pas accessible.

Ce dont vous aurez besoin

Comme utilisateur de maintenance, vous devez avoir accès à la console de maintenance.

Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés, tels qu'Active Directory ou LDAP, exécutent l'authentification d'identification. 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 est redémarré automatiquement après la désactivation de l'authentification SAML.

Étapes

1. Connectez-vous à la console de maintenance.
2. Dans le **Menu principal**, entrez 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.

Lors de la prochaine tentative d'accès à l'interface graphique Unified Manager, les utilisateurs distants vont

entrer leurs identifiants dans la page de connexion de Unified Manager au lieu de la page de connexion IDP.

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

Page 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'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager.

- Vous devez avoir le rôle Administrateur d'applications 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 cocher la case Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IDP**

  URI permettant d'accéder au IDP à partir du serveur Unified Manager. Les exemples d'URI sont répertoriés ci-dessous.

  Exemple d'URI ADFS :

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

  Exemple d'URI :

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

- **Métadonnées IDP**

  Les métadonnées IDP au format XML.

  Si l'URL IDP est accessible à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** pour remplir ce champ.

- **Système hôte (FQDN)**

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

- **URI hôte**

  URI permettant d'accéder au système hôte Unified Manager à partir du IDP.

- **Métadonnées hôte**

  Métadonnées du système hôte au format XML.

Informations sur le copyright

Informations sur les marques commerciales