



Utilisez SAML

SANtricity 11.7

NetApp
February 12, 2024

Sommaire

- Utilisez SAML 1
 - Configurer SAML 1
 - Modifier les mappages de rôles SAML 6
 - Exporter les fichiers SAML Service Provider 7

Utilisez SAML

Configurer SAML

Pour configurer l'authentification pour Access Management, vous pouvez utiliser les fonctionnalités SAML (Security assertion Markup Language) intégrées à la matrice de stockage. Cette configuration établit une connexion entre un fournisseur d'identité et le fournisseur de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Vous devez connaître l'adresse IP ou le nom de domaine de chaque contrôleur de la matrice de stockage.
- Un administrateur IDP a configuré un système IDP.
- Un administrateur IDP s'est assuré que le IDP prend en charge la possibilité de renvoyer un ID de nom lors de l'authentification.
- Un administrateur s'est assuré que les horloges du serveur IDP et du contrôleur sont synchronisées (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé depuis le système IDP et disponible sur le système local utilisé pour accéder à System Manager.

Description de la tâche

Un fournisseur d'identité (IDP) est un système externe utilisé pour demander des informations d'identification à un utilisateur et déterminer si cet utilisateur est correctement authentifié. Le IDP peut être configuré pour fournir une authentification multifacteur et utiliser n'importe quelle base de données utilisateur, telle qu'Active Directory. Votre équipe de sécurité est responsable du maintien du PDI. Un SP (Service Provider) est un système qui contrôle l'authentification des utilisateurs et l'accès. Lorsque Access Management est configuré avec SAML, la baie de stockage agit comme fournisseur de services pour demander l'authentification auprès du fournisseur d'identités. Pour établir une connexion entre le IDP et la matrice de stockage, vous partagez les fichiers de métadonnées entre ces deux entités. Ensuite, vous associez les entités utilisateur IDP aux rôles de baie de stockage. Enfin, vous testez la connexion et les connexions SSO avant d'activer SAML.



SAML et les services d'annuaire. Si vous activez SAML lorsque Directory Services est configuré en tant que méthode d'authentification, SAML remplace Directory Services dans System Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.



Modification et désactivation. une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

La configuration de l'authentification SAML est une procédure en plusieurs étapes.

Étape 1 : téléchargez le fichier de métadonnées IDP

Pour fournir à la baie de stockage des informations de connexion IDP, vous importez ces métadonnées dans System Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues. Il vous suffit de charger un seul fichier de

métadonnées pour la baie de stockage, même s'il existe deux contrôleurs.

Étapes

1. Sélectionnez **Paramètres > gestion des accès**.
2. Sélectionnez l'onglet **SAML**.

La page affiche un aperçu des étapes de configuration.

3. Cliquez sur le lien **Import Identity Provider (IDP) file**.

La boîte de dialogue Importer le fichier du fournisseur d'identités s'ouvre.

4. Cliquez sur **Parcourir** pour sélectionner et télécharger le fichier de métadonnées IDP que vous avez copié sur votre système local.

Une fois le fichier sélectionné, l'ID entité IDP s'affiche.

5. Cliquez sur **Importer**.

Étape 2 : exporter les fichiers du fournisseur de services

Pour établir une relation de confiance entre le fournisseur de services intégré et la baie de stockage, vous importez les métadonnées du fournisseur de services dans le fournisseur de services intégré. Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'autorisation. Le fichier contient des informations telles que le nom de domaine du contrôleur ou l'adresse IP, afin que le IDP puisse communiquer avec les fournisseurs de services.

Étapes

1. Cliquez sur le lien **Exporter les fichiers du fournisseur de services**.

La boîte de dialogue Exporter les fichiers du fournisseur de services s'ouvre.

2. Entrez l'adresse IP du contrôleur ou le nom DNS dans le champ **Controller A**, puis cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local. Si la matrice de stockage comprend deux contrôleurs, répétez cette étape pour le second contrôleur dans le champ **Controller B**.

Après avoir cliqué sur **Exporter**, les métadonnées du fournisseur de services sont téléchargées sur votre système local. Notez l'emplacement de stockage du fichier.

3. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

Il existe un fichier au format XML pour chaque contrôleur.

4. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur à partir des fichiers.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l'autorisation et l'accès à System Manager, vous devez mapper les attributs d'utilisateur du fournisseur intégré et les membres de groupes aux rôles prédéfinis de la baie de stockage.

Avant de commencer

- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Cliquez sur le lien pour les rôles **Mapping System Manager**.

La boîte de dialogue Role Mapping s'ouvre.

2. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper. Les expressions régulières sont prises en charge. Ces caractères spéciaux d'expression régulière doivent être échappés avec une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière: \.[]{}()<>*+.=!/?^\$	
Rôles	<p>Cliquez dans le champ et sélectionnez l'un des rôles de la matrice de stockage à mapper à l'attribut. Vous devez sélectionner individuellement chaque rôle à inclure. Le rôle Monitor est requis en combinaison avec les autres rôles pour se connecter à System Manager. Le rôle d'administrateur de sécurité est également requis pour au moins un groupe.</p> <p>Les rôles mappés incluent les autorisations suivantes :</p> <ul style="list-style-type: none">• Storage admin — accès en lecture/écriture complet aux objets de stockage (par exemple, volumes et pools de disques), mais pas d'accès à la configuration de sécurité.• Security admin — accès à la configuration de sécurité dans Access Management, gestion des certificats, gestion du journal d'audit et possibilité d'activer ou de désactiver l'interface de gestion héritée (symbole).• Support admin — accès à toutes les ressources matérielles de la baie de stockage, aux données de panne, aux événements MEL et aux mises à niveau du micrologiciel du contrôleur. Aucun accès aux objets de stockage ou à la configuration de sécurité.• Monitor — accès en lecture seule à tous les objets de stockage, mais pas d'accès à la configuration de sécurité.



Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

3. Si vous le souhaitez, cliquez sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.



Les mappages de rôles peuvent être modifiés après l'activation de SAML.

4. Lorsque vous avez terminé les mappages, cliquez sur **Enregistrer**.

Étape 4 : testez la connexion SSO

Pour vous assurer que le système IDP et la matrice de stockage peuvent communiquer, vous pouvez éventuellement tester une connexion SSO. Ce test est également effectué au cours de la dernière étape de l'activation de SAML.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

Étapes

1. Sélectionnez le lien **Test SSO Login**.

Une boîte de dialogue s'ouvre pour saisir les informations d'identification SSO.

2. Saisissez les informations d'identification d'un utilisateur disposant des autorisations d'administrateur de sécurité et de contrôle.

Une boîte de dialogue s'ouvre pendant que le système teste la connexion.

3. Recherchez un message Test réussi. Si le test s'exécute correctement, passez à l'étape suivante pour l'activation de SAML.

Si le test ne s'effectue pas correctement, un message d'erreur s'affiche avec des informations supplémentaires. Assurez-vous que :

- L'utilisateur appartient à un groupe avec des autorisations pour Security Admin et Monitor.
- Les métadonnées que vous avez téléchargées pour le serveur IDP sont correctes.
- Les adresses de contrôleur dans les fichiers de métadonnées du processeur de service sont correctes.

Étape 5 : activer SAML

La dernière étape consiste à terminer la configuration SAML pour l'authentification des utilisateurs. Au cours de ce processus, le système vous demande également de tester une connexion SSO. Le processus de test de connexion SSO est décrit à l'étape précédente.

Avant de commencer

- Le fichier de métadonnées IDP est importé dans System Manager.
- Un fichier de métadonnées Service Provider pour chaque contrôleur est importé dans le système IDP pour la relation de confiance.

- Au moins un mappage de rôle moniteur et administrateur de sécurité est configuré.



Modification et désactivation. une fois le langage SAML activé, vous *ne pouvez pas* le désactiver via l'interface utilisateur, ni modifier les paramètres IDP. Si vous devez désactiver ou modifier la configuration SAML, contactez le support technique pour obtenir de l'aide.

Étapes

1. Dans l'onglet **SAML**, sélectionnez le lien **Activer SAML**.

La boîte de dialogue confirmer l'activation de SAML s'ouvre.

2. Type `enable`, Puis cliquez sur **Activer**.
3. Saisissez les informations d'identification de l'utilisateur pour un test de connexion SSO.

Résultats

Une fois que le système active SAML, il met fin à toutes les sessions actives et commence à authentifier les utilisateurs via SAML.

Modifier les mappages de rôles SAML

Si vous avez déjà configuré SAML pour Access Management, vous pouvez modifier les mappages de rôles entre les groupes IDP et les rôles prédéfinis de la baie de stockage.

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- Un administrateur IDP a configuré les attributs utilisateur et l'appartenance au groupe dans le système IDP.
- SAML est configuré et activé.

Étapes

1. Sélectionnez **Paramètres > gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **mappage de rôles**.

La boîte de dialogue Role Mapping s'ouvre.

4. Attribuez des attributs utilisateur IDP et des groupes aux rôles prédéfinis. Un groupe peut avoir plusieurs rôles attribués.



Veillez à ne pas supprimer vos autorisations lorsque le langage SAML est activé, ou vous perdez l'accès à System Manager.

Détails du champ

Réglage	Description
Mappages	Attribut utilisateur
Spécifiez l'attribut (par exemple, « membre de ») pour le groupe SAML à mapper.	Valeur d'attribut
Spécifiez la valeur d'attribut du groupe à mapper.	Rôles



Le rôle Monitor est requis pour tous les utilisateurs, y compris l'administrateur. System Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor présent.

- Vous pouvez également cliquer sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
- Cliquez sur **Enregistrer**.

Résultats

Une fois cette tâche terminée, toutes les sessions utilisateur actives sont arrêtées. Seule votre session utilisateur actuelle est conservée.

Exporter les fichiers SAML Service Provider

Si nécessaire, vous pouvez exporter les métadonnées du Service Provider pour la matrice de stockage et réimporter le(s) fichier(s) dans le système IDP (Identity Provider).

Avant de commencer

- Vous devez être connecté avec un profil utilisateur qui inclut les autorisations d'administrateur de sécurité. Dans le cas contraire, les fonctions de gestion des accès ne s'affichent pas.
- SAML est configuré et activé.

Description de la tâche

Dans cette tâche, vous exportez les métadonnées des contrôleurs (un fichier par contrôleur). Le PDI a besoin de ces métadonnées pour établir une relation de confiance avec les contrôleurs et traiter les demandes d'authentification. Le fichier inclut des informations telles que le nom de domaine du contrôleur ou l'adresse IP que le IDP peut utiliser pour envoyer des demandes.

Étapes

- Sélectionnez **Paramètres > gestion des accès**.
- Sélectionnez l'onglet **SAML**.
- Sélectionnez **Exporter**.

La boîte de dialogue Exporter les fichiers du fournisseur de services s'ouvre.

4. Pour chaque contrôleur, cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.



Les champs de nom de domaine de chaque contrôleur sont en lecture seule.

Notez l'emplacement de stockage du fichier.

5. À partir du système local, recherchez le ou les fichiers de métadonnées du Service Provider que vous avez exportés.

Il existe un fichier au format XML pour chaque contrôleur.

6. À partir du serveur IDP, importez le ou les fichiers de métadonnées du fournisseur de services. Vous pouvez importer les fichiers directement ou saisir manuellement les informations du contrôleur.

7. Cliquez sur **Fermer**.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.