Utilisez SAML

SANtricity 11.8

NetApp
December 16, 2024

Sommaire

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 du contrôleur dans 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 le serveur IDP et l'horloge du contrôleur sont synchronisés (via un serveur NTP ou en ajustant les paramètres d'horloge du contrôleur).
- Un fichier de métadonnées IDP est téléchargé à partir du système IDP et est disponible sur le système local utilisé pour accéder à Unified 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 les services d'annuaire sont configurés comme méthode d'authentification, SAML remplace les services d'annuaire SAML dans Unified Manager. Si vous désactivez SAML ultérieurement, la configuration Directory Services retourne à sa configuration précédente.

Edition 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 les métadonnées IDP dans Unified Manager. Le système IDP a besoin de ces métadonnées pour rediriger les demandes d'authentification vers l'URL correcte et valider les réponses reçues.

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 le contrôleur et pour 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.

   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, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
4. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services pour établir la relation de confiance. Vous pouvez importer le fichier directement ou saisir manuellement les informations du contrôleur à partir du fichier.

Étape 3 : rôles de carte

Pour fournir aux utilisateurs l'autorisation et l'accès à Unified Manager, vous devez mapper les attributs d'utilisateur et les appartenances aux groupes d'un fournisseur d'identités 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 Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le contrôleur est importé dans le système IDP

pour la relation de confiance.

Étapes

1. Cliquez sur le lien **mapping Unified Manager** roles.

   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 par une barre oblique inverse (\) s'ils ne font pas partie d'un modèle d'expression régulière : \.[]{}()<>*+-=!?^$	
Rôles	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 d'autres rôles pour se connecter à Unified Manager. Le rôle d'administrateur de sécurité est également requis pour au moins un groupe. Les rôles mappés incluent les autorisations suivantes : • **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. Unified Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor.

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 Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le 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. Rechercher 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.
   - L'adresse du contrôleur dans les fichiers de métadonnées du processeur de service est correcte.

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 Unified Manager.
- Un fichier de métadonnées de fournisseur de services pour le 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.

> **Edition 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. Tapez `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 SAML est activé, faute de quoi vous perdrez l'accès à Unified 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. Unified Manager ne fonctionnera pas correctement pour un utilisateur sans le rôle Monitor.

5. Vous pouvez également cliquer sur **Ajouter un autre mappage** pour entrer plus de mappages de groupe à rôle.
6. 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 fournisseur de services pour la baie de stockage et réimporter le fichier dans le système du fournisseur d'identités.

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

Cette tâche permet d'exporter des métadonnées à partir du contrôleur. L'IDP a besoin de ces métadonnées pour établir une relation de confiance avec le contrôleur et pour 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

1. Sélectionnez **Paramètres › gestion des accès**.
2. Sélectionnez l'onglet **SAML**.
3. Sélectionnez **Exporter**.

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

4. Cliquez sur **Exporter** pour enregistrer le fichier de métadonnées sur votre système local.

   Le champ du nom de domaine est en lecture seule.

   Notez l’emplacement de stockage du fichier.

5. À partir du système local, localisez le fichier de métadonnées du fournisseur de services au format XML que vous avez exporté.
6. À partir du serveur IDP, importez le fichier de métadonnées du fournisseur de services. Vous pouvez importer le fichier directement ou saisir manuellement les informations relatives au contrôleur.
7. Cliquez sur **Fermer**.