



Configurez l'authentification SAML pour les services Web

ONTAP 9

NetApp
March 22, 2023

Table des matières

- Configurez l'authentification SAML pour les services Web 1
 - Configurez l'authentification SAML 1
 - Désactivez l'authentification SAML 3
 - Résolution des problèmes liés à la configuration SAML 4

Configurez l'authentification SAML pour les services Web

Configurez l'authentification SAML

Depuis ONTAP 9.3, vous pouvez configurer l'authentification SAML pour les services Web. Lorsque l'authentification SAML est configurée et activée, les utilisateurs sont authentifiés par un fournisseur d'identité externe (IDP) au lieu des fournisseurs de services d'annuaire tels qu'Active Directory et LDAP.

Ce dont vous avez besoin

- Vous devez avoir configuré l'IDP pour l'authentification SAML.
- Vous devez avoir l'URI IDP.

Description de la tâche

- L'authentification SAML s'applique uniquement au `http` et `ontapi` en termes de latence.

Le `http` et `ontapi` Les applications sont utilisées par les services web suivants : infrastructure processeur de service, API ONTAP ou System Manager.

- L'authentification SAML est applicable uniquement pour l'accès au SVM d'administration.

Étapes

1. Créez une configuration SAML pour que ONTAP puisse accéder aux métadonnées IDP :

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` Est l'adresse FTP ou HTTP de l'hôte IDP à partir de laquelle les métadonnées IDP peuvent être téléchargées.

`ontap_host_name` Est le nom d'hôte ou l'adresse IP de l'hôte du fournisseur de services SAML, qui, dans le cas présent, correspond au système ONTAP. Par défaut, l'adresse IP de la LIF de cluster-management est utilisée.

Vous pouvez éventuellement fournir les informations de certificat de serveur ONTAP. Par défaut, les informations de certificat de serveur Web ONTAP sont utilisées.

```
cluster_12::> security saml-sp create -idp-uri
https://scspr0235321001.gdl.englab.netapp.com/idp/shibboleth -verify
-metadata-server false
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.63.56.150/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

L'URL permettant d'accéder aux métadonnées de l'hôte ONTAP s'affiche.

2. À partir de l'hôte IDP, configurez le IDP avec les métadonnées de l'hôte ONTAP.

Pour plus d'informations sur la configuration du IDP, reportez-vous à la documentation IDP.

3. Activer la configuration SAML :

```
security saml-sp modify -is-enabled true
```

Tout utilisateur existant qui accède à l' http ou ontapi L'application est automatiquement configurée pour l'authentification SAML.

4. Si vous souhaitez créer des utilisateurs pour le http ou ontapi Application après la configuration de SAML, spécifiez SAML comme méthode d'authentification pour les nouveaux utilisateurs.

- a. Créez une méthode de connexion pour les nouveaux utilisateurs avec l'authentification SAML :

```
security login create -user-or-group-name user_name -application [http |
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1
-application http -authentication-method saml -vserver cluster_12
```

- b. Vérifiez que l'entrée utilisateur est créée :

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

User/Group	Authentication	Authentication	Acct	Second
Name	Application	Method	Role Name	Locked Method
admin	console	password	admin	no none
admin	http	password	admin	no none
admin	http	saml	admin	- none
admin	ontapi	password	admin	no none
admin	ontapi	saml	admin	- none
admin	service-processor	password	admin	no none
admin	ssh	password	admin	no none
admin1	http	password	backup	no none
**admin1	http	saml	backup	-
none**				

Informations associées

["Commandes de ONTAP 9"](#)

Désactivez l'authentification SAML

Vous pouvez désactiver l'authentification SAML lorsque vous souhaitez arrêter l'authentification des utilisateurs Web à l'aide d'un fournisseur d'identité externe (IDP). Lorsque l'authentification SAML est désactivée, les fournisseurs de services d'annuaire configurés tels qu'Active Directory et LDAP sont utilisés pour l'authentification.

Ce dont vous avez besoin

Vous devez être connecté depuis la console.

Étapes

1. Désactiver l'authentification SAML :

```
security saml-sp modify -is-enabled false
```

2. Si vous ne souhaitez plus utiliser l'authentification SAML ou si vous souhaitez modifier l'IDP, supprimez la configuration SAML :

```
security saml-sp delete
```

Résolution des problèmes liés à la configuration SAML

Si la configuration de l'authentification SAML échoue, vous pouvez réparer manuellement chaque nœud sur lequel la configuration SAML a échoué et effectuer une restauration suite à la défaillance. Au cours du processus de réparation, le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

Description de la tâche

Lorsque vous configurez l'authentification SAML, ONTAP applique la configuration SAML par nœud. Lorsque vous activez l'authentification SAML, ONTAP tente automatiquement de réparer chaque nœud en cas de problèmes de configuration. Si la configuration SAML est problématique sur n'importe quel nœud, vous pouvez désactiver l'authentification SAML, puis réactiver l'authentification SAML. Lorsque la configuration SAML ne s'applique pas à un ou plusieurs nœuds, même après la réactivation de l'authentification SAML, cela peut se présenter. Vous pouvez identifier le nœud sur lequel la configuration SAML a échoué, puis réparer manuellement ce nœud.

Étapes

1. Connectez-vous au niveau de privilège avancé :

```
set -privilege advanced
```

2. Identifiez le nœud sur lequel la configuration SAML a échoué :

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

                Node: node1
                Update Status: config-success
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text:
SAML Service Provider Enabled: false
                ID of SAML Config Job: 179

                Node: node2
                Update Status: config-failed
                Database Epoch: 9
                Database Transaction Count: 997
                Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
                ID of SAML Config Job: 180
2 entries were displayed.
```

3. Corrigez la configuration SAML sur le nœud défaillant :

```
security saml-sp repair -node node_name
```

```
cluster_12::~*> security saml-sp repair -node node2
```

```
Warning: This restarts the web server. Any HTTP/S connections that are  
active
```

```
    will be disrupted.
```

```
Do you want to continue? {y|n}: y
```

```
[Job 181] Job is running.
```

```
[Job 181] Job success.
```

Le serveur Web est redémarré et toutes les connexions HTTP ou HTTPS actives sont interrompues.

4. Vérifiez que le langage SAML est configuré sur tous les nœuds :

security saml-sp status show -instance

```
cluster_12::~*> security saml-sp status show -instance
```

```
    Node: node1
```

```
    Update Status: config-success
```

```
    Database Epoch: 9
```

```
    Database Transaction Count: 997
```

```
    Error Text:
```

```
SAML Service Provider Enabled: false
```

```
    ID of SAML Config Job: 179
```

```
    Node: node2
```

```
    Update Status: **config-success**
```

```
    Database Epoch: 9
```

```
    Database Transaction Count: 997
```

```
    Error Text:
```

```
SAML Service Provider Enabled: false
```

```
    ID of SAML Config Job: 180
```

```
2 entries were displayed.
```

Informations sur le copyright

Copyright © 2023 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 DÉLICTELLE (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.