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

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
                                                                  Second
User/Group                 Authentication                 Acct
Authentication
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

Informations sur les marques commerciales