



Configure SAML authentication for web services

ONTAP 9

NetApp
November 12, 2022

Table of Contents

- Configure SAML authentication for web services. 1
 - Configure SAML authentication 1
 - Disable SAML authentication 3
 - Troubleshoot issues with SAML configuration 4

Configure SAML authentication for web services

Configure SAML authentication

Beginning with ONTAP 9.3, you can configure Security Assertion Markup Language (SAML) authentication for web services. When SAML authentication is configured and enabled, users are authenticated by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

What you'll need

- You must have configured the IdP for SAML authentication.
- You must have the IdP URI.

About this task

- SAML authentication applies only to the `http` and `ontapi` applications.

The `http` and `ontapi` applications are used by the following web services: Service Processor Infrastructure, ONTAP APIs, or System Manager.

- SAML authentication is applicable only for accessing the admin SVM.

Steps

1. Create a SAML configuration so that ONTAP can access the IdP metadata:

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

`idp_uri` is the FTP or HTTP address of the IdP host from where the IdP metadata can be downloaded.

`ontap_host_name` is the host name or IP address of the SAML service provider host, which in this case is the ONTAP system. By default, the IP address of the cluster-management LIF is used.

You can optionally provide the ONTAP server certificate information. By default, the ONTAP web server certificate information is used.

```
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.

The URL to access the ONTAP host metadata is displayed.

2. From the IdP host, configure the IdP with the ONTAP host metadata.

For more information about configuring the IdP, see the IdP documentation.

3. Enable SAML configuration:

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

Any existing user that accesses the `http` or `ontapi` application is automatically configured for SAML authentication.

4. If you want to create users for the `http` or `ontapi` application after SAML is configured, specify SAML as the authentication method for the new users.
 - a. Create a login method for new users with SAML authentication: + **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. Verify that the user entry is created:

```
security login show
```

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

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication	Acct
------------	----------------	------

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**					

Related information

[ONTAP 9 Commands](#)

Disable SAML authentication

You can disable SAML authentication when you want to stop authenticating web users by using an external Identity Provider (IdP). When SAML authentication is disabled, the configured directory service providers such as Active Directory and LDAP are used for authentication.

What you'll need

You must be logged in from the console.

Steps

1. Disable SAML authentication:

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

2. If you no longer want to use SAML authentication or if you want to modify the IdP, delete the SAML configuration:

```
security saml-sp delete
```

Troubleshoot issues with SAML configuration

If configuring Security Assertion Markup Language (SAML) authentication fails, you can manually repair each node on which the SAML configuration failed and recover from the failure. During the repair process, the web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

About this task

When you configure SAML authentication, ONTAP applies SAML configuration on a per-node basis. When you enable SAML authentication, ONTAP automatically tries to repair each node if there are configuration issues. If there are issues with SAML configuration on any node, you can disable SAML authentication and then reenabling SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenabling SAML authentication. You can identify the node on which SAML configuration has failed and then manually repair that node.

Steps

1. Log in to the advanced privilege level:

```
set -privilege advanced
```

2. Identify the node on which SAML configuration failed:

```
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. Repair the SAML configuration on the failed node:

```
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.

The web server is restarted and any active HTTP connections or HTTPS connections are disrupted.

4. Verify that SAML is successfully configured on all of the nodes:

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.

Copyright information

Copyright © 2022 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.