# Manage access to web services

ONTAP 9

NetApp
August 15, 2023

# Table of Contents

# Manage access to web services

## Manage access to web services overview

A web service is an application that users can access by using HTTP or HTTPS. The cluster administrator can set up the web protocol engine, configure SSL, enable a web service, and enable users of a role to access a web service.

Beginning with ONTAP 9.6, the following web services are supported:

- Service Processor Infrastructure (`spi`)

  This service makes a node's log, core dump, and MIB files available for HTTP or HTTPS access through the cluster management LIF or a node management LIF. The default setting is `enabled`.

  Upon a request to access a node's log files or core dump files, the `spi` web service automatically creates a mount point from a node to another node's root volume where the files reside. You do not need to manually create the mount point. `

- ONTAP APIs (`ontapi`)

  This service enables you to run ONTAP APIs to execute administrative functions with a remote program. The default setting is `enabled`.

  This service might be required for some external management tools. For example, if you use System Manager, you should leave this service enabled.

- Data ONTAP Discovery (`disco`)

  This service enables off-box management applications to discover the cluster in the network. The default setting is `enabled`.

- Support Diagnostics (`supdiag`)

  This service controls access to a privileged environment on the system to assist problem analysis and resolution. The default setting is `disabled`. You should enable this service only when directed by technical support.

- System Manager (`sysmgr`)

  This service controls the availability of System Manager, which is included with ONTAP. The default setting is `enabled`. This service is supported only on the cluster.

- Firmware Baseboard Management Controller (BMC) Update (`FW_BMC`)

  This service enables you to download BMC firmware files. The default setting is `enabled`.

- ONTAP Documentation (`docs`)

  This service provides access to the ONTAP documentation. The default setting is `enabled`.

- ONTAP RESTful APIs (`docs_api`)

  This service provides access to the ONTAP RESTful API documentation. The default setting is `enabled`.

- File Upload and Download (`fud`)

  This service offers file upload and download. The default setting is `enabled`.

- ONTAP Messaging (`ontapmsg`)

  This service supports a publish and subscribe interface allowing you to subscribe to events. The default setting is `enabled`.

- ONTAP Portal (`portal`)

  This service implements the gateway into a virtual server. The default setting is `enabled`.

- ONTAP Restful Interface (`rest`)

  This service supports a RESTful interface that is used to remotely manage all elements of the cluster infrastructure. The default setting is `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

  This service provides resources to support the SAML service provider. The default setting is `enabled`.

- SAML Service Provider (`saml-sp`)

  This service offers services such as SP metadata and the assertion consumer service to the service provider. The default setting is `enabled`.

Beginning with ONTAP 9.7, the following additional services are supported:

- Configuration Backup Files (`backups`)

  This service enables you to download configuration backup files. The default setting is `enabled`.

- ONTAP Security (`security`)

  This service supports CSRF token management for enhanced authentication. The default setting is `enabled`.

# Manage the web protocol engine

You can configure the web protocol engine on the cluster to control whether web access is allowed and what SSL versions can be used. You can also display the configuration settings for the web protocol engine.

You can manage the web protocol engine at the cluster level in the following ways:

- You can specify whether remote clients can use HTTP or HTTPS to access web service content by using

the `system services web modify` command with the `-external` parameter.

- You can specify whether SSLv3 should be used for secure web access by using the `security config modify` command with the `-supported-protocol` parameter.
  By default, SSLv3 is disabled. Transport Layer Security 1.0 (TLSv1.0) is enabled and it can be disabled if needed.
- You can enable Federal Information Processing Standard (FIPS) 140-2 compliance mode for cluster-wide control plane web service interfaces.

  By default, FIPS 140-2 compliance mode is disabled.

  - **When FIPS 140-2 compliance mode is disabled**
    You can enable FIPS 140-2 compliance mode by setting the `is-fips-enabled` parameter to `true` for the `security config modify` command, and then using the `security config show` command to confirm the online status.
  - **When FIPS 140-2 compliance mode is enabled**
    - Beginning in ONTAP 9.11.1, TLSv1, TLSv1.1 and SSLv3 are disabled, and only TSLv1.2 and TSLv1.3 remain enabled. It affects other systems and communications that are internal and external to ONTAP 9. If you enable FIPS 140-2 compliance mode and then subsequently disable, TLSv1, TLSv1.1, and SSLv3 remain disabled. Either TLSv.1 or TLSv1.3 will remain enabled depending on the previous configuration.
    - For versions of ONTAP prior to 9.11.1, both TLSv1 and SSLv3 are disabled and only TLSv1.1 and TLSv1.2 remain enabled. ONTAP prevents you from enabling both TLSv1 and SSLv3 when FIPS 140-2 compliance mode is enabled. If you enable FIPS 140-2 compliance mode and then subsequently disable it, TLSv1 and SSLv3 remain disabled, but either TLSv1.2 or both TLSv1.1 and TLSv1.2 are enabled depending on the previous configuration.
- You can display the configuration of cluster-wide security by using the `system security config show` command.

If the firewall is enabled, the firewall policy for the logical interface (LIF) to be used for web services must be set up to allow HTTP or HTTPS access.

If you use HTTPS for web service access, SSL for the cluster or storage virtual machine (SVM) that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

In MetroCluster configurations, the setting changes you make for the web protocol engine on a cluster are not replicated on the partner cluster.

# Commands for managing the web protocol engine

You use the `system services web` commands to manage the web protocol engine. You use the `system services firewall policy create` and `network interface modify` commands to allow web access requests to go through the firewall.

| If you want to… | Use this command… |
| --- | --- |
| Configure the web protocol engine at the cluster level:<br>• Enable or disable the web protocol engine for the cluster<br>• Enable or disable SSLv3 for the cluster<br>• Enable or disable FIPS 140-2 compliance for secure web services (HTTPS) | `system services web modify` |
| Display the configuration of the web protocol engine at the cluster level, determine whether the web protocols are functional throughout the cluster, and display whether FIPS 140-2 compliance is enabled and online | `system services web show` |
| Display the configuration of the web protocol engine at the node level and the activity of web service handling for the nodes in the cluster | `system services web node show` |
| Create a firewall policy or add HTTP or HTTPS protocol service to an existing firewall policy to allow web access requests to go through firewall | `system services firewall policy create`<br><br>Setting the `-service` parameter to `http` or `https` enables web access requests to go through firewall. |
| Associate a firewall policy with a LIF | `network interface modify`<br><br>You can use the `-firewall-policy` parameter to modify the firewall policy of a LIF. |

# 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
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**
```

**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 reenable SAML authentication. There can be situations when SAML configuration fails to apply on one or more nodes even after you reenable 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.
```

# Manage web services

## Manage web services overview

You can enable or disable a web service for the cluster or a storage virtual machine (SVM), display the settings for web services, and control whether users of a role can access a web service.

You can manage web services for the cluster or an SVM in the following ways:

- Enabling or disabling a specific web service
- Specifying whether access to a web service is restricted to only encrypted HTTP (SSL)
- Displaying the availability of web services
- Allowing or disallowing users of a role to access a web service
- Displaying the roles that are permitted to access a web service

For a user to access a web service, all of the following conditions must be met:

- The user must be authenticated.

  For instance, a web service might prompt for a user name and password. The user's response must match a valid account.

- The user must be set up with the correct access method.

  Authentication only succeeds for users with the correct access method for the given web service. For the ONTAP API web service (`ontapi`), users must have the `ontapi` access method. For all other web

services, users must have the `http` access method.

> You use the `security login` commands to manage users' access methods and authentication methods.

- The web service must be configured to allow the user's access-control role.

> You use the `vserver services web access` commands to control a role's access to a web service.

If a firewall is enabled, the firewall policy for the LIF to be used for web services must be set up to allow HTTP or HTTPS.

If you use HTTPS for web service access, SSL for the cluster or SVM that offers the web service must also be enabled, and you must provide a digital certificate for the cluster or SVM.

## Commands for managing web services

You use the `vserver services web` commands to manage the availability of web services for the cluster or a storage virtual machine (SVM). You use the `vserver services web access` commands to control a role's access to a web service.

| If you want to… | Use this command… |
|---|---|
| Configure a web service for the cluster or anSVM:<br>• Enable or disable a web service<br>• Specify whether only HTTPS can be used for accessing a web service | `vserver services web modify` |
| Display the configuration and availability of web services for the cluster or anSVM | `vserver services web show` |
| Authorize a role to access a web service on the cluster or anSVM | `vserver services web access create` |
| Display the roles that are authorized to access web services on the cluster or anSVM | `vserver services web access show` |
| Prevent a role from accessing a web service on the cluster or anSVM | `vserver services web access delete` |

**Related information**

ONTAP 9 Commands

## Commands for managing mount points on the nodes

The `spi` web service automatically creates a mount point from one node to another

node's root volume upon a request to access the node's log files or core files. Although you do not need to manually manage mount points, you can do so by using the `system node root-mount` commands.

| If you want to… | Use this command… |
|---|---|
| Manually create a mount point from one node to another node's root volume | `system node root-mount create` Only a single mount point can exist from one node to another. |
| Display existing mount points on the nodes in the cluster, including the time a mount point was created and its current state | `system node root-mount show` |
| Delete a mount point from one node to another node's root volume and force connections to the mount point to close | `system node root-mount delete` |

**Related information**

ONTAP 9 Commands

# Manage SSL

The SSL protocol improves the security of web access by using a digital certificate to establish an encrypted connection between a web server and a browser.

You can manage SSL for the cluster or a storage virtual machine (SVM) in the following ways:

- Enabling SSL
- Generating and installing a digital certificate and associating it with the cluster or SVM
- Displaying the SSL configuration to see whether SSL has been enabled, and, if available, the SSL certificate name
- Setting up firewall policies for the cluster or SVM, so that web access requests can go through
- Defining which SSL versions can be used
- Restricting access to only HTTPS requests for a web service

# Commands for managing SSL

You use the `security ssl` commands to manage the SSL protocol for the cluster ora storage virtual machine (SVM).

| If you want to… | Use this command… |
|---|---|
| Enable SSL for the cluster oranSVM, and associate a digital certificate with it | `security ssl modify` |

| If you want to… | Use this command… |
| --- | --- |
| Display the SSL configuration and certificate name for the cluster oranSVM | `security ssl show` |

# Configure access to web services

Configuring access to web services allows authorized users to use HTTP or HTTPS to access the service content on the cluster or a storage virtual machine (SVM).

**Steps**

1. If a firewall is enabled, ensure that HTTP or HTTPS access is set up in the firewall policy for the LIF that will be used for web services:

   You can check whether a firewall is enabled by using the `system services firewall show` command.

   a. To verify that HTTP or HTTPS is set up in the firewall policy, use the `system services firewall policy show` command.

      You set the `-service` parameter of the `system services firewall policy create` command to `http` or `https` to enable the policy to support web access.

   b. To verify that the firewall policy supporting HTTP or HTTPS is associated with the LIF that provides web services, use the `network interface show` command with the `-firewall-policy` parameter.

      You use the `network interface modify` command with the `-firewall-policy` parameter to put the firewall policy into effect for a LIF.

2. To configure the cluster-level web protocol engine and make web service content accessible, use the `system services web modify` command.
3. If you plan to use secure web services (HTTPS), enable SSL and provide digital certificate information for the cluster or SVM by using the `security ssl modify` command.
4. To enable a web service for the cluster or SVM, use the `vserver services web modify` command.

   You must repeat this step for each service that you want to enable for the cluster or SVM.

5. To authorize a role to access web services on the cluster or SVM, use the `vserver services web access create` command.

   The role that you grant access must already exist. You can display existing roles by using the `security login role show` command or create new roles by using the `security login role create` command.

6. For a role that has been authorized to access a web service, ensure that its users are also configured with the correct access method by checking the output of the `security login show` command.

   To access the ONTAP API web service (`ontapi`), a user must be configured with the `ontapi` access method. To access all other web services, a user must be configured with the `http` access method.

You use the `security login create` command to add an access method for a user.

# Troubleshoot web service access problems

Configuration errors cause web service access problems to occur. You can address the errors by ensuring that the LIF, firewall policy, web protocol engine, web services, digital certificates, and user access authorization are all configured correctly.

The following table helps you identify and address web service configuration errors:

| This access problem… | Occurs because of this configuration error… | To address the error… |
| --- | --- | --- |
| Your web browser returns an `unable to connect` or `failure to establish a connection` error when you try to access a web service. | Your LIF might be configured incorrectly. | Ensure that you can ping the LIF that provides the web service.<br><br>You use the `network ping` command to ping a LIF. For information about network configuration, see the *Network Management Guide*. |
| | Your firewall might be configured incorrectly. | Ensure that a firewall policy is set up to support HTTP or HTTPS and that the policy is assigned to the LIF that provides the web service.<br><br>You use the `system services firewall policy` commands to manage firewall policies. You use the `network interface modify` command with the `-firewall-policy` parameter to associate a policy with a LIF. |
| | Your web protocol engine might be disabled. | Ensure that the web protocol engine is enabled so that web services are accessible.<br><br>You use the `system services web` commands to manage the web protocol engine for the cluster. |

| This access problem… | Occurs because of this configuration error… | To address the error… |
| --- | --- | --- |
| Your web browser returns a `not found` error when you try to access a web service. | The web service might be disabled. | Ensure that each web service that you want to allow access to is enabled individually.<br><br>You use the `vserver services web modify` command to enable a web service for access. |
| The web browser fails to log in to a web service with a user's account name and password. | The user cannot be authenticated, the access method is not correct, or the user is not authorized to access the web service. | Ensure that the user account exists and is configured with the correct access method and authentication method. Also, ensure that the user's role is authorized to access the web service.<br><br>You use the `security login` commands to manage user accounts and their access methods and authentication methods. Accessing the ONTAP API web service requires the `ontapi` access method. Accessing all other web services requires the `http` access method. You use the `vserver services web access` commands to manage a role's access to a web service. |

| This access problem… | Occurs because of this configuration error… | To address the error… |
| --- | --- | --- |
| You connect to your web service with HTTPS, and your web browser indicates that your connection is interrupted. | You might not have SSL enabled on the cluster or storage virtual machine (SVM) that provides the web service. | Ensure that the cluster or SVM has SSL enabled and that the digital certificate is valid.<br><br>You use the `security ssl` commands to manage SSL configuration for HTTP servers and the `security certificate show` command to display digital certificate information. |
| You connect to your web service with HTTPS, and your web browser indicates that the connection is untrusted. | You might be using a self-signed digital certificate. | Ensure that the digital certificate associated with the cluster or SVM is signed by a trusted CA.<br><br>You use the `security certificate generate-csr` command to generate a digital certificate signing request and the `security certificate install` command to install a CA-signed digital certificate. You use the `security ssl` commands to manage the SSL configuration for the cluster or SVM that provides the web service. |

## Copyright information



## Trademark information