



RESTCONF Agent

- [About the RESTCONF Agent, on page 1](#)
- [Guidelines and Limitations, on page 2](#)
- [Configuring the RESTCONF Agent, on page 2](#)
- [Using the RESTCONF Agent, on page 2](#)
- [Troubleshooting the RESTCONF Agent, on page 3](#)

About the RESTCONF Agent

Cisco NX-OS RESTCONF is an HTTP -based protocol for configuring data that are defined in YANG version 1, using datastores defined in NETCONF.

NETCONF defines configuration datastores and a set of Create, Retrieve, Update, and Delete (CRUD) operations that can be used to access these datastores. The YANG language defines the syntax and semantics of datastore content, operational data, protocol operations, and event notifications.

Cisco NX-OS RESTCONF uses HTTP operations to provide CRUD operations on a conceptual datastore containing YANG-defined data. This data is compatible with a server which implements NETCONF datastores.

The RESTCONF protocol supports both XML and JSON payload encodings. User authentication is done through the HTTP Basic Authentication.

The following table shows the Protocol operations that the Cisco NX-OS RESTCONF Agent supports:

RESTCONF	NETCONF Equivalent
OPTIONS	NETCONF: none
HEAD	NETCONF: none
GET	NETCONF: <get-config>, <get>
POST	NETCONF: <edit-config> (operation="create")
PUT	NETCONF: <edit-config> (operation="create/replace")
PATCH	NETCONF: <edit-config> (operation="merge")
DELETE	NETCONF: <edit-config> (operation="delete")

Guidelines and Limitations

The RESTCONF Agent has the following guideline and limitation:

- All Cisco Nexus 3100-V, 3100-XL, and the 3200 platform switches support RESTCONF.

Configuring the RESTConf Agent

The RESTConf Agent does not require any configuration in the configuration file (`/etc/mtx.conf`).

Using the RESTCONF Agent

General Commands

- Configure the following commands to enable HTTP or HTTPS access:

- `feature nxapi`
- `nxapi http port 80`
- `nxapi https port 443`

General Control Commands

You can enable or disable the RESTCONF Agent `[no] feature restconf` command.

Viewing the Agent Status

To view the status of the RESTCONF agent, use the `show feature` command and include the expression `restconf`.

```
switch-1# show feature | grep restconf
restconf                1                enabled
switch-1#
```

Sending a POST Request to the Server Using Curl

```
client-host % curl -X POST -H "Authorization: Basic YWRtaW46Y2lzY28=" -H "Content-Type:
application/yang.data+xml" -d '<always>enabled</always><rtrId>2.2.2.2</rtrId>'
"http://192.0.20.123/restconf/data/Cisco-NX-OS-device:System/bgp-items/inst-items/dm-items/Dm-list=default"
-i
```

```
HTTP/1.1 201 Created
Server: nginx/1.7.10
Date: Tue, 27 Sep 2016 20:25:31 GMT
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: nxapi_auth=admin:147500853169574134
Status: 201 Created
```

```
Location: /System/bgp-items/inst-items/dom-items/Dom-list=default/always/rtrId/
```

Sending a GET Request to the Server Using Curl

```
client-host % curl -X GET -H "Authorization: Basic YWRtaW46Y2lzY28=" -H "Accept:
application/yang.data+xml"
"http://192.0.20.123/restconf/data/Cisco-NX-OS-device:System/bgp-items/inst-items/dom-items/Dom-list?content=config"
-i

HTTP/1.1 200 OK
Server: nginx/1.7.10
Date: Tue, 27 Sep 2016 20:26:03 GMT
Content-Type: application/yang.data+xml
Content-Length: 395
Connection: keep-alive
Set-Cookie: nxapi_auth=admin:147500856185650327
Status: 200 OK

    <Dom-list>
      <name>default</name>
      <always>enabled</always>
      <bestPathIntvl>300</bestPathIntvl>
      <holdIntvl>180</holdIntvl>
      <kaIntvl>60</kaIntvl>
      <maxAsLimit>0</maxAsLimit>
      <pfxPeerTimeout>30</pfxPeerTimeout>
      <pfxPeerWaitTime>90</pfxPeerWaitTime>
      <reConnIntvl>60</reConnIntvl>
      <rtrId>2.2.2.2</rtrId>
    </Dom-list>
client-host %
```

Troubleshooting the RESTCONF Agent

Troubleshooting Connectivity

- Enable the web server by issuing the **feature nxapi** command.
- Ensure that the **nxapi http port 80** command is configured to open up the port for HTTP
- Ensure that the **nxapi https port 443** command is configured to open up the port for HTTPS.
- Ping the management port of the switch to verify that the switch is reachable.

