NETCONF Protocol Configuration Mode Commands

The NETCONF Protocol Configuration Mode is used to configure the ConfD/NETCONF interface (server confd) with the Cisco Network Service Orchestrator (NSO) and Elastic Services Controller (ESC).

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

autosave-config

Automatically saves the current ConfD configuration to a specified URL whenever a change is applied by NSO through the ConfD interface. By default, this command is disabled.

Important

This command is obsolete in StarOS 21.2 and later releases.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
[ no ] autosave-config url
```

no

Disables the autosave configuration.

url

Specifies the URL where the ConfD configuration will be saved as:

```
[file:]{/flash | /usb1 | /hd-raid | /sftp}[/<directory>]/<filename>
```

Usage Guidelines

Use this command to save the current ConfD configuration to a specified URL whenever a change is applied by NSO through the ConfD interface.

Example

The following command specifies a the URL to which the ConfD configuration will be saved:

```
autosave-config /flash/confd.cfg
```

bulkstats

Enables bulkstats collection and reporting via REST interface. By default, this command is disabled.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
[ no ] bulkstats
```

no

Disables bulkstats gathering on ConfD.

Usage Guidelines

Use this command to enable or disable populating ConfD with bulkstats operational data. When enabled, StarOS will send schema information to confdmgr while gathering statistics. Collected bulkstats are stored in the ConfD database for later retrieval over REST interface.

By default, this command is disabled.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command enables population of bulkstats operational data in ConfD:

```
bulkstats
```

The following command disables populating ConfD with bulkstats operational data:

```
no bulkstats
```

confd-user

Associates a username for all CLI operations via NETCONF. The user will be authenticated with verifiable credentials. This username is used for CLI logging purposes only.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
[ no ] confd-user username
```

no

Disables the ConfD administrative username.

username

Specifies the username as an alphanumeric string of 1 through 144 characters.

Usage Guidelines

Use this command to associate a username for all CLI operations via NETCONF.

Important The NETCONF or RESTful session must still be established with verifiable credentials.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command specifies a name to be associated with all NETCONF operations in the CLI logs:

```
confd-user admin4126
```

do show

Executes all **show** commands while in Configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
do show
```

Usage Guidelines

Use this command to run all Exec mode **show** commands while in Configuration mode. It is not necessary to exit the Config mode to run a **show** command.

The pipe character **|** is only available if the command is valid in the Exec mode.

Caution

There are some Exec mode **show** commands which are too resource intensive to run from Config mode. These include: **do show support collection**, **do show support details**, **do show support record** and **do show support summary**. If there is a restriction on a specific **show** command, the following error message is displayed:

```
Failure: Cannot execute 'do show support' command from Config mode.
```

end

Exits the current configuration mode and returns to the Exec mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
end
```

Usage Guidelines

Use this command to return to the Exec mode.

exit

Exits the current mode and returns to the parent configuration mode.

Product

All

Privilege

Security Administrator, Administrator

Syntax Description

```
exit
```

Usage Guidelines

Use this command to return to the parent configuration mode.

kpi

Configures the Key Performance Indicator (KPI) collection interval for Node Selection and Load Balancing (NSLB).

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
kpi seconds
```

kpi *seconds*

Configures the Key Performance Indicator (KPI) collection interval for NSLB. Default: disabled.

seconds is an integer value of 0 (disabled), or 10 through 120 which sets the time interval in seconds for collecting the following KPIs:

- Percentage session cpu usage
- Percentage session memory usage
- Percentage non session cpu usage
- Percentage non session memory usage
- Percentage session usage

Usage Guidelines

Use this command to enable ConfD/REST support for NSLB KPI collection.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command enables KPI collection with the collection interval of 30 seconds:

```
kpi 30
```

The following command disables KPI collection:

```
kpi 0
```

netconf

Configures the NETCONF interface.

Product

All (ASR 5500 and VPC platforms only)

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
netconf { notifications { events level { critical | error | warning |
unusual | info } | snmp } | port port_number }
 no netconf { notifications { events | snmp } |port }
```

no

Restores all the NETCONF parameters to their default values.

notifications events: Disables sending of StarOS events via NETCONF notifications.

notifications snmp: Disables sending of SNMP alerts/alarms via NETCONF notifications.

port: Resets the port number to 830.

notifications events level { critical | error | warning | unusual | info }

When enabled, events logged in StarOS will be sent out as NETCONF notifications on the stream named "StarOS." Level specifies the lowest event severity level that results in a notification. Default: disabled.

- **critical** - Level 1: Reports critical errors contained in log file.
- **error** - Level 2: Reports error notifications contained in log file.
- **warning** - Level 3: Reports warning messages contained in log file.
- **unusual** - Level 4: Reports unexpected errors contained in log file.
- **info** - Level 5: Reports informational messages contained in log file.

Important Any event that is of category "critical-info" (regardless of severity) will also be converted to notifications.

notifications snmp

When enabled, SNMP alerts and alarms will be sent out as NETCONF notifications on the stream named "StarOS_SNMP". Default: disabled.

This configuration setting does not affect the sending of SNMP alarms; if SNMP alarms are configured to be sent to an external server, they will continue to be sent.

The notification will not contain SNMP OIDs but will contain the content used to generate the SNMP alert.

port *port_number*

When **server confd** is enabled, the port is set to the NETCONF default port, 830. This keyword sets the NETCONF interface port number to something other than 830.

port_number must be an integer from 1 through 65535.

Important A change to the NETCONF interface port value will result in a planned restart of ConfD and temporary loss of connectivity over the NETCONF and REST (if enabled) interfaces.

Usage Guidelines Use this command to configure the NETCONF interface parameters.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command will generate NETCONF notifications for StarOS events of severity warning, error, or critical:

```
netconf notifications events warning
```

The following command disables NETCONF notifications for all StarOS events:

```
no netconf notifications events
```

The following command sets the NETCONF interface port number to 500:

```
netconf port 500
```

The following command resets the NETCONF interface port number to 830:

```
no netconf port
```

rest

Configures the REST interface.

Product All (ASR 5500 and VPC platforms only)

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration >NETCONF Protocol Configuration

configure > context local > server confd

Entering the above command sequence results in the following prompt:

```
[local]host_name(config-confd)#
```

Syntax Description

```
rest { auth-policy { none | peer | peer-fail } | certificate certificate_name
 | hostname host_name | port port_number }
no rest [ auth-policy | certificate | hostname | port ]
```

no

Restores all the REST parameters to their default values.

auth-policy: none

certificate: Removes any configured certificate and key. REST will not be operational without a valid certificate and key.

hostname: System name is used and matching of hostname is not mandated.

port: Use the default port, 443.

auth-policy { none | peer | peer-fail }

Controls the level of verification the server does on client certificates. CA (certificate authority) certificates can be configured using the existing **ca-certificate** command in Global Configuration mode.

- **none** - No authentication performed.
- **peer** - If the client does not provide a certificate, or the client provides a certificate and it is valid, the connection is allowed. If the client provides a certificate that is not valid, the connection is aborted.

  Important If **peer** is selected, CA certificates are recommended; otherwise, a client providing a valid certificate cannot be authenticated and connection will fail.

- **peer-fail** - Server requires the client to supply a client certificate and will fail the connection if certificate is not successfully validated.

  Important If **peer-fail** is selected, one or more CA certificates must be present on the device; otherwise, the REST interface will not be enabled.

certificate *certificate_name*

Configures certificate and private-key for REST interface.

certificate_name is an alphanumeric string of 1 to 128 characters.

Important The certificate specified must be present on the device. Certificate and the associated private-key can be configured using the existing **certificate** command in Global Configuration mode.

hostname *host_name*

Specifies a hostname the web server will serve. If configured, mandates the web server to only service requests whose Host field matches the configured hostname.

host_name is an alphanumeric string of 1 to 63 characters.

port *port_number*

Sets the REST interface port number to the specified value.

port_number must be an integer from 1 through 65535.

Usage Guidelines

Use this command to configure the REST interface parameters.

Important Changes to any REST interface parameters may result in a planned restart of ConfD and temporary loss of connectivity over the NETCONF and REST (if still enabled) interfaces.

Changes to global certificates which ConfD is using while REST is enabled will also result in a restart of ConfD.

For additional information, see the *NETCONF and ConfD* appendix of the *System Administration Guide*.

Example

The following command requires the client to supply a client certificate:

```
rest auth-policy peer-fail
```

The following command specifies no client authentication is required:

```
no rest auth-policy
```

The following command specifies existing certificate box1 for the REST interface:

```
rest certificate box1
```

The following command removes any configured certificate and key. REST will not be operational without a valid certificate and key.

```
no rest certificate
```

The following command mandates the web server to only serve URLs adhering to the hostname restconf:

```
rest hostname restconf
```

The following command specifies that the system name is used and matching of hostname is not mandated:

```
no rest hostname
```

The following command sets the REST interface port number to 700:

```
rest port 700
```

The following command resets the REST interface port number to 443:

```
no rest port
```