Configuring Application Assurance with CLI

This section provides information to configure Application Assurance entities using the command line interface. It is assumed that the user is familiar with basic configuration of policies.

Provisioning AA ISA MDA

The following illustrates syntax to provision AA ISA and configure ingress IOM QoS parameters. (The egress IOM QoS is configured in the **config>isa>application-assurance-grp>qos** context.)

CLI Syntax:
```
configure>card>mda mda-slot
 mda-type isa-aa
    network
       ingress
          pool
             slope-policy slope-policy-name
             resv-cbs percent-or-default
          queue-policy network-queue-policy-name
```

The following output displays AA ISA configuration example.

```
*A:cpm-a>config>app-assure# show mda 1/1
===============================================================================
MDA 1/1
===============================================================================
Slot  Mda   Provisioned           Equipped              Admin     Operational
            Mda-type              Mda-type              State     State
-------------------------------------------------------------------------------
1     1     isa-aa                isa-ms                up        up
===============================================================================
*A:cpm-a>config>app-assure#


*A:cpm-a>config>card# info
----------------------------------------------
        card-type iom-20g-b
        mda 1
            mda-type isa-aa
        exit
----------------------------------------------
*A:cpm-a>config>card#
```

Configuring an AA ISA Group

To enable AA on the router:

- Create an AA ISA group.
- Assign active and optional backup AA ISA(s) to an AA ISA group.
- Select the forwarding classes to divert.
- Enable the group.
- Optionally:
  - → Enable group policy partitioning
  - → Configure capacity cost threshold values
  - → Configure the number of transit prefix IP policies
  - → Configure IOM egress queues to the MS-ISA
  - → Enable overload cut through and configure the high and low watermarks values
  - → Configure performance statistics accounting

The following example illustrates AA ISA group configuration with:

- Primary AA ISA and warm redundancy provided by the backup AA ISA.
- "fail-to-wire" behavior configured on group failure.
- BE forwarding class selected for divert.
- Default IOM QoS for logical ISA egress ports. The ISA ingress QoS is configured as part of ISA provisioning (**config>card>mda>network>ingress>qos**).

The following commands illustrate AA ISA group configuration context.

CLI Syntax: config>>isa>application-assurance-group *isa-aa-group-id* [aa-sub-scale {residential|vpn}] [create]

```
backup mda-id
description description
divert-fc fc-name
no fail-to-open
isa-capacity-cost-high-threshold threshold
isa-capacity-cost-low-threshold threshold
partitions
primary mda-id
qos
   egress
      from-subscriber
         pool [pool-name]
         resv-cbs percent-or-default
```

```
                        slope-policy slope-policy-name
                     port-scheduler-policy port-scheduler-policy-name
                     queue-policy network-queue-policy-name
                     to-subscriber
                        pool [pool-name]
                           resv-cbs percent-or-default
                           slope-policy slope-policy-name
                        port-scheduler-policy port-scheduler-policy-name
                        queue-policy network-queue-policy-name
                [no] shutdown
```

The following output displays an AA ISA group configuration example.

```
A:ALU-A>config>isa>aa-grp# info detail
 ----------------------------------------------
    no description
    primary 1/2
    backup  2/2
    no fail-to-open
    isa-capacity-cost-high-threshold 4294967295
    isa-capacity-cost-low-threshold 0
    no partitions
    divert-fc be
    qos
       egress
         from-subscriber
              pool
                   slope-policy "default"
                   resv-cbs default
              exit
              queue-policy "default"
              no port-scheduler-policy
         exit
         to-subscriber
              pool
                   slope-policy "default"
                   resv-cbs default
              exit
              queue-policy "default"
              no port-scheduler-policy
         exit
       exit
    exit
    no shutdown
----------------------------------------------
A:ALU-A>config>isa>aa-grp#
```

Configuring Watermark Parameters

Use the following CLI syntax to configure thresholds for logs and traps when under high consumption of the flow table. The flow table has a limited size and these thresholds can be established to alert the user that the table is approaching capacity. These flow table watermarks represent number of flow contexts allocated on the ISA, which will be slightly higher than the actual number of existing flows at the point when the watermark is reached.

The low threshold is used while the high threshold is used as an alarm.

CLI Syntax:
```
config>application-assurance
 flow-table-high-wmark high-watermark
 flow-table-low-wmark low-watermark
```

Configuring a Group Policy

Beginning and Committing a Policy Configuration

To enter the mode to create or edit Application Assurance policies, you must enter the **begin** keyword at the **config>app-assure>group>policy** prompt. The **commit** command saves changes made to policies during a session. Changes do not take affect in the system until they have performed the commit function. The **abort** command discards changes that have been made to policies during a session.

The following error message displays when creating or modifying a policy without entering **begin** first.

```
A:ALA-B>config>app-assure>group>policy#
MINOR: AA #1005 Invalid Set - Cannot proceed with changes when in non-
edit mode
```

There are no default policy options. All parameters must be explicitly configured.

Use the following CLI syntax to begin a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    begin
```

Use the following CLI syntax to commit a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    commit
```

Aborting a Policy Configuration

Use the following CLI syntax to abort a policy configuration.

CLI Syntax:
```
config>app-assure# group group-id
 policy
    abort
```

Configuring an Application Filter

An operator can use an application filter to define applications based on ALU protocol signatures and a set of configurable parameters like IP flow setup direction, IP protocol number, server IP address and server TCP/UDP port. An application filter references an application configured as previously shown.

Use the following CLI syntax to configure an application filter entry.

CLI Syntax:

```
config>app-assure>group>policy# app-filter
 entry entry-id [create]
    application application-name
    description description-string
    expression expr-index expr-type {eq | neq} expr-string
    flow-setup-direction {subscriber-to-network | network-to-
       subscriber | both}
    ip-protocol-num {eq | neq} protocol-id
    protocol {eq | neq} protocol-signature-name
    server-address {eq | neq} ip-address[/mask]
    server-port {eq | neq | gt | lt} server-port-number
    server-port {eq|neq} range start-port-num end-port-num
    server-port {eq} {port-num | range start-port-num end-
       port-num} first-packet-trusted|first-packet-validate}
    no shutdown
```

The following example displays an application filter configuration.

```
*A:ALA-48>config>app-assure>group>policy>app-filter# entry 30 create
*A:ALA-48>config>app-assure>group>policy>app-filter>entry# info
----------------------------------------------
                      description "DNS traffic to local server on expected port #53"
                      protocol eq "dns"
                      flow-setup-direction subscriber-to-network
                      ip-protocol-num eq *
                      server-address eq 192.0.2.0/32
                      server-port eq 53
                      application "DNS_Local"
                      no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-filter>entry#
```

Configuring an Application Group

An operator can configure an application group to group multiple application into a single application assurance entity by referencing those applications to the group created.

Use the following CLI syntax to configure an application group.

CLI Syntax: `config>app-assure>group>policy# app-group` *`application-group-name`* `[create]`
`description` *`description`*

The following example displays an application group configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-group "Peer to Peer" create
*A:ALA-48>config>app-assure>group>policy>app-grp# info
----------------------------------------------
                  description "Peer to Peer file sharing applications"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-grp#
```

Configuring an Application

An operator can configure an application to group multiple protocols, clients or network applications into a single Application Assurance application by referencing it later in the created application filters as display in other sections of this guide.

Use the following CLI syntax to configure an application.

CLI Syntax: `config>app-assure>group>policy# application` *`application-name`* `[create]`

```
            app-group app-group-name
            description description
```

The following example displays an application configuration.

```
*A:ALA-48>config>app-assure>group>policy# application "SQL" create
*A:ALA-48>config>app-assure>group>policy>app# info
----------------------------------------------
                  description "SQL protocols"
                  app-group "Business Critical Applications"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app#
```

Configuring an Application Profile

Use the following CLI syntax to configure an application profile.

CLI Syntax: config>app-assure>group>policy# app-profile *app-profile-name* [create]
characteristic *characteristic-name* value *value-name*
description *description-string*
divert

The following example displays an application profile configuration.

```
*A:ALA-48>config>app-assure>group>policy# app-profile "Super" create
*A:ALA-48>config>app-assure>group>policy>app-prof# info
----------------------------------------------
                  description "Super User Application Profile"
                  divert
                  characteristic "Server" value "Prioritize"
                  characteristic "ServiceBw" value "SuperUser"
                  characteristic "Teleworker" value "Yes"
                  characteristic "VideoBoost" value "Priority"
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>app-prof#
```

Configuring a Policer

Use the following CLI syntax to configure a policer.

CLI Syntax: config>app-assure>group>policy# policer *policer-name* type *type* granularity *granularity* create
action {priority-mark | permit-deny}
adaptation-rule pir *adaptation-rule*
description *description-string*
mbs *maximum burst size*
rate *pir-rate*
tod-override *tod-override-id* [create]

The following example displays an Application Assurance policer configuration.

```
*A:ALA-48>config>app-assure>group# policer "RegDown_Policer" type dual-bucket-bandwidth
granularity subscriber create

*A:ALA-48>config>app-assure>group>policer# info
----------------------------------------------
                description "Control the downstream aggregate bandwidth for Regular 1Mbps
subscribers"
                rate 1000 cir 500
                mbs 100
                cbs 50
----------------------------------------------
*A:ALA-48>config>app-assure>group>policer#
```

Configure an HTTP Error Redirect

Use the following CLI syntax to configure an HTTP error redirect policy:

CLI Syntax:
```
config>app-assure>group>http-error-redirect redirect-name
create
           no http-error-redirect redirect_name
            description description-string
            no description
            error-code error-code [custom-msg-size custom-msg-size]
            no error-code error-code
            http-host http-host // eg. www.demo.barefruit.com
            no http-host
            participant-id participant-id // 32-char string used by tem-
               plate 1
            no participant-id
            no] shutdown
            template template-id // {1, 2} one for Barefruit, 2= Xerocole
            no template
```

The following example displays an Application Assurance HTTP redirect configuration.

```
*A:ALA-48>config>app-assure>group# http-error-redirect "redirect-404"
create
        description "redirect policy of 404 to Barefruit servers"
        error-code 404
        http-host
          att.barefruit.com
        participant-id att-ISP
        template 1


*A:ALA-48>config>app-assure>group> http-error-redirect# redirect-404
info
----------------------------------------------
               description "redirect policy of 404 to Barefruit servers"
                template 1
                http-host "att.barefruit.com"
                participant-id "att-ISP"

                error-code 404

*A:ALA-48>config>app-assure>group>http-error-redirect#
```

Configure an HTTP Policy Redirect

Use the following CLI syntax to configure an HTTP redirect policy:

CLI Syntax:
```
config>app-assure>group# http-redirect redirect-name [create]
    description description-string
    no description
    template template-id// {1} 1, 2, 3 are acceptable
    http-host URL // redirect URL e.g. www.isp.com/block-msg
    no http-host
    [no] shutdown
no http-redirect redirect-name
```

The following example displays an Application Assurance http redirect configuration.

```
*A:ALA-48>config>app-assure>group# http-redirect "redirectgaming" create
           description "redirect policy for blocked http gaming traffic"
           template 1
           http-host bt.com/blockgamingmsg
           no shutdown


*A:ALA-48>config>app-assure>group> http-redirect# redirectgaming info
----------------------------------------------
           description " redirect policy for blocked http gaming traffic "
           template 1
           http-host "bt.com/blockgamingmsg"

*A:ALA-48>config>app-assure>group>http-redirect#
```

The following example displays AQP entry to block all http gaming traffic (AppGroup httpGaming) and perform redirect:

```
A:ALA-48>config>app-assure>group>policy>aqp>entry#
------------------------------------------------------------------------------
           entry 100 create
               match
                   app-group eq httpGaming
               exit
               action
                   drop
                   http-redirect redirectgaming
               exit
           no shutdown
           exit
------------------------------------------------------------------------------
A:ALA-48>config>app-assure>group>policy>aqp#
```

Configure ICAP URL Filtering

To configure the system for ICAP URL Filtering, the operator needs to:

- Create an aa-interface and assign an ip address to each AA ISA within an IES or VPRN service. This routed interface is then used by the system to establish TCP communication with the ICAP server.
- Create an http-redirect policy (used by the url-filter to redirect http traffic).
- Create a url-filter, configure the icap server ip-address, redirect-policy, and default action.
- Verify that the aa-interface(s) and url-filter are operationally up.

Use the following CLI syntax to configure the aa-interfaces for each AA ISA:

CLI Syntax:

```
config>service>vprn# aa-interface <aa-if-name> [create]
 config>service>vprn>aa-if# aa-interface interface <ip-int-
    name> [create]
 description <description-string>
 no description
 address <ipv4_subnet/31>
 no address
    sap <card/mda/aa-svc:vlan> [create]
       description <description-string>
       no description
       egress
          [no] filter
          [no] qos
       exit
       ingress
          [no] qos
       exit
       [no] shutdown
    exit
```

The following examples displays an AA interface created for the ISA card 1/2 using IP address 172.16.2.1/31:

```
A:7750>config>service>ies# info
----------------------------------------------
            aa-interface "aa-if1" create
                address 172.16.2.1/31
                sap 1/2/aa-svc:10 create
                    egress
                        filter ip 10
                    exit
                    no shutdown
                exit
                no shutdown
            exit
```

In the example above, 172.16.2.1 is used by the CPM side of the interface while the ISA itself is automatically assigned 172.16.2.0 based on the /31 subnet.

Recommendations:

- More than one aa-interface can be configured per AA ISA card, however, the operator needs to use the same service vlan across all these interfaces for a given url-filter object.
- Configure an egress ip filter under the sap towards the ISA AA interface to only allow selected ip addresses or subnet (subnet examples: icap servers, network management).

Use the following CLI syntax to configure the url-filter:

CLI Syntax:

```
config>app-assure>group#
 url-filter <url-filter-name> [create]
    description <description-string>
    no description
    vlan-id <service-port-vlan-id>
    no vlan-id
    default-action {allow | block-all | block-http-redirect
       <redirect-name>}
    no default-action
    icap-http-redirect <http-redirect-name>
    no icap-http-redirect
    icap-server <ip-address[:port]> [create]
       description <description-string>
       no description
       [no] shutdown
    no icap-server <ip-address[:port]>
    [no] shutdown
 no url-filter <url-filter-name>
```

The following examples displays a url-filter configuration:

```
*A:7750>config>app-assure>group# url-filter "optenet1" create
        vlan-id 10
        default-action block-http-redirect "http-redirect-portal"
        icap-http-redirect "http-redirect-portal"
        icap-server 172.16.1.101 create
            no shutdown
        exit
        no shutdown
```

The following examples displays the AQP entry to enable icap url-filtering for opted-in subscribers based on ASO characteristics:

```
A:7750>config>app-assure>group>policy>aqp# entry 100 create
        match
            characteristic "url-filter" eq "yes"
```

```
exit
action
    url-filter "optenet1"
exit
no shutdown
```

Configure HTTP Notification

Use the following CLI syntax to configure an HTTP Notification policy.

CLI Syntax:
```
config>app-assure>group#
    http-notification <http-notification-name> [create]
       description <description-string>
       no description
       script-url <script-url-name>
       no script-url
       interval {one-time | <minimum-interval>}
       template <template-id>
       no template
       [no] shutdown
    no http-notification <http-notification-name>
```

The following example displays an HTTP notification policy configured with a minimum interval of 5 minutes:

```
A:7750>config>app-assure>group# http-notification "in-browser-notification" create
A:7750>config>app-assure>group>http-notif# info
----------------------------------------------
        description "In Browser Notification Example"
        template 1
        script-url "http://1.1.1.1/In-Browser-Notification/script.js"
        interval 5
        no shutdown
----------------------------------------------
```

The following examples displays the AQP entry required to match this policy based on an ASO characteristic:

```
A:7750>config>app-assure>group>policy>aqp# info
----------------------------------------------
            entry 200 create
                match
                    characteristic "in-browser-notification" eq "yes"
                exit
                action
                    http-notification "in-browser-notification"
                exit
                no shutdown
            exit
----------------------------------------------
```

Configuring an Application QoS Policy

Use the following CLI syntax to configure an application QoS policy.

CLI Syntax:

```
config>app-assure>group>policy# app-qos-policy
            entry entry-id [create]
               action
                  bandwidth-policer policer-name
                  drop
                  flow-count-limit policer-name
                  flow-rate-limit policer-name
                  http-error-redirect redirect-name
                  mirror-source [all-inclusive] mirror-service-id
                  remark
                     dscp in-profile dscp-name out-profile dscp-name
                     fc fc-name
                     priority priority-level
               description description-string
               match
                  aa-sub sap {eq | neq} sap-id
                  aa-sub esm {eq | neq} sub-ident-string
                  aa-sub spoke-sdp {eq | neq} sdp-id:vc-id
                  app-group {eq | neq} application-group-name
                  application {eq | neq} application-name
                  characteristic characteristic-name {eq} value-name
                  dscp {eq | neq} dscp-name
                  dst-ip {eq | neq} ip-address[/mask]
                  dst-port {eq | neq} port-num
                  dst-port {eq | neq} range start-port-num end-port-num
                  src-ip {eq | neq} ip-address[/mask]
                  src-port {eq | neq} port-num
                  src-port {eq | neq} range start-port-num end-port-num
                  traffic-direction {subscriber-to-network | network-to-
                    subscriber | both}
               no shutdown
```

The following example displays an application QoS policy configuration.

```
*A:ALA-48>config>app-assure>group>policy>aqp# entry 20 create
-----------------------------------------------
                        description "Limit downstream bandwidth to Reg_1M subscribers"
                        match
                            traffic-direction network-to-subscriber
                            characteristic "ServiceBw" eq "Reg_1M"
                        exit
                        action
                            bandwidth-policer "RegDown_Policer"
                        exit
                        no shutdown
-----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>aqp#
```

The following example display an AQP entry configuration to mirror all positively identified only P2P traffic (AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled.

```
A:ALA-48>config>app-assure>group>policy>aqp#
------------------------------------------------------------------------------
   entry 100 create
     match
          app-group eq P2P
          characteristic aa-sub-mirror eq enabled
     exit
     action                      # mirror to an existing mirror service id
          mirror-source 100
     exit
   no shutdown
   exit
------------------------------------------------------------------------------
A:ALA-48>config>app-assure>group>policy>aqp#
```

The following example displays an AQP entry to mirror all P2P traffic (all positively identified P2P traffic and any unidentified traffic that may or may not be P2P - AppGroup P2P) for a subset of subscribers with ASO characteristic **aa-sub-mirror** enabled (the order is significant):

```
A:ALA-48>config>app-assure>group>policy>aqp>entry#
------------------------------------------------------------------------------
   entry 100 create
     match
          app-group eq P2P
          characteristic aa-sub-mirror value enabled
     exit
     action
          mirror-source all-inclusive 100
     exit
   no shutdown
   exit
------------------------------------------------------------------------------
A:ALA-48>config>app-assure>group>policy>aqp#
```

Configuring Application Service Options

Use the following CLI syntax to configure application service options.

CLI Syntax:
```
config>app-assure>group>policy# app-service-options
            characteristic characteristic-name [create]
               default-value value-name
               value value-name
```

The following example displays an application service options configuration.

```
*A:ALA-48>config>app-assure>group>policy>aso# info
----------------------------------------------
                  characteristic "Server" create
                      value "Block"
                      value "Permit"
                      value "Prioritize"
                      default-value "Block"
                  exit
                  characteristic "ServiceBw" create
                      value "Lite_128k"
                      value "Power_5M"
                      value "Reg_1M"
                      value "SuperUser"
                      default-value "Reg_1M"
                  exit
                  characteristic "Teleworker" create
                      value "No"
                      value "Yes"
                      default-value "No"
                  exit
                  characteristic "VideoBoost" create
                      value "No"
                      value "Priority"
                      default-value "No"
                  exit
----------------------------------------------
*A:ALA-48>config>app-assure>group>policy>aso#
```

Configuring AA Volume Accounting and Statistics

A network operator can configure AA volume statistic collection and accounting on both AA ISA system and subscriber levels.

The following commands illustrate the configuration of statistics collection and accounting policy on an AA group/partition aggregate level (without subscriber context).

CLI Syntax:
```
config>app-assure>group>statistics>app-group
 accounting-policy act-policy-id
 collect-stats
```

CLI Syntax:
```
config>app-assure>group>statistics>application
 accounting-policy act-policy-id
 collect-stats
```

CLI Syntax:
```
config>app-assure>group>statistics>protocol
 accounting-policy act-policy-id
 collect-stats
```

These commands illustrate the configuration of statistics collection and accounting policy for each AA subscriber in the system.

CLI Syntax:
```
config>app-assure>group>statistics>aa-sub
 accounting-policy acct-policy-id
 aggregate-stats
 app-group app-group-name export-using export-method [export-
    method...(upto 2 max)]
 application application-name export-using export-method [ex-
    port-method...(upto 2 max)]
 charging-group charging-group-name export-using export-meth-
    od [export-method...(upto 2 max)]
 collect-stats
 exclude-tcp-retrans
 max-throughput-stats
 protocol protocol-name export-using export-method
 radius-accounting-policy rad-acct-plcy-name
```

These commands illustrate configuration of special study mode for a subset of AA subscribers (configured) to collect all protocol and/or application statistics with an AA subscriber context.

CLI Syntax:
```
config>app-assure>group>statistics# aa-sub-study {applica-
tion|protocol}
 accounting-policy acct-policy-id
 collect-stats
```

For details on accounting policy configuration (including among others AA record type selection and customized AA subscriber record configuration) refer to the 7750 SR OS System Management Guide.

The following output illustrates per AA-subscriber statistics configuration that elects statistic collection for a small subset of all application groups, applications, protocols:

```
*A:ALU-40>config>app-assure>group>statistics>aa-sub# info
----------------------------------------------
                    accounting-policy 4
                    collect-stats
                    app-group "File Transfer"
                    app-group "Infrastructure"
                    app-group "Instant Messaging"
                    app-group "Local Content"
                    app-group "Mail"
                    app-group "MultiMedia"
                    app-group "Business_Critical
                    app-group "Peer to Peer"
                    app-group "Premium Partner"
                    app-group "Remote Connectivity"
                    app-group "Tunneling"
                    app-group "Unknown"
                    app-group "VoIP"
                    app-group "Web"
                    app-group "Intranet"
                    application "BitTorrent"
                    application "eLearning"
                    application "GRE"
                    application "H323"
                    application "TLS"
                    application "HTTP"
                    application "HTTPS"
                    application "HTTPS_Server"
                    application "HTTP_Audio"
                    application "HTTP_Video"
                    application "eMail_Business"
                    application "eMail_Other"
                    application "Oracle"
                    application "Skype"
                    application "SAP"
                    application "SIP"
                    application "SMTP"
                    application "SQL_Alltypes"
                    application "TFTP"
                    protocol "bittorrent"
                    protocol "dns"
                    protocol "sap"
                    protocol "skype"
----------------------------------------------
*A:ALU-40>config>app-assure>group>statistics>aa-sub#
```

Configuring Cflowd Collector

The following output displays an Application Assurance cflowd collector configuration example:

Example:
```
*A:ALA-48# configure application-assurance group 1 cflowd
collector 138.120.131.149:55000 create
*A:ALA-48>config>app-assure>group>cflowd>collector$description
"cflowd_collector_NewYork"
*A:ALA-48>config>app-assure>group>cflowd>collector# no shutdown
*A:ALA-48>config>app-assure>group>cflowd>collector# exit


*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
    collector 138.120.131.149:55000 create
         description "cflowd_collector_NewYork"
    no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
```

Configuring AA Volume, TCP and RTP Performance Reporting

CLI Syntax:
```
config>application-assurance>group isa-aa-group-id
 cflowd
 collector ip-address[:port] [create]
 no collector ip-address[:port]
 description description-string
 no description
    [no] shutdown
 rtp-performance
    flow-rate sample-rate
    no flow-rate
    flow-rate2 sample-rate2
    no flow-rate2
 tcp-performance
    flow-rate sample-rate
    no flow-rate
    flow-rate2 sample-rate2
    no flow-rate2
 template-retransmit seconds
 no template-retransmit
 [no] shutdown
 volume
    rate sample-rate
    no rate
    [no] shutdown
```

CLI Syntax:
```
config>application-assurance
 group isa-aa-group-id[:partition [create]]
 no group isa-aa-group-id[:partition
    cflowd
       volume
          [no] shutdown
       rtp-performance
          [no] app-group app-group-name [flow-rate|flow-rate
          2]
          [no] application application-name [flow-rate|flow-
          rate 2]
          [no] shutdown
       tcp-performance
          [no] app-group app-group-name [flow-rate|flow-rate
          2]
          [no] application application-name [flow-rate|flow-
          rate 2]
          [no] shutdown
Note: The default if flow-rate
```

The following example shows a configuration that:

- Enables per-flow volume stats for group 1, partition 1 and configures sampling rate to 1/1000.
- Enables per-flow TCP performance stats for web_traffic application within group 1, partition 1 and configures TCP sampling rate to 1/500.
- Enables per-flow TCP performance stats for citrix_traffic application within group 1, partition 1 using TCP sampling rate2 to 1/100.
- Enables per-flow RTP A/V performance stats for voip_traffic application within group 1, partition 1 and configures rtp sampling rate to 1/10.

```
*A:ALA-48# configure application-assurance group 1 cflowd
*A:ALA-48>config>app-assure>group>cflowd# volume rate 1000
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate 500
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance flow-rate2 100
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance   flow-rate 10
*A:ALA-48>config>app-assure>group>cflowd# no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
                collector 138.120.131.149:55000 create
                    description "cflowd_collector_NewYork"
                exit
                volume
                    rate 1000
                exit
                tcp-performance
                    flow-rate 500
                    flow-rate 100
                rtp-performance
                    flow-rate 10
                exit
                no shutdown
----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#


*A:ALA-48# configure application-assurance group 1:1 cflowd
*A:ALA-48>config>app-assure>group>cflowd#
*A:ALA-48>config>app-assure>group>cflowd# volume no shutdown
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance application "web_traffic"
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance application "citrix" [flow-
rate2]
*A:ALA-48>config>app-assure>group>cflowd# tcp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance application "voip_traffic"
*A:ALA-48>config>app-assure>group>cflowd# rtp-performance no shutdown
*A:ALA-48>config>app-assure>group>cflowd# info
----------------------------------------------
            volume
                no shutdown exit
            rtp-performance no shutdown
                application "voip_traffic"
            tcp-performance
                no shutdown
                application "web_traffic"
                application “citrix” flow-rate2
```

```
    exit
-----------------------------------------------
*A:ALA-48>config>app-assure>group>cflowd#
```