Troubleshooting Network Infrastructue Components

Cisco ASA 5500 Series

Common problems

This section describes common problems with the ASA, with possible causes and recommended actions,

Note Send traps northbound, and not to Prime Collaboration Assurance.

1. **Symptom**

   The context configuration was not saved, and was lost when you reloaded.

   Possible cause

You did not save each context within the context execution space. If you are configuring contexts at the command line, you did not save the current context before you changed to the next context.

Recommended action

Save each context within the context execution space using the **copy start run** command. Load the startup configuration as your active configuration. Then change the password and then enter the **copy run start** command. Or use the **write memory all** command to save all contexts. This can take significant time on a large system.

2. **Symptom**

   You cannot make a Telnet or SSH connection to the ASA interface.

   Possible cause

   You did not enable Telnet or SSH to the ASA.

   Recommended action

   Enable Telnet or SSH to the ASA.

3. **Symptom**

   You cannot ping the ASA interface.

   Possible cause

   You disabled ICMP to the ASA.

   Recommended action

   Enable ICMP to the ASA for your IP address using the **icmp** command.

4. **Symptom**

   You cannot ping through the ASA, although the access list allows it.

   Possible cause

   You did not enable the ICMP inspection engine or apply access lists on both the ingress and egress interfaces.

   Recommended action

   Because ICMP is a connectionless protocol, the ASA does not automatically allow returning traffic through. In addition to an access list on the ingress interface, you either need to apply an access list to the egress interface to allow replying traffic, or enable the ICMP inspection engine, which treats ICMP connections as stateful connections.

5. **Symptom**

   Traffic does not pass between two interfaces on the same security level.

   Possible cause

   You did not enable the feature that allows traffic to pass between interfaces at the same security level.

   Recommended action

   Enable the feature.

6. **Symptom**

   IPsec tunnels do not duplicate during a failover to the standby device.

Possible cause

The switch port that the ASA is plugged into is set to 10/100 instead of 1000.

Recommended action

Set the switch port that the ASA is plugged into to 1000.

For more information about troubleshooting for the Cisco ASA 5500 Series, see:

Cisco ASA 5500 Series Configuration Guide using the CLI

Cisco Session Border Controller Series Aggregation Services Routers

Gigabit Ethernet 0 Troubleshooting

The Gigabit Ethernet Management interface is automatically part of its own VRF. This VRF, named *Mgmt-intf*, is automatically configured on the Cisco Session Border Controller Series Router and is dedicated to the Management Ethernet interface.

Gigabit Ethernet 0 is always in VRF *Mgmt-intf*.

Commands

```
TFTP with Gigabit Ethernet 0
FTP with Gigabit Ethernet 0
Telnet with Gigabit Ethernet 0
```

Command Syntax

```
ip tftp source-interface gigabitethernet 0
ip ftp source-interface gigabitethernet 0
ip telnet source-interface gigabitethernet 0
```

Hardware Troubleshooting

To troubleshoot hardware failures, consider the following:

- All memories are error checking and correcting (ECC) protected.
  - `show platform hardware slot` (for example, DRAM memory statistics).
  - Multibit errors (MBE) still cause crashes.
- `Cman`

  (chassis manager) controls signaling.
- Start with `show platform`, `show log`.
- More details are available in `show plat ha slot`.

Software Troubleshooting

To troubleshoot software failures, consider the following:

- Use a top-down approach, for example: IOS > fman_rp > fman_fp > QFP.
- If possible, determine whether the issue is platform-independent (PI), or platform-dependent (PD).
- Expect some differences from legacy platforms. For example, `debug ip icmp` does not show echo replies because the Cisco Quantum Flow Processor (QFP) generates the echo replies directly.
- You can have a responsive console with broken forwarding (RP up and FP down).

Debugging

Use the following debug information to help troubleshoot:

- IOS debugs
- For other debugs, `debug platform [software|hardware] …`
    - Remember which debugs you enable.
    - Do not use `un all` to disable the debugs. Use `no debug` with the same syntax to disable a debug.
    - Do not use `no debug platform all`.

Cisco IOS-XE Command Line Interface

The Cisco IOS-XE is identical in look, feel, and usage to the Cisco IOS CLI for the platform-independent (PI) side.

Commands

All platform-dependent (PD) commands are available under the following commands:

- `show platform [software|hardware] …`
- `request platform [software|hardware] …`
- `debug platform [software|hardware] …`
- `set platform [software|hardware] …`

Access the Linux Shell

ASR 1001 requires a shell license. Follow these steps to access the Linux shell:

Procedure

Step 1 Configure the following:

<2.3.0: service internal

>= 2.3.0: platform shell

Step 2 Enter request platform software system shell [r0 | f0 | 0 | 1 |…] where 0 = sip slot 0.

Tracebacks

Tracebacks now include a TraceKey. The TraceKey uniquely identifies the image.

```
Traceback= 1#dbfc17e68d86773af5be2dd64151ab7d
:400000+6C0AFB :400000+652825 :400000+64F866
:400000+61C574 :400000+6132F2 :400000+612F88
:400000+611066 :400000+2E05AFA :400000+626DAA
```

Other Troubleshooting Scenarios

The following are other common troubleshooting scenarios.

Crashes

Do not configure Cisco Session Border Controller for coredump. Depending on the component that is experiencing the crash, you get the following:

```
crashinfo (bootflash:/ or harddisk:/…)
coredump (bootflash:/core/… or harddisk:/core/…)
```

Examples

```
SIP_2_mcpcc-lc-ms_6786.core.gz -> IOSd on SIP2 crash
CEMBROS_RP_0_blogin_412.core.gz -> blogin on RP0 crash
CEMBROS_RP_0_ppc_linux_iosd-_22903.core.gz -> IOS crash
kernel.rp_20110831060507.core.gz -> RP kernel crash
Bsns-asr1006-1_ESP_1_cpp-mcplo-ucode_012612022323.core.gz -> QFP ucode crash
```

High CPU

Use the following information to troubleshoot high CPU:

- In IOSd, high CPU is rare because the ESP handles forwarding.
  - `show processes cpu sorted`
  - `show stack <PID>`
  - No CPU profiling support
- In the QFP, high CPU can happen as a result of a flow lock issue.
  - `show platform hardware qfp active datapath utilization`
- In Linux processes in Control processors (SIP, FP, RP)
  - 'top' in the Linux shell
  - `sh platform software status control-processor brief`

- In the crypto engine
  - `show platform hardware crypto-device utilization`

Packet Drops

Use the following information to troubleshoot packet drops:

- `show platform hardware qfp active statistics drop`
- QFP Drops Per Interface or Subinterface Per Feature
  - `debug platform hardware qfp active interface if-stats int-name GigabitEthernet0/0/7.100`
  - `show platform hardware qfp active interface if-name GigabitEthernet0/0/7.100 statistics drop_summary subinterface`
- ACLs with the log (not punted)
- IP SLA, EEM
- Debug platform hardware qfp active feature
- `show memory commands` to check for any possible memory leakage if a crash is due to a memory over run.

CEF

Use the following information to troubleshoot CEF:

- `show ip cef ../.. platform internal`
- VRF name > ID
  - `sh plat so vrf [rp|fp] active vrf`
- IOS
  - `show ip route`
  - `show ip cef int`
  - `show adj int`
- FMAN
  - `show platform software [rp|fp] active cef prefix .. detail`
- QFP
  - `show platform hardware qfp active feature cef-mpls prefix ip …`

Multicast

Use the following information to troubleshoot multicast:

- IOS
  - `show ip mroute <G> [count]`
  - `show ip pim int <I> count`
  - `show ip mrib route <G>`
  - `show ip mfib <G>`
- FMAN
  - `show platform software ip fp active mfib …`
  - `show platform software multicast …`
- QFP
  - `show platform hardware qfp active feature multicast v4mcast ...`

NAT

All NAT troubleshooting is done on QFP. Use the following information to troubleshoot NAT:

- IOS
  - `show ip nat translations`
  - `show ip nat stat`
  - `debug ip nat <ACL> > cpp_cp.log file`
- FMAN
  - `show platform software nat fp active translation ...`
- QFP
  - `show platform hardware qfp active feature nat datapath sess-dump`

Sniffing Packets

See the following for information on sniffing packets:

- ERSPAN
- Local ERSPAN = SPAN
- Packet tracing (with TAC)
- Dropped packets (with TAC)
- In 3.7S: Embedded Packet Capture

Tracing

For more information, use the following trace commands:

- `set platform software trace …`
- `show platform software trace message`
- `show platform software trace level …`

The tracelogs are in the harddisk:/tracelogs. Different trace levels (default = notice, others = debug, emergency, error, info, noise, notice, verbose, warning) are available.

Cisco MDS 9000 Family

Gather Information

Use the following commands to gather general information on your device:

```
show module
show version
show running-config
show logging log
show interfaces brief
show fcns
show flogi
show hardware internal errors
show zoneset active
show accounting log
show interface fc
show interface vsan
```

View Logs

Use the following commands to access and view logs on a switch:

```
Musky-9506# show logging ?
console Show console logging configuration
info Show logging configuration
last Show last few lines of logfile
level Show facility logging configuration
logfile Show contents of logfile
module Show module logging configuration
monitor Show monitor logging configuration
nvram Show NVRAM log
server Show server logging configuration
<cr> Carriage Return
```

For more information about troubleshooting for the Cisco MDS 9000 Family, see the *Cisco MDS 9000 SAN-OS Software Release 2.x* at http://www.cisco.com/c/en/us/support/storage-networking/mds-9000-nx-os-san-os-software/products-troubleshooting-guides-list.html.

Cisco Nexus 5500 Series

View Logs

System is not responsive

If system performance is slow or nonresponsive, some system resources can be over utilized. For example, an incorrect logging level can generate many messages resulting in an impact on system resources.

Check the logging level on the chassis. If you have a logging level setting such as 6 or 7, many messages are generated and performance can be impacted. Use the following commands to display the amount of resources that are being used.

```
show proc cpu | inc syslogd
show proc cpu
show run | inc logging
show system resource
```

Check the vpc status.

```
show vpc
show vpc consistency-parameters
```

Syslog server is not getting messages from DUT

Although the syslog server is configured, the destination syslog server is not receiving messages from DUT. The syslog server might not be accessible or the logging level might not be appropriate.

Check to see if the destination syslog server is accessible from VRF management. Use the following command to ping the server:

```
ping <dest-ip> vrf management
```

Check that the syslog configuration on the DUT has use-vrf management. Use the following command:

```
logging server 10.193.12.1 5 use-vrf management
```

Check that the appropriate logging level is enabled for logging messages. Use the following command:

```
show logging info
```

If the logging level is not appropriate, then set the appropriate level using the following command:

```
logging level <feature> <log-level>
```

For more information about troubleshooting the Cisco Nexus 5500 Series, see the *Cisco Nexus 5500 Troubleshooting Guide* at http://www.cisco.com/c/en/us/support/switches/nexus-5000-series-switches/products-troubleshooting-guides-list.html.

Cisco Nexus 7000 Series

Gather Information

Use the following commands to gather general information about your device:

```
show module
show version
show running-config
show logging log
show interfaces brief
show vlan
show spanning-tree
show {ip | ipv6} routing
show processes | include ER
show accounting log
show tech
```

View Logs

Cisco NX-OS generates many types of system messages on the device and sends them to a syslog server. You can view these messages to determine what events could have led up to the current problem condition that you are facing. Use the following commands to access and view logs in Cisco NX-OS:

```
switch# show logging ?
console Show console logging configuration
info Show logging configuration
internal syslog syslog internal information
ip IP configuration
last Show last few lines of logfile
level Show facility logging configuration
logfile Show contents of logfile
loopback Show logging loopback configuration
module Show module logging configuration
monitor Show monitor logging configuration
nvram Show NVRAM log
onboard show logging onboard
pending server address pending configuration
pending-diff server address pending configuration diff
server Show server logging configuration
session Show logging session status
status Show logging status
timestamp Show logging timestamp configuration
```

For more information about troubleshooting the Cisco Nexus 7000 Series, see *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide* at:

Cisco Nexus 7000 Series NX-OS Troubleshooting Guide.

Cisco UC Manager Session Management Edition

For information about troubleshooting for Cisco UC Manager Session Management Edition, see:

Cisco Unified Communications Manager Session Management Edition Troubleshoot and Alerts.

Cisco UCS Manager

For information about troubleshooting for Cisco UCS Manager, see:

Cisco UCS Manager Troubleshoot and Alerts

Log Collection

You can modify log levels and filters to configure the logs to display. Each log has a severity, product group, and context filter. The log output is rate-limited.

Note If you log to the console and the log level is set too low, the console can quickly become saturated with logs.

Logging Level Control

The console log level defaults to 63. All logs greater than or equal to the console log level display. The filter log level defaults to 50.

Command Syntax

debug sbc <*name*>**log-level ?**

Logging Levels

The log severity levels are as follows:

- 90+: Fatal logs
- 80+: Error logs
- 70+: Unexpected condition logs
- 63+: Configuration error logs (default)
- 60+: Operational logs
- 55+: Call logs
- 50+: Audit logs
- 40+: Statistic logs
- 30+: Verbose logs
- 20+: Verbose statistics
- 10+: Internal diagnostics
- 0: All

Collect Logs

Procedure

Step 1 Enable enough logging buffer for your situation.

```
(config)# logging buffered 99999
(config)# no logging console
```

Step 2 Turn on the appropriate debug level for your situation.

```
# debug sbc SBC-TAC log-level console 50
```

Step 3 Recreate the call flow or issue.

Step 4 Dump the PD log and IPS trace. The default location is to hard disk.

```
# sbc dump-diagnostics
```

Note

```
debug sbc [sbc] log-level console 0
```

The command should be running before you perform dump diagnostics. Issue the dump diagnostics command to start the diagnostics dumping and to stop it.

Step 5 Display the logging or redirect the logging to a file.

```
# show logging | redirect harddisk:mylog.txt
```

Logging Filters

Filter logs according to product group or context. A SIP filter is an example of a product group filter. An adjacency name filter is an example of a context filter.

You can define multiple filters. Filter logs are inclusive. To isolate a log, set the console log level to 100 and activate the filter for the desired context or product group.

Logging Filter Control

The filter log level defaults to 50.

Command Syntax

```
debug sbc <name> filter ?
```

Example

```
#debug sbc global filter?
adjacency  Adjacency name
  bill       Billing ID
  billing    Billing events
  bm         Bandwidth Manager
  cac        Call Admission Control
  call       Call events
  control    H.248 controller
  h323       H.323
  icc        Interworking Call Control
  ipv4       IPv4 address
  ipv6       IPv6 address
  media      Media events
  mgm        Media Gateway Manager
  number     Caller or dialed number
  overview   Showing flow of control
  protocol   Protocol messages
  radius     RADIUS
  routing    Routing
  sip        SIP
  stubs      Portable code Stubs
```

Show Commands

Display Adjacency States

To display the detailed field output of a specified adjacency, use the *show sbc sbe adjacencies detail* command.

Note If the peer status is down , make sure that you can ping the signaling peer by way of virtual routing and forwarding (VRF).

Command Syntax

show sbc {*sbc-name* **} sbe adjacencies {***adjacency name***} detail**

Example

```
#sh sbc asr sbe adjacencies SU-PGW-hpgw311a-1 detail
SBC Service "asr"
  Adjacency SU-PGW-hpgw311a-1 (SIP)
    Status:                Attached
    Signaling address:     10.210.1.2:default, VRF SU-PGW
    IPsec server port:     0
    Signaling-peer:        10.121.31.11:5060 (Default)
    Signaling-peer status: Down
    Signaling-peer priority: 2147483647
    Signaling-peer switch: always
    Peer status: Up
    Current peer index:        3
    Force next hop:        Yes
    Force next hop select: Out-of-dialog
    Admin Domain:          None
    Account:               AAQ-PGW
    Group:                 None
```

Display Overall Media Statistics (Session Border Controller)

To display the statistics for media streams that have been processed, use the show **sbc dbe media-stats** command.

Command Syntax

show sbc {*sbc-name***} dbe media-stats**

Example

```
#sh sbc asr dbe media-stats
SBC Service "asr"
  Available Bandwidth     = Unlimited
  Available Flows         = 131072
  Available Packet Rate   = Unlimited
  Active Media Flows      = 0
```

```
 Peak Media Flows        = 8
 Total Media Flows       = 929
 Active Transcoded Flows = 0
 Peak Transcoded Flows   = 0
 Total Transcoded Flows  = 0
 Active Signaling Flows  = 0
 Peak Signaling Flows    = 0
 Total Signaling Flows   = 0
 SBC Packets Received    = 21034794
 SBC Octets Received     = 1470560584
 SBC Packets Sent        = 21021185
 SBC Octets Sent         = 1469618900
 SBC Packets Discarded   = 14915
 SBC Octets Discarded    = 999122
 No Media Count          = 176
```

Display Platform Software Status Control Processor

For information about the usage of the Route Processor, use the **show platform software status control-processor brief** command.

Command Syntax

show platform software status control-processor brief

Example

```
# show platform software status control-processor brief
Load Average
 Slot  Status  1-Min  5-Min 15-Min
  RP0 Healthy   0.02   0.10   0.08
  RP1 Healthy   0.00   0.13   0.09
 ESP0 Healthy   0.00   0.15   0.10
 ESP1 Healthy   0.01   0.18   0.13
 SIP0 Healthy   0.00   0.06   0.04

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
  RP0 Healthy  8133924  1804132 (12%)  6329792 (77%)   5132856 (63%)
  RP1 Healthy  8133924  1758800 (11%)  6375124 (78%)   5130308 (63%)
 ESP0 Healthy  2022288   552424 (16%)  1469864 (70%)   2464260 (117%)
 ESP1 Healthy  2022288   552616 (16%)  1469672 (70%)   2464680 (117%)
 SIP0 Healthy   478904   331268 (63%)   147636 (18%)    271072 (51%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
  RP0    0   0.19   0.29   0.00  99.40   0.00   0.09   0.00
         1   0.00   0.00   0.00 100.00   0.00   0.00   0.00
  RP1    0   0.20   0.60   0.00  99.19   0.00   0.00   0.00
         1   0.10   1.20   0.00  98.70   0.00   0.00   0.00
 ESP0    0   1.60   2.70   0.00  95.69   0.00   0.00   0.00
 ESP1    0   0.20   0.10   0.00  99.69   0.00   0.00   0.00
 SIP0    0   1.60   2.00   0.00  96.40   0.00   0.00   0.00
```

Other Useful Show Commands

General

```
show clock
show version
show running-config
```

DBE

```
show sbc <name> dbe addresses
show sbc <name> dbe controllers
show sbc <name> dbe forwarder-stats
show sbc <name> dbe media-flow-stats
show sbc <name> dbe signaling-flow-stats
show sbc <name> dbe history
```

SBE

```
show sbc <name> sbe sip stats
show sbc <name> sbe call-rate-stats
show sbc <name> sbe calls
show sbc <name> sbe call-stats-currenthour
show sbc <name> sbe policy-failure-stats currenthour
```

PD and IPS Log for Case Report

To debug SBC services, two types of tracing and logging are available:

- PD: The Problem Determination log is similar to the IOS log, where all system event messages are automatically saved in a log file.
- IPS: The Interprocess Signaling trace shows the graphical call flow of a call. Use the executable utility *sigtrace* to postprocess the IPS trace.

Generate a PD Log and IPS Trace

Procedure

Step 1 Make sure sbc diagnostics sparse is not configured on SBC.

Step 2 Run **sbc dump-diagnostics**. The command removes previous logging information.

Step 3 Debug **sbc** <*sbc-name*> **log-level buffer 0**.

Step 4 Show run.

Step 5 Reproduce the problem.

Step 6 Run **sbc dump-diagnostics** again.

Step 7 Get the latest PD/IPS log in either bootflash or harddisk.

```
#dir *.log
Directory of bootflash:/*.log
Directory of bootflash:/
```

```
41  rw    50503  Oct 19 2010 02:22:20 +00:00  20101019_022220_manual_pdtrc.log
44  rw   965685  Oct 19 2010 02:22:20 +00:00  20101019_022220_manual_ipstrc_buf.log
89  rw  9784704  Oct 19 2010 07:29:07 +00:00  20101019_023634_manual_ipstrc_1.log
```

Step 8 Use the **ftp: or more** command to review the PD log to determine the reason for the failure.

Example

```
#sbc dump-diagnostics
#
Dumping diagnostics to harddisk:/20090518_105331_manual_pdtrc.log
Dumping diagnostics to harddisk:/20090518_105331_manual_ipstrc.log
```

Common Debug Scenarios

The following are common debug scenarios including the most common fix.

Configuration Error

Session Border Controller basic configuration involves many lines of configuration. Always review the configuration and check for typos.

SIP/H.323 Call Does Not Go Through

If the issue is related to routing or SIP/ H.323 signaling, enable PD logs with the debug command as explained in the Collect Logs, on page 11 section. Review the PD logs to determine the root cause.

No Media Flow While Signaling Looks Good

It is likely that RTP packets cannot reach the SBC. Ensure that the media-address on SBC is reachable from both endpoints.

High Traffic Troubleshooting

Use the **show sip statistics** command to isolate the adjacency that is causing the issue.

Integrated Services Router G1

This section covers troubleshooting for Cisco 1800 Series, 2800 Series, and 3800 Series ISR G1 (SRST).

For more information, see:

Cisco 1800 Series Integrated Services Routers Troubleshooting TechNotes

Cisco 2800 Series Integrated Services Routers Troubleshooting TechNotes

Cisco 3800 Series Integrated Services Routers Troubleshooting TechNotes

Integrated Services Router G2

This section covers troubleshooting for Cisco 1900 Series, 2900 Series, and 3900 Series ISR G2 (SRST).

Fault Indications

Check the following LED indications to isolate faults:

With the power switch on, is the SYS LED on green?

- If the LED is green and continuous, the router has booted and the software is functional.
- If the LED is blinking green, the system is booting or in ROM monitor mode.
- If the LED is off, the system board is faulty.
- If the LED is amber, check for a system error.

With the power switch on and the SYS LED on and green, does the fan operate?

- If no, check the fan.
- If yes, the power system is functioning.

With the power switch on and the SYS LED off, does the fan operate?

- If yes, the router is receiving power. The fan is connected directly to the DC outputs of the power supply.
- If no, check the power source and power cable.

Does the router shut down after being on a short time?

- Check for an environmentally induced shutdown.
- If no, check the power source and power cable.

Does the router partially boot up?

- Check for a power supply failure by inspecting the SYS LED on the front panel of the router. If the SYS LED is blinking or continuously green, the power supply is functional.
- If the SYS LED is not on contact customer service.

For more information, see *Troubleshooting Cisco 3900 Series, 2900 Series, and 1900 Series ISRs*, at:

http://www.cisco.com/en/US/products/ps10538/prod_troubleshooting_guides_list.html

VMware vCenter

For information about troubleshooting for VMware vCenter, go to:

https://www.vmware.com/support/vcenter-server.html

Troubleshooting Cluster Connections

The following table provides the list of error messages, and the corresponding references for troubleshooting clusters' connectivity.

Table 1: Cluster Connectivity Error Messages

Error Message	References or Recommended Action
Cluster connection failed. The CHPA service is inactive.	For assistance on activating services, see Working with Services, on page 19.
Cluster connection failed. The UCPA service is inactive.	
Cluster connection failed. Verify the following entities: • Cisco AXL Web Service is active • ADMIN credentials • Network address	• For assistance on activating services, see Working with Services, on page 19. • To either verify or update application details like credentials, network address, and so on; click the corresponding application in the **Monitoring Application** column. **Note** If credentials are updated, restart the Cisco HCS Provisioning Adapter (CHPA) service.
Cluster connection failed. Verify the configuration of service provider's address.	
Cluster connection failed. Verify ADMIN credentials.	
Cluster connection failed. Verify the following entities: • Network address • The version, and credentials of cluster	
Cluster connection failed. Verify the following entities: • Connectivity to UCXN • ADMIN credentials • The version, and address of network	• To verify connectivity to Cisco Unity Connection, check the network connectivity. • To either verify or update admin credentials, or network address; click the corresponding application in the **Monitoring Application** column. **Note** If Cisco Unity Connection credentials are updated, restart the Cisco Unity Connection Provisioning Adapter (UCPA) service.

Working with Services

To start, stop, activate, or restart services or to configure service parameters for services on the Cisco HCM-F platform, you must use the Command Line Interface (CLI). You can start, stop, activate, or refresh only one service at a time. When a service stops, you cannot start it until the service is stopped. Likewise, when a service starts, you cannot stop it until the service is started.

The following table shows the commands that you need to work with services on the Cisco HCM-F platform:

Table 2: Service CLI Commands

Task	Command
Display a list of services and service status	**utils service list**
Activate a service	**utils service activate** *servicename*
Stop a service	**utils service stop** *servicename*
Start a service	**utils service start** *servicename*
Restart a service	**utils service restart** *servicename*
Show service parameters	**show hcs** *servicetype* ?
Set service parameters	**set hcs** *servicetype serviceparametername***?** Select a value from the displayed values.