This article provides configuration examples for administrative tasks. For details about configuring administrative functions on the ACE, see the *Cisco Application Control Engine Module Administration Guide*.

To return to the main article, click here.

Contents

Example of a Remote Access Configuration

The following CLI example shows how to configure remote access to the ACE through the use of class maps, policy maps, and service policies:

Step 1. Enter configuration mode and set the maximum number of Telnet and SSH sessions.

```
host1/Admin# config

host1/Admin(config)# telnet maxsessions 3

host1/Admin(config)# ssh maxsessions 3
```

Step 2. Create and configure a class map for network management traffic. Here you can also specify the subnets and/or hosts that are able to access the ACE management. The following CLI shows that only users from the 10.0.0.0/24 subnet can access the ACE via TELNET or SSH, but anyone can use PING to verify reach-ability to the ACE.

```
host1/Admin(config)# class-map type management match-any L4_REMOTE-MGT_CLASS

host1/Admin(config-cmap-mgmt)# description Allows Telnet, SSH, and ICMP protocols

host1/Admin(config-cmap-mgmt)# 2 match protocol telnet 10.0.0.0 255.0.0.0

host1/Admin(config-cmap-mgmt)# 3 match protocol ssh 10.0.0.0 255.0.0.0

host1/Admin(config-cmap-mgmt)# 4 match protocol icmp any

host1/Admin(config-cmap-mgmt)# exit

host1/Admin(config)#
```

Step 3. Create and configure a policy map that activates the SSH and Telnet management protocol classifications.

```
host1/Admin(config)# policy-map type management first-match L4_REMOTE-MGT_POLICY

host1/Admin(config-pmap-mgmt)# class L4_REMOTE-MGT_CLASS
```

```
host1/Admin(config-pmap-mgmt-c)# permit

host1/Admin(config-pmap-mgmt-c)# exit

host1/Admin(config-pmap-mgmt)# exit

host1/Admin(config)#
```

Step 4. Apply the traffic policy to a specific VLAN interface or globally to all VLAN interfaces and enable the interface.

Apply to a specific VLAN interface:

```
host1/Admin(config)# interface vlan 50

host1/Admin(config-if)# ip address 192.168.1.1 255.255.255.0

host1/Admin(config-if)# service-policy input L4_REMOTE-MGT_POLICY

host1/Admin(config-if)# no shutdown

host1/Admin(config-if)# exit

host1/Admin(config)#
```

Apply globally to all VLAN interfaces:

```
host1/Admin(config)# service-policy input REMOTE_MGMT_ALLOW_POLICY
```

Step 6. Generate the SSH private key and corresponding public key for use by the SSH server.

```
host1/Admin(config)# ssh key rsa1 1024 force
```

Step 7. Save the configuration to Flash memory.

```
host1/Admin(config)# do copy running-config startup-config
```

Example of a Redundant Configuration

This section shows an example of a redundant configuration and illustrates a running-configuration that defines fault tolerance (FT) for a single ACE module operating. You must configure a maximum of two ACE modules (peers) for redundancy to fail over from the active module to the standby module.

With two ACE appliances, **you have to tag/trunk the port** on switches where you will connect the FT interfaces.

Note All FT parameters are configured in the Admin context.

This configuration addresses the following redundancy components:

- A peer hostname for the redundant ACE.
- A shared-vlan-hostid and peer shared-vlan-hostid so that the redundant ACEs don't use the same bank of MAC addresses.
- An FT peer definition, including an FT query VLAN interface.
- A dedicated FT VLAN for communication between the members of an FT group. You must configure this same VLAN on both peer modules. With appliances, tag/trunk the port on external

switches.
- An FT peer definition, including an FT query VLAN interface.
- An FT group that is associated with the Admin context.
- A critical tracking and failure detection process for an interface.

The redundancy-specific configuration elements appear in bold in the example.

```
hostname ACE_Module_1
peer hostname ACE_Module_2
shared-vlan-hostid 5
peer shared-vlan-hostid 6

access-list ACL1 line 10 extended permit ip any any

class-map type management match-any L4_REMOTE-MGT_CLASS
  2 match protocol telnet any
  3 match protocol ssh any
  4 match protocol icmp any
  5 match protocol http any
  7 match protocol snmp any
  8 match protocol https any

policy-map type management first-match L4_REMOTE-MGT_POLICY
  class L4_REMOTE-MGT_CLASS
    permit

interface vlan 100
  ip address 192.168.83.219 255.255.255.0
  peer ip address 192.168.83.230 255.255.255.0
  alias 192.168.83.200 255.255.255.0
  access-group input ACL1
  service-policy input L4_REMOTE-MGT_POLICY
  no shutdown

ft interface vlan 200
  ip address 192.168.1.1 255.255.255.0
  peer ip address 192.168.1.2 255.255.255.0
  no shutdown

ft peer 1
  ft-interface vlan 200
  heartbeat interval 300
  heartbeat count 10
  query-interface vlan 100

ft group 1
  peer 1
  priority 200
  associate-context Admin
  inservice

ft track interface TRACK_VLAN100
  track-interface vlan 100
  peer track-interface vlan 200
  priority 50
  peer priority 5

ip route 0.0.0.0 0.0.0.0 192.168.83.1
```

Example of an SNMP Configuration

The following example illustrates a running-configuration that verifies the current status of a real server through SNMP and the CLI. It also verifies that SNMP traps are sent when a real server or virtual server is not operational. This example illustrates that you can restrict the client source host IP address allowed to connect to the ACE. The policy map is applied to all of the VLAN interfaces associated with the context. The SNMP configuration appears in bold in the example.

```
access-list ACL1 line 10 extended permit ip any any

rserver host SERVER1
  ip address 192.168.252.245
  inservice

rserver host SERVER2
  ip address 192.168.252.246
  inservice

rserver host SERVER3
  ip address 192.168.252.247
  inservice

serverfarm host SFARM1
  probe HTTP_PROBE
  rserver SERVER1
    conn-limit max 3 min 2
    inservice

serverfarm host SFARM2
  probe HTTP
  rserver SERVER2
    conn-limit max 500 min 2
    inservice
  rserver SERVER3
    conn-limit max 500 min 2
    inservice

class-map type http loadbalance match-all L7_INDEX-HTML_CLASS
  2 match http url /index.html
class-map match-all L4_MAX-CONN-VIP_105_CLASS
  2 match virtual-address 192.168.120.105 any

class-map type management match-any L4_REMOTE-ACCESS-LOCAL_CLASS
  description Enables SNMP remote management for local users
  1 match protocol snmp source-address 192.168.0.0 255.248.0.0
  2 match protocol snmp source-address 172.16.64.0 255.255.252.0
class-map type http loadbalance match-all L7_URL*_CLASS
  2 match http url .*

policy-map type management first-match L4_SNMP-REMOTE-MGT_POLICY
  class L4_REMOTE-ACCESS-LOCAL_CLASS
    permit

policy-map type loadbalance first-match L7_LB-SF_MAX-CONN_POLICY
  class L7_INDEX-HTML_CLASS
    serverfarm SFARM1
  class L7_URL*_CLASS
    serverfarm SFARM2

policy-map multi-match L4_VIP_POLICY
  class L4_MAX-CONN-VIP_105_CLASS
    loadbalance vip inservice
```

```
    loadbalance policy L7_LB-SF_MAX-CONN_POLICY
    loadbalance vip icmp-reply
    appl-parameter http advanced-options PERSIST-REBALANCE

service-policy input L4_REMOTE-MGT_POLICY

snmp-server user user1 Network-Monitor auth sha "adcd1234"
snmp-server community ACE-public group ro
snmp-server contact "User1 user1@cisco.com"
snmp-server location "San Jose CA"
snmp-server host 192.168.0.236 traps version 2c ACE-public
snmp-server enable traps slb vserver
snmp-server enable traps slb real
snmp-server enable traps syslog
snmp-server enable traps snmp authentication
snmp-server enable traps snmp linkup
snmp-server enable traps snmp linkdown

ip route 0.0.0.0 0.0.0.0 192.168.252.1
```

Example of an ACE CLI Command and the XML Equivalent

The following example shows a typical VShell (VSH) CLI command configuration and its equivalent XML configuration commands:

```
##############################
## TO/FROM CP CONFIGURATION ##
##############################

conf t
access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
ip address 10.0.0.145 255.255.255.0
no shut
exit
ip route 0.0.0.0 0.0.0.0 10.0.0.1
end

<access-list id="acl1" config-type="extended" perm-value="permit"
protocol-name="ip" src- type="any" dest-type="any"/>
<interface type="vlan" number="80">
<access-group type="input" name="acl1"/>
<ip_address address="10.0.0.145" netmask="255.255.255.0"/>
<shutdown sense="no"/>
</interface>
<ip_route dest-address="0.0.0.0" dest-mask="0.0.0.0"
gateway="10.0.0.1"/>

############################
## BRIDGING CONFIGURATION ##
############################

conf t
access-list acl1 extended permit ip any any
int vlan 80
access-group input acl1
bridge-group 1
no shut
exit

int vlan 90
```

```
access-group input acl1
bridge-group 1
no shut
exit
end

<access-list id="acl1" config-type="extended" perm-value="permit"
protocol-name="ip" src-type="any" dest-type="any"/>
<interface type="vlan" number="80">
<access-group type="input" name="acl1"/>
<bridge-group value="1"/>
<shutdown sense="no"/>
</interface>
<interface type="vlan" number="90">
<access-group type="input" name="acl1"/>
<bridge-group value="1"/>
<shutdown sense="no"/>
</interface>
```