Configure High Availability

The following sections specify the common configuration steps to configure High Availability for a Cisco Catalyst 8000V running on any cloud service provider.

Configuring IOX and the Guestshell on Cisco IOS XE

The following Cisco IOS XE configuration shows the commands that are required to access the guestshell. You do not need to configure these prerequisites as they are included automatically in the startup-config file.

SUMMARY STEPS

1. Perform the following configuration:
2. To configure High Availability, you must verify whether IOX is configured and running:
3. Enter the following command to verify that the guest application is defined and running:

DETAILED STEPS

	Command or Action	Purpose

Step 1	Perform the following configuration:
	Example:
	`iox`
	`ip nat inside source list GS_NAT_ACL interface GigabitEthernet1 vrf GS overload ip route vrf GS 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.35.1 global`
	`interface VirtualPortGroup0 vrf forwarding GS`
	`ip address 192.168.35.101 255.255.255.0`
	`ip nat inside no mop enabled no mop sysid`
	`ip access-list standard GS_NAT_ACL permit 192.168.35.0 0.0.0.255`
	`app-hosting appid guestshell`	

	Command or Action	Purpose
	app-vnic gateway1 virtualportgroup 0 guest-interface 0 guest-ipaddress 192.168.35.102 netmask 255.255.255.0 app-default-gateway 192.168.35.101 guest-interface 0 name-server0 8.8.8.8	
Step 2	To configure High Availability, you must verify whether IOX is configured and running: **Example:** show iox Virtual Service Global State and Virtualization Limits: Infrastructure version : 1.7 Total virtual services installed : 0 Total virtual services activated : 0 Machine types supported : LXC Machine types disabled : KVM Maximum VCPUs per virtual service : 1 Resource virtualization limits: Name Quota Committed Available --- system CPU (%) 75 0 75 memory (MB) 3072 0 3072 bootflash (MB) 20000 0 5745 IOx Infrastructure Summary: --------------------------- IOx service (CAF) : Running IOx service (HA) : Not Running IOx service (IOxman) : Running Libvirtd : Running	
Step 3	Enter the following command to verify that the guest application is defined and running: **Example:** show app-hosting list show app-hosting list App id State --- guestshell RUNNING	If the state of the guestshell displays DEPLOYED in the output of the preceding command, you must enable the guestshell by using the following command: guestshell enable Interface will be selected if configured in app-hosting Please wait for completion guestshell activated successfully Current state is: ACTIVATED guestshell started successfully Current state is: RUNNING Guestshell enabled successfully

Configure a Tunnel Between the Cisco Catalyst 8000V Routers

You must configure a tunnel between the Cisco Catalyst 8000V routers and enable Bi-directional Forwarding Detection (BFD) and a routing protocol (EIGRP or BGP) on the tunnel for peer failure detection. To authenticate and encrypt IP traffic as it traverses a network, either use an IPsec tunnel or VxLAN GPE tunnel.

Step 1 To configure an IPsec tunnel, enter the configuration mode commands to give the following configuration. The command crypto isakmp policy 1 defines an IKE policy, with a high priority (1), and enters config-isakmp configuration mode.

Example:

```
Crypto isakmp policy 1
encr aes 256 authentication pre-share
```

```
crypto isakmp key cisco address 0.0.0.0
!
crypto ipsec transform-set uni-perf esp-aes 256 esp-sha-hmac mode tunnel
!
crypto ipsec profile vti-1
set security-association lifetime kilobytes disable set security-association lifetime seconds 86400
  set transform-set uni-perf
set pfs group2
!
interface Tunnel1
ip address 192.168.101.1 255.255.255.252
load-interval 30
tunnel source GigabitEthernet1 tunnel mode ipsec ipv4
tunnel destination 23.96.91.169 tunnel protection ipsec profile vti-1
bfd interval 100 min_rx 100 multiplier 3
```

Step 2 To create a VxLAN GPE tunnel, enter the following configuration

```
interface Tunnel100
ip address 192.168.101.1 255.255.255.0
bfd interval 100 min_rx 100 multiplier 3 tunnel source GigabitEthernet1
tunnel mode vxlan-gpe ipv4 tunnel destination 40.114.93.164
tunnel vxlan vni 10000
```

For further information on configuring a VxLAN GPE tunnel, see the Carrier Ethernet Configuration Guide.

The tunnel destination address must be the public IP address of the corresponding Cisco Catalyst 8000V. For the tunnel IP address, use any unique IP address. However, the tunnel endpoints of each redundantCisco Catalyst 8000V must be in the same subnet.

Note To allow VxLAN to pass traffic through the tunnel, you must ensure that UDP ports 4789 and 4790 are allowed in the cloud's network security group. See the cloud provider's documentation for configuring network security filters.

Configuring EIGRP over Virtual Tunnel Interfaces

Configure EIGRP over the virtual tunnel interfaces using the following steps.

Note Other than using EIGRP, which is the protocol that is used in the following steps, you also have the option of using either BGP, or OSPF.

Before you begin

Configure either a VxLAN or IPsec tunnel between the Cisco Catalyst 8000V routers.

Step 1 **router eigrp** *as-number*

Example:

```
Device(config)# router eigrp 1
```

Enables the EIGRP routing process and enters the router configuration mode.

Step 2 **network** *ip-address subnet-mask*

Share the network of the tunnel using EIGRP.

Example:

```
network 192.168.101.0 0.0.0.255
```

Step 3 **bfd all-interfaces**

Enables BFD globally on all the interfaces that are associated with the EIGRP routing process.

Example:

```
Device(config-router)# bfd all-interfaces
```

Step 4 **end**

Exits the router configuration mode and returns the router to the privileged EXEC mode.

Example:

```
Device(config-router)# end
```

Step 5 **show bfd neighbors**

Verifies that the BFD neighbor is active and displays the routing protocols that BFD has registered.

Example:

```
Device# show bfd neighbors

IPv4 Sessions
NeighAddr      LD/RD        RH/RS    State  Int
192.168.101.2  4097/4097    Up       Up     Tu100
```

Verify the Tunnel Surface

To verify that the tunnel interface is configured and enabled, run the `show ip interface brief` command.

Example:

```
# show ip interface brief
 IP-Address OK? Method Status Protocol
GigabitEthernet1 192.168.35.20 YES DHCP up up
GigabitEthernet2 192.168.36.12 YES DHCP up up
Tunnel1                 172.17.1.1         YES NVRAM      up up
VirtualPortGroup0 192.168.35.101     YES NVRAM      up up
```

Configure the BFD Peer Router

Run the following command:

Example:

```
redundancy
cloud-ha bfd peer <peer_router_ip_address>
```

This configuration command identifies the peer router. The IP address is that of the peer Cisco Catalyst 8000V within the tunnel carrying the BFD protocol between the two Cisco Catalyst 8000V routers.

Install the High Availability Package

Step 1 Run the `#Router> guestshell` command to enter the guestshell.

Step 2 Install the appropriate Python package based on the cloud provider on which the Cisco Catalyst 8000V instance is running:

Cloud Provider	Package Name
Microsoft Azure	csr_azure_ha
Amazon Web Services	csr_aws_ha
Google Cloud Platform	csr_gcp_ha

Note The package name for Microsoft Azure is the same for both HAv2 and HAv3. If you perform an install by executing the `pip install csr_azure_ha --user` command, the latest HA V3 is downloaded.

Step 3 Install the package that is appropriate for your cloud service provider by using the `[guestshell@guestshell]$ pip install <package_name> --user` command.

Step 4 From the home directory, navigate to the subdirectory named `cloud:[guestshell@guestshell]$ cd cloud`.