



This PDF is generated from authoritative online content, and is provided for convenience only. This PDF cannot be used for legal purposes. For authoritative understanding of what is and is not supported, always use the online content. To copy code samples, always use the online content.

Integration Reference Manual

Configuring BIG-IP LTM

12/17/2025

Configuring BIG-IP LTM

The following page provides an overview of the main steps that are required in order to configure the BIG-IP LTM. Complete all steps in the order in which they are listed.

Integrating with BIG-IP LTM

1. Check Prerequisites.

Verify that BIG-IP LTM is working

The procedures in this topic assume that the BIG-IP LTM is properly licensed and fully functional, with login and password access configured. For more information, see BIG-IP LTM specific documentation.

2. Configure VLANs.

Configuring VLANs

Purpose

To configure two VLANs (Virtual Local Area Networks): one VLAN for the external interface (physical interface 1.3) and one VLAN for the internal (SIP Server side) interface (physical interface 1.6). VLANs are used to logically associate Self IP interfaces with physical interfaces on the BIG-IP LTM.

Prerequisites

- You are logged in to the BIG-IP LTM web interface.

Start

1. Go to **Network > VLANs > VLAN List**.
2. Click **Create**.
3. In the dialog box that appears, specify the following properties:
 - a. **Name**: Enter the VLAN name for the external interface—for example, `dc1ext`.
 - b. **Tag**: 4092 (it is set automatically).

- c. Resources > Interfaces > Untagged: Select 1.3 in the Available section and click the left-pointing arrow button to move it into the Untagged section.

Network > VLANs > VLAN List > dc1ext

Properties Layer 2 Static Forwarding Table

General Properties

Name	dc1ext
Partition / Path	Common
Description	DC1 External
Tag	4092

Resources

Interfaces

Untagged	Available	Tagged
1.3	1.1 1.2 1.4 1.5 1.6	

Configuration: Basic

Source Check: ☐

MTU: 1500

Auto Last Hop: Default

Configuring a VLAN for the External Interface

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the VLAN name for the internal interface—for example, dc2sip.
 - b. Tag: 4090 (it is set automatically).
 - c. Resources > Interfaces > Untagged: Select 1.6 in the Available section and click the left-pointing arrow button to move it into the Untagged section.

Network > VLANs > VLAN List > dc1ext

Properties Layer 2 Static Forwarding Table

General Properties

Name	dc1ext
Partition / Path	Common
Description	DC1 External
Tag	4092

Resources

Interfaces

Untagged	Available	Tagged
1.3	1.1 1.2 1.4 1.5 1.6	

Configuration: Basic

Source Check: ☐

MTU: 1500

Auto Last Hop: Default

Configuring a VLAN for the Internal Interface

7. Click Finished.
-

End

3. Configure Self IP addresses.

Configuring Self IP addresses

Purpose

To configure two Self IP addresses—one for the external interface and one for the internal interface—and associate them with the VLANs, to access hosts in those VLANs.

Prerequisites

- [Procedure: Configuring VLANs](#)

Start

1. Go to Network > Self IPs.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for the Self IP address—for example, dc1ipext.
 - b. IP Address: Enter the IP address for the internal interface—for example, 192.168.166.229.
 - c. Netmask: Enter the netmask—for example, 255.255.255.240.
 - d. VLAN: Select the name of the VLAN to which you want to assign the Self IP address—for example, dc1ext.

Configuration	
Name	dc1ipext
Partition / Path	Common
IP Address	192.168.166.229
Netmask	255.255.255.240
VLAN / Tunnel	dc1ext
Port Lockdown	Allow Default
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)

Configuring a Self IP Address for the External Interface

4. Click Finished.
5. Click Create.

6. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for the Self IP address—for example, dc2ipsip.
 - b. IP Address: Enter the IP address for the internal interface—for example, 192.168.167.96.
 - c. Netmask: Enter the netmask—for example, 255.255.255.128.
 - d. VLAN: Select the name of the VLAN to which you want to assign the self IP address—for example, dc2sip.

The screenshot shows the 'Properties' tab for a Self IP address named 'dc2ipsip'. The configuration fields are as follows:

Configuration	
Name	dc2ipsip
Partition / Path	Common
IP Address	192.168.167.96
Netmask	255.255.255.128
VLAN / Tunnel	dc2sip
Port Lockdown	Allow Default
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)

Configuring a Self IP Address for the Internal Interface

7. Click Finished.

End

4. Configure the Default IP route.

Configuring the Default IP route

Purpose

To configure the default IP route.

Prerequisites

- [Procedure: Configuring Self IP addresses](#)

Start

1. Go to Network > Routes.
2. Click Add.
3. In the dialog box that appears, specify the following properties:

- a. Name: Enter Default.
- b. Resource: Select Use Gateway.
- c. Gateway Address: Enter the IP address for this default IP route—for example, 192.168.166.225.

Properties	
Name	Default
Partition / Path	Common
Destination	0.0.0.0
Netmask	0.0.0.0
Partition	Common
Resource	Use Gateway...
Gateway Address	IP Address 192.168.166.225

Configuring Default IP Route

4. Click Finished.

End

5. Configure SIP Server nodes.

Configuring SIP Server nodes

Purpose

To configure two SIP Server nodes, primary and backup.

Prerequisites

- [Procedure: Configuring the Default IP route](#)

Start

1. Go to Local Traffic > Nodes.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the node name—for example, nodeHa01Primary.
 - b. Address: Enter the IP address for the primary SIP Server node—for example, 192.168.167.125.
 - c. Health Monitors: Select Node Specific.

- d. Select Monitors > Active: Select icmp.

Local Traffic » Nodes: Node List » nodeHa01Primary

Properties Statistics

General Properties

Name	nodeHa01Primary
Address	
Partition / Path	Common
Description	192.168.167.125
Availability	Available (Enabled) - Node address is available
Health Monitors	icmp
Current Connections	3
State	<input checked="" type="radio"/> Enabled (All traffic allowed) <input type="radio"/> Disabled (Only persistent or active connections allowed) <input type="radio"/> Forced Offline (Only active connections allowed)

Configuration

Health Monitors: Node Specific

Select Monitors:

Active	Available
Common icmp	Common gateway_icmp https_443 real_server snmp_dca

Availability Requirement: All Health Monitor(s)

Ratio: 1

Connection Limit: 0

Configuring a Primary SIP Server Node

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the node name—for example, nodeHa01Backup.
 - b. Address: Enter the IP address for the backup SIP Server node—for example, 192.168.167.126.
 - c. Health Monitors: Select Node Specific.
 - d. Select Monitors > Active: Select icmp.

The screenshot shows the configuration page for a node named 'nodeHa01Backup'. The interface is divided into two main sections: 'General Properties' and 'Configuration'.

General Properties:

- Name: nodeHa01Backup
- Address: 192.168.167.126
- Partition / Path: Common
- Description: (empty field)
- Availability: ● Available (Enabled) - Node address is available
- Health Monitors: ● icmp
- Current Connections: 0
- State: ☒ Enabled (All traffic allowed)
☐ Disabled (Only persistent or active connections allowed)
☐ Forced Offline (Only active connections allowed)

Configuration:

- Health Monitors: Node Specific
- Select Monitors:

Active

Common
icmp

Available

Common
gateway_icmp
https_443
real_server
snmp_dca
- Availability Requirement: All Health Monitor(s)
- Ratio:
- Connection Limit:

Configuring a Backup SIP Server Node

7. Click Finished.

6. Configure a health monitor.

Configuring a health monitor

In general, the BIG-IP LTM uses health monitors to determine whether a server to which messages can be routed is operational (active). Servers that are flagged as not operational (inactive) will cause the BIG-IP LTM to route messages to another server if one is present in the same server pool. However, primary and backup SIP Servers must be configured as the only members of the same server pool—one member active (primary) and one member inactive (backup).

In this procedure, the BIG-IP LTM is configured to use the health monitor of SIP type in UDP mode. This means that the `OPTIONS` request method will be sent to both primary and backup SIP Servers. Any response to `OPTIONS` is configured as Accepted Status Code.

SIP Server always starts in backup mode, establishes a permanent connection with the Genesys Management Layer, and changes its role to primary only if a trigger from the Management Layer is received. Such trigger is only generated if no other primary SIP Server is currently running. After switching to primary mode, SIP Server responds to UDP packets received on the SIP port specified by the sip-port configuration option. Therefore, after receiving the `OPTIONS` request from the BIG-IP

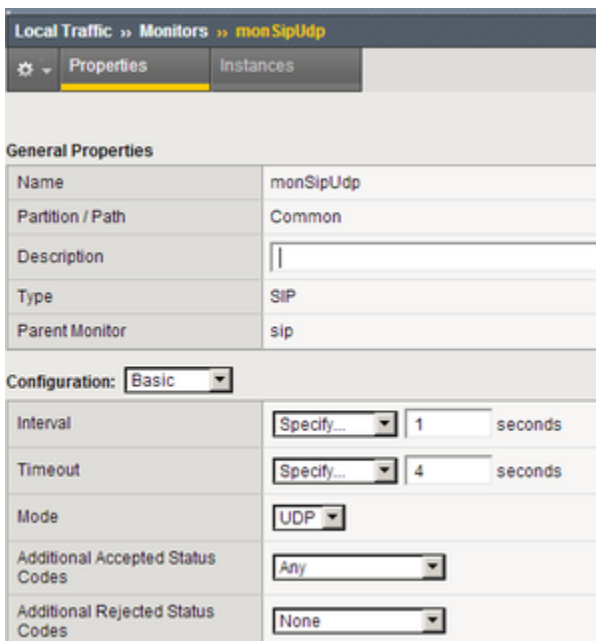
LTM, SIP Server responds to the health check, and the BIG-IP LTM marks SIP Server as active.

When running in backup mode, SIP Server ignores UDP messages. Since the BIG-IP LTM does not receive any response to the OPTIONS request, it marks the backup SIP Server as inactive. If SIP Server does not respond because of network latency or other reasons, the BIG-IP LTM will mark SIP Server as inactive, and continue sending ping messages periodically.

The Interval setting defines how often pool members (primary and backup) are checked for presence. The Timeout setting defines the waiting time before an unresponsive member of the pool is marked as inactive. Regardless of the member's status (or SIP Server status), the BIG-IP LTM will always check servers for presence. When an inactive member responds to the health check, it is marked as active. In this configuration, the Interval parameter is set to 1 second and Timeout to 4 seconds in order to minimize a possible delay that might result from a switchover.

Start

1. Go to Local Traffic > Monitors.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this health monitor—for example, monSipUdp.
 - b. Type: Select SIP.
 - c. Configuration: Select Basic.
 - d. Interval: Enter 1 (seconds).
 - e. Timeout: Enter 4 (seconds).
 - f. Mode: Select UDP.
 - g. Additional Accepted Status Codes: Select Any.



Local Traffic » Monitors » monSipUdp

Properties Instances

General Properties

Name	monSipUdp
Partition / Path	Common
Description	
Type	SIP
Parent Monitor	sip

Configuration: Basic

Interval	Specify... 1 seconds
Timeout	Specify... 4 seconds
Mode	UDP
Additional Accepted Status Codes	Any
Additional Rejected Status Codes	None

Configuring a Health Monitor

4. Click Finished.

End

7. Configure a server pool.

Configuring a server pool

Purpose

To configure a server pool with which the BIG-IP LTM will communicate.

Start

1. Go to Local Traffic > Pools.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this server pool—for example, the poolHa01.
 - b. Health Monitors > Active: Select monSipUdp.
 - c. Action On Service Down: Select Reselect.
 - d. Priority Group Activation: Select Disabled.

The screenshot shows the 'Local Traffic > Pools > Pool List > poolHa01' configuration page. The 'Properties' tab is selected. The 'General Properties' section shows the pool name 'poolHa01', partition 'Common', and availability status 'Available (Enabled) - The pool is available'. The 'Configuration' section is set to 'Advanced'. The 'Health Monitors' section shows two monitors: 'monSipUdp' (Active) and 'gateway_icmp' (Available). The 'Availability Requirement' is set to 'All'. Other settings include 'Allow SNAT' (Yes), 'Allow NAT' (Yes), 'Action On Service Down' (Reselect), 'Slow Ramp Time' (0 seconds), 'IP ToS to Client' (Pass Through), 'IP ToS to Server' (Pass Through), 'Link QoS to Client' (Pass Through), 'Link QoS to Server' (Pass Through), 'Reselect Tries' (0), 'Enable Request Queueing' (No), 'Request Queue Depth' (0), and 'Request Queue Timeout' (0 ms).

General Properties	
Name	poolHa01
Partition / Path	Common
Description	
Availability	Available (Enabled) - The pool is available

Configuration: **Advanced**

	Active	Available
Health Monitors	Common monSipUdp	Common gateway_icmp http http_head_f5 https

Availability Requirement	All Health Monitor(s)
Allow SNAT	Yes
Allow NAT	Yes
Action On Service Down	Reselect
Slow Ramp Time	0 seconds
IP ToS to Client	Pass Through
IP ToS to Server	Pass Through
Link QoS to Client	Pass Through
Link QoS to Server	Pass Through
Reselect Tries	0
Enable Request Queueing	No
Request Queue Depth	0
Request Queue Timeout	0 ms

Configuring a Server Pool

4. Click Finished.

End

8. Add server pool members.

Adding server pool members

Purpose

To add primary and backup SIP Servers to the server pool. Note that they must be the only members of this server pool.

Start

1. Go to Local Traffic > Pools > poolHa01 > Members.
2. Click Add.
3. In the dialog box that appears, specify the following properties:
 - a. Node Name: Select the primary server node you created in [Configuring SIP Server nodes](#). In our example, it would be nodeHa01Primary.
 - b. Address: Specify the IP address of the primary server node. In our example, it would be 192.168.167.125.
 - c. Service Port: Enter 5060.

Local Traffic > Pools: Pool List > poolHa01

Properties Members Statistics

Member Properties

Node Name	nodeHa01Primary
Address	192.168.167.125
Service Port	5060
Partition / Path	Common
Description	
Parent Node	nodeHa01Primary
Availability	Available (Enabled) - Pool member is available
Health Monitors	monSipUdp
Current Connections	2
State	<input checked="" type="radio"/> Enabled (All traffic allowed) <input type="radio"/> Disabled (Only persistent or active connections allowed) <input type="radio"/> Forced Offline (Only active connections allowed)

Configuration: Basic

Ratio	1
Priority Group	0
Connection Limit	0

Adding the Primary SIP Server to the Server Pool

4. Click Finished.
5. Click Add.
6. In the dialog box that appears, specify the following properties:
 - a. Node Name: Select the backup server node you created in the [Configuring SIP Server nodes](#). In our example, it would be nodeHa01Backup.
 - b. Address: Specify the IP address of the backup server node. In our example, it would be 192.168.167.126.
 - c. Service Port: Enter 5060.

Local Traffic > Pools: Pool List > poolHa01

Members

Member Properties

Node Name	nodeHa01Backup
Address	192.168.167.126
Service Port	5060
Partition / Path	Common
Description	
Parent Node	nodeHa01Backup
Availability	Offline (Enabled) - Pool member has been marked down by a monitor
Health Monitors	monSipUdp
Current Connections	0
State	<input checked="" type="radio"/> Enabled (All traffic allowed) <input type="radio"/> Disabled (Only persistent or active connections allowed) <input type="radio"/> Forced Offline (Only active connections allowed)

Configuration: Basic

Ratio: 1

Priority Group: 0

Connection Limit: 0

Adding the Backup SIP Server to the Server Pool

- Click Finished.
- Set the Load Balancing Method to Round Robin.
- Go to Local Traffic > Pools. The status of the nodeHa01Primary server pool member displays as available (green).

Local Traffic > Pools: Pool List > poolHa01

Members

Load Balancing

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Update

Current Members

Status	Member	Address	Ratio	Priority Group	Connection Limit	Partition
<input checked="" type="checkbox"/>	nodeHa01Primary5060	192.168.167.125	1	0 (Active)	0	Common
<input type="checkbox"/>	nodeHa01Backup5060	192.168.167.126	1	0 (Inactive)	0	Common

The Server Pool of Two Members

End

9. Configure data groups.

Configuring data groups

Purpose

To configure data groups that will be used by the iRule. One data group (dataGroupSnatHa01)

contains physical IP addresses of primary and backup SIP Server nodes. The second data group (dataGroupSnatExcludedHa01) contains IP addresses of the systems that will be excluded from applying SNAT, such as Genesys Configuration Server, Genesys Message Servers and other SIP Servers in multi-site deployments (see the [Device Communication Groups](#) figure).

Start

1. Go to Local Traffic > iRules > Data Group List.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this data group—for example, dataGroupSnatExcludedHa01.
 - b. Type: Select Address.
 - c. Address Records > Type Host > Address: Enter the host IP address of the primary server node—for example, 192.168.167.125.
 - d. Click Add.
 - e. Address Records > Type Host > Address: Enter the host IP address of the backup server node—for example, 192.168.167.126.
 - f. Click Add.

Local Traffic > iRules : Data Group List > dataGroupSnatHa01

Properties

General Properties

Name	dataGroupSnatHa01
Partition / Path	Common
Type	Address

Records

Type: ☒ Host ☐ Network

Address:

Value:

Add

Address Records

192.168.167.125 := nodeHa01Primary
192.168.167.126 := nodeHa01Backup

Configuring a Data Group for SNAT

4. Click Finished.
5. Click Create.
6. In the dialog box that appears, specify the following properties:

- a. Name: Enter the name for this data group—for example, dataGroupSnatExcluded01.
- b. Type: Select Address.
- c. Address Records > Type Host > Address: Enter the host IP address of Genesys Configuration Server—for example, 172.21.83.193.
- d. Click Add.

The screenshot shows the 'Local Traffic > iRules > Data Group List > dataGroupSnatExcludedHa01' configuration page. The 'Properties' tab is selected. Under 'General Properties', the 'Name' is 'dataGroupSnatExcludedHa01', 'Partition / Path' is 'Common', and 'Type' is 'Address'. Under 'Records', the 'Type' is set to 'Host' (radio button selected), and the 'Address' field contains '172.21.83.193'. An 'Add' button is visible below the address field.

Configuring a Data Group for SNAT Exclusions

7. Click Finished.

End

10. Configure a SNAT pool.

Configuring a SNAT pool

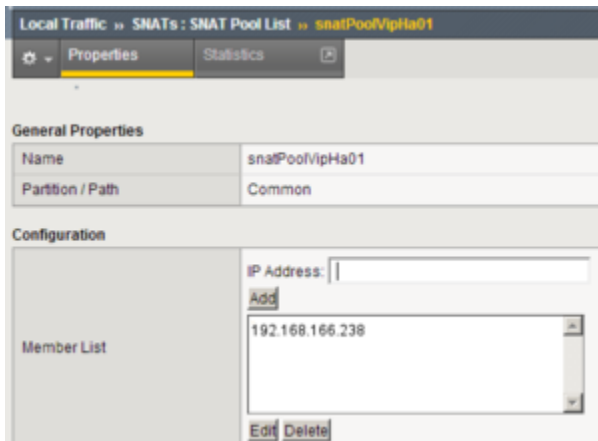
Purpose

To configure a SNAT pool that specifies the Virtual IP address to be used as a source IP address for any packet that originates from the primary or backup SIP Server to which SNAT is applied (with the exception of the devices specified in the dataGroupSnatExcluded01 data group). SNAT is the mapping of one or more original IP addresses to a translation address.

Start

1. Go to Local Traffic > SNATs.
-

2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this SNAT pool—for example, `snatPoolVipHa01`.
 - b. Configuration > Members List > IP Address: Enter the IP address to be used as a source IP address—for example, `192.168.166.238`.
 - c. Click Add.



Configuring a SNAT Pool

4. Click Finished.

End

11. Configure an iRule.

Configuring an iRule

Purpose

To configure an iRule that is used to perform SNAT to the Virtual IP address to any packets that originate from the primary or backup SIP Server (with the exception of the packets addressed to Configuration Server and the Genesys T-Library Clients group). This iRule will then be associated with a Virtual Server for the outbound traffic, `vsWildcardOutbound`. In this deployment architecture, the HA synchronization traffic between primary and backup SIP Servers does not pass through the BIG-IP LTM, that is why it is excluded from applying SNAT.

Start

1. Go to Local Traffic > iRules.

2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this iRule—for example, iRuleSnatOutboundHa01.
 - b. Definition: Enter the following text:

```
#=====#
# Apply SNAT as specified in snatPoolVipHa01 for all
# packets originated from dataGroupSnatHa01 members.
# Exclude packets addressed to members of
# dataGroupSnatExcludedHa01.
#=====#
when CLIENT_ACCEPTED {
  if { [class match [IP::remote_addr] equals dataGroupSnatHa01] }
  {
    if { [class match [IP::local_addr] equals dataGroupSnatExcludedHa01] }
    {
    }
    else
    {
      snatpool snatPoolVipHa01
    }
  }
}
```

4. Click Finished.

End

12. Configure a Virtual Server.

Configuring a Virtual Server

Complete the following steps:

[+] Configuring a Virtual Server for outbound traffic

Purpose

To configure a Virtual Server to be used for outbound traffic. It is associated with a VLAN that is configured for the internal interface (see [Procedure: Configuring VLANs](#)) and it has iRule assigned to Resources, which applies SNAT to all packets (except for packets addressed to Configuration Server).

Prerequisites

- [Procedure: Configuring an iRule](#)

Start

1. Go to Local Traffic > Virtual Servers.

2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this Virtual Server—for example, vsWildCardOutbound.
 - b. Type: Select Forwarding (IP).
 - c. Destination > Type: Select Network.
 - d. Destination > Address: Enter 0.0.0.0.
 - e. Destination > Mask: Enter 0.0.0.0.
 - f. Service Port: Enter * All Ports.
 - g. Configuration: Select Advanced.
 - h. Protocol: Select * All Protocols.
 - i. VLAN Traffic: Select Enabled on...
 - j. VLAN List Selected: Select dc2sip.
 - k. SNAT Pool: Select None.
 - l. Source Port: Select Preserve.

The screenshot shows the configuration page for a virtual server named 'vsWildCardOutbound'. The 'General Properties' section includes fields for Name, Partition/Path, Description, Type (Forwarding (IP)), Destination (Type: Network, Address: 0.0.0.0, Mask: 0.0.0.0), Service Port (0), Availability (checked), and State (Enabled). The 'Configuration: Advanced' section includes Protocol (* All Protocols), Protocol Profile (Client) (fastL4), RTSP Profile (None), Statistics Profile (None), VLAN and Tunnel Traffic (Enabled on...), VLANs and Tunnels (Selected: Common, dc2sip; Available: Common, dc1ext, dc1sip, dc1tlib, dc2ext), SNAT Pool (None), Rate Class (None), Traffic Class (Enabled/Available), Connection Limit (0), and Source Port (Preserve).

Configuring a Wildcard Virtual Server for Outbound Traffic

4. Click Finished.
5. Go to Local Traffic > Virtual Server List > vsWildcardOutbound > Resources.
6. Add iRule as follows:

Resources > iRule Enabled > iRuleSnatOutboundHa01

End

[+] Configuring a Virtual Server for inbound traffic

Purpose

To configure a Virtual Server for inbound traffic. In Layer 3/ Routing configuration mode, the BIG-IP LTM passes through only those packets that have a destination matching a virtual server. Having the Virtual Server for inbound traffic allows packets with a destination that matches the physical IP address of the primary or backup SIP Server to pass through.

Start

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this Virtual Server—for example, vsWildCardInbound.
 - b. Type: Select Forwarding (IP).
 - c. Destination > Type: Select Network.
 - d. Destination > Address: Enter 0.0.0.0.
 - e. Destination > Mask: Enter 0.0.0.0.
 - f. Service Port: Enter * All Ports.
 - g. Configuration: Select Advanced.
 - h. Protocol: Select * All Protocols.
 - i. VLAN Traffic: Select Enabled on....
 - j. VLAN List Selected: Select dc1ext.

Local Traffic » Virtual Servers: Virtual Server List » vsWildCardInbound

Properties Resources Statistics

General Properties

Name	vsWildCardInbound
Partition / Path	Common
Description	
Type	Forwarding (IP)
Destination	Type: Host Network Address: 0.0.0.0 Mask: 0.0.0.0
Service Port	0 * All Ports
Availability	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Advanced

Protocol	* All Protocols
Protocol Profile (Client)	fastL4
RTSP Profile	None
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	<div> <div>Selected</div> <div>Common dc1ext</div> </div> <div> <div>Available</div> <div>Common dc1sip dc1lib dc2ext dc2sip</div> </div>
SNAT Pool	None
Rate Class	None
Traffic Class	<div>Enabled</div> <div>Available</div>
Connection Limit	0
Source Port	Preserve

Configuring a Wildcard Virtual Server for Inbound Traffic

4. Click Finished.

End

[+] Configuring Virtual Servers for UDP and TCP SIP communications

Purpose

To configure two virtual servers to handle traffic directed to a Virtual IP address: one virtual server for SIP communications using the UDP as a transport protocol and one virtual server for SIP communications using the TCP as a transport protocol. The Virtual IP address is used by SIP clients to contact SIP Server. In other words, the Virtual IP address hides two physical IP addresses (used by the primary and backup servers) and presents the SIP Server HA pair as a single entity for all SIP-based communications.

Start

1. Go to Local Traffic > Virtual Servers.
2. Click Create.
3. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this Virtual Server—for example, vsVipUdpHa01.
 - b. Destination > Type: Select Host.
 - c. Destination > Address: Enter the IP address for this Virtual Server—for example, 192.168.166.238.
 - d. Service Port: Enter 5060 and select Other.
 - e. State: Select Enabled.
 - f. Configuration: Select Advanced.
 - g. Type: Select Standard.
 - h. Protocol: Select UDP.
 - i. SMTP Profile: Select None.
 - j. SIP Profile: Select sip.
 - k. VLAN Traffic: Select Enabled on...
 - l. VLAN List Selected: Select dc1ext.

Local Traffic > Virtual Servers: Virtual Server List > vsVipUdpHa01

Properties Resources Statistics

General Properties

Name	vsVipUdpHa01
Partition / Path	Common
Description	
Type	Standard
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.166.238
Service Port	5060 Other:
Availability	●
State	Enabled

Configuration: Advanced

Protocol	UDP
Protocol Profile (Client)	udp
Protocol Profile (Server)	(Use Client Profile)
SSL Profile (Client)	<div>Selected</div> <div>Available</div> <div>Common clientssl clientssl-insecure-compatible wom-default-clientssl</div>
SSL Profile (Server)	<div>Selected</div> <div>Available</div> <div>Common serverssl serverssl-insecure-compatible wom-default-serverssl</div>
Authentication Profiles	<div>Enabled</div> <div>Available</div> <div>Common ssl_cc_idap ssl_ocdp ssl_ocsp</div>
RTSP Profile	None
DNS Profile	None
RADIUS Profile	None
SIP Profile	sip
Statistics Profile	None
VLAN and Tunnel Traffic	Enabled on
VLANs and Tunnels	<div>Selected</div> <div>Available</div> <div>Common dc1ext</div> <div>Common dc1sip dc1lib dc2ext dc2sip</div>
SNAT Pool	None
Rate Class	None
Traffic Class	<div>Enabled</div> <div>Available</div>
Connection Limit	0
Address Translation	<input checked="" type="checkbox"/> Enabled
Port Translation	<input checked="" type="checkbox"/> Enabled
Source Port	Preserve

Configuring a Virtual Server for UDP-Based Communications

4. Click Finished.
5. Select Resources > Load Balancing > Default Pool: Select poolHa01.
6. Click Update.
7. Go to Local Traffic > Virtual Servers.
8. Click Create.
9. In the dialog box that appears, specify the following properties:
 - a. Name: Enter the name for this Virtual Server—for example, vsVipTcpHa01.
 - b. Destination > Type: Select Host.
 - c. Destination > Address: Enter the IP address for this Virtual Server—for example, 192.168.166.238.
 - d. Service Port: Enter 5060 and select Other.
 - e. State: Select Enabled.
 - f. Configuration: Select Basic.
 - g. Type: Select Standard.
 - h. Protocol: Select TCP.
 - i. SMTP Profile: Select None.
 - j. SIP Profile: Select sip.
 - k. VLAN Traffic: Select Enabled on...
 - l. VLAN List Selected: Select dc1ext.

Local Traffic > Virtual Servers: Virtual Server List > vsVipTcpHa01

General Properties

Name	vsVipTcpHa01
Partition / Path	Common
Description	
Type	Standard
Destination	Type: <input checked="" type="radio"/> Host <input type="radio"/> Network Address: 192.168.166.238
Service Port	5060 Other: <input type="text"/>
Availability	<input checked="" type="checkbox"/>
State	Enabled

Configuration: Basic

Protocol	TCP
OneConnect Profile	None
NTLM Conn Pool	None
HTTP Profile	None
HTTP Compression Profile	None
Web Acceleration Profile	None
FTP Profile	None
SSL Profile (Client)	<div> <div>Selected</div> <div>Available</div> <div>Common clientssl clientssl-insecure-compatible wom-default-clientssl</div> </div>
SSL Profile (Server)	<div> <div>Selected</div> <div>Available</div> <div>Common serverssl serverssl-insecure-compatible wom-default-serverssl</div> </div>
VLAN and Tunnel Traffic	Enabled on...
VLANs and Tunnels	<div> <div>Selected</div> <div>Available</div> <div>Common dc1ext dc1sip dc1fib dc2ext dc2sip</div> </div>
SNAT Pool	None

Creating a Virtual Server for TCP-Based Communications

10. Click Finished.
11. Select Resources > Load Balancing > Default Pool: Select poolHa01.
12. Click Update.

End

Note: SNAT pool must not be activated as the configuration element of Virtual Server. SNAT must not be applied to SIP messages sent by clients to SIP Server. Enabling SNAT for these messages results in a broken call flow, as in some circumstances the SNAT is not aligned with SIP Protocol.

<verttabber>