



Packet Capture

Avi Technical Reference (v17.1)

Copyright © 2020

Packet Capture

[view online](#)

Overview

Packet capture in Avi Vantage runs a TCPdump for the designated virtual service or Service Engine and provides complete visibility into the packet transmission.

Virtual services may be on a single Service Engine (SE) or scaled out across multiple active SEs. The traffic captures will be automatically executed on all SEs actively handling traffic for a virtual service. After the capture is completed, the SE will forward the *pcap* file to the Controller, which aggregates and sorts the client and server data into a single file.

Note: It is highly recommended to set a limit for the capture. This limit may either be the maximum number of packets to receive or the duration of the capture, in minutes. After reaching the limit, the capture will be terminated and sent to the Controller.

Capturing Virtual Service Traffic using UI

Navigate to Operations > Traffic Capture. The Capture Configuration section displays the parameters defined for any captures that are currently in progress. To begin a new capture, select the edit icon on the right of the box.

Traffic Capture: demoavi.com

Select Virtual Service *
demoavi.com

• Capture Settings •

Filter to Capture

All Traffic Choose Client IP, IP Range, Subnet Mask Number of Packets Duration

IP Address, IP Range, Subnet Mask Number of Packets Packets

Size of Packets * Bytes

• Advanced Settings •

Health Monitor Options

Cancel Start Capture

- **Select Virtual Service ?** From the dropdown list, select the virtual service you want to capture the traffic for. This capture includes both the client-to-SE and SE-to-server side of the connection. The traffic will be captured on all SEs handling traffic for that virtual service.

Capture Settings

- **Filter to Capture:**
- **All Traffic ?** Select this option to capture all traffic.

- Choose Client IP, IP Range, Subnet Mask ? Select this option to capture traffic only for the specified IP address, list or range of IP addresses, or subnet. The IP addresses can be client or server addresses. * To specify a list, use a space between each address. For example: 10.1.1.1 10.1.1.99 192.168.8.200 * To specify a range, use the following format: 10.1.1.1-10.1.1.255 * To specify a subnet, use the following format: 10.1.1/24
- Number of Packets ? Select this option and specify the maximum number of packets to capture in the core.
- Duration ? Select this option and specify the time in minutes to run the capture.
- Size of Packets ? Specify the size of the packet, in bytes, to be captured. This is similar to the `snaplen` option in TCPdump. To capture the entire packet, enter 0.
- Advanced Settings
 - Health Monitor Options: Indicates whether to capture packets from health checks.
 - None: Excludes health monitoring traffic (the default)
 - Include: Includes health monitoring traffic
 - Only: Captures only health monitoring traffic

Note: If 'Include' or 'Only' are selected, then Avi Vantage will capture *all* SE health monitor traffic for the SEs in which the VS is hosted, including other VS/pool health monitor traffic.

When a capture is started, the Capture Configuration section indicates the progress of the capture.

Completed Captures

After the capture is completed, the Controller collates data from multiple SEs and formats the data into a *pcap* file. These captures are then displayed in the Completed Captures section of the UI. The table displays the Date, Virtual Service Name, and Size of Packets captured. You can export the captures by downloading them in the *pcap* format, using the icon available at the far right column of the table. The capture file can be viewed using any common traffic capture utilities, such as, Wireshark.

Capturing Virtual Service Traffic using CLI

To capture packets using the Avi CLI, log into the `shell` prompt and enter the packet capture sub-mode for the desired virtual service:

```
debug virtualservice Test-virtual service
Updating an existing object. Currently, the object is:
+-----+-----+
| Field | Value |
+-----+-----+
| uuid  | virtualservice-0-1 |
| name  | Test-virtual service |
+-----+-----+
```

Parameters may be defined for the packet capture. By default, the capture is performed within the context of the selected virtual service. It is also performed on all Avi SEs that are handling the virtual service traffic and includes the packets from the client and server side of the SE.

Parameter	Definition
<code>capture_params duration</code>	Time, in minutes. Default is unlimited.
<code>capture_params num_pkts</code>	Maximum number of packets to collect. Default is unlimited.

<code>capture_params pkt_size</code>	Packet size, or snap length, to capture. Default is unlimited.
<code>debug_ip addr</code>	IPv4 address format
<code>debug_ip prefixes</code>	IPv4 prefix format <x.x.x/x>
<code>debug_virtual service_hm_include</code>	Include health monitor packets in the capture
<code>debug_virtual service_hm_none</code>	Omit health monitor packets from the capture (the default)
<code>debug_virtual service_hm_only</code>	Capture only health monitor packets

The `debug_ip` command enters a sub-mode. This allows multiple IP addresses or IP subnets to be entered. Omit the `debug_ip` option for subsequent entries. Save to commit the desired IPs and return to the previous menu.

Note: By default, no maximum packets or duration of time to be captured are defined. It is recommended to include a maximum packet capture as shown in the following example. Without a limit, the capture will run until the Avi SE drive is full, potentially disrupting service.

Specify parameters, including the maximum number of packets to capture:

```
debugvirtualsevice> capture_params num_pkts 1000
debugvirtualsevice> debug_ip addr 10.10.10.10
debugvirtualsevice:debug_ip> save
```

Begin capturing based on the previously configured parameters:

```
debugvirtualsevice> capture
debugvirtualsevice> save
+-----+-----+
| Field | Value |
+-----+-----+
| uuid | virtualservice-0-1 |
| name | Test-VS |
| debug_ip | |
| addr[1] | 10.10.10.10 |
| capture | True |
| capture_params | |
| duration | 0 mins |
| num_pkts | 1000 |
+-----+-----+
```

Re-enter the packet capture sub-mode and stop an ongoing packet capture:

```
debug virtualservice Test-virtual service
debugvirtualsevice> no capture
debugvirtualsevice> save
```

Exporting Packet Capture

Export the packet capture to a remote system that can view it via a tool such as TCPdump or Wireshark:

```
show debug virtualservice Test-virtual service capture
Please specify the destination directory: /tmp
Downloaded the attachment to /tmp/virtual service_virtualservice.20141205_192033.pcap
bash
```

```
scp /tmp/virtual service_virtualservice.192033.pcap user@10.1.1.1:/tmp
```