Persistence Settings

https://campus.barracuda.com/doc/18874379/

The Barracuda Load Balancer ADC supports multiple options to direct clients back to the same Real Server, depending on the Service type. You can also modify the persistence configuration globally for all services.

For information about how to configure persistence for service groups, see How to Configure Service Groups and Service Group Persistence.

Global Persistence Setting

You can configure persistence globally for all services configured on the Barracuda Load Balancer ADC. Go to **Advanced > System Configuration**. Under **Global Settings**, there is an option called **Disable Maintenance Persistence**. When **Disable Maintenance Persistence** is set to **Yes**, new connections from the persistent clients are not forwarded to the maintenance server. Also, new connections from the persistent clients are not forwarded to the backup server when the main server is available for load balancing.

The default setting for **Disable Maintenance Persistence** is **No**. When a real server is in maintenance mode for a Layer 4 service, the Barracuda Load Balancer ADC continues to forward new connections to the real server from persistent clients within the specified persistent timeout period.

The following examples illustrate how the Barracuda Load Balancer ADC behaves when **Disable Maintenance Persistence** is set to **No**:

Example 1

For example, you have configured a Layer 4 service called S1, set the persistent timeout period to 240 seconds, and have configured two servers for the service, R1 and R2. A client makes a connection (Conn1) to service S1. The Barracuda Load Balancer ADC links connection Conn1 to server R1. The administrator then puts server R1 in maintenance mode. New requests going through Conn1 continue to use server R1.

If Client C1 makes a new connection Conn2 to service S1 within the specified persistent timeout period (240 seconds), the Barracuda Load Balancer ADC links this connection (Conn2) to server R1 only.

Example 2

The following example shows how the Barracuda Load Balancer ADC will behave when using the default setting for **Disable Maintenance Persistence** (**No**) and a server failure occurs.

You have configured a Layer 4 service called S1, set the persistent timeout period to 240 seconds, and have configured two servers for the service, R1 (main server) and R2 (backup server). A client makes a connection (Conn1) to service S1. The Barracuda Load Balancer ADC links connection Conn1 to server R1. If real server R1 experiences a failure or is disabled by the administrator, the Barracuda Load Balancer ADC sets the weight of real server R2 to 1.

If Client C1 then attempts to connect to real server R1, the Barracuda Load Balancer ADC forwards the connection (Conn1) to server R2. If real server R1 comes back online, the Barracuda Load Balancer ADC changes real server R2's weight to 0. Real server R2 continues to receive data on connection Conn1 from client C1. By default (Disable Maintenance Persistence is set to No) new connections from Client C1 are also forwarded to R2.

HTTP/HTTPS

There are a variety of supported persistence methods for HTTP/HTTPS sessions:

- **Cookie Insert** – Routes the first request from a client to one of the servers based on the load balancing algorithm. At the same time, it inserts a cookie to identify the client. Subsequent requests from the client include the persistence cookie, so they can be routed to the same server as the first request was.
- **Cookie Passive** – Similar to Cookie Insert, only the server inserts the cookie if needed. This provides additional optimization because requests are load-balanced normally unless there is a requirement to persist a session, which is indicated by the presence of a cookie.
- **Source IP Address** – Subsequent requests from a client with a recurring IP address or systems from the same subnet go to the same Real Server.
- **HTTP Header** – All incoming HTTP requests are directed to the same Real Server based on the value of a header. The application (e.g., Microsoft Exchange) specifies the name of the header to be examined.
- **URL Parameter** – All incoming HTTP requests are directed to the same Real Server based on the value of the specified parameter in the URL.

Layer 4 -TCP, TCP Proxy, Secure TCP Proxy, Layer 4 – UDP, FTP or FTP SSL

Only Source IP Address persistence is supported. An individual source IP address can be used or you can specify a subnet mask so that subsequent TCP connections or UDP datagrams from systems from

the same subnet go to the same Real Server.

UDP Proxy

A UDP Proxy Service supports persistence using both Source IP Address and Client IP Port to distribute the traffic across all of the Real Servers. This helps mitigate the fact that many UDP applications involve all client requests coming from one client IP address.

Layer 7 - RDP

Session persistence is achieved by querying Windows Server® 2003 Terminal Services Session Directory, Windows Server 2008 Terminal Services Session Broker or Windows Server 2008 R2 Session Broker. See Remote Desktop Services Load Balancing.