Real Server Testing Methods

https://campus.barracuda.com/doc/75695969/

These are the testing methods that the Barracuda Load Balancer ADC Service Monitor can use to check the health of the real servers associated with a service. The testing method configured at the service level is executed on every real server that provides that service, unless a different test is configured at the real server level.

To specify a test on a service basis, go to the **Basic > Services** page and edit the service. To specify a test on a real server basis, edit the real server on the **Basic > Services** page.

The tests use the real server port configured on the **Edit Server** page for the service except in the following cases:

- The real server port is set to ALL. The tests use the default port for the test type (for example, SMTP = 25, HTTP = 80, DNS = 53, HTTPS = 443, IMAP = 143, POP = 110, FTP = 21 and SNMP = 161).
- Some of the tests allow you to specify the port, including **Specific HTTP Port** and **RDP Test**.

The minimum value for the test interval, meaning the time between test start times, is 5 seconds, and the default is 30 seconds. The test interval is also the length of time the test is allowed to complete before it is considered to have failed.

Test Name	Description	Test Target	Test Match
Ping	The Service Monitor issues a network ping.		
TCP Port Check	For services specified with TCP-based ports, the Service Monitor validates that the port is open. For UDP-based services and services defied with ALL ports, the Service Monitor issues a network ping.		

UDP Port Check	Check if the UDP port is open by sending a 0 byte datagram to the real server IP address and port. This test depends on receiving an ICMP Port Unreachable message to determine the result. If there is a firewall that prevents outbound ICMP messages, the test assumes that the port is open. The UDP test method only works if the server is still reachable but the port is down. If the server is down, you cannot use the UDP test method since UDP is a connection-less protocol. For such a scenario, you need to either: • Configure UDP and Ping Test for the monitor group and bind the monitor group to a service, server, or GSLB site. • Configure the application level monitor test.		
HTTP	Performs an HTTP GET request to the specified URL. The real server is used as a proxy server to retrieve the page, so the forward proxy setting on the real server must be enabled. You can also specify additional headers to be sent with the HTTP request in the format Header1:Value1, Header2:Value2, etc. Make sure to specify the expected HTTP response status code when accessing the URL, as any other status code is considered an error. Recommended: 200	Enter the complete URL starting with *http:*.	Enter a pattern expected in the resulting HTML.
Simple HTTP	Performs an HTTP GET request to the specified relative URL on the real server being tested. The actual URL used is `http://[real_server_ip]:[port][URL]`. You can also specify additional headers to be sent with the HTTP request in the format Header1:Value1, Header2:Value2, etc. Make sure to specify the expected HTTP response status code when accessing the URL, as any other status code is considered an error. Recommended: 200	Enter the root relative URL (for example, /cgi-bin/index.cgi).	Enter a pattern expected in the resulting HTML.
Simple HTTPS	Same as Simple HTTP test but using SSL. The actual URL used is `https://[real_server_ip]:[port][URL]`. You can also specify additional headers to be sent with the HTTP request in the format Header1:Value1, Header2:Value2, etc. Make sure to specify the expected HTTP response status code when accessing the URL, as any other status code is considered an error. Recommended: 200	Enter the root relative URL (for example, /cgi-bin/index.cgi) in the Test Target box.	Enter a pattern expected in the resulting HTML.

HTTPS Test	Performs a HTTPS GET request to the specified URL. The real server is used as a proxy server to retrieve the page, so the forward proxy setting on the real server must be enabled. You can also specify additional headers to be sent with the HTTP request in the format Header1:Value1, Header2:Value2, etc. Make sure to specify the expected HTTP response status code when accessing the URL, as any other status code is considered an error. Recommended: 200	Enter the complete URL starting with *https:*.	Enter a pattern expected in the resulting HTML.
DNS	Sends a DNS query to retrieve the IP address of the specified hostname. This value is compared to the IP address in the Test Match box.	Enter a fully qualified hostname in the Test Target box.	To validate resolution to a specific IP address, enter that IP in the Test Match box.
IMAP	Simple Test for IMAP service. If no username and password are provided, this test only verifies availability of the IMAP service on the real server.	Optional: Username to log in as.	Optional: Password to use.
POP3	Simple Test for POP3 service. If no username and password are provided, this test only verifies availability of the POP3 service on the real server.	Optional: Username to log in as.	Optional: Password to use.
SMTP	Simple Test for SMTP service.	Enter the domain for the mail server to be tested.	Optional: Enter a pattern that is expected in the banner of the SMTP Server.
SNMP	Do an SNMP Get using the OID in the Test Target box and match the response to the pattern in the Test Match box. If the Test Target box is empty, the test checks if the SNMP is available on the real server.	Optional: Enter a valid SNMP OID in the Test Target box.	Optional: Enter a pattern to match in the response.
SIP	Simple Test for SIP service. This test sends an OPTIONS packet to the SIP server to check availability of the SIP service.		
SIP TLS	Uses SIP over an encrypted TLS channel.		
LDAP/AD	Bind Test for LDAP/AD service. If no username and password are provided, the LDAP/AD test verifies availability of anonymous user.	Optional: Username with full LDAP schema.	Optional: Password to use.
LDAPS/AD	Bind Test for LDAPS/AD service. If no username and password are provided, the LDAPS/AD test verifies availability of the anonymous user.	Optional: Username with full LDAP schema.	Optional: Password to use.
Barracuda Spam Firewall	The Barracuda Load Balancer ADC's IP address must be exempted from any Rate Control settings on the Barracuda Spam Firewall.	Enter the domain for the mail server to be tested.	Optional: Enter a pattern that is expected in the banner of the SMTP Server.

Specific HTTP Port	Performs an HTTP GET request using a specified port to a relative URL on the real server being tested. The URL has the format `http://[real_server_ip]:[port][URL]`.	Enter the TCP port followed by a ":" and the root relative URL (for example, 8080:/cgi-bin/index.cgi).	Enter a pattern expected in the resulting HTML.
RADIUS Auth	Tests the availability of a RADIUS server.	Enter the secret to use with the RADIUS server.	Enter a username and password separated by "|". Example: username|password
RADIUS Acct	Tests the availability of a RADIUS server by making an accounting request.	Enter the secret to use with the RADIUS server.	Enter a username and password separated by "|". Example: username|password
RDP Test	Attempts an RDP connection to each real server to check the availability of the Terminal service.	Enter the port on the real server to use, if different than the port specified on the **Edit Server** page.	
FTP Test	Attempts a TCP connection to each real server to check the availability of FTP.		
FTPS Test	Attempts a TCP connection to each real server to check the availability of FTPS.		
SFTP Test	Uses FTP over SSH. Requires username and password to log into the FTP server. Checks that it is possible to open the connection to the FTP server using SSH.	N/A	N/A
MS Sharepoint	Validates access and verifies availability of the SharePoint application. Requires username and password to log into the Sharepoint application.	Enter the root relative URL (for example, /cgi-bin/index.cgi).	Enter a pattern that is expected in the resulting HTML.
MS Sharepoint Secure	Validates access and verifies availability of the Secure SharePoint server. Requires username and password.	Enter the root relative URL (for example, /cgi-bin/index.cgi).	Enter a pattern that is expected in the resulting HTML.
MYSQL	Checks the MYSQL services on the configured mysql port by sending the mysql query to the specified database. You must also include a valid username and password for the MYSQL server.	Enter the MYSQL query to the server.	Enter the expected return string for the MYSQL query.
Always Pass	This test is used for troubleshooting or for services used for management access to real servers. This test always passes regardless of the condition of the real server.		