HTTPS Health Monitor

Avi Technical Reference (v18.2)

HTTPS Health Monitor

view online

Introduction

The HTTPS monitor type can be used to validate the health of HTTPS encrypted web servers. Use this monitor when Avi Vantage is either passing SSL encrypted traffic directly from clients to servers, or Avi Vantage is providing SSL encryption between itself and the servers. This article covers the configuration specific for HTTPS monitor.

Creating a HTTPS Health Monitor

To create a HTTPS monitor,

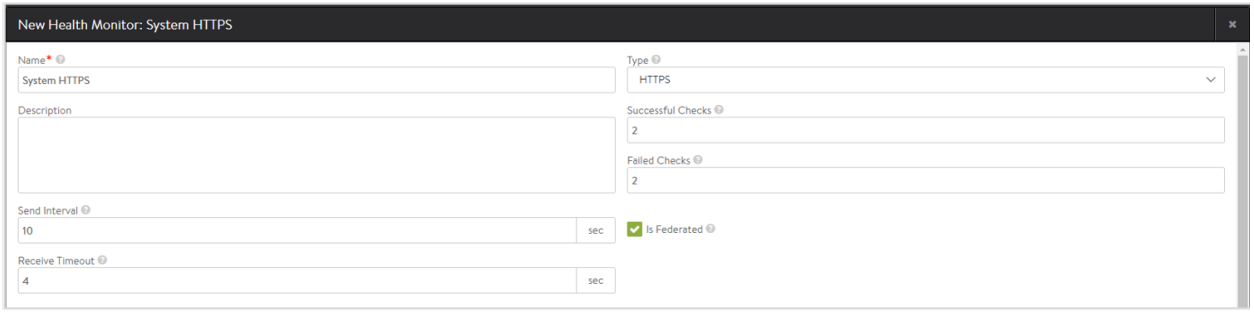
1. From the Avi UI, navigate to Templates > Profiles >Health Monitors.
2. Click on Create to view the New Health Monitor screen.
3. Enter a unique Name for the monitor.
4. Enter a Description.
5. Select HTTPS as the Type of Health Monitor.

   Notes:

- Once the Type of Monitor is selected, options specific to the health monitor type are displayed.
- Starting with release 18.2.3, once the Type field is set and the monitor profile is created, the Avi UI will not permit a change to the Type field.

6. Enter the Send Interval value (in seconds). This value determines how frequently the health monitor initiates an active check of a server. The frequency range is 1 to 3600.
7. Enter the Receive Timeout, value (in seconds). The server must return a valid response to the health monitor within the specified time limit. The receive timeout range is 1 to 2400 or the send interval value minus 1 second.
   Note: If the status of a server continually flips between up and down, this may indicate that the receive timeout is too aggressive for the server.
8. Enter Successful Checks. This is the number of consecutive health checks that must succeed before Avi Vantage marks a down server as up. The minimum is 1, and the maximum is 50.
9. Enter Failed Checks This is the number of consecutive health checks that on failing, Avi Vantage marks a server as down. The minimum is 1, and the maximum is 50.

10. Click on the option Is Federated? to replicate the object across the federation. When this option is not selected, the object is visible within the Controller-cluster and its associated SEs. `is_federated` is set to True only when GSLB is turned on. A federated health monitor is used for GSLB purposes while it is not applicable for a regular health-monitor. This implies that a GSLB service cannot be associated with a regular health monitor, because GSLB service is a federated object, while the health monitor is not. Conversely, a pool cannot be associated with a federated health monitor because the pool is not a federated object.

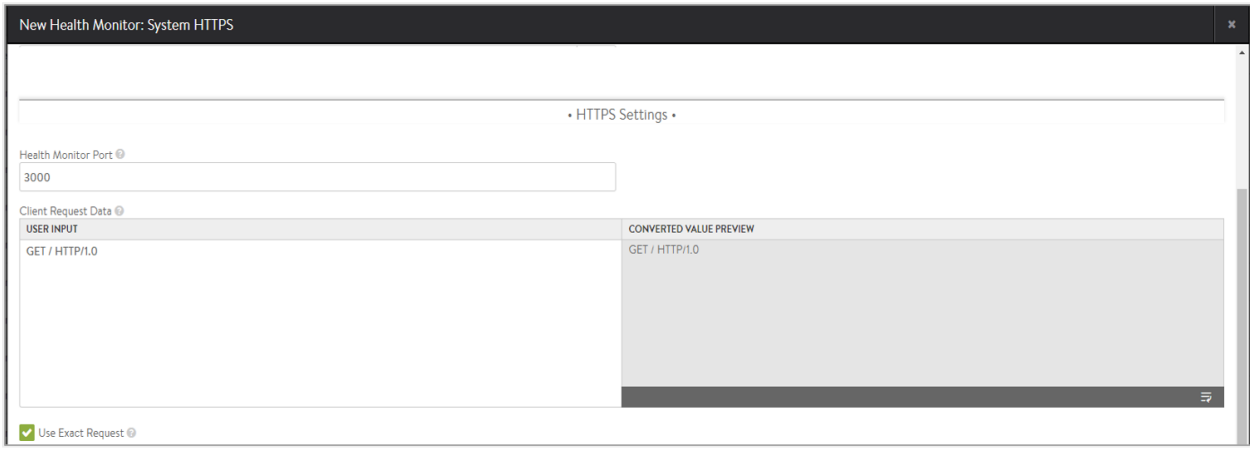


11. Enter the HTTPS Settings as discussed below:

    1. Specify a Health Monitor Port that should be used for the health check. When this setting is blank, the default port configured for the server will be used. When it is specified, clients may be directed to a different port than what is monitored. For instance, a server at HTTP port 80 may have two health monitors attached, one for HTTP default port, and a second for HTTPS specifically on port 443. If both health monitors pass, the server can receive traffic on HTTP port 80. This ensures clients can input items in their shopping cart and later purchase those items over SSL on 443.
    2. Use the field Client Request Data, to send an HTTP request to the web server. Avi Vantage does not validate the request, as different servers may support unique request syntax.

    - Method: Any method may be used, though GET, POST and HEAD are the most common for monitoring. If no method is defined, Avi Vantage will use GET. * GET /index.htm
      * POST /upload.asp HTTP/1.0: www.site.com-Length: 1012345
    - Path: The path may include the URI and query, such as `/index.htm?user=test`. If no path is specified, Avi Vantage will use /
    - Version: The HTTP version can be 1.0 or 1.1. If no version is specified, Avi Vantage will use 1.0.
    - Host: If no host header is specified, Avi Vantage includes a host header populated with the server's name. HTTP 1.1 servers expect a host header to be included in the request.
    - Carriage Return: By default, Avi Vantage will add a carriage return line feed to the end of the send string in the form of . For HTTP 1.0, and additional may be required. For send strings that require multiple lines of data, such as headers, the carriage returns may need to be added, such as in the POST example above.

    3. Select Use Exact Request to use the exact http_request string as specified by the user. This will avoid automatic insertion of headers like host header.



    4. In the Response Code field, enter HTTPS response codes to match successful. A successful HTTPS monitor requires either the response code, the server response data, or both fields to be populated. The response code expects the server to return a response code within the specified range. For a GET request, a server should

usually return a 200, 301 or 302. For a HEAD request, the server will typically return a 304. A response code by itself does not validate the server?s response content, just the status.

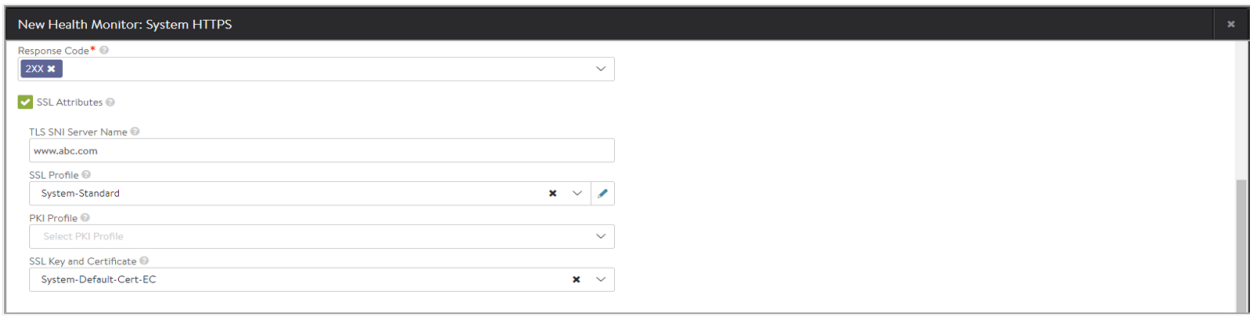
5. Click on SSL Attributes to allow SSL encrypted traffic to pass to servers without decrypting in the load balancer (the SE). Since the traffic is still SSL / HTTPS, we still are expected to conduct a relevant health monitor.

- Starting Avi Vantage release 18.2.3, the TLS SNI Server Name field is introduced. Enter a fully qualified DNS hostname to include SSL host header extension during TLS handshakes. If no value is specified, the value from the pool will be inherited from the pool. Prior to Avi Vantage release 18.2.3, the HTTPS Health Monitor inherited the TLS SNI Server Name from the pool that it is attached to. However, only one SNI server name could be specified in the pool. Attaching multiple HTTPS health monitors to the pool was not applicable as these health monitors would try to monitor the same domain names on a specified ip:port, sometimes with mismatching SSL certificates and keys. This resulted in the pools being marked down.

  Note: If Use Exact Request, is enabled, Avi Vantage will not check the validity of the host specified. A mismatch between the host name and the TLS SNI server name, violates a standard in RFC 6066.

- Select an existing SSL Profile or create a new one, as required. This defines the ciphers and SSL versions to be used for the health monitor traffic to the backend servers.
- Select an existing PKI Profile or create a new one, as required. This will be used as to validate the SSL certificate presented by the server.

- Select an existing SSL Key and Certificate or create a new one, as required.

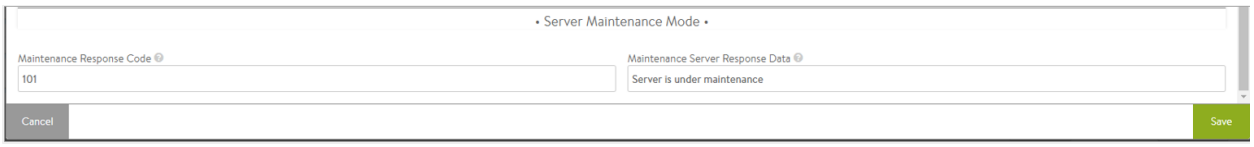


12. Enter the Server Maintenance Mode settings as discussed below:

    1. Enter Maintenance Response Code under Server Maintenance Mode. If the defined HTTP response code is seen in the server response, place the server in maintenance mode. Multiple response codes may be used via comma separation.

    2. Enter Maintenance Server Response Data. If the defined string is seen in the server response, place the server in maintenance mode.
       Note: Custom server response can be used to mark a server as disabled. During this time, health checks will continue, and servers operate the same as if manually disabled, which means existing client flows are allow to continue, but new flows are sent to other available servers. Once a server stops responding with the maintenance string it will be brought online, being marked up or down as it normally would based on the server response data.

This allows an application owner to gracefully bleed connections from a server prior to taking the server offline without the requirement to log into Avi Vantage to first place the server in disabled state.



13. Click on Create.

Example Health Check

Sample HTTPS health check send string:

```
GET /health/local HTTP/1.0
User-Agent: avi/1.0
Host: 10.10.10.3
Accept: */*
```

Sample server response:

```
HTTP/1.0 200 OK
Server: Apache-Coyote/1.1
Cache-Control: no-cache, no-store
Pragma: no-cache
Content-Type: text/plain
Content-Length: 15
Date: Fri, 20 May 2016 18:23:05 GMT
Connection: close

Health Check Ok
```

The server response includes both the response code: *200*, and the Server Response Data: *Health Check ok*. Therefore this server will be marked up. Notice that Avi automatically includes additional headers in the send string, including User-Agent, Host, and Accept to ensure the server receives a fully formed request.

SSL Attributes in HTTPS Health Monitor

Behavior Change

The SSL settings on health monitor are always considered if provided. If SSL settings for the health monitor are not provided, the health monitor falls back to using pool SSL settings. An HTTPS health monitor needs SSL settings on either the health monitor config itself or in the pool config. If is absent in both, Avi Vantage reports an error.

Upgrade Impact

Upgrade happens smoothly and needs no manual configuration. Upgrading from releases prior to 17.1 causes the HTTPS health monitor to use pool SSL settings. If a new SSL config is added to the health monitor, it will be placed into effect.

Related Articles

- Read the Overview of Health Monitors article for general monitor information, implementation, and other monitor types.

- The Health Monitor Profile article introduces and explains the various settings available for all kinds of health monitors.

The HTTPS health monitor may only be applied to a pool whose virtual service has an HTTP application profile attached. Health monitoring of HTTPS is covered in the SSL Attributes in HTTPS Health Monitor section at the end of this article.