API Management

API Gateway Full Healthcheck Policies

Contents

1. Healthcheck APIGW 7.5.3 Architecture

This topic describes how to perform a full components healthcheck plus a zero downtime policy deployment to API Gateway in a multi-node API Gateway environment with a load balancer.

Note: The section Create Cassandra HC Policy is an improvement of the Healthcheck LB Service, and the reason is to validate, at the same time, API Gateway, API Manager and Cassandra. It is highly recommended.

Note2: This specification is designed for Axway API Gateway 7.5.3 or newer

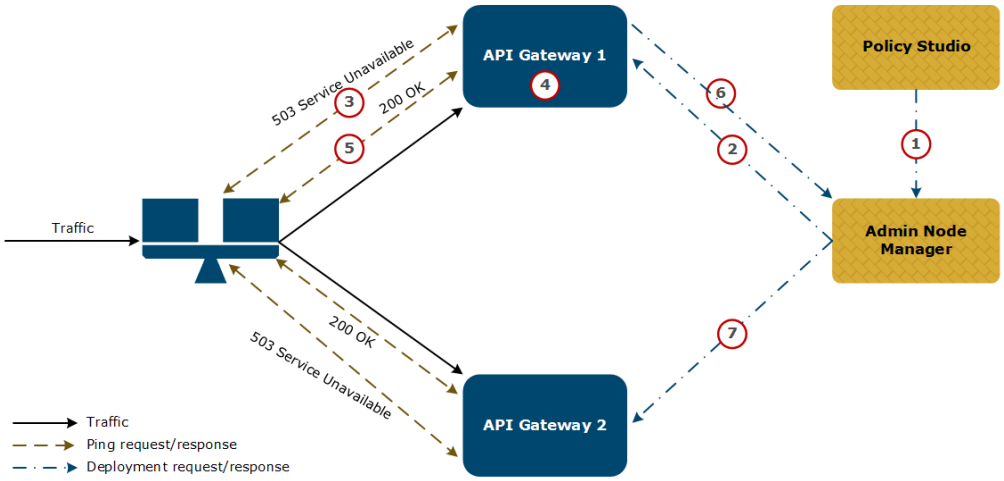
Source:
https://docs.axway.com/bundle/APIGateway_753_AdministratorGuide_allOS_en_HTML5/page/Content/AdminGuideTopics/admin_zdd.htm

2. Introduction to Zero Downtime Deploy

When you deploy configuration (for example, a .fed file) to a group of API Gateways, the configuration is deployed sequentially to each API Gateway in the group. While the configuration is being deployed to a given API Gateway there is a service interruption during which that API Gateway cannot process traffic.

Zero downtime deployment enables you to orchestrate deployment to a load-balanced set of API Gateways, ensuring that a subset can always process traffic.

The following diagram illustrates the process:



1. A user initiates deployment of new configuration from Policy Studio.
2. The Admin Node Manager starts deployment in `API Gateway 1`.
3. `API Gateway 1` starts responding to a ping from the load balancer with `503 Service Unavailable`. The load balancer stops routing traffic to `API Gateway 1`.
4. `API Gateway 1` performs the deployment.
5. `API Gateway 1` starts responding to the load balancer ping with `200 OK`. The load balancer starts routing traffic to `API Gateway 1` again.
6. `API Gateway 1` informs the Admin Node Manager that deployment is complete.
7. The Admin Node Manager repeats step 2 through step 6 for `API Gateway 2`.

3. Introduction to Virtualized Healthcheck

The purpose is to provide a full healthcheck solution to verify in one way, the API Gateway service (8443), API Manager Traffic Service (8065) and Cassandra Health.

The method is to expose a policy by a relative path and virtualize it on API Manager. The Load Balancer must use this virtualized API to healthcheck.

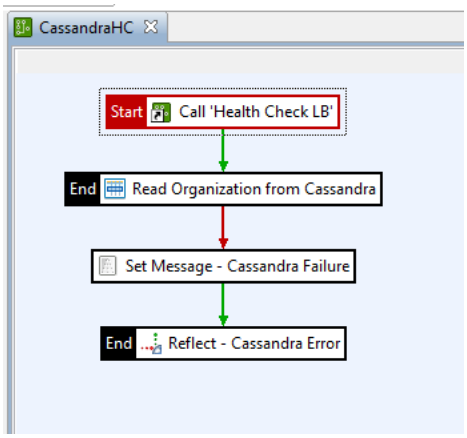
The policy does an explicit “SELECT” to Cassandra by reading the Community organization from API Portal collection.

- If return True, follow by the default HealthcheckLB validation
- If it can’t be reached there is an issue with Cassandra, and the healthcheck fail.

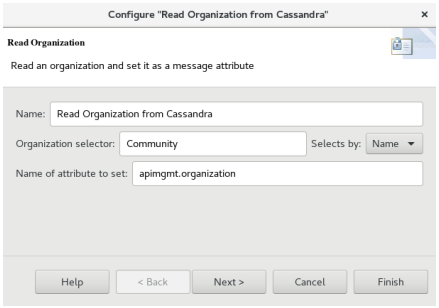
4. Create the CassandraHC Policy

Create a policy to enhance the HealthcheckLB policy to validate Cassandra health.

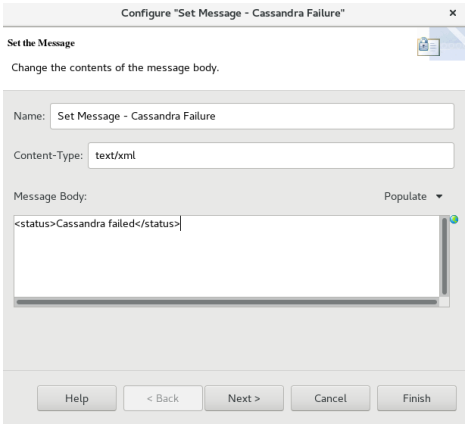
Create a new policy CassandraHC and organize the filters as the image below.



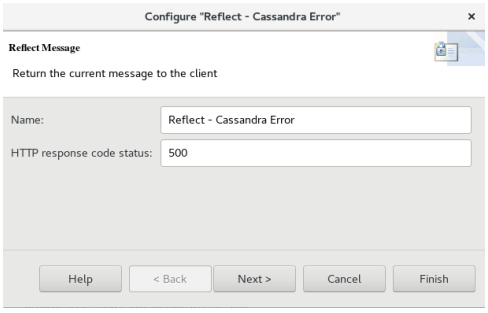
Edit the “Read Organization” filter to search the Community organization from API Portal.



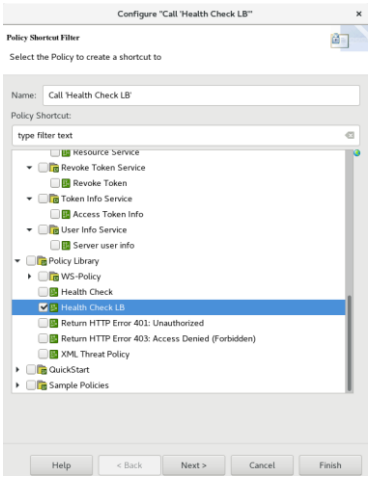
Edit the “Set Message” filter to create the Cassandra error message.



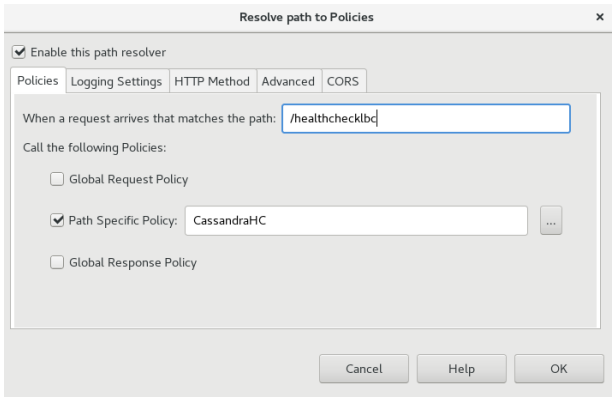
Edit the “Reflect Message” filter



Create a Policy shortcut to HealthcheckLB.



Create a relative path to expose the policy.

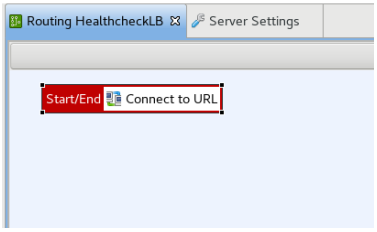


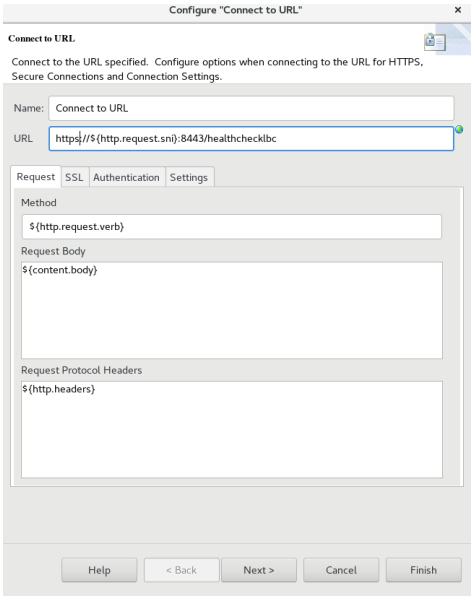
Deploy the configuration

5. Create the Routing Policy

The healthcheck must be fully executed into the same host. This policy ensures that each APIMGR always connect to its own APIGW. The variable `${http.request.sni}` has the hostname of the APIGW server processing the current transaction.

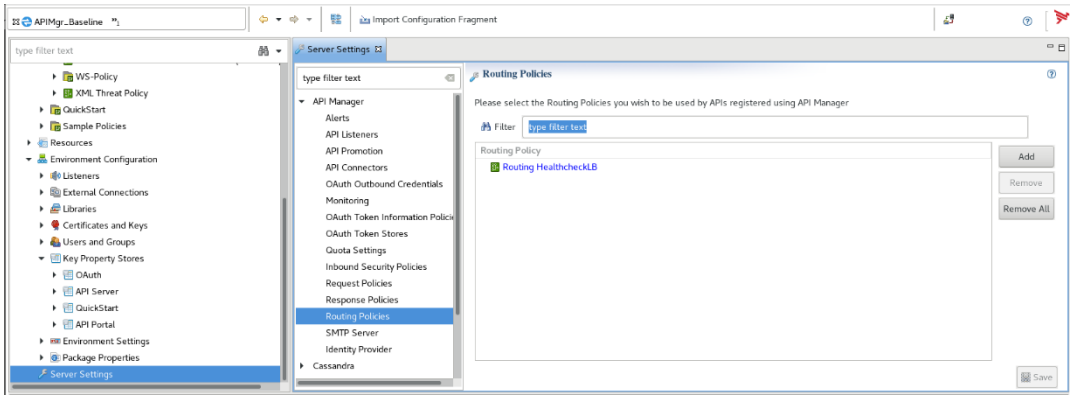
On Policy Studio, create the policy “Routing HealthcheckLB”





Set the policy to API Manager Routing policies

Policy Studio > Server Settings > API Manager > Routing Policies



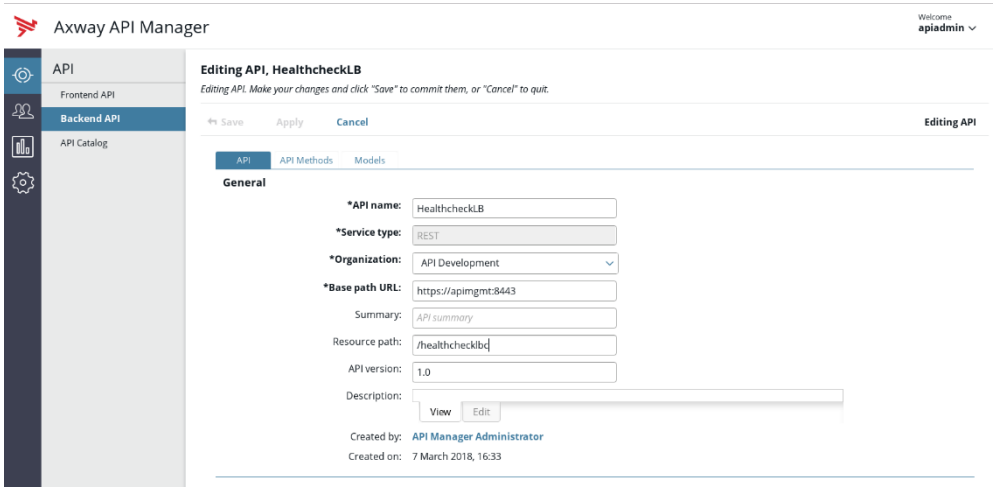
Deploy the configuration

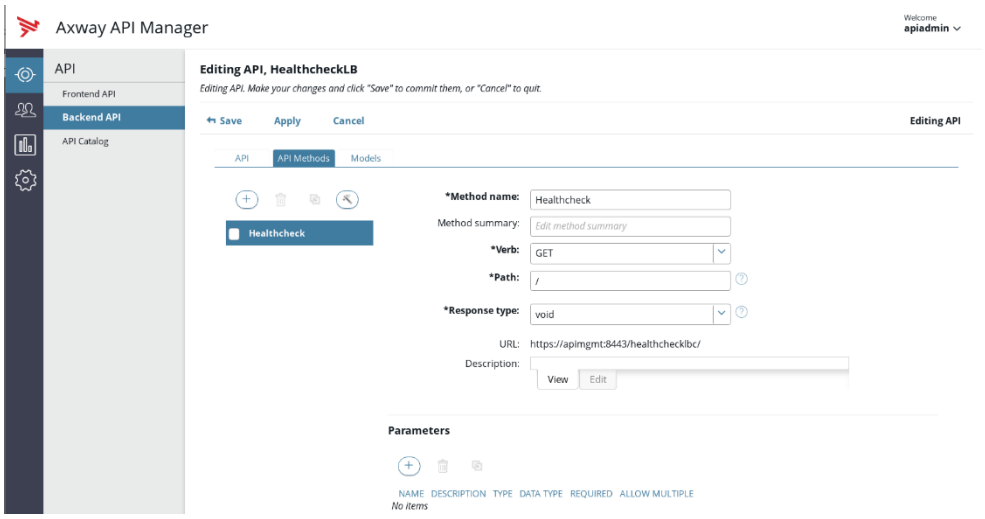
6. Virtualize the API

Register Backend API

Create the API definitions and its Method, following the configurations below.

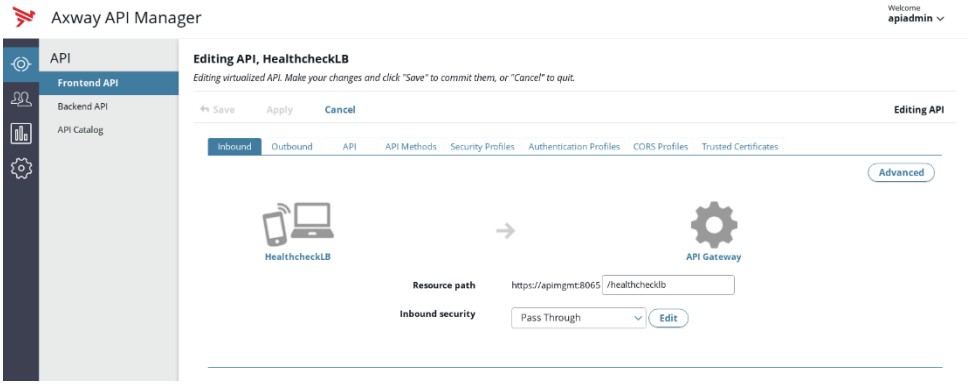
Note: In a HA architecture, can be used any host as Basepath URL. A policy will be used to route the traffic and ensure that the incoming API MGR request reach the same APIGW Server. (See 5 - Create the Routing Policy)





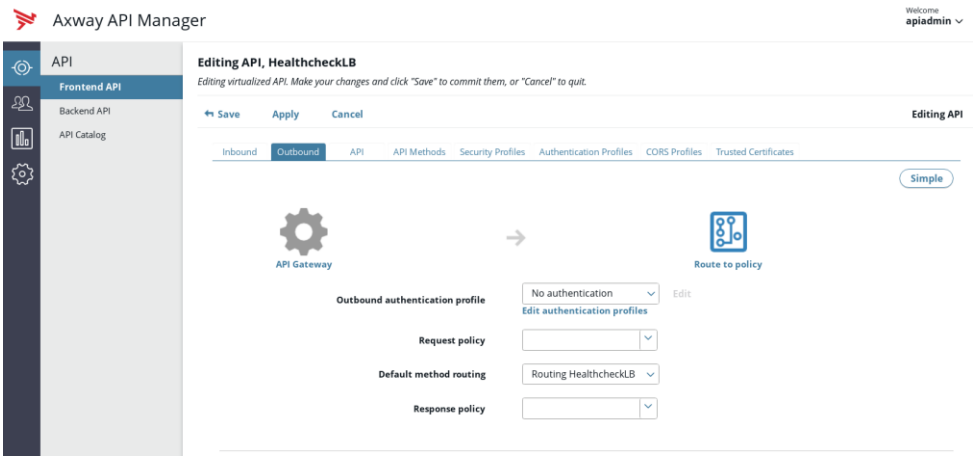
Virtualize on Frontend

Set the Inbound Security

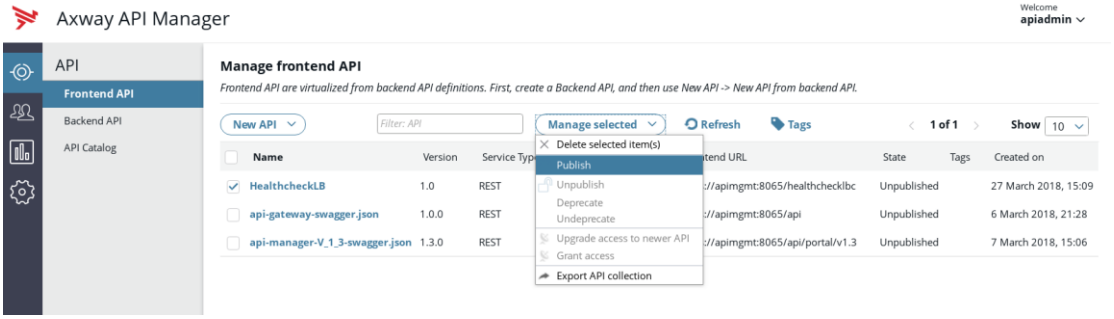


Set the outbound Configuration

Click on Advanced button, top-right screen. Select the policy “Routing HealthcheckLB” as default method Routing.



Save the API and set the API as Published



Test the API

https://apimgmt:8065/healthchecklbc

7. Deploy Zero Downtime Configuration

To perform a zero downtime policy deployment, follow these steps:

1. Enable zero downtime deployment in Policy Studio, and set the delays before and after deployment. For more information, see Zero downtime settings.

2. Configure your load balancer to ping the Health Check LB policy periodically to determine if each API Gateway is healthy. This is available on the following default URL:

   https://APIGAMANAGER_HOST:8065/healthchecklbc

3. Initiate deployment to a group of API Gateways using API Gateway Manager, Policy Studio, or managedomain. For more information, see Deploy API Gateway configuration. The configuration is deployed sequentially to each API Gateway in the group.

4. When deployment is initiated on each API Gateway:
   a. The Health Check LB policy returns a 503 Service Unavailable response. This indicates to the load balancer that this API Gateway is not available for traffic and the load balancer stops routing to it.
   b. After the specified delay before deployment (for example, 10 seconds), the configuration is deployed to the API Gateway.
   c. When the deployment is complete, the Health Check LB policy returns a 200 OK response. This indicates to the load balancer that this API Gateway is available for traffic again.
   d. After the specified delay after deployment (for example, 10 seconds), a response is sent to the deployment request. Deployment can now be initiated to the next API Gateway in the group.