

[Networking Products](https://cloud.google.com/products/networking/) (https://cloud.google.com/products/networking/)

[Traffic Director](https://cloud.google.com/traffic-director/) (https://cloud.google.com/traffic-director/)

[Documentation](https://cloud.google.com/traffic-director/docs/) (https://cloud.google.com/traffic-director/docs/) [Guides](#)

# Troubleshooting Traffic Director deployments

This document provides information to help you resolve Traffic Director configuration issues.

## Proxies do not connect to Traffic Director

If your sidecar proxies do not connect to Traffic Director, do the following:

- Check the sidecar proxy logs for any errors connecting to `trafficdirector.googleapis.com`.
- If you have set up netfilter (via `iptables`) to redirect all traffic to the sidecar proxy, make sure that the user (UID) as whom you run the proxy is excluded from redirection. Otherwise, this causes traffic to continuously loop back to the proxy.
- Make sure that you enabled the Traffic Director API for the project. Under the APIs & services for your project, look for errors for the Traffic Director API.

[GO TO THE API LIBRARY PAGE](https://console.cloud.google.com/project/_/apis/libraries) (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/PROJECT/\_/APIS/LIBRARIES)

- Confirm that API access scope of the VM is set to allow full access to the GCP APIs. This is done by specifying `--scopes=https://www.googleapis.com/auth/cloud-platform` at VM creation time.
- Confirm that the service account has the correct permissions. For more information, read [Enabling the service account to access the Traffic Director API](https://cloud.google.com/traffic-director/docs/setting-up-traffic-director#enable-service-account) (https://cloud.google.com/traffic-director/docs/setting-up-traffic-director#enable-service-account)
- Confirm that you can access `trafficdirector.googleapis.com:443` from the VM. If there are issues with this access, possible reasons could be firewall preventing access to

`trafficdirector.googleapis.com` over TCP port 443 or DNS resolution issues for `trafficdirector.googleapis.com` hostname.

- If you're using Envoy for the sidecar proxy, confirm that the Envoy version is release 1.9.1 or later.

## Service configured with Traffic Director is not reachable

If a service configured with Traffic Director is not reachable, confirm that the sidecar proxy is running and able to connect to Traffic Director.

If you are using Envoy as sidecar proxy, you can confirm this by running the following commands.

1. From the command line, confirm that the Envoy process is running.

```
ps aux | grep envoy
```

2. Inspect Envoy's runtime configuration to confirm that dynamic resources were configured by Traffic Director. You can see the config by running this command:

```
curl http://localhost:15000/config_dump
```

3. Ensure that traffic interception for the sidecar proxy is set up correctly.

For the redirect setup with iptables, run the `iptables` command and then `grep` the output to ensure that your rules are there:

```
sudo iptables -t nat -S | grep ISTIO
```

The following is an example of the output for `iptables` intercepting the VIP `10.0.0.1/32`, and forwarding it to an Envoy proxy running on port 15001 as UID 1006:

```
-N ISTIO_IN_REDIRECT  
-N ISTIO_OUTPUT  
-N ISTIO_REDIRECT  
-A OUTPUT -p tcp -j ISTIO_OUTPUT  
-A ISTIO_IN_REDIRECT -p tcp -j REDIRECT --to-ports 15001  
-A ISTIO_OUTPUT -m owner --uid-owner 1006 -j RETURN  
-A ISTIO_OUTPUT -d 127.0.0.1/32 -j RETURN
```

```
-A ISTIO_OUTPUT -d 10.0.0.1/32 -j ISTIO_REDIRECT  
-A ISTIO_OUTPUT -j RETURN
```

If the VM instance is created through the GCP Console, some ipv6-related modules are not installed and available before a restart. This causes `iptables` to fail because of missing dependencies. In this case, restart the VM and rerun the setup process, which should solve the problem. A Compute Engine VM that you created using `gcloud` commands is not expected to have this problem.

## Service stops being reachable when Envoy access logging is configured

If you used `TRAFFICDIRECTOR_ACCESS_LOG_PATH` to configure Envoy access log as described in the [Configuring additional attributes for sidecar proxies](https://cloud.google.com/traffic-director/docs/traffic-director-per-proxy-config) (<https://cloud.google.com/traffic-director/docs/traffic-director-per-proxy-config>), make sure that the system user running Envoy proxy has permissions to write to the specified access log location.

Failure to provide necessary permissions will result in listeners not being programmed on the proxy and can be detected by checking for the following error message in the Envoy proxy log:

```
gRPC config for type.googleapis.com/envoy.api.v2.Listener rejected:  
Error adding/updating listener(s) TRAFFICDIRECTOR_INTERCEPTION_LISTENER:  
unable to open file '/var/log/envoy.log': Permission denied
```



To solve the problem change permissions of the chosen file for the access log to be writable by the Envoy user.

## Applications are unable to connect to services not configured in Traffic Director

Make sure that you have set up traffic interception only for the IP-addresses of services that are configured in Traffic Director. If all traffic is intercepted, then connections to the services not configured in Traffic Director are silently discarded by the sidecar proxy.

## Traffic is looping within a node or a node crashes

If netfilter (`iptables`) is set up to intercept all traffic, ensure that the user (UID) that is used to run the sidecar proxy is excluded from traffic interception. Otherwise, traffic sent by the sidecar proxy is looped back to the proxy indefinitely. The sidecar proxy process might crash as a result. In the reference configuration, the netfilter rules do not intercept traffic from the proxy user.

## Traffic Director behavior when most endpoints are unhealthy

When 99% of endpoints are unhealthy, for better reliability, Traffic Director configures the data plane to disregard the health status of the endpoints and balance traffic among all of the endpoints, because it is possible that the serving port is still functional.

## What's next

- See [Traffic Director Concepts](https://cloud.google.com/traffic-director/docs/traffic-director-concepts) (<https://cloud.google.com/traffic-director/docs/traffic-director-concepts>) for information on how Traffic Director works.

---

*Except as otherwise noted, the content of this page is licensed under the [Creative Commons Attribution 4.0 License](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>), and code samples are licensed under the [Apache 2.0 License](https://www.apache.org/licenses/LICENSE-2.0) (<https://www.apache.org/licenses/LICENSE-2.0>). For details, see our [Site Policies](https://developers.google.com/terms/site-policies) (<https://developers.google.com/terms/site-policies>). Java is a registered trademark of Oracle and/or its affiliates.*

*Last updated January 8, 2020.*