

AppSentinels API Security Platform

F5 Integration

Revision	Date Modified	Author	Comments
1.0	08-09-2024	Sachin	Initial Version
1.1	13-02-2025	Sachin	Updated with snapshots and more details of integration
1.2	21-02-2025	Sachin	iRule attachment pre-condition, section updated – Attach the iRule to Virtual Server

Contents

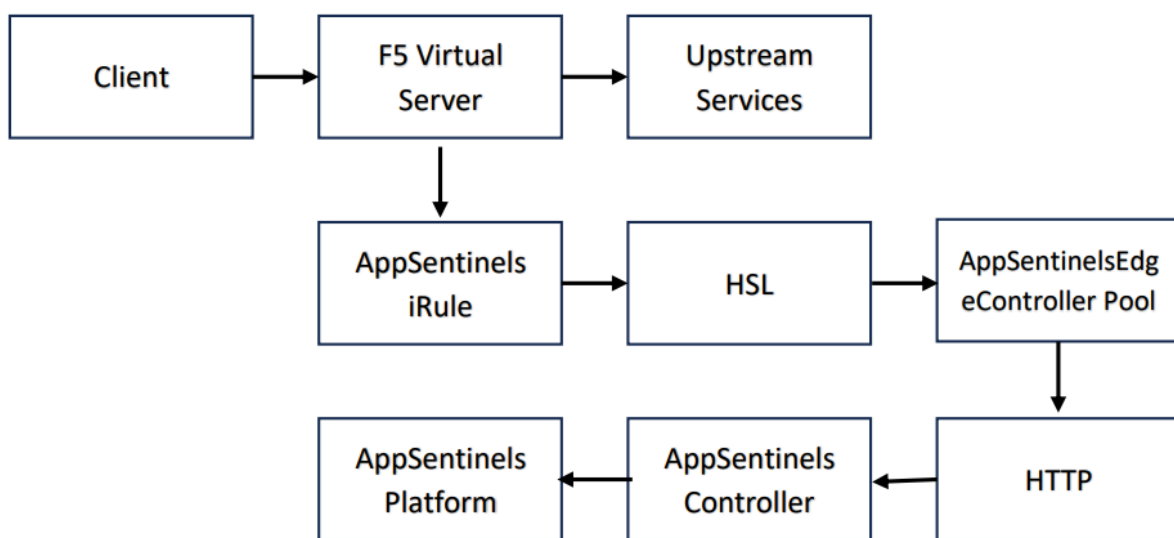
1.	Introduction.....	4
2.	Integration Configuration for HSL based logging over HTTP.....	4
2.1	Detailed Steps.....	4
2.1.1	Edge Controller Pool Creation	4
2.1.2	iRule Creation for log forwarding	6
2.1.3	Attach the iRule to Virtual Servers	6
3.	Integration Configuration for HSL based logging over HTTPS.....	8
3.1	Approach.....	8
3.2	TLDR	8
3.3	Detailed Steps	8
3.3.1	Edge Controller Pool Creation	8
3.3.3	Edge Controller Virtual Server and Virtual Pool Creation.....	10
3.3.4	iRule Creation for log forwarding	12
3.3.5	Attach the iRule to Virtual Servers	13
4.	API version of F5 device.....	13

1. Introduction

AppSentinels API Security Platform offers robust integration with F5 Load Balancer systems, leveraging High-Speed Logging (HSL) as a reliable mechanism to forward API traffic logs. This integration provides seamless visibility and enhanced security capabilities for API traffic originating from F5 infrastructure. HSL is designed for high-volume and low overhead logging mechanism, ensuring minimal performance overhead on the F5 system.

F5 Ref: [High Speed Logging](#)

2. Integration Configuration for HSL based logging over HTTP



TLDR

- Create Pool: Configure a pool named AppsentinelsEdgeController for the edge-controller.
- Specify Details: Add the edge-controller's IP/hostname and port (default: 9004).
- iRule Creation: Develop an iRule for AppSentinels' integration.
- Assign iRule: Attach the iRule to relevant virtual servers under Properties > Resources > iRules.
- Ensure Connectivity: Confirm TCP connectivity between the F5 system and the edge-controller VM on port 9004.
- iRule Logging: The iRule will use HSL logging to forward logs to the edge-controller.

2.1 Detailed Steps

2.1.1 Edge Controller Pool Creation

- Go to Local Traffic > Virtual Servers > Pools > Pool List and the click on Create. Name the pool for the edge-controller as AppsentinelsEdgeController. If a different name is

used, ensure it is updated in the iRule script. Optionally, enable TCP-based health monitoring for the pool.

- Specify the edge-controller details: Provide the IP address or hostname of the edge-controller and set the listening port to 9004 (default).

Local Traffic » Pools : Pool List » **New Pool...**

Configuration: Basic

Name: AppsentinelsEdgeController

Description:

Health Monitors:

Active: /Common, tcp

Available: standard_bd_monitor_mobilelatm, standard_bd_monitor_mobileus, standard_bd_monitor_us, tcp_half_open, udp

Resources:

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

New Members:

Node Name: HostedEdgeController (Optional)

Address: devsaas3.appsentinels.ai

Service Port: 9004 HTTP

Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
HostedEdgeController	devsaas3.appsentinels.ai	9004		0

Edit Delete

Cancel Repeat Finished

- Click on Finished when done
- Check the status of the controller endpoint by going to Local Traffic > Pools > Pool List > AppsentinelsEdgeController. The status should show as available

Local Traffic » Pools : Pool List » **AppsentinelsEdgeController**

Properties Members Statistics

Load Balancing:

Load Balancing Method: Round Robin

Priority Group Activation: Disabled

Update

Current Members:

✓	▼	Status	Member	Address	Service Port	FQDN	Ephemeral	Ratio	Priority Group	Connection Limit	Partition /
☐		●	HostedEdgeController:9004	34.100.132.211	9004		No	1	0 (Active)	0	Common

Enable Disable Force Offline Remove

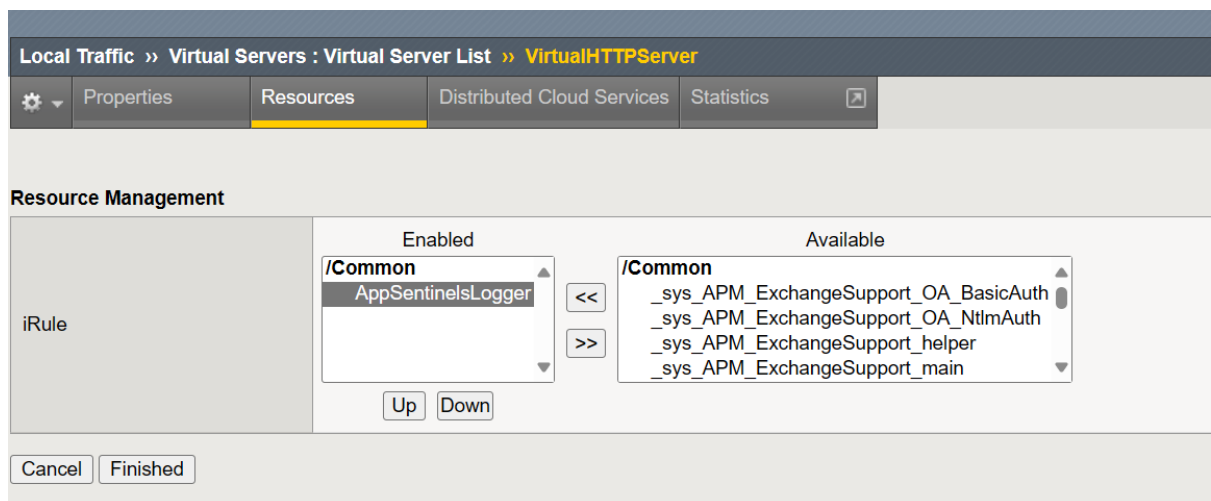
- This ensures connectivity between F5 system Edge-Controller VM over TCP port 9004 is open.

2.1.2 iRule Creation for log forwarding

- Create an iRule by navigating to Local Traffic > iRules > iRule List > Create
- Copy paste the iRule contents provided by Appsentinels
- This iRule will forward API logs to the AppsentinelsEdgeController pool. If the backend pool is different for edge controller, please change the value of variable EDGE_CONTROLLER_POOL appropriately. Ideally there is no change needed in iRule
- If there is host based API routing towards edge controller, set the EDGE_CONTROLLER_HOST appropriately. This will set the host header of the HTTP logs
- Name this iRule as AppSentinelsLogger and Save

2.1.3 Attach the iRule to Virtual Servers

- Identify all Virtual Servers requiring AppSentinels integration.
- Ensure the client profile for the virtual server has HTTP enabled. Since the iRule listens to HTTP events, this is mandatory
- For each Virtual Server, go to Local Traffic > Virtual Servers > Virtual Server List > [Selected Virtual Server] > Resources > iRules (Manage)
- Attach the iRule created above to these Virtual Servers



Local Traffic » Virtual Servers : Virtual Server List » **VirtualHTTPServer**

⚙️ Properties **Resources** Security Distributed Cloud Services Statistics

Load Balancing

Default Pool	httpserverpool ▼
Default Persistence Profile	None ▼
Fallback Persistence Profile	None ▼

Update

iRules Manage...

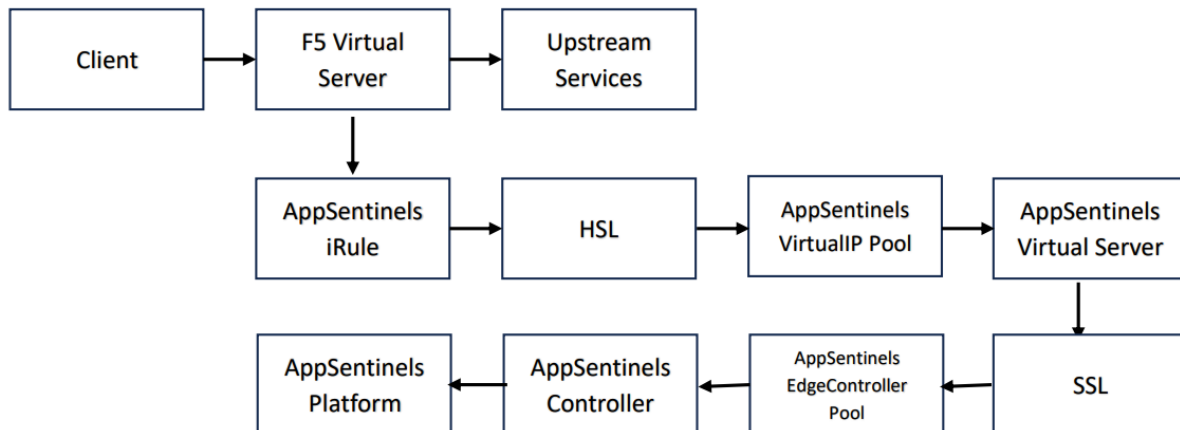
Name
/Common/AppSentinelsLogger

Policies Manage...

Name

- Repeat the process for each of the virtual servers of interest
- The iRule uses ****F5 HSL logging**** to send API logs to the ``AppsentinelsEdgeController`` pool.

3. Integration Configuration for HSL based logging over HTTPS



3.1 Approach

F5 doesn't provide a capability to perform SSL encryption at iRule or HSL layer. However, virtual servers have this capability. To perform logging over HTTPS, we leverage this capability. We create a virtual server to represent AppSentinels Edge controller which can perform encryption of outgoing logs in HTTPS.

3.2 TLDR

- Create a Pool: Name it AppsentinelsEdgeController for the edge-controller.
- Specify Details: Add the edge-controller's IP/hostname and port (default: 9004).
- Create an SSL Virtual Server: Name it AppSentinelsVirtualServer with source 0.0.0.0/0 and any available destination.
- Apply SSL Profile: Attach an appropriate SSL profile to AppSentinelsVirtualServer
- Attach Pool: Link the AppsentinelsEdgeController pool to the AppSentinelsVirtualServer.
- Create a Frontend Pool: Name it AppSentinelsVirtualIPPool, providing the same IP and port as AppSentinelsVirtualServer.
- Update iRule: Point the iRule to AppSentinelsVirtualServer instead of the AppsentinelsEdgeController pool.

3.3 Detailed Steps

3.3.1 Edge Controller Pool Creation

- Go to Local Traffic > Virtual Servers > Pools > Pool List and then click on Create. Name the pool for the edge-controller as AppsentinelsEdgeController. If a different name is used, ensure it is updated in the iRule script. Optionally, enable TCP-based health monitoring for the pool.
- Specify the edge-controller details: Provide the IP address or hostname of the edge-controller and set the listening port to 9004 (default).

Local Traffic » Pools : Pool List » **New Pool...**

Configuration: Basic ▾

Name	AppsentinelsEdgeController	
Description		
Health Monitors	Active /Common tcp	Available standard_bd_monitor_mobilelatm standard_bd_monitor_mobileus standard_bd_monitor_us tcp_half_open udp

Resources

Load Balancing Method	Round Robin ▾
Priority Group Activation	Disabled ▾
New Members	☒ New Node ☐ New FQDN Node ☐ Node List
	Node Name: HostedEdgeController (Optional)
	Address: devsaas3.appsentinels.ai
	Service Port: 9004 HTTP ▾
	Add

Node Name	Address/FQDN	Service Port	Auto Populate	Priority
HostedEdgeController	devsaas3.appsentinels.ai	9004		0

- Click on Finished when done
- Check the status of the controller endpoint by going to Local Traffic > Pools > Pool List > AppsentinelsEdgeController. The status should show as available

Local Traffic » Pools : Pool List » **AppsentinelsEdgeController**

⚙️ Properties **Members** Statistics

Load Balancing

Load Balancing Method	Round Robin ▾
Priority Group Activation	Disabled ▾

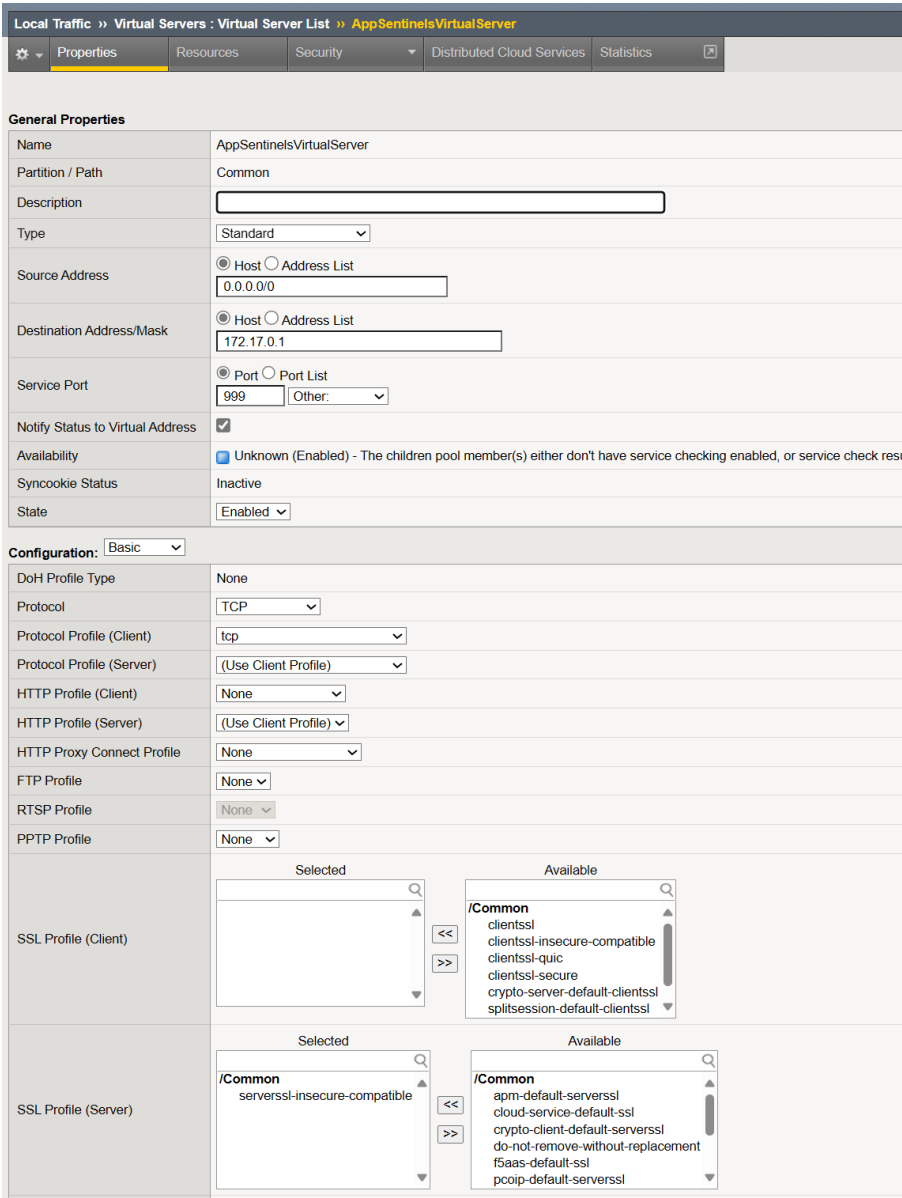
Current Members

✓	▼	Status	Member	▲	Address	◆	Service Port	◆	FQDN	◆	Ephemeral	◆	Ratio	◆	Priority Group	◆	Connection Limit	◆	Partition /
☐		●	HostedEdgeController:9004		34.100.132.211		9004				No		1		0 (Active)		0		Common

- This ensures connectivity between F5 system Edge-Controller VM over TCP port 9004 is open.

3.3.3 Edge Controller Virtual Server and Virtual Pool Creation

- Go to Local Traffic > Virtual Servers > Virtual Server List and then click on Create to create a new Virtual Server for SSL processing. Name it AppSentinelsVirtualServer. Set the source address as 0.0.0.0/0 to accept traffic from all sources. Because this is a virtual server which doesn't terminate any external traffic provide any available destination address and port. This will function as a virtual IP and need not exist in the system.
- Select the appropriate SSL profile (Server):
 - Use `serverssl-insecure` if the SSL certificate is self-signed at the controller.
 - Use `serverssl` for other SSL certificates.
- Do NOT attach AppSentinelsLogger to this Virtual Server



Local Traffic » Virtual Servers : Virtual Server List » AppSentinelsVirtualServer

Properties Resources Security Distributed Cloud Services Statistics

General Properties

Name	AppSentinelsVirtualServer
Partition / Path	Common
Description	
Type	Standard
Source Address	Host Address List 0.0.0.0/0
Destination Address/Mask	Host Address List 172.17.0.1
Service Port	Port Port List 999 Other:
Notify Status to Virtual Address	☒
Availability	☒ Unknown (Enabled) - The children pool member(s) either don't have service checking enabled, or service check res
Synccookie Status	Inactive
State	Enabled

Configuration: Basic

DoH Profile Type	None
Protocol	TCP
Protocol Profile (Client)	tcp
Protocol Profile (Server)	(Use Client Profile)
HTTP Profile (Client)	None
HTTP Profile (Server)	(Use Client Profile)
HTTP Proxy Connect Profile	None
FTP Profile	None
RTSP Profile	None
PPTP Profile	None
SSL Profile (Client)	Selected Available /Common clientssl clientssl-insecure-compatible clientssl-quic clientssl-secure crypto-server-default-clientssl splitsession-default-clientssl
SSL Profile (Server)	Selected Available /Common serverssl-insecure-compatible /Common apm-default-serverssl cloud-service-default-ssl crypto-client-default-serverssl do-not-remove-without-replacement f5aas-default-ssl pcoip-default-serverssl

- Click on Finished to save

- Go back again to Local Traffic > Virtual Servers > Virtual Server List > AppSentinelsVirtualServer
- Under the Resources section of AppSentinelsVirtualServer, attach the previously created pool AppsentinelsEdgeController.
- Do NOT attach AppSentinelsLogger to this Virtual Server

Local Traffic >> Virtual Servers : Virtual Server List >> AppSentinelsVirtualServer

Load Balancing

Default Pool	AppsentinelsEdgeController
Default Persistence Profile	None
Fallback Persistence Profile	None

iRules

Name
No records to display.

Policies

Name
No records to display.

- Since HSL can only send logs to a pool, create an additional pool named AppSentinelsVirtualIPPool as the frontend for AppSentinelsVirtualServer. Use the same unused virtual IP address and port as defined for AppSentinelsVirtualServer.
- Go to Local Traffic > Virtual Servers > Pools > Pool List and click on create. Name the pool as AppSentinelsVirtualIPPool. No health check required as this is an internal endpoint.

Local Traffic » Pools : Pool List » **New Pool...**

Configuration: Basic ▾

Name	AppSentinelsVirtualIPPool	
Description		
Health Monitors	Active	Available / Common gateway_icmp http http2 http2_head_f5

Resources

Load Balancing Method	Round Robin ▾										
Priority Group Activation	Disabled ▾										
New Members	☒ New Node ☐ New FQDN Node ☐ Node List										
	Node Name: SSLEncryptingPool (Optional)										
	Address: 172.17.0.1										
	Service Port: 999 Select... ▾										
	Add										
	<table border="1"> <thead> <tr> <th>Node Name</th> <th>Address/FQDN</th> <th>Service Port</th> <th>Auto Populate</th> <th>Priority</th> </tr> </thead> <tbody> <tr> <td>SSLEncryptingPool</td> <td>172.17.0.1</td> <td>999</td> <td></td> <td>0</td> </tr> </tbody> </table>	Node Name	Address/FQDN	Service Port	Auto Populate	Priority	SSLEncryptingPool	172.17.0.1	999		0
Node Name	Address/FQDN	Service Port	Auto Populate	Priority							
SSLEncryptingPool	172.17.0.1	999		0							
	Edit Delete										

Cancel Repeat Finished

- Click on Finished
- Ensure that controller is configured to listen on HTTPS

3.3.4 iRule Creation for log forwarding

- Create an iRule by navigating to Local Traffic > iRules > iRule List > Create
- Copy paste the iRule contents provided by Appsentinels
- Update the iRule to point to AppSentinelsVirtualIPPool instead of the default AppsentinelsEdgeController pool, ensuring traffic is routed correctly.

```

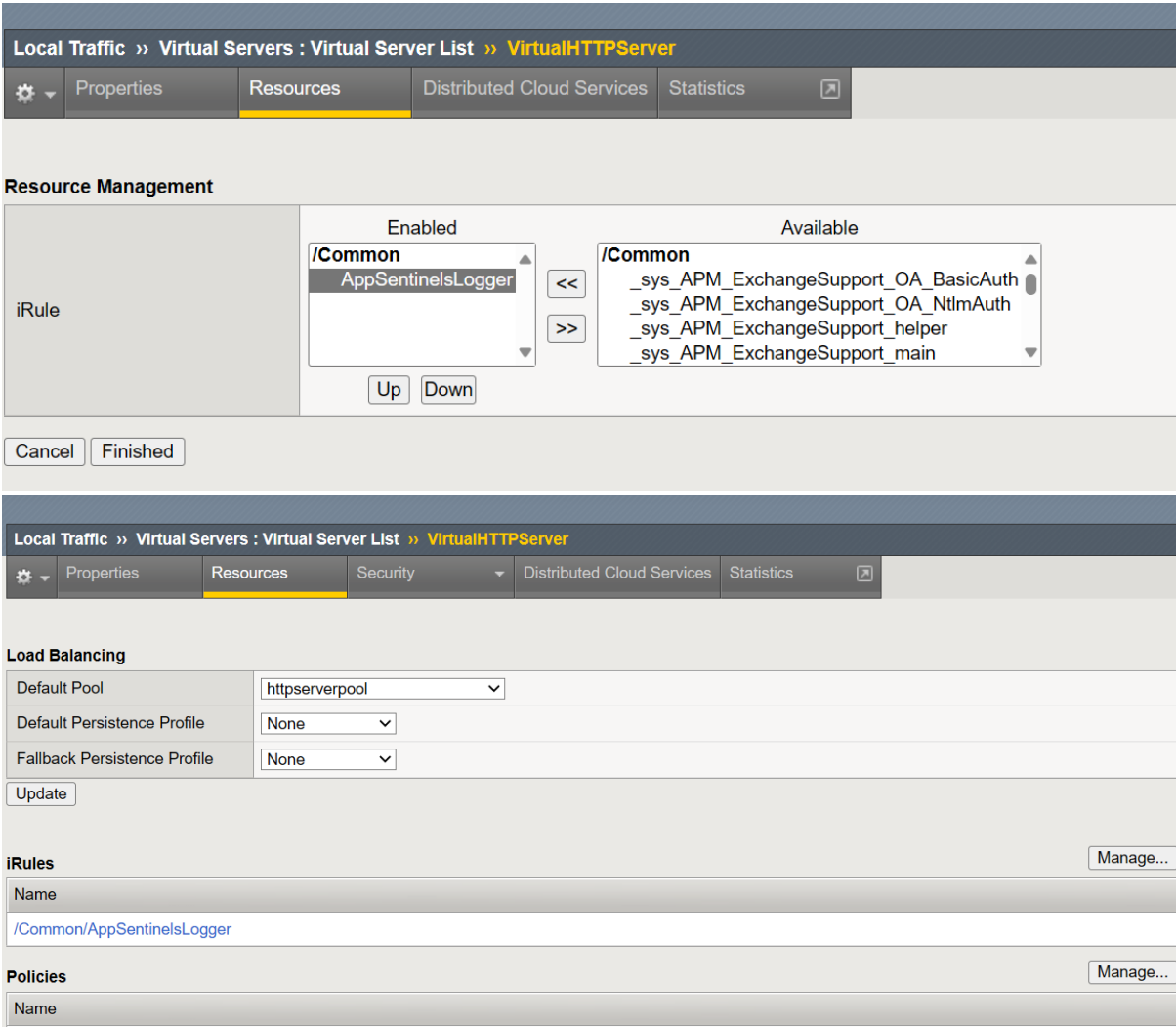
25
26 ▾ when RULE_INIT {
27     set static::EDGE_CONTROLLER_POOL "AppSentinelsVirtualIPPool "
28
29     # Dummy for host header in logging request

```

- Go to Local Traffic > iRules > iRules List > AppSentinelsLogger. Change the value of EDGE_CONTROLLER_POOL variable to achieve this. Click on Update.
- If there is host based API routing towards edge controller, set the EDGE_CONTROLLER_HOST appropriately. This will set the host header of the HTTPS logs
- Name this iRule as AppSentinelsLogger and Save

3.3.5 Attach the iRule to Virtual Servers

- Identify all Virtual Servers requiring AppSentinels integration
- Ensure the client profile for the virtual server has HTTP enabled. Since the iRule listens to HTTP events, this is mandatory
- For each Virtual Server, go to Local Traffic > Virtual Servers > Virtual Server List > [Selected Virtual Server] > Resources > iRules (Manage)
- Attach the iRule created above to these Virtual Servers



Local Traffic » Virtual Servers : Virtual Server List » VirtualHTTPServer

Properties Resources Distributed Cloud Services Statistics

Resource Management

iRule

Enabled

/Common
AppSentinelsLogger

Available

/Common
_sys_APM_ExchangeSupport_OA_BasicAuth
_sys_APM_ExchangeSupport_OA_NtlmAuth
_sys_APM_ExchangeSupport_helper
_sys_APM_ExchangeSupport_main

Up Down

Cancel Finished

Local Traffic » Virtual Servers : Virtual Server List » VirtualHTTPServer

Properties Resources Security Distributed Cloud Services Statistics

Load Balancing

Default Pool httpserverpool

Default Persistence Profile None

Fallback Persistence Profile None

Update

iRules Manage...

Name
/Common/AppSentinelsLogger

Policies Manage...

Name

- Repeat the process for each of the virtual servers of interest
- The iRule uses ****F5 HSL logging**** to send API logs to the `AppsentinelsEdgeController` pool.

4. API version of F5 device

The API version increments with the image versions. This can be determined in one of the following ways:

- Using the iControlRest API to query the current API version.

```
curl -X GET -sku <username:password> -H "Content-Type: application/yang-data+json"
https://<f5host>/mgmt/tm/sys/version | jq .
```

Sample output

```
curl -X GET -sku <username:pass> -H "Content-Type: application/yang-data+json"
https://<hostname>:8443/mgmt/tm/sys/version | jq .
{
  "selfLink": "https://localhost/mgmt/tm/sys/version?ver=16.1.5",
  "entries": {
    ....
  }
}
```

- Alternatively, check the version through the System > Software Management > Image List in the UI.