Azure App Gateway Configuration - ArcGIS Workflow Manager

Alex Campbell

6/1/21

Contents

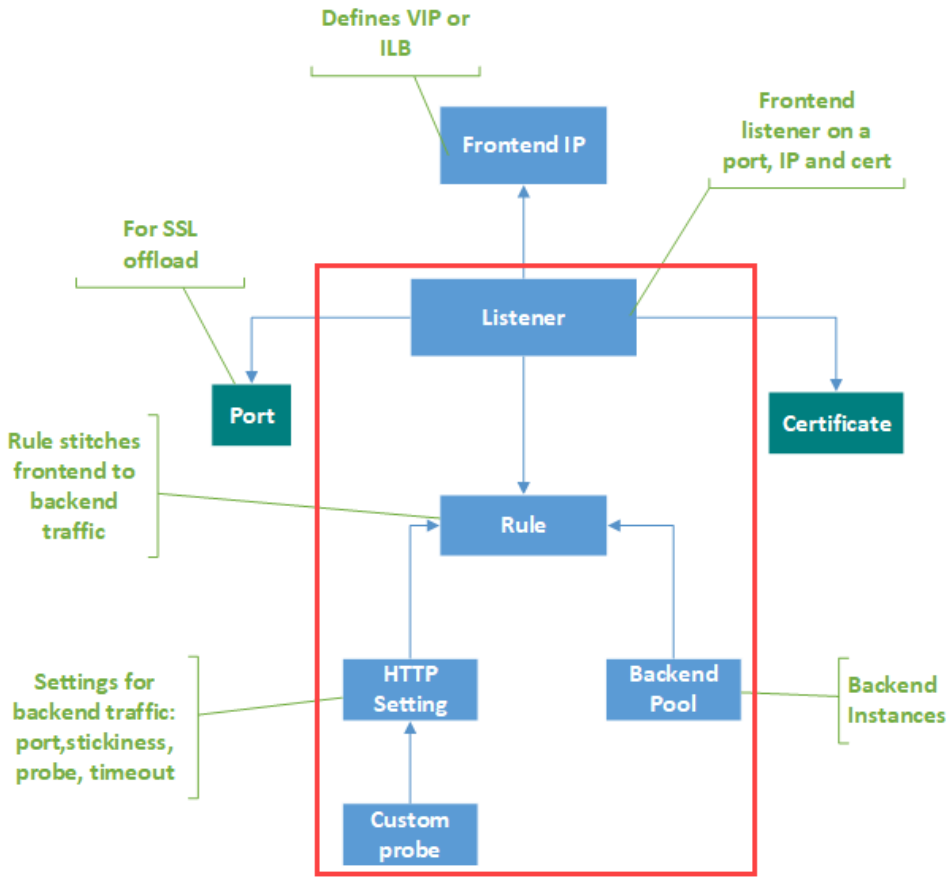
Background

As part of a proof-of-concept activity, Esri Professional Services staff was tasked with determining the appropriate configuration of an Azure Application Gateway (v2) with the new services-based ArcGIS Workflow Manager. This guide assumes some knowledge of basic Application Gateway configuration and how it can be used to act as a reverse proxy for ArcGIS Enterprise in Azure.

Following the deployment of a base 10.9 ArcGIS Enterprise deployment with ArcGIS Enterprise Cloud Builder for Microsoft Azure, the new Workflow Manager server was installed on top of the Hosting server. Although the test environment was a single-machine deployment of Enterprise, the configuration parameters should still apply to the recommended separated deployment pattern displayed below.

Application Gateway Configuration

The below sections outline a brief general discussion of the purpose of each of the settings within the Application Gateway (App Gateway) and focused instructions on configurations specific to ArcGIS Workflow Manager. We will focus on the highlighted components as it pertains to Workflow Manager Server.



Listeners

Listeners are configured within the App Gateway to check for incoming requests. As described in the Microsoft documentation:

> *"A listener is a logical entity that checks for incoming connection requests. A listener accepts a request if the protocol, port, hostname, and IP address associated with the request match the same elements associated with the listener configuration."*

When deploying App Gateway with ArcGIS Enterprise, two listeners should be configured. By default, Cloud Builder will create a listener for HTTP (80) and HTTPS (443) traffic respectively. Each listener is then associated with a Rule that allows the App Gateway to forward traffic over the specified port to the appropriate backend destination.

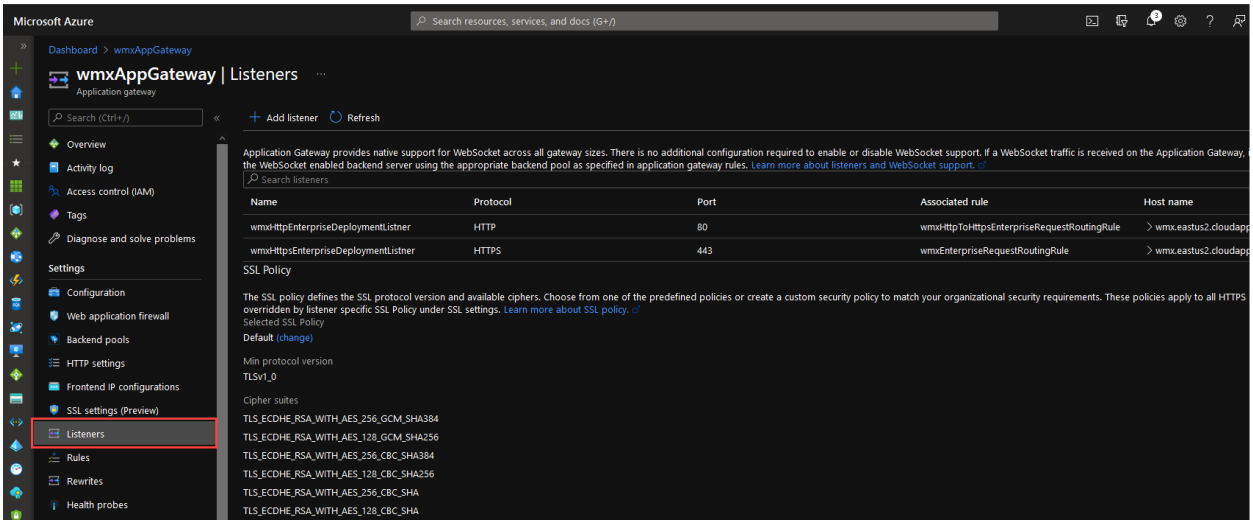


Figure - Application Gateway Listener Overview

For both listeners, you will specify the public IP address of the App Gateway along with the Port and Host name of the listener.

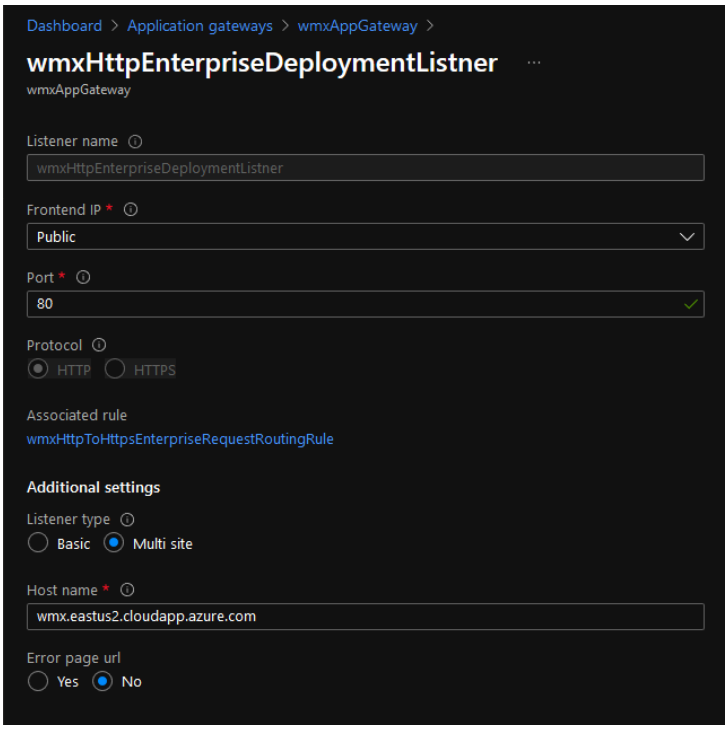


Figure - HTTP Listener Configuration

Since your HTTPS listener will utilize TLS to encrypt traffic, you must also specify the TLS certificate for your public alias.

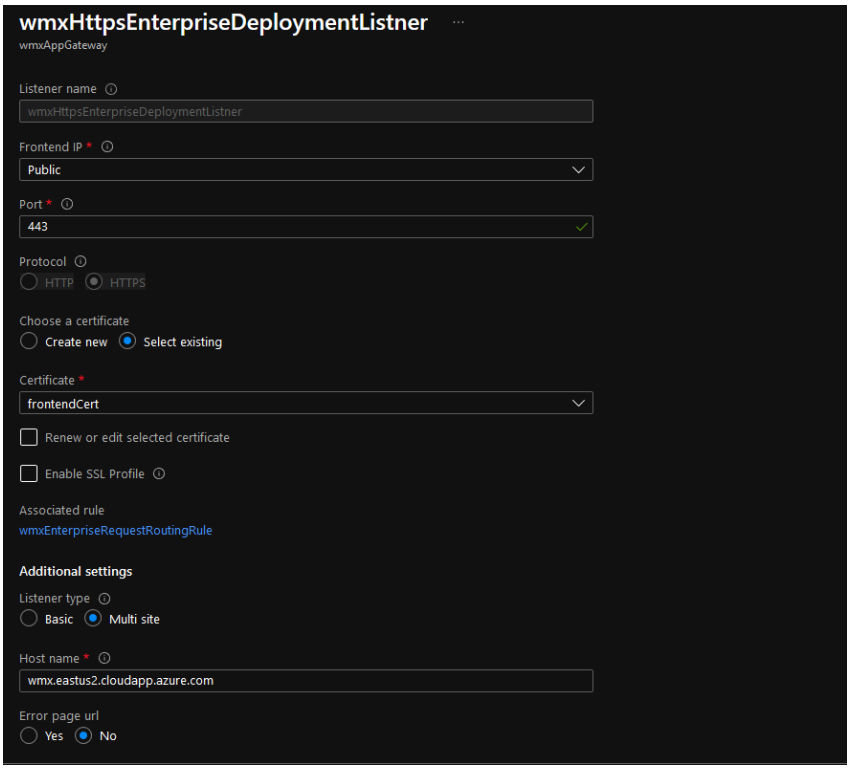


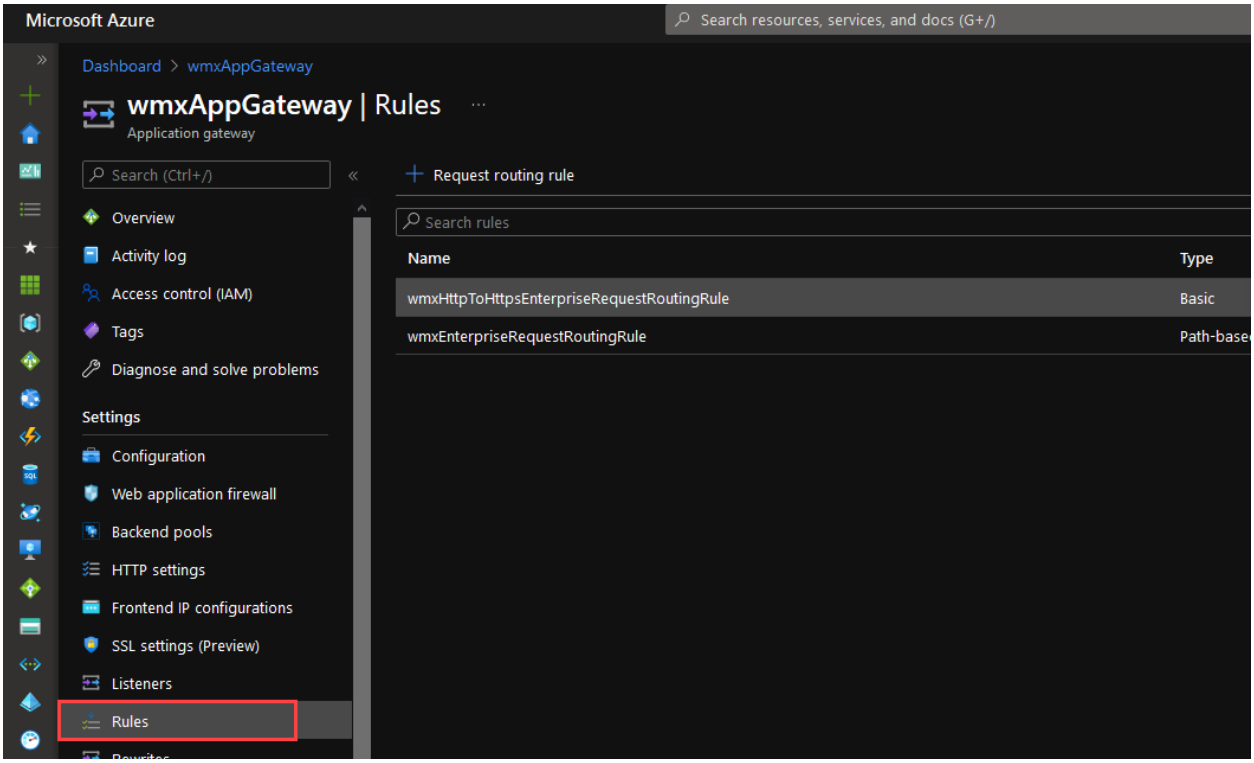
Figure - HTTPS Listener Configuration

Rules

Request routing rules are what pulls together our listener, HTTP settings, and backend pools. As described by Microsoft:

"A request routing rule is a key component of an application gateway because it determines how to route traffic on the listener. The rule binds the listener, the backend server pool, and the backend HTTP settings.

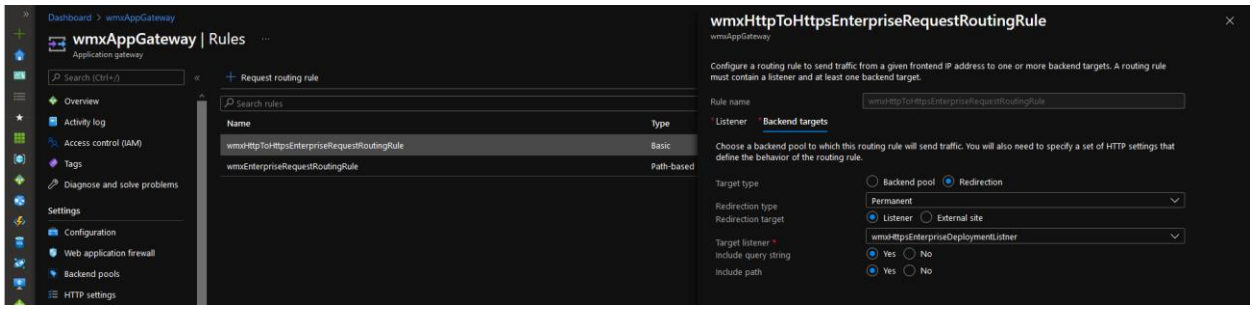
When a listener accepts a request, the request routing rule forwards the request to the backend or redirects it elsewhere. If the request is forwarded to the backend, the request routing rule defines which backend server pool to forward it to. The request routing rule also determines if the headers in the request are to be rewritten. One listener can be attached to one rule."



Basic Rules

There are two main types of request routing rules in the Application Gateway, Basic and Path-Based. Basic rules direct all traffic on the associated listener to the associated backend pool. For ArcGIS Enterprise, a single basic rule is created to redirect traffic from the HTTP listener (80) to the HTTPS listener (443).

Setting	Value
Listener	HTTP Listener
Target Type	Redirection
Redirection Type	Permanent
Redirection Target	Listener
Target Listener	HTTPS Listener
Include Query String	Yes
Include Path	Yes



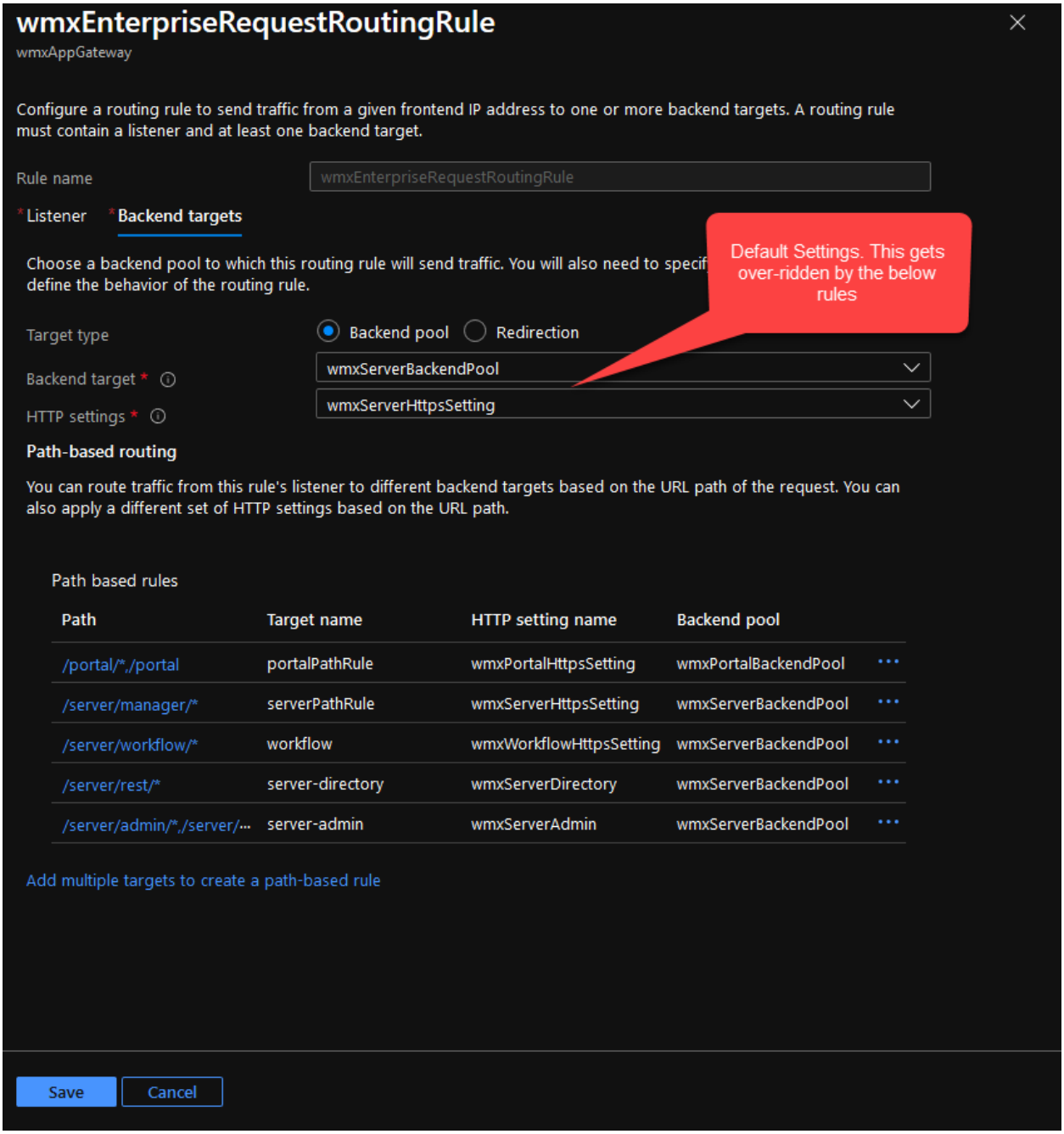
Path-Based Rules

Path-based rules direct traffic to backend pools based on the evaluation of the request URL against a set of defined paths. If the URL path matches that of a specific rule, the App Gateway will re-route the traffic accordingly. If the path does not match any of the path-based rules, traffic is sent to the default backend pool via the default HTTP setting.

In a standard base deployment of ArcGIS Enterprise, only two rules are required: one for Portal, and one for Server. Because Workflow Server is installed as an extension of an existing ArcGIS Server site, we are required to use an explicit path for each endpoint within that Server. Again, this may be avoidable depending on the configuration of the system, and how App Gateway evaluates rules, but in testing this was the requirement.

Note: Although Portal, Server, and Workflow Server are all listening for traffic on different ports and/or machines, a single path-based rule can be created as each path will override the base settings specified in the upper section of the configuration.

Target Name	Path	HTTP Setting	Backend Pool
Portal	/portal/*,/portal	Portal	Portal
Server Manager	/server/manager/*	Server Manager	Server
Server Directory	/server/rest/*	Server Directory	Server
Server Admin	/server/admin/*	Server Admin	Server
Workflow Server	/server/workflow/*	Workflow Server	Server or Stand-alone Workflow Server

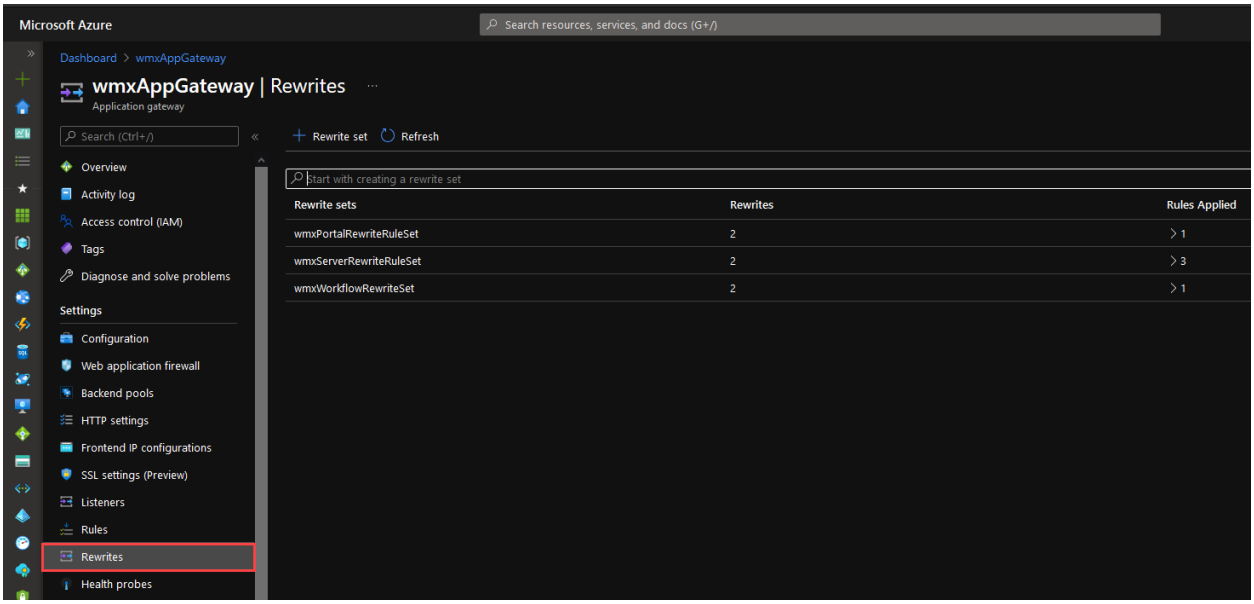


Rewrites

Rewrite rules allow you to add, remove, or update HTTP request and response headers as the request moves through the App Gateway on to the backend pool. Rewrite rules are configured as sets in App Gateway with three main components:

- Request Routing Rule Association – The desired routing rule to apply the rewrite. With path-based routing the rewrite configuration is defined based on the desired path out of the rules specified above.

- Rewrite Condition – An optional configuration, the action will occur if the request or response meets the condition
- Rewrite Type – Request Headers, Response Headers, URL Components



In a standard base deployment, only two rewrite sets would be created, each applied to a single path (Portal and Server). As noted above, because we have multiple Server site endpoints to handle, we will apply the Server rewrite to three paths. Additionally, Workflow Manager requires different rewrites and a third rewrite set must be created accordingly.

Server Rewrites	
Setting	Value
Set Name	Server Rewrite Rule Set
Associated Routing Rules	Server Manager, Server Directory, Server Admin
Rewrite Rule Name	XForwardedHostRewrite
Rule Sequence (Lower evaluates first)	50
Action	Set request header “X-Forwarded-Host” = {http_req_host}
Rewrite Rule Name	ServerRewrite
Rule Sequence	100
Condition	If Common Response Header “Location” equals “(https?):\/\/[^\/]+:6443\/(?:arcgis|server)(.*)$”
Action #1	Set Custom Response Header “RewriteLocationValue” = {http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}

Action #2	Set Common Response Header “Location” = {http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}

Workflow Server Rewrites	
Setting	Value
Set Name	Workflow Server Rewrite Rule Set
Associated Routing Rules	Workflow Server
Rewrite Rule Name	XForwardedHostRewrite
Rule Sequence (Lower evaluates first)	50
Action	Set request header “X-Forwarded-Host” = {http_req_host}
Rewrite Rule Name	WorkflowRewrite
Rule Sequence	100
Condition	If Common Response Header “Location” equals “(https?):\/\/[^\/]+:13443\/(?:arcgis|server|workflow)(.*)$”
Action #1	Set Custom Response Header “RewriteLocationValue” = {http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}
Action #2	Set Common Response Header “Location” = {http_resp_Location_1}://{http_req_host}/server{http_resp_Location_2}

HTTP Settings

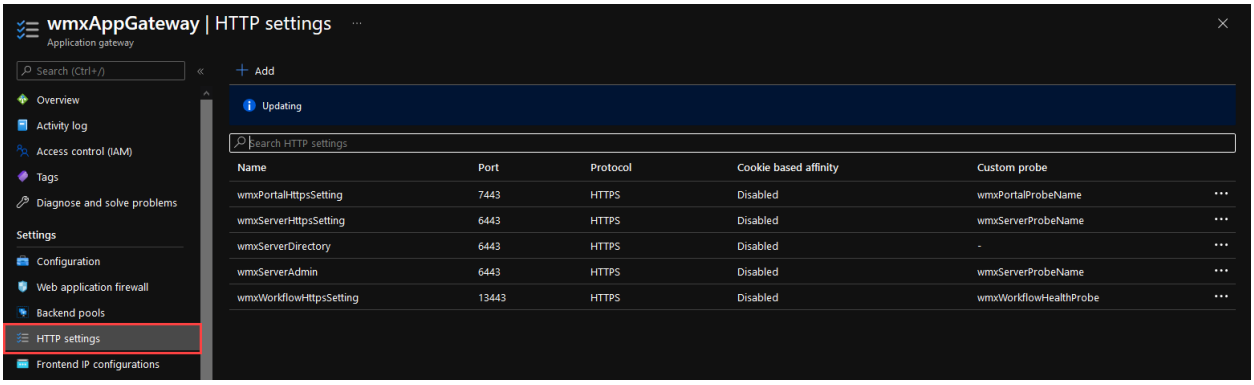
HTTP Settings allow you to specify the port number, protocol, and other details about how the request routing rules route traffic to the backend servers. As described by Microsoft:

“The port and protocol used in the HTTP settings determine whether the traffic between the application gateway and backend servers is encrypted (providing end-to-end TLS) or unencrypted.

This component is also used to:

- *Determine whether a user session is to be kept on the same server by using the cookie-based session affinity.*
- *Gracefully remove backend pool members by using connection draining.*
- *Associate a custom probe to monitor the backend health, set the request timeout interval, override host name and path in the request, and provide one-click ease to specify settings for the App Service backend.”*

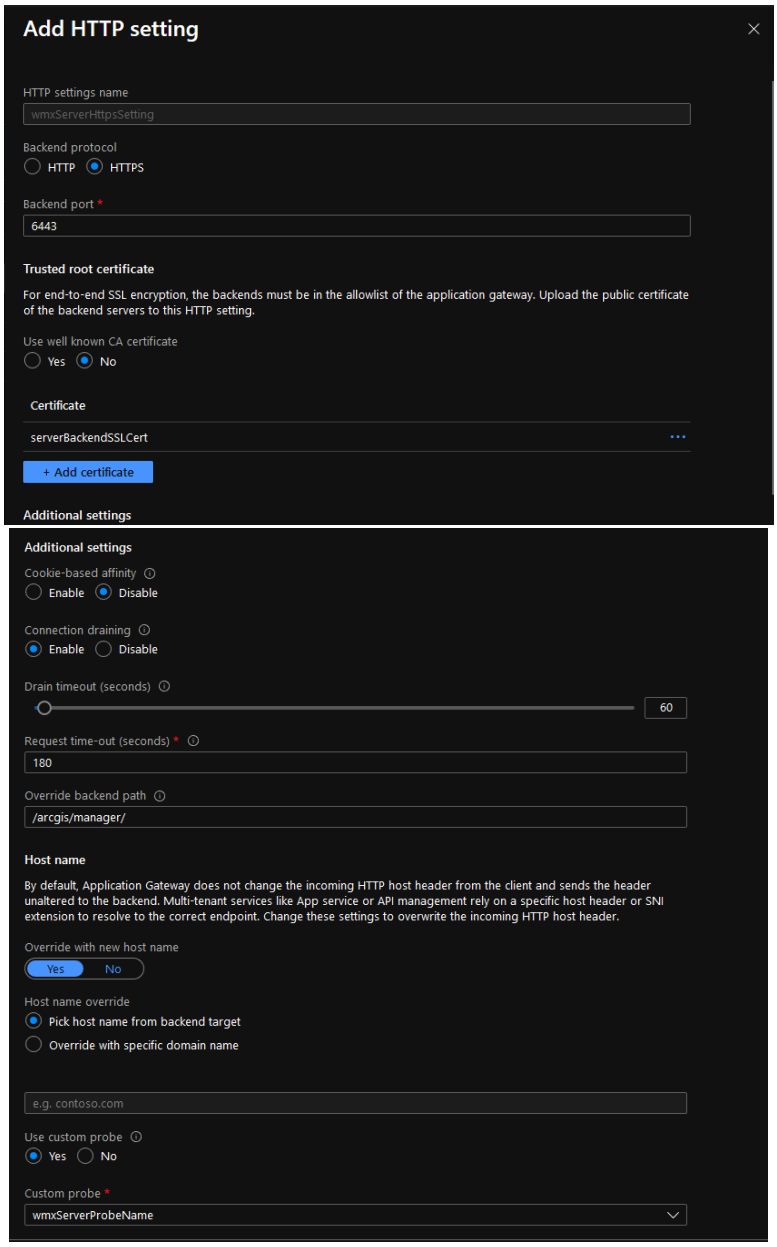
In a base configuration of Application Gateway for ArcGIS Enterprise, two HTTP settings are created: one for Portal, and one for Server. Because the Workflow Server was installed into the Hosting Server, a HTTP setting must be created for each of the Server endpoints individually. This is related to how Application Gateway evaluates it's request rules and may be avoidable depending on your deployment pattern.



Below, each ArcGIS Server related HTTP setting is detailed. For all the Hosting (GIS) Server endpoints, the port will be 6443 with the only difference being the "Override backend path" to specify which part of Server we want to direct traffic in our rules.

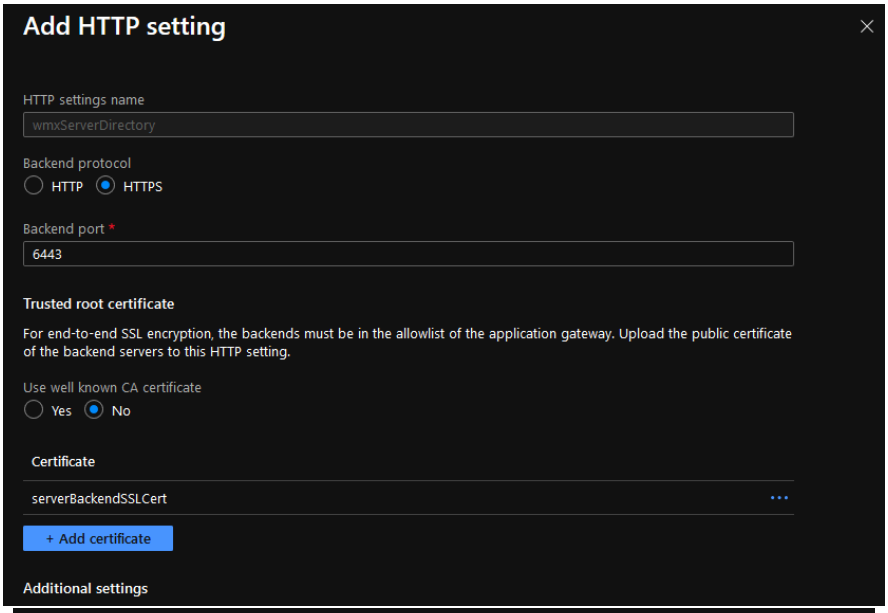
Server Manager:

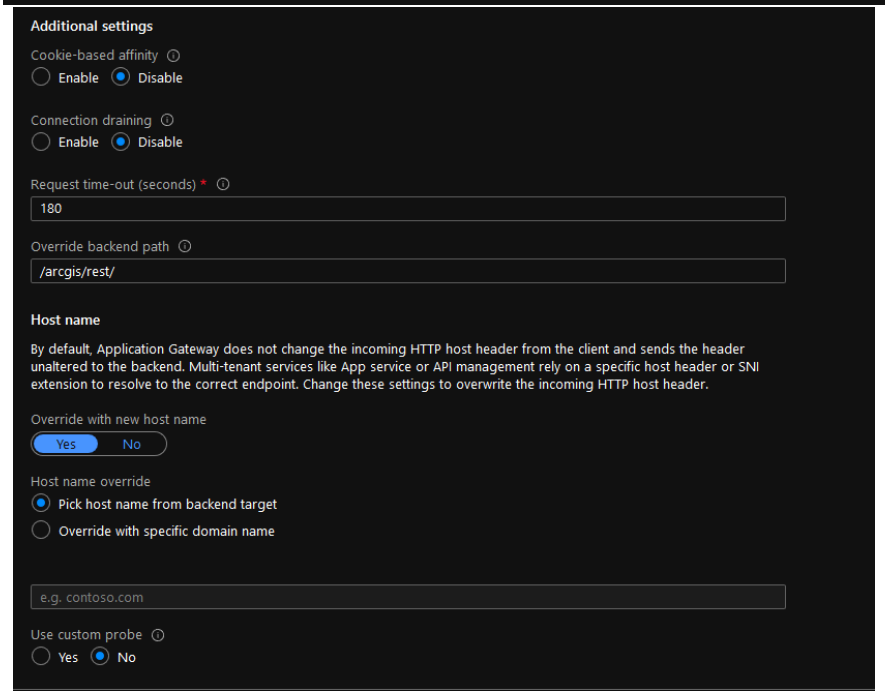
Setting	Value
Port	6443
Request Time-Out	180 (Seconds)
Override Backend Path	/arcgis/manager
Custom Probe	ArcGIS Server Health Probe



Server Directory (/rest/services):

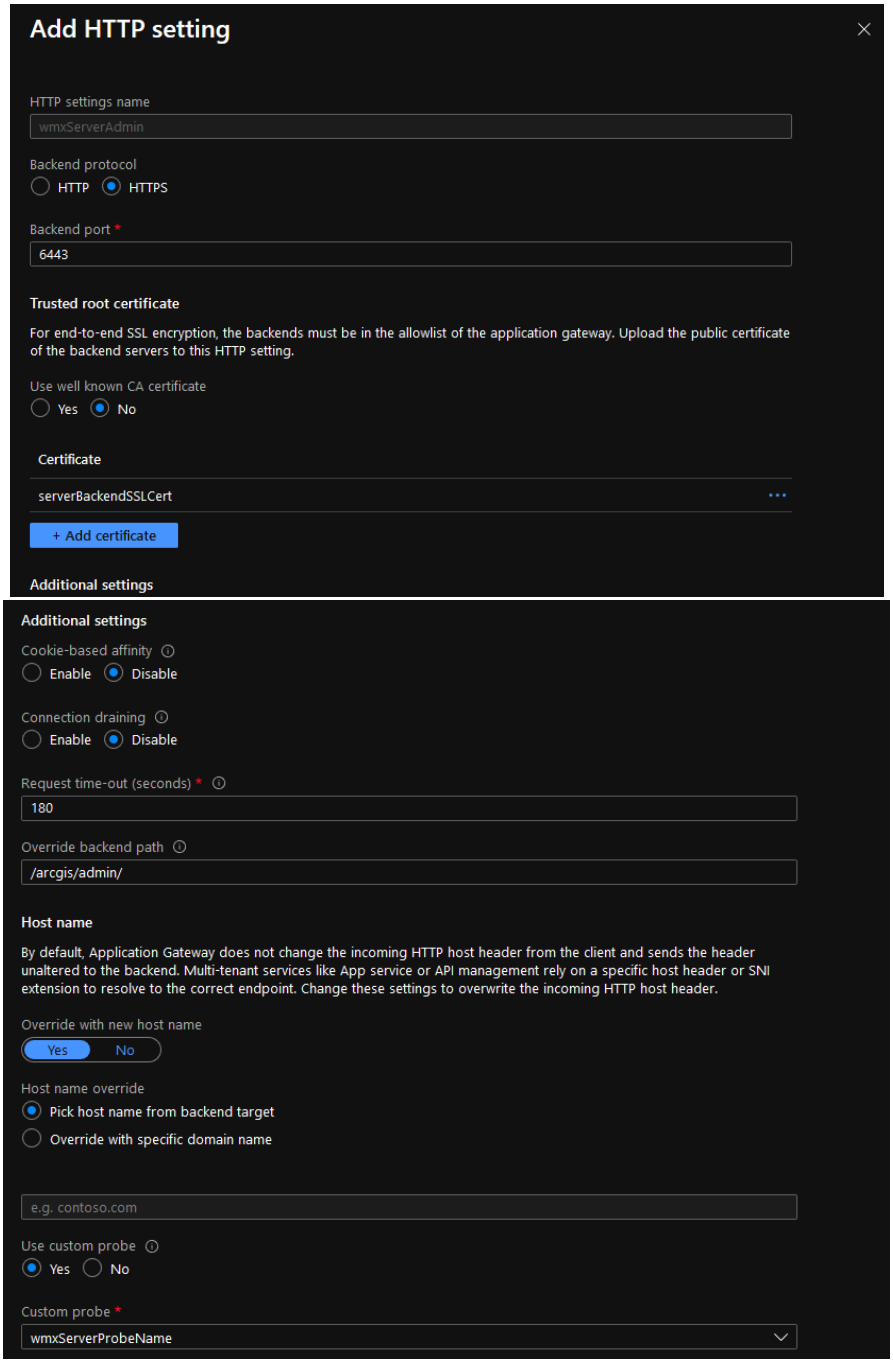
Setting	Value
Port	6443
Request Time-Out	180 (Seconds)
Override Backend Path	/arcgis/rest/
Custom Probe	ArcGIS Server Health Probe





Server Admin:

Setting	Value
Port	6443
Request Time-Out	180 (Seconds)
Override Backend Path	/arcgis/admin/
Custom Probe	ArcGIS Server Health Probe

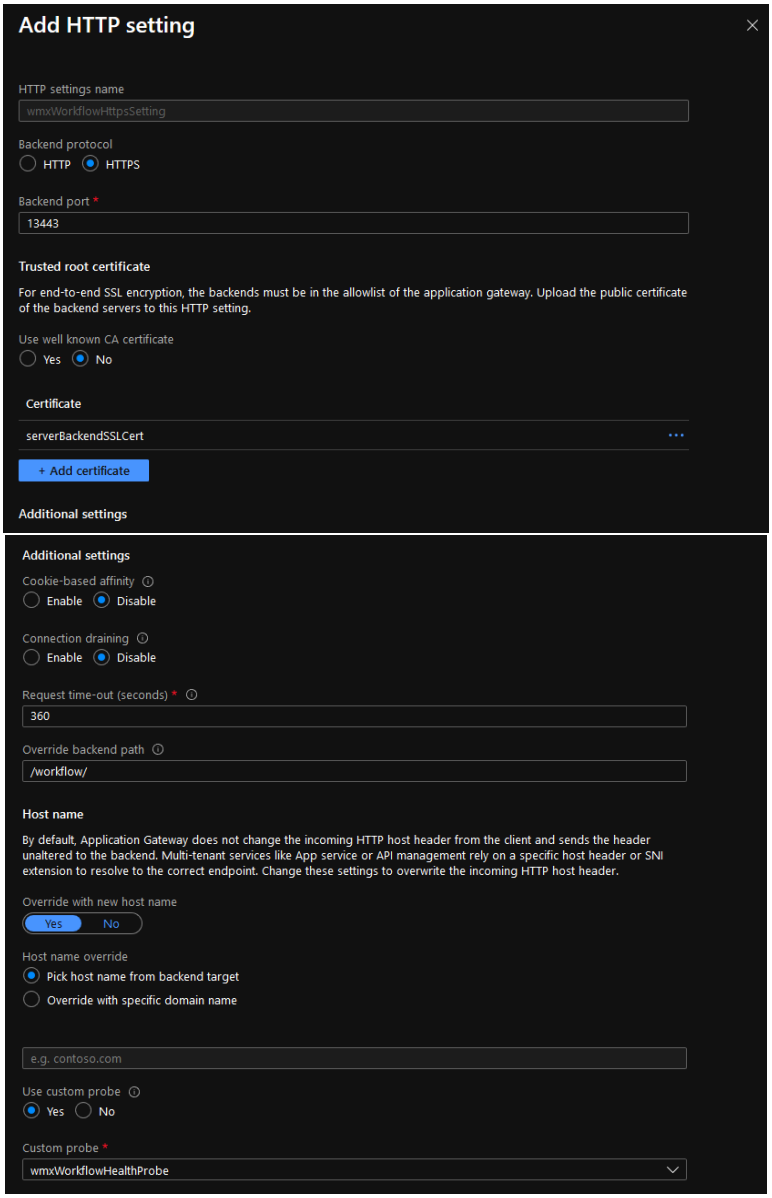


Workflow Server

Workflow Manager Server has different requirements and therefore has a slightly different HTTP Setting. The following details are required for successful operation of Workflow Server.

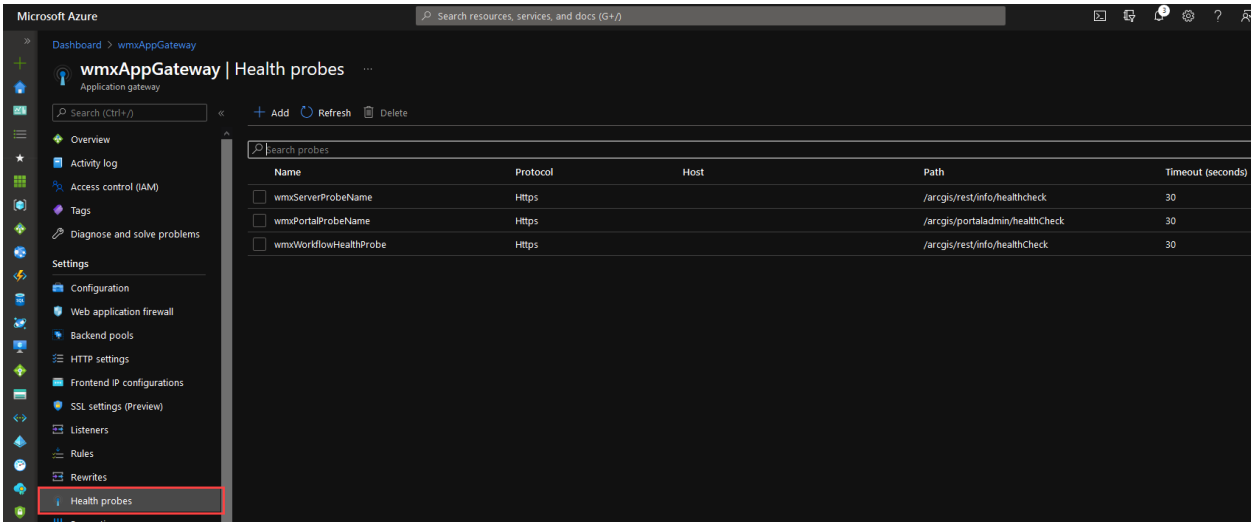
Setting	Value
Port	13443
Request Time-Out	360 (Seconds)
Override Backend Path	/workflow/

Custom Probe	See below for probe details. Because Workflow Server does not currently provide a non-authenticated health check, we need to use the default GIS Server health check endpoint over port 6443 for this setting.



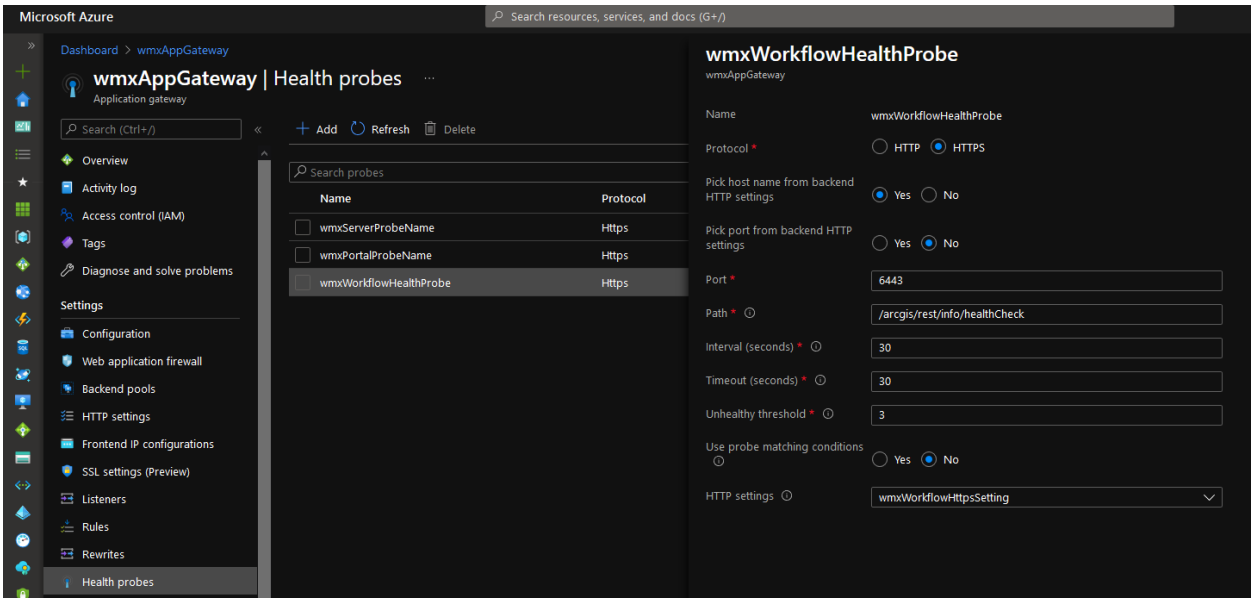
Health Probes

Health probes check the health of the resources within a specified backend pool and automatically removes unhealthy resources after failure to the probe. For ArcGIS Enterprise, the built-in health check functionality can be used to assess the health of each component (Portal/Server).



Currently, Workflow Server does not have a non-authenticated health check endpoint and therefore the underlying Server site's health check must be configured.

Setting	Value
Protocol	HTTPS
Pick host name from backend HTTP settings	Yes
Pick port from backend HTTP settings	No
Port	6443
Path	/arcgis/rest/info/healthCheck
Interval	30 (seconds)
Timeout	30 (seconds)
Unhealthy threshold	3
Use probe matching conditions	No
HTTP Settings	Workflow HTTP Setting

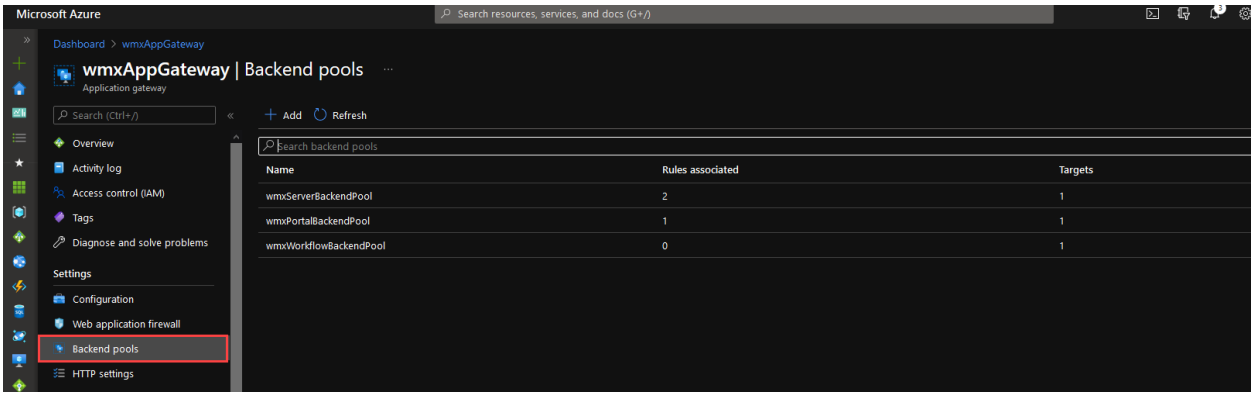


Backend Pools

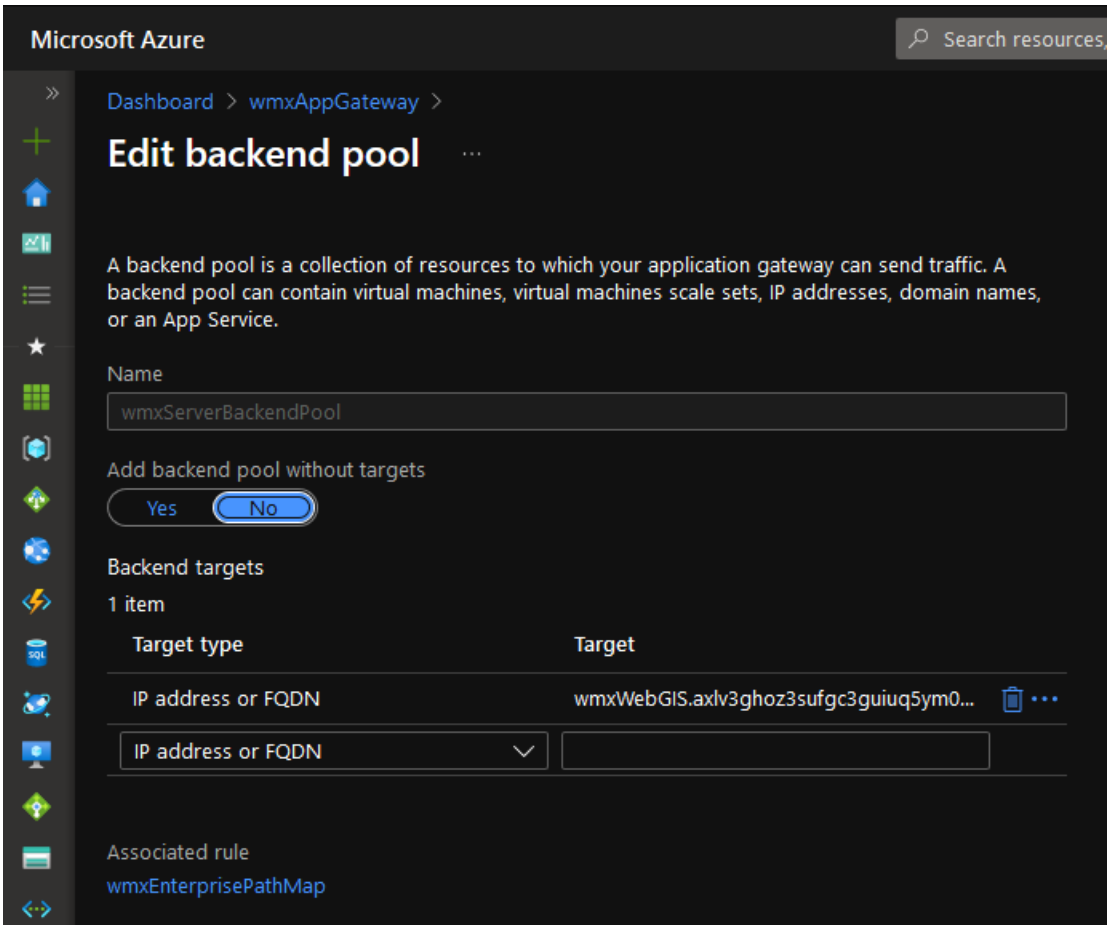
Backend Pools route requests in the chain to your backend servers. They can contain:

- NICs
- Virtual machine scale sets
- Public IP addresses
- Internal IP addresses
- FQDN
- Multitenant backends

For ArcGIS Enterprise, we are going to utilize the FQDN of the backend servers as the destination for the backend pools. In the screenshot below, an additional backend pool has been setup to model what a multi-machine environment would look like within the Azure Portal.



Each Backend Pool will have a single target, pointing at the FQDN of the machine hosting the component we are interested in (Portal, Server, Workflow Server, etc..).


Microsoft Azure
Search resources
Dashboard > wmxAppGateway >
Edit backend pool
A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machines scale sets, IP addresses, domain names, or an App Service.
Name
wmxServerBackendPool
Add backend pool without targets
Yes
No
Backend targets
1 item
Target type
Target
IP address or FQDN
wmxWebGIS.axlv3ghoz3sufgc3guiuq5ym0...
IP address or FQDN
Associated rule
wmxEnterprisePathMap