Overview

This documentation describes the deployment of an Azure Application Gateway in front of Imaging v3.

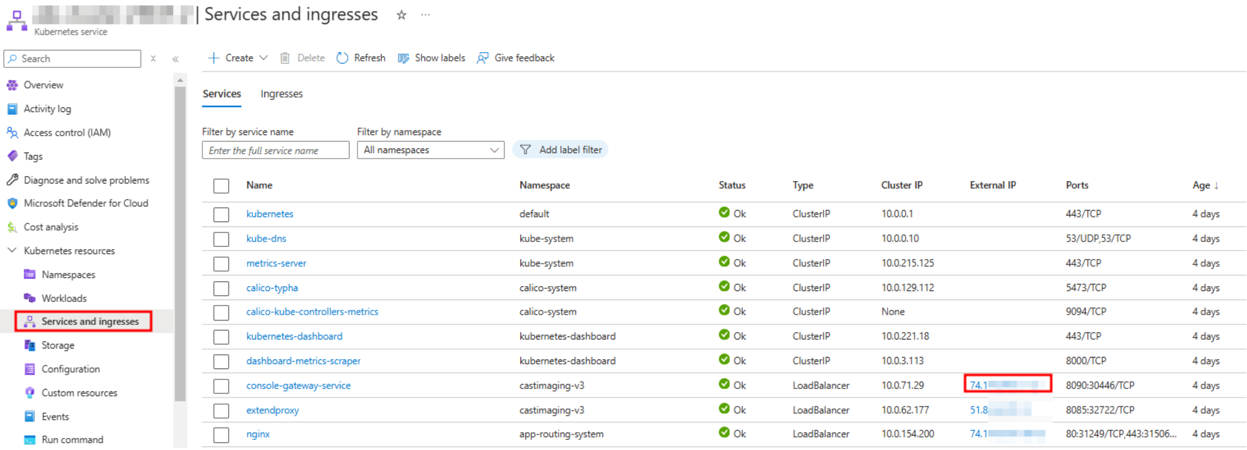
Prerequisites

- You own a valid certificate in the PFX format with the associated passphrase.
- You have the required permissions on your Azure tenant to create Application Gateways.
- You have the required permissions to create a DNS record on the desired DNS zone which will point to your Application Gateway listener IP address.

Procedure

Retrieve console-gateway-service external IP

Retrieve the console-gateway-service pod external IP.



[redacted] | Services and ingresses

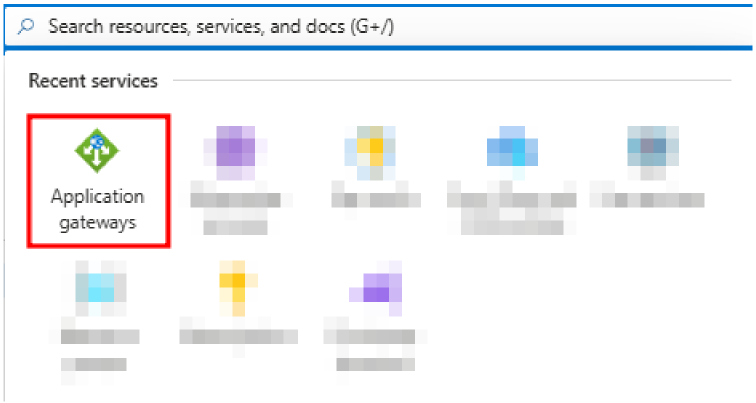
Filter by service name: *Enter the full service name*

Filter by namespace: All namespaces

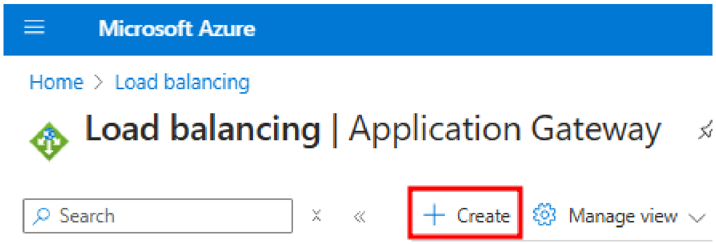
□	Name	Namespace	Status	Type	Cluster IP	External IP	Ports	Age ↓
□	kubernetes	default	✓ Ok	ClusterIP	10.0.0.1		443/TCP	4 days
□	kube-dns	kube-system	✓ Ok	ClusterIP	10.0.0.10		53/UDP,53/TCP	4 days
□	metrics-server	kube-system	✓ Ok	ClusterIP	10.0.215.125		443/TCP	4 days
□	calico-typha	calico-system	✓ Ok	ClusterIP	10.0.129.112		5473/TCP	4 days
□	calico-kube-controllers-metrics	calico-system	✓ Ok	ClusterIP	None		9094/TCP	4 days
□	kubernetes-dashboard	kubernetes-dashboard	✓ Ok	ClusterIP	10.0.221.18		443/TCP	4 days
□	dashboard-metrics-scraper	kubernetes-dashboard	✓ Ok	ClusterIP	10.0.3.113		8000/TCP	4 days
□	console-gateway-service	castimaging-v3	✓ Ok	LoadBalancer	10.0.71.29	74.1[redacted]	8090:30446/TCP	4 days
□	extendproxy	castimaging-v3	✓ Ok	LoadBalancer	10.0.62.177	51.8[redacted]	8085:32722/TCP	4 days
□	nginx	app-routing-system	✓ Ok	LoadBalancer	10.0.154.200	74.1[redacted]	80:31249/TCP,443:31506...	4 days

Create the Application Gateway

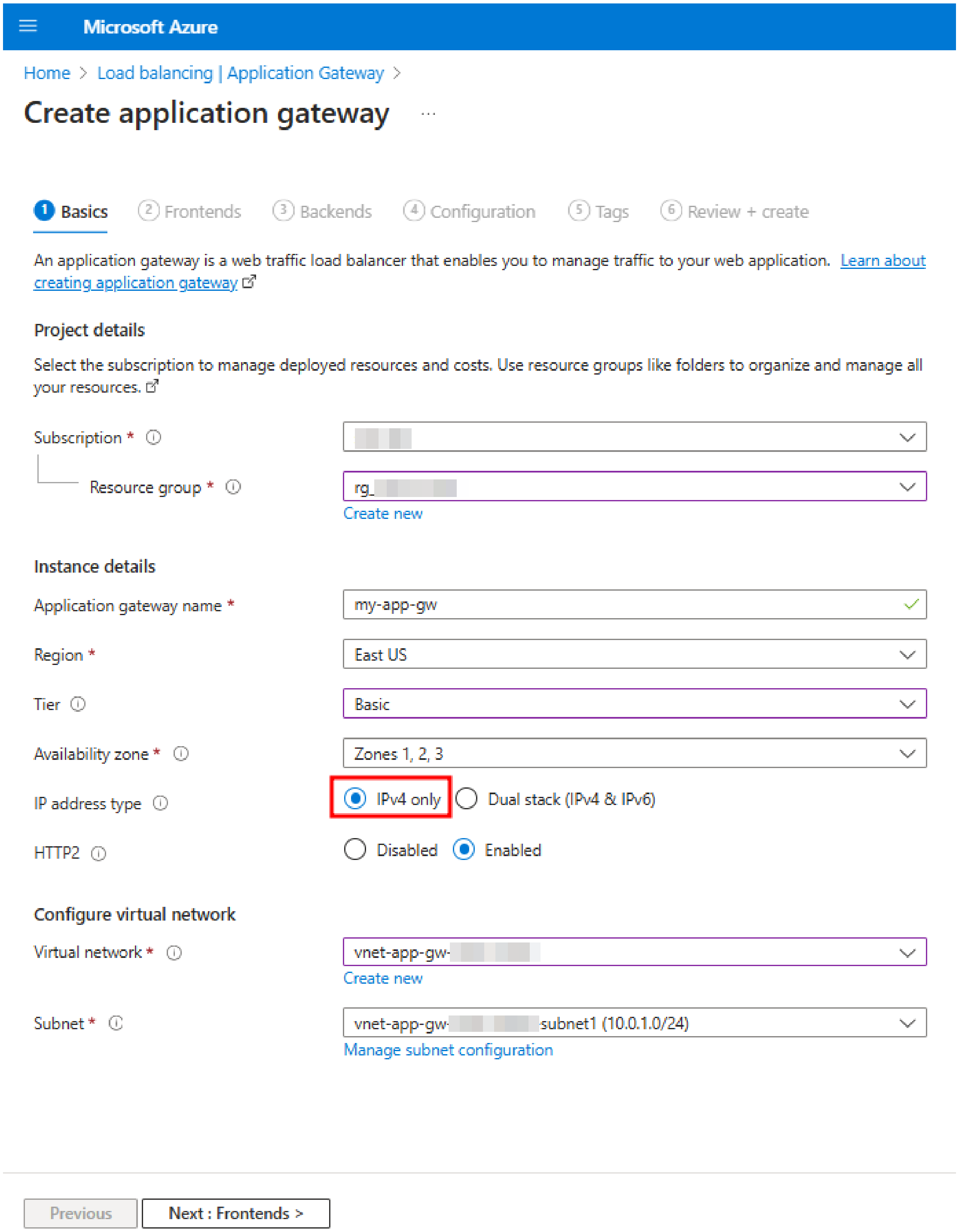
Search for the Azure Application Gateways service.



Create a new one.



Set the usual settings as desired. You will need to use a subnet dedicated to Application Gateways. Only use IPv4 IP address types as IPv6 is not yet supported on Imaging.



Create application gateway ...

An application gateway is a web traffic load balancer that enables you to manage traffic to your web application. Learn about creating application gateway

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	[redacted]
Resource group *	rg_[redacted] Create new

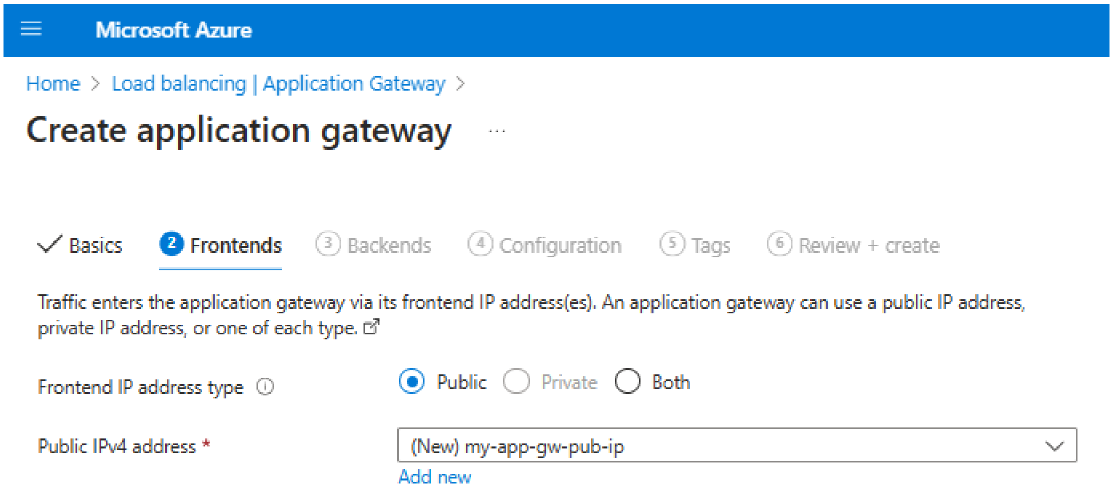
Instance details

Application gateway name *	my-app-gw
Region *	East US
Tier	Basic
Availability zone *	Zones 1, 2, 3
IP address type	● IPv4 only ○ Dual stack (IPv4 & IPv6)
HTTP2	○ Disabled ● Enabled

Configure virtual network

Virtual network *	vnet-app-gw-[redacted] Create new
Subnet *	vnet-app-gw-[redacted]subnet1 (10.0.1.0/24) Manage subnet configuration

Configure a new IP address or use an existing one.



Create application gateway ...

✓ Basics 2 Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

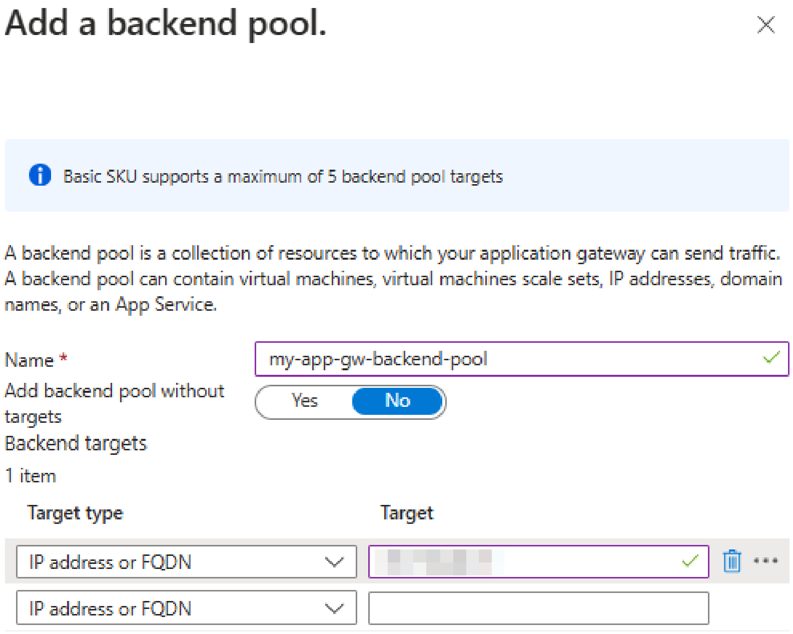
Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type: ● Public ○ Private ○ Both

Public IPv4 address *: (New) my-app-gw-pub-ip

Add new

Create a new backend pool. Use the console-gateway-service external IP you retrieved above.



Add a backend pool.

Basic SKU supports a maximum of 5 backend pool targets

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 *: my-app-gw-backend-pool ✓

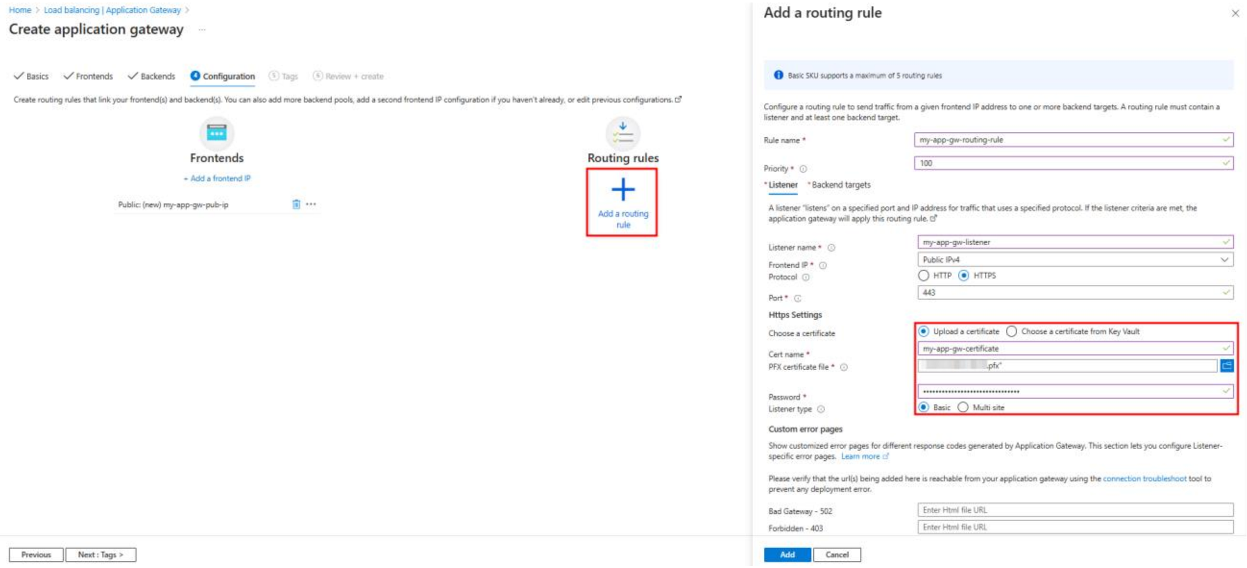
Add backend pool without targets: Yes [✓ No]

Backend targets

1 item

Target type	Target
IP address or FQDN	[redacted] ✓
IP address or FQDN	

Configure the listener. Choose the “Upload a certificate” option and upload a certificate which will be valid for the FQDN you plan to use for the Application Gateway.



Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

Public: (new) my-app-gw-pub-ip

Add a routing rule

Basic SKU supports a maximum of 5 routing rules

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name * my-app-gw-routing-rule

Priority * 100

*Listener *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule.

Listener name * my-app-gw-listener

Frontend IP * Public IPv4

Protocol ○ HTTP ● HTTPS

Port * 443

Https Settings

Choose a certificate ● Upload a certificate ○ Choose a certificate from Key Vault

Cert name * my-app-gw-certificate

PFX certificate file * "[redacted].pfx"

Password * ********************************

Listener type ● Basic ○ Multi site

Custom error pages

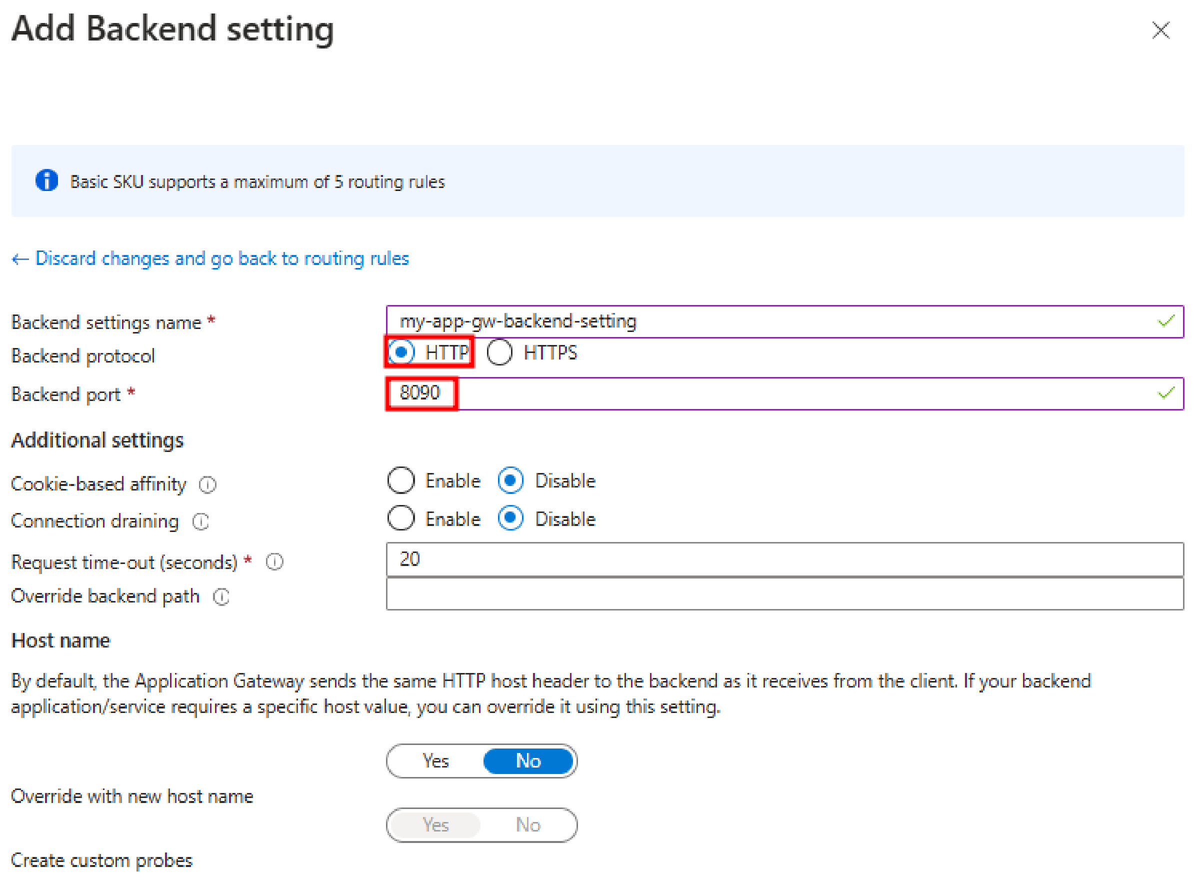
Show customized error pages for different response codes generated by Application Gateway. This section lets you configure Listener-specific error pages. Learn more

Please verify that the url(s) being added here is reachable from your application gateway using the connection troubleshoot tool to prevent any deployment error.

Bad Gateway - 502 Enter Html file URL

Forbidden - 403 Enter Html file URL

Configure the backend target with the following backend setting.



Add Backend setting

Basic SKU supports a maximum of 5 routing rules

Backend settings name * my-app-gw-backend-setting

Backend protocol ● HTTP ○ HTTPS

Backend port * 8090

Additional settings

Cookie-based affinity ○ Enable ● Disable

Connection draining ○ Enable ● Disable

Request time-out (seconds) * 20

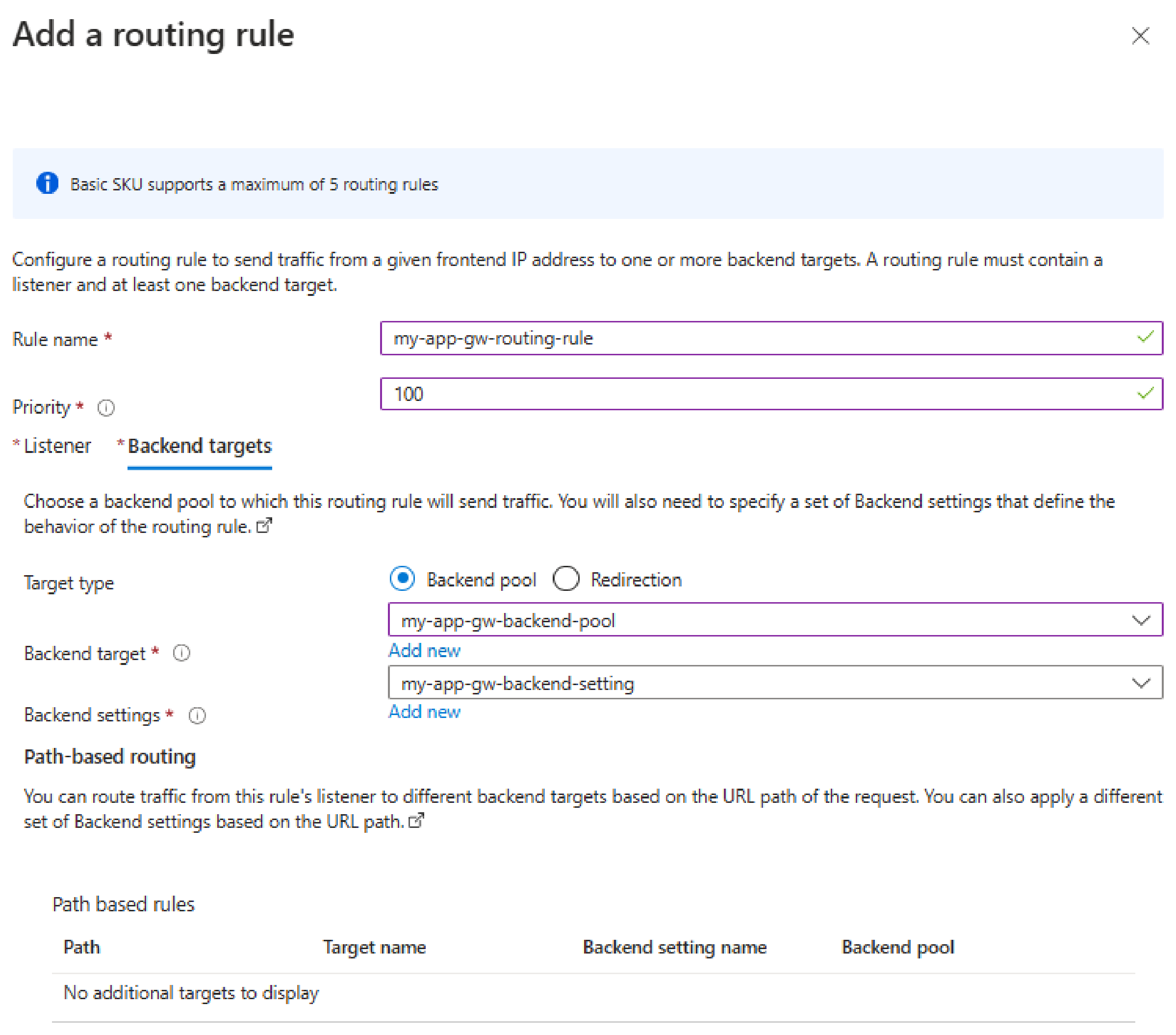
Override backend path

Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

Override with new host name Yes [✓ No]

Create custom probes Yes No



Add a routing rule

ⓘ Basic SKU supports a maximum of 5 routing rules

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name *	my-app-gw-routing-rule ✓
Priority * ⓘ	100 ✓

Choose a backend pool to which this routing rule will send traffic. You will also need to specify a set of Backend settings that define the behavior of the routing rule.

Target type	● Backend pool ○ Redirection
Backend target * ⓘ	my-app-gw-backend-pool Add new
Backend settings * ⓘ	my-app-gw-backend-setting Add new

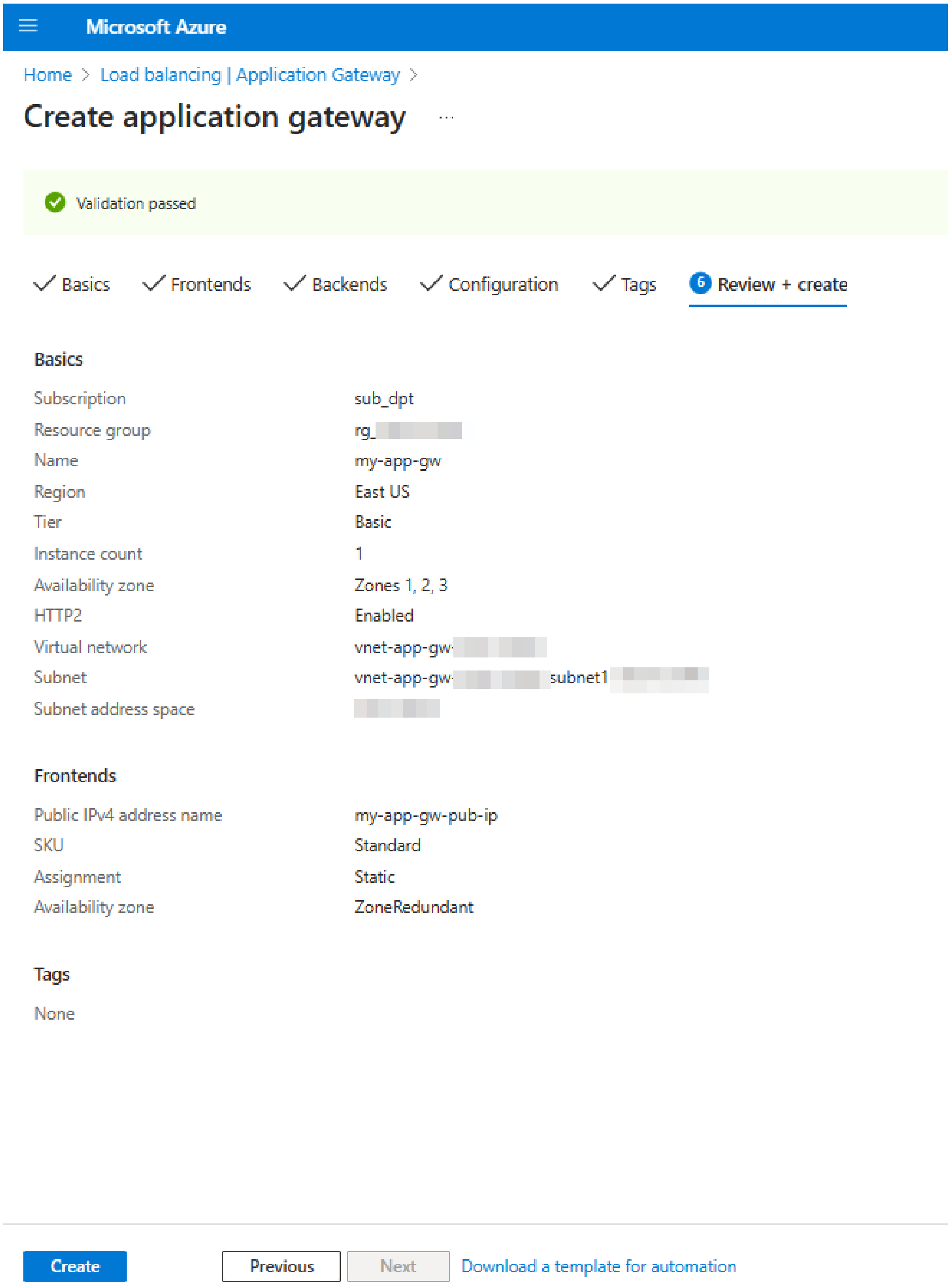
Path-based routing

You can route traffic from this rule's listener to different backend targets based on the URL path of the request. You can also apply a different set of Backend settings based on the URL path.

Path based rules

Path	Target name	Backend setting name	Backend pool
No additional targets to display			

Review the settings and click on the create button.



Home > Load balancing | Application Gateway >

Create application gateway

Validation passed

✓ Basics ✓ Frontends ✓ Backends ✓ Configuration ✓ Tags 6 Review + create

Basics

Subscription	sub_dpt
Resource group	rg_[redacted]
Name	my-app-gw
Region	East US
Tier	Basic
Instance count	1
Availability zone	Zones 1, 2, 3
HTTP2	Enabled
Virtual network	vnet-app-gw-[redacted]
Subnet	vnet-app-gw-[redacted] subnet1 [redacted]
Subnet address space	[redacted]

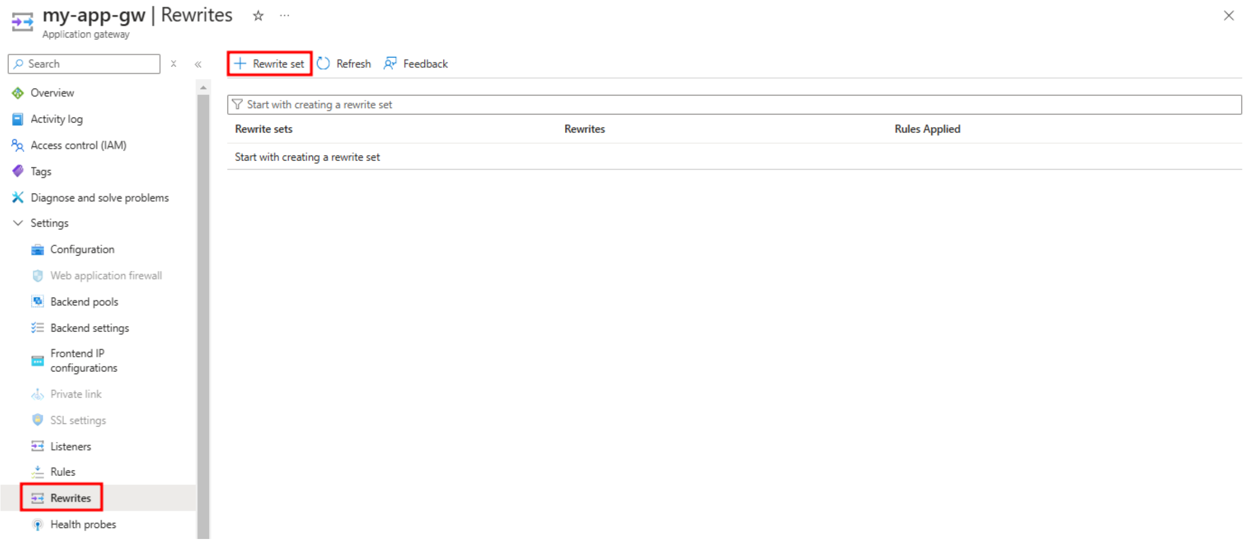
Frontends

Public IPv4 address name	my-app-gw-pub-ip
SKU	Standard
Assignment	Static
Availability zone	ZoneRedundant

Tags

None

Wait for your Application Gateway to be deployed, then create a new Rewrite set.

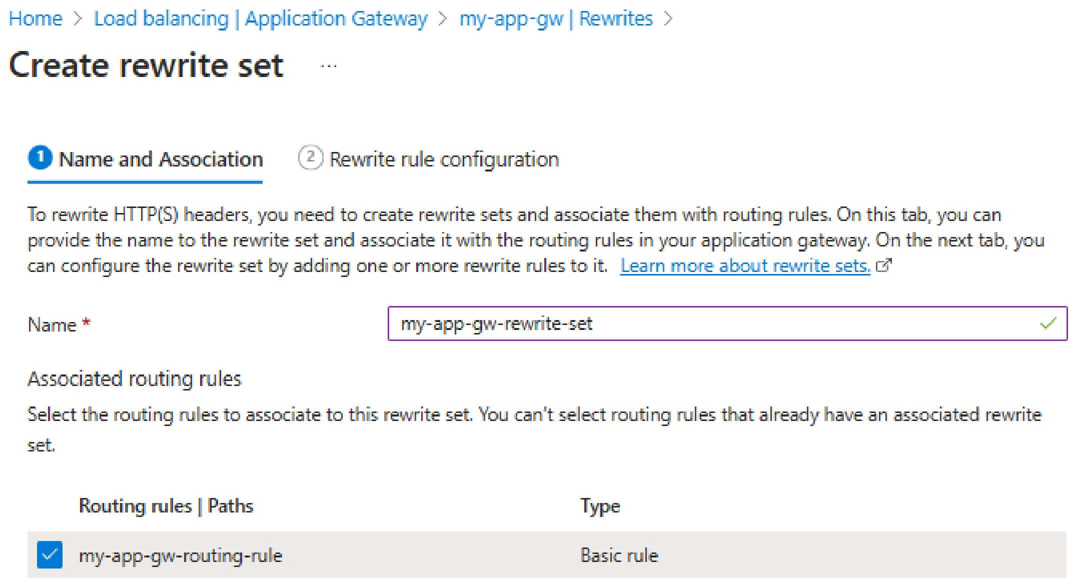


my-app-gw | Rewrites

Application gateway

Start with creating a rewrite set

Rewrite sets	Rewrites	Rules Applied
Start with creating a rewrite set		



Home > Load balancing | Application Gateway > my-app-gw | Rewrites >

Create rewrite set ...

1 Name and Association
2 Rewrite rule configuration

To rewrite HTTP(S) headers, you need to create rewrite sets and associate them with routing rules. On this tab, you can provide the name to the rewrite set and associate it with the routing rules in your application gateway. On the next tab, you can configure the rewrite set by adding one or more rewrite rules to it. Learn more about rewrite sets.

Name * my-app-gw-rewrite-set

Associated routing rules

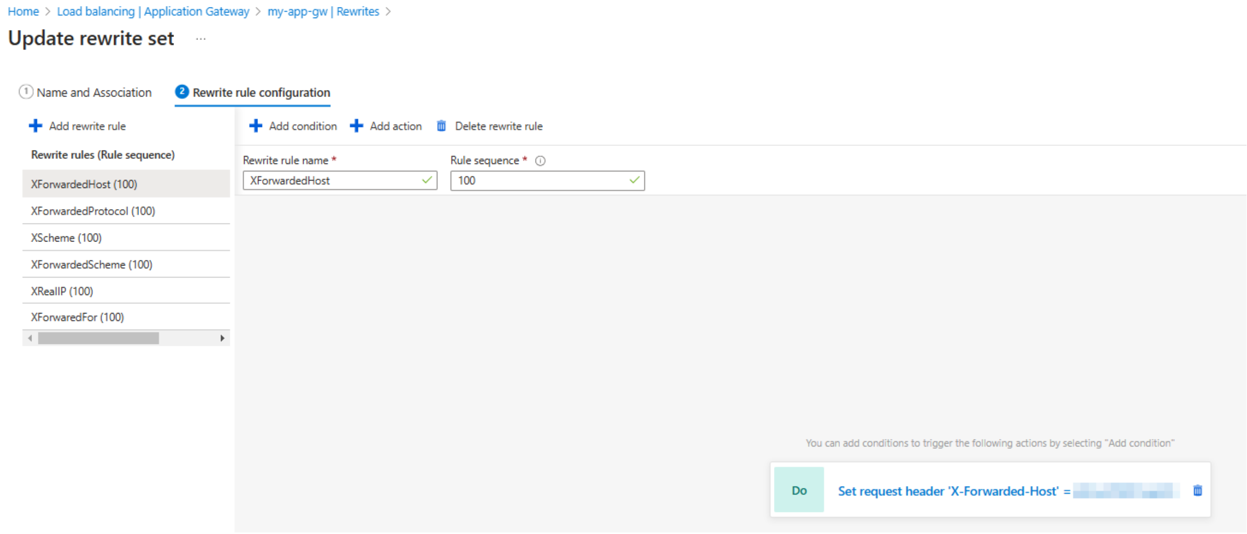
Select the routing rules to associate to this rewrite set. You can't select routing rules that already have an associated rewrite set.

	Routing rules | Paths	Type
☑	my-app-gw-routing-rule	Basic rule

Create the following rewrite rules. For the “XForwardedHost” rule, make sure to specify the FQDN you plan to use for the Application Gateway (e.g. subdomain.domain.tld).

Rewrite rule name	Rule sequence	Rewrite type	Action type	Header name	Common header	Header value
XForwardedHost	100	Request Header	Set	Common header	X-Forwarded-Host	<your public Application Gateway FQDN>
XForwardedProtocol	100	Request Header	Set	Common header	X-Forwarded-Proto	https
XScheme	100	Request Header	Set	Custom header	X-Scheme	https
XForwardedScheme	100	Request Header	Set	Custom header	X-Forwarded-Scheme	https
XRealIP	100	Request Header	Delete	Custom header	X-Real-IP	
XForwaredFor	100	Request Header	Delete	Custom header	X-Forwarded-For	

Finally, you should get a result as below.



Rewrite rules (Rule sequence)

- XForwardedHost (100)
- XForwardedProtocol (100)
- XScheme (100)
- XForwardedScheme (100)
- XRealIP (100)
- XForwaredFor (100)

Rewrite rule name *: XForwardedHost

Rule sequence *: 100

You can add conditions to trigger the following actions by selecting "Add condition"

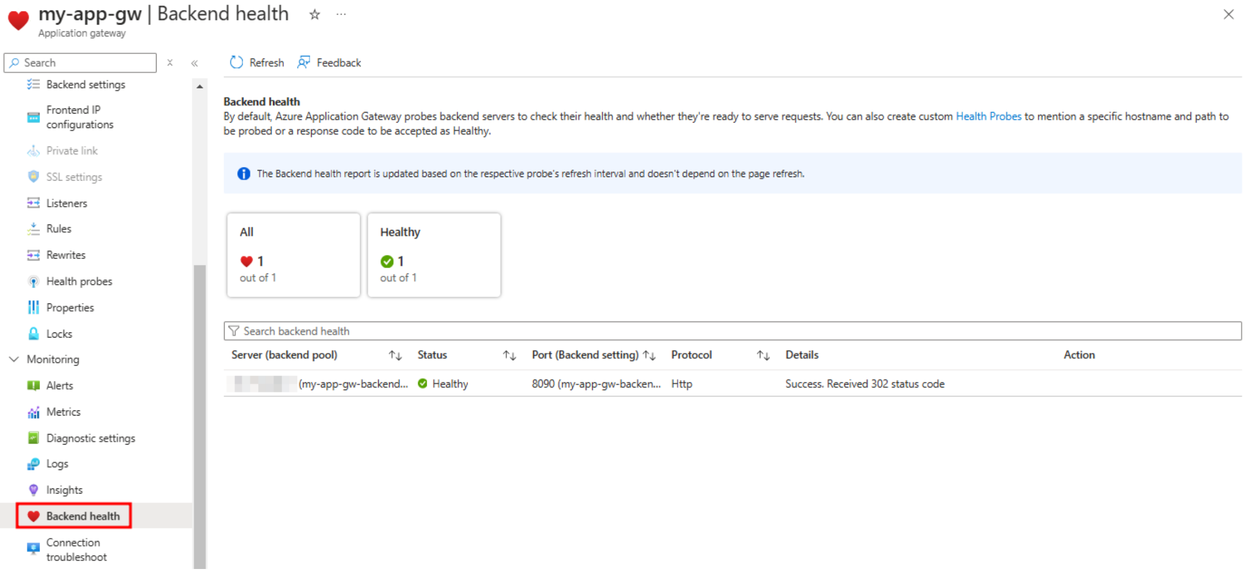
Do Set request header 'X-Forwarded-Host' = [redacted]

Create the Application Gateway DNS record

Make sure that the FQDN you plan to use for the Imaging deployment points to the Application Gateway public IP.

Resolve issues

If you encounter issues when connecting through the Application Gateway, carefully review all the procedure steps. Also confirm that the Application Gateway backend is healthy. It should return a 302 as below.



Backend health

By default, Azure Application Gateway probes backend servers to check their health and whether they're ready to serve requests. You can also create custom Health Probes to mention a specific hostname and path to be probed or a response code to be accepted as Healthy.

The Backend health report is updated based on the respective probe's refresh interval and doesn't depend on the page refresh.

Server (backend pool)	Status	Port (Backend setting)	Protocol	Details	Action
[redacted] (my-app-gw-backend...	Healthy	8090 (my-app-gw-backen...	Http	Success. Received 302 status code	