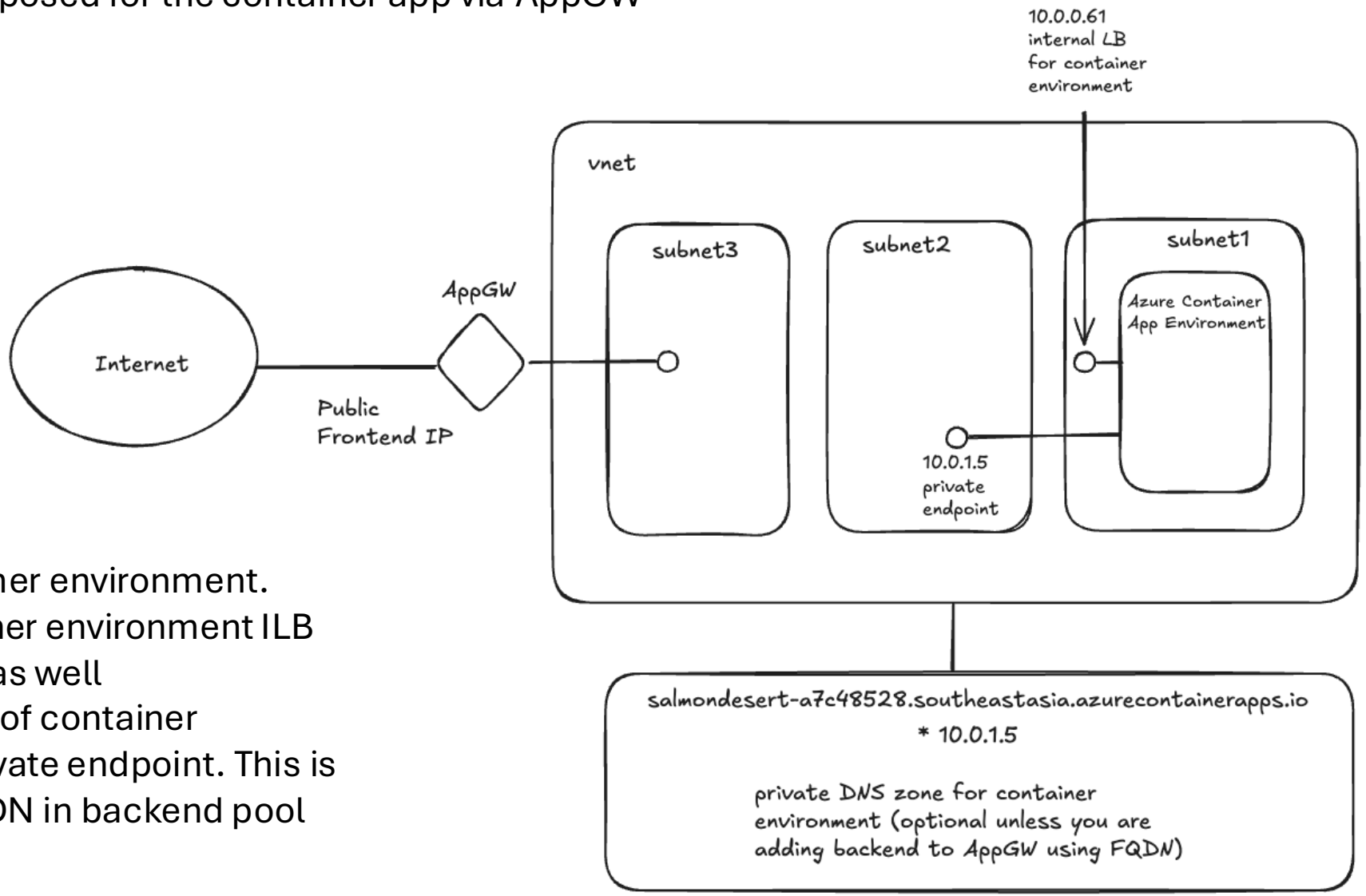
Azure Container Environment in virtual network, fronted by AppGW

In this example only HTTP is exposed for the container app via AppGW



Optional:

- Private endpoint for Container environment. AppGW can use the container environment ILB IP of 10.0.0.61 as backend as well
- Private DNS zone for FQDN of container environment pointing to private endpoint. This is only required if you use FQDN in backend pool instead of IP.

Backend set to ILB or defaultIP of the container environment and it works

Home > Load balancing and content delivery | Application gateways > testappgw2 | Backend pools >

Backend health

Refresh Feedback

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.

All	Healthy
1 out of 1	1 out of 1

Search backend health

Server (backend pool)	Status	Port (Backend setting)	Protocol	Details	Action
10.0.0.61 (backendpool1)	Healthy	80 (http-settings)	Http	Success. Received 200 status code	

jzwong — -zsh — 129×28

```
< etag: "689ca245-267"
< accept-ranges: bytes
<
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
* Connection #0 to host 57.158.134.5 left intact
jzwong ~  $
```

Backend set to private endpoint of the container environment and it works

Home > Load balancing and content delivery | Application gateways > testappgw2 | Backend pools >

Backend health

Refresh Feedback

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.

All	Healthy
1 out of 1	1 out of 1

Search backend health

Server (backend pool)	Status	Port (Backend setting)	Protocol	Details	Action
10.0.1.5 (backendpool1)	Healthy	80 (http-settings)	Http	Success. Received 200 status code	

jzwong — -zsh — 129×28

```
< etag: "689ca245-267"
< accept-ranges: bytes
<
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
* Connection #0 to host 57.158.134.5 left intact
jzwong ~ $
```

HTTP backend settings on the AppGW, must override with FQDN of container app

Add Backend setting

http-settings

Backend protocol

HTTP HTTPS

Backend port *

80

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

If the backend service is a multi-tenant Azure service such as App Services, Functions, or Portal Apps, we recommend using Custom domain method, instead of overriding the hostname. Using override host name with default domains (azurewebsites.net, azuremicroservices.io, etc.) is good only for the basic tests and operations.

Host name override

Pick host name from backend target

Override with specific domain name

Host name *

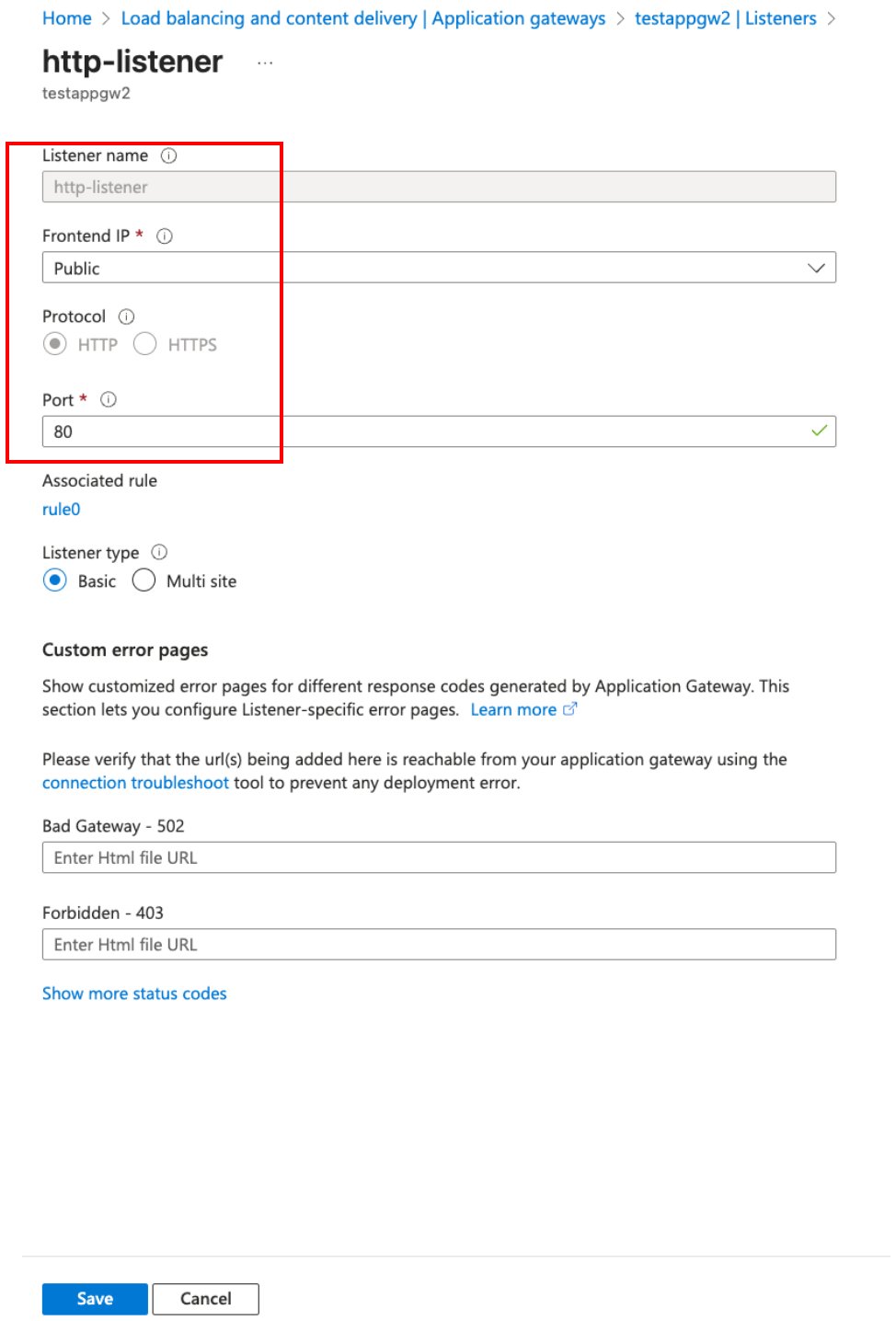
nginx.salmondesert-a7c48528.southeastasia.azurecontainerapps.io

Use custom probe

Yes No

Save Cancel

HTTP listener on port 80 on AppGW



Rule listener configuration

rule0

testappgw2

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: rule0

Priority * : 200

*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 * : http-listener

Save Cancel

Rule backend configuration

rule0

testappgw2

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: rule0

Priority *: 200

* Listener * **Backend targets**

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 *: backendpool1

Backend settings *: http-settings

Save Cancel

Azure Container Environment showing virtual network integration and its defaultIP or ILB of 10.0.0.61

Home > Container Apps Environments >

testacaenv
Container Apps Environment

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Dapr components
  - Certificates
  - Workload profiles
  - Networking
  - Azure Files
  - Identity
  - Planned Maintenance
  - Locks
- Apps
  - Apps
- Services
- Monitoring
- Automation
- Help

Refresh Delete

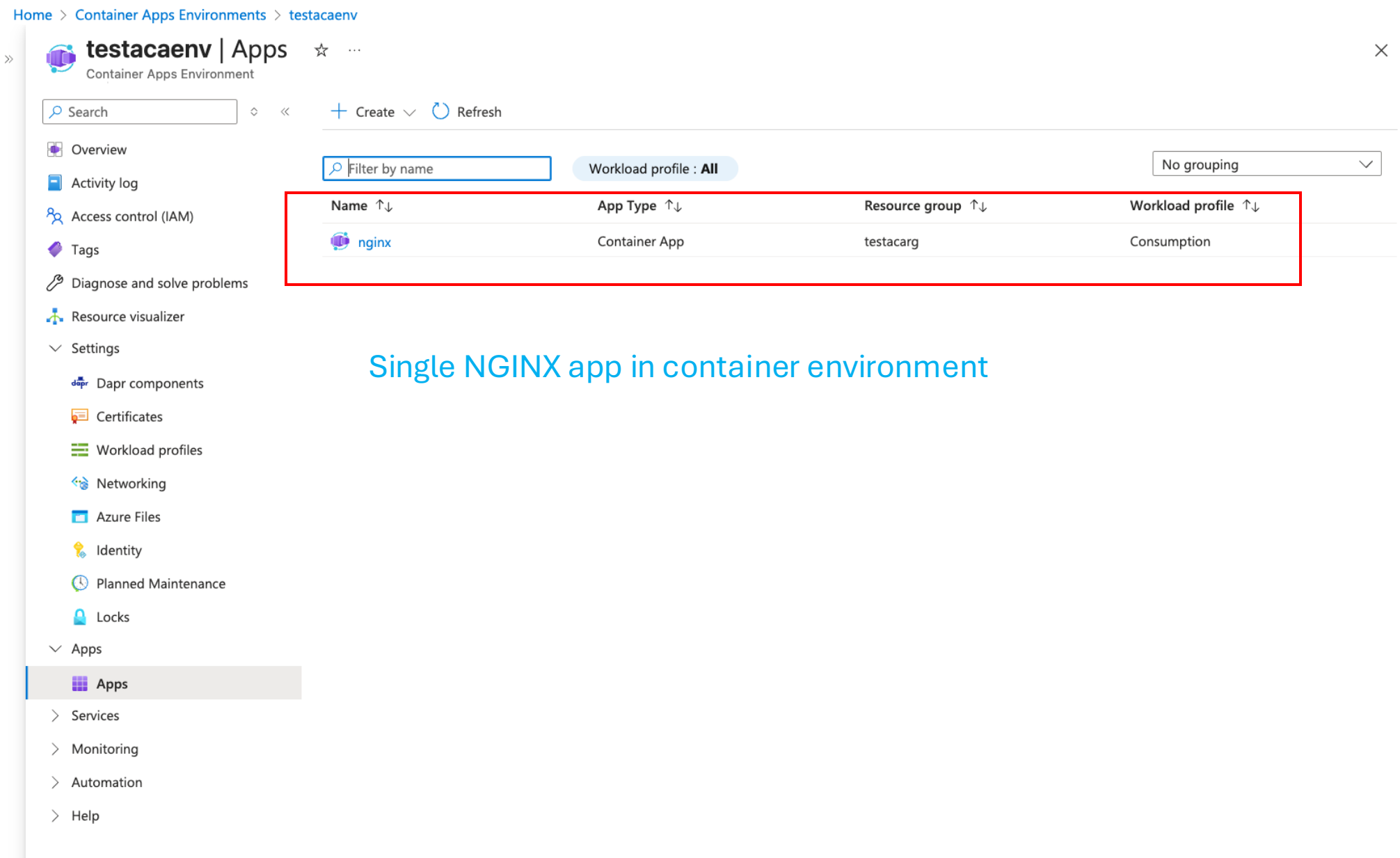
Essentials

Resource group (...	: testacarg
Status	: Succeeded
Location (move)	: Southeast Asia
Subscription (move)	: ME-MngEnvMCAP627202-chianwong-1
Subscription ID	: 68be2809-9674-447c-a43d-261ef2862c29
.NET Aspire Dashbo...	: Not yet active (set up)
Environment type	: Workload profiles
Virtual network	: testacavnet
Infrastructure subnet	: subnet1
Static IP	: 10.0.0.61
Applications	: 1
KEDA version	: 2.16.1
Dapr version	: 1.13.6-msft.6

Tags (edit) : Add tags

Applications Get started Monitoring Tutorials

Name	App Type	Resource Group
nginx	Container App	testacarg



Single NGINX app in container environment

Home > Container Apps Environments > testacaenv

testacaenv | Networking

Container Apps Environment

Search

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Dapr components
  - Certificates
  - Workload profiles
  - Networking
  - Azure Files
  - Identity
  - Planned Maintenance
  - Locks
- Apps
  - Apps
- Services
- Monitoring
- Automation
- Help

General | Ingress settings | Encryption | Custom DNS Suffix

View and manage network access to your Azure Container Apps environment.

Public Network Access

Public Network Access *

Enable: Allows incoming traffic from the public internet.

Disable: Block all incoming traffic from the public internet.

These settings are currently disabled since your app environment is internal

Virtual network

These options can't be modified post create.

Virtual network	testacavnet
Subnet	subnet1
Virtual IP	Internal (The endpoint is an internal load balancer)
Infrastructure resource group	testacarg

Private Endpoints

Private endpoints enable secure inbound access from the chosen virtual network. When configured, your app cannot be configured to allow public network access. Get more info

Private Endpoints	1 Private Endpoint

Public network access disabled, integrated with virtual network with private endpoint

Home > Container Apps Environments > testacaenv

testacaenv | Networking

Container Apps Environment

Search

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Dapr components
  - Certificates
  - Workload profiles
  - Networking
  - Azure Files
  - Identity
  - Planned Maintenance
  - Locks
- Apps
  - Apps
- Services
- Monitoring
- Automation
- Help

General | **Ingress settings** | Encryption | Custom DNS Suffix

Select an ingress mode based on your app needs. Check metrics

Ingress mode *

- (●) Default
  Automatic scaling based on demand
- ( ) Premium (preview)
  Recommended for high-demand workloads

Default ingress settings on container environment

Home > Container Apps Environments > testacaenv

testacaenv | Networking

Container Apps Environment

Search

Refresh

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Dapr components
  - Certificates
  - Workload profiles
  - Networking
  - Azure Files
  - Identity
  - Planned Maintenance
  - Locks
- Apps
  - Apps
- Services
- Monitoring
- Automation
- Help

General | Ingress settings | Encryption | **Custom DNS Suffix**

Customize the DNS suffix to your domain name below. If you want to customize the domain name itself, navigate to App. Learn more

DNS suffix * Enter DNS suffix

Domain validation

To validate your domain ownership, copy the hostname records below and enter them with your domain provider.

Type	Host	Value
A	*.<DNS suffix>	10.0.0.61

Wildcard certificate

Upload a wildcard TLS certificate for your domain.

Source * Select the source of certificate

Default DNS suffix settings on container environment

Home > Container Apps Environments > testacaenv | Networking > Private Endpoint connections > testacapep

testacapep | DNS configuration

Private endpoint

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Application security groups
  - DNS configuration
  - Properties
  - Locks
- Monitoring
- Automation
- Help

Add configuration Refresh

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint using a private DNS zone. You can also utilize your own DNS servers. Learn more

Customer Visible FQDNs

DNS records visible to the customer

Network Interface	IP addresses	FQDN
testacapep-nic		
	10.0.1.5	
		*.salmondesert-a7c48528.southeastasia.azurecontainerapps.io

Configuration name	FQDN	IP address	Subscription	Private DNS zone	DNS zone group
privatelink-south...			ME-MngEnvMCAP627202-c...	privatelink.southeastasi...	default
	salmondesert-a7c48528.priv...			-	-
		10.0.1.5		-	-

Container App environment private endpoint IP

Home > Container Apps Environments > testacaenv | Apps > nginx

nginx | Ingress

Container App

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Application
  - Revisions and replicas
  - Containers
  - Scale
  - Volumes
- Settings
- Networking
  - Ingress
  - Custom domains
  - CORS
- Security
- Monitoring
- Automation
- Help

Refresh Send us your feedback

When you enable Ingress, all traffic will be directed to your latest revision by default. To change traffic settings, go to the revision management page

Enable ingress for applications that need an HTTP or TCP endpoint.

Ingress	[x] Enabled
Ingress traffic	( ) Limited to Container Apps Environment Select this option if you want to restrict traffic to this container app from within the Container App Environment (•) Limited to VNet Select this option if you want to restrict traffic to this container app from within the Virtual Network
Ingress type	(•) HTTP ( ) TCP
Client certificate mode	(•) Ignore ( ) Accept ( ) Require
Transport	Auto
Insecure connections	[x] Allowed
Target port	80
Endpoint(s)	https://nginx.salmondesert-a7c48528.southeastasia.azurecontainerapps.io
Session affinity	[ ] Enabled

Additional TCP ports

IP Restrictions

Access restrictions allow you to define lists of allow/deny rules to control traffic to your app. If there are no rules defined then your app will accept traffic from any address.

IP Security Restrictions Mode	(•) Allow all traffic (default) ( ) Allow traffic from IPs configured below, deny all other traffic ( ) Deny traffic from IPs configured below, allow all other traffic

Ingress settings for container app – allow insecure connections, limited to vnet, target port 80

Home > Private DNS zones > salmondesert-a7c48528.southeastasia.azurecontainerapps.io

salmondesert-a7c48528.southeastasia.azurecontainerapps.io | Recordsets

Private DNS zone

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
- DNS Management
  - Recordsets
  - Virtual Network Links
- Monitoring
- Automation
- Help

Add | Refresh | Delete | Give feedback

A record set is a collection of records in a zone that have the same name and are the same type. Record Sets will be automatically fetched in batches of 100 as you scroll through the existing record sets. Learn more

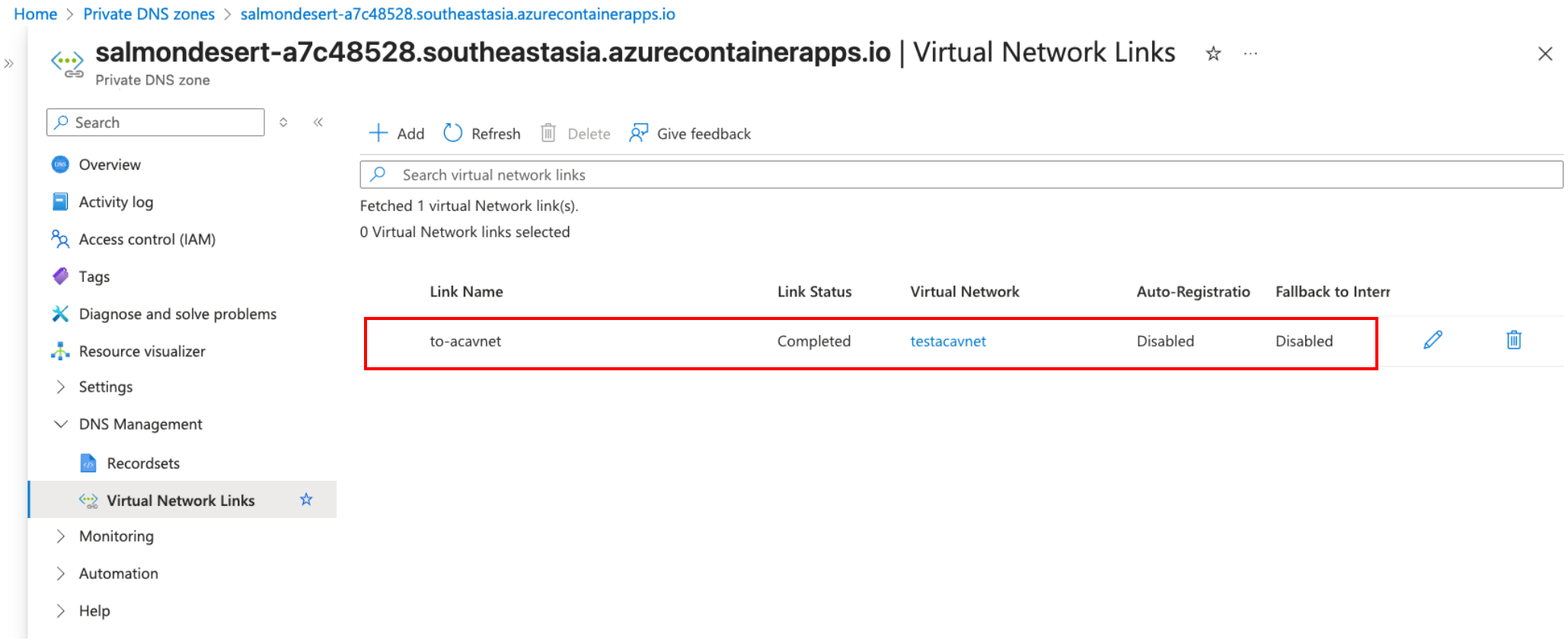
Search

Fetched 3 record set(s).

0 record sets selected

Name	Type	TTL	Value	Auto registered
*	A	3600	10.0.1.5	False
@	SOA	3600	Email: azureprivatedns-host.microsoft.com Host: azureprivatedns.net Refresh: 3600 Retry: 300 Expire: 2419200 Minimum TTL: 10 Serial number: 1	False
@	A	3600	10.0.1.5	False

The private DNS zone is optional – only required if you use FQDN in AppGW backend settings



Virtual link from private DNS zone to the vnet

Home > Network foundation | Virtual networks > testacavnet

testacavnet | Subnets

Virtual network

Subnet | Refresh | Manage users | Delete

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.

Search subnets

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
subnet1	10.0.0.0/24	-	250	Microsoft.App/environments	testacavnet...	-
subnet3	10.0.2.0/24	-	availability ...	Microsoft.Network/applicationG...	testacavnet...	-
subnet2	10.0.1.0/24	-	249	-	testacavnet...	-

Subnet 1 – container app environment
Subnet 2 – private endpoint of container app environment
Subnet 3 – application gateway

Home > Network foundation | Virtual networks > testacavnet | Subnets > testacavnet-subnet3-nsg-southeastasia

testacavnet-subnet3-nsg-southeastasia | Inbound security rules

Network security group

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Inbound security rules
  - Outbound security rules
  - Network interfaces
  - Subnets
  - Properties
  - Locks
- Monitoring
- Automation
- Help

Add | Hide default rules | Refresh | Delete | Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Filter by name | Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
1000	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
1010	AllowAnyHTTPSInbou···	443	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Inbound NSG rules required for TCP 80 and 443 for application gateway subnet

NSG for AppGW subnet needs to allow TCP 443 and 80

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | admin@MngEnvMCAP6... KITKAT (MNGENVMCAP627202....

Home > Network foundation | Virtual networks > testacavnet | Subnets > testacavnet-subnet1-nsg-southeastasia

testacavnet-subnet1-nsg-southeastasia | Inbound security rules

Network security group

Search

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Resource visualizer
- Settings
  - Inbound security rules
  - Outbound security rules
  - Network interfaces
  - Subnets
  - Properties
  - Locks

Add | Hide default rules | Refresh | Delete | Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more

Filter by name | Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Default inbound NSG rules on subnet for Azure Container App Environment

jzwong — -zsh — 129×28

```
< etag: "689ca245-267"
< accept-ranges: bytes
<
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
* Connection #0 to host 57.158.134.5 left intact
jzwong ~ $
```

NSG for container environment subnet is default

Home > Network foundation | Virtual networks > testacavnet | Subnets >

testacavnet-subnet2-nsg-southeastasia

Network security group

Diagnose connectivity issues related to this security group +2

Move | Delete | Refresh | Give feedback

Essentials

JSON View

Resource group (move) : testacarg

Location : Southeast Asia

Subscription (move) : ME-MngEnvMCAP627202-chianwong-1

Subscription ID : 68be2809-9674-447c-a43d-261ef2862c29

Tags (edit) : Add tags

Custom security rules : 0 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

Default NSG inbound rules for subnet of private endpoint for container environment

Filter by name | Port == all | Protocol == all | Source == all | Destination == all | Action == all

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInB...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

jzwong — -zsh — 129×23

```
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
* Connection #0 to host 57.158.134.5 left intact
jzwong ~ $
```

NSG for private endpoint subnet is default

Access to public IP of AppGW via HTTP