FortiOS - Deploying Auto Scaling on Azure

Version 6.0 and 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET COOKBOOK
http://cookbook.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdocs@fortinet.com

September 25, 2019
FortiOS 6.0 and 6.2 Deploying Auto Scaling on Azure
01-600-000000-20190925

TABLE OF CONTENTS

Deploying autoscaling on Azure

You can deploy FortiGate virtual machines to support Azure Autoscale. This requires a manual deployment incorporating one ore more Virtual Machine Scale Sets (VMSS) and network related components, as well as Azure Function App scripts. Fortinet provides a FortiGate Autoscale for Azure deployment package to facilitate the deployment.

Multiple FortiGate-VM instances form a VMSS to provide highly efficient clustering at times of high workloads. FortiGate-VM instances are scaled out automatically according to predefined workload levels. Autoscaling is achieved by using FortiGate-native high availability (HA) features such as `config-sync`, which synchronizes operating system (OS) configurations across multiple FortiGate-VM instances at the time of scale-out events.

FortiGate Autoscale for Azure is available with FortiOS 6.0.6 and later versions as well as with FortiOS 6.2.1 and later versions and supports On-Demand (PAYG) instances.

Acronyms

The following acronyms are used throughout this document.

Acronym	Expansion
ASG	Autoscaling Group
BYOL	Bring Your Own License
CIDR	Classless Inter-Domain Routing
ELB	Elastic Load Balancer
FGT	FortiGate
PAYG	Pay As You Go
VMSS	Virtual Machine Scale Set
VM	Virtual Machine

Planning

Deploying FortiGate Autoscale for Azure requires the use of deployment templates. Following are descriptions of the templates included in the version 1.0.x deployment package for deploying with PAYG instances only.

Template	Description
`deploy_funcapp.json`	Template to deploy the Function App.
`deploy_funcapp.params.json`	Editable parameter template paired with `deploy_funcapp.json`.
`deploy_scaleset.json`	Template to deploy the Scale Set.
`deploy_scaleset.params.json`	Editable parameter template paired with `deploy_scaleset.json`.

Prerequisites

Installing and configuring FortiGate Autoscale for Azure requires knowledge of the following:

- Configuring a FortiGate using the CLI
- Azure deployment templates
- Azure Functions

It is expected that FortiGate Autoscale for Azure will be deployed by DevOps engineers or advanced system administrators who are familiar with the above.

Before starting the deployment, the following steps must be carried out:

1. Log into your Azure account. If you do not already have one, create one by following the on-screen instructions.
2. Create a service principal, making note of the following items as they will be needed to deploy the Function App:
   - *Tenant ID* (used for the parameter *"Tenant ID" on page 11*). This is under Azure *Active Directory > Properties > Directory ID*.
   - *Application ID* (used for the parameter *"Rest App ID" on page 12*). This is under Azure *Active Directory > App registrations > {your-app}*.
   - *Application secret* (used for the parameter *"Rest App Secret" on page 12*). The application secret only appears once and cannot be retrieved.

Obtaining the deployment package

The FortiGate Autoscale for Azure deployment package is located in the Fortinet GitHub project.

To obtain the package, do one of the following:

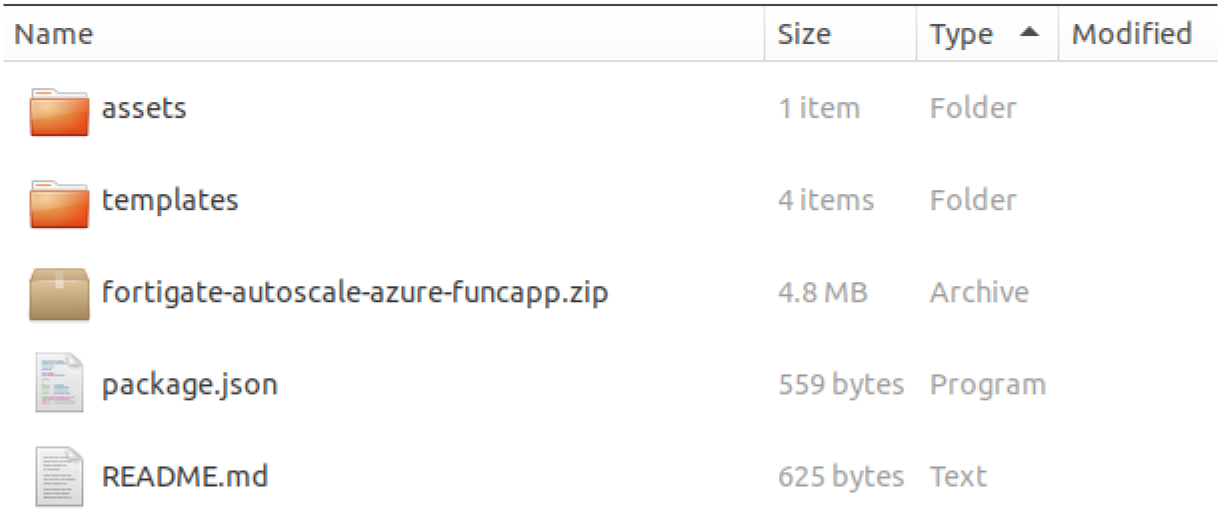
- Visit the FortiGate Autoscale GitHub project release page and download the `fortigate-autoscale-azure-template-deployment.zip` for the version you want to use.

  This documentation is for the *Version 2.0.x* release which supports any combination of BYOL and PAYG instances.

  Documentation for *Version 1.0.x* (which only supports PAYG instances) is no longer maintained and is only available as a PDF in the 1.0.x GitHub repository.

- Download the entire source code for the version you are using, then run the `npm run build-azure-azure-template-deployment` command on the project root directory to generate the `fortigate-autoscale-azure-template-deployment.zip` file. The generated file will be available in the *dist* directory.

Unzip the `fortigate-autoscale-azure-template-deployment.zip` file on your local PC. The following files and folders will be extracted to the *fortigate-autoscale-azure-template-deployment* folder:



Name	Size	Type ▲	Modified
assets	1 item	Folder	
templates	4 items	Folder	
fortigate-autoscale-azure-funcapp.zip	4.8 MB	Archive	
package.json	559 bytes	Program	
README.md	625 bytes	Text	

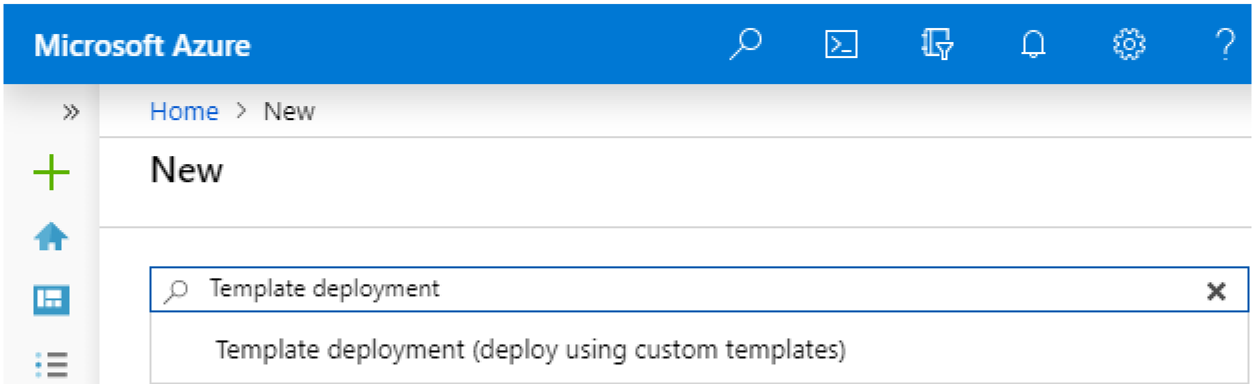
Extracted content is described below:

Extracted Item	Description
assets	This folder contains the *configset* files.
templates	This folder contains the files described in the section "Planning" on the previous page.
fortigate-autoscale-azure-funcapp.zip	This is the function source file. This file should be uploaded to a file host online so that it is accessible to Azure. During the deployment you will specify the URL to this file in the parameter *"Package Res URL" on page 13*.

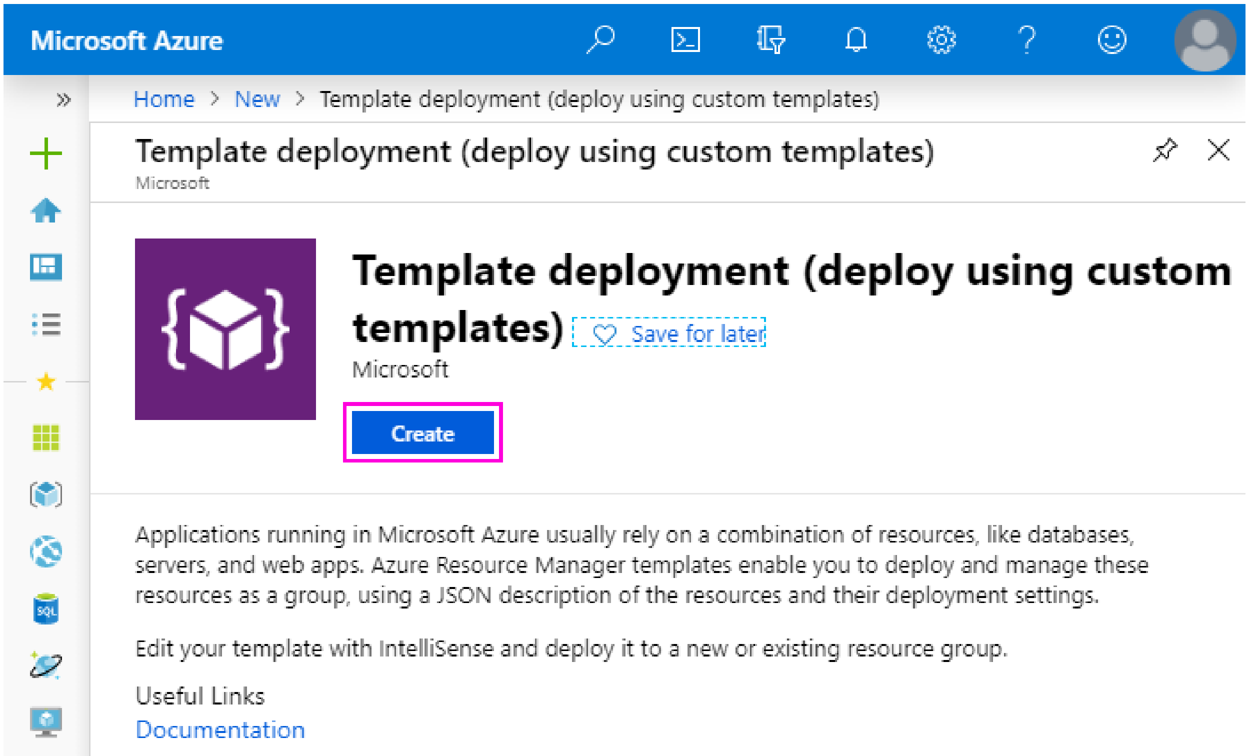
Creating a template deployment

To create a template deployment:

1. In the Azure portal, select *Create a resource* and search for "Template deployment".



2. Click *Create*.


Microsoft Azure
Home > New > Template deployment (deploy using custom templates)
Template deployment (deploy using custom templates)
Microsoft
Save for later
Create
Useful Links
Documentation

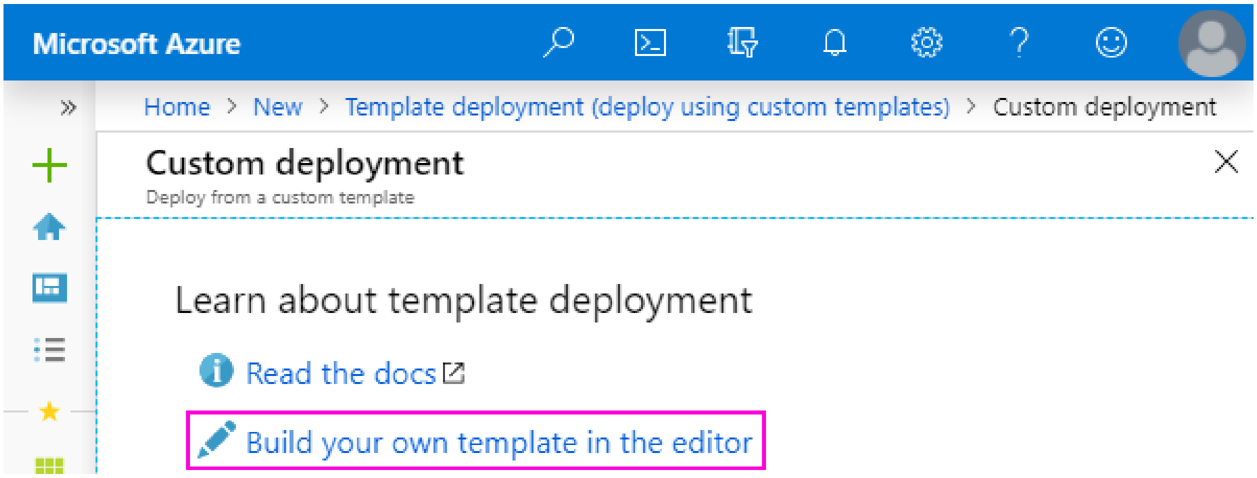
Template deployment (deploy using custom templates)

Microsoft

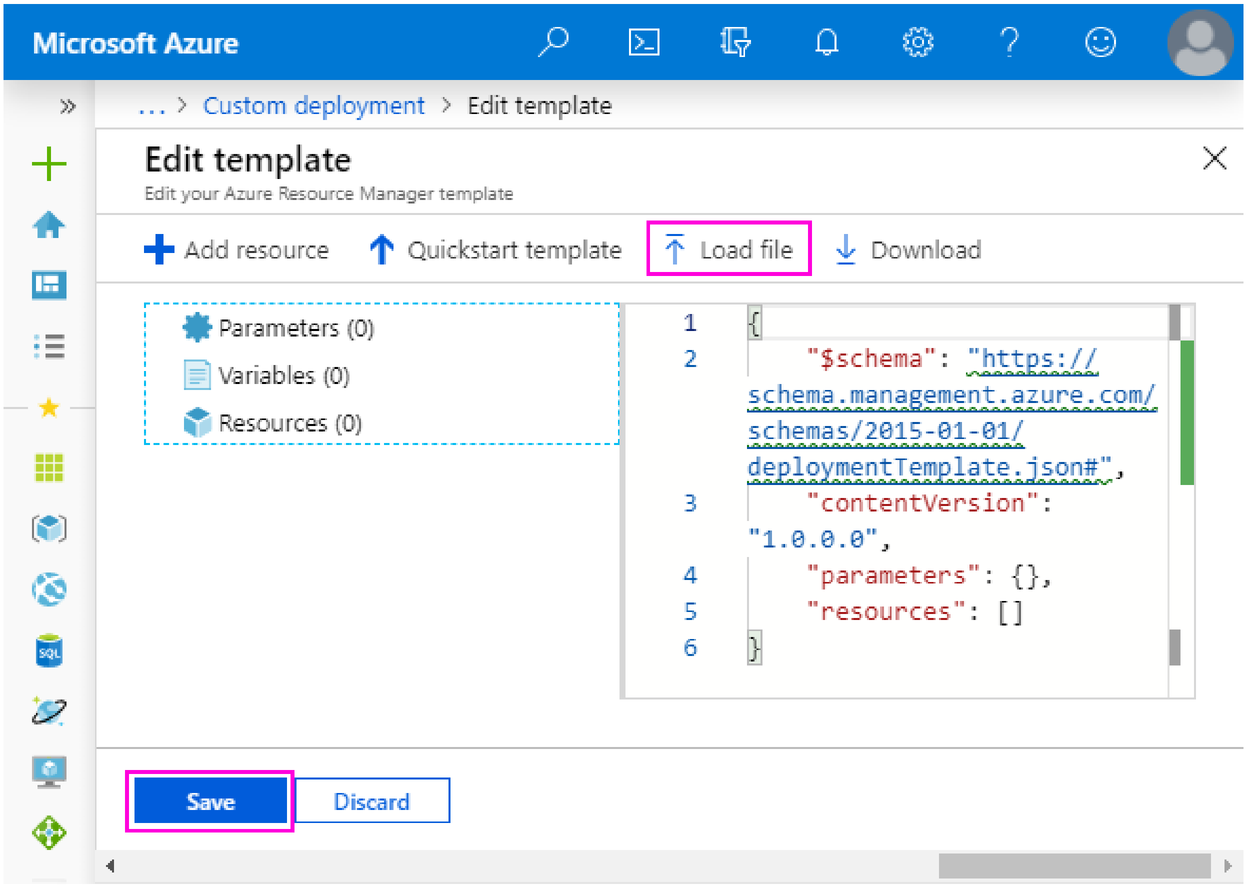
Applications running in Microsoft Azure usually rely on a combination of resources, like databases, servers, and web apps. Azure Resource Manager templates enable you to deploy and manage these resources as a group, using a JSON description of the resources and their deployment settings.

Edit your template with IntelliSense and deploy it to a new or existing resource group.

3. Click *Build your own template in the editor*.

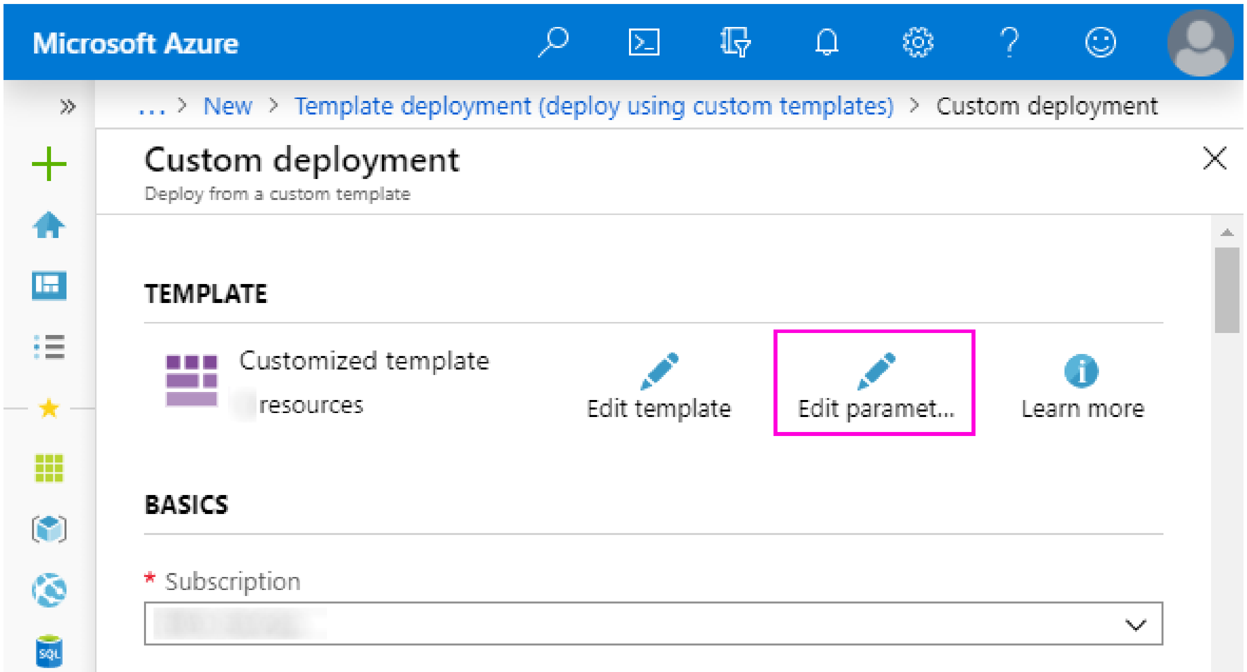

Microsoft Azure
Home > New > Template deployment (deploy using custom templates) > Custom deployment
Custom deployment
Deploy from a custom template
Learn about template deployment
Read the docs
Build your own template in the editor

4. Replace the template code with the provided `.json` code or click *Load file* to load the provided `.json` file. Then click *Save*.



```
{
    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {},
    "resources": []
}
```

5. (Optional) In the *Custom deployment* screen, click *Edit parameters* to load a predefined `.params.json` file.


Microsoft Azure
... > New > Template deployment (deploy using custom templates) > Custom deployment

Custom deployment

Deploy from a custom template

TEMPLATE

Customized template

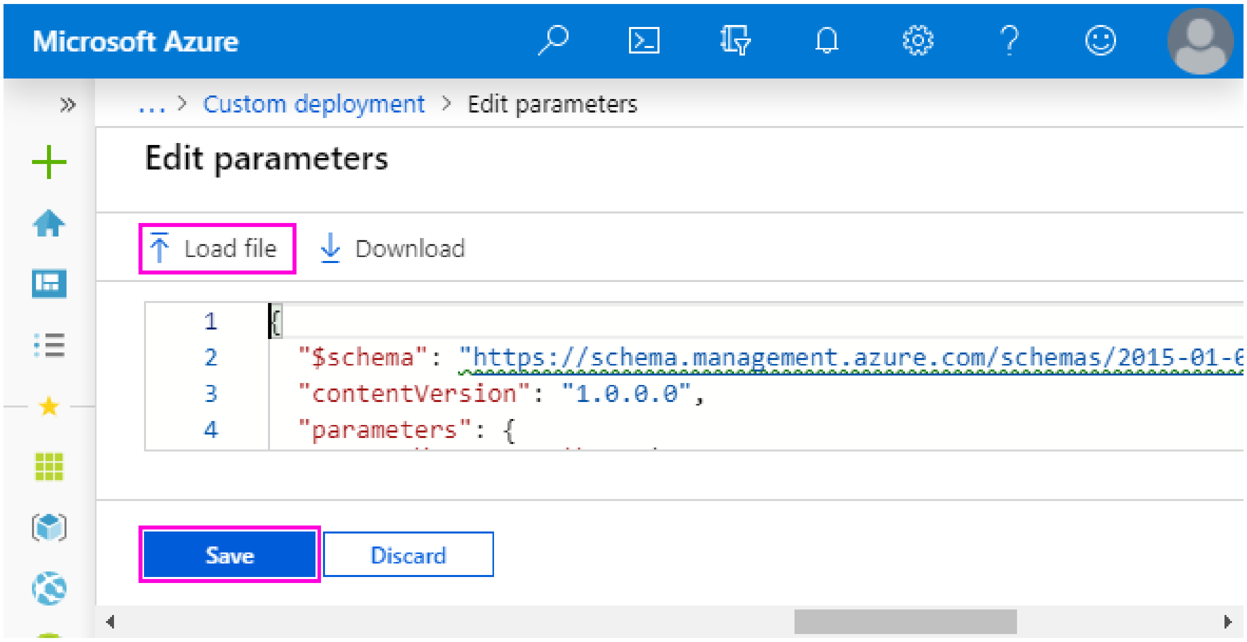
resources

Edit template
Edit paramet...
Learn more

BASICS

* Subscription

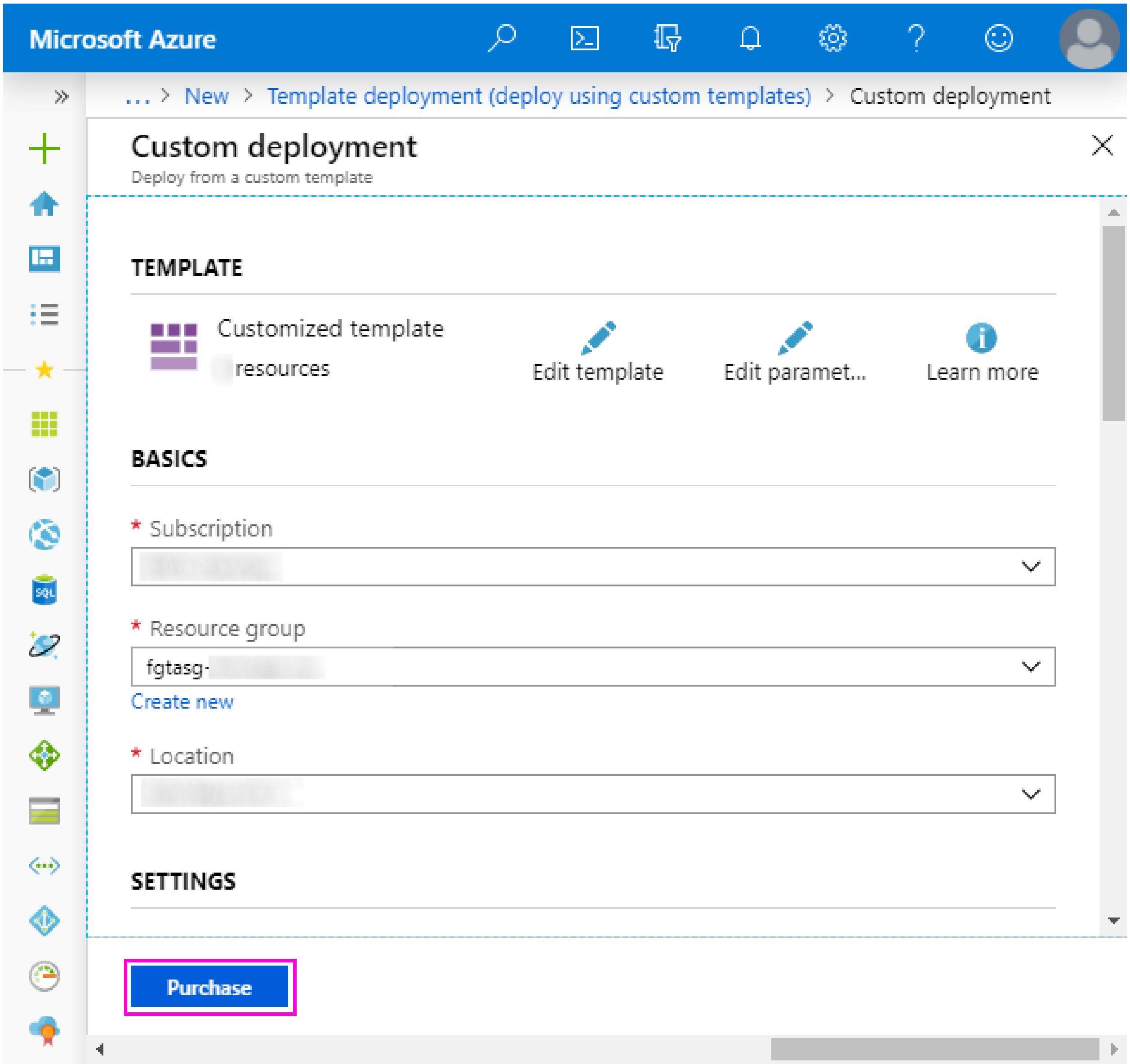
Replace the parameter code with the provided `.params.json` code or click *Load file* to load the provided `.params.json` file. Then click *Save*



Edit parameters

```
{
  "$schema": "https://schema.management.azure.com/schemas/2015-01-0
  "contentVersion": "1.0.0.0",
  "parameters": {
```

6. Review and update parameters.


Microsoft Azure
... > New > Template deployment (deploy using custom templates) > Custom deployment
Edit template
Edit paramet...
Learn more
Create new
Purchase

Custom deployment

Deploy from a custom template

TEMPLATE

Customized template
[redacted] resources

BASICS

* Subscription
[redacted]

* Resource group
fgtasg-[redacted]

* Location
[redacted]

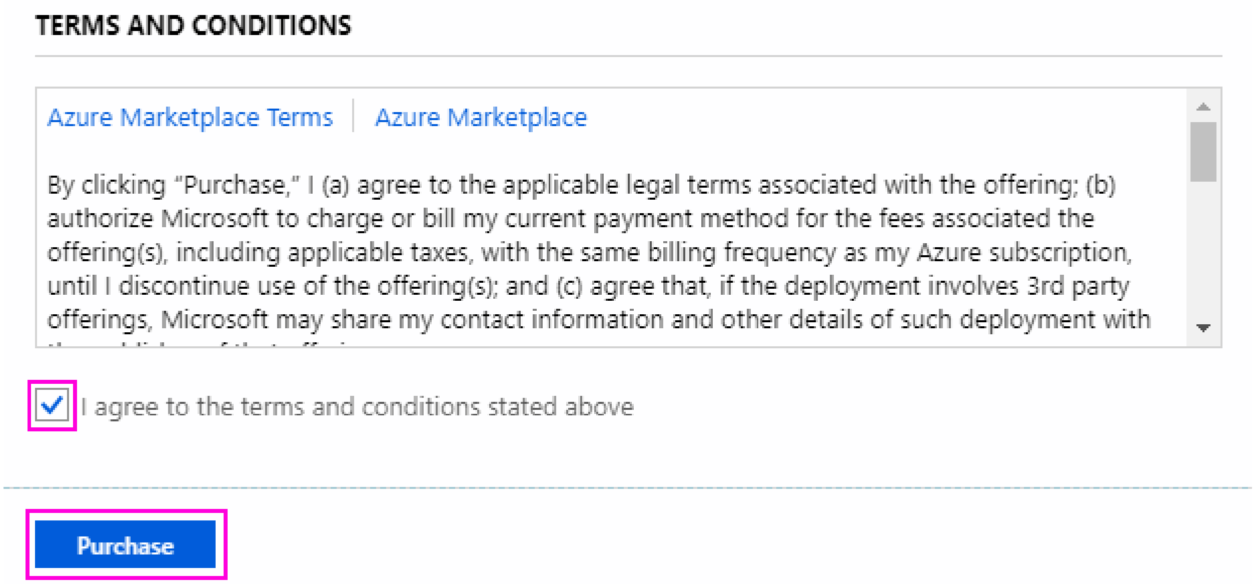
SETTINGS

All custom deployments have these BASIC parameters:

- *Subscription*: The Azure subscription FortiGate Autoscale for Azure will be deployed in.
- *Resource group*: The resource group you are deploying to.
- *Location*: The region the resources will be deployed in.

SETTINGS parameters are specific to the custom template being deployed. The parameters displayed in this section are described in the section "Configurable variables" on the next page.

7. When all parameters have been provided and the terms and conditions have been agreed to, click *Purchase*.



TERMS AND CONDITIONS

Azure Marketplace Terms | Azure Marketplace

By clicking "Purchase," I (a) agree to the applicable legal terms associated with the offering; (b) authorize Microsoft to charge or bill my current payment method for the fees associated the offering(s), including applicable taxes, with the same billing frequency as my Azure subscription, until I discontinue use of the offering(s); and (c) agree that, if the deployment involves 3rd party offerings, Microsoft may share my contact information and other details of such deployment with

☑ I agree to the terms and conditions stated above

Configurable variables

Following is a list of variables used during deployment of the version 1.0.x deployment package and referenced throughout this guide.

Parameters required for Function App deployment

Parameter	Default	Description
Function App Name	Requires input	Name of the Function App that will be created.
Cosmos DB Name	Requires input	Name of the Cosmos DB that will be created. This field must be between 3 and 31 characters and can contain only lowercase letters, numbers and the '-' character.
Storage Account Type	Requires input	Storage account type.
Tenant ID	Requires input	The Azure Directory ID for the Active Directory (AD) of your current subscription. This is under *Azure Active Directory* > *Properties* > *Directory ID*. Make note of this when creating a service principal during the "Prerequisites" on page 5.
Subscription ID	Requires input	Your Azure Subscription ID.

Parameter	Default	Description
Rest App ID	Requires input	*Application ID* for the Registered app. This is under *Azure Active Directory* > *App registrations* > *{your-app}*. Make note of this when creating a service principal during the "Prerequisites" on page 5.
Rest App Secret	Requires input	*Authentication key* for the Registered app. Make note of this when creating a service principal during the "Prerequisites" on page 5.
Heart Beat Loss Count	Requires input	Number of consecutively lost heartbeats. When the Heart Beat Loss Count has been reached, the Virtual Machine (VM) is deemed unhealthy and failover activities will commence.
Scaling Group Resource Group Name	Requires input	Name of the resource group that the Scale Set and its components will be deployed in. In our example, this is *fgtasg-scaleset*. Each service should be deployed into its own resource group.
Scaling Group Name Prefix	fgtasg	The prefix each VMSS name is given when deploying the FortiGate Autoscale template. Must be at most 10 characters long and only contain uppercase letters, lowercase letters, and numbers. The value of this parameter should be the same as for *deploy_scaleset.json*.
Script Timeout	230	Timeout value (in seconds) for the Azure function script.
Election Wait Time	Requires input	The maximum time (in seconds) to wait for a master election to complete.
PSK Secret	Requires input	The pre-shared key used by FortiGate-VMs in the Scale Set to synchronize configuration items. This field has a maximum of 128 characters. Changes to the PSK secret after FortiGate Autoscale for Azure has been deployed are not reflected here. For new instances to be spawned with the changed PSK secret, this environment variable will need to be manually updated.

Parameter	Default	Description
Package Res URL	Requires input	The public URL of the function source file named `fortigate-autoscale-azure-funcapp.zip`, and can be found inside the `fortigate-autoscale-azure-template-deployment.zip`. This URL must be accessible by Azure.

Parameters required for Scale Set deployment

Parameter	Default	Description
Instance Type	Standard_F2	Size of the VMs in the VMSS. For assistance in choosing the size, refer to the Microsoft article Compute optimized virtual machine sizes.
FOS Version	6.0.6	FortiOS version supported by FortiGate Autoscale for Azure.
VNet New Or Existing	new	Create a new Virtual Network or use an existing one.
VNet Name	autoscalevnet	Azure virtual network name.
Subnet Address Prefix	10.0.0.0/16	Prefix for IP addresses in the virtual network in CIDR notation.
Subnet 1 Name	subnet1	Public facing subnet 1 name.
Subnet 1 Prefix	10.0.1.0/24	Subnet 1 prefix in CIDR notation.
Subnet 2 Name	subnet2	Protected subnet 2 name.
Subnet 2 Prefix	10.0.2.0/24	Subnet 2 prefix in CIDR notation.
Subnet 2 Load Balancer IP Address	10.0.2.10	Static IP address of the internal load balancer on subnet 2.
Subnet 3 Name	subnet3	Private subnet 3 name.
Subnet 3 Prefix	10.0.3.0/24	Subnet 3 prefix in CIDR notation.
Public IP New Or Existing	new	Create a new public IP address or use an existing one.
Public IP Address Name	autoscalepip	Public IP address name.

Parameter	Default	Description
Scaling Group Name Prefix	fgtasg	The prefix each VMSS name is given when deploying the FortiGate Autoscale template. Must be at most 10 characters long and only contain uppercase letters, lowercase letters, and numbers. The value of this parameter should be the same as for *deploy_funcapp.json*.
Initial Capacity	1	The initial number of VM instances in the VMSS. Ranges from *MinCapacity* to *MaxCapacity*.
Min Capacity	1	Minimum number of VM instances in the VMSS (less than or equal to *MaxCapacity*).
Max Capacity	2	Maximum number of VM instances in the VMSS.
Scale Out Threshold	80	Percentage of CPU utilization at which scale-out should occur.
Scale In Threshold	20	Percentage of CPU utilization at which scale-in should occur.
Admin Username	azureadmin	FortiGate-VM administrator username on all VMs.
Admin Password	Requires input	FortiGate-VM administrator password on all VMs. This field must be between 11 and 26 characters and must include at least one uppercase letter, one lowercase letter, one digit, and one special character such as (! @ # $ %).
Endpoint URL	Requires input	Function App public URL.

Deploying FortiGate Autoscale for Azure (PAYG instances)

To deploy FortiGate Autoscale for Azure (PAYG instances):

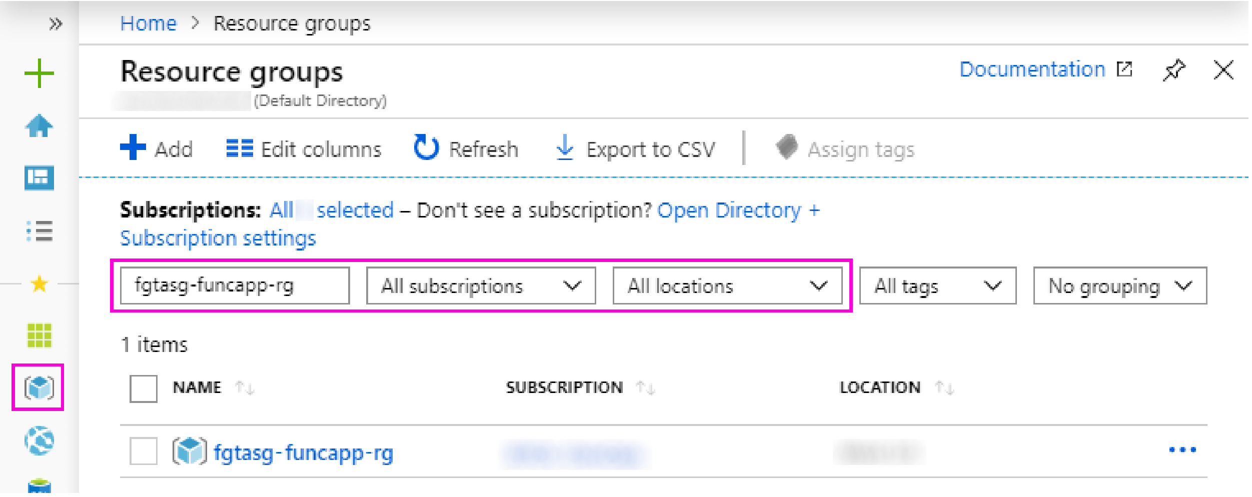
1. Create two (2) resource groups. One will be for the Function App and the other will be for the Scale Set. The deployment instructions in this guide uses resource groups with names that start with *fgtasg-* and end with *-rg*.

   The location must be the same for both resource groups.

2. Create a template deployment for the Function App using the template file `deploy_funcapp.json`. For details on how to do this, refer to the section "Creating a template deployment" on page 7.
3. Obtain the endpoint URL of the Function App. For details on how to do this, refer to the section "Obtaining the endpoint URL of the Function App" below.
4. Upload `configset` files to the Storage account. For details on how to do this, refer to the section "Uploading configset files to the Storage account" on page 17.
5. Create a template deployment for the Scale Set using the template file `deploy_scaleset.json`. For details on how to do this, refer to the section "Creating a template deployment" on page 7.

Obtaining the endpoint URL of the Function App

1. In the Azure console, from the left navigation column, select *Resource groups*.
2. Locate the resource group in which you deployed the Function App template by scrolling through the list or by using one or more of the name, subscription, and location filters. In our example below, this is *fgtasg-funcapp-rg*. Once you locate it, click the name to load the resource group *Overview* page.



Resource groups

[redacted] (Default Directory)

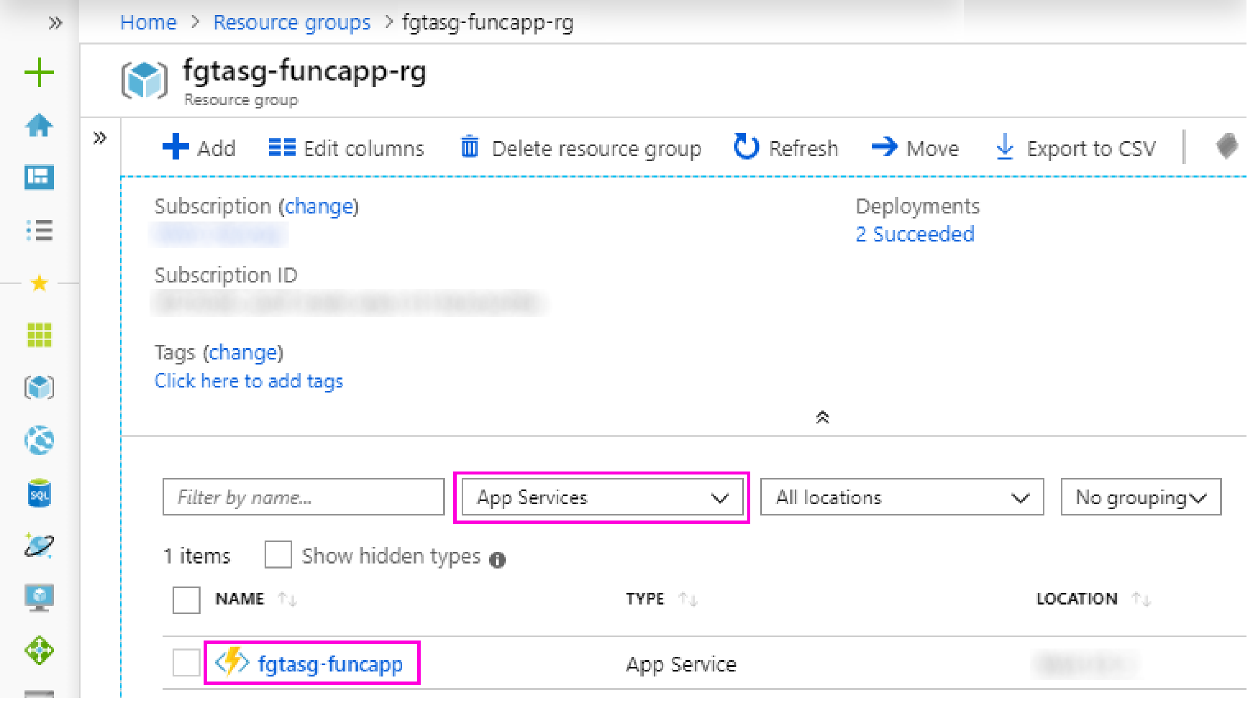
Subscriptions: All [redacted] selected – Don't see a subscription? Open Directory + Subscription settings

fgtasg-funcapp-rg | All subscriptions | All locations | All tags | No grouping

1 items

NAME	SUBSCRIPTION	LOCATION
fgtasg-funcapp-rg	[redacted]	[redacted]

3. Load the Function App by clicking its name. It is the item of type *App Service*.



Home > Resource groups > fgtasg-funcapp-rg

fgtasg-funcapp-rg
Resource group

Add | Edit columns | Delete resource group | Refresh | Move | Export to CSV

Subscription (change)
[redacted]

Deployments
2 Succeeded

Subscription ID
[redacted]

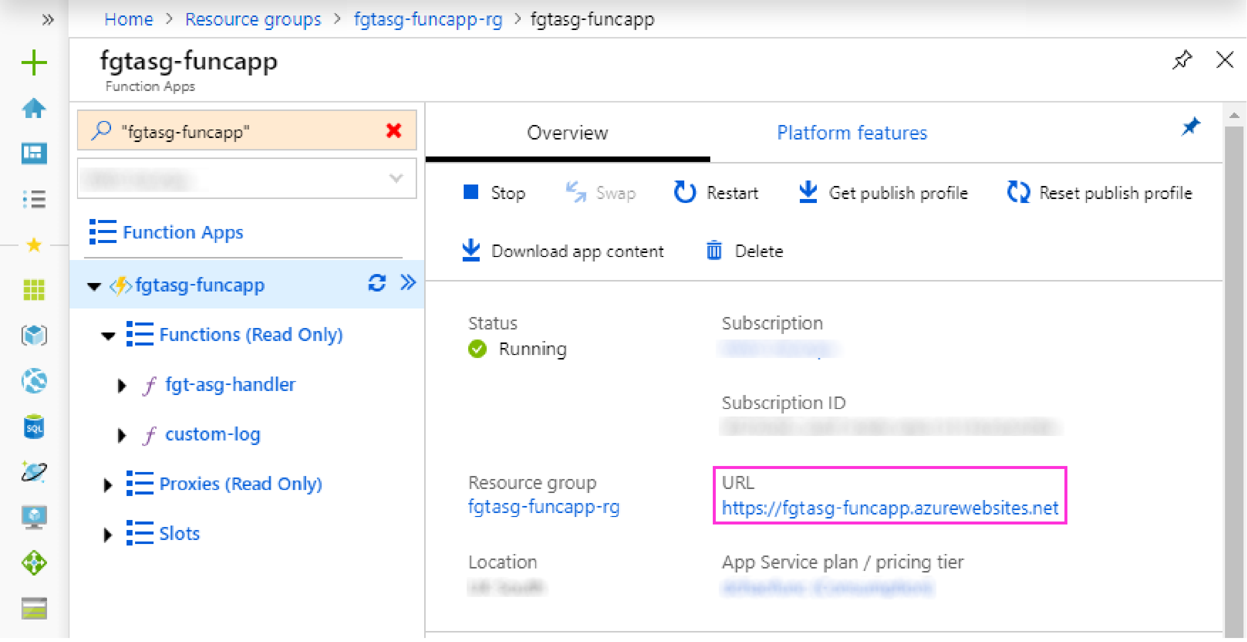
Tags (change)
Click here to add tags

Filter by name... | App Services | All locations | No grouping

1 items □ Show hidden types

□	NAME	TYPE	LOCATION
□	fgtasg-funcapp	App Service	[redacted]

4. Make note of the URL as you will need it to deploy the Scale Set template. In our example, the URL is *https://fgtasg-funcapp.azurewebsites.net*.



Home > Resource groups > fgtasg-funcapp-rg > fgtasg-funcapp

fgtasg-funcapp
Function Apps

Status
Running

Subscription
[redacted]

Subscription ID
[redacted]

Resource group
fgtasg-funcapp-rg

URL
https://fgtasg-funcapp.azurewebsites.net

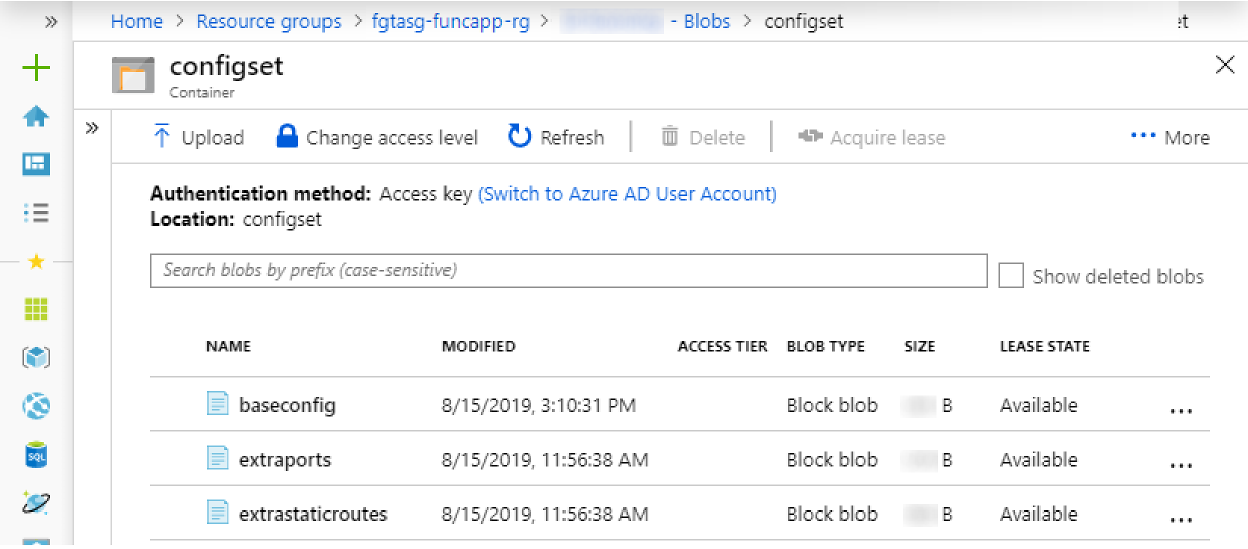
Location
[redacted]

App Service plan / pricing tier
[redacted]

Uploading `configset` files to the Storage account

1. Load the resource group in which you deployed Function App template.
2. Load the Storage account by clicking its name.
3. From the Storage account navigation column, click *Blobs*.
4. Create a container and name it *configset*. Leave the Public access level as *Private*.
5. Upload all the files in the *configset* folder of the deployment package to this container.

The blob container will look as shown below:


Home > Resource groups > fgtasg-funcapp-rg > [redacted] - Blobs > configset
configset
Container
Upload
Change access level
Refresh
Delete
Acquire lease
More
Search blobs by prefix (case-sensitive)
☐ Show deleted blobs

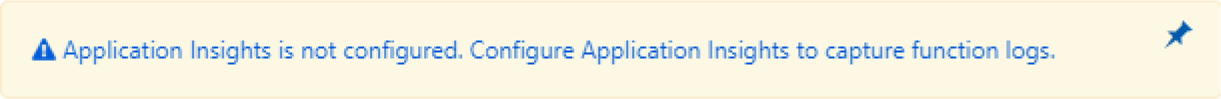
Authentication method: Access key (Switch to Azure AD User Account)
Location: configset

NAME	MODIFIED	ACCESS TIER	BLOB TYPE	SIZE	LEASE STATE	
baseconfig	8/15/2019, 3:10:31 PM		Block blob	[redacted] B	Available	...
extraports	8/15/2019, 11:56:38 AM		Block blob	[redacted] B	Available	...
extrastaticroutes	8/15/2019, 11:56:38 AM		Block blob	[redacted] B	Available	...

Post-deployment configuration

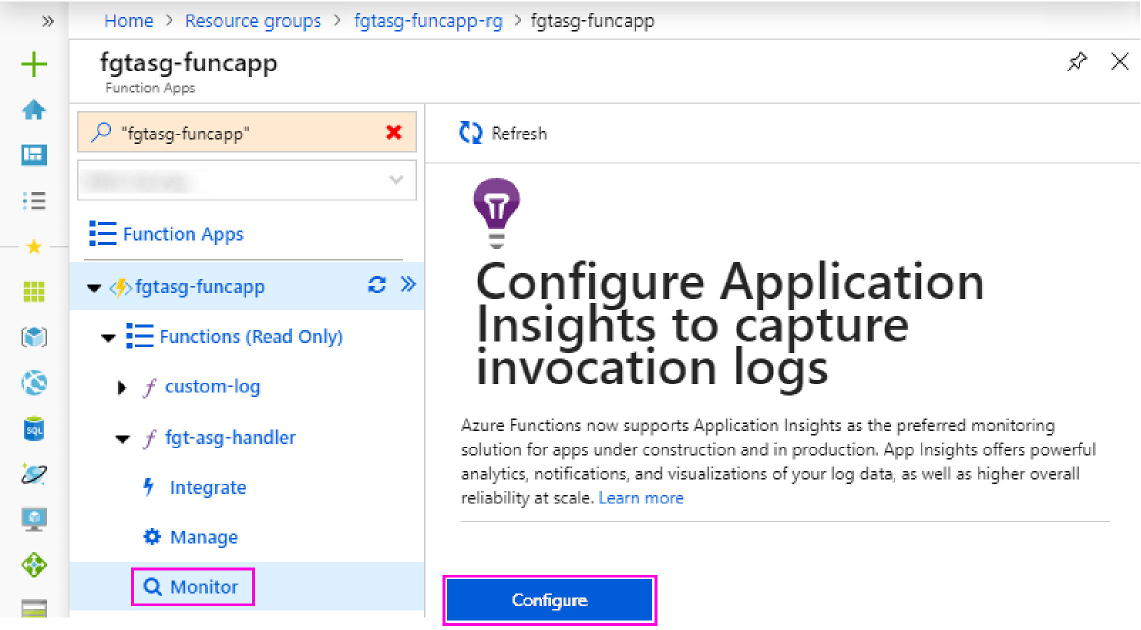
It is recommended that you enable *Application Insights* to capture logs for the Azure functions. This will assist in troubleshooting the deployment.

1. Load the Function App as described in steps 1 - 3 of the section "Obtaining the endpoint URL of the Function App" on page 15. In our example below, this is *fgtasg-funcapp*.
2. If you see the banner below, click it to configure *Application Insights*.



⚠ Application Insights is not configured. Configure Application Insights to capture function logs.

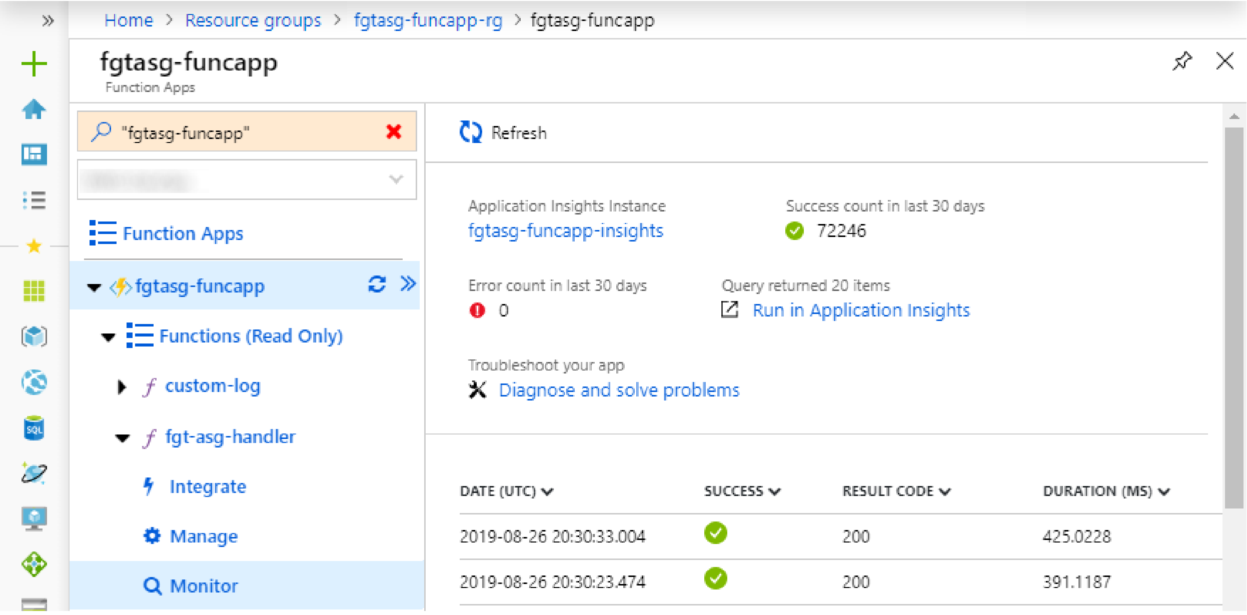
Otherwise, expand the function to select *Monitor* and then click *Configure*.



Configure Application Insights to capture invocation logs

Azure Functions now supports Application Insights as the preferred monitoring solution for apps under construction and in production. App Insights offers powerful analytics, notifications, and visualizations of your log data, as well as higher overall reliability at scale. Learn more

3. Once enabled, you can review the logs to troubleshoot the Azure Function code.



Application Insights Instance: fgtasg-funcapp-insights

Success count in last 30 days: 72246

Error count in last 30 days: 0

Query returned 20 items: Run in Application Insights

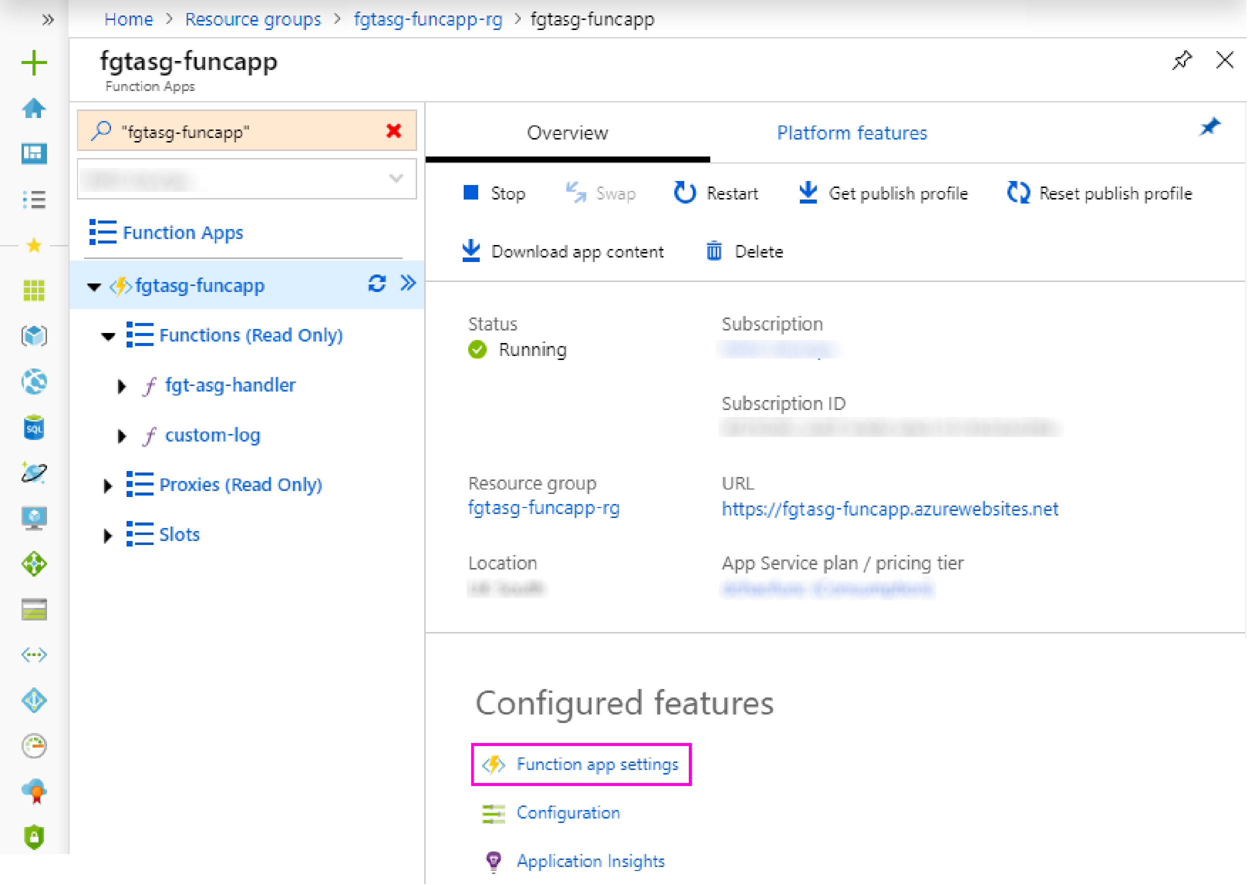
Troubleshoot your app: Diagnose and solve problems

DATE (UTC)	SUCCESS	RESULT CODE	DURATION (MS)
2019-08-26 20:30:33.004	✓	200	425.0228
2019-08-26 20:30:23.474	✓	200	391.1187

To change settings after deployment:

1. Load the Function App as described in steps 1 - 3 of the section "Obtaining the endpoint URL of the Function App" on page 15.

2. Under *Configured features*, click *Function app settings*.



Status: Running

Subscription: [redacted]

Subscription ID: [redacted]

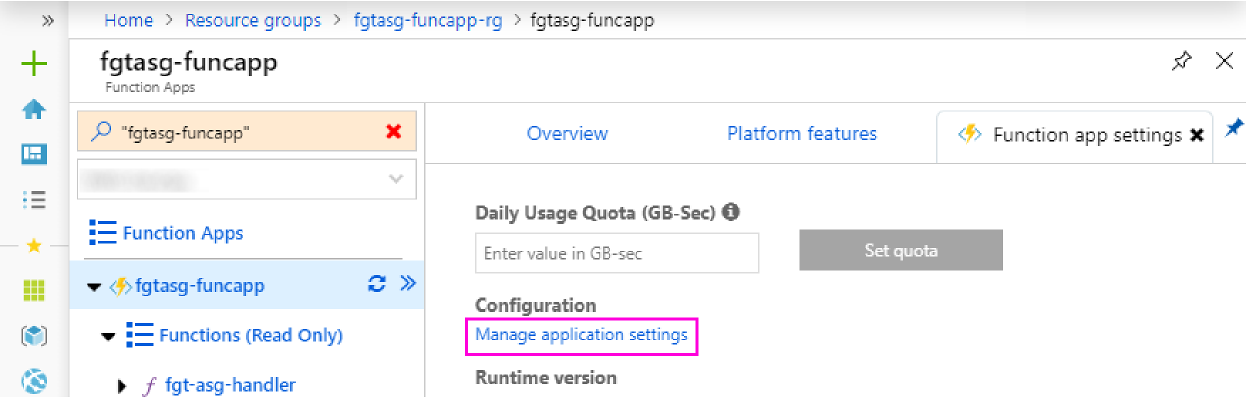
Resource group: fgtasg-funcapp-rg

URL: https://fgtasg-funcapp.azurewebsites.net

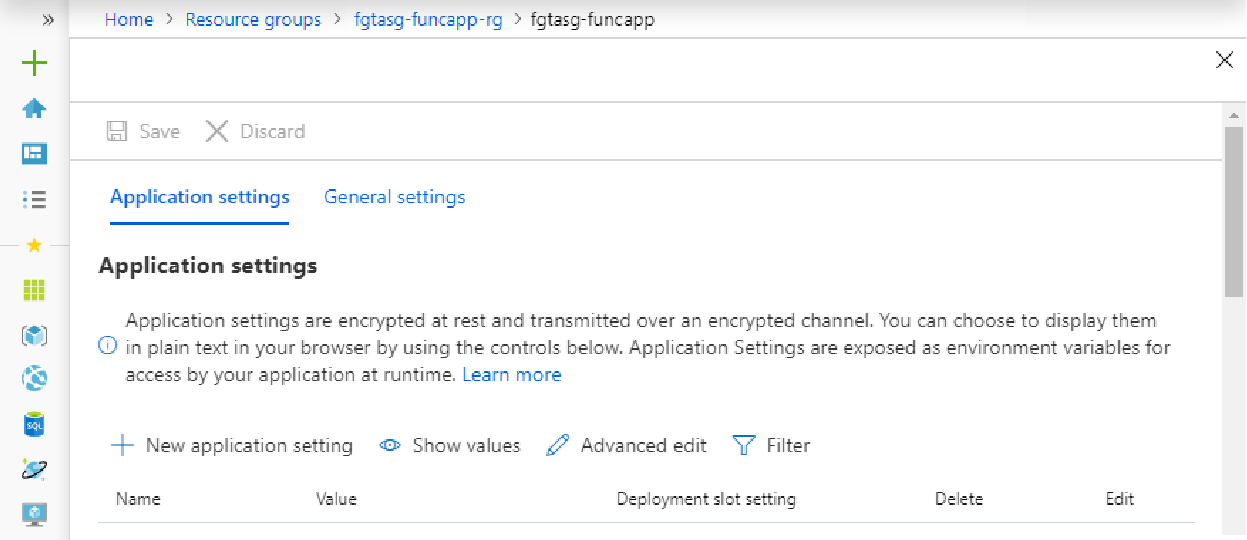
Location: [redacted]

App Service plan / pricing tier: [redacted]

3. Click *Manage application settings*.



4. Click *Manage application settings*.



Home > Resource groups > fgtasg-funcapp-rg > fgtasg-funcapp

Application settings

Application settings are encrypted at rest and transmitted over an encrypted channel. You can choose to display them in plain text in your browser by using the controls below. Application Settings are exposed as environment variables for access by your application at runtime. Learn more

Name	Value	Deployment slot setting	Delete	Edit

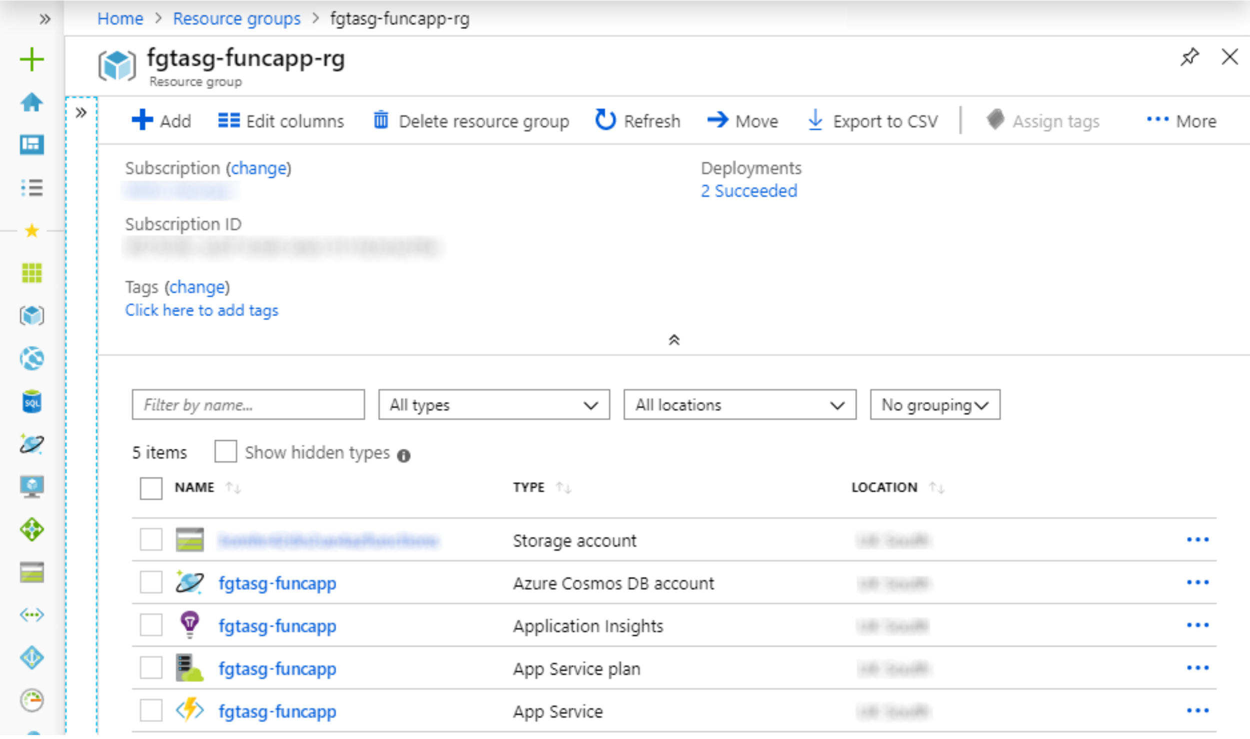
5. Edit settings as needed.

Verifying the PAYG deployment

In the resource group you created for the Function App (*fgtasg-funcapp-rg* in our example), you will find the following components:

- 1 Storage account
- 1 Azure Cosmos DB account
- 1 Application Insights (if you enabled it)
- 1 App Service plan
- 1 App Service (this is the Function App)

The Function App resource group *Overview* page will look as shown below:



Subscription (change)
[redacted]

Subscription ID
[redacted]

Deployments
2 Succeeded

Tags (change)
Click here to add tags

Filter by name... | All types | All locations | No grouping

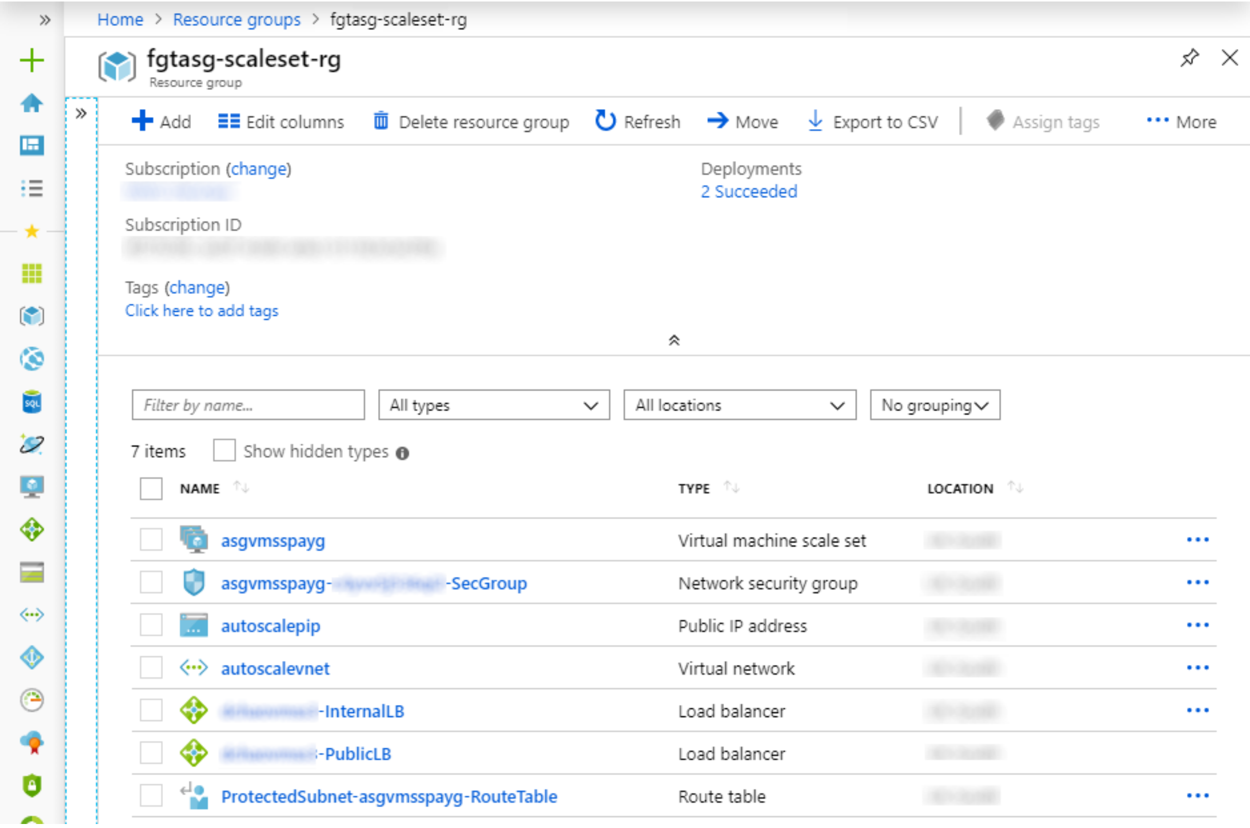
5 items □ Show hidden types

□	NAME	TYPE	LOCATION
□	[redacted]	Storage account	[redacted]
□	fgtasg-funcapp	Azure Cosmos DB account	[redacted]
□	fgtasg-funcapp	Application Insights	[redacted]
□	fgtasg-funcapp	App Service plan	[redacted]
□	fgtasg-funcapp	App Service	[redacted]

In the resource group you created for the Scale Set (*fgtasg-scaleset-rg* in our example), you will find the following components:

- 1 Virtual machine scale set
- 1 Network security group
- 1 Public IP address
- 1 Virtual network
- 1 Internal Load balancer
- 1 Public Load balancer
- 1 Route table

The Scale Set resource group *Overview* page will look as shown below:



Subscription (change)
[redacted]

Subscription ID
[redacted]

Tags (change)
Click here to add tags

Deployments
2 Succeeded

Filter by name... | All types | All locations | No grouping

7 items □ Show hidden types

NAME	TYPE	LOCATION
asgvmsspayg	Virtual machine scale set	[redacted]
asgvmsspayg-[redacted]-SecGroup	Network security group	[redacted]
autoscalepip	Public IP address	[redacted]
autoscalevnet	Virtual network	[redacted]
[redacted]-InternalLB	Load balancer	[redacted]
[redacted]-PublicLB	Load balancer	[redacted]
ProtectedSubnet-asgvmsspayg-RouteTable	Route table	[redacted]

Verify the following components:

- the Function App
- the database
- the master election

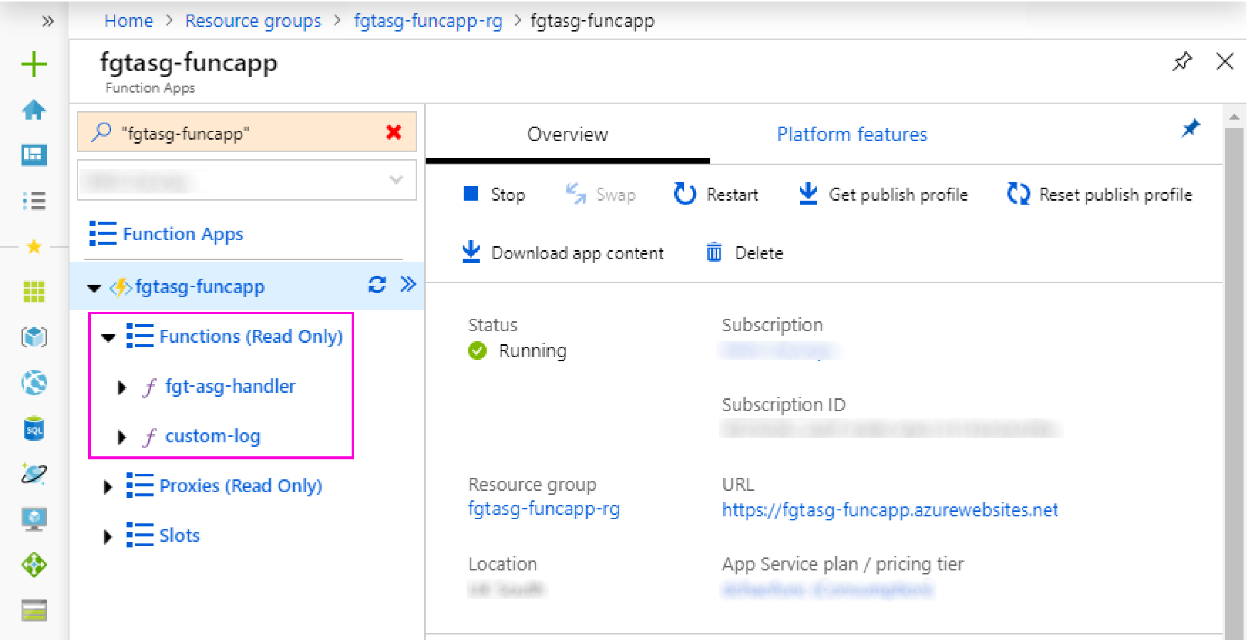
To verify the Function App:

Load the Function App as described in steps 1 - 3 of the section "Obtaining the endpoint URL of the Function App" on page 15.

You should see two functions on the left:

- *fgt-asg-handler*: The main autoscaling function.
- *custom-log*: A function to retrieve function logs for troubleshooting purposes.

The Function App *Overview* page will look as shown below:



Status: Running

Subscription: [redacted]

Subscription ID: [redacted]

Resource group: fgtasg-funcapp-rg

URL: https://fgtasg-funcapp.azurewebsites.net

Location: [redacted]

App Service plan / pricing tier: [redacted]

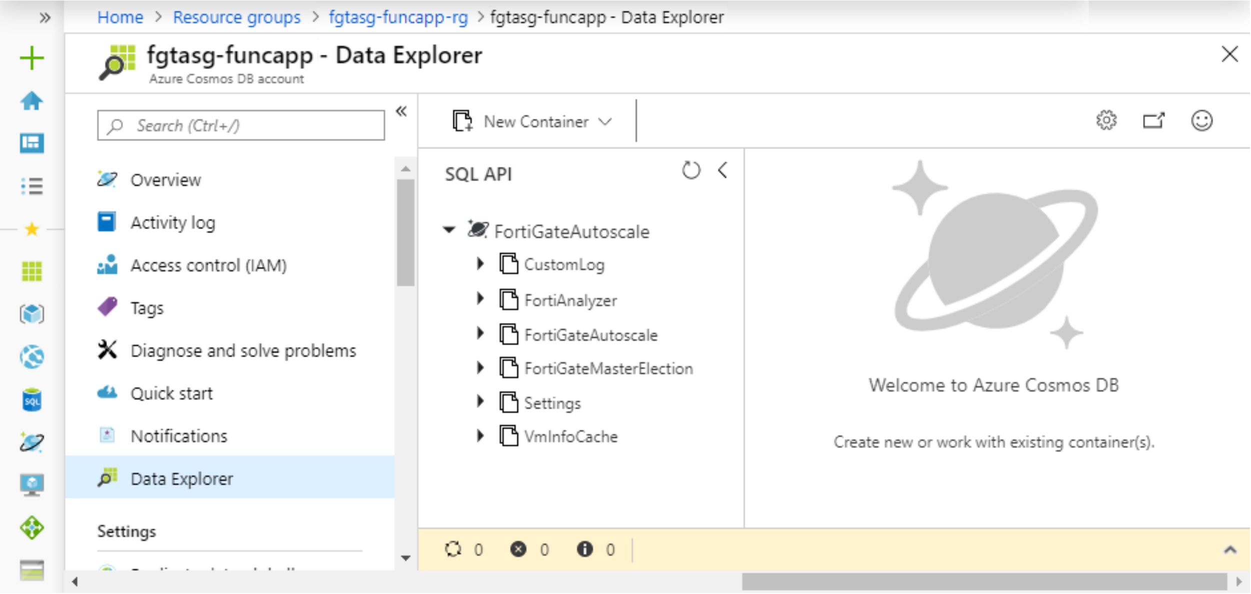
To verify the database:

1. From the Function App resource group overview page, click the *Azure Cosmos DB* account name.
2. From the navigation column, click *Data Explorer*.

You will see the following DB and tables:

- *Database:* FortiGateAutoscale
- *Tables:*
  - CustomLog
  - FortiAnalyzer
  - FortiGateAutoscale
  - FortiGateMasterElection
  - Settings
  - VmInfoCache

The database *Data Explorer* page will look as shown below:



To verify the master election:

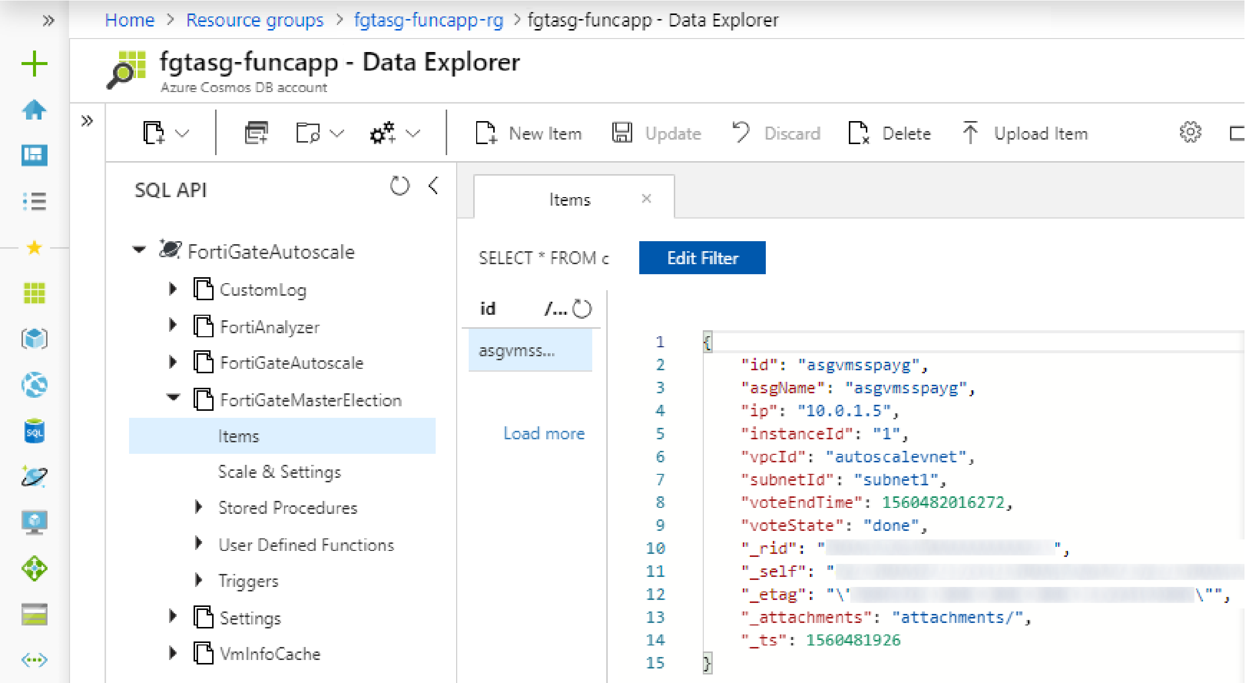
The elected master FortiGate-VM will be logged in the CosmosDB *FortiGateAutoscale* in the table *FortiGateMasterElection*.

1. Expand the *FortiGateMasterElection* table and click on *Items.*
2. The master record will be the only item in the table. Click the master record (*asgvmsspayg* in our example).

In the master record,

- *instanceId* is the index of the FortiGate-VM in the Scale Set.
- *asgName* is the name of the Scale Set in which the master FortiGate-VM is located.
- *ip* is the primary private IP address of the current master FortiGate-VM.
- *subnetId* is the ID of the subnet in which the master FortiGate-VM is located.
- *voteState* is the state of the voting process.
  - *pending*: election of the master instance is still in progress. You should wait for its completion. At this point in time, the final master instance is not yet known.
  - *done*: the master election process is done.
- *vpcId* is the ID of the VPC in which the master FortiGate-VM instance is located.

The *Items* page will look as shown below:



SELECT * FROM c

```
{
    "id": "asgvmsspayg",
    "asgName": "asgvmsspayg",
    "ip": "10.0.1.5",
    "instanceId": "1",
    "vpcId": "autoscalevnet",
    "subnetId": "subnet1",
    "voteEndTime": 1560482016272,
    "voteState": "done",
    "_rid": "[redacted]",
    "_self": "[redacted]
    "_etag": "\"[redacted]\"",
    "_attachments": "attachments/",
    "_ts": 1560481926
}
```

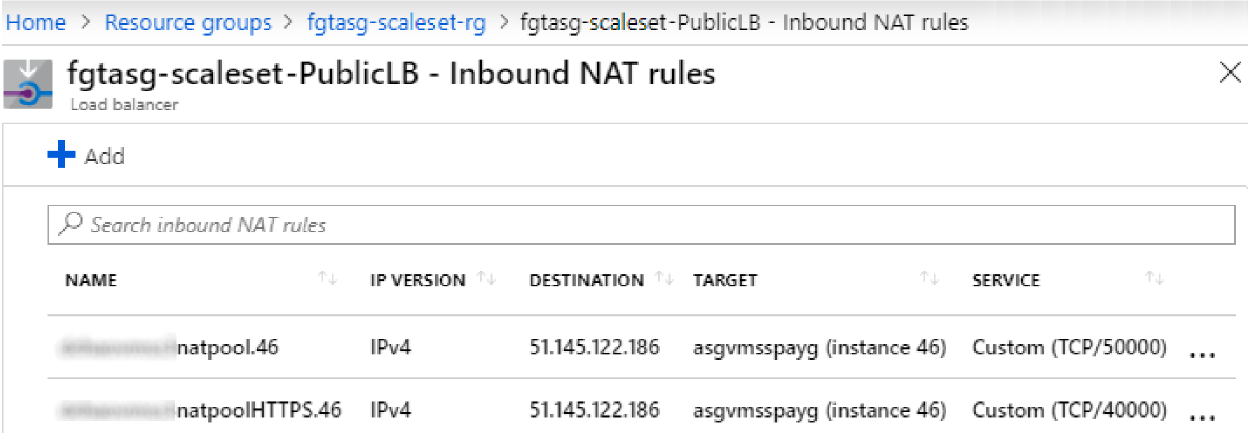
Connecting to the FortiGate-VM instances

To connect to a FortiGate-VM, you can use SSH commands or the web GUI using HTTPS with the IPv4 public IP address.

From the Scale Set resource group overview page, click the external load balancer name to load it. From the navigation column, click *Inbound NAT Rules*. For each instance in the scale set you will see two rules:

- One rule for SSH access to the instance.
- One rule for HTTPS access to the instance.

The *Inbound NAT Rules* page will look as shown below:



Home > Resource groups > fgtasg-scaleset-rg > fgtasg-scaleset-PublicLB - Inbound NAT rules

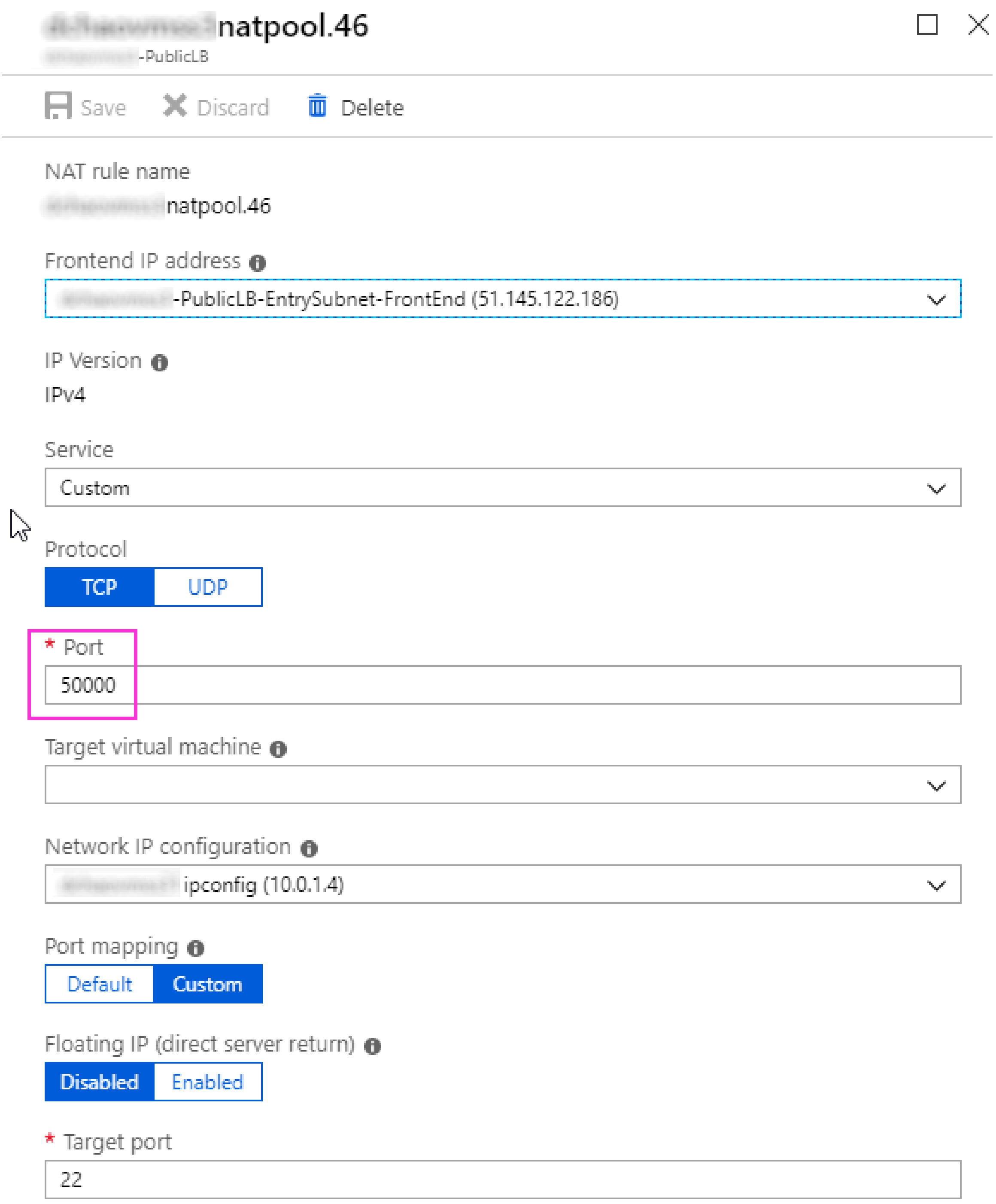
fgtasg-scaleset-PublicLB - Inbound NAT rules

Load balancer

NAME	IP VERSION	DESTINATION	TARGET	SERVICE	
[redacted]natpool.46	IPv4	51.145.122.186	asgvmsspayg (instance 46)	Custom (TCP/50000)	...
[redacted]natpoolHTTPS.46	IPv4	51.145.122.186	asgvmsspayg (instance 46)	Custom (TCP/40000)	...

To access a FortiGate-VM instance, you need the Front End IP address and port number of the instance you wish to connect to. The Front End IP address is listed on the *Inbound NAT Rules* page. To obtain the port number, click the entry for the method you will use to access the instance (SSH or HTTPS). The port number will be listed midway down the page.

An example of an SSH access rule is shown below:



NAT rule name
[redacted]natpool.46

Frontend IP address
[redacted]-PublicLB-EntrySubnet-FrontEnd (51.145.122.186)

IP Version
IPv4

Service
Custom

Protocol
[✓ TCP] UDP

* Port
50000

Target virtual machine

Network IP configuration
[redacted]ipconfig (10.0.1.4)

Port mapping
Default [✓ Custom]

Floating IP (direct server return)
[✓ Disabled] Enabled

* Target port
22

Troubleshooting

Application Insights can help you troubleshoot the deployment. In the PAYG licensing deployment (version 1.0.x), it is enabled in the section "Post-deployment configuration" on page 17.

FortiGate master election was not successful

If the FortiGate-VM master election is not successful, reset the master election. If the reset does not solve the problem, please contact support.

How to reset the master election

To reset the master election, navigate to the CosmosDB *FortiGateAutoscale* and open the table *FortiGateMasterElection* and delete the only record in the table.

A new master FortiGate-VM will be elected and a new record will be created in the table as the result.

For details on locating the database table *FortiGateMasterElection*, refer to the section "To verify the master election:" on page 24.

Appendix

FortiGate Autoscale for Azure features

Major components

- *The Function App*. The Function App handles all the autoscaling features including: master/slave role assignment, license distribution, and failover management.
- *The PAYG Scale Set* The Scale Set contains 1 to many FortiGate-VMs of the PAYG licensing model. This scale set is scalable and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters Scale Out Threshold and Scale In Threshold. As such, this Scale Set may initially have no instances.
- *The Blob Containers*.
  - The *configset* container contains files that are loaded as the initial configuration of a new FortiGate-VM instance.
    - *baseconfig* is the base configuration. This file can be modified as needed to meet your network requirements. Placeholders such as {SYNC_INTERFACE} are explained in the "Configset placeholders" below table below.
- *Database tables*. These tables are required to store information such as health check monitoring, master election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.
- *Networking Components* These are the load-balancing rules, autoscaling settings, virtual network, and routing-related components. You are expected to create your own client and server instances that you want protected by the FortiGate-VM.

Configset placeholders

When the FortiGate-VM requests the configuration from the autoscaling handler function, the placeholders in the table below will be replaced with actual values for the Autoscaling group.

Placeholder	Type	Description
{SYNC_INTERFACE}	Text	The interface for FortiGate-VMs to synchronize information. Specify as port1, port2, port3, etc. All characters must be lowercase.
{CALLBACK_URL}	URL	The full URL of the autoscaling handler function.
{PSK_SECRET}	Text	The Pre-Shared Key used in FortiOS.
{ADMIN_PORT}	Number	The admin port will be replaced with 443.

Function App environment variables for the PAYG deployment

Variable name	Description
RESOURCE_GROUP	Name of the resource group where the Scale Set is deployed in.
SCALING_GROUP_NAME_PAYG	Name of the PAYG VMSS. This name is made by adding "*payg*" to the value of the related parameter *"Scaling Group Name Prefix" on page 12*.
SCALING_GROUP_NAME_BYOL	A reserved variable not used in this version. It takes the value of SCALING_GROUP_NAME_PAYG.
MASTER_SCALING_GROUP_NAME	This takes the value of SCALING_GROUP_NAME_PAYG.
REST_APP_ID	Descriptions of these variables are identical to those of the related parameters which are described in the section "Configurable variables" on page 11. • REST_APP_ID: *"Rest App ID" on page 12* • REST_APP_SECRET: *"Rest App Secret" on page 12* • WEBSITE_RUN_FROM_ZIP: *"Package Res URL" on page 13* • SCALESET_DB_ACCOUNT: *"Cosmos DB Name" on page 11* • TENANT_ID: *"Tenant ID" on page 11* • HEART_BEAT_LOSS_COUNT: *"Heart Beat Loss Count" on page 12* • FORTIGATE_PSKSECRET: *"PSK Secret" on page 12* • SCRIPT_TIMEOUT: *"Script Timeout" on page 12* • ELECTION_WAIT_TIME: *"Election Wait Time" on page 12* • SUBSCRIPTION_ID: *"Subscription ID" on page 11*
REST_APP_SECRET	
WEBSITE_RUN_FROM_ZIP	
SCALESET_DB_ACCOUNT	
TENANT_ID	
HEART_BEAT_LOSS_COUNT	
FORTIGATE_PSKSECRET	
SCRIPT_TIMEOUT	
ELECTION_WAIT_TIME	
SUBSCRIPTION_ID	
REST_API_MASTER_KEY	This is the CosmosDB account access key automatically created with the CosmosDB account.
REQUIRED_CONFIG_SET	This is a comma delimited string for additional *configsets* to load. (Reserved for future use.)
UNIQUE_ID	This variable must be left blank (empty).
CUSTOM_ID	This variable must be left blank (empty).
AZURE_STORAGE_ACCOUNT	This is the Blob Storage account name automatically created during the deployment.
AZURE_STORAGE_ACCESS_KEY	This is the Blob Storage account access key automatically created with the Blob Storage account.
DEBUG_SAVE_CUSTOM_LOG	A troubleshooting variable. Set to *true* to save script logs to the DB table *CUSTOM_LOG*. This is the default behavior. Set to *false* to disable this feature.

Variable name	Description
DEBUG_LOGGER_OUTPUT_QUEUE_ENABLED	A troubleshooting variable. Set to *true* to concatenate all log output into one (1) log item in the Azure logging system. Set to *false* for every log output to have its own log item in the Azure logging system. This is the default behavior.

FortiGate Autoscale for Azure HA topology (PAYG instances)

In this sample HA setup, each FortiGate-VM has two interfaces.

- Port1 (external): 10.0.1.x/24 subnet1
- Port2 (internal): 10.0.2.x/24 subnet2

Instance 1:

- Port1: 10.0.1.5
- Port2: 10.0.2.5

Instance 2:

- Port1: 10.0.1.4
- Port2: 10.0.2.4

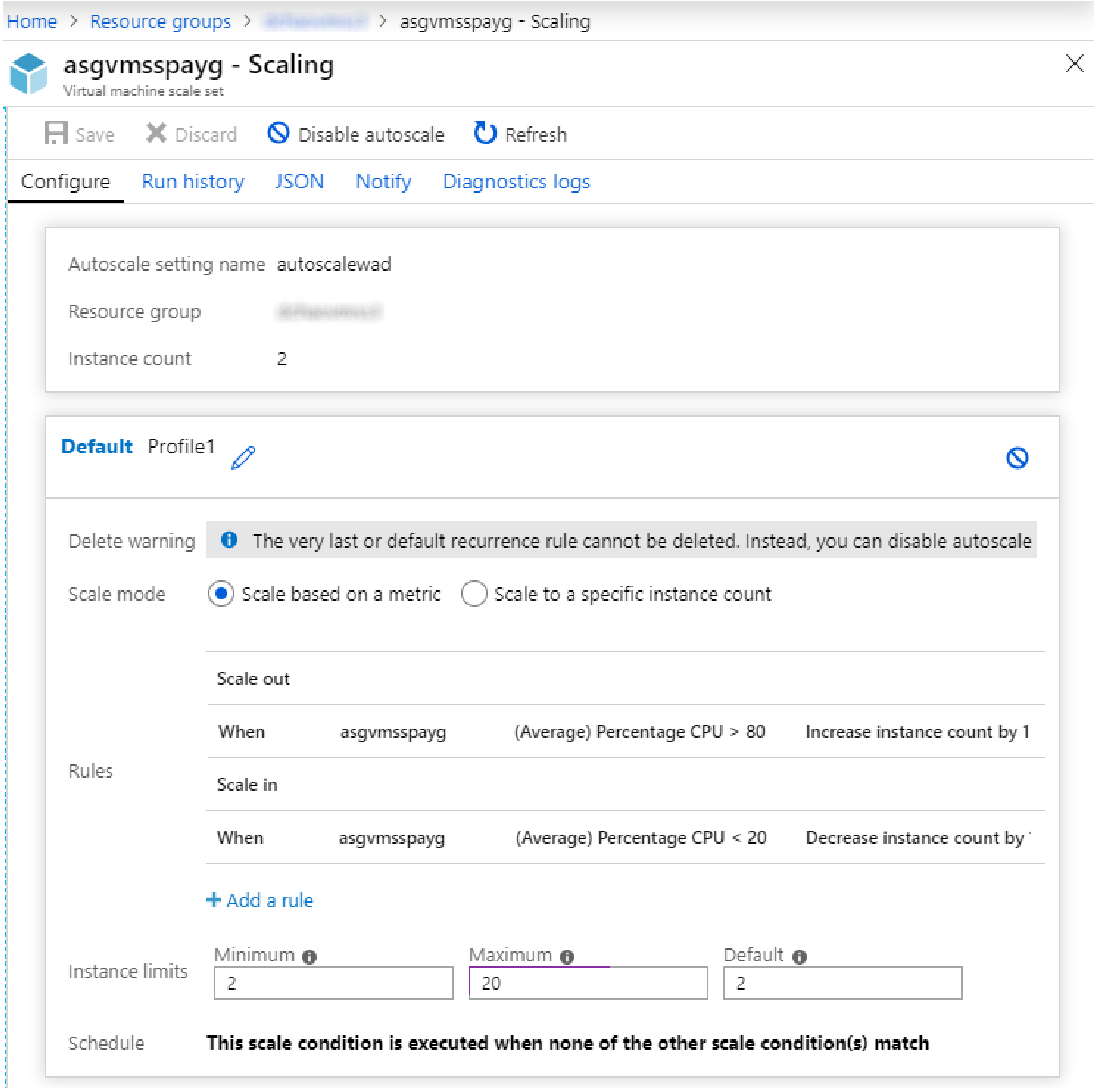
Each subnet has its own load balancer to allocate the traffic to each instance pool.

By default, the Autoscaling group is set to one instance.

To increase the number of instances:

1. Load the resource group in which you deployed the Scale Set template.
2. From the overview page, click the *Virtual machine scale set* name (*asgvmsspayg* in our example).
3. From the navigation column, under *Settings*, click *Scaling*.

The configuration page will look as shown below:



asgvmsspayg - Scaling
Virtual machine scale set

Autoscale setting name	autoscalewad
Resource group	[redacted]
Instance count	2

Default Profile1

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale

Scale mode: ● Scale based on a metric ○ Scale to a specific instance count

Rules:

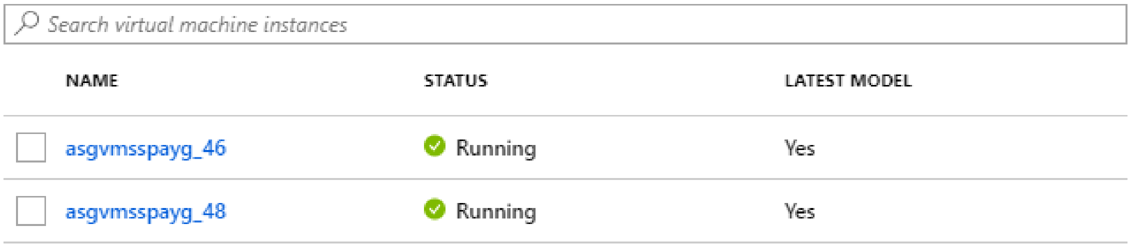
Scale out			
When	asgvmsspayg	(Average) Percentage CPU > 80	Increase instance count by 1
Scale in			
When	asgvmsspayg	(Average) Percentage CPU < 20	Decrease instance count by '

+ Add a rule

Instance limits: Minimum 2 | Maximum 20 | Default 2

Schedule: **This scale condition is executed when none of the other scale condition(s) match**

In this example, the *Minimum* and *default* instances has been increased to two. Once Autoscaling finishes spawning new instances, you can see the new instances by going to the navigation column. Under *Settings*, click *Instances*. In our example, we now additionally see *instance 48*.



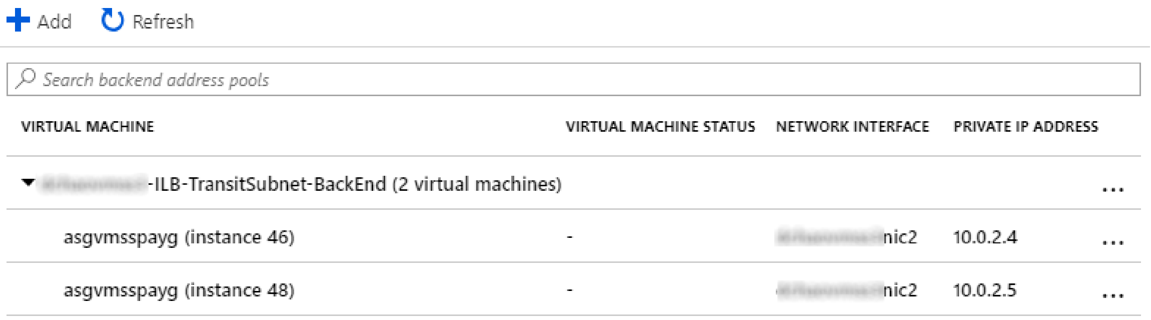
	NAME	STATUS	LATEST MODEL
□	asgvmsspayg_46	✓ Running	Yes
□	asgvmsspayg_48	✓ Running	Yes

The Load Balancers will also have been updated.

To view the load balancers:

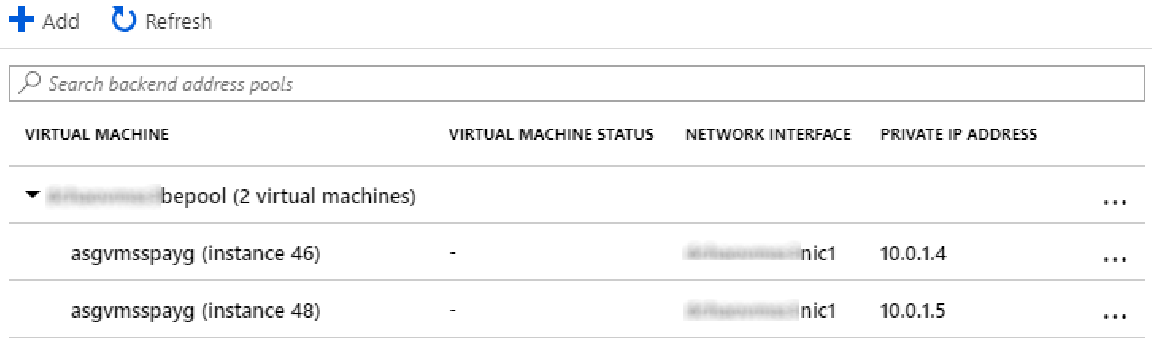
1. Load the resource group in which you deployed the Scale Set template.
2. From the overview page, click the link for the Internal or External load balancer.
3. From the navigation column, under *Settings*, click *Backend pools*.

Following is an example of internal load balancer instances:



VIRTUAL MACHINE	VIRTUAL MACHINE STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS	
▾ [redacted]-ILB-TransitSubnet-BackEnd (2 virtual machines)				...
asgvmsspayg (instance 46)	-	[redacted]nic2	10.0.2.4	...
asgvmsspayg (instance 48)	-	[redacted]nic2	10.0.2.5	...

Following is an example of external load balancer instances:

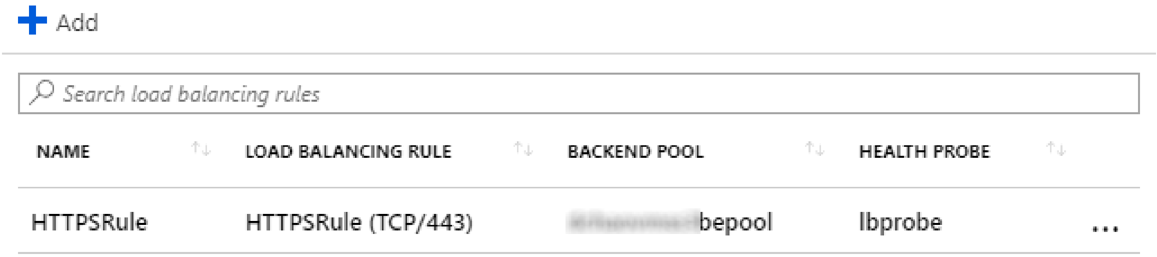


VIRTUAL MACHINE	VIRTUAL MACHINE STATUS	NETWORK INTERFACE	PRIVATE IP ADDRESS	
▾ [redacted]bepool (2 virtual machines)				...
asgvmsspayg (instance 46)	-	[redacted]nic1	10.0.1.4	...
asgvmsspayg (instance 48)	-	[redacted]nic1	10.0.1.5	...

To configure the type of traffic to load balance on:

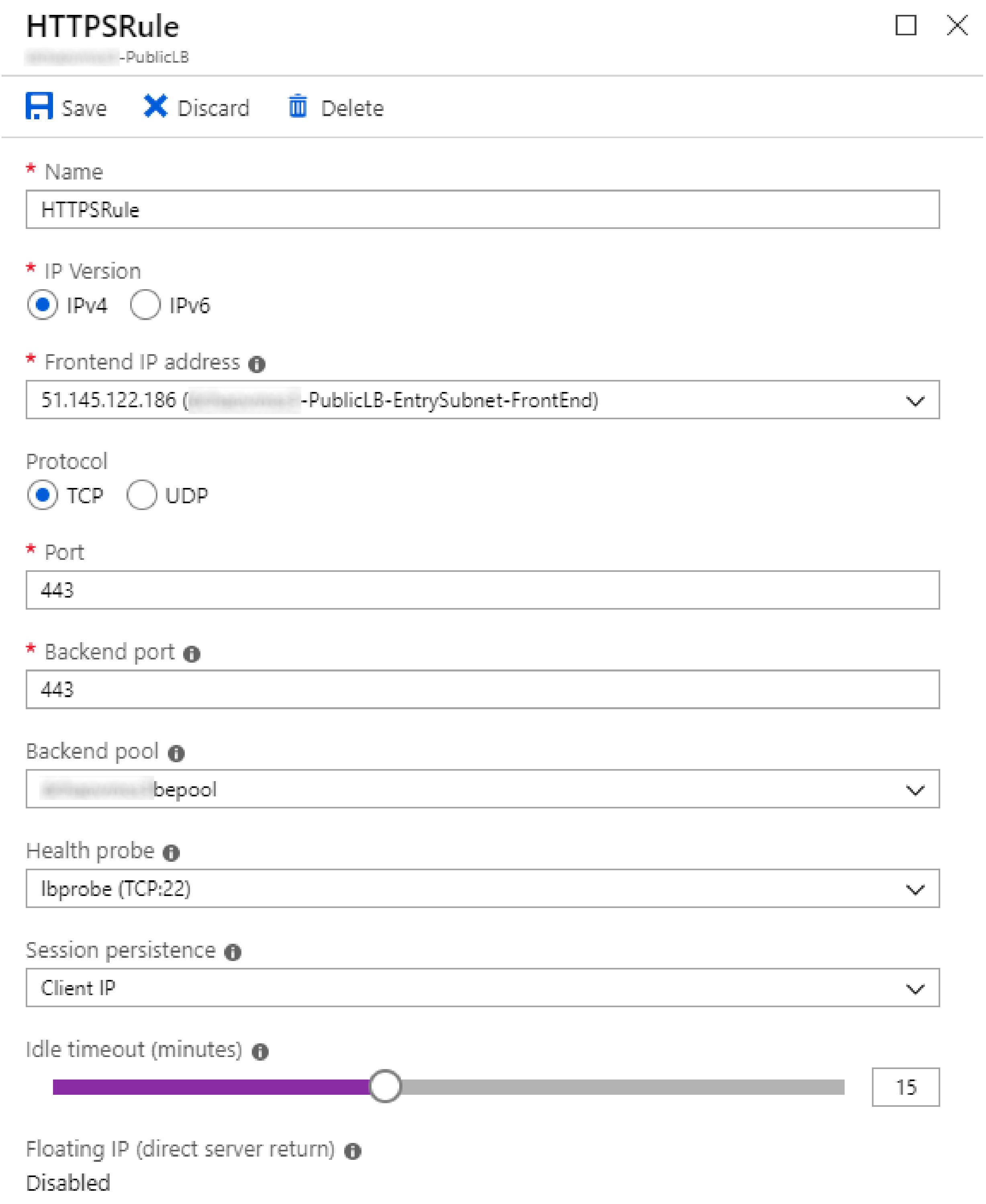
1. Load the resource group in which you deployed the Scale Set template.
2. From the overview page, click the link for the Internal or External load balancer.
3. From the navigation column, under *Settings*, click *Load balancing rules*.

An example of a rule list:



NAME	LOAD BALANCING RULE	BACKEND POOL	HEALTH PROBE	
HTTPSRule	HTTPSRule (TCP/443)	[redacted]bepool	lbprobe	...

Click into the rule to see more details. This sample rule below allocates HTTPS traffic (443) to the backend pool from the front end public IP address using the SSH port for health probe traffic.



HTTPSRule

[redacted]-PublicLB

* Name

HTTPSRule

* IP Version

● IPv4 ○ IPv6

* Frontend IP address

51.145.122.186 ([redacted]-PublicLB-EntrySubnet-FrontEnd)

Protocol

● TCP ○ UDP

* Port

443

* Backend port

443

Backend pool

[redacted]bepool

Health probe

lbprobe (TCP:22)

Session persistence

Client IP

Idle timeout (minutes)

15

Floating IP (direct server return)

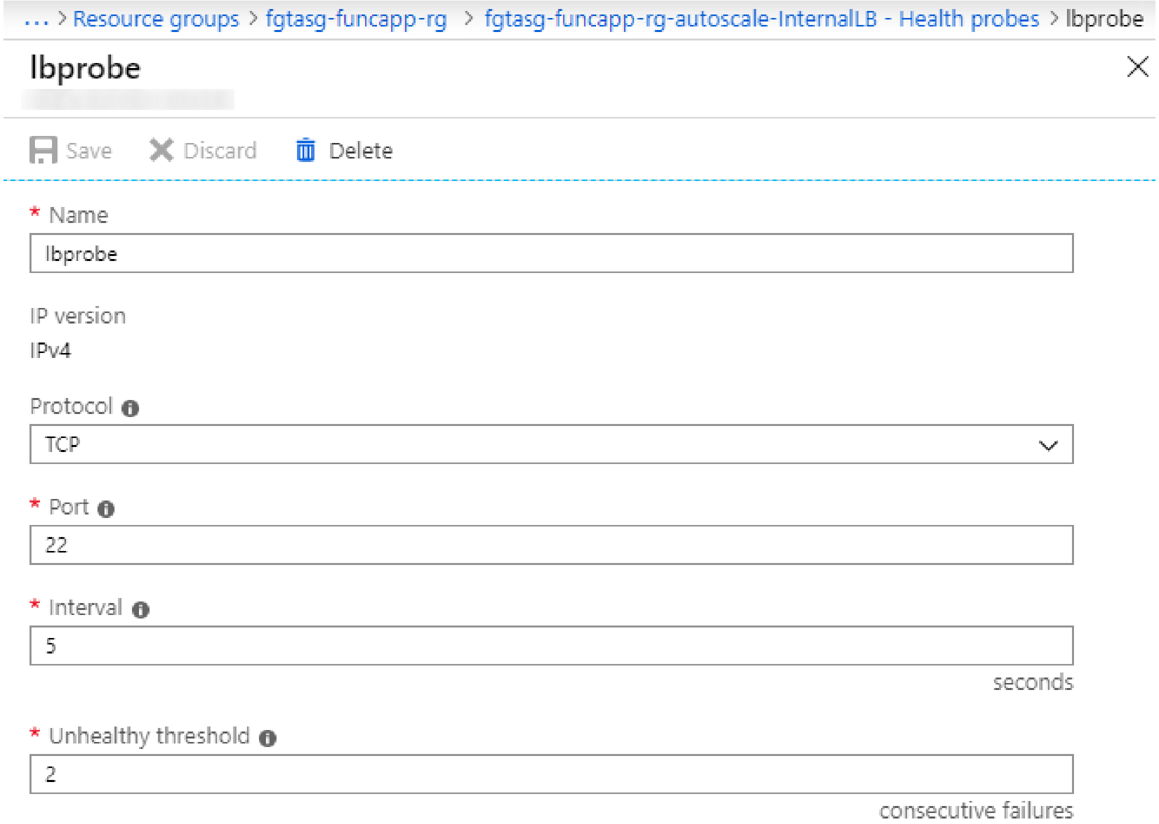
Disabled

To view health probes:

1. Load the resource group in which you deployed the Scale Set template.
2. From the overview page, click the link for the Internal or External load balancer.

3. From the navigation column, under *Settings*, click *Health probes*.
4. The *lbprobe* is listed. Click the name to view the probe.

An example of a health probe:



... > Resource groups > fgtasg-funcapp-rg > fgtasg-funcapp-rg-autoscale-InternalLB - Health probes > lbprobe

lbprobe

* Name: lbprobe

IP version: IPv4

Protocol: TCP

* Port: 22

* Interval: 5 seconds

* Unhealthy threshold: 2 consecutive failures

This example shows the use of port 22 for the probe. Ensure `allowaccess` has SSH enabled on the FortiGate-VM interface.

```
config system interface
   edit "port1"
      set vdom "root"
      set mode dhcp
      set allowaccess ping https ssh fgfm
      set type physical
      set src-check disable
      set description "ext"
      set snmp-index 1
   next
end
```

Azure also sends probing traffic from IP address 168.63.129.16. Ensure this route also exists on the internal interface (s). Port 2 is the internal interface in the below example.

```
config router static
   edit 1
      set dst 168.63.129.16 255.255.255.255
      set gateway 10.0.2.1
      set device "port2"
   next
end
```

Otherwise, Azure may consider the instances non-operational and may not forward traffic to them.

Cloud-init (PAYG instances)

In Autoscaling, FortiGate-VM uses the `cloud-init` feature to pre-configure the instances when they first come up. During deployment of the Scale Set template, you were required to enter a value for the "Endpoint URL" on page 14 parameter. The example was as following:

Endpoint URL: https://fgtasg-funcapp.azurewebsites.net/api/

FortiGate uses this parameter value to send requests to different functions within this Endpoint URL location to retrieve necessary configurations after initialization. Following is an example of output from a FortiGate-VM instance:

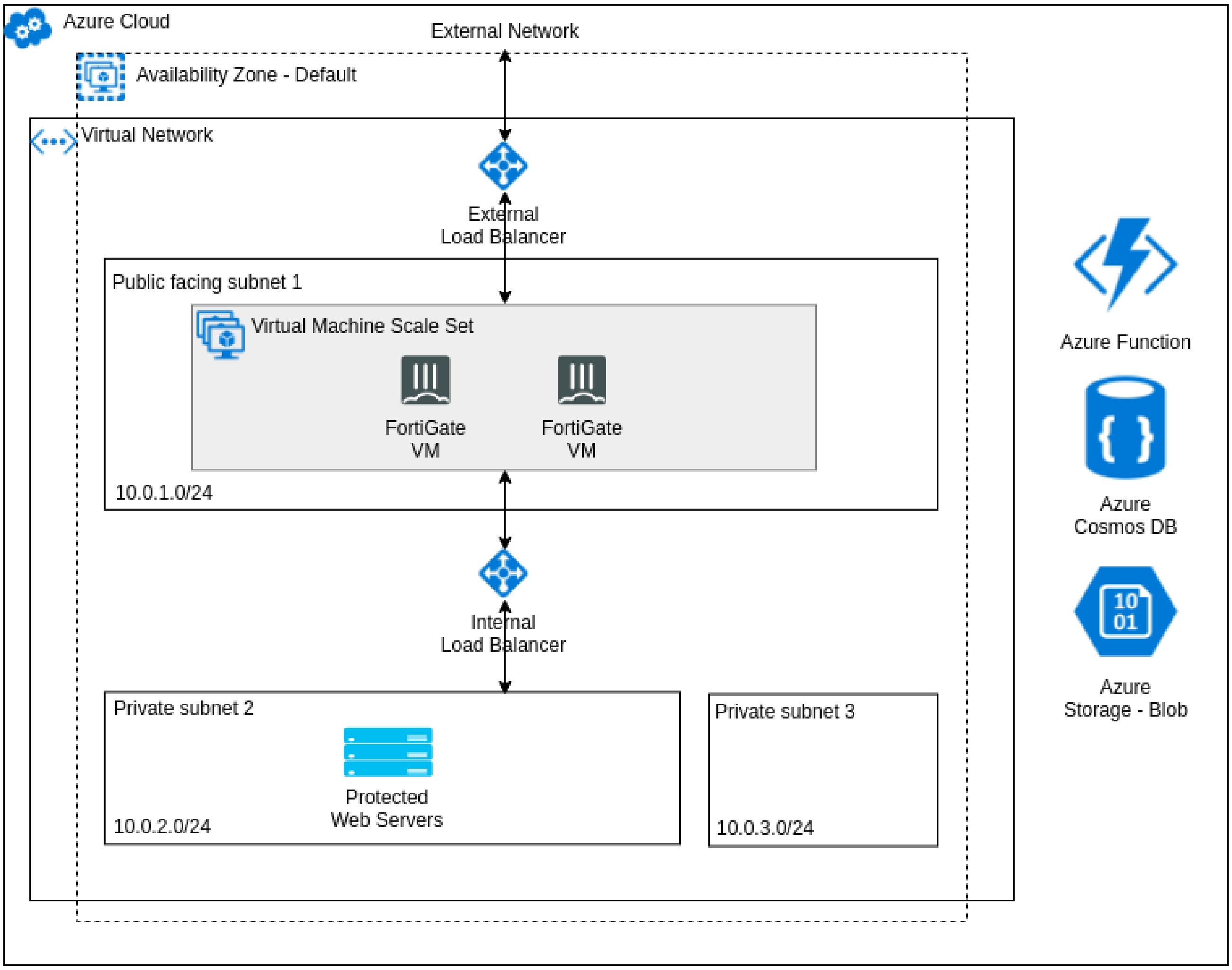
FortiGate-VM cloudinit output

```
# diag debug cloudinit show
>> Checking metadata source azure
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure waiting for customdata file
>> Azure customdata file found
>> Azure cloudinit decrypt successfully
>> Azure Fos-instance-id: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
>> Azure couldn't find mime link
>> Azure trying to get config script from https://fgtasg-funcapp.azurewebsites.net/api/fgt-
     asg-handler
>> Azure download config script successfully
>> Azure customdata processed successfully
>> Run config script
>> Finish running script
>> fgtasg-vmss300000W $
>> fgtasg-vmss300000W $ config system dns
>> fgtasg-vmss300000W (dns) $ unset primary
>> fgtasg-vmss300000W (dns) $ unset secondary
>> fgtasg-vmss300000W (dns) $ end
>> fgtasg-vmss300000W $ config system auto-scale
>> fgtasg-vmss300000W (auto-scale) $ set status enable
>> fgtasg-vmss300000W (auto-scale) $ set sync-interface "port1"
>> fgtasg-vmss300000W (auto-scale) $ set role slave
>> fgtasg-vmss300000W (auto-scale) $ set master-ip 10.0.1.5
>> fgtasg-vmss300000W (auto-scale) $ set callback-url https://fgtasg-
     funcapp.azurewebsites.net/api/fgt-asg-handler
>> fgtasg-vmss300000W (auto-scale) $ set psksecret FortinetPSK#
>> fgtasg-vmss300000W (auto-scale) $ end
>> fgtasg-vmss300000W $
>> fgtasg-vmss300000W $ config sys interface
>> fgtasg-vmss300000W (interface) $ edit "port2"
>> fgtasg-vmss300000W (port2) $ set mode dhcp
>> fgtasg-vmss300000W (port2) $ set defaultgw disable
>> fgtasg-vmss300000W (port2) $ set allowaccess ping https ssh http fgfm
>> fgtasg-vmss300000W (port2) $ next
>> fgtasg-vmss300000W (interface) $ end
>> fgtasg-vmss300000W $
>> fgtasg-vmss300000W $ config system global
>> fgtasg-vmss300000W (global) $ set admin-sport 8443
>> fgtasg-vmss300000W (global) $ end
```

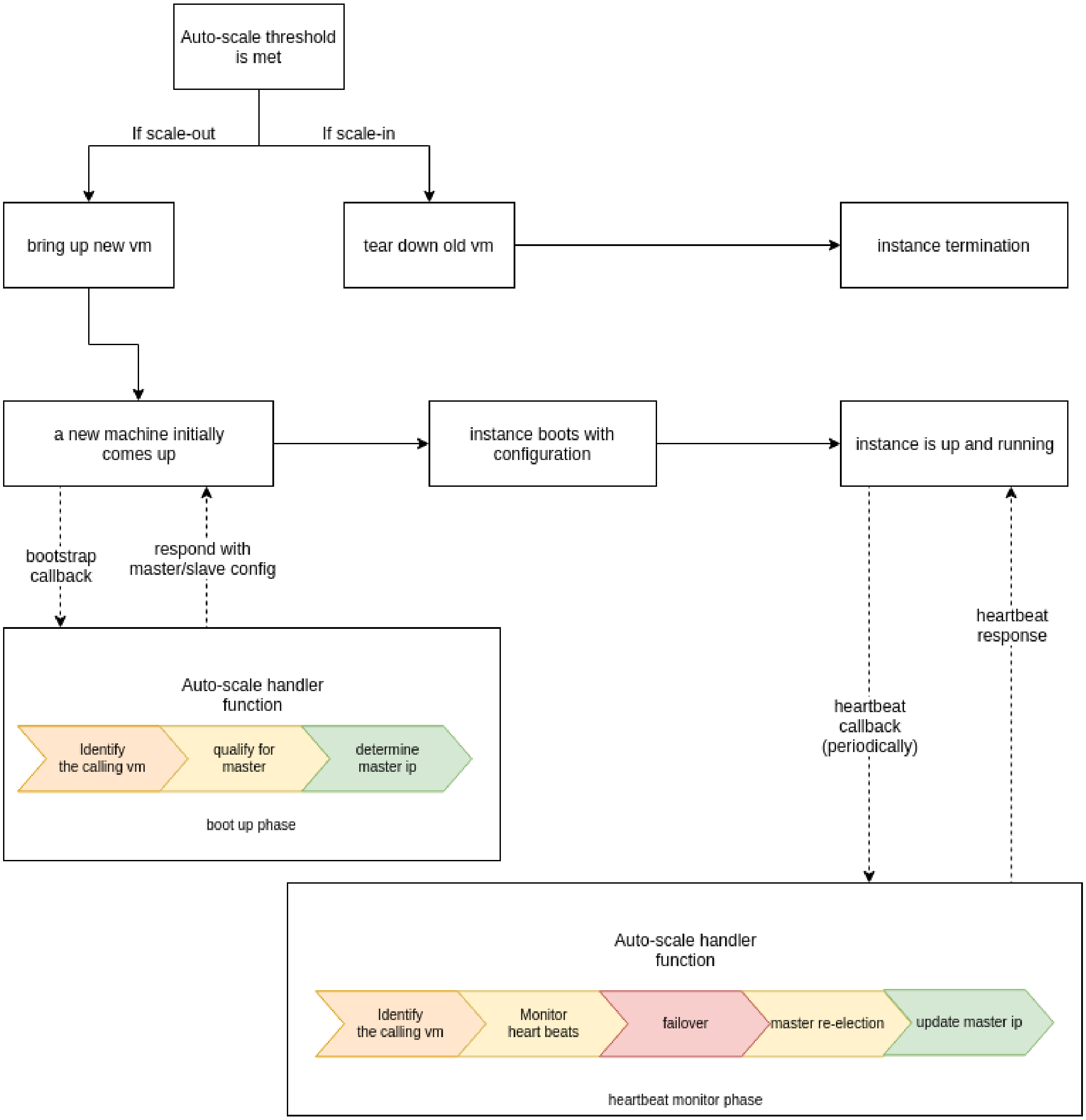
Architectural diagrams

The following diagrams illustrate the different aspects of the architecture of FortiGate Autoscale for Azure.

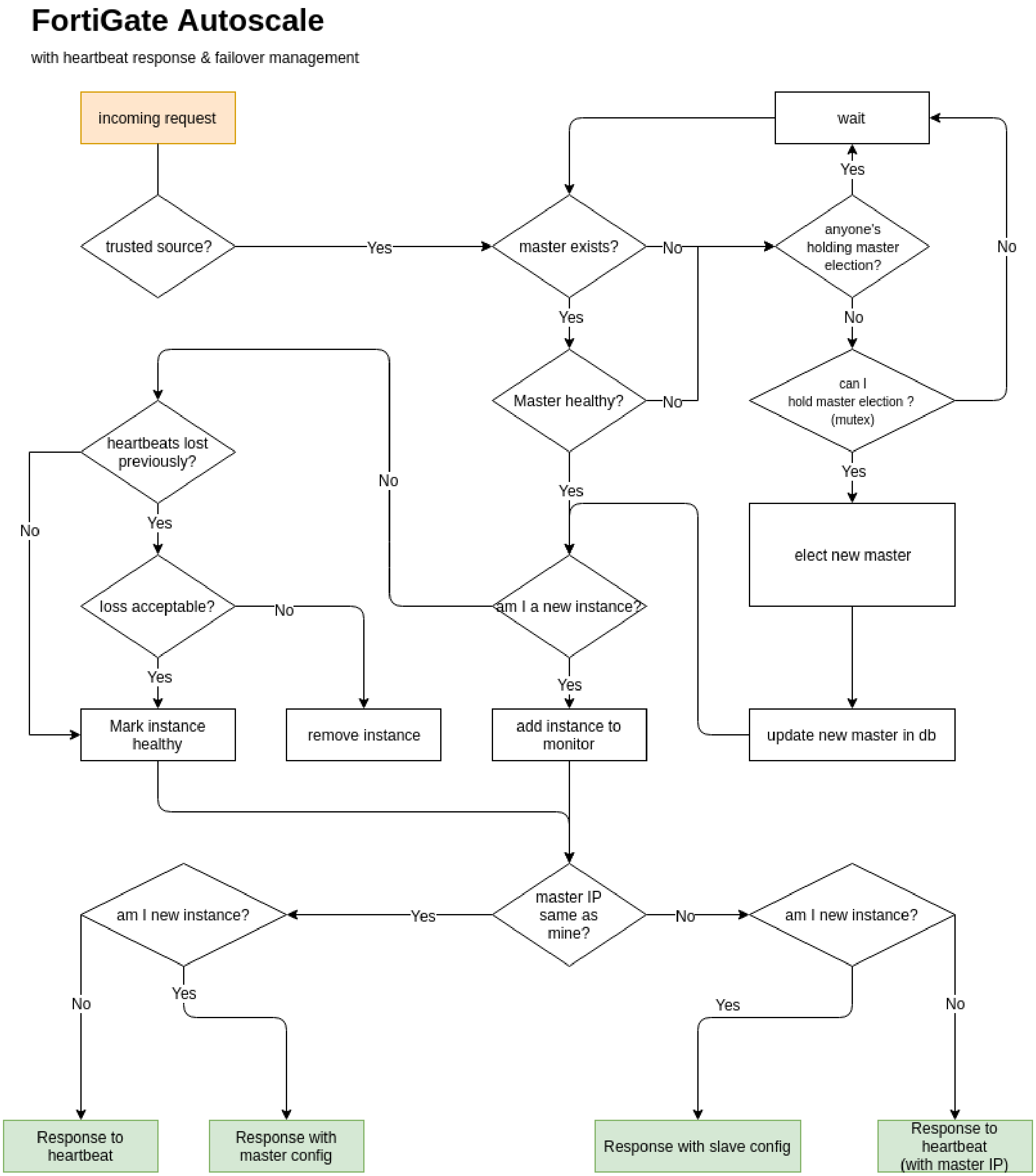
FortiGate Autoscale for Azure architecture (PAYG instances only)



Autoscale handler flowchart



Master election



Change Log

Date	Change Description
2018-10-12	Initial release.
2019-08-23	Updated "Deploying autoscaling on Azure" on page 4
2019-09-25	Revised to cover the 1.0.x template only.