FortiOS - Azure Administration Guide

Version 6.4

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 TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

August 25, 2021
FortiOS 6.4 Azure Administration Guide
01-640-615183-20210825

TABLE OF CONTENTS

Deploying autoscaling on Azure

You can deploy FortiGate virtual machines (VMs) to support autoscaling on Azure. Existing resources can be included when specified during the deployment. By integrating FortiAnalyzer, you can consolidate logging and reporting for your FortiGate cluster. Fortinet provides a FortiGate Autoscale for Azure deployment package to facilitate the deployment

Multiple FortiGate-VM instances form a Virtual Machine Scale Sets (VMSS) to provide highly efficient clustering at times of high workloads. FortiGate Autoscale for Azure incorporates one or more VMSS, network related components, and Azure Function App scripts. FortiGate-VM instances are scaled out automatically according to predefined workload levels. When a spike in traffic occurs, FortiGate instances are automatically added to the VMSS. 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 6.4.5 and supports any combination of On-Demand (PAYG) and Bring Your Own License (BYOL) instances.

FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5 can be incorporated into Fortinet FortiGate Autoscale to use extended features that include storing logs into FortiAnalyzer.

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 you begin

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 for Autoscale to interact with the different Azure services. The creation of the service principal may be done by a different Azure account.

The service principal requires *read* and *write* permissions which can be granted by adding the *Contributor* role to the service principal. In order to grant the service principal such permissions, the Azure account used to create the service principal requires the following permissions:

- *Microsoft.Authorization/roleAssignments/write* (to add role assignments)
- *Microsoft.Authorization/roleAssignments/delete* (to remove role assignments)

These permissions are included in the roles *User Access Administrator* and *Owner*. For details, refer to the Microsoft article Add or remove role assignments using Azure RBAC and the Azure portal.

Note the following items as you need them to deploy the Function App:

Item	Where to find it	Relevant FortiOS parameter
Application ID	You can find this item in Azure Active Directory > App registrations > (your app).	Service Principal App ID on page 16
Application secret	Only appears once. You cannot retrieve the application secret.	Service Principal App Secret on page 16
Object ID	Open the Azure CLI and enter the command `az ad sp show --id <the service principal client id>`. The object ID displayed may differ from the object ID displayed in Azure Active Directory > App registrations > (your-app). Use the value from the AzureCLI.	Service Principal Object ID on page 16

For details on the FortiOS parameters, see Configurable variables on page 12.

3. Confirm that you have a valid subscription to the PAYG and/or BYOL marketplace listings for FortiGate, as required for your deployment.

Without the valid subscriptions, the deployment will fail with errors.

Requirements when using an existing VNet

When using an existing VNet, ensure that the following FortiGate Autoscale for Azure requirements have been satisfied.

- IP address ranges in the VNets satisfy the Microsoft requirements listed in the article What address ranges can I use in my VNets?
- The VNet must contain 4 subnets.
  - The FortiGate VMSS will be deployed in one of the subnets. This subnet must:
    - be a clean subnet (i.e. is not used by any other resource.)
    - have two service endpoints that have been manually enabled, one for *Microsoft.AzureCosmosDB*, and one for *Microsoft.Web*.
    - should have its name specified in the *Subnet 1 Name on page 17* parameter.
  - The 3 other subnets will be protected by the FortiGate VMSS.
- Route tables have been created to route traffic between the FortiGate VMSS subnet and the other subnets.
- One network security group is associated with the 4 subnets in the VNet.
- (Optional) One available (i.e. not associated with any resource) public IP address to be used for the external load balancer that will be created during template deployment.
  - This IP address must be of the 'standard' SKU in order to match the VMSS.
  - This requirement is optional as a new IP address can be created during template deployment, as specified by the Frontend IP Deployment Method on page 14 parameter.
- All of the above components above reside in the same resource group.

Obtaining the deployment package

The FortiGate Autoscale for Azure deployment package is located in the Fortinet Autoscale for Azure GitHub project. Navigate to the project release page and download `fortigate-autoscale-azure.zip` for the latest version.

Unzip this file on your local PC. Extracted content used in the deployment is described below:

Extracted Item	Description
assets	This folder contains *configset* files which can be modified as needed to meet your network requirements. For details on the allowable modifications, refer to the bullet for *The Blob Containers* in the section Appendix > Major components on page 37. In the section Uploading files to the Storage account on page 18 these files are loaded as the initial configuration of a new FortiGate-VM instance.
templates	This folder contains. deployment templates. The files `deploy_fortigate_autoscale.hybrid_licensing.*` are used to deploy FortiGate Autoscale for Azure.

Extracted Item	Description
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 16*.

Deploying FortiGate Autoscale for Azure

Deploying FortiGate Autoscale for Azure involves Creating a template deployment on page 8 and Uploading files to the Storage account on page 18.

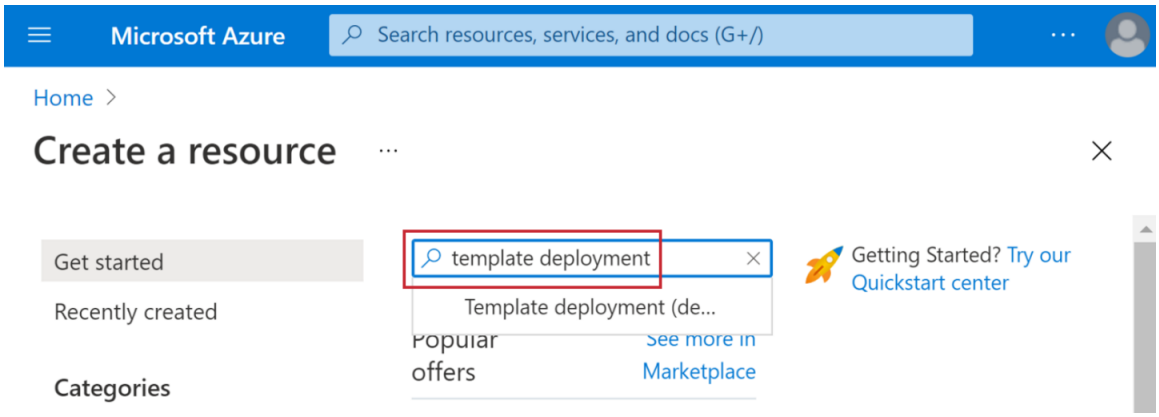
To deploy FortiGate Autoscale for Azure:

1. Create a template deployment using the template file `deploy_fortigate_autoscale.hybrid_licensing.json` and the parameter file `deploy_fortigate_autoscale.hybrid_licensing.params.json`.
2. Upload `configset` files to the Storage account.
3. If you will be using BYOL instances, upload `license` files to the Storage account.
4. Verify the deployment as described in the section Verifying the deployment on page 20.
5. Start the VMSS as described in the section Starting a VMSS on page 28.

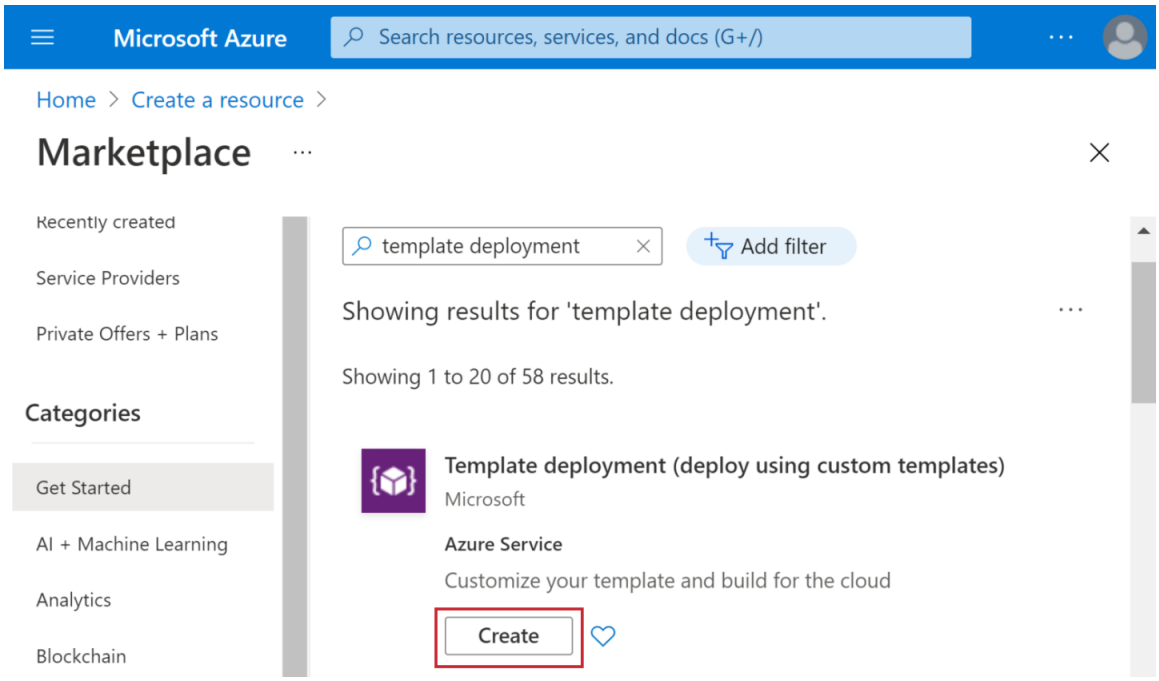
Creating a template deployment

To create a template deployment:

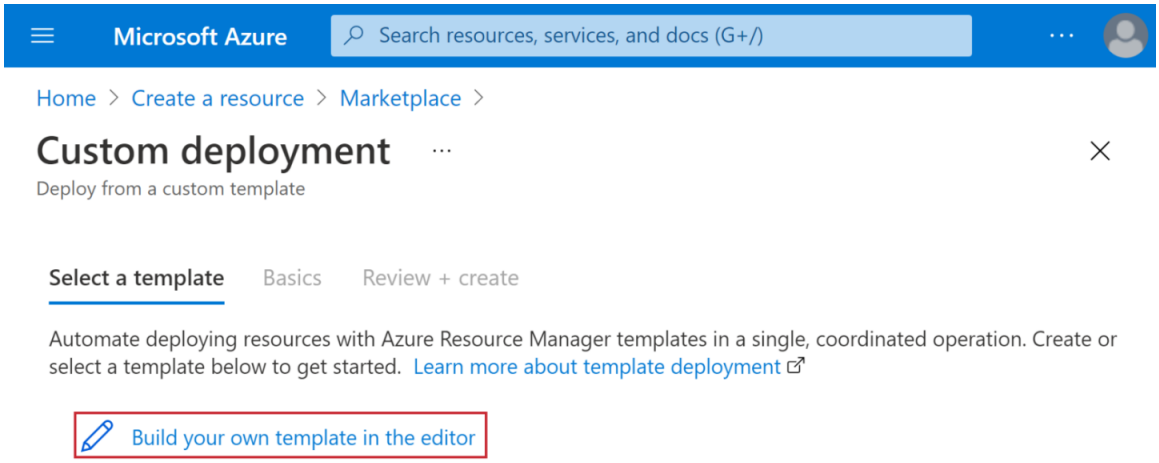
1. In the Azure portal, select *Create a resource* and search for "Template deployment".



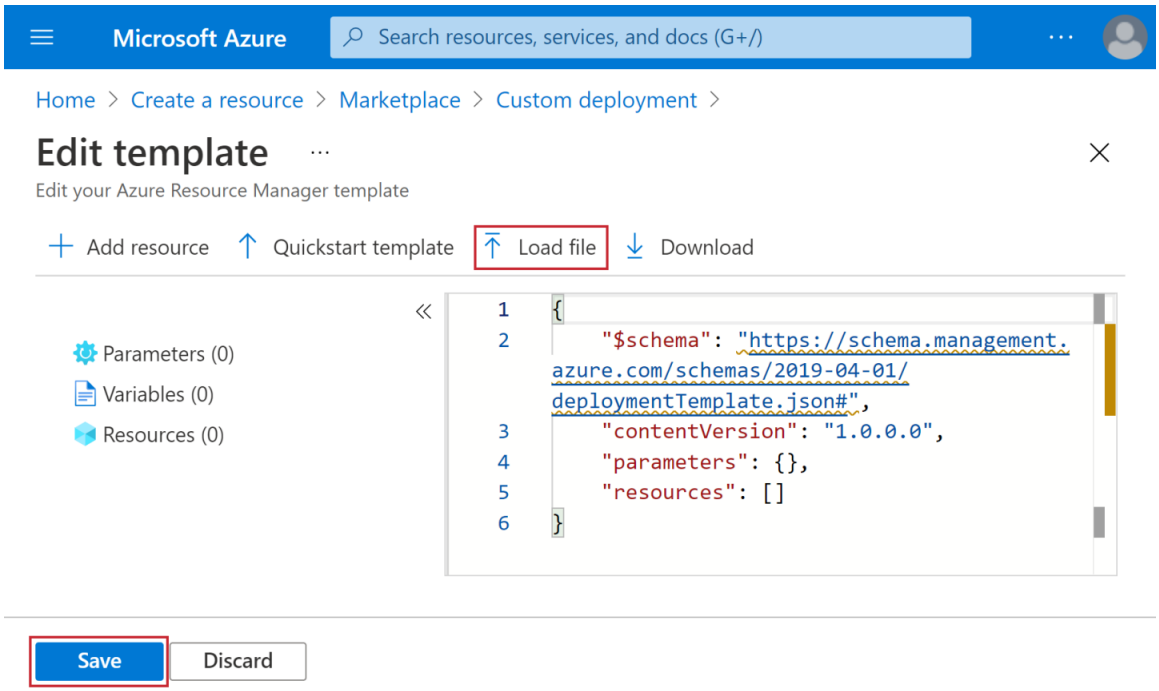
2. Click *Create*.



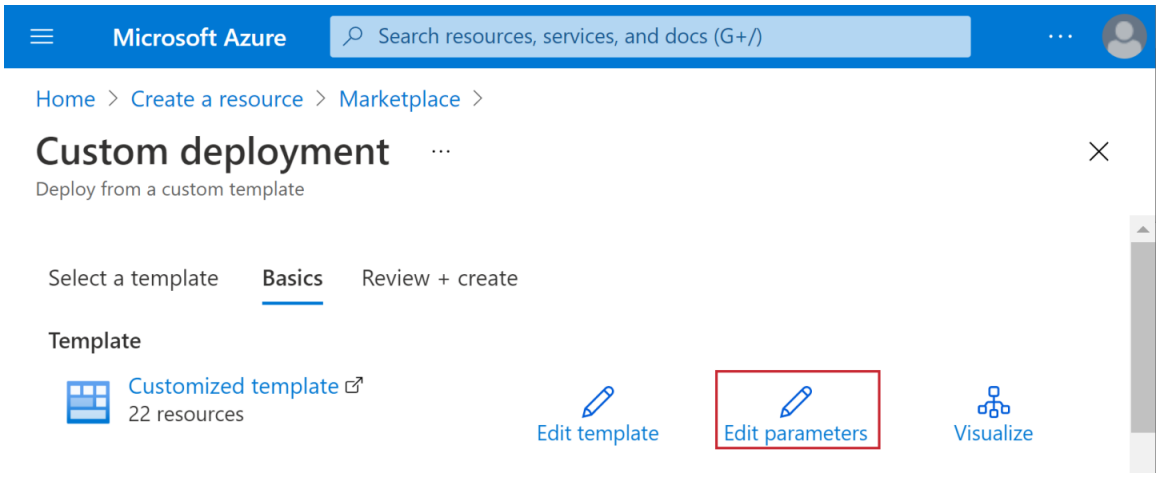
3. Click *Build your own template in the editor*.



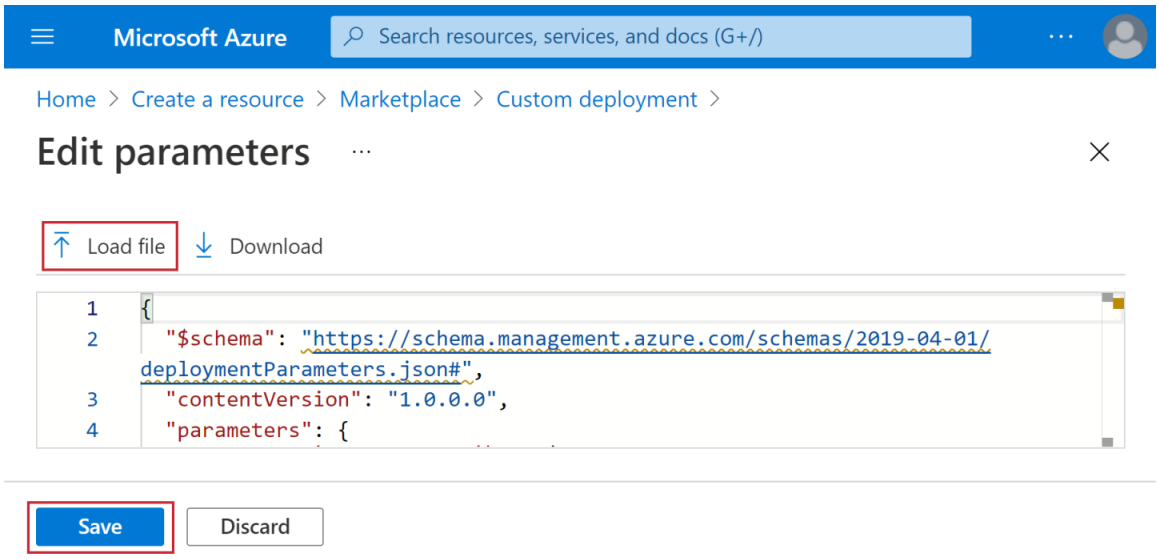
4. Click *Load file* to load the provided template file; then click *Save*.



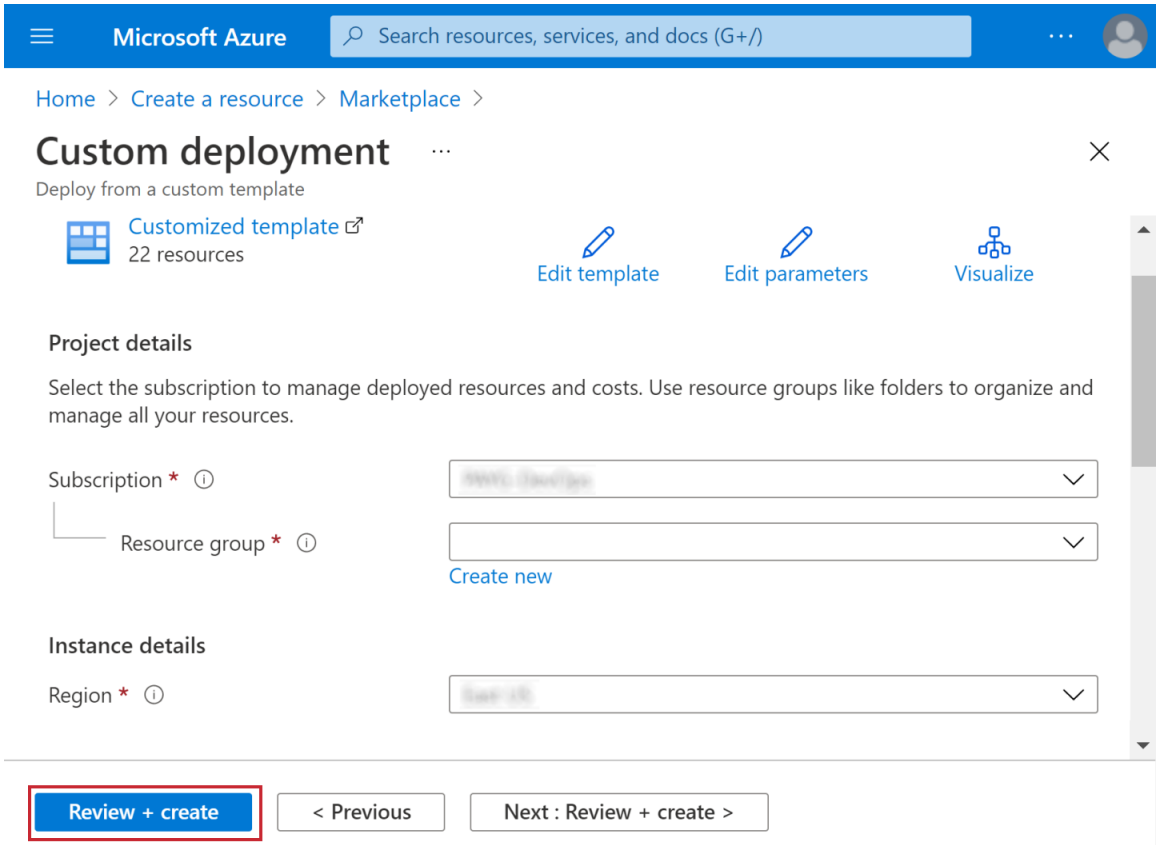
5. (Optional) In the *Custom deployment* screen, click *Edit parameters*.



Click *Load file* to load a predefined `.params.json` file; then click *Save*.



6. Review and update parameters; then click *Review + create*.



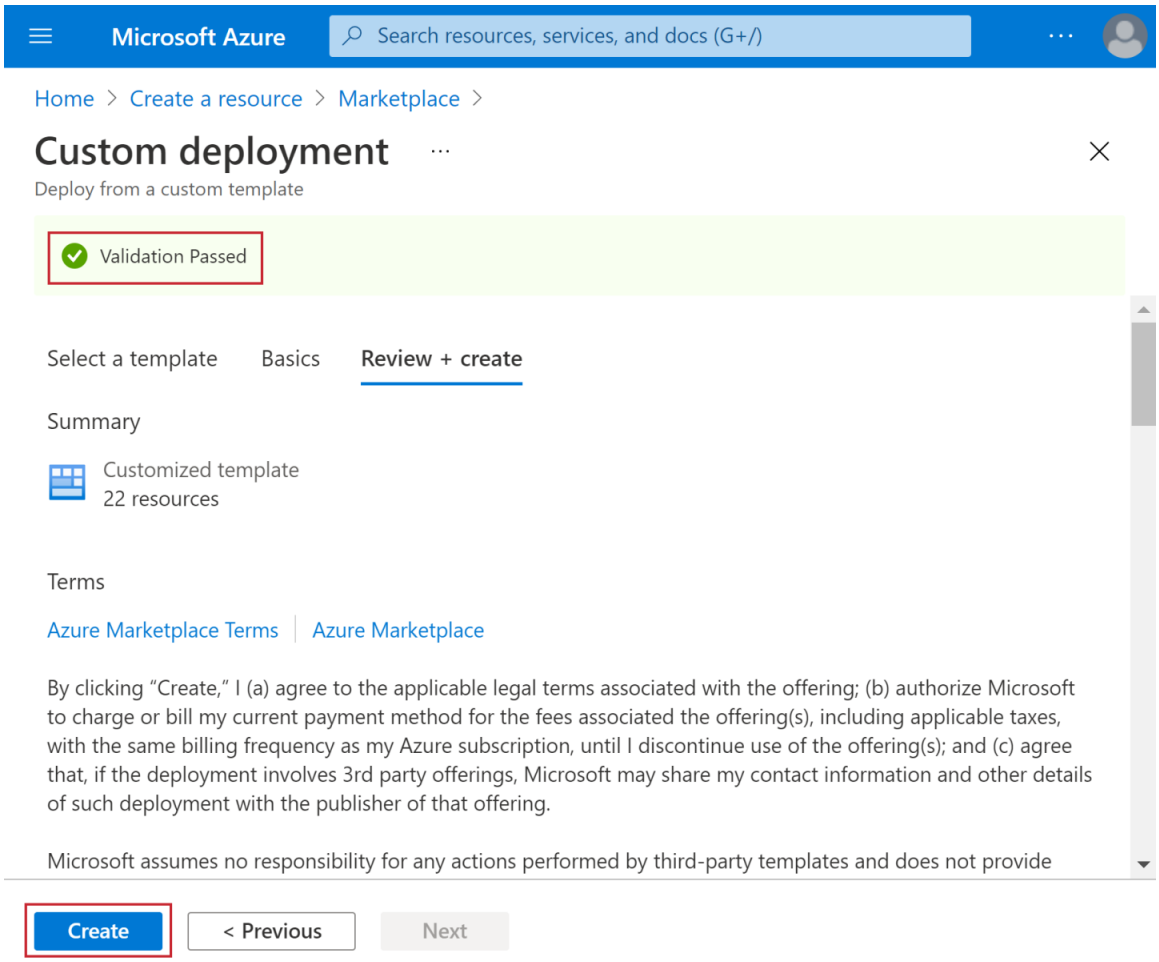
Project details are described as follows:

- *Subscription*: The Azure subscription FortiGate Autoscale for Azure will be deployed in.
- *Resource group*: The resource group FortiGate Autoscale for Azure will be deployed in. In the section Configurable variables on page 12, this will be referred to as the *Autoscale resource group*.

Parameters under *Instance details* are described in the section Configurable variables on page 12.

7. If parameter validation has not passed, click *Previous* and make the necessary corrections.

8. Review the Azure Marketplace Terms, optionally review the parameters again, and click *Create*.



Configurable variables

Following is a list of variables used during deployment and referenced throughout this guide.

Parameter name	Default value	Description
Region	Requires input	The region in which the FortiGate Autoscale for Azure resources will be deployed in. Not every resource is available in every region.

Parameter name	Default value	Description
Access Restriction IP Range	Requires input	Specify IP ranges (single IPv4 address or Classless Inter-Domain Routing (CIDR) range) to allow access from the Internet or from your on-premises network to the CosmosDB and Function App. Specify at least one entry for security purposes. For multiple entries, each entry must be separated by a comma and no trailing comma is allowed.  0.0.0.0/0 accepts connections from any IP address. We recommend that you use a constrained CIDR range to reduce the potential of inbound attacks from unknown IP addresses.
Admin Password	Requires input	FortiGate administrator password on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled. 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 (! @ # $ %).
Admin Username	azureadmin	FortiGate administrator username on all VMs as well as the FortiAnalyzer if FortiAnalyzer integration is enabled.
BYOL Instance Count	2	The number of FortiGate instances the BYOL VMSS should have at any time. For High Availability in BYOL-only and Hybrid use cases, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing.  Users can set the size to less than or equal to the number of valid licenses they own and the number should not exceed the *Max BYOL Instance Count*. Licenses can be purchased from FortiCare.
FortiAnalyzer Autoscale Admin Password	Requires input	Password for the FortiAnalyzer Autoscale Admin Username on page 13. The password must conform to the FortiAnalyzer password policy and have a minimum length of 8 and a maximum length of 128. If you need to enable KMS encryption, refer to the documentation.
FortiAnalyzer Autoscale Admin Username	Requires input	The name of the secondary administrator-level account in the FortiAnalyzer, which FortiGate Autoscale uses to connect to the FortiAnalyzer to authorize any FortiGate device in the Auto Scaling group. To conform to the FortiAnalyzer naming policy, the user name can only contain numbers, lowercase letters, uppercase letters, and hyphens. It cannot start or end with a hyphen (-).
FortiAnalyzer Custom Private IP Address	Requires input	The custom private IP address to be used by the FortiAnalyzer. Must be within the Public subnet 1 CIDR range. Required if FortiAnalyzer Integration Options on page 14 is set to 'yes'. If FortiAnalyzer Integration Options on page 14 is set to 'no', any input will be ignored.
FortiAnalyzer Instance Type	Requires input	Size of the FortiAnalyzer-VM.

Parameter name	Default value	Description
		 Not all instance types are supported. Review FortiAnalyzer instance type support prior to selecting an instance.
FortiAnalyzer Integration Options	yes	Choose 'yes' to incorporate FortiAnalyzer into FortiGate Autoscale for Azureto use extended features that include storing logs into FortiAnalyzer.
FortiAnalyzer Version	6.4.5	FortiAnalyzer version supported by FortiGate Autoscale for Azure.
FortiGate PSK Secret	Requires input	The secret key used by FortiGate instances to securely communicate with each other. Must contain numbers and letters and may contain special characters. Maximum length is 128.
		 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.
FOS Version	6.4.5	FortiOS version supported by FortiGate Autoscale for Azure.
Frontend IP Deployment Method	create new public IP address	Deployment method for the Frontend Public IP address for the external load balancer. If set to 'create new public IP address', the IP address will be deployed to the resource group where the VNet is located. If set to 'use existing public IP address', the existing IP address must reside in the same resource group as the VNet and it must be of the 'standard' SKU in order to match the VMSS. Please refer to the section Requirements when using an existing VNet on page 6.
Frontend IP Name	Requires input	Name of the Frontend Public IP address. When the Frontend IP Deployment Method on page 14 parameter is set to 'create new public IP address', this parameter can be left empty and a name will be generated.
Heart Beat Delay Allowance	30	The maximum amount of time (in seconds) allowed for network latency of the FortiGate heartbeat arriving at the Autoscale handler function. Minimum is 30.
Heart Beat Interval	60	The length of time (in seconds) that the FortiGate waits between sending heartbeat requests to the Autoscale handler function. Minimum is 30. Maximum is 120.
Heart Beat Loss Count	3	Number of consecutively lost heartbeats. When the Heart Beat Loss Count has been reached, the VM is deemed unhealthy and failover activities will commence.
Instance Type	Standard_F4	Size of the VMs in the VMSS. For assistance in choosing the size, refer to the Microsoft article Compute optimized virtual machine sizes.

Parameter name	Default value	Description
Key Vault Name	Requires input	Name of the Key Vault to be used by FortiGate Autoscale. This parameter can be left empty and a name will be generated. If specified, the name must be globally unique and not belong to a Key Vault in the soft deleted state.
Load Balancer IP	10	The last octet of the Frontend Private IP address to be used by the Load Balancer. For example, if set to 10, the Private IP address for the Load Balancer in the subnet with prefix 10.0.1.0/24 would be 10.0.1.10.
Max BYOL Instance Count	2	Maximum number of FortiGate instances in the BYOL VMSS. Maximum number of FortiGate instances in the BYOL VMSS. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing. This number must be greater than or equal to the Min BYOL Instance Count on page 15.  Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.
Max PAYG Instance Count	6	Maximum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing. This number must be greater than or equal to the Min PAYG Instance Count on page 15.
Min BYOL Instance Count	2	Minimum number of FortiGate instances in the BYOL VMSS. For specific use cases, set to 0 for PAYG-only, and >= 2 for BYOL-only or hybrid licensing.  For BYOL-only and hybrid licensing deployments, this parameter must be at least 2. If set to 1 and the instance fails to work, the current FortiGate configuration will be lost.
Min PAYG Instance Count	0	Minimum number of FortiGate instances in the PAYG VMSS. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing.  For PAYG-only deployments, this parameter must be at least 2. If it is set to 1 and the instance fails to work, the current FortiGate configuration will be lost.
Network Security Group Name	Conditionally requires input	Name of the Network Security Group associated with the subnets in the VNet. Required when using an existing VNet. The value should match the name of the existing Network Security Group associated with the subnets in the VNet. When creating a new VNet, you may specify a name for the Network Security Group. If left empty, a name will be generated.

Parameter name	Default value	Description
PAYG Instance Count	0	The number of FortiGate instances the PAYG VMSS should have at any time. For High Availability in a PAYG-only use case, ensure at least 2 FortiGates are in the group. For specific use cases, set to 0 for BYOL-only, >= 2 for PAYG-only, and >= 0 for hybrid licensing.
Package Res URL	Requires input	The public URL of the function source file named `fortigate-autoscale-azure-funcapp.zip`, and can be found inside `fortigate-autoscale-azure.zip`. The public URL of the deployment package zip file that contains the resource used to deploy the Function App. The default URL points to the GitHub release corresponding to this ARM template contentVersion.  This URL must be accessible by Azure.
Primary Election Timeout	90	The maximum time (in seconds) to wait for the election of the primary instance to complete.
Resource Name Prefix	Requires input	The prefix for all applicable resource names. Can only contain lowercase letters and numbers. Maximum length is 10.
Scale In Threshold	20	Percentage of CPU utilization at which scale-in should occur.
Scale Out Threshold	80	Percentage of CPU utilization at which scale-out should occur.
Service Plan Tier	Premium (P1V2)	The pricing tier for the function service plan.  The Free plan is for trial and demo only. Do not use it in a production environment.
Service Principal App ID	Requires input	*Application ID* for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 5.
Service Principal App Secret	Requires input	Password (*Authentication key*) for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 5.
Service Principal Object ID	Requires input	*Object ID* for the Registered app used as the Autoscale Function App API request service principal. This is the value that was noted when creating a service principal in the section Prerequisites on page 5.
Storage Account Type	Standard_LRS	Storage account type.

Parameter name	Default value	Description
Subnet 1 Name	Conditionally requires input	The *Subnet # Name* parameters specify the name of the subnet. • *Subnet 1* is the subnet in which to deploy the FortiGate VMSS. • *Subnets 2-4* are the subnets to be protected by the FortiGate.  Required when using an existing VNet. Values should match the subnet of the target VNet. When creating a new VNet, any input value will be ignored.
Subnet 2 Name	Conditionally requires input	
Subnet 3 Name	Conditionally requires input	
Subnet 4 Name	Conditionally requires input	
Subnet 1 Address Range	10.0.0.0/24	The *Subnet # Address Range* parameters define the address range for the subnet, in CIDR notation. The address range must be contained by the address space of the virtual network as defined in VNet Address Space on page 17. After deployment, the address range of a subnet which is in use can't be edited.  Required when using an existing VNet. Values should match the address range of the target VNet. When creating a new VNet, any input value will be ignored.
Subnet 2 Address Range	10.0.1.0/24	
Subnet 3 Address Range	10.0.2.0/24	
Subnet 4 Address Range	10.0.3.0/24	
VNet Address Space	10.0.0.0/16	IP address space of the VNet in CIDR notation. E.g. 10.0.0.0/16. Required when using an existing VNet; the value should match the address space of the target VNet.
VNet Deployment Method	create new	Options for Virtual Network (VNet) deployment: • create new • use existing  The VNet resource group (specified in the VNet Resource Group Name on page 17 parameter) must be in the same region as the Autoscale resource group (specified in the *Resource group* parameter). If using an existing VNet, refer to the section Requirements when using an existing VNet on page 6.
VNet Name	Conditionally requires input	Name of the Azure VNet to connect to FortiGate Autoscale. Required when using an existing VNet. When creating a new VNet, this parameter can be left empty and a name will be generated.
VNet Resource Group Name	Conditionally requires input	Name of the resource group that contains the VNet and related network components.

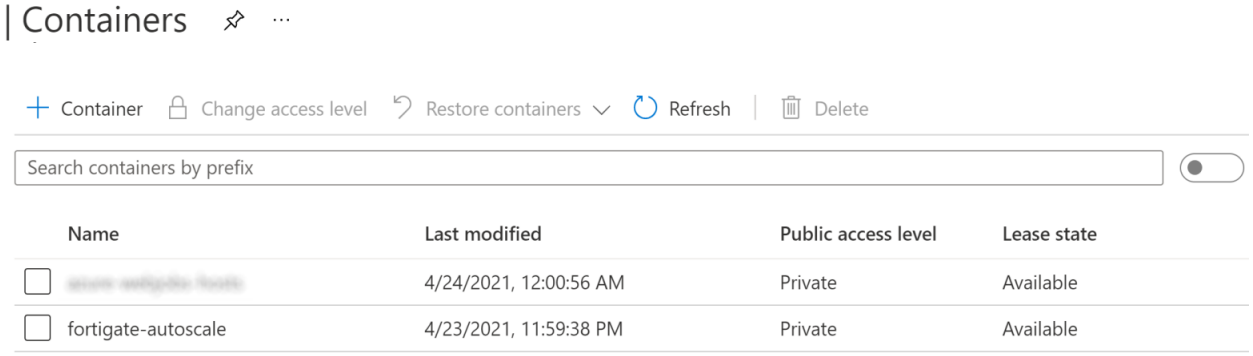
Parameter name	Default value	Description
		Required if the VNet is not in the Autoscale resource group (specified in the parameter *Resource group*). If not specified, the Autoscale resource group will be used. For details, refer to the description for the parameter VNet Deployment Method on page 17. This resource group must be in the same region as the Autoscale resource group.

Uploading files to the Storage account

The template deployment will create the storage container `fortigate-autoscale` in the resource group you selected or created in step 6 of the section Creating a template deployment on page 8.

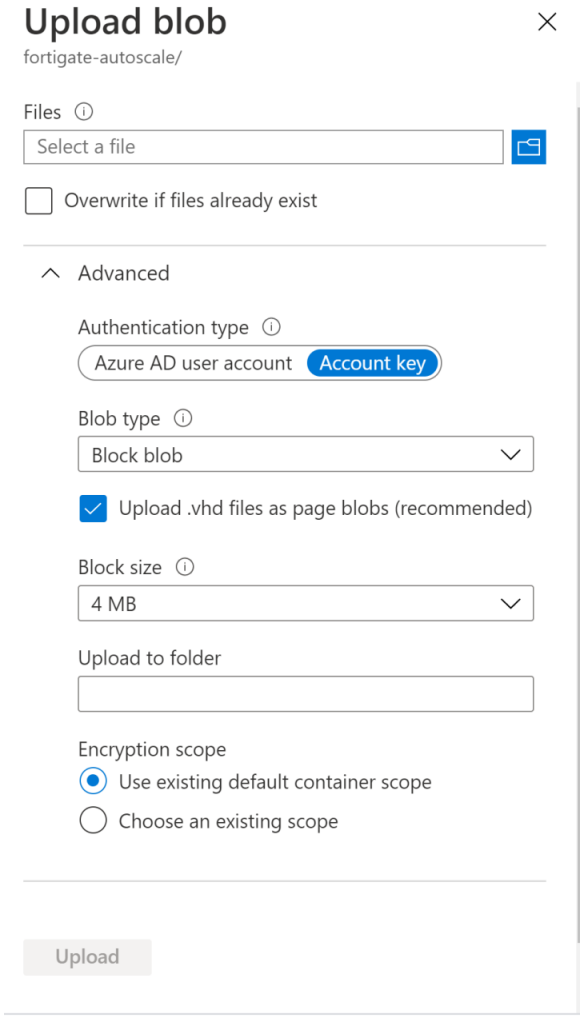
To upload files to the storage container:

1. From the Resource group, load the Storage account by clicking its name.
2. From the Storage account navigation column, under *Data storage*, click *Containers*. The `fortigate-autoscale` container will be listed.



3. Click the `fortigate-autoscale` container.
4. Click *Upload*.

5. In the *Upload blob*, click *Advanced* to display more options.



6. Specify the folder to upload to in *Upload to folder*:
   - For *configset* files, enter `assets/configset`.
   - For *license* files, enter `assets/license-files/fortigate`.
7. Select a file or files to upload:
   - For *configset* files, select all the files in the *configset* folder of the deployment package.
   - For *license* files, select your BYOL license file(s).

   If you provide two license files with the same content, only one of them will be used, the other one will be ignored.

   If you upload a file with the same name but different content, there are two outcomes:
   - If the old license has not been distributed, the new file completely replaces the old one
   - If the old license has been distributed, the new file is treated as a new license. The old license is still valid, but it cannot be redistributed in the future.
8. Click *Upload*.

Verifying the deployment

FortiGate Autoscale for Azure deploys the following components:

- 1 Public Load balancer
  - This load balancer will be associated with the FortiGate subnet and the Frontend Public IP address to receive inbound traffic.
- 1 Internal Load balancer
  - This load balancer will be associated with all 4 subnets.
- 1 Network security group (associated with all 4 subnets)
- 1 Virtual machine scale set for BYOL
- 1 Virtual machine scale set for PAYG
- 1 Virtual machine for FortiAnalyzer (only if deployed with FortiAnalyzer integration)
- 1 Virtual network
- 1 Public IP address
- 3 Route tables
- 1 Azure Cosmos DB account
- 1 Function App
- 1 Application Insights (automatically enabled if your region supports it)
- 1 App Service plan
- 2 Disk components for use by FortiAnalyzer (only if deployed with FortiAnalyzer integration)
- 1 Key vault
- 1 Storage account

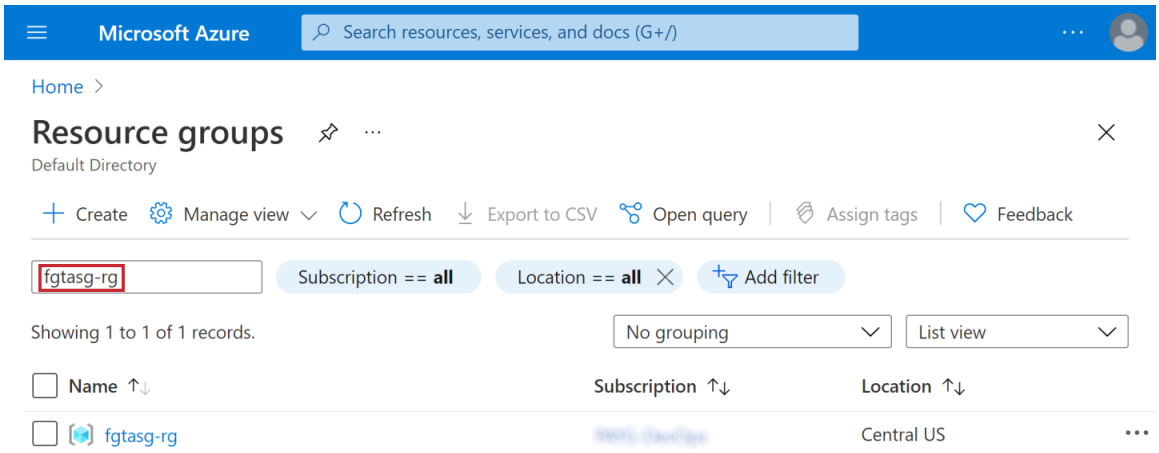
For deployments that have two resource groups, the network related components are deployed to the VNet resource group and the DB, Storage account, and Function App related components are deployed to the Autoscale resource group.

FortiGate Autoscale for Azure is fully deployed once you verify the following components:

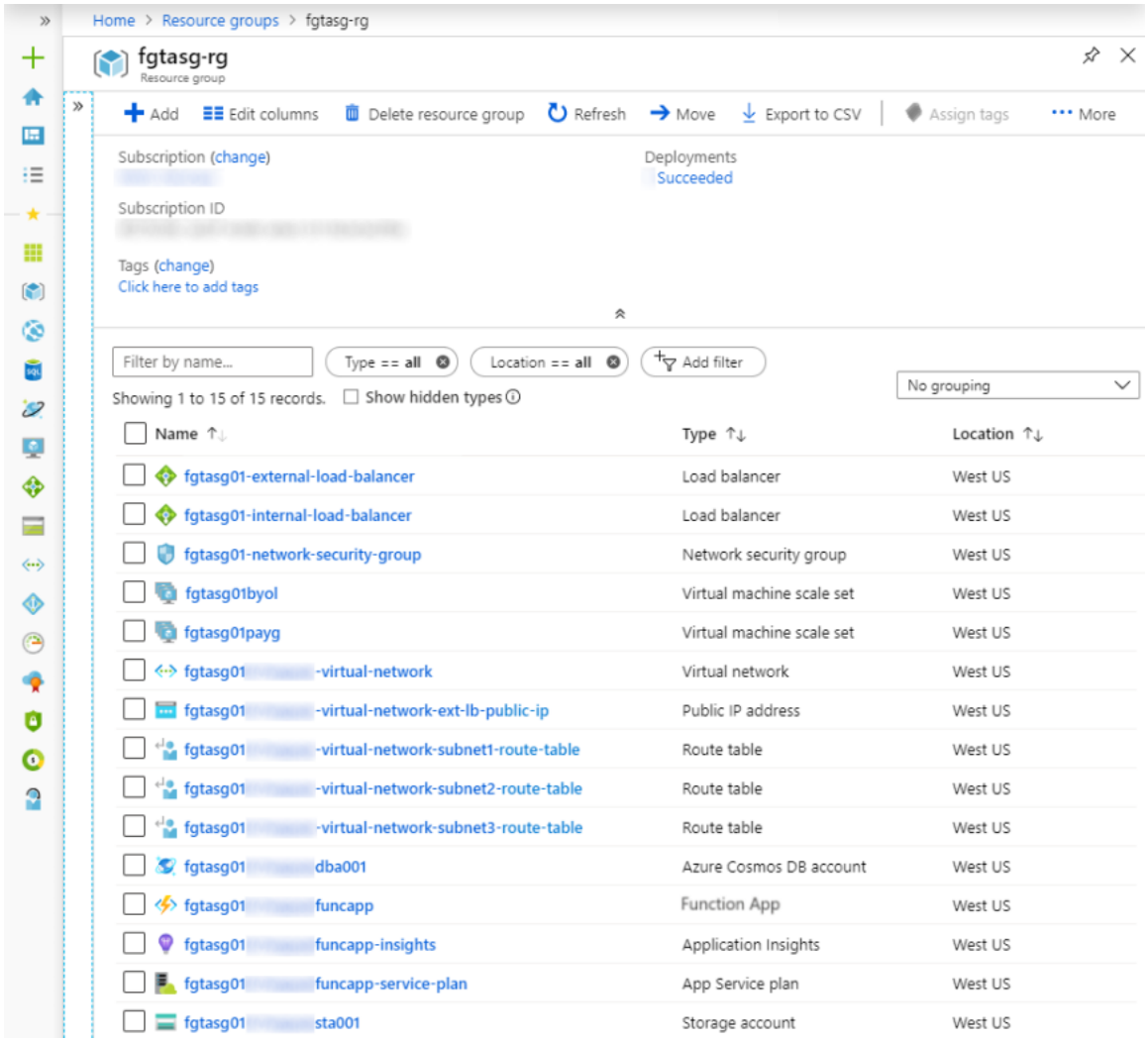
- the Function App
- the database
- the primary election

To load a resource group:

1. In the Azure console, from the left navigation column, select *Resource groups*.
2. Locate the resource group you wish to load by scrolling through the list or by using one or more of the name, subscription, and location filters. In the example below, this is *fgtasg-rg*.

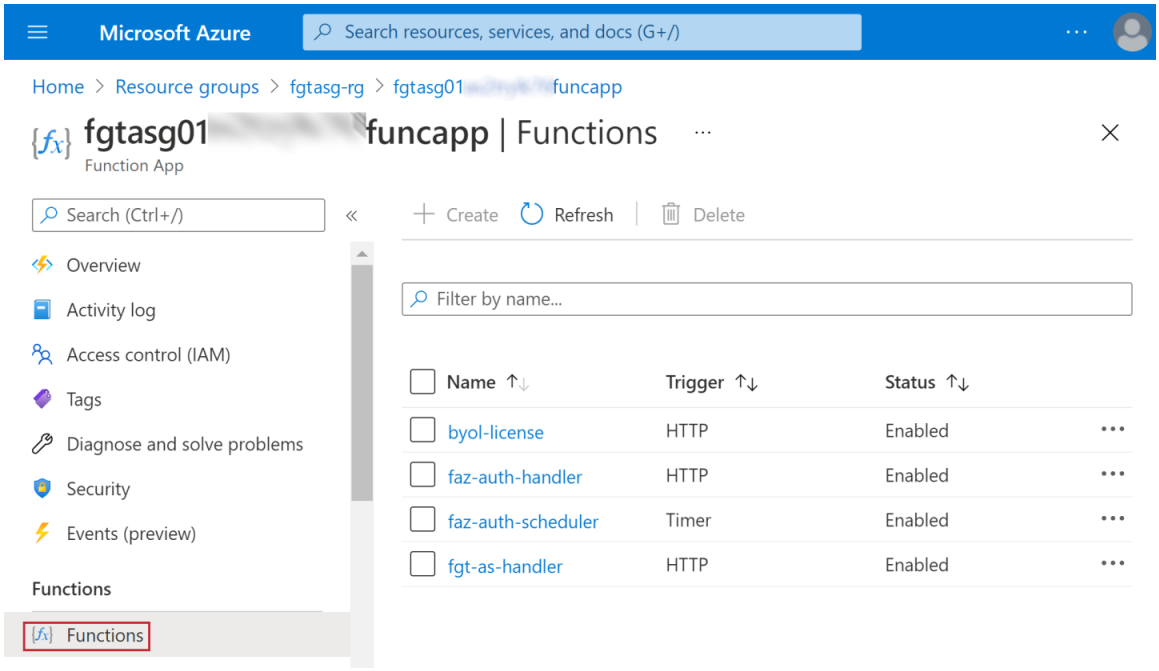


3. Click the name to load the resource group *Overview* page. In the example deployment, the VNet resource group is the same as the Autoscale resource group.



To verify the Function App:

1. From the Autoscale resource group *Overview* page, load the Function App by clicking the name of the item of type *Function App*.
2. From the navigation column, select *Functions*.



You should see four functions on the right:

- *byol-license*: The function to distribute BYOL licenses.
- *faz-auth-handler*: The function to handle authorization of FortiGate in the FortiAnalyzer.
- *faz-auth-scheduler*: The function to handle authorization of FortiGate in the FortiAnalyzer on a timely basis.
- *fgt-as-handler*: The main autoscaling function.

To verify the database:

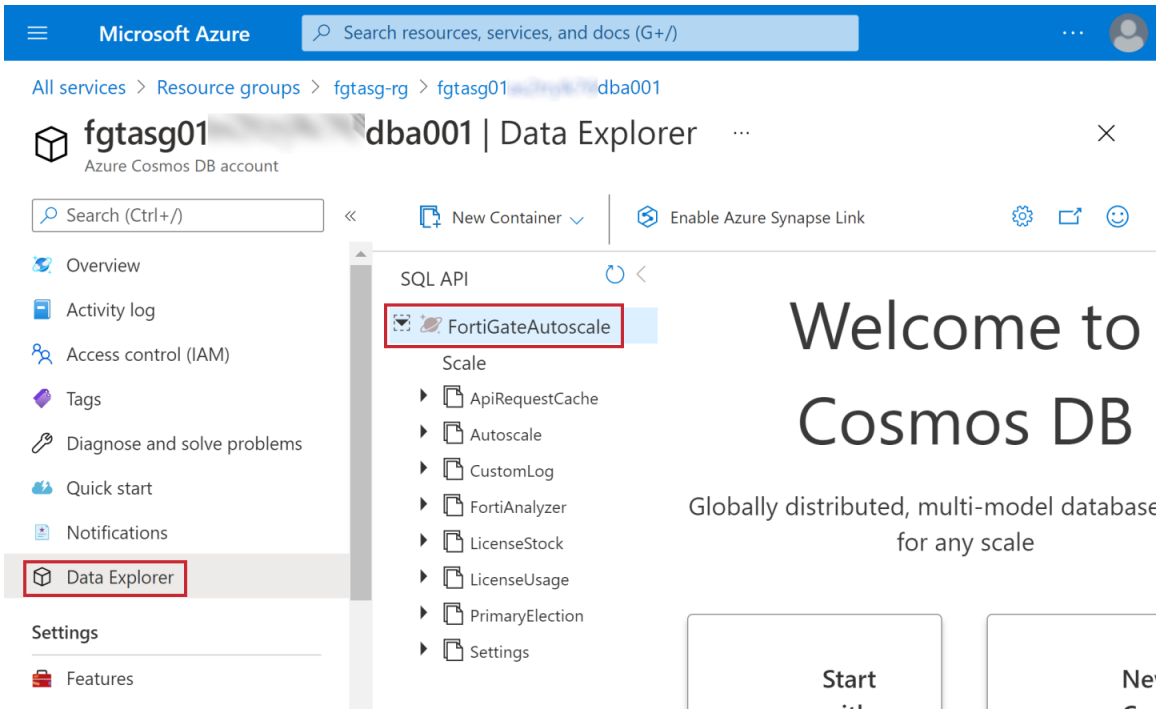
1. From the Autoscale resource group *Overview* page, click the *Azure Cosmos DB account* name.
2. From the navigation column, click *Data Explorer*.
3. Expand the database *FortiGateAutoscale*.

You will see the following database and tables:

- *Database:* FortiGateAutoscale
- *Tables:*
  - ApiRequestCache
  - Autoscale
  - CustomLog
  - FortiAnalyzer
  - LicenseStock
  - LicenseUsage

- PrimaryElection
- Settings

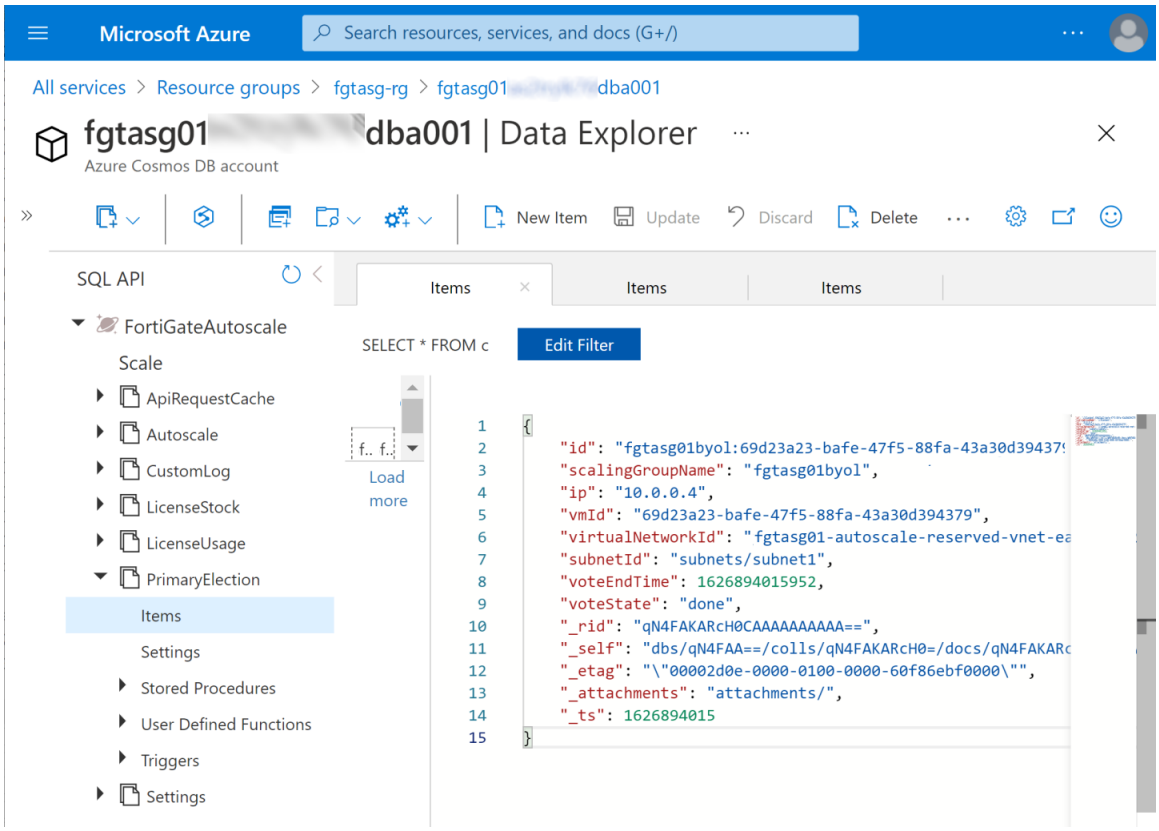
The database *Data Explorer* page will look as shown below:



To verify the primary election:

The elected primary FortiGate-VM will be logged in the CosmosDB *FortiGateAutoscale* in the table *FortiGatePrimaryElection*.

1. Expand the *FortiGatePrimaryElection* table and click on *Items*.
2. There will be one item in the table, select it.



- *id* is the unique identifier of a database record.
- *scalingGroupName* is the name of the Scale Set in which the primary FortiGate-VM is located.
- *ip* is the primary private IP address of the current primary FortiGate-VM.
- *vmId* is the index of the FortiGate-VM in the Scale Set.
- *virtualNetworkID* is the ID of the Virtual Network in which the primary FortiGate-VM instance is located.
- *subnetId* is the ID of the subnet in which the primary FortiGate-VM is located.
- *voteEndTime* is the Unix time stamp for when this primary election should expire if the vote state cannot change to *done* by this time.
- *voteState* is the state of the voting process.
  - *pending*: election of the primary instance is still in progress. You should wait for its completion. At this point in time, the final primary instance is not yet known.
  - *done*: the primary election process has completed.

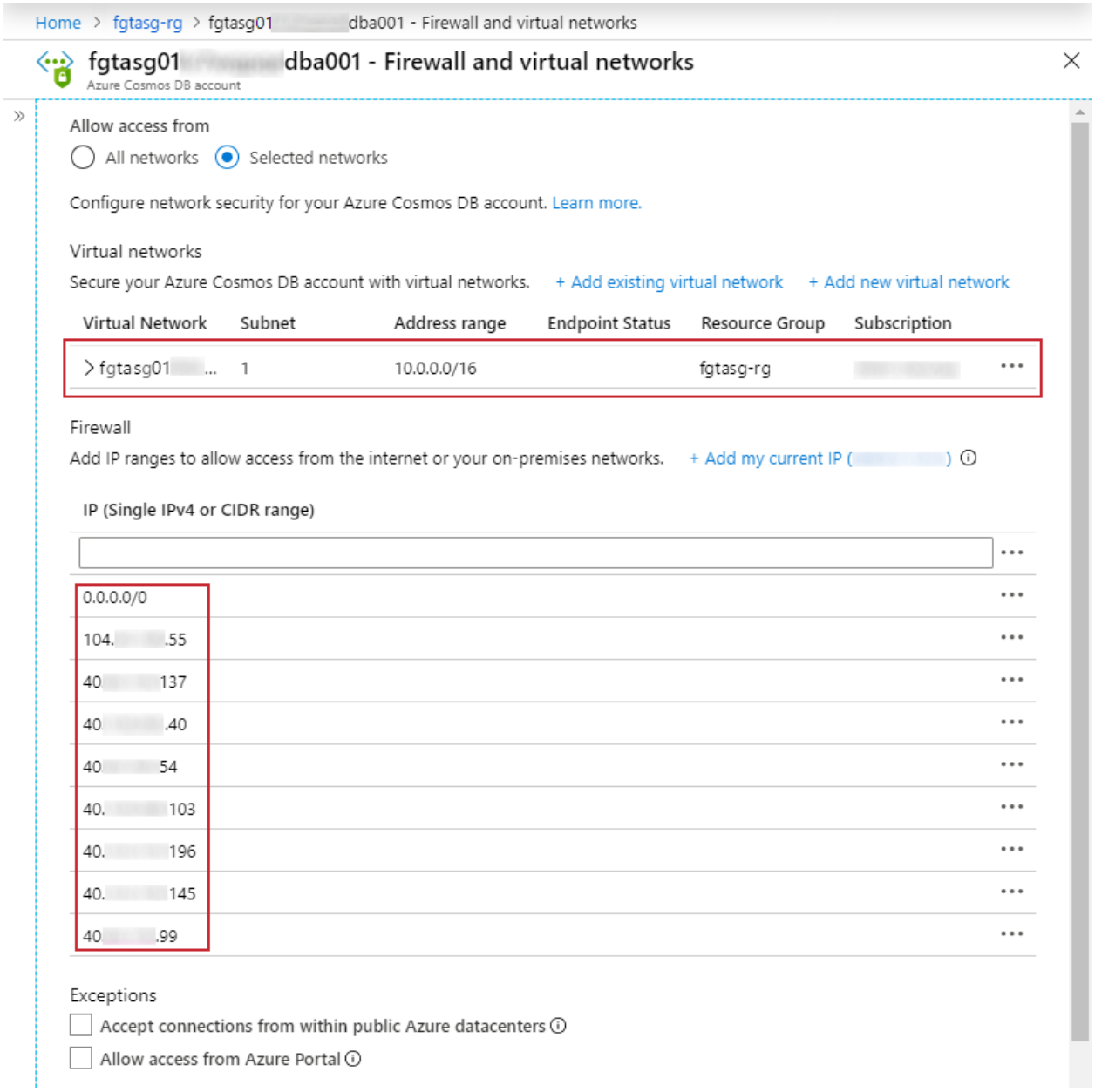
Security features for network communication

Security features are automatically enabled and configured as described in the following sections.

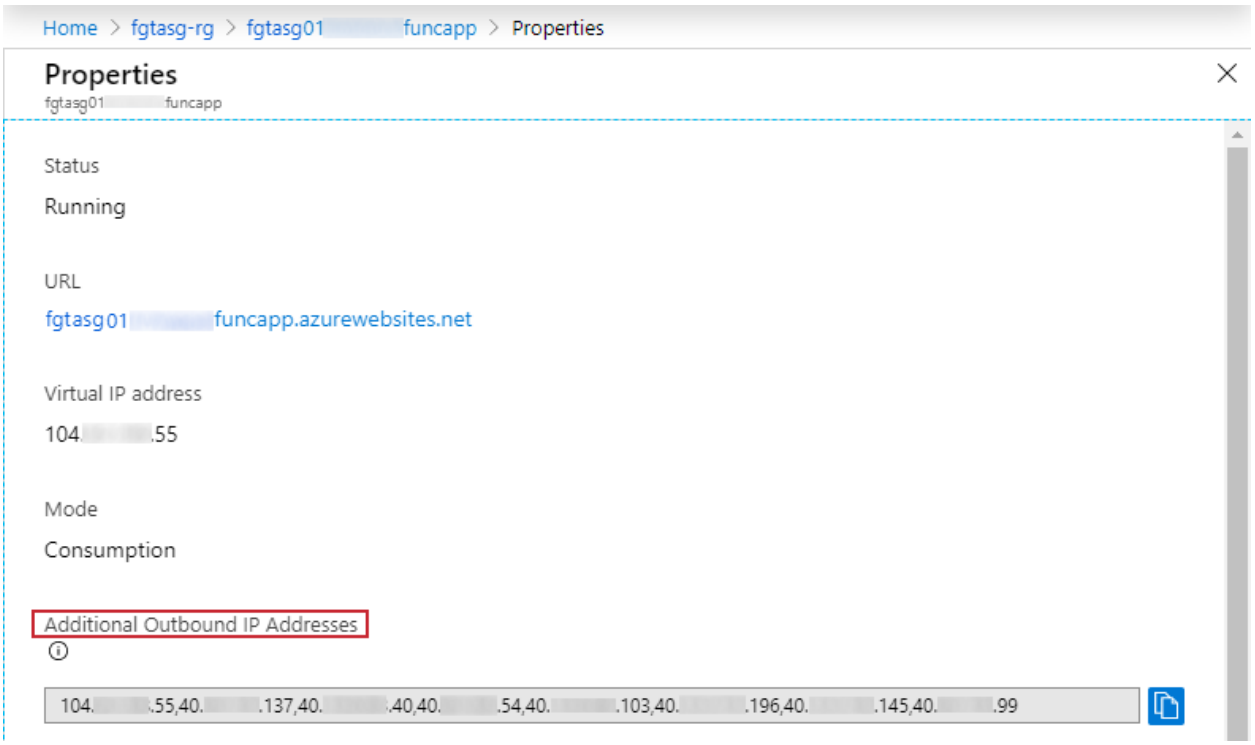
Database

Firewalls are set for IP address ranges and the VNet. The firewall only allow interactions with the DB tables from the FortiGate subnet, Function App additional outbound IP addresses, and user-defined IPv4 IP ranges.

To view the firewalls, load the Cosmos DB. From the *Settings* section of the left navigation tree, click *Networking* and then click *Firewall and virtual networks*.



The IP addresses listed in the Firewall section include the set of all possible Function App outbound IP addresses as obtained from the *Additional Outbound IP Addresses* field of the Function App *Properties*. To view these IP addresses, load the Function App, click the *Platform features* tab and then click *Properties*. Each IP address in the list has been added as an entry in the Cosmos DB firewall.

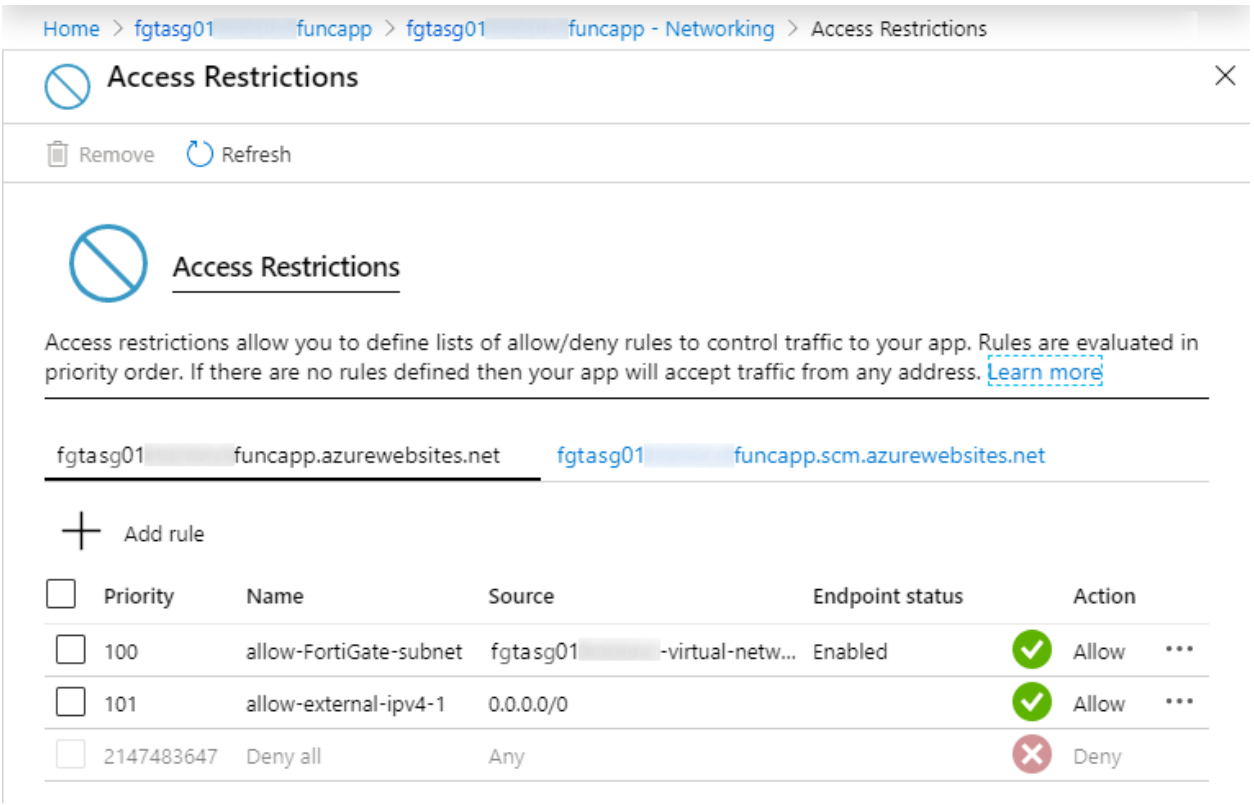


If Function App *Additional Outbound IP Addresses* change, the Cosmos DB firewall must be manually updated so that each IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked. For details on when Function App outbound IP addresses change, refer to the Microsoft article When outbound IPs change.

Function App

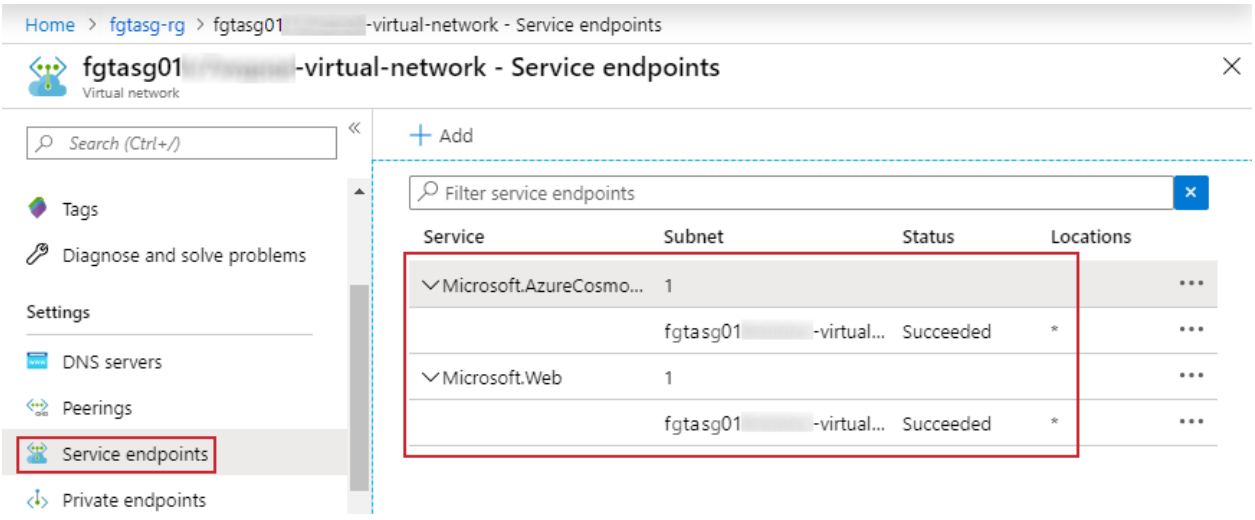
Requests are restricted by source. Incoming requests are only allowed from the FortiGate subnet and from user-defined IPv4 IP ranges.

To view *Access Restrictions*, load the Function App. In the right hand pane, click the *Platform features* tab and then click *All settings*. From the *Settings* section of the left navigation tree, click *Networking* and then click *Configure Access Restrictions*.



Virtual Network

The service endpoints for Azure services are enabled. Service endpoints should be enabled for the minimum number of Azure services required for Autoscale.



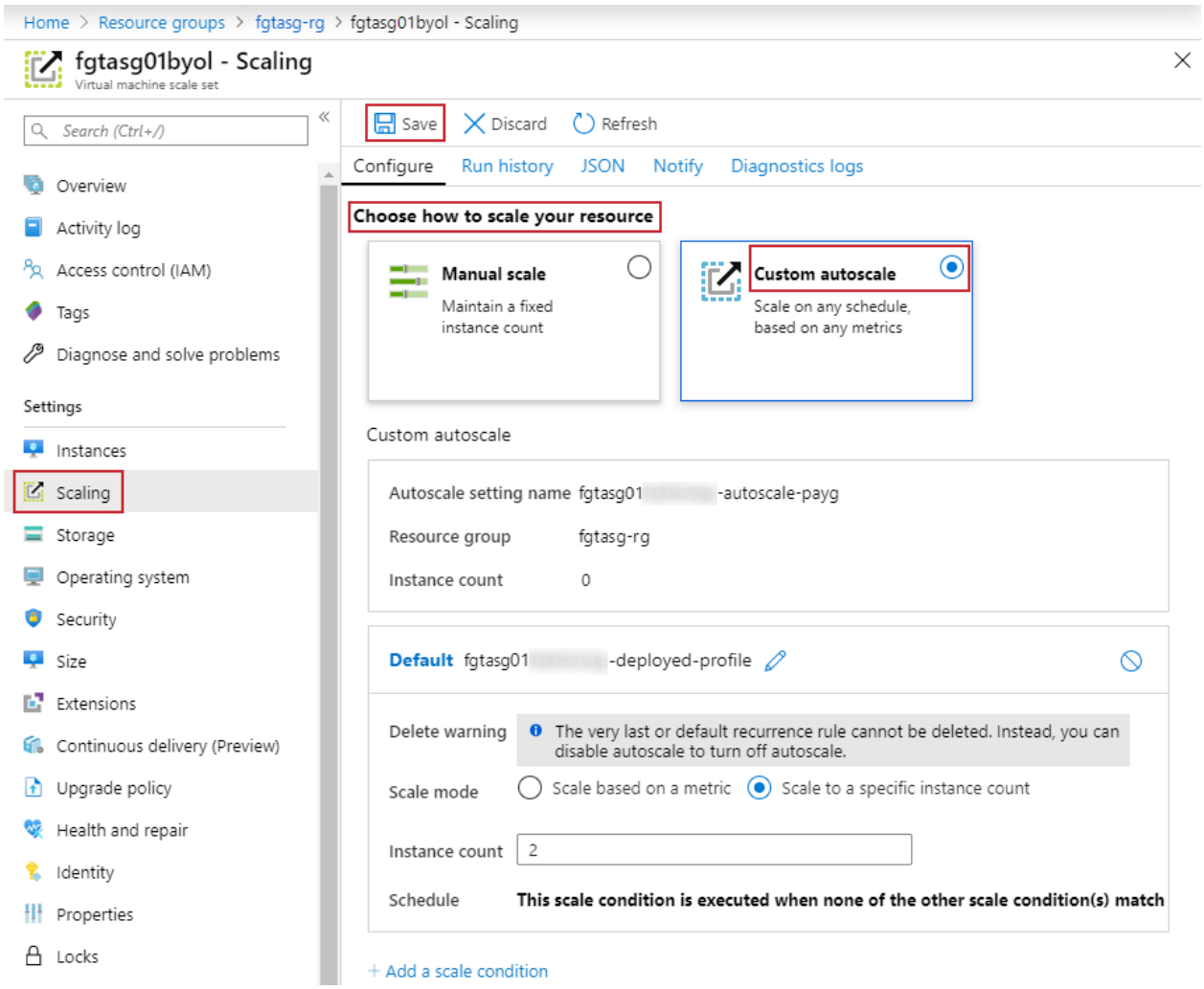
Starting a VMSS

Your deployment will have two Virtual machine scale sets (VMSS), one for BYOL instances and one for PAYG instances. For deployments using only one instance type, start that VMSS. For Hybrid licensing deployments, start both VMSS.

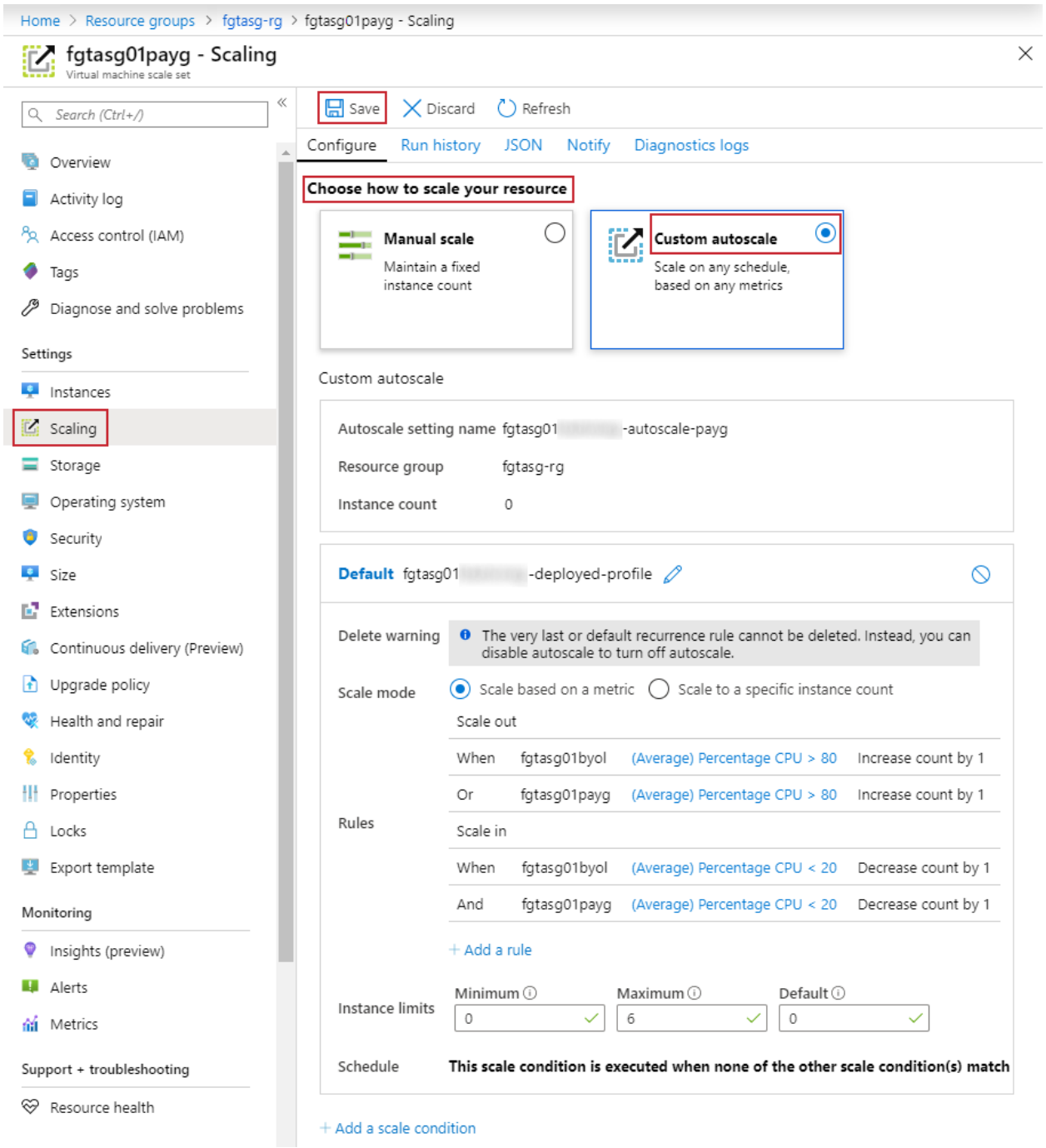
To start a VMSS:

1. Load the resource group that contains the VMSS. In deployments with one resource group, this value is specified in the *Resource group* parameter in step 6 of the section Creating a template deployment on page 8. If your deployment has a separate resource group for the VNet, load that one instead. That resource group is specified in the VNet Resource Group Name on page 17 parameter.
2. Load the *Virtual machine scale set* by clicking its name.
3. From the Virtual machine scale set account navigation column, under *Settings*, click *Scaling*.
4. Under *Choose how to scale your resource*, click *Custom autoscale*.
5. Click *Save*.

The BYOL *Custom autoscale* appears as shown in the image:



The PAYG *Custom autoscale* appears as shown in the image:


Home > Resource groups > fgtasg-rg > fgtasg01payg - Scaling
fgtasg01payg - Scaling
Virtual machine scale set
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Instances
Scaling
Storage
Operating system
Security
Size
Extensions
Continuous delivery (Preview)
Upgrade policy
Health and repair
Identity
Properties
Locks
Export template
Monitoring
Insights (preview)
Alerts
Metrics
Support + troubleshooting
Resource health
Save
Discard
Refresh
Configure
Run history
JSON
Notify
Diagnostics logs
Choose how to scale your resource
Manual scale
Maintain a fixed instance count
Custom autoscale
Scale on any schedule, based on any metrics
Custom autoscale
Autoscale setting name fgtasg01 -autoscale-payg
Resource group fgtasg-rg
Instance count 0
Default fgtasg01 -deployed-profile
Delete warning
The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.
Scale mode
Scale based on a metric
Scale to a specific instance count
Rules
Scale out
When fgtasg01byol (Average) Percentage CPU > 80 Increase count by 1
Or fgtasg01payg (Average) Percentage CPU > 80 Increase count by 1
Scale in
When fgtasg01byol (Average) Percentage CPU < 20 Decrease count by 1
And fgtasg01payg (Average) Percentage CPU < 20 Decrease count by 1
Add a rule
Instance limits
Minimum
Maximum
Default
0
6
0
Schedule
This scale condition is executed when none of the other scale condition(s) match
Add a scale condition

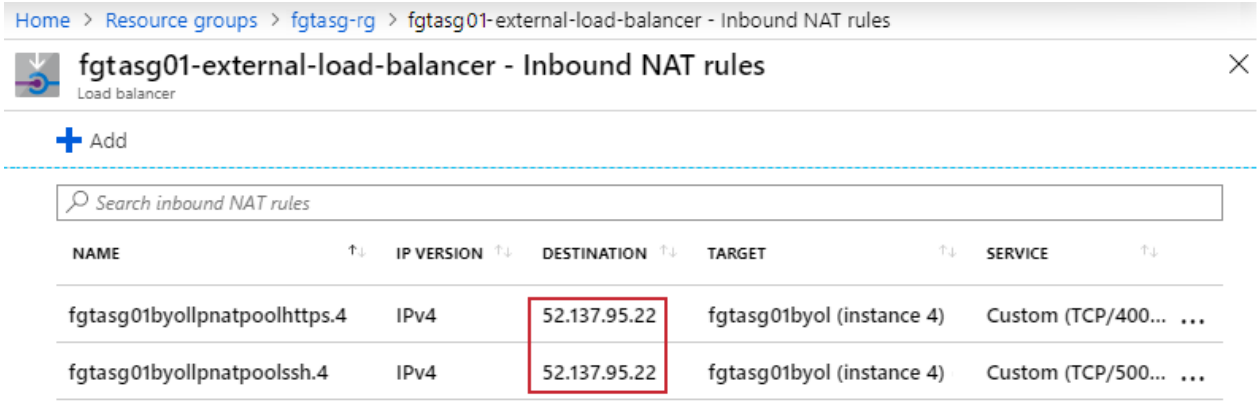
Connecting to the FortiGate-VM instances

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 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:

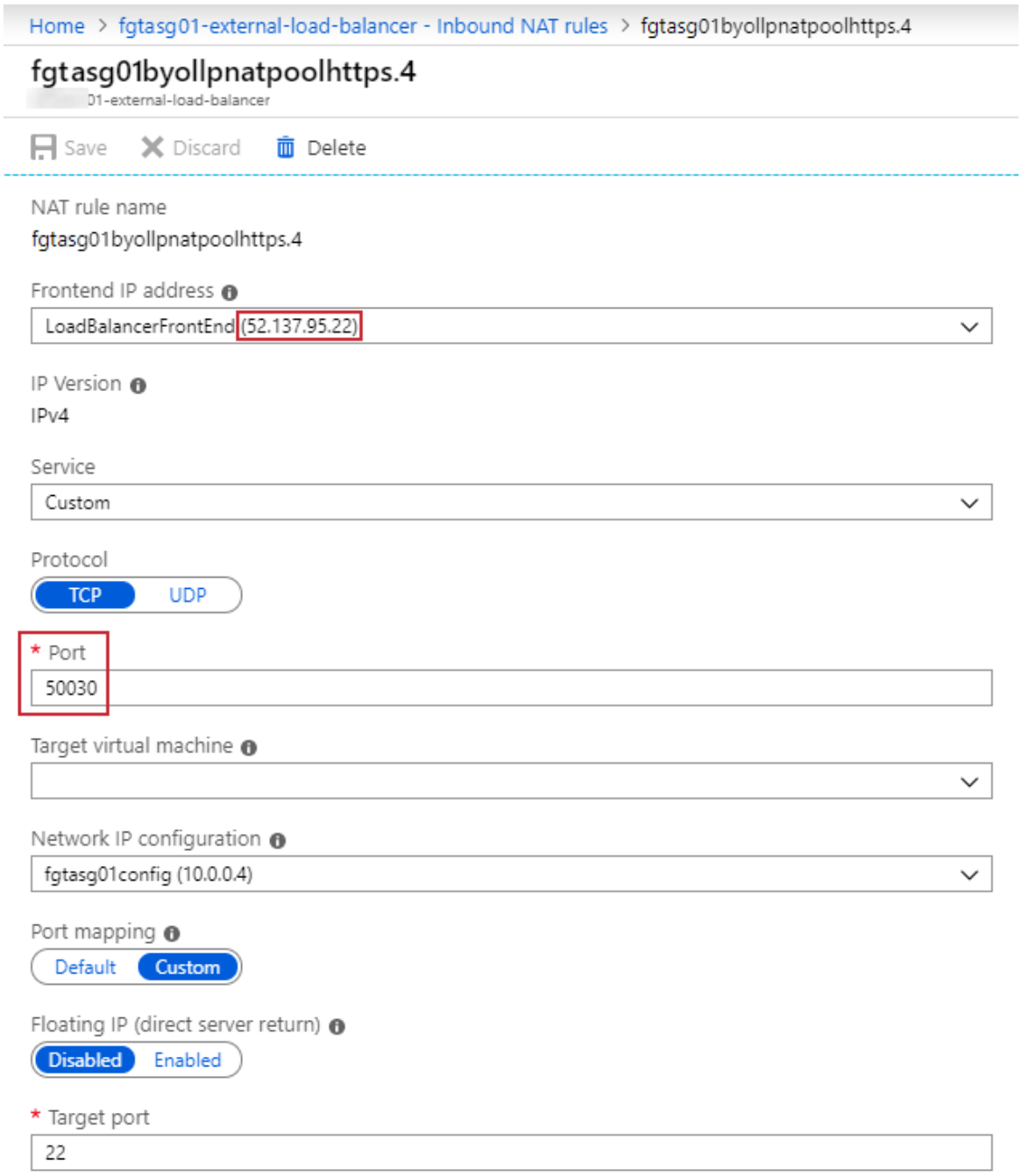
- One rule for SSH access to the instance.
- One rule for HTTPS access to the instance.

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



To access a FortiGate-VM instance, you need the Frontend IP address and port number of the instance you wish to connect to. The Frontend 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. (The IP address is also listed).

An example of an SSH access rule is shown below:


Home > fgtasg01-external-load-balancer - Inbound NAT rules > fgtasg01byollpnatpoolhttps.4
fgtasg01byollpnatpoolhttps.4
01-external-load-balancer
Save
Discard
Delete
NAT rule name
fgtasg01byollpnatpoolhttps.4
Frontend IP address
LoadBalancerFrontEnd (52.137.95.22)
IP Version
IPv4
Service
Custom
Protocol
TCP
UDP
* Port
50030
Target virtual machine
Network IP configuration
fgtasg01config (10.0.0.4)
Port mapping
Default
Custom
Floating IP (direct server return)
Disabled
Enabled
* Target port
22

Troubleshooting

Determining the FortiGate Autoscale release version

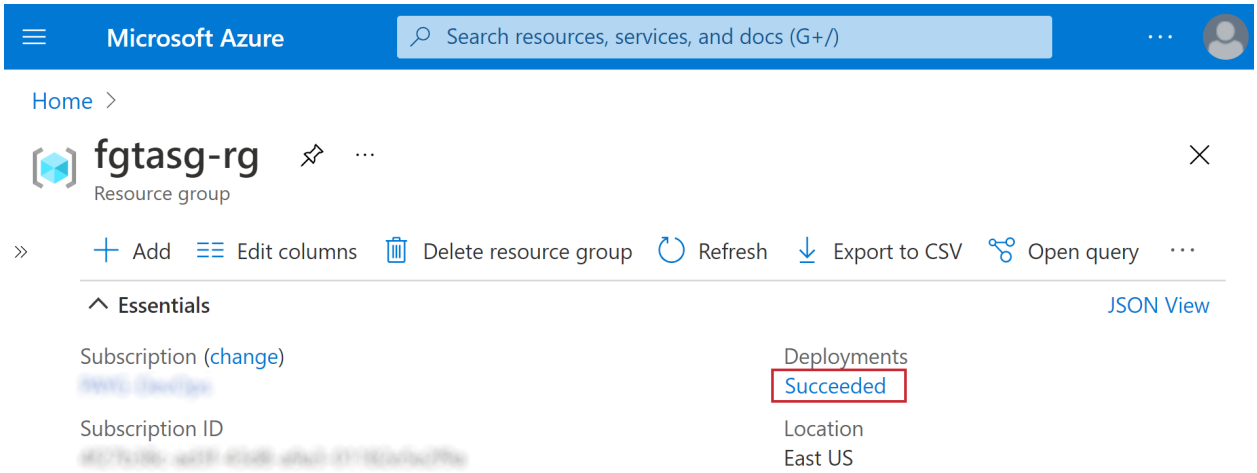
To determine the release version of a deployment, navigate to the *Microsoft.Template Outputs* by following the steps in Locating deployment Outputs on page 33. The release version is in the `deploymentPackageVersion`.

Election of the primary FortiGate was not successful

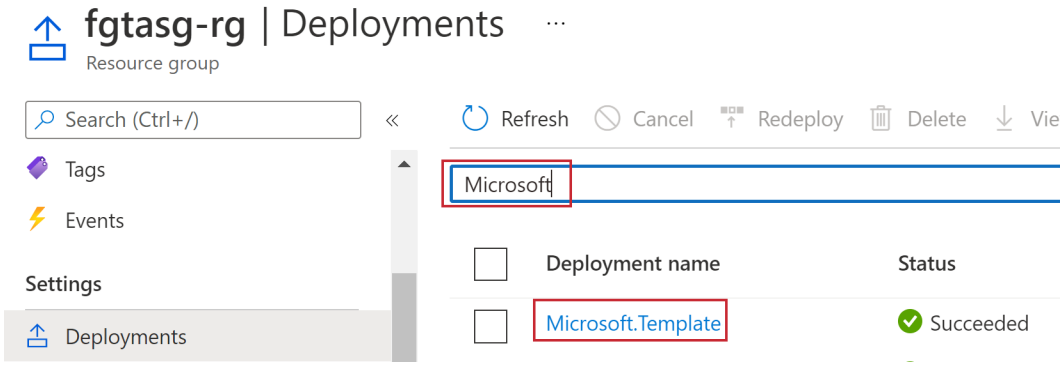
If the election of the primary FortiGate is not successful, reset the elected primary FortiGate. If the reset does not solve the problem, please contact support.

Locating deployment Outputs

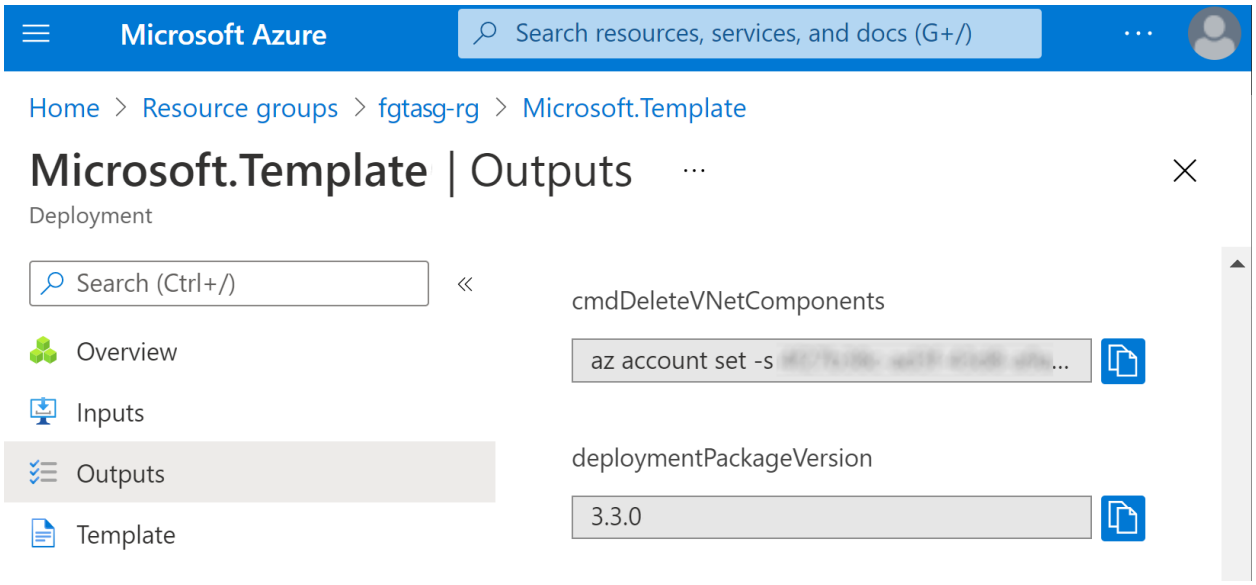
1. Load the resource group *Overview* page. For details, refer to the section To load a resource group: on page 20.
2. Click the link under *Deployments*.



3. From the *Deployments* page, click the *Microsoft.Template*.



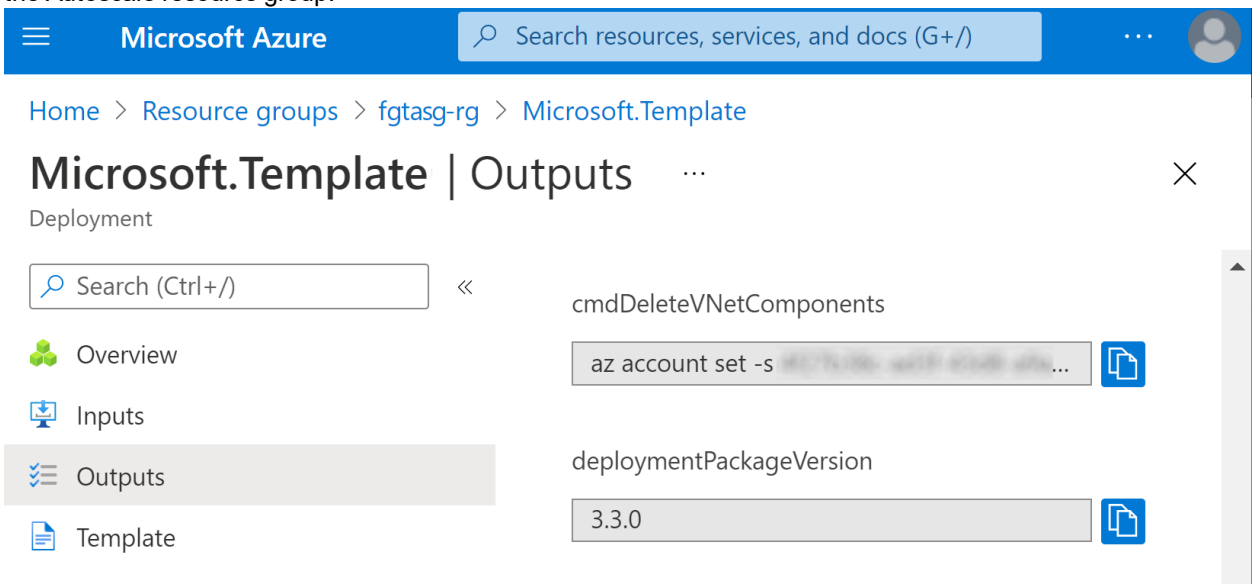
4. In the navigation column, click *Outputs*.



Redeploying with an existing VNet fails

Prior to redeploying with your existing VNet, you must ensure that the VNet meets the Requirements when using an existing VNet on page 6. You must also perform a VNet related cleanup using the following steps:

1. Load the deployment Outputs for the VNet resource group. If your deployment only has one resource group, this is the Autoscale resource group.



2. Copy the value of `cmdDeleteVNetComponents` and run it as an Azure CLI command (click >_ to launch the CLI) to perform the required cleanup.
3. If your deployment has two resource groups, delete the Autoscale resource group. Otherwise, delete the following components:
   - Azure Cosmos DB account
   - App Service

- Application Insights (if present)
- App Service plan
- Storage account

4. Delete the following components from the VNet resource group:
   - the Public Load balancer
   - the Internal Load balancer
   - the Virtual machine scale set for BYOL
   - the Virtual machine scale set for PAYG
   - the Public IP address (if created by the autoscale deployment and you don't want to reuse it)

Resetting the elected primary FortiGate

To reset the elected primary FortiGate, navigate to the CosmosDB *FortiGateAutoscale* and open the table *FortiGatePrimaryElection* and delete the only item in the table.

A new primary FortiGate will be elected and a new record will be created as a result.

For details on locating the CosmosDB *FortiGateAutoscale* and the table *FortiGatePrimaryElection*, refer to the section Verifying the deployment on page 20.

Stack has stopped working

If the stack stops working when it previously used to work, look up the Function App *Additional Outbound IP Addresses* and ensure that each listed IP address has a corresponding entry in the Cosmos DB firewall. Any IP address not listed in the Cosmos DB firewall will be blocked, thus causing the Autoscale function to be blocked.

For details on how the Cosmos DB firewall is configured, refer to the section Security features for network communication on page 24.

For details on when Function App outbound IP addresses change, refer to the Microsoft article When outbound IPs change.

Troubleshooting using Application Insights

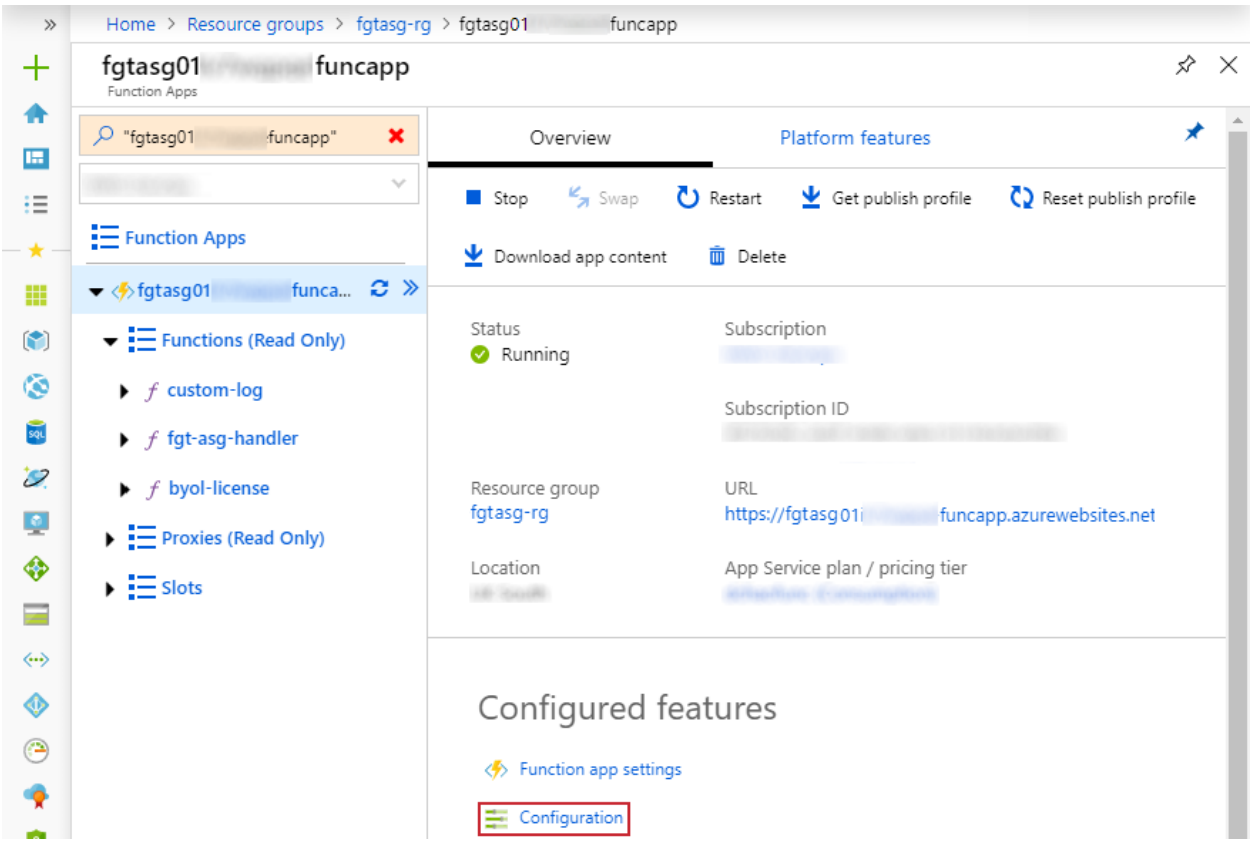
Application Insights can help you troubleshoot the deployment. It is automatically enabled if your region supports it.

Troubleshooting using environment variables

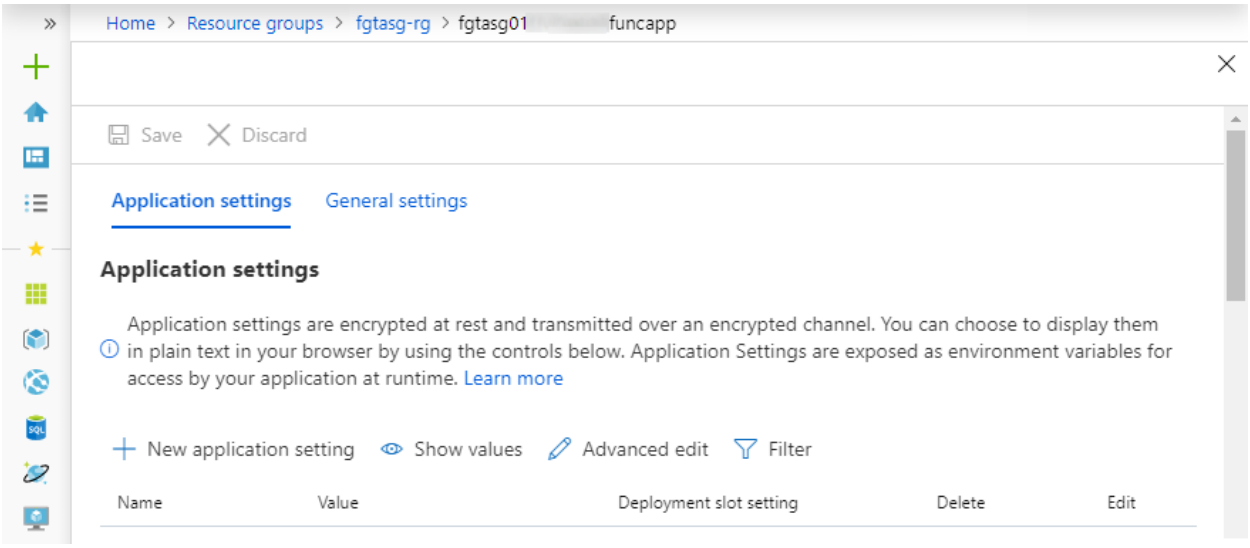
Environment variables are available to assist in troubleshooting the current FortiGate Autoscale deployment. These variables and details on how to use them are listed in the section Troubleshooting environment variables on page 39

1. Load the Function App. For detailed steps, refer to the Function App portion of the section Verifying the deployment on page 20.

2. Under *Configured features*, click *Configuration* .



3. Edit settings as needed.



Changing environment variables other than the troubleshooting ones can cause unexpected behavior. Modify them at your own risk.

Appendix

FortiGate Autoscale for Azure features

Major components

- *The Function App*. The Function App handles all the autoscaling features including: primary/secondary role assignment, license distribution, and failover management.
- *The BYOL Scale Set*. This scale set contains 0 to many FortiGate-VMs of the BYOL licensing model and is a VMSS with a fixed size. Users can set the size to match the number of valid licenses they own. Licenses can be purchased from FortiCare.

  For BYOL-only and hybrid licensing deployments, the *BYOL instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *The PAYG Scale Set*. The Scale Set contains 0 to many FortiGate-VMs of the PAYG licensing model and will dynamically scale-out or scale-in based on the scaling metrics specified by the parameters *Scale Out Threshold* and *Scale in Threshold*.

  For PAYG-only deployments, the *PAYG instance Count* must be at least 2. These FortiGate-VMs are the main instances and are fixed and running 7x24. If it is set to 1 and the instance fails to work, the current FortiGate-VM configuration will be lost.

- *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 on page 38 table below.
    - *httproutingpolicy* and *httpsroutingpolicy* are provided as part of the base configset - for a common use case - and specify the FortiGate firewall policy for VIPs for *http* routing and *https* routing respectively. This common use case includes a VIP on port 80 and a VIP on port 443 with a policy that points to an internal load balancer.
    - *extrastaticroute* is empty by default. Configurations for static routes can be added if they are needed in a network. An example of manually adding a static route:

      ```
      # config router static
         edit 1
            set dst 168.63.129.16 255.255.255.255
            set gateway <subnet gateway>
            set priority <any number>
            set device "<port name>"
         next
      end
      ```
  - The *fgt-asg-license* container contains the BYOL license files.

- *Database tables*. These tables are required to store information such as health check monitoring, primary election, state transitions, etc. These records should not be modified unless required for troubleshooting purposes.
- *Networking Components*.
  - One virtual network
  - Two Load Balancers (with names ending with *-external-load-balancer* and *-internal-load-balancer*)
  - One network security group (with a name ending with *-network-security-group*)
  - One public IP address
  - Four route tables

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.
{HEART_BEAT_ INTERVAL}	Number	The time interval (in seconds) that the FortiGate-VM waits between sending heartbeat requests to the Autoscale handler function. This placeholder is only in the hybrid licensing deployment.

Function App environment variables

Azure infrastructure related environment variables

The variables in the table below hold information that enables the function to use the required Azure services. Changing their values may cause services to be unreachable by the function. Modify them at your own risk.

Variable name	Description
RESOURCE_GROUP	Name of the resource group where the template is deployed in.
CLIENT_ID	Descriptions of these variables are identical to those of the related parameters which are described in the section Configurable variables on page 12. • REST_APP_ID: *Service Principal App ID on page 16* • REST_APP_SECRET: *Service Principal App Secret on page 16* • WEBSITE_RUN_FROM_ZIP: *Package Res URL on page 16*
CLIENT_SECRET	
WEBSITE_RUN_FROM_ZIP	
AUTOSCALE_DB_PRIMARY_ KEY	This is the CosmosDB account access key automatically created with the CosmosDB account.

Variable name	Description
TENANT_ID	The Azure Directory ID for the Active Directory of your current subscription.
SUBSCRIPTION_ID	Your Azure Subscription ID.
AUTOSCALE_DB_ACCOUNT	The CosmosDB account created for the current FortiGate Autoscale deployment.
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.

FortiGate Autoscale required environment variables

Changing the values of the following variables can cause unexpected function behavior. Modify them at your own risk.

Variable name	Description
UNIQUE_ID	Reserved, empty string.
CUSTOM_ID	Reserved, empty string.
RESOURCE_TAG_PREFIX	An Autoscaling feature variable that is automatically created. Reserved for future use.
AUTOSCALE_KEY_VAULT_NAME	Name of the Key Vault service.

Troubleshooting environment variables

The following variables assist in troubleshooting the current FortiGate Autoscale deployment.

Variable name	Description
DEBUG_SAVE_CUSTOM_LOG	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.
DEBUG_LOGGER_OUTPUT_QUEUE_ENABLED	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.
DEBUG_LOGGER_TIMEZONE_OFFSET	Set to the UTC offset of the current deployment location for a better logging display time.

For details on how to modify the troubleshooting environment variables, refer to the section Troubleshooting using environment variables on page 35.

Cloud-init

In Auto Scaling, a FortiGate uses the `cloud-init` feature to pre-configure the instances when they first come up. During template deployment, an internal API Gateway endpoint will be created.

A FortiGate sends requests to the endpoint to retrieve necessary configuration after initialization.

Use this FOS CLI command to display information for your devices:

```
# diagnose debug cloudinit show
```

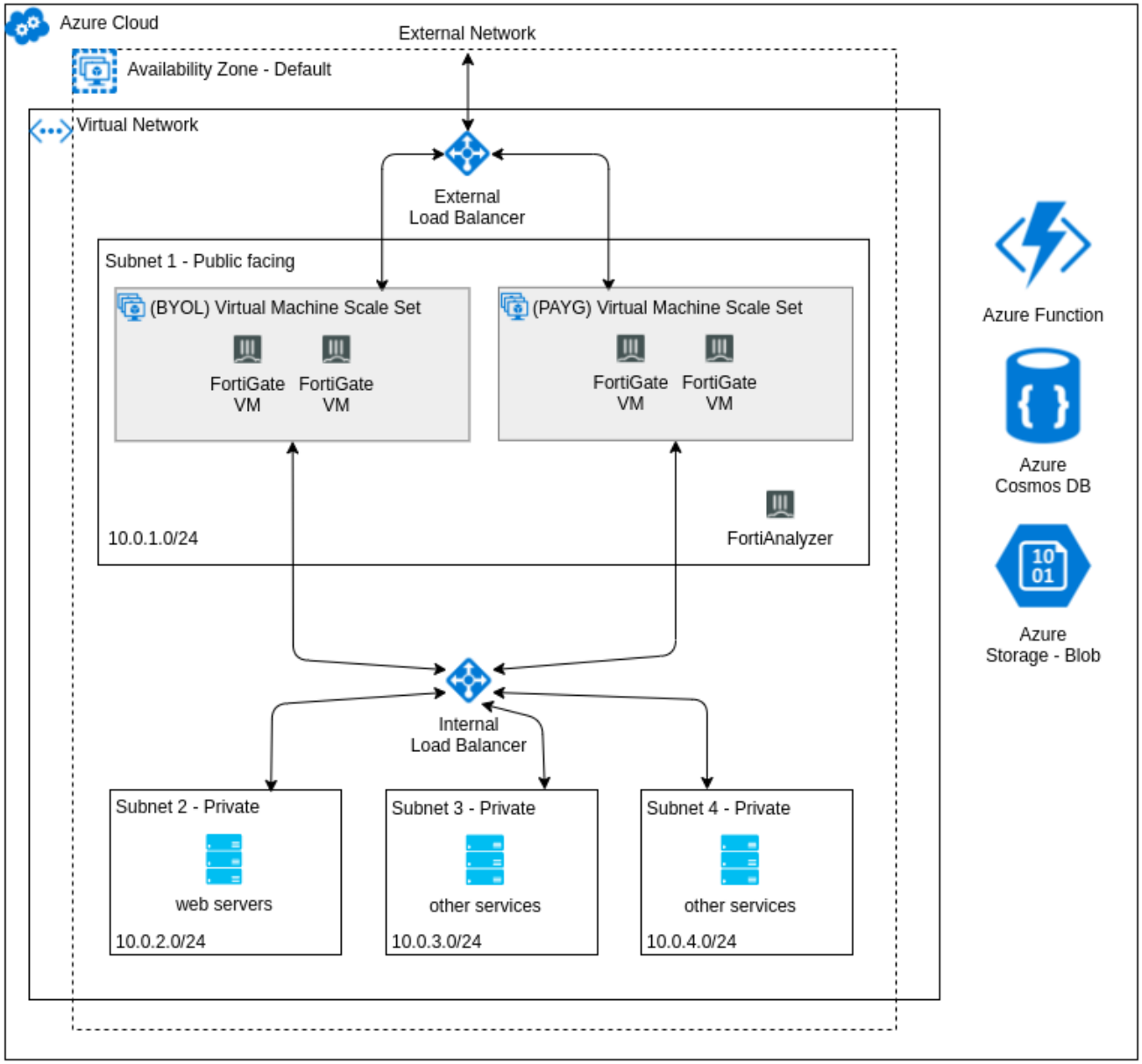
VPN output can be retrieved with this FOS CLI command:

```
# diagnose vpn tun list
```

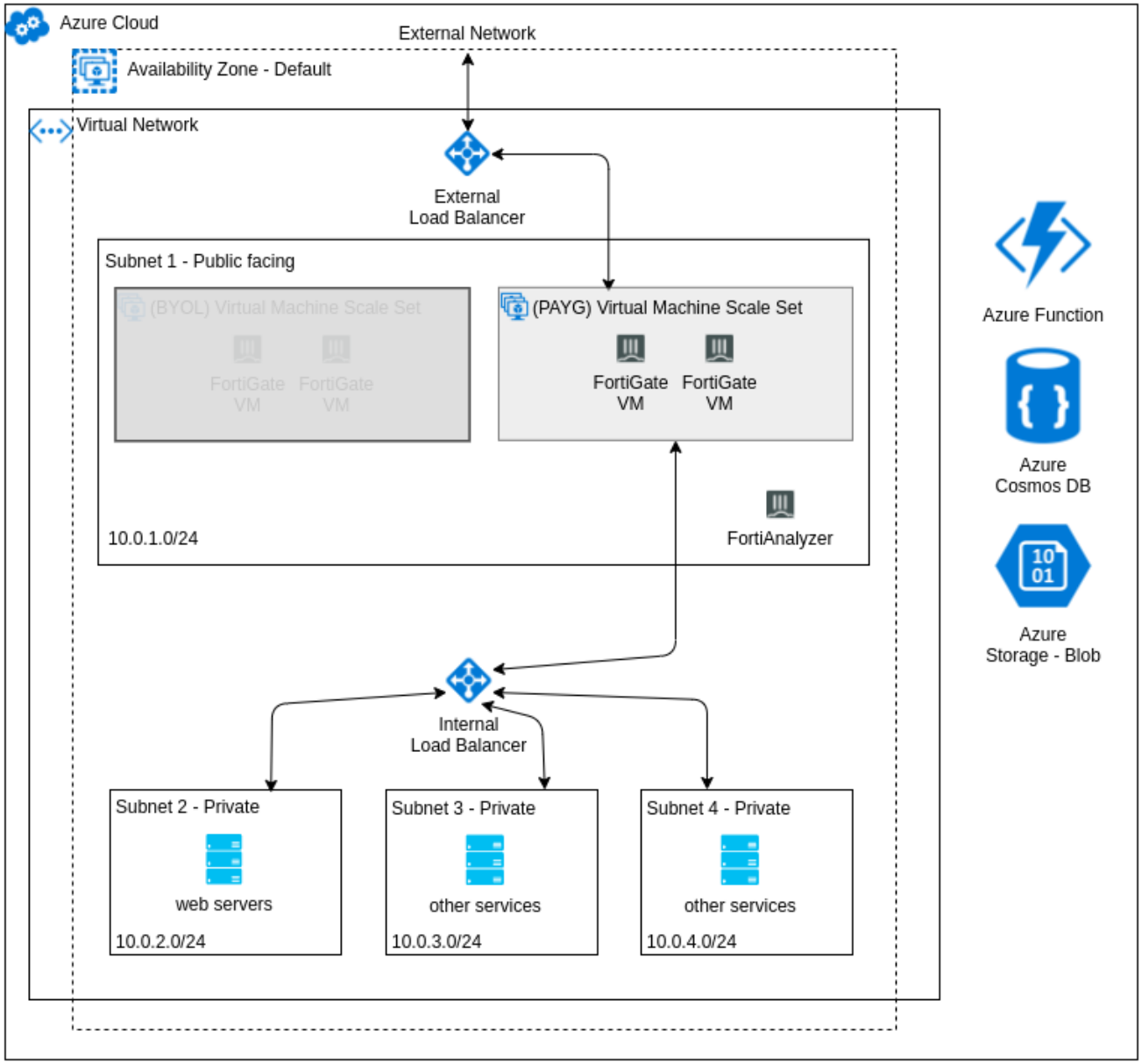
Architectural diagrams

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

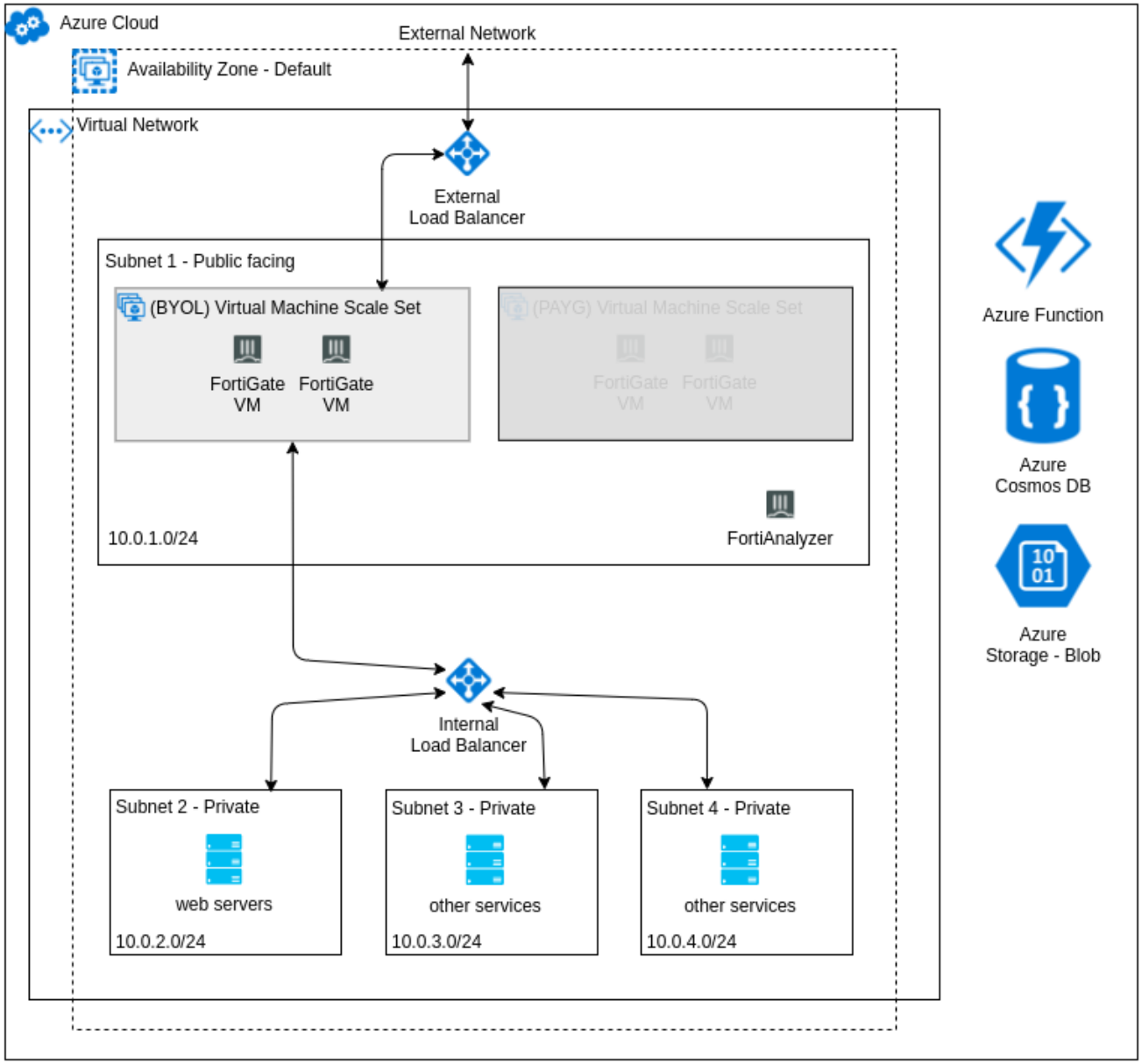
FortiGate Autoscale for Azure architecture (hybrid licensing)



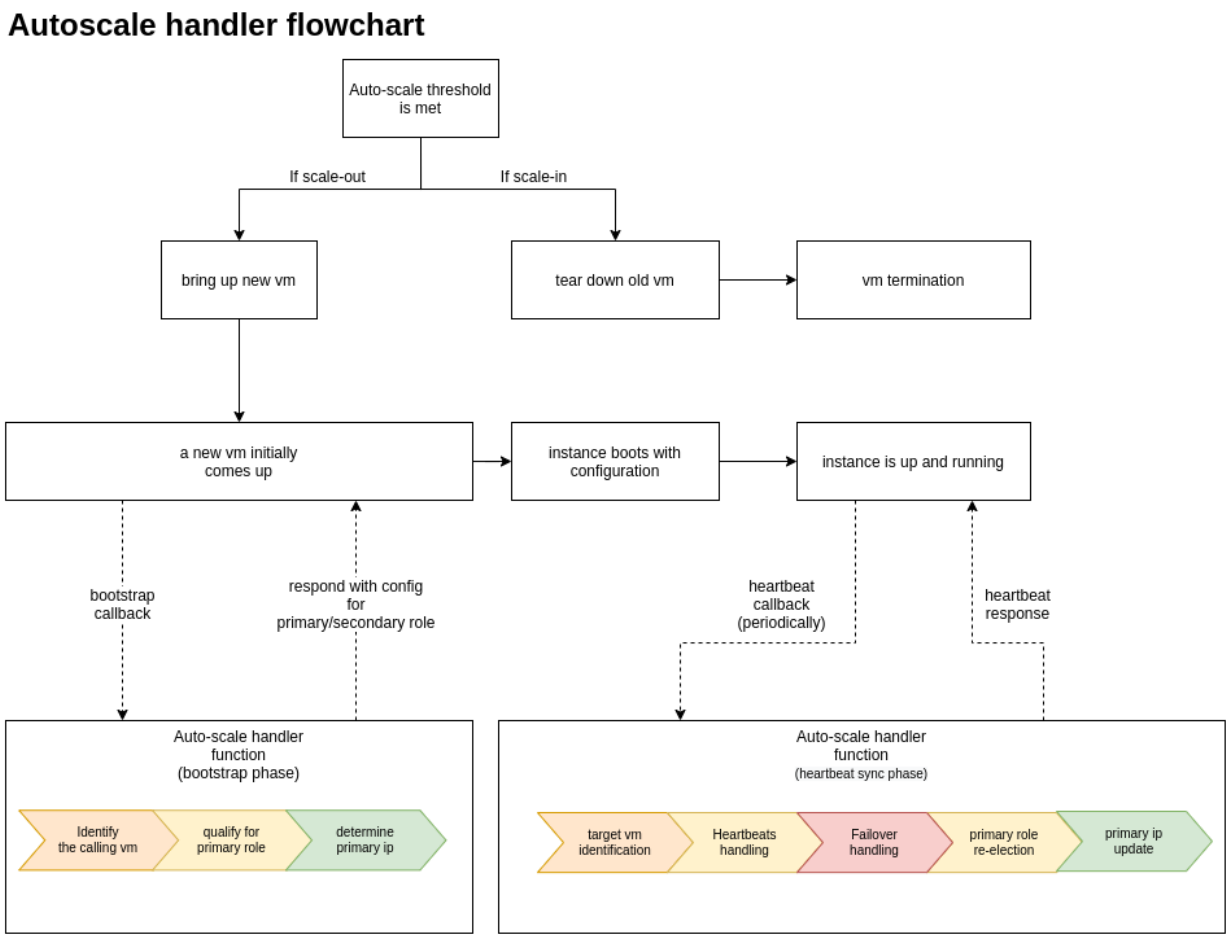
FortiGate Autoscale for Azure architecture (PAYG instances only)



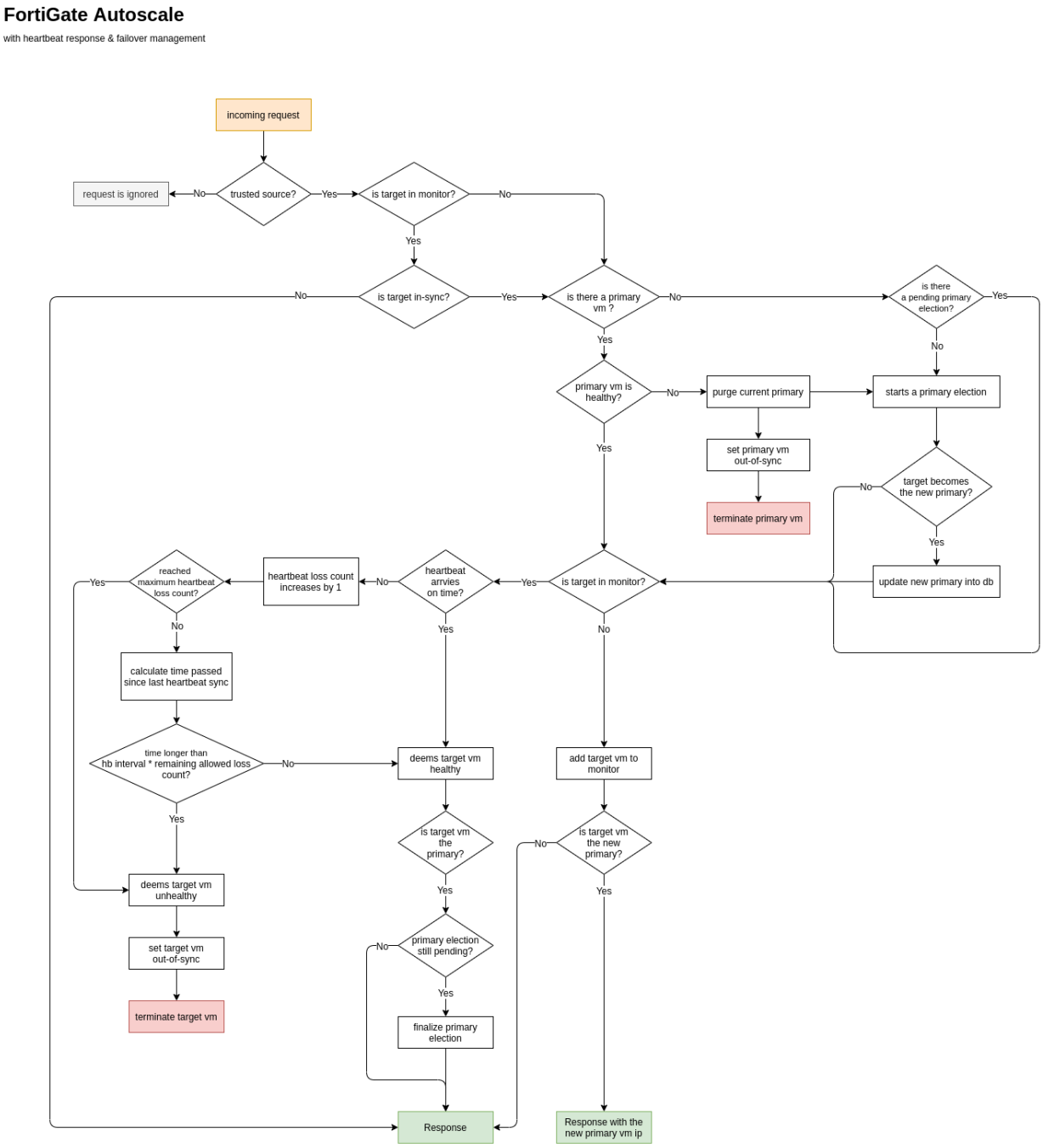
FortiGate Autoscale for Azure architecture (BYOL instances only)



Autoscale handler flowchart



Primary election



Upgrading the deployment

An existing FortiGate Autoscale for Azure deployment can be upgraded in one specific scenario:

- It was deployed with the 2.0.9 template.

To determine which template was used in your deployment, refer to the section Determining the FortiGate Autoscale release version on page 33.

Read these instructions completely before starting an upgrade.

A deployment with the 2.0.9 template can be upgraded only to the 3.3.2 template. During the upgrade, users can optionally consolidate logging and reporting for the FortiGate cluster by integrating FortiAnalyzer 6.2.5 or FortiAnalyzer 6.4.5.

Prerequisites

- Linux Operating System
- NodeJS 14
- Azure CLI
- FortiGate Autoscale for Azure upgrade templates

Obtaining the templates

The FortiGate Autoscale for Azure upgrade templates are located in the Fortinet Autoscale for Azure GitHub project. Navigate to the 2.0.9 upgrade (3.3.2) release and download `fortigate-autoscale-azure.zip`.

Unzip this file on your local PC. The `templates` folder will contain these files:

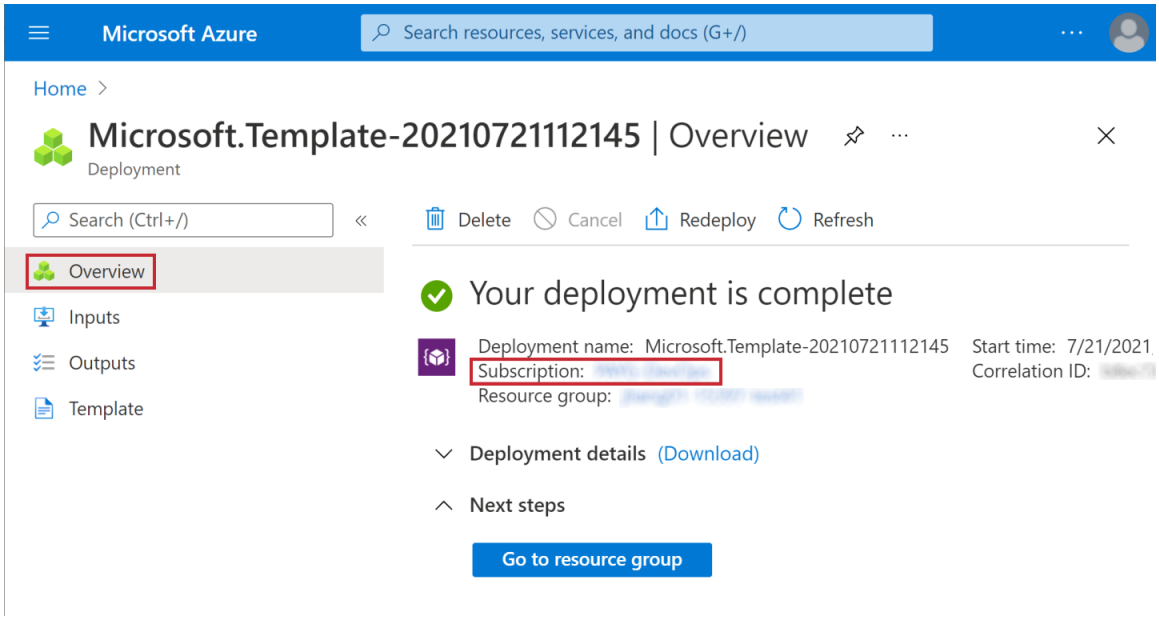
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.preparation.json`
  This template prepares the environment for the upgrade.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.json`
  This template performs the upgrade from the 2.0.9 template to the 3.3.2 template and pairs with the optional parameter template.
- (optional) `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.params.json`
  This parameter template pairs with the upgrade template.
- `upgrade_fortigate_autoscale_from_2.0.9_to_3.3.2.cleanup.json`
  This template finalizes the upgrade process.

Before you start

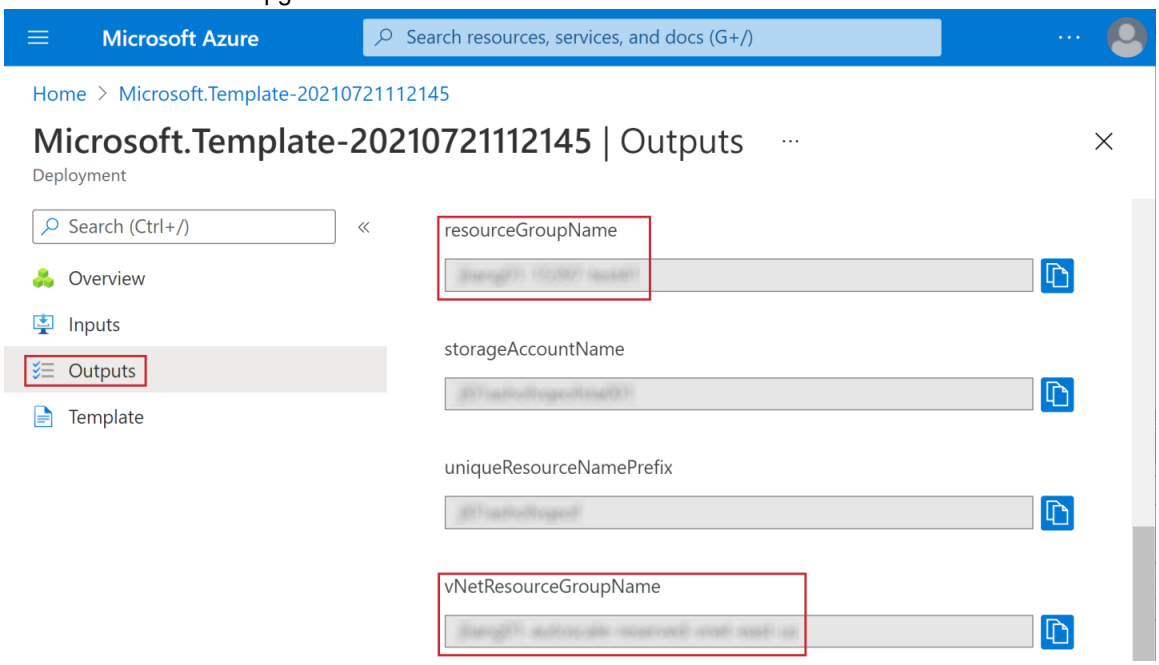
Upgrading the deployment requires values from the existing 2.0.9 deployment. The following sections describe how to locate these values.

Locating values from the 2.0.9 deployment

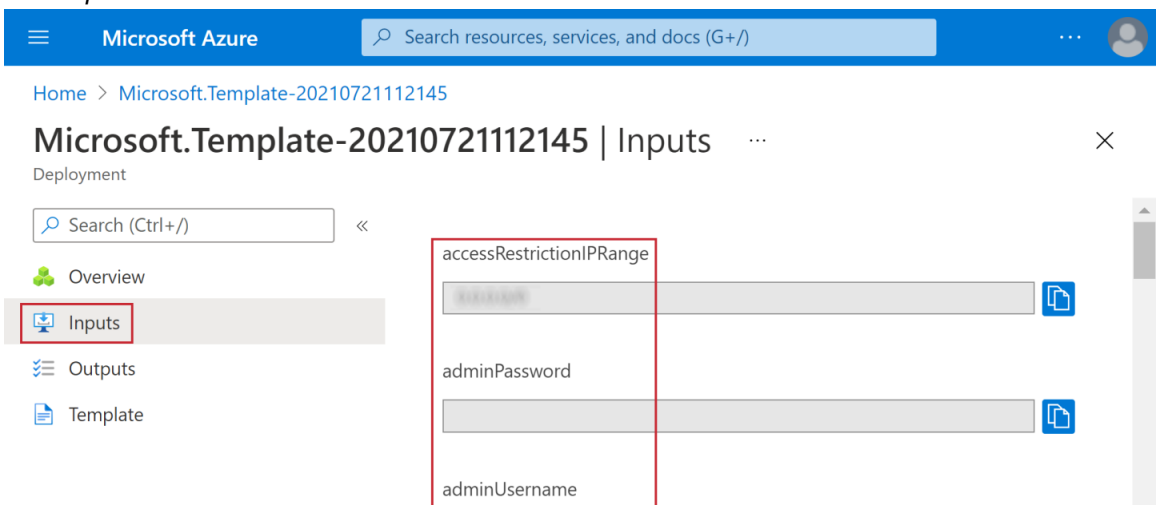
1. Navigate to the *Microsoft.Template Overview* by following the steps 1-3 of the section Locating deployment Outputs on page 33.
2. On the *Overview* page, note the value for the parameter *Subscription* as you will need it for the upgrade.



3. Click *Outputs*and note the values for the parameters *resourceGroupName* and *vNetResourceGroupName* as you will need them for the upgrade.



4. Click *Inputs*.



5. Make note of values on this page as you will need them for the upgrade.

Upgrade iteration

Upgrade Iteration is an important parameter throughout the entire process. The allowable values for *Upgrade Iteration* are limited to the numbers 2 thru 9. This value is used to form a unique name for the new resources related to the upgrade. If there are errors during the upgrade, the entire stack can be rolled back - the *Upgrade Iteration* value is used to remove the resources which were created.

When performing the upgrade for the first time, set *Upgrade Iteration* to 2. If errors occur, rollback the upgrade and start over with *Upgrade Iteration* set to 3. Repeat if necessary, increasing the value of *Upgrade Iteration* each time.

When a deployment is rolled back, the Key Vault will be soft-deleted. Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the AzureCLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

Performing the upgrade

The upgrade solution described here is a rollback-capable solution for preparing, creating, and removing resources. The steps below will guide you through the upgrade process.

Before starting an upgrade, ensure that the values for the 2.0.9 template deployment have been located.

1. Deploy the preparation template as described in the section Deploying the preparation template on page 49.
2. Deploy the upgrade template as described in the section Deploying the upgrade template on page 49.

3. Verify the newly deployed resources. For details, refer to the section Verifying the deployment on page 52.

Do not start the BYOL or PAYG VMSS until you initialize the database. In other words, ensure the instance number of the VMSS is set to 0.

4. Initialize the database. For details, refer to the section Initializing the database on page 52.
5. Start the two new VMSS. For details, refer to the section Starting a VMSS on page 28.
6. Observe the FortiGate-VMs running in the two VMSS and ensure they are running correctly.
7. Deploy the cleanup template. For details, refer to the section Deploying the cleanup template on page 54.

Deploying the preparation template

1. Create a template deployment using the preparation template. For details, refer to the section Creating a template deployment on page 8. When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Subscription	*	*	Use the value from the 2.0.9 template deployment. Do not change it.
Resource group		resourceGroupName	
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.
Upgrade Iteration	*	*	Refer to the section Upgrade iteration on page 48.

* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

2. When deployment of the preparation template has completed, navigate to the *Outputs*. For details, refer to the section Locating deployment Outputs on page 33.
3. Copy the `cmdUpdateAllInOne` command.
4. Open a terminal in your Linux OS.
5. Log in to your Azure account with the command `az login`.
6. Run the command `cmdUpdateAllInOne`.
7. Wait for the command to be fully finished.

Deploying the upgrade template

1. Create a template deployment using the upgrade template. For details, refer to the section Creating a template deployment on page 8. For descriptions of the variables, refer to the section Configurable variables on page 12. When prompted for parameters, use values as described in the table used when creating a template deployment with the preparation template and from the table below:

Parameter display name	2.0.9 template Input	Value to use
Access Restriction IP Range	accessRestrictionIPRange	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Admin Password	adminPassword	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Admin Username	adminUsername	Use the value from the 2.0.9 template deployment.
BYOL Instance Count	byolInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
FOS Version	fosVersion	Use values from the drop-down list. The latest version is recommended.
Forti Analyzer Autoscale Admin Password	*	Follow the instructions in the parameter description.
Forti Analyzer Autoscale Admin Username	*	
Forti Analyzer Custom Private IP Address	*	
Forti Analyzer Instance Type	*	
Forti Analyzer Integration Options	*	
Forti Analyzer Version	*	
Forti Gate PSK Secret	fortiGatePSKSecret	Requires manual input. The value from the 2.0.9 template deployment is recommended; a new value may be entered.
Heart Beat Delay Allowance	heartBeatDelayAllowance	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Heart Beat Interval	heartBeatInterval	
Heart Beat Loss Count	heartBeatLossCount	
Instance Type	instanceType	
Key Vault Name	*	Follow the instructions in the parameter description.

Parameter display name	2.0.9 template Input	Value to use
Max BYOL Instance Count	maxBYOLInstanceCount	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Max PAYG Instance Count	maxPAYGInstanceCount	
Min BYOL Instance Count	minBYOLInstanceCount	
Min PAYG Instance Count	minPAYGInstanceCount	
PAYG Instance Count	PAYGInstanceCount	
Package Res URL	packageResURL	Use the template default value. Do not change it.
Primary Election Timeout	masterElectionTimeout	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Scale In Threshold	scaleInThreshold	
Scale Out Threshold	scaleOutThreshold	
Service Plan Tier	*	Follow the instructions in the parameter description.
Service Principal App ID	restAppID	Use the value from the 2.0.9 template deployment. Do not change it
Service Principal App Secret	restAppSecret	
Service Principal Object ID	*	Follow the instructions in the parameter description.
Storage Account Type	storageAccountType	Use the value from the 2.0.9 template deployment. May be adjusted to meet the new needs.
Subnet1Name	subnet1Name	Follow the instructions in the parameter description.
Subnet2Name	subnet2Name	
Subnet3Name	subnet3Name	
Subnet4Name	subnet4Name	
Vnet Address Space	vnetAddressSpace	Use the value from the 2.0.9 template deployment. Do not change it.
Vnet Name	vnetName	

If the deployment does not complete successfully, go to the section Troubleshooting the upgrade on page 55.

2. Upload `configset` files to the Storage account. For details, refer to the section Uploading files to the Storage account on page 18.
3. If you will be using BYOL instances, upload `license` files to the Storage account.

License files from the 2.0.9 deployment can be reused . However, re-using a license will invalidate the FortiGate which is currently using the license.

Verifying the deployment

The FortiGate Autoscale for Azure 3.3.2 template will be deployed into the Resource Group and a new set of the following 6 resources will be created:

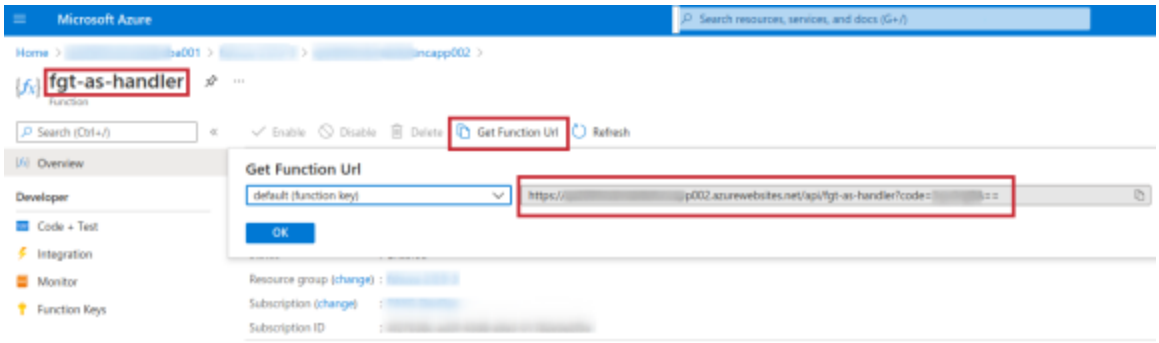
- Function App
- App Service plan
- Application Insights
- Storage account
- Azure Cosmos DB account
- Virtual machine scale set (BYOL)
- Virtual machine scale set (PAYG)

These resources will be created with the same name as the previous 2.0.9 resources with the iteration number appended. For example, if the Upgrade Iteration is 2, the number appended is 002. Verify that they have been created. For details on verifying components, refer to the section Verifying the deployment on page 20.

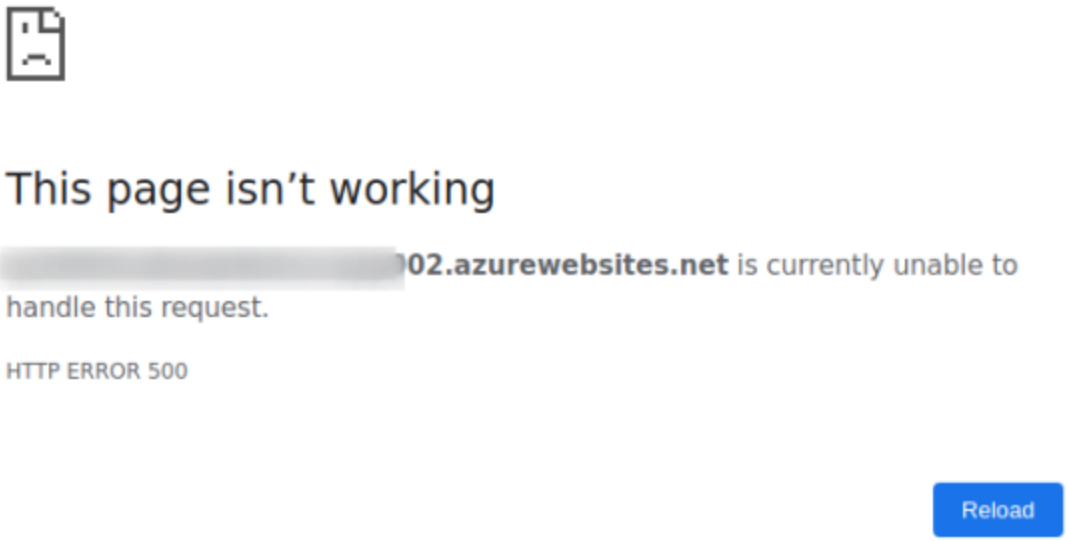
Initializing the database

Do not scale out the BYOL or PAYG VMSS until you initialize the database.

1. Navigate to the `fgt-as-handler` function. For details on how to do this, refer to the section To verify the Function App: on page 22.
2. Click *Get Function Url* to obtain the Function URL:

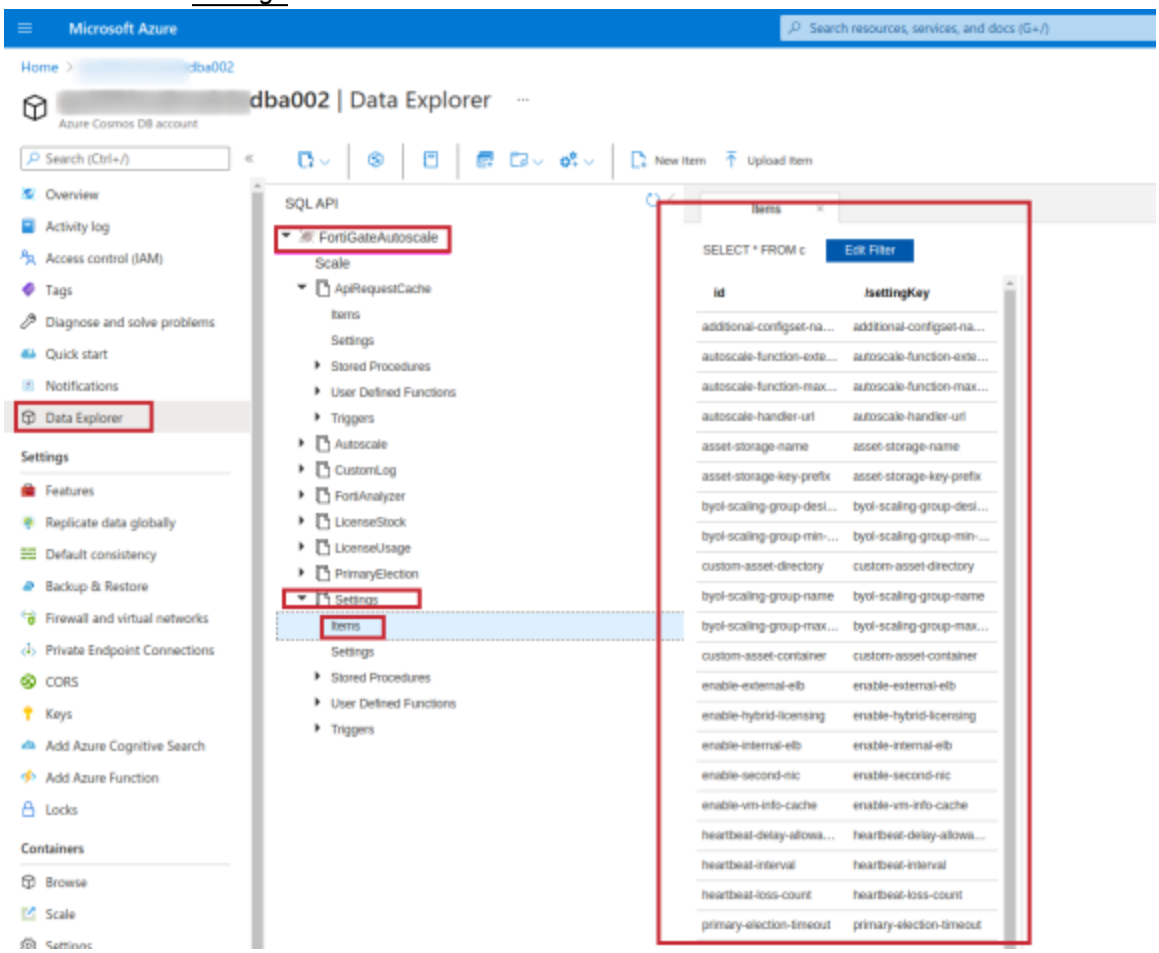


3. Open a web browser to run the URL. The expected response is an error as shown below:



4. Navigate to the cosmos DB account of the current upgrade iteration. For details on how to do this, refer to steps 1 and 2 in the section To verify the database: on page 22.
5. On the right hand side, expand the database *FortiGateAutoscale*.
6. Expand the container *Settings*.
7. Click on *Items*.

8. Confirm that the *Settings* container has items.



Deploying the cleanup template

1. Create a template deployment using the cleanup template. For details, refer to the section Creating a template deployment on page 8. When prompted for parameters, use values as described in the table below:

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Subscription	*	*	
Resource group		resourceGroupName	Use the value from the 2.0.9 template deployment. Do not change it.
Resource Name Prefix	resourceNamePrefix		
Vnet Resource Group Name		vNetResourceGroupName	
Region	*	*	This value cannot be changed. It is tied to the Resource group.

Parameter display name	2.0.9 template Input	2.0.9 template Ouput	Value to use
Upgrade Iteration	*	*	Use the iteration number for the upgrade iteration you want to continue with

* indicates that there isn't a value present in the 2.0.9 template Inputs or Outputs.

2. When deployment of the cleanup template has completed, navigate to the *Outputs*.
3. Copy the command appropriate for your activity:
   - To finalize the upgrade, copy the `cleanUpOldComponentCmdDeleteAllInOne` command.
   - To roll back the upgrade, copy the `upgradeIterationCmdDeleteAllInOne` command.
4. Open a terminal in your Linux OS.
5. Log in to your Azure account with the command `az login`.
6. Run the copied command.
7. Wait for the command to be fully finished.

Troubleshooting the upgrade

As long as an upgrade process isn't finalized, it is regarded as an incomplete upgrade iteration. Reasons for not finalizing can include errors and user intervention.

In the case of an incomplete upgrade iteration, roll back the upgrade iterationand perform the upgrade again with a different value for *Upgrade Iteration*. It is suggested that the value be increased by 1 with each successive deployment.

Rolling back an incomplete upgrade iteration

Users have the option of rolling back an upgrade iteration by deploying the cleanup template. When deployed, newly created resources related to the upgrade iteration will be released. It is recommended to rollback right away before starting a new upgrade iteration. This option must be used if all the allowable *Upgradte Iteration* values (2-9) have been used up.

When a deployment is rolled back, the Key Vault will be soft-deleted. Once the Key Vault is permanently deleted, the *Upgrade Iteration* number can be reused. To permanently delete the Key Vault, open the AzureCLI and run the `upgradeIterationCmdDeleteKeyVaultPermanent` command from the *Outputs* of the cleanup template.

Document history

Template	Date Released	Details
special release	August 25, 2021	This special release is for upgrading from the 2.0.9 template to the 3.3.2 template. The upgrade release package is located on the Fortinet Autoscale for Azure release page tag 2.0.9 upgrade (3.3.2).
3.3.2	June 11, 2021	Documentation was not updated.
3.3.0	May 25, 2021	Added support for FortiAnalyzer.
3.1.1	February 4, 2021	Added support for FortiOS 6.4.3. Removed support for FortiOS 6.2.x.
3.0.0	September 23, 2020	Added support for FortiOS 6.2.3.
2.0.5	February 25, 2020	Added support for FortiOS 6.0.9.
2.0	October 8, 2019	FortiGate Autoscale 2.0.0 General Availability Added support for Hybrid Licensing (any combination of BYOL and/or PAYG instances).
1.0	April 19, 2019	FortiGate Autoscale General Availability Supports auto scaling for PAYG instances only. Requires FortiOS 6.0.6 or FortiOS 6.2.1. Documentation is no longer maintained and is only available as a PDF: • Deploying auto scaling on Azure 1.0