vMX100 Setup Guide for Microsoft Azure

Overview

This document is a walkthrough for setting up a virtual MX (vMX100) appliance in the Microsoft Azure Marketplace. After completing the steps outlined in this document, you will have a virtual MX appliance running in Azure that serves as an AutoVPN termination point for your physical MX devices.

Currently, the vMX100 on Azure supports a one-armed VPN concentrator configuration with split-tunnel VPN architecture. For more info on how to deploy a one-armed concentrator, please refer to this document.

Key Concepts

Before deploying a virtual MX, it is important to understand several key concepts:

Concentrator Mode

All MXs can be configured in either NAT or VPN concentrator mode. There are important considerations for both modes. For more detailed information on concentrator modes, click here.

One-Armed Concentrator

In this mode the MX is configured with a single Ethernet connection to the upstream network. All traffic will be sent and received on this interface. This is the only supported configuration for MX appliances serving as VPN termination points into Azure.

NAT Mode Concentrator

In this mode the MX is configured with a single Ethernet connection to the upstream network and one Ethernet connection to the downstream network. VPN traffic is received and sent on the WAN interfaces connecting the MX to the upstream network and the decrypted, unencapsulated traffic is sent and received on the LAN interface that connects the MX to the downstream network.

> **Note**: This is not supported for virtual MX VPN concentrators operating within Azure.

VPN Topology

There are several options available for the structure of the VPN deployment.

Split Tunnel

In this configuration, branches will only send traffic across the VPN if it is destined for a specific subnet that is being advertised by another MX in the same Dashboard organization. The remaining traffic will be checked against other available routes, such as static LAN routes and third-party VPN routes, and if not matched will be NATed and sent out the branch MX unencrypted.

Full Tunnel

In full tunnel mode all traffic that the branch or remote office does not have another route to is sent to a VPN hub.

> **Note**: This is not supported for virtual MX VPN concentrators operating within Azure.

Azure Terminology

This document will make reference to several key Azure-specific terms and concepts.

Azure Virtual Network

A virtual network is where a block of associated IP addresses, DNS settings, security policies and route tables can be configured and managed.

Azure Resource Manager (ARM) and Azure Classic

Azure has different types of virtual network environments, which represent two different methods of deploying and managing Azure virtual environments. The vMX uses 'managed applications', which is an MSFT platform, and is **not** compatible with Azure 'classic' deployments.

Resource group

A resource group is a container within Microsoft Azure's infrastructure where resources, such as virtual machines are stored.

Azure Managed Applications

Managed Applications within Azure serve as the network used to manage and support the Cisco Meraki virtual MX.

Additional Information

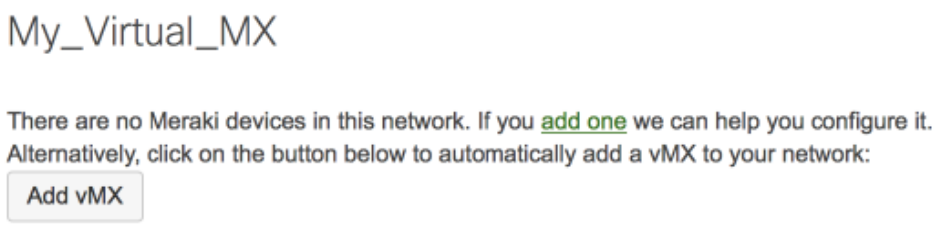
During the setup of your vMX100 instance, or over the course of working within Azure, you may encounter additional terminology which is not defined in this document. To find out more about these terms, and for additional details on the terms listed above, please see the Microsoft Azure glossary.

Meraki Dashboard Configuration

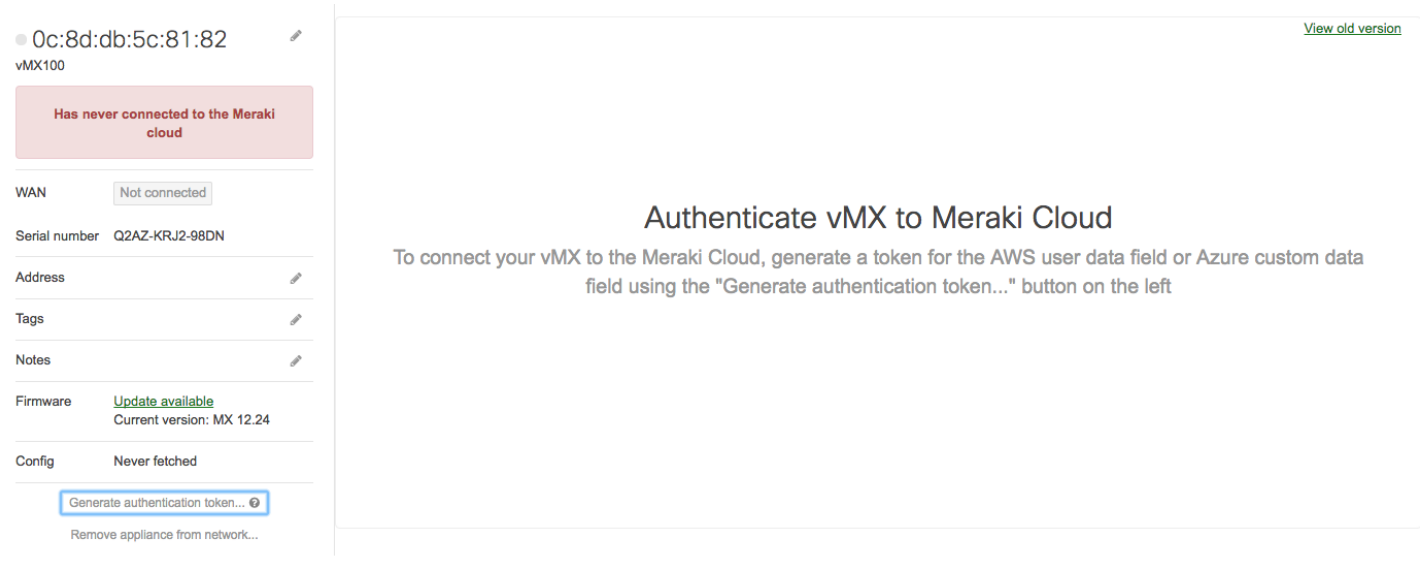
Begin by creating a new Security Appliance network in your organization. This guide will walk you through creating a new network in the Meraki Dashboard.

The Meraki Dashboard will require a vMX100 license to be added before you are able to continue. If you do not have access to a vMX100 license, please reach out to your Meraki Reseller or Sales Rep.

Once you have created the network and added the appropriate license you will be able to deploy a new vMX100 to your network by clicking on 'Add vMX':



After you add the new vMX100 to your network, click on “Generate authentication token” to generate the token for Azure custom-data field.



Copy the newly generated token and save it for the next part in 'Azure Setup'. It will be used when creating a new resource group and will be added to the 'Meraki Authentication Token' field of the Azure template.

> The authentication token **must** be entered into the Azure instance within 1 hour of generating it. If it has been more than 1 hour then a new token must be generated.

Next, follow the steps outlined in this guide to configure the vMX100 as a one-armed concentrator.

On the Site-to-Site VPN page, add each subnet in your resource group that should be accessible to remote Auto VPN peers to the list of 'Local Network(s).' For more information on configuring Auto VPN, please refer to the Site to Site VPN settings documentation.

> Configuring a static IP on a vMX100 in Microsoft Azure via Dashboard is currently not supported. Attempting to configure one will result in the node losing network connectivity and going offline.

Azure Setup

Before You Begin

You must have the following before you begin:

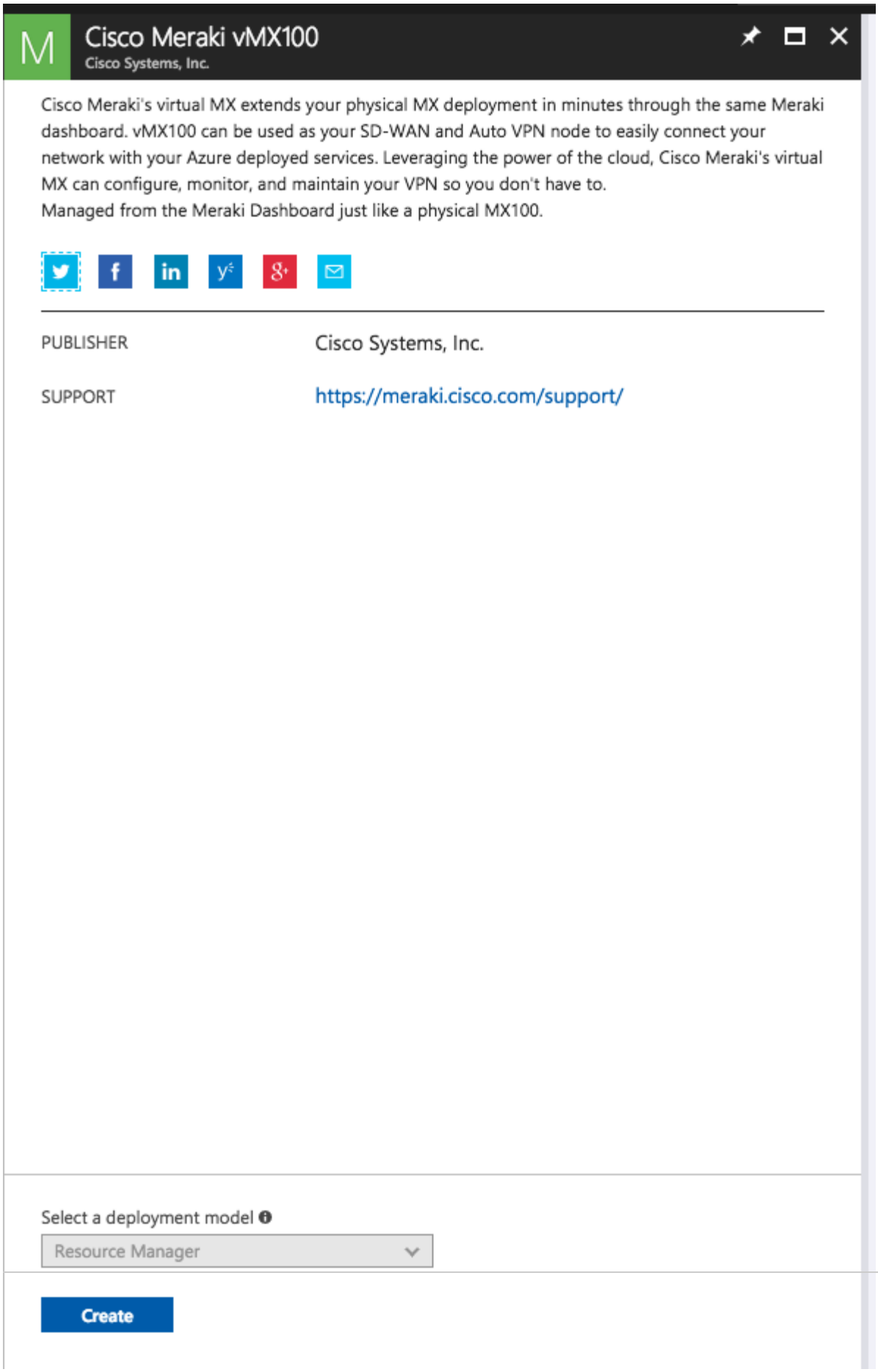
- An Azure virtual network and virtual subnet on a resource groups separate from the resource group you will be creating to host the vMX. To find more information about this, please click here.

> **Note**: Your virtual network must be in a separate resource group from the one hosting your vMX. If you assign the vMX to a resource group that already contains a virtual network/virtual subnet, you will not be able to deploy the vMX.

This section walks you through configuring the necessary requirements within Microsoft Azure, and adding a vMX100 instance to your resource group. For more details on setting up a resource group and other components, please refer to Azure's Documentation here.

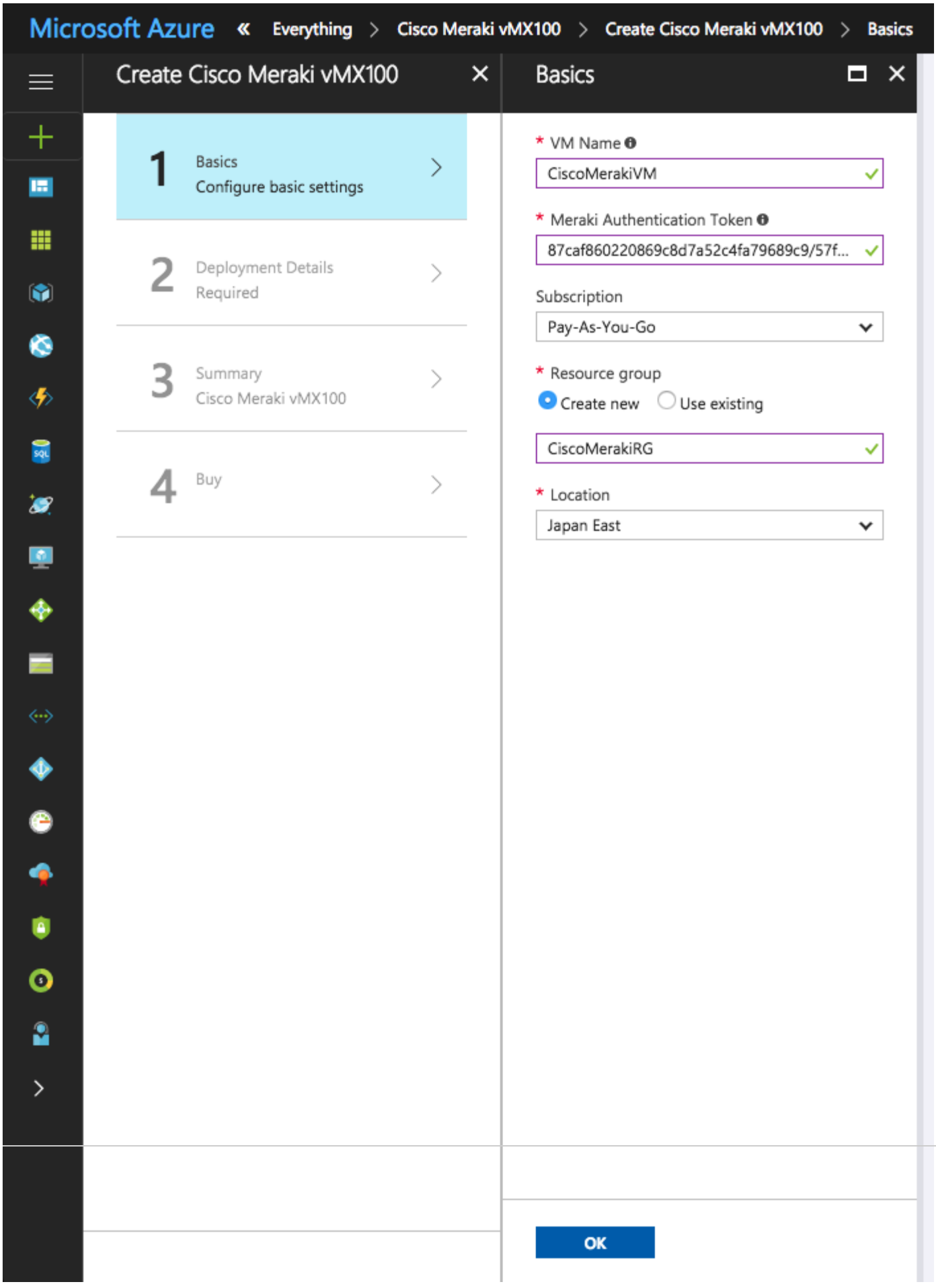
Accessing the Offer

To gain access to the VM Offer, please access this link. A screenshot of the Marketplace list of Cisco Meraki vMX100 in Azure is included below:


Cisco Meraki vMX100
Cisco Systems, Inc.
Cisco Meraki's virtual MX extends your physical MX deployment in minutes through the same Meraki dashboard. vMX100 can be used as your SD-WAN and Auto VPN node to easily connect your network with your Azure deployed services. Leveraging the power of the cloud, Cisco Meraki's virtual MX can configure, monitor, and maintain your VPN so you don't have to.
Managed from the Meraki Dashboard just like a physical MX100.
PUBLISHER
Cisco Systems, Inc.
SUPPORT
https://meraki.cisco.com/support/
Select a deployment model
Resource Manager
Create

From the Marketplace listing, click on 'Create.'

After creating, you will be prompted to configure basic settings:


Microsoft Azure
Everything
Cisco Meraki vMX100
Create Cisco Meraki vMX100
Basics
Create Cisco Meraki vMX100
1
Basics
Configure basic settings
2
Deployment Details
Required
3
Summary
Cisco Meraki vMX100
4
Buy
Basics
* VM Name
CiscoMerakiVM
* Meraki Authentication Token
87caf860220869c8d7a52c4fa79689c9/57f...
Subscription
Pay-As-You-Go
* Resource group
Create new
Use existing
CiscoMerakiRG
* Location
Japan East
OK

VM Name: Choose a name for your Cisco Meraki vMX100 VM, it can be any name.

Meraki Authentication Token: Paste the token previously generated on the Meraki dashboard.

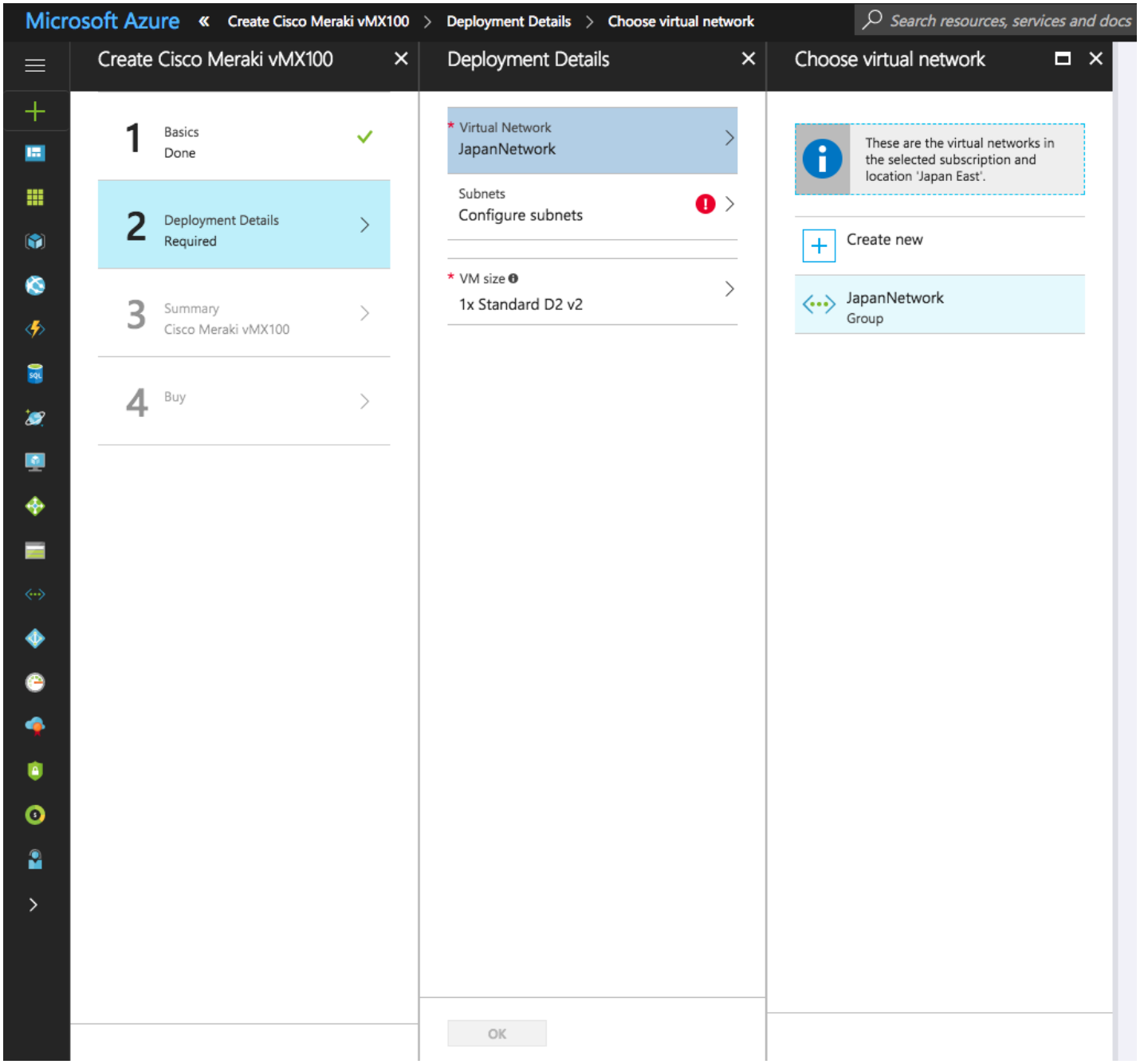
Subscription: Choose the subscription that you want to be billed for from the drop-down menu.

Resource group: Create a new resource group with any name.

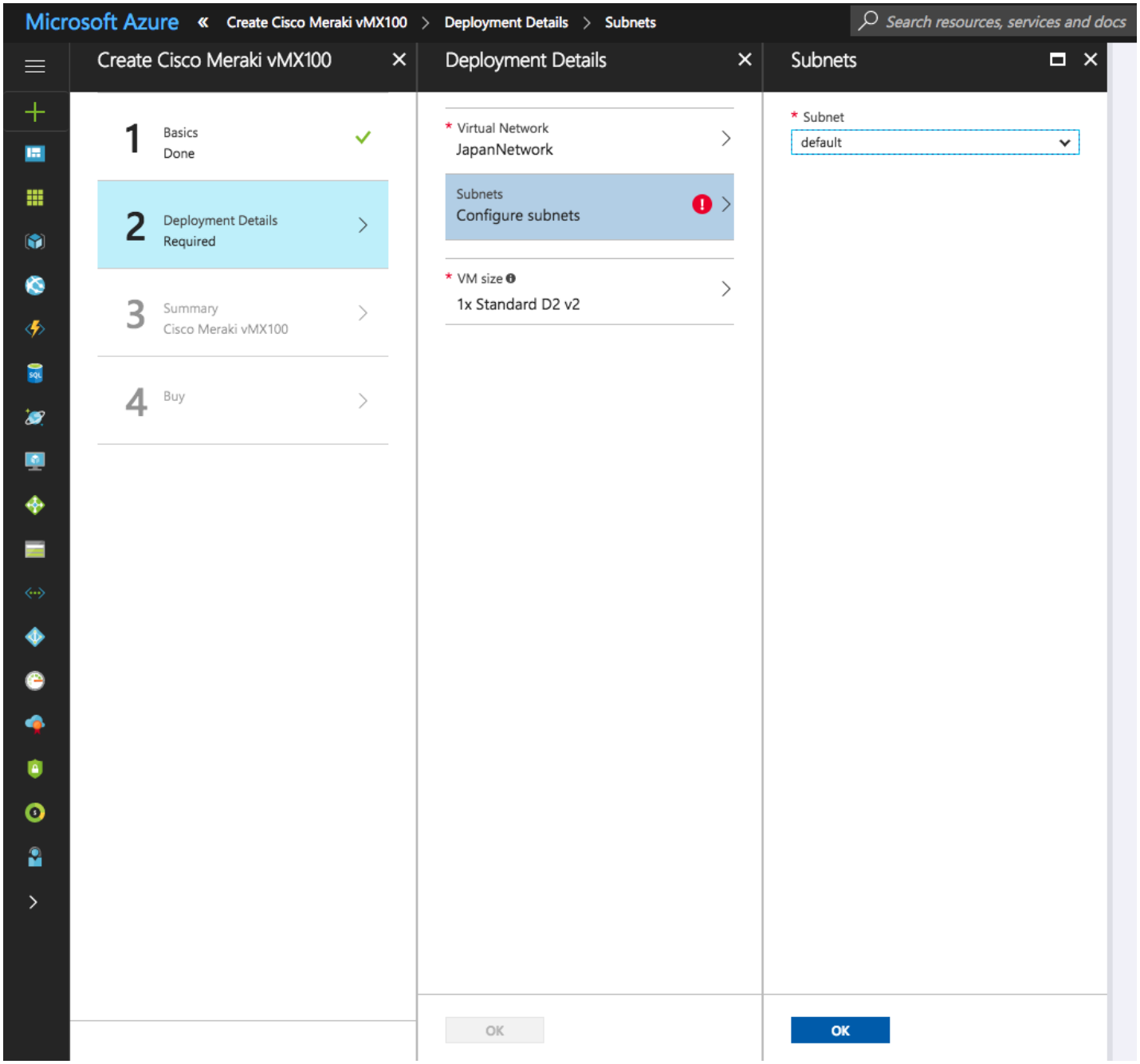
Location: Select the region where the vMX100 will be deployed in.

After completing all the basic settings configuration, hit 'OK.'

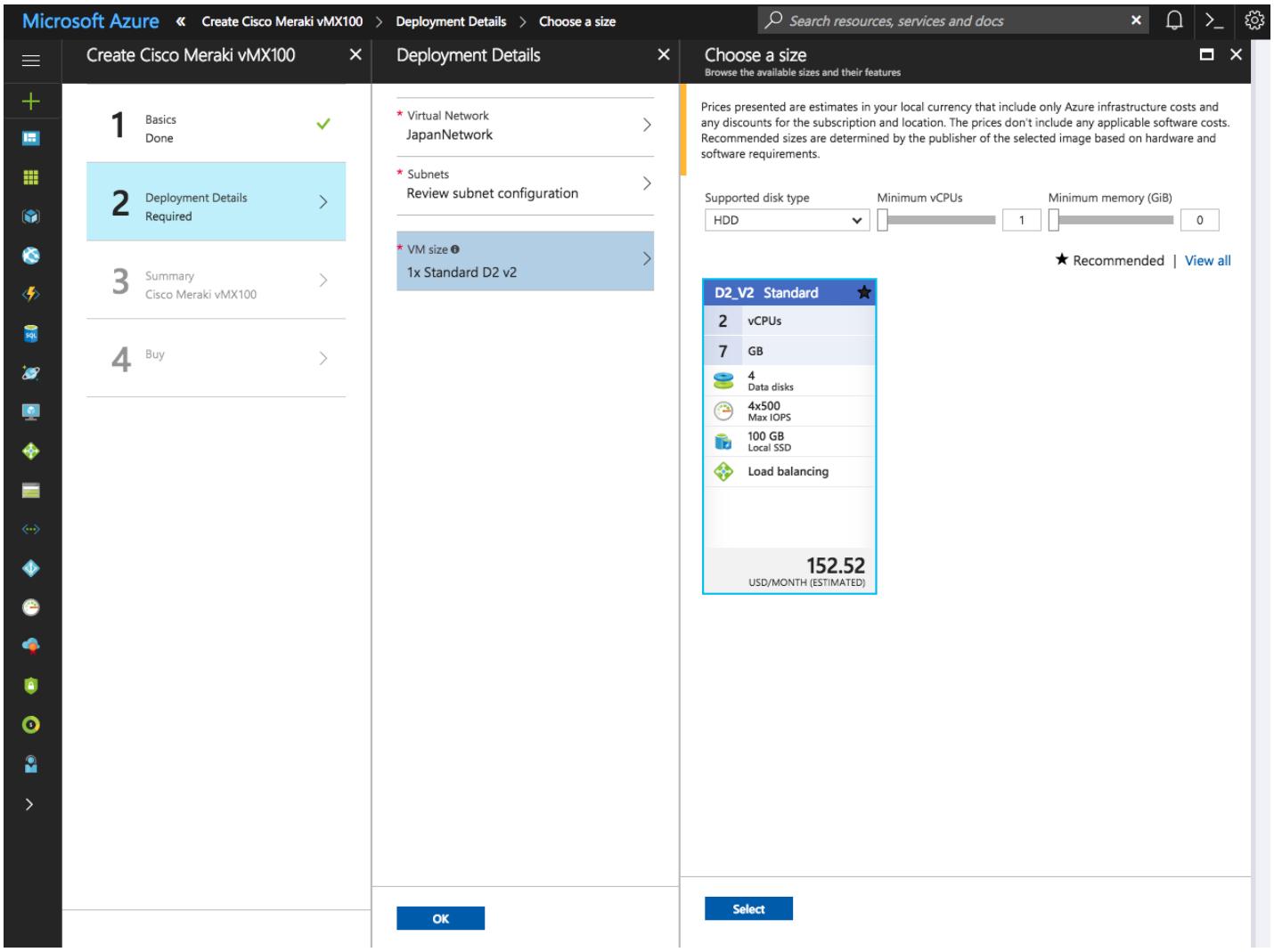
Choose an existing Virtual Network from the list:



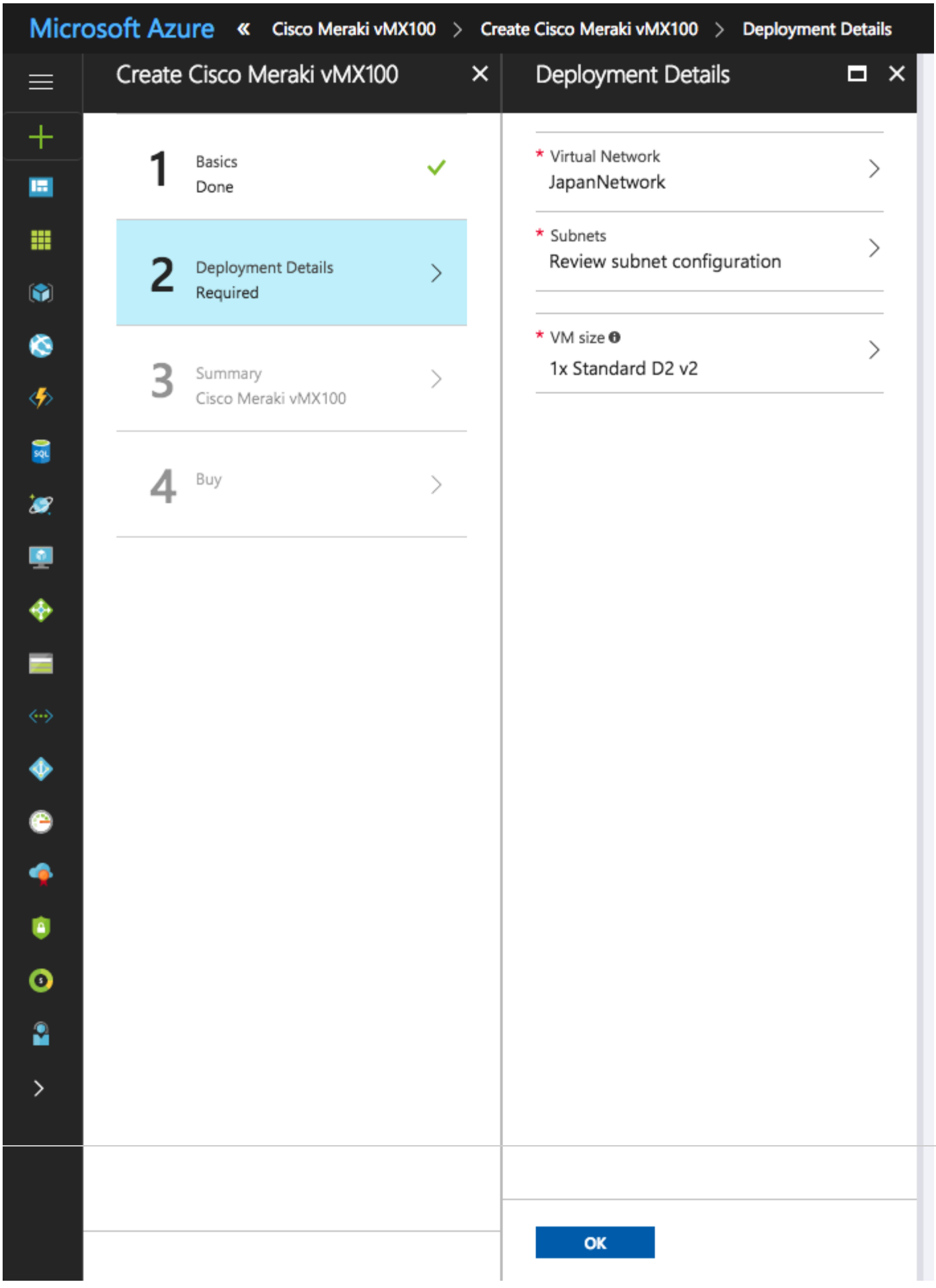
Then choose the subnet in which the vMX will be deployed. To find more information about subnets in Azure, click here.

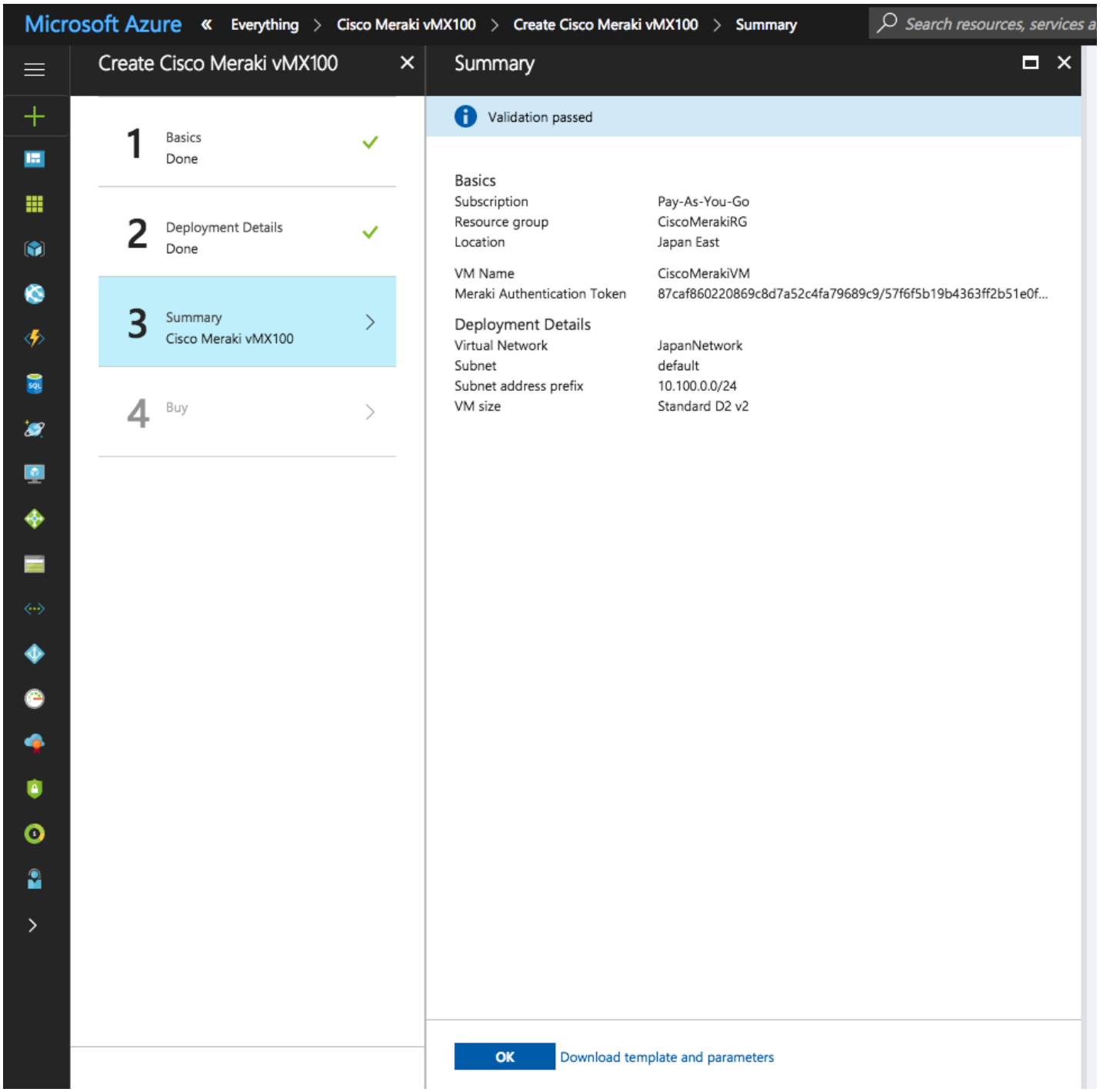


Choose the VM size which will be D2_V2 Standard:

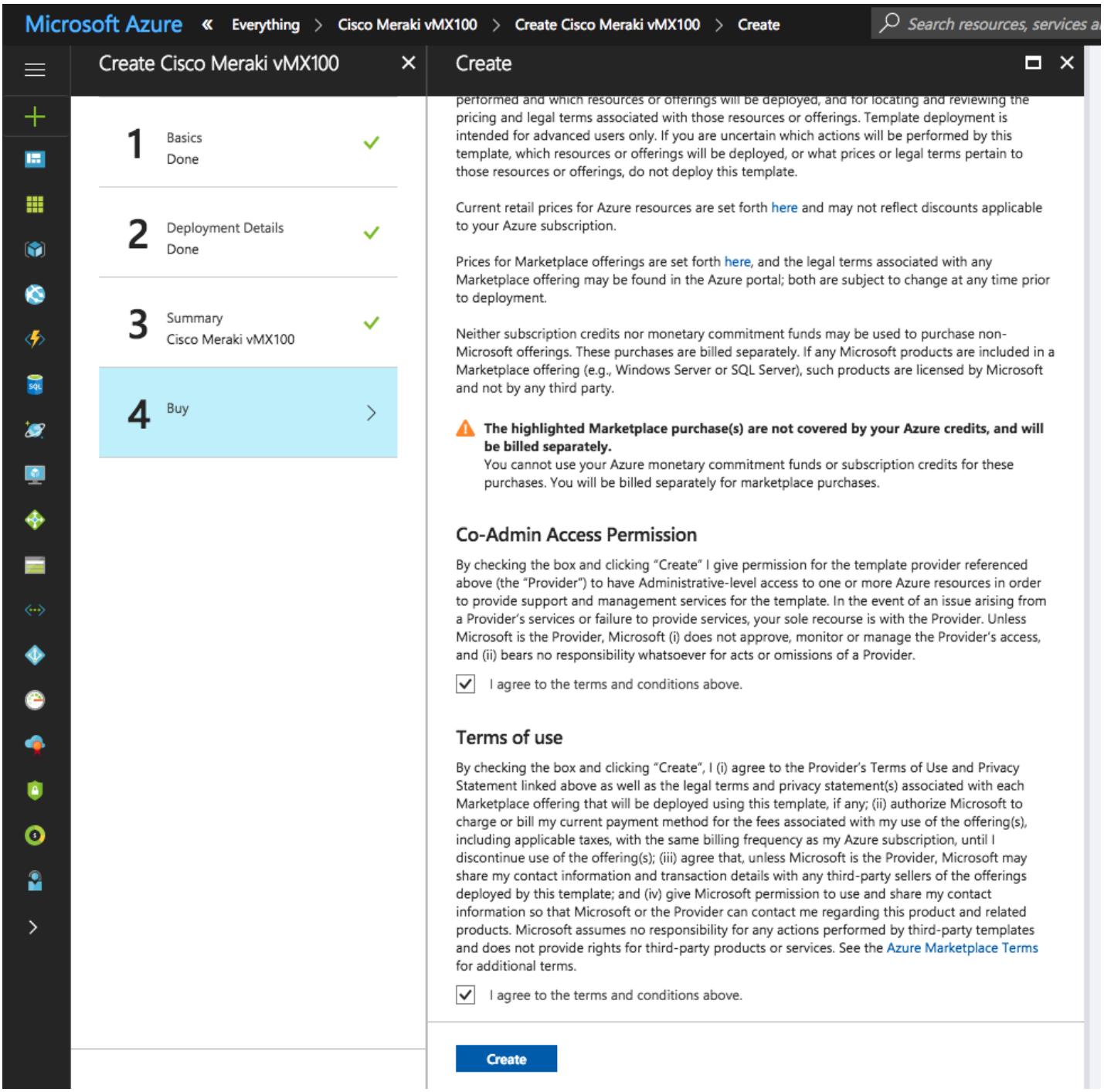


Review the deployment details before hitting 'OK.'

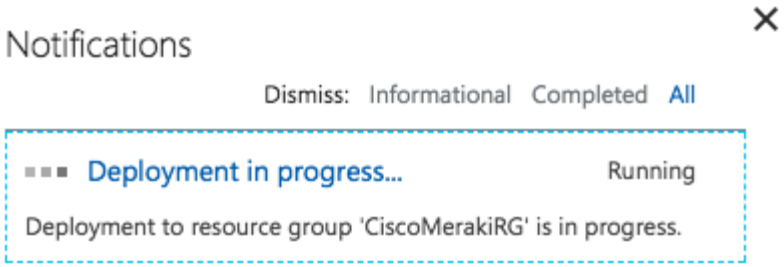

Microsoft Azure
Cisco Meraki vMX100
Create Cisco Meraki vMX100
Deployment Details
Create Cisco Meraki vMX100
1 Basics
Done
2 Deployment Details
Required
3 Summary
Cisco Meraki vMX100
4 Buy
Deployment Details
* Virtual Network
JapanNetwork
* Subnets
Review subnet configuration
* VM size
1x Standard D2 v2
OK



Review the terms of use and privacy policy before hitting 'Create.'

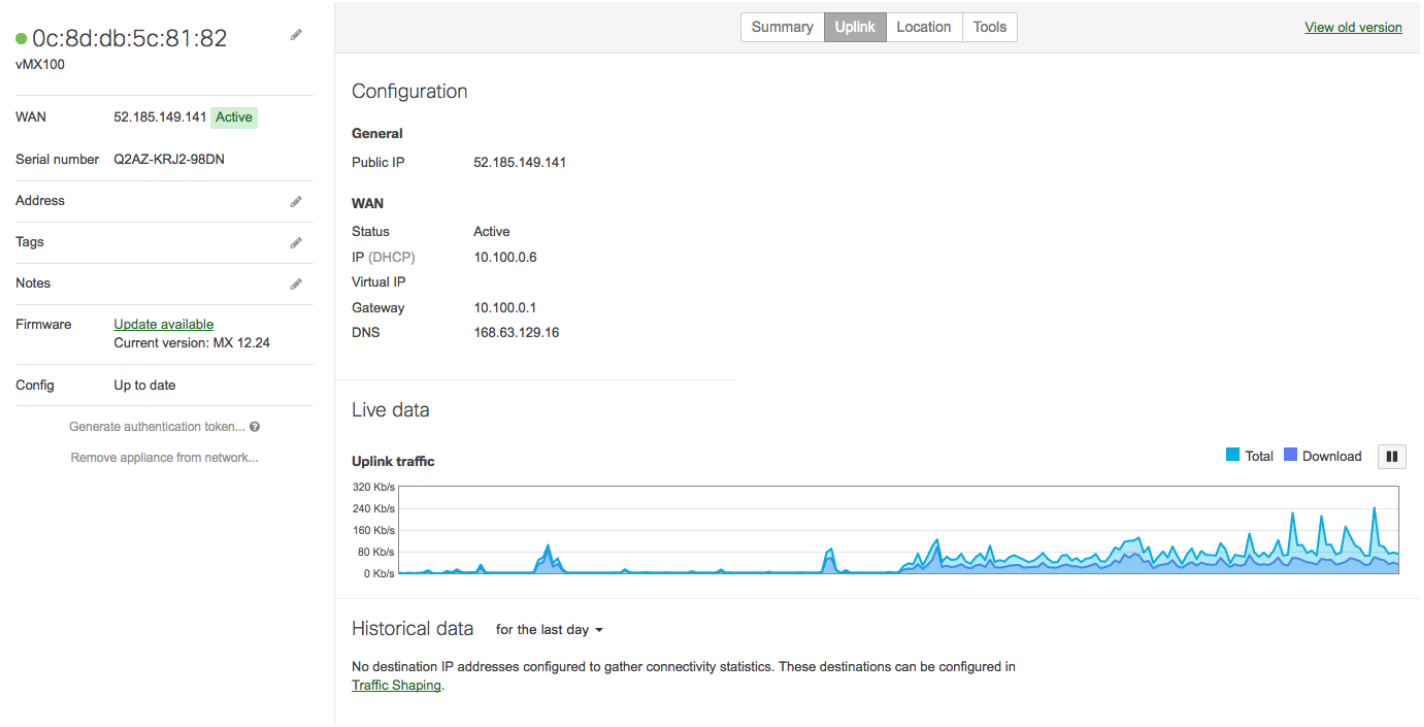


After you click on 'Purchase,' the deployment will begin:



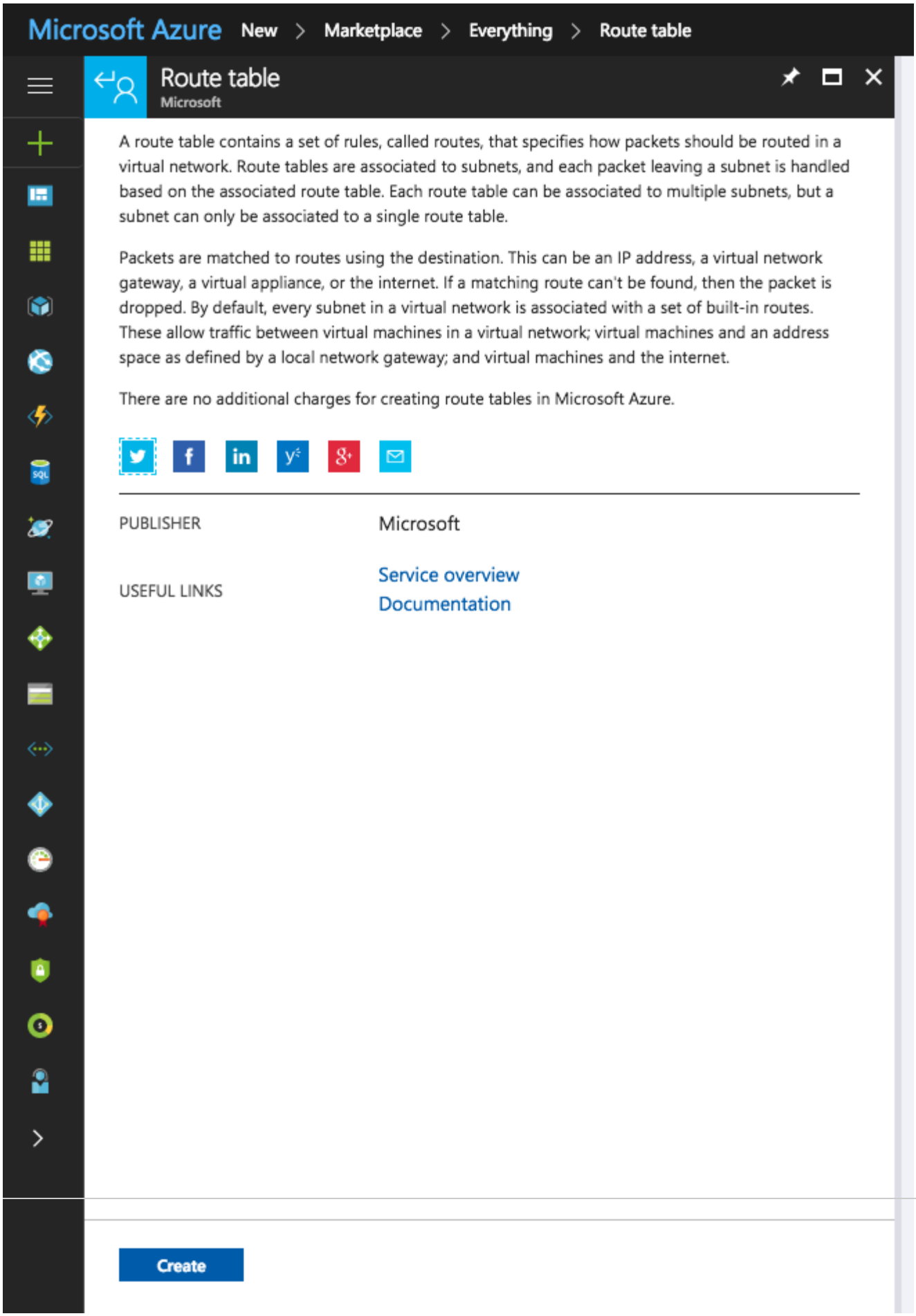
Once this has been completed, it may be several minutes before the deployment completes and the instance launches.

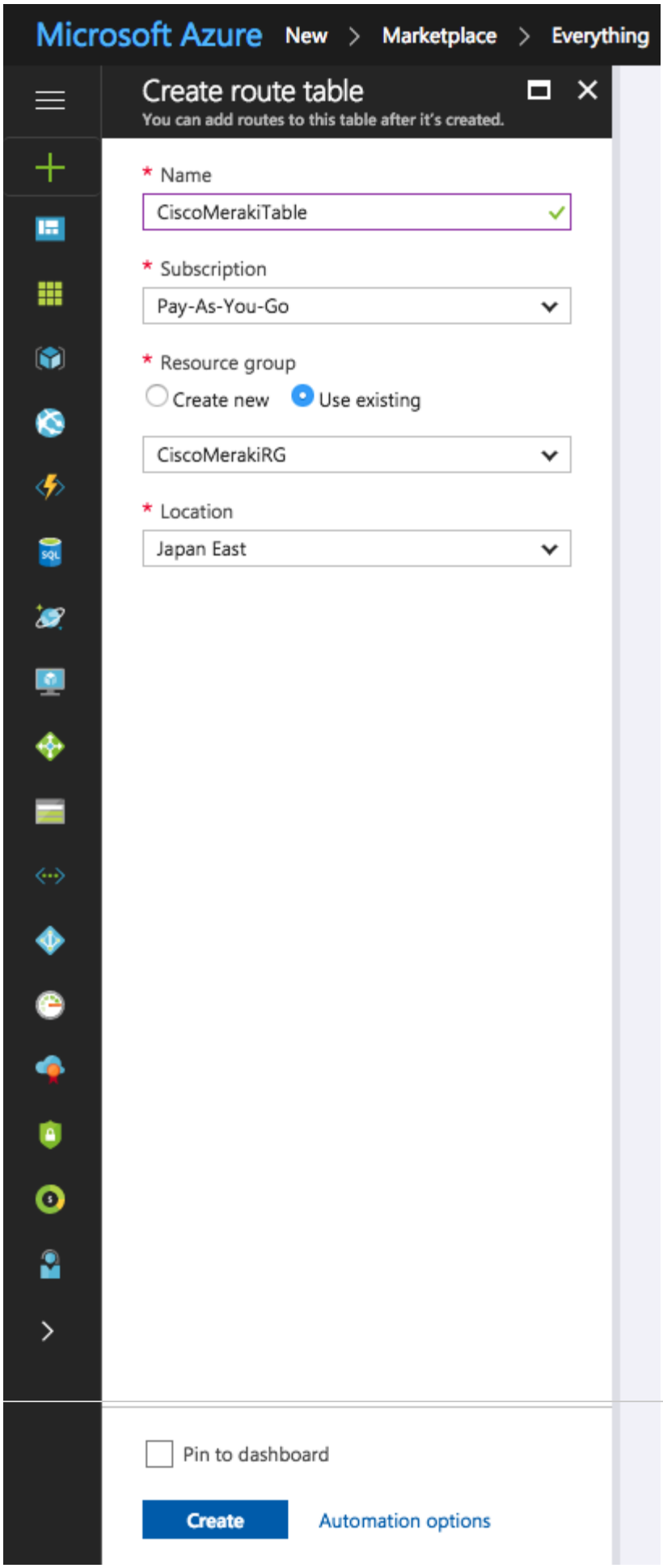
> **Note**: Once the deployment has finished, it is expected that a new resource group will be created with the name of the resource group you referenced, appended with a random string of characters.



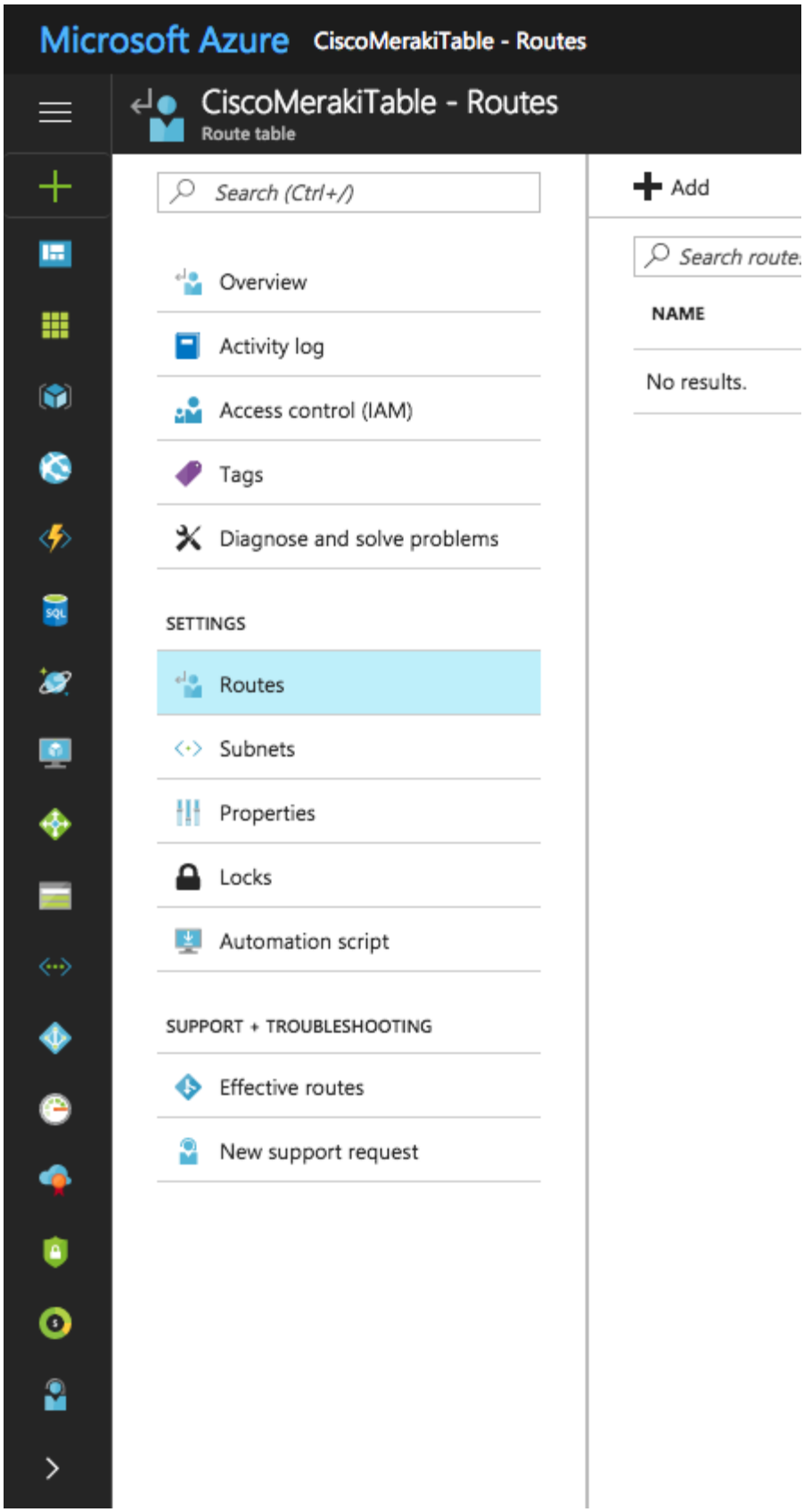
Once the vMX100 is online, a route table needs to be created including the Auto VPN subnets so that the Azure resources know how to access the Meraki subnets over Auto VPN.

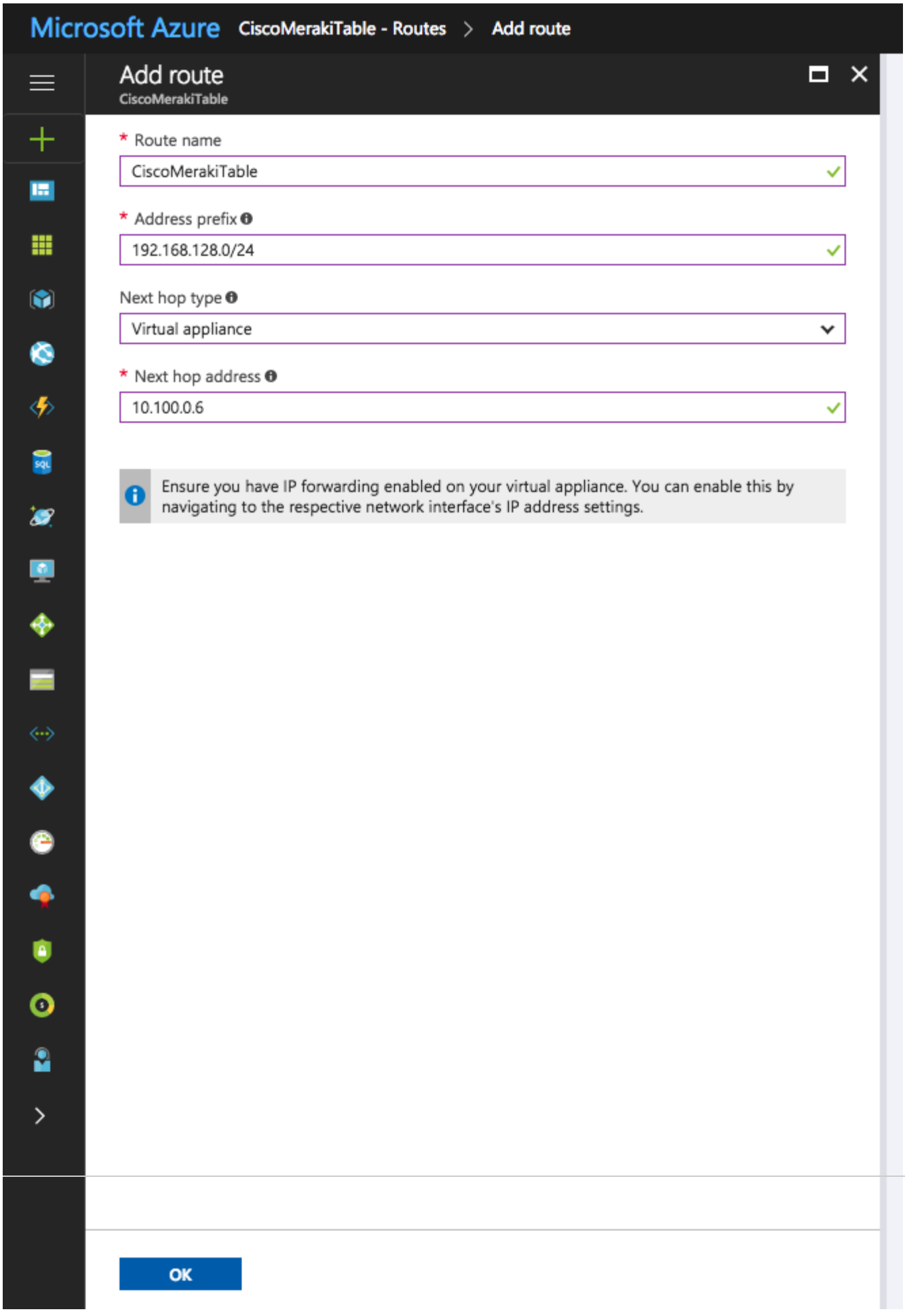
To create a route table, click on "New" and then "Route Table".


Microsoft Azure
New
Marketplace
Everything
Route table
Route table
Microsoft
A route table contains a set of rules, called routes, that specifies how packets should be routed in a virtual network. Route tables are associated to subnets, and each packet leaving a subnet is handled based on the associated route table. Each route table can be associated to multiple subnets, but a subnet can only be associated to a single route table.
Packets are matched to routes using the destination. This can be an IP address, a virtual network gateway, a virtual appliance, or the internet. If a matching route can't be found, then the packet is dropped. By default, every subnet in a virtual network is associated with a set of built-in routes. These allow traffic between virtual machines in a virtual network; virtual machines and an address space as defined by a local network gateway; and virtual machines and the internet.
There are no additional charges for creating route tables in Microsoft Azure.
PUBLISHER
Microsoft
USEFUL LINKS
Service overview
Documentation
Create


Microsoft Azure
New
Marketplace
Everything
Create route table
You can add routes to this table after it's created.
* Name
CiscoMerakiTable
* Subscription
Pay-As-You-Go
* Resource group
Create new
Use existing
CiscoMerakiRG
* Location
Japan East
Pin to dashboard
Create
Automation options

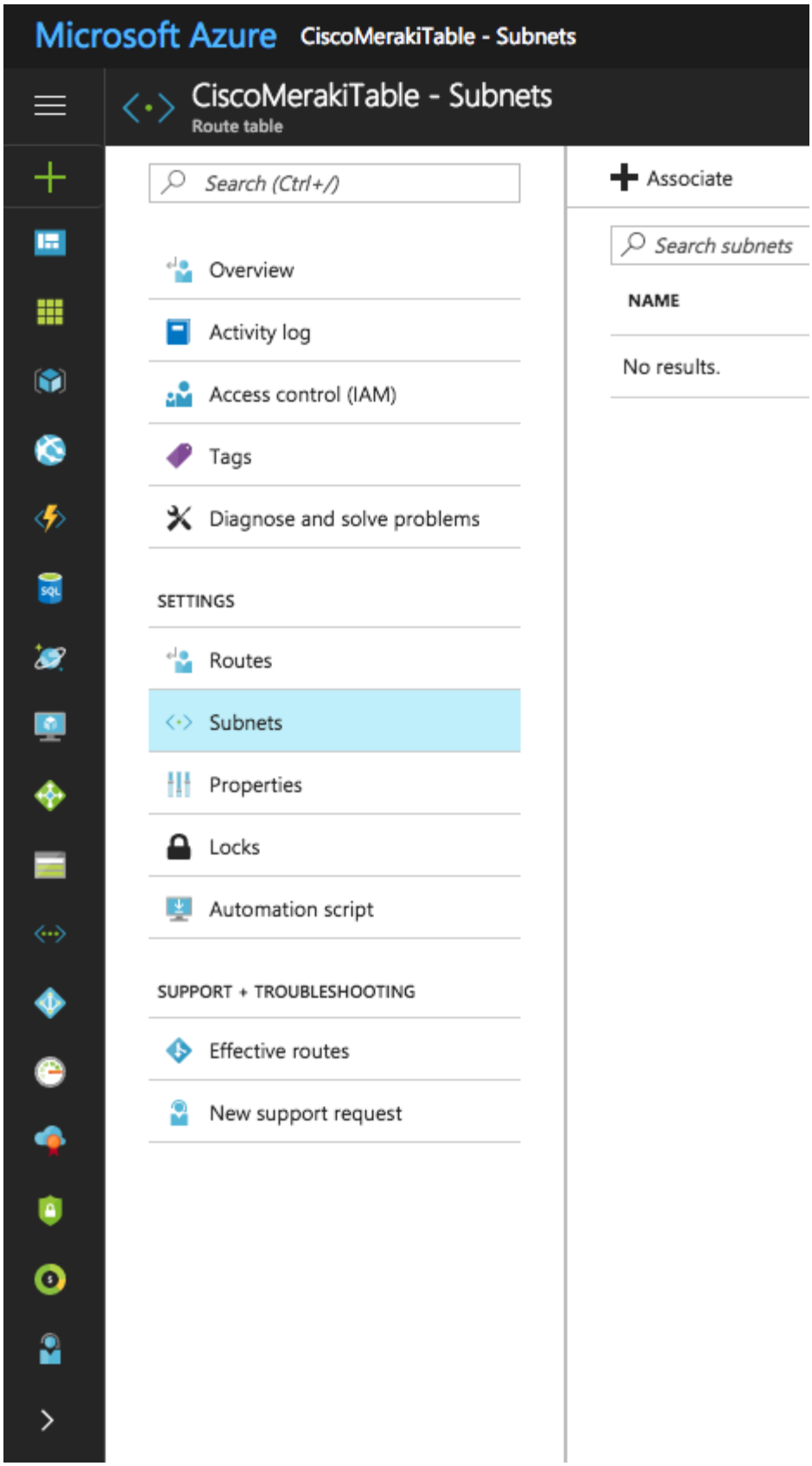
Once the Route Table has been created, add the VPN routes pointing to the vMX100 as the next hop, including the Client VPN subnet is applicable:


Microsoft Azure
CiscoMerakiTable - Routes
CiscoMerakiTable - Routes
Route table
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Routes
Subnets
Properties
Locks
Automation script
SUPPORT + TROUBLESHOOTING
Effective routes
New support request
Add
Search route
NAME
No results.

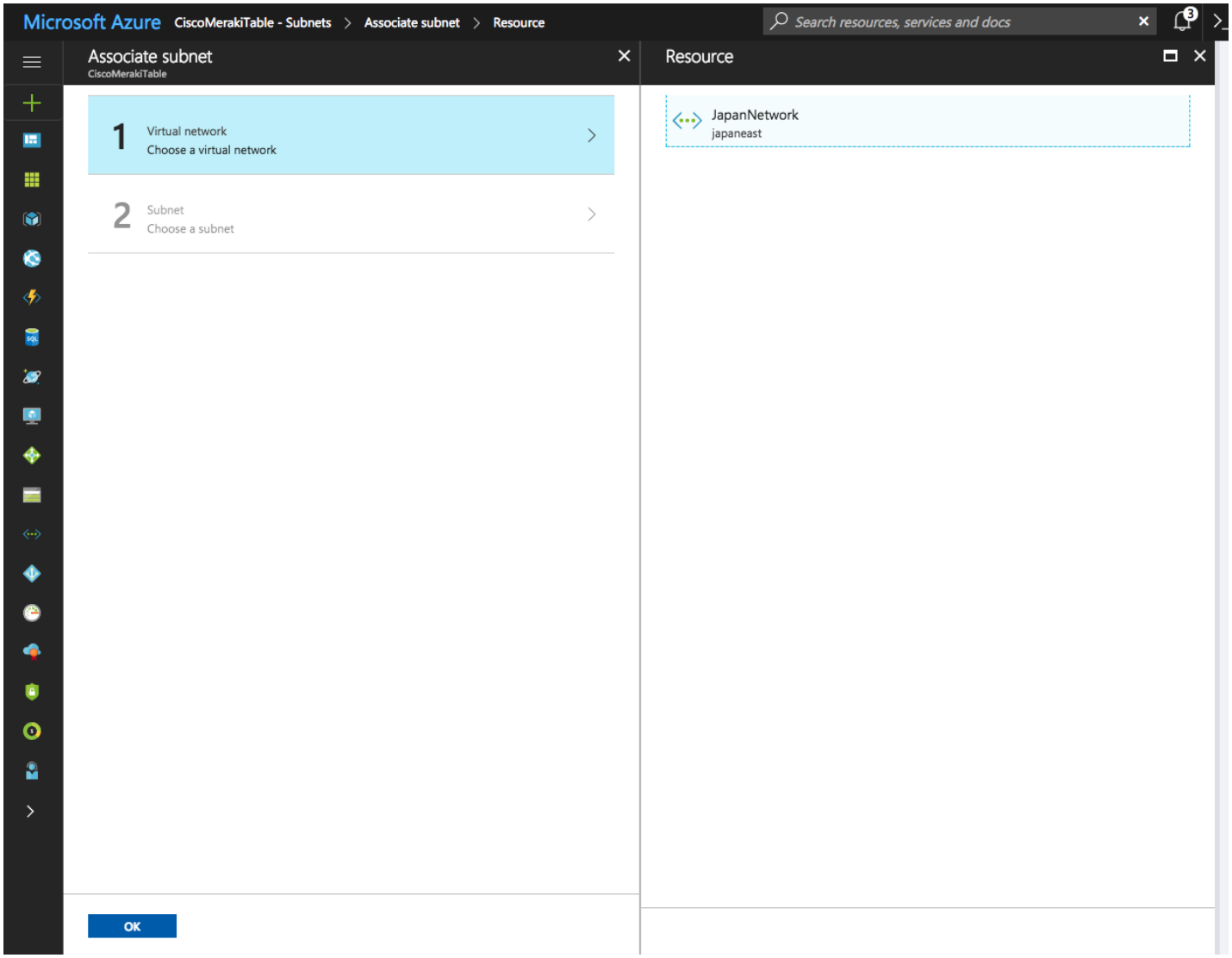

Microsoft Azure
CiscoMerakiTable - Routes
Add route
Add route
CiscoMerakiTable
* Route name
CiscoMerakiTable
* Address prefix
192.168.128.0/24
Next hop type
Virtual appliance
* Next hop address
10.100.0.6
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.
OK

Please ignore the IP forwarding warning, it has already been enabled in the backend.

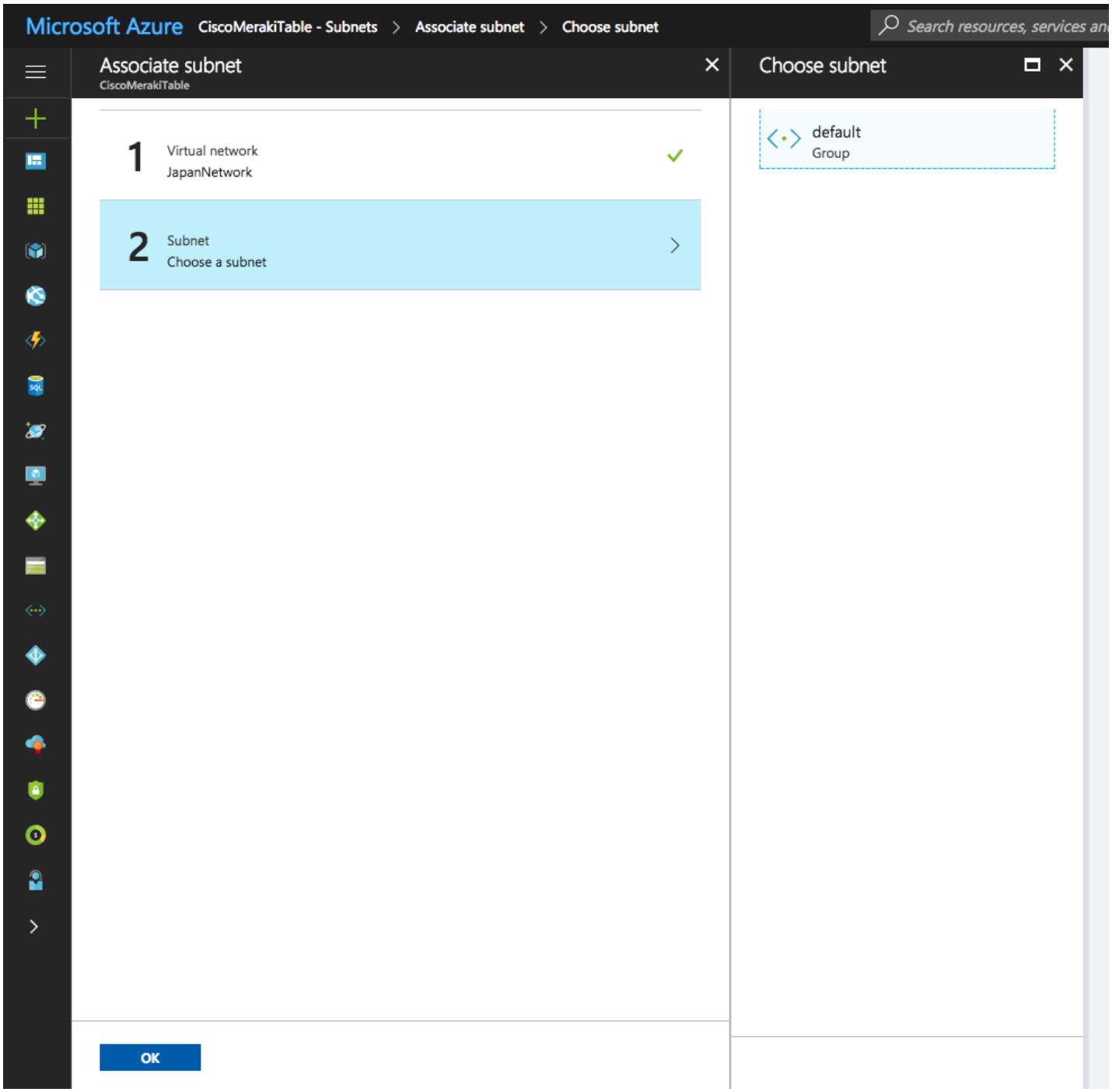
Finally, associate the Route Table with the Subnet where the vMX was deployed. Click on "Subnets" and then "Associate".


Microsoft Azure
CiscoMerakiTable - Subnets
CiscoMerakiTable - Subnets
Route table
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Routes
Subnets
Properties
Locks
Automation script
SUPPORT + TROUBLESHOOTING
Effective routes
New support request
Associate
Search subnets
NAME
No results.

Choose the Virtual Network where the vMX was deployed:



Then, choose the subnet used to deploy the vMX100 and click on 'OK.'



Once the subnet has been associated, enable Site to Site VPN on Dashboard.

Troubleshooting

The virtual MX security appliance is fully managed through the Cisco Meraki Dashboard. This requires the vMX100 to establish bi-directional communication to the Meraki Cloud. If, after following the steps above, the vMX100 is inaccessible, please ensure the following:

1. The following characters are not being used in the template: ' ~ ! @ # $ % ^ & * ( ) = + _ [ ] { } \\\\ | ; : ' \\\" , < > / ?.\" '.
2. Azure naming convention does not support spaces, make sure spaces in resource names are eliminated.
3. The token is entered into the Meraki Authentication Token field within an hour of being generated.
4. The DNS server is reachable from the subnet that the vMX100 is in and can resolve https://config-2037.meraki.com.
5. A Route Table has been created and associated to the correct subnet(s).

Please note that Meraki Support does not troubleshoot Azure specific firewall rules and deployments.

vMX100 on Azure CSP Portal

Meraki vMX100 is currently not available on the CSP portal. In the meantime, there is a workaround using an ARM template which has been attached to this article. If a CSP partner needs to deploy vMX100, then perform the following to access the portal in the context of the customer:

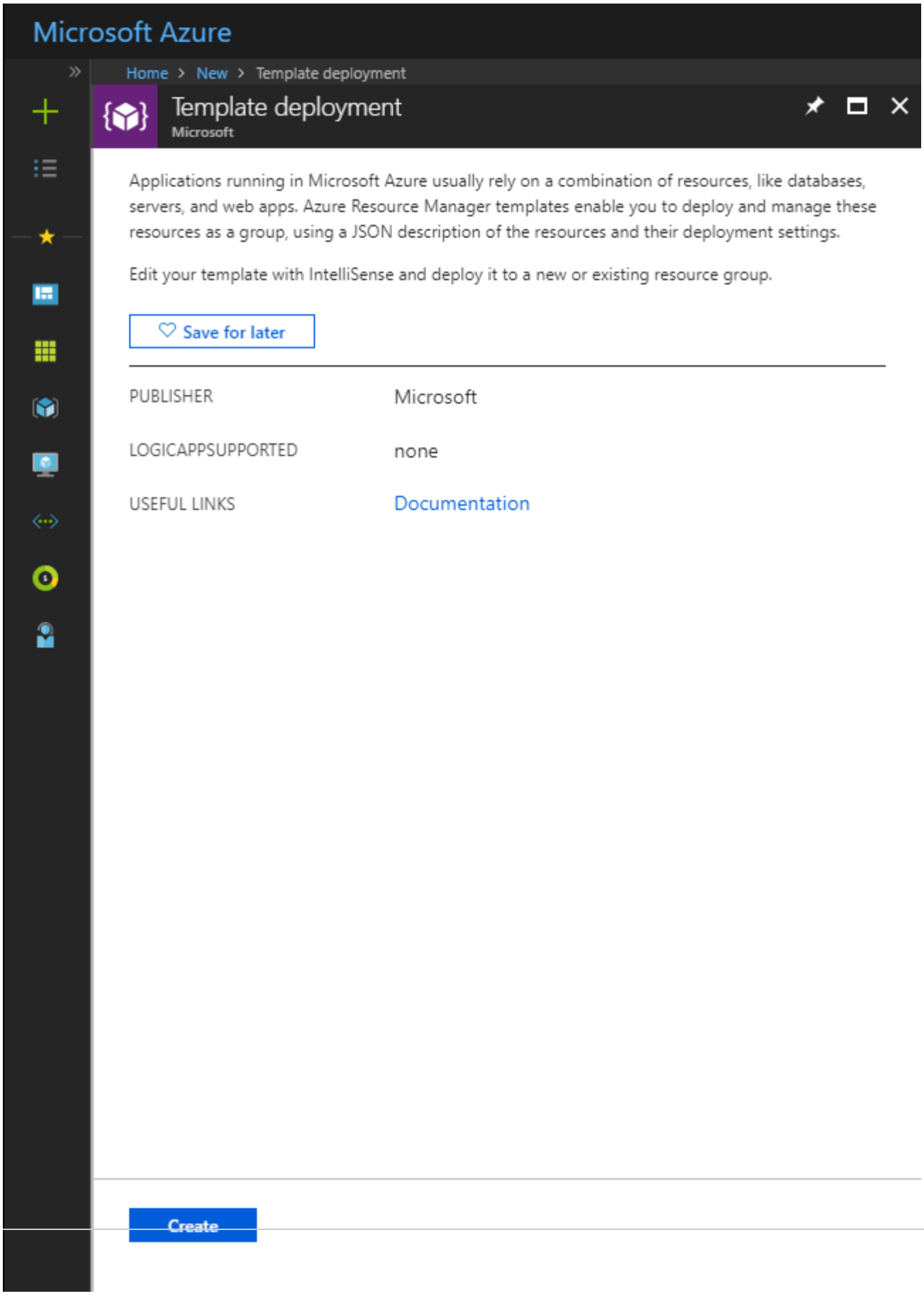
1. Login to Partner Center with credentials that have admin agent privileges
2. Click Dashboard and then Customers
3. Click on the customer where this resource should be deployed
4. Click Service Management and then click on the Microsoft Azure Management portal link

The above task will load the Azure Management portal, and it will be scoped to the context of the customer. This will enable you to deploy the template using the appropriate Azure subscription. To deploy this template perform the following

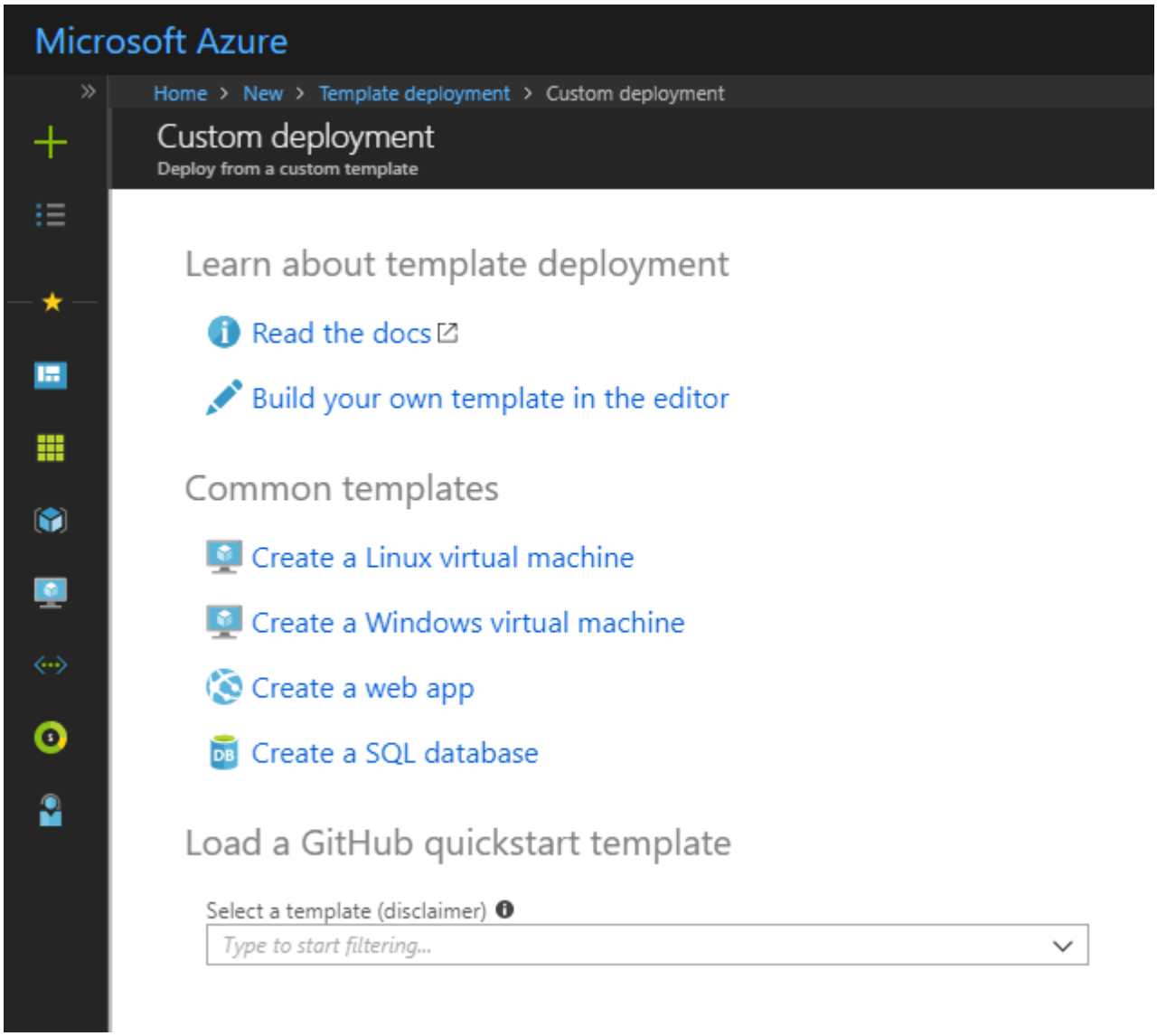
1. Extract the contents of the attached zip archive

2. Click the + *Create a resource* button located in the upper left

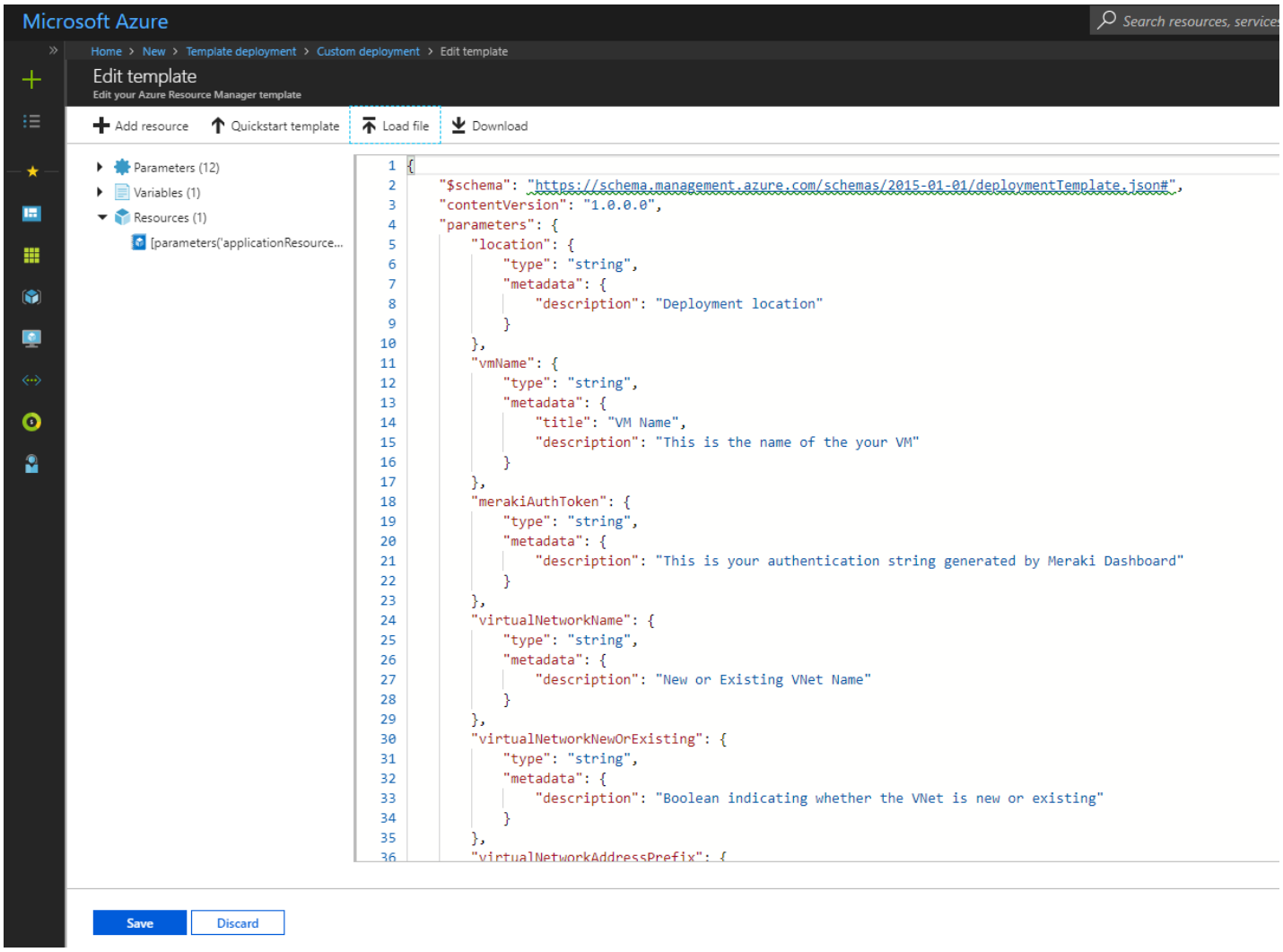
3. Search the marketplace for *Template deployment*, click the item, and then click the *Create* button


Microsoft Azure
Home > New > Template deployment
Template deployment
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.
Save for later
PUBLISHER
Microsoft
LOGICAPPSUPPORTED
none
USEFUL LINKS
Documentation
Create

4. Click the *Build your own template in the editor* link as shown in the figure below



5. Click the *Load File* button found at the top. Select the *azuredeploy.json* file and then click *Ok* to load the template



6. Click the *Save* button to complete the process of loading the template

7. Click the *Edit parameters* button

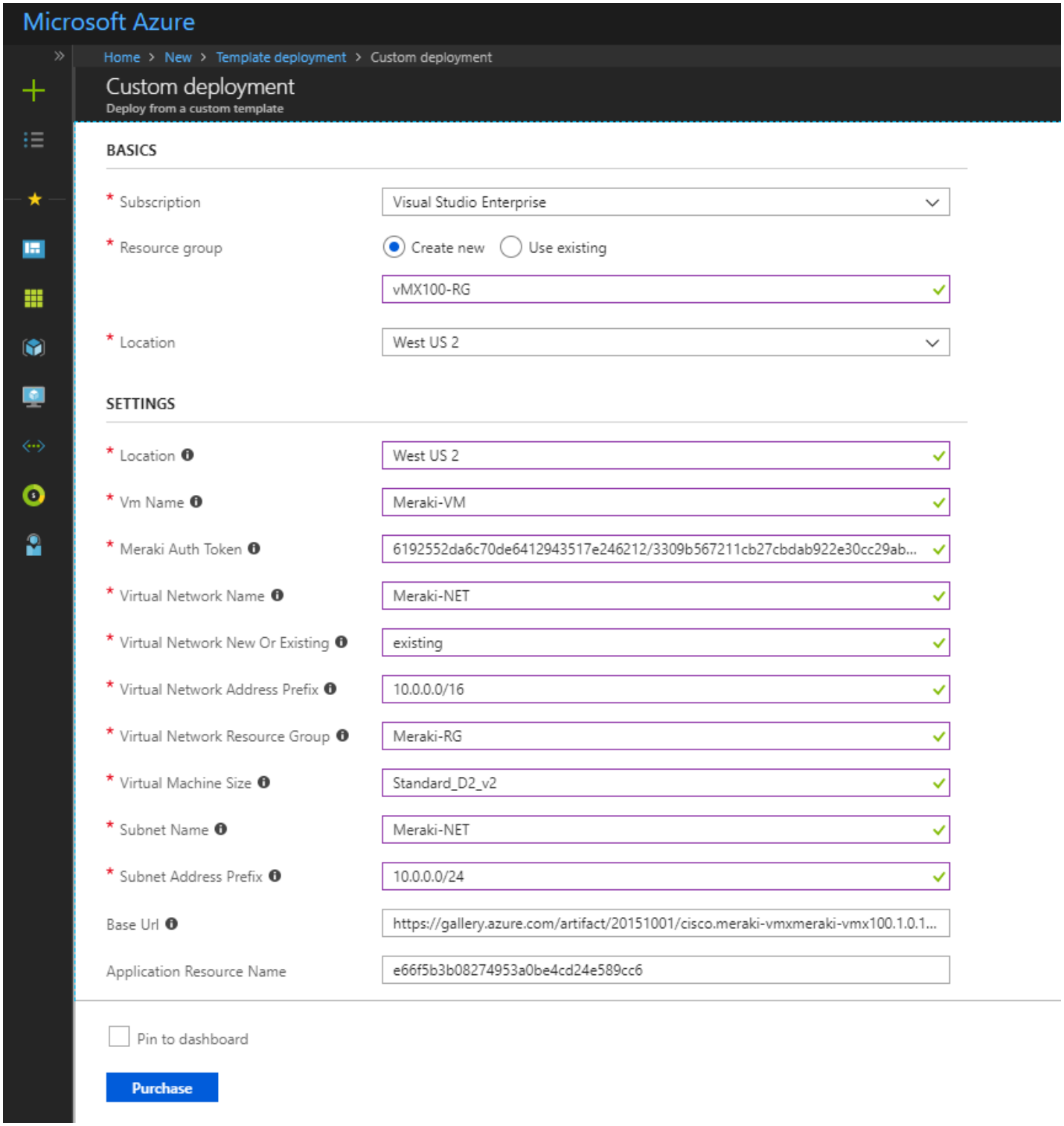
8. Click the *Load File* button found at the top. Select the *azuredeploy.parameter.json* file and then click *Ok* to load the parameters

9. Click the *Save* button to complete the process of loading the parameters

10. Modify the *Settings* value to correctly match the customer's environment.

> Please note that for the "Basics" section a new resource group should be created to avoid locking existing resources.

When filling out the "Settings" section, use the information of an existing Virtual Network.



11. Check the *I agree to the terms and conditions stated above* checkbox after you have reviewed the terms and condition. By checking the box you will be agreeing to the terms.

12. Click the *Purchase* button

This will start the deployment and within a few moments, the appliance will be deployed.