vAPV Installation Guide for Microsoft Azure

Copyright Statement

Copyright©2016 Array Networks, Inc., 1371 McCarthy Blvd, Milpitas, California 95035, USA. All rights reserved.

This document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and compilation. No part of this document may be reproduced in any form by any means without prior written authorization of Array Networks, Inc. Documentation is provided "as is" without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

Array Networks, Inc., reserves the right to change any products described herein at any time, and without notice. Array Networks, Inc. assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Array Networks, Inc. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Array Networks, Inc.

Warning: Modifications made to the Array Networks unit, unless expressly approved by Array Networks, Inc., could void the user's authority to operate the equipment.

Contacting Array Networks

Please use the following information to contact us at Array Networks:

- **Website:**

https://www.arraynetworks.com/

- **Telephone:**

Phone: (408)240-8700

Toll Free: 1-866-692-7729 (1-866-MY-ARRAY)

Support: 1-877-992-7729 (1-877-99-ARRAY)

Fax: (408)240-8754

Telephone access to Array Networks, Inc. is available Monday through Friday, 9 A.M. to 5 P.M. PST.

- **E-mail:**

info@arraynetworks.com

- **Address:**

1371 McCarthy Boulevard

Milpitas, California 95035, USA

Revision History

Date	Description
September 10, 2015	Initial official version.
July 28, 2016	Updated for the APV 8.6 release in August 2016.

Table of Contents

1 Introduction

Array vAPV is a virtual version of the Array APV Series application delivery controller, which provides comprehensive layer 3-7 load balancing and traffic management, acceleration and Web application firewall with DDoS protection.

Microsoft Azure is a cloud computing platform and infrastructure, created by Microsoft, for building, deploying and managing applications and services through a global network of Microsoft-managed and Microsoft partner-hosted datacenters. It provides both platform-as-a-service (PaaS) and Infrastructure-as-a-service (IaaS) services and supports many different programming languages, tools and frameworks, including both Microsoft-specific and third-party software and systems.

Array now provides support for deploying the vAPV as an instance (virtual machine) on the Microsoft Azure cloud computing platform. Array vAPV is available as an instance image in the Azure Marketplace. With this support, Microsoft Azure customers can leverage Array vAPV load balancing and other valuable features to better meet their business needs in the Azure cloud-computing environment.

1.1 Supported Instance Types

Microsoft Azure supports multiple virtual machine sizes (instance types), which are different in disk sizes, processing speed and other capacities. Array vAPV for Azure currently supports the following instance types:

Table 1–1 Instance Types

Instance Type	Purpose
A0~A3	General purpose compute: Basic tier (without Load Balancing)
A0~A3	General purpose compute: Standard tier
D1~D2	Optimized compute: 60% faster CPUs, more memory, and local SSD

Note: The vAPV instance for Azure supports a maximum of 32 CPUs and 64 GB memory.

For details of system configurations that each instance type supports, please refer to http://azure.microsoft.com/en-us/pricing/details/virtual-machines/.

1.2 How Array vAPV Works on Microsoft Azure

In a Microsoft Azure cloud service with the vAPV instance deployed, user traffic will be received by the Azure cloud service first, and then forwarded to the vAPV instance based on the inbound security rules. Then the vAPV instance will forward the user traffic to the servers, as shown in the following figure:

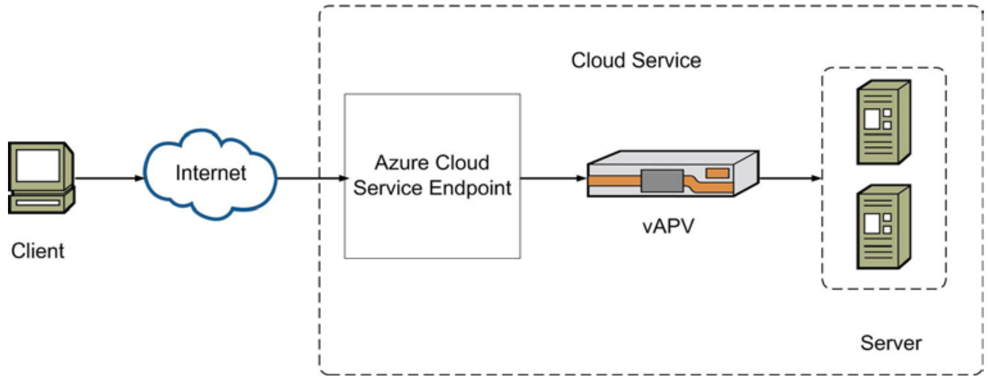


Figure 1–1 Azure Cloud Service with vAPV Deployed

1.3 Usage Limitations and Guidelines

- Currently, vAPV for Azure has the following limitations:
- In the Azure cloud service architecture, the vAPV instance is provided only one interface. The vAPV instance can have two IP addresses: one public IP address and one private IP address. These IP addresses can be obtained via DHCP only. On the vAPV instance, all the VIPs, management IP addresses and IP addresses used for communication with real servers must use the private IP address obtained via DHCP. Please do not change the private IP address manually for the vAPV instance; otherwise, it will lead to network interruption.
- Azure forwards the user traffic destined for the public IP address to the vAPV based on inbound security rules. Therefore, inbound security rules should be configured for ports of vAPV's SLB virtual services and management services on Azure.
- vAPV for Azure supports the following features:
  - Server Load Balancing (SLB) (Layer 3-7)
  - SSL Acceleration (software SSL only)
  - HTTP Proxy (content rewrite, compression, cache, etc.)
  - Application Security
- vAPV for Azure supports only the BYOL (Bring Your Own License) license mode. Please refer to the section 2.3 Loading the vAPV License for how to load the vAPV license.

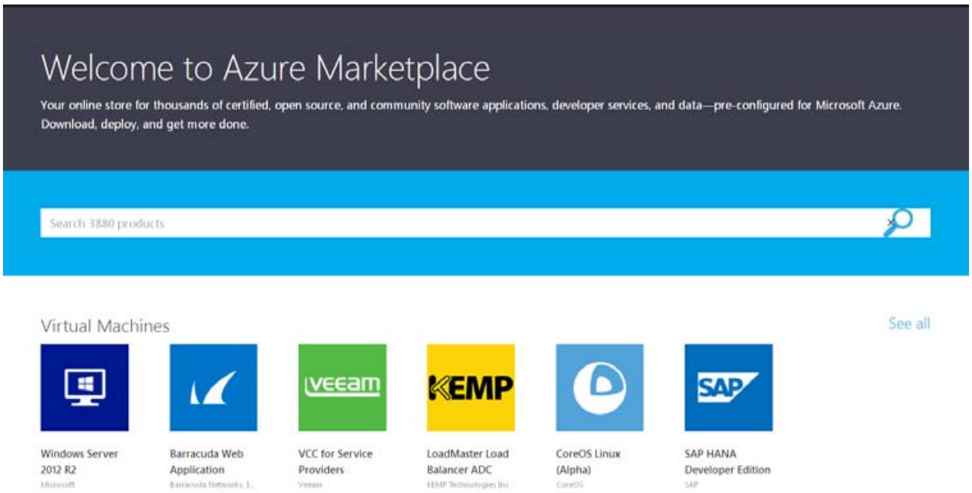
2 Deployment

This section describes the deployment process of the vAPV instance on Microsoft Azure.

2.1 Deploying the vAPV Instance on Microsoft Azure

To deploy the vAPV instance on Microsoft Azure, please perform the following steps:

1. Log into Microsoft Azure (http://azure.microsoft.com) with a valid account. Click **Partners** and then Click **Browse the Marketplace**, as shown in the following figure.

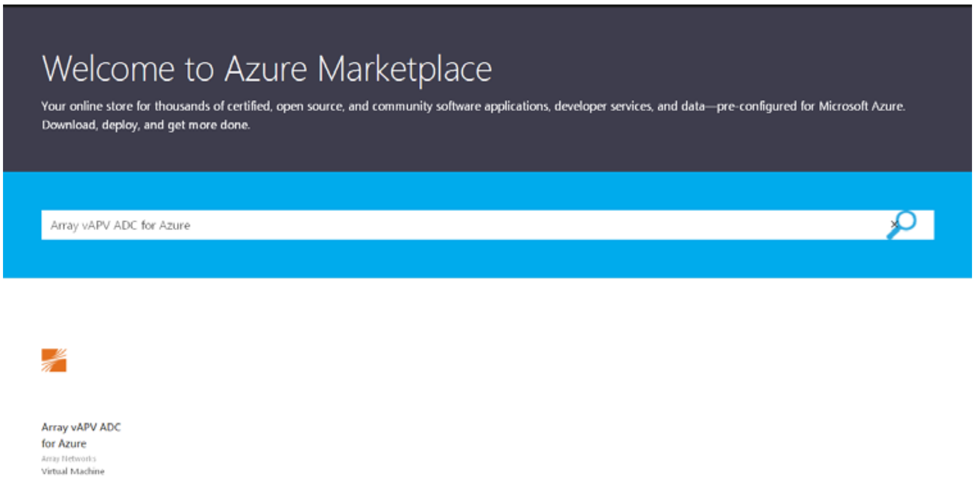


Welcome to Azure Marketplace

Your online store for thousands of certified, open source, and community software applications, developer services, and data—pre-configured for Microsoft Azure. Download, deploy, and get more done.

Figure 2–1 Enter the Marketplace

2. Enter “**Array vAPV ADC for Azure**” in the search box and press “Enter”, as shown in the following figure.

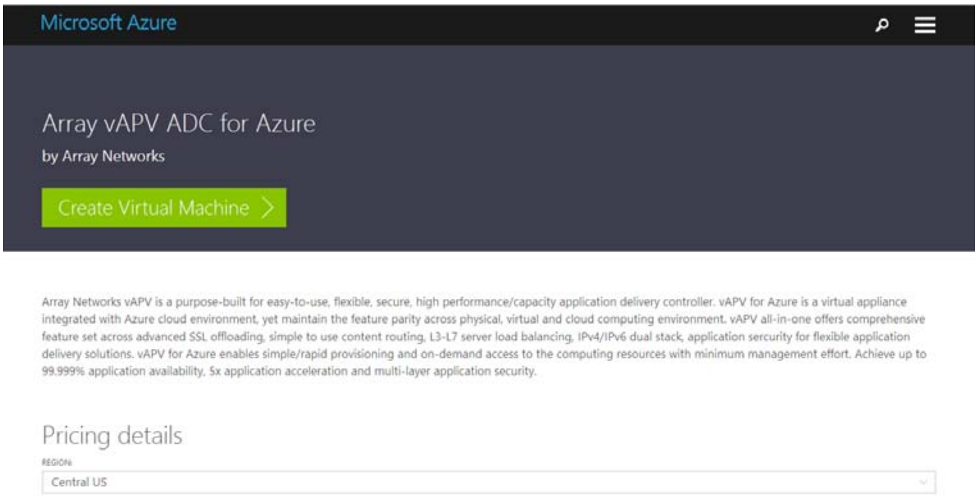


Welcome to Azure Marketplace

Your online store for thousands of certified, open source, and community software applications, developer services, and data—pre-configured for Microsoft Azure. Download, deploy, and get more done.

Figure 2–2 Search for the vAPV image

3. Click **Array vAPV ADC for Azure** and then click **Create Virtual Machine** on the pop-up page, as shown in the following figure.



Array vAPV ADC for Azure

by Array Networks

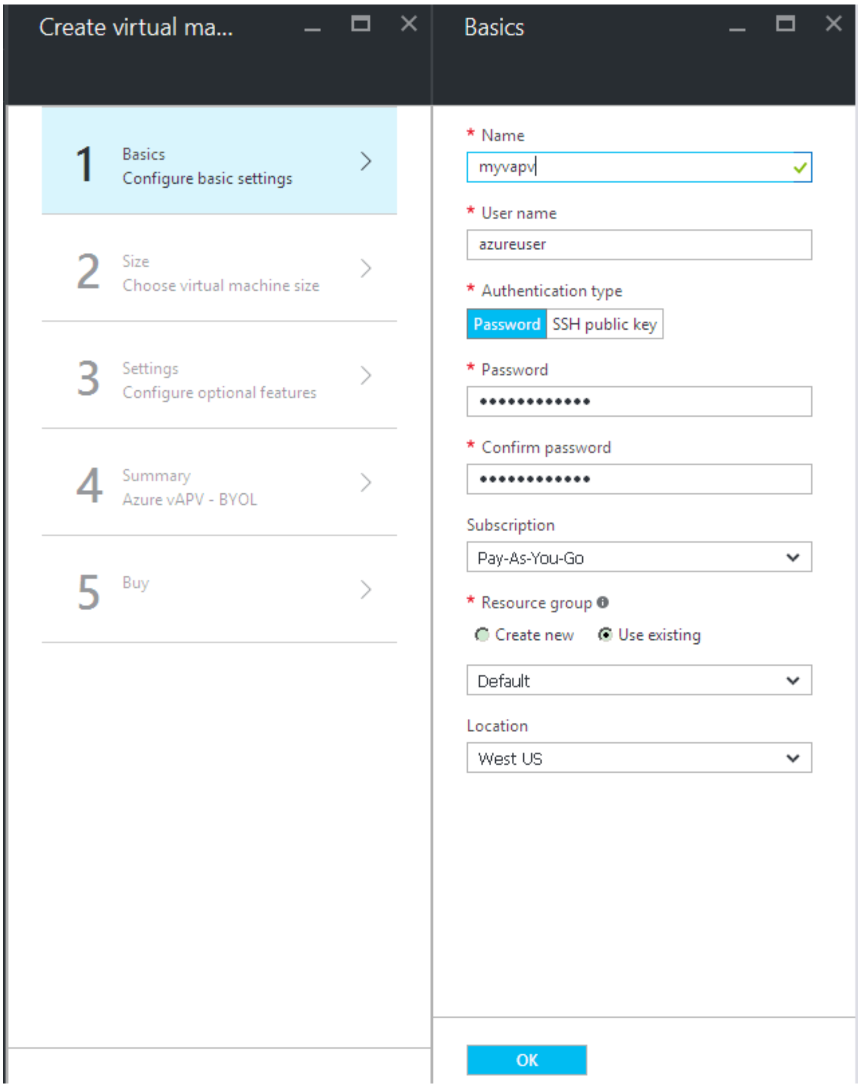
Array Networks vAPV is a purpose-built for easy-to-use, flexible, secure, high performance/capacity application delivery controller. vAPV for Azure is a virtual appliance integrated with Azure cloud environment, yet maintain the feature parity across physical, virtual and cloud computing environment. vAPV all-in-one offers comprehensive feature set across advanced SSL offloading, simple to use content routing, L3-L7 server load balancing, IPv4/IPv6 dual stack, application sercurity for flexible application delivery solutions. vAPV for Azure enables simple/rapid provisioning and on-demand access to the computing resources with minimum management effort. Achieve up to 99.999% application availability, 5x application acceleration and multi-layer application security.

Pricing details

REGION: Central US

Figure 2–3 Create a Virtual Machine

4. Click **Create** at the bottom-left corner on the pop-up page. Specify the parameters **Name**, **User Name**, **Password**, **Confirm password** and **Resource group**, select the **Authentication type** to be used and related parameters, and click **OK**, as shown in the following figure.



1 Basics
Configure basic settings

2 Size
Choose virtual machine size

3 Settings
Configure optional features

4 Summary
Azure vAPV - BYOL

5 Buy

* Name: myvapv

* User name: azureuser

* Authentication type: Password | SSH public key

* Password: ••••••••••••

* Confirm password: ••••••••••••

Subscription: Pay-As-You-Go

* Resource group: ○ Create new ● Use existing

Default

Location: West US

Figure 2–4 Configure Basic Setting of the vAPV Instance

5. Select the desired **virtual machine** size, and click **Select**, as shown in the following figure.

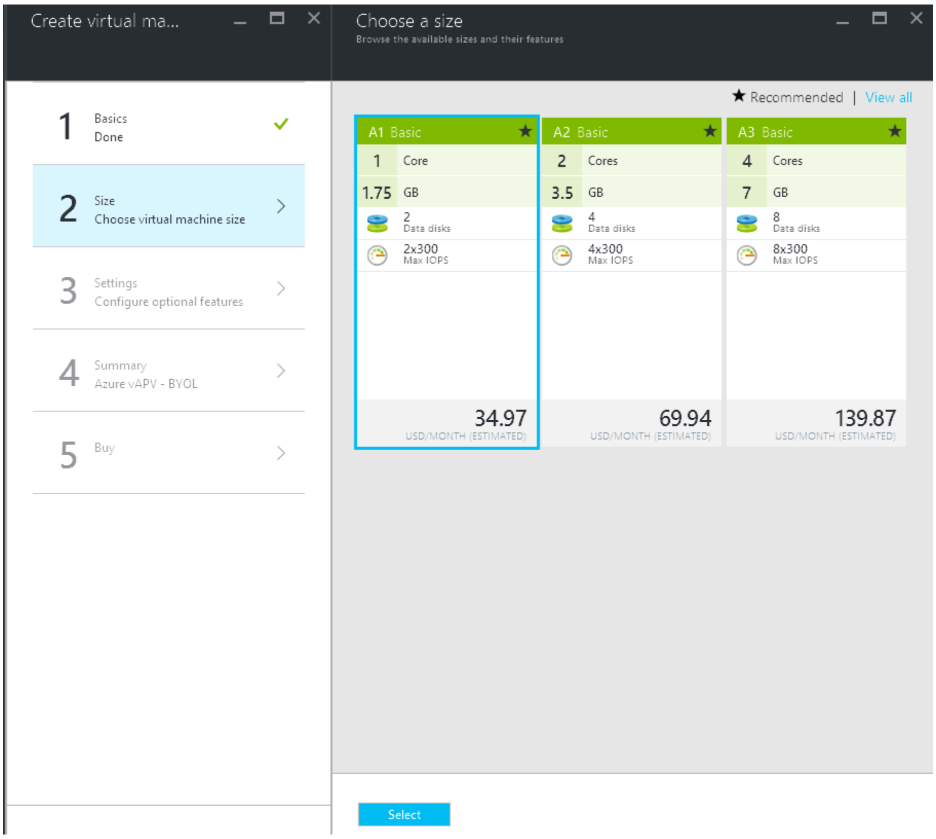
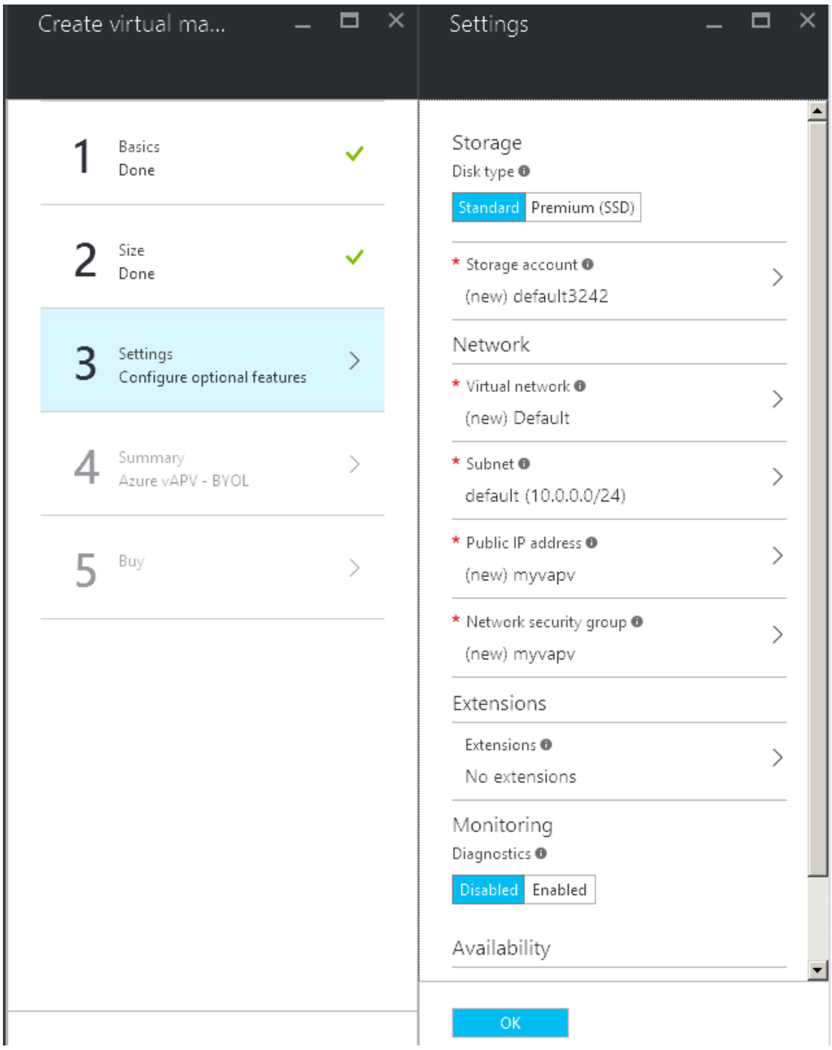

Create virtual ma...
1 Basics Done
2 Size Choose virtual machine size
3 Settings Configure optional features
4 Summary Azure vAPV - BYOL
5 Buy
Choose a size
Browse the available sizes and their features
★ Recommended | View all
A1 Basic ★
1 Core
1.75 GB
2 Data disks
2x300 Max IOPS
34.97 USD/MONTH (ESTIMATED)
A2 Basic ★
2 Cores
3.5 GB
4 Data disks
4x300 Max IOPS
69.94 USD/MONTH (ESTIMATED)
A3 Basic ★
4 Cores
7 GB
8 Data disks
8x300 Max IOPS
139.87 USD/MONTH (ESTIMATED)
Select

Figure 2–5 Choose the Size for the vAPV Instance

6. Specify the **Disk type** parameter and other related parameters, and set **Diagnostics** to **Disabled**. Click **OK**, as shown in the following figure.



1 Basics
Done ✓

2 Size
Done ✓

3 Settings
Configure optional features >

4 Summary
Azure vAPV - BYOL >

5 Buy >

Storage

Disk type
[✓ Standard] Premium (SSD)

* Storage account
(new) default3242

Network

* Virtual network
(new) Default

* Subnet
default (10.0.0.0/24)

* Public IP address
(new) myvapv

* Network security group
(new) myvapv

Extensions

Extensions
No extensions

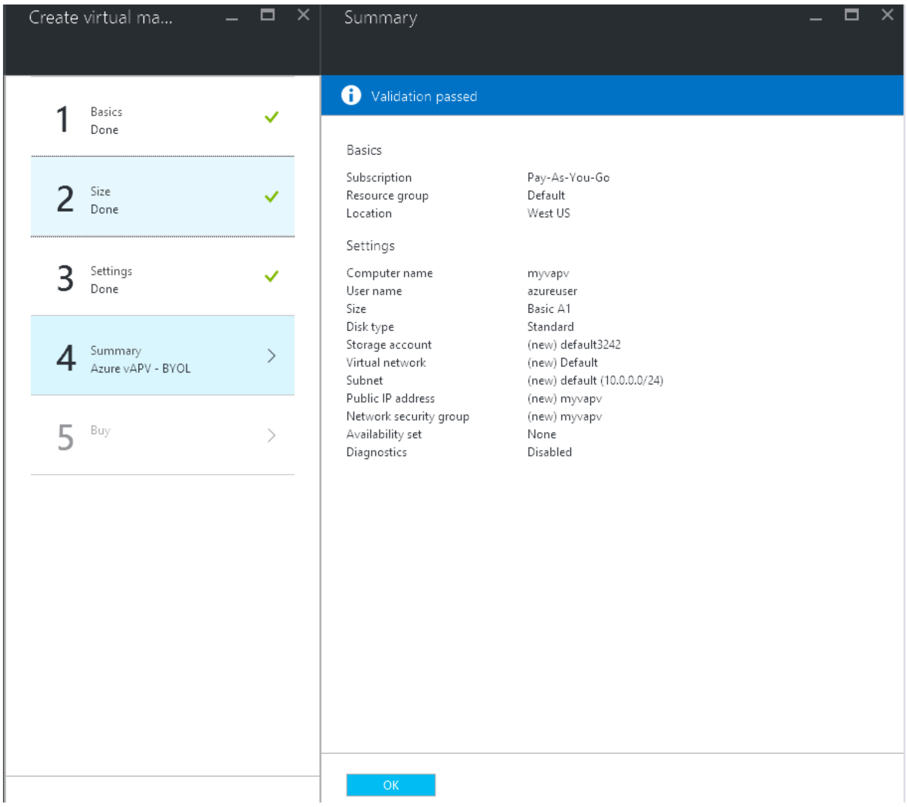
Monitoring

Diagnostics
[✓ Disabled] Enabled

Availability

Figure 2–6 Configure Optional Features for the vAPV Instance

7. Check the summary of the vAPV instance that you just created. If the settings are as you wish, click **OK** then, as show in the following figure.



Validation passed

Basics

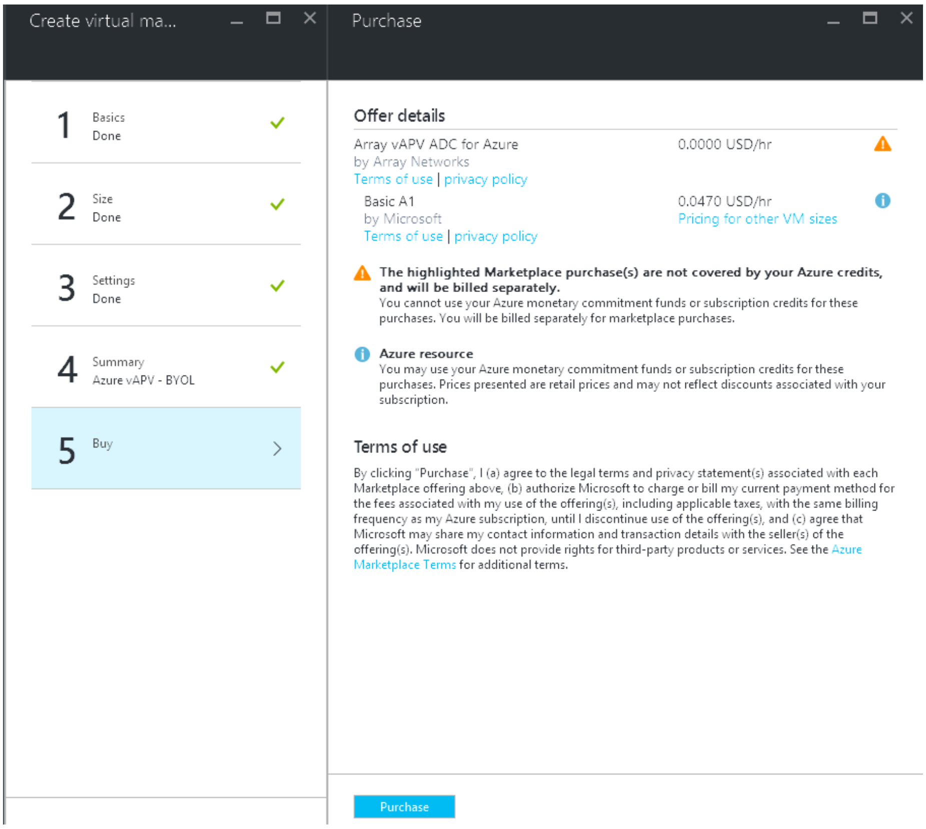
Subscription	Pay-As-You-Go
Resource group	Default
Location	West US

Settings

Computer name	myvapv
User name	azureuser
Size	Basic A1
Disk type	Standard
Storage account	(new) default3242
Virtual network	(new) Default
Subnet	(new) default (10.0.0.0/24)
Public IP address	(new) myvapv
Network security group	(new) myvapv
Availability set	None
Diagnostics	Disabled

Figure 2–7 Check Summary of the vAPV Instance

8. Click **Purchase** to purchase the vAPV instance.



Offer details

Array vAPV ADC for Azure by Array Networks Terms of use | privacy policy	0.0000 USD/hr
Basic A1 by Microsoft Terms of use | privacy policy	0.0470 USD/hr Pricing for other VM sizes

The highlighted Marketplace purchase(s) are not covered by your Azure credits, and will be billed separately.
You cannot use your Azure monetary commitment funds or subscription credits for these purchases. You will be billed separately for marketplace purchases.

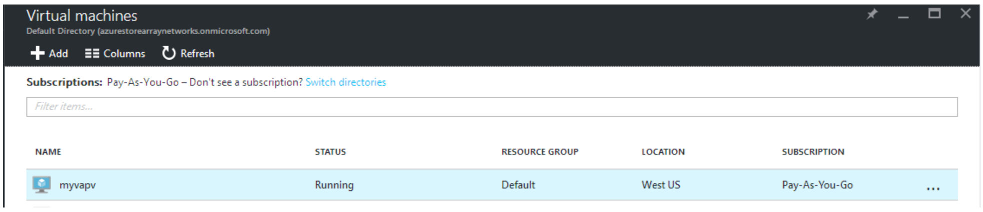
Azure resource
You may use your Azure monetary commitment funds or subscription credits for these purchases. Prices presented are retail prices and may not reflect discounts associated with your subscription.

Terms of use

By clicking "Purchase", I (a) agree to the legal terms and privacy statement(s) associated with each Marketplace offering above, (b) authorize Microsoft to charge or bill my current payment method for the fees associated with my use of 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 Microsoft may share my contact information and transaction details with the seller(s) of the offering(s). Microsoft does not provide rights for third-party products or services. See the Azure Marketplace Terms for additional terms.

Figure 2–8 Purchase the vAPV Instance

The newly created vAPV instance will be displayed, as shown in the following figure.



Virtual machines
Default Directory (azurestorearraynetworks.onmicrosoft.com)

Subscriptions: Pay-As-You-Go – Don't see a subscription? Switch directories

NAME	STATUS	RESOURCE GROUP	LOCATION	SUBSCRIPTION
myvapv	Running	Default	West US	Pay-As-You-Go

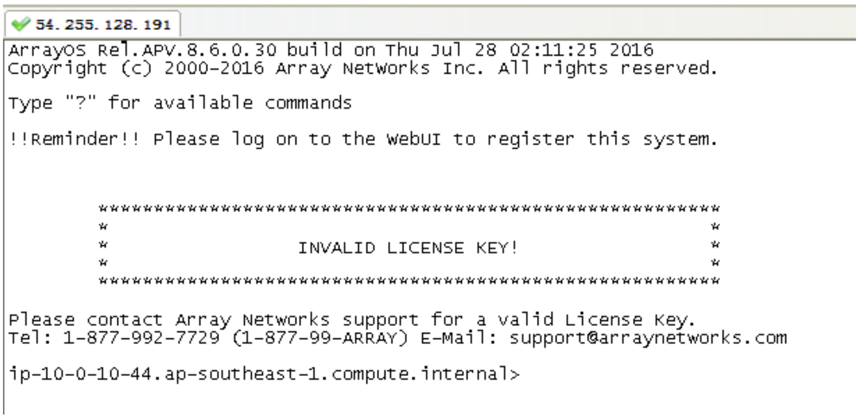
Figure 2–9 vAPV Instance Deployed Successfully

2.2 Accessing the vAPV Instance

2.2.1 Accessing the vAPV Instance via SSH

You can connect to the vAPV instance via SSH after the status of the newly created vAPV instance becomes "Running".

To access the vAPV instance via SSH, use its DNS name or the public IP address and SSH port 22 as the SSH access point.



```
ArrayOS Rel.APV.8.6.0.30 build on Thu Jul 28 02:11:25 2016
Copyright (c) 2000-2016 Array Networks Inc. All rights reserved.

Type "?" for available commands

!!Reminder!! Please log on to the WebUI to register this system.


        ******************************************************
        *                                                    *
        *                 INVALID LICENSE KEY!               *
        *                                                    *
        ******************************************************

Please contact Array Networks support for a valid License Key.
Tel: 1-877-992-7729 (1-877-99-ARRAY) E-Mail: support@arraynetworks.com

ip-10-0-10-44.ap-southeast-1.compute.internal>
```

Figure 2–10 Access the vAPV Instance via SSH

2.2.2 Accessing the vAPV Instance via WebUI

To access the vAPV via WebUI, you first need to access the vAPV instance via SSH to make the following configurations:

- Enable the WebUI using the "**webui on**" command.
- (Optional) Configure the WebUI port using the "**webui port**" command.

After the preceding configurations are completed, you need to configure inbound and outbound security rules for the vAPV instance to make the WebUI service publicly accessible. For details, please refer to the section 2.4 Adding Inbound/Outbound Security Rules.

2.3 Loading the vAPV License

In order to load the license you need to purchase a vAPV license directly from Array Networks. Then perform the following steps to load the vAPV license:

1. Access the vAPV instance via SSH.
2. View the software version, model and serial number of the vAPV by executing the "**show version**" command.
3. Contact Array Networks Customer Support to obtain a valid license key.
4. Execute the "**system license**" command in the Config mode, paste the license key and press "Enter". Then the license will be successfully loaded.

2.4 Adding Inbound/Outbound Security Rules

After the vAPV instance is successfully deployed and starts up, an inbound security rule is automatically added for the SSH management service of the vAPV instance and the outbound SSH traffic is permitted by default. Therefore, you can access the vAPV instance via SSH using the public IP address directly. However, other services, such as the WebUI management service and SLB virtual services, are still not publicly accessible. To make these services publicly accessible, you need to configure inbound security rules and outbound security rules.

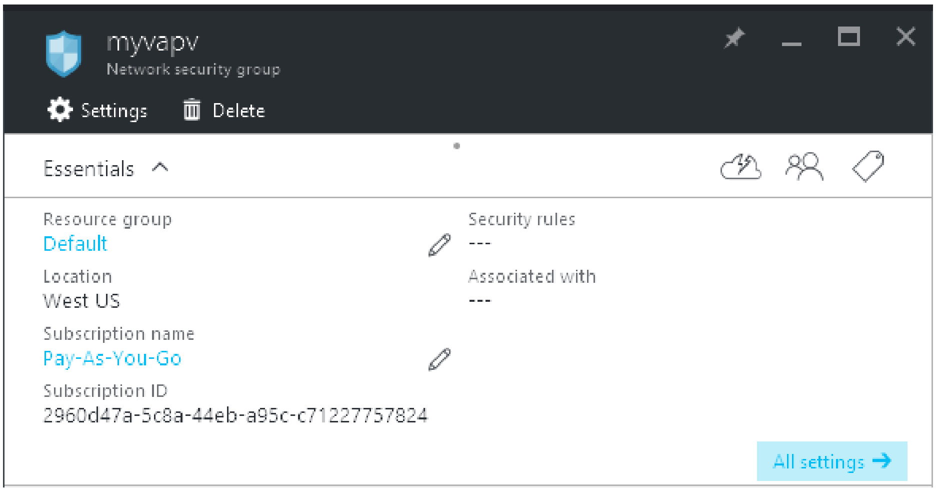
Note: The SSH management service is enabled by default. To disable the SSH management service, please delete the inbound security rule configured for the SSH management service by clicking the ··· button of the created vAPV instance in the **Inbound security rules** page. For how to access the **Inbound security rules** page, please refer to 2.4.2 Adding Inbound Security Rules.

2.4.1 Adding Outbound Security Rules

Generally, the outbound traffic of the vAPV instance should be permitted. Therefore, you can simply configure an outbound security rule with a low priority to permit all outbound traffic. Also, you can configure an outbound security rule with a higher priority to deny the outbound traffic to a specified destination. The security rule with a higher priority will take precedence over the one with a lower priority. The smaller the value, the higher the priority.

To configure an outbound security rule to permit all outbound traffic, perform the following steps:

1. Click **PORTAL**. Select **Browse** > **Network security groups**. Select the newly created vAPV and click **All Settings**, as shown in the following figure.

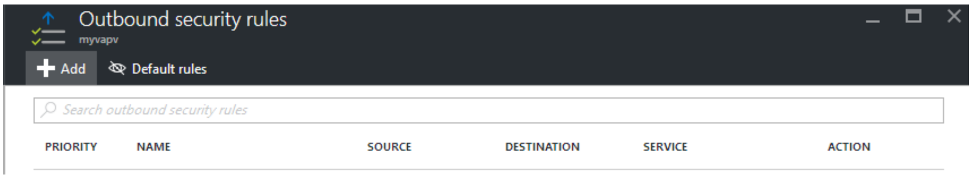


Resource group
Default
Location
West US
Subscription name
Pay-As-You-Go
Subscription ID
2960d47a-5c8a-44eb-a95c-c71227757824
Security rules

Associated with

Figure 2–11 vAPV Summary

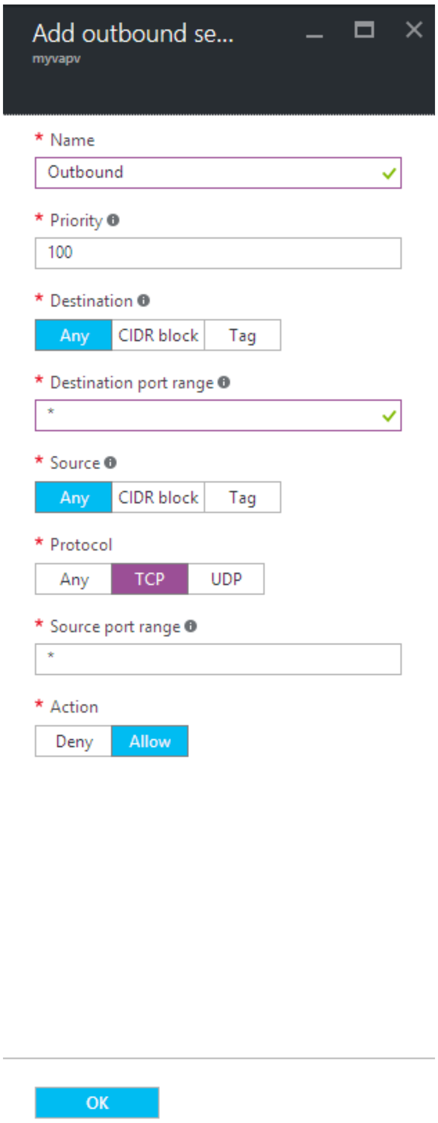
2. Click **Outbound security rules** and click the **Add** button, as shown in the following figure.



PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION

Figure 2–12 Add an Outbound Security Rule

3. Specify the required parameters according to the following figure and click **OK**.



* Name
Outbound

* Priority
100

* Destination
[✓ Any] CIDR block Tag

* Destination port range
*

* Source
[✓ Any] CIDR block Tag

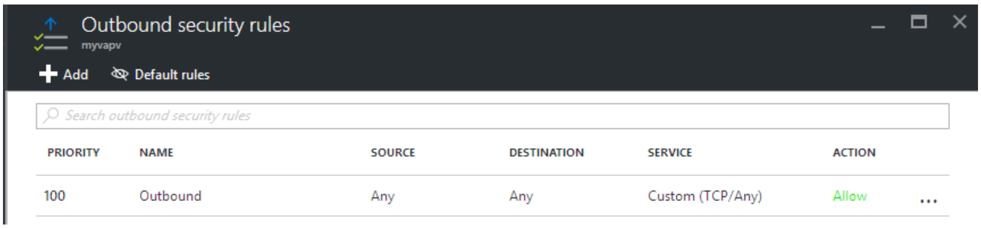
* Protocol
Any [✓ TCP] UDP

* Source port range
*

* Action
Deny [✓ Allow]

Figure 2–13 Set Parameters for the Outbound Security Rule

Then the newly added outbound security rules will be displayed in the **Outbound security rules** page, as shown in the following figure.



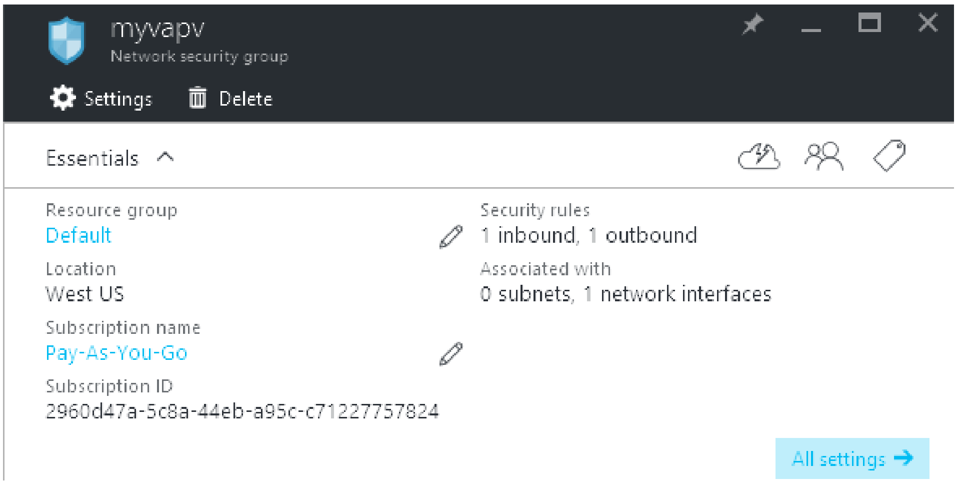
PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION	
100	Outbound	Any	Any	Custom (TCP/Any)	Allow	...

Figure 2–14 Outbound Security Rules

2.4.2 Adding Inbound Security Rules

To add an inbound security rule of a service provided by the vAPV instance, perform the following steps (using the New WebUI as an example):

1. Click **PORTAL**. Select **Browse** > **Network security groups**. Select the newly created vAPV and click **All Settings**, as shown in the following figure.



Resource group: Default

Location: West US

Subscription name: Pay-As-You-Go

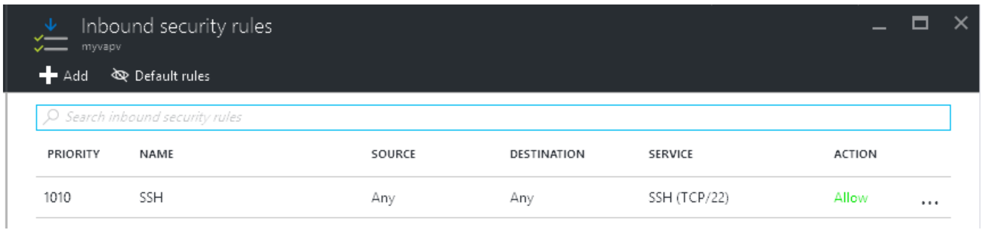
Subscription ID: 2960d47a-5c8a-44eb-a95c-c71227757824

Security rules: 1 inbound, 1 outbound

Associated with: 0 subnets, 1 network interfaces

Figure 2–15 vAPV Summary

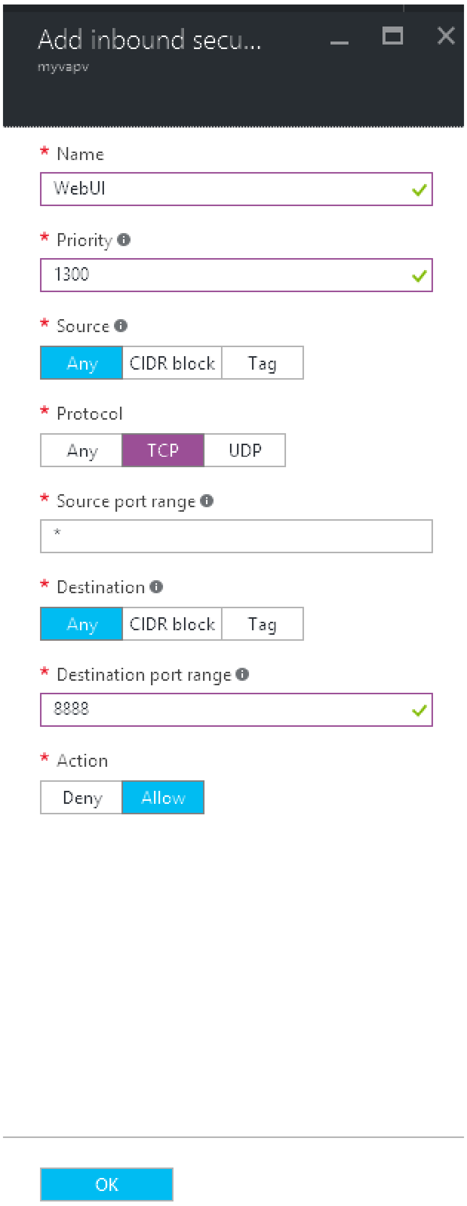
2. Click **Inbound security rules** and click the **Add** button, as shown in the following figure.



PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	SSH	Any	Any	SSH (TCP/22)	Allow

Figure 2–16 Add an Inbound Security Rule

3. Specify the required parameters and click **OK**, as shown in the following figure.



Add inbound secu...
myvapv

* Name
WebUI ✓

* Priority
1300 ✓

* Source
[✓ Any] CIDR block Tag

* Protocol
Any [✓ TCP] UDP

* Source port range
*

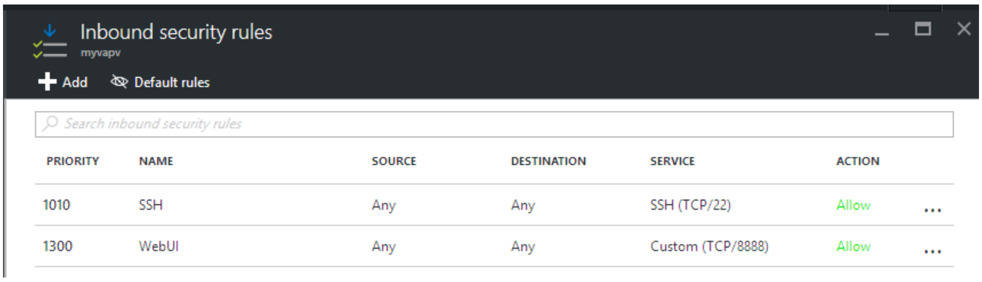
* Destination
[✓ Any] CIDR block Tag

* Destination port range
8888 ✓

* Action
Deny [✓ Allow]

Figure 2–17 Set Parameters for the Inbound Security Rule

Then the newly added WebUI Ports will be displayed in the **Inbound security rules** page, as shown in the following figure. Now you can connect to the vAPV instance via WebUI using the public IP address and port.



PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
1010	SSH	Any	Any	SSH (TCP/22)	Allow
1300	WebUI	Any	Any	Custom (TCP/8888)	Allow

Figure 2–18 Inbound Security Rules