

vAPV Installation Guide for Amazon Web Services (AWS)



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 22, 2015	Initial official version.
July 28, 2016	Added the information about Pre-license.



Table of Contents

Copyright Statement I
Contacting Array Networks II
Revision HistoryIII
Table of ContentsIV
1 Introduction1
1.1 How Array vAPV Works on AWS1
1.2 Supported Instance Types2
1.3 Supported ENIs
1.4 Usage Limitations and Guidelines
2 Deployment
2.1 Creating the Amazon VPC
2.2 Launching the vAPV EC2 Instance
2.3 Adding the Other Interfaces to the vAPV Instance
2.4 Adding Secondary Private IP Addresses to the External Interface
2.5 Adding Elastic IPs to the Network Interfaces
2.6 Accessing the vAPV Instance
2.6.1 Accessing the vAPV Instance via SSH12
2.6.2 Accessing the vAPV Instance via WebUI
2.7 Loading the vAPV License



1 Introduction

Array Networks vAPV is an easy-to-use, flexible, secure, high performance/capacity virtual application delivery controller. Amazon Web Services (AWS) is a leading cloud-computing platform that helps enterprises move their business from the physical network infrastructure to the cloud.

vAPV for AWS is a virtual appliance integrated with the AWS cloud environment, providing almost all of the same features as physical APV appliances. vAPV offers a comprehensive feature set including simple-to-use content routing, L3-L7 server load balancing, IPv4/IPv6 dual stack, application security and SSL offloading (using software SSL) for flexible application delivery solutions. vAPV for AWS enables simple and rapid provisioning and on-demand access to computing resources with minimum management effort, and helps achieve up to 99.999% application availability, 5x application acceleration and multi-layer application security.

Array vAPV is available as an Amazon Machine Image (AMI) in the AWS marketplace and can be deployed as an Amazon Elastic Cloud Compute (EC2) instance. With this support, AWS customers can leverage Array vAPV load balancing and other valuable features to better meet their business needs.

1.1 How Array vAPV Works on AWS

AWS provides different types of Web services, such as Amazon Virtual Private Cloud (VPC) and EC2.

Amazon VPC provisions a private, isolated section of the Amazon Web. Services (AWS) cloud where you can launch Amazon AWS resources in a virtual network that you define. With Amazon VPC, you can define a virtual network topology that closely resembles a traditional network that you might operate in your own data center.

Amazon EC2 is a Web service that provides resizable compute capacity in the cloud. Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instance types comprise varying combinations of CPU, memory, storage, and networking capacity and give you the flexibility to choose the appropriate mix of resources for your applications.

In deployment, Array vAPV and real services are launched as EC2 instances within an Amazon VPC, as shown in the following figure.





Figure 1-1 Typical Deployment Scenario of vAPV for AWS

Usually, an APV appliance needs to use multiple interfaces, for example one interface for management, one interface for receiving client requests and one interface for connecting real services.

Within the Amazon VPC, the vAPV instance has a default elastic network interface (ENI) that is assigned a primary private IP address. Additional ENIs can then be created and attached to the vAPV instance in the Amazon VPC. Each ENI can have multiple private IP addresses. The total number of supported ENIs and private IP addresses per instance depends on the instance type (refer to 1.3 Supported ENIs). For each private IP address, you can associate a public elastic IP address (EIP) to make the instance reachable from the Internet. You can also configure your Amazon EC2 instance to be assigned a public IP address at launch from Amazon's pool of public IP addresses.

For more information, please refer to http://aws.amazon.com/documentation.

1.2 Supported Instance Types

The vAPV AMI can be launched as an EC2 instance of the types shown in the following table.

Instance Family	Instance Type
	m4.large
Conoral nurnaca	m4.xlarge
General purpose	m4.2xlarge
	m4.4xlarge

Table 1–1 Supported Instance Types

When an EC2 instance is launched, the specified instance type determines the hardware of the host computer used for your instance and offers different compute, memory, and storage capabilities. For details on compute, memory, and storage capabilities of each instance type, please refer to http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instance-types.html.



1.3 Supported ENIs

Each EC2 instance type supports a different number of ENIs and a different number of private IP addresses per ENI. The following table lists the number of ENIs and private IP addresses per ENI supported by the EC2 instance types that the vAPV AMI supports.

Instance Type	Number of ENIs	Number of Private IP Addresses per ENI
m4.large	2	10
m4.xlarge	4	15
m4.2xlarge	4	15
m4.4xlarge	8	30

Table 1–2 Supported ENIs

1.4 Usage Limitations and Guidelines

- In the AWS cloud service architecture, the vAPV instance should be deployed in an AWS VPC to use multiple subnets (interfaces). It is recommended to use three subnets for one vAPV instance: one for management connection, one for external connection and one for internal connection. You should configure the route table correctly to make sure that the management and external subnets are publicly accessible.
- vAPV for AWS supports the following features:
 - WebWall
 - L4SLB (L4 Server Load Balancing)
 - L7SLB (L7 Server Load Balancing)
 - Caching
 - SSL Acceleration (software SSL only)
 - tProxy
 - SWCompression (Software Compression)
 - LLB (Link Load Balancing)
 - GSLB (Global Server Load Balancing)
 - QoS
 - MultiLang (Multi-language)
 - DynRoute (Dynamic Route)
 - IPv6
 - WAF

©2016 Array Networks, Inc. All Rights Reserved.



 vAPV for AWS supports both the BYOL (Bring Your Own License) model and the pre-license model. For the pre-license model, you need to purchase the AWS vAPV image with the vAPV license loaded beforehand. Users do not need to load the license again. For the BYOL model, please refer to section 2.7 Loading the vAPV License, to learn how to load the vAPV license.



2 Deployment

This section describes the process of deploying the vAPV EC2 instance within the Amazon VPC.

2.1 Creating the Amazon VPC

The deployment of the vAPV on AWS is similar to deployment in a physical network infrastructure. Before deploying the vAPV, you need to use the Amazon VPC to create a private isolated network on the AWS.

When creating the Amazon VPC, it is recommended to add at least three /24 subnets, one for the instance's management interface (management subnet), one for the instance's interface to receive client requests (external subnet) and one for the instance's interface to communicate with real services (internal subnet). Please configure routing tables to ensure that the management subnet and external subnet are accessible from the Internet.

For more information about creating and configuring the VPC, please refer to <u>http://aws.amazon.com/cn/documentation/vpc/</u>.

2.2 Launching the vAPV EC2 Instance

To launch the vAPV EC2 instance on AWS, please perform the following steps:

1. Log into AWS (<u>http://aws.amazon.com</u>) with a valid credential and switch to the AWS EC2 management console, as shown in the following figure:





Figure 2–1 EC2 Management Console

- 2. In the **Create Instance** area of the **EC2 Dashboard** page, click the **Launch Instance** button, as shown in the preceding figure.
- 3. In the Step 1: Choose an Amazon Machine Image (AMI) page, click the AWS Marketplace tab, enter "vAPV" in the search box and click the Select button to select the "Array Networks vAPV - BYOL" image, as shown in the following figure.



Figure 2-2 Select the vAPV AMI

4. In the **Step 2: Choose an Instance Type** page, select one of the instance types supported by the vAPV AMI, such as "m4.large", and click the **Next: Configure Instance Details** button, as shown in the following figure.

Step 2 Amazon E and netwo	2: Choose an Inst C2 provides a wide selection king capacity, and give you th	ance Type of instance types optim e flexibility to choose th	ized to fit different use o le appropriate mix of res	ases. Instances are vi ources for your applica	tual servers that can run applicati tions. Learn more about instance	ions. They have varying combin e types and how they can meet	ations of CPU, memory, storage, vour computing needs.
Filter by:	All instance types 👻	Current generation	n 👻 Show/Hide C	Columns			
Current Note: Th	ly selected: m4.large (6.5 EC e vendor recommends using	Us, 2 vCPUs, 2.4 GHz a m4.large instance (o	, Intel Xeon E5-2676v3, Ir larger) for the best exp	8 GIB memory, EBS or serience with this produ	nhý) ict.		
	Family	- Туре -	VCPUs () +	Memory (GiB) +	Instance Storage (CB)	EBS-Optimized Available	Network Performance () -
0	General purpose	t2 nano	1	0.5	EBS only		Low to Moderate
Ø	General purpose	12 micro Free tier eligible	Ŧ	t:	EBS only		Low to Moderate
0	General purpose	t2.smail	1	2	EBS only	*	Low to Moderate
0	General purpose	12.medium	2	4	EBS only	-	Low to Moderate
0	General purpose	t2.large	2	8	EBS only		Low to Moderate
	General purpose	m4 Jarge	2	8	EBS only	Yes	Moderate
	General purpose	m4.xdarge	4:	16	EBS only	Yes	High
	General purpose	m4.2xlarge	8	32	EBS only	Yes	High
	General purpose	m4 4stame	18	64	EBS only	Yes	Hinh



Figure 2–3 Select the Instance Type

5. In the **Step 3: Configure Instance Details** page, set the **Network** parameter to an existing VPC and set the **Subnet** parameter to the management subnet of the VPC. In the **Network** Interface area, click the **Add Device** button to add another interface to the instance and assign the internal subnet to this new interface. Then click the **Review and Launch** button, as shown in the following figure.

step 3: Co onfigure the inst stance, and mor	enfigure Instance ance to suit your requirem e	ents. Y	etails ou can launch multiple instances from the same AM, re	quest Sp	ot in	istances to take	advantag	e of the lower	pricing, assign an access r	management role to the
	Number of instances	۲	1 Launch into Auto	Scaling	Gro	ub 🕕				
	Purchasing option	۲	Request Spot instances							
	Network	0	vpc-23efd54a (172.31.0.0/18) (default)	×	с	Create new VP	C.			
	Subnet	۲	No preference (default subnet in any Availability Zon	e) 💽		Create new sul	onet			
	Auto-assign Public IP	۲	Use subnet setting							
	Placement group	$^{\odot}$	No placement group							
	IAM role	•	None	×	С	Create new IAM	t role			
	Shutdown behavior	۲	Stop							
Enable	termination protection	$^{\odot}$	C Protect against accidental termination							
	Monitoring	۲	Enable Cloud/Vatch detailed monitoring Additional charges apply.							
E	BS-optimized instance	$^{(i)}$	Launch as EBS-optimized instance							
	Tenancy	١	Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.	*						
						5	Cancel	Previous	Review and Launch	Next Add Storage

Figure 2–4 Configure Instance Details

6. Click the **6. Configure Security Group** tab, add security group rules to allow access via SSH and WebUI and then click the **Review and Launch** button, as shown in the following figure.

Assign	CSelect an existing security	A Buonb nb		
Secu	rity group name: Array Networks vAPV - B Description: This security group was	YOL-ArrayOS APV 8-6-0-x-AVVSAutogenByAV reperated by AVVS Marketplace and is based on	SMP-	
Type (i)	Protocol ()	Port Range ()	Source ()	
SSH 💽	TCP	22	Anywhere 💌 0.0.0.0/0	6
Custom TCP Rule	TCP	8888	Anywhere 🖹 0.0.0.0/0	6
Custom TCP Rule 💽	TCP	8889	Anywhere 💌 0.0.0.0/0	6
Warning Rules with source	of 0.0.0/0 allow all IP addresses to access you	instance. We recommend setting security grou	a rules to allow access from known IP addresses only.	

Figure 2–5 Configure Security Group Rules





WebUI and for port 8889 of the Legacy WebUI.

7. Review the instance information and click the **Launch** button, as shown in the following figure.

A Im op You You	prove your instances' security. Your security group, Array Networks vAPV - BYOL-ArrayOS APV 8-6-0-x-AWSAutogenByAWSMP-, is en to the world. I instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only I can also open additional parts in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. Edit security groups
A Yo To I usa	ur instance configuration is not eligible for the free usage tier aurch an instance that's eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and ge restrictions.
AMI Det	tails Edit A
Anay	Array Networks vAPV - BYOL vAPV Vitual Application Delivery Controllers improve application availability, performance and security Roof Device Type ets – Witualization type from
	Hourly Software Fees: \$0.00 per hour on m4 Jarge instance Software charges will begin once you laurch this AMI and continue unol you terminate the instance.
	By launching this product, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement

Figure 2–6 Review and Launch the Instance

8. In the prompted dialog box, select **Create a new key pair** from the drop-down list box, specify the **Key pair name** parameter, and click the **Download Key Pair** button to download the key file and then click the **Launch Instances**, as shown in the following figure.

Select	an existing key pair or create a new key	pair	×
A key pair Together private ke AMIs, the	consists of a public key that AWS stores, and a privat , they allow you to connect to your instance securely. Fo y file is required to obtain the password used to log int private key file allows you to securely SSH into your ins	e key file that you store or Windows AMIs, the o your instance. For Lin tance.	i. IUX
Note: The Learn mo	e selected key pair will be added to the set of keys auth ore about removing existing key pairs from a public AMI	orized for this instance.	
Crea	te a new key pair	•	
Key p	air name		
		Download Key Pair	
•	You have to download the private key file (*.pem file) continue. Store it in a secure and accessible locatio able to download the file again after it's created.	before you can n. You will not be	
	Cance	Launch Instances	

Figure 2–7 Create the New Key Pair

The newly created vAPV instance will be launched successfully as shown the following figure.



Launch Status

Your instances are now launching	
The following instance launches have b	een initiated: I-787ba9b7 View launch log
e Get notified of estimated charges	
Create billing alerts to get an email noti	fication when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).
low to connect to your instances	
'our instances are launching, and it may take a mmediately and continue to accrue until you sto	few minutes until they are in the running state, when they will be ready for you to use. Usage hours on your new instances will start op or terminate your instances.
Click View Instances to monitor your instances' nstances.	status. Once your instances are in the running state, you can connect to them from the Instances screen. Find out how to connect to your
 Getting started with your software 	
To get started with vAPV Virtual Application De Controller	alivery To manage your software subscription
View Usage Instructions	Open Your Software on AWS Marketplace
 Here are some helpful resources to ge 	it you started
How to connect to your Linux instance	Amazon EC2: User Guide
Learn about AWS Free Usage Tier	Amazon EC2: Discussion Forum
While your instances are launching you can also	D
Create status check alarms to be notified whi Create and attach additional EBS volumes (# Manage security groups	an these instances fail status checks. (Additional charges may apply) udditional charges may apply)
	View Instances

Figure 2–8 vAPV Instance Launched Successfully

2.3 Adding the Other Interfaces to the vAPV Instance

To use more interfaces, you will need to add other interfaces to the vAPV instance after it is launched.

To add a network interface to the vAPV instance:

1. Access the AWS EC2 management console, click the **Network Interfaces** link in the navigation pane, and then click the **Create Network Interface** button, as shown in the following figure.

Tags	Q,	Filter by tags and att	inbute	s or search by keywa	prid -					0	IC C 1 to 6	of6	> >
Reports Limits		Name		Network interf +	Subnet ID	 VPC ID	 Zone	.*	Secu-	Description ~	Instance ID	- s	Status
INSTANCES				em-16e3d7b	subnet-25e6854c	vpc-23ef#54a	ap-southeast-1b		hau		i-561adcQ) in-use
Instances		Management_test		erii-48683d3e	subnet-73#6204	vpc-e8#4d8d	ap-southeast-1a		WAP	Primary netwo	i-787ba9b7) in-use
Spot Requests				eni-85388313	subnet-22efd54b	vpc-23ef854a	ap-southeast-1a		lau		i-015760ce) in-use
Reserved Instances				eni-d2e45ca4	subnet-22efd54b	vpc-23ef#54a	ap-southeast-1a		lau		i-3241 a5fd) in-use
⊒ IMAGES				eni-fe7fc88	subnet-22e6d54b	vpc-23etd54a	ap-southeast-1a		tau		Fa05dbt6f) in-use
AMIs Bundle Tasks				eni-fe875188	subnet-c7b61fb0	vpc-d931øfbd	ap-southeast-1a		def	internal		•	available
 ELASTIC BLOCK STORE Volumes Snapshots 	-								_				,
NETWORK & SECURITY Security Groups Elastic IPs Placement Groups Key Pairs	Sele	ct a network inter	face	above									

Figure 2–9 Create a Network Interface

2. In the **Create New Interface** dialog box, specify the parameters and click the **Yes**, **Create** button, as shown in the following figure.



Description	(i)	Internal	
Subnet	(j)	subnet-65ff6212 (10.0.20.0/24) ap-southeast-1a 🔹	
Private IP	(i)	auto assign	
Security groups	(i)	sg-7932761c - default - default VPC security group * sg-863276e3 - vAPV Virtual Application Delivery Controller-ArrayOS	

Figure 2–10 Set the Parameters of the Network Interface

3. Select the entry of the newly created network interface and click the **Attach** button. In the **Attach Network Interface** dialog box, specify the **Instance ID** parameter and click the **Attach** button, as shown in the following figure.



Figure 2–11 Attach the Network Interface to the Instance

2.4 Adding Secondary Private IP Addresses to the External Interface

To provide virtual services, secondary private IP addresses need to be added to the external interface of the vAPV instance.

To add a secondary private IP address to the external interface:

1. Access the AWS EC2 management console, and click the **Network Interfaces** link in the navigation pane. Select the entry of the external interface and click the **Actions** button to select **Manage Private IP Address**, as shown in the following figure.



AMIs	Eilter by tags an	d attributes or search by keyw	nrd	Attach	
Bundle Tasks	Name	 Network interf * 	Subnet ID	Detach Delete Manage Private IP Addresses	e
Volumes		eni-1f5e3d7b	subnet-25efd	Associate Address	southeast-1b
Snapshots		eni-33e1b445	subnet-55ff62		southeast-1a
NETWORK & SECURITY		eni-43e1b435	subnet-65ff62	Change Termination Behavior	outheast-1
Security Groups		eni-46fbae30	subnet-73ff62	Change Security Groups	southeast-1a
Elastic IPs		eni-853883f3	subnet-22efd	Add/Edit Tags	southeast-1a
Placement Groups Key Pairs	Network Interface:	eni-33e1b445	1 100.00	Change Description Create Flow Log	

Figure 2–12 Manage Private IP Addresses

2. In the **Manage Private IP** Addresses dialog box, click the **Assign new IP** link to add a new secondary IP address, and then click the **Yes**, **Update** button, as shown in the following figure.

	Ma	Nanage Private IP Addresses							
	etwork interface. Leave the P address that you want to	D							
	•	eth2: eni-33e1b445 - External - 10.0.30.0/24							
		Private IP	Public IP						
		10.0.30.77							
		10.0.30.78		Undo					
		Assign new IP							
		ow reassignment	(i)						
	•	Are you sure • 1 specified	you want to perform the foll I private IP addresses will b	owing changes: e assigned to eni-33e1	0445				
					Cancel Yes, Updat	te			

Figure 2–13 Add a New IP Address

When configuring server load balancing (SLB) virtual services, you should use the secondary private IP address as the VIP. To make the secondary private IP address publicly accessible, you need to add an elastic IP and associate it with the secondary private IP address. The next section describes this process.

2.5 Adding Elastic IPs to the Network Interfaces

To make the management interface and the external interface of the vAPV instance publicly accessible, you need to add the elastic IPs and associate them with the private IP addresses of the network interfaces.

To add the elastic IP to a network interface:

1. Access the AWS EC2 management console, click the **Elastic IPs** link in the navigation pane, and then click the **Allocate New Address** button. In the **Allocate New Address** dialog box, click the **Yes, Allocate** button, as shown in the following figure.



EC2 Dashboard	Allocate New Address Actions V
Events	Allocate New Address Actions
Tags	Q Filter by attributes or search by keyword
Reports	
Limits	Allocate New Address X
INSTANCES	
Instances	Are you sure you want to allocate a new IP address?
Spot Requests	
Reserved Instances	Cancel Yes, Allocate
IMAGES	
AMIs	
Bundle Tasks	
ELASTIC BLOCK STORE	
Volumes	
Snapshots	
NETWORK & SECURITY	
Security Groups	
Elastic IPs	Select an address above
Placement Groups	
Key Pairs	
Network Interfaces	

Figure 2–14 Allocate the New Address

2. Select the entry of the newly created elastic IP, click the **Actions** button and select the **Associate Address** item, as shown in the following figure.

	Allocate New Address	Actions A				
1	Q. Filter by attributes or	Allocate New Address Release Addresses				
	Elastic IP	Associate Address Disassociate Address	Private IP Address	Scope	-	Public DNS
	52.76.0.192			чрс		

3. In the Associate Address screen, specify the parameters Network Interface and Private IP Address and click the Associate button, as shown in the following figure.

Select the insta	ance OR network interface to which y	ou wish to associate this IP address (52.	76.8.192)			
	Instance	Search instance ID or Name tag				
		Or				
	Network Interface	eni-48683d3e				
	Private IP Address	10.0.10.59*	•	(i)		
		Reassociation		1		
War If you	ning rassociate an Elastic IP address with	your instance, your current public IP add	ress is rele	ased, Learn r	nore about <u>public IP</u>	

Figure 2–15 Associate the Elastic IP

2.6 Accessing the vAPV Instance

2.6.1 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 the public DNS Name or IP address and the SSH port 22 as the SSH access point.

For the Bring Your Own License model, the downloaded private key file will be required for logging into the vAPV instance. After you successfully log into the vAPV instance, the following screen will be displayed.



Figure 2–16 Access the vAPV Instance via SSH



Note: For the Bring Your Own License model, the INVALID LICENSE KEY message is displayed because you have not yet entered the license information. That process is described in section 2.7 Loading the vAPV License.

2.6.2 Accessing the vAPV Instance via WebUI

To access the vAPV via WebUI, you will first need to access the vAPV instance via SSH to perform the following configurations in the Config mode:

- Change the password of the default account (array) using the "**passwd user array** *new_password*" command.
- 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 can access the WebUI of the vAPV instance at https://<EIP>:<WebUI_port> using a Web browser. On the login page, enter "array" as the username and the previously configured "new_password" as the password to pass the authentication.



5	Array		Search Q		± 8	⊖ 🕅 🛓 array
в	Dashboard		🔿 System Dashboard 🛛 🚧 Graph			
-	System	~	0 System info		▲ System Status	0
•	Network	~	Host Name	: AR	CPU Usign	1/100
P	Routing	~	Boot Time	Tue Sep 22 14:27:04 GMT (+0000) 2015		
A	NAT	~	Current Time	Sec Oct 10 14:55:29 GMT (+0000) 2015	Memory Deage	2731/4096 MII
13	High Availability	*	Up Time	18 days, 28 mins,	Disk Usage	7/100
4	sua.	~	SSL Hardware	No HW Available		
0	GSLB	~	Model	Array APV 6250	Curnection per Second Request per Second	0
*		~	Serial Number	0437A3345200010002262016313760		
-	Educa Tanka	-	Software Build Information	ArrayO5 ReLAPV.8.6.0.1 build on Fri Aug 28 10:26:11 2015		

Figure 2–17 Access the vAPV Instance via WebUI

2.7 Loading the vAPV License

If you are using the pre-license model for the vAPV, your license is already loaded and you can skip this step. If you are using the Bring Your Own License model, to purchase a license from Array Networks and load the license to the system, please execute the following steps:

- 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". The license will be successfully loaded.

Alternatively, you can load the license via WebUI. To load the license, select **System > System Management > System License > License Key**.