

Juniper Advanced Threat Prevention Appliance

vCore for AWS Quick Start Guide

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA

408-745-2000

www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Juniper Advanced Threat Prevention All-in-One Quick Start Guide
Copyright© 2018 Juniper Networks, Inc. All rights reserved.

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical document consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

About the Documentation

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes. Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>.
- Search for known bugs: <https://prsearch.juniper.net/>.
- Find product documentation: <http://www.juniper.net/documentation/>.
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>.
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>.
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>.
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>.
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>.

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).
- For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>

Inside This Guide

- JUNIPER ATP APPLIANCE TECHNOLOGY INTEGRATES WITH AMAZON WEB SERVICES (AWS) BY PROVIDING VIRTUAL CORE IMAGES THAT CAN BE RUN ON THE AWS PLATFORM. THE VIRTUAL CORE IS PROVIDED IN AN AMI (AMAZON MACHINE IMAGE) FORMAT THAT IS LAUNCHED AS AN AWS EC2 INSTANCE.
- JUNIPER ATP APPLIANCE vCORE COMPONENTS
- AWS vCORE INSTANCE REQUIREMENTS
- AWS vCORE EBS VOLUME ENCRYPTION
- vCORE LICENSING
- vCORE SPECIFICATIONS
- INSTALLATION PREREQUISITES
- TO INSTALL AND CONFIGURE THE AWS vCORE AMI
- VERIFYING AWS CONFIGURATIONS
- ACCESSING THE JUNIPER ATP APPLIANCE CENTRAL MANAGER WEB UI
- WHAT TO DO NEXT?

Welcome to the Juniper ATP Appliance vCore for AWS Solution.

Juniper ATP Appliance technology integrates with Amazon Web Services (AWS) by providing Virtual Core images that can be run on the AWS platform. The Virtual Core is provided in an AMI (Amazon Machine Image) format that is launched as an AWS EC2 instance.

An Amazon AMI provides the information required to launch a configured Juniper ATP Appliance vCore instance as a virtual server in the Amazon Cloud. Many Juniper ATP Appliance AMI vCore instances as needed can be launched from an AMI, and vCore instances can be launch from as many different AMIs as needed. The Juniper ATP Appliance vCore AWS solution is both robust and flexible.

With Juniper ATP Appliance vCore for AWS, both the Primary Core (i.e., Core + Central Manager (CM) and the connected Secondary Cores are installed and run from the AWS platform. Each vCore instance status is displayed at the AWS management console, and all connectivity status is shown at the Juniper ATP Appliance CM Web UI.

For example, any connectivity status change between the Primary Core and the Secondary Core(s) is shown in real time. If an AWS Secondary Core instance is stopped, the Secondary Core connectivity status changes to offline at the Juniper ATP Appliance CM Web UI. Likewise, after booting an AWS Secondary Core instance (from the AWS management console), the Secondary Core connectivity status display at the Juniper ATP Appliance Web UI will change to online.

Distributed collectors (local) are connected to the AWS vCore.

Juniper ATP Appliance vCore Components

The Juniper ATP Appliance AWS vCore consists of the Core and Central Manager components packaged into the Amazon AMI format; distributed Collectors are not included. The AMI includes all relevant metadata as well as the virtual server root volume and data volume.

A Secondary Core can be launched from the same AMI, using the same Core clustering procedure currently employed when configuring a Virtual Core to run on a vSphere platform; refer to the Core-CM Quick Start Guide for more information.

All detection engine OS image files (for both Windows XP and Windows 7) are also packaged into the vCore AMI (similar to the manner in which images are bundled into a Juniper ATP Appliance Virtual Core OVA).

AWS vCore Instance Requirements

The AWS vCore is launched from the Juniper ATP Appliance vCore AMI. It must satisfy the following requirements:

- The network interface should be in DHCP mode
- Any firewall rules must allow access to the vCore AMI instance once it is imported
- The CM/Core virtual instance must have a public IP address only if it needs to be accessed from the Internet. If the CM/Core is only to be accessed from within the VPC connecting to the corporate private networks, a public IP address may not be needed. Proper security group rules should be set to limit appropriate inbound and outbound traffic.

Once a vCore instance is created, the vCore instance volume will stay in the particular AWS region of the EC2 for which it was defined.

AWS vCore EBS Volume Encryption

During configuration at the AWS Console, administrators can choose whether or not to encrypt an EBS disk when launching an EC2 vCore instance as an AMI. Refer to the AWS web sites for more technical details regarding EBS volume encryption.

vCore Licensing

The vCore license key is activated and validated daily through GSS. The Juniper ATP Appliance vCore will trigger the license validation check daily. If the license key is soon to expire (within 14 days), an alert will pop up when logging into the Juniper ATP Appliance UI.

A UUID is required to generate a license for an AWS install. The AWS Virtual Core license status is displayed in the Central Manager Web UI to allow customer to track license key is expiry.

If a vCore license key is not activated, or fails validation on a regular basis, or expires, the data path and analysis services are suspended.

vCore Specifications

The Juniper ATP Appliance AWS vCore specifications are indicated as follows:

Juniper ATP Appliance supports use of the following two instance types:

- Compute Optimized C4.4Xlarge
- Compute Optimized C4.8Xlarge

Note that overall performance is a function of the type of disk volume type chosen for the EC2 instances from which the vCore is running.

Once the AWS Core is deployed, customers can change the vCore AMI instance type, which may include changes of CPU, memory and disk type and size.

Installation Prerequisites

- **REQUIRED:** Open port ranges 52466 - 53466 in the AWS security group between the Master Core and Secondary Cores are required in addition to ports 443 and 22.
- AWS Customer Account ID - needed in order to share the Juniper ATP Appliance AMI with the customer account
- Determination of which Amazon ZONE to use
- Provide this information to Customer Support. The AMI will be shared with each customer using the provided AWS account ID, and will be set to the specific AWS ZONE requested.

NOTE Primary Core/CM and Secondary Cores/Mac Cores must be on the same network, and allow all ports, with no Port Address (PAT) or Network Address Translation (NAT).

To Install and Configure the AWS vCore AMI

Juniper ATP Appliance vCore for AWS requires both Juniper ATP Appliance and AWS licensed accounts. The installations and configuration process uses both the Amazon AWS Management Console (Part 1) as well as the Juniper ATP Appliance vCore Central Manager Web UI and CLI (Part 2).

NOTE After purchasing the vCore AMI license, share the vCore AMI with your AWS customer account by using the AWS Management Console to configure and launch the vCore AMI.

A general AWS AMI configuration workflow is provided below; be sure to refer to the AWS Management Console operations guide for more detailed console usage information.

Part 1- Amazon AWS Management Console vCore AMI Configuration

1. Log into your AWS database account at the Amazon AWS Management Console.
`console.aws.amazon.com`
2. From the AWS Management Console Dashboard, select EC2 services.
3. In EC2 Services, click the IMAGES>AMIs option from the left menu of the AWS Console. Also click on the drop-down menu to change the image ownership type from "Owned by Me" to "Private Images".:
4. Select the Juniper ATP Appliance AMI image to be installed by clicking its radio button in the table.
5. From the Zone DropDown menu, select the Zone for which the AMI is to be configured. In our example, the Juniper ATP Appliance "rsa-demo-cm" AMI is selected. (The Juniper ATP Appliance AMI will have been shared with you before you launch the AWS Core.)
6. Click Launch to begin configuration of this Juniper ATP Appliance vCore AMI instance, in EC2, for your enterprise.
7. From the "Choose an Instance Type" page, select an instance type for the AMI. In our example, we selected "c4 large". Click Next: Configure Instance.

The screenshot shows the AWS Management Console interface for 'Step 2: Choose an Instance Type'. The top navigation bar includes 'AWS', 'Services', 'Edit', and a region dropdown set to 'N. California'. Below the navigation bar is a progress bar with seven steps: 1. Choose AMI, 2. Choose Instance Type (active), 3. Configure Instance, 4. Add Storage, 5. Tag Instance, 6. Configure Security Group, and 7. Review. The main content area displays a table of instance types. The table has columns for a radio button, instance type, vCPUs, memory, storage, EBS, and network. The 'c4.xlarge' instance type is selected, indicated by a blue radio button and a blue highlight. The 'Review and Launch' button is highlighted in blue at the bottom right of the table.

	Instance Type	vCPUs	Memory	Storage	EBS	Network
<input type="radio"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-
<input type="radio"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-
<input type="radio"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes
<input type="radio"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes
<input checked="" type="radio"/>	Compute optimized	c4.xlarge	2	3.75	EBS only	Yes
<input type="radio"/>	Compute optimized	c4.xlarge	4	7.5	EBS only	Yes
<input type="radio"/>	Compute optimized	c4.2xlarge	8	15	EBS only	Yes
<input type="radio"/>	Compute optimized	c4.4xlarge	16	30	EBS only	Yes
<input type="radio"/>	Compute optimized	c4.8xlarge	36	60	EBS only	Yes
<input type="radio"/>	Compute optimized	c3.large	2	3.75	2 x 16 (SSD)	-

At the bottom of the table, there are four buttons: 'Cancel', 'Previous', 'Review and Launch' (highlighted), and 'Next: Configure Instance'.

8. From the "Configure Instance Details" page, select an existing customer-defined Virtual Private Cloud (VPC) from the Network dropdown menu; in our example, we've selected rsa-demo-1.

Step 3: Configure Instance Details
 Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot Instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: ☒ Request Spot Instances

Network: vpc-cf0fc3aa (172.31.0.0/16) (default) [Create new VPC](#)

Subnet: vpc-9d804bf8 (10.2.0.0/16) | rsg-demo-1 [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: No placement group

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: ☒ Protect against accidental termination

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

To create a new VPC, click the Create New VPC link and follow the stepped procedure.

9. Define the VPC subnet in the Subnet field; in our example, we used AWS 10.2.0.0/16.

To create a new subnet, click the Create New Subnet link and follow the stepped procedure.

10. Confirm that the subnet is using an Auto-Assigned Public IP, as in the example shown above. This allows the Juniper ATP Appliance vCore to be accessed from the Internet.
11. Click to Enable termination protection to protect against accidental termination.

NOTE Each AMI instance uses a private IP and a public IP. If you are planning on installing one vCore + Central Manager with several Secondary Core, you must have a public IP address assignment. Note that the Secondary Core does not need a public IP because it does not contain a Web UI.

ALSO: Some enterprises connect their AWS VPC to a private network using VPN. In this case, there is no need to assign a public IP to the subnet because internet access can be configured via the VPN.

12. Click Next: Add Storage.

NOTE Click "Encrypted" to encrypt the data volume.

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/sda1	snap-1e873827	512	General Purpose (SSD)	1536 / 3000	<input checked="" type="checkbox"/>	Not Encrypted
EBS	/dev/sdb	snap-af7b6e96	1024	General Purpose (SSD)	3072	<input checked="" type="checkbox"/>	Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag](#)

13. Juniper ATP Appliance already provides 1 TeraByte of storage in the Core. Due to the limitations of the AWS storage volume max size, there is no need for further configuration on this page; do not add extra storage to the vCore. Click Next.
14. From the "Tag Instance" page, click Create Tag and enter a tag name and description.

Step 5: Tag Instance
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)
Name	test-awscore-doc-1

[Create Tag](#) (Up to 10 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security](#)

15. Click Next: Configure Security to proceed.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server, allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more about Amazon EC2 security groups.](#)

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name: launch-wizard-3

Description: launch-wizard-3 created 2015-04-23T14:25:25.902-07:00

Type	Protocol	Port Range	Source
SSH	TCP	22	Anywhere 0.0.0.0/0

Add Rule

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review](#)

16. A security group is essentially a firewall in AWS. Most customers already have a preexisting firewall, so choose Select an existing security group, or Create a new security group. Do ensure there are rules in the Security Group that allow communication between AWS Core and AWS Secondary Cores.
17. If creating a new security group, enter a name and description in the Security Group Name field and the Description field, respectively.
18. Enter port designation; Juniper ATP Appliance vCore only allows for port 22, 80 and 443. Click Next.

Step 6: Configure Security Group

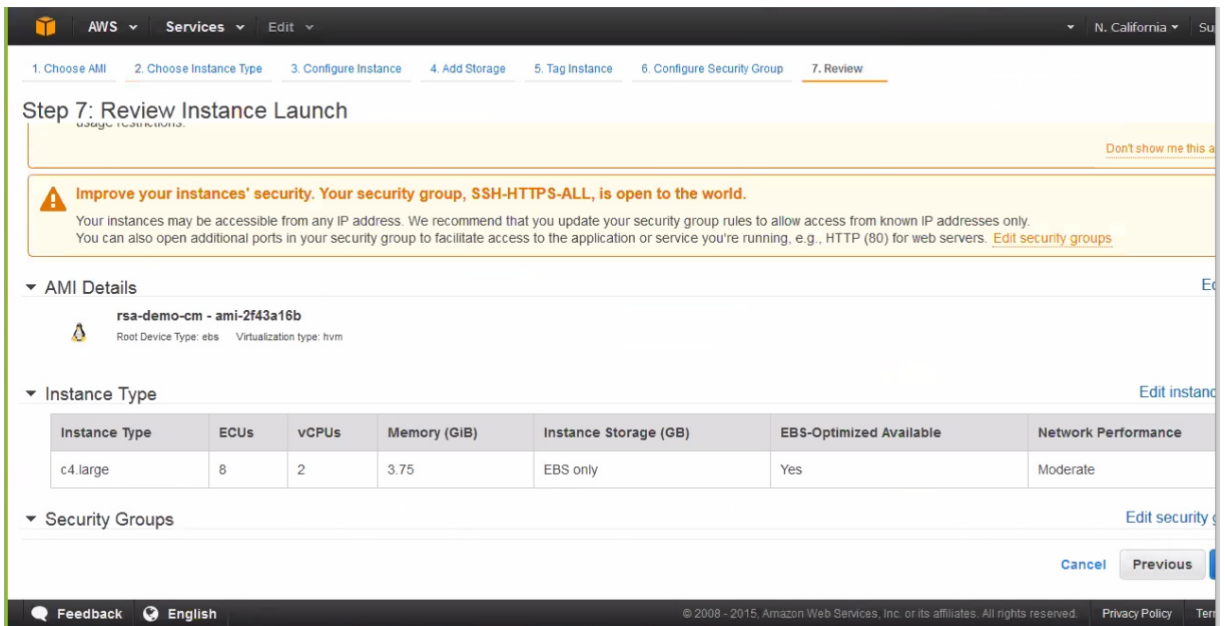
Assign a security group: ☐ Create a new security group ☒ Select an existing security group

Security Group ID	Name	Description	Action
<input type="checkbox"/> sg-85c273e0	default	default VPC security group	Copy to clipboard
<input type="checkbox"/> sg-31c57454	SSH-HTTPS-ALL	launch-wizard-3 created 2015-04-10T21:33:29.359-07:00	Copy to clipboard

Inbound rules for sg-31c57454

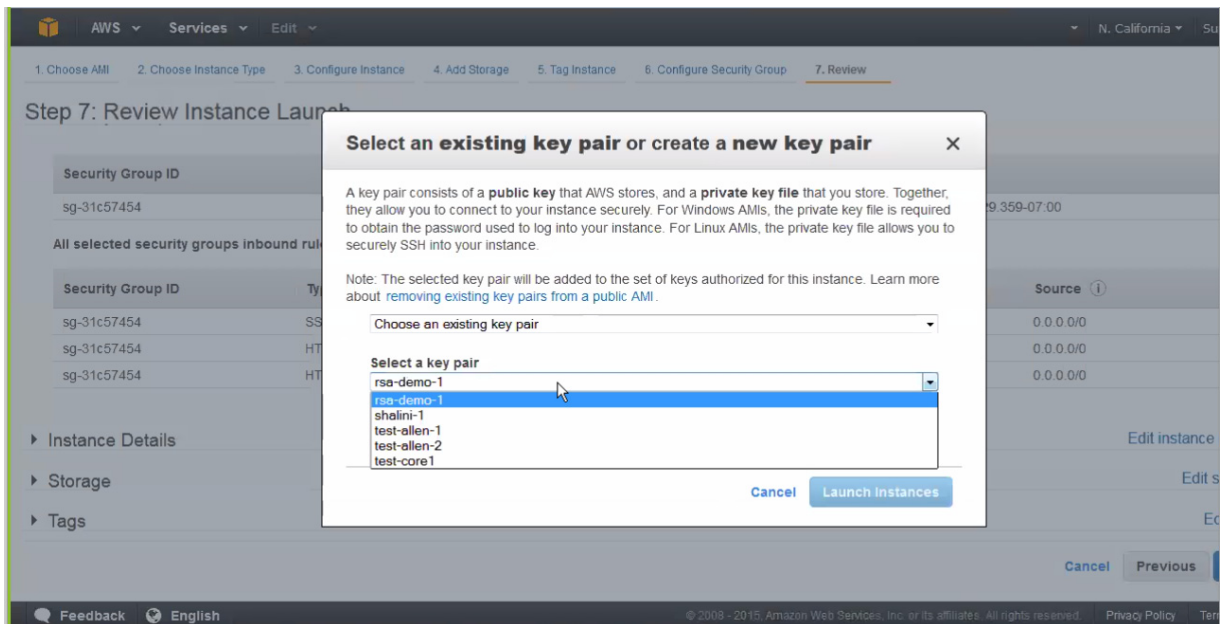
Type	Protocol	Port Range	Source
SSH	TCP	22	0.0.0.0/0
HTTP	TCP	80	0.0.0.0/0

[Cancel](#) [Previous](#) [Review and create](#)



NOTE You can configure an SSH key although the Juniper ATP Appliance vCore already includes password protection. To add extra protection, add a key pair first, then use Juniper ATP Appliance password for CLI-only login. AWS requires you to set a key pair. You will not be able to use a pem-only login.

19. To configure an SSH Key, select an existing key pair or create a new key pair:

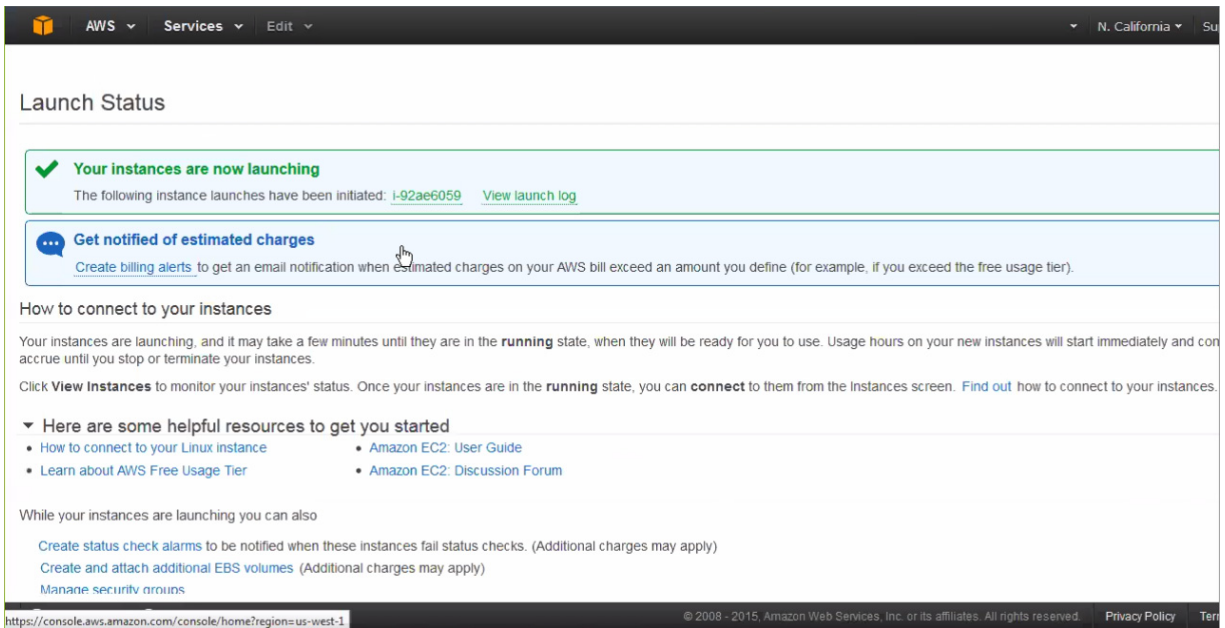


20. If selecting an existing security group, select then choose from the list and click Next.

The “Review Instance Launch” page displays:

21. From the “Review Instance Launch” page, review the Instance Launch details, then either click Edit Instance to make changes, or click Launch to instantiate.

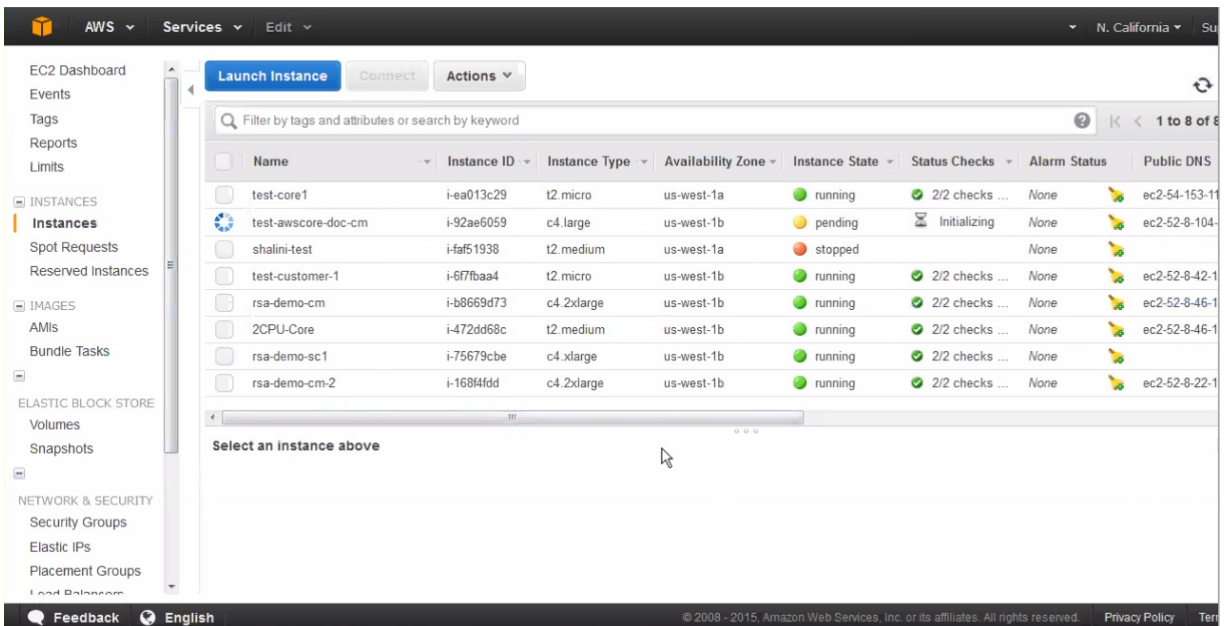
The Launch Status window displays;



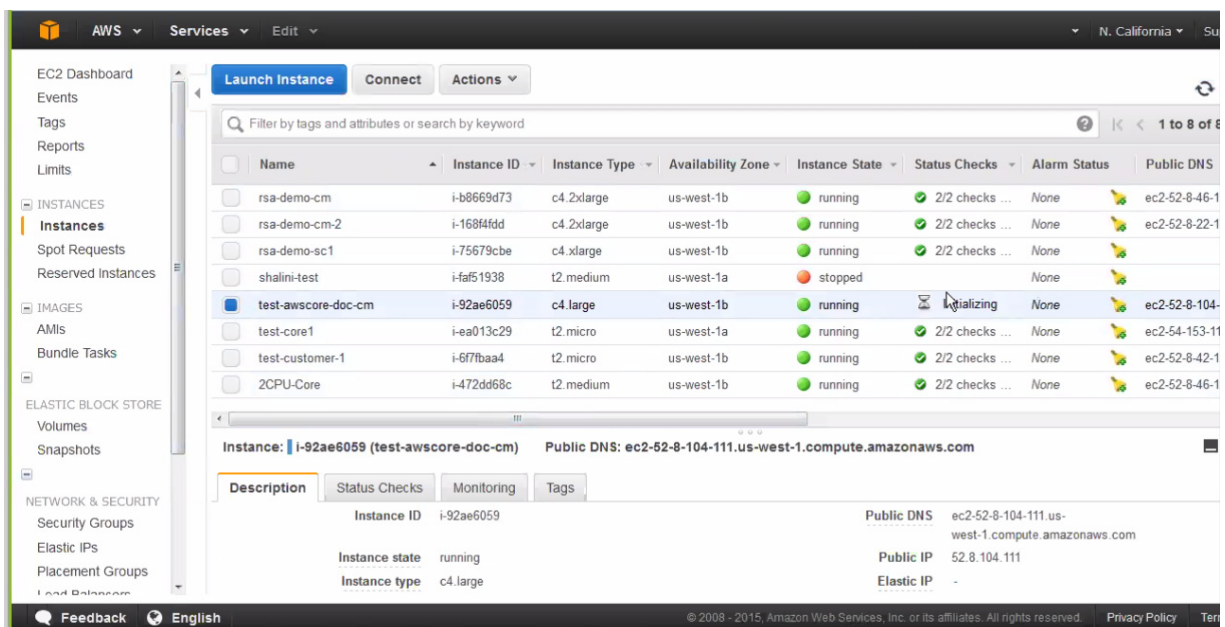
Part 2 - Running the Juniper ATP Appliance vCore AMI Instance

Next, you will initialize the Juniper ATP Appliance vCore AMI Instance from the AWS Management Console, then verify the AMI at the Juniper ATP Appliance Central Manager CLI using the **show ip** command.

1. Open the AWS Management Console Instances page to view the launched AMI Instance status. When a launched Instance finishes initializing, it will display a green icon to indicate “running” status.



2. Select the launched Instance then open the panel at the bottom of the Instances table to review Instance details.
3. Copy the Instance ID and the Instance Type "c4-large2." for the vCore CLI configuration.



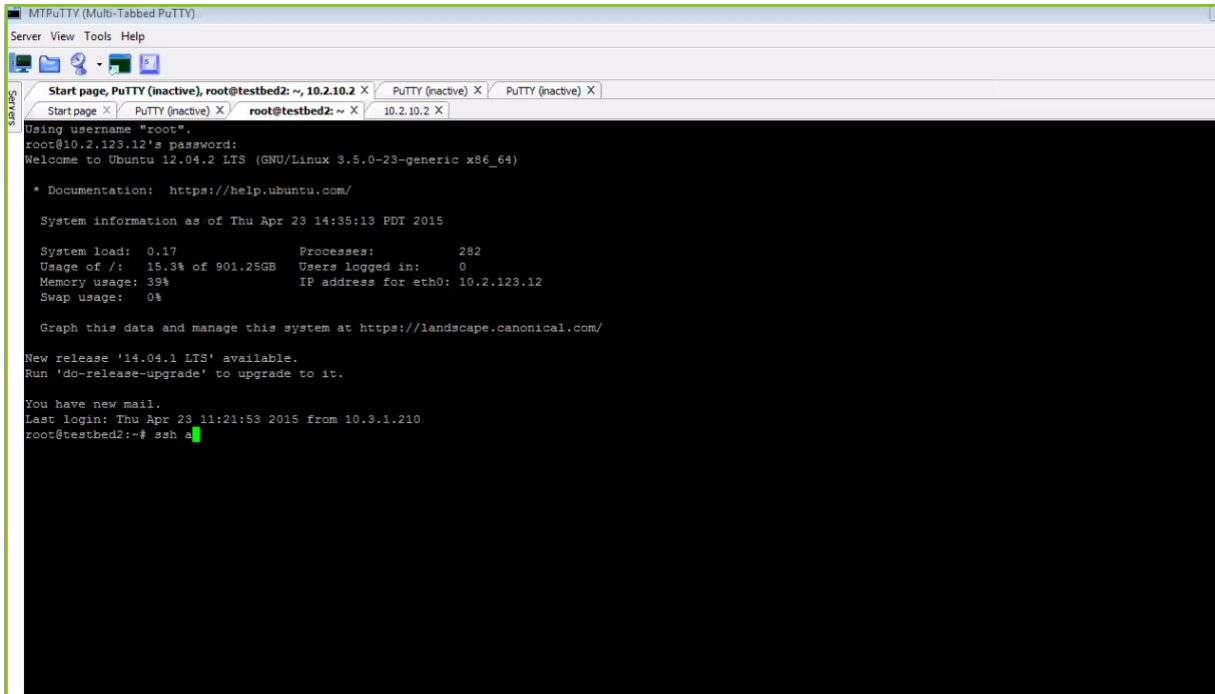
NOTE It is very important to be aware that the private IP address is the DHCP setting, and it will stay static in AWS and should never change during proper operations.

Note also that you cannot change the AMI hostname, although you can change the DNS if necessary.

About DNS: Because the AWS vCore is not located in the enterprise, the reverse DNS on threat targets do not resolve to the expected target hostname. This is rarely confusing when connected via VPN from

the corporate network to the VPC. Generally, internal DNS servers are not exposed outside the enterprise, so the Juniper ATP Appliance cannot configure the AWS vCore to reach an internal DNS server. If the internal DNS server uses an outward facing IP address and you, as admin, are willing to allow connections to it, this is a reasonable solution. Note that the DNS server that the vCore uses will not have the DNS information of the networks where the Juniper ATP Appliance Traffic Collector is located. This is typical of distributed deployments where the Traffic Collector and the Core/CM are not located in the same enterprise networks.

4. Copy the Public IP address to access the vCore AWS Instance CLI via SSH/PuTTY:



```
MTTPuTTY (Multi-Tabbed PuTTY)
Server View Tools Help

Start page, PuTTY (inactive), root@testbed2: ~, 10.2.10.2 X
Start page X PuTTY (inactive) X root@testbed2: ~ X 10.2.10.2 X

Using username "root".
root@10.2.123.12's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

System information as of Thu Apr 23 14:35:13 PDT 2015

System load:  0.17               Processes:    282
Usage of /:   15.3% of 901.25GB   Users logged in:  0
Memory usage: 39%               IP address for eth0: 10.2.123.12
Swap usage:   0%

Graph this data and manage this system at https://landscape.canonical.com/

New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

You have new mail.
Last login: Thu Apr 23 11:21:53 2015 from 10.3.1.210
root@testbed2:~# ssh a
```

5. At the Juniper ATP Appliance CLI prompt, type **server** to enter CLI Server mode, then from Server mode, run the CLI command **show ip** to display private and public IPs, as shown below. These should match the AWS configuration.

NOTE For more information about AWS-specific CLI commands, and usage of CLI modes and commands, refer to the CLI Command Reference Guide.

Year	2000	2001	2002	2003
1	1	1	1	1
2	1	1	1	1
3	1	1	1	1
4	1	1	1	1
5	1	1	1	1
6	1	1	1	1
7	1	1	1	1
8	1	1	1	1
9	1	1	1	1
10	1	1	1	1
11	1	1	1	1
12	1	1	1	1
13	1	1	1	1
14	1	1	1	1
15	1	1	1	1
16	1	1	1	1
17	1	1	1	1
18	1	1	1	1
19	1	1	1	1
20	1	1	1	1
21	1	1	1	1
22	1	1	1	1
23	1	1	1	1
24	1	1	1	1
25	1	1	1	1
26	1	1	1	1
27	1	1	1	1
28	1	1	1	1
29	1	1	1	1
30	1	1	1	1
31	1	1	1	1
32	1	1	1	1
33	1	1	1	1
34	1	1	1	1
35	1	1	1	1
36	1	1	1	1
37	1	1	1	1
38	1	1	1	1
39	1	1	1	1
40	1	1	1	1
41	1	1	1	1
42	1	1	1	1
43	1	1	1	1
44	1	1	1	1
45	1	1	1	1
46	1	1	1	1
47	1	1	1	1
48	1	1	1	1
49	1	1	1	1
50	1	1	1	1
51	1	1	1	1
52	1	1	1	1
53	1	1	1	1
54	1	1	1	1
55	1	1	1	1
56	1	1	1	1
57	1	1	1	1
58	1	1	1	1
59	1	1	1	1
60	1	1	1	1
61	1	1	1	1
62	1	1	1	1
63	1	1	1	1
64	1	1	1	1
65	1	1	1	1
66	1	1	1	1
67	1	1	1	1
68	1	1	1	1
69	1	1	1	1
70	1	1	1	1
71	1	1	1	1
72	1	1	1	1
73	1	1	1	1
74	1	1	1	1
75	1	1	1	1
76	1	1	1	1
77	1	1	1	1
78	1	1	1	1
79	1	1	1	1
80	1	1	1	1
81	1	1	1	1
82	1	1	1	1
83	1	1	1	1
84	1	1	1	1
85	1	1	1	1
86	1	1	1	1
87	1	1	1	1
88	1	1	1	1
89	1	1	1	1
90	1	1	1	1
91	1	1	1	1
92	1	1	1	1
93	1	1	1	1
94	1	1	1	1</

On the Central Manager Config>Golden Image VMs page, note that 32-bit images are available for AWS; see figure below for reference.

ADVANCED THREAT PREVENTION APPLIANCE

Refresh Data System Health juniper Doc

Dashboard Incidents File Uploads Mitigation Reports Custom Rules **Config**

Notifications

System Profiles

- Password Reset
- Roles
- Zones
- Users
- SAML Settings
- RADIUS Settings
- System Settings
- Certificate Management
- GSS Settings
- Web Collectors
- Email Collectors
- Secondary Cores
- Golden Image VMs**
- Licensing

Image Name: Description: VNC ID: Architecture: 32-bit RAM Size (GB): 20 VNC Protocol: Yes/No

Network Segment: default

Cancel

Current VM Images

Description	Enabled	Status	Actions
GI - Demo	No	Running, VNC Id: 1	Controls Delete Edit

Verifying AWS Configurations

To verify interface configurations, use the following CLI commands (refer to the CLI Command Reference Guide for more information):

Table 1 Verify interface configurations

vCore CLI (Mode) & Command	Purpose
JATP (diagnosis)# setupcheck all	Run a check of all system components
JATP (server)# show interface	Verify interface connectivity and status
JATP (server)# show ip <interface>	Verify traffic [example: show ip eth1]
JATP (server)# ping x.x.x.x	Ping connected devices.
JATP (server)# show ip	Display AWS public and private IP addresses.

NOTE: Be sure to refer to the Juniper ATP Appliance CLI Command Reference for more information.

Accessing the Juniper ATP Appliance Central Manager Web UI

To access the Juniper ATP Appliance Central Manager (CM) Web UI, use HTTP/HTTPS; enter the configured Juniper ATP Appliance Server IP address or hostname in any web browser address field, and accept the SSL certificate when prompted. You are required to log into the CM Web UI.

To Log in to the Central Manager

1. In the Juniper ATP Appliance Login window, enter the default username `admin` and the password `1JATP1234`

NOTE The Juniper ATP Appliance Web UI login username and password are separate from the CLI `admin` username and password.

1. When prompted to reset the password, re-enter the password `1JATP1234` as the “old” password, and enter a new password (twice).
2. At login, the Juniper ATP Appliance Central Manager Dashboard is displayed, as shown below. The Dashboard tab includes aggregated malware detection information and provides system status and health information. Additional configurations are made from the Configuration tab. Refer to the Juniper ATP Appliance Operator's Guide for more information.

The Juniper ATP Appliance CM Dashboard provides in-context and aggregated malware detection information as well as system status and health information. Additional configurations are made from the Configuration tab. Refer to the Juniper ATP Appliance Operator's Guide or online help for more information.

Use the Config tab to verify that the new Collector is calling the Central Manager (CM) Web UI, and is online and actively inspecting and collecting traffic.

What to Do Next?

- Navigate to the Configuration tab and select System Settings> Licensing from the left panel; upload your license key (obtained from your sales representative).
- Use the Central Manager (CM) Web UI Dashboard and Config pages to confirm traffic monitoring and detection activity. The CM updates security intelligence every 5 minutes, so you may need to wait 5 minutes to see activity at the Web UI.
- Review the Juniper ATP Appliance Core/Central Manager Quick Start Guide if planning to install additional Cores, Clustered Cores, Secondary Cores or OVA Cores.
- Review the Juniper ATP Appliance All-in-One Quick Start Guide for information about All-in-One platform installation and configuration.
- Review the Juniper ATP Appliance Traffic Collectors Quick Start Guide if planning to install additional or remote Web or Email Traffic Collectors.
- Refer to the Juniper ATP Appliance Mac Mini OS X Engine Quick Start Guide for information about installing a Mac Mini Detection Engine.
- Refer to the Juniper ATP Appliance CLI Command Reference for information about Collector CLI commands.
- Refer to the Juniper ATP Appliance Operator's Guide for information about all products and usage.
- Refer to the Juniper ATP Appliance HTTP API Guide for information about accessing and managing Juniper ATP Appliance advanced threat detection using APIs, including processing data, device and software configuration.
- Refer to the Juniper ATP Appliance CEF Logging Support for SIEM Integration Guide for information about CEF logging.

