



Palo Alto Networks Application Framework - Lab Guide

Table of contents

Full Lab Deployment Instructions

[Application-Framework-Lab](#)

Application Framework FAQs

[Application-Framework-FAQs](#)

API Usage Examples

[API-Curl-Examples](#)

API Explorer Only Deployment Instructions

[API-Explorer-Lab](#)

Application-Framework-Lab

Palo Alto Networks Application Framework Full Lab Deployment via AWS CloudFormation

This document describes how to automatically set up a lab environment on Amazon Web Services that can be used to generate logs for Palo Alto Networks Application Framework. It is meant for Palo Alto Networks Partners that need a quick way to start developing for Application Framework.

It also provides instructions on how to pair the API Explorer application with Application Framework.

Doc Revision: 2018-05-01-07:41:39 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/Application-Framework-Lab>
- Documentation PDF (incl FAQ): <https://github.com/PaloAltoNetworks/appframeworklab/blob/master/pdf/LabGuide.pdf>
- AWS Full Lab CFT JSON file - <https://raw.githubusercontent.com/PaloAltoNetworks/appframeworklab/master/cft/appframework-lab.json>
- NGFW S3 Bucket Zip: <https://paloaltonetworks.box.com/s/88f9zonvr7fb5ihf49kbcrcdw4kfp2>
- LAB Miscellaneous S3 Bucket Zip: <https://github.com/PaloAltoNetworks/appframeworklab/blob/master/buckets/appframework-conf.zip>

Prerequisites

This lab environment requires the following:

- A valid Palo Alto Networks Customer Support Portal (CSP) Account with the **SuperUser**, **Logging Service** and **Directory Sync Service** roles enabled for your organization
- A valid AWS Account
- Palo Alto Networks Licenses:
 - Panorama (serial number and support Auth Code)
 - VM-Series Firewall (2x Auth Codes per firewall (base and bundle))
 - Logging Services (Auth Code)
- AWS Region with 5 available Elastic IPs (4 if not deploying Kali Linux)
- Files required for deployment (provided by Palo Alto Networks):
 - CloudFormation Template (JSON file)
 - 2 ZIP files containing the S3 bucket data
- (Not mandatory but highly recommended) A second or third level domain configured in AWS Route53 (i.e. lab.yourcompany.com with NS records pointing to AWS Route 53 DNS Servers): ask your Palo Alto Networks representative for more details.

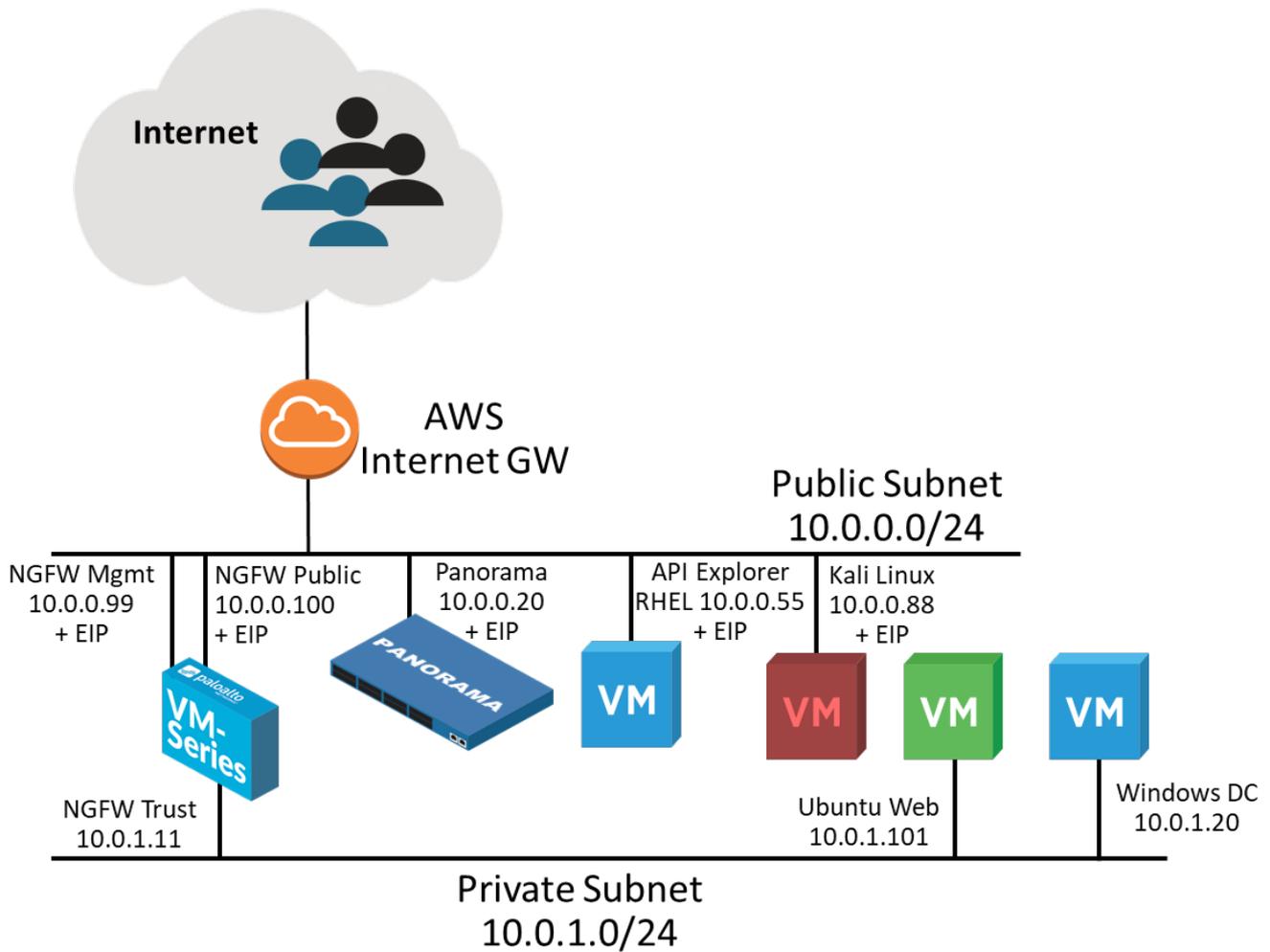
Lab Topology and features

The AWS CloudFormation template automatically deploys a network topology that can be used to generate different logs end events to be sent to the Palo Alto Networks Application Framework.

The following components are included in the template:

- Panorama (10.0.0.20 + EIP assigned for remote reachability)
- Next-Generation Firewall VM Series with the following interfaces:
 - Management: 10.0.0.99 (+ EIP assigned for remote reachability)
 - Public (10.0.0.100) (+ EIP assigned for remote reachability)
 - Internal (10.0.1.11)
- API Explorer VM running RHEL (10.0.0.55 + EIP assigned for remote reachability)
- Kali Linux VM (10.0.0.88 + EIP assigned for remote reachability)
- Ubuntu Web Server behind the firewall (10.0.1.101, reachable via SSH through the firewall Public EIP on port 221)
- Windows Server 2012 R2 Domain Controller behind the firewall (10.0.1.20, reachable via RDP through the firewall Public EIP on port 3389)

The network topology is depicted in the following diagram:



Once created, the environment automatically starts generating traffic through a web crawler installed on the Ubuntu Web server VM. It automatically and periodically updates the User-to-IP mapping on the firewall via API, so the traffic logs will appear with "user1" as source user. The crawler also periodically downloads a sample test PE from the Palo Alto Networks web site, that will trigger a Wildfire event. SSL Decryption is automatically enabled on the firewall with SSL Forward Proxy, and all the web requests from the VMs in the private subnet are decrypted: both the Ubuntu Web server VM and the Windows Domain Controller trust the Firewall pre-created certificate for SSL Decryption. The certificate used by the NGFW for decryption is static and has been pre-added in the environment configuration to simplify the automation: it is possible to replace it post deployment (instructions are not provided in this document).

- For details on VM information and useful commands, see Appendix A
- For details on EIP associations, see Appendix B

Some URL categories (sports, finance) are configured to be blocked or to generate alerts on the firewall, and the web crawler will hit those categories, to automatically generate URL filter events.

A Kali Linux VM is also deployed and can be used to generate attacks on the Ubuntu Web Server VM, in order to generate Threat Logs on the Firewall (need to be done manually, see Appendix A).

NAT rules are configured on the Firewall Public Interface (10.0.1.100, with an EIP associated to it) that allow reachability to the VMs behind it:

- Port 3389 to RDP into the Windows Domain Controller
- Port 22 to SSH on the ubuntu Web VM

The CloudFormation template allows to specify an Administrative password that is automatically configured on the following systems:

- Next-Generation Firewall (for the *admin* user)
- Panorama (for the *admin* user)
- API Explorer VM (for the *ec2-user* user)
- API Explorer application (for the *admin* user)
- Kali Linux VM (for the *ec2-user* user)
- Windows Domain Controller:
 - Domain Admin user (specified at deployment, default is 'paloalto')
 - Other users (user1, user2, user3 -- also with Domain Admin privileges)

Since the password is used widely, it's recommended to select one with a good level of complexity.

Note: if you delete the Stacks deployed through this CFT, make sure you manually delete the EC2 Volumes that are left, otherwise you will end up using space unnecessarily.

Security Hardening Considerations

This environment is meant for development use only, it's not security hardened for production. Specifically, the following security considerations should be known:

- Password authentication via SSH is enabled on both API Explorer (ec2-user user) and Ubuntu Web server (ubuntu user) VMs, using the Administrative password
- Active Directory Password Complexity is disabled
- Administrative password is provided as an environment variable for the installation scripts on the API Explorer, Ubuntu Web Server and Windows Server VMs (part-001 script in Linux VMs, c:\cfn\scripts\pw.txt in Windows), so it may be visible in some of the log files (i.e. /tmp/panorama_setup.log and /var/log/user-data.log on the API Explorer VM and under the logs in c:\cfn on the Windows Server VM)
- The Panorama/NGFW SSH private key must be uploaded in the S3 bucket to automate the password reset process

To perform manual hardening of the environment, the following post-deployment steps are suggested:

- Manually change all the passwords
- Replace the SSH key for authentication on NGFW and Panorama for admin users
- Disable Password based authentication on API Explorer and Ubuntu Web Server VMs

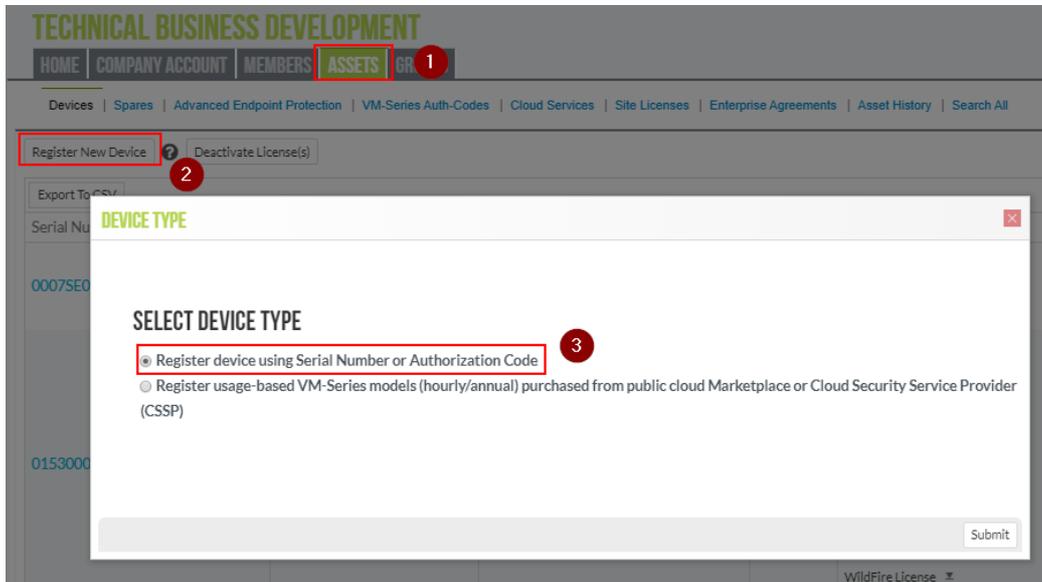
- Re-enable Password complexity on Domain Controller
- Replace the Decryption SSL certificate on NGFW, and import it on both Ubuntu Web Server VMs and Domain Controller

This document is not meant to provide instructions for the above steps.

Palo Alto Networks Customer Support Portal Configuration

This section describes how to register the licenses and activate the services on the Palo Alto Networks Customer Support Portal (CSP)

1. Login to support.paloaltonetworks.com using your CSP (Customer Support Portal) account
2. Navigate to "Assets" and click on "Register New Device", then select "Register device using Serial Number or Authorization Code", then "Submit"

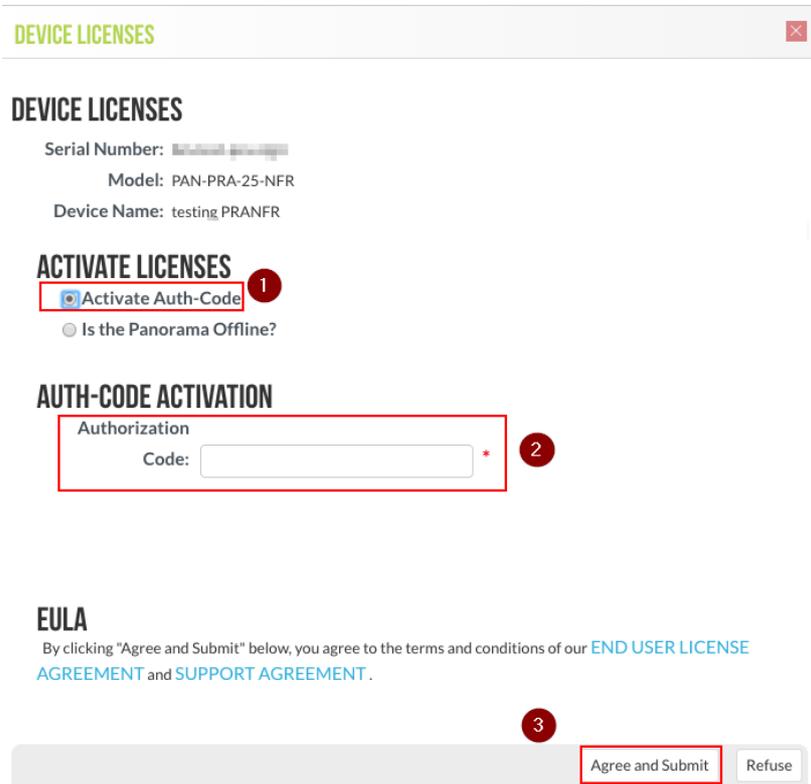


3. Insert your Panorama serial number and fill in the other required fields. Then click on **Agree and Submit**:

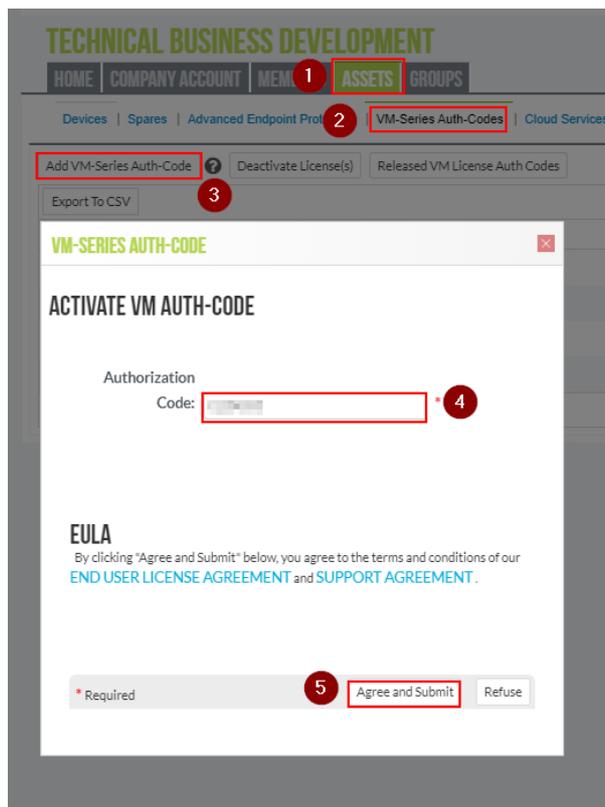
4. You will need to associate the Panorama Support Authcode with the Panorama serial that you registered. From the **Devices** page under the "Assets" tab, click on the **Actions** icon on the line that correspond to the Panorama serial number you just added:

Serial Number	Model Name	Device Name	Group	License	Actions	Auth Code	Expiration Date	ASC	Device Tag	OS Release	Virtual Platform
00075E00	PAN-PRA-25-1	Partner Panorama		AutoFocus Device License Device Management License Logging Service Premium Support		XXXXXXXXXX	10/27/2020			8.1.0	Amazon AWS

5. Select **Activate Auth-Code**, insert the Panorama support Auth-Code (the one that corresponds to the PAN-SVC-NFR-PRA-25 SKU) and click on **Agree and Submit**:



6. Navigate to "Assets", then go to "VM-Series Auth-Codes", select "Add VM-Series Auth-Code". Enter the VM-Series Auth-Code (the one that corresponds to the PAN-VM-100-NFR SKU) and click on "Agree and Submit":



7. Navigate to "Assets", then select "Cloud Services" and click on "Activate Cloud Services Auth-Code".

8. Enter the Logging Service Auth-Code. Then select the serial number of the Panorama device that you entered in the previous step, and the region (americas). Then click on "Agree and Submit":

ACTIVATE CLOUD SERVICES AUTH-CODE

Upon activation of your Cloud Service, please go to the Logging Service app on [Cloud Services Portal](#) to adjust log quota for this app. [More details](#)

Authorization

Code: * 1

Panorama: * 2

Logging Region: * 3

EULA

By clicking "Agree and Submit" below, you agree to the terms and conditions of our [END USER LICENSE AGREEMENT](#) and [SUPPORT AGREEMENT](#).

* Required

4

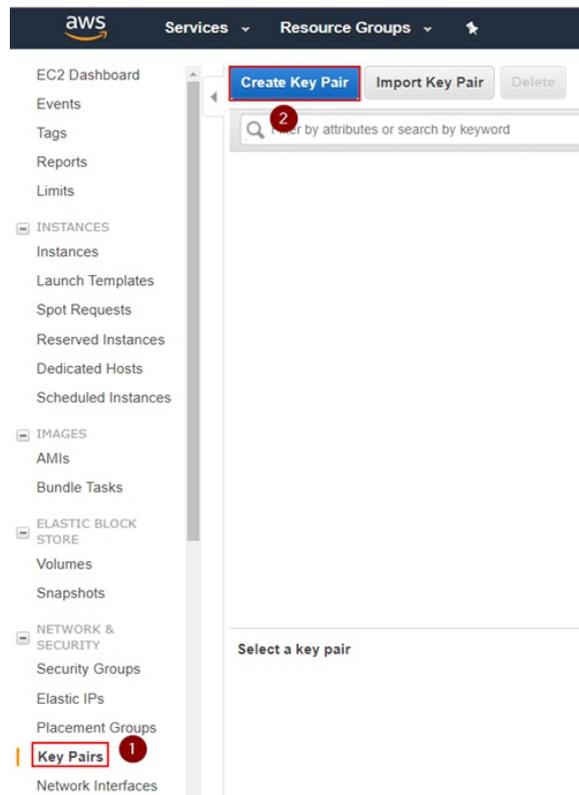
Note: If you don't see the option to activate the Cloud Services, you might not have the required permissions in CSP.

##AWS Configuration

This section describes the configuration of the AWS required components to deploy the lab components. You'll need a KeyPair, two S3 buckets and (optional) a Route53 Hosted Zone. You'll also need to accept the terms for Palo Alto Networks VM-Series, Panorama and Kali Linux.

Key Pair Creation

1. Navigate to your selected region (i.e. us-east-1), select the **EC2** service and under **Network & Security** select **Key Pairs** and click on **Create Key Pair**:



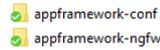
2. Insert a keypair name and click on **Create**. In the example, we use "paloalto". This will create a "paloalto.pem" private key and the AWS Web UI will prompt you to download it.



3. Download the Private Key to your local machine. The file name of this example will be **paloalto.pem**, but you can choose an arbitrary name. You will need to upload this file in an S3 bucket later.

S3 Bucket Pre-Configuration

Palo Alto Networks should have provided you two URLs to download the required files, that you will need to upload into 2 separate S3 buckets. One is used for the Firewall provisioning and the other for the miscellaneous lab configurations. Download and unzip the archives in two separate folders that correspond to the two buckets:



In the example we use **appframework-ngfw** for the firewall configuration and **appframework-conf** for the lab miscellaneous configuration. You can use any arbitrary name for the S3 buckets, but they will have to be unique in AWS.

If you look inside the **configuration** bucket folder (appframework-conf in the example), you will see 3 sub-folders (keys, opt, templates):



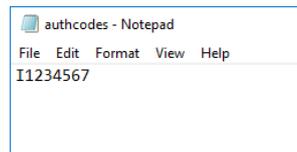
If you look inside the **NGFW** bucket folder (appframework-ngfw in the example), you will see 4 folders (config, content, license, software):



Most of the files should be left untouched, however there are two actions required before uploading the files to AWS S3.

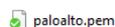
To prepare the configuration files do the following:

1. Add the Firewall Auth-Code:
2. On your local machine, navigate to the folder that corresponds to the NGFW configuration bucket (appframework-ngfw in the example), go to the **license** sub-folder and edit the **"authcodes"** file and insert (without any newlines) the NGFW Auth-Code you received from Palo Alto Networks:



Note: you will need to use the authcode that corresponds to the **PAN-VM-100-NFR** SKU, the same one you previously registered in the Customer Support Portal.

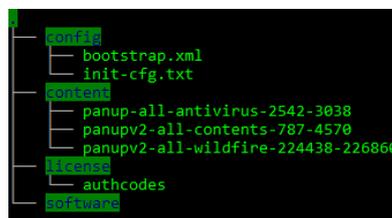
- Save the file
- Add the Firewall and Panorama AWS Private Key
- On your local machine, navigate to the folder that corresponds to the lab configuration bucket (appframework-conf in the example), go to the **Keys** sub-folder and copy in it the private key file that you previously generated and downloaded from the AWS UI (paloalto.pem in the example):



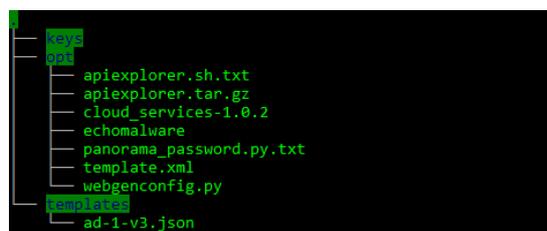
- You can name your key filename however you prefer, but that exact filename will have to be entered as the input to the CFT file later in the deployment process.

Once you've updated the files, the trees of both folders should look similar to the following:

1. NGFW Configuration Folder (filenames in the **content** folder might differ):



2. Lab Configuration folder:

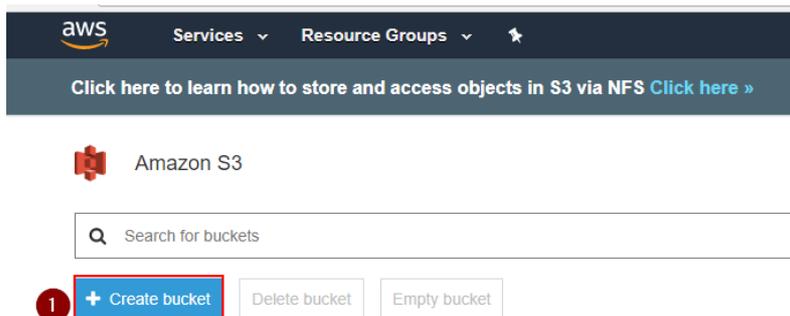


You are now ready to create the S3 Buckets in AWS and upload these files.

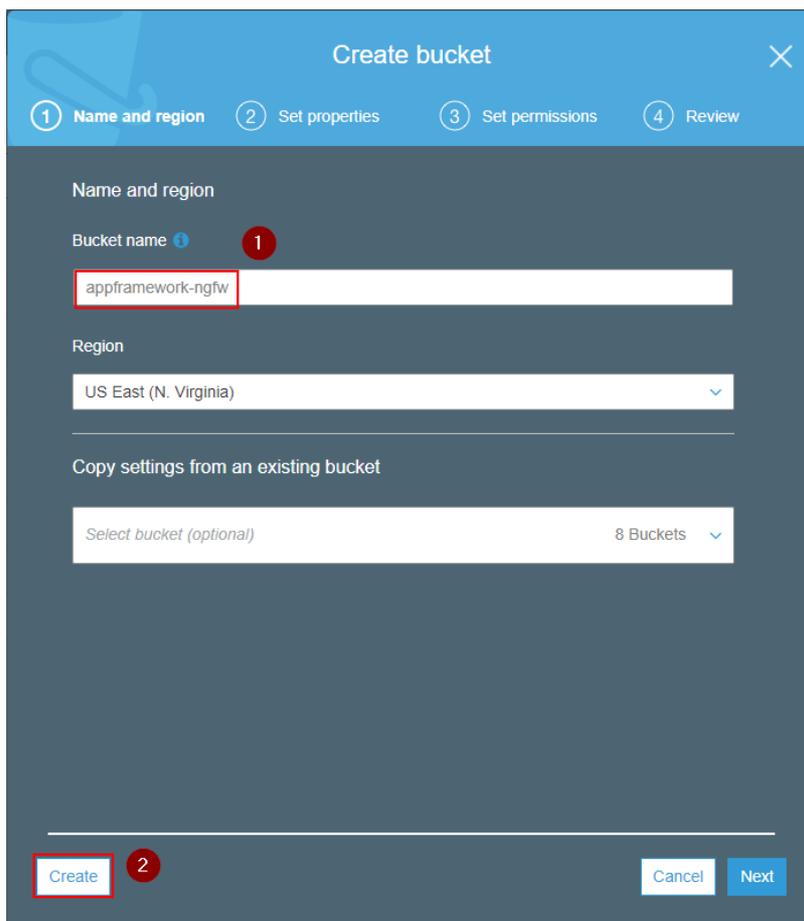
S3 Bucket Creation and Upload

To create the S3 Buckets and upload the files, go through the following steps:

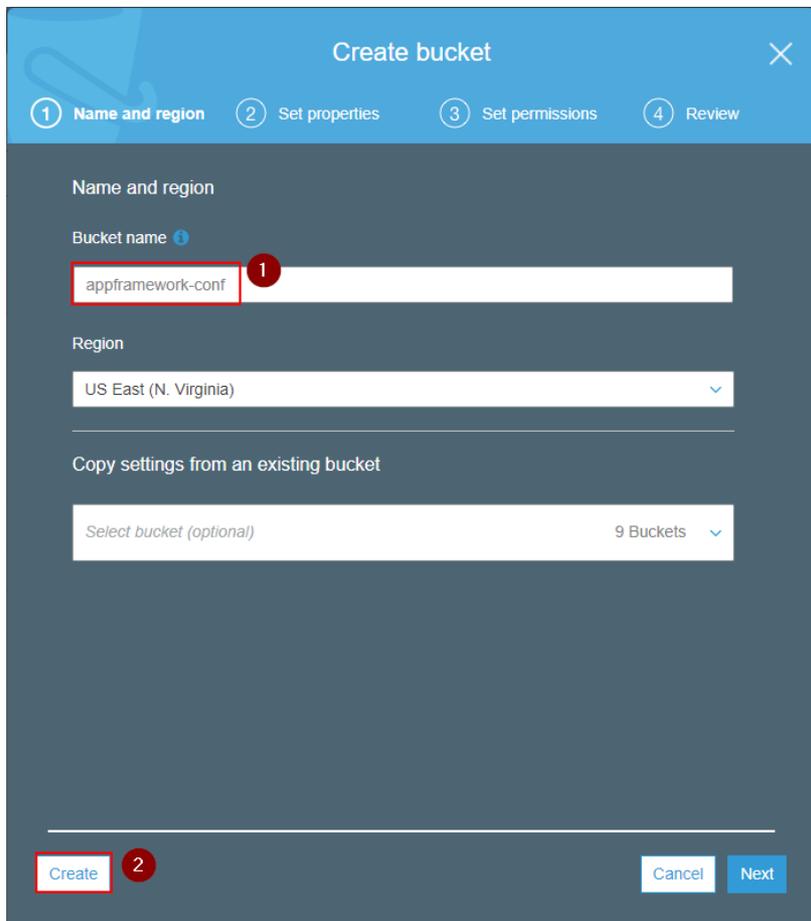
1. Go to AWS S3 and create two S3 buckets for the NGFW and lab configuration respectively `appframework-ngfw` and `appframework-conf` in the example). To create an S3 bucket, click on **Create Bucket**:



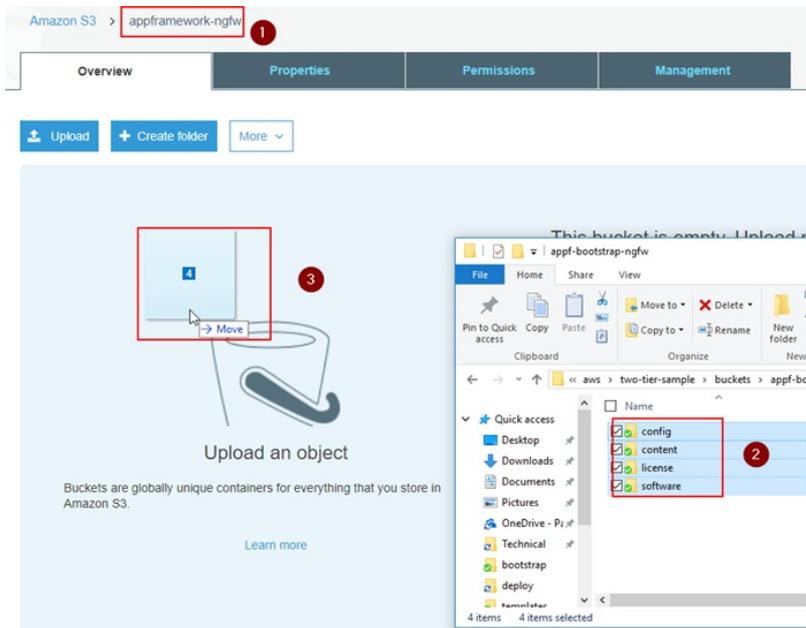
2. Enter the name of the Firewall configuration bucket (`appframework-ngfw` in the example) and select **Create**:



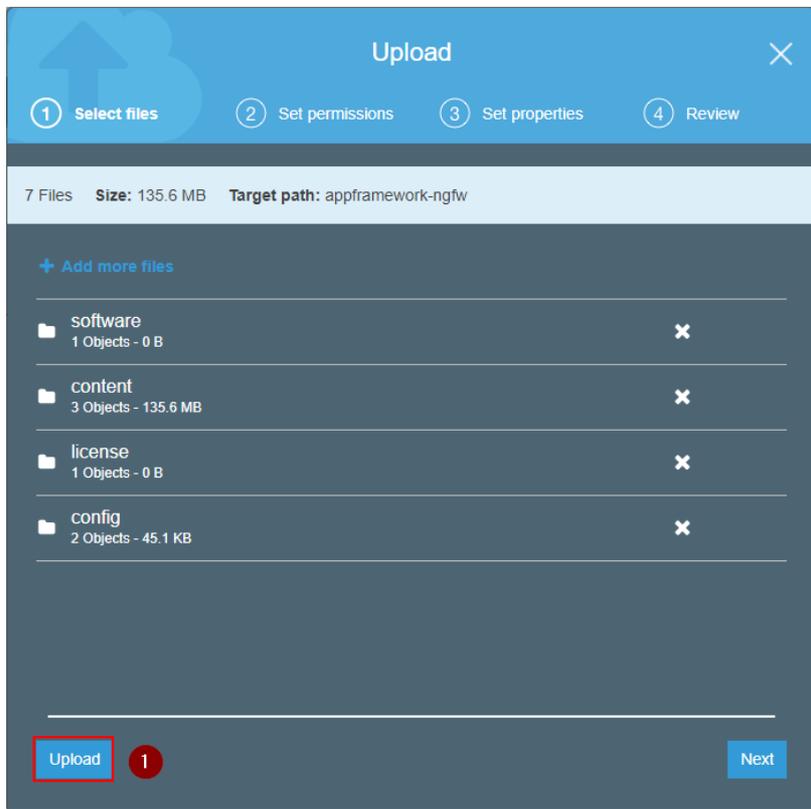
3. Repeat the same process for the Miscellaneous lab configuration S3 bucket (`appframework-conf` in the example):



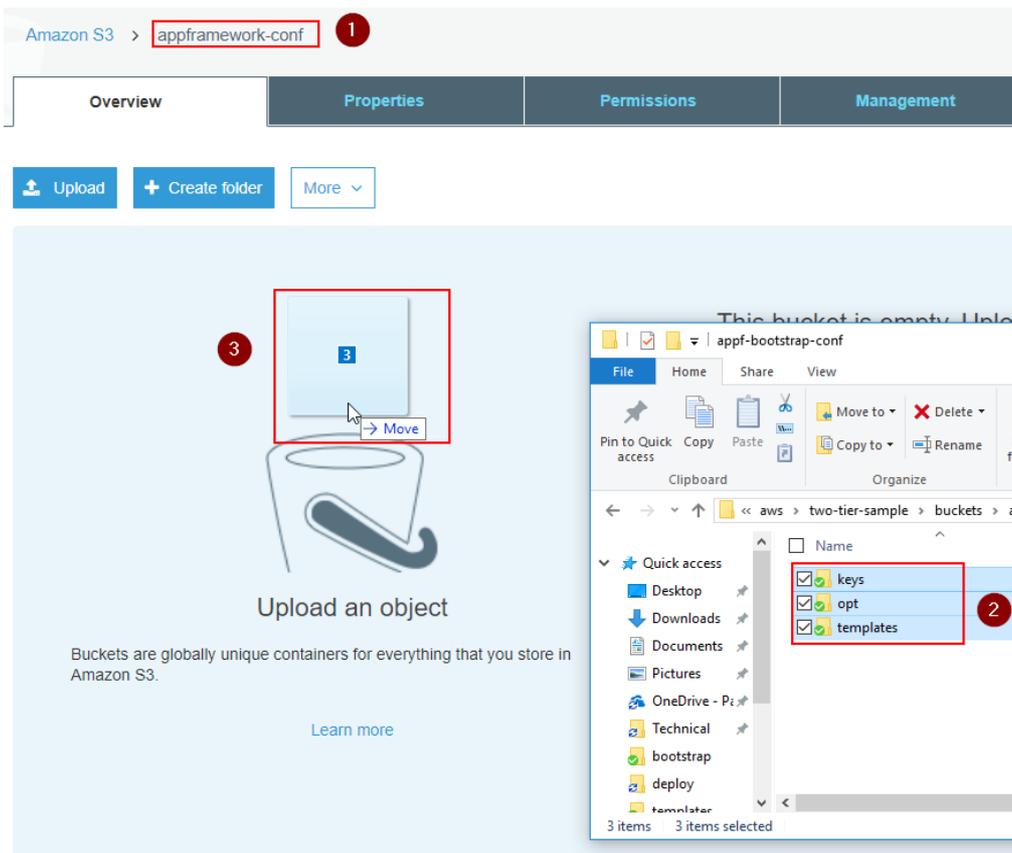
4. You can now upload the content in the respective buckets by dragging and dropping the files from your computer using the AWS S3 UI. The next picture shows the appframework-ngfw bucket:

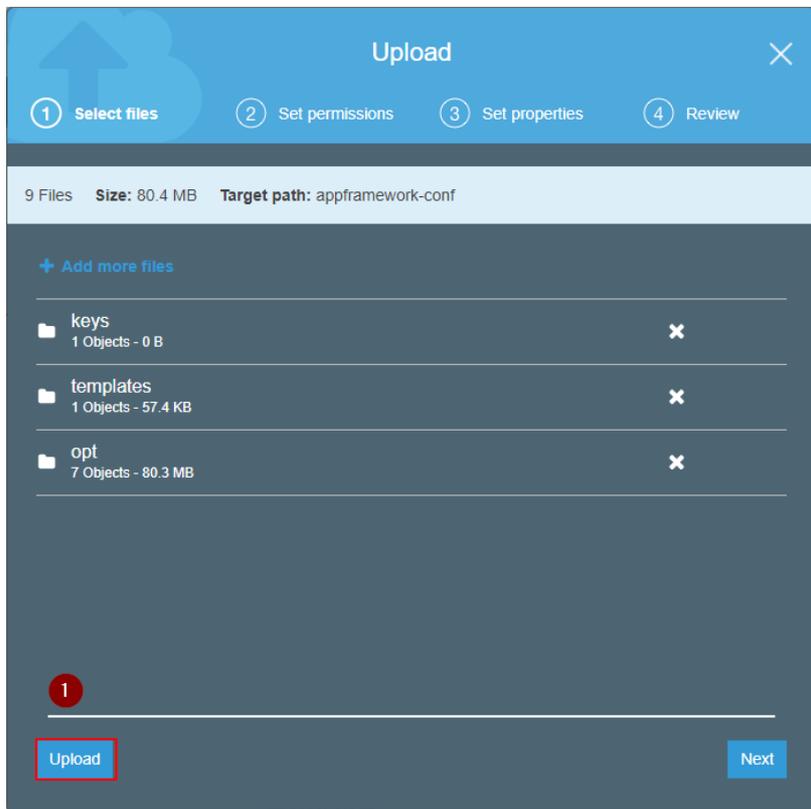


5. Make sure the 4 folders (config, content, license, software) are copied in the root of the S3 bucket, and click **Upload**:



6. Repeat the process for the lab configuration bucket:





Note: the Drag&Drop feature sometimes doesn't copy all the files. Please double check that you have everything there.

Route53 Zone Configuration

The CloudFormation Template deploys a series of VMs (Firewall, Panorama, API Explorer, Kali Linux, etc.) and AWS can automatically associate DNS names to the Elastic IPs that are used by EC2. To do that, you need a Route53 public Hosted Zone configured in your AWS environment. This step is optional: you can just connect to the VMs via their Elastic IP addresses, or manually configure your DNS entries at a later stage if you're not using Route53. However, this step is highly recommended.

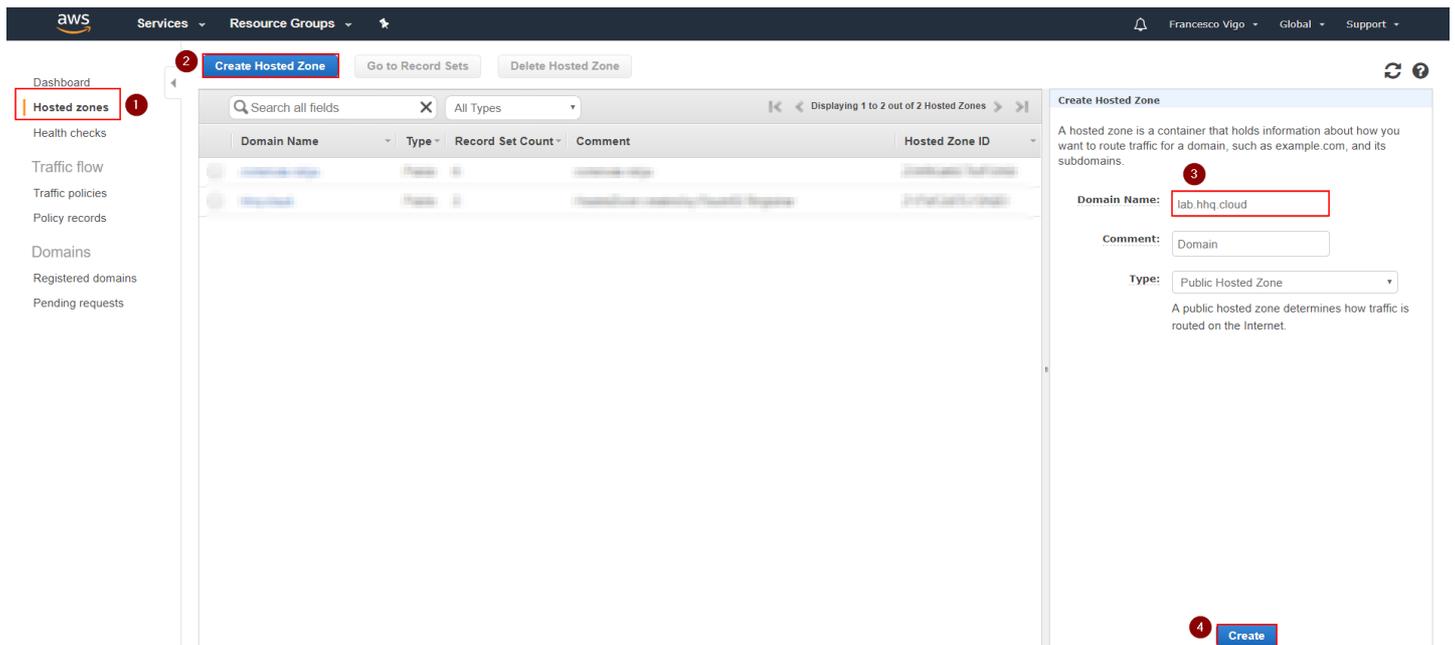
The public DNS zone you use can either be an existing second-level domain (i.e. yourcompanylab.com), or a third-level domain (lab.yourcompany.com). It must be publicly resolvable, so you need to be the registered owner of the domain. As an option, you can register a new domain directly through the AWS console and add it automatically in Route53.

If you don't have the opportunity to use a second or third level domain in Route53, ask your Palo Alto Networks contact for support to get a fourth level domain delegated to your Route53 DNS Servers.

Note: the CFT can automate the creation and registration of a valid SSL certificate that corresponds to the FQDN of your API Explorer instance (this way the browser won't provide warnings when you connect to it), through a free service called "Let's Encrypt" (<https://letsencrypt.org>). If you want to automatically generate the Let's Encrypt certificate through the CFT, you must have the Route53 configuration enabled, otherwise the process will fail. Hence, if you don't want to use Route53 for this step, the API Explorer certificate must be a self-signed one. The CFT parameters provide options to disable the configuration of Route53 and Let's Encrypt.

To configure a Hosted zone in AWS Route 53, proceed through the following steps:

1. Navigate to AWS **Route53**, go to **Hosted zones** and click on **Create Hosted Zone**. Enter the domain name: it must be a public domain name (second or third level) where you have permissions configure name servers for (i.e. yourcompanylab.com or lab.yourcompany.com). The type must be **Public Hosted Zone**. Then click on **Create**:



2. Look at the AWS Name Servers listed in the NS record and configure your Domain Hosting provider platform to use them for the selected domain:

Name	Type	Value	Evaluate Target Health	Health Check ID	TTL	Region	Weight	Geolocate
lab.hhq.cloud.	NS	ns-829.awsdns-39.net. ns-1192.awsdns-21.org. ns-2012.awsdns-59.co.uk. ns-36.awsdns-04.com.	-	-	172800			
lab.hhq.cloud.	SOA	ns-36.awsdns-04.com. awsdns-hostmaster.amazon.	-	-	900			

In this example we are using the third-level domain `lab.hhq.cloud`.

Note: if you registered the domain through AWS, you don't need any additional configuration as it will be automatically registered in Route

53. If you're using a different domain hosting platform (i.e. GoDaddy, NameCheap, etc), the configuration on how to configure your domain to use AWS Route53 DNS servers will be different depending on your provider.

If you're being helped by Palo Alto Networks to use a fourth level domain, please provide the Name Servers to your contact.

Activate Kali Linux and Palo Alto Networks VMs Series on AWS Marketplace

To deploy some of the VMs, you first need to activate them on the AWS marketplace. Note that deploying Kali Linux is optional (is useful to generate threats in the firewall logs) so, if you don't need it, you can skip the step for Kali Linux (but not for NGFW and Panorama).

To activate the solutions on the AWS Marketplace, follow this procedure:

1. Navigate to the AWS Marketplace (<https://aws.amazon.com/marketplace>), search for "kali" and click on the search icon:

2. In the results page, click on **Kali Linux**:

kali (1 result) showing 1 - 1

Kali Linux

★★★★★ (5) | Version Kali Linux 2018.1* | Sold by Kali Linux

Kali Linux is a Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. Kali contains several hundred tools targeted towards Linux/Unix, Other 2018.1 - 64-bit Amazon Machine Image (AMI)

showing 1 - 1

3. In the Kali Linux page, click on **Continue to Subscribe**:

4. Select **Manual Launch** and click on **Accept Software Terms**:

Manual Launch
With EC2 Console, API or CLI

Service Catalog
Copy to SC and Launch

Click "Accept Software Terms" to gain access to this Software

Once you accept these terms, you will have access to this software in any supported region. You can then launch the AMIs listed below directly from the EC2 console, EC2 APIs, or with other AWS management tools.

Price for your Selections:

Price will be dependent on usage

Accept Software Terms

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 \(EULA\)](#) and your use of AWS services is subject to the [AWS Customer Agreement](#).

5. Repeat the same procedure for both Palo Alto Networks **"VM-Series Next-Generation Firewall (BYOL)"** and **"Palo Alto Networks Panorama"**

VM-Series Next-Generation Firewall (BYOL)

[Manual Launch](#)
With EC2 Console, API or CLI

[Service Catalog](#)
Copy to SC and Launch

Launch Options

You can click the "Launch with EC2 Console" buttons below and follow the instructions to launch an instance of this software.

You can also find and launch these AMIs by searching for the AMI IDs (shown below) in the "Community AMIs" tab of the EC2 Console Launch Wizard.

You can view this information at a later time by visiting the Your Software page. For help, see step-by-step instructions for launching Marketplace Products from the AWS Console.

▼ **Version**

PAN-OS 8.1.0, released 03/13/2018

[Usage Instructions](#)

Palo Alto Networks Panorama

[1-Click Launch](#)
Review, modify and launch

[Manual Launch](#)
With EC2 Console, API or CLI

[Service Catalog](#)
Copy to SC and Launch

Click "Accept Software Terms & Launch with 1-Click" to launch this software with the settings below

Once you accept the terms, you will have access to launch any version of this software in any supported region. For future launches, you can return to this page or launch directly from the EC2 console, APIs or CLI.

▶ **Version**

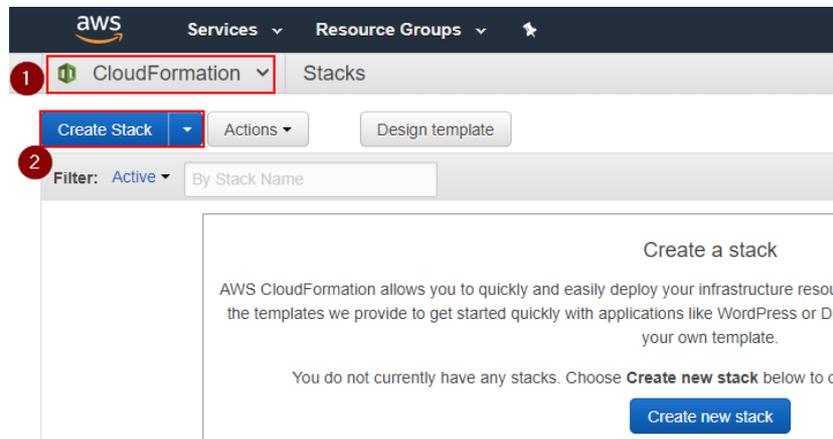
Panorama 8.1.0, released 03/13/2018

Deploy the CloudFormation Template

You can now deploy the AWS CloudFormation Template (CFT) to create the lab environment. Before starting, make sure that you have 5 Elastic IPs (EIPs) available in the region you want to deploy the CFT (by default AWS limits EIPs to 5 per region per account).

Proceed with the following steps:

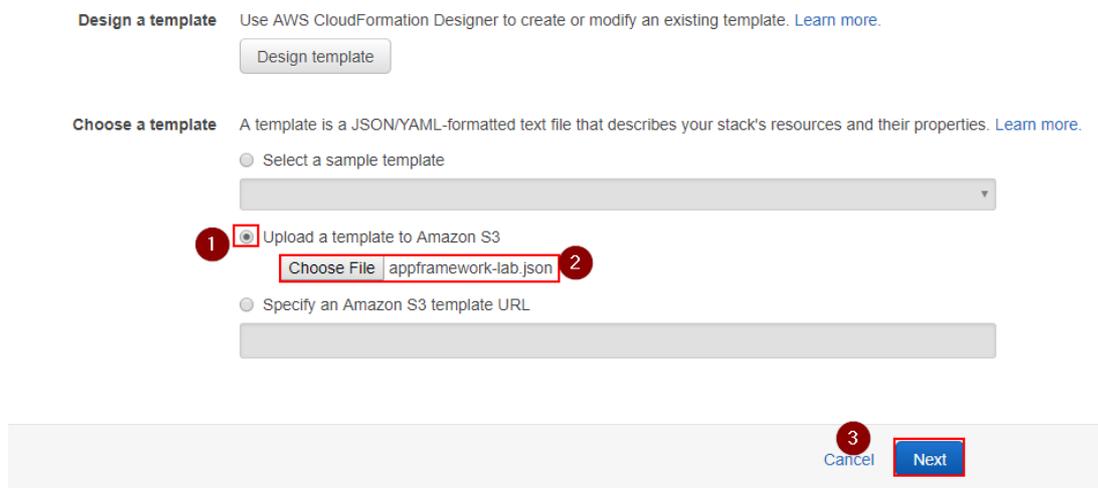
1. Navigate to "AWS CloudFormation" and select "Create Stack":



2. Select "Upload a template to Amazon S3"; and upload the template JSON file provided by Palo AltoNetworks `appframework-lab.json` in the example), then click on **Next**:

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.



3. Insert the required parameters:

- **Stack name:** an arbitrary name for this deployment (i.e. PartnerLab1)
- **Admin Password:** an arbitrary password that will be used for the following systems:
 - NGFW admin user
 - Panorama admin user
 - API Explorer VM ec2-user user (SSH login with password will be enabled)
 - API Explorer application admin user
 - Ubuntu Web Server ubuntu user (SSH login with password will be enabled)
 - Kali Linux ec2-user
 - Windows Domain Controller admin (the default username is "paloalto", but can be changed in the advanced parameters below)
 - Windows Domain Users (user1, user2, user3)
- **Environment Config Bucket Name:** the name of the S3 miscellaneous lab configuration bucket that you previously created. In the example `appframework-conf` was used.
- **Bootstrap Bucket Name:** the name of the S3 NGFW configuration bucket that you previously created. In the example, `appframework-ngfw` was used.
- **Bootstrap Bucket Region:** select the AWS region where the Bootstrap Bucket was created (`us-east-1` in the example)
- **Private Key File:** the relative path in the configuration bucket of the NGFW/Panorama private key file. In the example the file is named `paloalto.pem` and you uploaded it in the `keys` subfolder of the environment configuration bucket. Hence, the parameter would be `"keys/paloalto.pem"`. If you named the file differently, provide the right name.
- **EC2 VMs Key Name:** from the drop down menu, select the KeyPair that you want to use for the non-Palo Alto Networks VMs (Kali Linux, API Explorer VM, Ubuntu VM). It can be the KeyPair that you previously created in EC2, or a different one of your choice.
- **Panorama and NGFW Key Name:** from the drop down menu, select the KeyPair that you want to use for the Palo Alto Networks VMs (Panorama and NGFW). This **must** be the KeyPair that you have previously created (named "paloalto" in the example), whose private key was uploaded to the miscellaneous lab configuration S3 bucket.
- **Panorama Serial:** Insert the Panorama Serial number that was provided by Palo Alto Networks
- **DNS Domain Name:** Insert the domain name zone that you have configured on Route53. If you don't have it, add a domain name and select "false" under both the "Configure Route53" AND the "Create API Explorer LetsEncrypt Cert" fields in the Advanced Configuration section. In the example we use the `hhq.cloud` domain.
- **LetsEncrypt Email:** Insert your (valid) email address that will be used to request a Let's Encrypt SSL certificate for the API Explorer.

Leave the other parameters to the default values unless you are a power user and you know what you're doing.

The following screenshot shows an example configuration:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

Stack name

Parameters

Basic Configuration - REQUIRED

Admin Password	<input type="password" value="*****"/>	Password for API Explorer, NGFW/Panorama admin, VMs ec2-user/ubuntu users (SSH password auth enabled), Windows DC admin and users. Must be at least 8 characters containing letters, numbers and symbols
Environment Config S3 Bucket Name	<input type="text" value="appframework-conf"/>	Bucket name for non-Firewall configuration (i.e. myappframeworkbucket-conf)
Bootstrap S3 Bucket Name	<input type="text" value="appframework-ngfw"/>	S3 Bucket name for FW bootstrap configuration (i.e. myappframeworkbucket-conf)
Bootstrap S3 Bucket Region	<input type="text" value="us-east-1"/>	S3 Region where the FW bootstrap bucket is located
Private Key File	<input type="text" value="keys/paloalto.pem"/>	Private Key File with Path in the Environment Configuration S3 Bucket (i.e. keys/paloalto.pem)
EC2 VMs Key Name	<input type="text" value="paloalto"/>	Name of an existing EC2 KeyPair to enable SSH access to VMs. Except NGFW and Panorama
Panorama and NGFW Key Name	<input type="text" value="paloalto"/>	Name of an existing EC2 KeyPair to enable SSH access to NGFW and Panorama
Panorama Serial	<input type="text" value="0000000000"/>	Panorama Serial Number (provided by Palo Alto Networks)
DNS Domain Name	<input type="text" value="hhq.cloud"/>	DNS Domain Name or Route53 Hosted Zone Name (i.e. panwlab.mycompany.com)
LetsEncrypt Email	<input type="text" value="devrel@paloaltonetworks.com"/>	Email address to provide to Letsencrypt for API Explorer SSL certificate generation (i.e. user@mycompany.com)

4. Click on "Next" twice.

5. In the Review page, at the bottom, under 'Capabilities', check the 'I acknowledge that AWS CloudFormation might create IAM resources with custom names' box, and click on 'Create':

Capabilities

i The following resource(s) require capabilities: [AWS::IAM::Role, AWS::CloudFormation::Stack]
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)

I acknowledge that AWS CloudFormation might create IAM resources with custom names.



[Quick Create Stack](#) (Create stacks similar to this one, with most details auto-populated)

Note: the CFT will create two IAM roles to allow some of the VMs to Read the files from the two S3 buckets that you've previously created.

6. Sit down and relax, the whole process will take 30-35 minutes to complete:

Stack Name	Created Time	Status	Description
<input type="checkbox"/> PartnerLab1-DomainControll... NESTED	2018-03-22 21:13:19 UTC-0700	CREATE_IN_PROGRE...	This template creates 1 Active Directory Domain Controller in a private subnet. The d...
<input checked="" type="checkbox"/> PartnerLab1	2018-03-22 21:12:13 UTC-0700	CREATE_IN_PROGRE...	Palo Alto Networks AppFramework PlayGround with API Explorer

7. The deployment will show **CREATE_COMPLETE** once everything is done:

CloudFormation Stacks

Create Stack Actions Design template

Filter: Active By Stack Name Showing 2 stacks

Stack Name	Created Time	Status	Description
PartnerLab1-DomainControll... NESTED	2018-03-22 21:13:19 UTC-0700	CREATE_COMPLETE	This template creates 1 Active Directory Domain Controller in a private subnet. The d...
<input checked="" type="checkbox"/> PartnerLab1	2018-03-22 21:12:13 UTC-0700	CREATE_COMPLETE	Palo Alto Networks AppFramework Playground with API Explorer

Note: if you run in an error, make sure you added the right licenses and Auth-Codes, check the FAQ document and reach out to your Palo Alto Networks contact for support.

8. Select the template and click on the **Outputs** tab of the to view the deployment information (IP addresses and FQDNs) of the lab:

Filter: Active By Stack Name Showing 2 stacks

Stack Name	Created Time	Status	Description
PartnerLab1-DomainControll... NESTED	2018-03-28 15:05:46 UTC-0700	CREATE_COMPLETE	This template creates 1 Active Directory Domain Controller in a private subnet. The default Domain Administrator password will be the one retrieved from the instance. Additional users (user1, user2, us...
<input checked="" type="checkbox"/> PartnerLab1	2018-03-28 15:04:40 UTC-0700	CREATE_COMPLETE	Palo Alto Networks AppFramework Playground with API Explorer

Overview **Outputs** Resources Events Template Parameters Tags Stack Policy Change Sets Rollback Triggers

Key	Value	Description	Export Name
APIExplorerAppURL	https://apiexplorer.lab.hhq.cloud	API Explorer URL	
KaliLinuxIP	52.15.80.97	Kali Linux Public IP	
PanoramaURL	https://panorama.lab.hhq.cloud	Panorama URL	
FirewallManagementURL	https://ngfw.lab.hhq.cloud	VM-Series management interface URL	
PublicIPAddress	18.218.130.35	Public IP Address	

9. You can also see all the DNS records added to Route53 records for easier access:

Dashboard

Hosted zones

Health checks

Traffic flow

Traffic policies

Policy records

Domains

Registered domains

Pending requests

Back to Hosted Zones Create Record Set Import Zone File Delete F

Record Set Name Any Type Aliases Only Weighted O

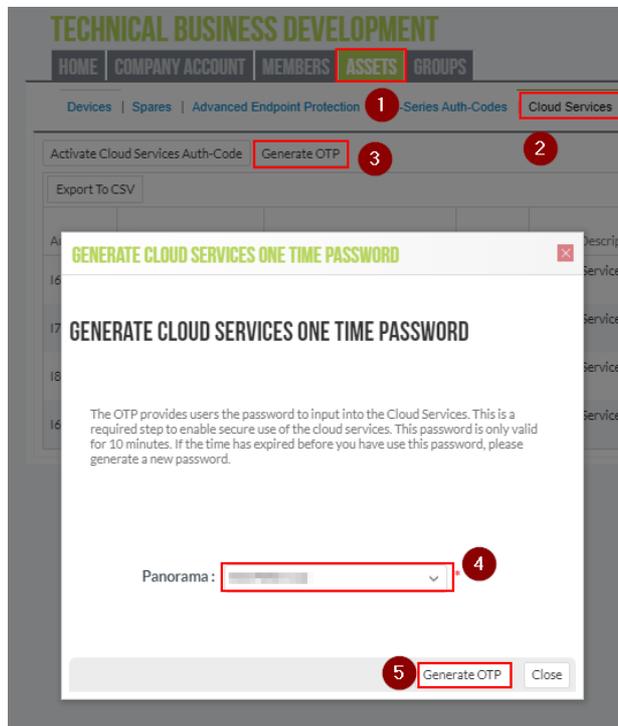
Name	Type	Value
lab.hhq.cloud.	NS	ns-829.awsdns-39.net. ns-1192.awsdns-21.org. ns-2012.awsdns-59.co.uk. ns-36.awsdns-04.com.
lab.hhq.cloud.	SOA	ns-36.awsdns-04.com. awsdns-hostmaster.amazon.
apiexplorer.lab.hhq.cloud.	A	18.217.43.119
kali.lab.hhq.cloud.	A	52.15.80.97
ngfw.lab.hhq.cloud.	A	18.188.91.210
panorama.lab.hhq.cloud.	A	18.221.237.136
public.lab.hhq.cloud.	A	18.218.130.35

AT THIS STAGE YOU SHOULD STOP. A MANUAL CONFIGURATION STEP TO POINT THE FIREWALL AND PANORAMA TO THE DEVELOPER INSTANCES IS REQUIRED, PLEASE REACH OUT TO YOUR PALO ALTO NETWORKS TECHNICAL CONTACT FOR THIS.

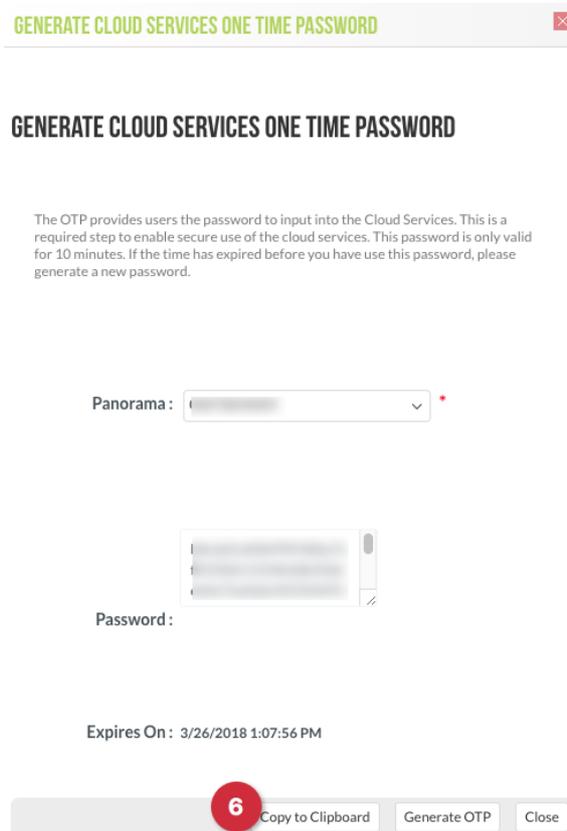
Panorama Pairing with Logging Service

The last step of the process requires to pair your Panorama Instance with Logging Service:

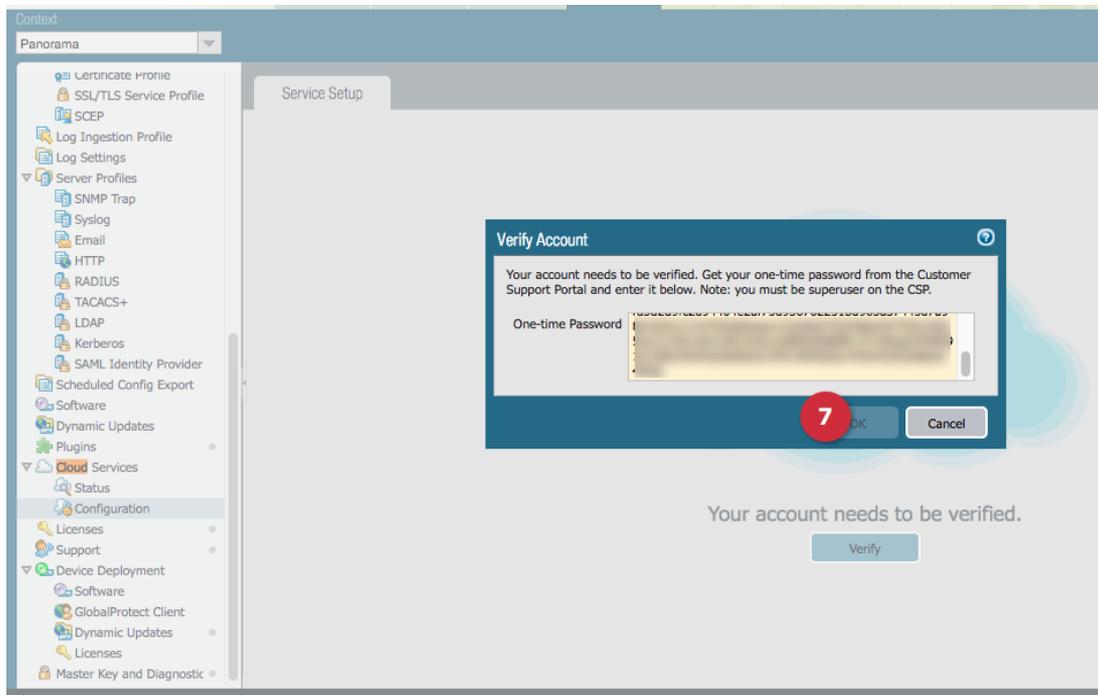
1. Navigate back to <https://support.paloaltonetworks.com> and login with your CSP credentials
2. Go to "Assets", "Cloud Services" and click "Generate OTP". Select the Panorama instance you've created (corresponding to the Panorama Serial Number) and click on "Generate OTP":



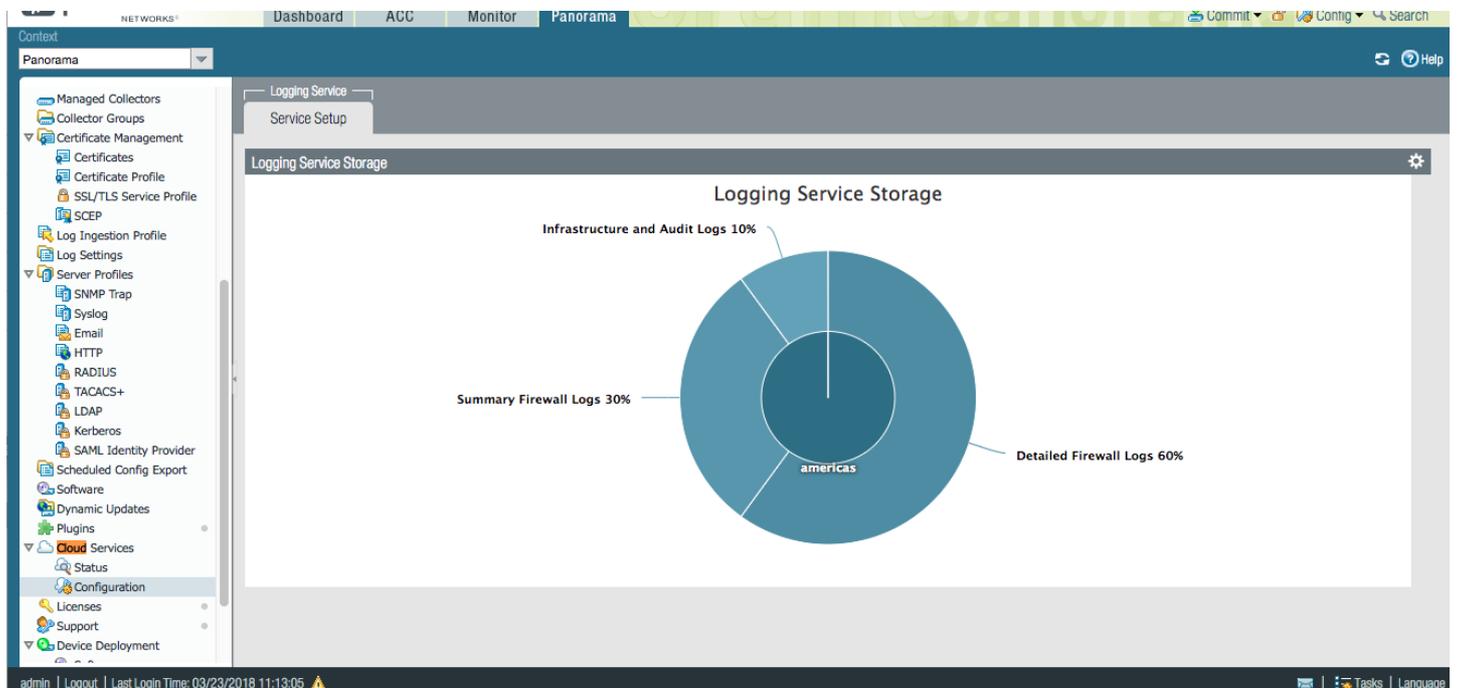
- Copy the generated One Time Password in your browser clipboard by clicking on **Copy to Clipboard** (6):



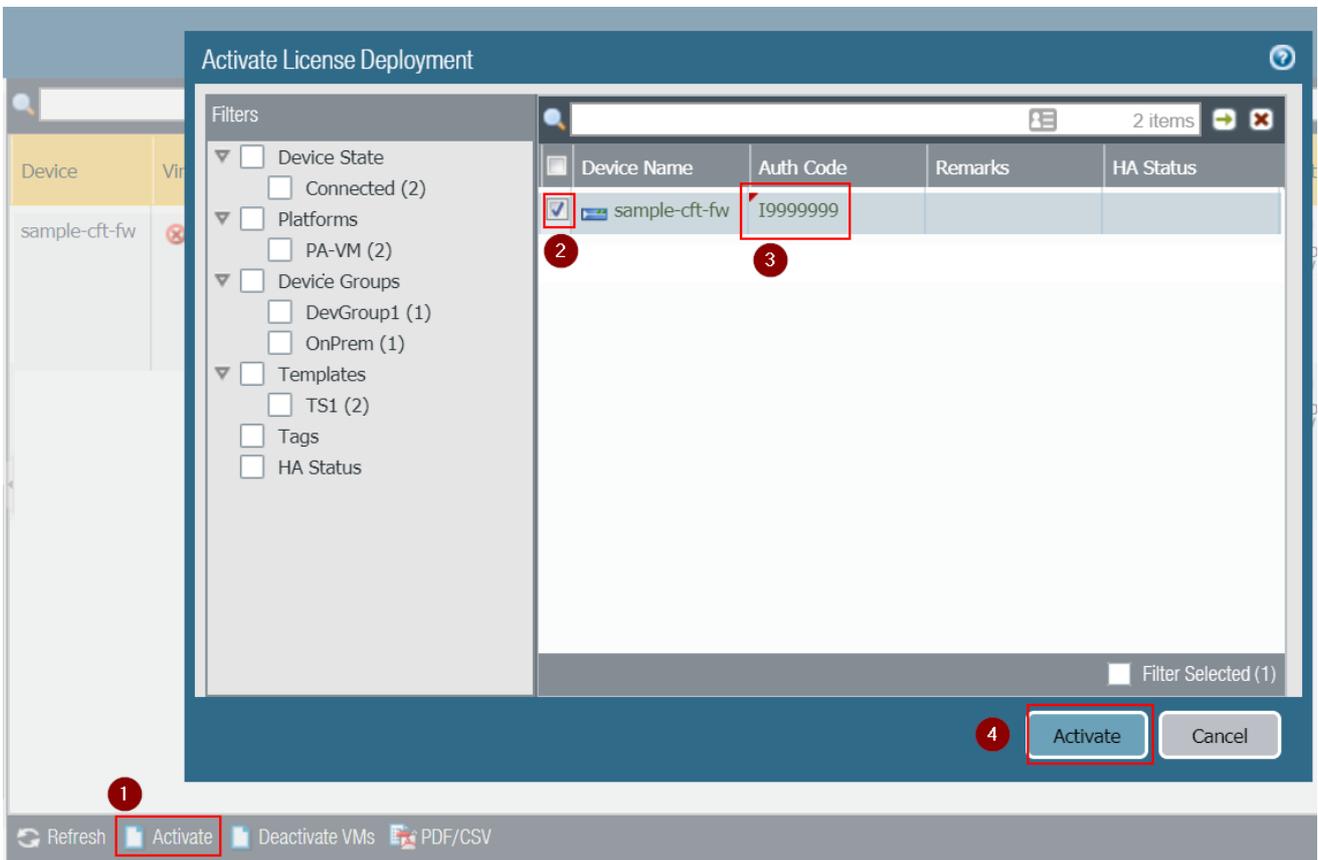
- Login to Panorama via the web UI, navigating to <https://panorama.lab.yourdomain.com> (assuming that Route53 has used to automatically create the FQDN, otherwise look at the EIP of the Panorama instance). Use the "admin" user and the password you have configured in the template.
- On the Panorama UI, navigate to **Panorama**, **Cloud Services**, **Configuration**.
- Insert the previously copied One Time Password (OTP) to complete the pairing and click on **OK** (7):



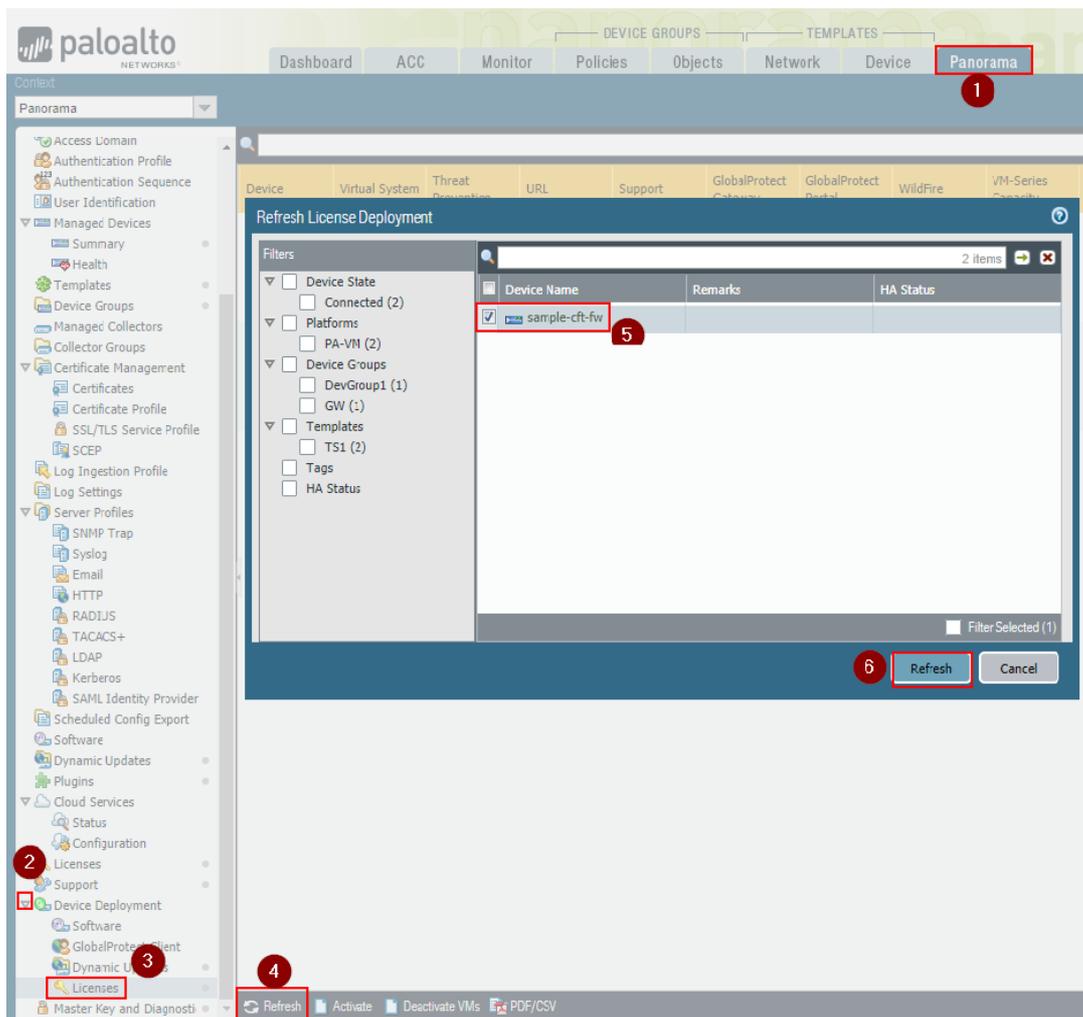
After the pairing is complete, in the "Configuration" page under "Cloud Services", you should see a dashboard similar to the following:



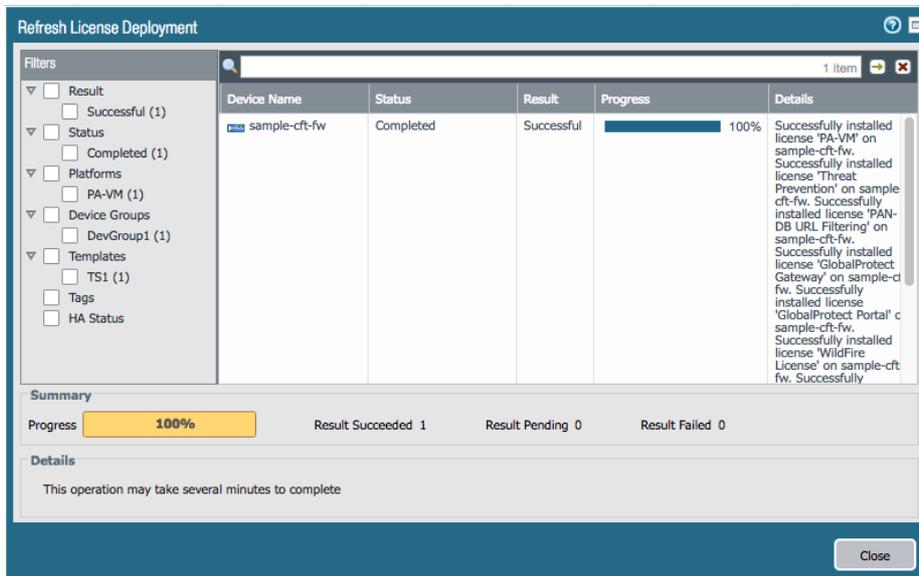
7. On the Panorama UI, navigate to **Panorama**, **Device Deployment**, **Licenses** and click on **Activate**.
8. Select the firewall (**sample-cft-fw** in the example), insert the Services Bundle Auth-Code (the one that corresponds to the **PAN-VM-100-BND-NFR4** SKU) and click on **Activate**:



9. On the Panorama UI, navigate to "Panorama", "Device Deployment", "Licenses" and click on Refresh.
10. Select the firewall (sample-cft-fw in the example) and click on Refresh* to refresh the licenses:



The refresh process will take a few seconds. Wait until it completes:



After the license refresh is complete, wait a few minutes.

Under the Monitor tab in Panorama you should be able to view Logs (see Appendix C)

Congratulations, the setup is complete!

You can work with your Palo Alto Networks contact to register the API Explorer application in the Application Portal, and then activate it (see the next section of this document for details)

API Explorer App Activation Process

This section describes how to Activate the API Explorer application and start interacting with the APIs.

Note: this section requires the manifest file activation part to be already configured, otherwise you will not see your API Explorer application in the App Portal. You will also be provided **Client ID** and a **Client Secret** by your Palo Alto Networks contact.

To activate the API Explorer, follow this process:

1. Navigate to the App Portal beta environment: <https://apps-stg4.app-portal-beta.us.paloaltonetworks.com> and Sign in with your Customer Support Portal credentials:



2. Activate an instance of Directory Sync Service by clicking on the **Activate** button in the **Directory Sync** tile:

Your Palo Alto Networks Cloud Services Apps



Logging Service



Activate New App

If you have activated an app and do not see it above, you might not have the roles required to access the app. Please go to the Customer Support Portal to obtain the roles from your organization's administrator.

More Available Palo Alto Networks Apps



Directory Sync
Allow Palo Alto Networks Cloud Services to access your organization's directory

1 Activate [Learn More →](#)



Magnifier
Discover malicious activity and stop attackers and malware operating inside your network

[Learn More →](#)



Traps
Advanced, multi-method malware prevention that protects users and endpoints

[Learn More →](#)

3. Enter an arbitrary **Instance Name** and select **Americas** as **Region**, then click on **OK**:

Directory Sync ✕

* Instance Name: 1

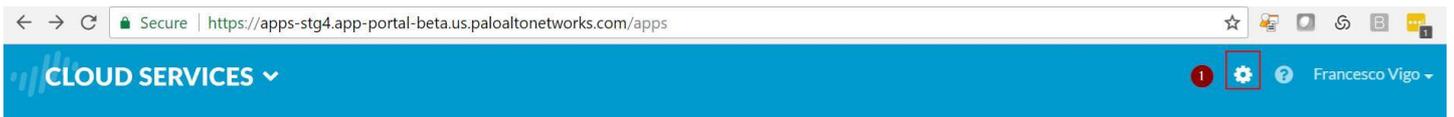
Description:

* Region: 2

3

Note: You don't need to actually register an Active Directory agent to it if you don't need to interact with AD data to build your integration. Or you can deploy the Directory Sync Agent on the windows Domain Controller, by following the Getting Started Guide, not covered by this manual

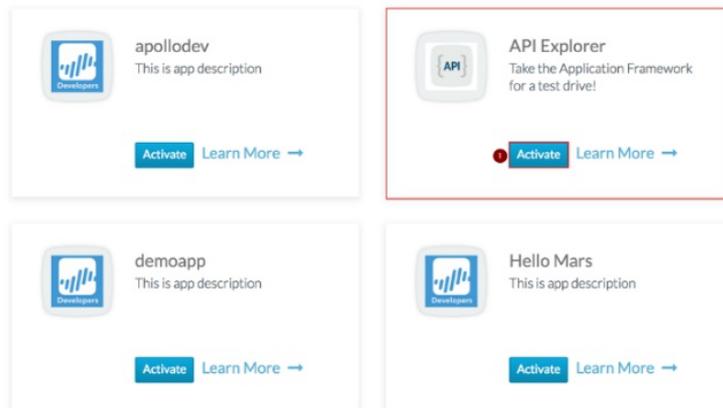
4. Review the configuration by clicking on the Settings icon in the top right corner:



Make sure that you have a Logging Service instance, and a Directory Sync instance.

5. Go back to the main page and navigate to the bottom of the Application Portal page, under **Partner Apps on the Application Framework**. Select the application (i.e. YourCompany - API Explorer) and click on the **Activate** icon:

Partner Apps on the Application Framework



Note: if you don't see your API Explorer App, reach out to your Palo Alto Networks technical contact for support.

6. Enter the required parameters, then select **'Agree and Submit'**:

✕

Activate API Explorer

License Type: `api_explorer`

* Company Name: 1

* Instance Name: 2

Description:

* Region: 2

* Logging Service: 3

If not all Logging Service instances appear, you may need to [activate purchased licenses](#).

* Directory Sync: 4

* Developer Name:

* Email Address:

* Company:

* Department:

* Company URL:

EULA: By clicking "Agree and Activate", you accept the terms of the [End User License Agreement](#).

6

7. At this point you should see the instance of your "API Explorer" App in the **"Your Palo Alto Networks Cloud Services Apps"** section of the App Portal:

Your Palo Alto Networks Cloud Services Apps

Technical Business Development ▾



Directory Sync



Logging Service



API Explorer



Activate New App

8. Click on your API Explorer App icon and you will be redirected to your API Explorer instance (the FQDN of your AWS API Explorer instance). Login as **admin** (the password is the one you set as part of the CloudFormation Template parameters, same as Firewall and Panorama):

Note: Make sure that you login on the API explorer App for the first time through link on the Cloud Services Portal. Do not login on the API Explorer by navigating to the FQDN directly with your browser, as some required tokens must be passed to the API Explorer by the Cloud Services Portal through the link.

9. At the first Login, the API explorer app will ask you to perform the Activation. Click on the **Activate** button:

⚠ FURTHER ACTIVATION STEPS REQUIRED ⚠

NOTICE: Some features of your API EXPLORER will have limited functionality until the activation steps are completed.

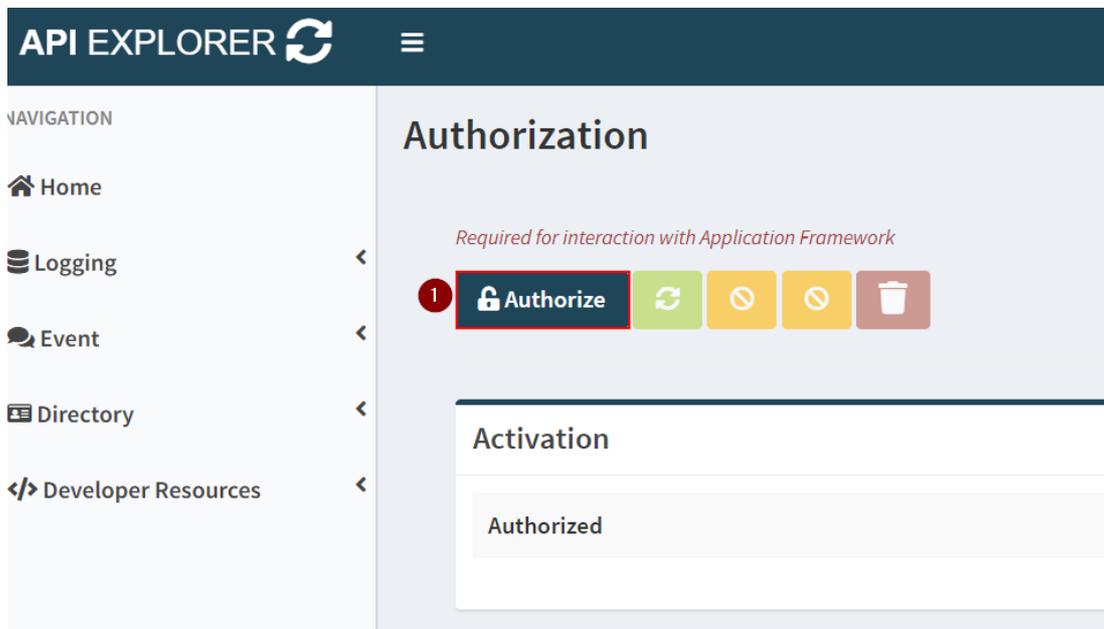
Activation Steps:

1. Click **Activate** button.
2. Click the **Authorize** button and provide the following to begin authorization:
 - Client ID
 - Client Secret
 - Redirect URI
 - Scope
3. When prompted, authenticate using your CSP credentials.
4. Complete and submit the "Request for Approval" form.

Note: If successful, your API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.

Cancel**1** **Activate**

10. In the Authorization page, click on "Authorize":



11. Insert the required parameters:

a. Client ID and Client Secret that you obtained from your

Palo Alto Networks technical contact

b. Redirect URI should be correspond to your API Explorer instance

with the /auth-callback route (i.e.
-<https://apiexplorer.lab.yourcompany.com/auth-callback> -
https://apiexplorer-stg4.lab.hhq.cloud/auth-callback in this
example)

c. Scope must be "logging-service:read", "event-service:read"

and "***directory-sync-service:read***". Do not select write scopes
at the moment.

12. Click on "Authorize":

API EXPLORER Authorization

Contact your Developer Relations representative if you are missing any of the required fields.

Client ID *

api_explorer_fv2 

Client Secret *

.....   

Redirect URI * /auth-callback

https://apiexplorer-stg4.lab.hhq.cloud/auth-callback 

Scope * (select one or more)

logging-service:read event-service:read directory-sync-service:read 

Note: If successful, API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.



13. The "Request for Approval" page on the Identity Provider will show up. Click on "Allow":

Request for Approval

APIExpFV-STG4 is requesting permission for the following:

- Read Logging Service
- Read Event Service
- Read Directory Sync Service

Consent info:

- APIExpFV-STG4: fvigo-stg4-test
- Logging Service: (no name)
- Directory Sync Service: DirSyncInstance1



APIExpFV-STG4

Take the Application Framework for a test drive!

14. If the authorization is successful, you should see the Tokens in the Authorization page, and the application should work:

Authorization

SUCCESS

Required for Interaction with Application Framework



Activation

Scope	logging-service:read event-service:read directory-sync-service:read
Instance ID	4623954708994114687
Client ID	api_explorer
Authorized	True

Tokens

Refresh-Token
Access-Token
Token-Type	bearer
Expires-At	Tuesday, April 3rd, 2018 1:03:49 PM

Congratulations: You can now use the functions of the API Explorer. For example, the "Query Explorer" from the left menu.

Make sure you look at the [Application-Framework-FAQs](#) for additional details.

Appendix A: Explanation of the CFT services and usage

Kali Linux VM

Used to generate exploits to trigger Threat events on NGFW

Access server directly with SSH private key with the **ec2-user** user:

```
# ssh -i paloalto.pem ec2-user@kali.lab.yourcompany.com
```

Run threats against web server:

```
# sudo uniscan -u http://10.0.0.100 -esqdbw
```

API Explorer VM

Runs the API Explorer application

Access the WebUI: <https://apiexplorer.lab.yourcompany.com>

You can also access directly with SSH private key with the **ec2-user** user:

```
# ssh -i paloalto.pem ec2-user@apiexplorer.lab.yourcompany.com
```

Public IP

Public IP of the NGFW eth1 interface :

- Use port 221 to access WEB VM through SSH (username is **ubuntu**)
- Use port 3389 to access Windows Domain controller through RDP

Next-Generation Firewall (NGFW)

Palo Alto Networks Next-Generation Firewall

Access directly with SSH private key with the **admin** user:

```
# ssh -i paloalto.pem admin@ngfw.lab.yourcompany.com
```

Or via the WebUI: <https://ngfw.lab.yourcompany.com>

Panorama

Palo Alto Networks Panorama

Access directly with SSH private key with the **admin** user:

```
# ssh -i paloalto.pem admin@panorama.lab.yourcompany.com
```

Or via the WebUI: <https://panorama.lab.yourcompany.com>

Ubuntu Web Server

Traffic generation VM and Web Server

Internal address that can be reached through NGFW public interface (see above)

A web crawler runs on it (for URL and traffic logs, etc)

Access server with SSH private key through firewall mapped port 221 with the **ubuntu** user:

```
# ssh -i paloalto.pem ubuntu@public.lab.yourcompany.com -p 221
```

Useful commands:

- `# crontab -l` (shows the command in the crontab to register IP-to-User mapping with the NGFW API every 15 minutes)
- `# /home/ubuntu/web-traffic-generator` (web traffic generator. It's started during the first boot but won't restart at VM reboot). Configuration is in `config.py`
- Restart the Web traffic Generator with the following command: `REQUESTS_CA_BUNDLE=/etc/ssl/certs/ca-certificates.crt nohup python /home/ubuntu/web-traffic-generator/gen.py 1>>/tmp/webgen.stdout 2>>/tmp/webgen.stderr &`

Domain Controller:

Windows 2012R2 Domain Controller

Internal IP that can be reached via RDP through NGFW public interface (see above)

Login as yourdomain\youruser (default `PANWDOMAIN\paloalto`), or as `user1`, `user2` or `user3`

The password is the one you configured in the CFT.

You can install the Directory Sync Service agent on this VM if you want to use it.

Appendix B: Default hostname to IP and VM Mapping

Public Hostname	Internal IP	EIP assigned?	VM
kali	10.0.0.88	Y	Kali Linux VM
apiexplorer	10.0.0.55	Y	API Explorer VM
public	10.0.0.100	Y	NGFW Public Interface
ngfw	10.0.0.99	Y	NGFW Management Interface
panorama	10.0.0.20	Y	Panorama Management Interface
N/A	10.0.1.101	N	Ubuntu Web Server VM
N/A	10.0.1.20	N	Windows Domain Controller VM

Appendix C: Sample log outputs in the monitor tab

Traffic

Generate Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	Device SN	Device Name
03/26 15:16:59	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	11.9k	0070550000401...	sample-ct-fw
03/26 15:16:58	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	412	0070550000401...	sample-ct-fw
03/26 15:16:58	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	11.3k	0070550000401...	sample-ct-fw
03/26 15:16:57	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	406	0070550000401...	sample-ct-fw
03/26 15:16:56	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	14.3k	0070550000401...	sample-ct-fw
03/26 15:16:55	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	642	0070550000401...	sample-ct-fw
03/26 15:16:54	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	23.210.101.240	443	web-browsing	allow	Allow Outbound Browsing	tcp-fin	13.5k	0070550000401...	sample-ct-fw
03/26 15:16:54	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	572	0070550000401...	sample-ct-fw
03/26 15:16:52	end	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\user1	10.0.0.2	53	dns	allow	Allow all outbound	aged-out	410	0070550000401...	sample-ct-fw

Threat

Receive Time	Type	Name	From Zone	To Zone	Source address	Source User	Destination address	To Port	Application	Action	Severity	File Name	URL
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:23	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	Joomla Visites Component Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	critical	10.0.0.100/admi...	
03/26 15:37:22	vulnerability	PHP Remote File Include Vulnerability	L3-Untrust	L3-Trust	10.0.0.88		10.0.0.100	80	web-browsing	reset-both	medium	10.0.0.100/zoo...	

Note: to see these you should generate some threats with Kali Linux, as explained in Appendix A.

URL Filtering

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device Panorama

Context: Panorama Device Group: All

Generate Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action	Headers Inserted	Device SN	Device Name
03/26 15:17:22	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:20	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:19	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:18	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:17	news	www.wired.com...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.190.194	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:17	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:17	society	www.condenast....	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	151.101.40.239	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:15	news	digg.com/	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	184.169.136.19	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:13	shopping	www.craigslist.o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:13	shopping	www.craigslist.o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-cft-fw
03/26 15:17:11	shopping	www.craigslist.o...	L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	208.82.238.17	web-browsing	allow		0070550000401...	sample-cft-fw

Wildfire Submissions

paloalto NETWORKS

Dashboard ACC Monitor Policies Objects Network Device Panorama

Context: Panorama Device Group: All

Generate Time	File Name	URL	Source Zone	Destination Zone	Source address	Source User	Destination address	Dest. Port	Application	Rule	Verdict	Action	Severity
03/26 15:16:26	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:12:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:10:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:08:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:06:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:04:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high
03/26 15:00:27	wildfire-test-pe-f...		L3-Trust	L3-Untrust	10.0.1.101	panwdomain\us...	52.8.161.117	80	web-browsing	Allow Outbound Browsing	malicious	allow	high

Application-Framework-FAQs

Application Framework Partner Beta Program - Frequently Asked Questions

Doc Revision: 2018-05-01-07:41:39 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/Application-Framework-FAQs>

What is the Application Framework Partner Beta Program?

- As Ignite 2018 draws near, Palo Alto Networks is providing partners preview access to the Application Framework to work on their specific integrations.

Where can I go to find/acquire X?

- API reference and Getting-Started documentation (ask your Palo Alto Networks representative to get access to the shared folder if you cannot reach it)
 - <https://paloaltonetworks.app.box.com/folder/46344564211>
- Authorization codes/serials/licenses
 - Please contact your Palo Alto Networks representative.
- pancloud SDK
 - <https://github.com/PaloAltoNetworks/pancloud>
- API Explorer (sample app)
 - <https://github.com/PaloAltoNetworks/apiexplorer>
- Lab Deployment Documentation
 - <https://github.com/PaloAltoNetworks/appframeworklab/wiki>

How can I report an issue/bug with X?

- APIs
 - Please contact your Palo Alto Networks representative.
- pancloud SDK
 - Create a GitHub issue following the submission guidelines published in the repo.
 - Gitter: <https://gitter.im/PaloAltoNetworks/pancloud>
 - Contact your Palo Alto Networks representative.
- API explorer
 - Create a GitHub issue following the submission guidelines published in the repo.
 - Gitter: <https://gitter.im/PaloAltoNetworks/pancloud>
 - Contact your Palo Alto Networks representative.

How can I deploy X?

- API Explorer
 - <https://paloaltonetworks.box.com/s/s0hc5umuxsumjb6t3vcwtknzh9isbkcf>
- Developer Environment on AWS
 - <https://paloaltonetworks.box.com/s/s0hc5umuxsumjb6t3vcwtknzh9isbkcf>

How can I register my own app?

- Work with your Palo Alto Networks representative to generate the required manifest.json file.

Where do I find my client_id, client_secret, etc., needed for authorization/OAuth?

- Contact your Palo Alto Networks representative.

How are we tracking customers who click from the app portal to the 3rd-party app.

- Although the Cloud Services Portal logs the username of the person that "Activates" a 3rd-party app, it will be up to the vendor/partner to record tracking/accounting data when a user "Signs Up" or "Signs In" for/to the 3rd-party app from the CSP.

How does a 3rd-party partner get paid for app usage?

- This has not been defined yet.

Can we develop with dummy data/sample logs in Logging Service?

- Yes, we have the option to stream any log type to any Logging Service instance (using jlogger). The sample logs are derived from our Palo Alto Networks demo labs and do not contain sensitive data.
- However, unless the circumstances require it, it is recommended for 3rd-party developers to deploy or configure a lab suitable for generating logs. We provide an AWS CloudFormation Template (CFT) that can be used for the purpose.

What region is the Logging Service data center physically located?

- North America.

Are Logging Service column names supported in SQL filter SELECT expressions?

- Please refer to the official API documentation for supported features. Undocumented features are not supported and subject to change without notice. Developers should avoid using undocumented features.
- Column names in SELECT expressions are not supported but may return valid results. For example, to return only the source and destination IP address columns, include those column name in the SELECT expression, e.g:
 - `SELECT src,dst FROM panw.traffic`
 - For names that conflict with SQL keywords, prepend the underscore character to the field name, e.g:
 - `SELECT _from FROM panw.traffic`

How often can the Event Service API be polled? Why doesn't Event Service API push data?

- Push will not be available in 1.0. You should poll as often as needed by your app.

Why does the Event Service poll return an empty list even when logs are present?

- There are subtle but significant differences in the Event Service and Logging Service SQL filters that can produce unexpected results.
- For the Event Service, the table reference must be enclosed in back quotes. For example:
 - `{"filters":{"panw.traffic":{"SELECT * FROM panw.traffic"}}` will return no results.
 - `{"filters":{"panw.traffic":{"SELECT * FROM `panw.traffic`"}}` works as expected.

Where do I get the "channelID" for the Event Service?

- Use the static value `"EventFilter"`

What is the duration of the OAuth Authorization Token?

- 1 hour (3600 seconds). You can use the `refresh token` to generate a new `authorization token`

How can the app framework protect against real time threats?

- Please continue to rely on a properly configured NGFW, Traps, WildFire, for protection against real-time threats.
- Retroactive protection is possible using a combination of MineMeld,

EDLs, or a 3rd-party supplied on-premise agent capable of updating NGFW firewall security policy.

Why I cannot generate the OTP on Customer Support Portal?

- Please make sure that your account has **SuperUser**, **Logging Service** and **Directory Sync Service** permissions on Cloud Services Portal

Logging Service doesn't work (I can't see logs on Panorama):

- Check that you have the proper licenses registered in Panorama (navigate to "Panorama" - "Licenses" and make sure you have both "Logging Service" licenses and Support (can be either "Standard" or "Premium")):

The screenshot shows the Palo Alto Networks Panorama configuration interface. The left sidebar contains a navigation tree with 'Licenses' highlighted. The main content area displays details for four licenses:

- AutoFocus Device License:** Date Issued: March 29, 2018; Date Expires: October 27, 2020; Description: AutoFocus Device License.
- Device Management License:** Date Issued: March 29, 2018; Date Expires: Never; Description: VM Panorama license to manage up to 25 devices.
- Premium:** Date Issued: March 29, 2018; Date Expires: March 29, 2019; Description: 24 x 7 phone support; advanced replacement hardware service.
- Logging Service:** Date Issued: March 29, 2018; Date Expires: March 29, 2019; Description: Cloud Service; Log Storage TB: 1.

- Check that you have the proper licenses registered in the Firewall (navigate to "Panorama" - "Device Deployment" - "Licenses" and make sure you have "Support", "URL", "Threat Prevention", "WildFire", "VM-Series Capacity" and "Logging Service" licenses enabled:

The screenshot shows the Palo Alto Networks Panorama configuration interface. The left sidebar contains a navigation tree with 'Licenses' highlighted. The main content area displays a table of licenses for a device named 'sample-cft-fw'.

Device	Virtual System	Threat Prevention	URL	Support	GlobalProtect Gateway	GlobalProtect Portal	WildFire	VM-Series Capacity	AutoFocus	Logging Service	Decryption Port Mirror	Decryption Broker
sample-cft-fw		Expires: 4/2/2019	PaloAlto Networks Expires: 4/2/2019	Expires: 4/2/2019	Expires: 4/2/2019		Expires: 4/2/2019			Expires: 5/9/2028		

- On the Panorama CLI, run the following commands and provide the output to your Palo Alto Networks Representative:
 - `show plugins cloud_services logging-service info`
 - `request plugins cloud_services logging-service status`
 - `show system state | match lcaas`
 - `show system state | match cust`
- On the Firewall CLI, run the command "`show logging-status`". The output should be like the one in following picture:

```
admin@sample-cft-fw> show logging-status
-----
Type          Last Log Created      Last Log Fwdd        Last Seq Num Fwdd    Last Seq Num Ackd    Total Logs Fwdd
-----
> CMS 0
  Not Sending to CMS 0
> CMS 1
  Not Sending to CMS 1
>Log Collection Service
'Log Collection log forwarding agent' is active and connected to 74.217.90.118
config 2018/04/02 00:21:17 2018/04/02 16:01:19      11      11      1
system 2018/04/02 18:57:26 2018/04/02 18:57:26    15026   15026   136
threat 2018/04/02 18:57:43 2018/04/02 18:57:46   204109  204101  2724
traffic 2018/04/02 18:57:41 2018/04/02 18:57:46  409905  409899  5277
hipmatch Not Available      Not Available         0        0        0
gtp-tunnel Not Available      Not Available         0        0        0
userid 2018/04/02 18:45:10 2018/04/02 18:45:26    405     405     12
auth Not Available      Not Available         0        0        0
sctp Not Available      Not Available         0        0        0
```

- Other useful Firewall CLI commands (provide the output to your Palo Alto Networks Representative):

- `request logging-service-forwarding certificate info`
- `request logging-service-forwarding status`
- `request logging-service-forwarding customerinfo show`
- `show system state | match cust`
- `show system state | match lcaas`
- `less mp-log lcaas_agent.log`
- `tail mp-log ms.log`
- `debug log-receiver rawlog_fwd_dpi stats global show verbose`
- **Restart Log Receiver on Firewall:**
- `debug software restart process log-receiver`

API-Curl-Examples

Palo Alto Networks Application Framework API Explorer Curl Examples

This document describes some examples on how to interact with the Application Framework API using *curl*.

Doc Revision: 2018-05-01-07:41:39 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/API-Curl-Examples>

Logging Service

Create a query

The following example shows how to run a query for 10 logs from the *panw.traffic* table. Note that the **AUTH_TOKEN** must be provided. *startTime* and *endTime* are used to determine the time window during which logs are searched.

```
curl -X POST -H "Content-Type: application/json" -H "Authorization: Bearer AUTH_TOKEN" -d '{"startTime": 0, "endTime": 1609459200, "maxWaitTime": 0, "query": "SELECT * FROM panw.traffic LIMIT 10"}' "https://api-gw-stg4.us.paloaltonetworks.com/logging-service/v1/queries"
```

The response will look similar to:

```
{ "queryId": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "sequenceNo": 0, "queryStatus": "RUNNING", "clientParameters": {}, "result": { "esResult": null, "esQuery": { "table": [ "panw.traffic" ], "query": { "aggregations": {}, "size": 10, "selections": {}, "params": {} } } }
```

You can extract the *queryId* (*a8c81c89-0a2e-419c-b771-9283a2722e9a*) and use it to collect results.

Get Poll results

To poll for a query result, use the following command (specifying the right *queryId*):

```
curl -X GET -H "Content-Type: application/json" -H "Authorization: Bearer AUTH_TOKEN" "https://api-gw-stg4.us.paloaltonetworks.com/logging-service/v1/queries/a8c81c89-0a2e-419c-b771-9283a2722e9a/0"
```

The response will look similar to:

```
{ "queryId": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "sequenceNo": 0, "queryStatus": "JOB_FINISHED", "clientParameters": {}, "result": { "esResult": { "took": 335, "hits": { "total": 6489137, "maxScore": 2, "hits": [ [ LOGS_HERE ] ], "id": "a8c81c89-0a2e-419c-b771-9283a2722e9a", "from": 0, "size": 10, "completed": true, "state": "COMPLETED", "timed_out": false }, "esQuery": { "table": [ "panw.traffic" ], "query": { "aggregations": {}, "size": 10, "selections": {}, "params": {} } } }
```

If the status is still *RUNNING* wait until it completes and try again. If the status is *FINISHED* there will be other results in additional sequences. If the status is *JOB_FINISHED* it is the last result set. Please look at the documentation for more details.

Delete Query

To delete a query, use the following command (specifying the right *queryId*):

```
curl -X DELETE -H "Content-Type: application/json" -H "Authorization: Bearer YOUR_TOKEN" "https://api-gw-stg4.us.paloaltonetworks.com/logging-service/v1/queries/a8c81c89-0a2e-419c-b771-9283a2722e9a"
```

A successful response will be:

```
{ "success": true }
```

API-Explorer-Lab

Palo Alto Networks Application Framework API Explorer Deployment via AWS CloudFormation

This document describes how to automatically set up an Application Framework API Explorer instance on Amazon Web Services. It is meant for Palo Alto Networks Partners that need a quick way to start developing for Application Framework.

It also provides instructions on how to pair the API Explorer application with Application Framework.

Doc Revision: 2018-05-01-07:41:39 (UTC)

Please make sure you always download the latest revision of this document and the required files:

- Wiki home: <https://github.com/PaloAltoNetworks/appframeworklab/wiki>
- This document: <https://github.com/PaloAltoNetworks/appframeworklab/wiki/API-Explorer-Lab>
- Documentation PDF: <https://github.com/PaloAltoNetworks/appframeworklab/blob/master/pdf/LabGuide.pdf>
- API Explorer JSON file: <https://raw.githubusercontent.com/PaloAltoNetworks/appframeworklab/master/ctf/apiexplorer-ctf.json>

Prerequisites

This lab environment requires the following:

- A valid AWS Account
- A Palo Alto Networks Enabled Network Instance
- AWS Region with 1 available Elastic IP
- (Not mandatory but highly recommended) A second or third level domain configured in AWS Route53 (i.e. lab.yourcompany.com with NS records pointing to AWS Route 53 DNS Servers): ask your Palo Alto Networks representative for more details.

Security Hardening Considerations

This environment is meant for development use only, it's not security hardened for production. Specifically, the following security considerations should be known:

- Administrative password is provided as an environment variable for the installation scripts on the API Explorer and Ubuntu Web Server VMs, so it may be visible in some of the log files (i.e. /tmp/panorama_setup.log on the API Explorer VM)

To perform manual hardening of the environment, the following post-deployment steps are suggested:

- Manually change all the passwords

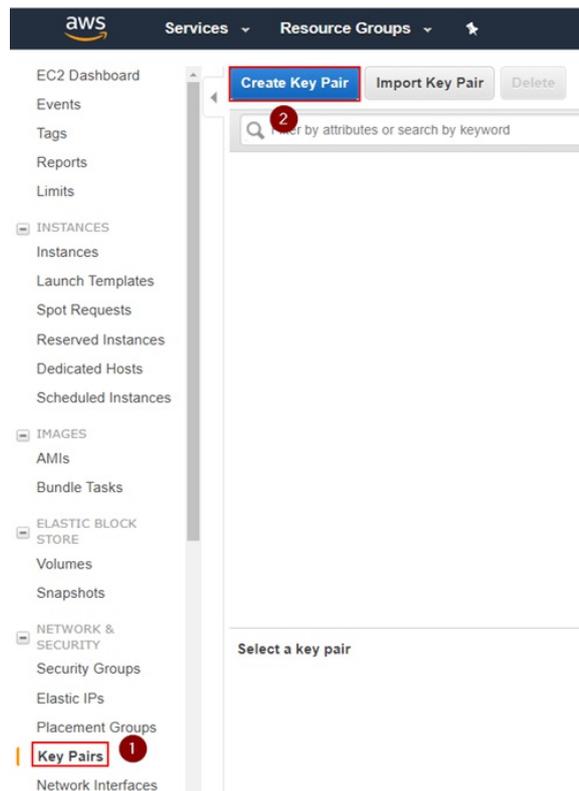
This document is not meant to provide instructions for the above steps.

AWS Configuration

This section describes the configuration of the AWS required components to deploy the lab components. You'll need a KeyPair and (optional) a Route53 Hosted Zone. Y

Key Pair Creation

1. Navigate to your selected region (i.e. us-east-1), select the EC2 service and under "Network & Security" select "Key Pairs" and click on "Create Key Pair":



2. Insert a keypair name and click on "Create". In the example, we use "paloalto". This will create a "paloalto.pem" private key and the AWS Web UI will prompt you to download it.



3. Download the Private Key to your local machine. The file name of this example will be `paloalto.pem`, but you can choose an arbitrary name. Y

Route53 Zone Configuration

The CloudFormation Template deploys a VM (API Explorer) and AWS can automatically associate DNS names to the Elastic IPs that are used by EC2. To do that, you need a Route53 public Hosted Zone configured in your AWS environment. This step is optional: you can just connect to the VMs via their Elastic IP addresses, or manually configure your DNS entries at a later stage if you're not using Route53. However, this step is highly recommended.

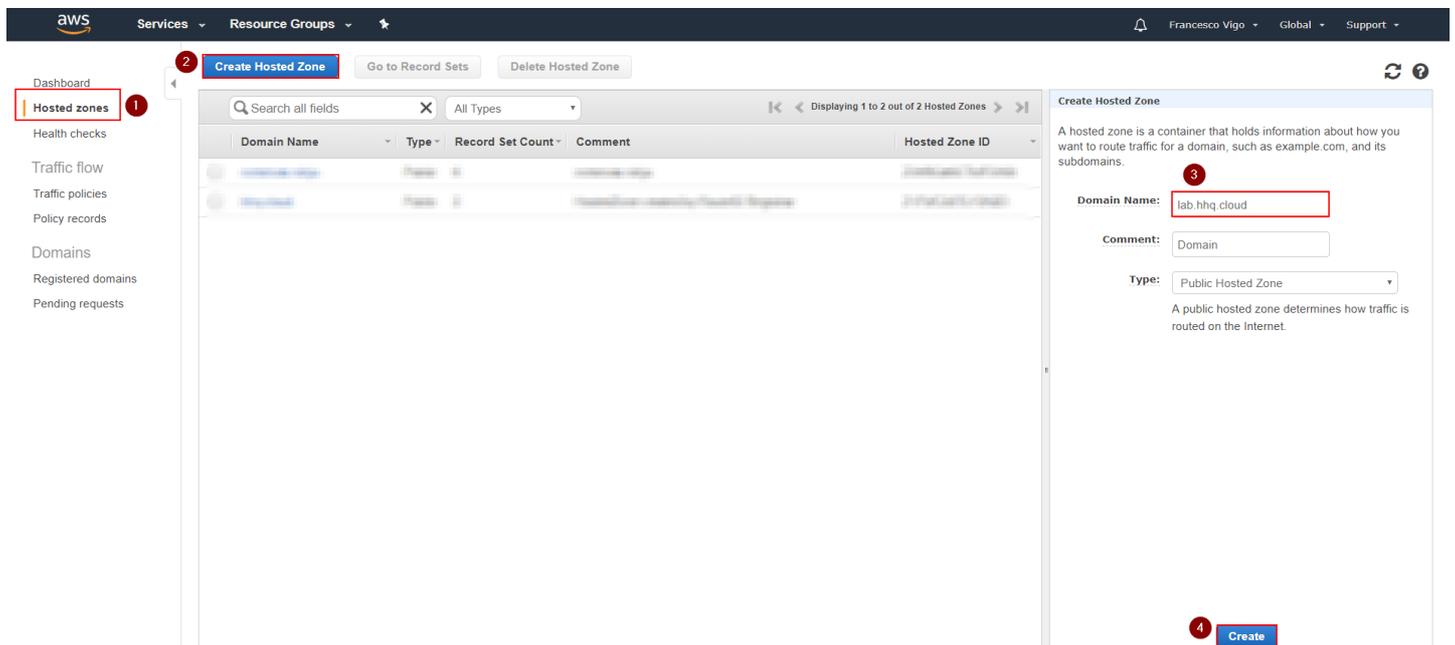
The public DNS zone you use can either be an existing second-level domain (i.e. `yourcompanylab.com`), or a third-level domain (`lab.yourcompany.com`). It must be publicly resolvable, so you need to be the registered owner of the domain. As an option, you can register a new domain directly through the AWS console and add it automatically in Route53.

If you don't have the opportunity to use a second or third level domain in Route53, ask your Palo Alto Networks contact for support to get a fourth level domain delegated to your Route53 DNS Servers.

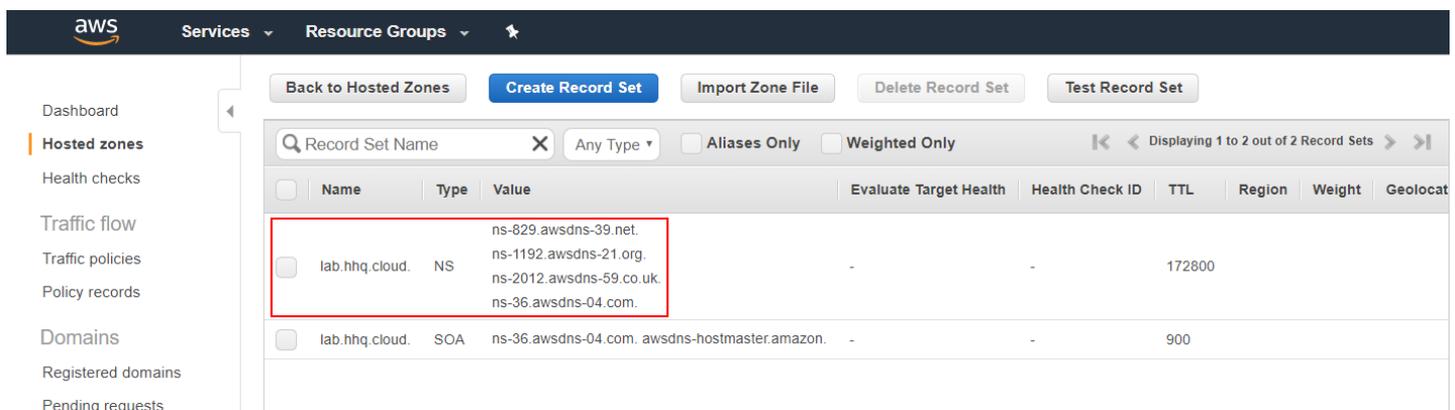
Note: the CFT can automate the creation and registration of a valid SSL certificate that corresponds to the FQDN of your API Explorer instance (this way the browser won't provide warnings when you connect to it), through a free service called "Let's Encrypt" (<https://letsencrypt.org>). If you want to automatically generate the Let's Encrypt certificate through the CFT, you must have the Route53 configuration enabled, otherwise the process will fail. Hence, if you don't want to use Route53 for this step, the API Explorer certificate must be a self-signed one. The CFT parameters provide options to disable the configuration of Route53 and Let's Encrypt.

To configure a Hosted zone in AWS Route 53, proceed through the following steps:

1. Navigate to AWS "Route53", go to "Hosted zones" and click on "Create Hosted Zone". Enter the domain name: it must be a public domain name (second or third level) where you have permissions configure name servers for (i.e. `yourcompanylab.com` or `lab.yourcompany.com`). The type must be "Public Hosted Zone." Then click on **Create**:



2. Look at the AWS Name Servers listed in the NS record and configure your Domain Hosting provider platform to use them for the selected domain:



In this example we are using the third-level domain `lab.hhq.cloud`.

Note: if you registered the domain through AWS, you don't need any additional configuration as it will be automatically registered in Route

53. If you're using a different domain hosting platform (i.e. GoDaddy, NameCheap, etc), the configuration on how to configure your domain to use AWS Route53 DNS servers will be different depending on your provider.

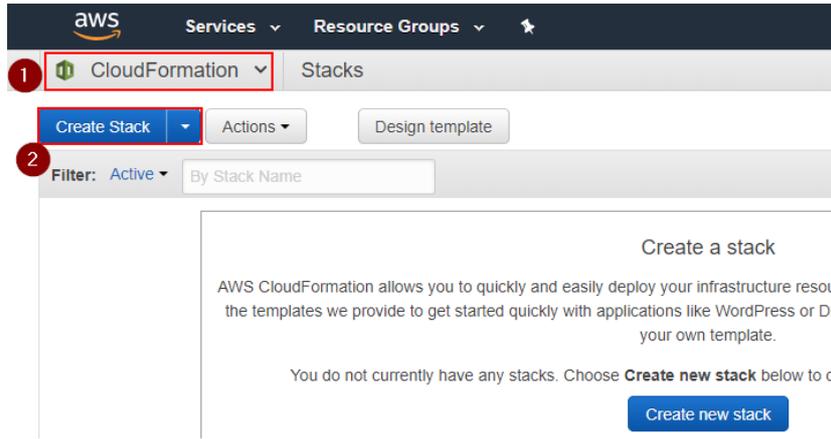
If you're being helped by Palo Alto Networks to use a fourth level domain, please provide the Name Servers to your contact.

Deploy the CloudFormation Template

You can now deploy the AWS CloudFormation Template (CFT) to create the lab environment. Before starting, make sure that you have one Elastic IP (EIP) available in the region you want to deploy the CFT (by default AWS limits EIPs to 5 per region per account).

Proceed with the following steps:

1. Navigate to "AWS CloudFormation" and select "Create Stack":



2. Select "Upload a template to Amazon S3", and upload the template JSON file provided by Palo Alto Networks (apiexplorer-cft.json in the example), then click on Next:

Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. [Learn more.](#)

Design template

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. [Learn more.](#)

Select a sample template

Upload a template to Amazon S3

Choose File apiexplorer-cft.json

Specify an Amazon S3 template URL

Cancel

Next

3. Insert the required parameters:

- **Stack name:** an arbitrary name for this deployment (i.e. PartnerLab1)
- **Admin Password:** an arbitrary password that will be used for the API Explorer application admin user.
- **EC2 VMs Key Name:** from the drop down menu, select the KeyPair that you want to use for the non-Palo Alto Networks VMs (Kali Linux, API Explorer VM, Ubuntu VM). It can be the KeyPair that you previously created in EC2, or a different one of your choice.
- **DNS Domain Name:** Insert the domain name zone that you have configured on Route53. If you don't have it, add a domain name and select "false" under both the "Configure Route53" AND the "Create API Explorer LetsEncrypt Cert" fields in the Advanced Configuration section. In the example we use the **hhq.cloud** domain.
- **LetsEncrypt Email:** Insert your (valid) email address that will be used to request a Let's Encrypt SSL certificate for the API Explorer.

Leave the other parameters to the default values unless you are a power user and you know what you're doing.

The following screenshot shows an example configuration:

Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more](#).

Stack name

Parameters

Basic Configuration - REQUIRED

Admin Password

Password for API Explorer: Must be at least 8 characters containing letters, numbers and symbols

EC2 VM Key Name

Name of an existing EC2 KeyPair to enable SSH access to the VM

DNS Domain Name

DNS Domain Name or Route53 Hosted Zone Name (i.e. panwlab.mycompany.com)

LetsEncryptEmail

Email address to provide to Letsencrypt for API Explorer SSL certificate generation (i.e. user@mycompany.com)

4. Click on "Next" twice.

5. In the Review page, Click on "Create":

[Quick Create Stack](#) (Create stacks similar to this one, with most details auto-populated)

Cancel Previous Create

6. Sit down and relax, the whole process will take a few minutes to complete:

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_IN_PROGRE...	Palo Alto Networks Application Framework ...

7. The deployment will show **CREATE_COMPLETE** once everything is done:

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_COMPLETE	Palo Alto Networks Application Framework ...

8. Select the template and click on the **Outputs** tab of the to view the deployment information (IP addresses and FQDNs) of the lab:

Filter: Active ▾ By Stack Name Showing 3 stacks

Stack Name	Created Time	Status	Description
<input checked="" type="checkbox"/> PartnerLab1	2018-04-09 08:37:53 UTC-0700	CREATE_COMPLETE	Palo Alto Networks Application Framework ...

Key	Value	Description	Export Name
APIExplorerAppURL	https://apiexplorer.hhq.cloud	API Explorer URL	

###AT THIS STAGE YOU SHOULD STOP AND MAKE SURE THAT THE CLOUD ENVIRONMENT IS READY. PLEASE REACH OUT TO YOUR PALO ALTO NETWORKS TECHNICAL CONTACT FOR THIS.

API Explorer App Activation Process

This section describes how to Activate the API Explorer application and start interacting with the APIs.

Note: this section requires the manifest file activation part to be already configured, otherwise you will not see your API Explorer application in the App Portal. You will also be provided a **Client ID** and a **Client Secret** by your Palo Alto Networks contact.

To activate the API Explorer, follow this process:

1. Navigate to the App Portal beta environment: <https://apps-stg4.app-portal-beta.us.paloaltonetworks.com> and Sign in with your Customer Support Portal credentials:



2. Activate an instance of Directory Sync Service by clicking on the **Activate** button in the **Directory Sync** tile:

Your Palo Alto Networks Cloud Services Apps



If you have activated an app and do not see it above, you might not have the roles required to access the app. Please go to the Customer Support Portal to obtain the roles from your organization's administrator.

More Available Palo Alto Networks Apps



Directory Sync
Allow Palo Alto Networks Cloud Services to access your organization's directory

1 Activate [Learn More →](#)



Magnifier
Discover malicious activity and stop attackers and malware operating inside your network

[Learn More →](#)



Traps
Advanced, multi-method malware prevention that protects users and endpoints

[Learn More →](#)

3. Enter an arbitrary **Instance Name** and select **Americas** as **Region**, then click on **OK**:

Directory Sync ✕

* Instance Name: 1

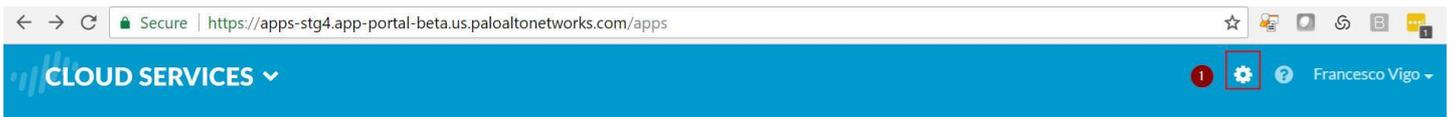
Description:

* Region: 2

3

Note: You don't need to actually register an Active Directory agent to it if you don't need to interact with AD data to build your integration. Or you can deploy the Directory Sync Agent on the windows Domain Controller, by following the Getting Started Guide, not covered by this manual

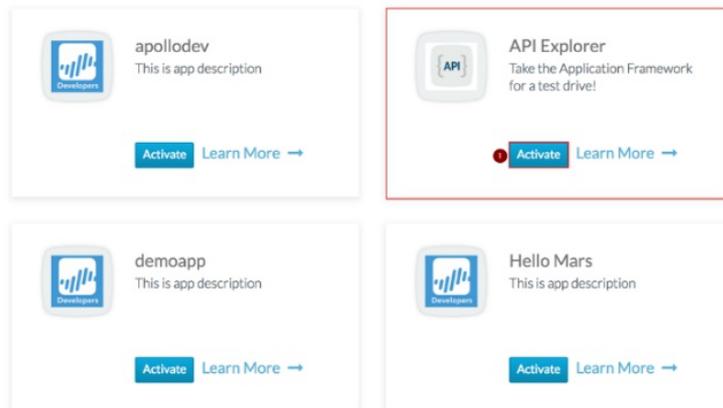
4. Review the configuration by clicking on the Settings icon in the top right corner:



Make sure that you have a Logging Service instance, and a Directory Sync instance.

5. Go back to the main page and navigate to the bottom of the Application Portal page, under **Partner Apps on the Application Framework**. Select the application (i.e. YourCompany - API Explorer) and click on the **Activate** icon:

Partner Apps on the Application Framework



Note: if you don't see your API Explorer App, reach out to your Palo Alto Networks technical contact for support.

6. Enter the required parameters, then select **'Agree and Submit'**:

✕

Activate API Explorer

License Type: `api_explorer`

* Company Name: 1

* Instance Name: 2

Description:

* Region: 2

* Logging Service: 3

If not all Logging Service instances appear, you may need to [activate purchased licenses](#).

* Directory Sync: 4

* Developer Name:

* Email Address:

* Company: 5

* Department:

* Company URL:

EULA: By clicking "Agree and Activate", you accept the terms of the [End User License Agreement](#).

6

7. At this point you should see the instance of your "API Explorer" App in the **"Your Palo Alto Networks Cloud Services Apps"** section of the App Portal:

Your Palo Alto Networks Cloud Services Apps

Technical Business Development ▾



Directory Sync



Logging Service



API Explorer



Activate New App

8. Click on your API Explorer App icon and you will be redirected to your API Explorer instance (the FQDN of your AWS API Explorer instance). Login as **admin** (the password is the one you set as part of the CloudFormation Template parameters, same as Firewall and Panorama):

Note: Make sure that you login on the API explorer App for the first time through link on the Cloud Services Portal. Do not login on the API Explorer by navigating to the FQDN directly with your browser, as some required tokens must be passed to the API Explorer by the Cloud Services Portal through the link.

9. At the first Login, the API explorer app will ask you to perform the Activation. Click on the **Activate** button:

⚠ FURTHER ACTIVATION STEPS REQUIRED ⚠

NOTICE: Some features of your API EXPLORER will have limited functionality until the activation steps are completed.

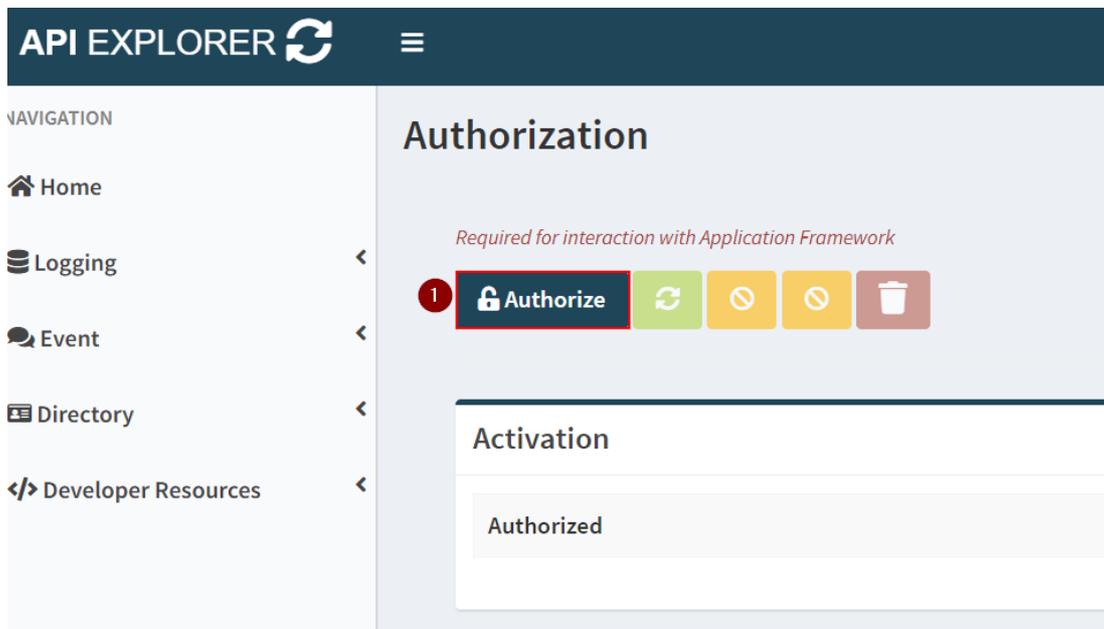
Activation Steps:

1. Click **Activate** button.
2. Click the **Authorize** button and provide the following to begin authorization:
 - Client ID
 - Client Secret
 - Redirect URI
 - Scope
3. When prompted, authenticate using your CSP credentials.
4. Complete and submit the "Request for Approval" form.

Note: If successful, your API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.

Cancel **1** **Activate**

10. In the Authorization page, click on "Authorize":



11. Insert the required parameters:

a. **Client ID** and **Client Secret** that you obtained from your

Palo Alto Networks technical contact

b. Redirect URI should be correspond to your API Explorer instance

with the /auth-callback route (i.e.
-<https://apiexplorer.lab.yourcompany.com/auth-callback> -
https://apiexplorer-stg4.lab.hhq.cloud/auth-callback in this
example)

c. Scope must be "**logging-service:read**", "**event-service:read**"

and *****directory-sync-service:read***** . Do not select **write** scopes
at the moment.

12. Click on "Authorize":

API EXPLORER Authorization

Contact your Developer Relations representative if you are missing any of the required fields.

Client ID *

api_explorer_fv2 

Client Secret *

.....   

Redirect URI * /auth-callback

https://apiexplorer-stg4.lab.hhq.cloud/auth-callback 

Scope * (select one or more)

logging-service:read event-service:read directory-sync-service:read 

Note: If successful, API EXPLORER will receive tokens necessary for interacting with your Logging, Event and Directory-Sync instances.



13. The "Request for Approval" page on the Identity Provider will show up. Click on "Allow":

Request for Approval

APIExpFV-STG4 is requesting permission for the following:

- Read Logging Service
- Read Event Service
- Read Directory Sync Service

Consent info:

- APIExpFV-STG4: fvigo-stg4-test
- Logging Service: (no name)
- Directory Sync Service: DirSyncInstance1

{ API }

APIExpFV-STG4

Take the Application Framework for a test drive!

14. If the authorization is successful, you should see the Tokens in the Authorization page, and the application should work:

Authorization

SUCCESS

Required for Interaction with Application Framework

Authorize   

Activation	
Scope	logging-service:read event-service:read directory-sync-service:read
Instance ID	4623954708994114687
Client ID	api_explorer
Authorized	True

Tokens	
Refresh-Token 
Access-Token 
Token-Type	bearer
Expires-At	Tuesday, April 3rd, 2018 1:03:49 PM

Congratulations: You can now use the functions of the API Explorer. For example, the "Query Explorer" from the left menu.

Appendix A: Explanation of the CFT services and usage

API Explorer VM

Runs the API Explorer application

Access the WebUI: <https://apiexplorer.lab.yourcompany.com>

You can also access directly with SSH private key with the `ec2-user` user:

```
# ssh -i paloalto.pem ec2-user@apiexplorer.lab.yourcompany.com
```

Appendix B: Default hostname to IP and VM Mapping

Public Hostname	Internal IP	EIP assigned?	VM
apiexplorer	10.0.0.55	Y	API Explorer VM