Palo Alto Networks Application Framework - Lab Guide

Copyright (C) 2018 - Palo Alto Networks, Inc.

Table of contents

Palo-Alto-Networks-Application-Framework-Lab.md

Palo-Alto-Networks-Application-Framework-Lab.md

Palo Alto Networks Application Framework 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's 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: 2018-04-09-01:06:47

Prerequisites

This lab environment requires the following:

- 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) 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.

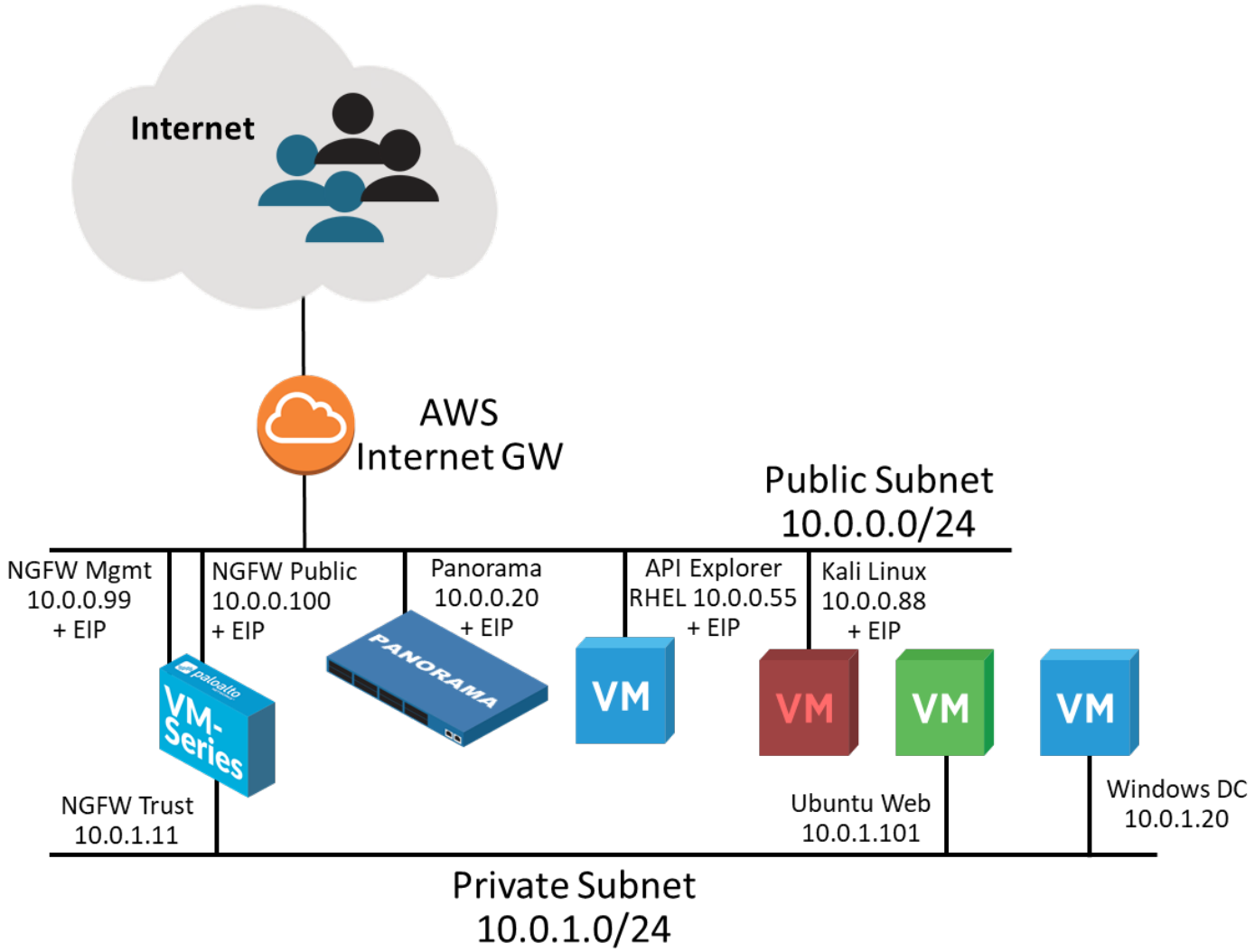
Lab Topology and features

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 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 221** 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 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)
- 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:

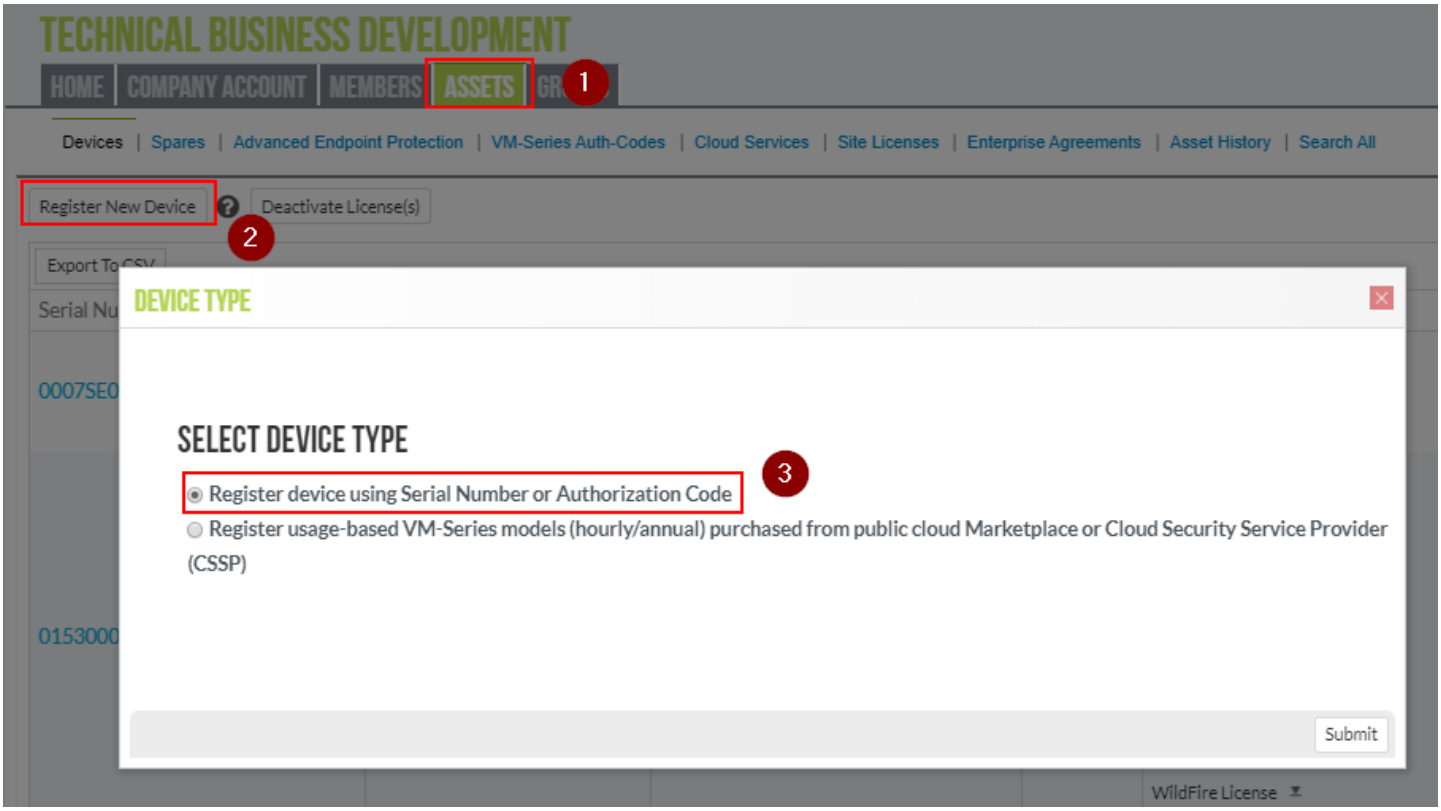
- Manually change all the passwords
- Replace the SSH key for authentication on NGFW and Panorama for admin users
- Disable Password based authentication on API Explorer and Ubuntu Web Server VMs
- Re-enable Password complexity on Domain Controller
- Replace the Decryption SSL certificate on NGFW, and import it on both Ubuntu Web Server VMs and Domain Controller

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

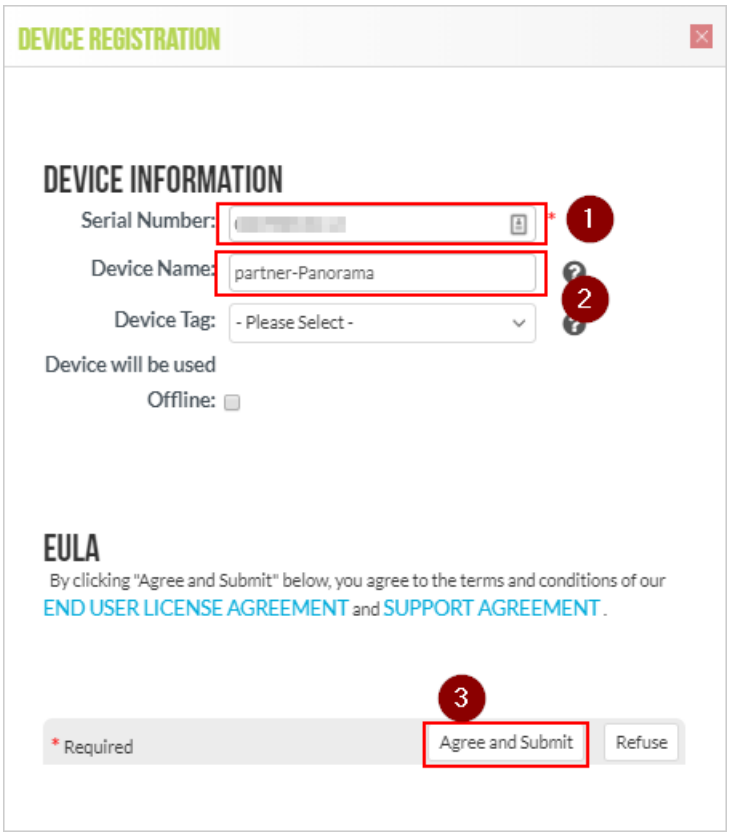
Palo Alto Networks Customer Support Portal Configuration

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

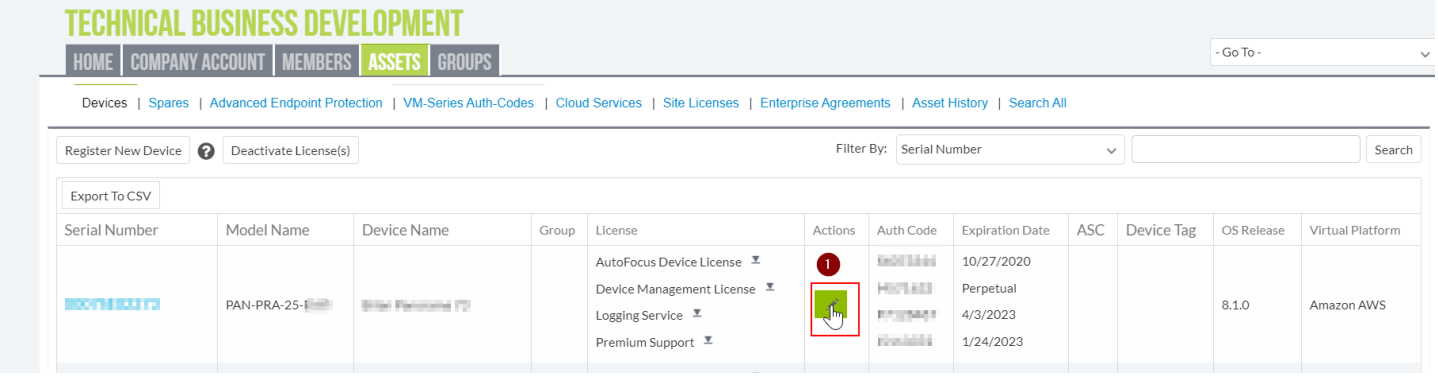
1. Login to *support.paloaltonetworks.com* using your CSP (Customer Support Portal) account
2. Navigate to "**Assets**" and click on "**Register New Device**", then select "**Register device using Serial Number or Authorization Code**", then "**Submit**""



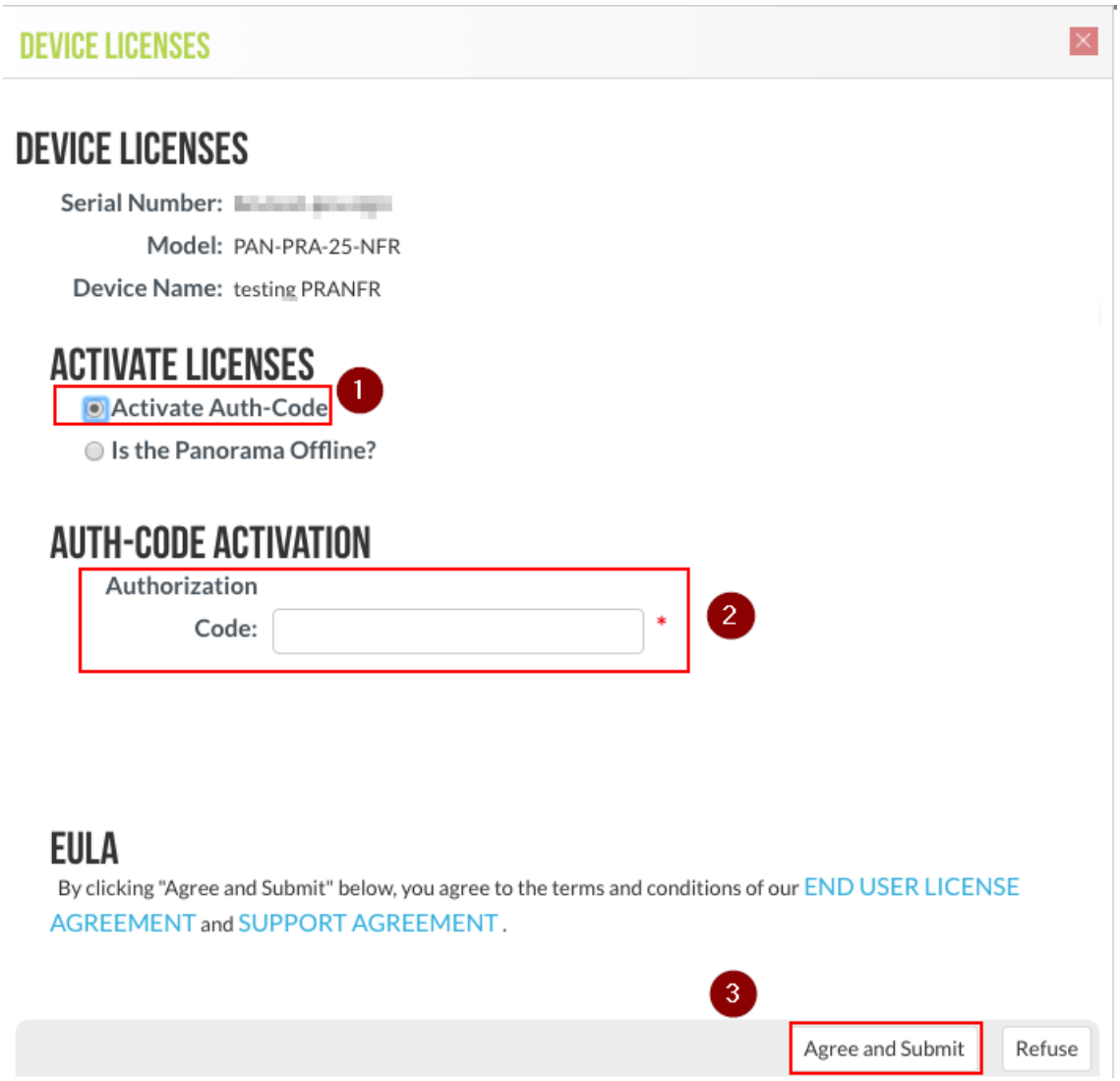
3. Insert your Panorama serial number and fill in the other required fields. Then click on **Agree and Submit**":



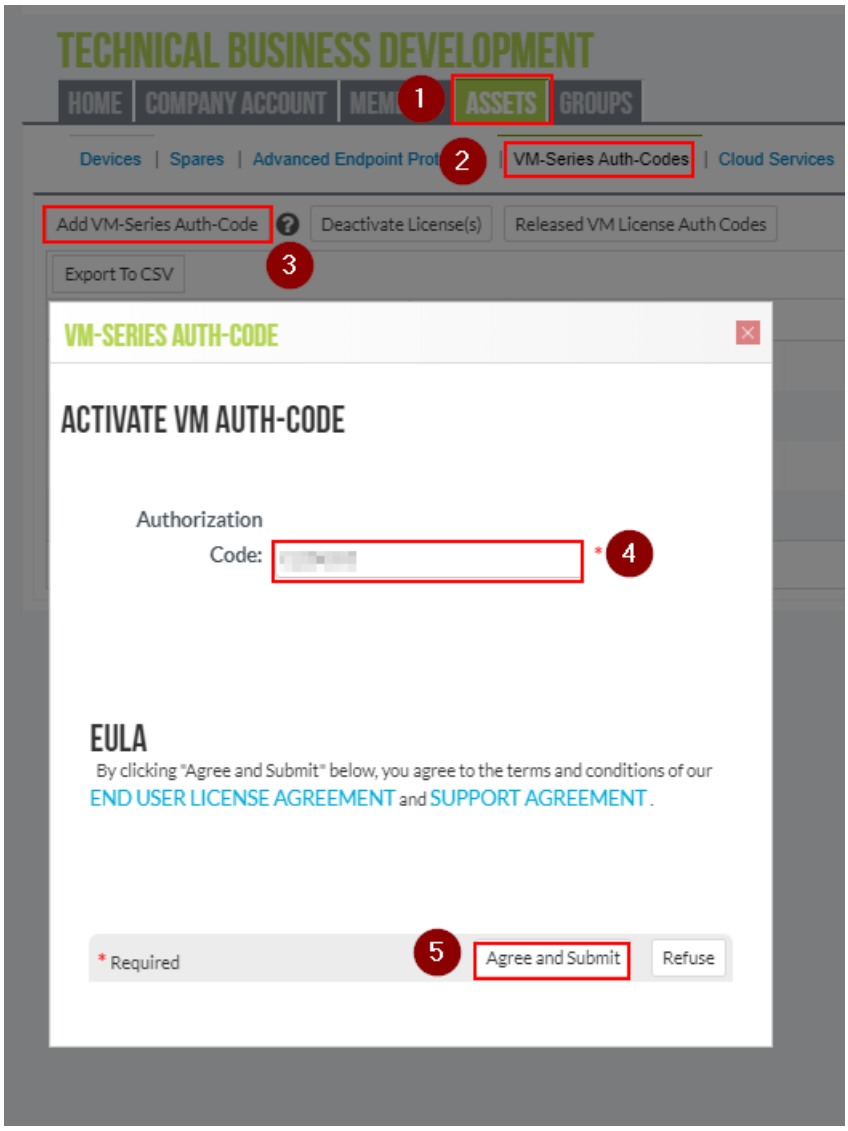
4. You will need to associate the Panorama Support Authcode with the Panorama serial that you registered. From the **Devices**" page under the "**Assets**" tab, click on the "**Actions**" icon on the line that correspond to the Panorama serial number you just added:



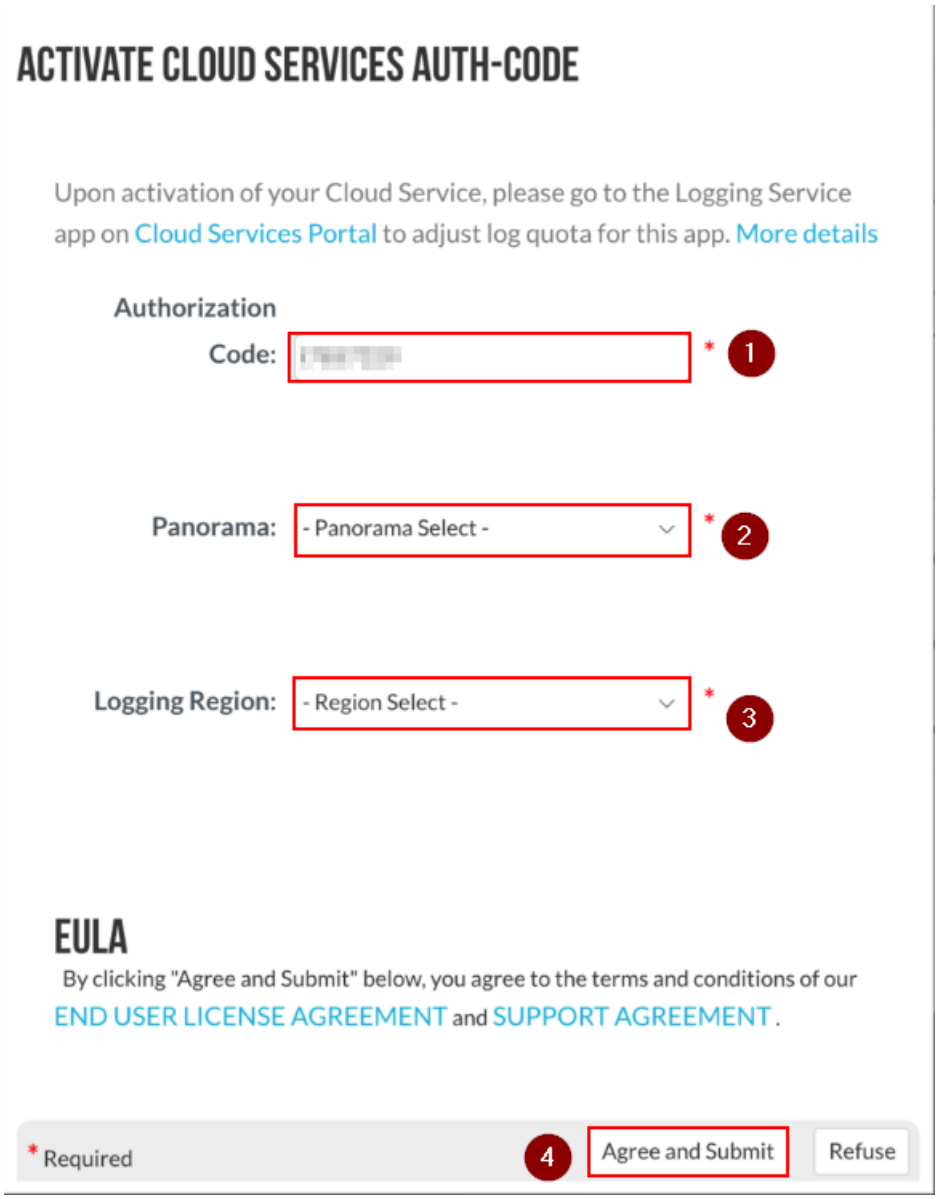
5. Select "**Activate Auth-Code**", insert the Panorama support Auth-Code (the one that corresponds to the PAN-SVC-NFR-PRA-25 SKU) and click on "**Agree and Submit**"":



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:**":

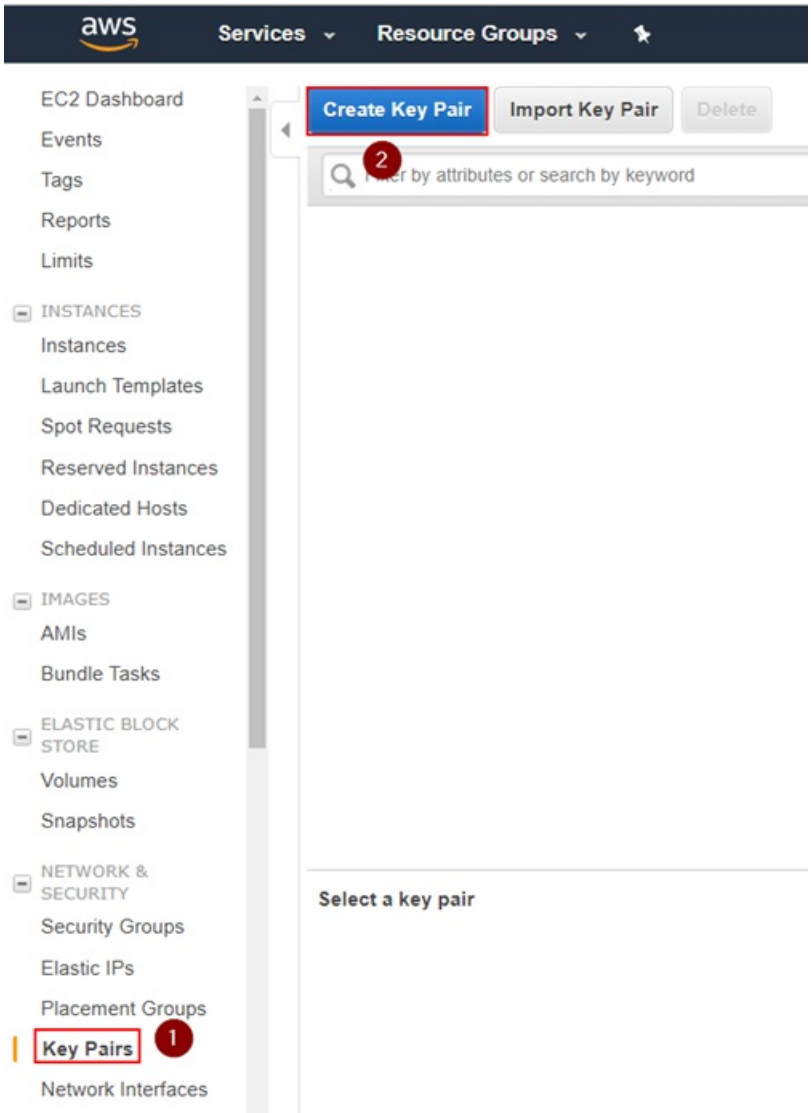


##AWS Configuration

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**':

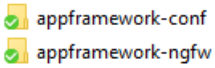


2. Insert a keypair name and click on "**Create**". In the example, we use "paloalto". This will create a "paloalto.pem" private key and the AWS Web UI will prompt you to download it.

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.

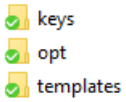
S3 Bucket Pre-Configuration

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:

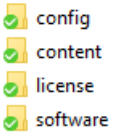


In the example we use **appframework-ngfw** for the firewall configuration and **appframework-conf** for the lab miscellaneous configuration. You can use any arbitrary name for the S3 buckets, but they will have to be unique in AWS.

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



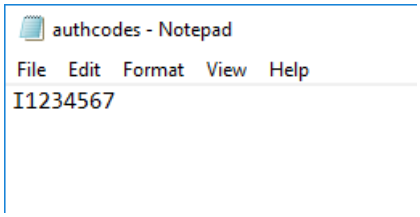
If you look inside the **NGFW** bucket folder (appframework-ngfw in the example), you will see 4 folders (config, content, license, software):



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

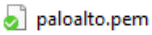
To prepare the configuration files do the following:

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.

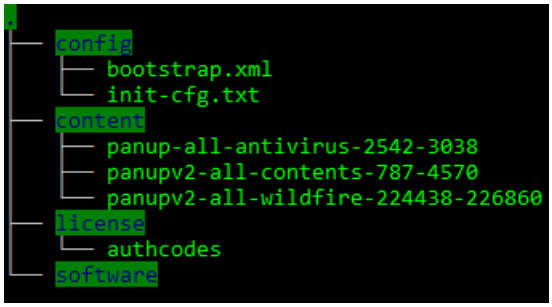
- Save the file
- Add the Firewall and Panorama AWS Private Key
- On your local machine, navigate to the folder that corresponds to the lab configuration bucket (appframework-conf in the example), go to the **keys** sub-folder and copy in it the private key file that you previously generated and downloaded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



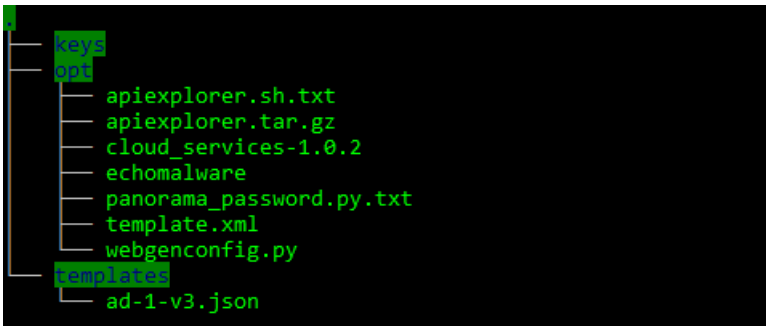
- You can name your key filename however you prefer, but that exact filename will have to be entered as the input to the CFT file later in the deployment process.

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:

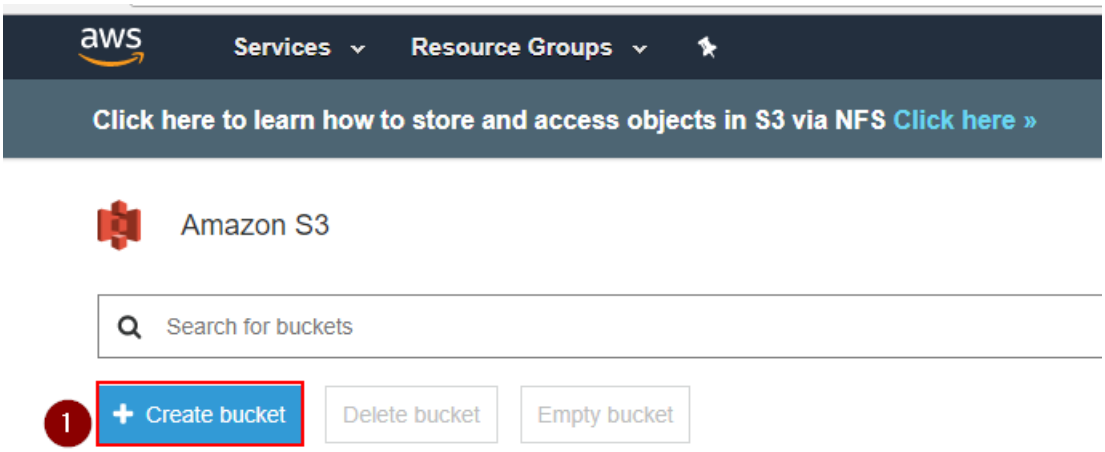


You are now ready to create the S3 Buckets in AWS and upload these files.

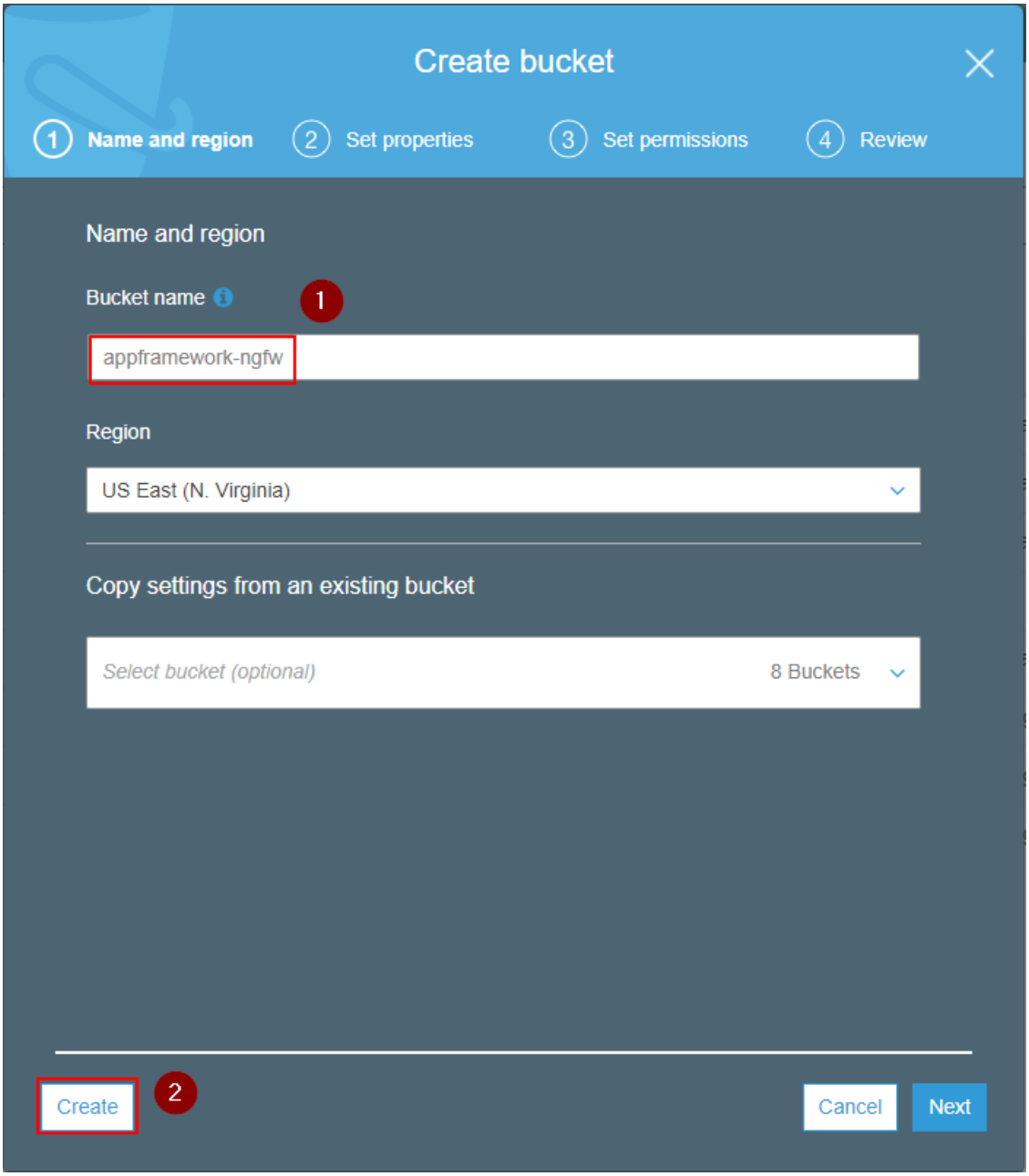
S3 Bucket Creation and Upload

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

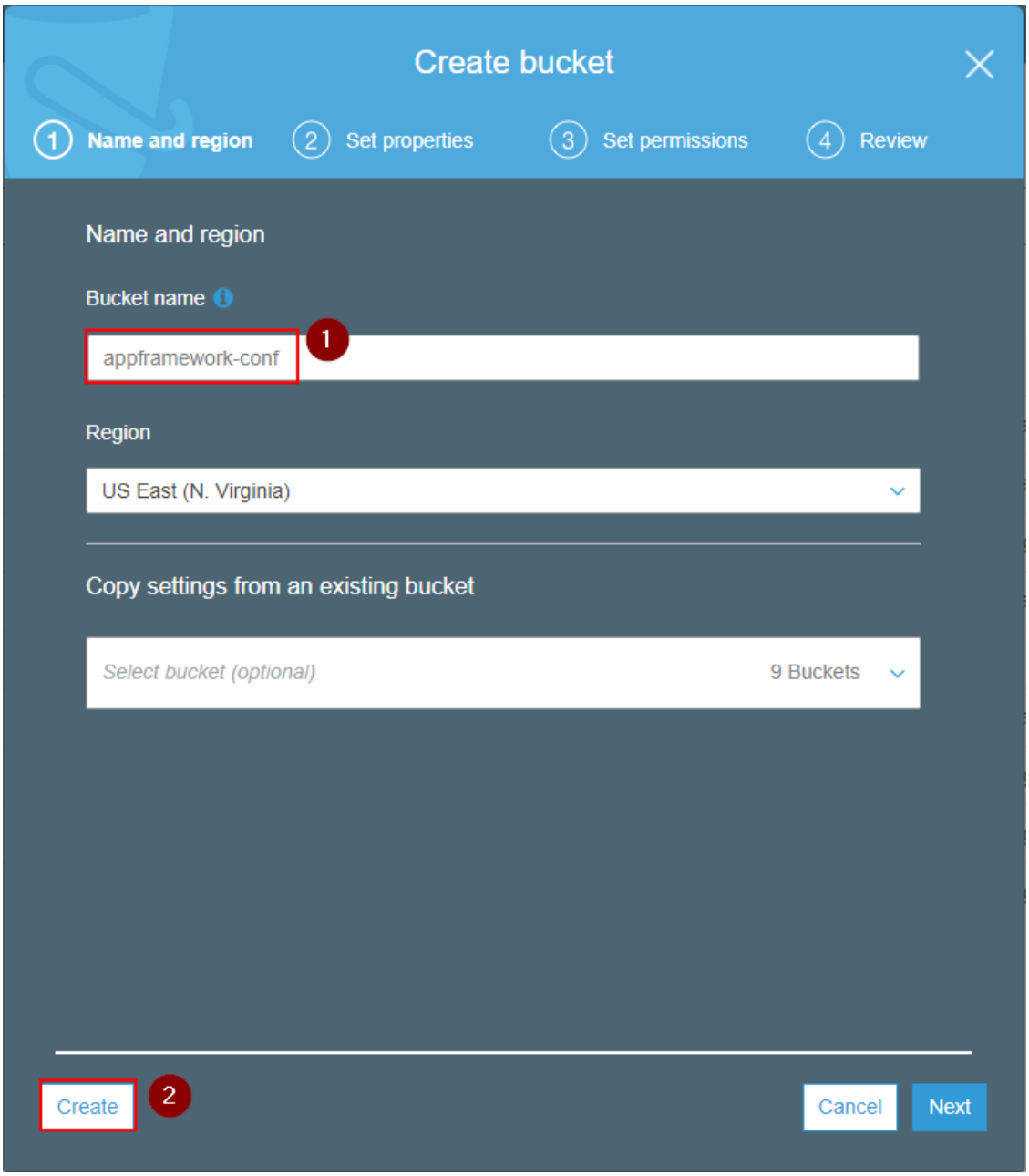
1. Go to AWS S3 and create two S3 buckets for the NGFW and lab configuration respectively (**appframework-ngfw** and **appframework-conf** in the example). To create an S3 bucket, click on **"Create Bucket"**:



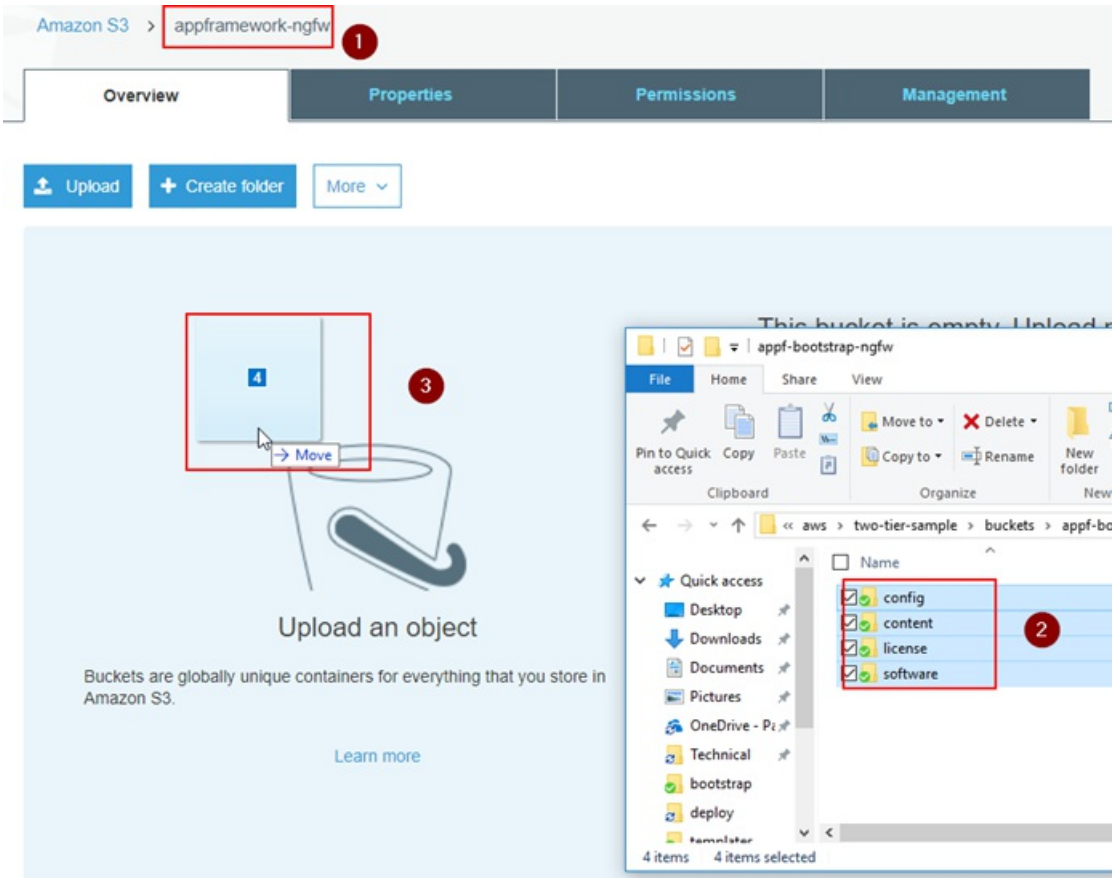
2. Enter the name of the Firewall configuration bucket (appframework-ngfw in the example) and select **Create**:



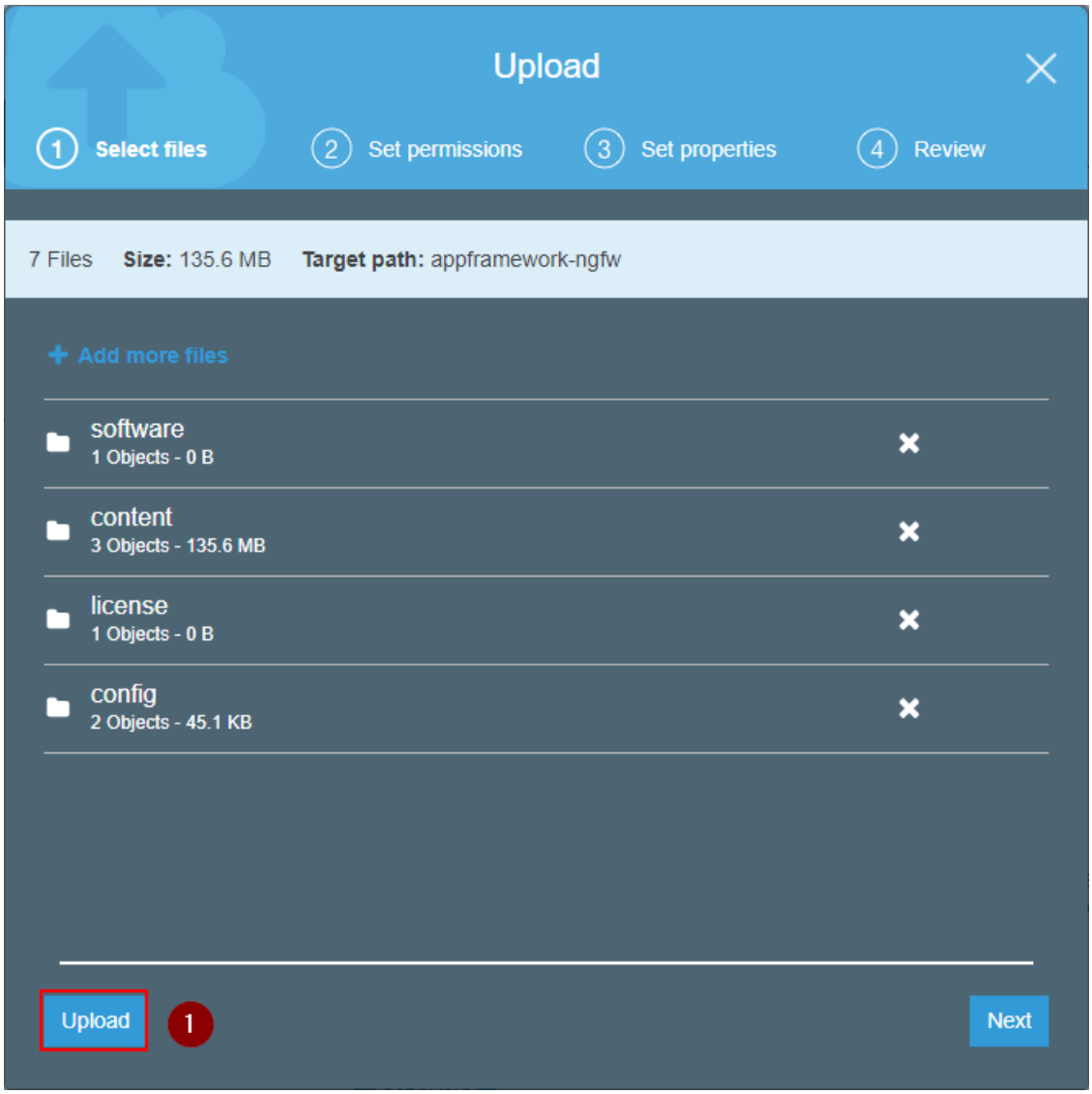
3. Repeat the same process for the Miscellaneous lab configuration S3 bucket (appframework-conf in the example):



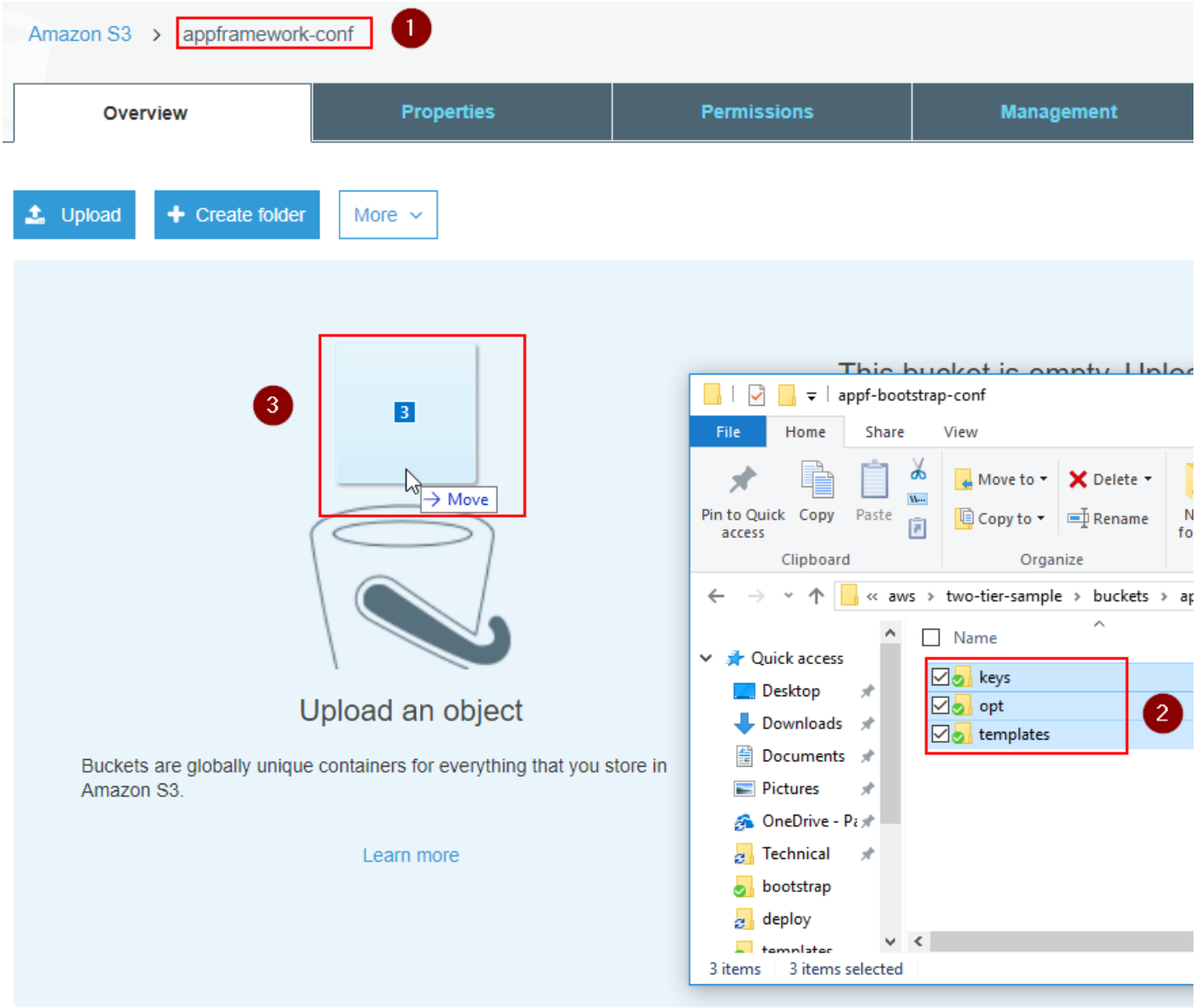
4. You can now upload the content in the respective buckets by dragging and dropping the files from your computer using the AWS S3 UI. The next picture shows the appframework-ngfw bucket:

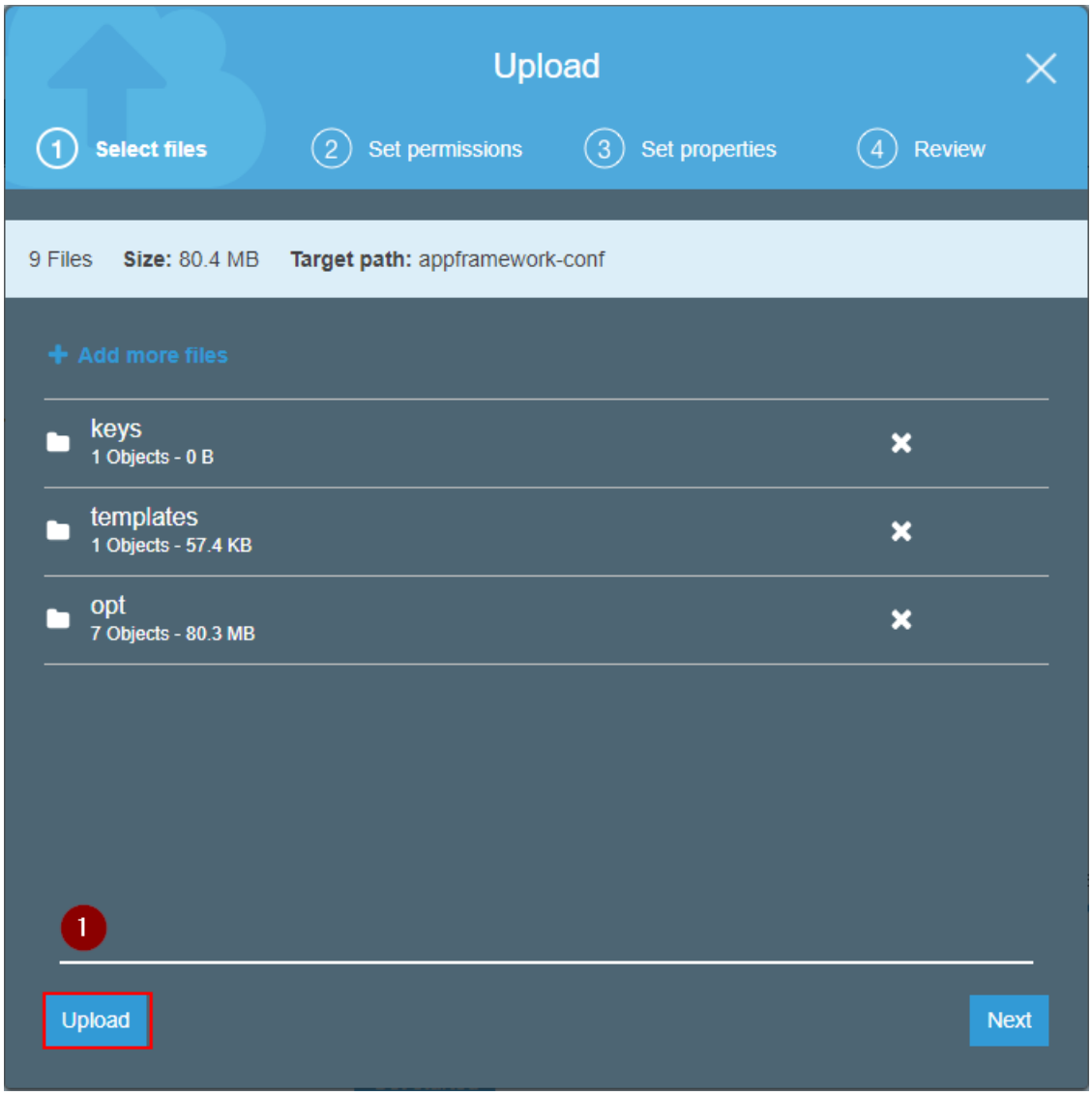


5. Make sure the 4 folders (config, content, license, software) are copied in the root of the S3 bucket, and click **Upload:**



6. Repeat the process for the lab configuration bucket:





Route53 Zone Configuration

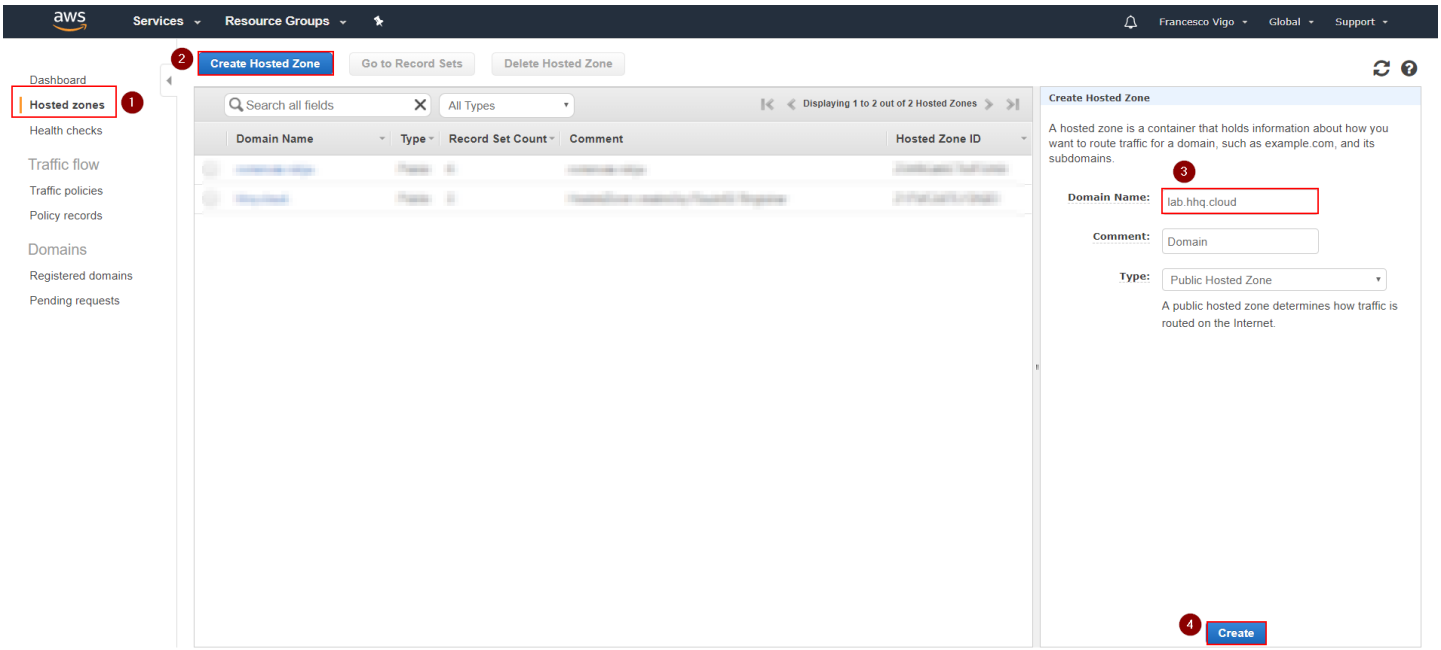
The CloudFormation Template deploys a series of VMs (Firewall, Panorama, API Explorer, Kali Linux, etc.) and AWS can automatically associate DNS names to the Elastic IPs that are used by EC2. To do that, you need a Route53 public Hosted Zone configured in your AWS environment. This step is optional: 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 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.

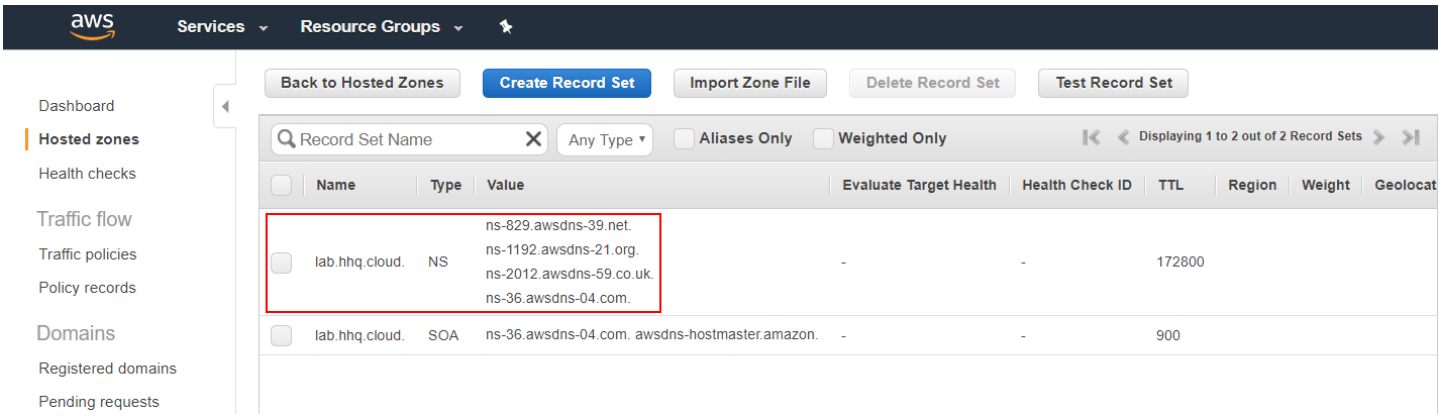
Note: the CFT can automate the creation and registration of a valid SSL certificate that corresponds to the FQDN of your API Explorer instance (this way the browser won't provide warnings when you connect to it), through a free service called "Let's Encrypt" (https://letsencrypt.org). If you want to 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

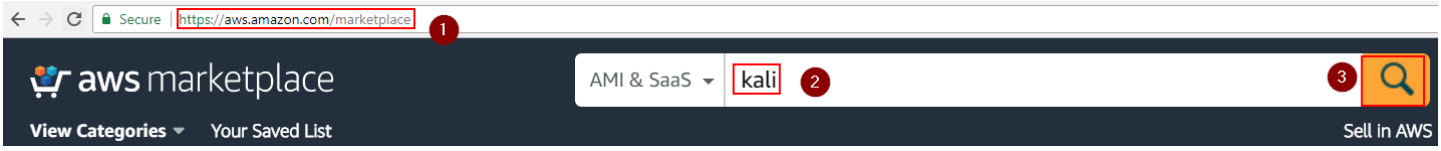
53. If you're using a different domain hosting platform (i.e. GoDaddy, NameCheap, etc), the configuration on how to configure your domain to use AWS Route53 DNS servers will be different depending on your provider.

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

To deploy the VMs, you first need to activate them on the AWS marketplace. Note that deploying Kali Linux is optional so, if you don't want to, you can skip the step for Kali Linux (but not for NGFW and Panorama).

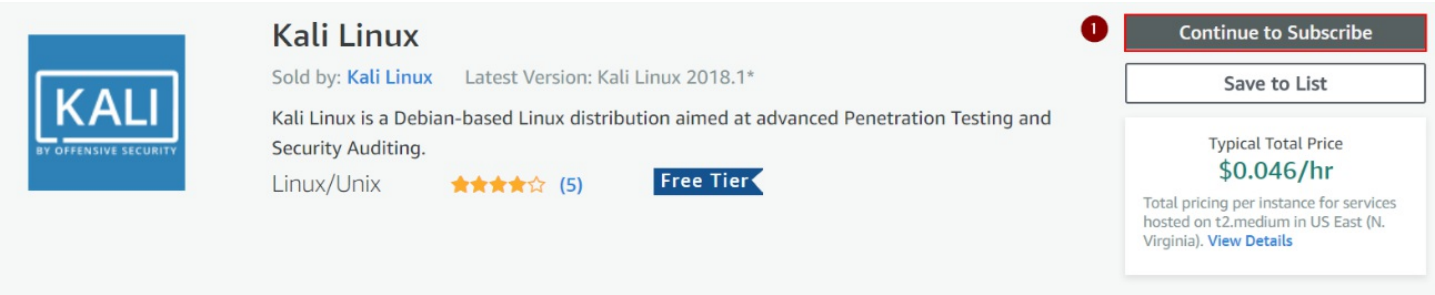
To activate the solutions on the AWS Marketplace, follow this procedure:

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

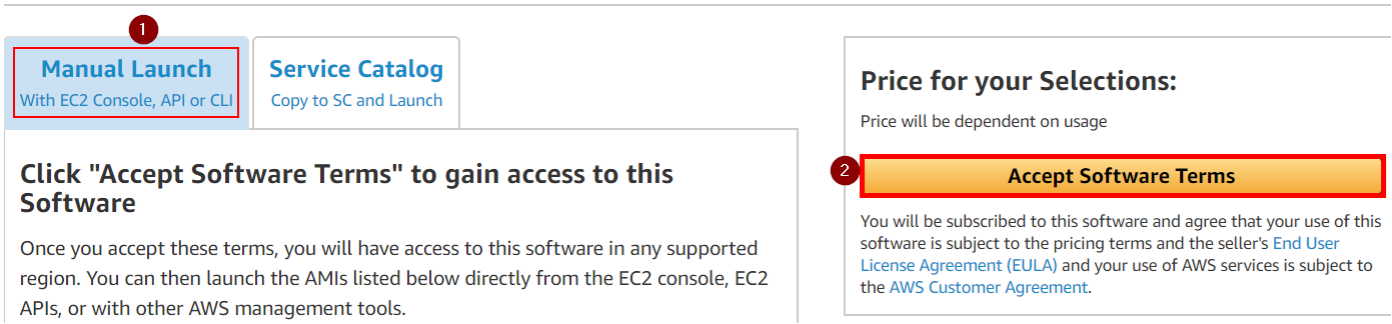


2. In the results page, click on '**Kali Linux**":

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



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



{

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

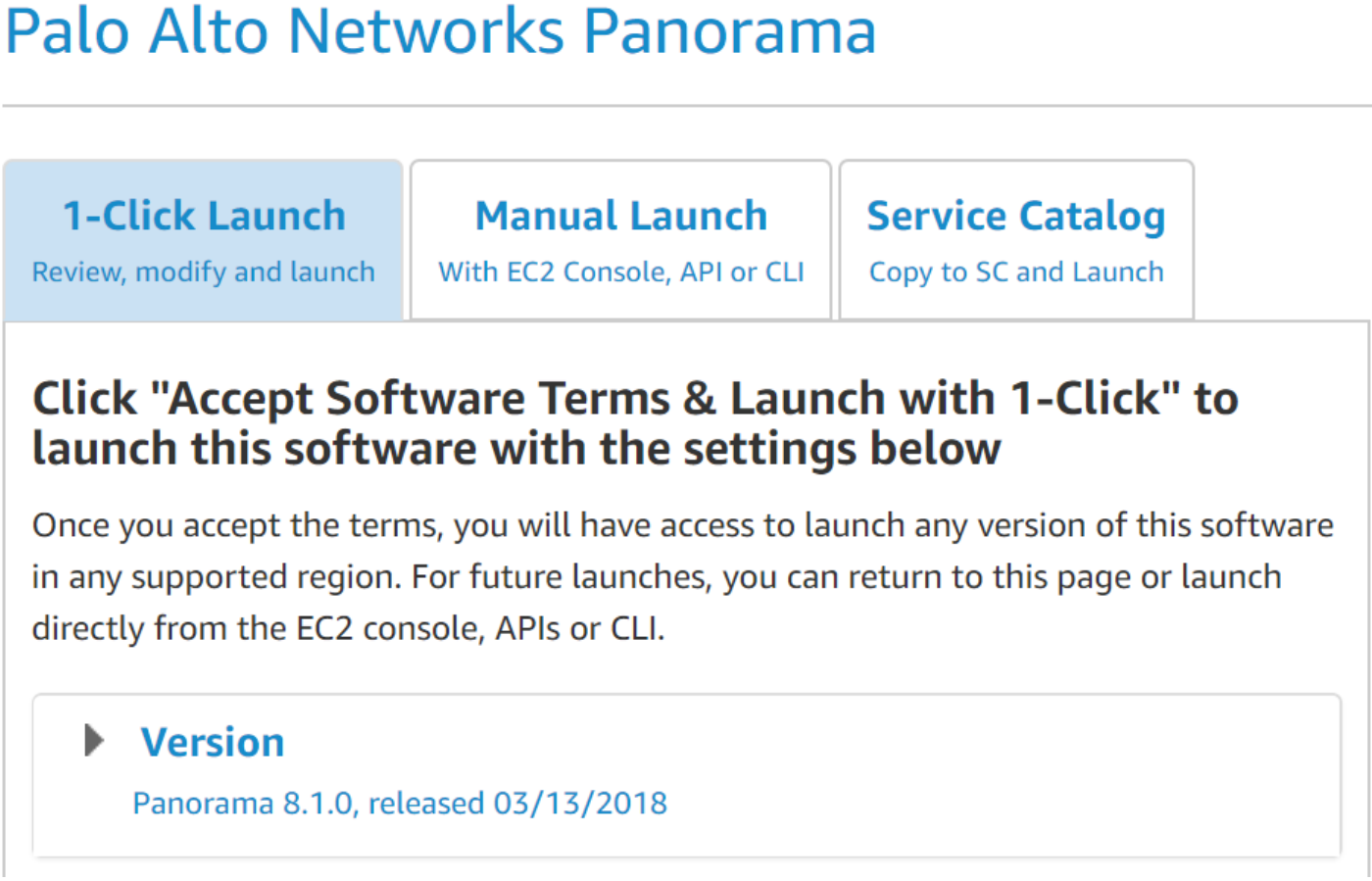
Launch Options

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

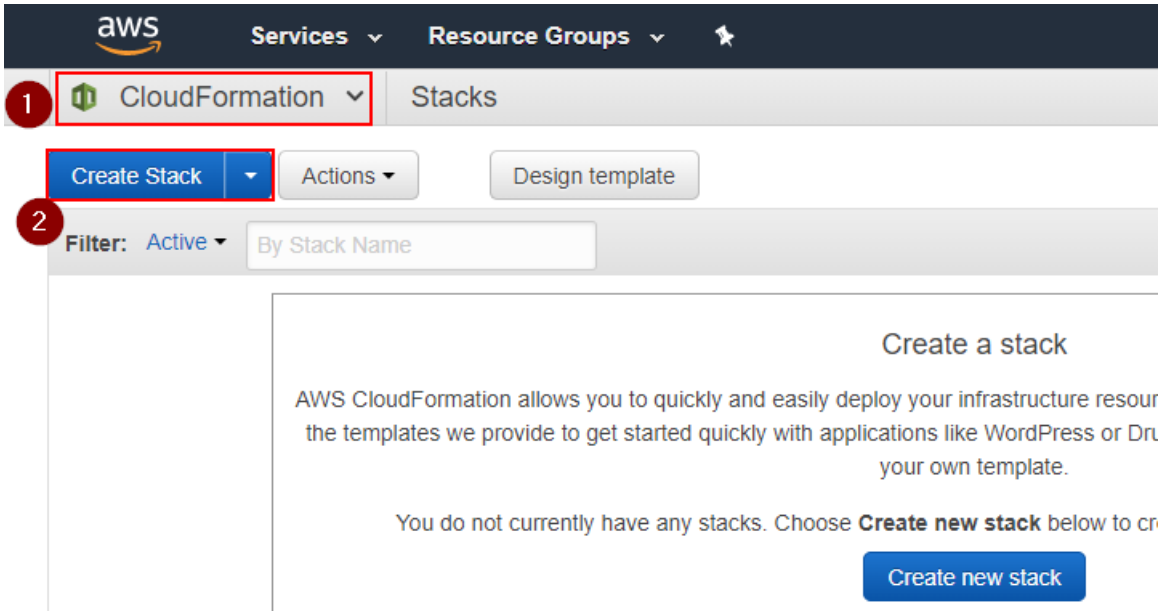


{

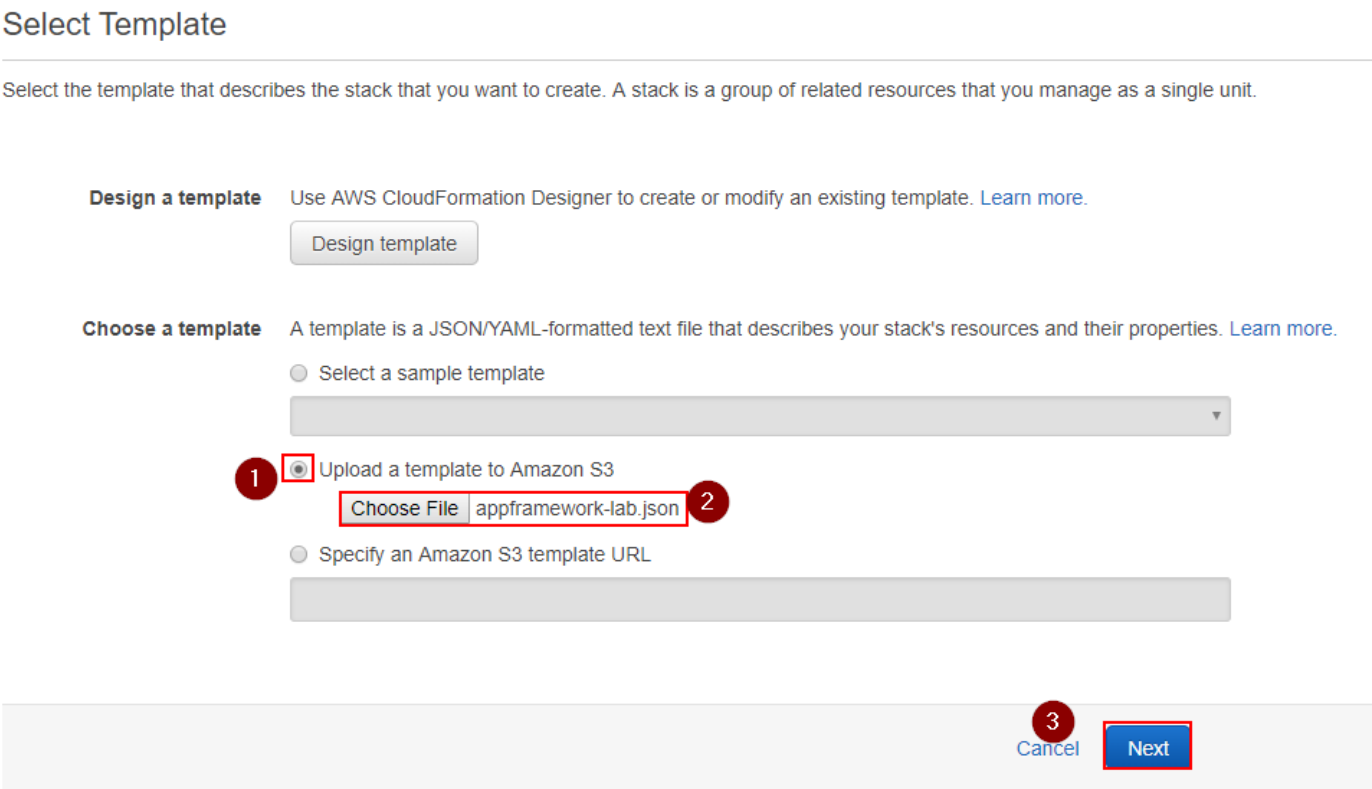
Deploy the CloudFormation Template

You can now deploy the CloudFormation Template (CFT) to create the lab environment, with the following procedure:

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**:



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 Eplorer 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 PartnerLab1

Parameters

Basic Configuration - REQUIRED

Admin Password ••••••••••

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 appframework-conf — Bucket name for non-Firewall configuration (i.e. myappframeworkbucket-conf)

Bootstrap S3 Bucket Name appframework-ngfw — S3 Bucket name for FW bootstrap configuration (i.e. myappframeworkbucket-conf)

Bootstrap S3 Bucket Region us-east-1 — S3 Region where the FW bootstrap bucket is located

Private Key File keys/paloalto.pem — Private Key File with Path in the Environment Configuration S3 Bucket (i.e. keys/paloalto.pem)

EC2 VMs Key Name paloalto

Name of an existing EC2 KeyPair to enable SSH access to VMs. Except NGFW and Panorama

Panorama and NGFW Key Name paloalto

Name of an existing EC2 KeyPair to enable SSH access to NGFW and Panorama

Panorama Serial 00000000000 — Panorama Serial Number (provided by Palo Alto Networks)

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

LetsEncrypt Email 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

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.

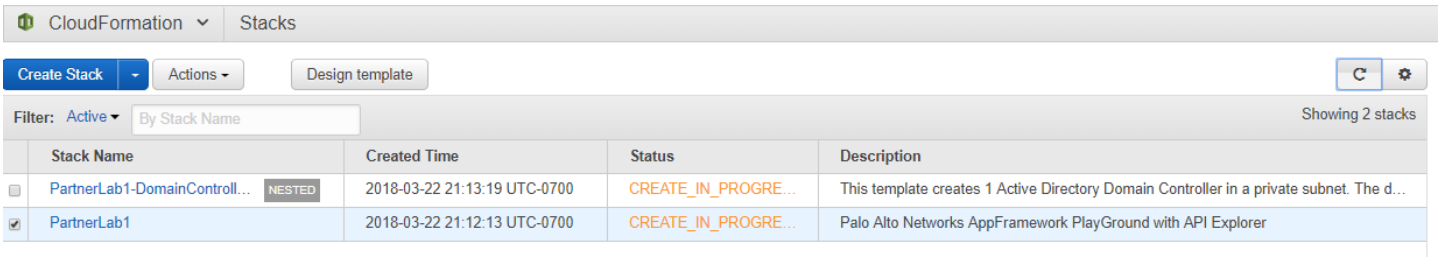
☑ **I acknowledge that AWS CloudFormation might create IAM resources with custom names.** (1)

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

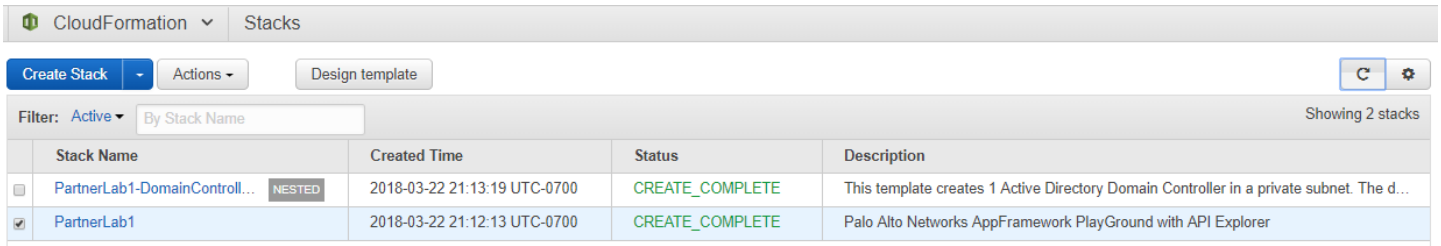
(2) Cancel Previous **Create**

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.

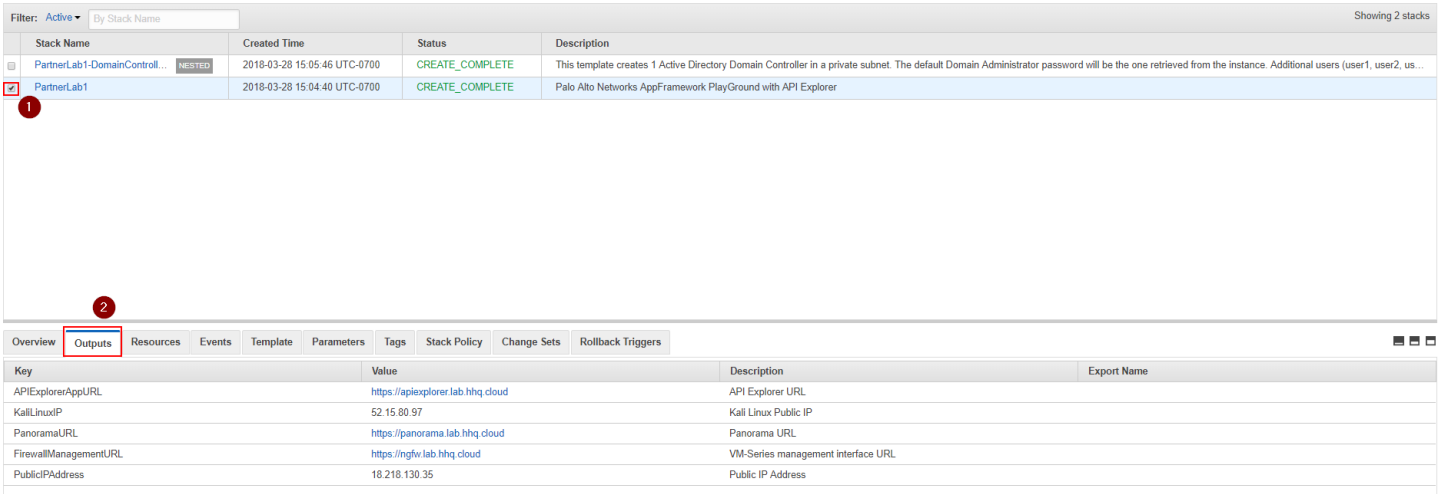
6. Sit down and relax, the whole process will take 30-35 minutes to complete:



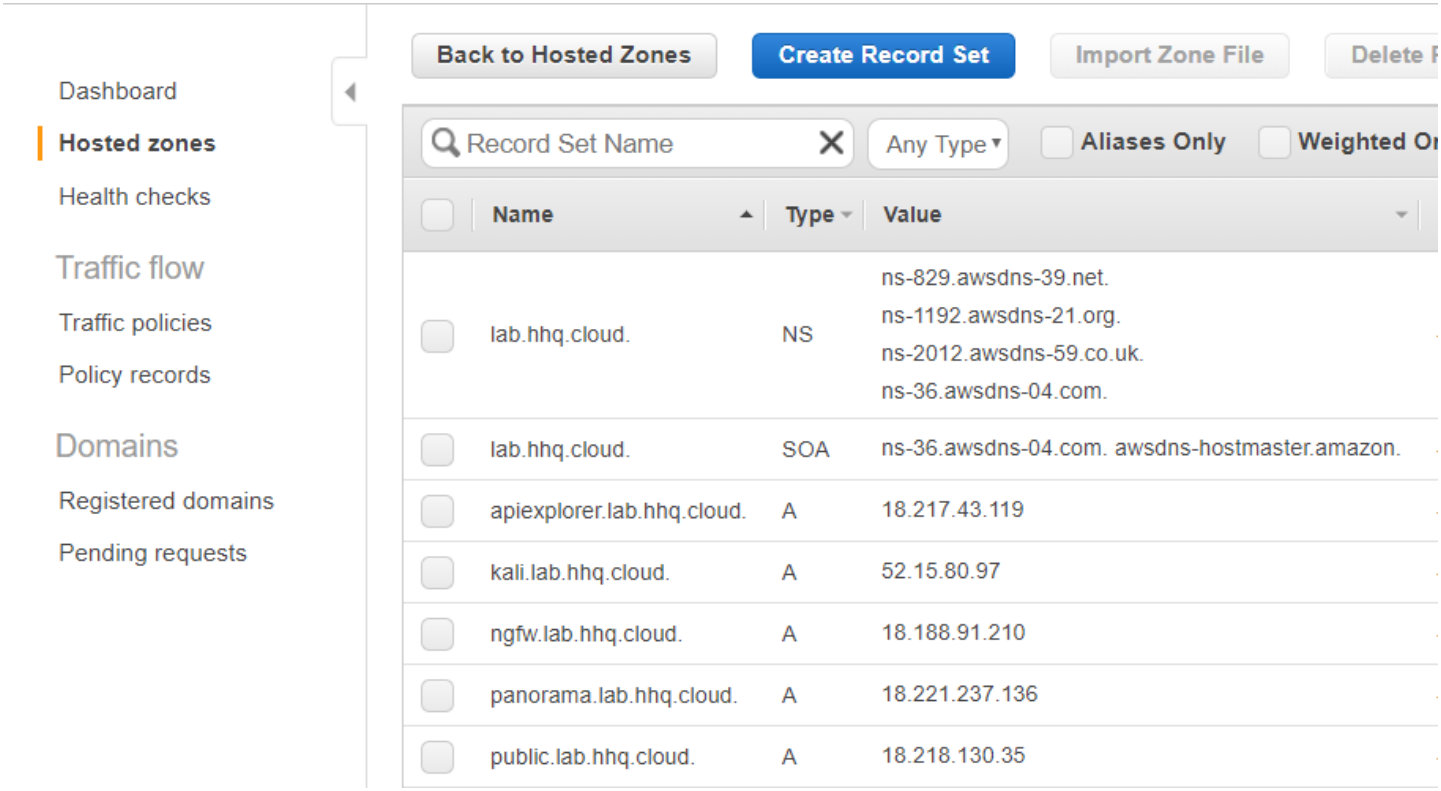
7. The deployment will show **CREATE_COMPLETE** once everything is done:



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



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



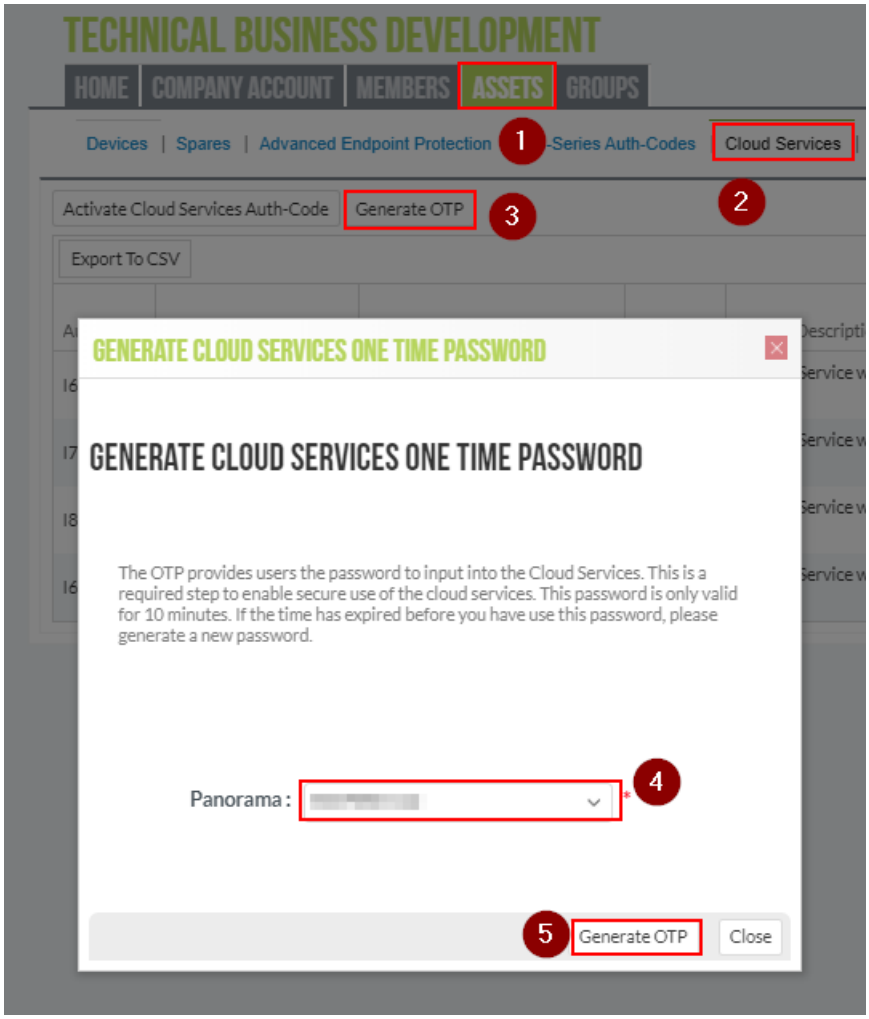
Copyright (C) 2018 - Palo Alto Networks, Inc.

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.

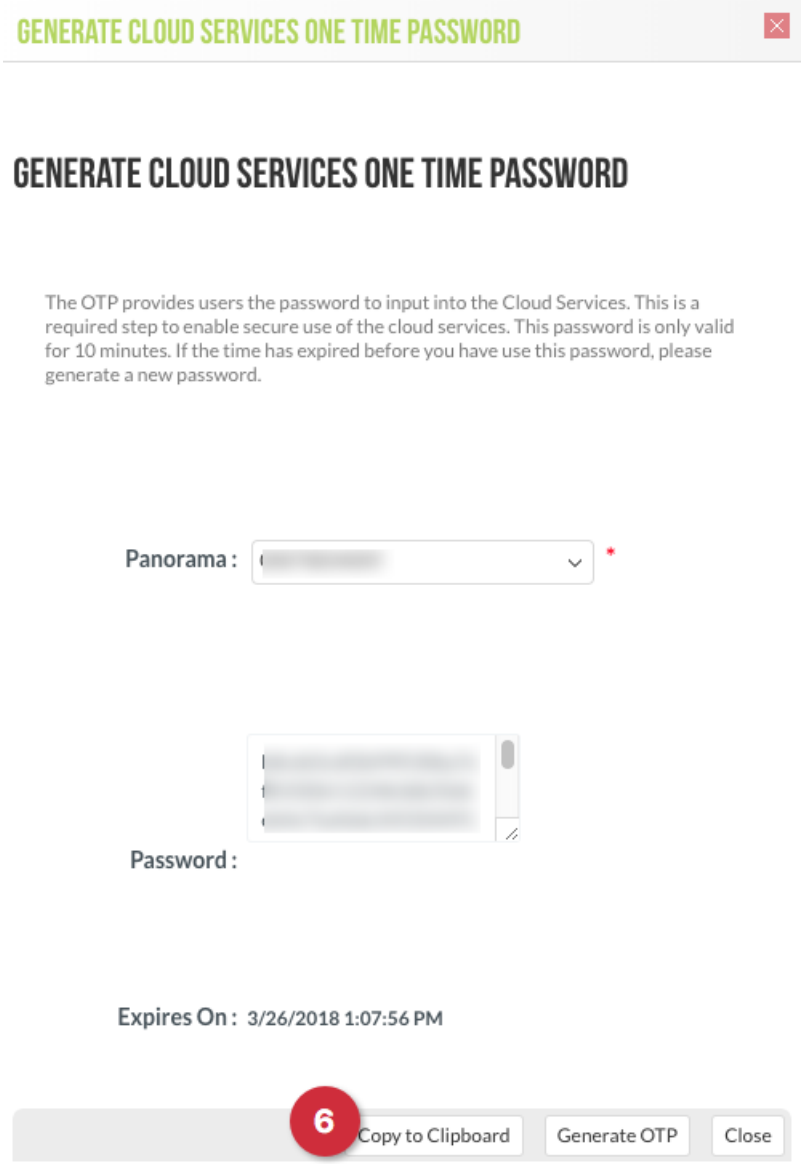
Panorama Pairing with Logging Service

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

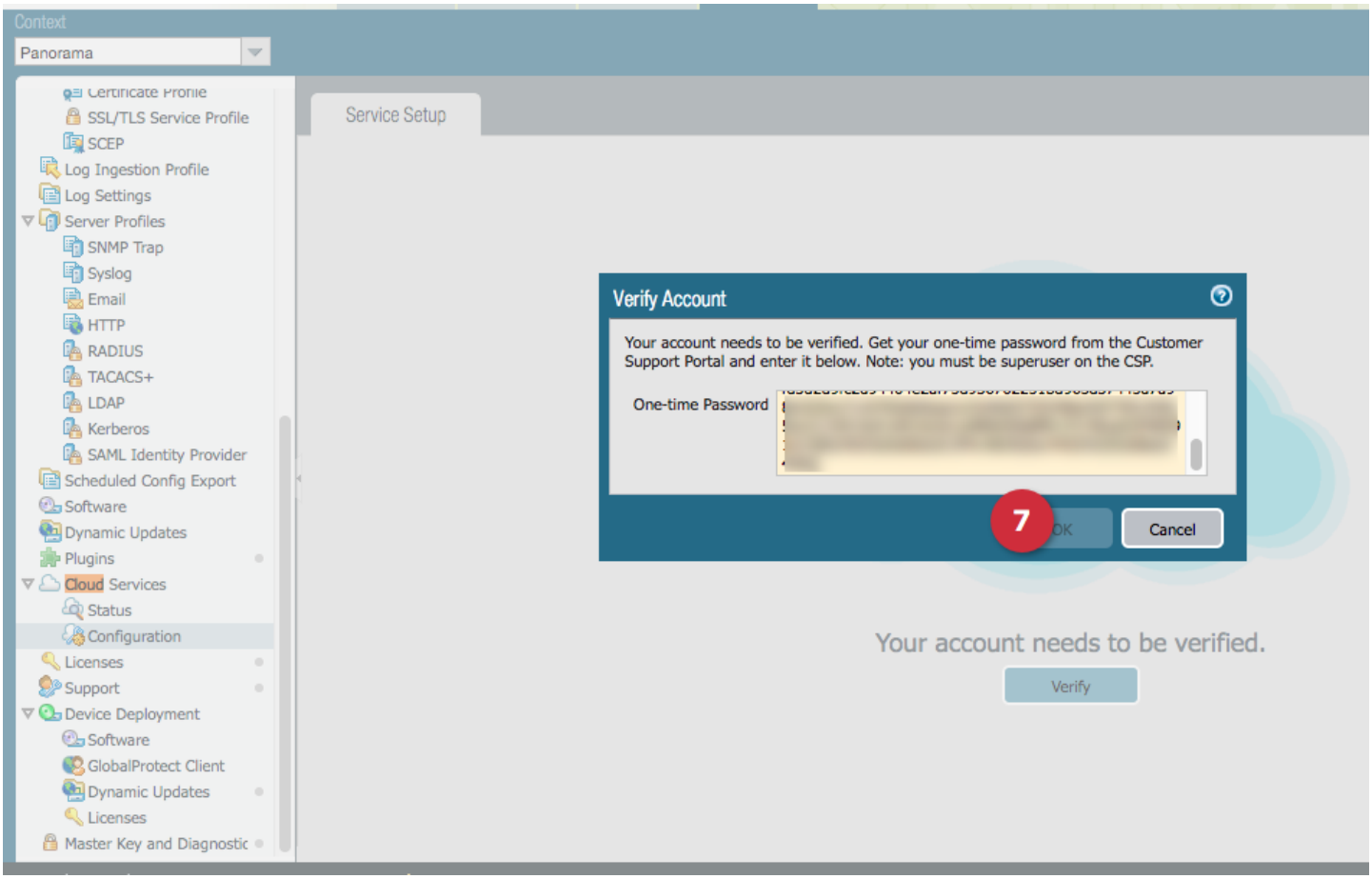
1. Navigate back to https://support.paloaltonetworks.com and login with your CSP credentials
2. Go to **"Assets"**, "**Cloud Services**" and click "**Generate OTP**". Select the Panorama instance you've created (corresponding to the Panorama Serial Number) and click on **Generate OTP**:



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

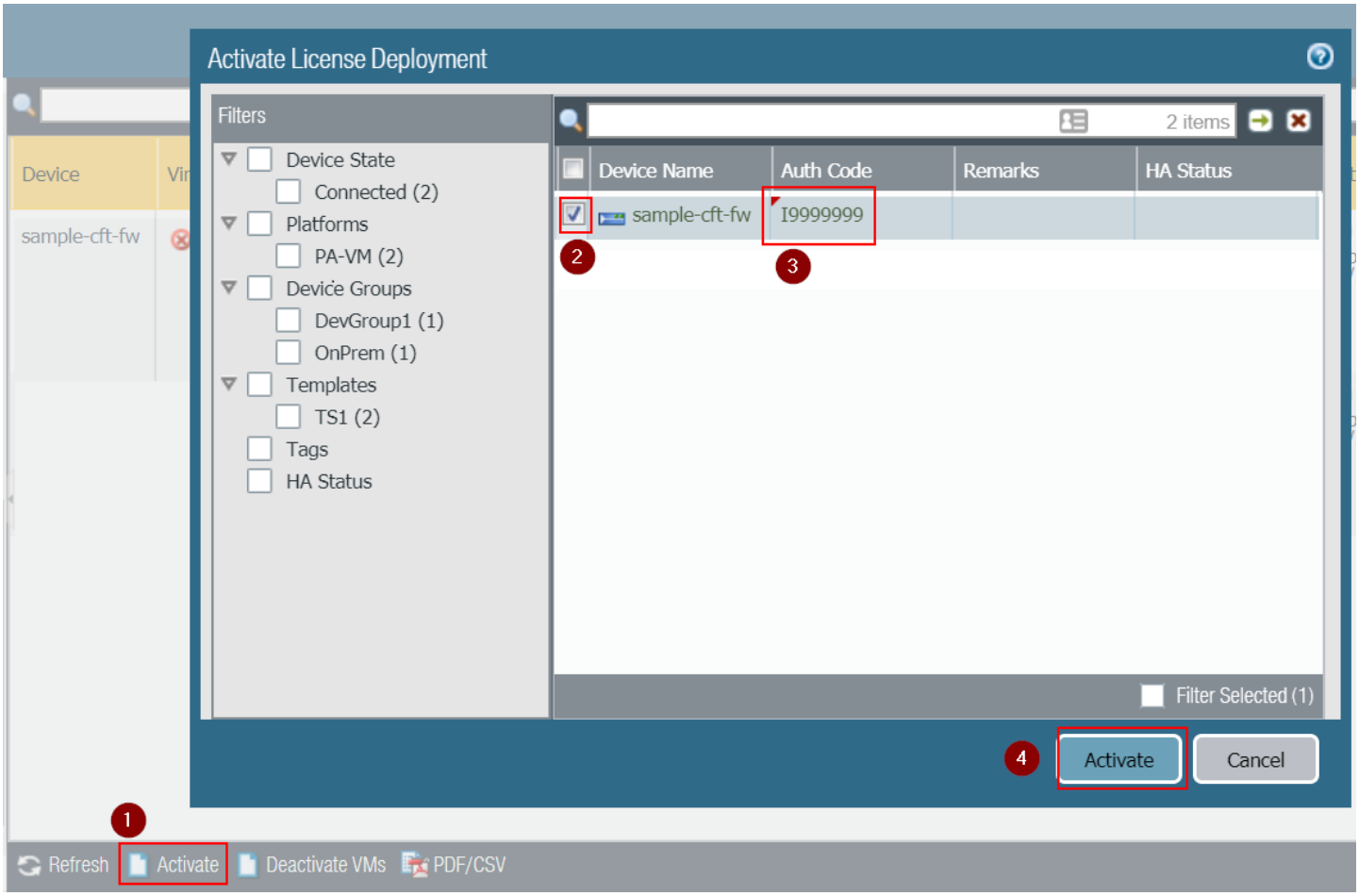


4. Login to Panorama via the web UI, navigating to https://panorama.lab.yourdomain.com (assuming that Route53 has used to automatically create the FQDN, otherwise look at the EIP of the Panorama instance). Use the "admin" user and the password you have configured in the template.
5. On the Panorama UI,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

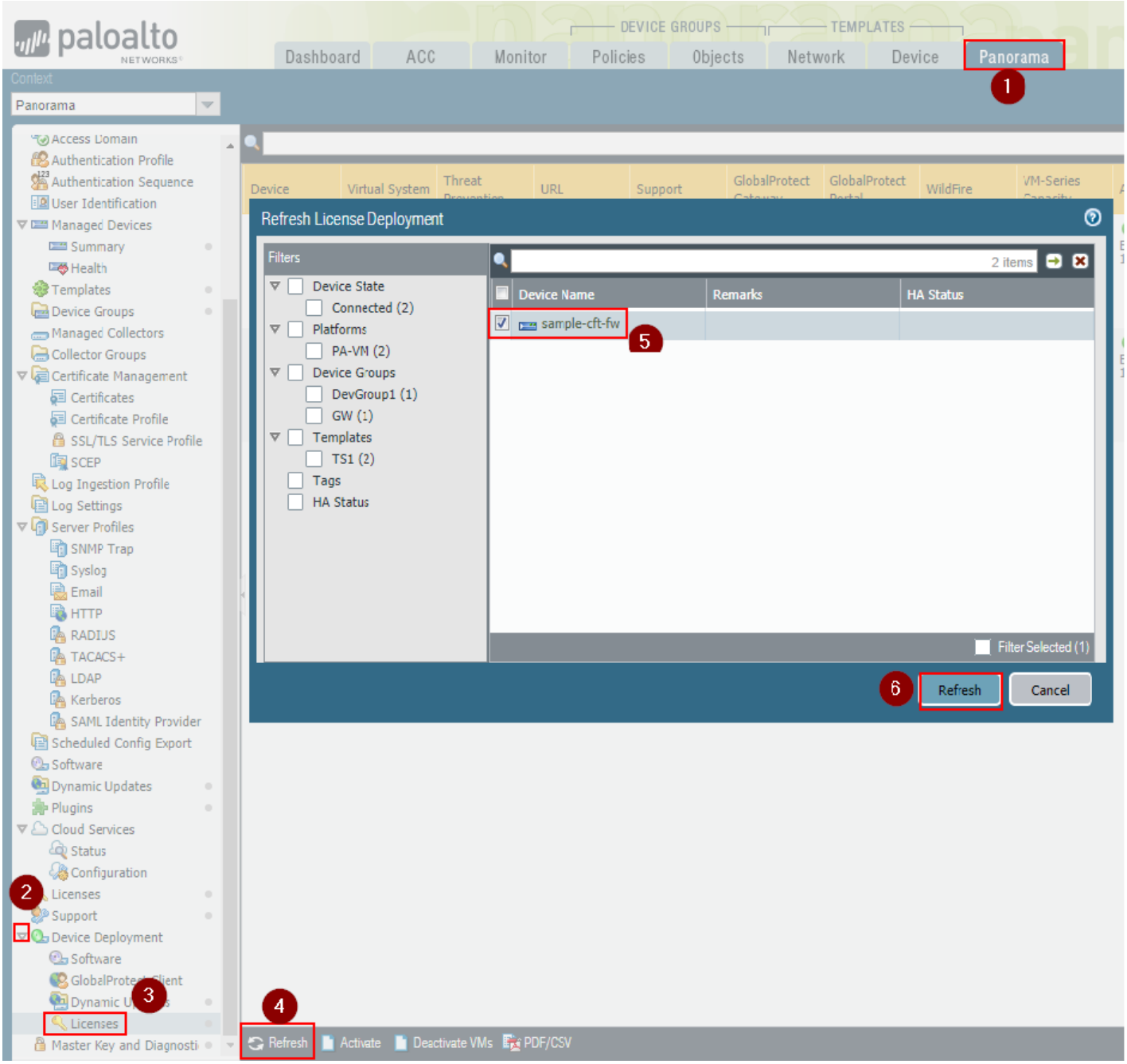


After the pairing is complete, in the "Configuration" page under "Cloud Services", you should see a dashboard similar to the following:

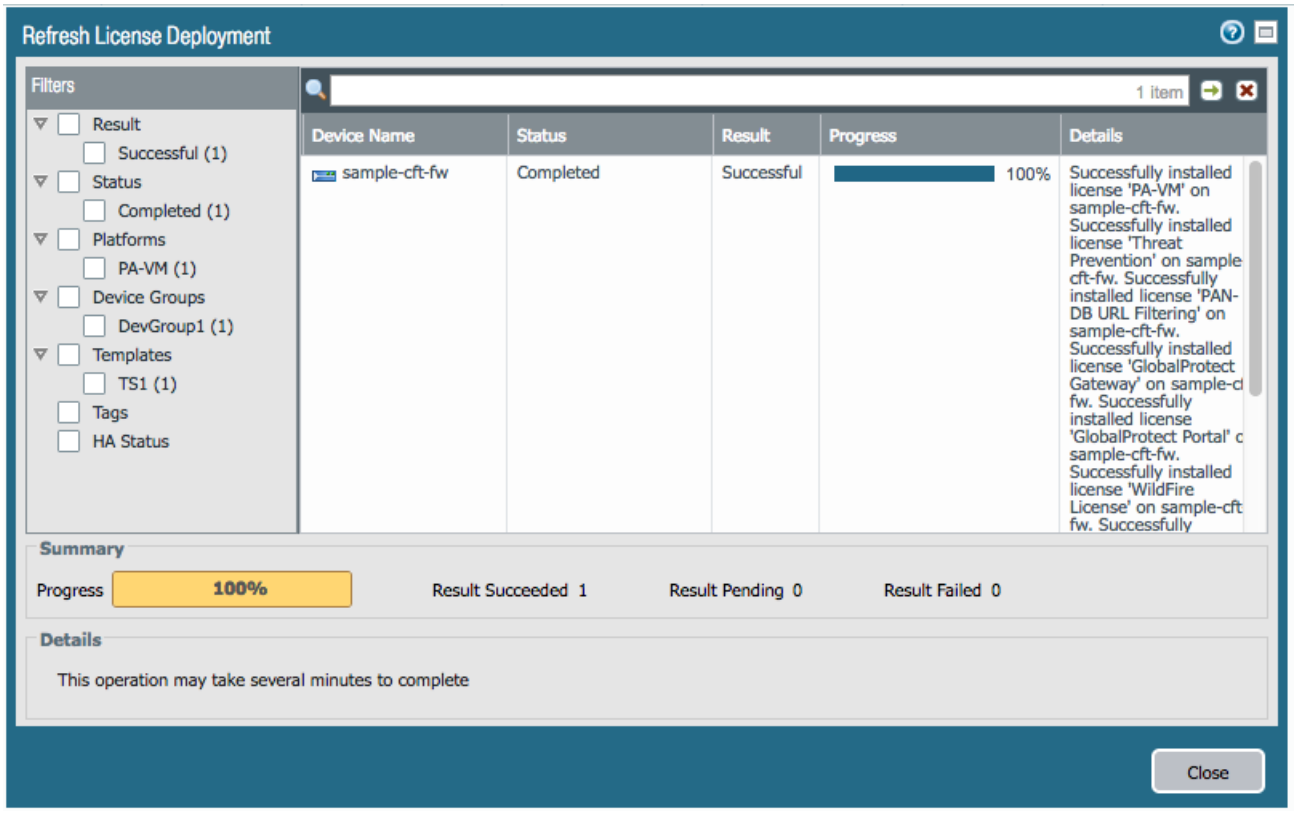
7. On the Panorama UI, navigate to '**Panorama**", "**Device Deployment**", "**Licenses**" and click on "**Activate**"
8. Select the firewall (**sample-cft-fw** in the example), insert the Services Bundle Auth-Code (the one that corresponds to the PAN-VM-100-BND-NFR4 SKU) and click on "**Activate**":



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 contacts to register the API Explorer application in the Application Portal, and then activate it (see the next section of this document for details)

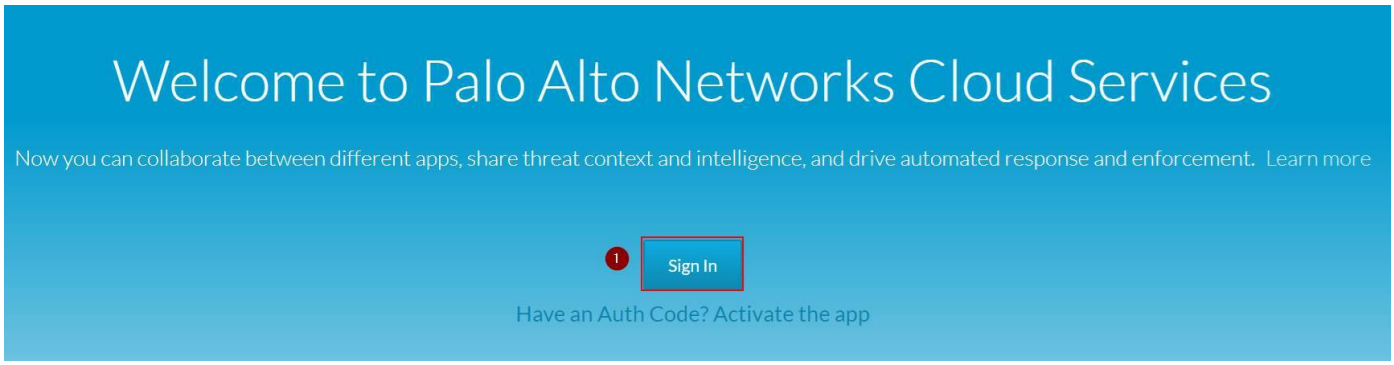
API Explorer App Activation Process

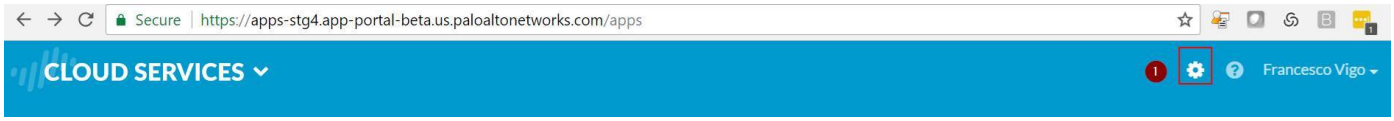
This section describes how to Activate the API Explorer application and start interacting with the APIs.

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.

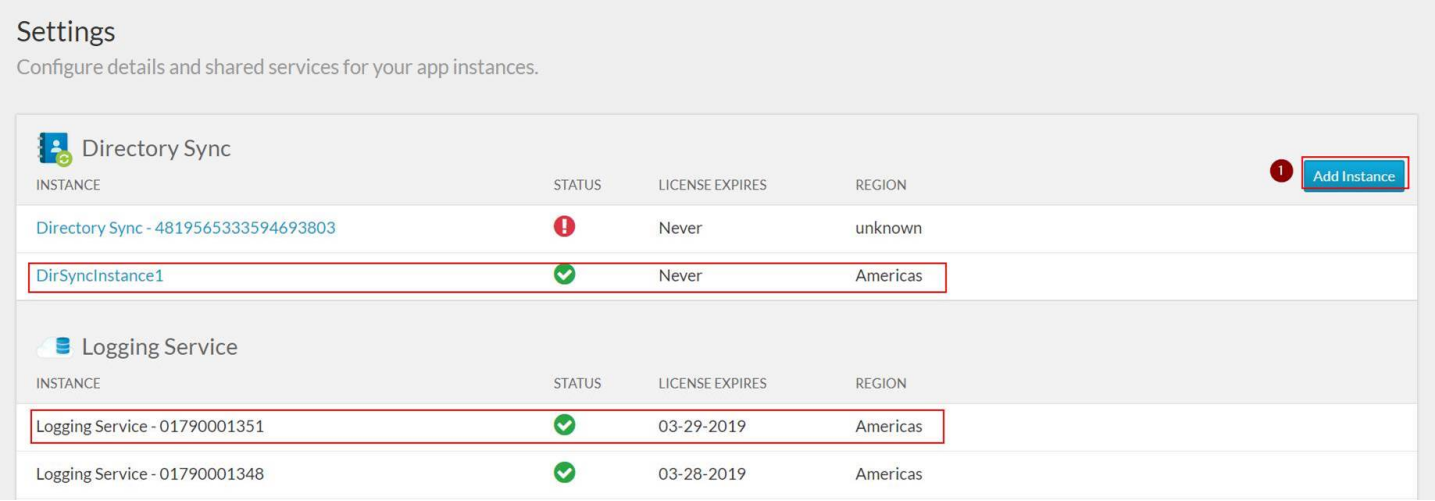
To activate the API Explorer, follow this process:

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:

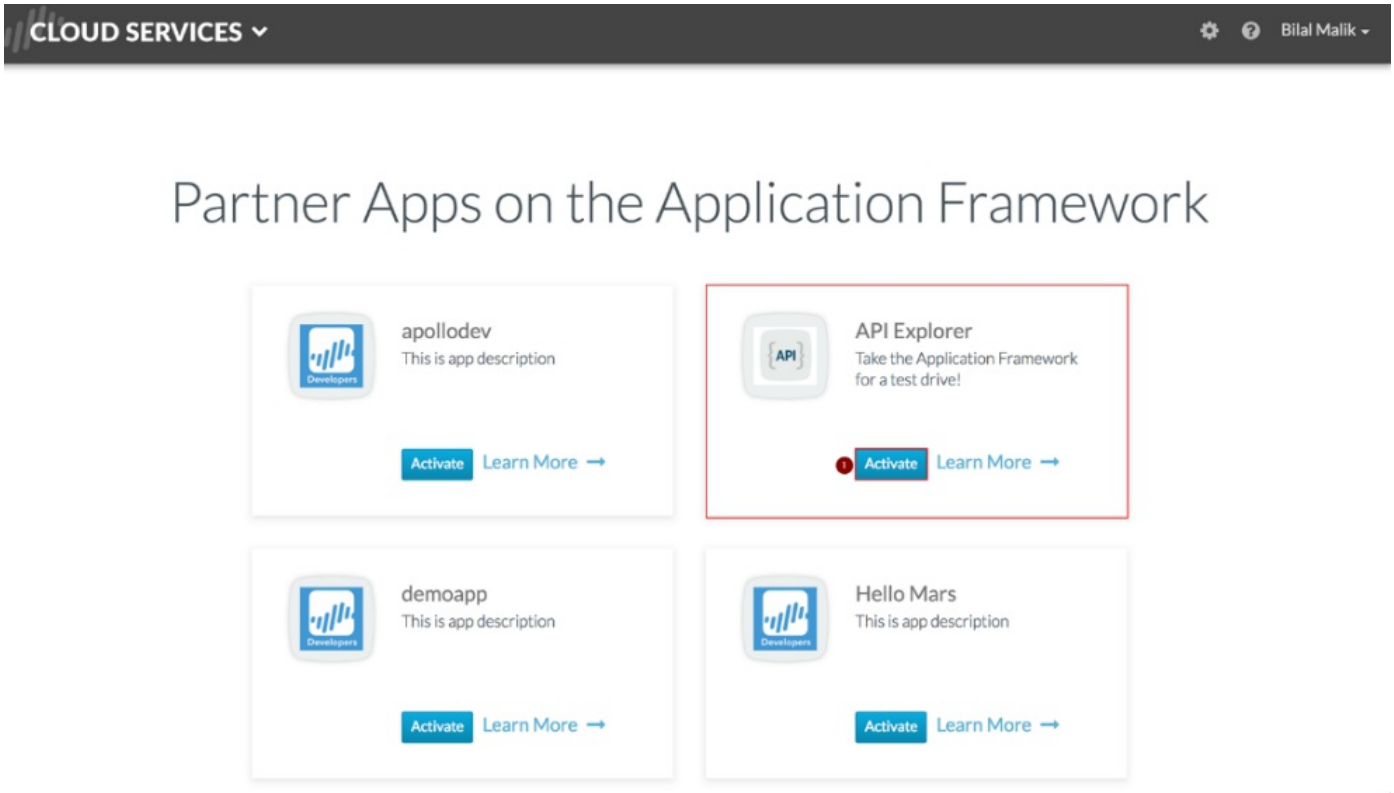


2. 

Click on the Settings icon in the top right corner:
3. Make sure that you have a Logging Service instance, and a Directory Sync instance. If the latter is missing, just create one (click on **"Add Instance"** . 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 ask your Palo Alto Networks contact to get some sample data added to it):

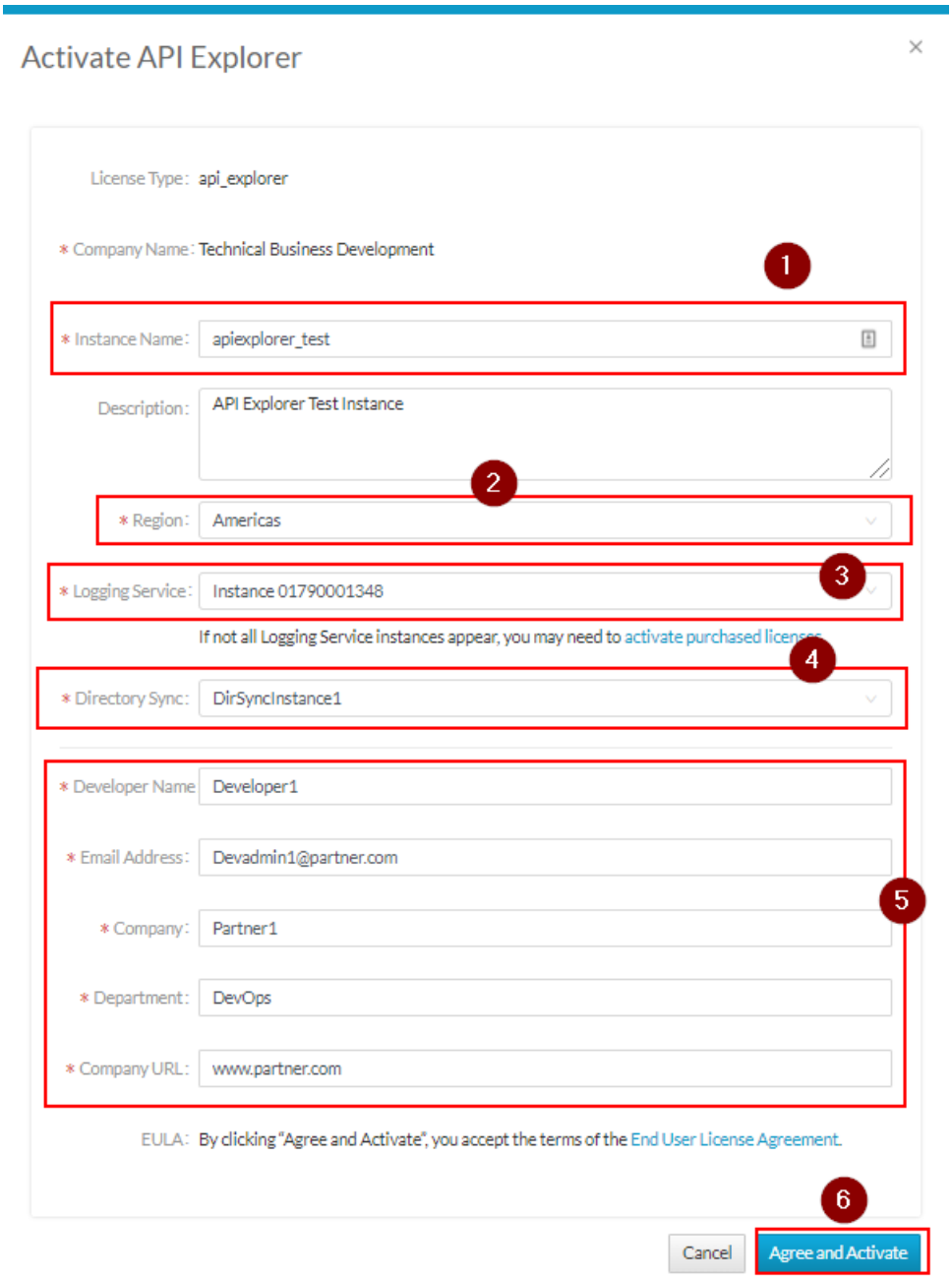


4. Navigate to the botton of the Application Portal page, under "**Partner Apps on the Application Framework**". Select the application (i.e. API Explorer yourcompany) and click on the "**Activate**" icon:

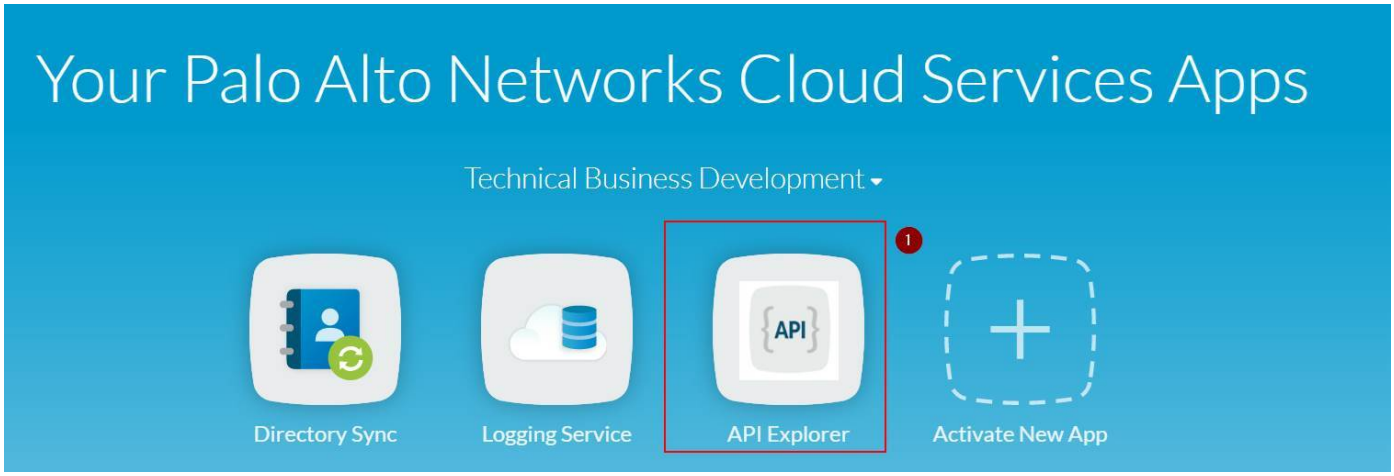


Note: if you don't see your API Explorer App, reach out to your Palo Alto Networks technical contact.

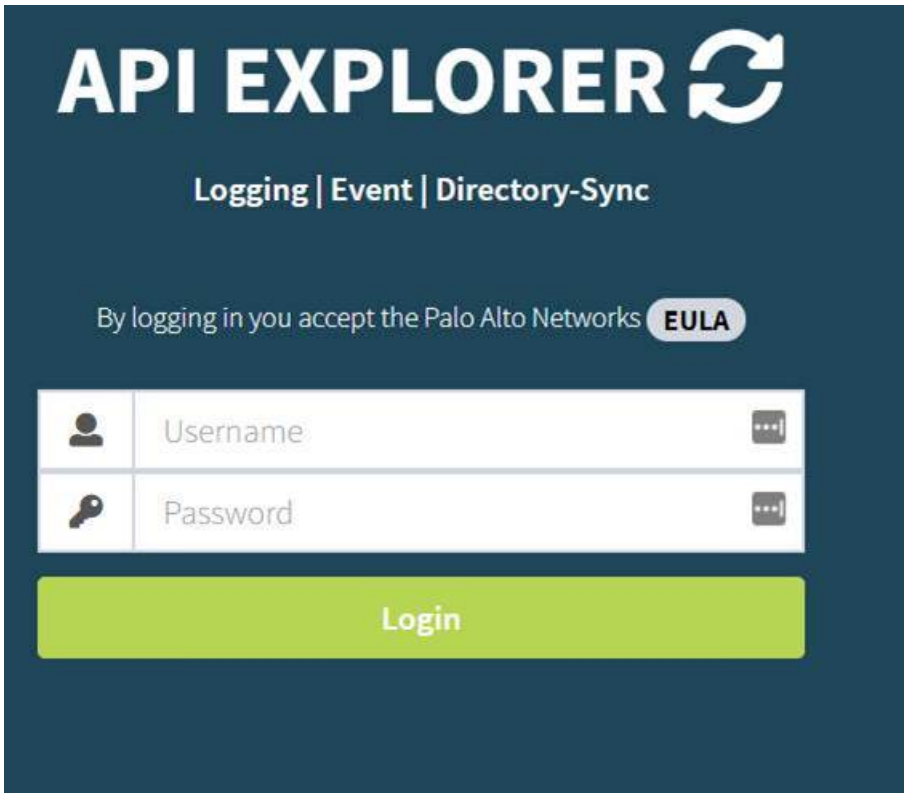
5. Enter the required parameters, then select **Agree and Submit**:



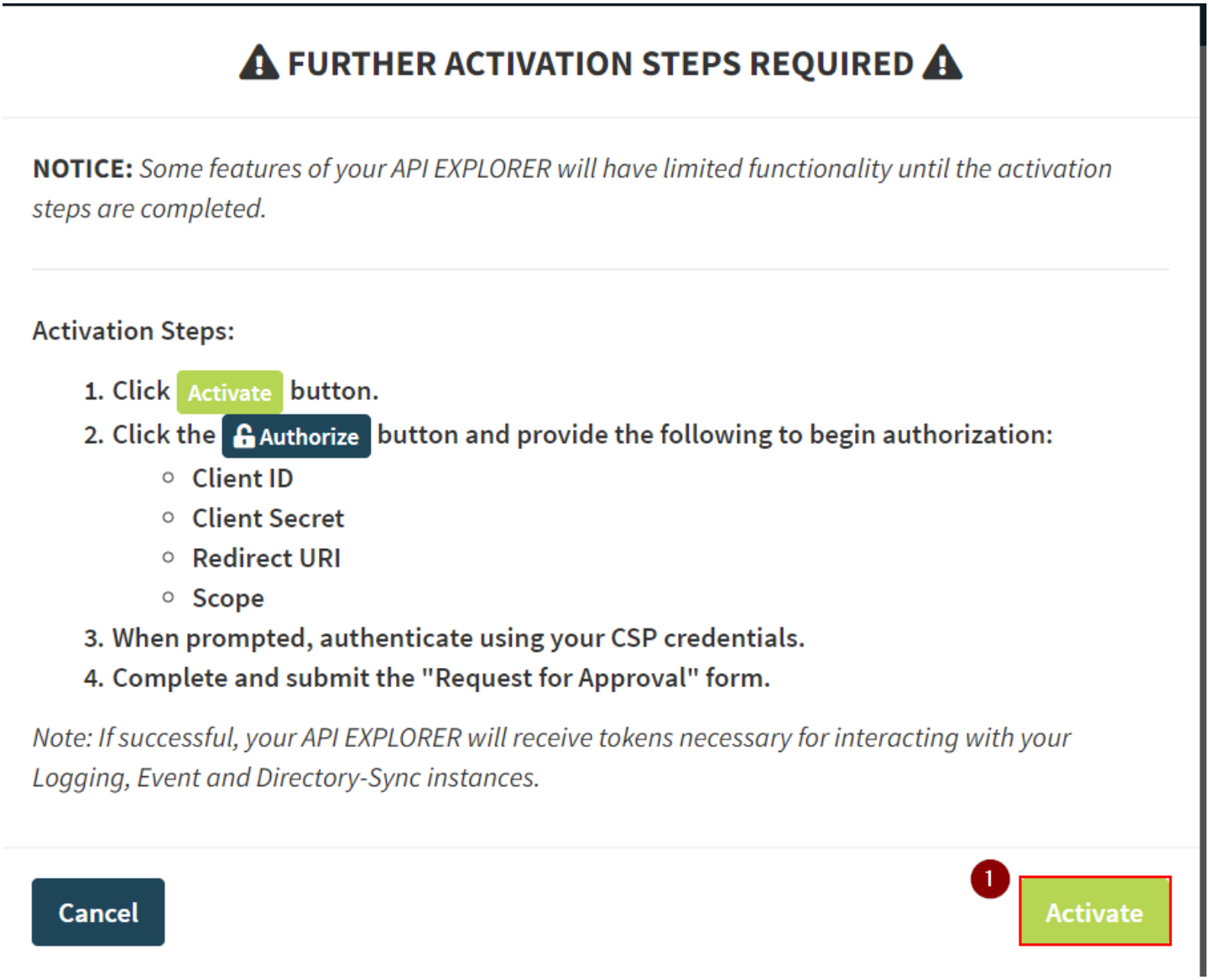
6. At this point you should see your "API Explorer" App in the **"Your Palo Alto Networks Cloud Services Apps"** section of the App Portal:



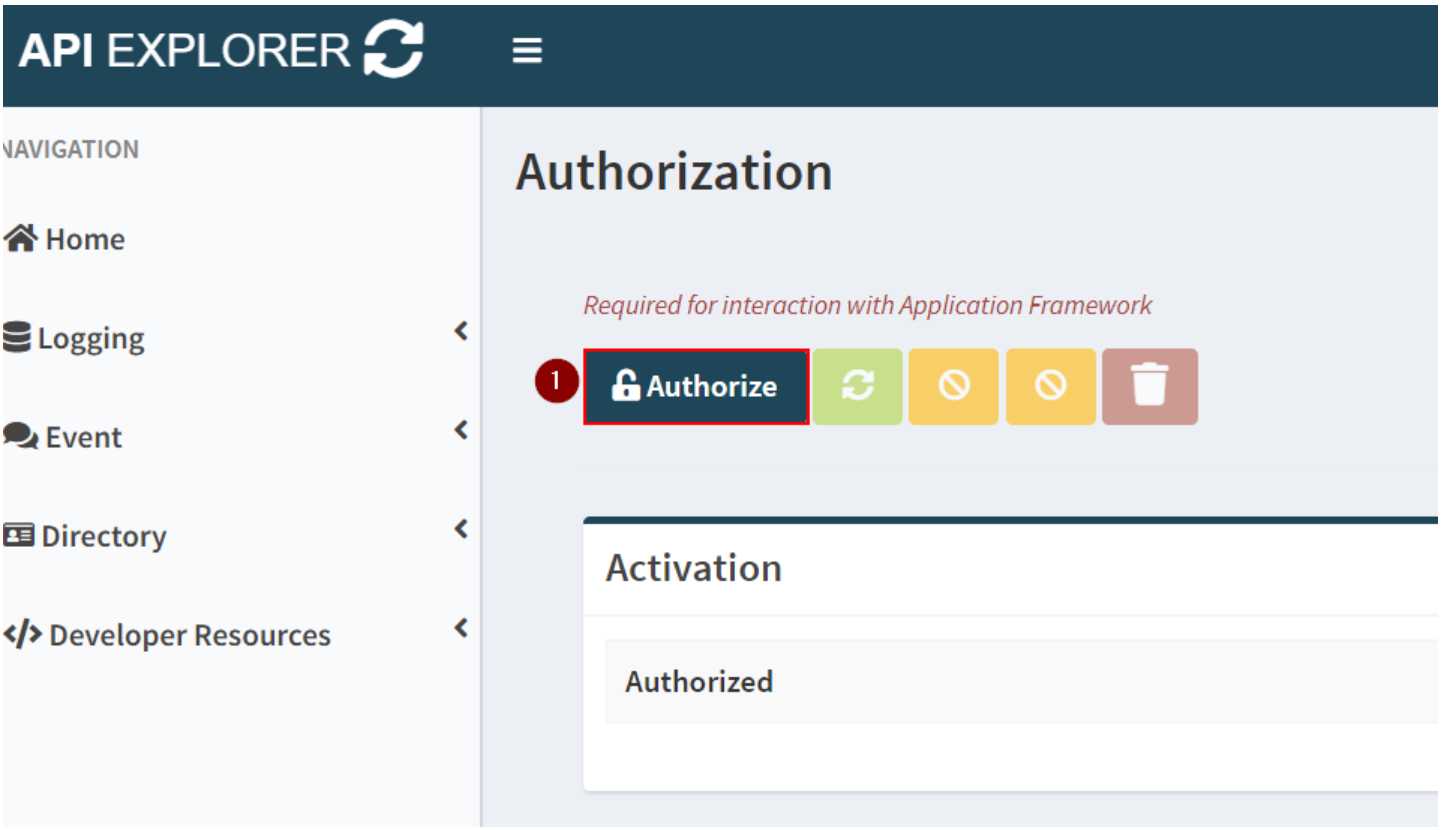
7. Click on your API Explorer App icon and you will be redirected to your API Explorer instance (the FQDN of your AWS instance). **Login** as **admin** (the password is the one you set as part of the CloudFormation Template parameters, same as Firewall and Panorama):



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



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



10. Insert the required parameters:

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

    > **Palo** Alto Networks technical contact

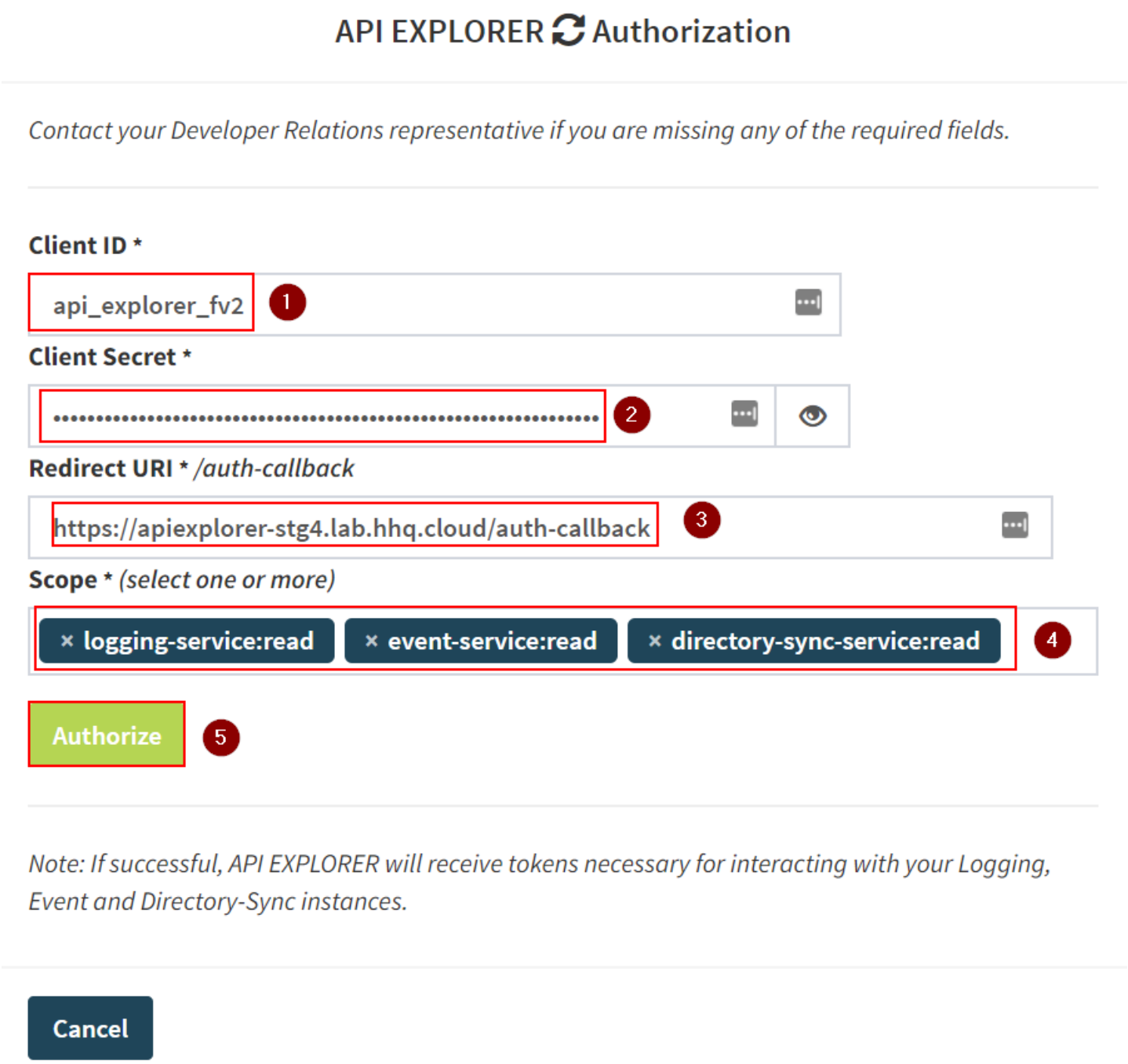
    b. Redirect URI should be correspond to your API Explorer instance

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

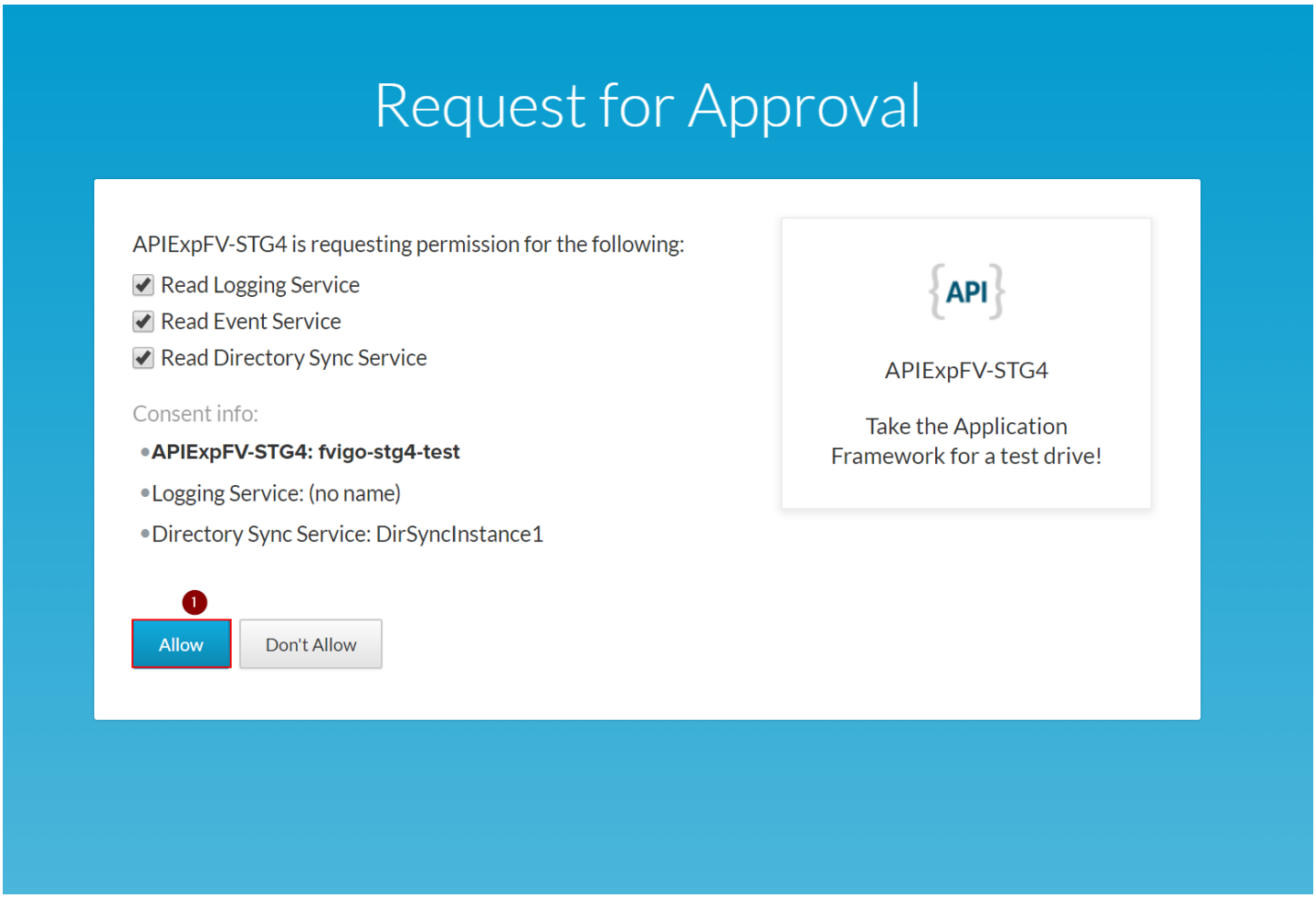
    c. Scope must be **logging-service:read** , **event-service:read**

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

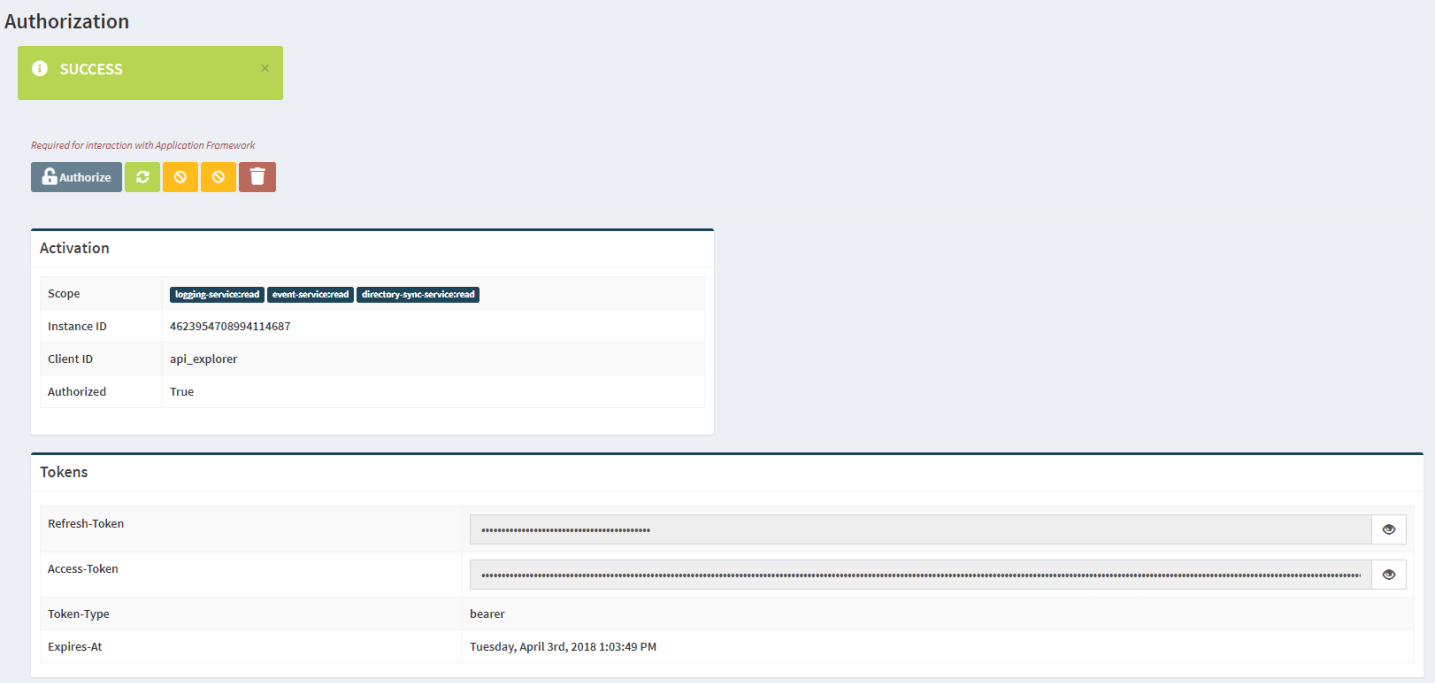
11. Click on **Authorize**:



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



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



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

###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

####Useful Commands:

[Run threats against web server]: # sudo uniscan -u http://10.0.0.100 -esqdwb

###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 VMthrough SSH (username is **ubuntu**)
- Use port 3389 to accessWindows Domain controller through RDP

###Next-Generation Firewall (NGFW)

Palo Alto Networks Next-Generation Firewall

Access directly with SSH privatekey 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 bereached through NGFW public interface (see above)

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

Access server with SSH private key through firewall mapped port221 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 butwon't restart at VM reboot). Configuration is in config.py

Restart the Web traffic Generatorwith 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.

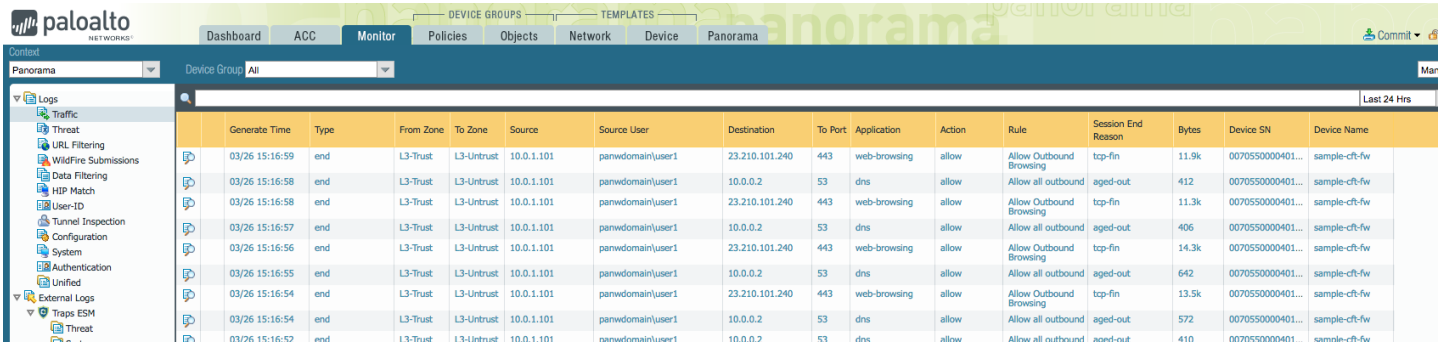
You can install the Directory Sync Service agent on this VM if you want to use it.

Appendix B: Default hostname to IP and VM Mapping

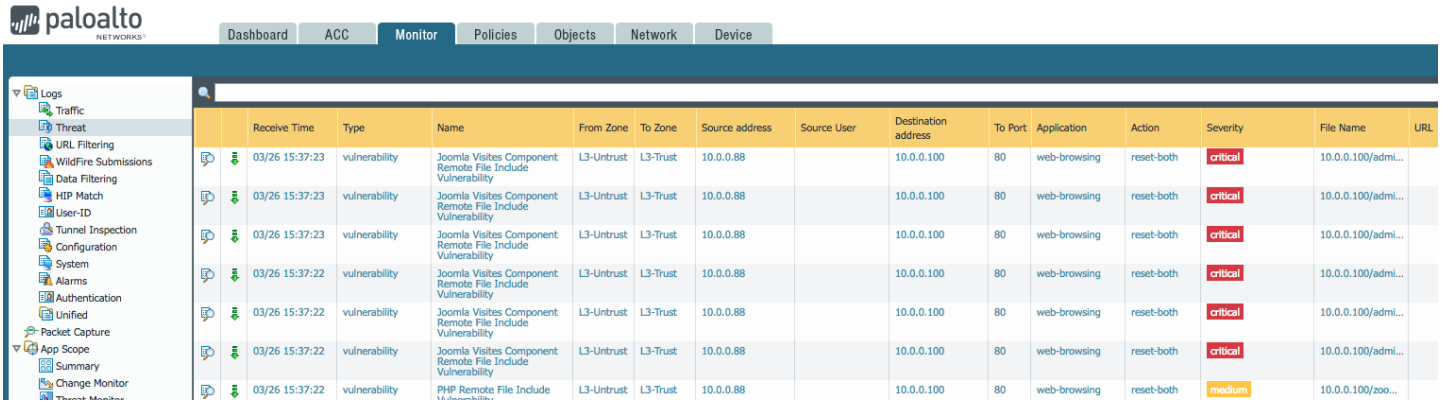
Public Hostname	Internal IP	EIP assigned?	VM
kali	10.0.0.88	Y	Kali Linux VM
apiexplorer	10.0.0.55	Y	API Explorer VM
public	10.0.0.100	Y	NGFW Public Interface
ngfw	10.0.0.99	Y	NGFW Management Interface
panorama	10.0.0.20	Y	Panorama Management Interface
N/A	10.0.1.101	N	Ubuntu Web Server VM
N/A	10.0.1.20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

Appendix C: Sample log outputs in the monitor tab

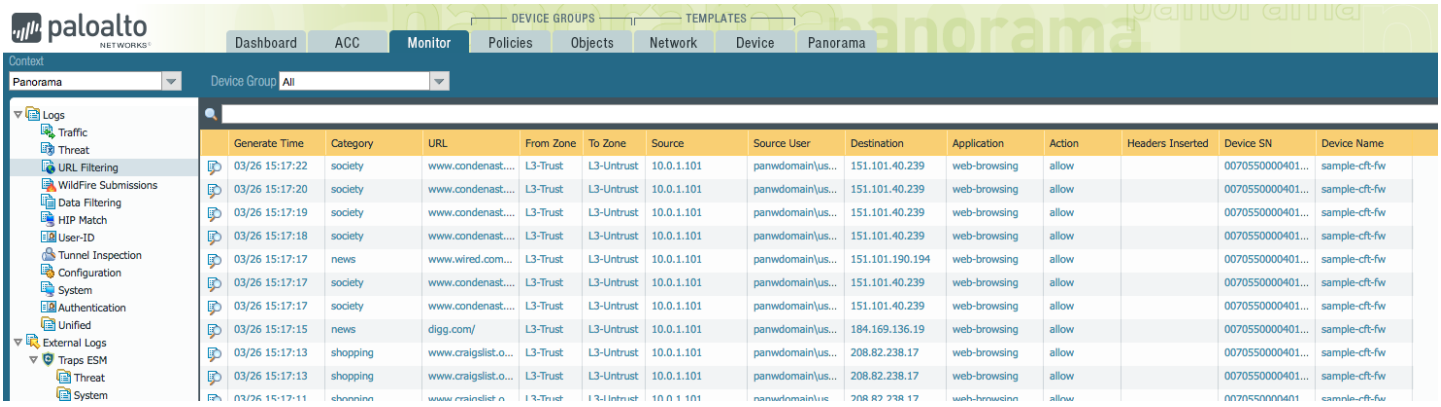
Traffic



Threat



URL Filtering



Copyright (C) 2018 - Palo Alto Networks, Inc.

Wildfire Submissions

Generate Time	File Name	URL	Source Zone	Destination Zone	Source address	Source User	Destination address	Desti... 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

Copyright (C) 2018 - Palo Alto Networks, Inc.