**Prisma - Twistlock**

Friday, June 7, 2024

8:58 AM

**Installing Prisma Twistlock:**

**---------------------------------------**

* AWS Account: **lz-dev**
* EKS Cluster: **sbx-eks-cluster**
* Prisma Twistlock Installation Document:
  + <https://github.com/jfrog/log-analytics-prometheus>

**Prisma Cloud Twistlock Dev Settings:**

**---------------------------------------------------**

<https://twistlock.sbx.lz.us-cert.gov/>

**Username:** admin

**Password:** TwistlockPassword1

**Download Latest Software:**

**--------------------------------------**

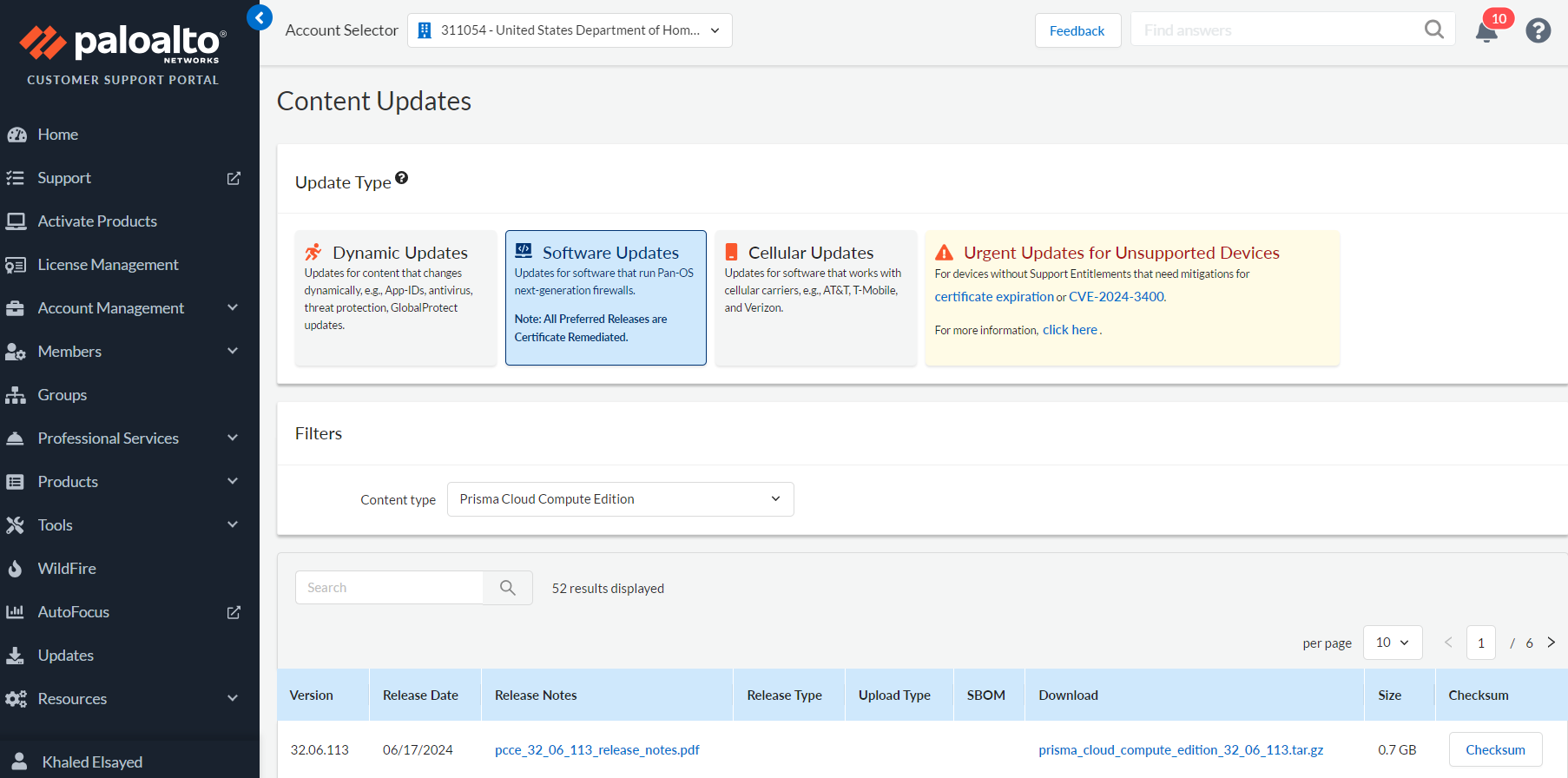
<https://support.paloaltonetworks.com/Updates/SoftwareUpdates/311054>

**Username:** khaled.elsayed@associates.cisa.dhs.gov

**Password:** Hanaa123456789@

**Product Content Type:** Prisma Cloud Compute Edition

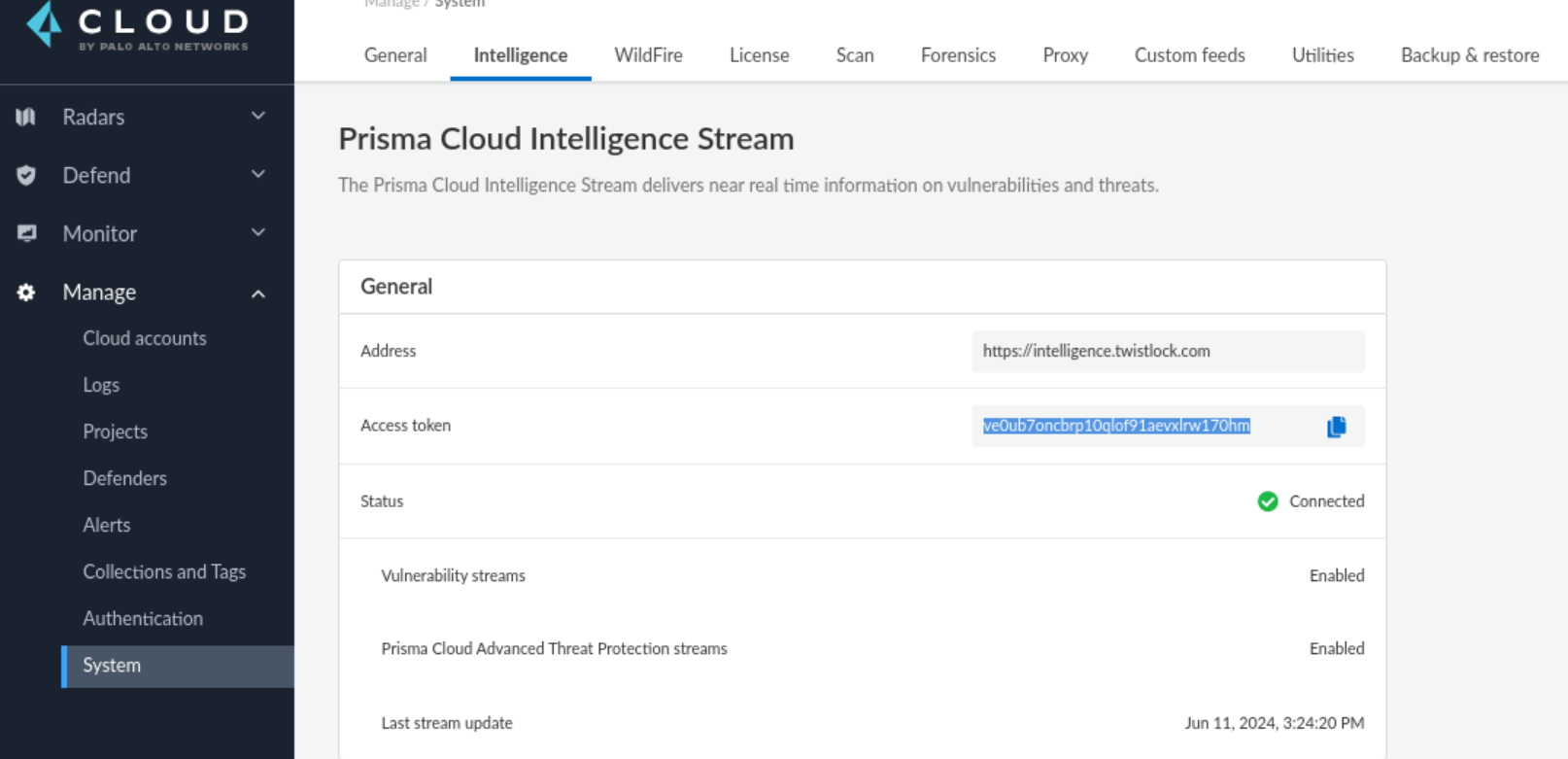
**Filename:** prisma\_cloud\_compute\_edition\_32\_06\_113.tar.gz



**Get the Access Token:**

**-------------------------------**

**Copy the Access Token to use it during the next step for generating the "twistlock\_console.yaml" configuration file.**



**Installation Steps:**

**-------------------------**

**Use the Access Token while running the command below, to generate the "twistlock\_console.yaml" configuration file.**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ linux/twistcli console export kubernetes --service-type LoadBalancer**

Enter access token (required for pulling the Console image):

Neither storage class nor persistent volume labels were provided, using cluster default behavior

**Saving output file to /home/khaled.elsayed/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files/twistlock\_console.yaml**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ ls -l**

total 1394784

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 243884 May 5 04:30 eula\_red\_hat\_universal\_base\_image.pdf

drwxr-xr-x 4 workspaces\khaled.elsayed workspaces\domain users 4096 Jun 11 12:19 linux

-r--r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 1180740 May 5 04:30 openapi.json

drwxr-xr-x 3 workspaces\khaled.elsayed workspaces\domain users 4096 May 5 04:30 osx

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 762375489 Jun 11 12:16 prisma\_cloud\_compute\_edition\_32\_05\_124.tar.gz

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 54445684 May 5 04:30 prisma-cloud-jenkins-plugin.hpi

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 771127 May 5 04:30 prisma-oss-licenses.txt

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 4211 May 5 04:30 twistlock.cfg

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 609101289 May 5 04:23 twistlock\_console.tar.gz

**-rw------- 1 workspaces\khaled.elsayed workspaces\domain users 7199 Jun 11 15:35 twistlock\_console.yaml**

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 34341 May 5 04:30 twistlock-license.pdf

-rwxr-xr-x 1 workspaces\khaled.elsayed workspaces\domain users 51751 May 5 04:30 twistlock.sh

drwxr-xr-x 2 workspaces\khaled.elsayed workspaces\domain users 4096 May 5 04:30 windows

**Check the Generated Configuration File:**

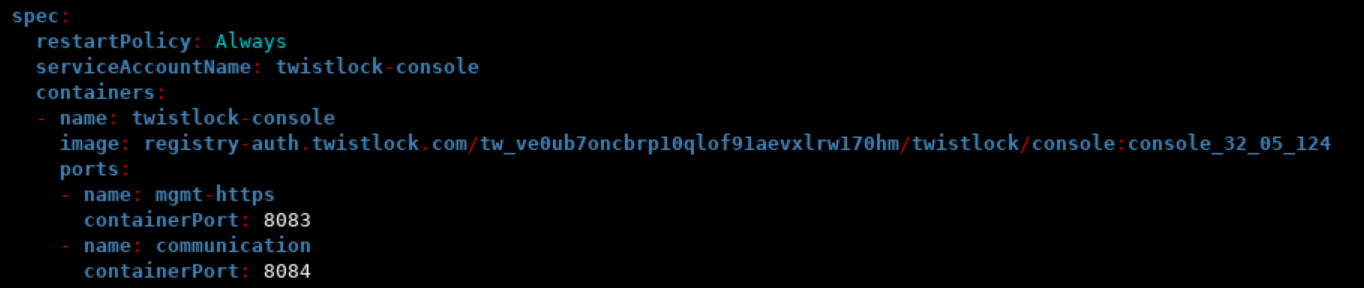
**--------------------------------------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ cat twistlock\_console.yaml**

**Make sure that token in the generated file is short like the one shown below.**

image: registry-auth.twistlock.com/**tw\_ve0ub7oncbrp10qlof91aevxlrw170hm**/twistlock/console:console\_32\_05\_124

The token should be the same copied from the Intelligence Section under



**Create a Copy of the Yaml Config File:**

**----------------------------------------------------**

**Make a copy before doing any changes to be able to restore it if needed.**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ cp twistlock\_console.yaml twistlock\_console\_copy.yaml**

**Change the Name of the Yaml Configuration File:**

**--------------------------------------------------------------------**

**Add the Environment Variable "sbx" Infront of the Configuration File.**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ mv twistlock\_console.yaml sbx\_twistlock\_console.yaml**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ ls -l**

total 1394792

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 243884 May 5 04:30 eula\_red\_hat\_universal\_base\_image.pdf

drwxr-xr-x 4 workspaces\khaled.elsayed workspaces\domain users 4096 Jun 11 12:19 linux

-r--r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 1180740 May 5 04:30 openapi.json

drwxr-xr-x 3 workspaces\khaled.elsayed workspaces\domain users 4096 May 5 04:30 osx

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 762375489 Jun 11 12:16 prisma\_cloud\_compute\_edition\_32\_05\_124.tar.gz

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 54445684 May 5 04:30 prisma-cloud-jenkins-plugin.hpi

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 771127 May 5 04:30 prisma-oss-licenses.txt

**-rw------- 1 workspaces\khaled.elsayed workspaces\domain users 7690 Jun 11 16:16 sbx\_twistlock\_console.yaml**

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 4211 May 5 04:30 twistlock.cfg

-rw------- 1 workspaces\khaled.elsayed workspaces\domain users 7199 Jun 11 15:59 twistlock\_console copy.yaml

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 609101289 May 5 04:23 twistlock\_console.tar.gz

-rw-r--r-- 1 workspaces\khaled.elsayed workspaces\domain users 34341 May 5 04:30 twistlock-license.pdf

-rwxr-xr-x 1 workspaces\khaled.elsayed workspaces\domain users 51751 May 5 04:30 twistlock.sh

drwxr-xr-x 2 workspaces\khaled.elsayed workspaces\domain users 4096 May 5 04:30 windows

**Update the following Section:**

**------------------------------------------**

**We need to update the following section in sbx\_twistlock\_console.yaml**

**Make sure you update the Loadbalancer CIDR Ranges, and Twistlock URL: twistlock.sbx.lz.us-cert.gov**

**From:**

```

apiVersion: v1

kind: Service

metadata:

labels:

name: console

name: twistlock-console

namespace: twistlock

spec:

ports:

- name: communication-port

port: 8084

- name: management-port-https

port: 8083

selector:

name: twistlock-console

type: LoadBalancer

```

**To:**

```

apiVersion: v1

kind: Service

metadata:

labels:

name: console

name: twistlock-console

namespace: twistlock

annotations:

external-dns.alpha.kubernetes.io/hostname: **twistlock.sbx.lz.us-cert.gov**

service.beta.kubernetes.io/aws-load-balancer-internal: 'true'

spec:

ports:

- name: communication-port

port: 8084

- name: management-port-https

port: 443

targetPort: 8083

selector:

name: twistlock-console

type: LoadBalancer

loadBalancerSourceRanges:

- 10.232.0.0/21

- 10.232.24.0/21

- 10.232.80.0/21

- 10.233.8.0/21

- 10.233.16.0/21

- 10.232.48.0/21

- 10.232.56.0/21

- 10.224.0.0/16

- 10.234.80.0/21

- 10.5.0.0/16

- 10.7.192.0/18

- 10.7.64.0/18

- 10.232.32.0/21

- 10.234.184.0/21

```

**Copy the "sbx\_twistlock\_console" to "twistlock\_prismacloud" Directory:**

**--------------------------------------------------------------------------------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud/Original\_Downloaded\_Files ❯ cp sbx\_twistlock\_console.yaml ../twistlock\_prismacloud**

**Make sure you are running in the Correct EKS Cluster:**

**--------------------------------------------------------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud ❯ kubectl config current-context**

sbx-eks-cluster

**Start the Kubernetes Installation:**

**-----------------------------------------------**

**Note that I didn't have to add "-n twistlock", because the "sbx\_twistlock\_console.yaml" file contains the configuration namespace: twistlock**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud ❯ kubectl create -f sbx\_twistlock\_console.yaml**

configmap/twistlock-console created

service/twistlock-console created

serviceaccount/twistlock-console created

persistentvolumeclaim/twistlock-console created

deployment.apps/twistlock-console created

Error from server (AlreadyExists): error when creating "**sbx\_twistlock\_console.yaml**": namespaces "**twistlock**" already exists

**Verify the Kubernetes Installation:**

**------------------------------------------------**

**The above installation results in creating ONLY One Pod for Twistlock, which is shown in Red.**

The other "**twistlock-defender**" **pods** were already there before the installation.

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ kubectl get pods -n twistlock**

NAME READY STATUS RESTARTS AGE

**twistlock-console-6dcc7fd579-7jk6n 1/1 Running 0 108s**

twistlock-defender-ds-t7vjp 0/1 ImagePullBackOff 0 9d

twistlock-defender-ds-wq4xb 0/1 ImagePullBackOff 0 9d

twistlock-defender-ds-zq7bf 0/1 ImagePullBackOff 0 9d

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock\_prismacloud ❯ kubectl get pods -n twistlock**

NAME READY STATUS RESTARTS AGE

**twistlock-console-6cd55dd4d6-m2vfz 1/1 Running 0 59s**

twistlock-defender-ds-7wdsm 1/1 Running 0 38d

twistlock-defender-ds-fqv7f 0/1 ImagePullBackOff 0 2d19h

twistlock-defender-ds-mnqxs 0/1 ImagePullBackOff 0 2d19h

twistlock-defender-ds-n5wl8 0/1 ImagePullBackOff 0 2d19h

twistlock-defender-ds-nvjx4 0/1 ImagePullBackOff 0 2d19h

twistlock-defender-ds-tkw6f 1/1 Running 0 55d

twistlock-defender-ds-wjclx 1/1 Running 0 55d

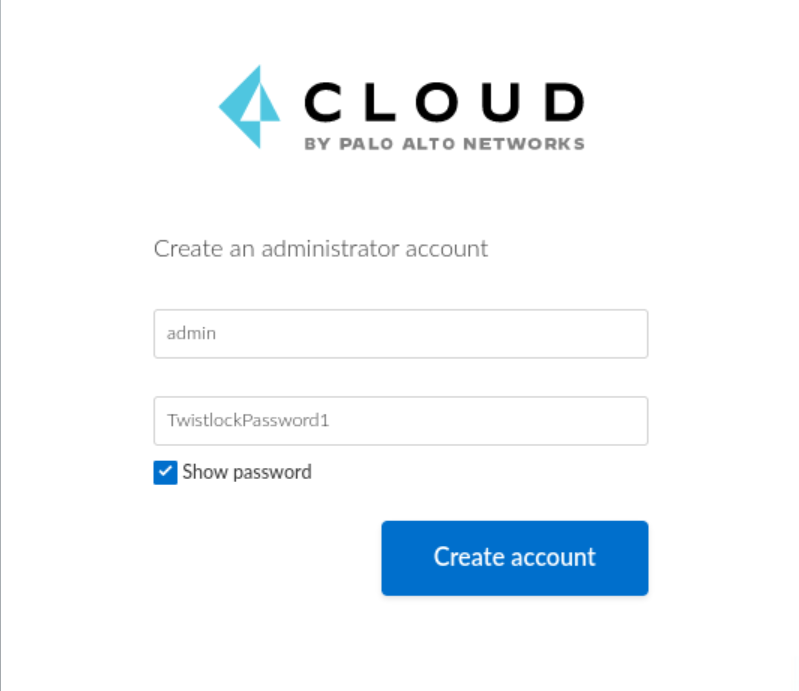
**Login to Twistlock URL:**

**----------------------------------**

<https://twistlock.sbx.lz.us-cert.gov/>

**Username:** admin

**Password:** TwistlockPassword1



**Reach out to Matt Jones to Get the License Key:**

**-------------------------------------------------------------------**

**File Location:** My Documents/DHS Certificates

**Filename:** TO9 - Prisma Cloud Compute - License Key.pdf

**Install the License Key**

hst0tkbf0O9ldgzws3rCGWBNjVsln6vpq5ABjenTbkNoYTBzzvCq1/rHakYq4bJALI+7D13BNisv6KbLM/NtS2lGD93d

LQbnFiqWIO7FlfDxw0qOFQdX32yayRxmo1g6KeAS6tglVroMMbUrCA0gfBMZX2DiEfb8UI14pVHQivRN4pBv2Nk

T7E8nVxoxOvC/NMpaWhLywey8hpNp1QkkQV+LFWn4+bOP5MsrL12lX8pYCW4gTL418RTjiTpa2pUqkAqngxVe

MbNWtxUHbLenmH6nxc8GDBGkdADms4nRD/09tGGmZdiJ4gdZ9zWuxtXZDcOdgfGF9vqKYLgc3aelfZN/wnKa++

vuMfvSbaEjnaldhdtyX8eoEpKi2e8uN1CDT7aEM/nGWOSe0XOOwbYG8mxESw9L0o1GgjkebX0w7a9vfDLnWthBm

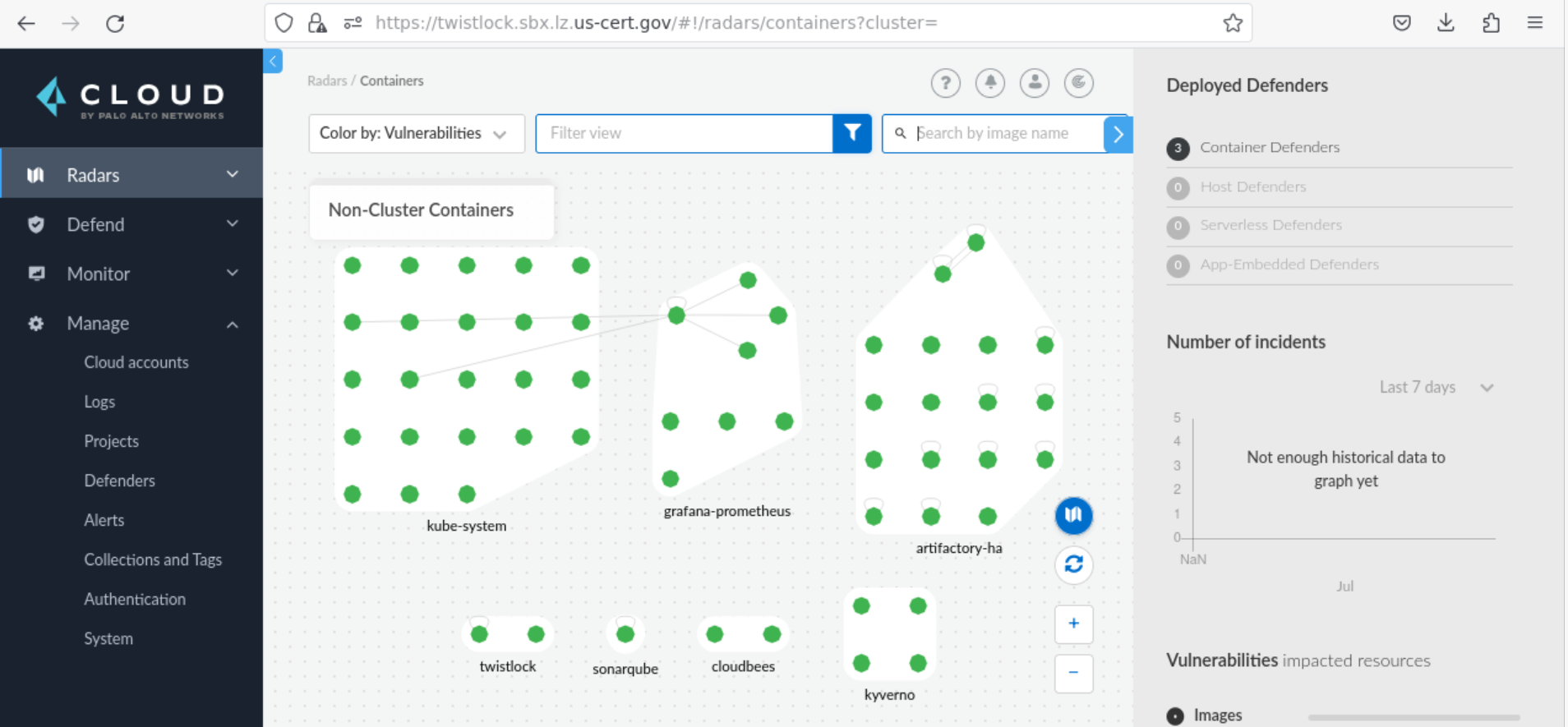
yW8+eMDSjUpj2X3IGvi7TGjaWV72DakWFWoKD4F5f17hLyR0Is2+GovGvYPZc+KXXOYMJpCb4jTiI5q5a1mSLD4

Cxcj2Z7G15k21OfSExEJv71CkgjIfM5ryg7RhA8veM6IuRfOd5EXJWNTGIvrXAJrAC95JnIfeDUSRCbEOhYGrRv12Jg

bQ0FVsKUsQJi0NeOGC0WUcqmcRd74z4G1/NKb63Jm3NCisP3p7GBcs7c1hxRoOarvOgY=

**Twistlock After Installing License Key:**

**----------------------------------------------------**



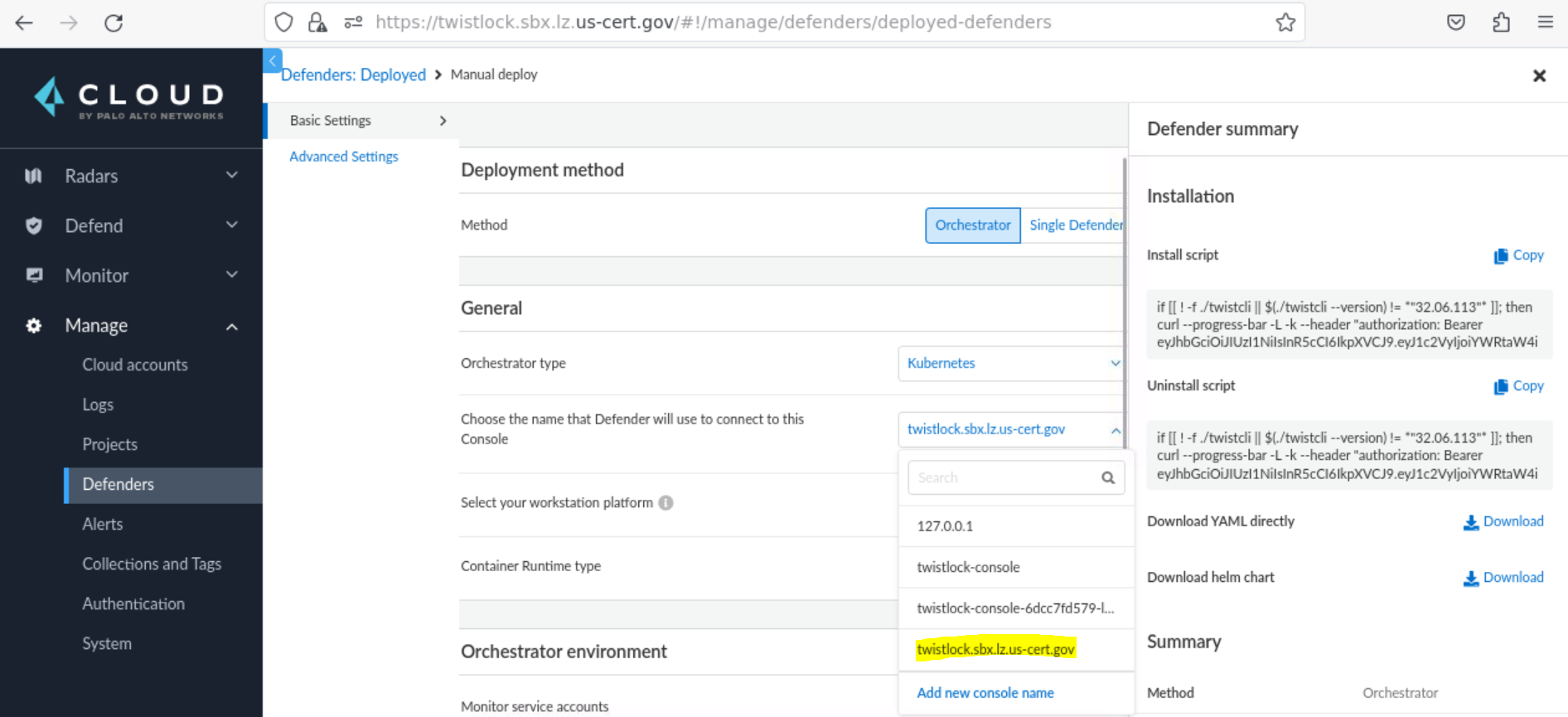
**Changing Domain Name:**

**-----------------------------------**

**Go to Manage --> Defenders --> Manual Deploy --> General --> Choose the name that Defender will use to connect to this Console.**

**Click "Add new console name"**

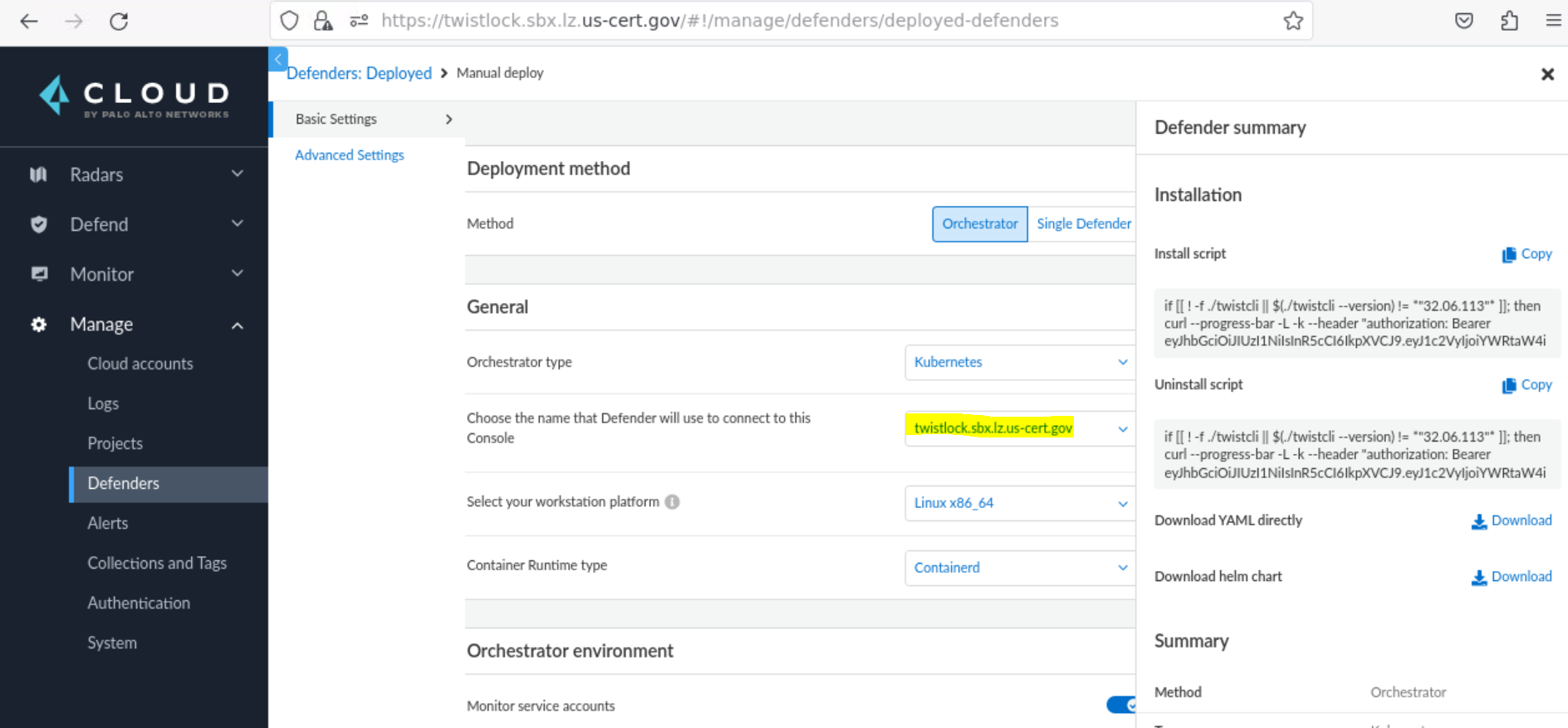
**New Console Name: twistlock.sbx.lz.us-cert.gov**



**Orchestrator Configuration:**

**----------------------------------------**

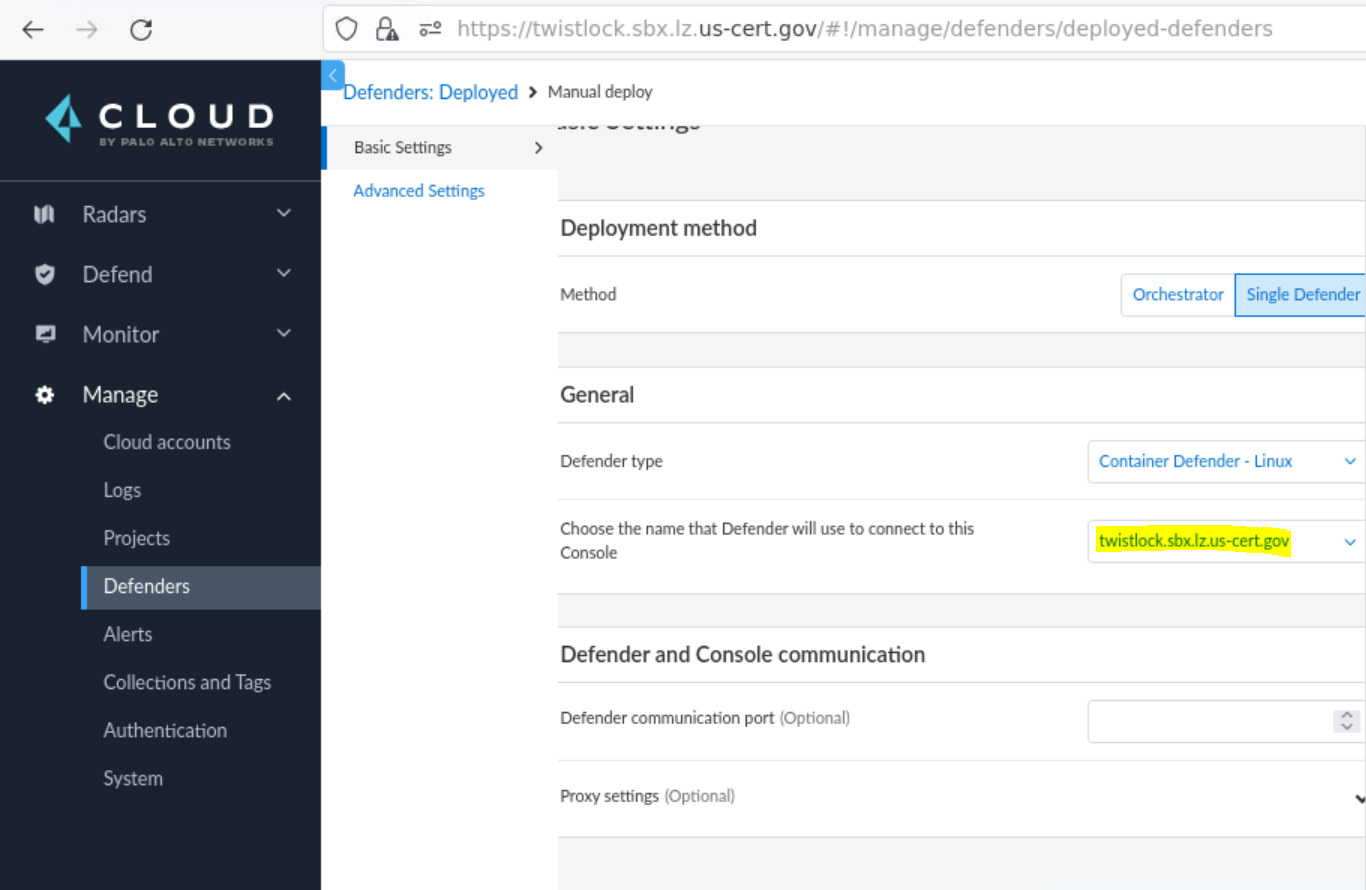
**Make sure that Orchestrator has this Console Name: twistlock.sbx.lz.us-cert.gov**



**Single Defender Configuration:**

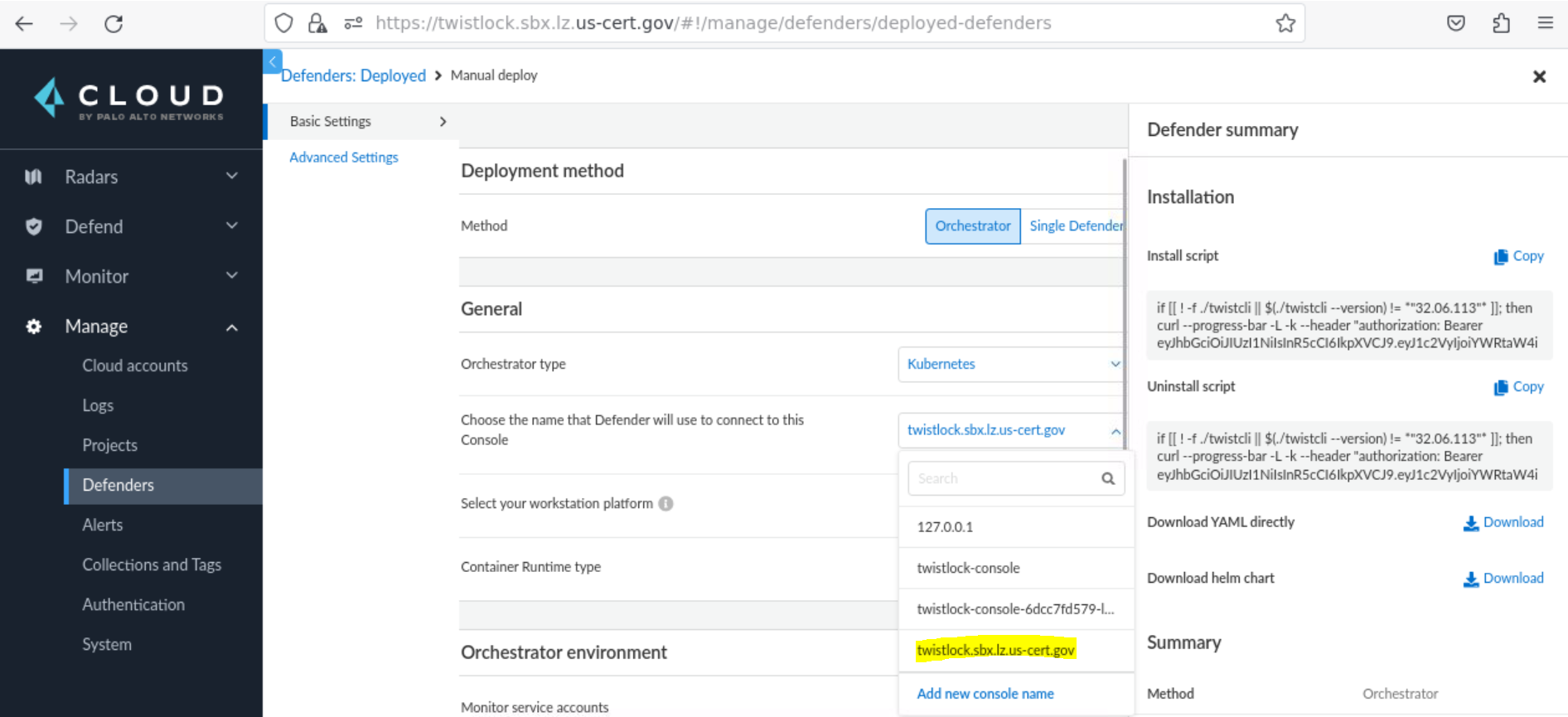
**--------------------------------------------**

**Make sure that Single Defender has the Same Console Name: twistlock.sbx.lz.us-cert.gov**



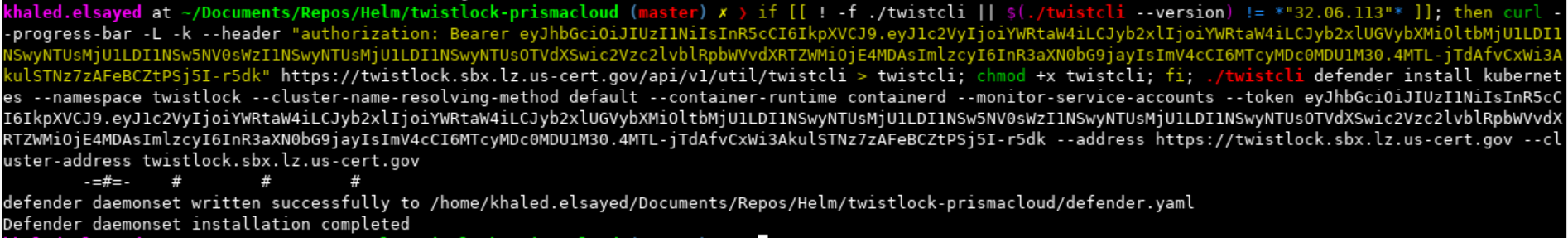
**Installing Defender:**

**----------------------------**



**Copy the Installation Script, and paste it into the Terminal:**

**---------------------------------------------------------------------------------**



**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯** if [[ ! -f ./twistcli || $(./twistcli --version) != \*"32.06.113"\* ]]; then curl --progress-bar -L -k --header "authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4iLCJyb2xlUGVybXMiOltbMjU1LDI1NSwyNTUsMjU1LDI1NSw5NV0sWzI1NSwyNTUsMjU1LDI1NSwyNTUsOTVdXSwic2Vzc2lvblRpbWVvdXRTZWMiOjE4MDAsImlzcyI6InR3aXN0bG9jayIsImV4cCI6MTcyMDc0MDU1M30.4MTL-jTdAfvCxWi3AkulSTNz7zAFeBCZtPSj5I-r5dk" <https://twistlock.sbx.lz.us-cert.gov/api/v1/util/twistcli> > twistcli; chmod +x twistcli; fi; ./twistcli defender install kubernetes --namespace twistlock --cluster-name-resolving-method default --container-runtime containerd --monitor-service-accounts --token eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJ1c2VyIjoiYWRtaW4iLCJyb2xlIjoiYWRtaW4iLCJyb2xlUGVybXMiOltbMjU1LDI1NSwyNTUsMjU1LDI1NSw5NV0sWzI1NSwyNTUsMjU1LDI1NSwyNTUsOTVdXSwic2Vzc2lvblRpbWVvdXRTZWMiOjE4MDAsImlzcyI6InR3aXN0bG9jayIsImV4cCI6MTcyMDc0MDU1M30.4MTL-jTdAfvCxWi3AkulSTNz7zAFeBCZtPSj5I-r5dk --address <https://twistlock.sbx.lz.us-cert.gov> --cluster-address twistlock.sbx.lz.us-cert.gov

-=#=- # # #

**defender daemonset written successfully to /home/khaled.elsayed/Documents/Repos/Helm/twistlock-prismacloud/defender.yaml**

**Defender daemonset installation completed**

**Verify Defender Installation:**

**----------------------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ kubectl get pods -n twistlock**

NAME READY STATUS RESTARTS AGE

twistlock-console-6dcc7fd579-lzgv9 1/1 Running 0 18m

twistlock-defender-ds-6q2sp 1/1 Running 0 110s

twistlock-defender-ds-b2c97 1/1 Running 0 110s

twistlock-defender-ds-swkkh 1/1 Running 0 110s

**Download and Read the "daemonset.yaml" YAML File from Defender Side Page:**

**--------------------------------------------------------------------------------------------------------------**



**Apply the Downloaded YAML File for Defender Installation:**

**------------------------------------------------------------------------------------**

**khaled.elsayed at ~/Downloads ❯ kubectl apply -f daemonset.yaml -n twistlock**

clusterrole.rbac.authorization.k8s.io/twistlock-view unchanged

clusterrolebinding.rbac.authorization.k8s.io/twistlock-view-binding configured

secret/twistlock-secrets configured

serviceaccount/twistlock-service unchanged

daemonset.apps/twistlock-defender-ds configured

service/defender unchanged

**Verify Defender Installation Completion:**

**--------------------------------------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ kubectl get pods -n twistlock**

NAME READY STATUS RESTARTS AGE

twistlock-console-6dcc7fd579-lzgv9 1/1 Running 0 18m

twistlock-defender-ds-6q2sp 1/1 Running 0 110s

twistlock-defender-ds-b2c97 1/1 Running 0 110s

twistlock-defender-ds-swkkh 1/1 Running 0 110s

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ kubectl get all -n twistlock**

NAME READY STATUS RESTARTS AGE

pod/twistlock-console-6dcc7fd579-lzgv9 1/1 Running 0 24m

pod/twistlock-defender-ds-76tlj 1/1 Running 0 66s

pod/twistlock-defender-ds-7st26 1/1 Running 0 68s

pod/twistlock-defender-ds-gwtnd 1/1 Running 0 70s

NAME TYPE CLUSTER-IP EXTERNAL-IP PORT(S) AGE

service/defender ClusterIP 172.20.60.10 <none> 443/TCP 7m2s

service/twistlock-console LoadBalancer 172.20.77.23 internal-a9ed48e4c670a4e6ab14a61e22c9c82e-1549141418.us-gov-west-1.elb.amazonaws.com 8084:31471/TCP,443:31383/TCP 24m

NAME DESIRED CURRENT READY UP-TO-DATE AVAILABLE NODE SELECTOR AGE

daemonset.apps/twistlock-defender-ds 3 3 3 3 3 <none> 7m2s

NAME READY UP-TO-DATE AVAILABLE AGE

deployment.apps/twistlock-console 1/1 1 1 24m

NAME DESIRED CURRENT READY AGE

replicaset.apps/twistlock-console-6dcc7fd579 1 1 1 24m

**Install the TLS Certificate inside Twistlock:**

**----------------------------------------------------------**

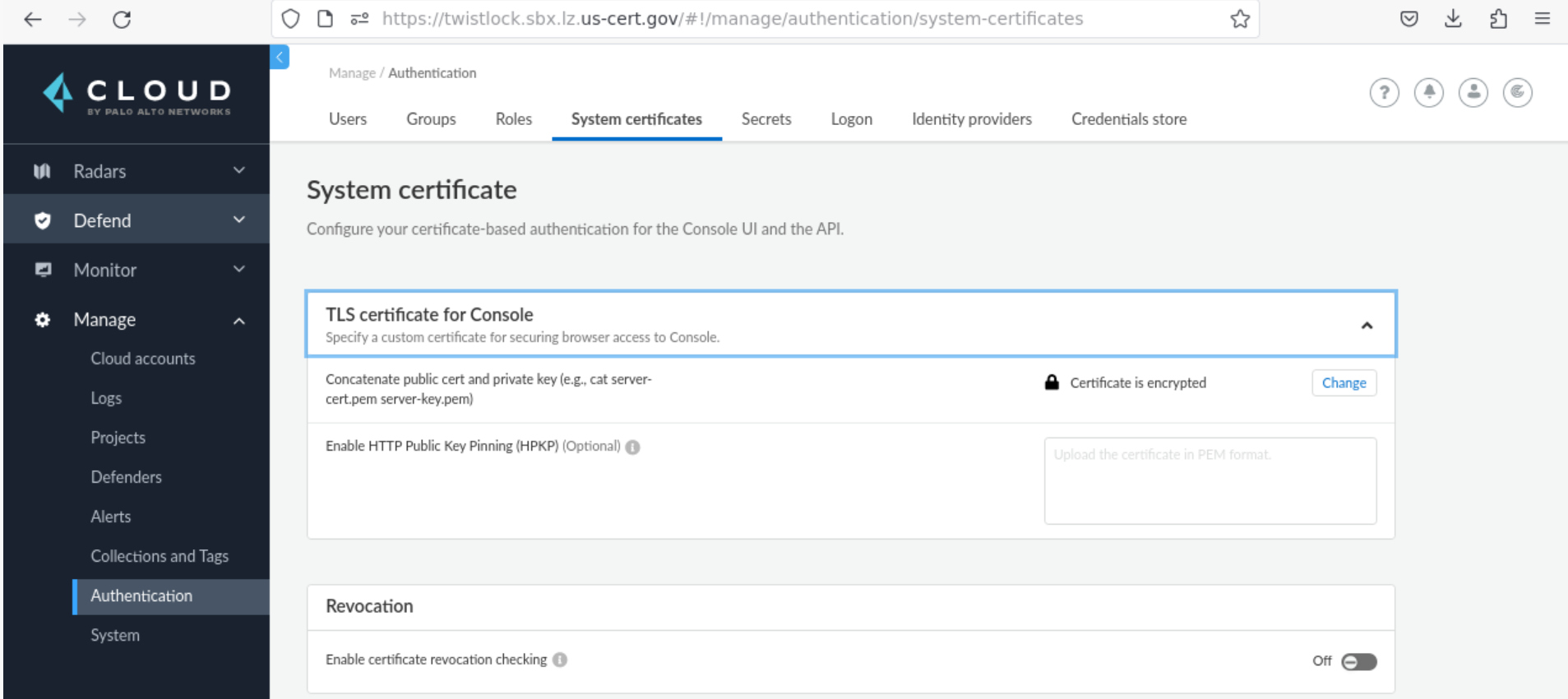
The **TLS Certificate** is the **Same** as the **DHS Certificate** that are created by **James Nguyen**

You need to move them to Amazon Workspace, Then you **install** them in the **following order. Key First Then the Pem Certificate.**

Then, Copy everything and Paste it inside the Twistlock Console.

**khaled.elsayed at ~/Downloads ❯ cat lz-twistlock-dev.key lz-twistlock-dev.pem**





**SAML Integration:**

**--------------------------**

**This happens through the Network and Access Art (NAART)**

**Send an E-mail to the following people to start the SAML integration process.**

**Technical People:**

* Keller, Robert (CTR) <ROBERT.KELLER@associates.cisa.dhs.gov>
* Heah, Nicholas (CTR) <nicholas.heah@associates.cisa.dhs.gov>
* Bonner, Lamarris (CTR) <lamarris.bonner@associates.cisa.dhs.gov>

**Product Owner & Proxy Product Owner:**

* **Government Lead:**
  + RAYMOND.PIERCE@cisa.dhs.gov
  + Crawford, Annamarie <annamarie.crawford@cisa.dhs.gov>
* **Proxy Product Owner**
  + Willars, Matthew (CTR) <matthew.willars@associates.cisa.dhs.gov>

**Scrum Masters:**

* Ngwa, Benjamin (CTR) <BENJAMIN.NGWA@associates.cisa.dhs.gov>
* Gupta, Gyanendra (CTR) <GYANENDRA.GUPTA@associates.cisa.dhs.gov>

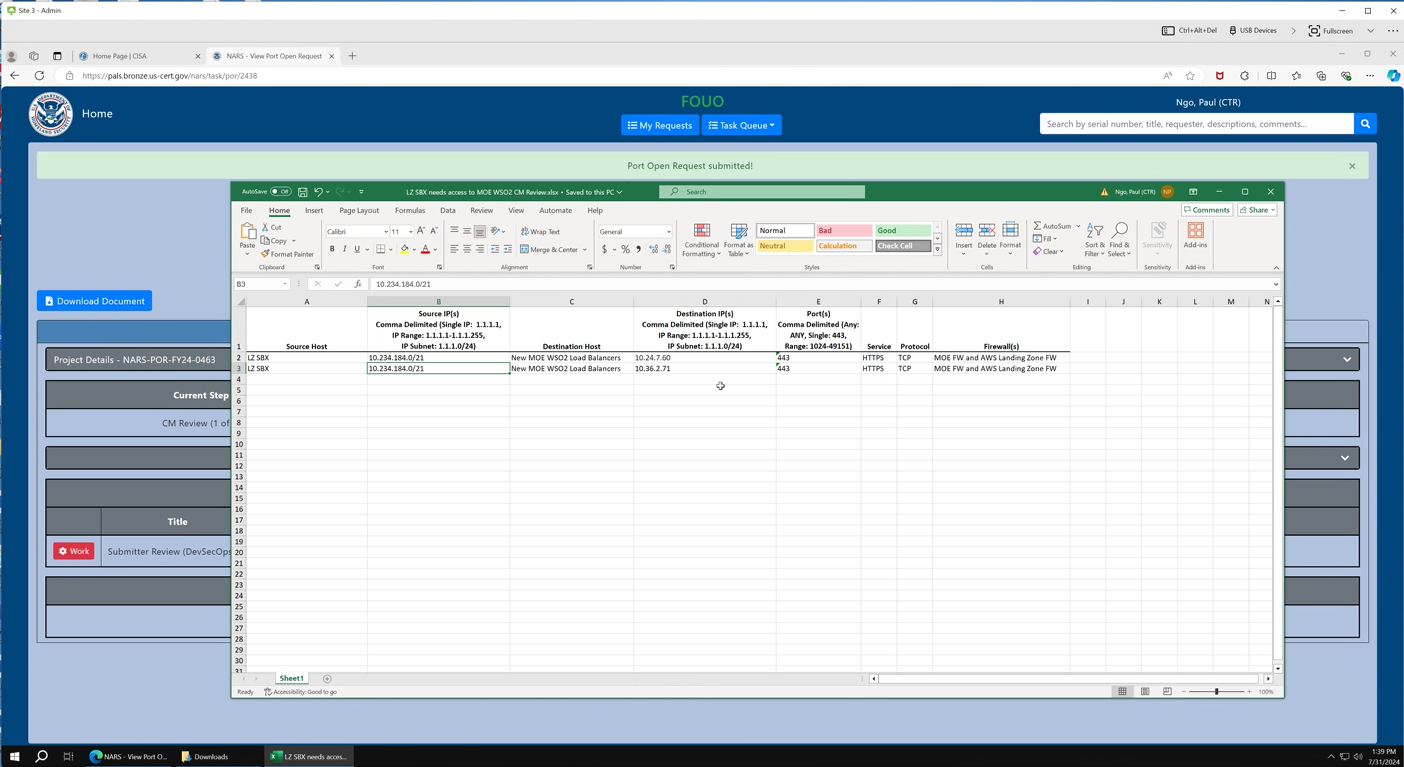
**We should ask them to help us in integrating the Pipeline Services in the SBX environment with the WSO2 SSO.**

**SAML Integration Process:**

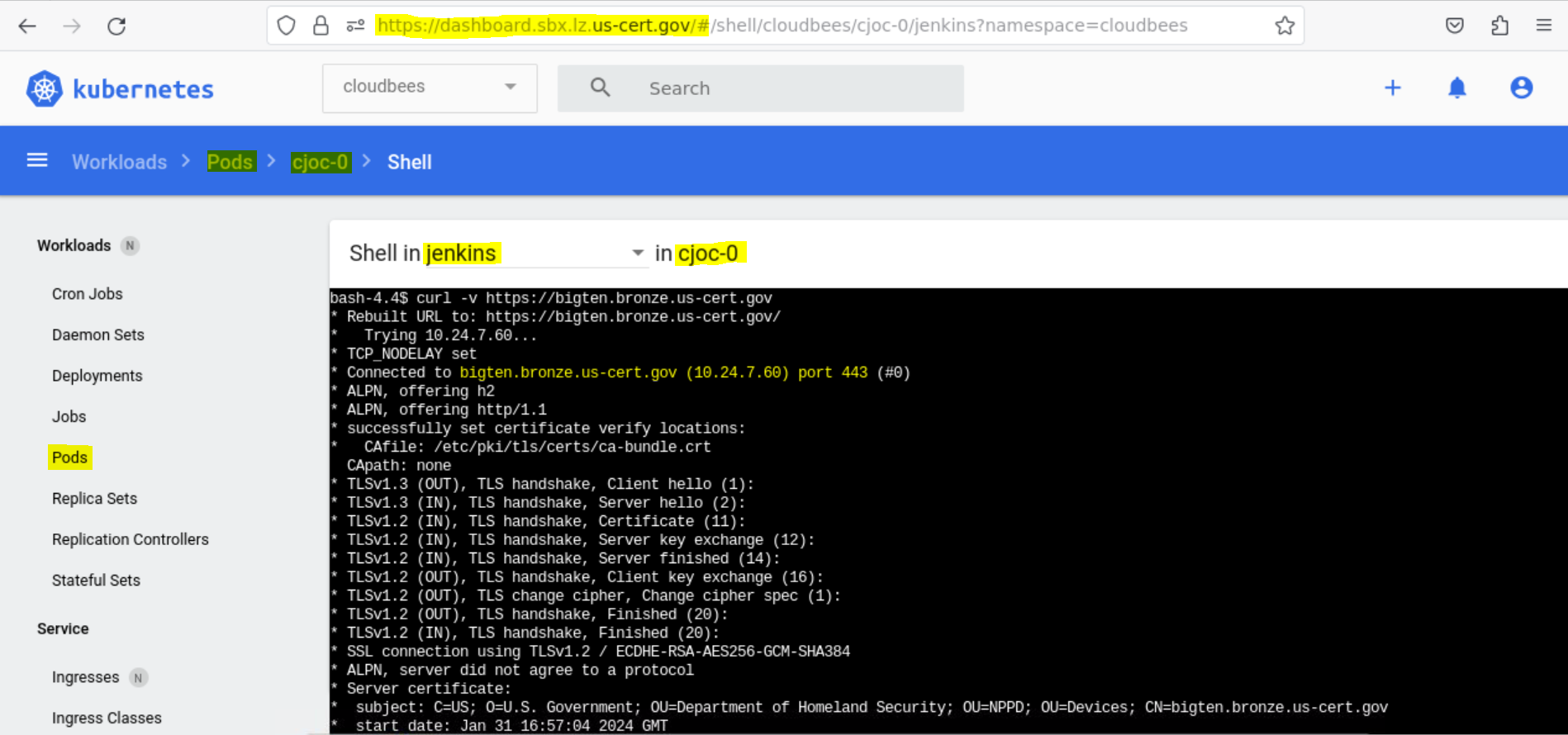
**-------------------------------------**

**We only need to submit this POR Request ONCE for All DevSecOps Services.**

1. **Submit a Port Open Request (POR) for All DevSecOps Services to open port 443 as shown below.**
2. **The POR Request need to have the following inputs in a Spreadsheet as shown below.**
   1. **Source Host: LZ SBX**
   2. **Source IP Address: 10.234.184.0/21**
      1. **This is the CIDR IP Range for the VPC that hosts all DevSecOps services in the lz-dev AWS account.**
   3. **Destination Host: New MOE WSO2 Load Balancers**
   4. **Destination IP Addresses:**
      1. **10.24.7.60**
         * **This is the IP Address of the SAML Integration Server in the MOE.**
      2. **10.36.2.71**
         * **This is the IP Address of the SAML Integration Server in the MOE.**
   5. **Port: 443**
   6. **Service: HTTPS**
   7. **Protocol: TCP**
   8. **Firewall: MOE FW and AWS Landing Zone FW**



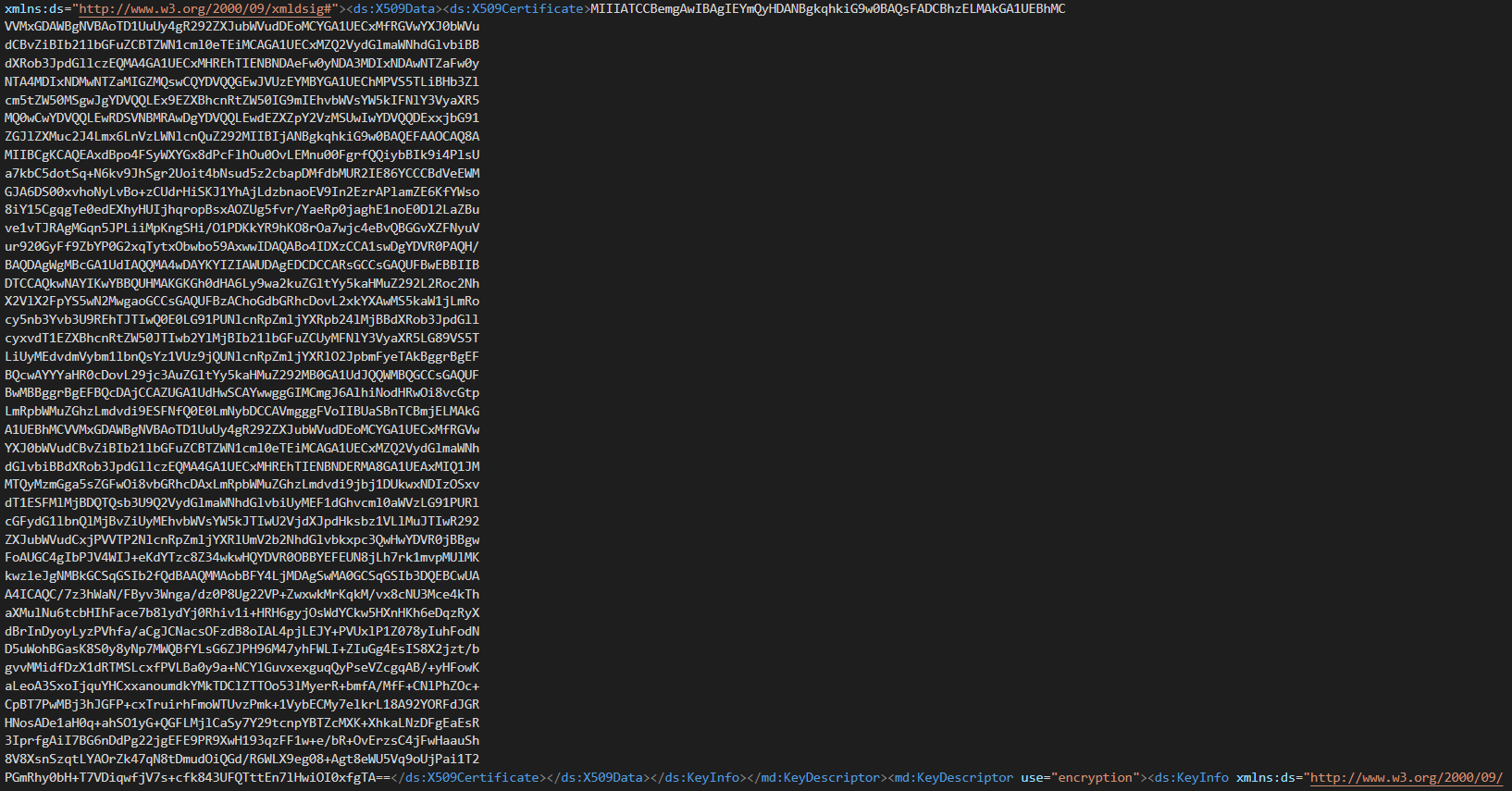
1. **Verify that Port "443" has been opened after the POR request has been completed**



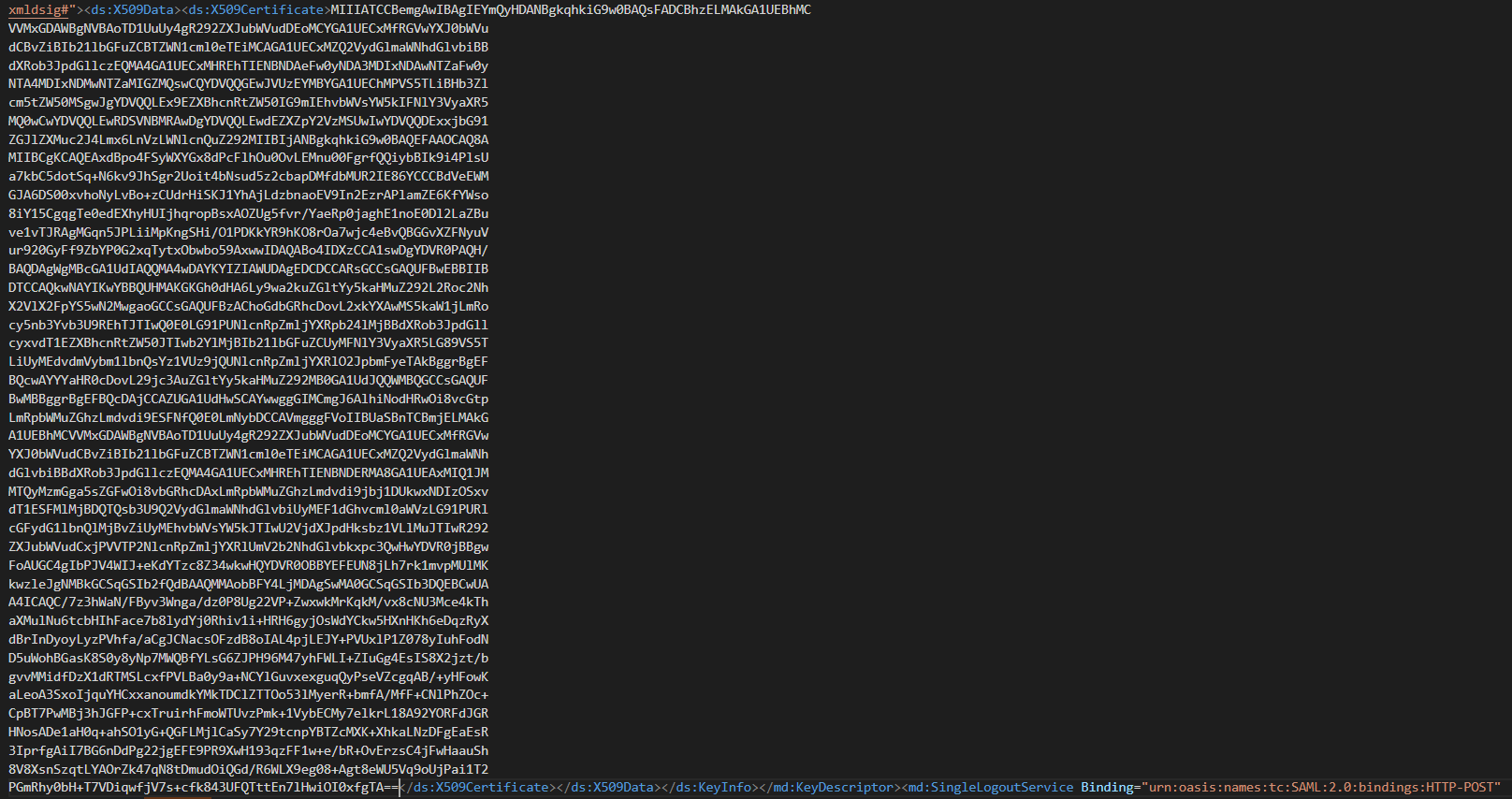
1. **Update the Metadata File for Twistlock DevSecOps service with the following inputs**

1. **Update the URL for Cloudbees Service**
   1. [**https://twistlock.sbx.lz.us-cert.gov**](https://twistlock.sbx.lz.us-cert.gov)

1. **Update the DHS Certificate for Twistlock Service**
   1. **This is the Same DHS Certificate that is being installed in lz-dev account in AWS Certificate Manager.**



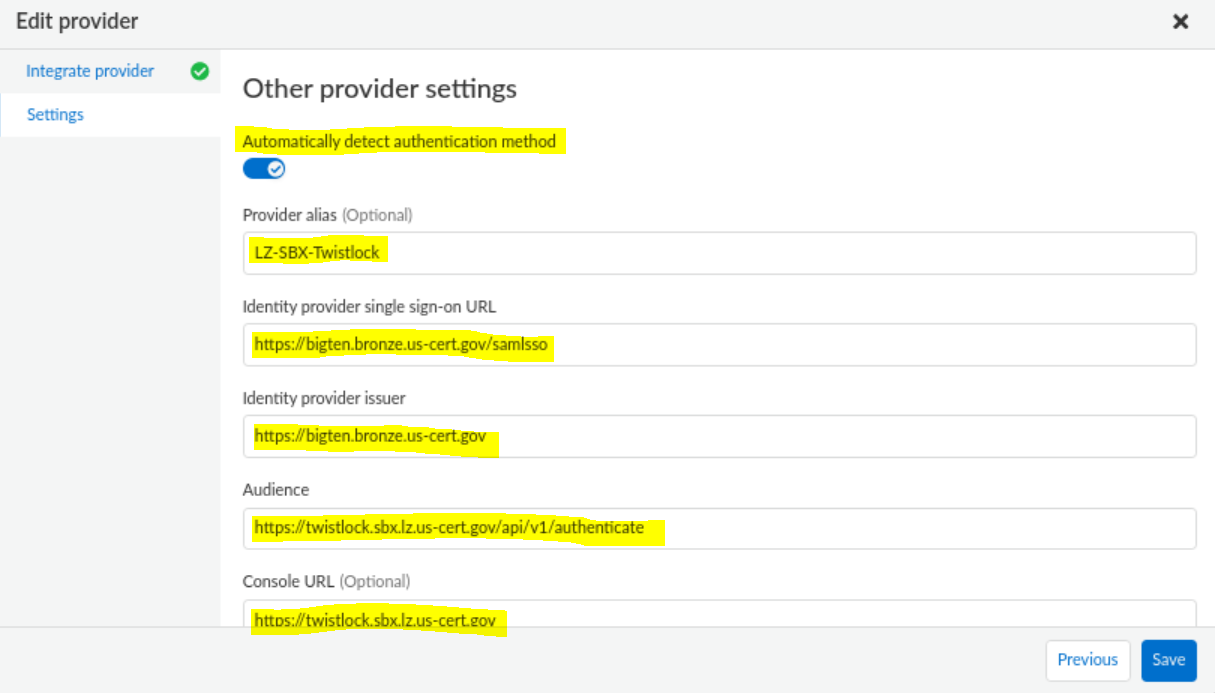
1. **Update the DHS Certificate of Twistlock Service in the Second Section as well.** 
   1. **Note that we use the Public Certificate in both sections. The Certificate Key is NOT used at all.**

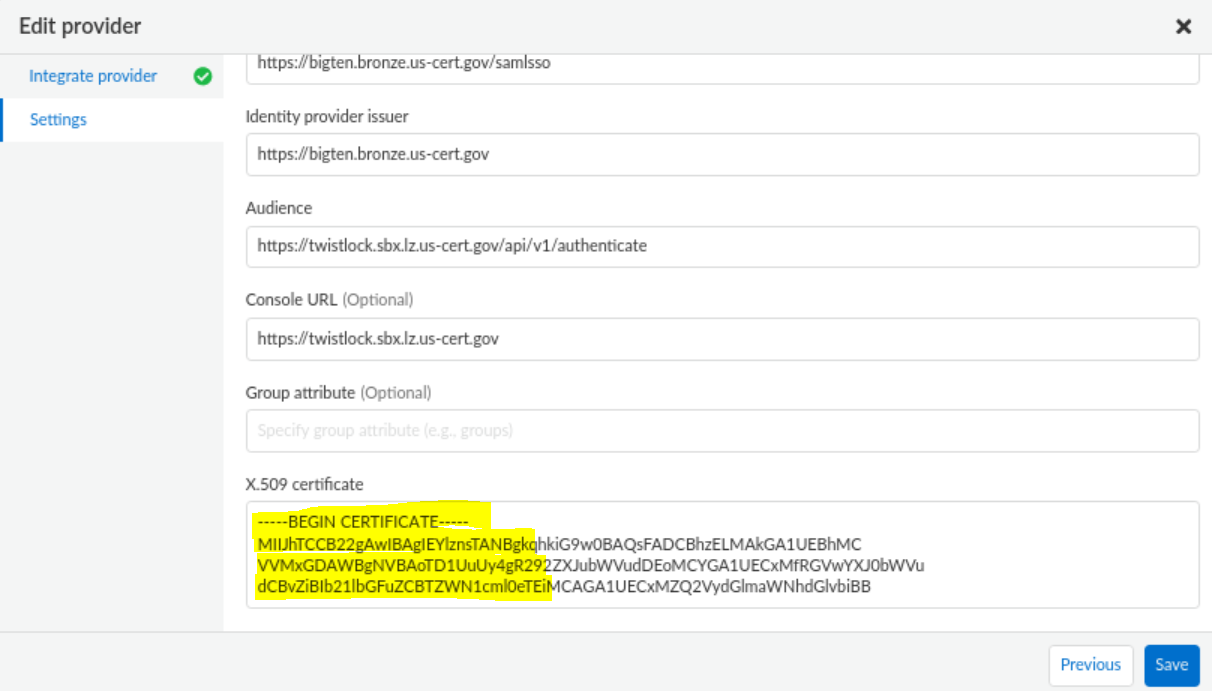


1. **Follow this Document to configure SAML for each Service.** 
   1. [**https://confluence.brass.us-cert.gov/display/POPTART/LZ+Pipeline+Service+Integration+with+SSO+-+WSO2**](https://confluence.brass.us-cert.gov/display/POPTART/LZ+Pipeline+Service+Integration+with+SSO+-+WSO2)

1. **Configure WSO2 Identity provider in Twistlock**

* Login Twistlock as an **administrator** → **Manage** → **Authentication** → **Identity providers** → **Add Provider**
* **Provider alias: LZ-SBX-Twistlock**
* **Identity provider single sign-on URL:** [**https://bigten.bronze.us-cert.gov/samlsso**](https://bigten.bronze.us-cert.gov/samlsso)
* **Identity provider issuer:** [**https://bigten.bronze.us-cert.gov**](https://bigten.bronze.us-cert.gov)
* **Audience:** [**https://twistlock.pb.lz.us-cert.gov/api/v1/authenticate**](https://twistlock.pb.lz.us-cert.gov/api/v1/authenticate)
* **Console URL:** [**https://twistlock.pb.lz.us-cert.gov**](https://twistlock.pb.lz.us-cert.gov)
* **X.509 certificate:** 
  + **Copy & Paste Certificate from the following file.**
  + **Location:** Desktop\SAML Integration\SBX\**bigtenpref5 - SAML Certificate Insterted inside Cloudbees SBX.xml**





**Configure Twistlock SBX to use Zscaler Certificates instead of LZ-Proxy:**

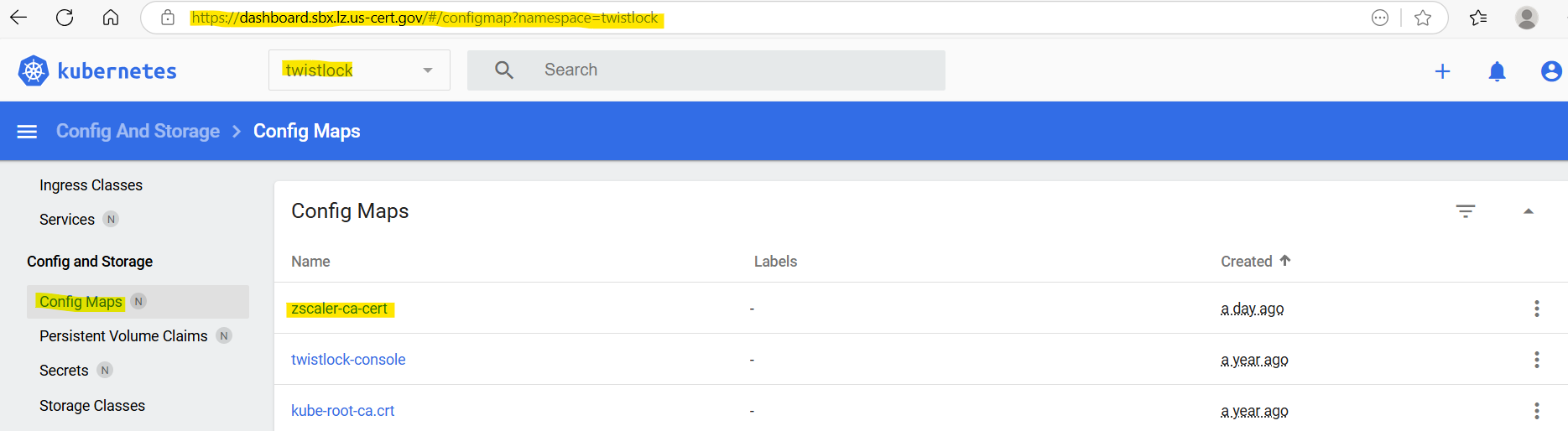
**------------------------------------------------------------------------------------------------**

**1- Create a filename of "zscaler.crt", which includes all the 4 zscaler certificates inside your Redhat Workspace.**

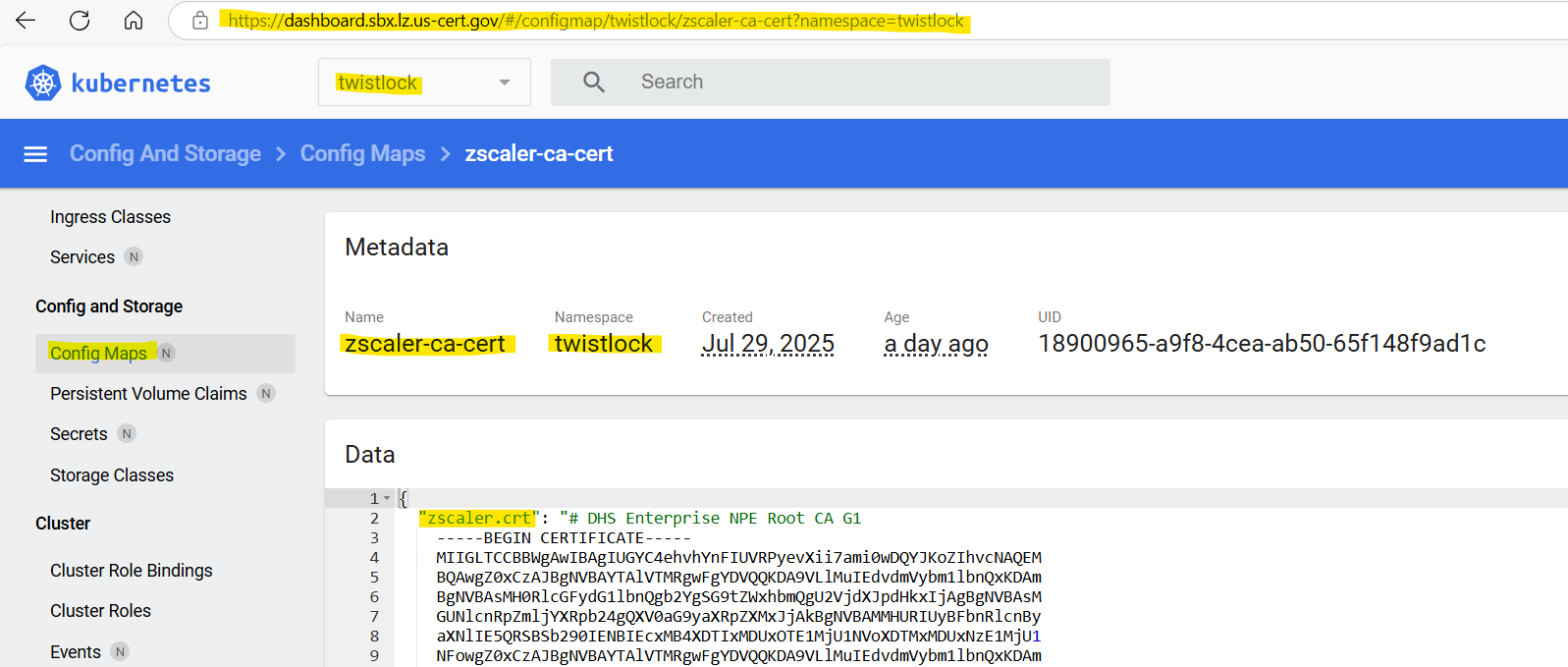
**2- Then, Create the Configmap for "zscaler-ca-cert" from this file "zscaler.crt".**

**khaled.fouad ~/Documents/Repos ❯ kubectl create configmap zscaler-ca-cert --from-file=zscaler.crt -n twistlock**

**configmap/zscaler-ca-cert created**



**The Configmap "zscaler-ca-cert" is created from this filename "zscaler.crt" as shown below.**



**3- Add the following configurations inside Twistlock-Console Deployment:**

* **Add a new volume for "zscaler-ca-volume" with Configmap of " zscaler-ca-cert"**

**spec:**

**volumes:**

- name: console-persistent-volume

persistentVolumeClaim:

claimName: twistlock-console

- name: twistlock-config-volume

configMap:

name: twistlock-console

defaultMode: 420

- name: syslog-socket

hostPath:

path: /dev/log

type: ''

**- name: zscaler-ca-volume**

**configMap:**

**name: zscaler-ca-cert**

**defaultMode: 420**

* **Add a new env for "SSL\_CERT\_FILE" with value of "/certs/zscaler.crt"**

**env:**

- name: CONFIG\_PATH

value: /data/config/twistlock.cfg

- name: INTELLIGENCE\_FEEDS\_FOLDER

value: /var/lib/twistlock/saas\_feeds

- name: LOG\_PROD

value: 'true'

- name: DATA\_RECOVERY\_ENABLED

value: 'true'

- name: COMMUNICATION\_PORT

value: '8084'

- name: MANAGEMENT\_PORT\_HTTPS

value: '8083'

- name: MANAGEMENT\_PORT\_HTTP

- name: DISABLE\_LIMITS

value: 'false'

- name: FIPS\_ENABLED

value: 'false'

**- name: SSL\_CERT\_FILE**

**value: /certs/zscaler.crt**

* **Add a new volumemount for "zscaler-ca-volume" with mountPath of "/certs" and readOnly = "true"**

**volumeMounts:**

- name: twistlock-config-volume

mountPath: /data/config/

- name: console-persistent-volume

mountPath: /var/lib/twistlock

subPath: var/lib/twistlock

- name: console-persistent-volume

mountPath: /var/lib/twistlock-backup

subPath: var/lib/twistlock-backup

- name: syslog-socket

mountPath: /dev/log

**- name: zscaler-ca-volume**

**readOnly: true**

**mountPath: /certs**

**4- Verify the Certs folder with "zscaler.crt" and Environment Variable for SSL\_CERT\_FILE=/certs/zscaler.crt exist in Twistlock-Console Pod:**



**Run Twistlock Scan Locally on Redhat-8 Workspace:**

**------------------------------------------------------------------------**

**1- Download nginx image to my Redhat-8 workspace.**

**-------------------------------------------------------------------------**

**khaled.fouad ~ ❯ docker pull docker.artifactory.pb.lz.us-cert.gov/nginx:latest**

Emulate Docker CLI using podman. Create /etc/containers/nodocker to quiet msg.

Trying to pull **docker.artifactory.pb.lz.us-cert.gov/nginx:latest...**

Getting image source signatures

Copying blob 1d9f51194194 done |

Copying blob 59e22667830b done |

Copying blob 140da4f89dcb done |

Copying blob 2ef442a3816e done |

Copying blob 96e47e70491e done |

Copying blob 4b1e45a9989f done |

Copying blob f30ffbee4c54 done |

Copying config 2cd1d97f89 done |

Writing manifest to image destination

2cd1d97f893f70cee86a38b7160c30e5750f3ed6ad86c598884ca9c6a563a501

**khaled.fouad ~/Downloads ❯ podman images**

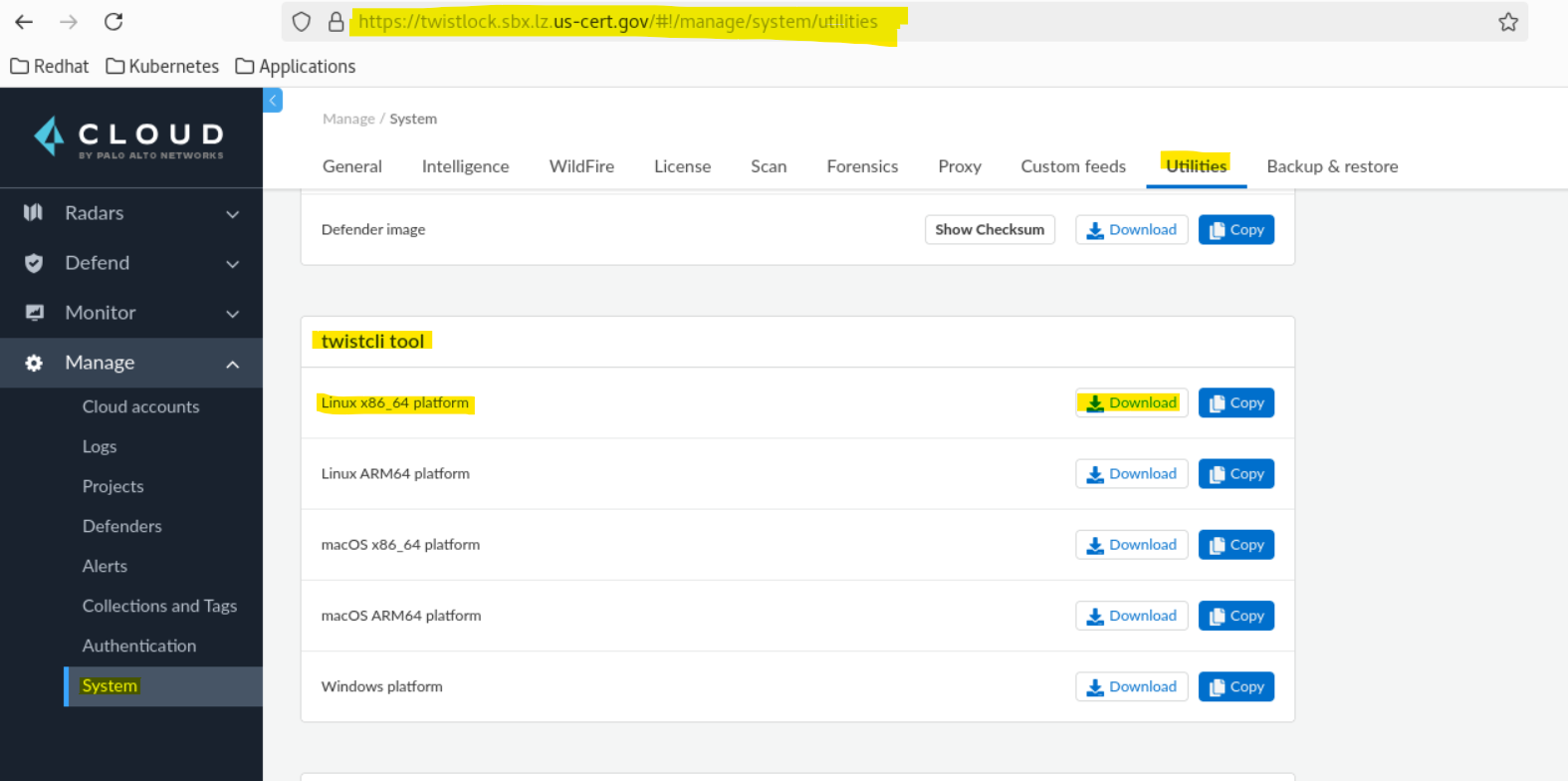
REPOSITORY TAG IMAGE ID CREATED SIZE

**docker.artifactory.pb.lz.us-cert.gov/nginx latest** 2cd1d97f893f 2 weeks ago 196 MB

docker.artifactory.pb.lz.us-cert.gov/**python** **latest** 4bbf6d52fe8d 6 weeks ago 1.04 GB

**2- Download the "twistcli" script from the Prisma Cloud Console**

**-------------------------------------------------------------------------------------------**



**3- Run the Twistlock scan using "twistcli" script, which I downloaded from the Prisma Cloud Console**

**-----------------------------------------------------------------------------------------------------------------------------------------**

**Original Command:**

**./twistcli** images scan --address=${input.prismacloudConsoleURL} --user=${input.prismacloudConsoleUser} --password=${input.prismacloudConsolePW} \

--compliance-threshold=${input.prismacloudCompliancePolicy} --vulnerability-threshold=${input.prismacloudVulnerabilityPolicy} --output-file=prisma-cloud-scan-results.json \

--podman-path=podman ${input.imageNamespace}/${input.imageName}:${input.imageVersion}

**khaled.fouad ~/Downloads ❯ ./twistcli images scan --address=https://twistlock.sbx.lz.us-cert.gov/ --user=admin --password=TwistlockPassword1 \**

**--output-file=prisma-cloud-scan-results.json \**

**--podman-path=podman docker.artifactory.pb.lz.us-cert.gov/nginx:latest**

**Scan results for: image docker.artifactory.pb.lz.us-cert.gov/nginx:latest 2cd1d97f893f70cee86a38b7160c30e5750f3ed6ad86c598884ca9c6a563a501**

**Vulnerabilities found for image docker.artifactory.pb.lz.us-cert.gov/nginx:latest: total - 25, critical - 0, high - 1, medium - 0, low - 24**

**Vulnerability threshold check results: PASS**

**Compliance found for image docker.artifactory.pb.lz.us-cert.gov/nginx:latest: total - 1, critical - 0, high - 1, medium - 0, low - 0**

**Compliance threshold check results: PASS**

Link to the results in Console: <https://twistlock.sbx.lz.us-cert.gov/#!/monitor/vulnerabilities/images/ci?search=2cd1d97f893f70cee86a38b7160c30e5750f3ed6ad86c598884ca9c6a563a501>

**Wrote scan results to prisma-cloud-scan-results.json**

**khaled.fouad ~/Downloads ❯ ll**

total 128M

**-rw-------. 1 khaled.elsayed.rh domain users 42K Jul 29 15:22 prisma-cloud-scan-results.json**

-rw-r--r--. 1 khaled.elsayed.rh domain users 2.4K Jul 29 14:51 settings.xml

-rwxr-xr-x. 1 khaled.elsayed.rh domain users 128M Jul 29 13:44 **twistcli**

drwx------. 3 khaled.elsayed.rh domain users 4.0K Jul 22 15:23 VIP\_Config\_Files

**3- Check the Twistlock Report:**

**------------------------------------------**

**khaled.fouad ~/Downloads ❯ cat prisma-cloud-scan-results.json**

{

"results": [

{

"id": "2cd1d97f893f70cee86a38b7160c30e5750f3ed6ad86c598884ca9c6a563a501",

"name": "docker.artifactory.pb.lz.us-cert.gov/nginx:latest",

"distro": "Debian GNU/Linux 12 (bookworm)",

"distroRelease": "bookworm",

"digest": "sha256:6533ddd664582430971e93e69cf343e3bfffceadeaaa97d4379c4d7a29f21d47",

"collections": [

"All"

],

"packages": [

{

"type": "os",

"name": "grep",

"version": "3.8-5",

"licenses": [

"GPL-3+"

]

},

**Twistlock Image Scanning Process:**

**------------------------------------------------**

**We are using the Twistlock plugin** which is **installed** on every **Cloudbees controller**, and the **plugin calls** the "**prismaCloudScanImage**" function to **scan the image**. This **function** is getting all its **required parameters** through the **pipeline** from the **pipeline-config namespace** inside **dso-eks-cluster**.

**This is showing the twistcli command** that is being used in the **pipeline** to **scan** the **image**, which is being **called** through the **Twistlock plugin.**

**============================================================================================================================**

**Tag image (mng-dev/submission-ms:v-develop.222) to host so Twistlock can scan it**

[Pipeline] sh

+ **podman tag docker.artifactory.pb.lz.us-cert.gov/mng-dev/submission-ms:latest docker.artifactory.pb.lz.us-cert.gov/mng-dev/submission-ms:v-develop.222**

[Pipeline] echo

PrismaCloud Scan of Image

[Pipeline] prismaCloudScanImage

**[PRISMACLOUD] Scanning images remotely on jenkins-submission-ms-222-gsgvx-znmn6**

**[PRISMACLOUD] Waiting for scanner to complete**

[**PRISMACLOUD**] **/home/jenkins/agent/workspace/submission-ms\_develop/twistcli5828895494295951337 images scan --docker-address unix:///var/run/docker.sock --podman-path podman --ci --publish --details --address** [**https://twistlock.pb.lz.us-cert.gov**](https://twistlock.pb.lz.us-cert.gov) **--ci-results-file twistlock-scan-result.json mng-dev/submission-ms:v-develop.222**

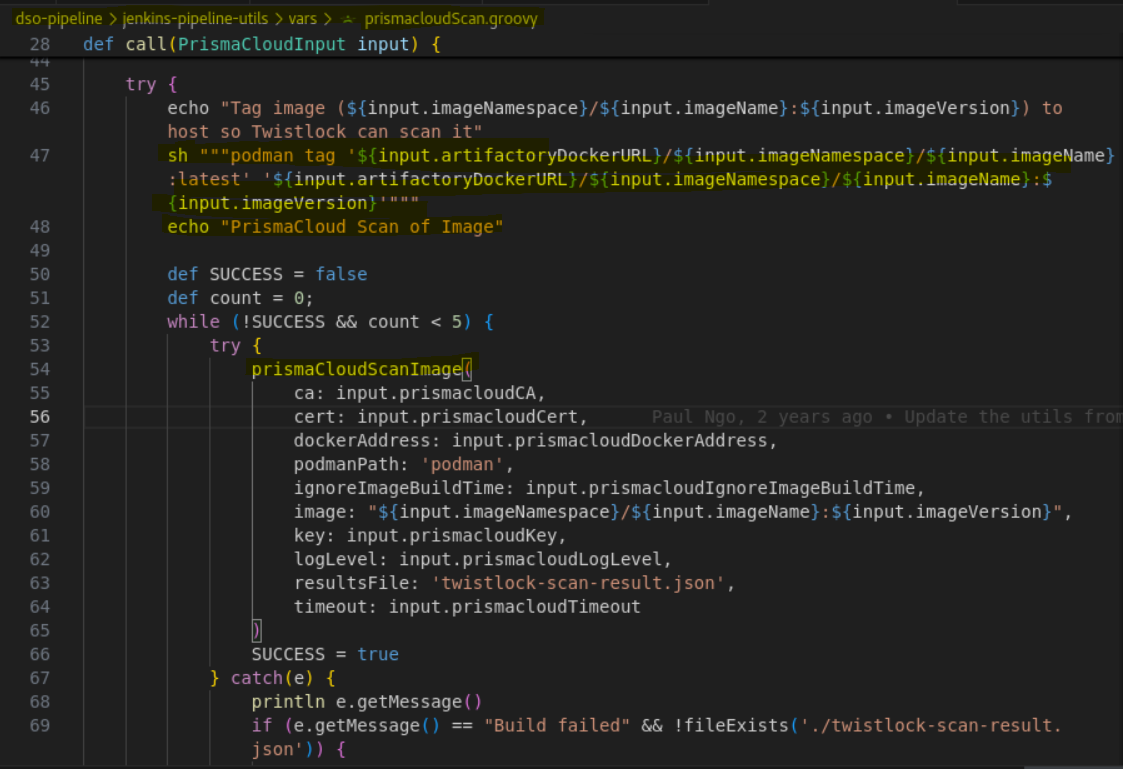
Executing sh script inside container jenkins-agent-image-mgmt of pod jenkins-submission-ms-222-gsgvx-znmn6

Executing command: "/home/jenkins/agent/workspace/submission-ms\_develop/twistcli5828895494295951337" "images" "scan" "--docker-address" "unix:///var/run/docker.sock" "--podman-path" "podman" "--ci" "--publish" "--details" "--address" "<https://twistlock.pb.lz.us-cert.gov>" "--ci-results-file" "twistlock-scan-result.json" "mng-dev/submission-ms:v-develop.222"

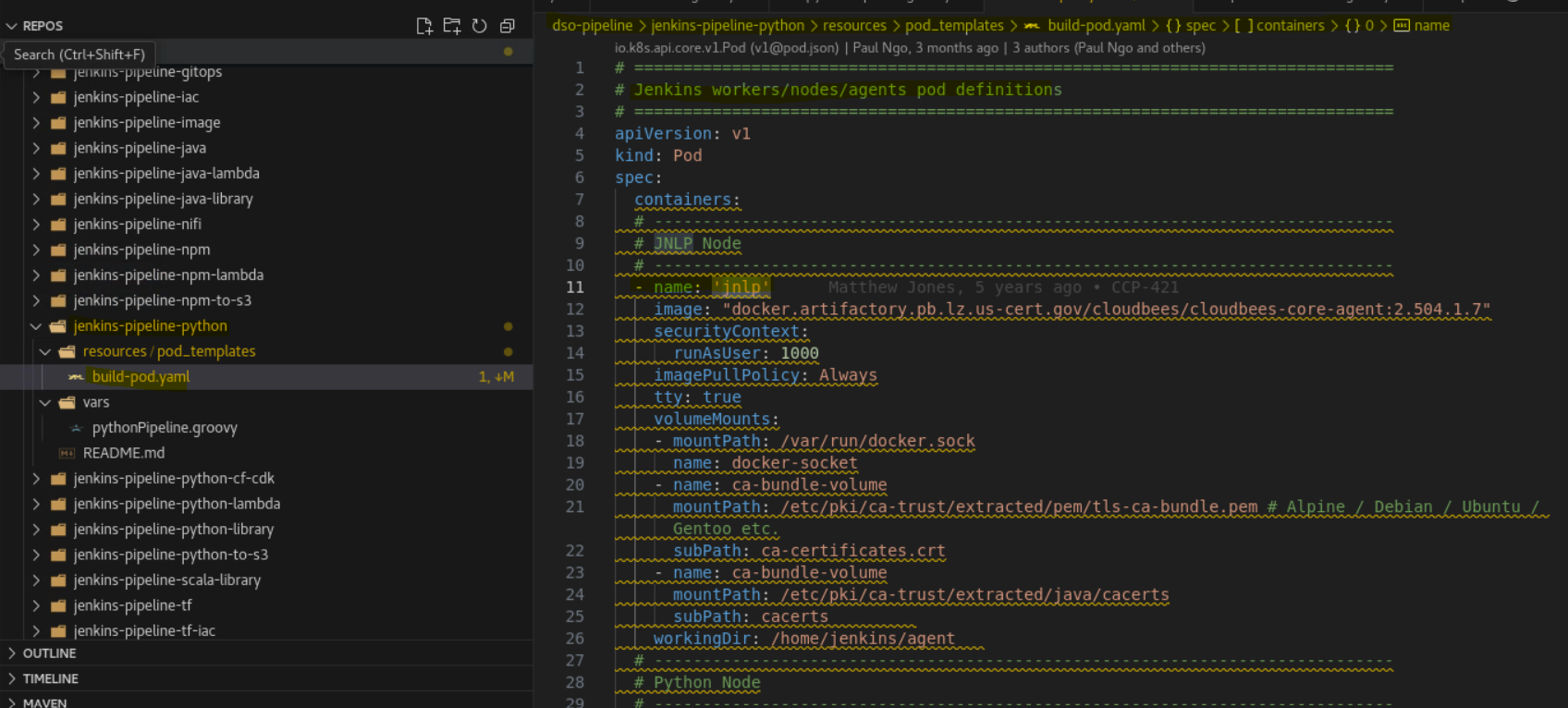
exit

**============================================================================================================================**

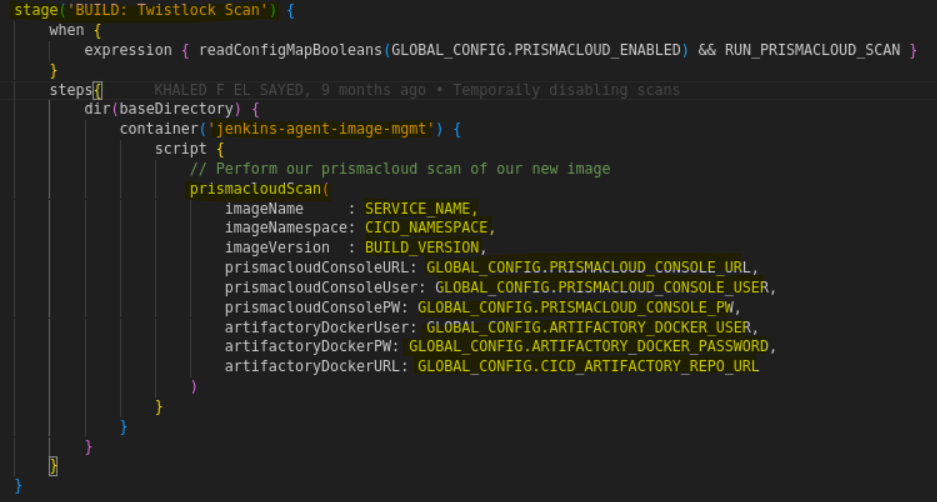
**This is the prismaCloudScan.groovy showing the prismaCloudScanImage, which is being called by the twistlock plugin.**



**The jnlp container is used for loading all the Cloudbees plugins, which include the twistlock plugin used for scanning docker images.**



**This is showing the Twistlock Scan Stage in Python pipeline which is calling the prismacloudScan function that is being used to scan docker images.**



**All of these variables are pulled from "pipeline-config" namespace inside "dso-eks-cluster".**

**These variables are configured in ConfigMap:**

* **"PRISMACLOUD\_CONSOLE\_URL"**: "<https://twistlock.pb.lz.us-cert.gov>",
* **"PRISMACLOUD\_ENABLED"**: "true",
* **"PRISMACLOUD\_THRESHOLD"**: "high",
* **"ARTIFACTORY\_DOCKER\_USER"**: "svc.artifactory",
* **"CICD\_ARTIFACTORY\_REPO\_URL"**: "docker.artifactory.pb.lz.us-cert.gov"

**These variables are configured in Secrets:**

* **PRISMACLOUD\_CONSOLE\_PW**: RCR2UyRjMHBzIzFEJHZTJGMwcHMjMQ==
* **PRISMACLOUD\_CONSOLE\_USER**: dHdpc3Rsb2NrLXNlcnZpY2U=
* **ARTIFACTORY\_DOCKER\_PASSWORD**: >-

Y21WbWRHdHVPakF4T2pFM05qZ3dOVEE0TWpjNlVHMDJSbmhsUm5KWFFXeHRTM2Q2Y0daaGRYQlVUems1YUhVMw==

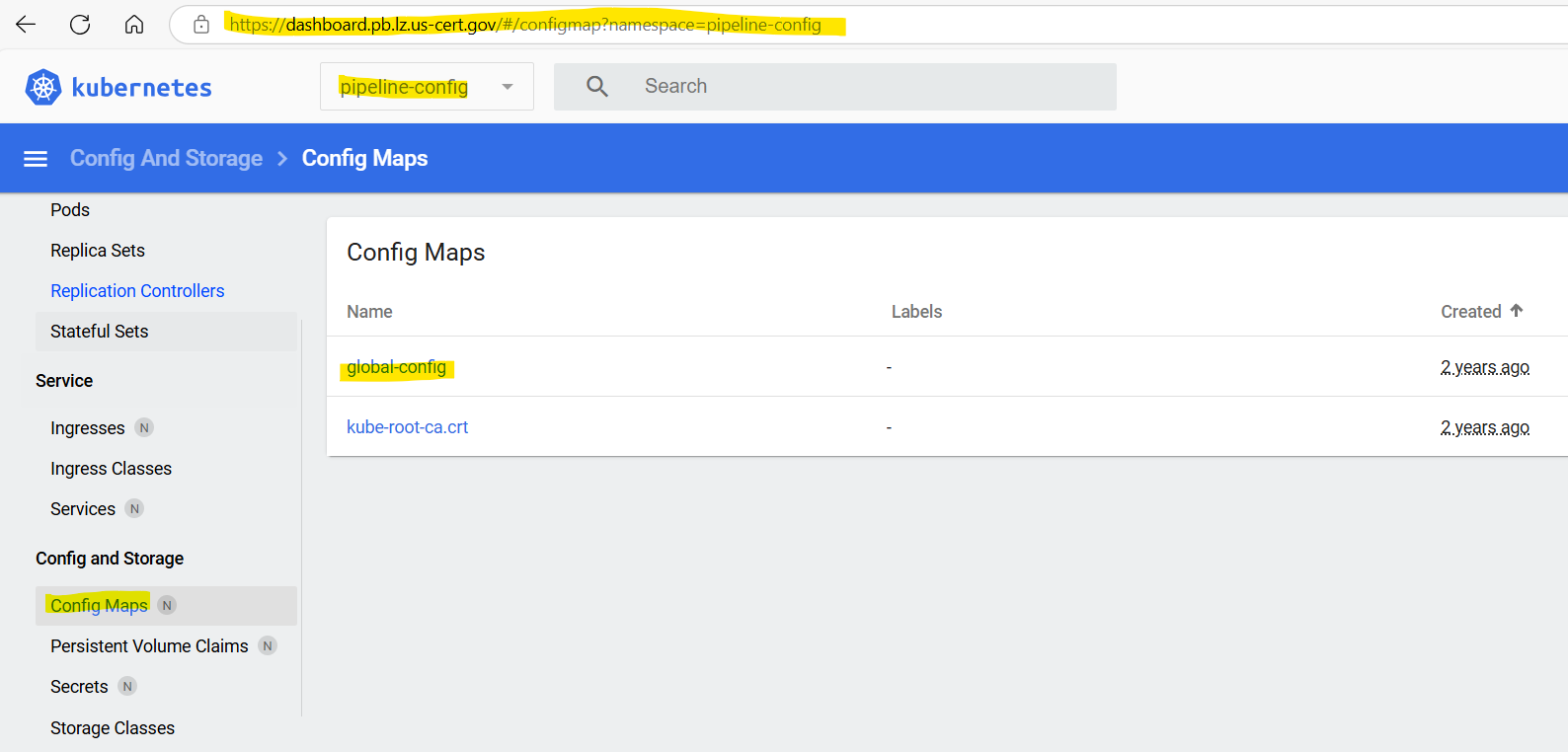
* **ARTIFACTORY\_PASSWORD: >-**

Y21WbWRHdHVPakF4T2pFM05qZ3dOVEE0TWpjNlVHMDJSbmhsUm5KWFFXeHRTM2Q2Y0daaGRYQlVUems1YUhVMw==

* **ARTIFACTORY\_USER**: c3ZjLmFydGlmYWN0b3J5

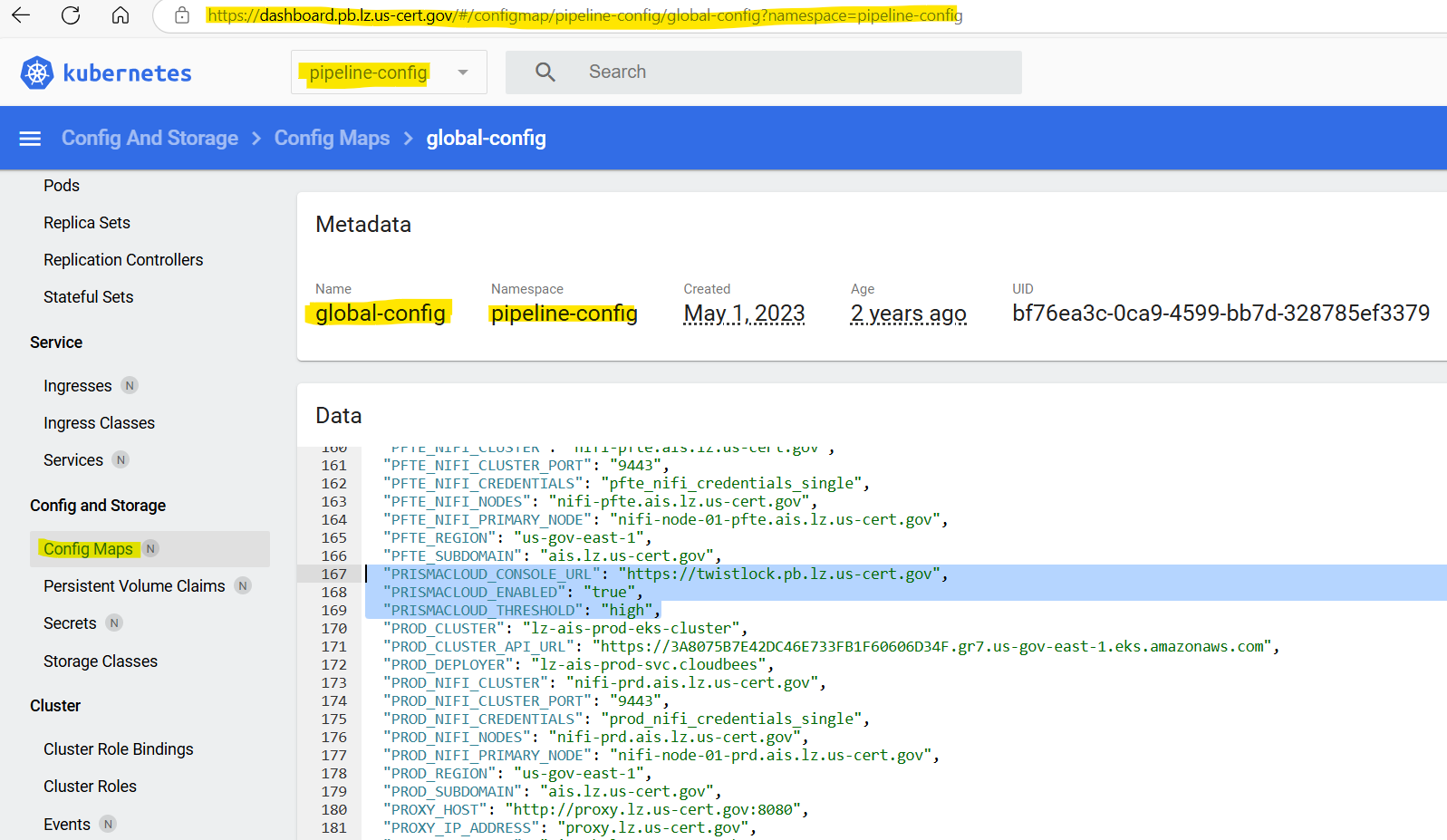
**global-config ConfigMap:**

**-----------------------------------**



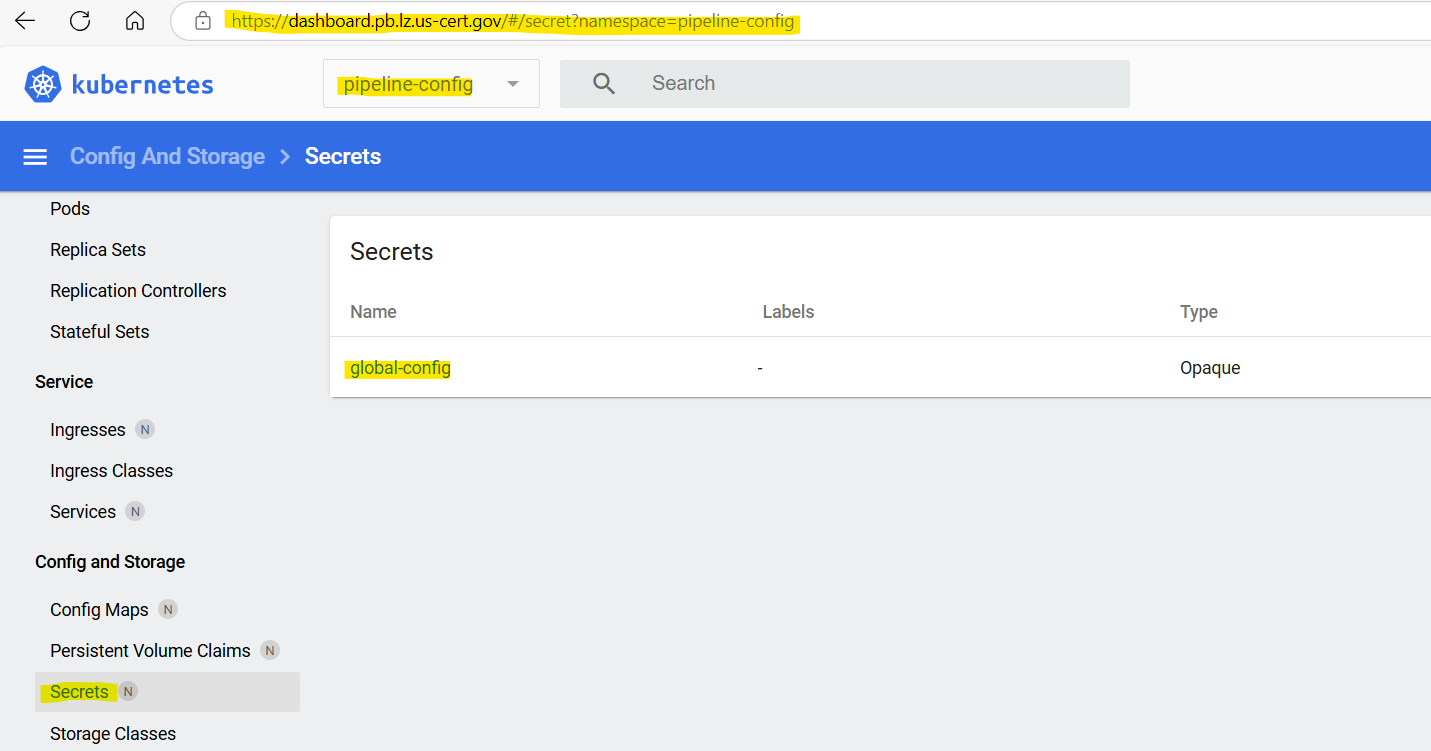
**global-config ConfigMap variables:**

**------------------------------------------------**



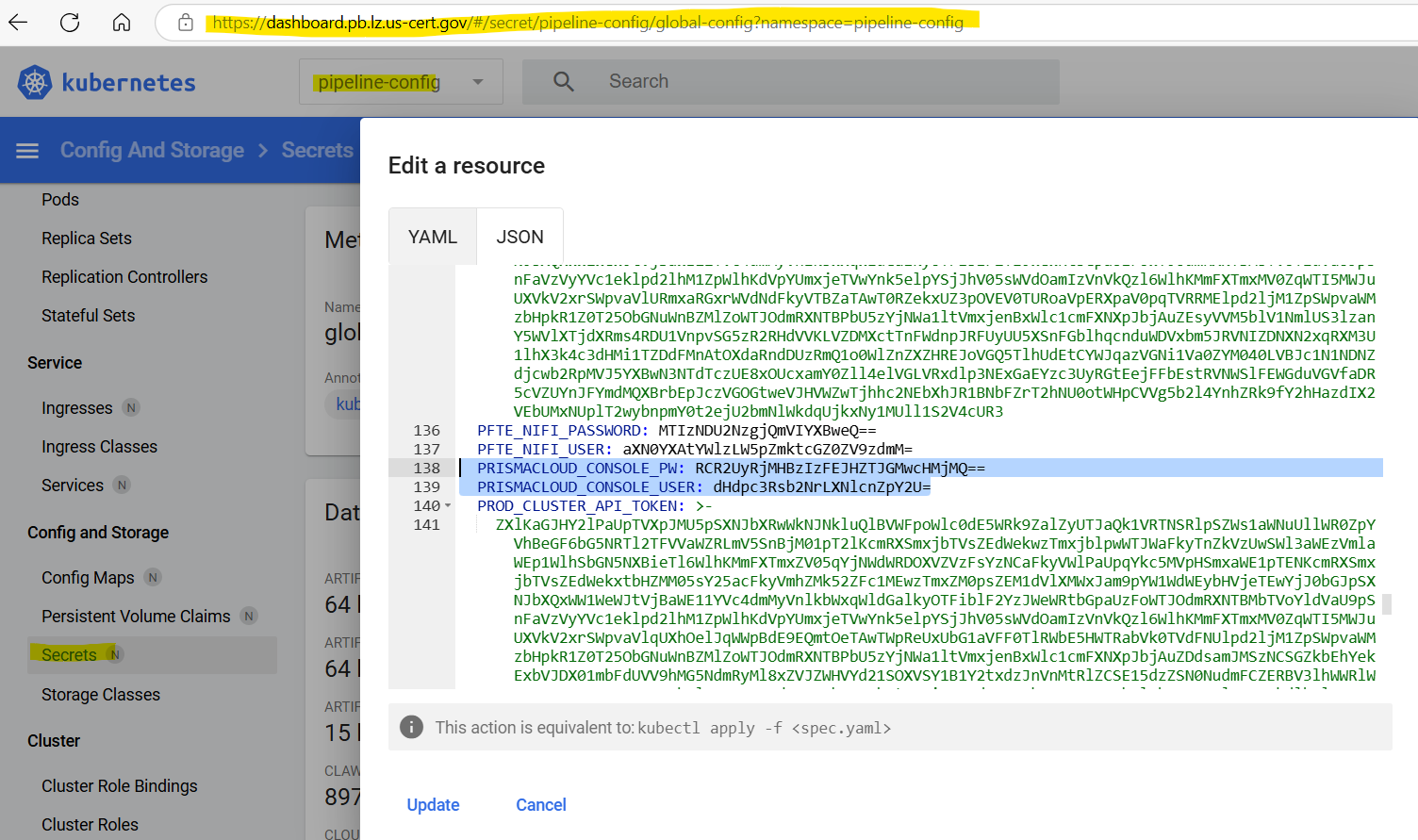
**global-config Secret:**

**--------------------------------**



**global-config Secret variables:**

**------------------------------------------**

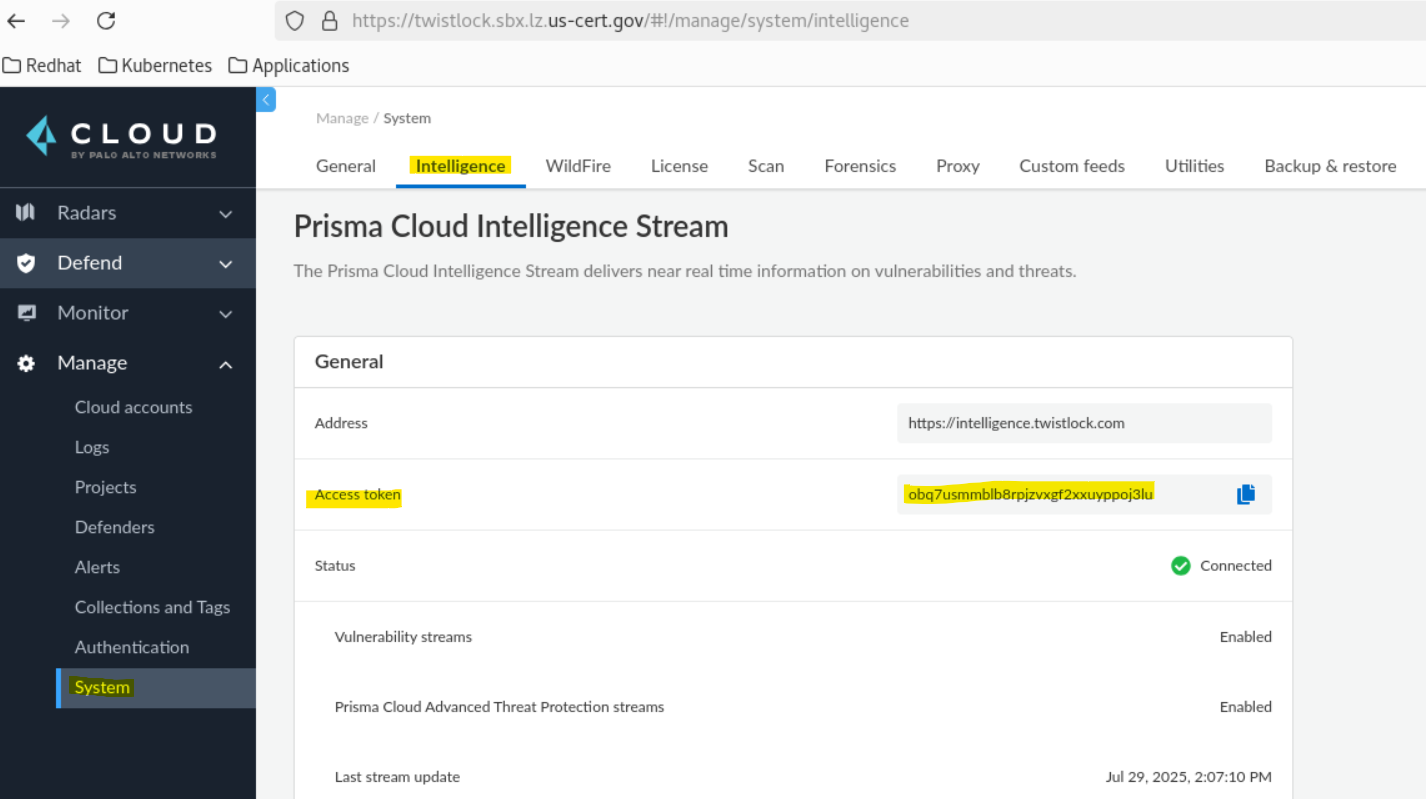


**Twistlock Token for Pulling Images:**

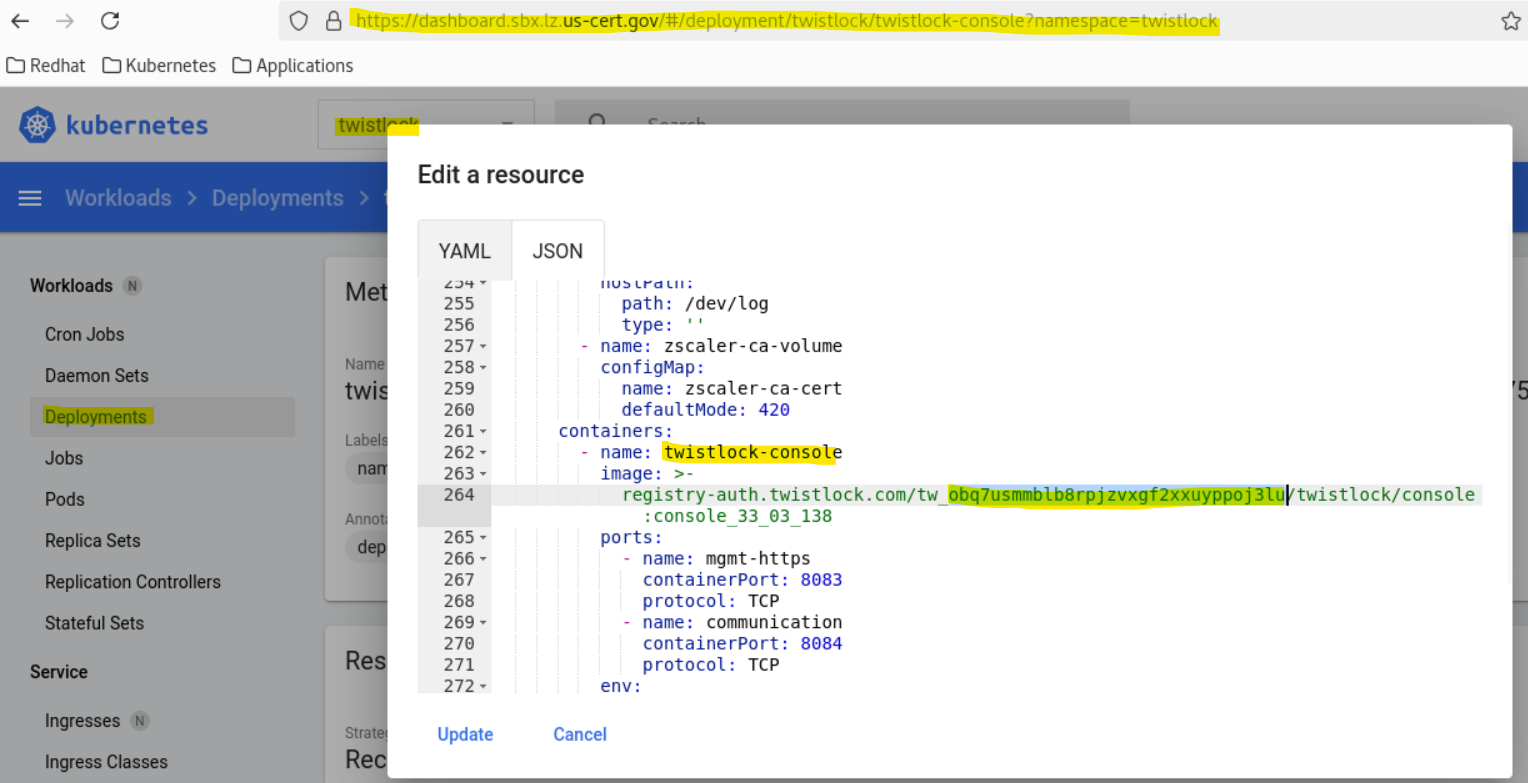
**--------------------------------------------------**

**This Token need to be defined inside the Twistlock deployment.**

**Remember that Sometimes this token need to be replaced, when we update Twistlock.**



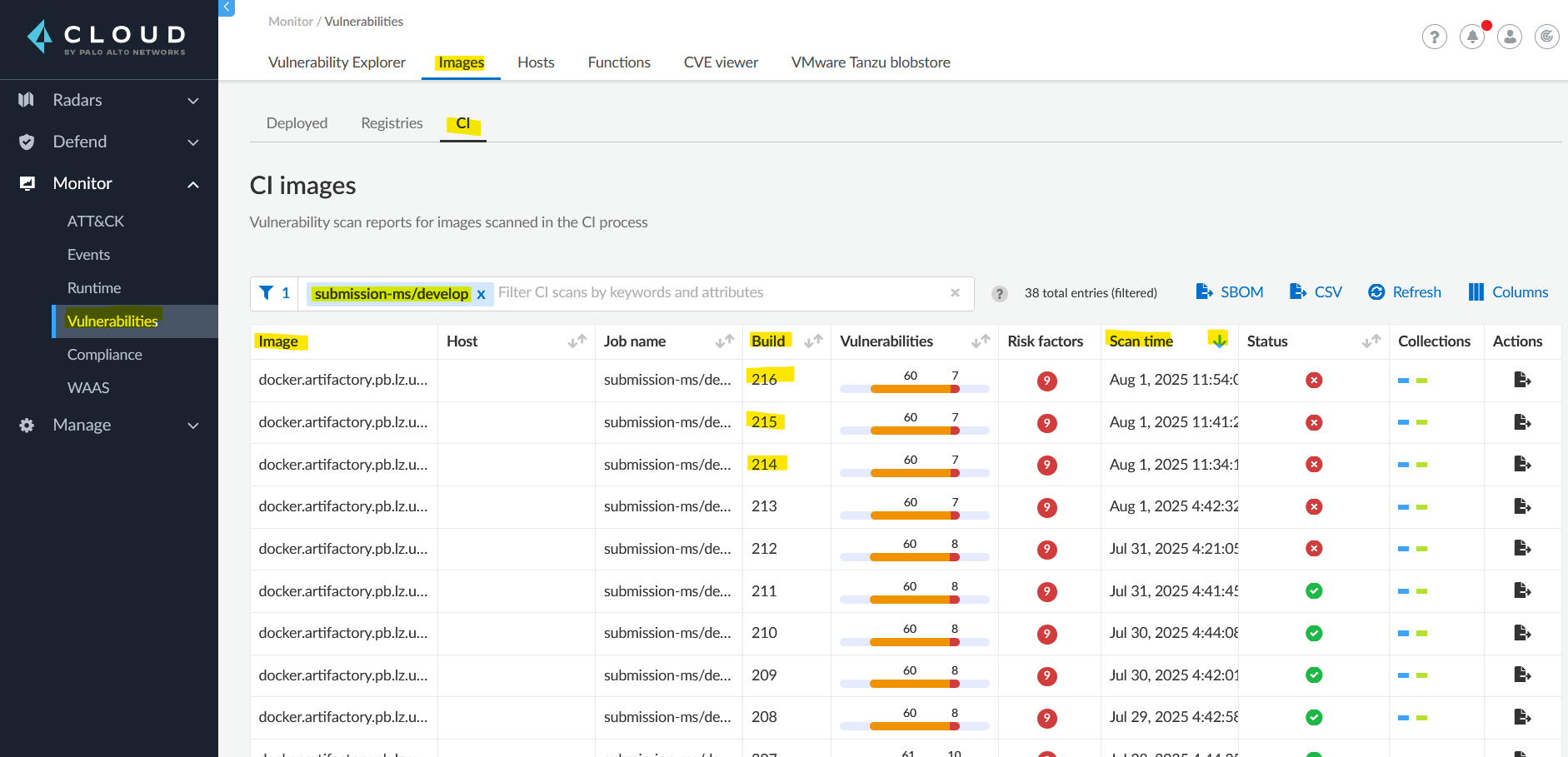
**This token is defined in the Twistlock Deployment as shown below.**



**Twistlock Image Scan:**

**-------------------------------**

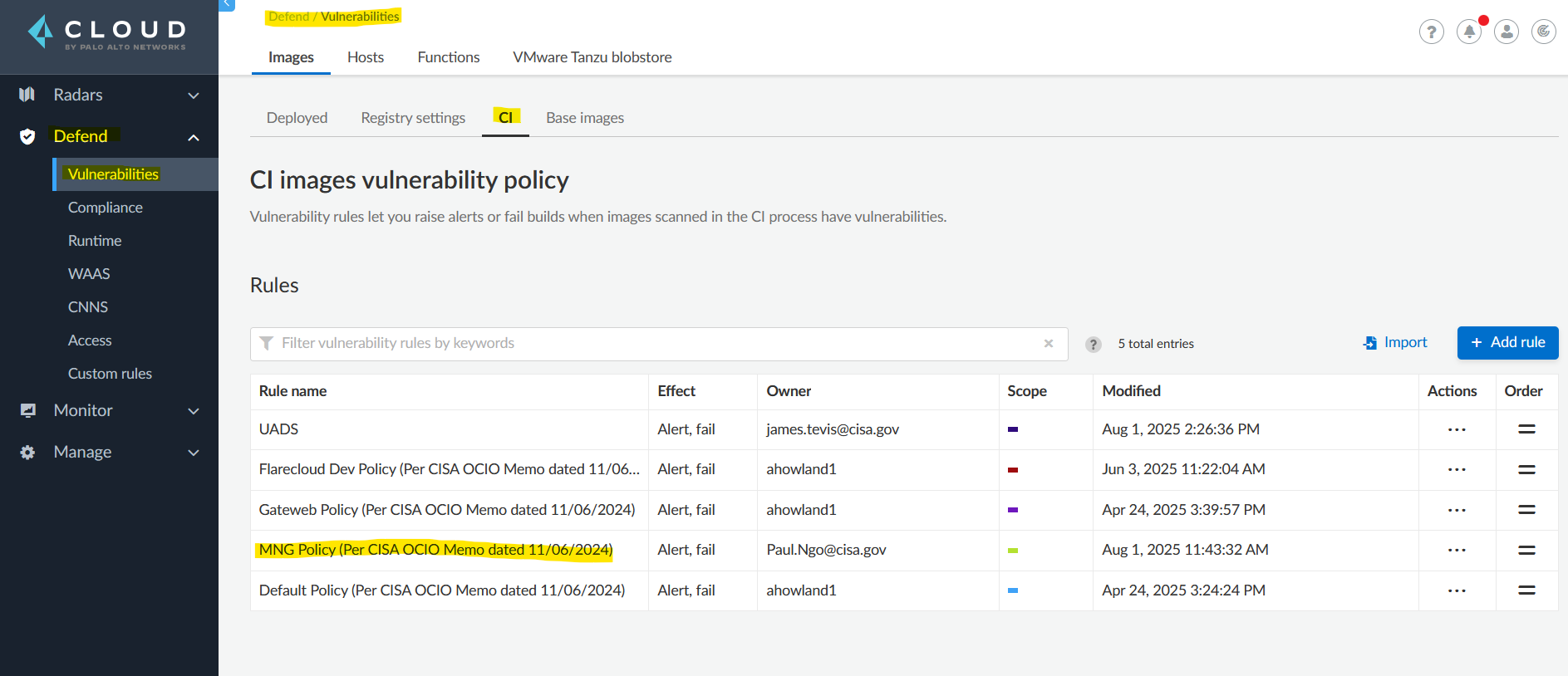
**This is showing the results for the vulnerabilities of the docker image scanning for malware submission-ms/develop branch.**

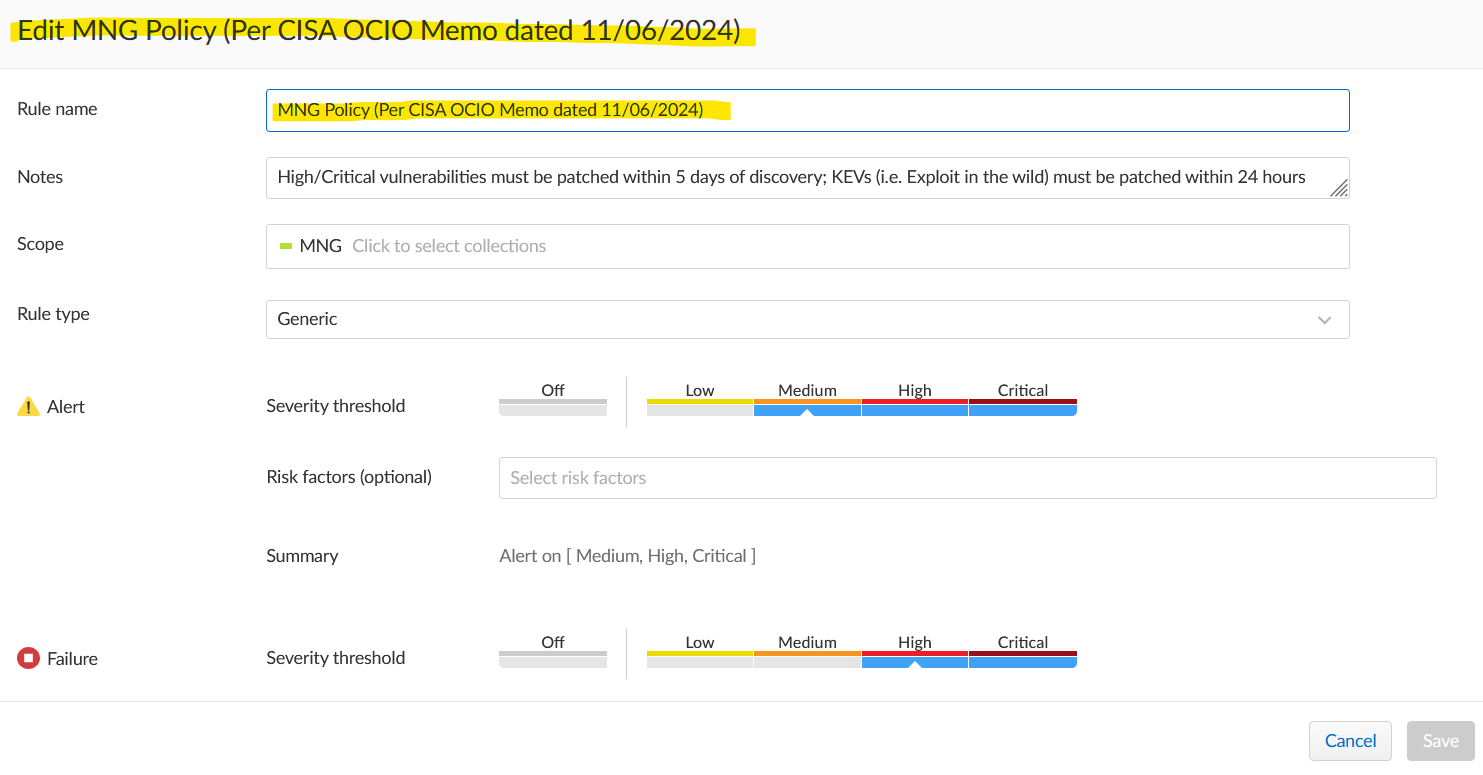


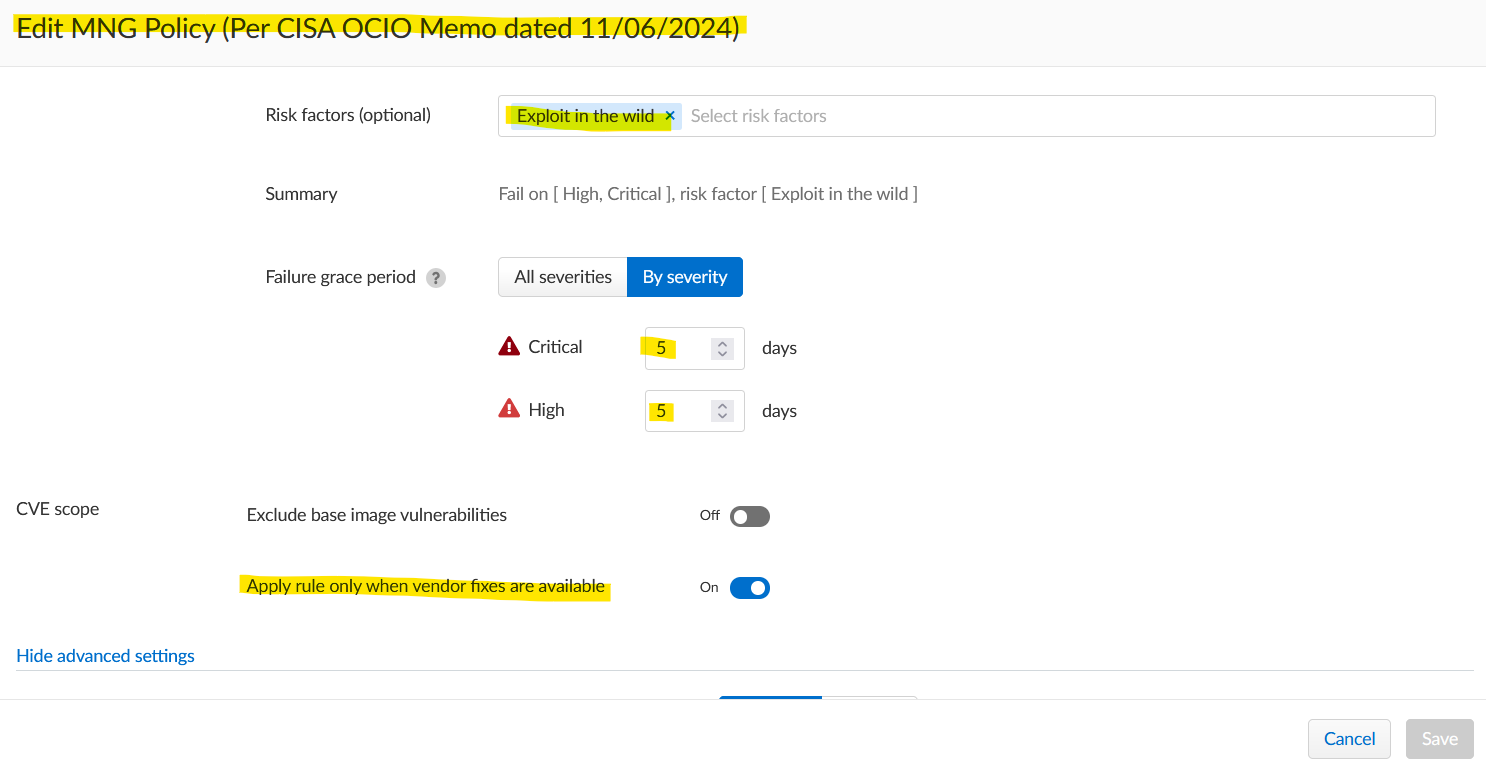
**Twistlock Image Scan:**

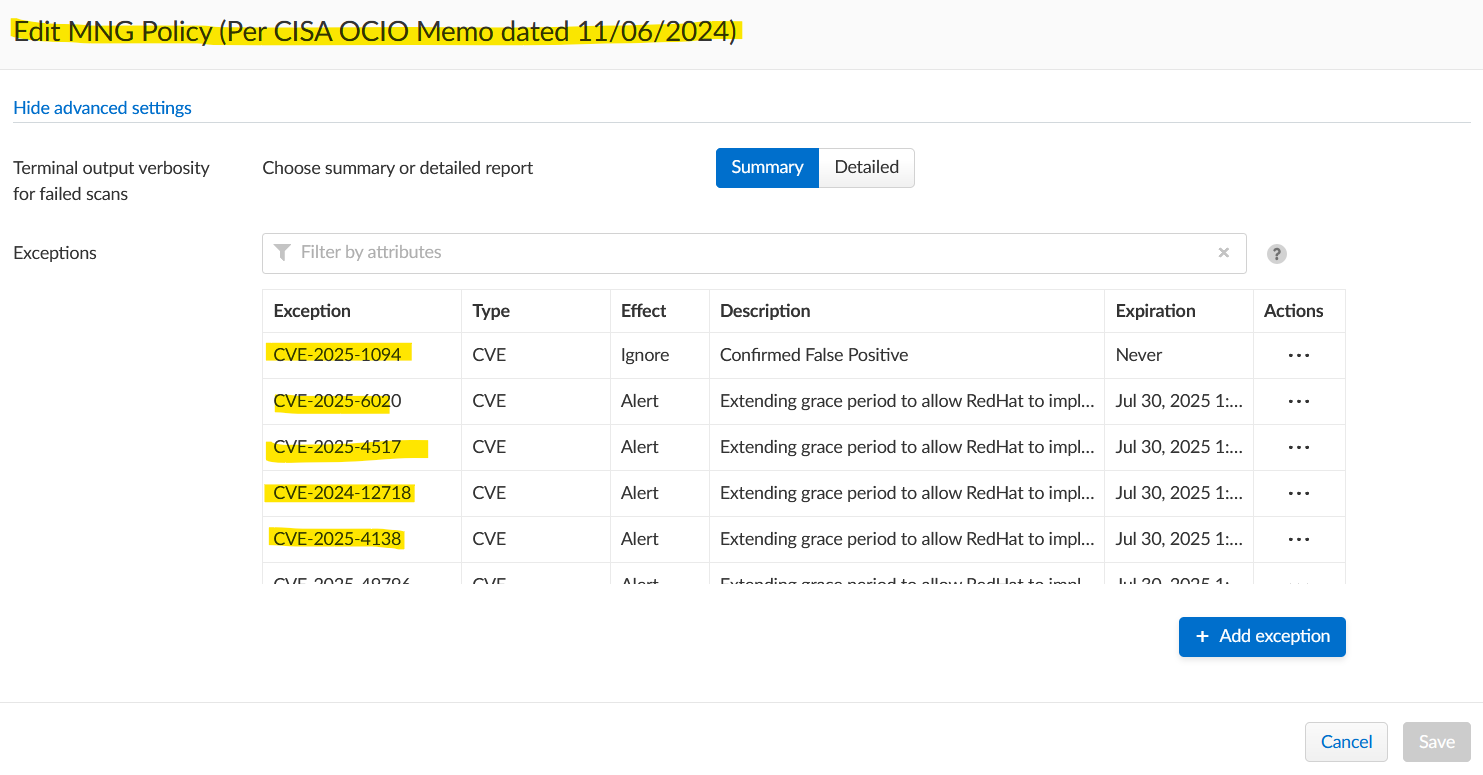
**-------------------------------**

**This is showing the exception rules applied for MNG to allow them to bypass certain vulnerabilities.**









**Twistlock Errors :**

**-------------------------**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud/New (master) ✗ ❯ nslookup twistlock.dev.lz.us-cert.gov**

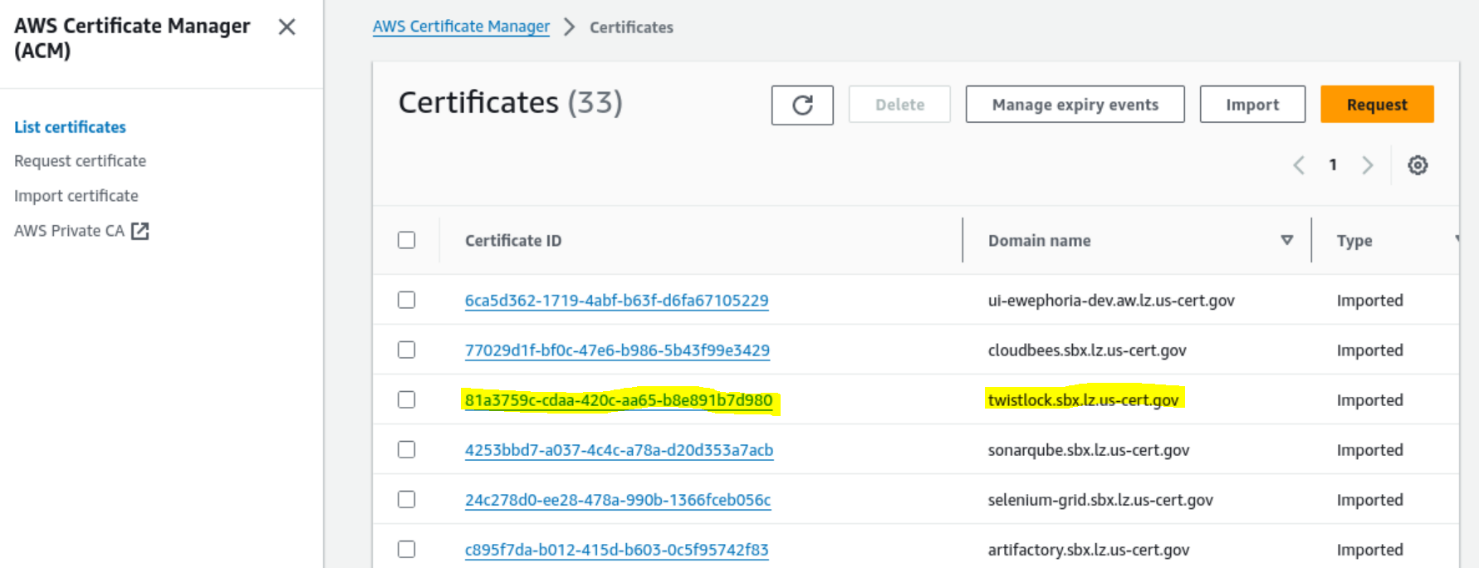
Server:                10.234.80.183

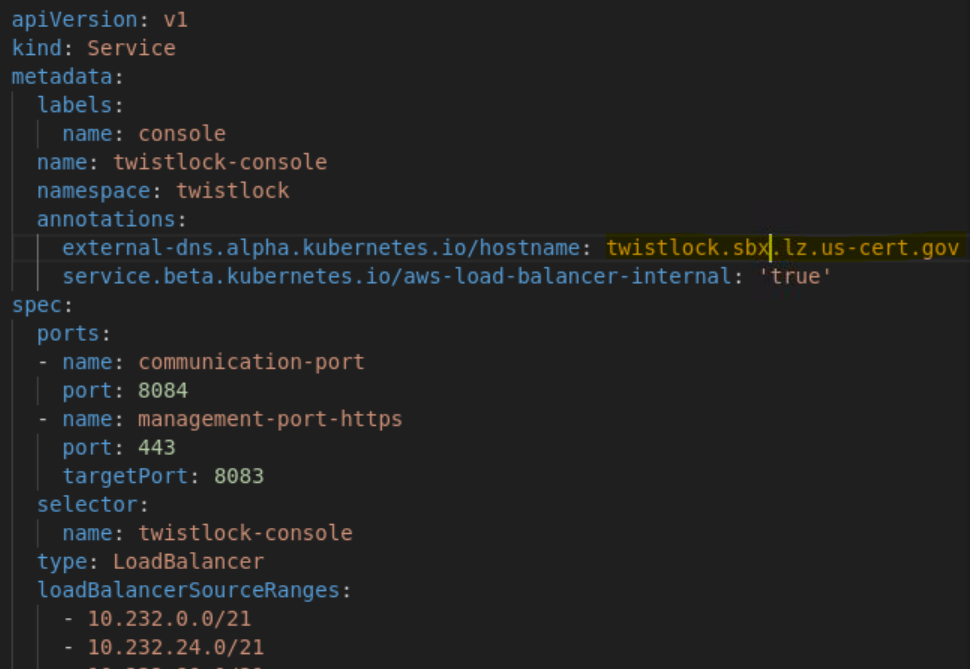
Address:        10.234.80.183#53

\*\* server can't find twistlock.dev.lz.us-cert.gov: NXDOMAIN

**Solution:**

**The twistlock service MUST be installed with the SAME URL that was used for requesting its DHS Certificate, which was requested for this Domain Name: twistlock.sbx.lz.us-cert.gov**





**Incorrect Version:**

**-------------------------**

This incorrect version resolves itself after a few minutes, once I accept the **Risk on Firefox** when opening the **twistlock URL**:

[**https://twistlock.sbx.lz.us-cert.gov**](https://twistlock.sbx.lz.us-cert.gov)

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ nslookup twistlock.sbx.lz.us-cert.gov**

Server:                10.234.80.183

Address:        10.234.80.183#53

Non-authoritative answer:

twistlock.sbx.lz.us-cert.gov        canonical name = internal-ab55e35d6de384b85b86cfad08a1aa21-617203748.us-gov-west-1.elb.amazonaws.com.

\*\* server can't find internal-ab55e35d6de384b85b86cfad08a1aa21-617203748.us-gov-west-1.elb.amazonaws.com: NXDOMAIN

**Correct Version:**

**-----------------------**

**This should be the case for any DevSecOps service, where the DevSecOps service like Twistlock or Sonarqube would be mapped to the Loadbalancer DNS Name.**

**khaled.elsayed at ~/Documents/Repos/Helm/twistlock-prismacloud (master) ✗ ❯ nslookup twistlock.sbx.lz.us-cert.gov**

Server:                10.234.80.183

Address:        10.234.80.183#53

Non-authoritative answer:

twistlock.sbx.lz.us-cert.gov        canonical name = internal-a9ed48e4c670a4e6ab14a61e22c9c82e-1549141418.us-gov-west-1.elb.amazonaws.com.

Name:        internal-a9ed48e4c670a4e6ab14a61e22c9c82e-1549141418.us-gov-west-1.elb.amazonaws.com

Address: 10.234.184.218

Name:        internal-a9ed48e4c670a4e6ab14a61e22c9c82e-1549141418.us-gov-west-1.elb.amazonaws.com

Address: 10.234.185.188

Name:        internal-a9ed48e4c670a4e6ab14a61e22c9c82e-1549141418.us-gov-west-1.elb.amazonaws.com

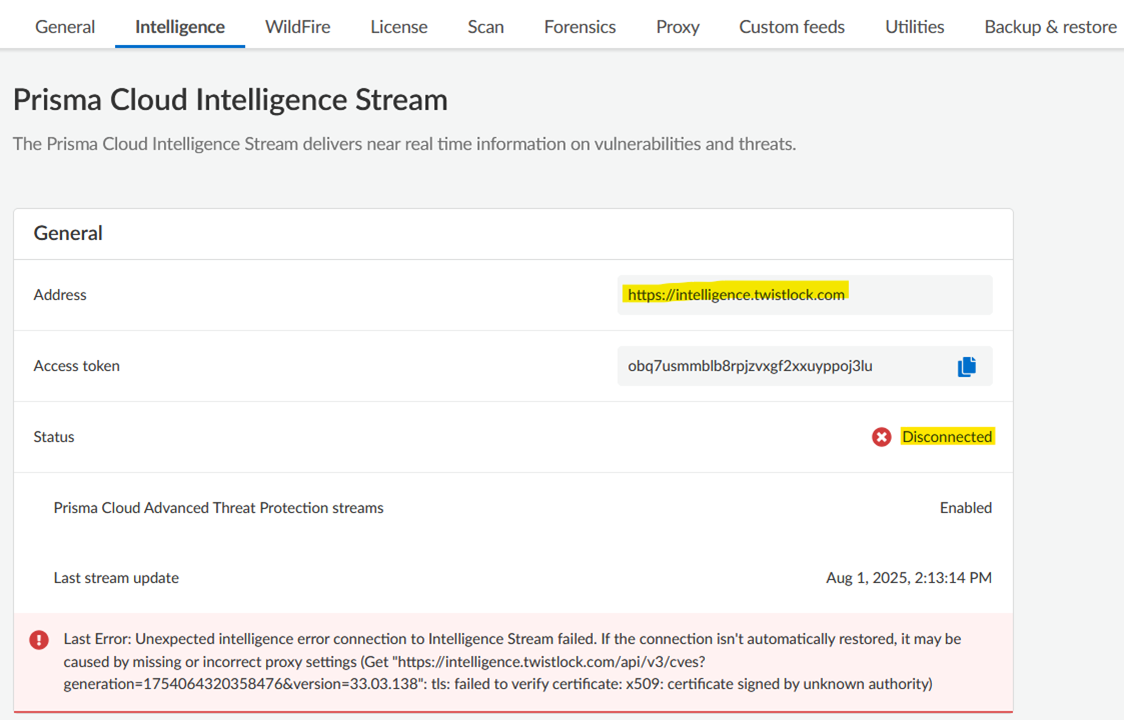
Address: 10.234.186.114

**===========================================================================================================================**

**===========================================================================================================================**

**Error:**

**This error is showing in Twistlock Production & Sandbox**



**Solution:**

**I checked the Zscaler certificates that we installed inside twistlock-console deployment in the Production & Sandbox Kubernetes, and I found that these configurations were removed. So, I configured them back and restarted all the twistlock pods.**

**1- Add the following configurations inside Twistlock-Console Deployment:**

* **Add a new volume for "zscaler-ca-volume" with Configmap of " zscaler-ca-cert"**

**spec:**

**volumes:**

- name: console-persistent-volume

persistentVolumeClaim:

claimName: twistlock-console

- name: twistlock-config-volume

configMap:

name: twistlock-console

defaultMode: 420

- name: syslog-socket

hostPath:

path: /dev/log

type: ''

**- name: zscaler-ca-volume**

**configMap:**

**name: zscaler-ca-cert**

**defaultMode: 420**

* **Add a new env for "SSL\_CERT\_FILE" with value of "/certs/zscaler.crt"**

**env:**

- name: CONFIG\_PATH

value: /data/config/twistlock.cfg

- name: INTELLIGENCE\_FEEDS\_FOLDER

value: /var/lib/twistlock/saas\_feeds

- name: LOG\_PROD

value: 'true'

- name: DATA\_RECOVERY\_ENABLED

value: 'true'

- name: COMMUNICATION\_PORT

value: '8084'

- name: MANAGEMENT\_PORT\_HTTPS

value: '8083'

- name: MANAGEMENT\_PORT\_HTTP

- name: DISABLE\_LIMITS

value: 'false'

- name: FIPS\_ENABLED

value: 'false'

**- name: SSL\_CERT\_FILE**

**value: /certs/zscaler.crt**

* **Add a new volumemount for "zscaler-ca-volume" with mountPath of "/certs" and readOnly = "true"**

**volumeMounts:**

- name: twistlock-config-volume

mountPath: /data/config/

- name: console-persistent-volume

mountPath: /var/lib/twistlock

subPath: var/lib/twistlock

- name: console-persistent-volume

mountPath: /var/lib/twistlock-backup

subPath: var/lib/twistlock-backup

- name: syslog-socket

mountPath: /dev/log

**- name: zscaler-ca-volume**

**readOnly: true**

**mountPath: /certs**

**2- Restart all Twistlock Pods:**

**khaled.fouad ~/Documents/Repos ❯ kubectl get pods -n twistlock --no-headers | awk '{print $1}' | xargs -n1 -I {} kubectl delete pod {} -n twistlock**

pod "**twistlock-console**-74849786fc-pzm85" deleted

pod "twistlock-**defender**-ds-2hgwp" deleted

pod "twistlock-**defender**-ds-6rhb6" deleted

pod "twistlock-**defender**-ds-bpjwd" deleted

pod "twistlock-**defender**-ds-ccwt2" deleted

pod "twistlock-**defender**-ds-ckmqm" deleted

pod "twistlock-**defender**-ds-g6lmw" deleted

pod "twistlock-**defender**-ds-n6r2s" deleted

pod "twistlock-**defender**-ds-nhw2v" deleted

pod "twistlock-**defender**-ds-pnjw6" deleted

pod "twistlock-**defender**-ds-q8w4t" deleted

pod "twistlock-**defender**-ds-rsb26" deleted

pod "twistlock-**defender**-ds-wrstf" deleted

pod "twistlock-**defender**-ds-z92kc" deleted

pod "twistlock-**defender**-ds-zjxzc" deleted

**3- Verify the configuration still persist in twistlock-console deployment:**

**If the configuration disappears again, Add them back and restart only the twistlock-console deployment then all the defender pods then attempt to restart all of them again and see if the configuration persist.**

**Production Environment:**



**Sandbox Environment:**

