MANAGE JUST-IN-TIME ACCESS WITH CYBERARK DYNAMIC PRIVILEGED ACCESS (DPA) IN AWS

PREREQUISITES:

Client Workstation Requirements

Modern Browser
Port 22 Outbound
SSH Client (PowerShell, Putty, etc)

AWS Lab:

Access your AWS lab for today's training at
https:/dashboard.eventengine.run/login?hash=6490-14def39704-77

CyberArk Lab

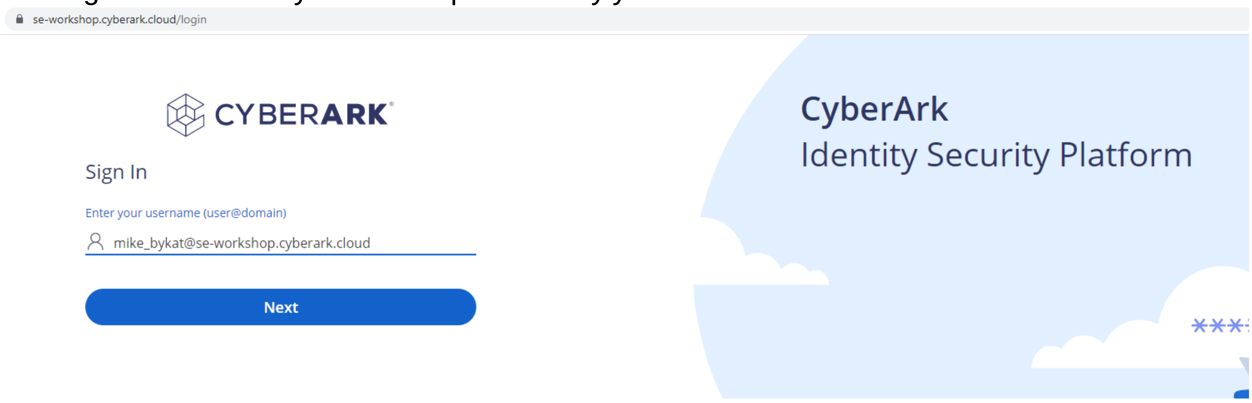
Your CyberArk instructor will provide the CyberArk lab link and your login information in your break-out room

SECTION 1: LOG IN AND CREATE DPA ROLE FOR GRANTING ACCESS

DPA uses CyberArk Identity for authentication and authorization. In this section we will create an Identity role for DPA and assign your user to it. This role will be used for the DPA recuring access policy configured later in section
Note: Active Directory users and groups are supported with DPA but we will be using CyberArk Cloud Directory users and roles for this workshop.

Sign into the DPA Admin Portal

1. Login to the Identity Portal link provided by your instructor


se-workshop.cyberark.cloud/login

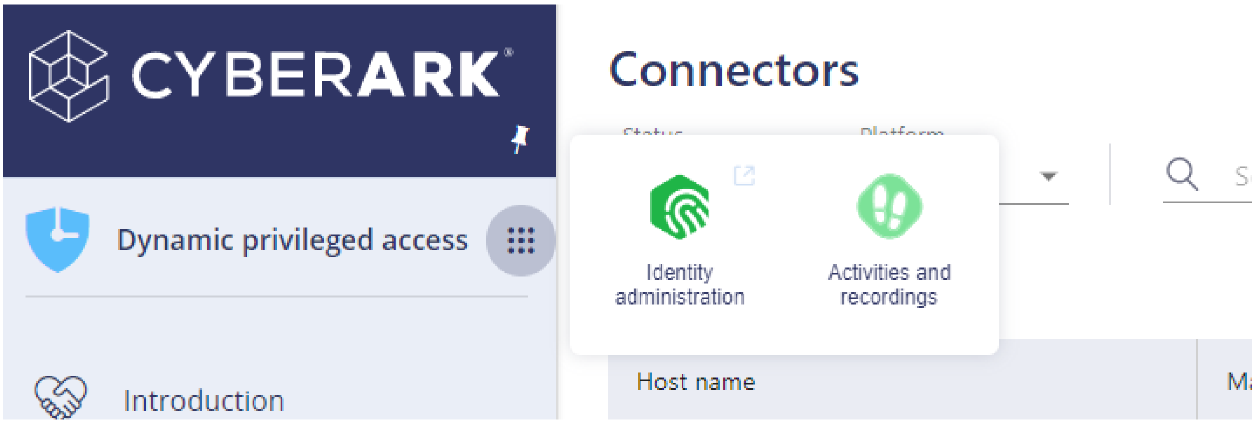
Sign In

Enter your username (user@domain)

mike_bykat@se-workshop.cyberark.cloud

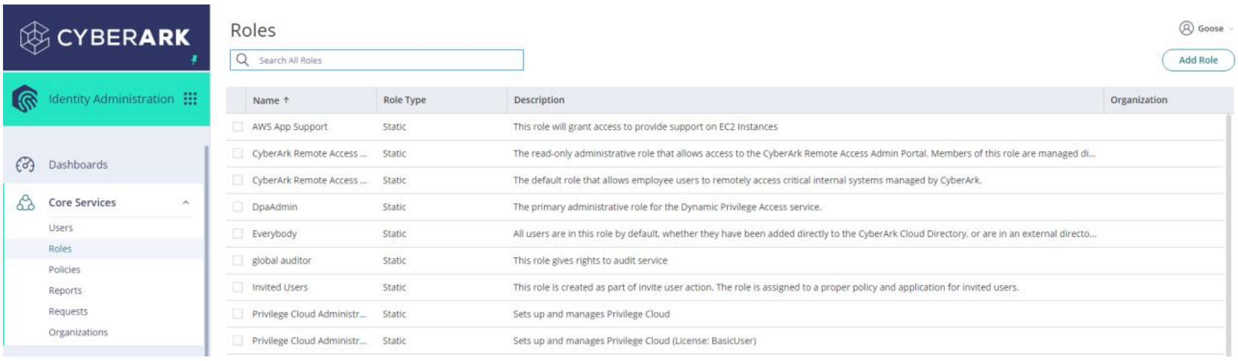
2. Your email address should be in a similar format to firstname.lastname@cyberark.cloud.xxxx

3. Click on Go to Identity Administration.



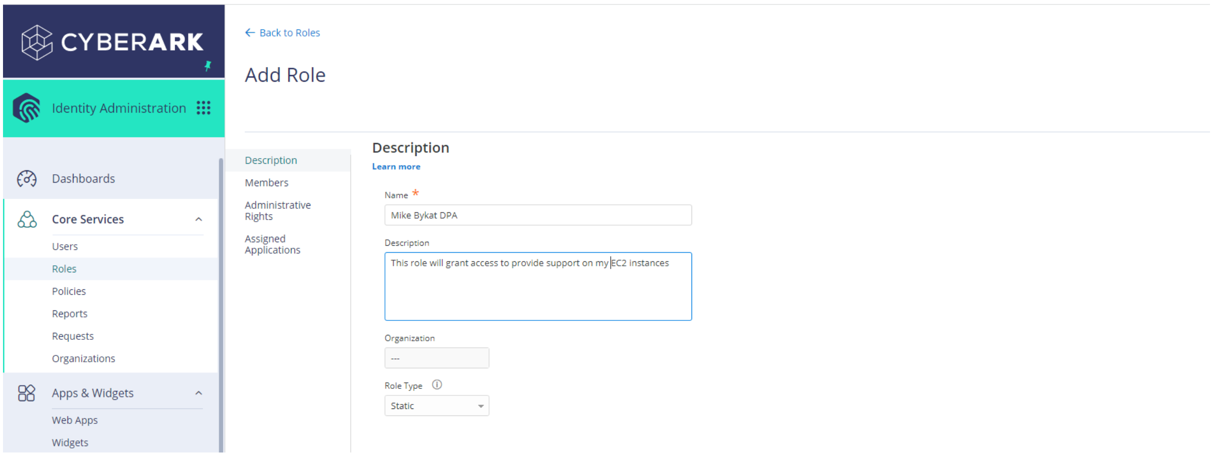
Create a role for DPA users

1. Under Core Services, click "Roles" on the left-hand side



Name	Role Type	Description	Organization
AWS App Support	Static	This role will grant access to provide support on EC2 Instances	
CyberArk Remote Access ...	Static	The read-only administrative role that allows access to the CyberArk Remote Access Admin Portal. Members of this role are managed di...	
CyberArk Remote Access ...	Static	The default role that allows employee users to remotely access critical internal systems managed by CyberArk.	
DpaAdmin	Static	The primary administrative role for the Dynamic Privilege Access service.	
Everybody	Static	All users are in this role by default, whether they have been added directly to the CyberArk Cloud Directory, or are in an external directo...	
global auditor	Static	This role gives rights to audit service	
Invited Users	Static	This role is created as part of invite user action. The role is assigned to a proper policy and application for invited users.	
Privilege Cloud Administr...	Static	Sets up and manages Privilege Cloud	
Privilege Cloud Administr...	Static	Sets up and manages Privilege Cloud (License: BasicUser)	

2. Click "Add Role on the top right corner
   a. Name: {yourname} DPA
   b. Description: This role will grant access to provide support on my EC2 Instances



Add Role

Description

Name *
Mike Bykat DPA

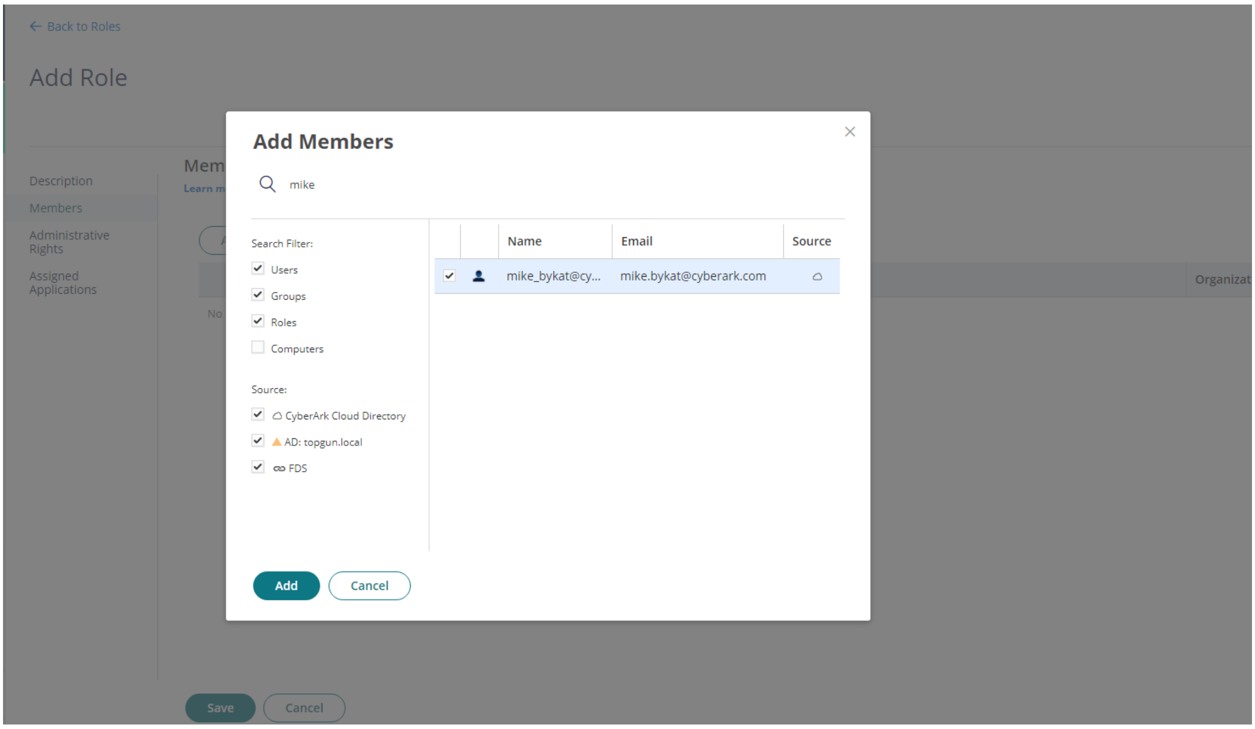
Description
This role will grant access to provide support on my EC2 instances

Organization

Role Type
Static

3. Select Members

a. Click “Add”
b. Search for your user
c. Check the box and click “add” (and don’t forget to click save as mentioned in step 4)



mike

Search Filter:
☑ Users
☑ Groups
☑ Roles
☐ Computers

Source:
☑ CyberArk Cloud Directory
☑ AD: topgun.local
☑ FDS

		Name	Email	Source
☑	👤	mike_bykat@cy...	mike.bykat@cyberark.com	☁

Add | Cancel

4. Save.

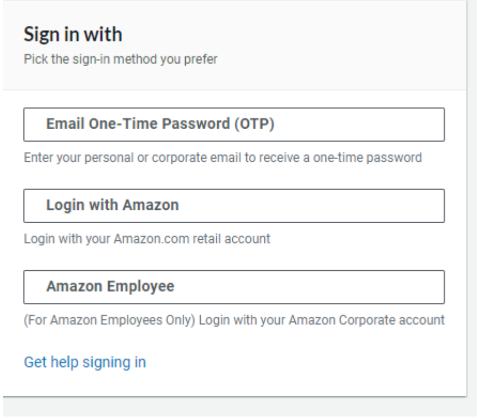
You have now assigned your user to a role that can be used to grant access later in the workshop.

SECTION 2: CREATE 2 AWS EC2 LINUX INSTANCES

Login to AWS

For today’s AWS Immersion Day, AWS has provided AWS accounts for each attendee:

1. Browse to the AWS Event Engine Link shared at the top of this document and in the chat
2. If prompted, enter in 6490-14def39704-77 as your hash
3. Select Email One-Time Password OTP



Sign in with

Pick the sign-in method you prefer

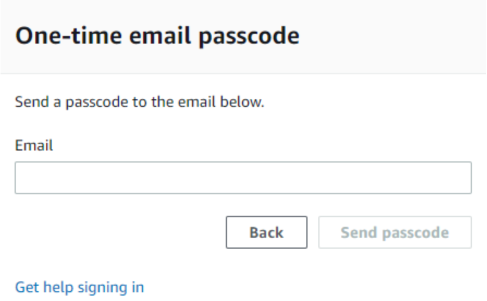
Enter your personal or corporate email to receive a one-time password

Login with your Amazon.com retail account

(For Amazon Employees Only) Login with your Amazon Corporate account

Get help signing in

4. Enter your email



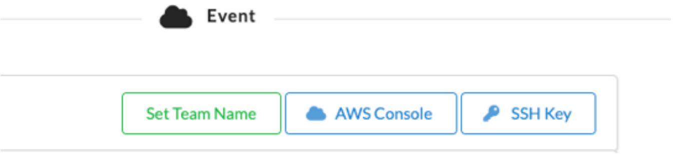
One-time email passcode

Send a passcode to the email below.

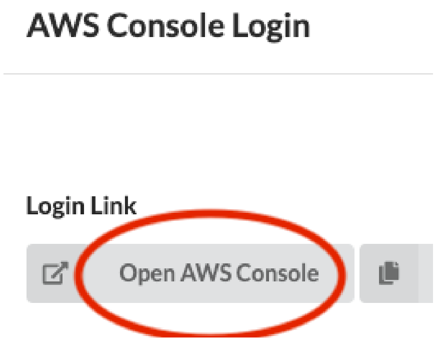
Email

Get help signing in

5. You should receive your one time token.
6. Choose AWS Console



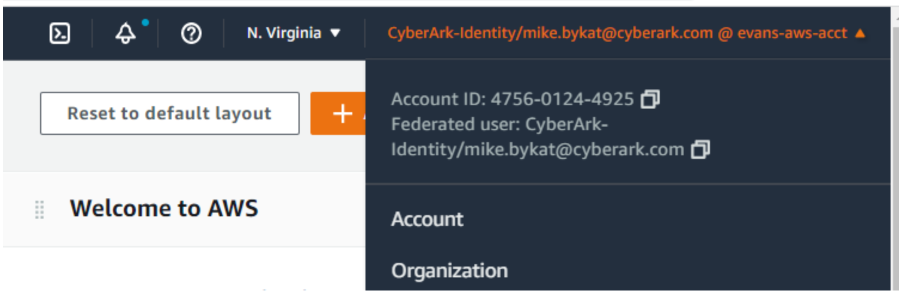
7. Click Open AWS Console



AWS Console Login

Login Link

8. You should now be logged into your individual AWS account. Take note of the AWS account you are working in; it can be found in the top right. You will need this account ID in Section 2 when creating your DPA console configuration. Example screenshot below of where to find the account ID:



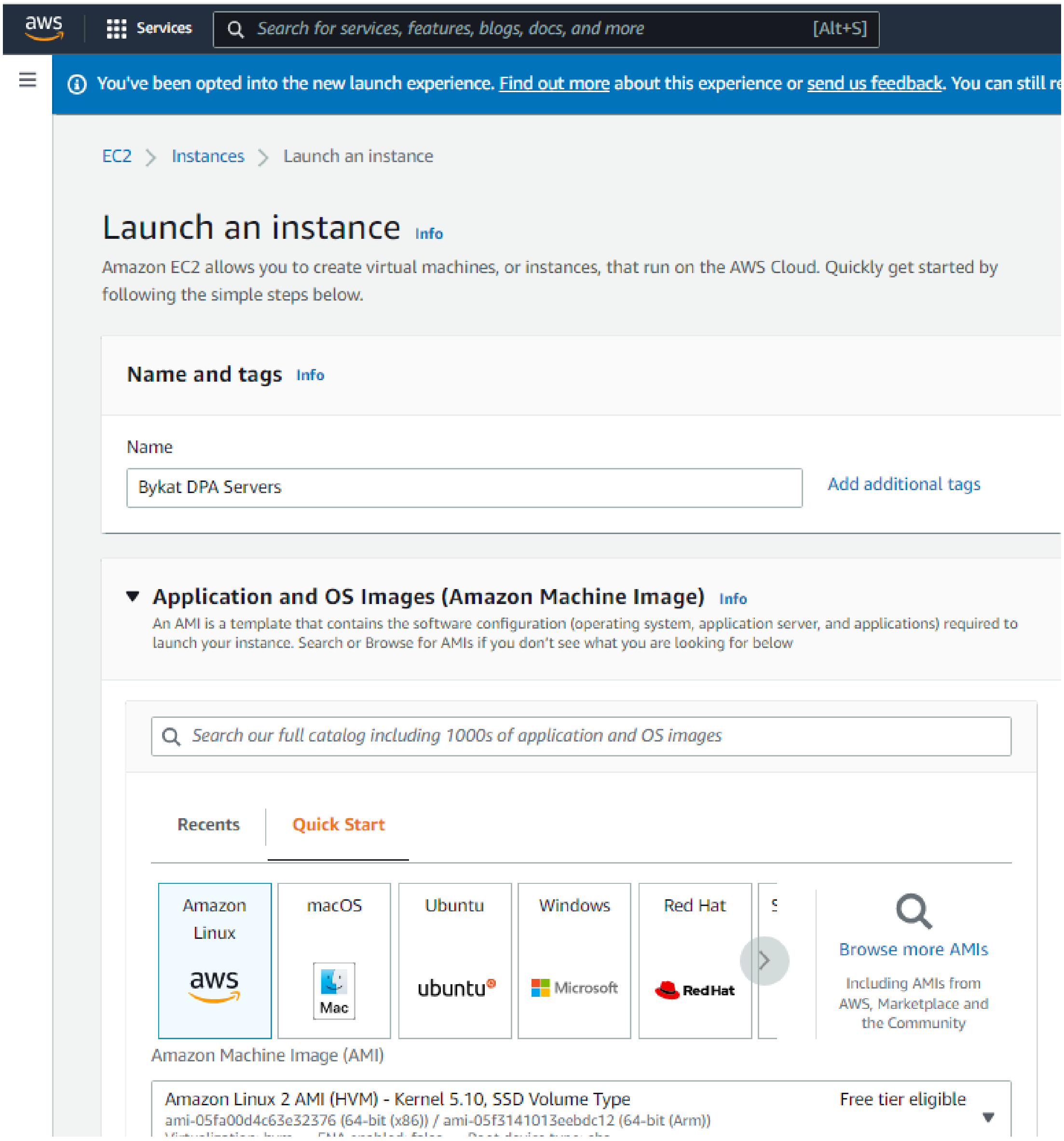
Account ID: 4756-0124-4925

Federated user: CyberArk-Identity/mike.bykat@cyberark.com

Create the DPA connector and target

In this section we will setup (2) EC2 instances that will be your DPA connector and DPA Target with inbound connectivity on port 22.

1. If you haven't done so prior, in the top right corner, change your region to the one identified by your instructor.
2. Navigate to EC2
3. Select Launch Instance > Launch Instance
4. Name your instance {Your name} DPA servers
5. The default selection, Amazon Linux 2 AMI – Kernel 5.10 will work just fine for this workshop; however, customers should reference our documentation when determining server requirements:



aws
Services
Search for services, features, blogs, docs, and more [Alt+S]

You've been opted into the new launch experience. Find out more about this experience or send us feedback. You can still re

EC2 > Instances > Launch an instance

Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Bykat DPA Servers

Add additional tags

Application and OS Images (Amazon Machine Image) Info

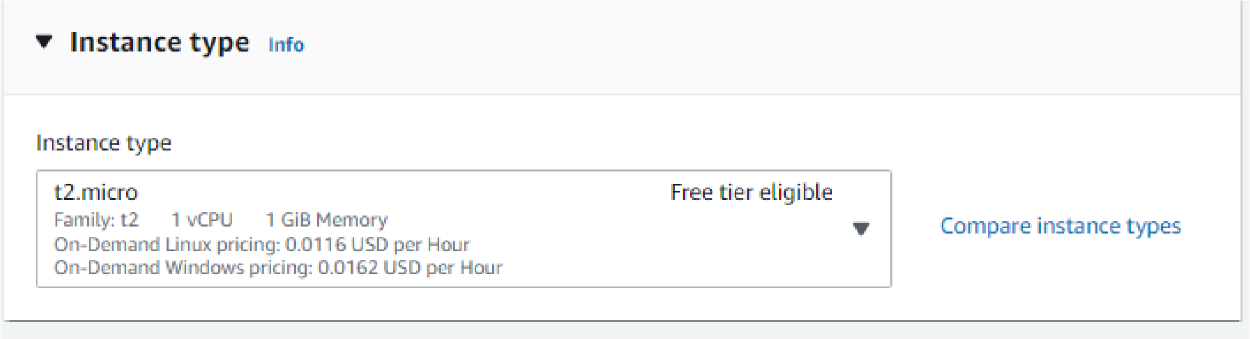
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type — Free tier eligible
ami-05fa00d4c63e32376 (64-bit (x86)) / ami-05f3141013eebdc12 (64-bit (Arm))

6. Similarly, the default free tier t2.micro instance type will work fine for our workshop:

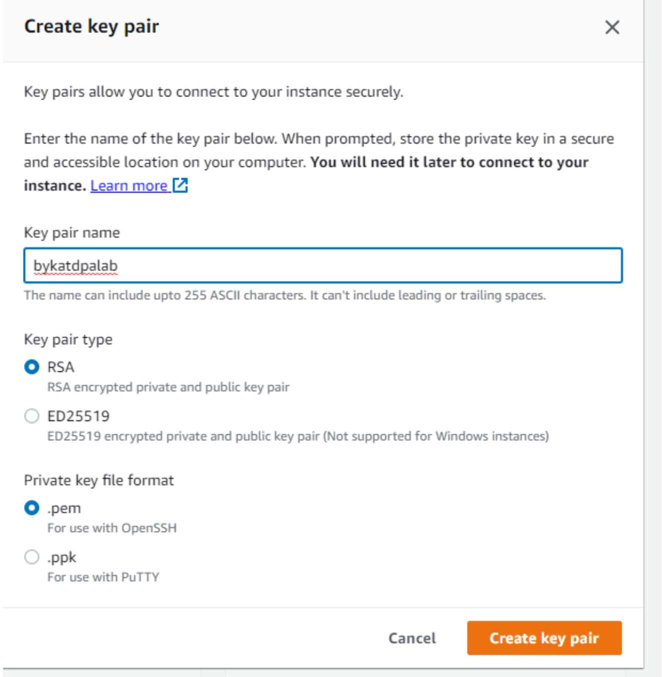


Instance type Info

Instance type

t2.micro — Free tier eligible
Family: t2 1 vCPU 1 GiB Memory
On-Demand Linux pricing: 0.0116 USD per Hour
On-Demand Windows pricing: 0.0162 USD per Hour

7. Click create a new key pair
    a. Name your keypair “Your Name DPA key pair”
    b. Download this keypair to your workstation and make note of the location.



Create key pair ×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** Learn more

Key pair name

bykatdpalab

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

● RSA
RSA encrypted private and public key pair

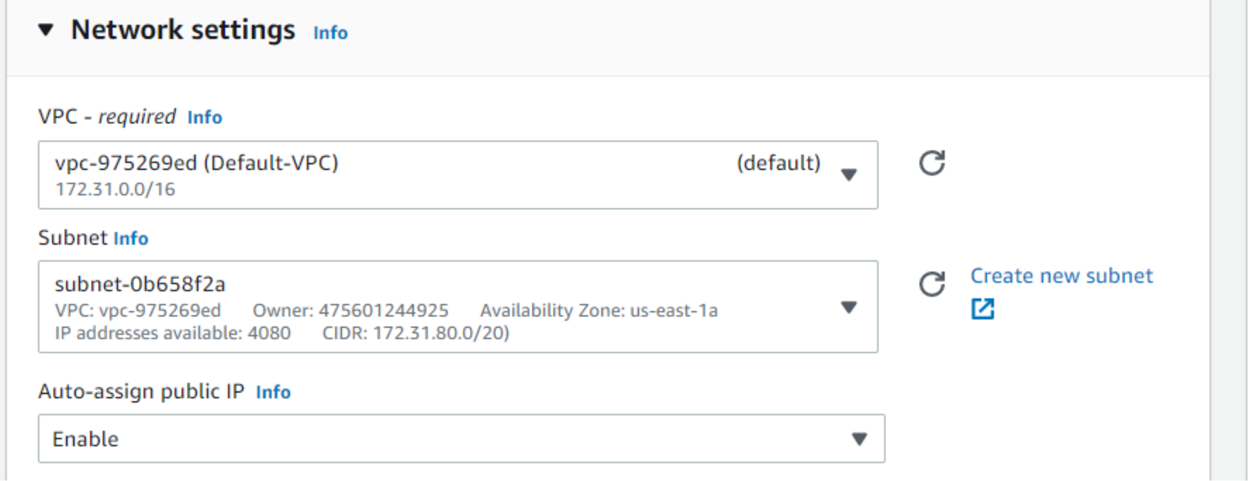
○ ED25519
ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

● .pem
For use with OpenSSH

○ .ppk
For use with PuTTY

8. Edit Network settings:
   a. Make the following updates:
      i. Network: select a VPC.
      ii. Subnet: select a Subnet.
      iii. Ensure Auto-assign public IP is set to enable.
         1. Note: This may not be needed in a production environment if there is VPN/direct connect access to the VMs.



▼ Network settings Info

VPC - *required* Info

vpc-975269ed (Default-VPC) (default)
172.31.0.0/16

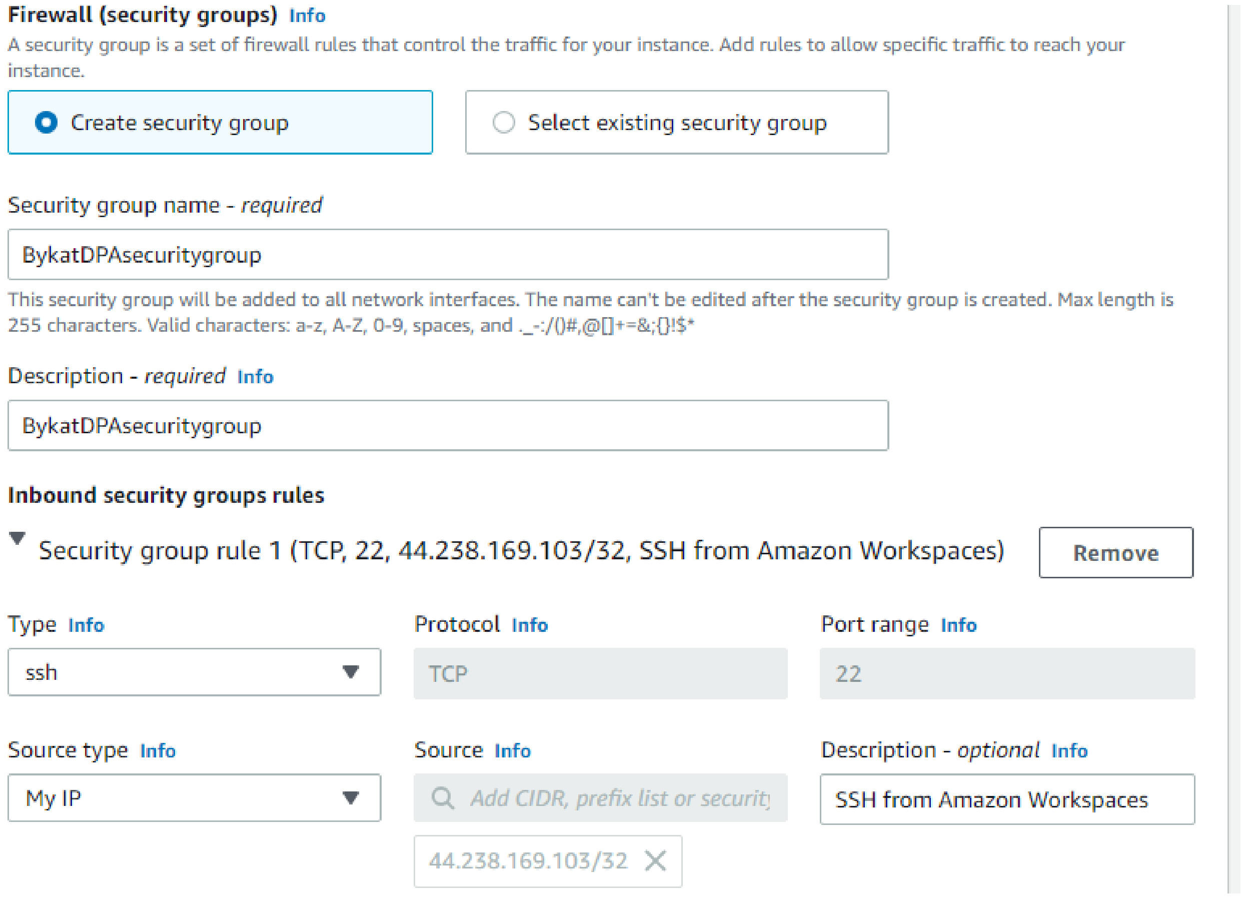
Subnet Info

subnet-0b658f2a
VPC: vpc-975269ed Owner: 475601244925 Availability Zone: us-east-1a
IP addresses available: 4080 CIDR: 172.31.80.0/20)

Auto-assign public IP Info

Enable

      iv. Name your security group “YourNameDPAsecuritygroup”
         1. Change Source type under rule 1 to be “My IP”
         2. Description: SSH from My IP Only
         3. We will edit the security group later to establish trust between the two servers, so make note of what you named it.



Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

● Create security group ○ Select existing security group

Security group name - *required*

BykatDPAsecuritygroup

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*

Description - *required* Info

BykatDPAsecuritygroup

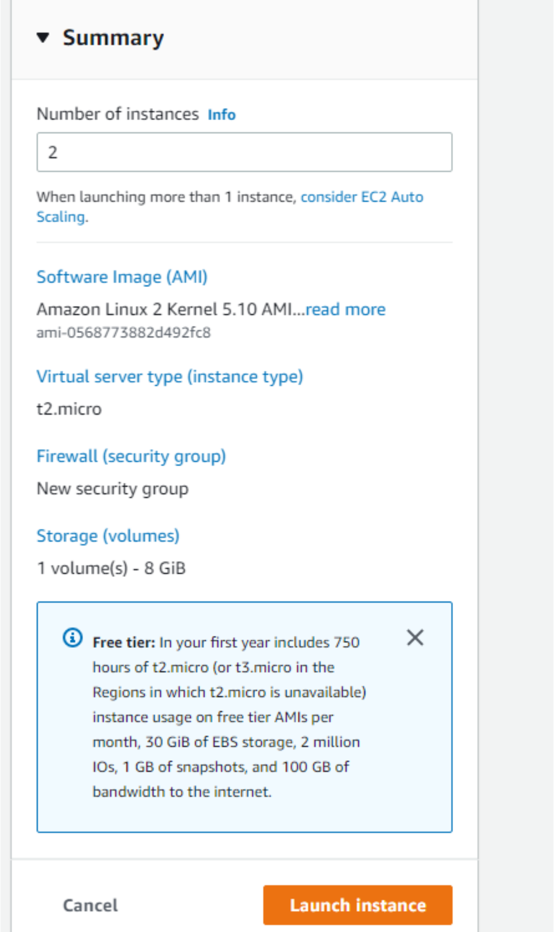
Inbound security groups rules

▼ Security group rule 1 (TCP, 22, 44.238.169.103/32, SSH from Amazon Workspaces) Remove

Type Info	Protocol Info	Port range Info
ssh	TCP	22

Source type Info	Source Info	Description - *optional* Info
My IP	*Add CIDR, prefix list or securit* 44.238.169.103/32 ✕	SSH from Amazon Workspaces

9. Leave other settings as default
10. IMPORTANT: In the top right hand corner increase number of instances from 1 to 2



Number of instances Info

2

When launching more than 1 instance, consider EC2 Auto Scaling.

Software Image (AMI)

Amazon Linux 2 Kernel 5.10 AMI...read more
ami-0568773882d492fc8

Virtual server type (instance type)

t2.micro

Firewall (security group)

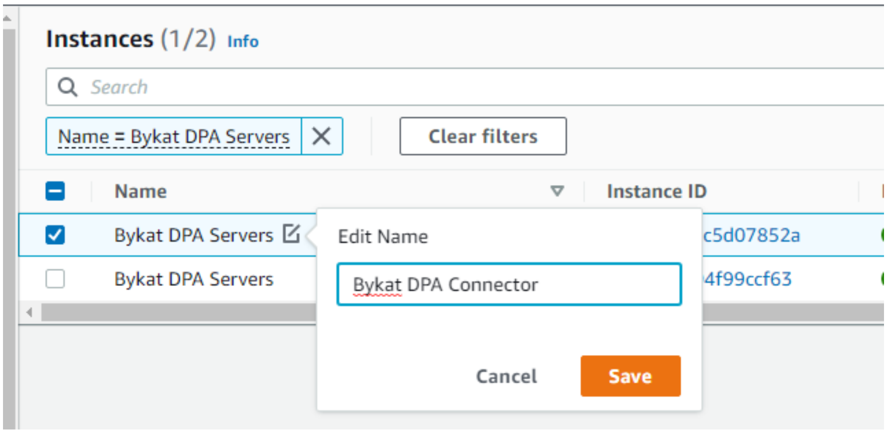
New security group

Storage (volumes)

1 volume(s) - 8 GiB

Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

11. Click Launch
12. Click View All instances and search for YourName DPA
13. Rename one server to YourName DPA Connector and to YourName DPA Target



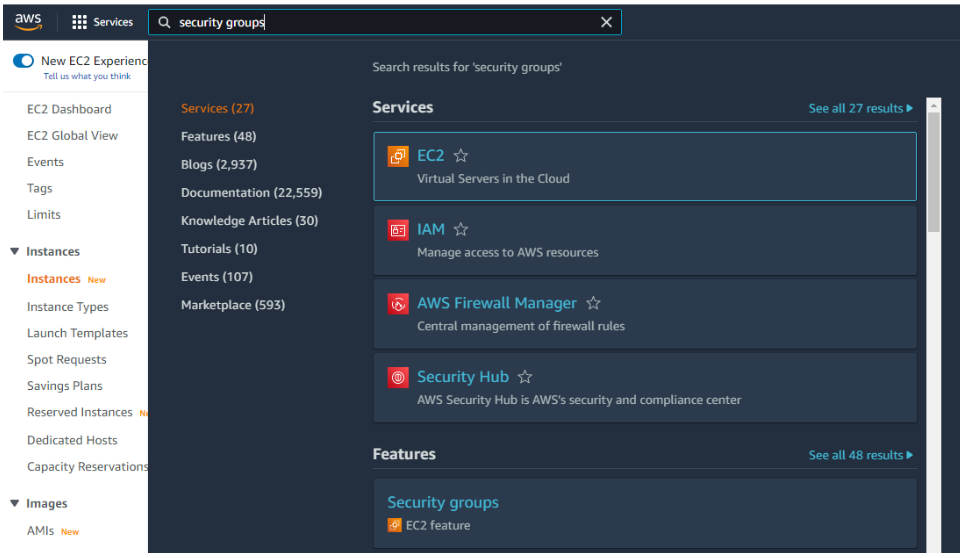
	Name	Instance ID
☑	Bykat DPA Servers	c5d07852a
□	Bykat DPA Servers	4f99ccf63

Edit Name: Bykat DPA Connector

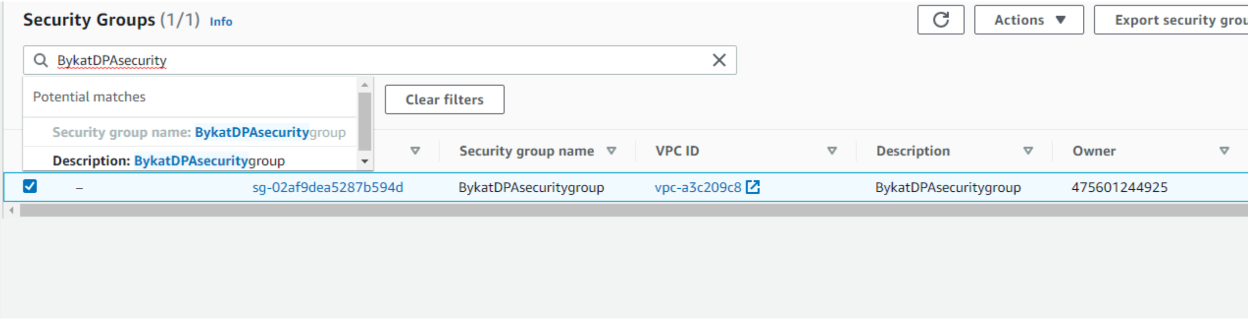
Create trust between EC2 instances

The Connector server needs to reach the target VMs on port 22. We will edit the security group we just created to allow this trust

1. Search for and navigate to Security groups



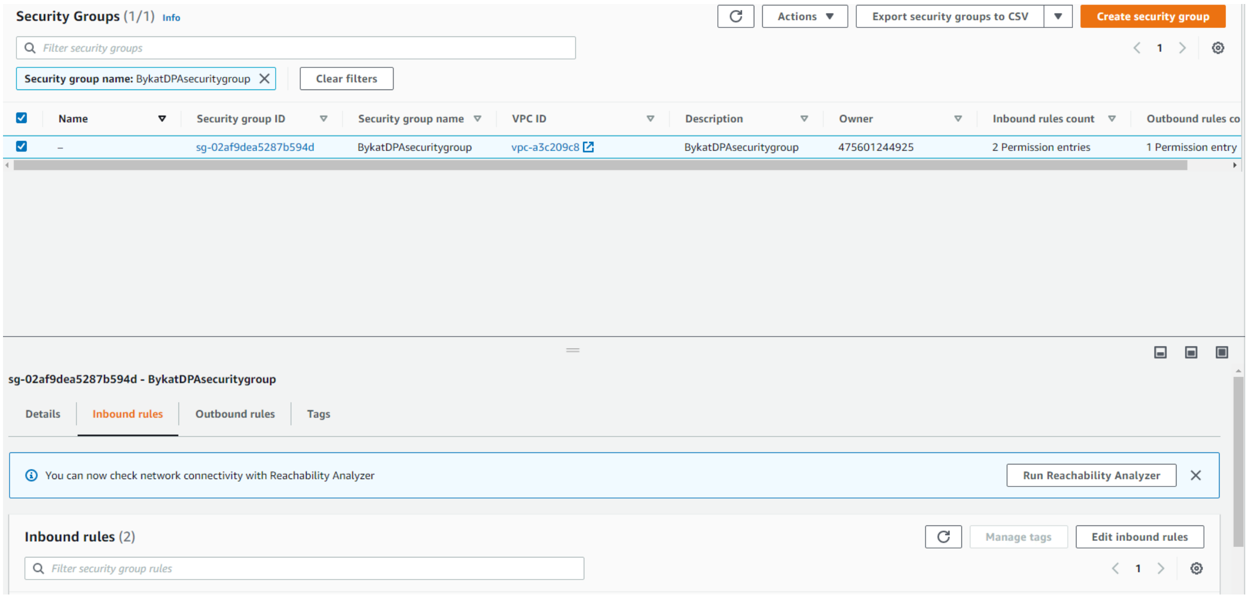
2. Search for the security group you just created called Yourname DPAsecuritygroup



Security Groups (1/1) Info
Actions
Export security grou
BykatDPAsecurity
Potential matches
Security group name: BykatDPAsecuritygroup
Description: BykatDPAsecuritygroup
Clear filters

☑		Security group name	VPC ID	Description	Owner
☑	– sg-02af9dea5287b594d	BykatDPAsecuritygroup	vpc-a3c209c8	BykatDPAsecuritygroup	475601244925

3. Check the box of the security group if it's not already checked
4. Select Inbound rules
5. Select Edit Inbound rules



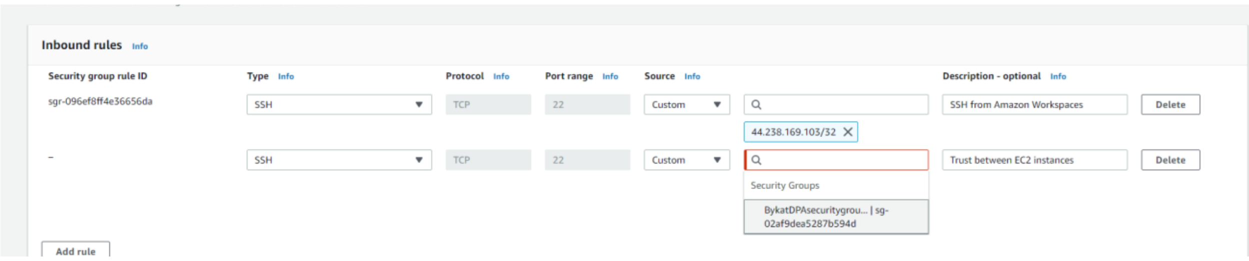
Security Groups (1/1) Info
Actions
Export security groups to CSV
Create security group
Filter security groups
Security group name: BykatDPAsecuritygroup
Clear filters

☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules co
☑	–	sg-02af9dea5287b594d	BykatDPAsecuritygroup	vpc-a3c209c8	BykatDPAsecuritygroup	475601244925	2 Permission entries	1 Permission entry

sg-02af9dea5287b594d - BykatDPAsecuritygroup

You can now check network connectivity with Reachability Analyzer

6. Select add rule
7. Change custom TCP to SSH
8. For source, select 'Custom' and search for the name of your security group
9. Description: Trust between EC2 instances that are part of this security group



Inbound rules Info

Security group rule ID	Type	Protocol	Port range	Source		Description - optional	
sgr-096ef8ff4e36656da	SSH	TCP	22	Custom	44.238.169.103/32	SSH from Amazon Workspaces	Delete
–	SSH	TCP	22	Custom	Security Groups BykatDPAsecuritygrou... | sg-02af9dea5287b594d	Trust between EC2 instances	Delete

10. Save rules

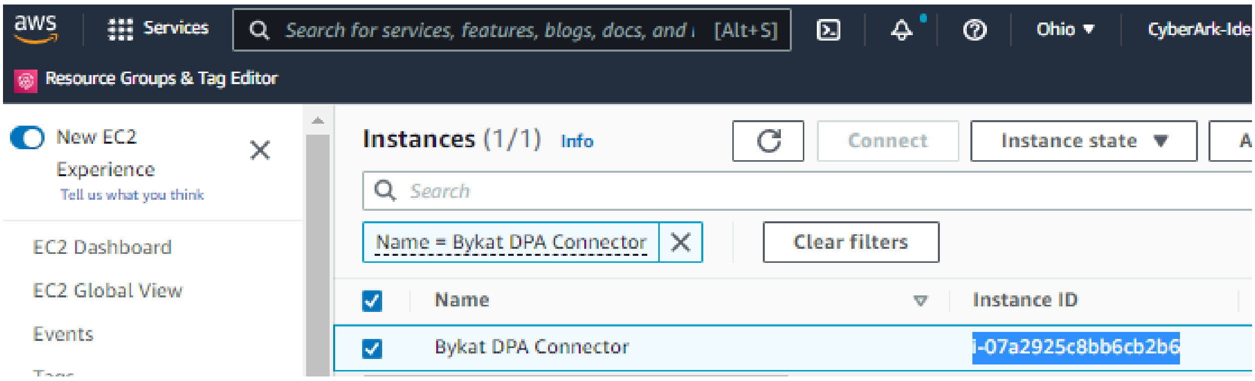
Test Access to the EC2 instances

Test access to DPA Connector

Let’s test access to your instance using PowerShell as your SSH Client.

1. Select your DPA Connector Server
   a. Copy the Public IP address and make note of it in your reference table

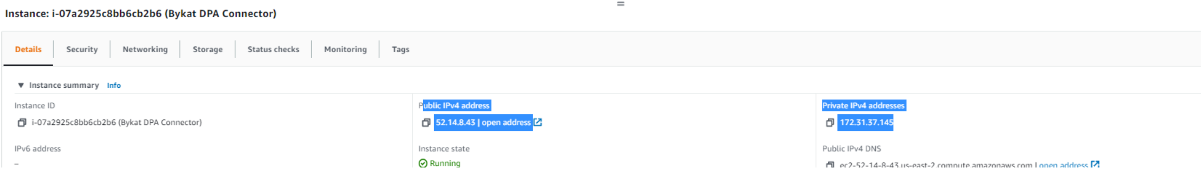
ssh



Name = Bykat DPA Connector

☑	Name	Instance ID
☑	Bykat DPA Connector	i-07a2925c8bb6cb2b6

   b. You can identify the public IP of your instance from the EC2 Console in the details section.



Instance: i-07a2925c8bb6cb2b6 (Bykat DPA Connector)

Instance ID: i-07a2925c8bb6cb2b6 (Bykat DPA Connector)

Public IPv4 address: 52.14.8.43 | open address

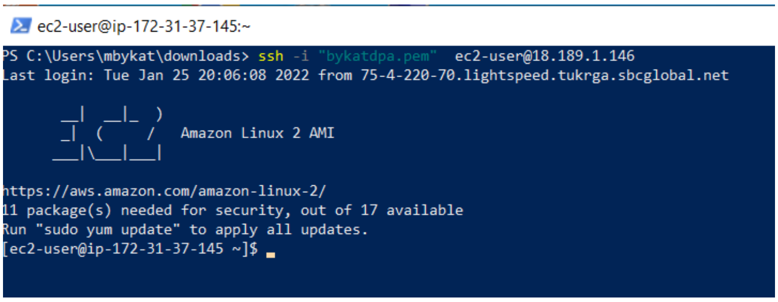
Private IPv4 addresses: 172.31.37.145

IPv6 address: –

Instance state: Running

Public IPv4 DNS: ec2-52-14-8-43.us-east-2.compute.amazonaws.com | open address

2. Open the downloads folder
   a. Click the file tab
   b. On Windows: Choose Open Windows PowerShell > Open Windows PowerShell
   c. On macOS: Launch Terminal and browse to the correct path of they key
   d. On macOS or Linux, Linux doesn't allow use of exposed Private keys so you will need to first run CHMOD 400 on the SSH key in order to set the permissions so the key can be used. Windows does not require this command to be run.
3. Run the following command, updating information according to your specifics:
   a. ***ssh -i “nameofyourcert.pem” ec2-user@publicIPofyourConnector***
   b. Example:



```
ec2-user@ip-172-31-37-145:~
PS C:\Users\mbykat\downloads> ssh -i "bykatdpa.pem"  ec2-user@18.189.1.146
Last login: Tue Jan 25 20:06:08 2022 from 75-4-220-70.lightspeed.tukrga.sbcglobal.net

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
11 package(s) needed for security, out of 17 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-37-145 ~]$ 
```

You've now successfully connected to your DPA Connector server via SSH. You can leave this connection open as we will use it in future steps.

Test access to your DPA Target VM

Repeat the same steps as above, but this time find and use the public IP address of the target VM

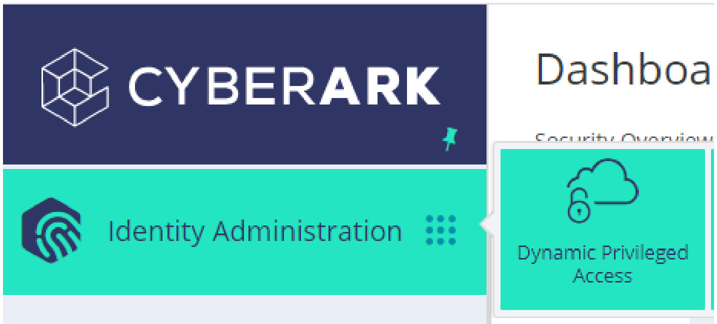
1. When making note of the target public IP, also copy the ec2 Instance ID and make note of it for later
    a. ***Ssh -i "nameofyourcert.pem" ec2-user@publicIPoftarget***

SECTION 3: SETUP AND INSTALL DPA

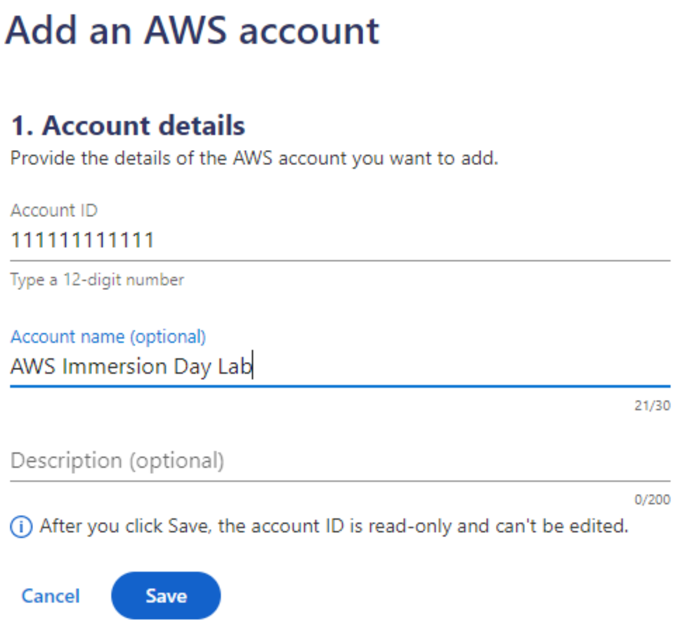
In this section, we will link the DPA environment to the AWS account where you provisioned the EC2 Instances in the section above.

Create a platform in the DPA Console

1. Navigate to Dynamic Privileged Access in the Workshop environment if you're not already there: (reference section 1 if you need to log back in)



2. Select "Platform Management" on the left side
3. Select "Amazon AWS"
4. Select "Add an Account".
    a. Enter the AWS Account ID we made of note of earlier in the table above
    b. Click Save



Add an AWS account

1. Account details

Provide the details of the AWS account you want to add.

Account ID
111111111111
Type a 12-digit number

Account name (optional)
AWS Immersion Day Lab
21/30

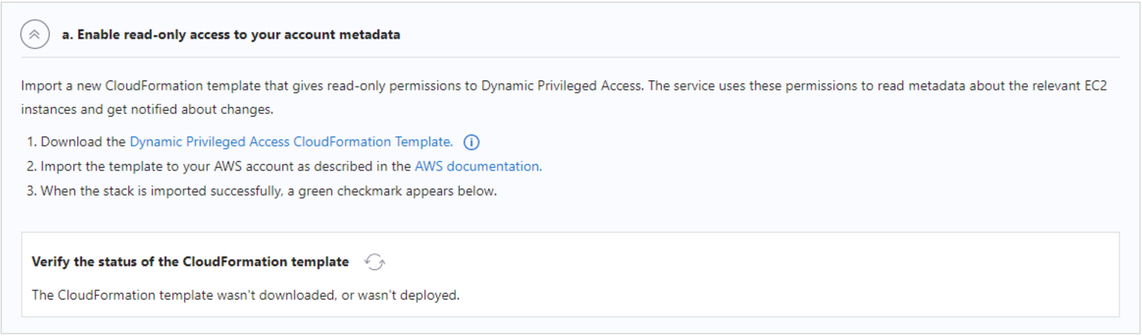
Description (optional)
0/200

ⓘ After you click Save, the account ID is read-only and can't be edited.

Enable read-only access to your account metadata

We'll now use a CloudFormation template to provide DPA the necessary access to the AWS environment specified.

1. In the DPA Console, right click "Dynamic Privileged Access CloudFormation Template" to copy the URL and paste it in the S3 link on the AWS side as shown in the create stack screen in step c. below.



a. Enable read-only access to your account metadata

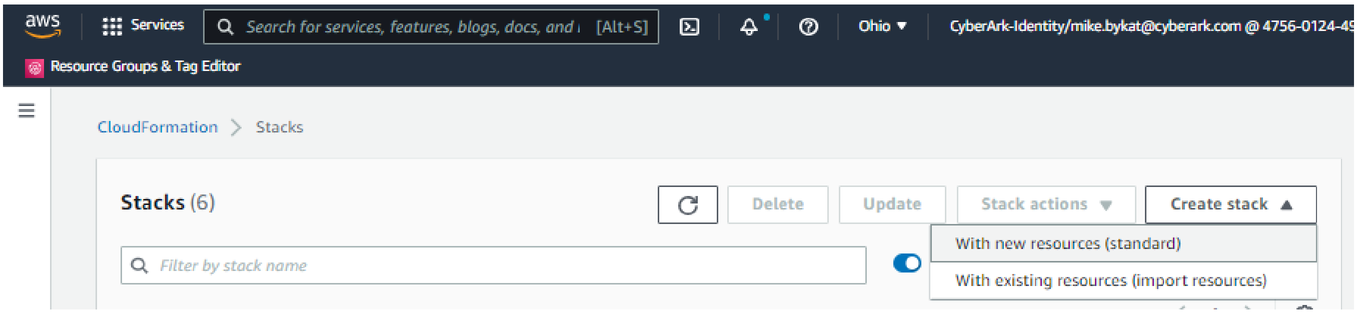
Import a new CloudFormation template that gives read-only permissions to Dynamic Privileged Access. The service uses these permissions to read metadata about the relevant EC2 instances and get notified about changes.

1. Download the Dynamic Privileged Access CloudFormation Template. ⓘ
2. Import the template to your AWS account as described in the AWS documentation.
3. When the stack is imported successfully, a green checkmark appears below.

Verify the status of the CloudFormation template

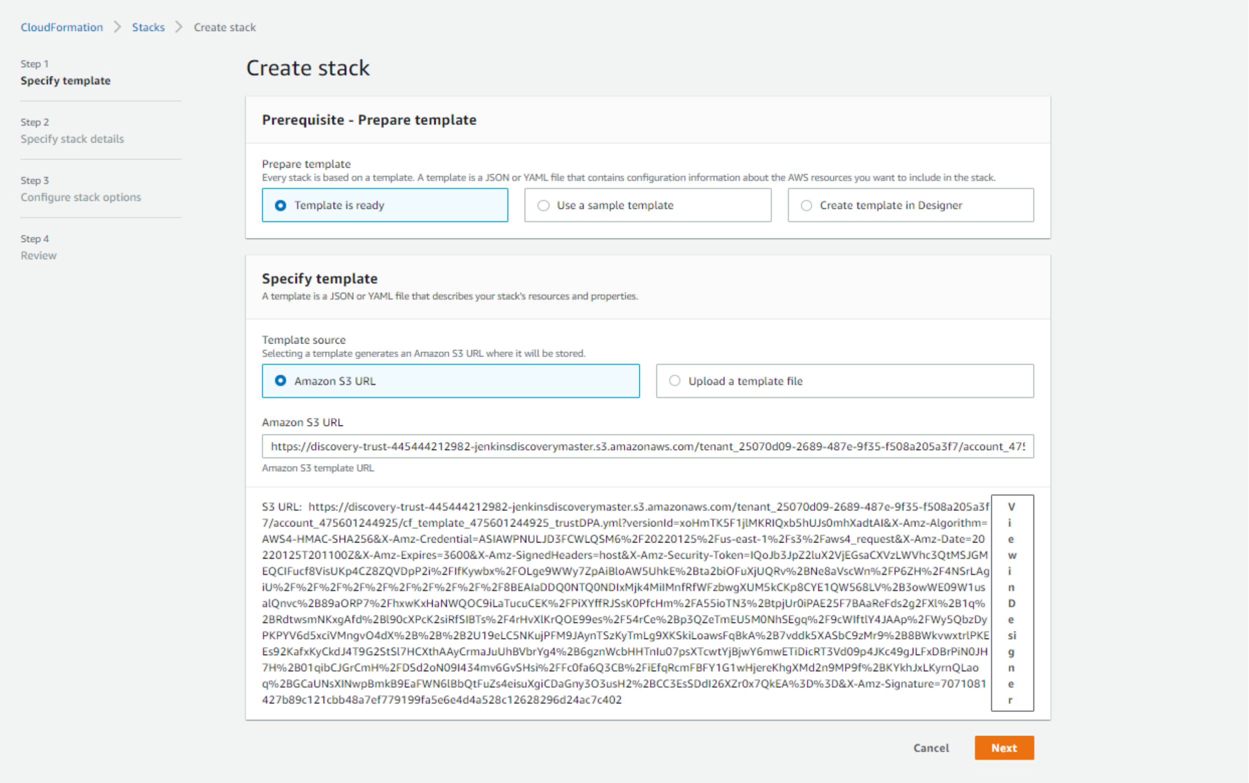
The CloudFormation template wasn't downloaded, or wasn't deployed.

a. In AWS, navigate to CloudFormation and click Create Stack in the top right
b. Choose With new resources (standard)



aws
Services
Search for services, features, blogs, docs, and i [Alt+S]
Ohio ▼
CyberArk-Identity/mike.bykat@cyberark.com @ 4756-0124-49
Resource Groups & Tag Editor
CloudFormation > Stacks
Stacks (6)
Delete
Update
Stack actions ▼
Create stack ▲
With new resources (standard)
With existing resources (import resources)
Filter by stack name

c. If not selected, select Amazon S3 URL radio button and paste the link you copied previously. It will automatically populate the template information as seen below.



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

● Template is ready ○ Use a sample template ○ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

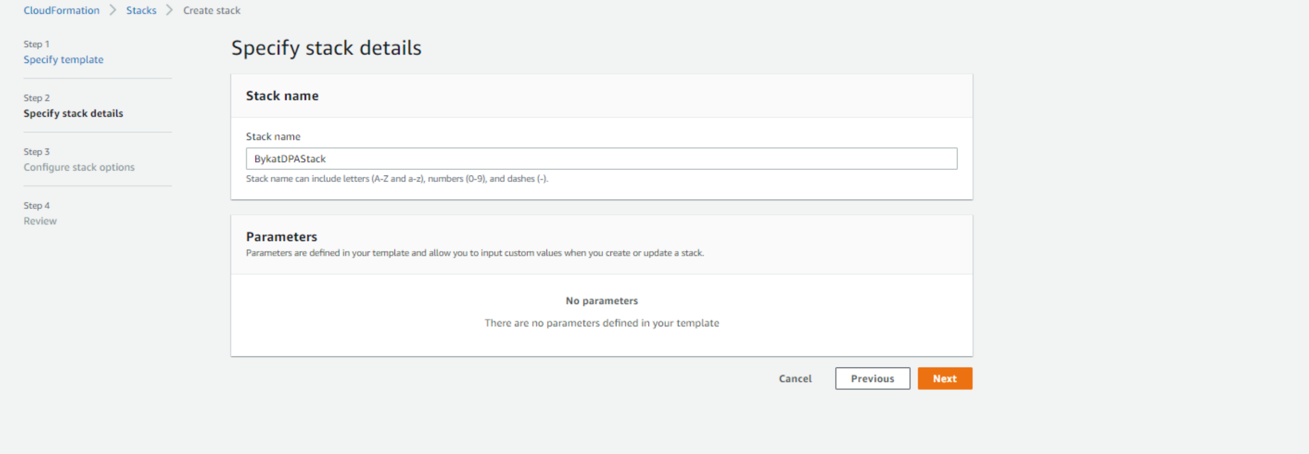
Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

● Amazon S3 URL ○ Upload a template file

Amazon S3 URL
https://discovery-trust-445444212982-jenkinsdiscoverymaster.s3.amazonaws.com/tenant_25070d09-2689-487e-9f35-f508a205a3f7/account_47!
Amazon S3 template URL

```
S3 URL:  https://discovery-trust-445444212982-jenkinsdiscoverymaster.s3.amazonaws.com/tenant_25070d09-2689-487e-9f35-f508a205a3f
7/account_475601244925/cf_template_475601244925_trustDPA.yml?versionId=xoHmTK5F1jlMKRIQxb5hUJs0mhXadtAI&X-Amz-Algorithm=
AWS4-HMAC-SHA256&X-Amz-Credential=ASIAWPNULJD3FCWLQSM6%2F20220125%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20
220125T201100Z&X-Amz-Expires=3600&X-Amz-SignedHeaders=host&X-Amz-Security-Token=IQoJb3JpZ2luX2VjEGsaCXVzLWVhc3QtMSJGM
EQCIFucf8VisUKp4CZ8ZQVDpP2i%2FIfKywbx%2FOLge9WWy7ZpAiBloAW5UhkE%2Bta2biOFuXjUQRv%2BNe8aVscWn%2FP6ZH%2F4NSrLAg
iU%2F%2F%2F%2F%2F%2F%2F%2F%2F%2F8BEAIaDDQ0NTQ0NDIxMjk4MiIMnfRfWFzbwgXUM5kCKp8CYE1QW568LV%2B3owWE09W1us
alQnvc%2B89aORP7%2FhxwKxHaNWQOC9iLaTucuCEK%2FPiXYffRJSsK0PfcHm%2FA55ioTN3%2BtpjUr0iPAE25F7BAaReFds2g2FXl%2B1q%
2BRdtwsmNKxgAfd%2Bl90cXPcK2siRfSIBTs%2F4rHvXlKrQOE99es%2F54rCe%2Bp3QZeTmEU5M0NhSEgq%2F9cWIftlY4JAAp%2FWy5QbzDy
PKPYV6d5xciVMngvO4dX%2B%2B%2B2U19eLC5NKujPFM9JAynTSzKyTmLg9XKSkiLoawsFqBkA%2B7vddk5XASbC9zMr9%2B8BWkvwxtrlPKE
Es92KafxKyCkdJ4T9G2StSl7HCXthAAyCrmaJuUhBVbrYg4%2B6gznWcbHHTnIu07psXTcwtYjBjwY6mwETiDicRT3Vd09p4JKc49gJLFxDBrPiN0JH
7H%2B01qibCJGrCmH%2FDSd2oN09I434mv6GvSHsi%2FFc0fa6Q3CB%2FiEfqRcmFBFY1G1wHjereKhgXMd2n9MP9f%2BKYkhJxLKyrnQLao
q%2BGCaUNsXINwpBmkB9EaFWN6lBbQtFuZs4eisuXgiCDaGny3O3usH2%2BCC3EsSDdI26XZr0x7QkEA%3D%3D&X-Amz-Signature=7071081
427b89c121cbb48a7ef779199fa5e6e4d4a528c12628296d24ac7c402
```

d. Click ‘Next’ and Name your stack accordingly.



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

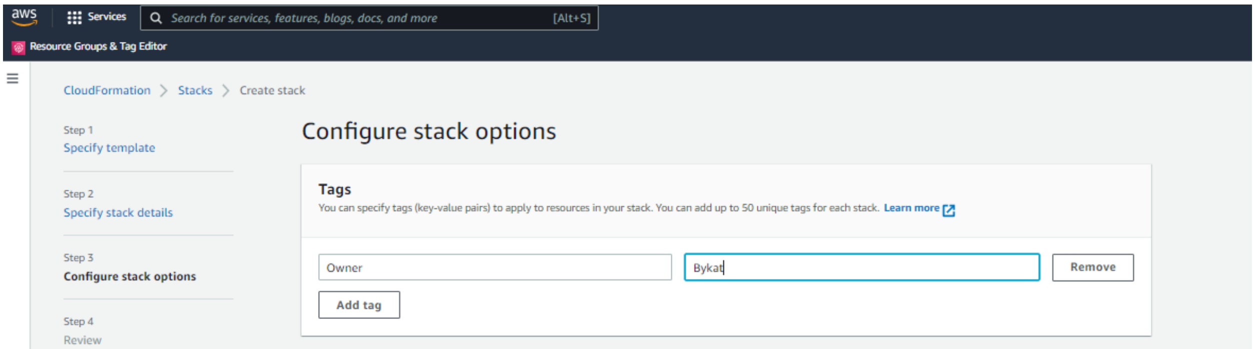
Stack name

Stack name
BykatDPAStack
Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters
Parameters are defined in your template and allow you to input custom values when you create or update a stack.

No parameters
There are no parameters defined in your template

e. Click ‘Next’ and create a tag called ‘Owner’ and your name as the value.


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Resource Groups & Tag Editor
CloudFormation > Stacks > Create stack
Step 1
Specify template
Step 2
Specify stack details
Step 3
Configure stack options
Step 4
Review
Remove
Add tag

Configure stack options

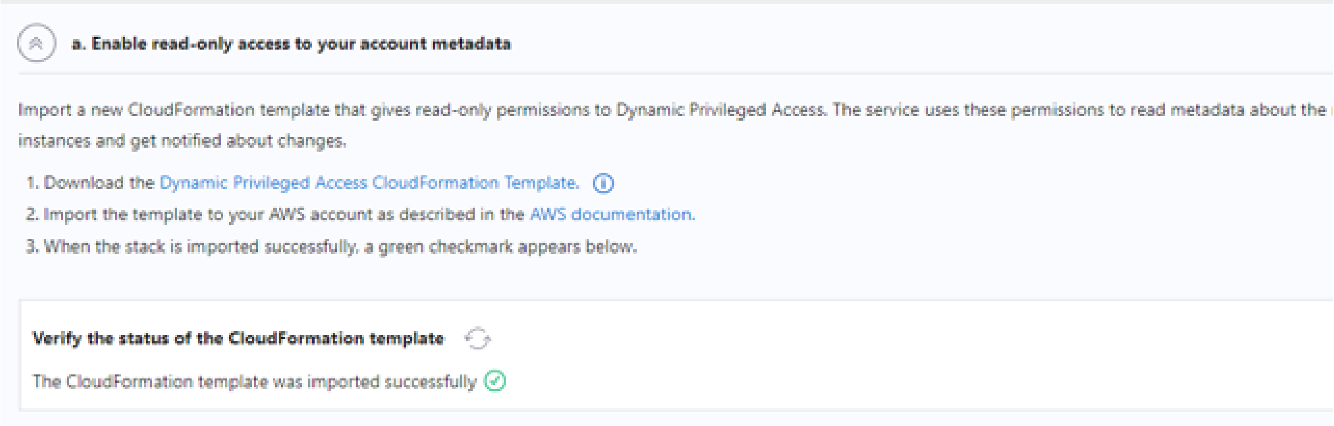
Tags

You can specify tags (key-value pairs) to apply to resources in your stack. You can add up to 50 unique tags for each stack. Learn more

Owner: Bykat

f. Click Next.

g. At the bottom of the page Check the box to Acknowledge then click ‘Create stack’. In about 30 seconds, refresh status in DPA console:



a. Enable read-only access to your account metadata

Import a new CloudFormation template that gives read-only permissions to Dynamic Privileged Access. The service uses these permissions to read metadata about the instances and get notified about changes.

1. Download the Dynamic Privileged Access CloudFormation Template.
2. Import the template to your AWS account as described in the AWS documentation.
3. When the stack is imported successfully, a green checkmark appears below.

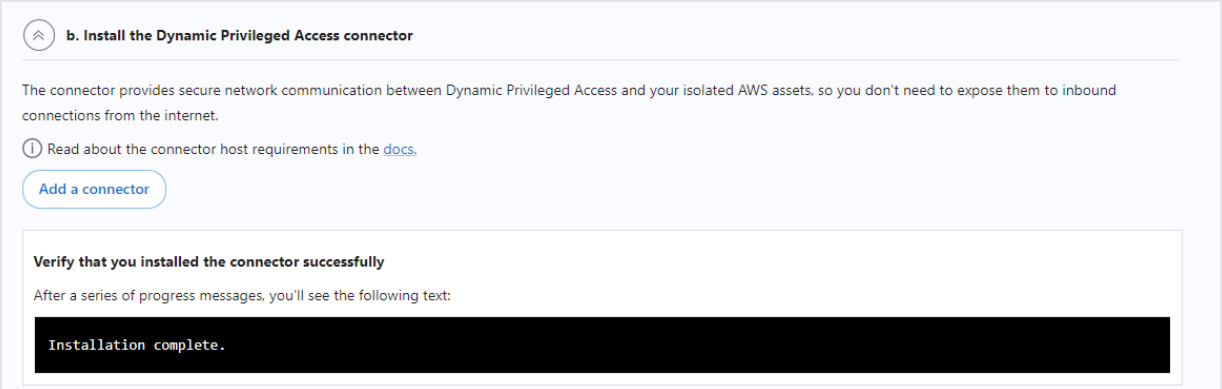
Verify the status of the CloudFormation template

The CloudFormation template was imported successfully ✓

Install the connector using the “Get Script” option.

Now, we’ll run the DPA connector installation script on the connector you created.

1. Under section B, click Add a connector.



b. Install the Dynamic Privileged Access connector

The connector provides secure network communication between Dynamic Privileged Access and your isolated AWS assets, so you don't need to expose them to inbound connections from the internet.

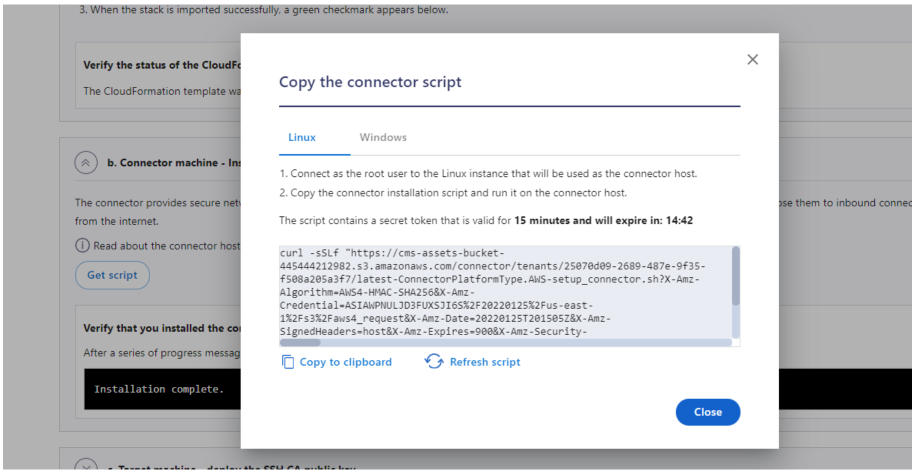
Read about the connector host requirements in the docs.

Verify that you installed the connector successfully

After a series of progress messages, you'll see the following text:

```
Installation complete.
```

2. Select Linux and choose next
3. Click Copy to clipboard



3. When the stack is imported successfully, a green checkmark appears below.

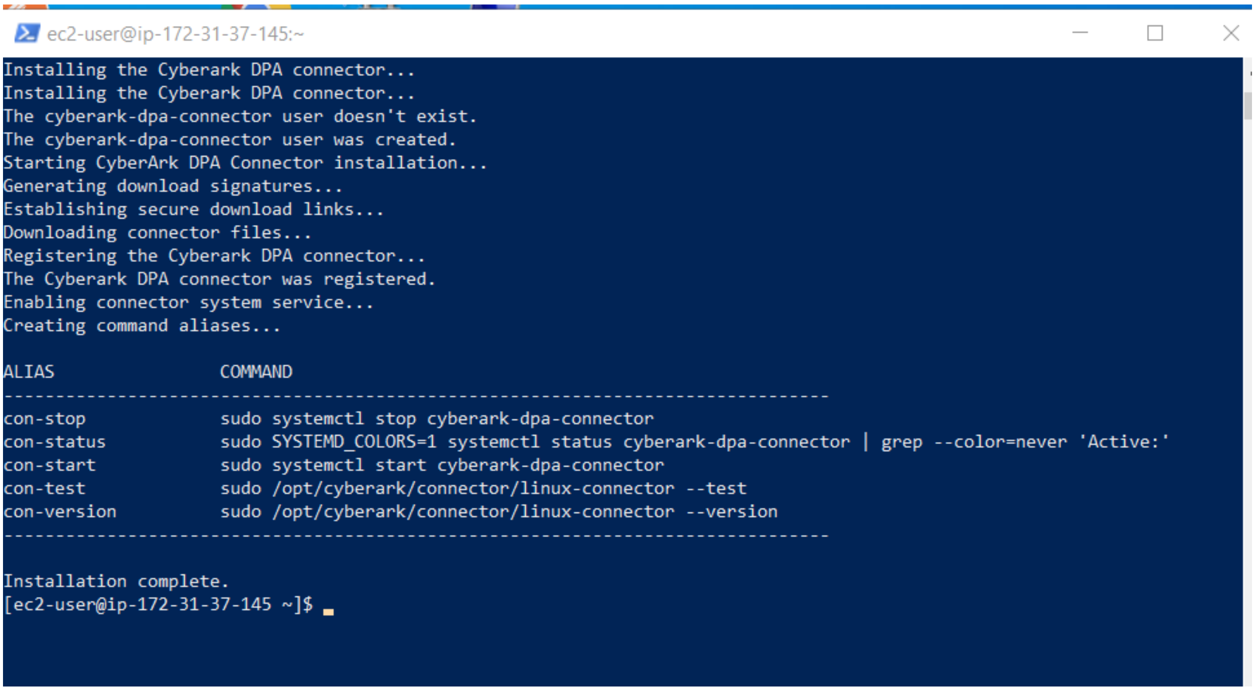
Copy the connector script

1. Connect as the root user to the Linux instance that will be used as the connector host.
2. Copy the connector installation script and run it on the connector host.

The script contains a secret token that is valid for **15 minutes and will expire in: 14:42**

```
curl -sSLf "https://cms-assets-bucket-
445444212982.s3.amazonaws.com/connector/tenants/25070d09-2689-487e-9f35-
f508a205a3f7/latest-ConnectorPlatformType.AWS-setup_connector.sh?X-Amz-
Algorithm=AWS4-HMAC-SHA256&X-Amz-
Credential=ASIAWPNULJD3FUXSJI6S%2F20220125%2Fus-east-
1%2Fs3%2Faws4_request&X-Amz-Date=20220125T201505Z&X-Amz-
SignedHeaders=host&X-Amz-Expires=900&X-Amz-Security-
```

4. Once copied, paste into the open PowerShell/Terminal SSH session to the Connector you established prior, or reconnect to your connector if needed. A right click of your mouse should auto paste. You should see something like this:



```
Installing the Cyberark DPA connector...
Installing the Cyberark DPA connector...
The cyberark-dpa-connector user doesn't exist.
The cyberark-dpa-connector user was created.
Starting CyberArk DPA Connector installation...
Generating download signatures...
Establishing secure download links...
Downloading connector files...
Registering the Cyberark DPA connector...
The Cyberark DPA connector was registered.
Enabling connector system service...
Creating command aliases...

ALIAS                   COMMAND
--------------------------------------------------------------------------------
con-stop                sudo systemctl stop cyberark-dpa-connector
con-status              sudo SYSTEMD_COLORS=1 systemctl status cyberark-dpa-connector | grep --color=never 'Active:'
con-start               sudo systemctl start cyberark-dpa-connector
con-test                sudo /opt/cyberark/connector/linux-connector --test
con-version             sudo /opt/cyberark/connector/linux-connector --version
--------------------------------------------------------------------------------

Installation complete.
[ec2-user@ip-172-31-37-145 ~]$ _
```

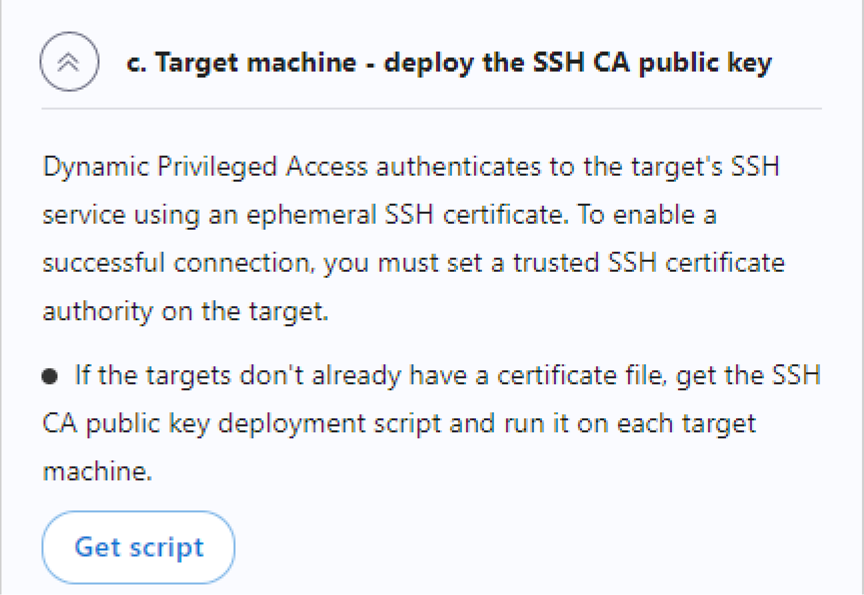
**If you get an error that ’Signature Expired’ - Go back to DPA and select ’Refresh Script’. Once refreshed, Copy to Clipboard again, paste into your PowerShell/Terminal window and run it again.

Deploy SSH CA on target machine

DPA works by having a public key on all target machines that the DPA connector can create a matching, temporary Private key to use for the connection. Customers can include this key as part of their server template, so when the VM spins up the public SSH key is already there. For this exercise, we will deploy the public key manually.

To do this, we’ll now run the SSH CA public key script from the DPA console:

1. Under section C, click Get Script.

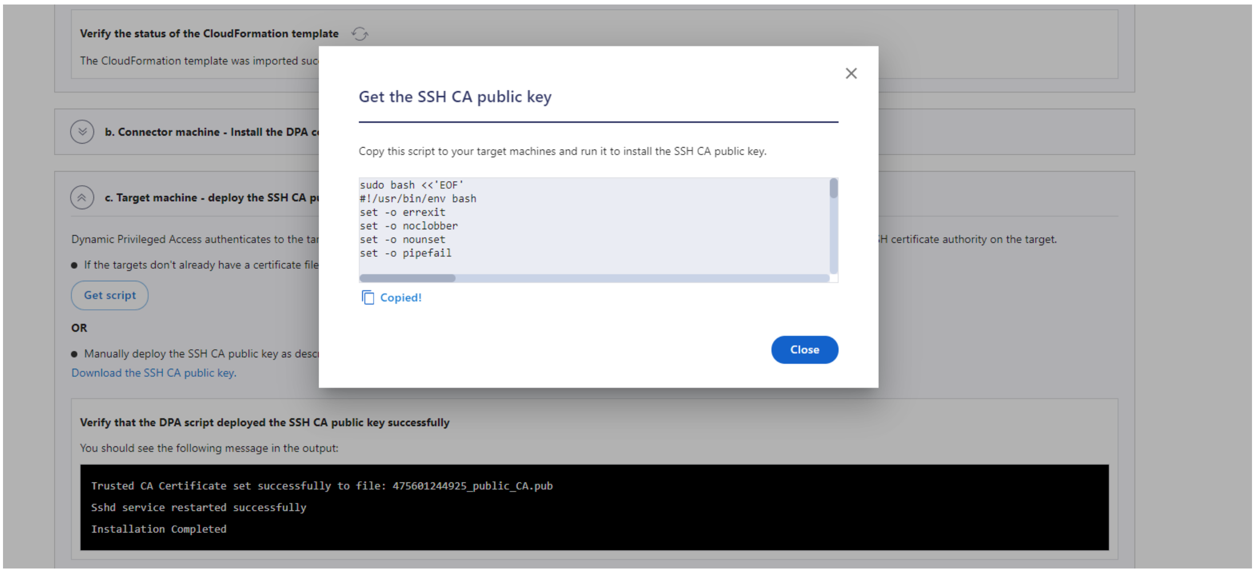


c. Target machine - deploy the SSH CA public key

Dynamic Privileged Access authenticates to the target's SSH service using an ephemeral SSH certificate. To enable a successful connection, you must set a trusted SSH certificate authority on the target.

- If the targets don't already have a certificate file, get the SSH CA public key deployment script and run it on each target machine.

2. Copy the script



Verify the status of the CloudFormation template
b. Connector machine - Install the DPA c
c. Target machine - deploy the SSH CA p
Get script
OR
Download the SSH CA public key.
Copied!
Close

The CloudFormation template was imported suc

Dynamic Privileged Access authenticates to the tar … H certificate authority on the target.

- If the targets don't already have a certificate file
- Manually deploy the SSH CA public key as desc

Get the SSH CA public key

Copy this script to your target machines and run it to install the SSH CA public key.

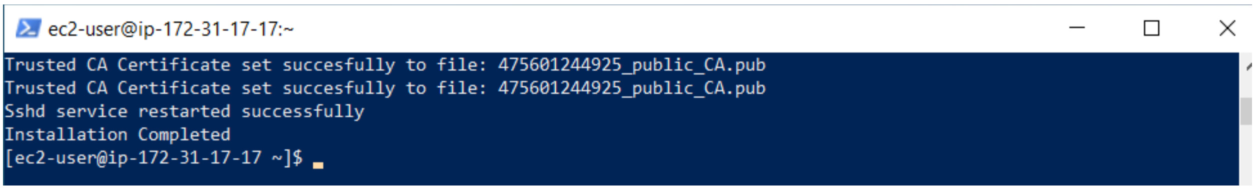
```
sudo bash <<'EOF'
#!/usr/bin/env bash
set -o errexit
set -o noclobber
set -o nounset
set -o pipefail
```

Verify that the DPA script deployed the SSH CA public key successfully

You should see the following message in the output:

```
Trusted CA Certificate set successfully to file: 475601244925_public_CA.pub
Sshd service restarted successfully
Installation Completed
```

3. Paste the script into the target server PowerShell/Terminal SSH session you established earlier or reconnect.
4. After pasting in, you should receive the following:



```
Trusted CA Certificate set succesfully to file: 475601244925_public_CA.pub
Trusted CA Certificate set succesfully to file: 475601244925_public_CA.pub
Sshd service restarted successfully
Installation Completed
[ec2-user@ip-172-31-17-17 ~]$ 
```

5. In the DPA console, Save your platform management settings.

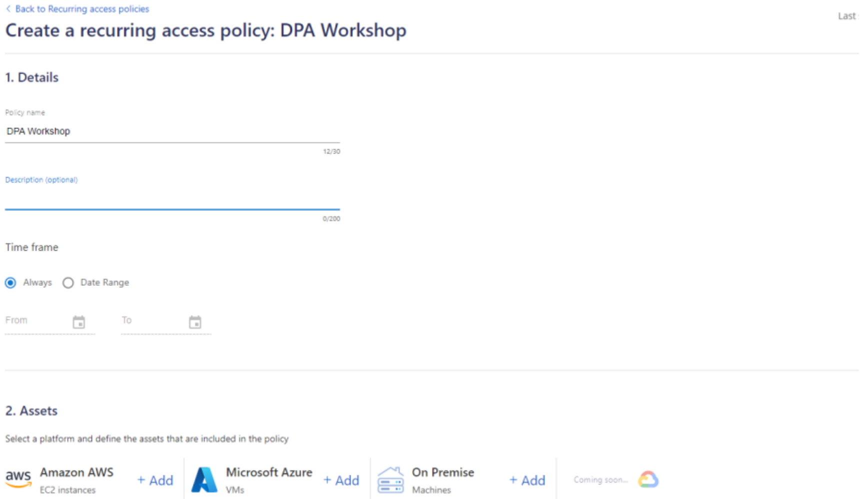
Congratulations! You have completed installation and configuration of all system requirements!

SECTION 4: RECURRING ACCESS POLICY

In this section, we will create an Access Policy that determines what machines (Using ABAC), who (Using CyberArk Identity), and when someone can connect to the target machine.

Create a DPA Access Policy

1. In DPA Console, navigate to Recurring access policies on the left-hand side and choose 'create policy'.
2. Name the Policy 'UserName DPA Workshop'.



‹ Back to Recurring access policies

Create a recurring access policy: DPA Workshop

Last

1. Details

Policy name: DPA Workshop (12/30)

Description (optional) (0/200)

Time frame

● Always ○ Date Range

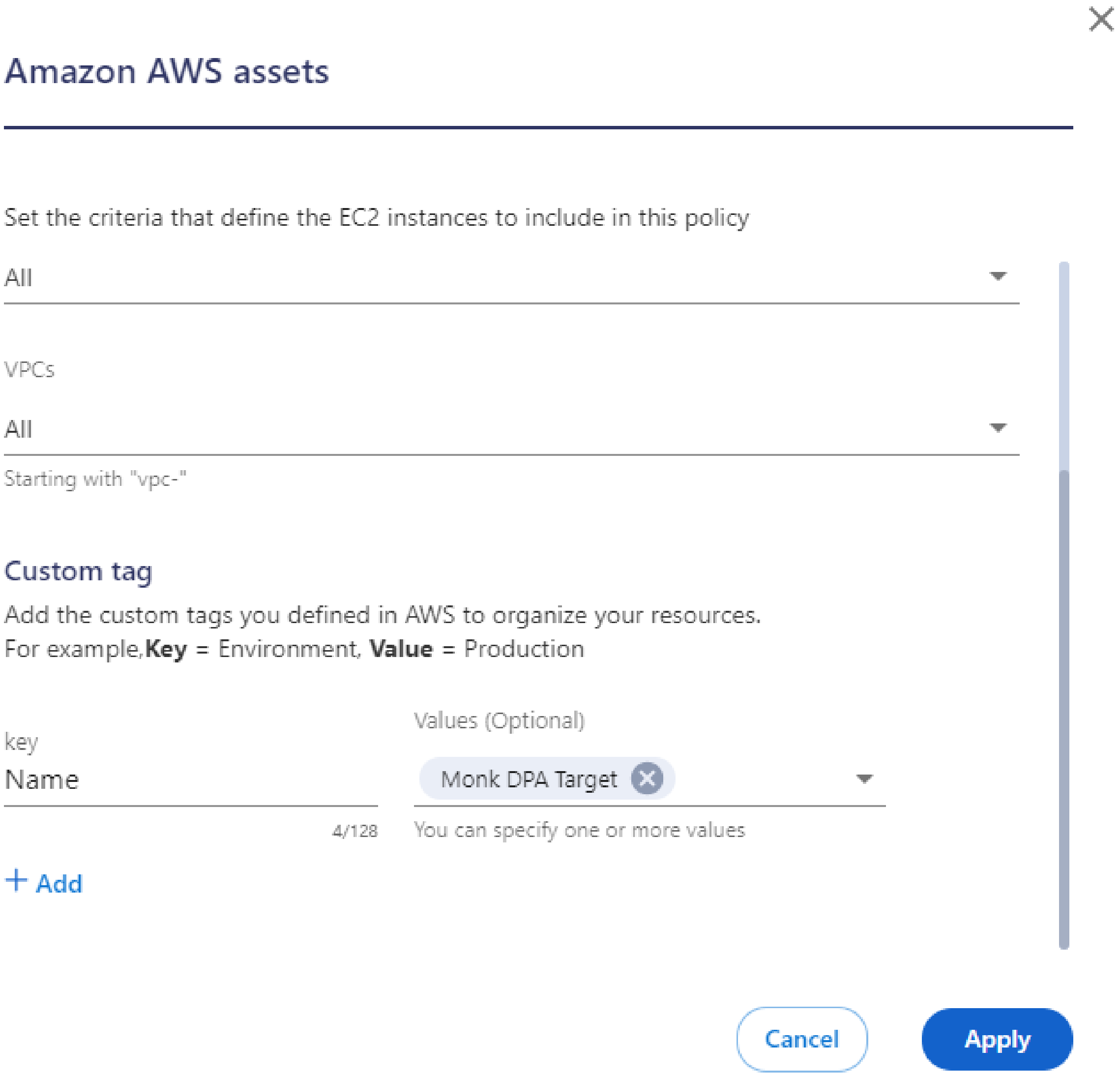
From To

2. Assets

Select a platform and define the assets that are included in the policy

aws Amazon AWS EC2 instances + Add
Microsoft Azure VMs + Add
On Premise Machines + Add
Coming soon...

3. Add an Amazon AWS instance under Assets
    a. This is where we set the Attribute Based Access Control that really differentiates DPA. Keep the default setting, 'All' for regions and VPCs, but use custom 'Name' tag created for your DPA Target server.
    b. You can find the tag by looking at your EC2 Instance, this is case sensitive!



Amazon AWS assets

Set the criteria that define the EC2 instances to include in this policy

All

VPCs

All

Starting with "vpc-"

Custom tag

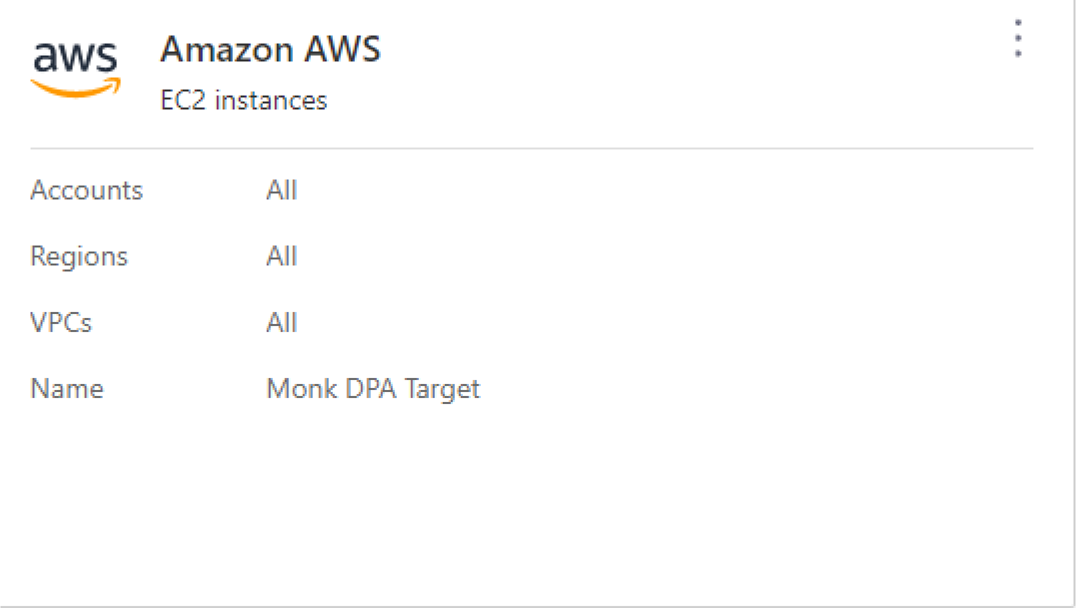
Add the custom tags you defined in AWS to organize your resources.
For example, **Key** = Environment, **Value** = Production

key: Name (4/128)

Values (Optional): Monk DPA Target

You can specify one or more values

4. Click Apply. Your console should look like this:

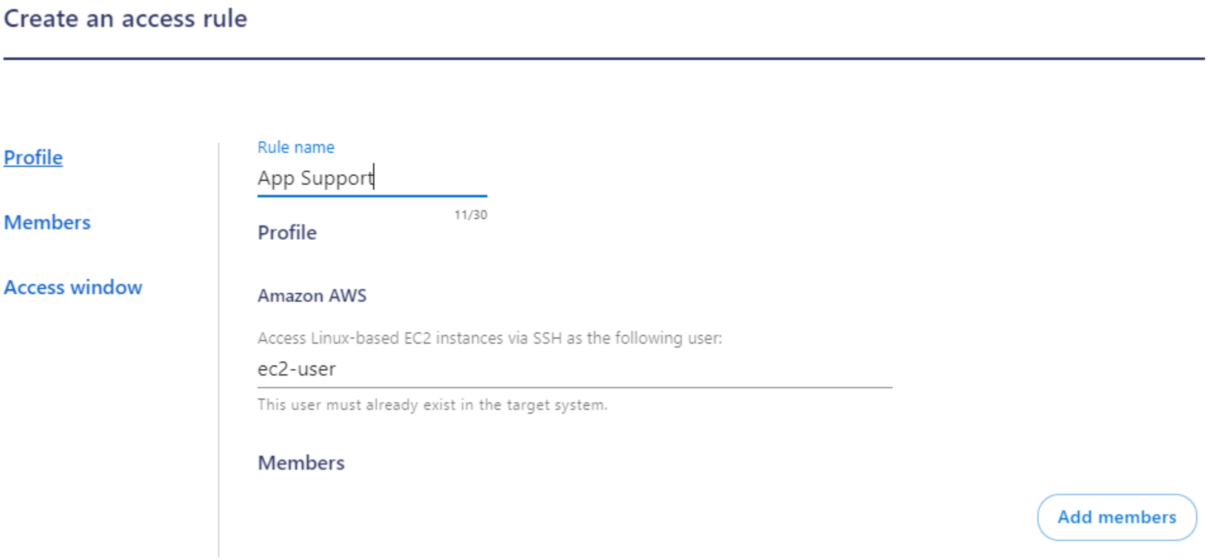


Amazon AWS

EC2 instances

Accounts	All
Regions	All
VPCs	All
Name	Monk DPA Target

5. Scroll down to the Access Rules section and select ‘Create an access rule’.
    a. Name your rule App Support or you can be creative if you wish
    b. Select EC2-user as the user that users will be logged in as on the machine
    c. Select ‘Add Members’ and search for YourName.



Create an access rule

Rule name: App Support

11/30

Profile

Amazon AWS

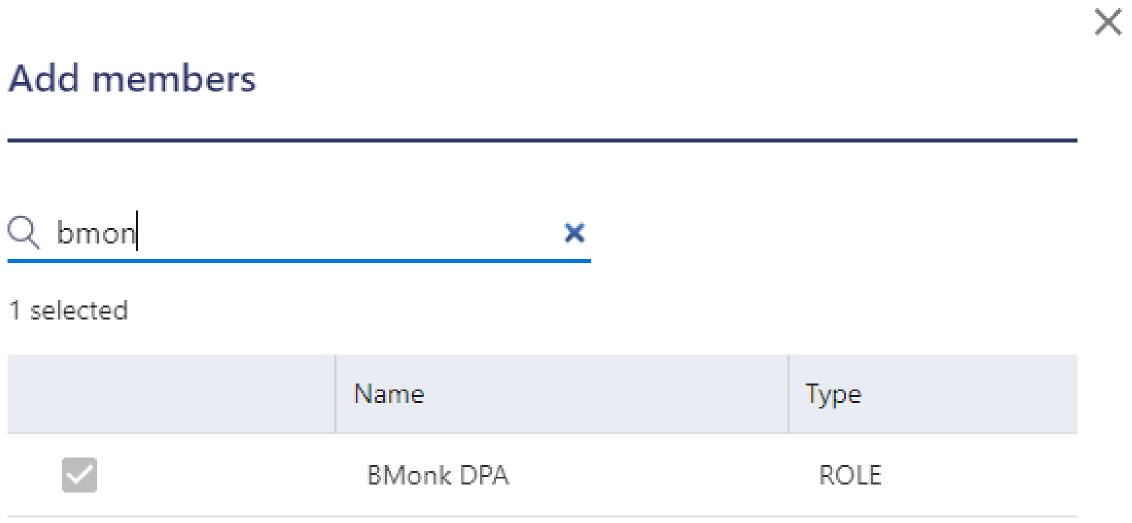
Access Linux-based EC2 instances via SSH as the following user:

ec2-user

This user must already exist in the target system.

Members

    d. Select the Role in we created in Identity previously. Click Add.



Add members

bmon

1 selected

	Name	Type
☑	BMonk DPA	ROLE

   e. Leave the default access window times or change to your liking, but confirm it includes your current time zone!

6. Click Create

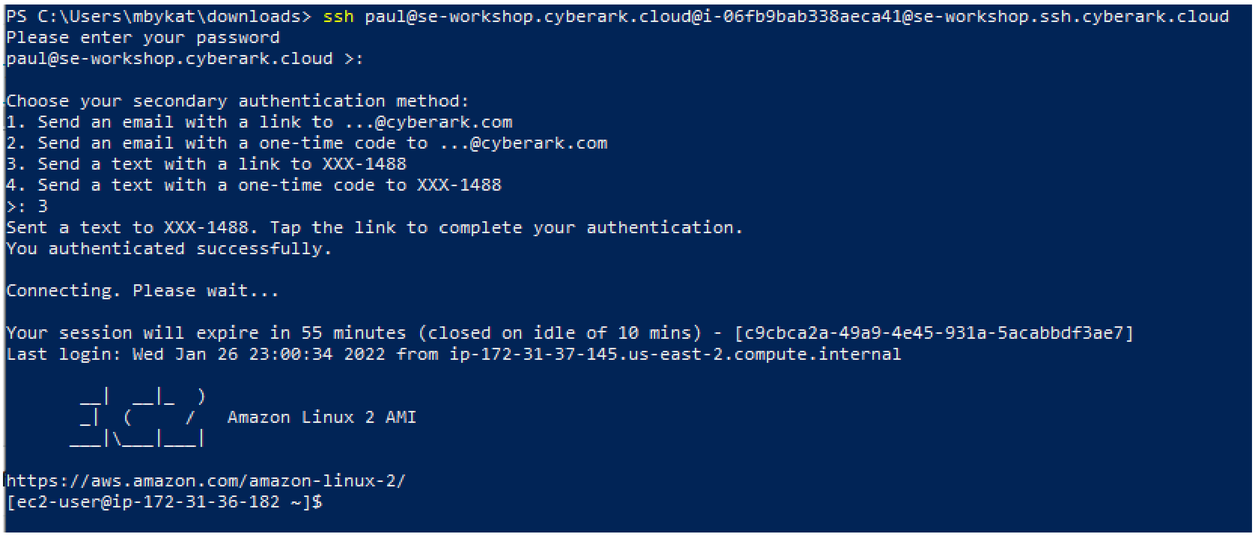
Awesome, it's now time to see it in action!

SECTION 5: CONNECT VIA DPA

Let's test!

1. Open PowerShell/Terminal on your local machine or your CLI of choice
2. Grab the ec2 instanceID of the target machine from the AWS Console to build the following connection string:
    a. Ssh user@yourDPAtenant@AWSInstanceID@yourDPAtenant.ssh.cyberark.cloud

    b. Mine looks like: Ssh firstname.lastname@cyberark.cloud.####@i-06fb9bab338aeca41@tenantname.ssh.cyberark.cloud
3. Hit enter or click connect
4. You will first be prompted for your password
5. Choose MFA to your email or phone (if it was provided in your user account)
6. If authenticated and authorized, you will be connected as the ec2-user on your target machine. That target is now reachable from your remote location with no VPN required.



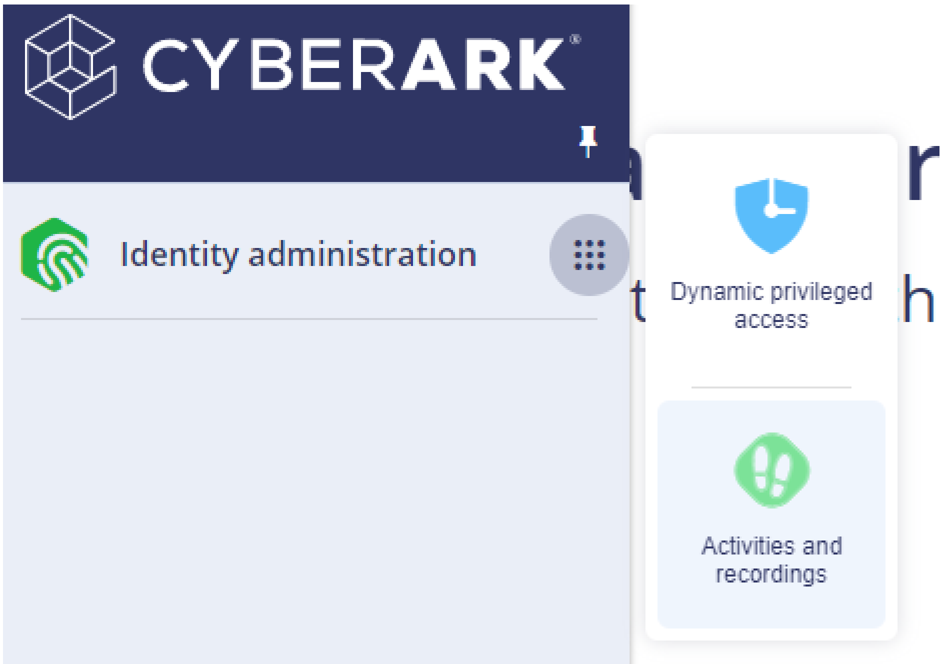
```
PS C:\Users\mbykat\downloads> ssh paul@se-workshop.cyberark.cloud@i-06fb9bab338aeca41@se-workshop.ssh.cyberark.cloud
Please enter your password
paul@se-workshop.cyberark.cloud >:

Choose your secondary authentication method:
1. Send an email with a link to ...@cyberark.com
2. Send an email with a one-time code to ...@cyberark.com
3. Send a text with a link to XXX-1488
4. Send a text with a one-time code to XXX-1488
>: 3
Sent a text to XXX-1488. Tap the link to complete your authentication.
You authenticated successfully.

Connecting. Please wait...

Your session will expire in 55 minutes (closed on idle of 10 mins) - [c9cbca2a-49a9-4e45-931a-5acabbdf3ae7]
Last login: Wed Jan 26 23:00:34 2022 from ip-172-31-37-145.us-east-2.compute.internal

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-36-182 ~]$
```

7. Run a command to trigger some audit information, such as ls or pwd.
8. Exit your session

Review Audit information

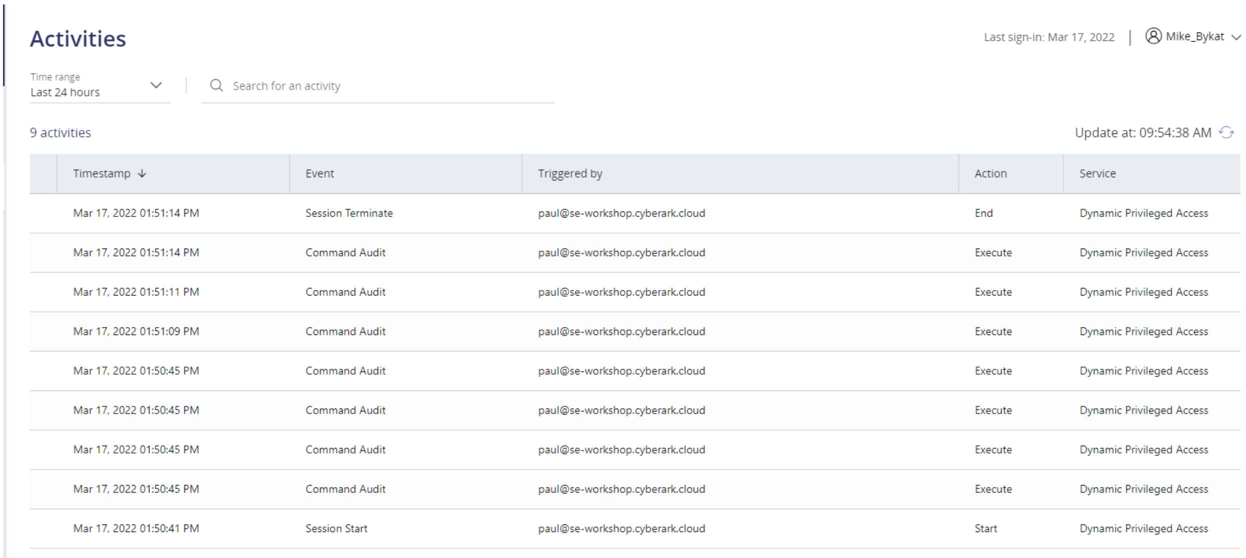
In this section we will review the Activities and Recordings section for auditing the sessions that have been established via DPA.

1. In the DPA console, select Activities and recordings as seen below.



2. You will be provided with a list of all activities of the last 24 hours by default. You could change this filter in the top left corner if you wanted.
   a. Note, it may take a couple minutes for session activity to appear.
3. Review the session you just established.
   a. You'll see the time of the activity, the event type, and who triggered it.
   b. You can select a particular event for additional session details.

c. PM/R&D may ask for some of this info if you're requesting troubleshooting assistance.



Activities

Last sign-in: Mar 17, 2022 | Mike_Bykat

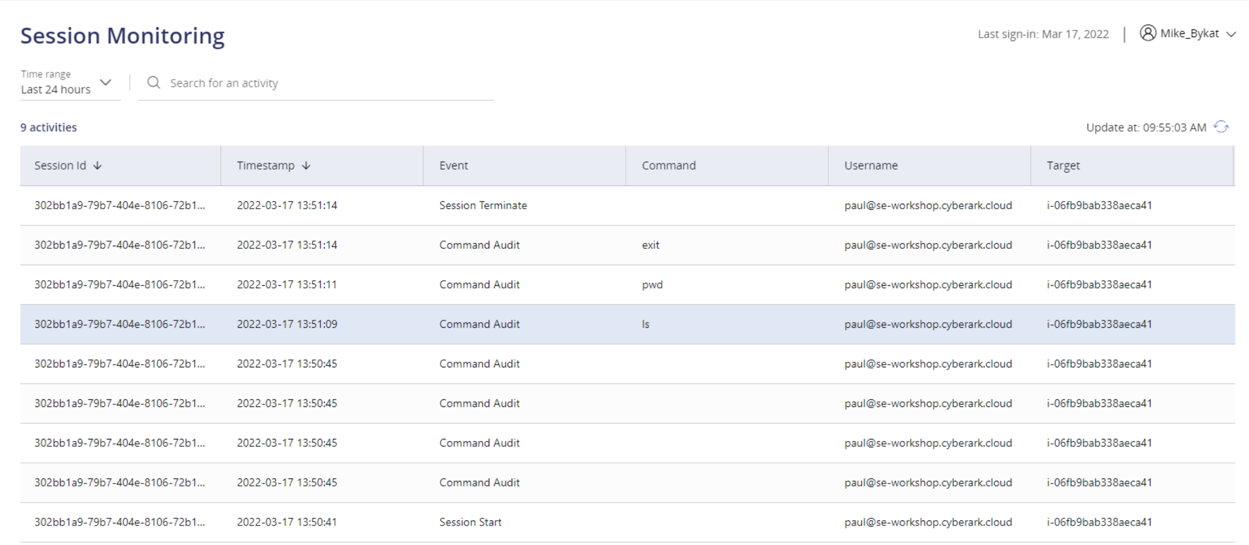
Time range: Last 24 hours | Search for an activity

9 activities

Update at: 09:54:38 AM

Timestamp	Event	Triggered by	Action	Service
Mar 17, 2022 01:51:14 PM	Session Terminate	paul@se-workshop.cyberark.cloud	End	Dynamic Privileged Access
Mar 17, 2022 01:51:14 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:51:11 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:51:09 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:50:45 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:50:45 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:50:45 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:50:45 PM	Command Audit	paul@se-workshop.cyberark.cloud	Execute	Dynamic Privileged Access
Mar 17, 2022 01:50:41 PM	Session Start	paul@se-workshop.cyberark.cloud	Start	Dynamic Privileged Access

4. Navigate to Session Monitoring on the left-hand side
5. Here you will see the actual commands that were run during this session, such as the ls and/or pwd.
   a. You can select a particular event for additional session details.



Session Monitoring

Last sign-in: Mar 17, 2022 | Mike_Bykat

Time range: Last 24 hours | Search for an activity

9 activities

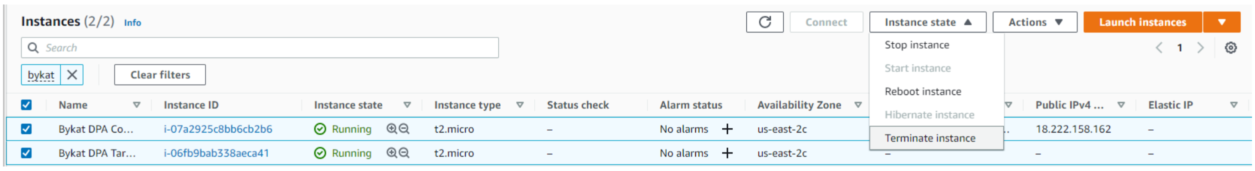
Update at: 09:55:03 AM

Session Id	Timestamp	Event	Command	Username	Target
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:51:14	Session Terminate		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:51:14	Command Audit	exit	paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:51:11	Command Audit	pwd	paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:51:09	Command Audit	ls	paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:50:45	Command Audit		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:50:45	Command Audit		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:50:45	Command Audit		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:50:45	Command Audit		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41
302bb1a9-79b7-404e-8106-72b1...	2022-03-17 13:50:41	Session Start		paul@se-workshop.cyberark.cloud	i-06fb9bab338aeca41

SECTION 6: CLEAN UP

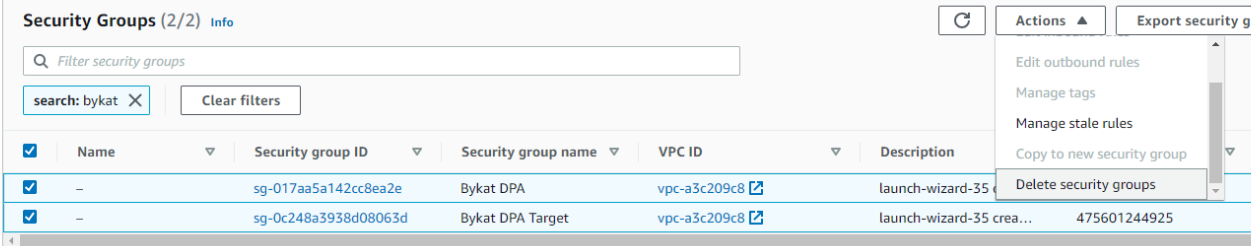
It's always best practice to delete your AWS resources to clean your AWS account.

1. Remove 2 AWS EC2 Instances
   a. Navigate to EC2>Instances
   b. Search for your instances and select the check boxes
   c. In the top right-hand corner choose instance state>terminate instance



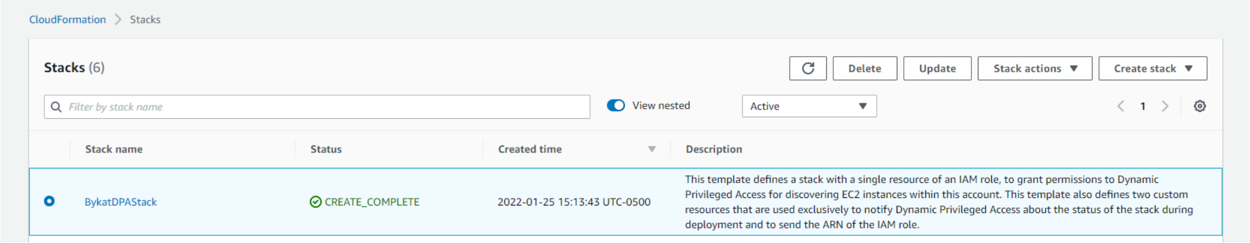
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone		Public IPv4 ...	Elastic IP
☑	Bykat DPA Co...	i-07a2925c8bb6cb2b6	✓ Running	t2.micro	–	No alarms +	us-east-2c	..	18.222.158.162	–
☑	Bykat DPA Tar...	i-06fb9bab338aeca41	✓ Running	t2.micro	–	No alarms +	us-east-2c	–	–	–

2. Remove 2 AWS Security Groups:
    a. Navigate to Network & Security > Security Groups
    b. Search for your security groups and select the check boxes
    c. In the top right-hand corner choose Actions > Delete security groups



☑	Name	Security group ID	Security group name	VPC ID	Description	
☑	–	sg-017aa5a142cc8ea2e	Bykat DPA	vpc-a3c209c8	launch-wizard-35 (	
☑	–	sg-0c248a3938d08063d	Bykat DPA Target	vpc-a3c209c8	launch-wizard-35 crea...	475601244925

3. Remove AWS cloud formation stack
    a. Navigate to Cloud Formation > Stacks
    b. Select the radio button for your stack
    c. Choose Delete in the top right corner



	Stack name	Status	Created time	Description
●	BykatDPAStack	✓ CREATE_COMPLETE	2022-01-25 15:13:43 UTC-0500	This template defines a stack with a single resource of an IAM role, to grant permissions to Dynamic Privileged Access for discovering EC2 instances within this account. This template also defines two custom resources that are used exclusively to notify Dynamic Privileged Access about the status of the stack during deployment and to send the ARN of the IAM role.

Thank you!