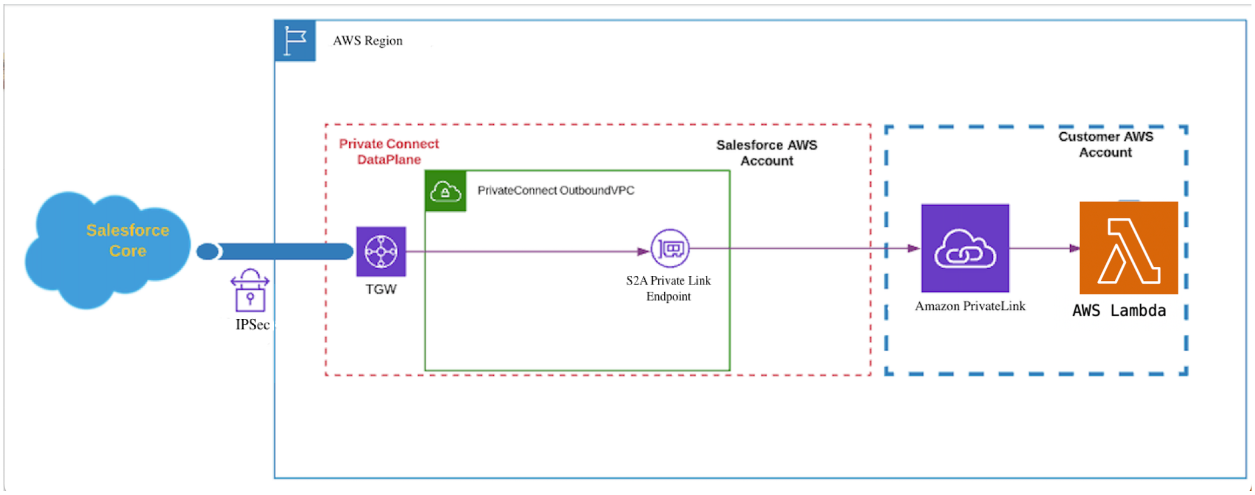
[Customer] Salesforce Private Connect: Outbound Private Connection to AWS Lambda from Salesforce Org

Salesforce Confidential

Overview

This documentation will demonstrate how customers can connect to AWS Lambda through Salesforce Private Connect outbound connection instead of the public internet.

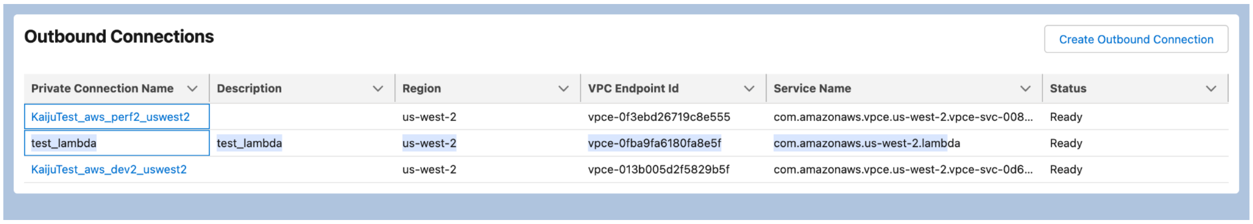


Goal

The traffic is going through an outbound connection instead of the public internet.

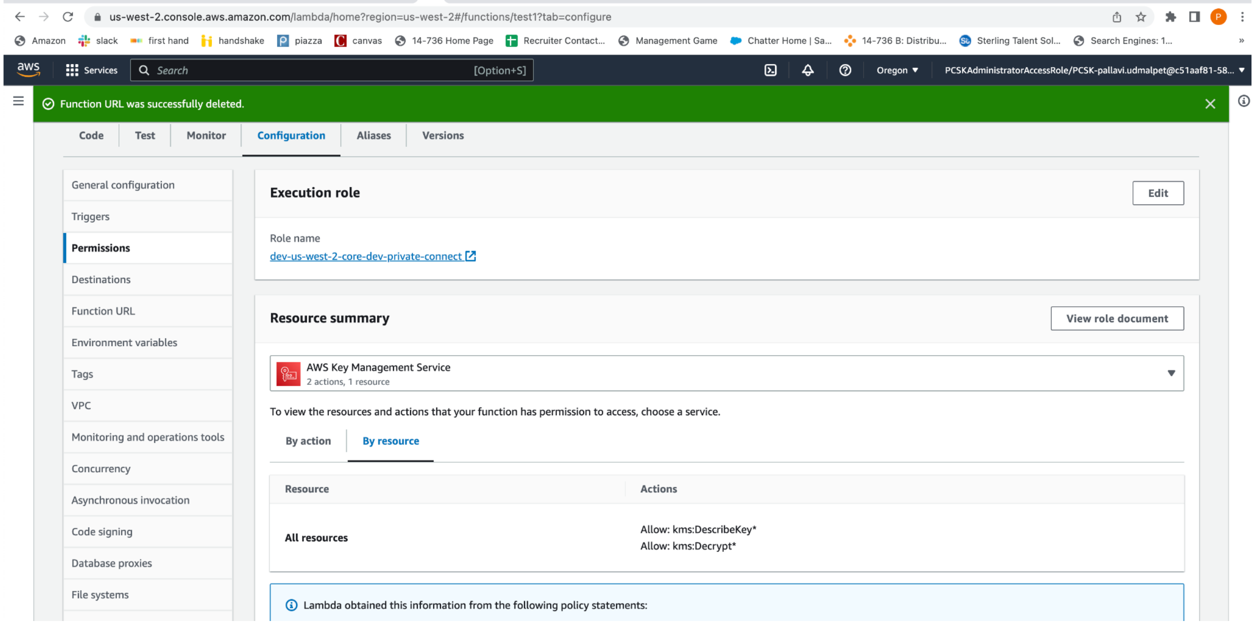
Steps

1. Go to the Salesforce Private Connect portal and create an outbound connection. (VPC Endpoint Service Name: com.amazonaws.<region>.lambda)



Outbound Connections

Private Connection Name	Description	Region	VPC Endpoint Id	Service Name	Status
KaijuTest_aws_perf2_uswest2		us-west-2	vpce-0f3ebd26719c8e555	com.amazonaws.vpce.us-west-2.vpce-svc-008...	Ready
test_lambda	test_lambda	us-west-2	vpce-0fba9fa6180fa8e5f	com.amazonaws.us-west-2.lambda	Ready
KaijuTest_aws_dev2_uswest2		us-west-2	vpce-013b005d2f5829b5f	com.amazonaws.vpce.us-west-2.vpce-svc-0d6...	Ready

1. Go to your AWS Account and create a Lambda (For this purpose I have created a dummy lambda with just a role with some policies such as: AWSLambdaBasicExecutionRole)
2. 

   us-west-2.console.aws.amazon.com/lambda/home?region=us-west-2#/functions/test1?tab=configure

   Function URL was successfully deleted.

   Execution role

   Role name
   dev-us-west-2-core-dev-private-connect

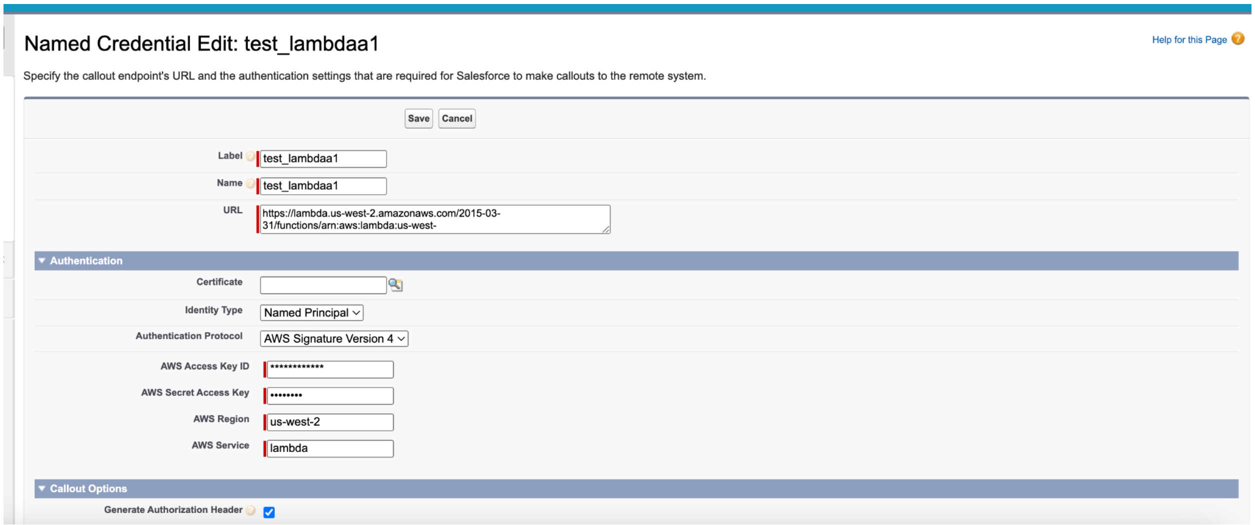
   Resource summary

   AWS Key Management Service
   2 actions, 1 resource

   To view the resources and actions that your function has permission to access, choose a service.

Resource	Actions
All resources	Allow: kms:DescribeKey* Allow: kms:Decrypt*

   Lambda obtained this information from the following policy statements:
3. Go to the Salesforce Named Credentials portal and configure an entry based on your authentication requirements. In this demo, we will use the New `Legacy` option to create an `AWS Signature Version 4` based named credentials and add the AWS Access Key ID and AWS Secret Access Key. (Follow the Permission Control section of the document to create a new user)
4. TheNamed credentials URL would be https://lambda.<region>.amazonaws.com/2015-03-31/functions/<function arn>/invocations

5. 

Named Credential Edit: test_lambdaa1

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

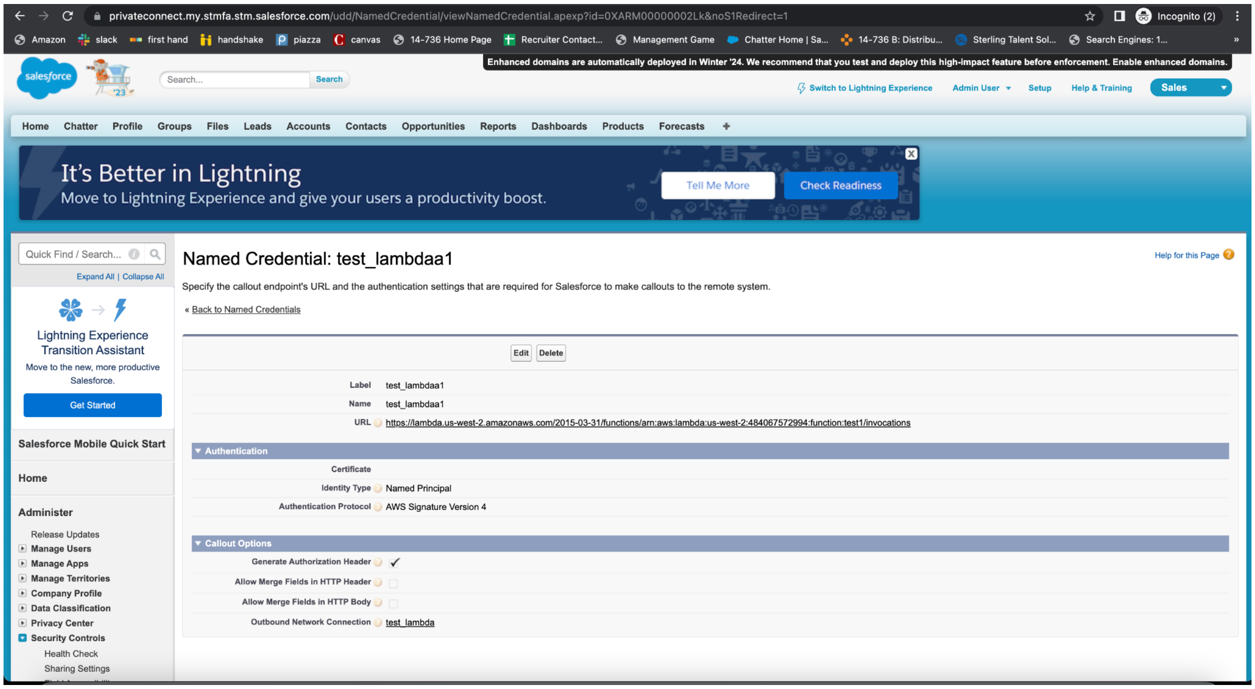
Label	test_lambdaa1
Name	test_lambdaa1
URL	https://lambda.us-west-2.amazonaws.com/2015-03-31/functions/arn:aws:lambda:us-west-

Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	AWS Signature Version 4
AWS Access Key ID	*************
AWS Secret Access Key	********
AWS Region	us-west-2
AWS Service	lambda

Callout Options

Generate Authorization Header	☑



privateconnect.my.stmfa.stm.salesforce.com/udd/NamedCredential/viewNamedCredential.apexp?id=0XARM00000002Lk&noS1Redirect=1

Enhanced domains are automatically deployed in Winter '24. We recommend that you test and deploy this high-impact feature before enforcement. Enable enhanced domains.

It's Better in Lightning
Move to Lightning Experience and give your users a productivity boost.

Named Credential: test_lambdaa1

Specify the callout endpoint's URL and the authentication settings that are required for Salesforce to make callouts to the remote system.

Label	test_lambdaa1
Name	test_lambdaa1
URL	https://lambda.us-west-2.amazonaws.com/2015-03-31/functions/arn:aws:lambda:us-west-2:484067572994:function:test1/invocations

Authentication

Certificate	
Identity Type	Named Principal
Authentication Protocol	AWS Signature Version 4

Callout Options

Generate Authorization Header	✓
Allow Merge Fields in HTTP Header	□
Allow Merge Fields in HTTP Body	□
Outbound Network Connection	test_lambda

1. Click the `Settings` icon in the top-right corner and then open `Developer Console`.
2. Follow the below steps to run a few operations against Lambda via a private connect outbound connection.

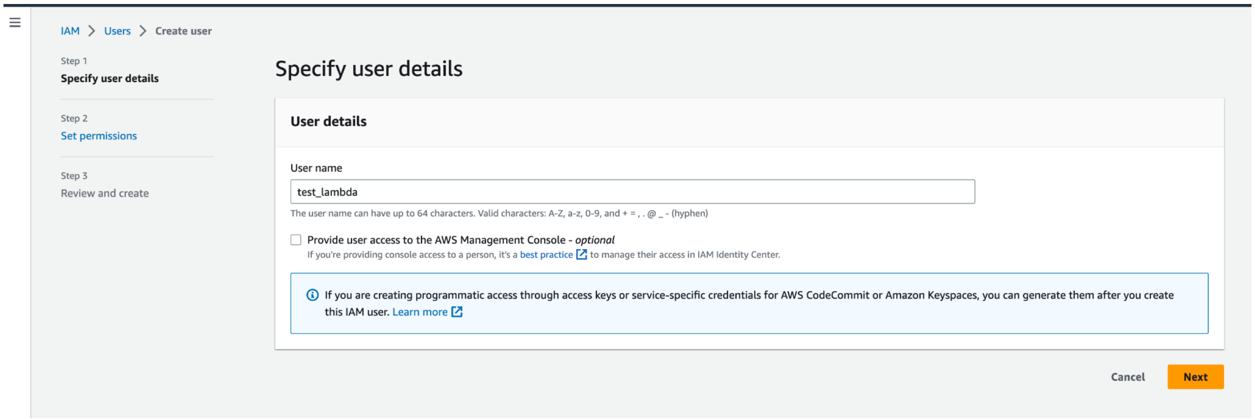
This apex code :

```
Http http = new Http();
HttpRequest request = new HttpRequest();
request.setEndpoint('callout:test_lambdaa1');
request.setMethod('POST');
//request.setHeader('X-Amz-Target', 'Lambda.');
```

```
request.setHeader('Content-Type', 'application/x-amz-json-1.1');
request.setHeader('X-Amz-Invocation-Type', 'Event');
request.setHeader('X-Amz-Log-Type', 'Tail');
HttpResponse response = http.send(request);
System.debug(response.getBody());
```

Permission Control

1. Create a new user:



Specify user details

User details

User name

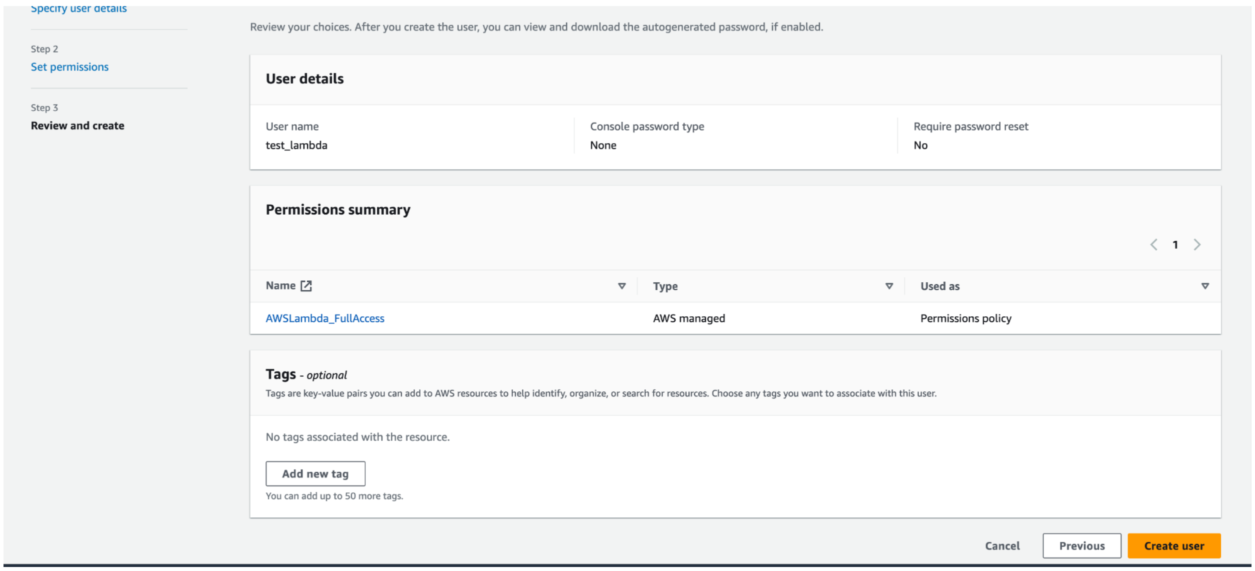
test_lambda

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)

□ Provide user access to the AWS Management Console - *optional*

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. Learn more



Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
test_lambda	None	No

Permissions summary

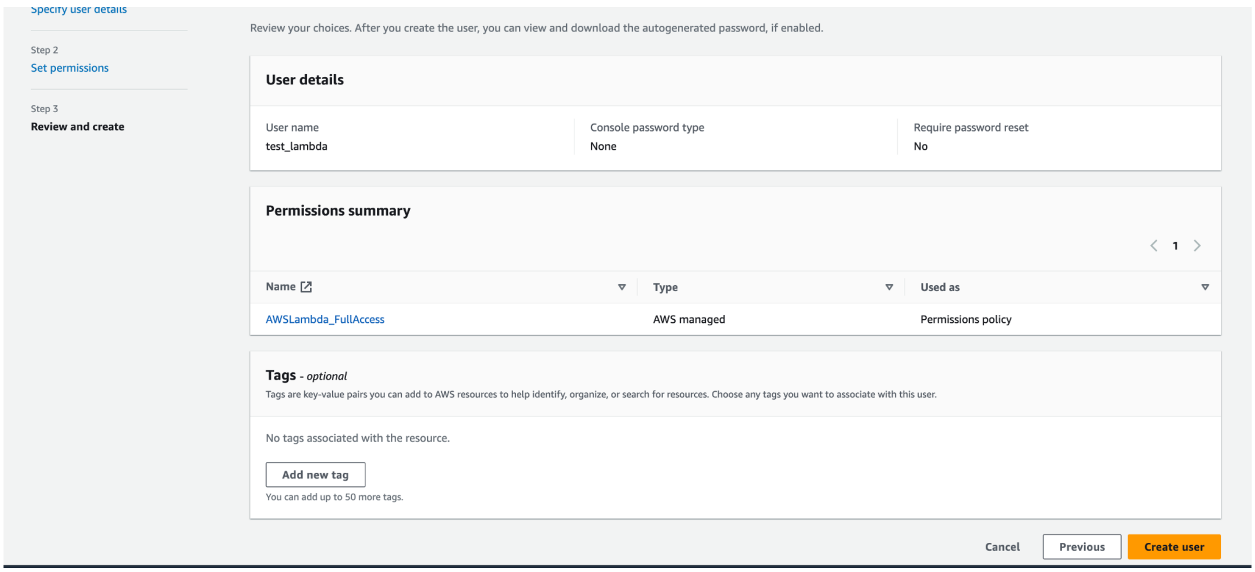
Name	Type	Used as
AWSLambda_FullAccess	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

You can add up to 50 more tags.



Specify user details
Step 2
Set permissions
Step 3
Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name test_lambda | Console password type None | Require password reset No

Permissions summary

AWSLambda_FullAccess | AWS managed | Permissions policy

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

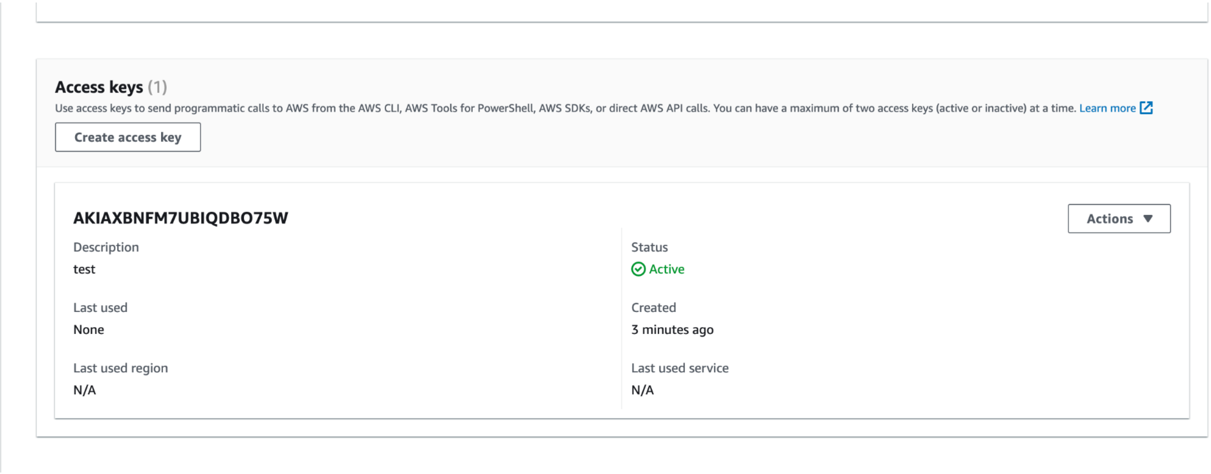
No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

1. Once the user is. created add the access keys



Access keys (1)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. Learn more

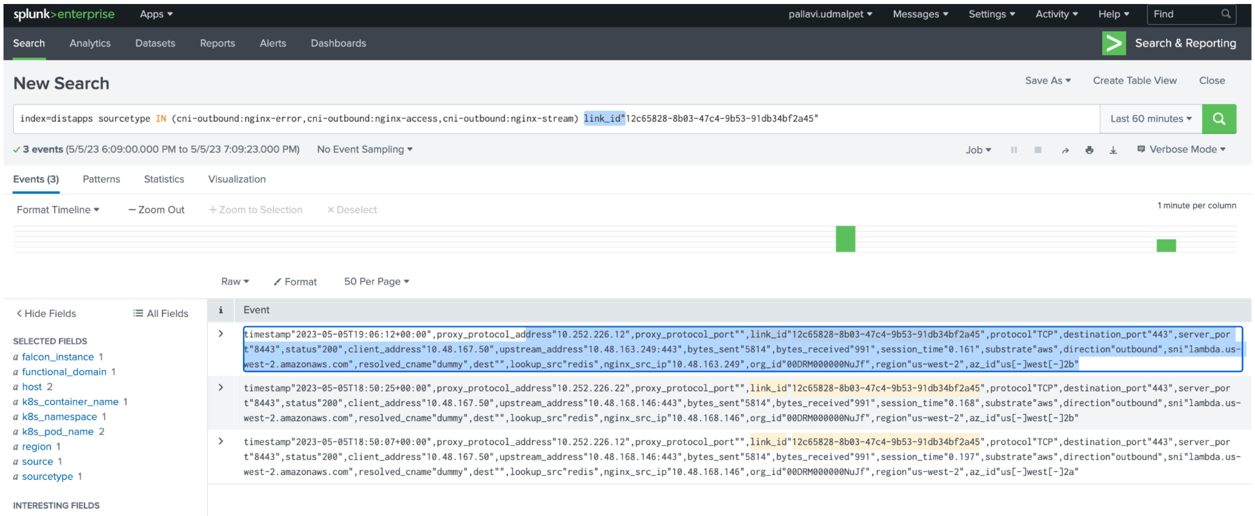
AKIAXBNFM7UBIQDBO75W

Description test	Status ✓ Active
Last used None	Created 3 minutes ago
Last used region N/A	Last used service N/A

1. once created store it locally and use it to create named credentials in step 4.

References for (PC team)

Nginx splunk logs:



New Search

```
index=distapps sourcetype IN (cni-outbound:nginx-error,cni-outbound:nginx-access,cni-outbound:nginx-stream) link_id"12c65828-8b03-47c4-9b53-91db34bf2a45"
```

✓ 3 events (5/5/23 6:09:00.000 PM to 5/5/23 7:09:23.000 PM) No Event Sampling ▾

SELECTED FIELDS
a falcon_instance 1
a functional_domain 1
a host 2
a k8s_container_name 1
a k8s_namespace 1
a k8s_pod_name 2
a region 1
a source 1
a sourcetype 1

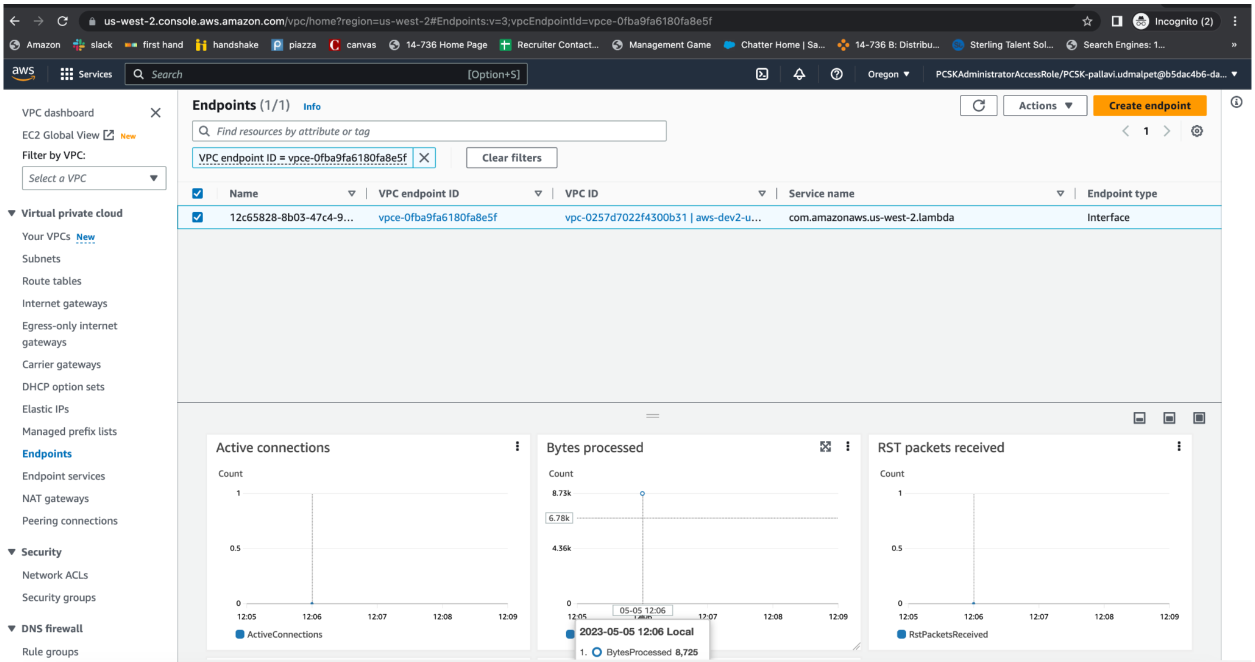
INTERESTING FIELDS

```
timestamp"2023-05-05T19:06:12+00:00",proxy_protocol_address"10.252.226.12",proxy_protocol_port"",link_id"12c65828-8b03-47c4-9b53-91db34bf2a45",protocol"TCP",destination_port"443",server_por
t"8443",status"200",client_address"10.48.167.50",upstream_address"10.48.163.249:443",bytes_sent"5814",bytes_received"991",session_time"0.161",substrate"aws",direction"outbound",sni"lambda.us-
west-2.amazonaws.com",resolved_cname"dummy",dest"",lookup_src"redis",nginx_src_ip"10.48.163.249",org_id"00DRM000000NuJf",region"us-west-2",az_id"us[-]west[-]2b"

timestamp"2023-05-05T18:50:25+00:00",proxy_protocol_address"10.252.226.22",proxy_protocol_port"",link_id"12c65828-8b03-47c4-9b53-91db34bf2a45",protocol"TCP",destination_port"443",server_por
t"8443",status"200",client_address"10.48.167.50",upstream_address"10.48.168.146:443",bytes_sent"5814",bytes_received"991",session_time"0.168",substrate"aws",direction"outbound",sni"lambda.us-
west-2.amazonaws.com",resolved_cname"dummy",dest"",lookup_src"redis",nginx_src_ip"10.48.168.146",org_id"00DRM000000NuJf",region"us-west-2",az_id"us[-]west[-]2b"

timestamp"2023-05-05T18:50:07+00:00",proxy_protocol_address"10.252.226.12",proxy_protocol_port"",link_id"12c65828-8b03-47c4-9b53-91db34bf2a45",protocol"TCP",destination_port"443",server_por
t"8443",status"200",client_address"10.48.167.50",upstream_address"10.48.168.146:443",bytes_sent"5814",bytes_received"991",session_time"0.197",substrate"aws",direction"outbound",sni"lambda.us-
west-2.amazonaws.com",resolved_cname"dummy",dest"",lookup_src"redis",nginx_src_ip"10.48.168.146",org_id"00DRM000000NuJf",region"us-west-2",az_id"us[-]west[-]2a"
```

vpce-endpoint metrics:



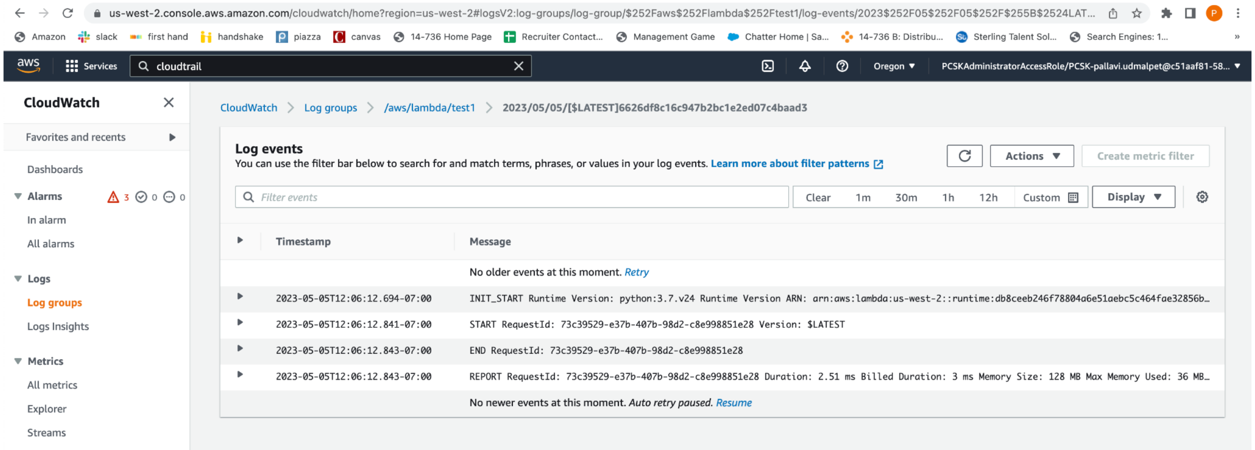
VPC endpoint ID = vpce-0fba9fa6180fa8e5f

☑	Name	VPC endpoint ID	VPC ID	Service name	Endpoint type
☑	12c65828-8b03-47c4-9...	vpce-0fba9fa6180fa8e5f	vpc-0257d7022f4300b31 | aws-dev2-u...	com.amazonaws.us-west-2.lambda	Interface

2023-05-05 12:06 Local

1. ○ BytesProcessed 8,725

Lambda logs:



CloudWatch > Log groups > /aws/lambda/test1 > 2023/05/05/[$LATEST]6626df8c16c947b2bc1e2ed07c4baad3

Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

```
Timestamp                        Message
                                 No older events at this moment. Retry
2023-05-05T12:06:12.694-07:00    INIT_START Runtime Version: python:3.7.v24 Runtime Version ARN: arn:aws:lambda:us-west-2::runtime:db8ceeb246f78804a6e51aebc5c464fae32856b…
2023-05-05T12:06:12.841-07:00    START RequestId: 73c39529-e37b-407b-98d2-c8e998851e28 Version: $LATEST
2023-05-05T12:06:12.843-07:00    END RequestId: 73c39529-e37b-407b-98d2-c8e998851e28
2023-05-05T12:06:12.843-07:00    REPORT RequestId: 73c39529-e37b-407b-98d2-c8e998851e28 Duration: 2.51 ms Billed Duration: 3 ms Memory Size: 128 MB Max Memory Used: 36 MB…
                                 No newer events at this moment. Auto retry paused. Resume
```