AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET214

# Introducing AWS Verified Access: Secure connections to your applications

Shovan Das

Product Manager EC2 VPC
AWS

Jess Szmajda

GM VPN
AWS

# Agenda

Connectivity needs of customers

Introducing Verified Access

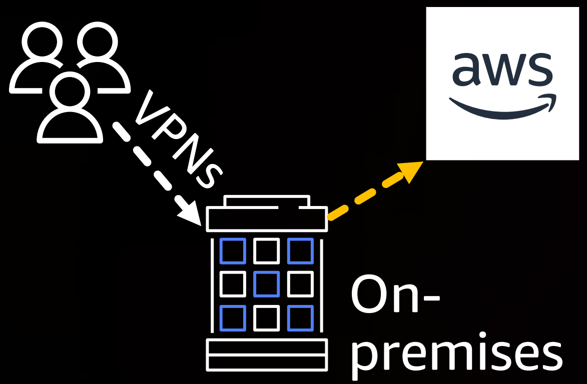
How Verified Access works

Verified Access policies

Console walkthrough

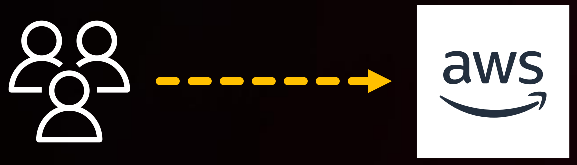
# The need for a simpler secure connectivity

## Through on-premises network



AWS Direct Connect or
AWS Site-to-Site VPN

## Directly connected



AWS Client VPN

## Granular access control

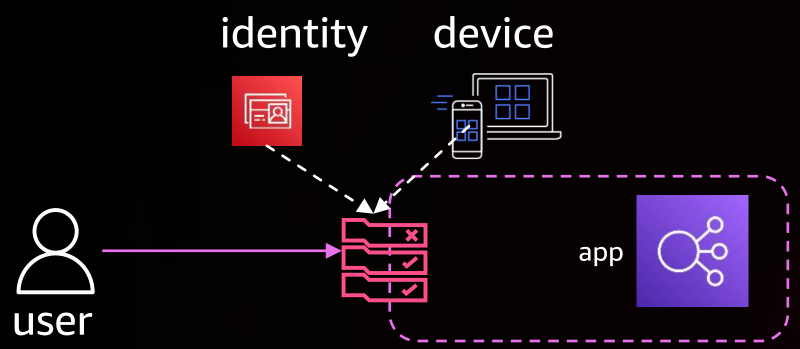
- Access policies per apps
- Access from anywhere: browser based, no agent

**Essentially asking for
Zero Trust Network Access**

# Zero Trust Network Access (ZTNA)

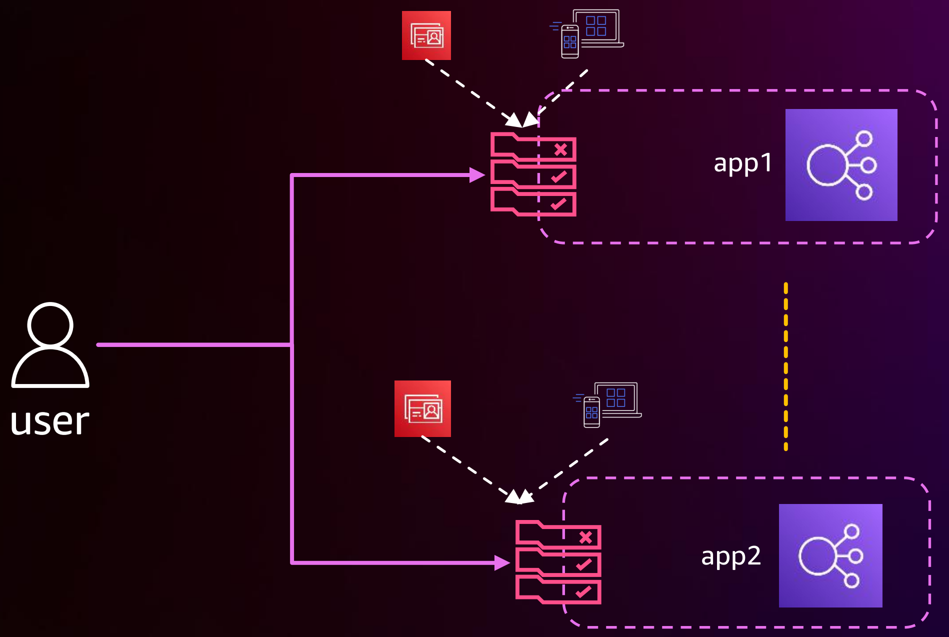
Zero Trust is a conceptual model and an associated set of mechanisms that focuses on providing security controls around digital assets *that do not solely or fundamentally depend on traditional network controls or network perimeters*

## Use additional sources to verify access



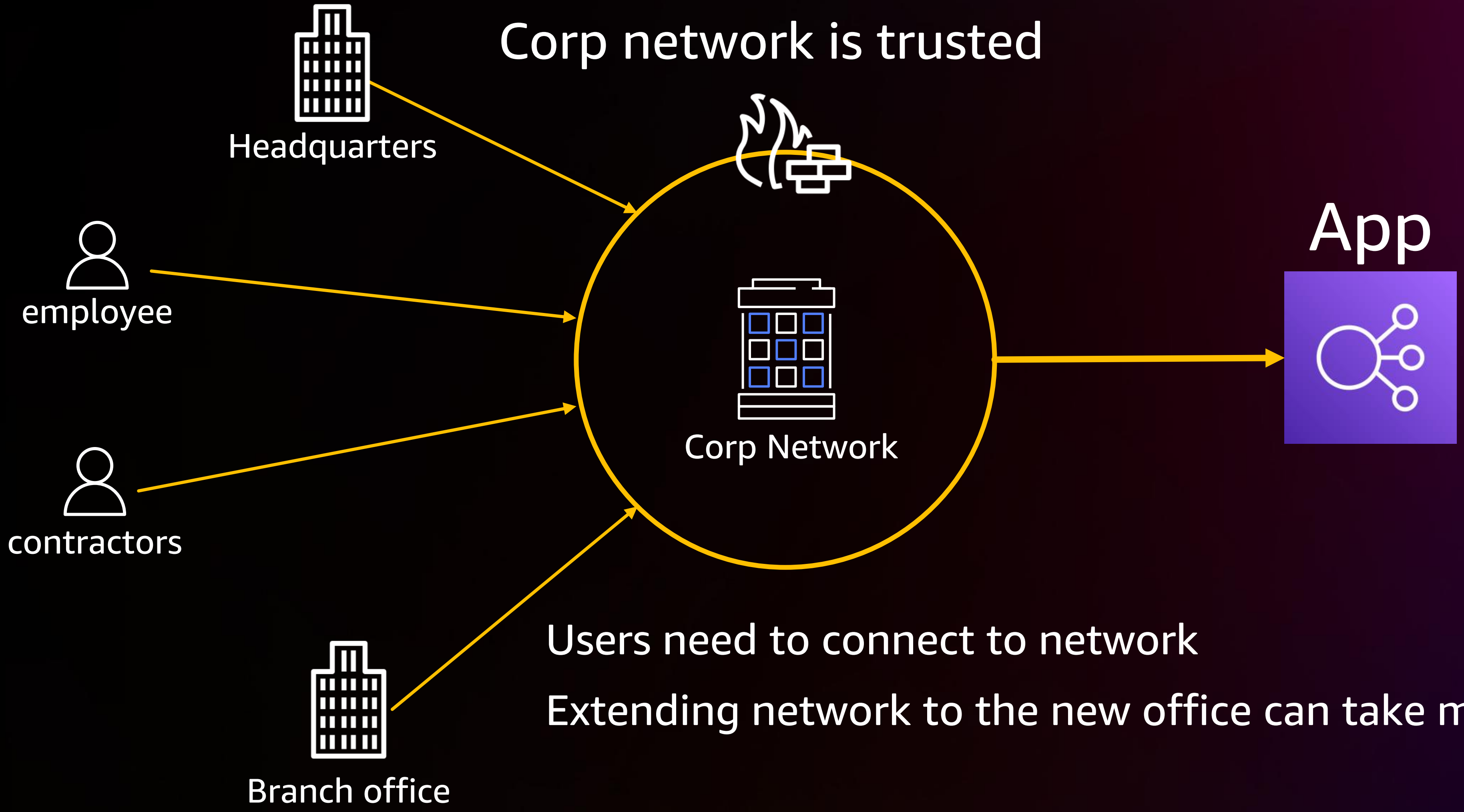
More sources: More trustworthiness

## Continuous verification



Evaluate trust on each request

# ZTNA example: Connectivity to apps
## (Before ZTNA: Traditional method)

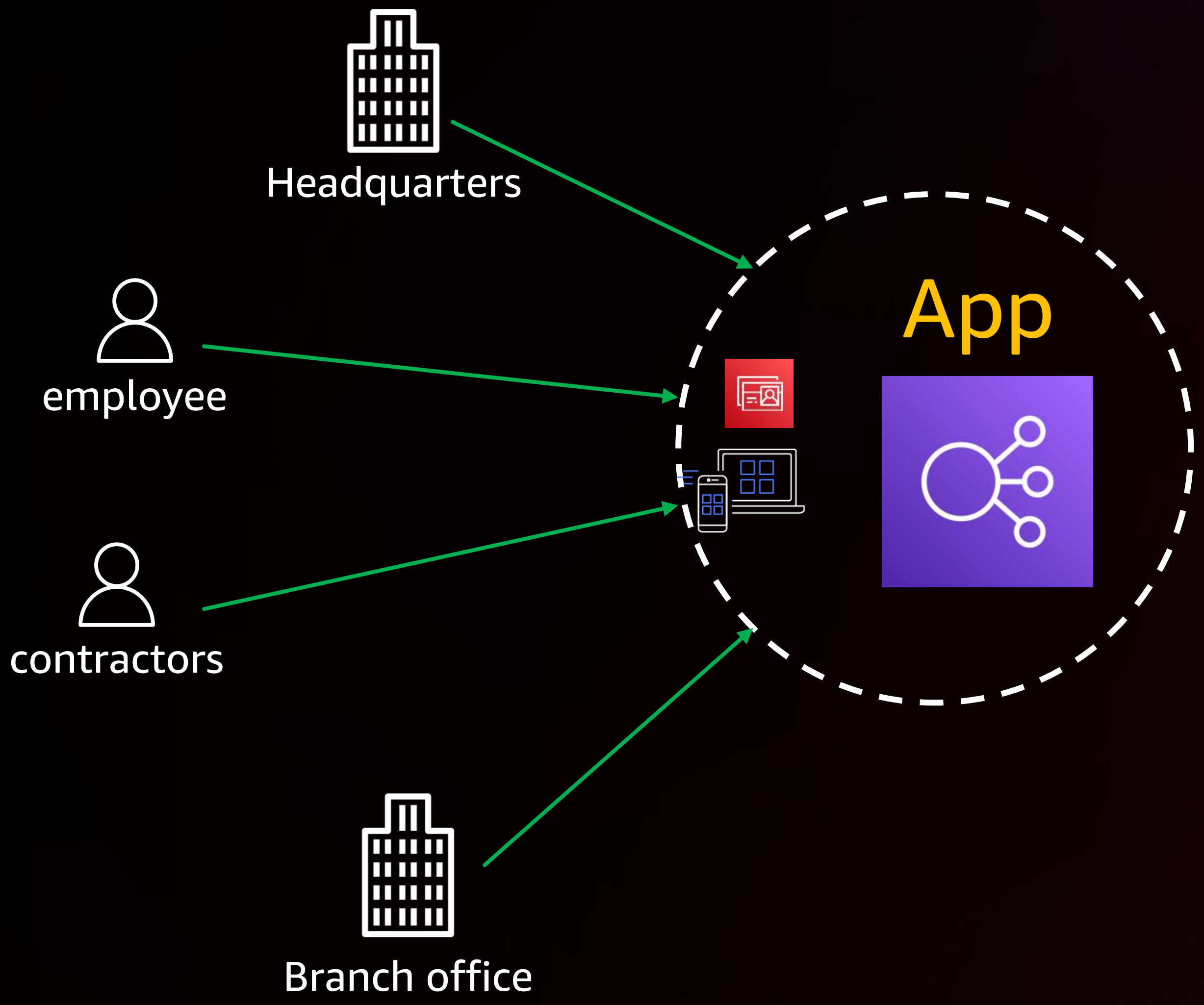


Users need to connect to network

Extending network to the new office can take months

# ZTNA example: Connectivity to apps

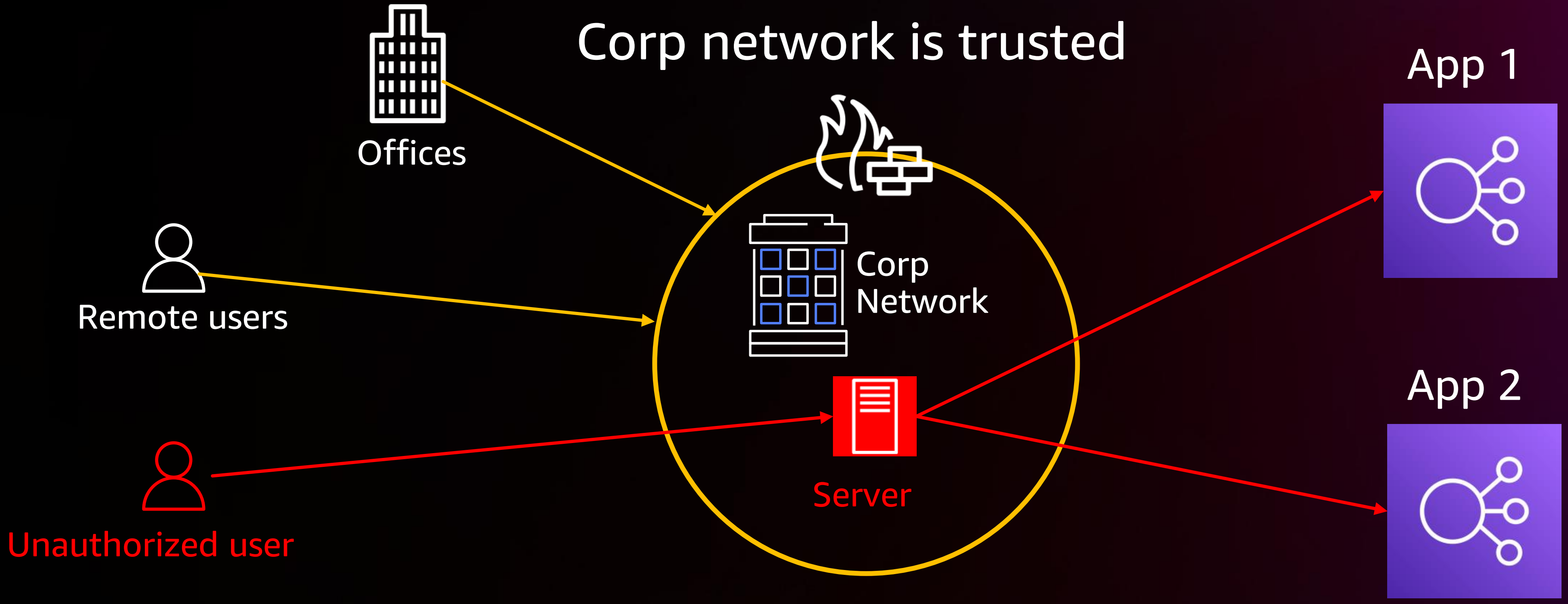
## (With ZTNA: App centric)



Users connect to apps directly

New branch offices can connect directly

# ZTNA example: App security
## (Before ZTNA: Traditional method)

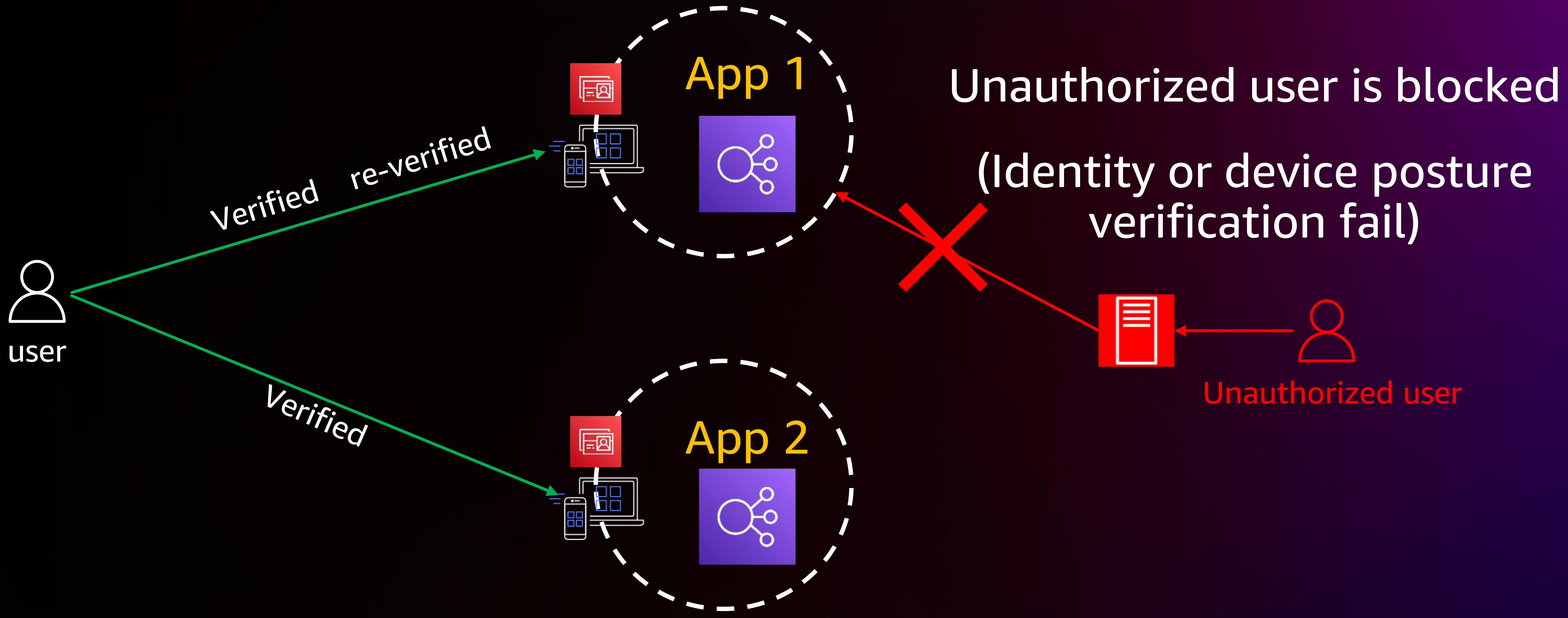


Unauthorized user gets a foothold

Potentially use the foothold to get access to apps with sensitive data

# ZTNA example: App security

## (With ZTNA: Continuous verification)



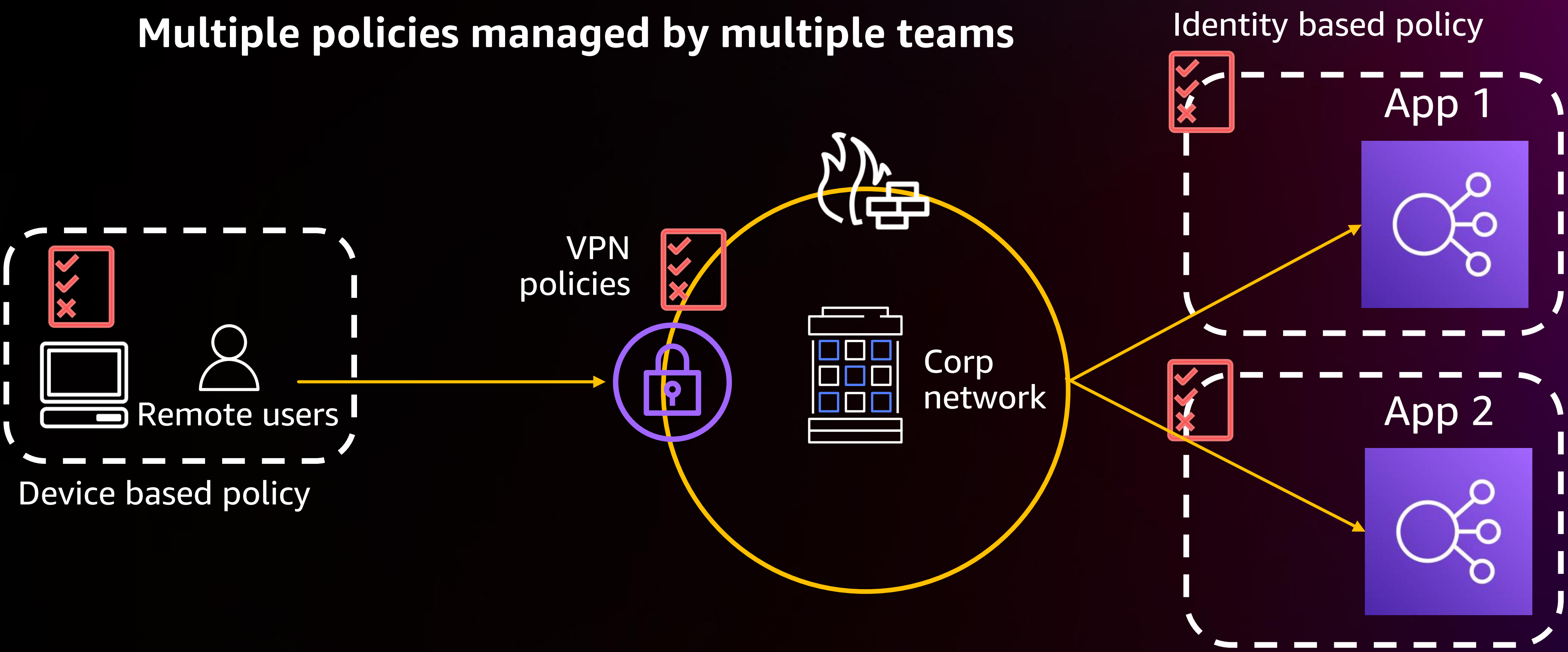
Unauthorized user is blocked

(Identity or device posture verification fail)

Each access request is verified

# The current solution

# How elements of Zero Trust are implemented today



**Network admins** manage VPN policies
**Developers** integrate identity into applications
**IT admins** manage which device can on-board the network

# Better solution: Introducing Verified Access

# Introducing AWS Verified Access

## Increase workforce mobility

Users access applications with a web browser, without any additional agents

## Improve security posture

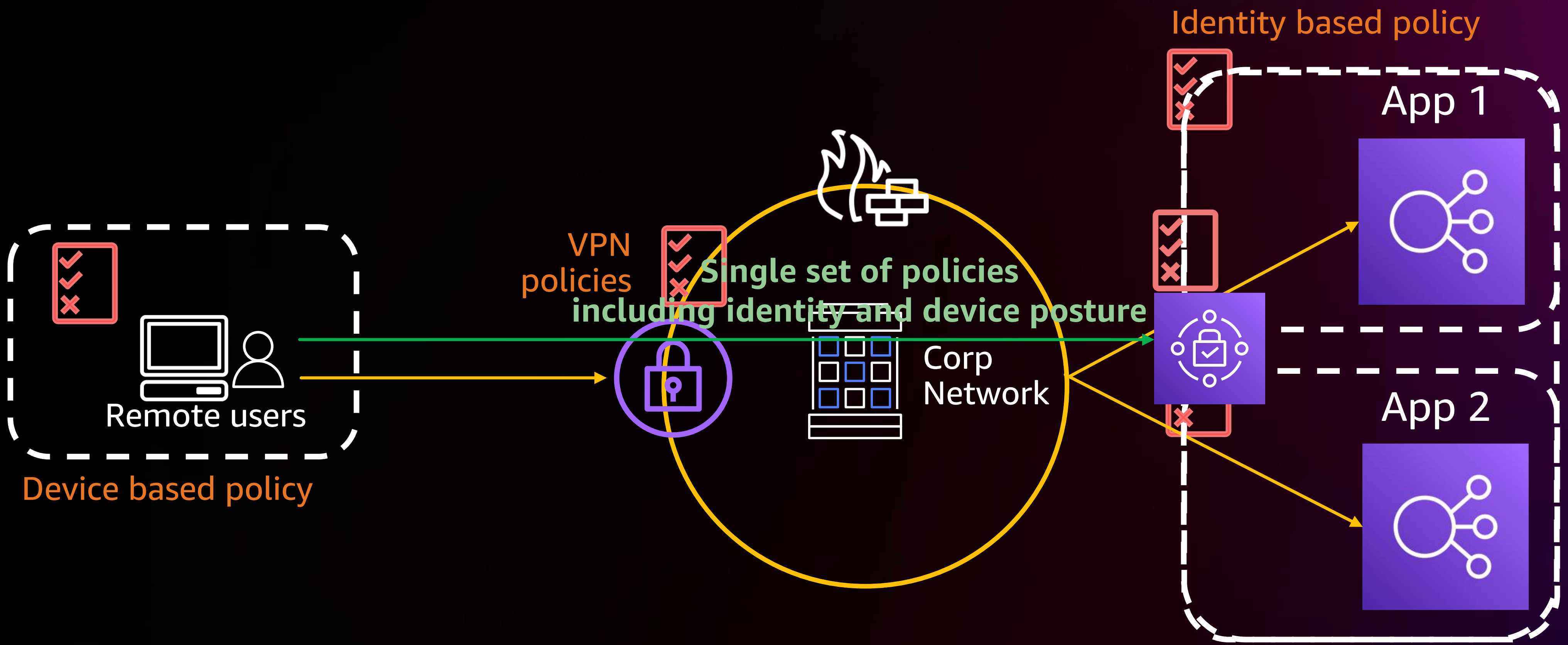
Built using AWS Zero Trust principles, evaluates each user request in real time using identity and device posture

## Simplify security operation

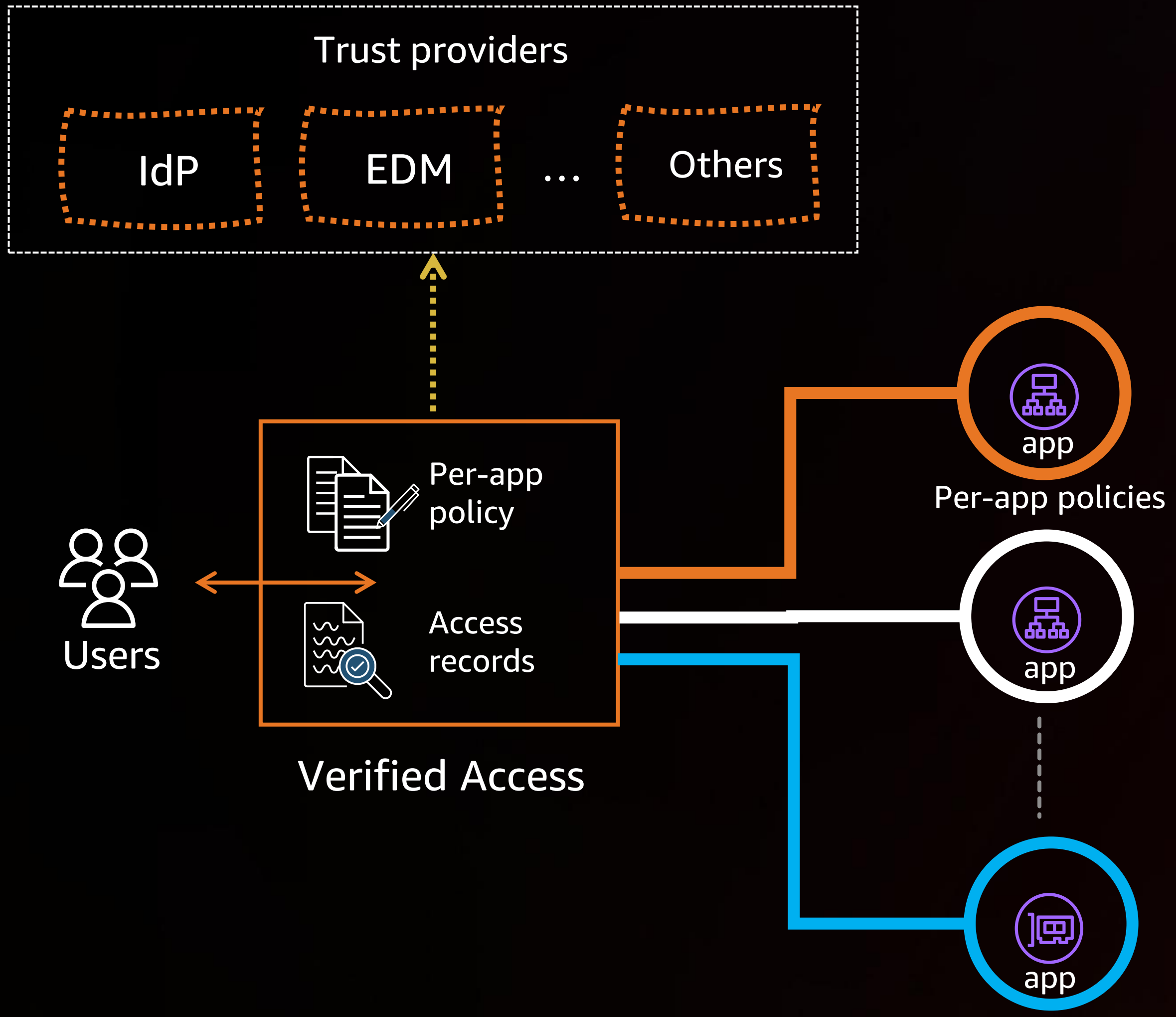
Onboard applications using a few clicks, create and manage all your access using a single set of policies

Work from anywhere with VPN-less secure access

# Simplify Zero Trust implementation

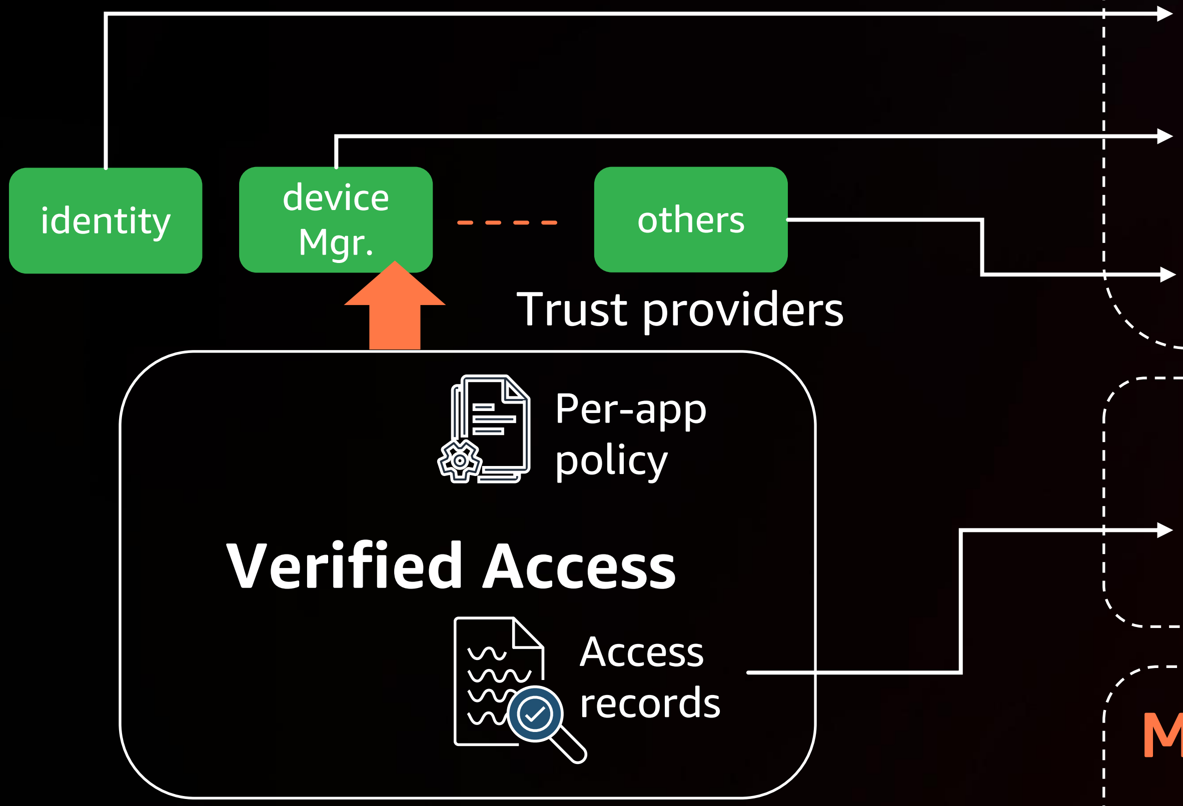


# Secure access to corporate application



- **Fine grained, dynamic authorization**
  Per-app policy evaluated with every request
- **Improve observability**
  Faster incidence response, auditability, meet compliance
- **Use your existing security services**
  Integrates with popular identity and device trust providers

# Verified Access – Partners



identity

device Mgr.

others

Trust providers

Per-app policy

Verified Access

Access records

## Trust providers

**IdP partners –** provide users identity

**Device security partners –** provide device context

**Contextual data partners –** provide behavioral analytics & geolocation, and many more

## SIEM/observability providers

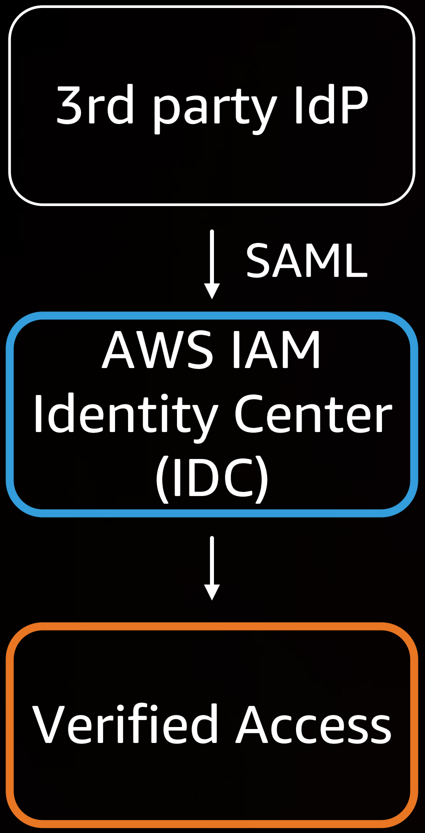
**Analyze risk & generate insights**

## Managed connectivity providers

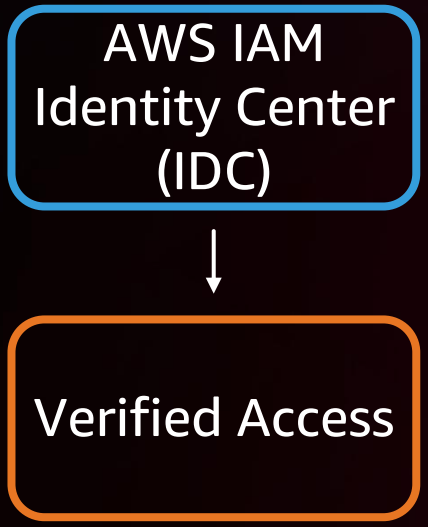
**Build a managed connectivity solution**

# Integration with identity providers

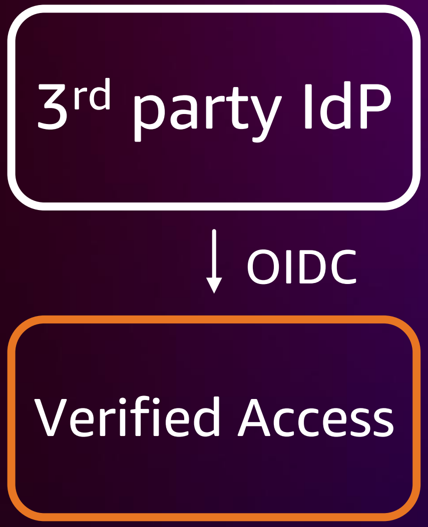
- Leverage your existing IDC integration
- Use IDC across services that need identity



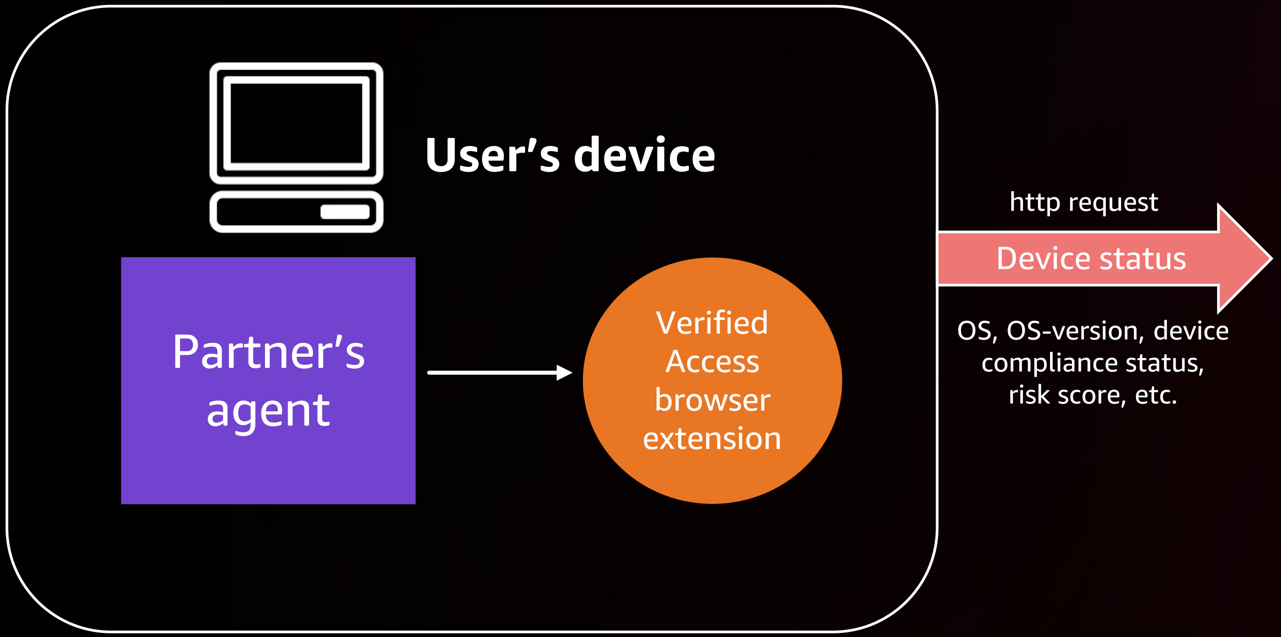
- Use IDC to manage your corporate identity



- Integrate OIDC IdP with Verified Access



# Integration with device security partners

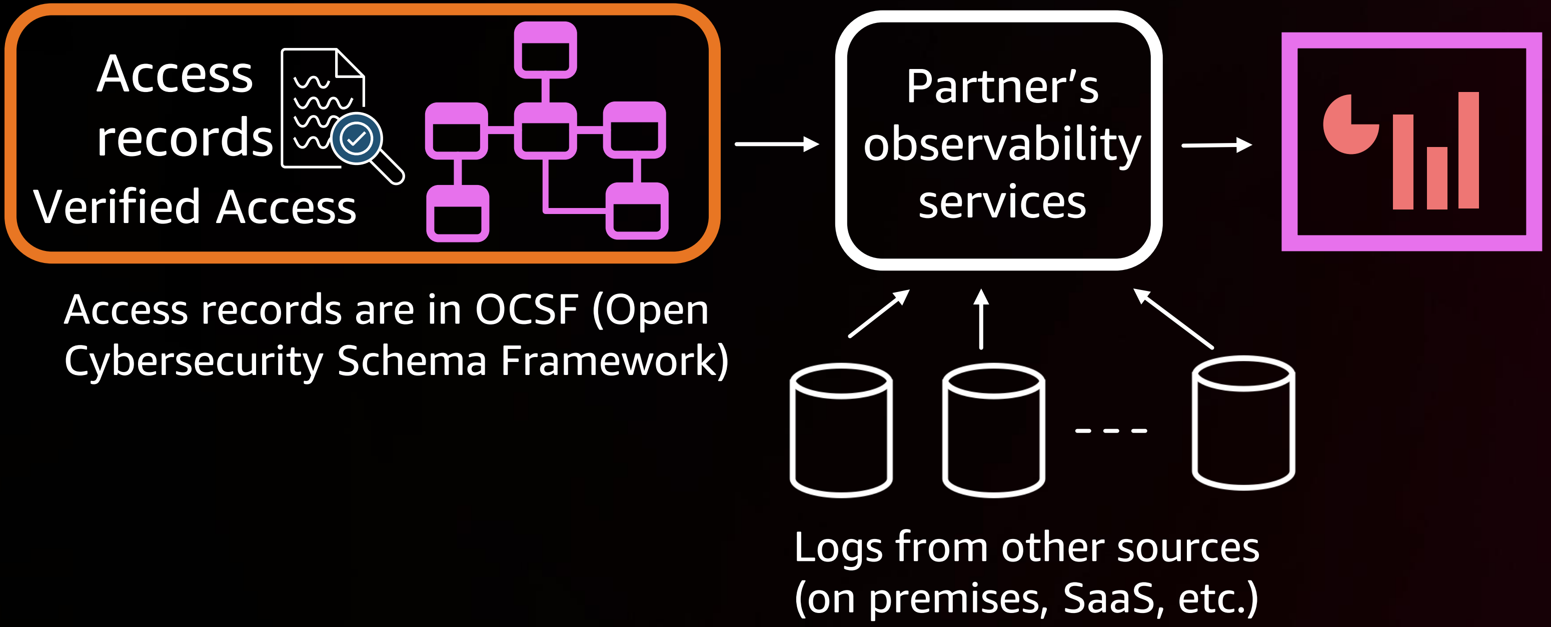

User's device
Partner's agent
Verified Access browser extension
http request
Device status
OS, OS-version, device compliance status, risk score, etc.

Browser extension: needed if access policies use device state

Chrome and Firefox supported, planning to add more

Standard browser: if access policies don't use device state

# Observability partners


Access records
Verified Access
Partner's observability services
Logs from other sources (on premises, SaaS, etc.)

Access records are in OCSF (Open Cybersecurity Schema Framework)

Behavioral analysis

Investigate security incidences

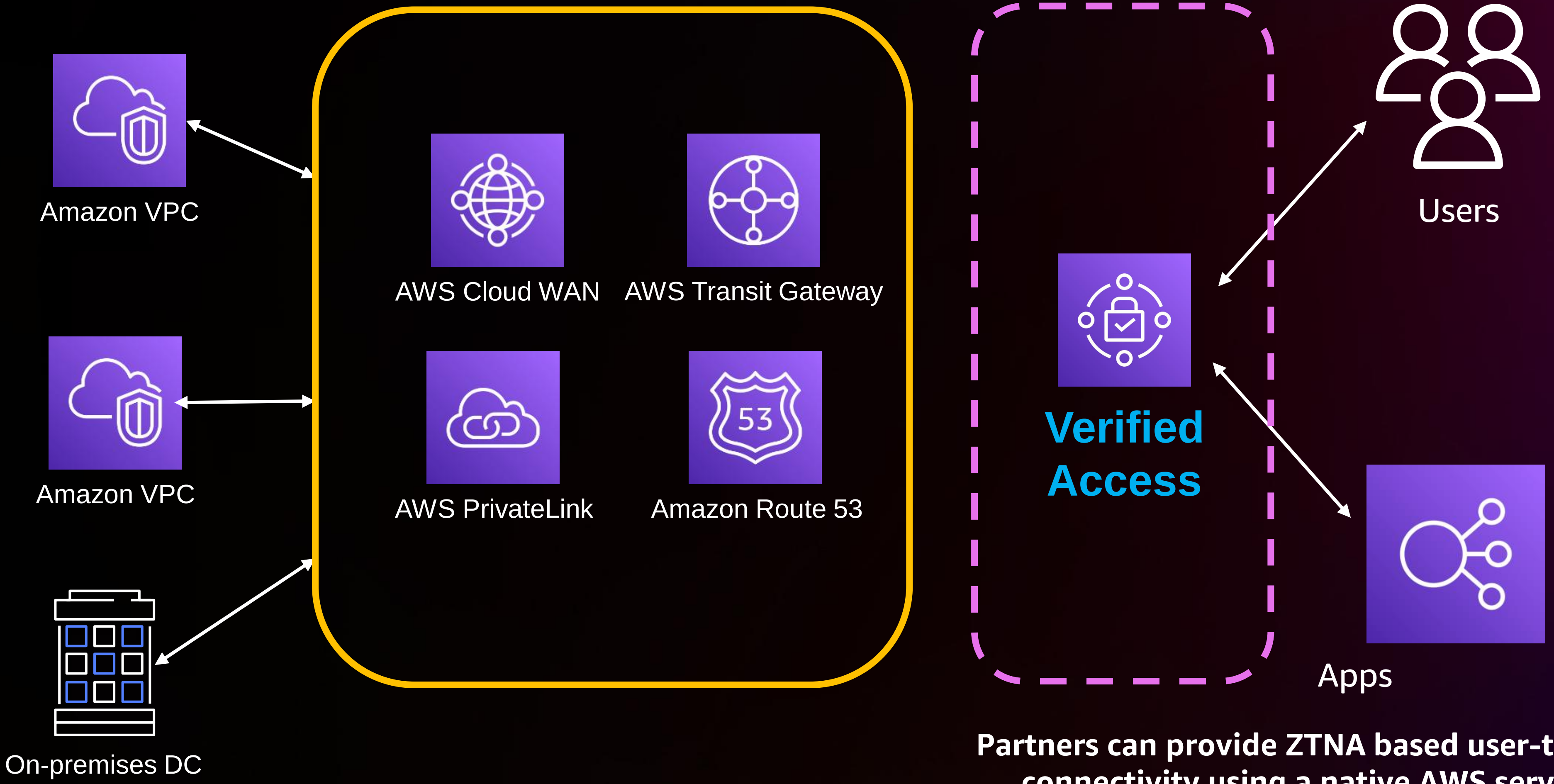
Audit for compliance

Troubleshoot connectivity

**OCSF** : open specification that normalizes security telemetry across products and services

# Managed connectivity partners

Use AWS native services (e.g., AWS Cloud WAN, TGW, AWS PrivateLink, Amazon Route 53) to create a managed connectivity fabric



Partners can provide ZTNA based user-to-app connectivity using a native AWS service

# AWS Verified Access partners

## Trust/network providers

CROWDSTRIKE

CYBERARK®

DUO

jamf

jumpcloud™

okta

prosimo

Ping Identity

## SIEM/observability providers

DATADOG

IBM

netskope

new relic

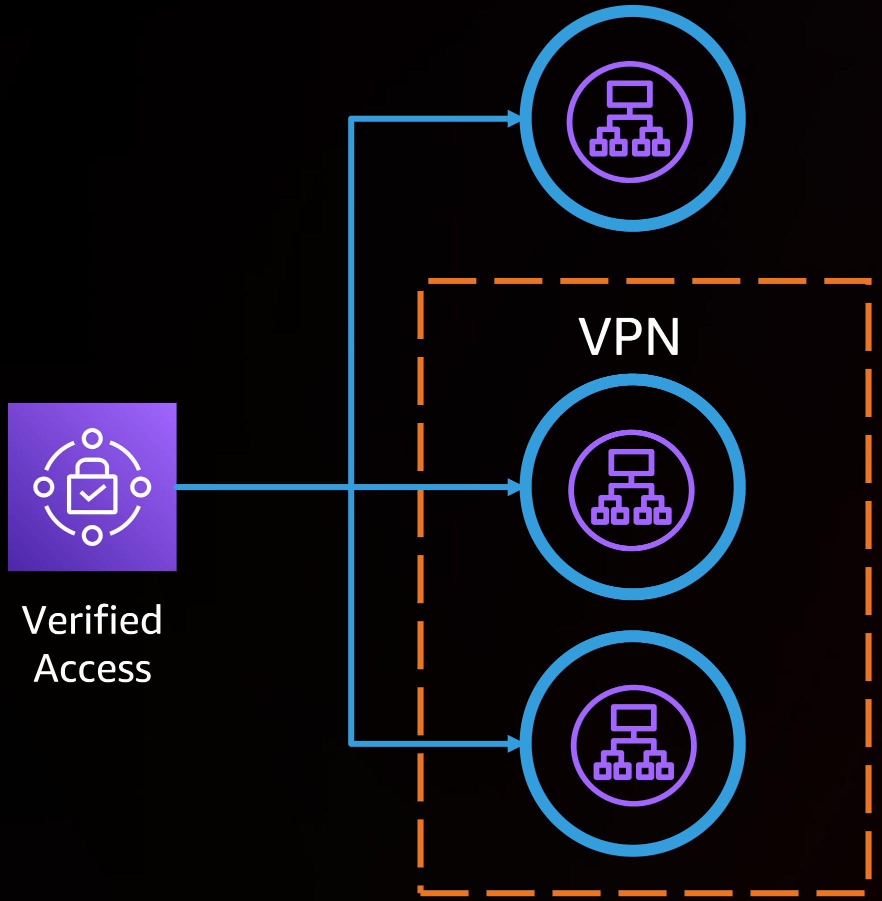
RAPID7

sumo logic

Trellix

# Migrating to Verified Access

# Migration to AWS Verified Access



**Add new apps to Verified Access**

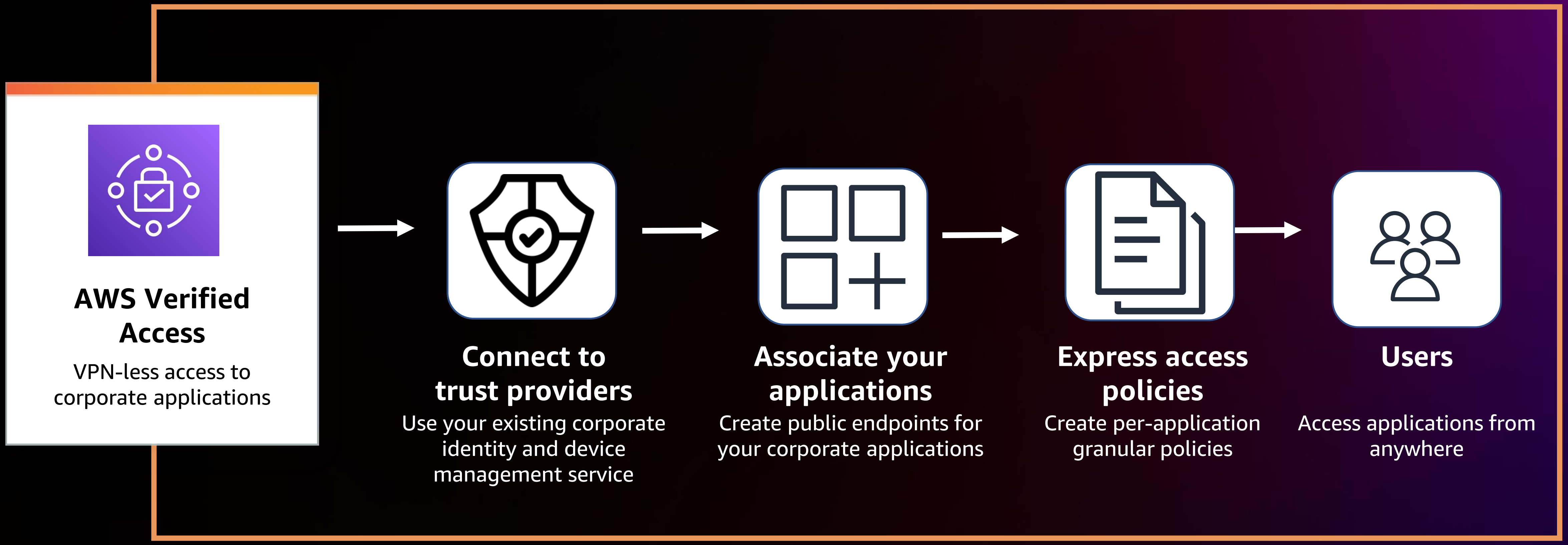
**Add Verified Access to existing apps**

- Users can access these apps by both VPN and internet
- Keep VPN policies

**Remove VPN path**

# How Verified Access works

# Set up AWS Verified Access



**AWS Verified Access**

VPN-less access to corporate applications

**Connect to trust providers**

Use your existing corporate identity and device management service

**Associate your applications**

Create public endpoints for your corporate applications

**Express access policies**

Create per-application granular policies

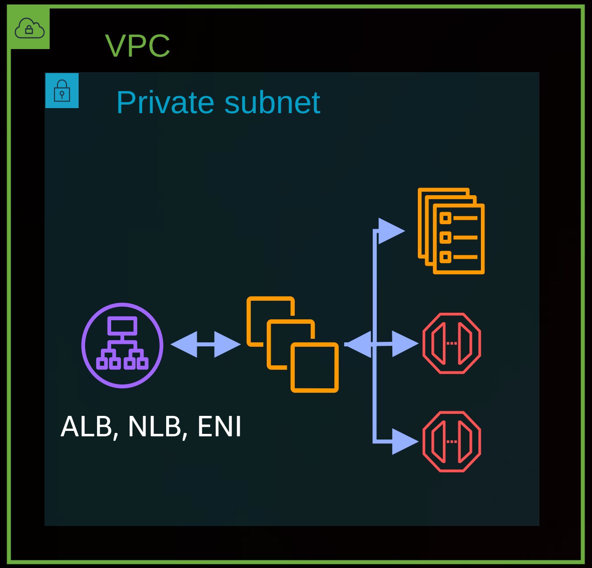
**Users**

Access applications from anywhere

# What is a corporate application

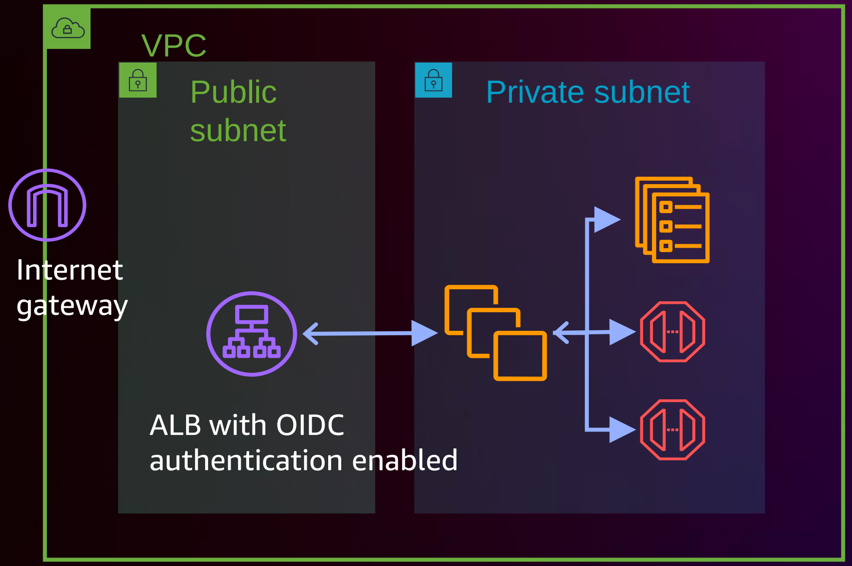
Corporate apps: developed by customers' engineering team, e.g., employee directory app
apps target can be Load Balancers (e.g. ALB, NLB) and elastic network interface (ENIs)

## Apps accessible by corp. network only



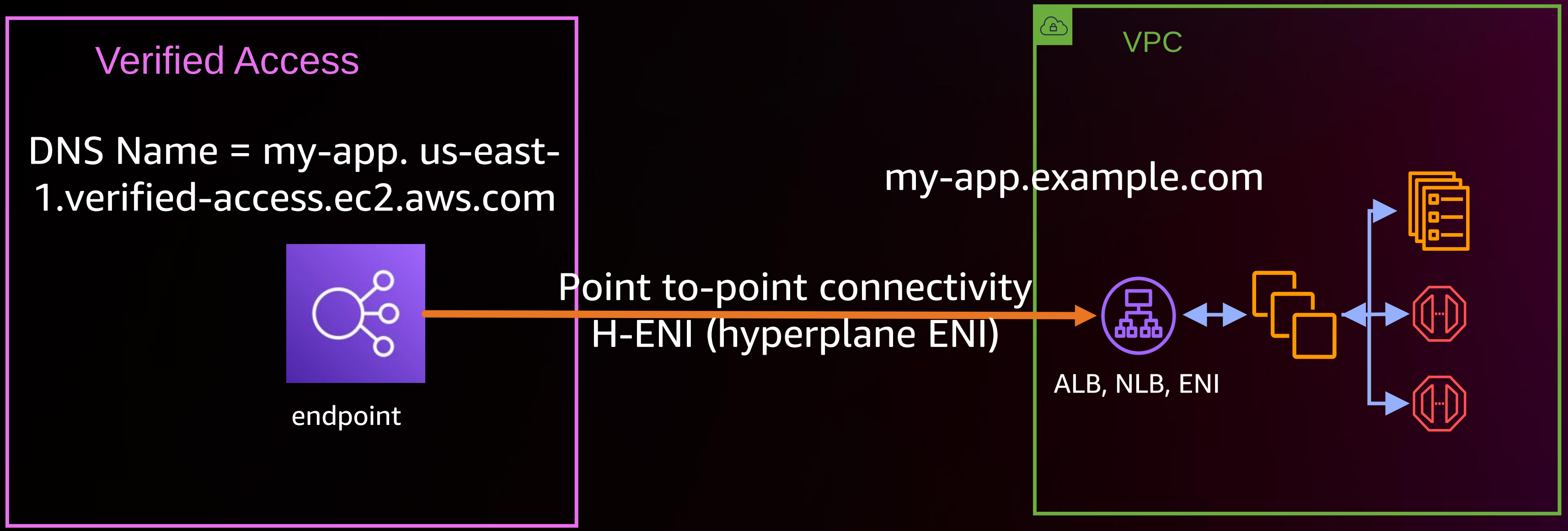
- Make apps accessible from anywhere
- Move app to Zero Trust architecture

## Internet accessible apps with OIDC integration



- Improve or maintain security (add device posture)
- Centralize and simplify access-policy mgmt.

# Associate applications with private access



Verified Access

DNS Name = my-app. us-east-1.verified-access.ec2.aws.com

endpoint

Point to-point connectivity
H-ENI (hyperplane ENI)

VPC

my-app.example.com

ALB, NLB, ENI

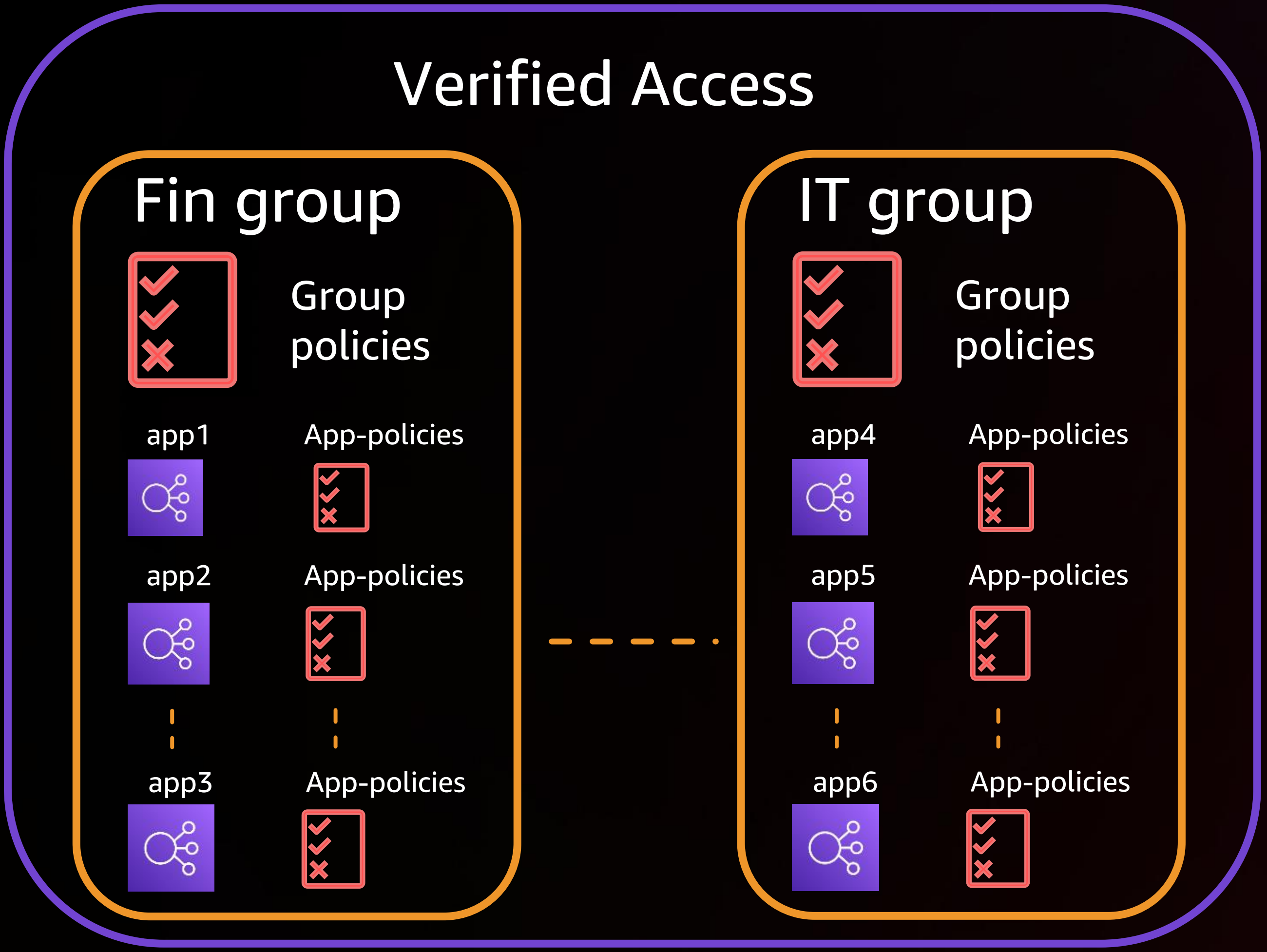
Verified Access and app can be different AWS account (Verified Access is sharable via RAM)

1. Add the App’s target (e.g. ALB, NLB, ENI)

2. Map apps DNS name to endpoints DNS name
(CNAME: my-app.example.com -> my-app. us-east-1.verified-access.ec2.aws.com)

3. Verified Access also connects the endpoint with your apps

# Verified Access groups



Group applications based on security needs

All apps in a group share the group-policy

Apps can have an app-level policy (optional)

# Verified Access policies

# Verified Access policies

What is Cedar

Why Cedar?

Cedar’s syntax

Cedar’s context and how data gets there

Cedar operators

Example policies

# Verified Access policies – Cedar

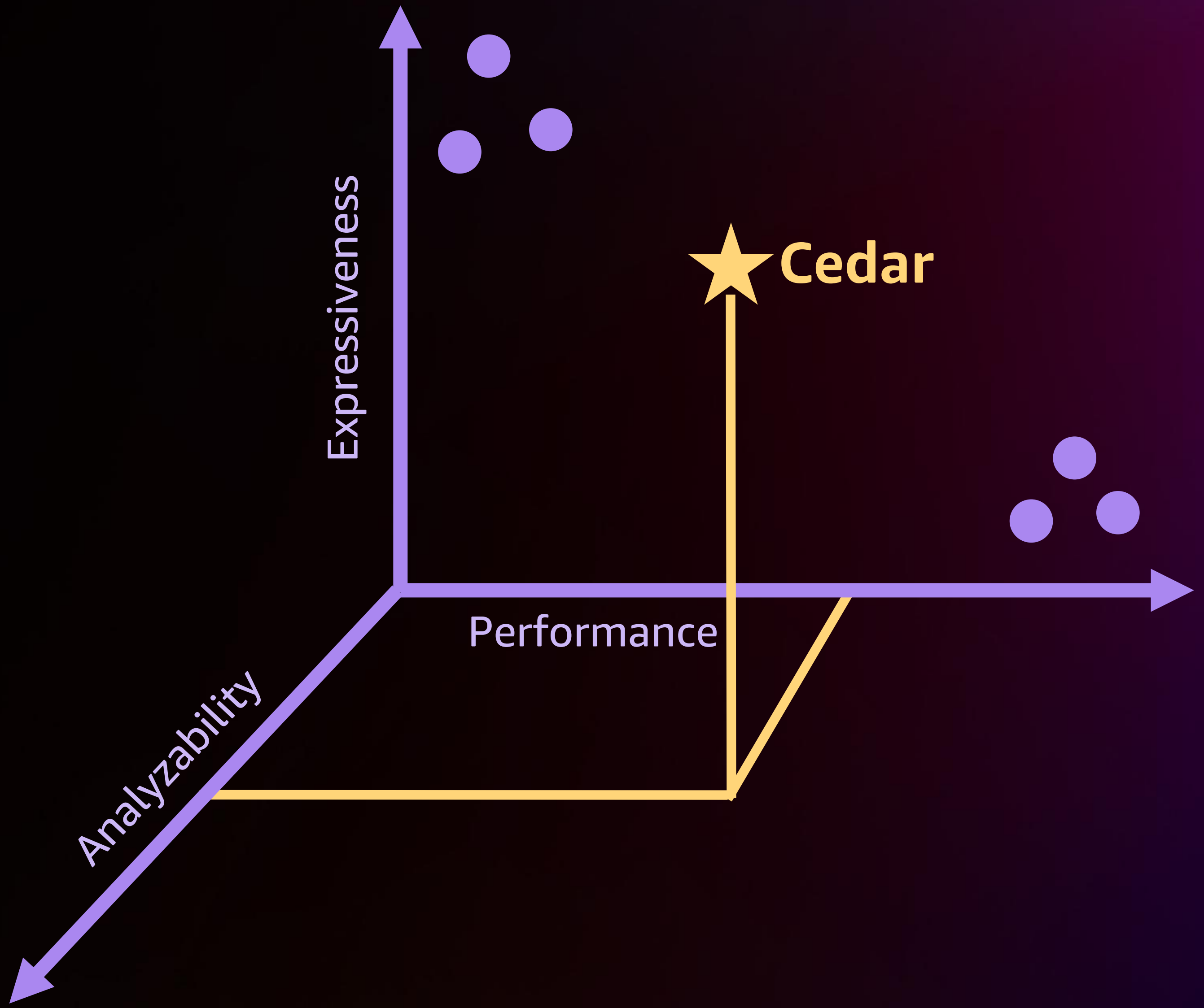
```
permit(principal, action, resource)
when {
  context.user.groups.contains(“Sales”)
  && context.device.risk == ”LOW”
}

forbid(principal, action, resource)
when {
  context.device.risk == “HIGH”
}
```

# Why Cedar?

Ergonomic syntax & semantics

Powerful static analysis tools

Fast & safe evaluation engine



# Cedar syntax

effect

```
permit(
```

scope

```
  principal,
  action,
  resource)
```

condition clause

```
when {
  context.device.assessment > 60 &&
  context.groups.contains(“sales”)
};
```

# Cedar’s context

```
context: {

  “usr_data”:
```

**User Information**

```
{
  “name”: “Jane Friday”,
  “email”: {
    “address”: “jane@example.com”,
    “verified”: true
  }
}
```

Policy reference name

```
  ”dev_data”:
```

**Device Information**

```
{
  “risk”: “LOW”,
  “osv”: “12.6.1”,
  “platform”: “macos”
}
```

```
}
```

# Cedar context

```
context: {

  “usr_data” : {
                 “name”: “Jane Friday”,
                 “email”: {
                   “address”: “jane@example.com”,
                   “verified”: true
                 }
               }

  ”dev_data” : {
                 “risk”: “LOW”,
                 “osv”: “12.6.1”,
                 “platform”: “macos”
               }
}
```

```
permit(principal, action, resource)
when {
   context.usr_data.email.verified == true
   && context.dev_data.risk == “LOW”
};
```

```
forbid(principal, action, resource)
when {
   context.usr_data.email.address like “*@untrusted.com”
   || context.dev_data.risk == “HIGH”
};
```

# Cedar operators

<table>
<tr><th>Symbol</th><th>Description</th><th>Example == true</th></tr>
<tr><td>==</td><td>Equality</td><td>1 == 1</td></tr>
<tr><td>!</td><td>Logical not</td><td>!(false)</td></tr>
<tr><td>&& ||</td><td>Logical and, logical or</td><td>(true || false)</td></tr>
<tr><td>< <= > >=</td><td>Numeric comparison</td><td>7 < 42</td></tr>
<tr><td>like</td><td>String comparison, wildcard operator: *</td><td>”jessica” like “jess*”</td></tr>
<tr><td>has</td><td>Object property check (object <i>has</i> property)</td><td>{“foo”: “bar”} has “foo”</td></tr>
<tr><td>.contains()</td><td>Set membership</td><td>[“a”, “b”].contains(“a”)</td></tr>
</table>

# Example Verified Access policies

```
permit(principal, action, resource) when {
  context.identity.groups.contains(“finance”)
  && context.device.assessment.overall > 80
};
```

Allow access when the user is in the “finance” group and their device has an overall assessment over 80

```
permit(principal, action, resource) when {
  context.identity.email like “*@example.com”
  && context.device.risk == “LOW”
};
```

Allow access when the user’s email is in the @example.com domain, and their device risk is reported Low

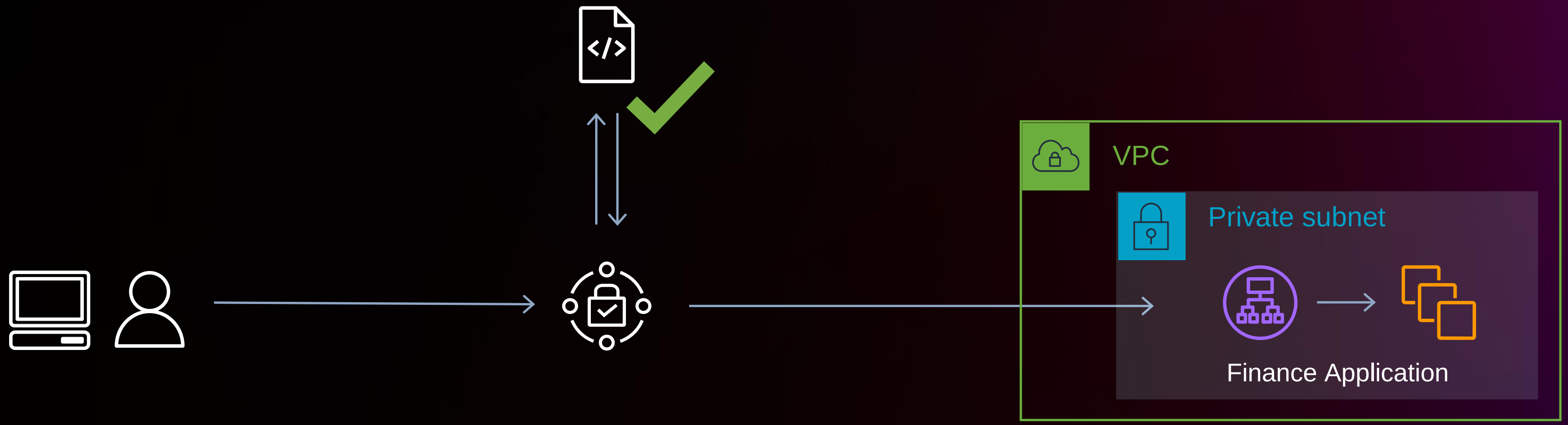
```
permit(principal, action, resource) when {
  context.http_request.http_method == “POST”
  && context.idp.groups has “Administrator”
  && context.dev.patched == true
};
```

Allow POSTs when the user is in the Administrator group and their device is patched

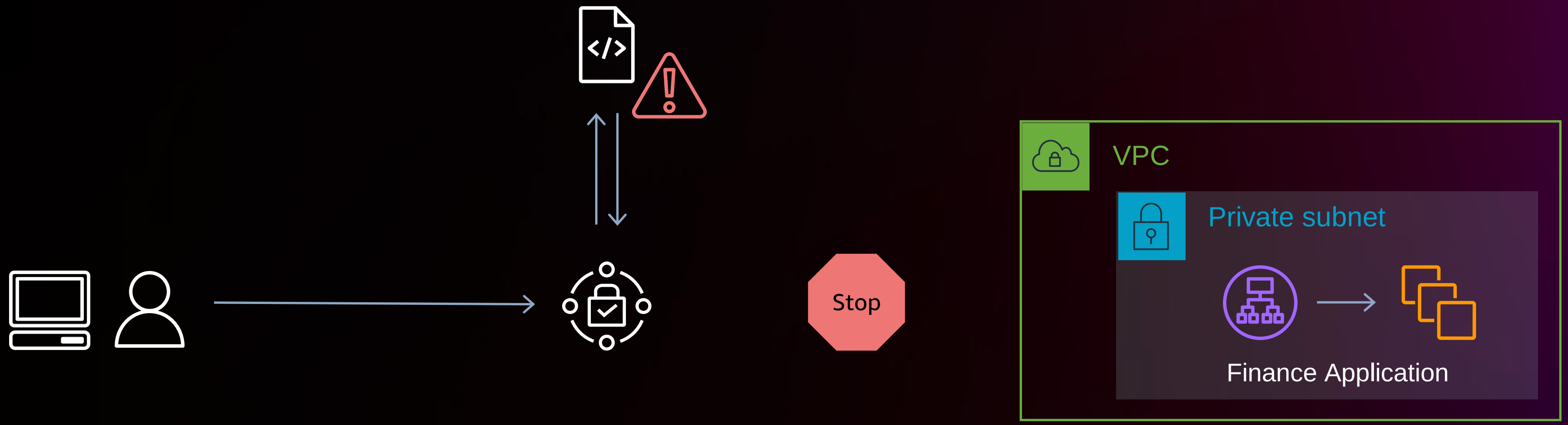
```
forbid(principal, action, resource) when {
   context.device.manufacturer == “ShadyCorp”
};
```

Deny access if the user is using an untrusted device

# Cedar – Isolated evaluation

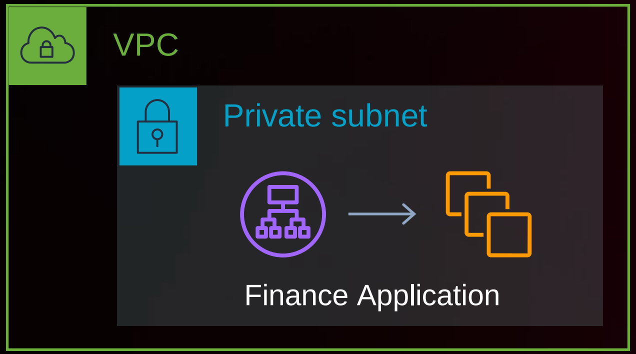


# Cedar – Isolated evaluation

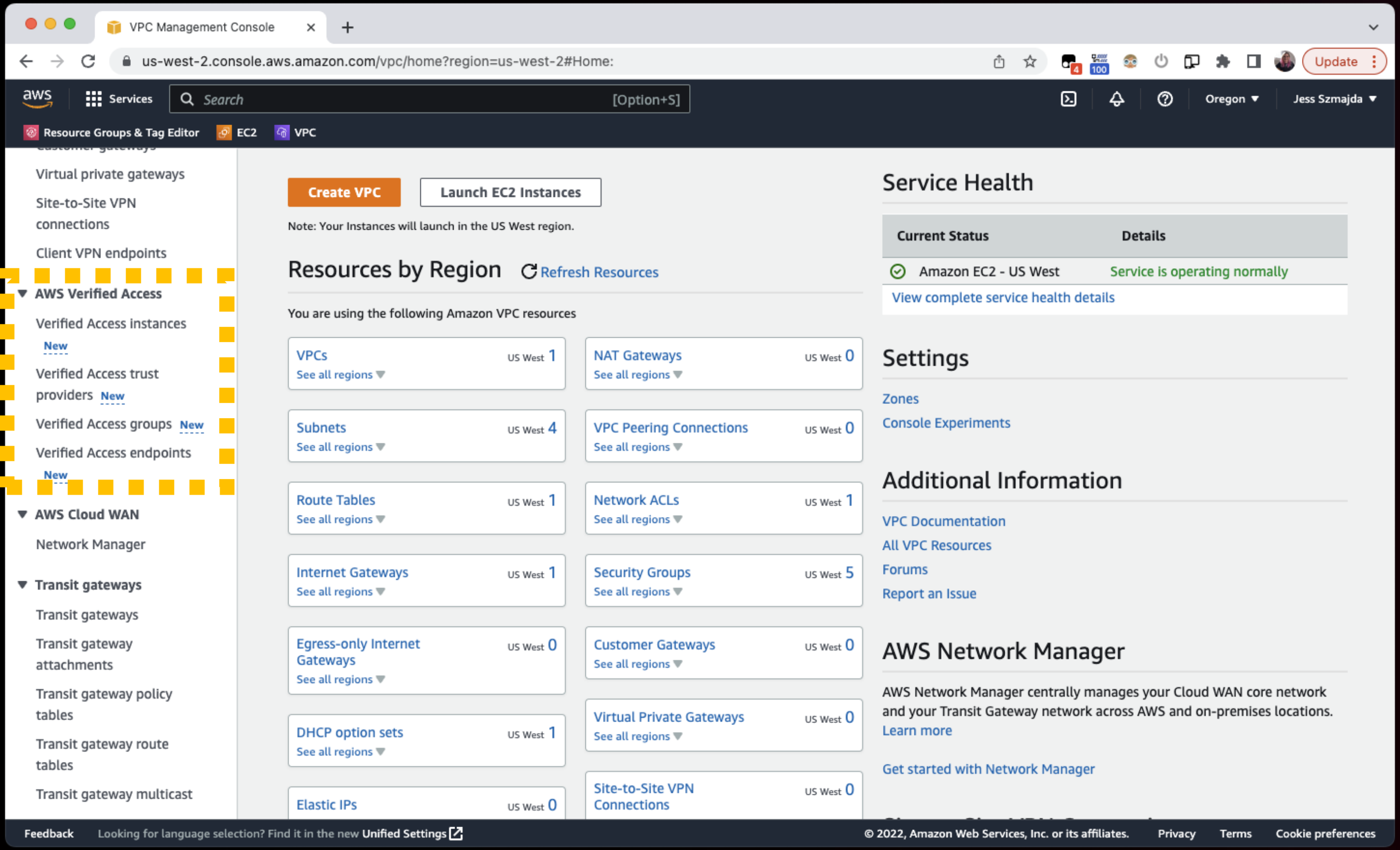


# Demo

# Demo – Publish private application



# Demo – Publish private application



VPC Management Console
us-west-2.console.aws.amazon.com/vpc/home?region=us-west-2#Home:
Update
aws
Services
Search
[Option+S]
Oregon ▼
Jess Szmajda ▼
Resource Groups & Tag Editor
EC2
VPC

Virtual private gateways

Site-to-Site VPN connections

Client VPN endpoints

▼ AWS Verified Access

Verified Access instances New

Verified Access trust providers New

Verified Access groups New

Verified Access endpoints New

▼ AWS Cloud WAN

Network Manager

▼ Transit gateways

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

Create VPC

Launch EC2 Instances

Note: Your Instances will launch in the US West region.

## Resources by Region

Refresh Resources

You are using the following Amazon VPC resources

| Resource | Region | Count |
|---|---|---|
| VPCs | US West | 1 |
| NAT Gateways | US West | 0 |
| Subnets | US West | 4 |
| VPC Peering Connections | US West | 0 |
| Route Tables | US West | 1 |
| Network ACLs | US West | 1 |
| Internet Gateways | US West | 1 |
| Security Groups | US West | 5 |
| Egress-only Internet Gateways | US West | 0 |
| Customer Gateways | US West | 0 |
| DHCP option sets | US West | 1 |
| Virtual Private Gateways | US West | 0 |
| Elastic IPs | US West | 0 |
| Site-to-Site VPN Connections | US West | 0 |

See all regions ▼

## Service Health

| Current Status | Details |
|---|---|
| ✓ Amazon EC2 - US West | Service is operating normally |

View complete service health details

## Settings

Zones

Console Experiments

## Additional Information

VPC Documentation

All VPC Resources

Forums

Report an Issue

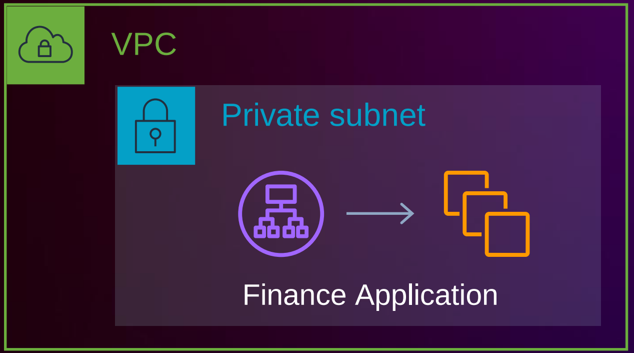
## AWS Network Manager

AWS Network Manager centrally manages your Cloud WAN core network and your Transit Gateway network across AWS and on-premises locations. Learn more

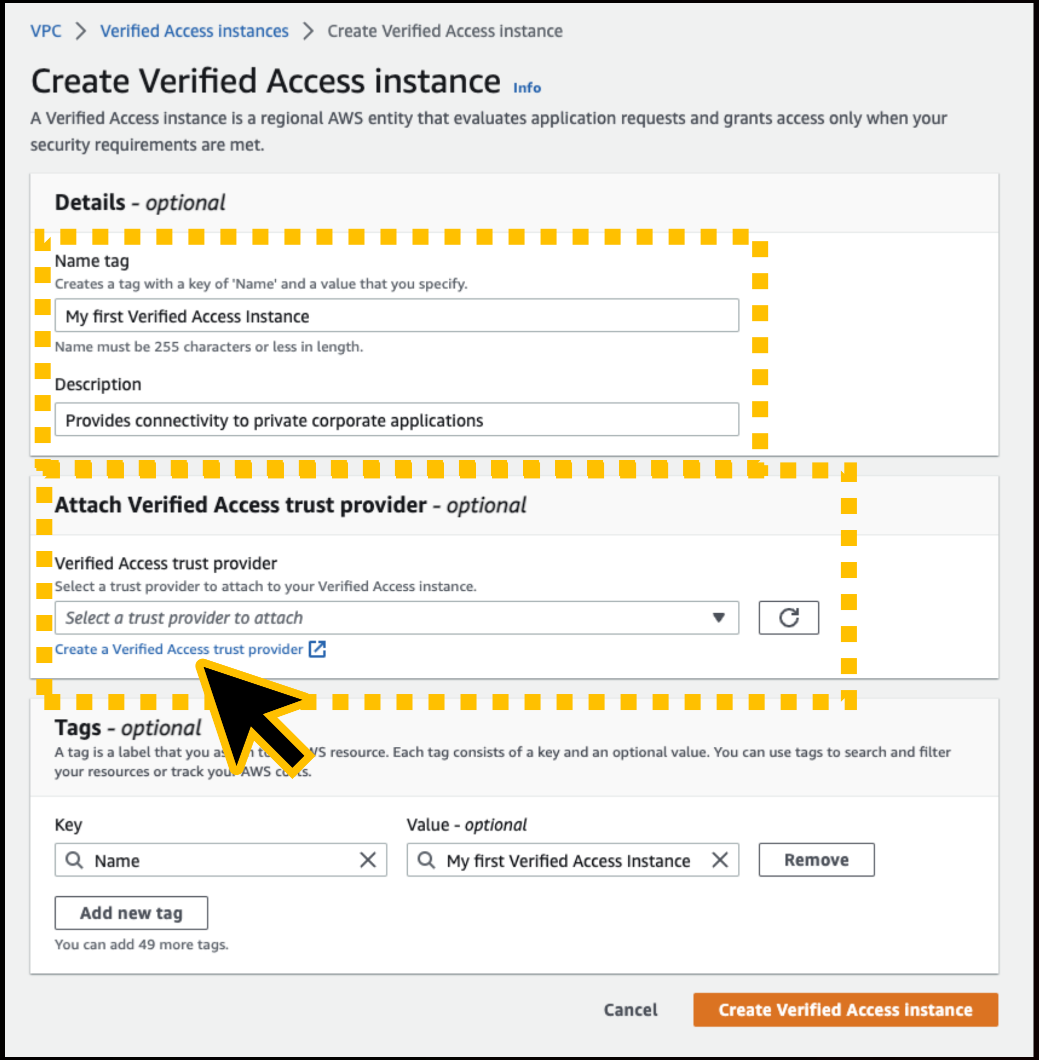
Get started with Network Manager

Feedback Looking for language selection? Find it in the new Unified Settings

© 2022, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



# Demo – Configure Verified Access instance



VPC > Verified Access instances > Create Verified Access instance

## Create Verified Access instance Info

A Verified Access instance is a regional AWS entity that evaluates application requests and grants access only when your security requirements are met.

### Details - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
My first Verified Access Instance
Name must be 255 characters or less in length.

Description
Provides connectivity to private corporate applications

### Attach Verified Access trust provider - *optional*

Verified Access trust provider
Select a trust provider to attach to your Verified Access instance.
*Select a trust provider to attach* ▼
Create a Verified Access trust provider

### Tags - *optional*

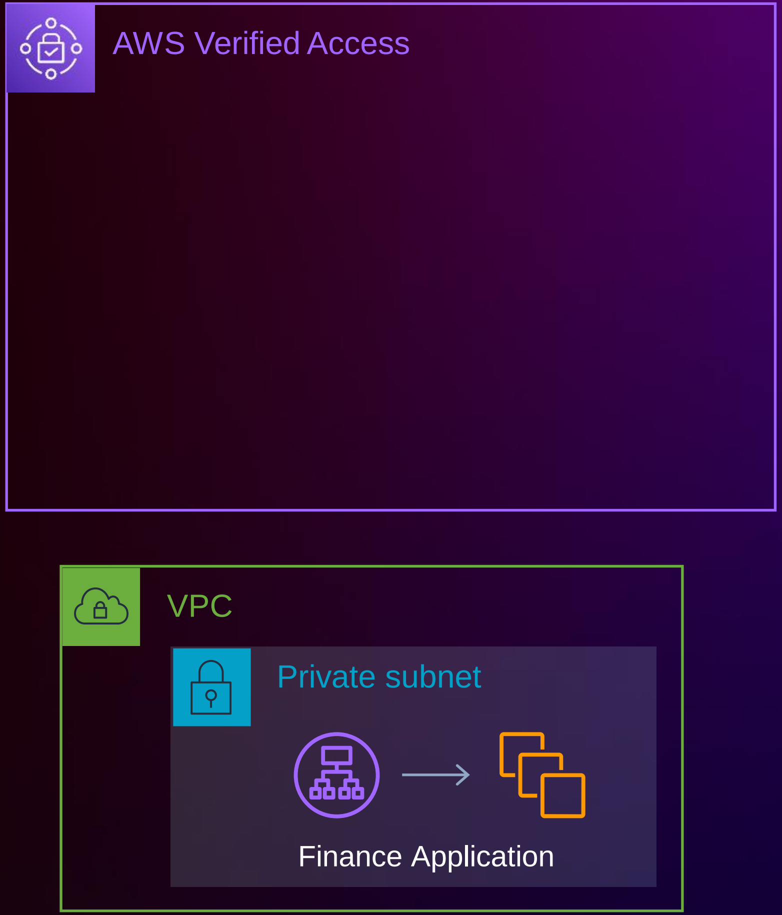
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* | |
|---|---|---|
| Name | My first Verified Access Instance | Remove |

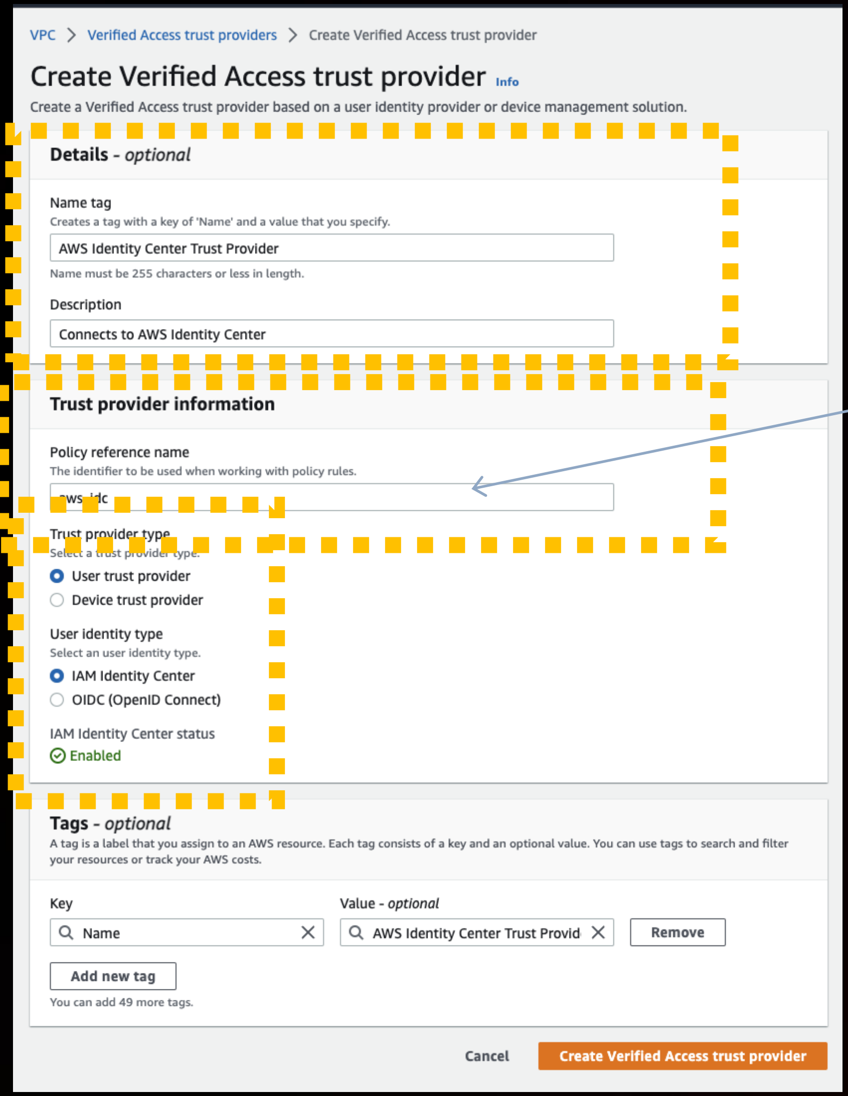
Add new tag

You can add 49 more tags.

Cancel    Create Verified Access instance



# Demo – Configure trust provider



VPC > Verified Access trust providers > Create Verified Access trust provider

## Create Verified Access trust provider Info

Create a Verified Access trust provider based on a user identity provider or device management solution.

**Details** - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
AWS Identity Center Trust Provider
Name must be 255 characters or less in length.

Description
Connects to AWS Identity Center

**Trust provider information**

Policy reference name
The identifier to be used when working with policy rules.
aws_idc

Trust provider type
Select a trust provider type.
● User trust provider
○ Device trust provider

User identity type
Select an user identity type.
● IAM Identity Center
○ OIDC (OpenID Connect)

IAM Identity Center status
✓ Enabled

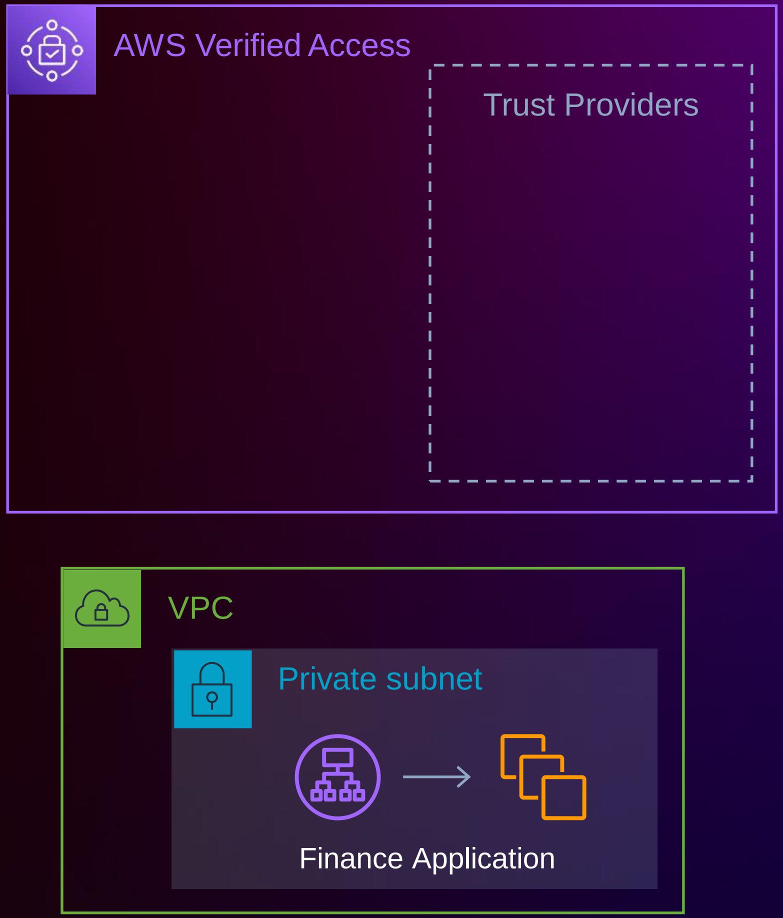
**Tags** - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* | |
|---|---|---|
| Name | AWS Identity Center Trust Provid | Remove |

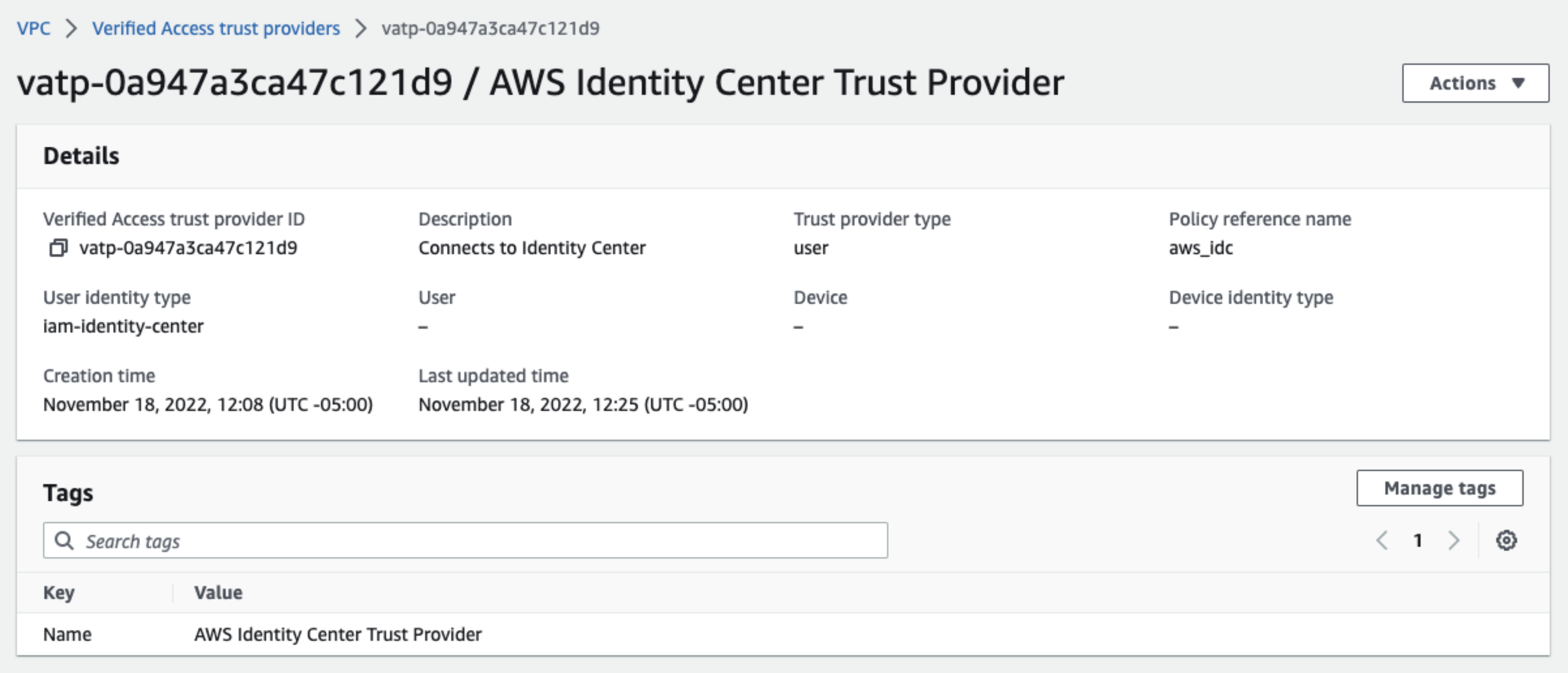
Add new tag
You can add 49 more tags.

Cancel | Create Verified Access trust provider

aws_idc



# Demo – Configure trust provider



VPC > Verified Access trust providers > vatp-0a947a3ca47c121d9

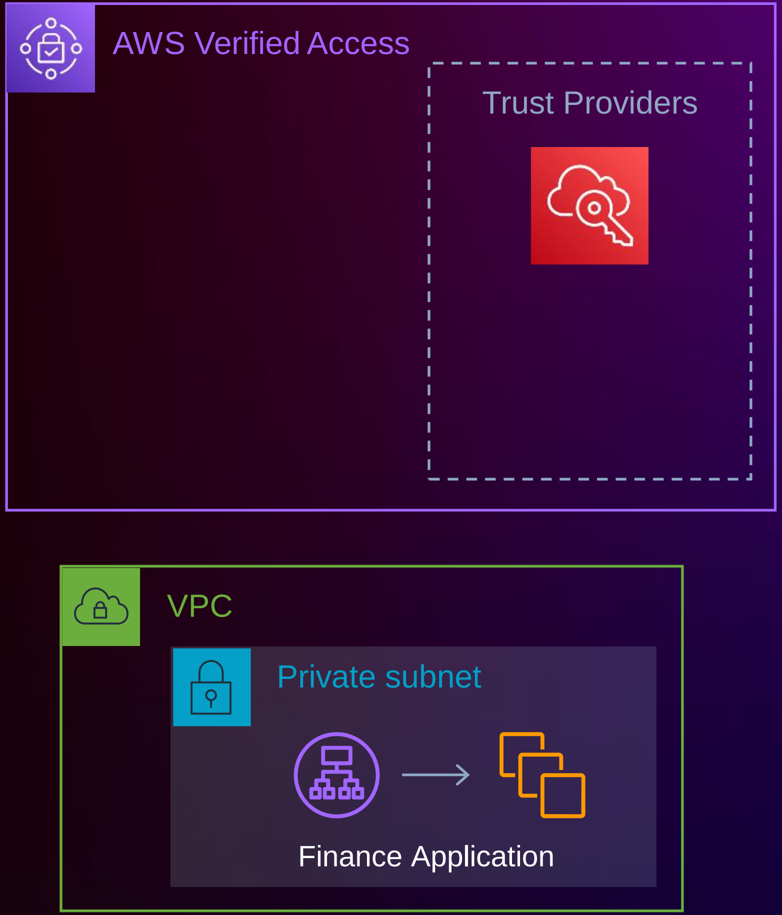
## vatp-0a947a3ca47c121d9 / AWS Identity Center Trust Provider

### Details

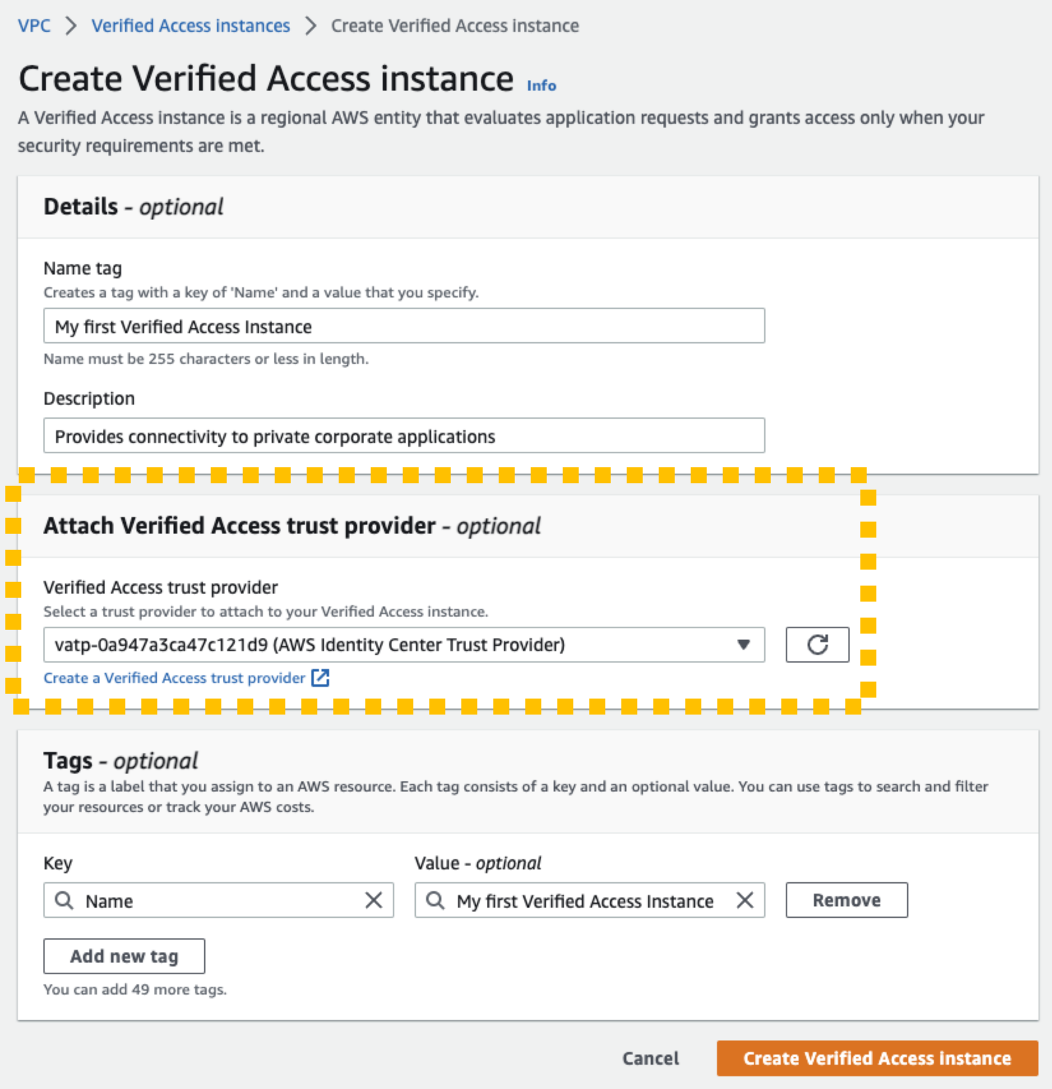
| | | | |
|---|---|---|---|
| Verified Access trust provider ID<br>vatp-0a947a3ca47c121d9 | Description<br>Connects to Identity Center | Trust provider type<br>user | Policy reference name<br>aws_idc |
| User identity type<br>iam-identity-center | User<br>– | Device<br>– | Device identity type<br>– |
| Creation time<br>November 18, 2022, 12:08 (UTC -05:00) | Last updated time<br>November 18, 2022, 12:25 (UTC -05:00) | | |

### Tags

| Key | Value |
|---|---|
| Name | AWS Identity Center Trust Provider |



# Demo – Select trust provider



VPC > Verified Access instances > Create Verified Access instance

## Create Verified Access instance Info

A Verified Access instance is a regional AWS entity that evaluates application requests and grants access only when your security requirements are met.

**Details** - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
My first Verified Access Instance
Name must be 255 characters or less in length.

Description
Provides connectivity to private corporate applications

**Attach Verified Access trust provider** - *optional*

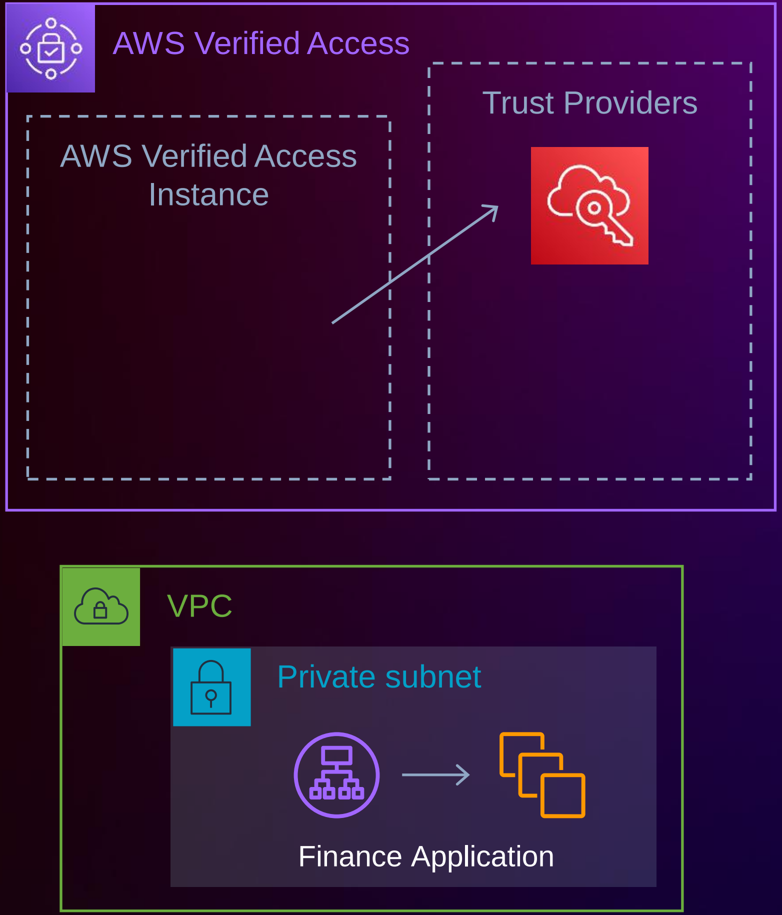
Verified Access trust provider
Select a trust provider to attach to your Verified Access instance.
vatp-0a947a3ca47c121d9 (AWS Identity Center Trust Provider)
Create a Verified Access trust provider

**Tags** - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

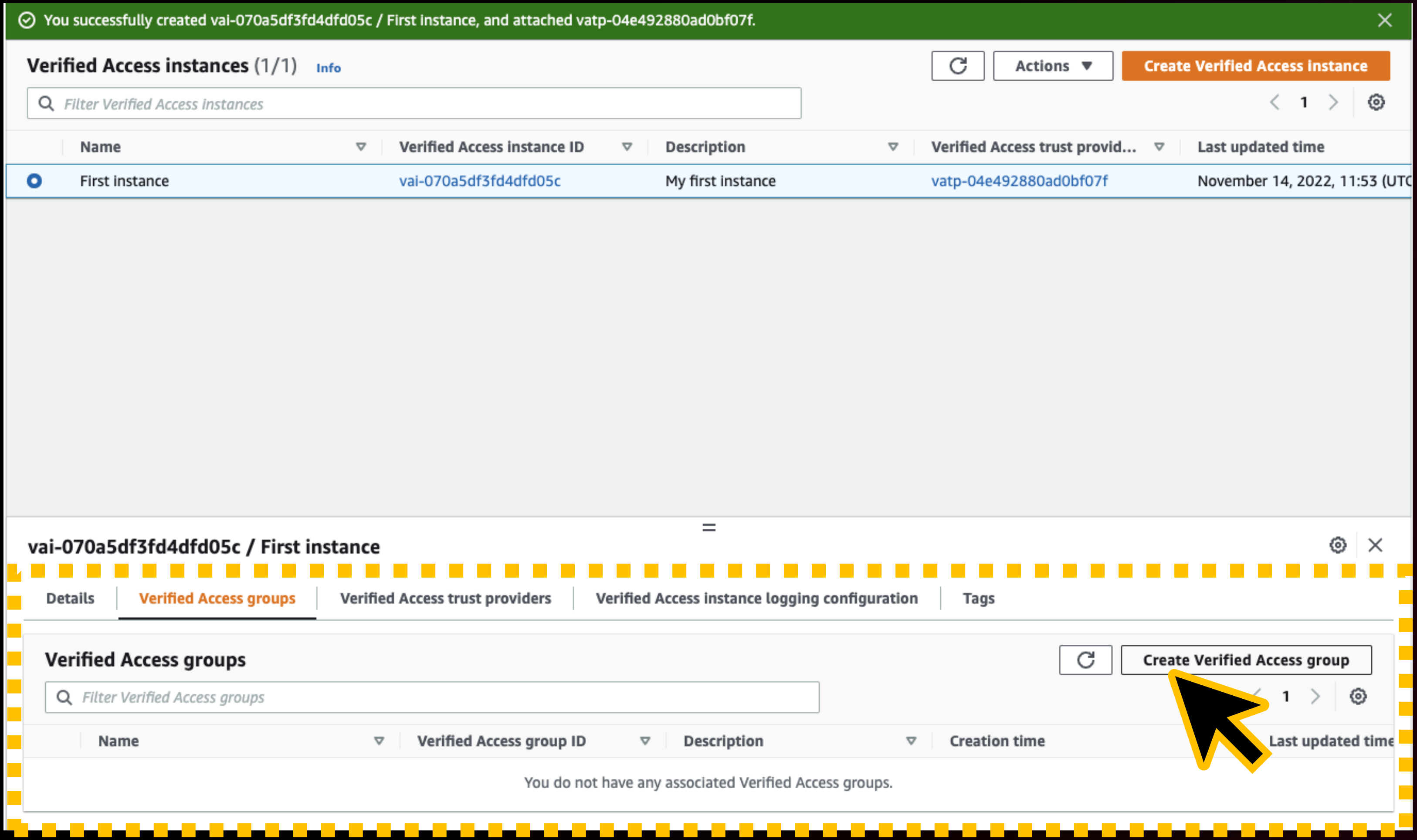
| Key | Value - *optional* | |
|---|---|---|
| Name | My first Verified Access Instance | Remove |

Add new tag
You can add 49 more tags.

Cancel | Create Verified Access instance



# Demo – Create Verified Access group



You successfully created vai-070a5df3fd4dfd05c / First instance, and attached vatp-04e492880ad0bf07f.

**Verified Access instances** (1/1) Info

Actions ▼
Create Verified Access instance
Filter Verified Access instances

| | Name | Verified Access instance ID | Description | Verified Access trust provid... | Last updated time |
|---|---|---|---|---|---|
| ● | First instance | vai-070a5df3fd4dfd05c | My first instance | vatp-04e492880ad0bf07f | November 14, 2022, 11:53 (UTC |

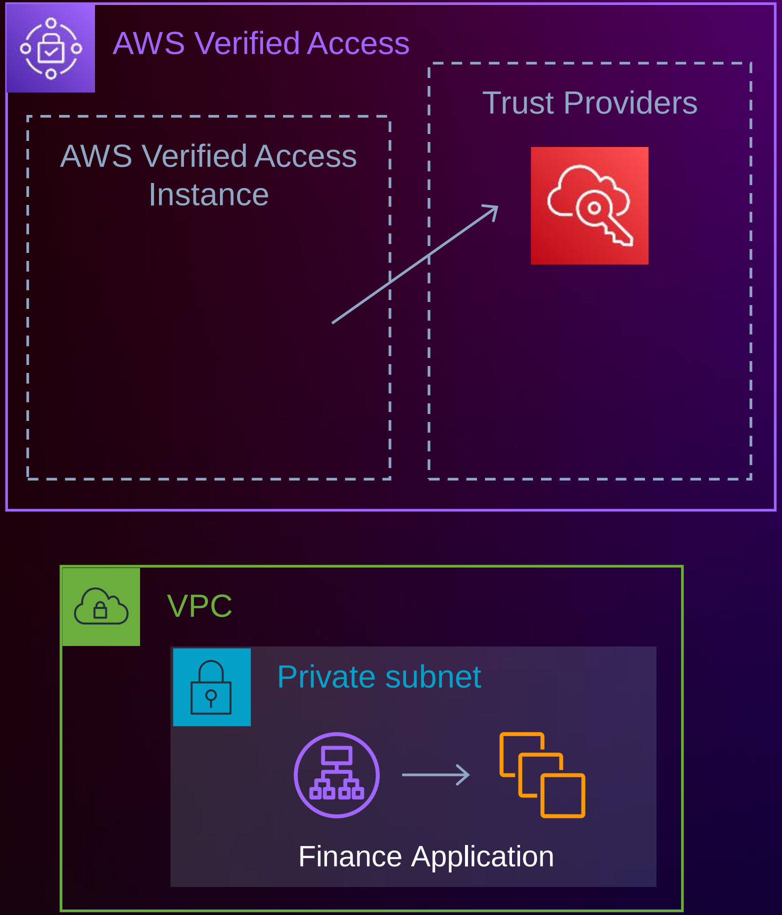
**vai-070a5df3fd4dfd05c / First instance**

Details
Verified Access groups
Verified Access trust providers
Verified Access instance logging configuration
Tags

**Verified Access groups**

| | Name | Verified Access group ID | Description | Creation time | Last updated time |
|---|---|---|---|---|---|

You do not have any associated Verified Access groups.



AWS Verified Access

AWS Verified Access Instance

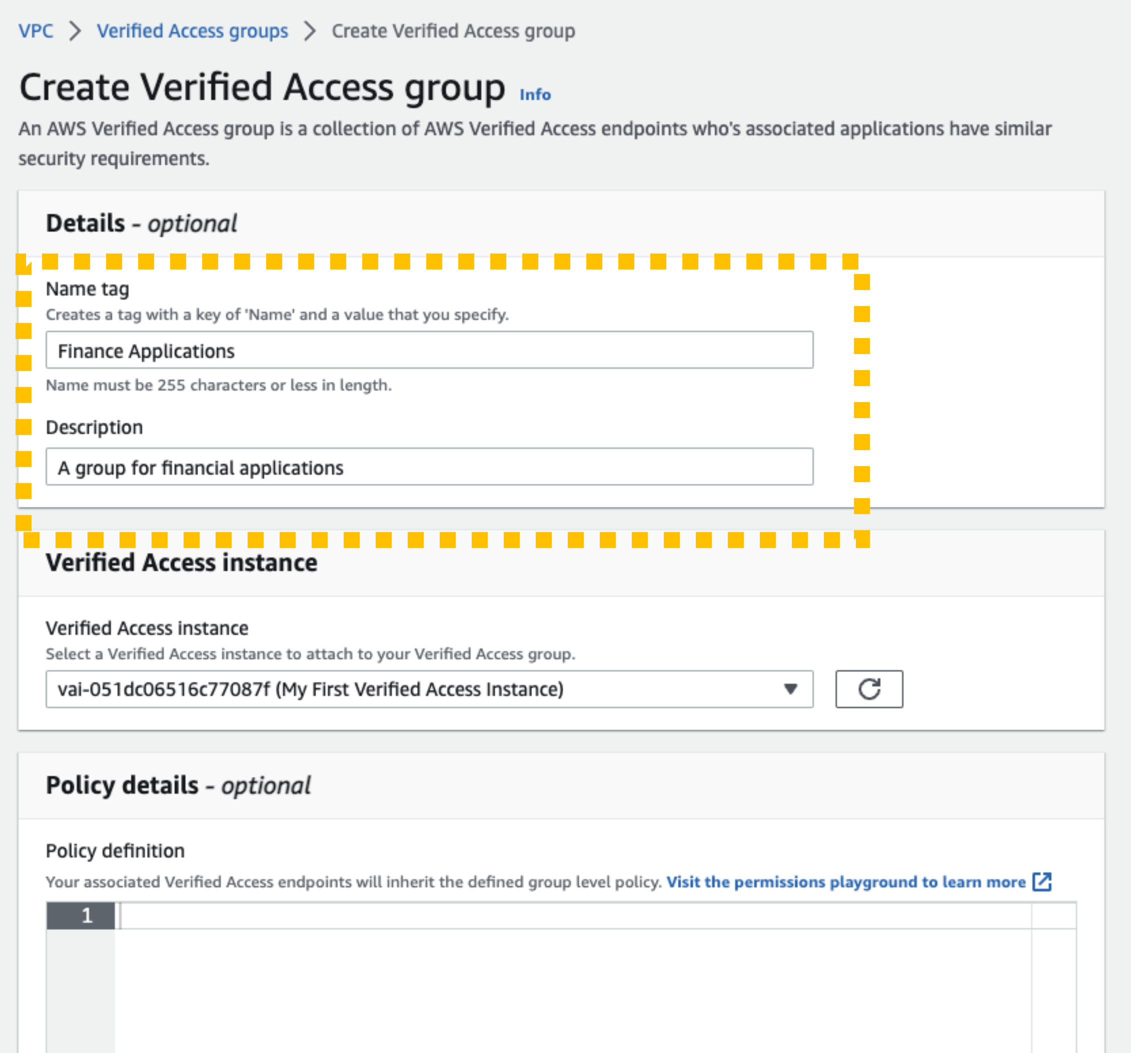
Trust Providers

VPC

Private subnet

Finance Application

# Demo – Create Verified Access group



VPC > Verified Access groups > Create Verified Access group

Create Verified Access group Info

An AWS Verified Access group is a collection of AWS Verified Access endpoints who's associated applications have similar security requirements.

**Details** - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
Finance Applications
Name must be 255 characters or less in length.

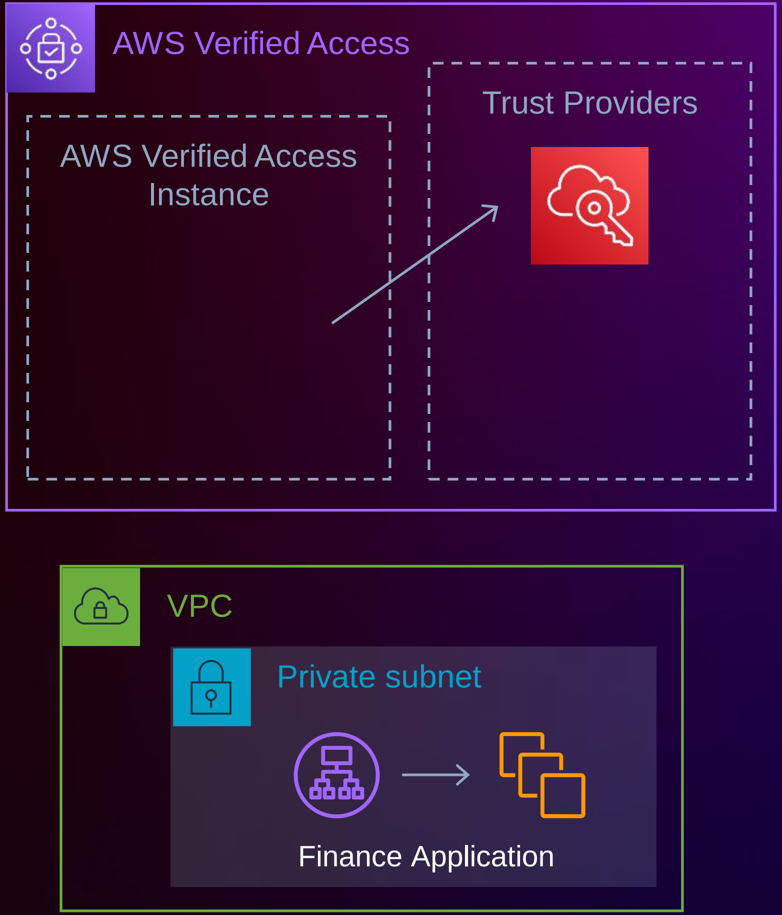
Description
A group for financial applications

**Verified Access instance**

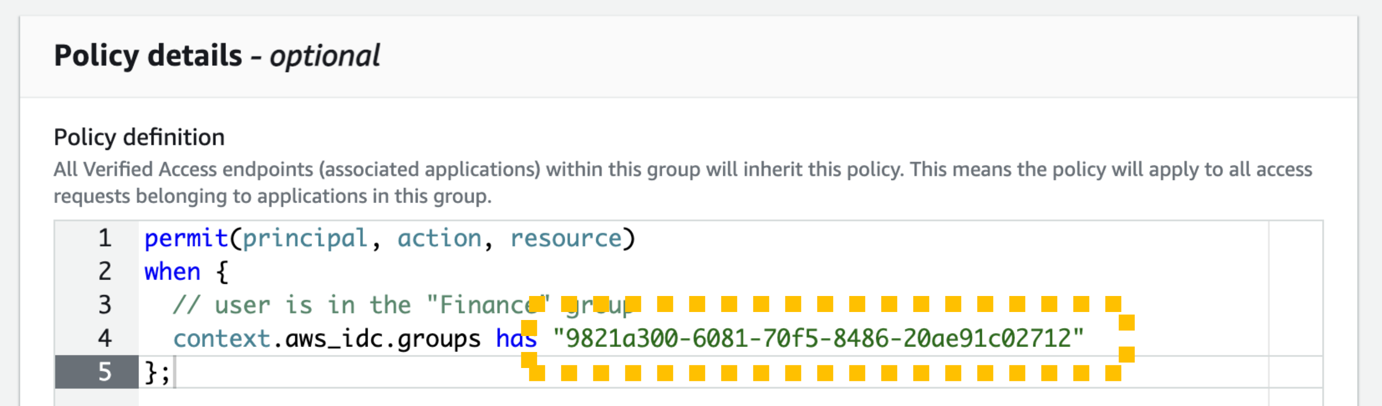
Verified Access instance
Select a Verified Access instance to attach to your Verified Access group.
vai-051dc06516c77087f (My First Verified Access Instance)

**Policy details** - *optional*

Policy definition
Your associated Verified Access endpoints will inherit the defined group level policy. Visit the permissions playground to learn more



# Demo – Write group policy



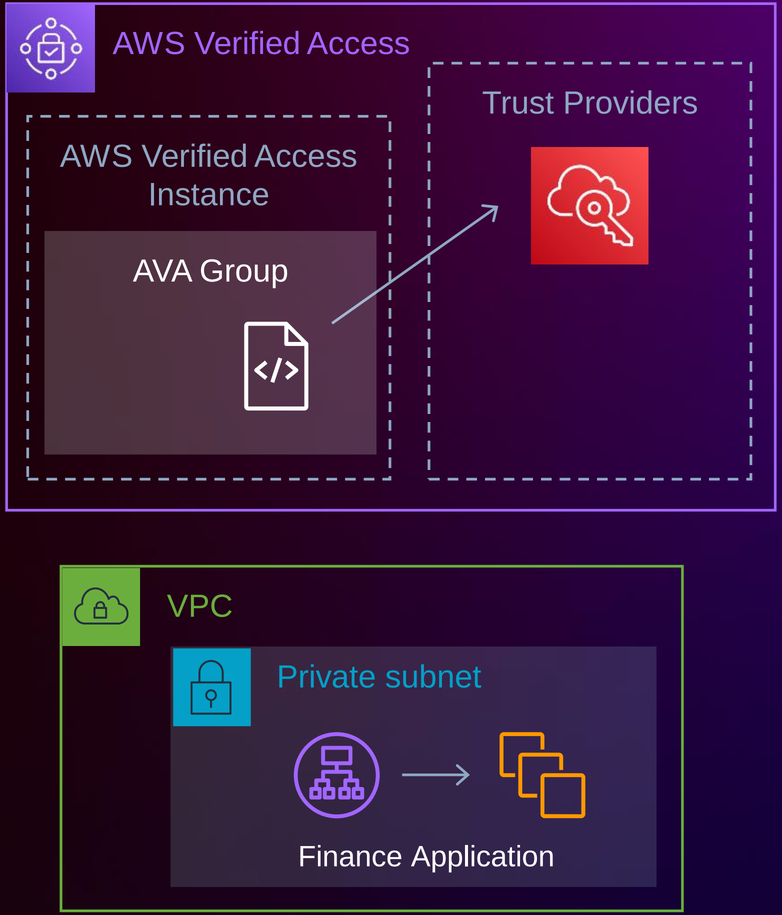
**Policy details** - *optional*

Policy definition

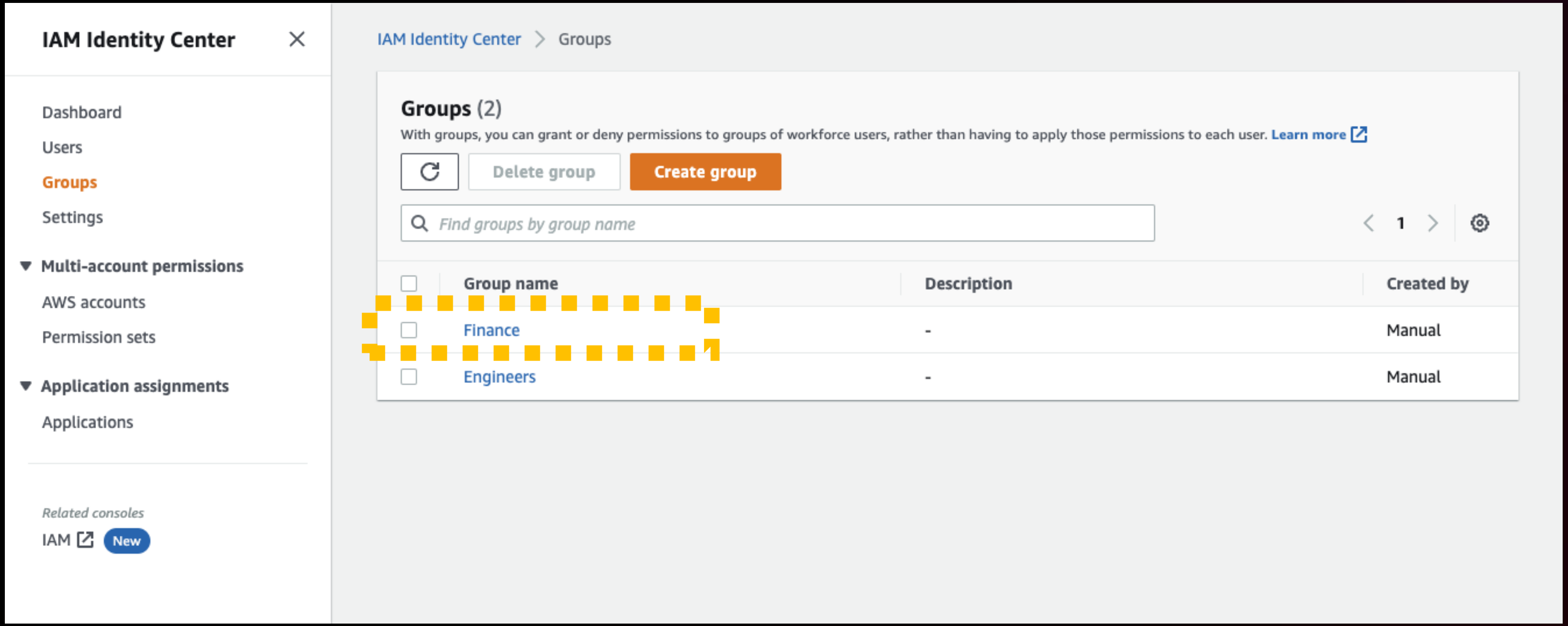
All Verified Access endpoints (associated applications) within this group will inherit this policy. This means the policy will apply to all access requests belonging to applications in this group.

```
permit(principal, action, resource)
when {
  // user is in the "Finance" group
  context.aws_idc.groups has "9821a300-6081-70f5-8486-20ae91c02712"
};
```

```
{
  “user”: {
    “user_id”: “f8f1a3a0-10d1-70cd-2453-fcf071d03773”,
    “user_name”: “test_user”,
    “email”: {
      “address”: “test@example.com”,
      “verified”: false
    }
  }
  “groups”: {
    “9821a300-6081-70f5-8486-20ae91c02712”: {
      “group_id”: “9821a300-6081-70f5-8486-20ae91c02712”,
      “group_name”: “Finance”
    },
    “08318370-c061-7018-509f-2022a83f3752”: {
      “group_id”: “08318370-c061-7018-509f-2022a83f3752”,
      “group_name”: “Engineers”
    }
  }
}
```



# Demo – Look up group ID



**IAM Identity Center** ✕

- Dashboard
- Users
- Groups
- Settings

▼ **Multi-account permissions**

- AWS accounts
- Permission sets

▼ **Application assignments**

- Applications

*Related consoles*

IAM New

IAM Identity Center > Groups

**Groups** (2)

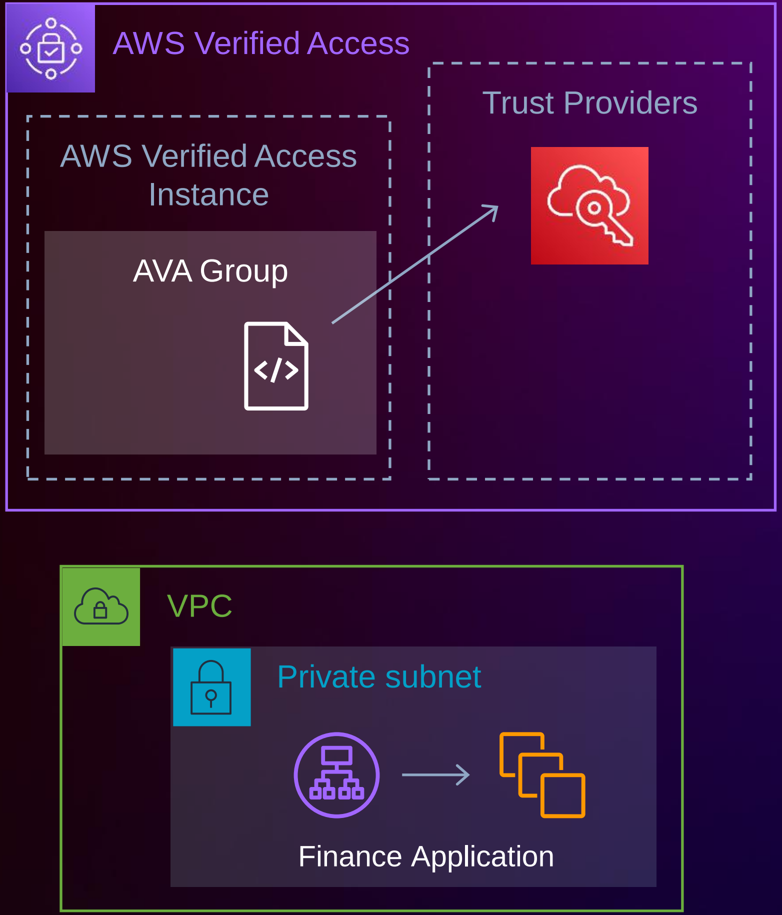
With groups, you can grant or deny permissions to groups of workforce users, rather than having to apply those permissions to each user. Learn more

Delete group | Create group

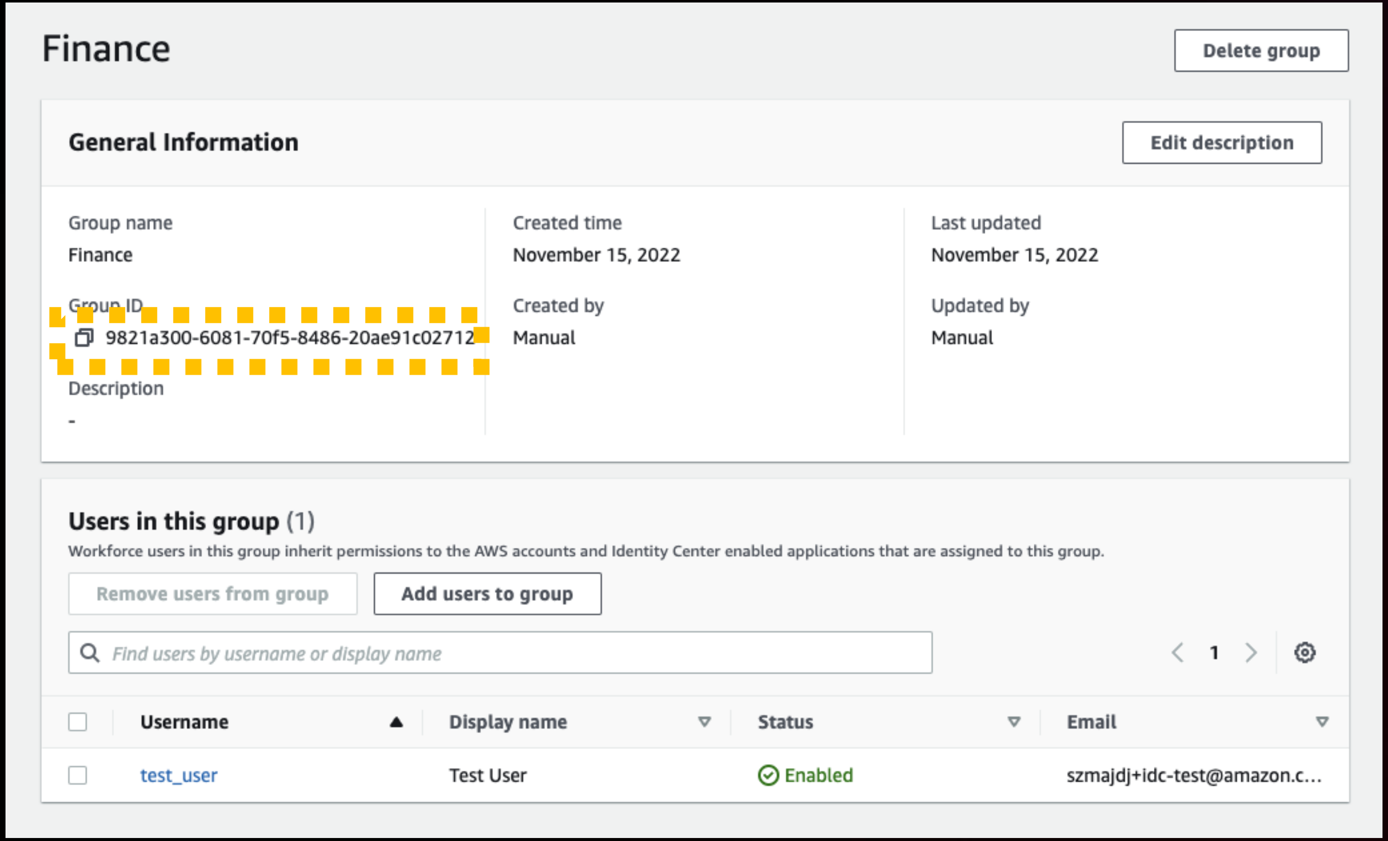
Find groups by group name

< 1 >

| □ | Group name | Description | Created by |
|---|---|---|---|
| □ | Finance | - | Manual |
| □ | Engineers | - | Manual |



# Demo – Look up group ID



## Finance

Delete group

### General Information

Edit description

| | | |
|---|---|---|
| Group name<br>Finance | Created time<br>November 15, 2022 | Last updated<br>November 15, 2022 |
| Group ID<br>9821a300-6081-70f5-8486-20ae91c02712 | Created by<br>Manual | Updated by<br>Manual |
| Description<br>- | | |

### Users in this group (1)

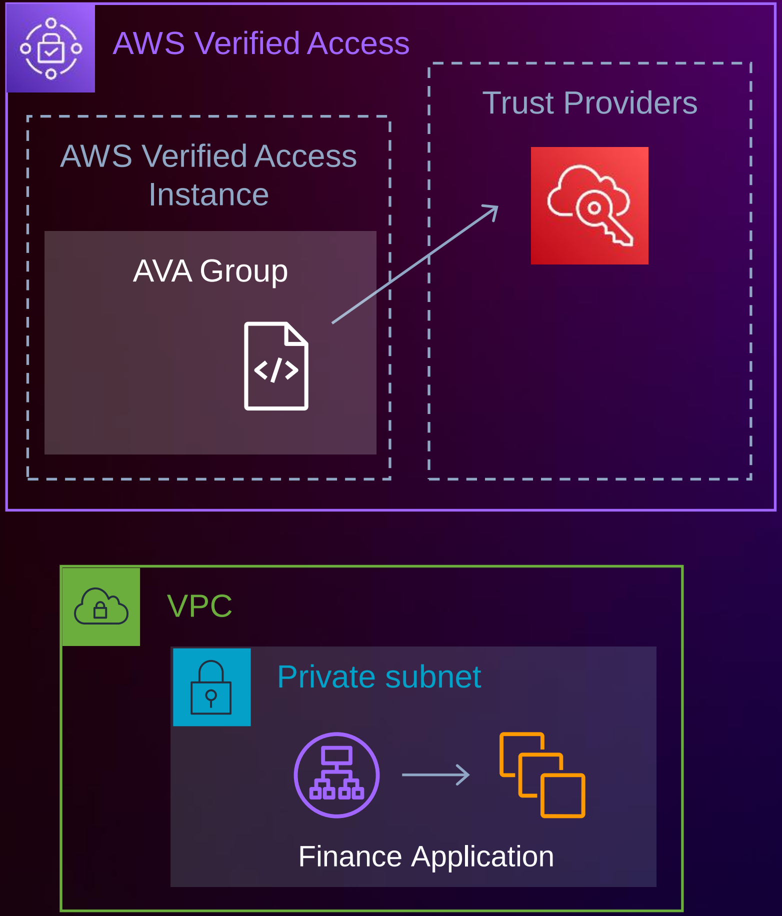
Workforce users in this group inherit permissions to the AWS accounts and Identity Center enabled applications that are assigned to this group.

Remove users from group | Add users to group

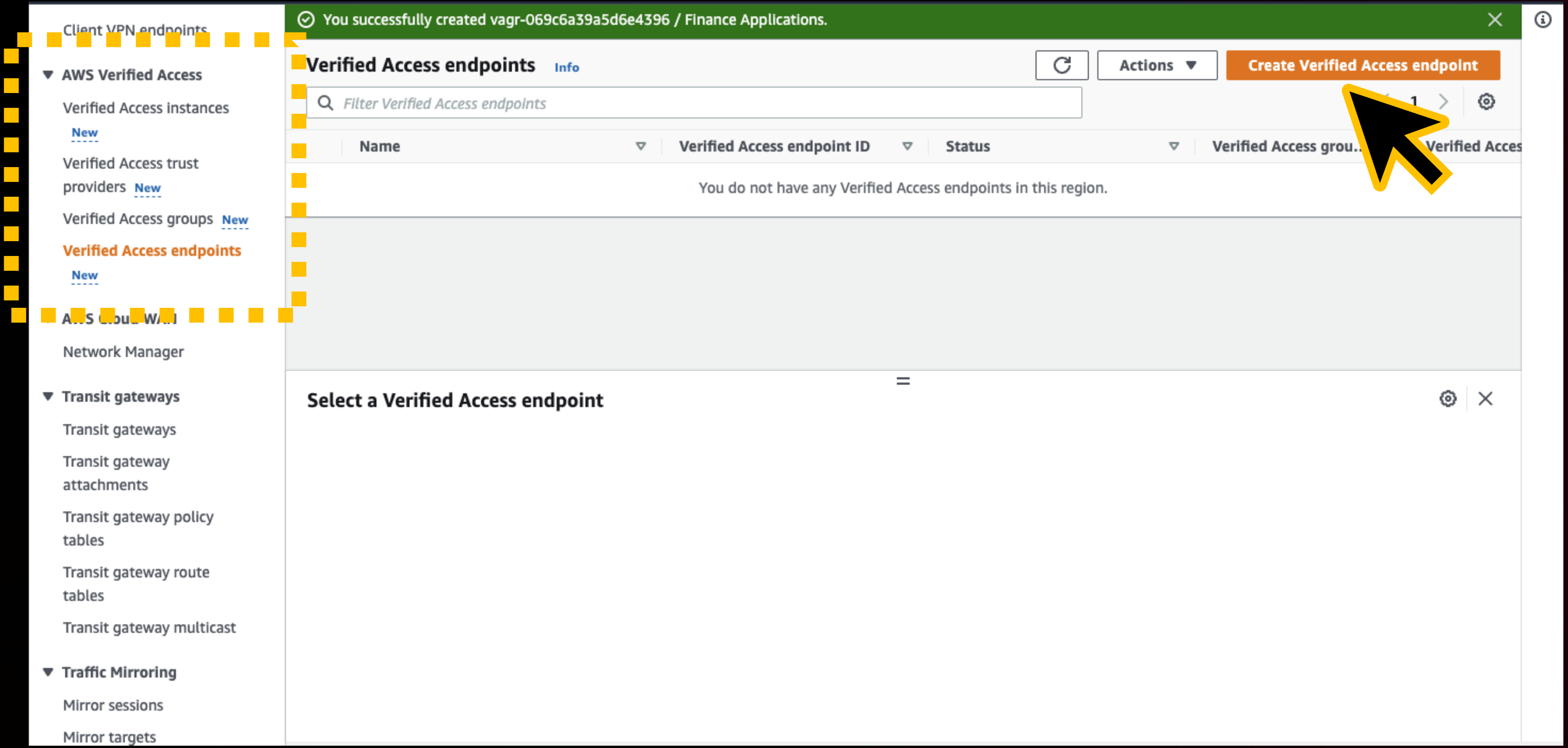
Find users by username or display name

< 1 >

| □ | Username | Display name | Status | Email |
|---|---|---|---|---|
| □ | test_user | Test User | ✓ Enabled | szmajdj+idc-test@amazon.c... |



# Demo – Create Verified Access endpoint



Client VPN endpoints

▼ AWS Verified Access

Verified Access instances New

Verified Access trust providers New

Verified Access groups New

Verified Access endpoints New

AWS Cloud WAN

Network Manager

▼ Transit gateways

Transit gateways

Transit gateway attachments

Transit gateway policy tables

Transit gateway route tables

Transit gateway multicast

▼ Traffic Mirroring

Mirror sessions

Mirror targets

You successfully created vagr-069c6a39a5d6e4396 / Finance Applications.

Verified Access endpoints Info

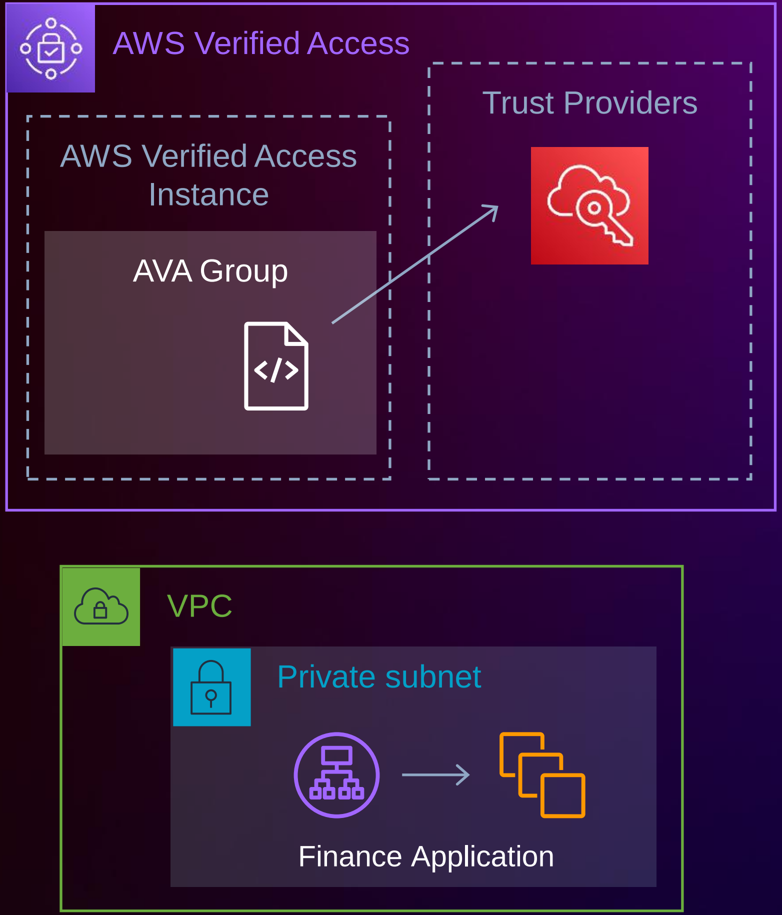
Actions ▼ | Create Verified Access endpoint

Filter Verified Access endpoints

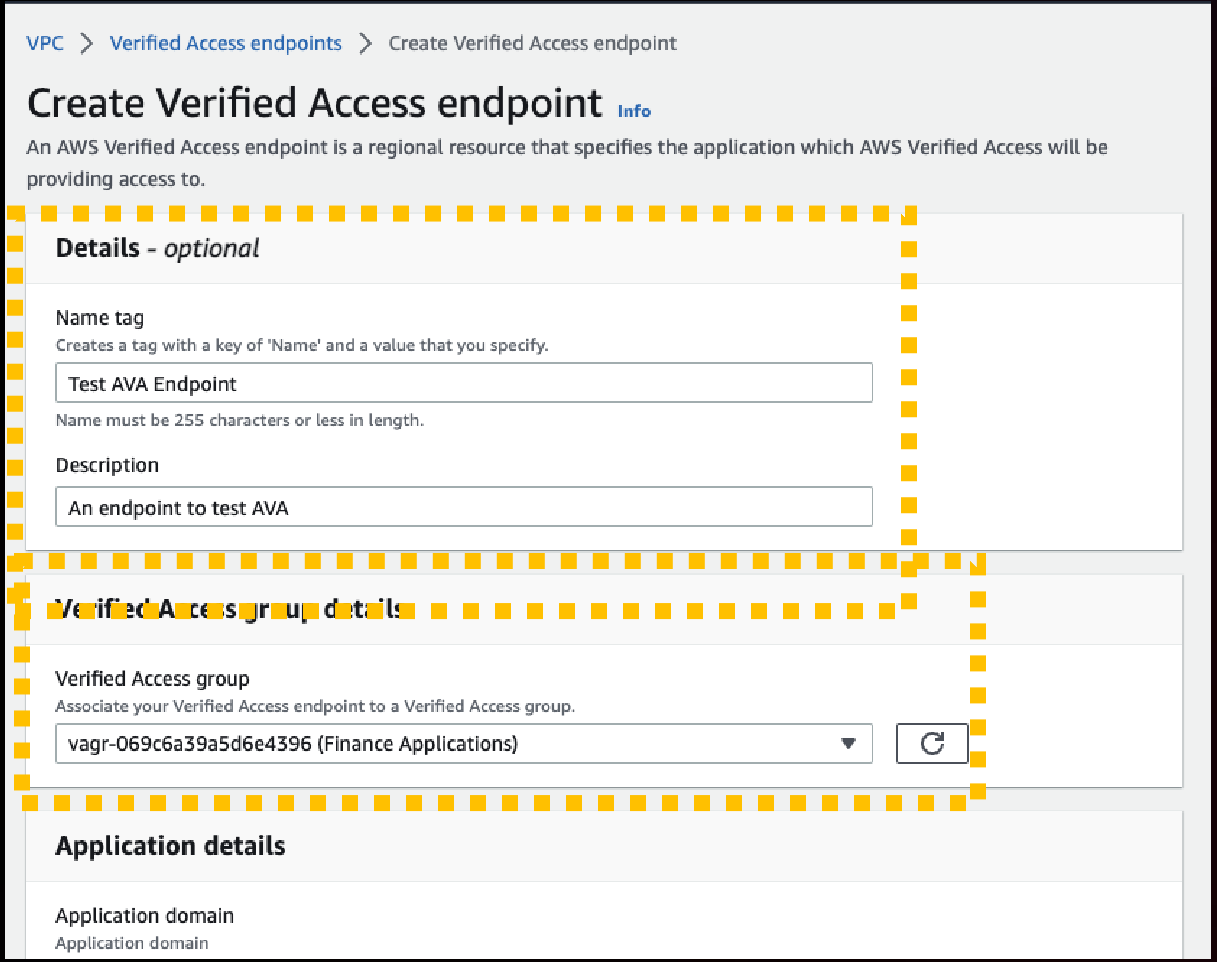
| Name | Verified Access endpoint ID | Status | Verified Access grou... | Verified Acces |
|---|---|---|---|---|

You do not have any Verified Access endpoints in this region.

Select a Verified Access endpoint



# Demo – Create Verified Access endpoint



VPC > Verified Access endpoints > Create Verified Access endpoint

## Create Verified Access endpoint Info

An AWS Verified Access endpoint is a regional resource that specifies the application which AWS Verified Access will be providing access to.

### Details - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
Test AVA Endpoint
Name must be 255 characters or less in length.

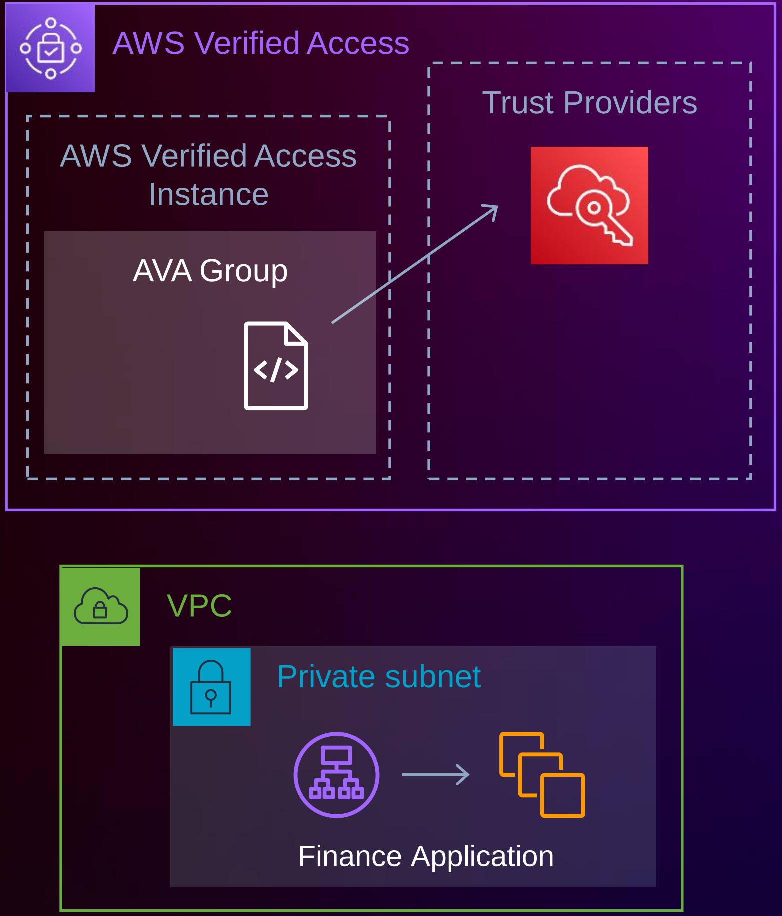
Description
An endpoint to test AVA

### Verified Access group details

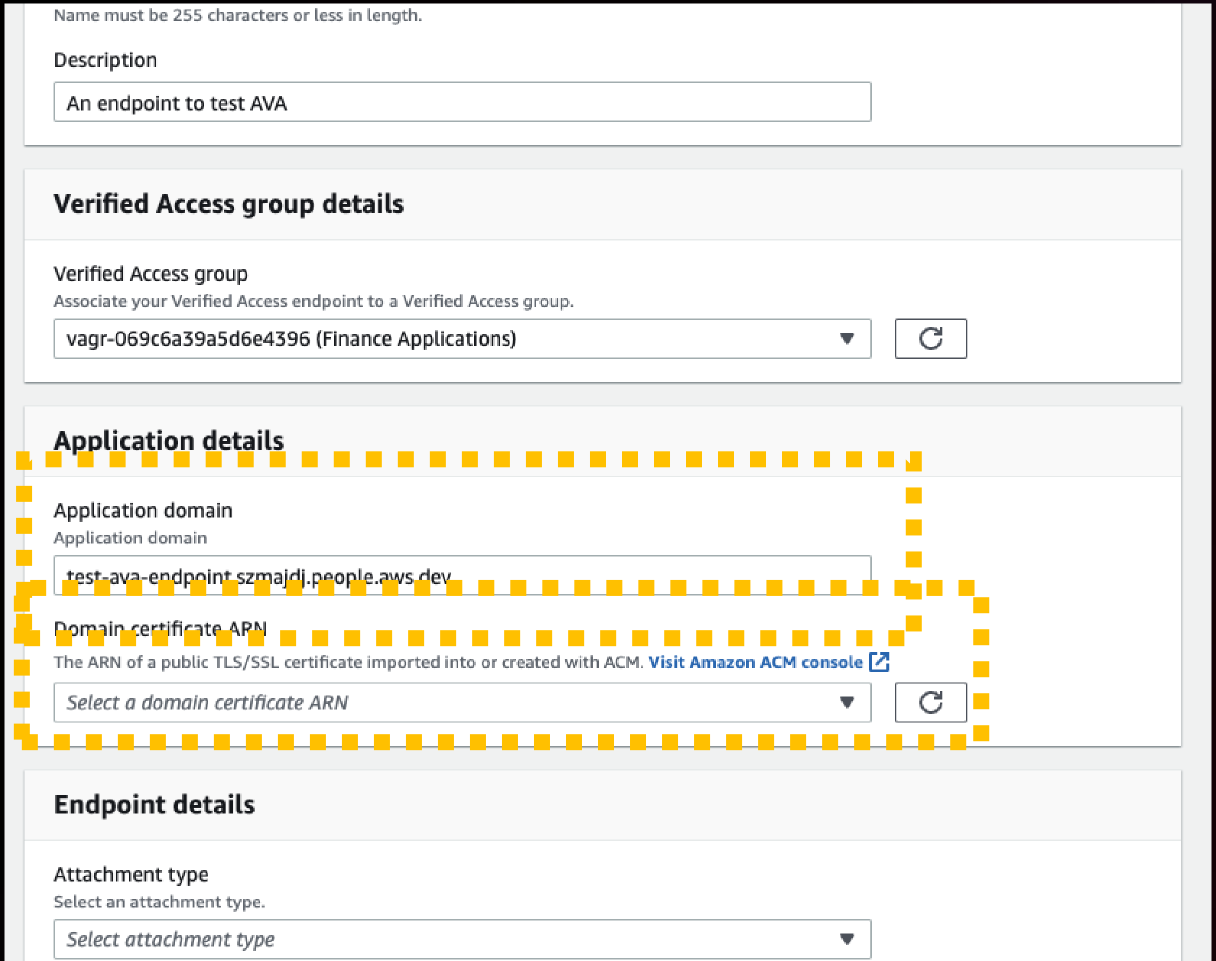
Verified Access group
Associate your Verified Access endpoint to a Verified Access group.
vagr-069c6a39a5d6e4396 (Finance Applications)

### Application details

Application domain
Application domain



# Demo – Configure endpoint domain



Name must be 255 characters or less in length.

Description

An endpoint to test AVA

**Verified Access group details**

Verified Access group

Associate your Verified Access endpoint to a Verified Access group.

vagr-069c6a39a5d6e4396 (Finance Applications)

**Application details**

Application domain

Application domain

test-ava-endpoint.szmajdj.people.aws.dev

Domain certificate ARN

The ARN of a public TLS/SSL certificate imported into or created with ACM. Visit Amazon ACM console

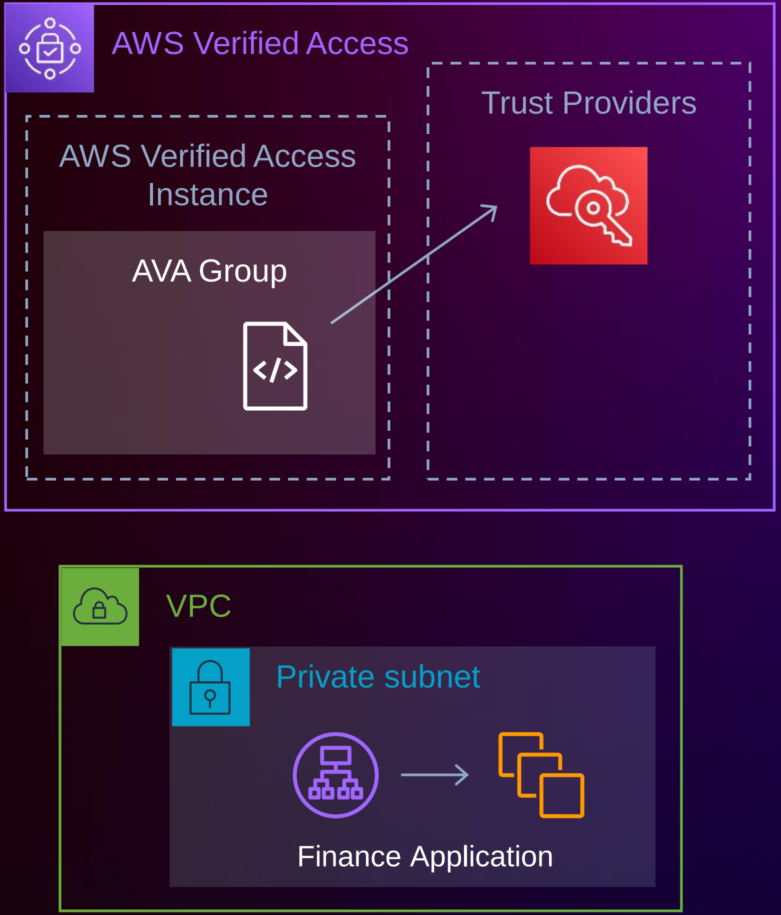
*Select a domain certificate ARN*

**Endpoint details**

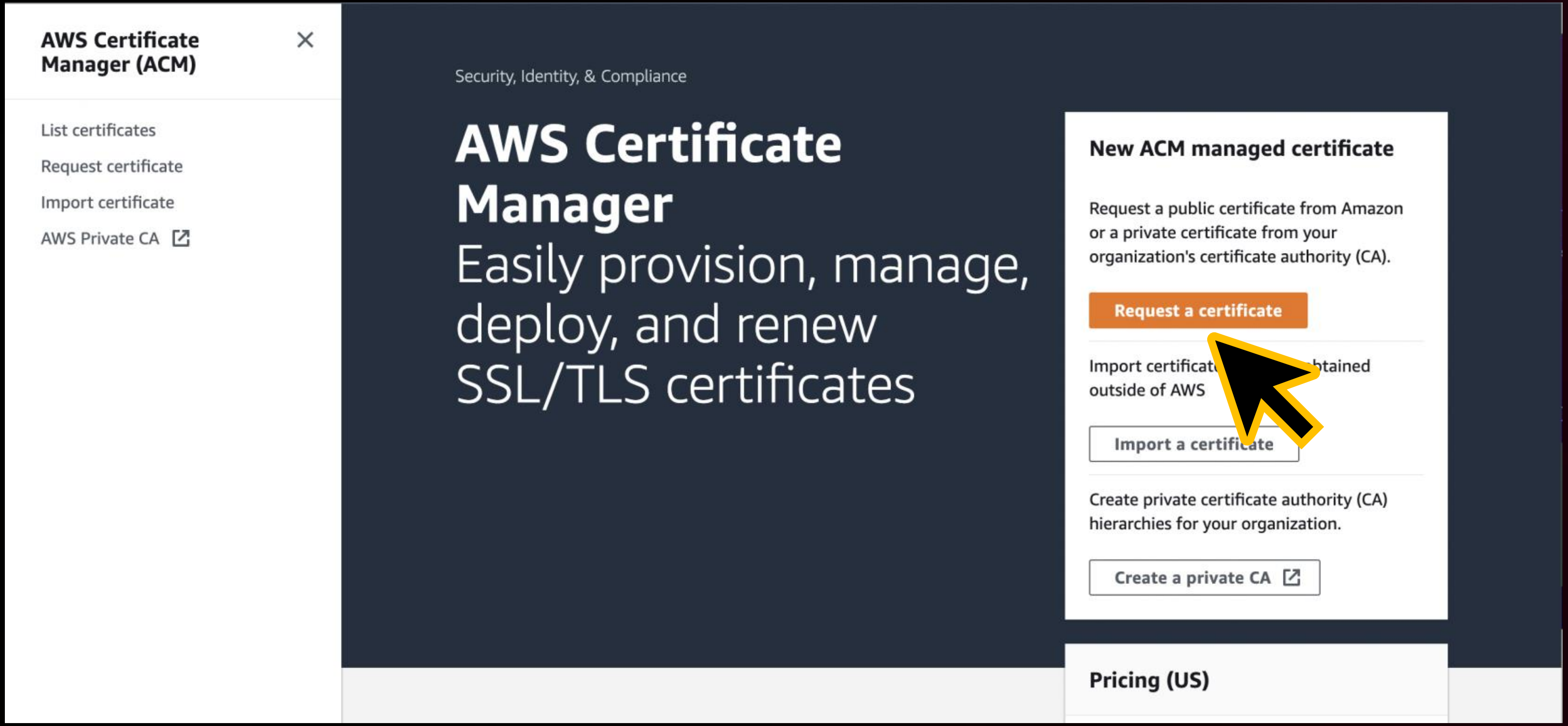
Attachment type

Select an attachment type.

*Select attachment type*



# Demo – Request endpoint domain certificate



**AWS Certificate Manager (ACM)**

- List certificates
- Request certificate
- Import certificate
- AWS Private CA

Security, Identity, & Compliance

## AWS Certificate Manager

Easily provision, manage, deploy, and renew SSL/TLS certificates

**New ACM managed certificate**

Request a public certificate from Amazon or a private certificate from your organization's certificate authority (CA).

Request a certificate

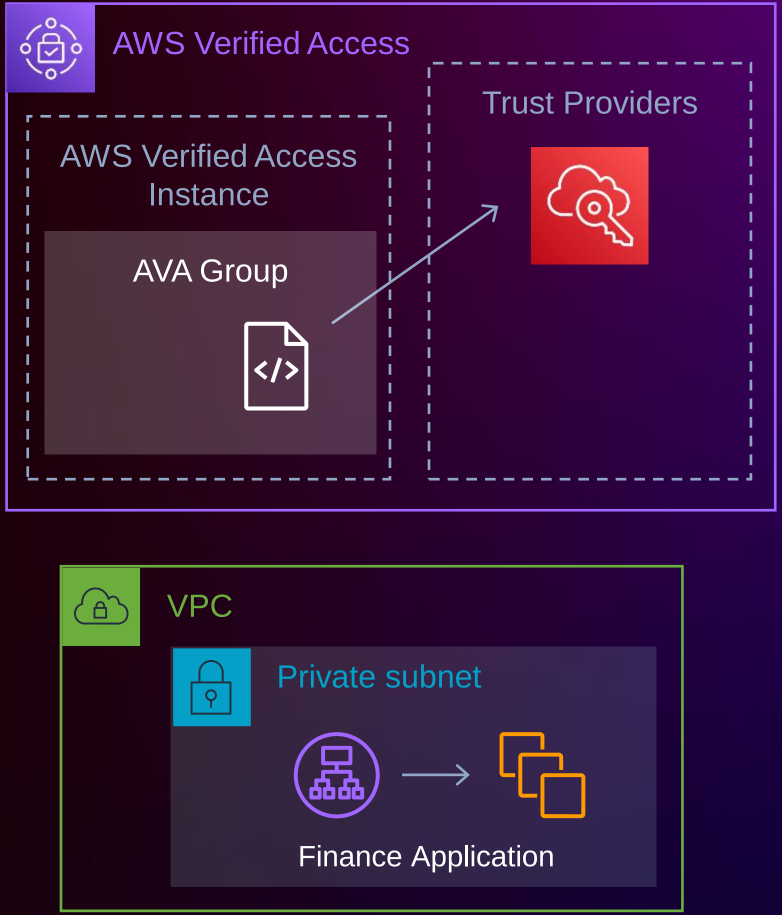
Import certificat btained outside of AWS

Import a certificate

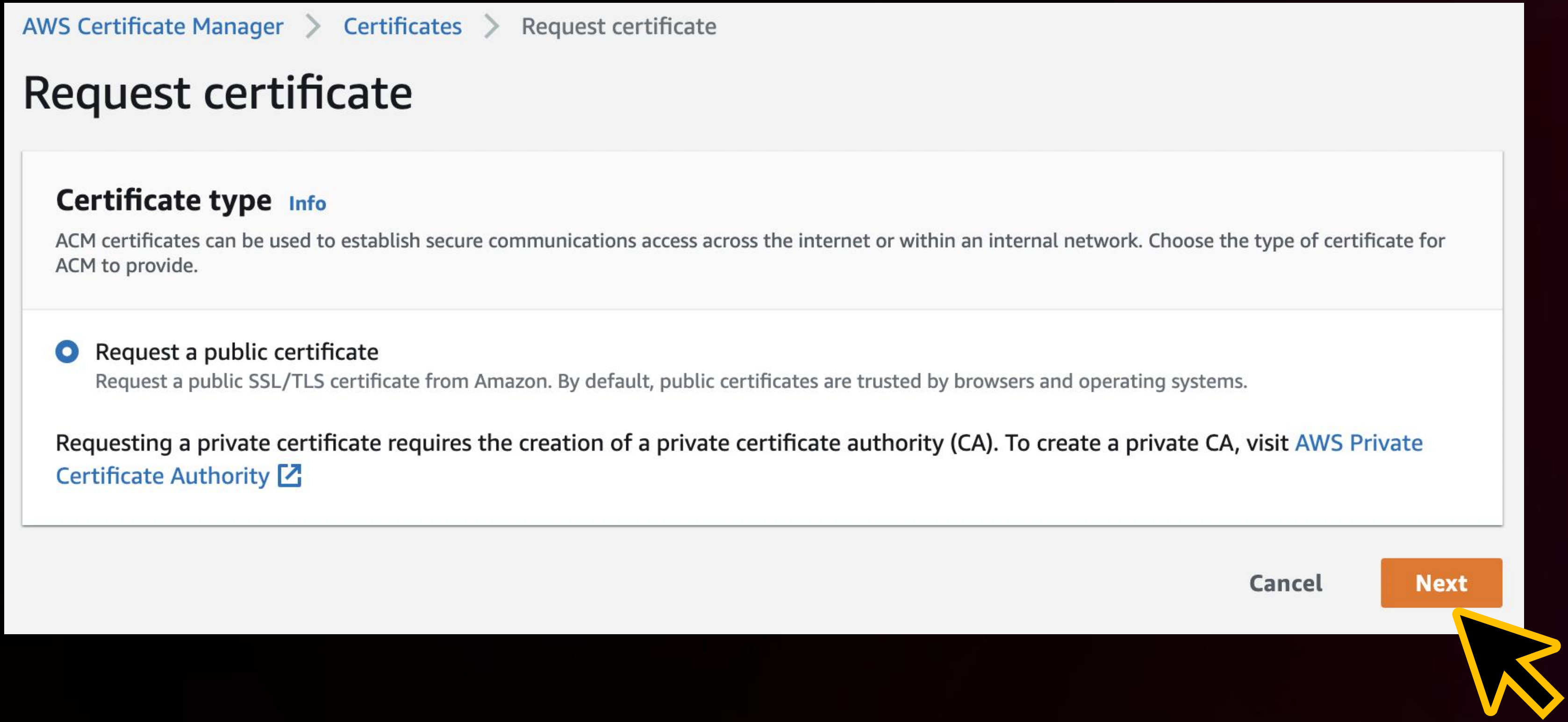
Create private certificate authority (CA) hierarchies for your organization.

Create a private CA

**Pricing (US)**



# Demo – Request endpoint domain certificate



AWS Certificate Manager > Certificates > Request certificate

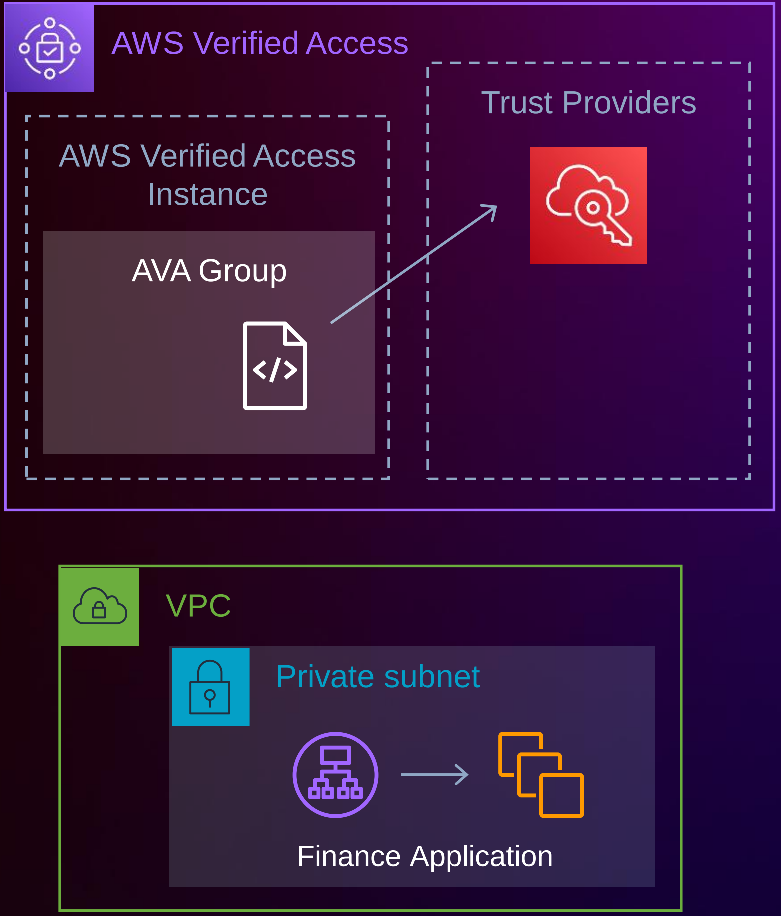
## Request certificate

### Certificate type Info

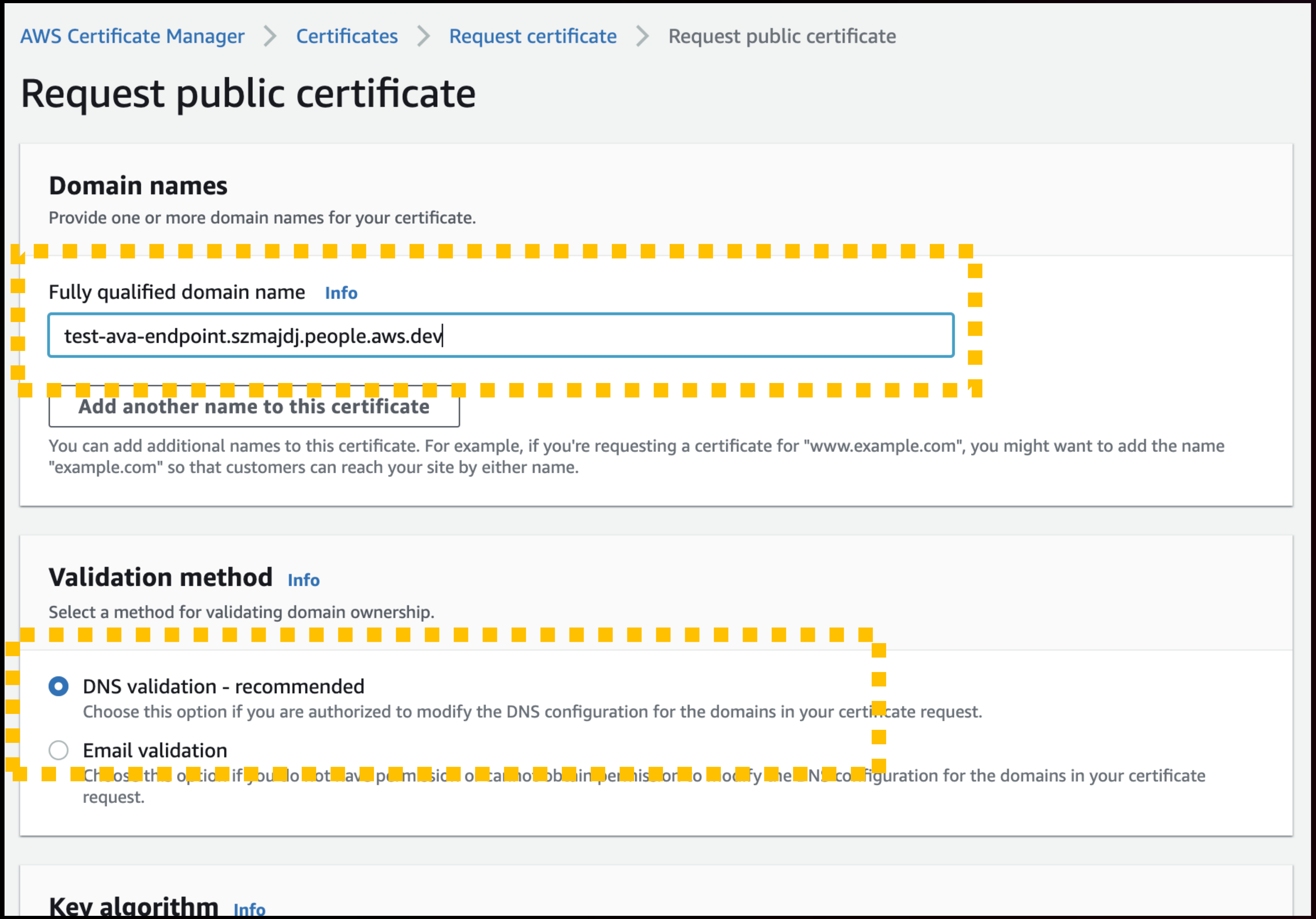
ACM certificates can be used to establish secure communications access across the internet or within an internal network. Choose the type of certificate for ACM to provide.

● Request a public certificate
Request a public SSL/TLS certificate from Amazon. By default, public certificates are trusted by browsers and operating systems.

Requesting a private certificate requires the creation of a private certificate authority (CA). To create a private CA, visit AWS Private Certificate Authority



# Demo – Request endpoint domain certificate



AWS Certificate Manager > Certificates > Request certificate > Request public certificate

## Request public certificate

### Domain names

Provide one or more domain names for your certificate.

Fully qualified domain name Info

test-ava-endpoint.szmajdj.people.aws.dev

Add another name to this certificate

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

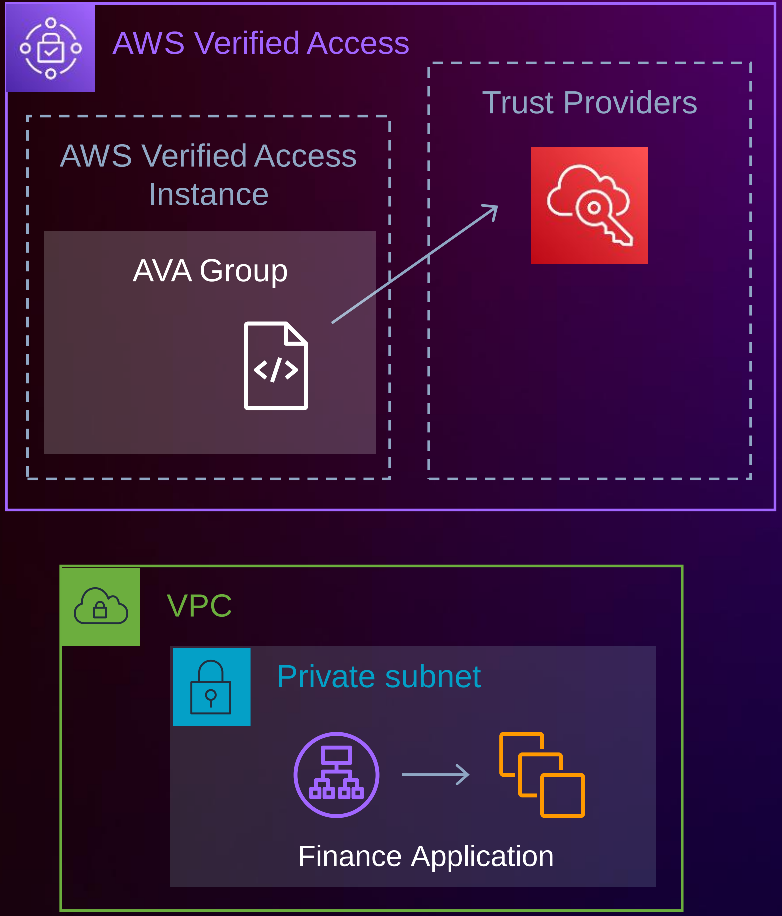
### Validation method Info

Select a method for validating domain ownership.

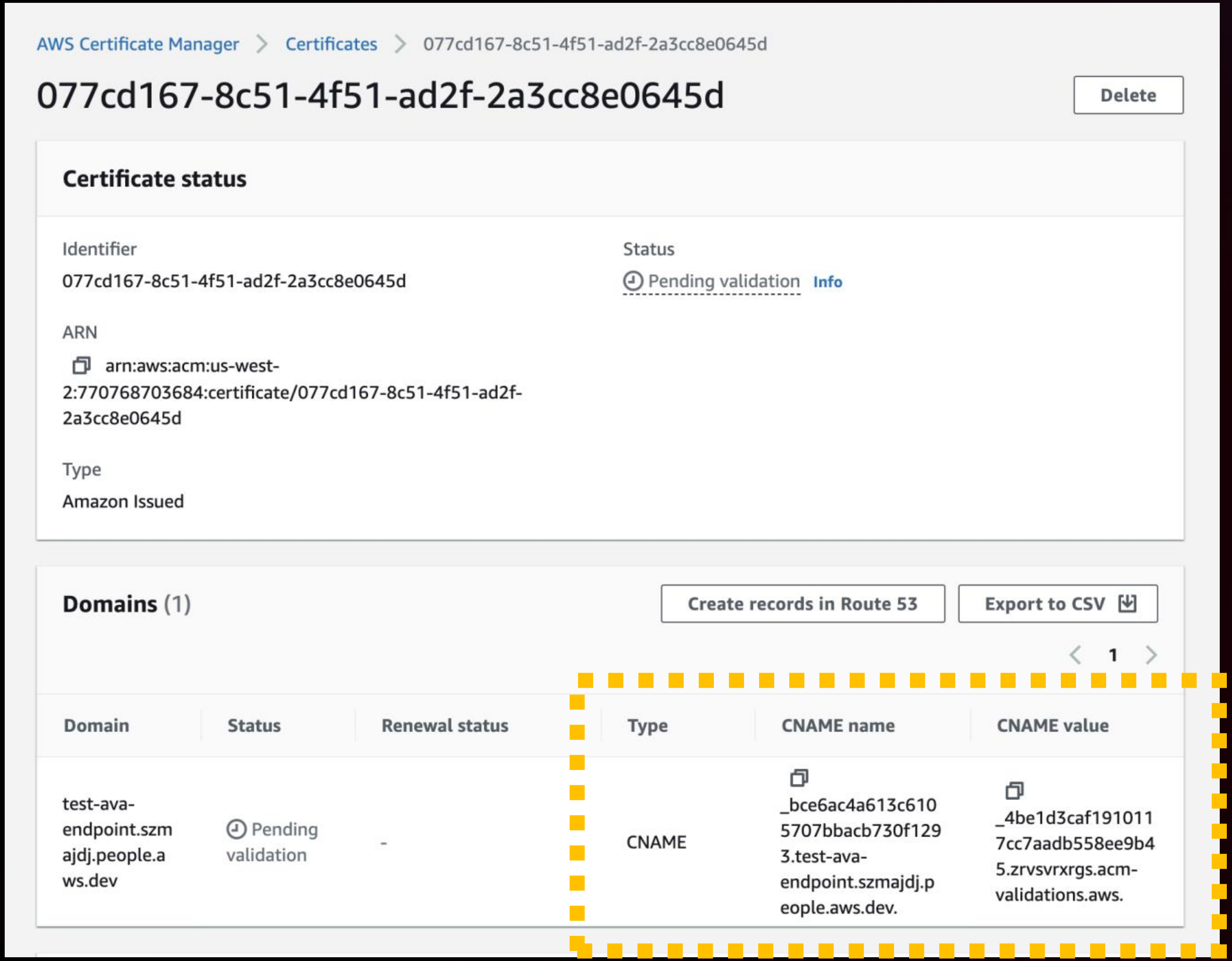
● DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

○ Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

### Key algorithm Info



# Demo – Request endpoint domain certificate



AWS Certificate Manager > Certificates > 077cd167-8c51-4f51-ad2f-2a3cc8e0645d

## 077cd167-8c51-4f51-ad2f-2a3cc8e0645d

Delete

### Certificate status

Identifier
077cd167-8c51-4f51-ad2f-2a3cc8e0645d

Status
Pending validation Info

ARN
arn:aws:acm:us-west-2:770768703684:certificate/077cd167-8c51-4f51-ad2f-2a3cc8e0645d

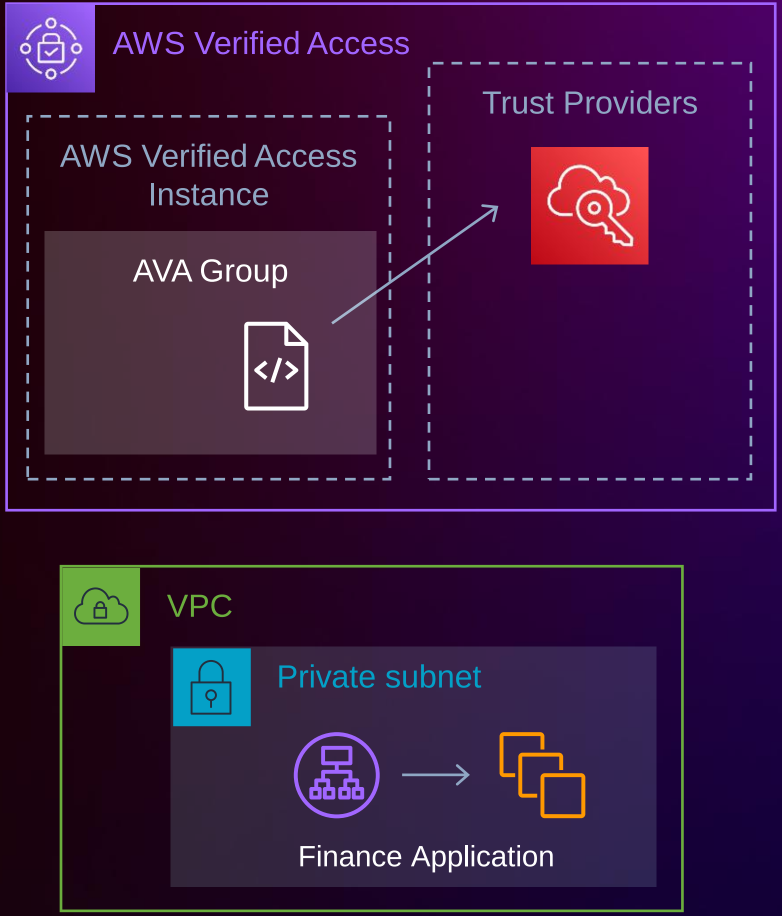
Type
Amazon Issued

### Domains (1)

Create records in Route 53 | Export to CSV

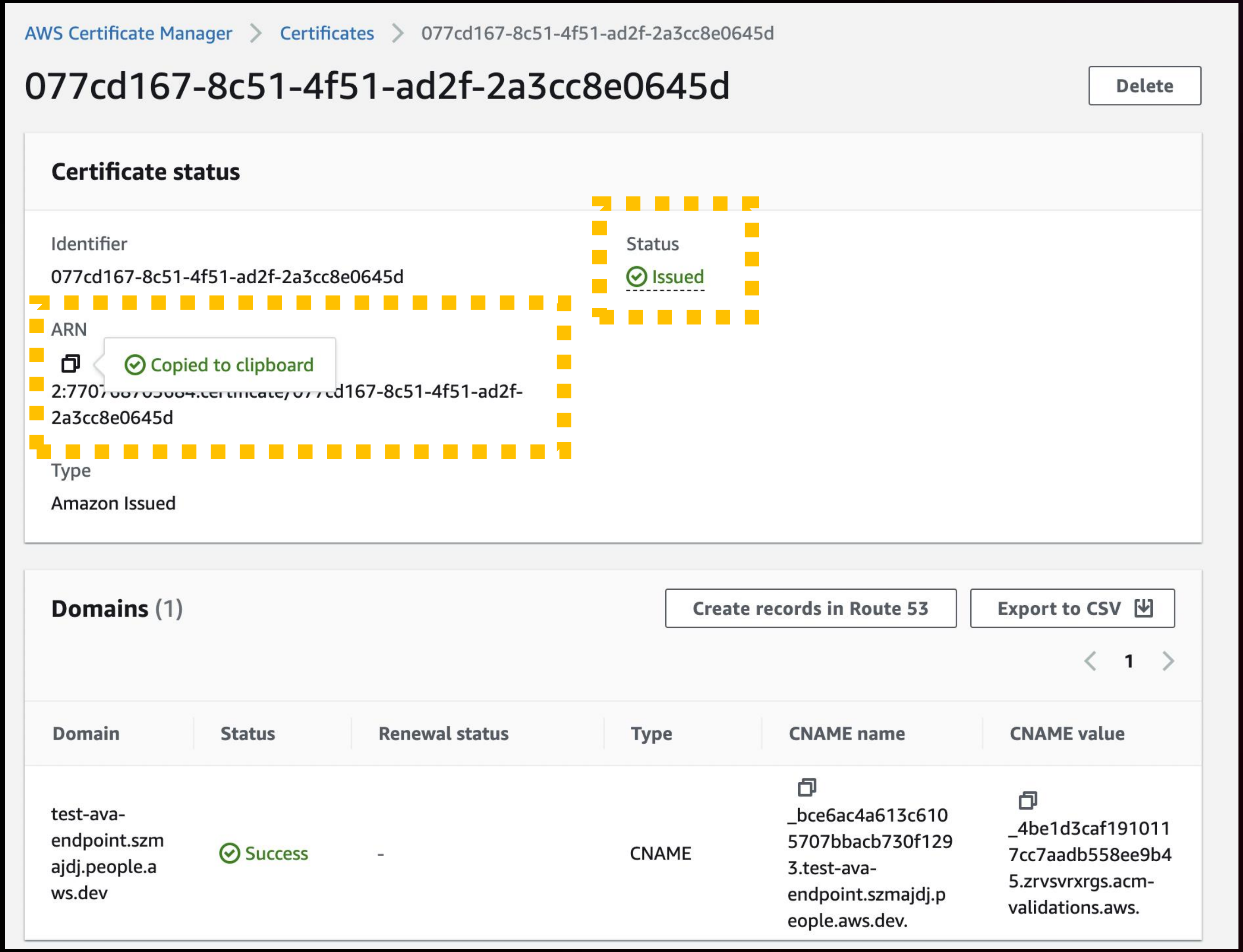
< 1 >

| Domain | Status | Renewal status | Type | CNAME name | CNAME value |
|---|---|---|---|---|---|
| test-ava-endpoint.szmajdj.people.aws.dev | Pending validation | - | CNAME | _bce6ac4a613c6105707bbacb730f1293.test-ava-endpoint.szmajdj.people.aws.dev. | _4be1d3caf1910117cc7aadb558ee9b45.zrvsvrxrgs.acm-validations.aws. |



© 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.

# Demo – Request endpoint domain certificate



AWS Certificate Manager > Certificates > 077cd167-8c51-4f51-ad2f-2a3cc8e0645d

## 077cd167-8c51-4f51-ad2f-2a3cc8e0645d

Delete

### Certificate status

Identifier
077cd167-8c51-4f51-ad2f-2a3cc8e0645d

Status
✓ Issued

ARN
Copied to clipboard
2:770768703684:certificate/077cd167-8c51-4f51-ad2f-2a3cc8e0645d

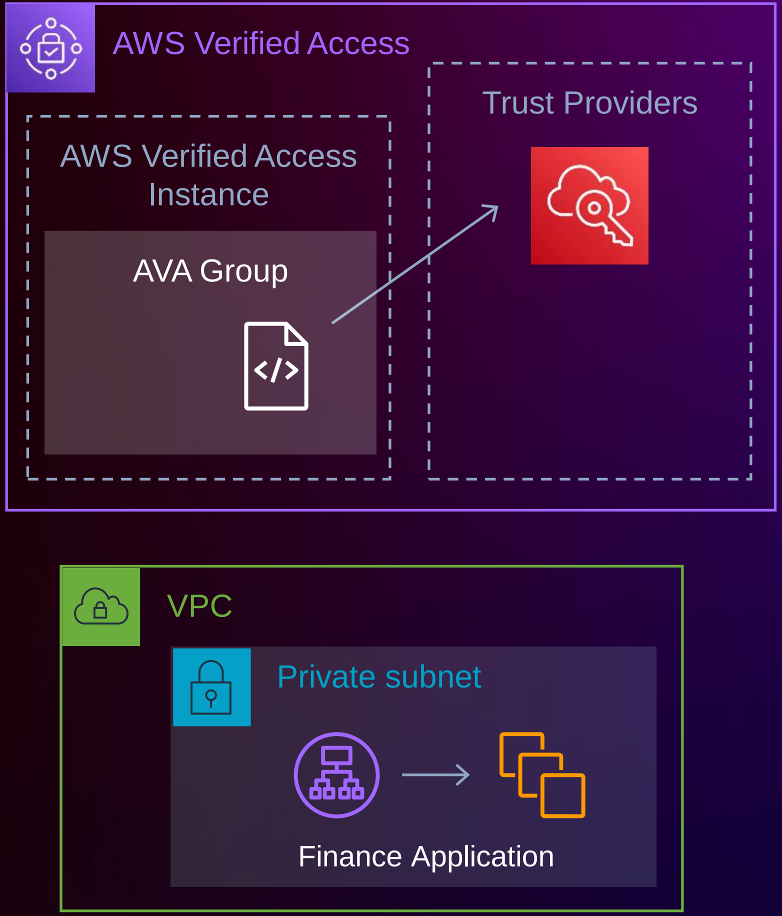
Type
Amazon Issued

### Domains (1)

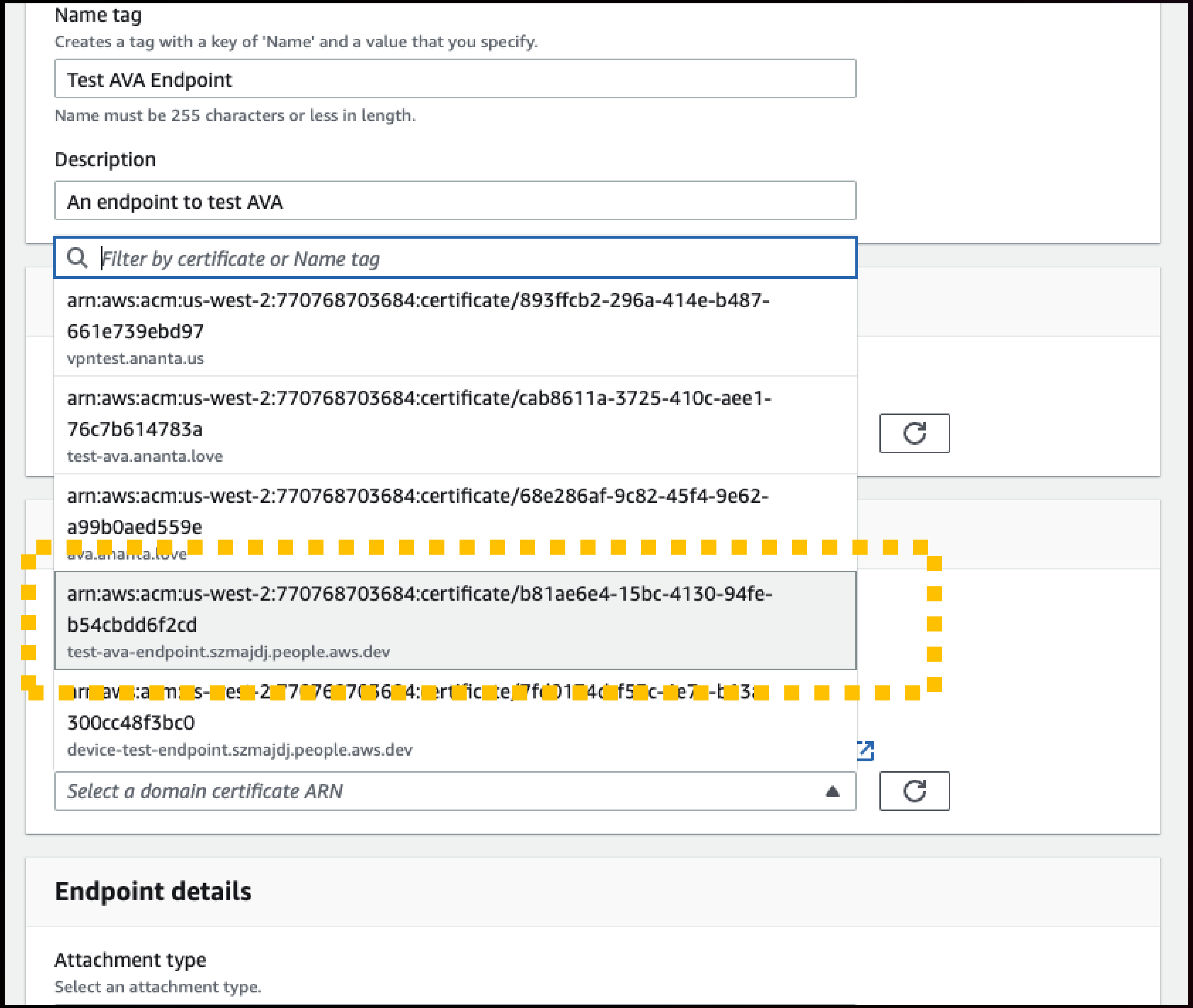
Create records in Route 53 | Export to CSV

< 1 >

| Domain | Status | Renewal status | Type | CNAME name | CNAME value |
|---|---|---|---|---|---|
| test-ava-endpoint.szmajdj.people.aws.dev | ✓ Success | - | CNAME | _bce6ac4a613c6105707bbacb730f1293.test-ava-endpoint.szmajdj.people.aws.dev. | _4be1d3caf1910117cc7aadb558ee9b45.zrvsvrxrgs.acm-validations.aws. |



# Demo – Configure endpoint domain



Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Test AVA Endpoint

Name must be 255 characters or less in length.

Description

An endpoint to test AVA

*Filter by certificate or Name tag*

arn:aws:acm:us-west-2:770768703684:certificate/893ffcb2-296a-414e-b487-661e739ebd97
vpntest.ananta.us

arn:aws:acm:us-west-2:770768703684:certificate/cab8611a-3725-410c-aee1-76c7b614783a
test-ava.ananta.love

arn:aws:acm:us-west-2:770768703684:certificate/68e286af-9c82-45f4-9e62-a99b0aed559e
ava.ananta.love

arn:aws:acm:us-west-2:770768703684:certificate/b81ae6e4-15bc-4130-94fe-b54cbdd6f2cd
test-ava-endpoint.szmajdj.people.aws.dev

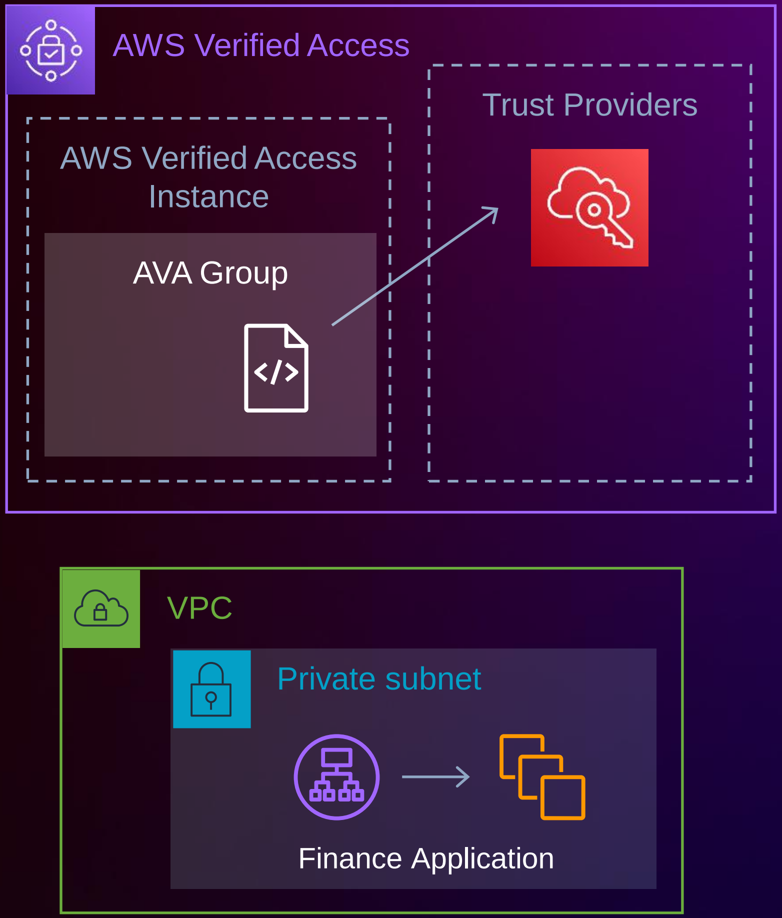
arn:aws:acm:us-west-2:770768703684:certificate/7fd01[illegible]4[illegible]f5[illegible]c-[illegible]e7[illegible]-b[illegible]3[illegible]300cc48f3bc0
device-test-endpoint.szmajdj.people.aws.dev

*Select a domain certificate ARN*

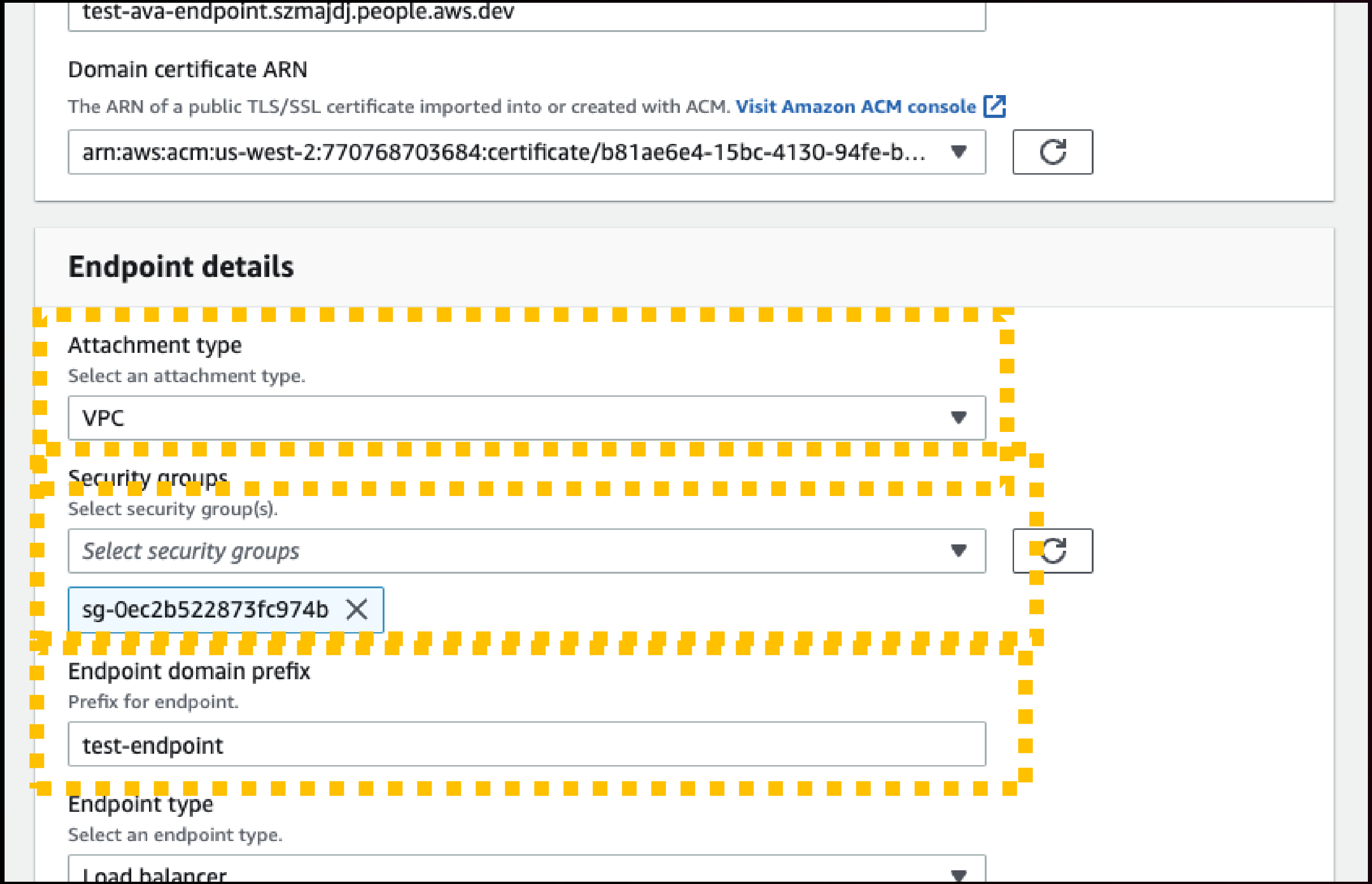
## Endpoint details

Attachment type

Select an attachment type.



# Demo – Configure endpoint details



test-ava-endpoint.szmajdj.people.aws.dev

Domain certificate ARN

The ARN of a public TLS/SSL certificate imported into or created with ACM. Visit Amazon ACM console

arn:aws:acm:us-west-2:770768703684:certificate/b81ae6e4-15bc-4130-94fe-b...

## Endpoint details

Attachment type

Select an attachment type.

VPC

Security groups

Select security group(s).

*Select security groups*

sg-0ec2b522873fc974b

Endpoint domain prefix

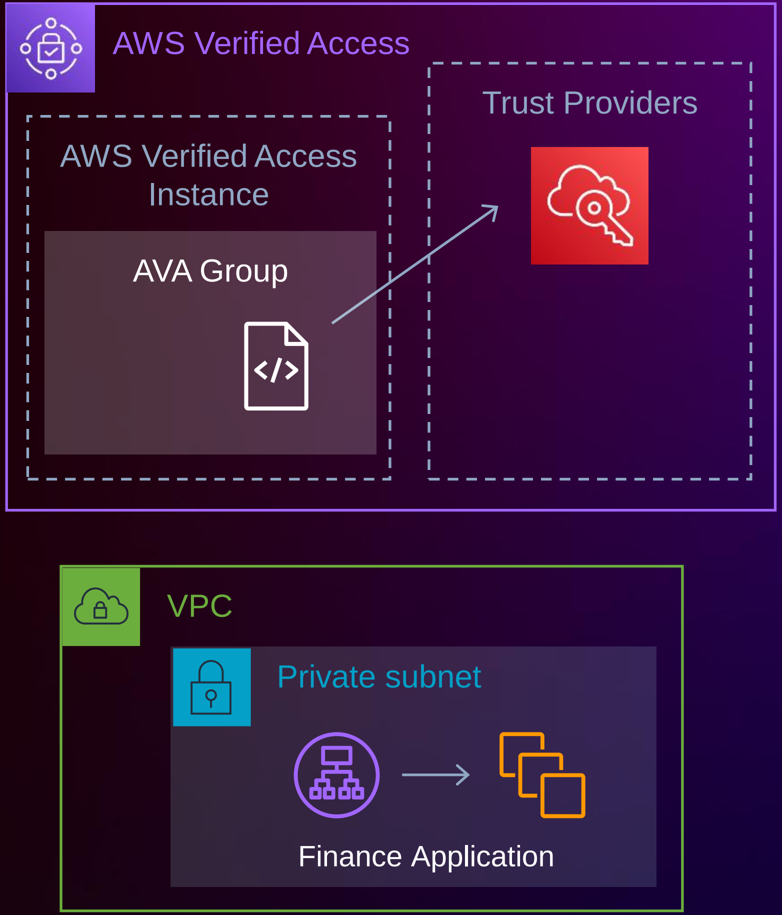
Prefix for endpoint.

test-endpoint

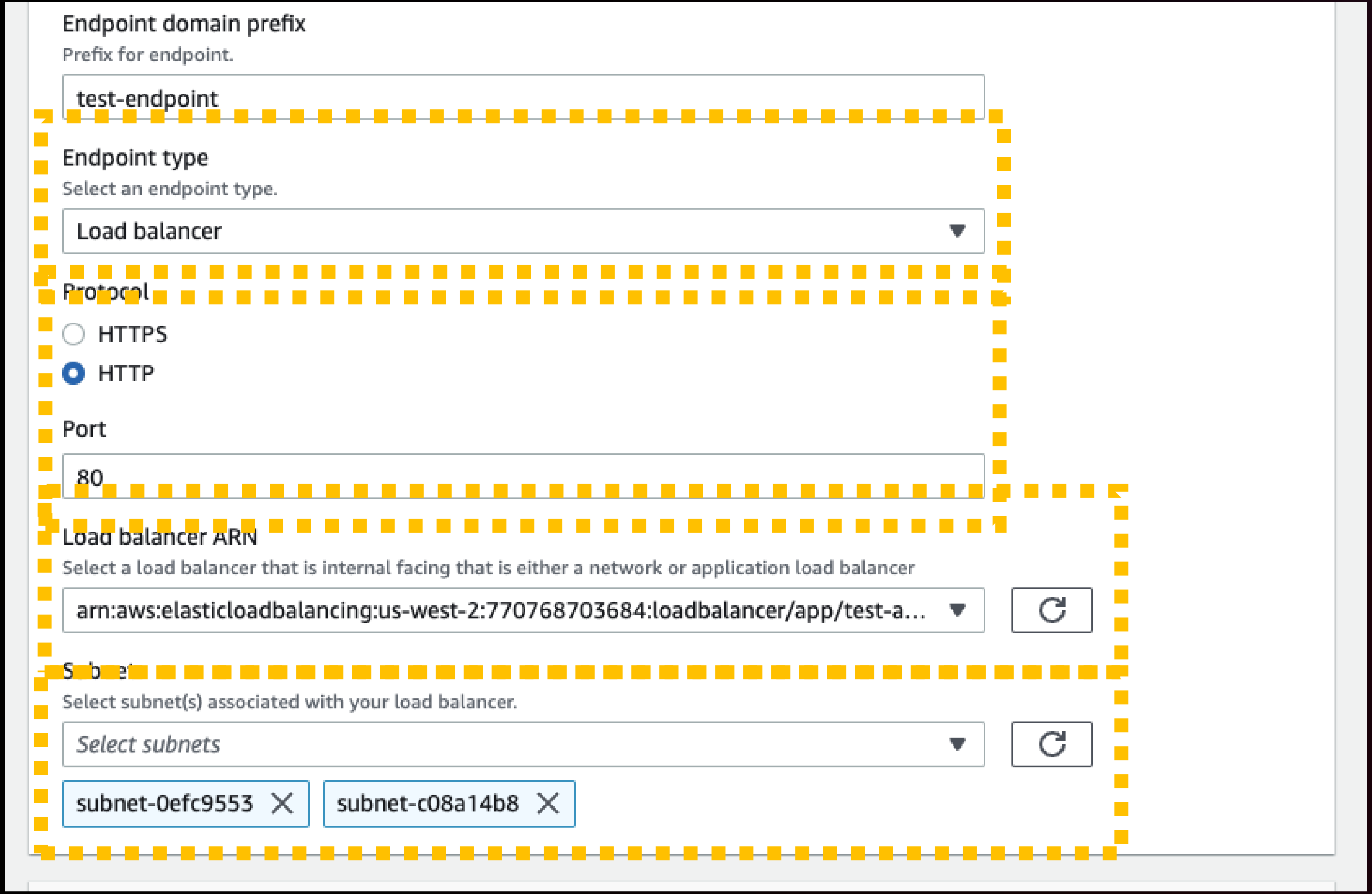
Endpoint type

Select an endpoint type.

Load balancer



# Demo – Configure endpoint details



Endpoint domain prefix
Prefix for endpoint.
test-endpoint

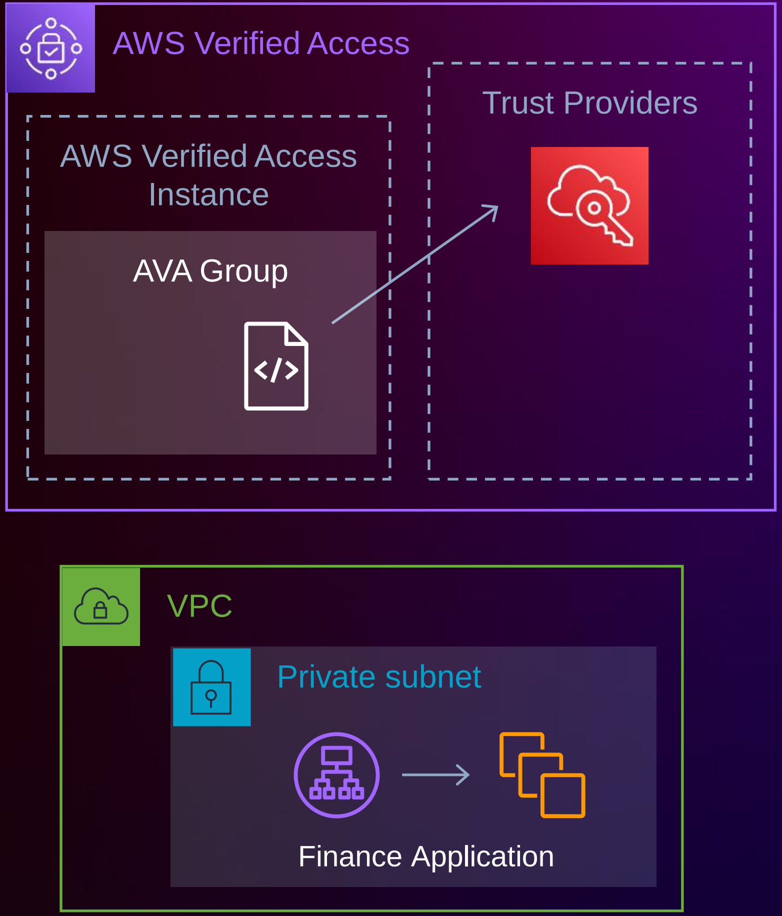
Endpoint type
Select an endpoint type.
Load balancer ▼

Protocol
○ HTTPS
● HTTP

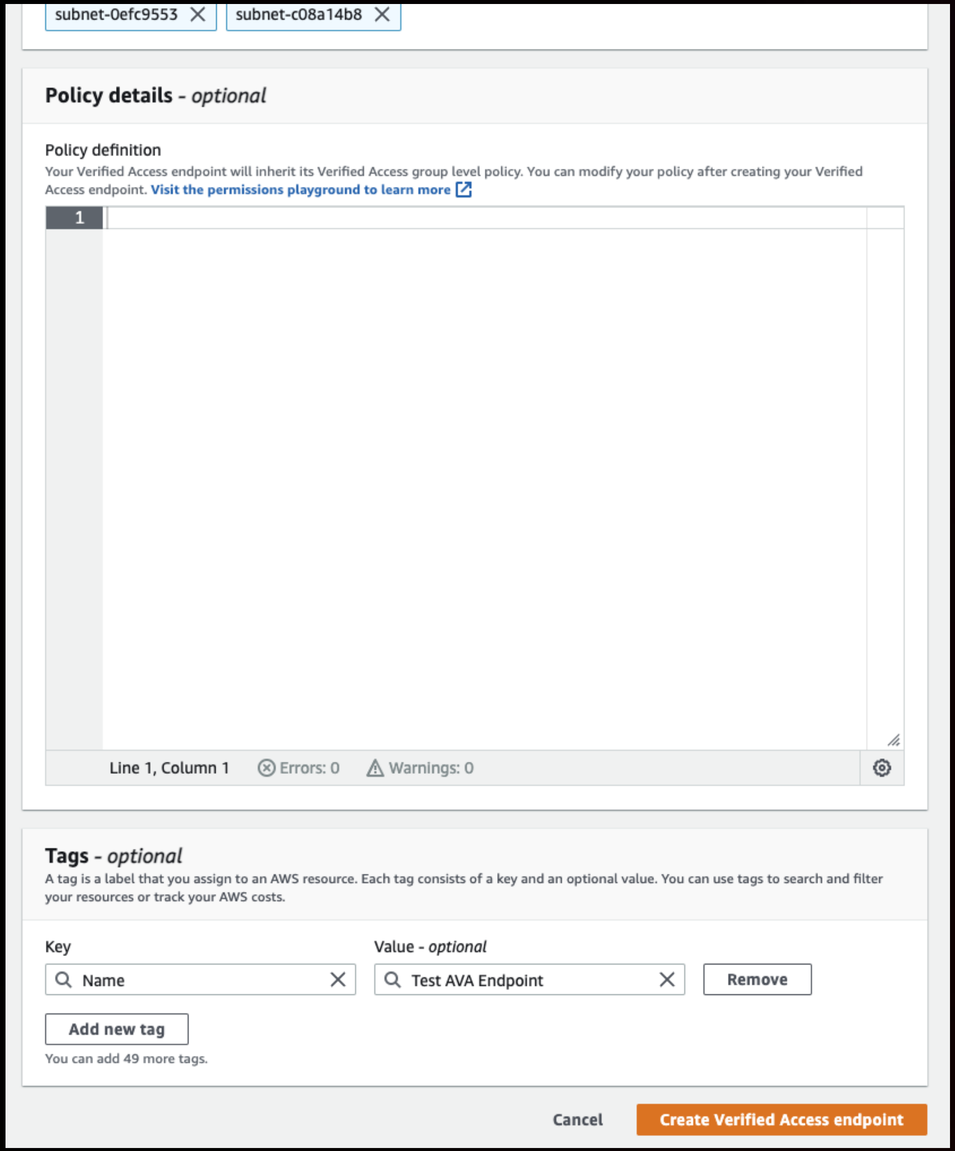
Port
80

Load balancer ARN
Select a load balancer that is internal facing that is either a network or application load balancer
arn:aws:elasticloadbalancing:us-west-2:770768703684:loadbalancer/app/test-a... ▼

Subnet
Select subnet(s) associated with your load balancer.
*Select subnets* ▼
subnet-0efc9553 ✕ subnet-c08a14b8 ✕



# Demo – Configure endpoint policy



subnet-0efc9553 ✕ subnet-c08a14b8 ✕

**Policy details** - *optional*

Policy definition

Your Verified Access endpoint will inherit its Verified Access group level policy. You can modify your policy after creating your Verified Access endpoint. Visit the permissions playground to learn more

```
1
```

Line 1, Column 1 Errors: 0 Warnings: 0

**Tags** - *optional*

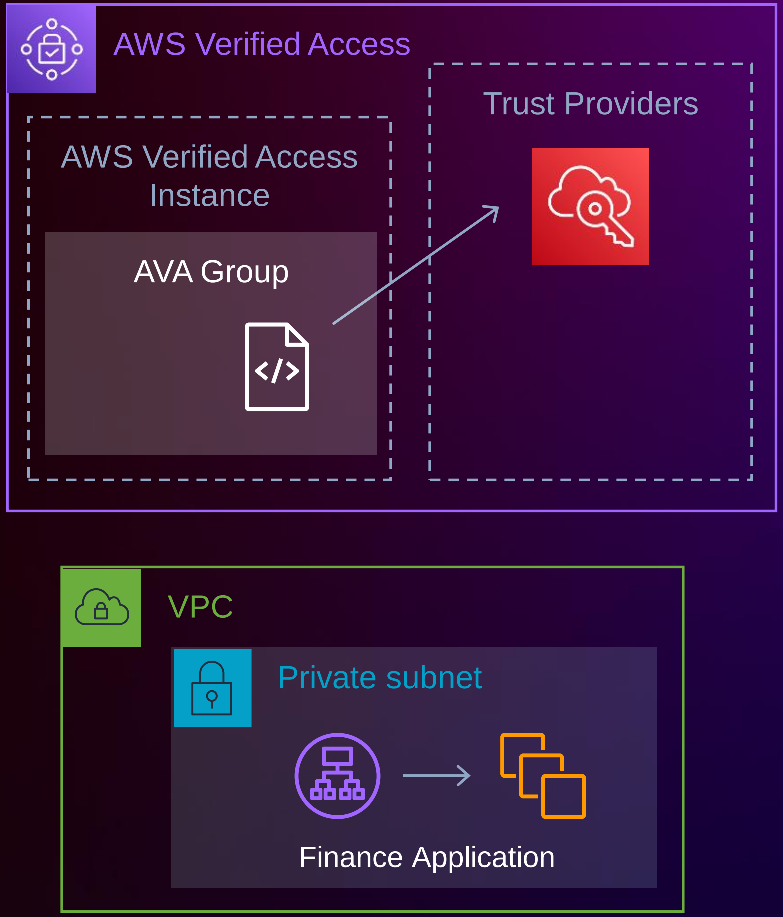
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

| Key | Value - *optional* | |
|---|---|---|
| Name | Test AVA Endpoint | Remove |

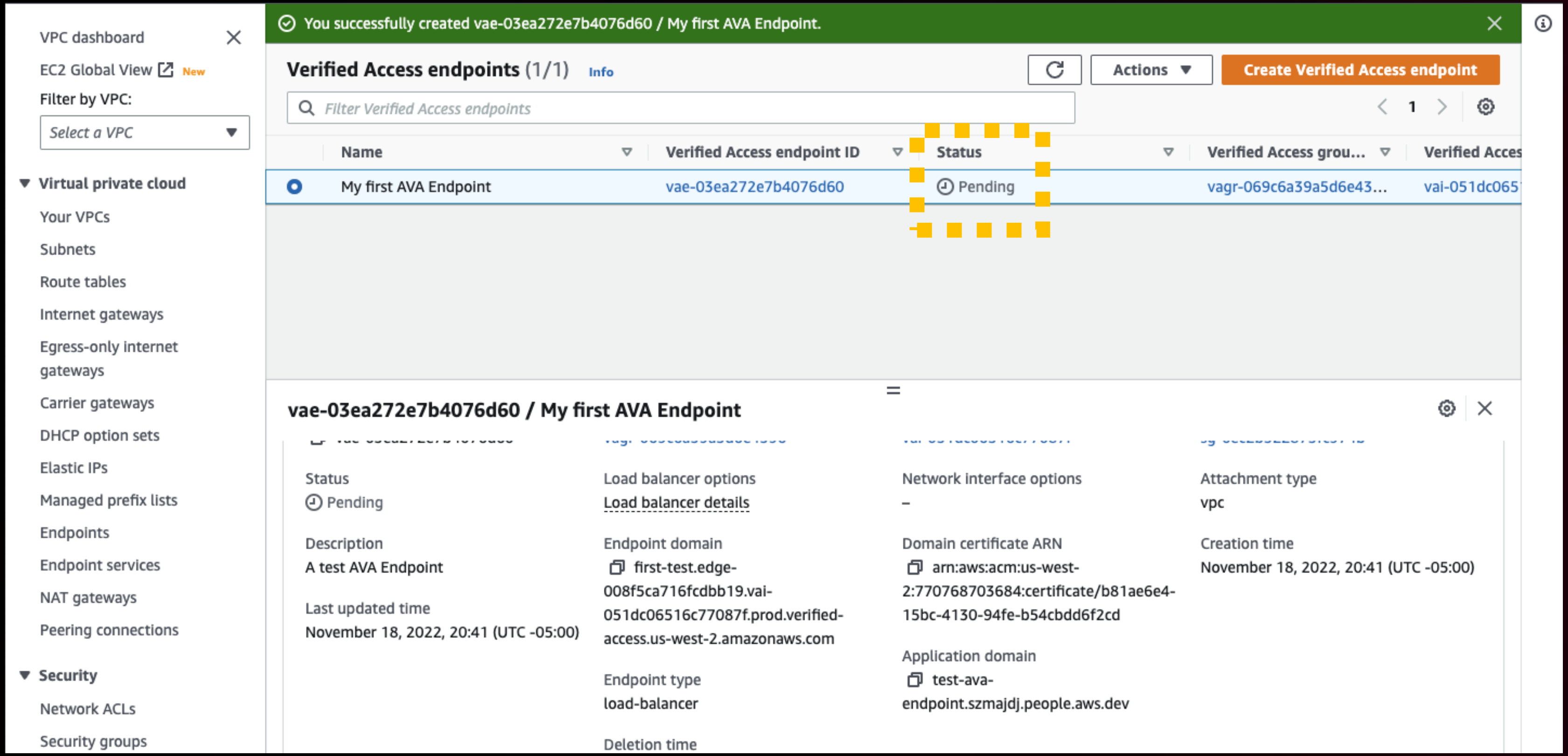
Add new tag

You can add 49 more tags.

Cancel Create Verified Access endpoint



# Demo – Create Verified Access endpoint



VPC dashboard

EC2 Global View New

Filter by VPC:

Select a VPC ▼

▼ Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections

▼ Security

- Network ACLs
- Security groups

You successfully created vae-03ea272e7b4076d60 / My first AVA Endpoint.

Verified Access endpoints (1/1) Info

Actions ▼ | Create Verified Access endpoint

Filter Verified Access endpoints

| | Name | Verified Access endpoint ID | Status | Verified Access grou... | Verified Acces |
|---|---|---|---|---|---|
| ● | My first AVA Endpoint | vae-03ea272e7b4076d60 | Pending | vagr-069c6a39a5d6e43... | vai-051dc065 |

vae-03ea272e7b4076d60 / My first AVA Endpoint

Status
Pending

Load balancer options
Load balancer details

Network interface options
–

Attachment type
vpc

Description
A test AVA Endpoint

Endpoint domain
first-test.edge-008f5ca716fcdbb19.vai-051dc06516c77087f.prod.verified-access.us-west-2.amazonaws.com

Domain certificate ARN
arn:aws:acm:us-west-2:770768703684:certificate/b81ae6e4-15bc-4130-94fe-b54cbdd6f2cd

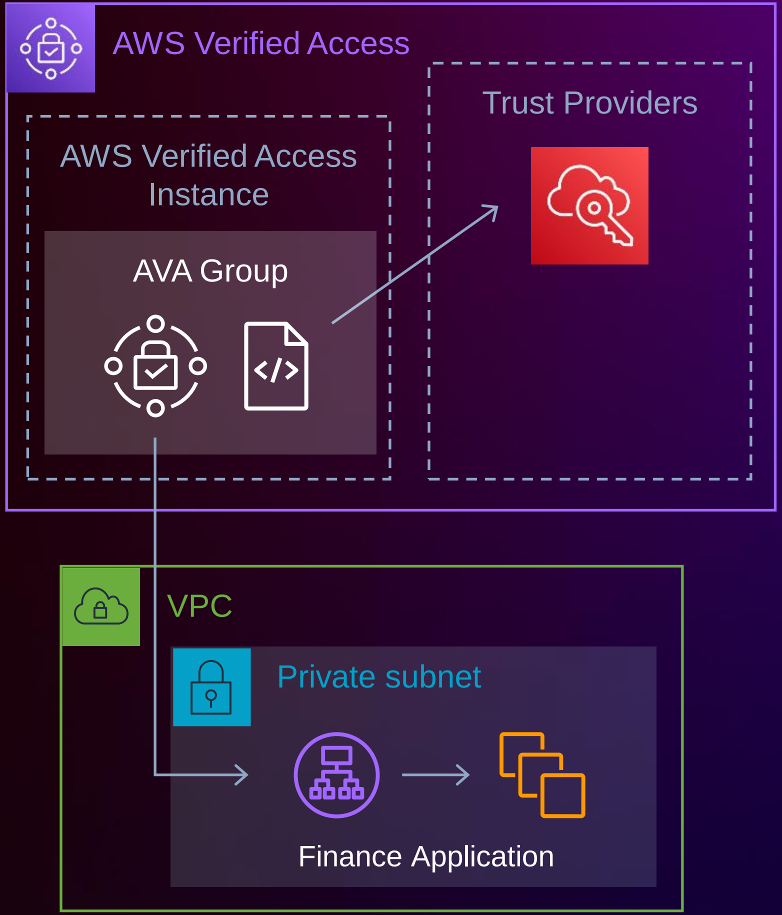
Creation time
November 18, 2022, 20:41 (UTC -05:00)

Last updated time
November 18, 2022, 20:41 (UTC -05:00)

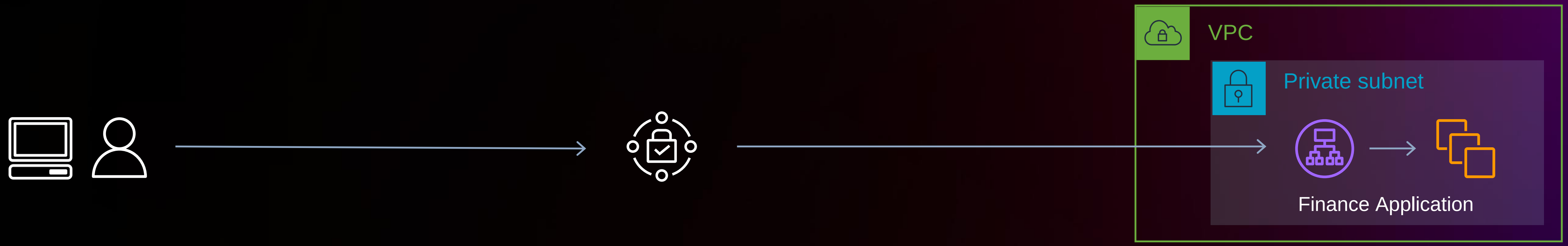
Application domain
test-ava-endpoint.szmajdj.people.aws.dev

Endpoint type
load-balancer

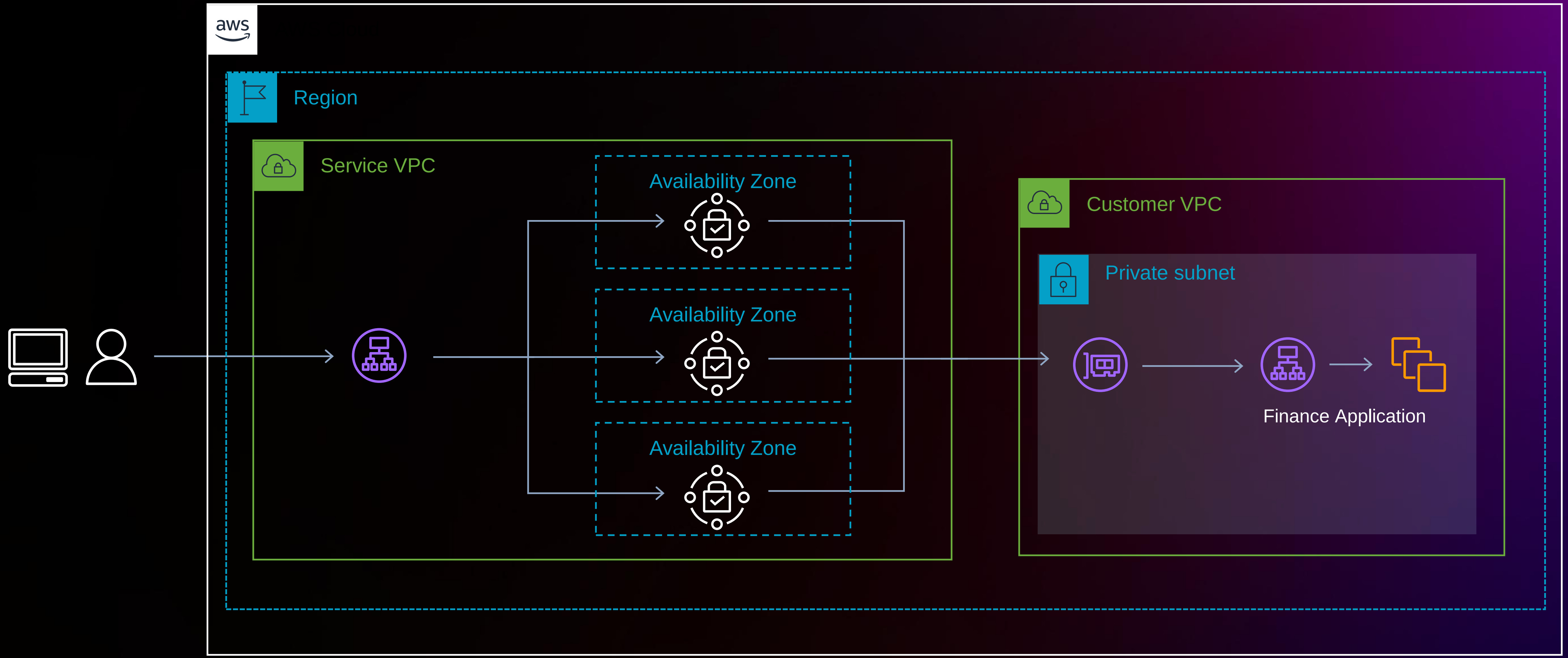
Deletion time



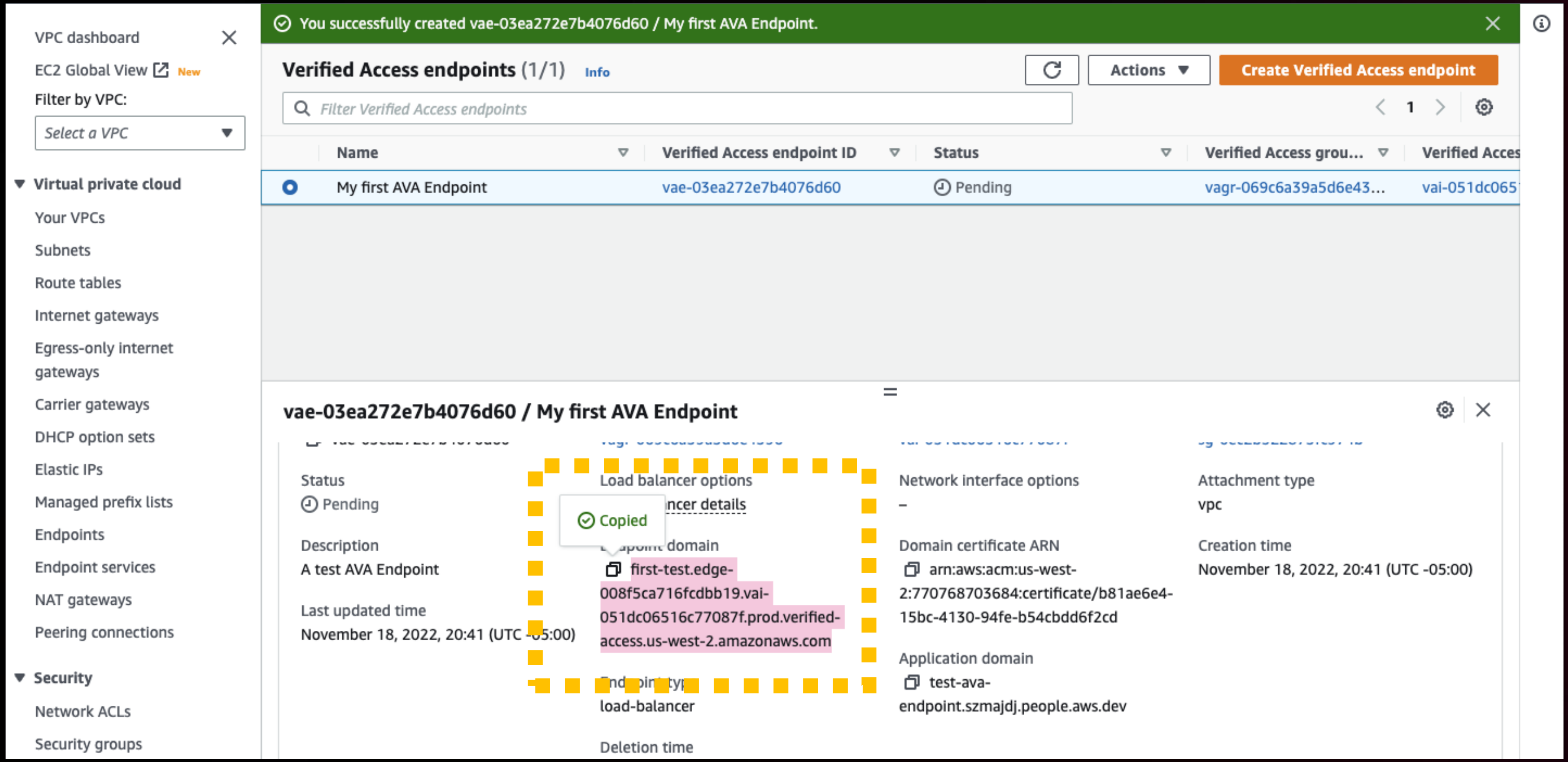
# Traffic flow



# Traffic flow



# Demo – Configure endpoint DNS



You successfully created vae-03ea272e7b4076d60 / My first AVA Endpoint.

**Verified Access endpoints** (1/1) Info

Actions
Create Verified Access endpoint
Filter Verified Access endpoints

| | Name | Verified Access endpoint ID | Status | Verified Access grou… | Verified Acces |
|---|---|---|---|---|---|
| ● | My first AVA Endpoint | vae-03ea272e7b4076d60 | Pending | vagr-069c6a39a5d6e43… | vai-051dc065 |

**vae-03ea272e7b4076d60 / My first AVA Endpoint**

Status
Pending

Description
A test AVA Endpoint

Last updated time
November 18, 2022, 20:41 (UTC -05:00)

Load balancer options
…ncer details

Copied

…domain
first-test.edge-008f5ca716fcdbb19.vai-051dc06516c77087f.prod.verified-access.us-west-2.amazonaws.com

End…typ…
load-balancer

Deletion time

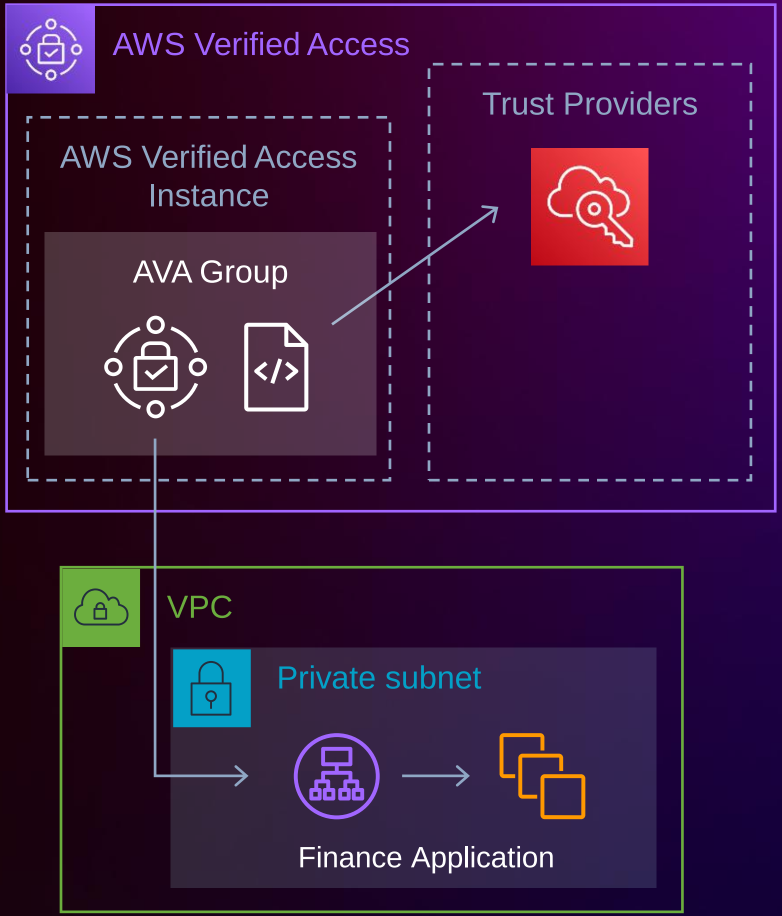
Network interface options
–

Domain certificate ARN
arn:aws:acm:us-west-2:770768703684:certificate/b81ae6e4-15bc-4130-94fe-b54cbdd6f2cd

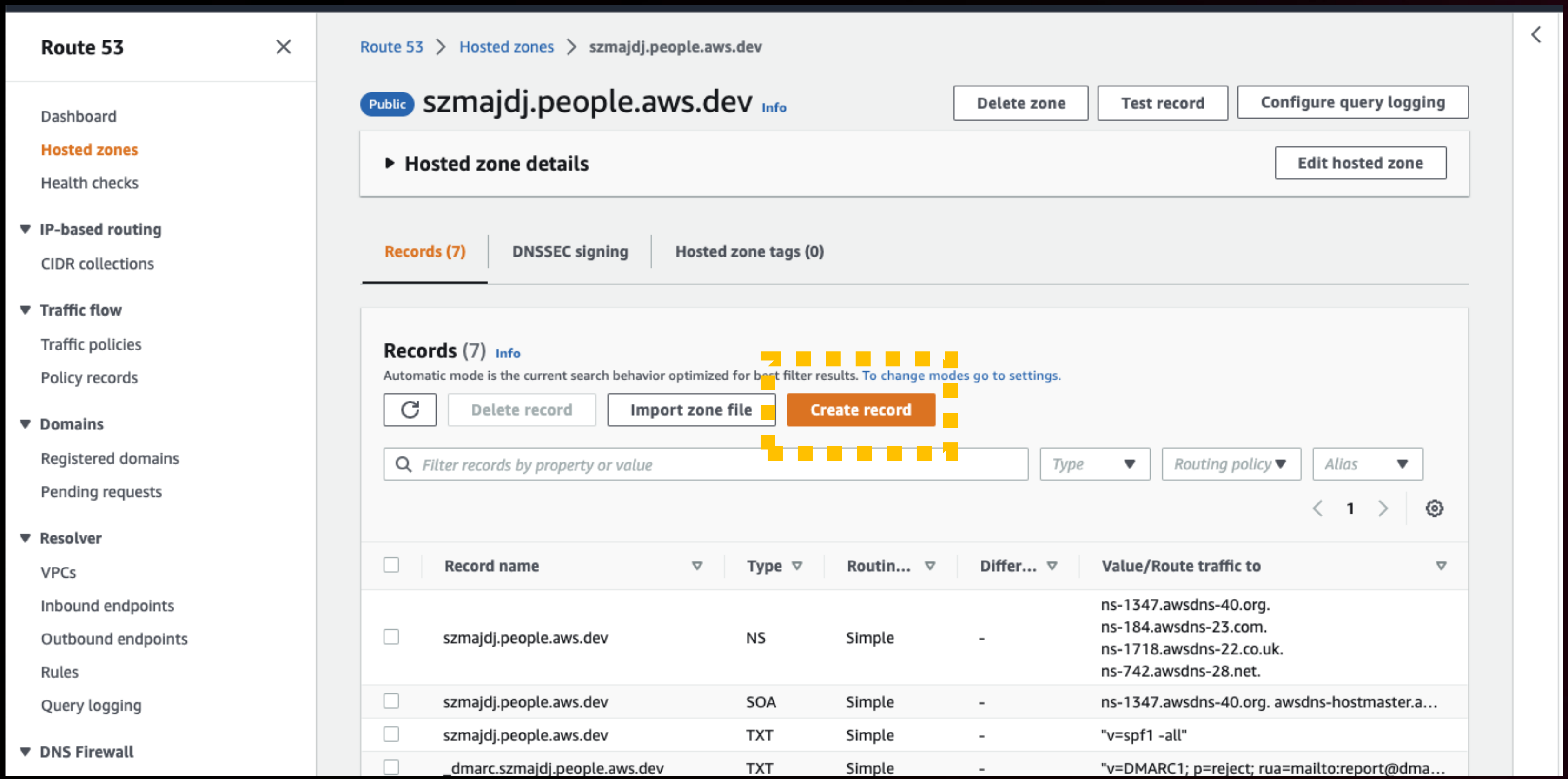
Application domain
test-ava-endpoint.szmajdj.people.aws.dev

Attachment type
vpc

Creation time
November 18, 2022, 20:41 (UTC -05:00)



# Demo – Configure endpoint DNS

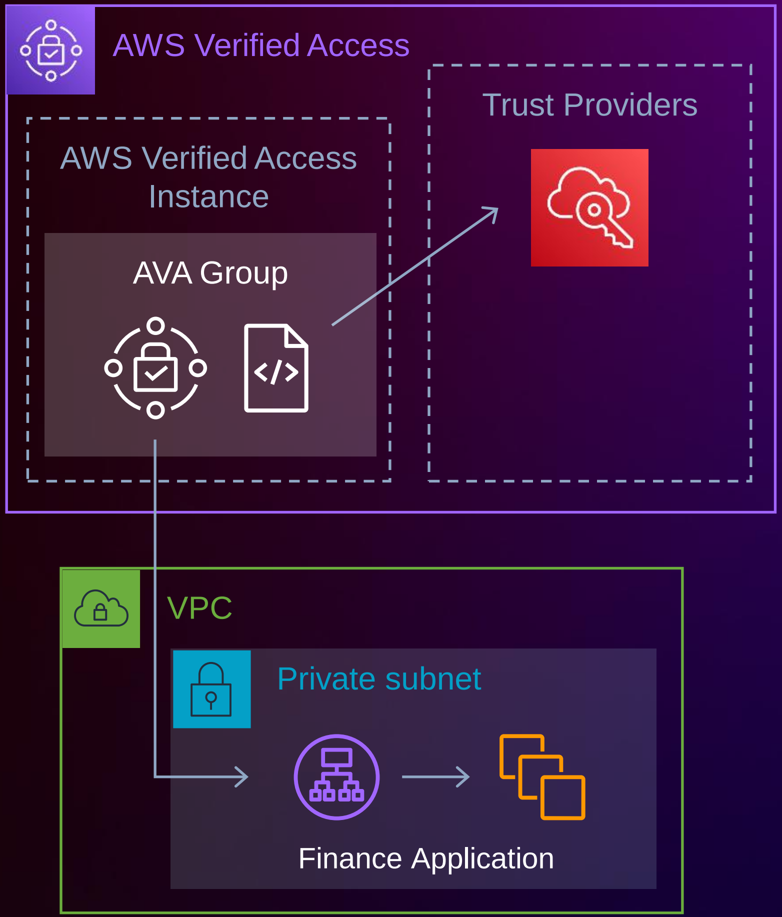


szmajdj.people.aws.dev

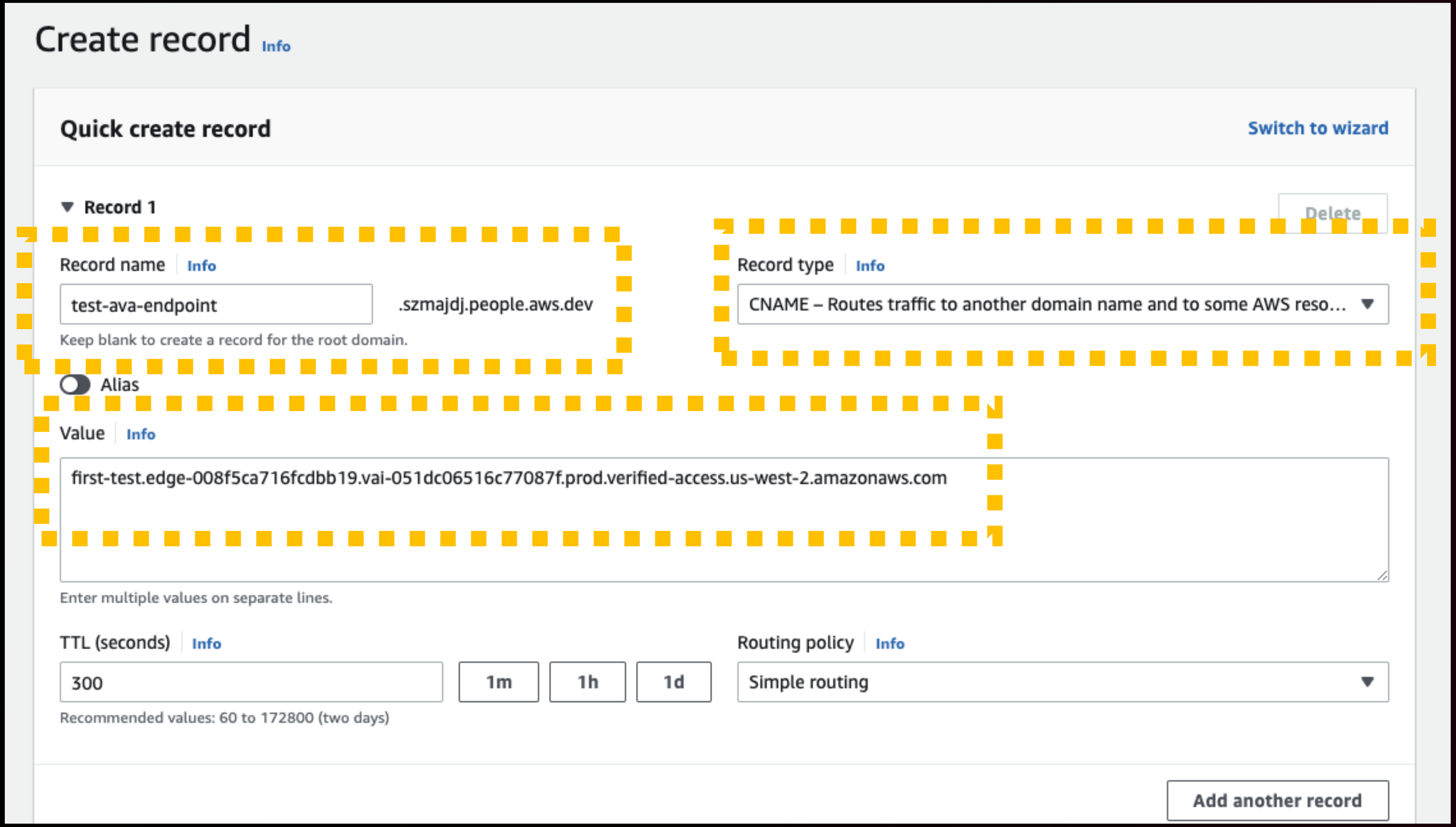
Records (7)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

| ☐ | Record name | Type | Routin... | Differ... | Value/Route traffic to |
|---|---|---|---|---|---|
| ☐ | szmajdj.people.aws.dev | NS | Simple | - | ns-1347.awsdns-40.org.<br>ns-184.awsdns-23.com.<br>ns-1718.awsdns-22.co.uk.<br>ns-742.awsdns-28.net. |
| ☐ | szmajdj.people.aws.dev | SOA | Simple | - | ns-1347.awsdns-40.org. awsdns-hostmaster.a... |
| ☐ | szmajdj.people.aws.dev | TXT | Simple | - | "v=spf1 -all" |
| ☐ | _dmarc.szmajdj.people.aws.dev | TXT | Simple | - | "v=DMARC1; p=reject; rua=mailto:report@dma... |



# Demo – Configure endpoint DNS



Create record Info

Quick create record

▼ Record 1

Record name Info

test-ava-endpoint .szmajdj.people.aws.dev

Keep blank to create a record for the root domain.

○ Alias

Record type Info

CNAME – Routes traffic to another domain name and to some AWS reso... ▼

Value Info

first-test.edge-008f5ca716fcdbb19.vai-051dc06516c77087f.prod.verified-access.us-west-2.amazonaws.com

Enter multiple values on separate lines.

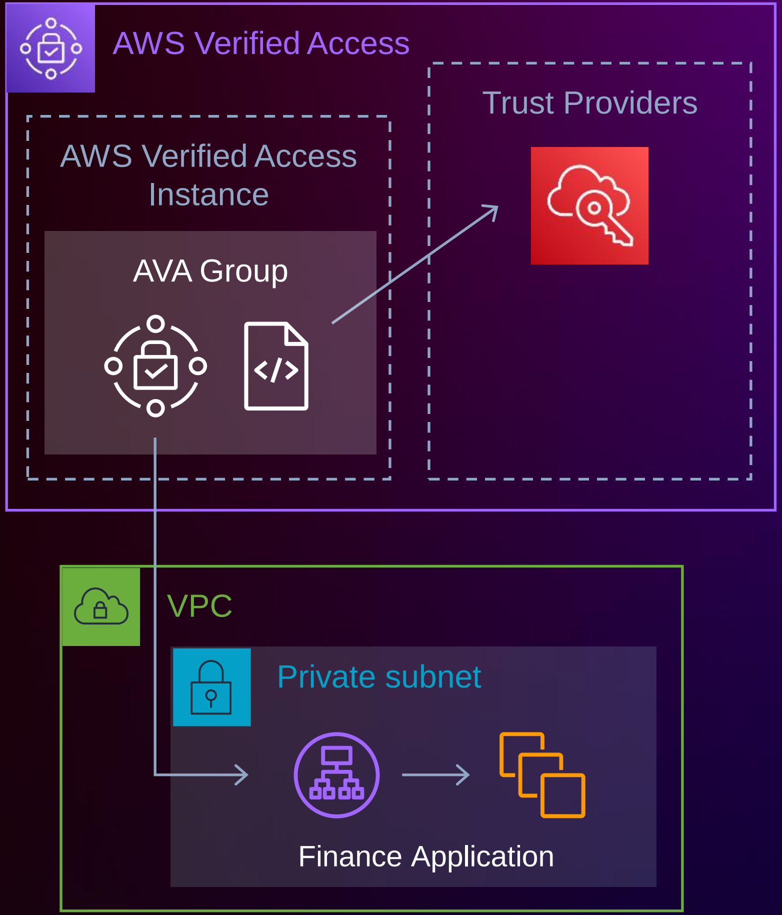
TTL (seconds) Info

300

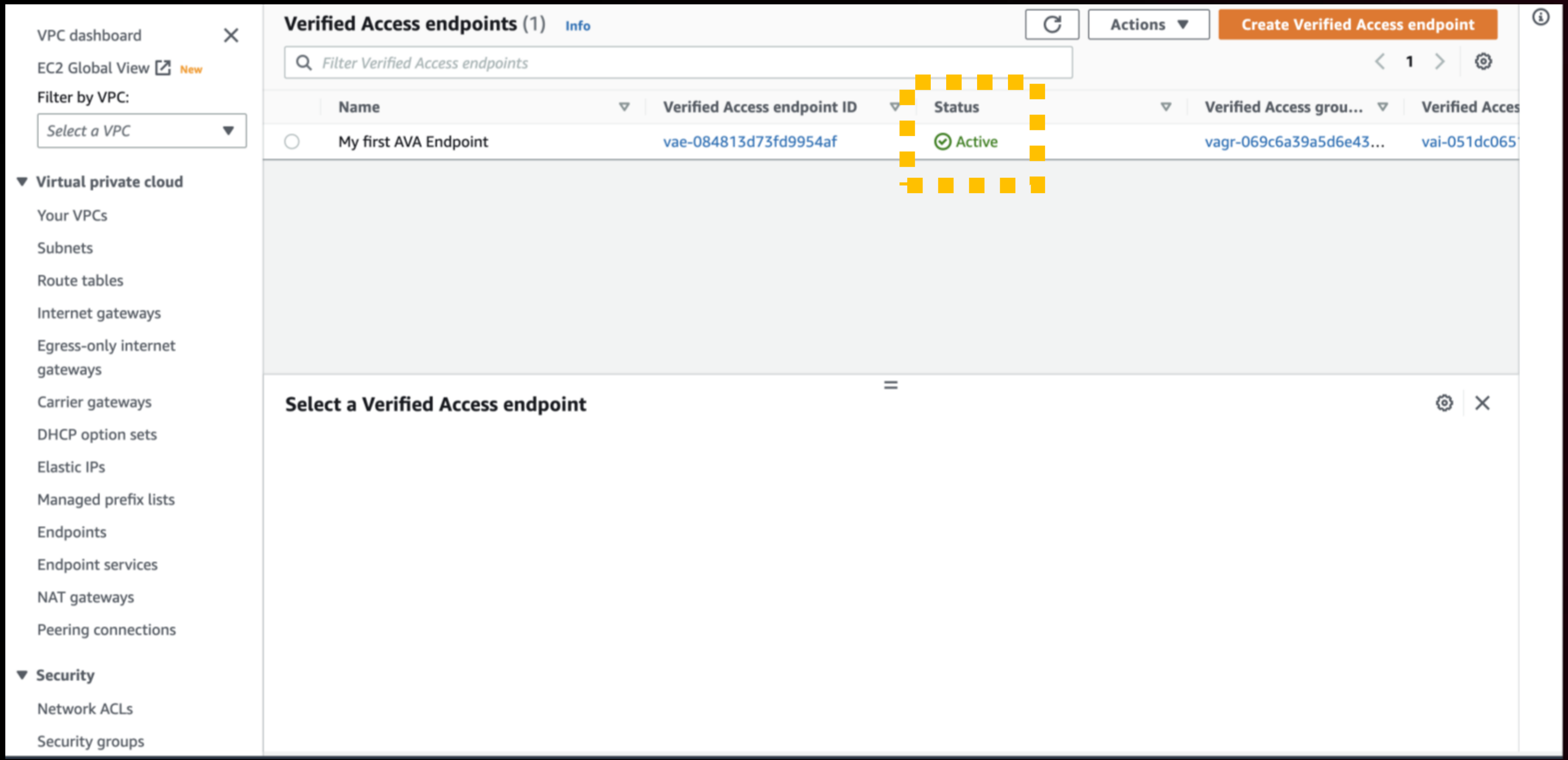
Recommended values: 60 to 172800 (two days)

Routing policy Info

Simple routing ▼



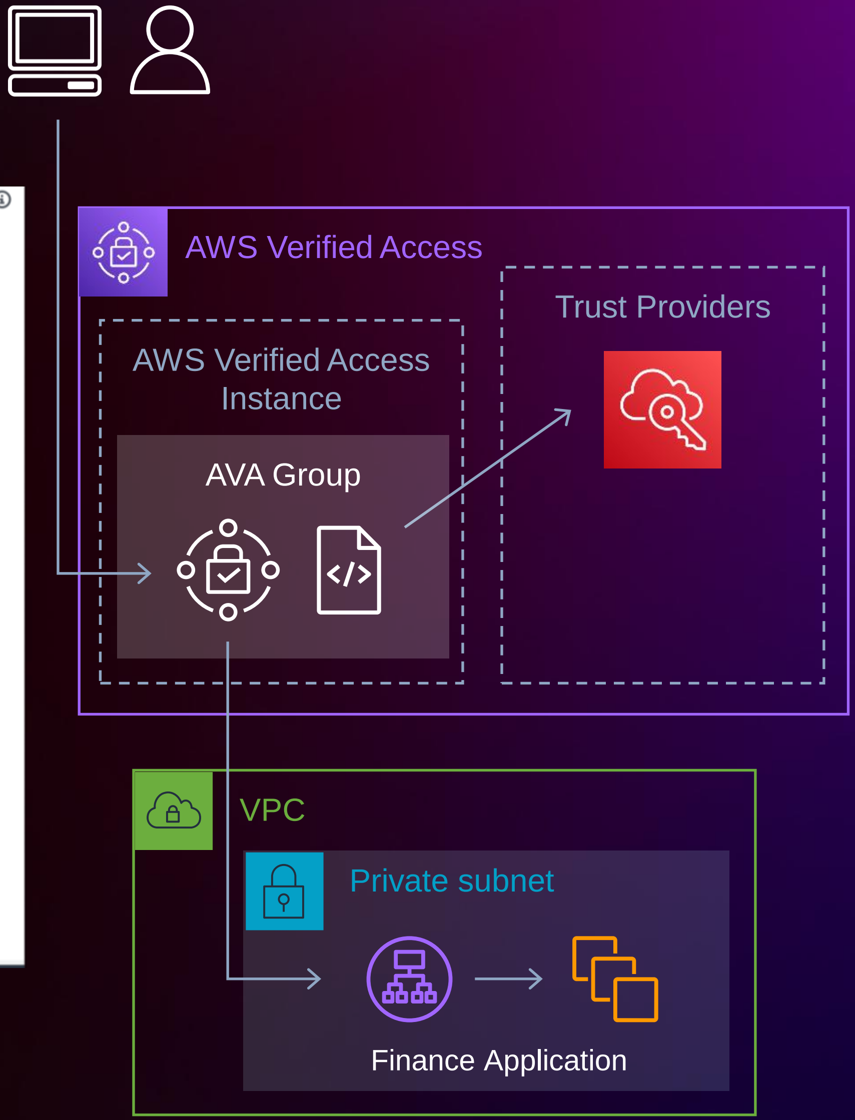
# Demo – Access private application



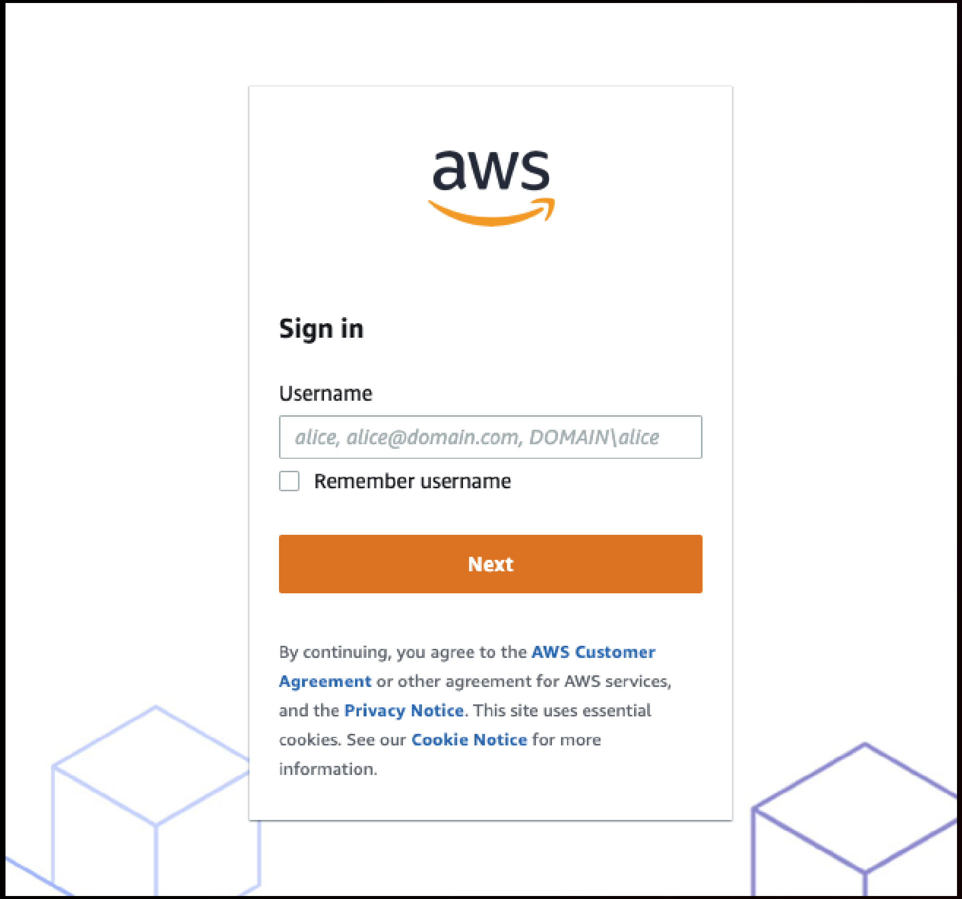
Verified Access endpoints (1)

| Name | Verified Access endpoint ID | Status | Verified Access grou... | Verified Acces |
|---|---|---|---|---|
| ○ My first AVA Endpoint | vae-084813d73fd9954af | ✓ Active | vagr-069c6a39a5d6e43... | vai-051dc065 |

Select a Verified Access endpoint



# Demo – Access private application



## Sign in

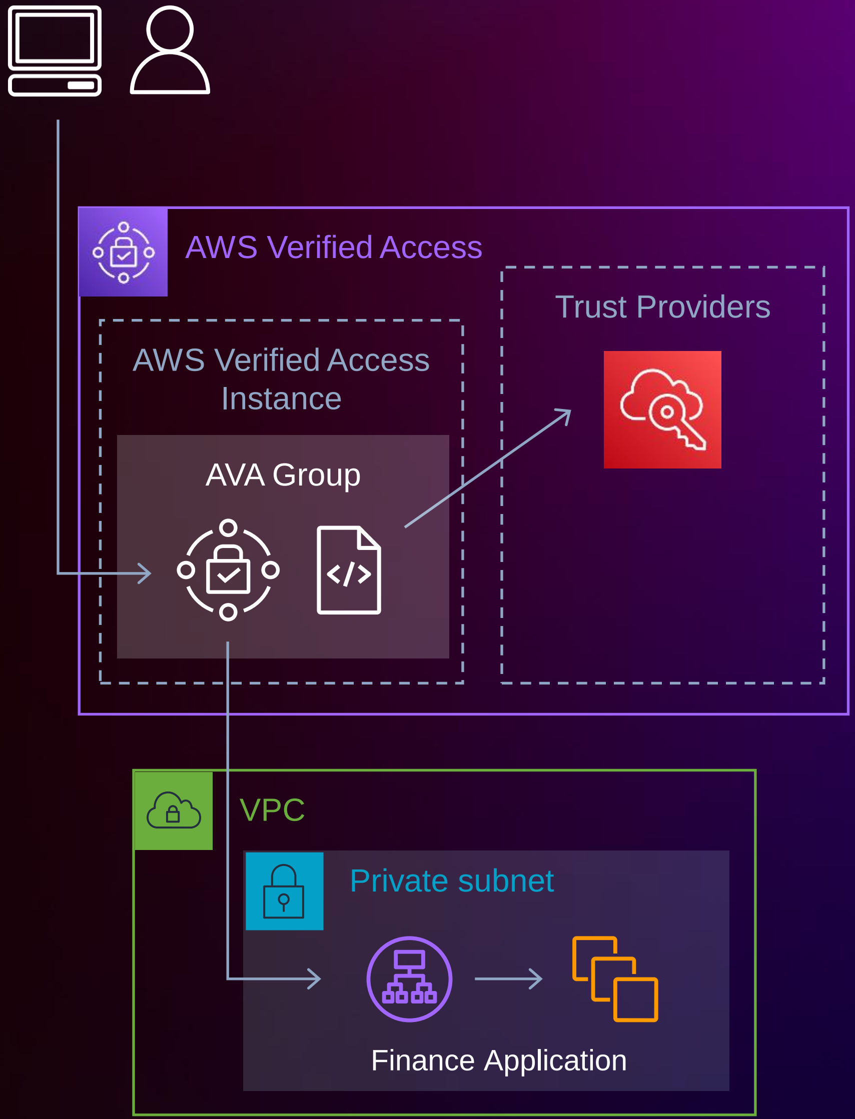
Username

alice, alice@domain.com, DOMAIN\alice

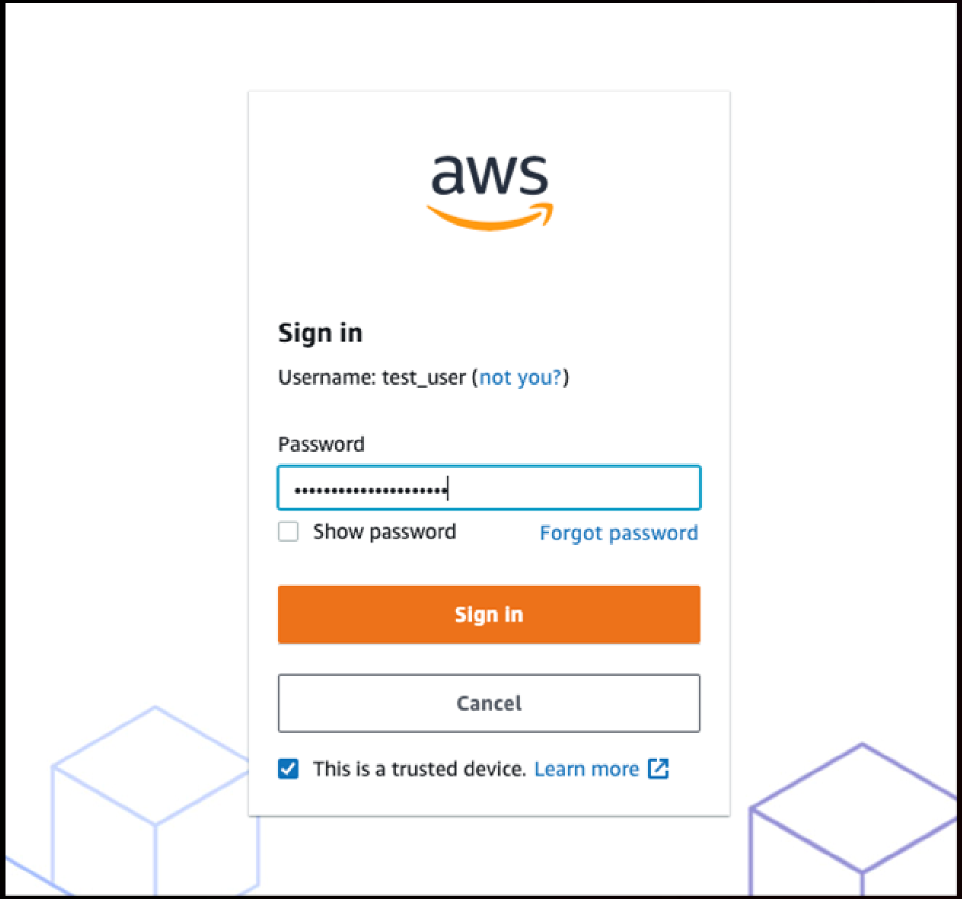
□ Remember username

Next

By continuing, you agree to the **AWS Customer Agreement** or other agreement for AWS services, and the **Privacy Notice**. This site uses essential cookies. See our **Cookie Notice** for more information.



# Demo – Access private application



Sign in

Username: test_user (not you?)

Password

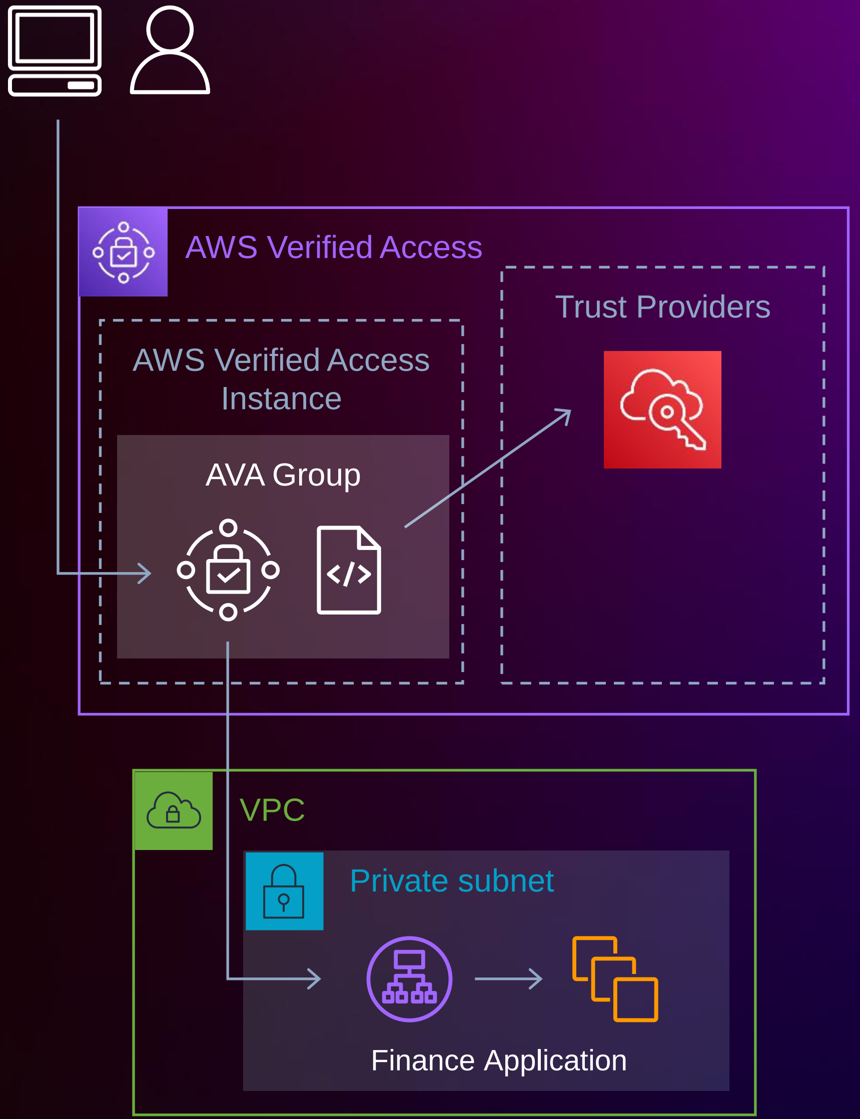
••••••••••••••••••••••

☐ Show password　Forgot password

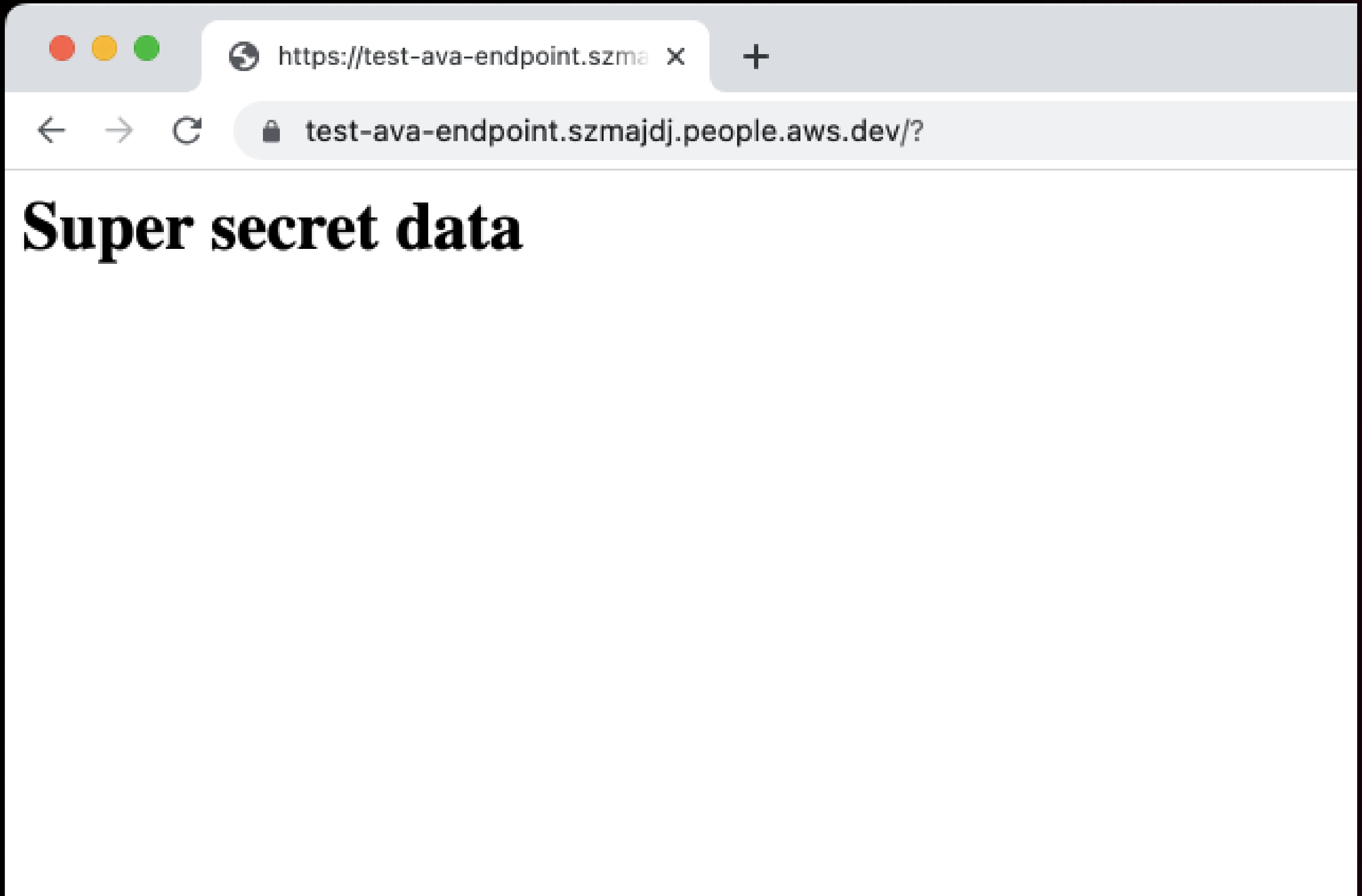
Sign in

Cancel

☑ This is a trusted device. Learn more

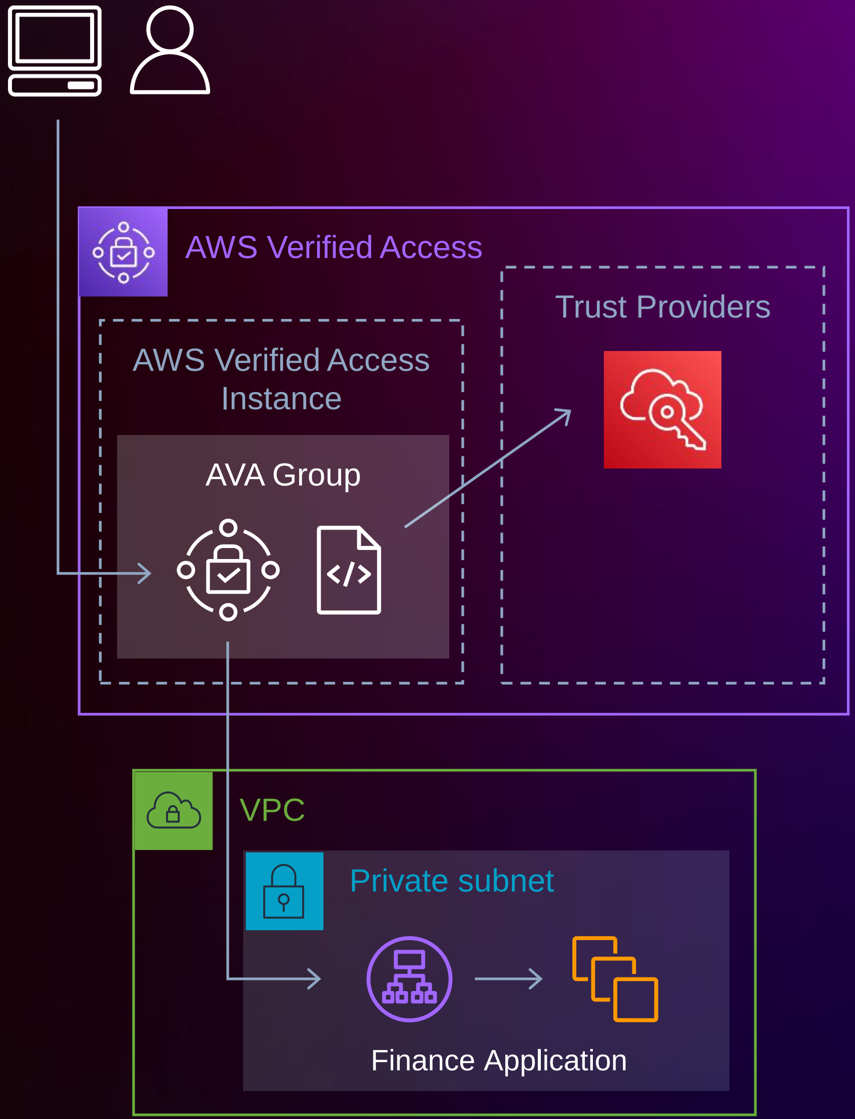


# Demo – Access private application

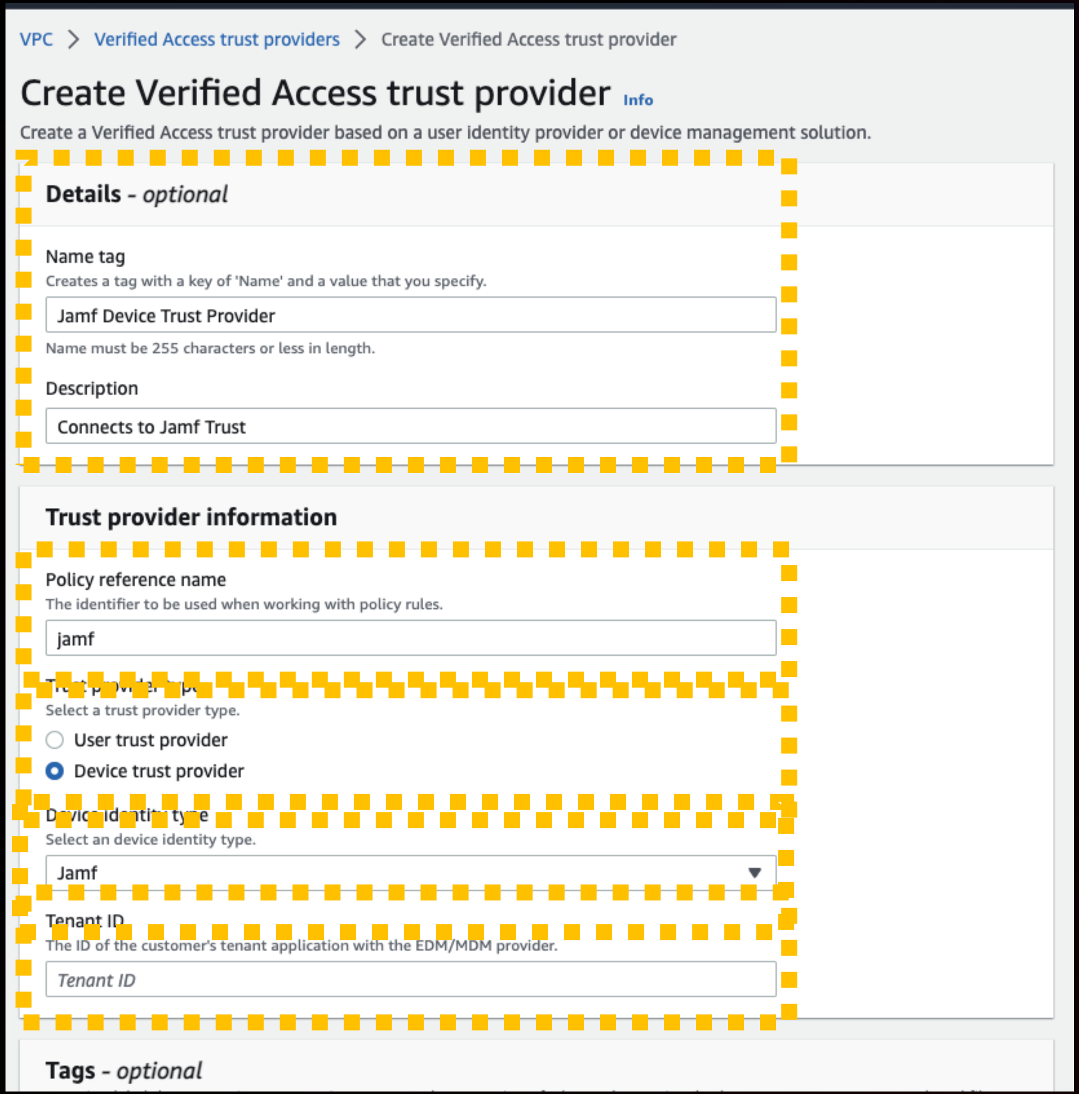


https://test-ava-endpoint.szma ✕
+
test-ava-endpoint.szmajdj.people.aws.dev/?

# Super secret data



# Demo – Create device trust providers



VPC > Verified Access trust providers > Create Verified Access trust provider

## Create Verified Access trust provider Info

Create a Verified Access trust provider based on a user identity provider or device management solution.

### Details - *optional*

Name tag

Creates a tag with a key of 'Name' and a value that you specify.

Jamf Device Trust Provider

Name must be 255 characters or less in length.

Description

Connects to Jamf Trust

### Trust provider information

Policy reference name

The identifier to be used when working with policy rules.

jamf

Trust provider type

Select a trust provider type.

○ User trust provider

● Device trust provider

Device identity type

Select an device identity type.

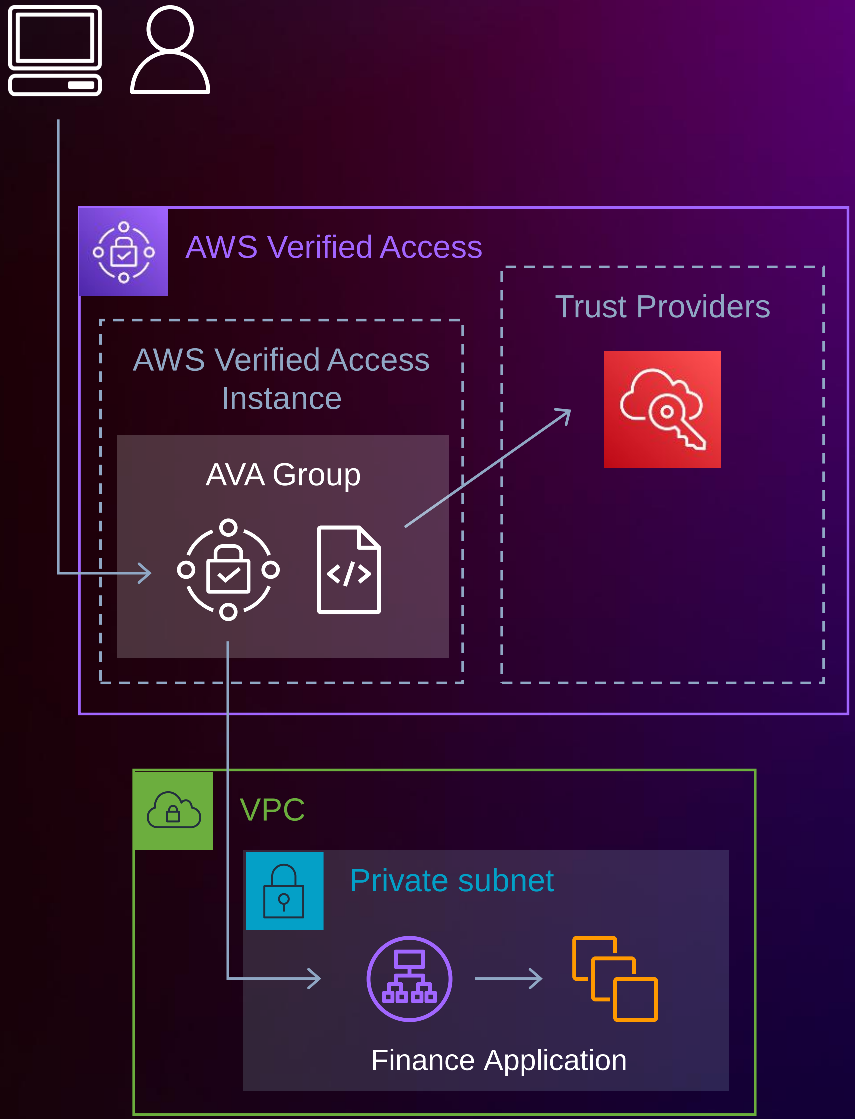
Jamf ▼

Tenant ID

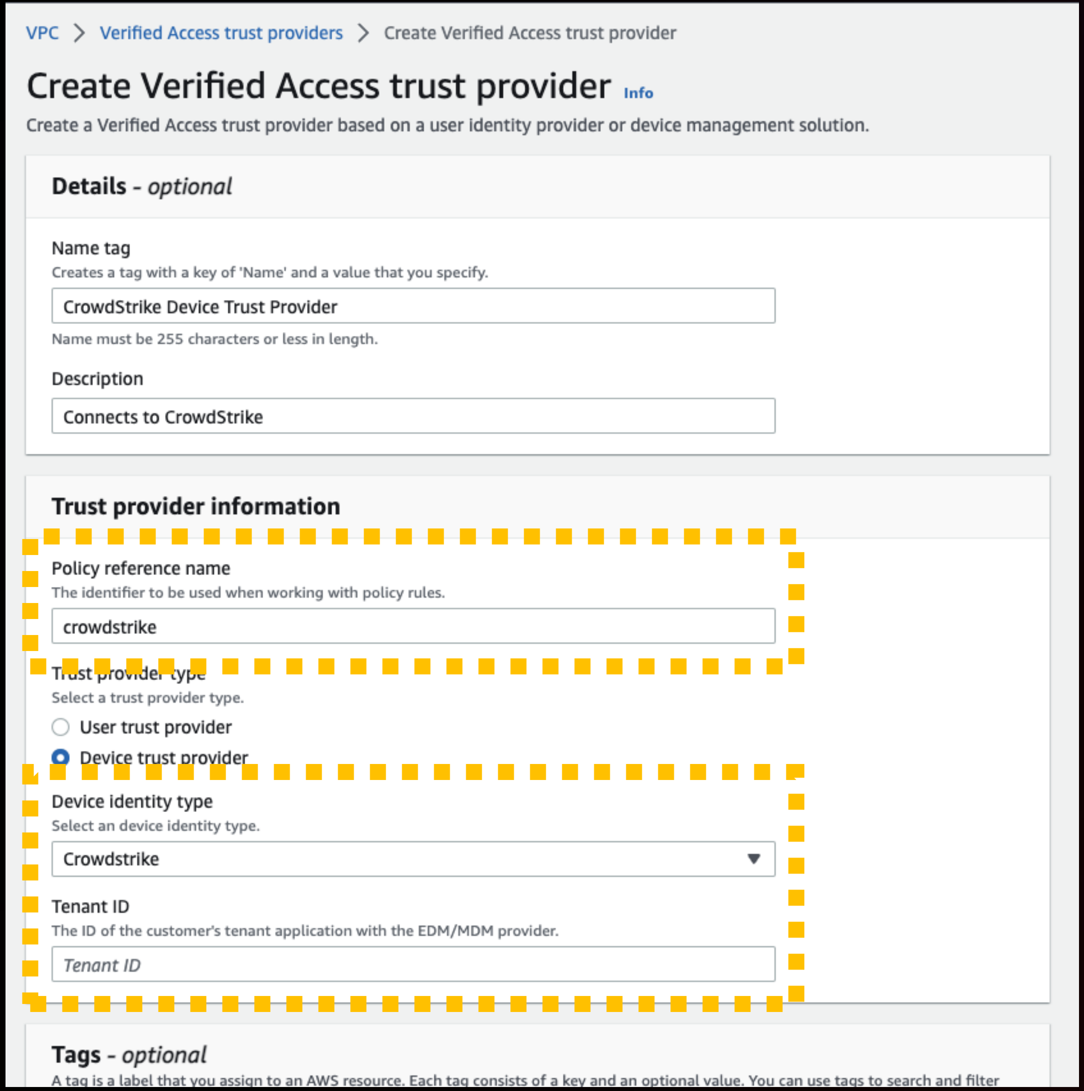
The ID of the customer's tenant application with the EDM/MDM provider.

*Tenant ID*

### Tags - *optional*



# Demo – Create device trust providers



VPC > Verified Access trust providers > Create Verified Access trust provider

Create Verified Access trust provider Info

Create a Verified Access trust provider based on a user identity provider or device management solution.

Details - *optional*

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
CrowdStrike Device Trust Provider
Name must be 255 characters or less in length.

Description
Connects to CrowdStrike

Trust provider information

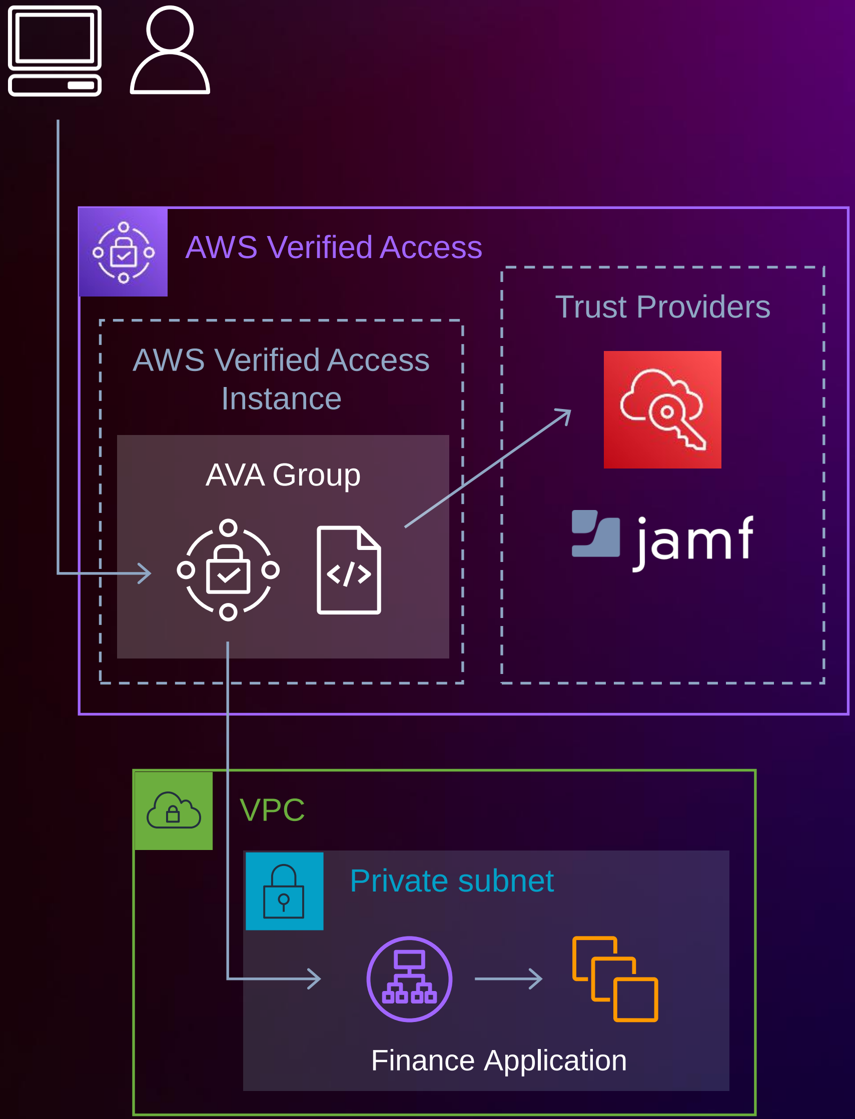
Policy reference name
The identifier to be used when working with policy rules.
crowdstrike

Trust provider type
Select a trust provider type.
○ User trust provider
● Device trust provider

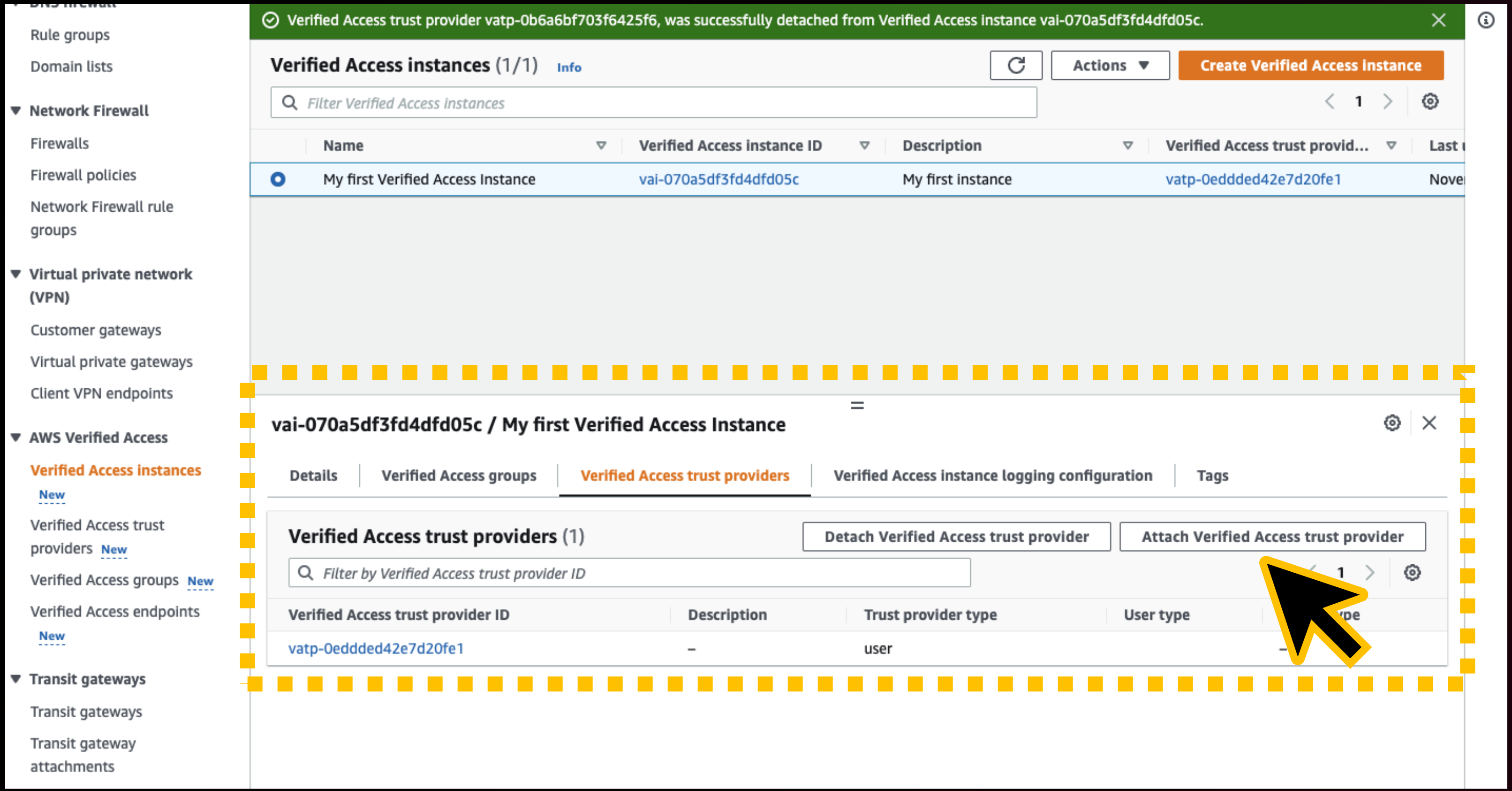
Device identity type
Select an device identity type.
Crowdstrike ▼

Tenant ID
The ID of the customer's tenant application with the EDM/MDM provider.
*Tenant ID*

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter



# Demo – Attach device trust providers



Rule groups
Domain lists
▼ Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Client VPN endpoints
▼ AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New
▼ Transit gateways
Transit gateways
Transit gateway attachments

Verified Access trust provider vatp-0b6a6bf703f6425f6, was successfully detached from Verified Access Instance vai-070a5df3fd4dfd05c.

## Verified Access instances (1/1) Info

Actions ▼
Create Verified Access instance
Filter Verified Access instances

| | Name | Verified Access instance ID | Description | Verified Access trust provid... | Last u |
|---|---|---|---|---|---|
| ● | My first Verified Access Instance | vai-070a5df3fd4dfd05c | My first instance | vatp-0edded42e7d20fe1 | Nove |

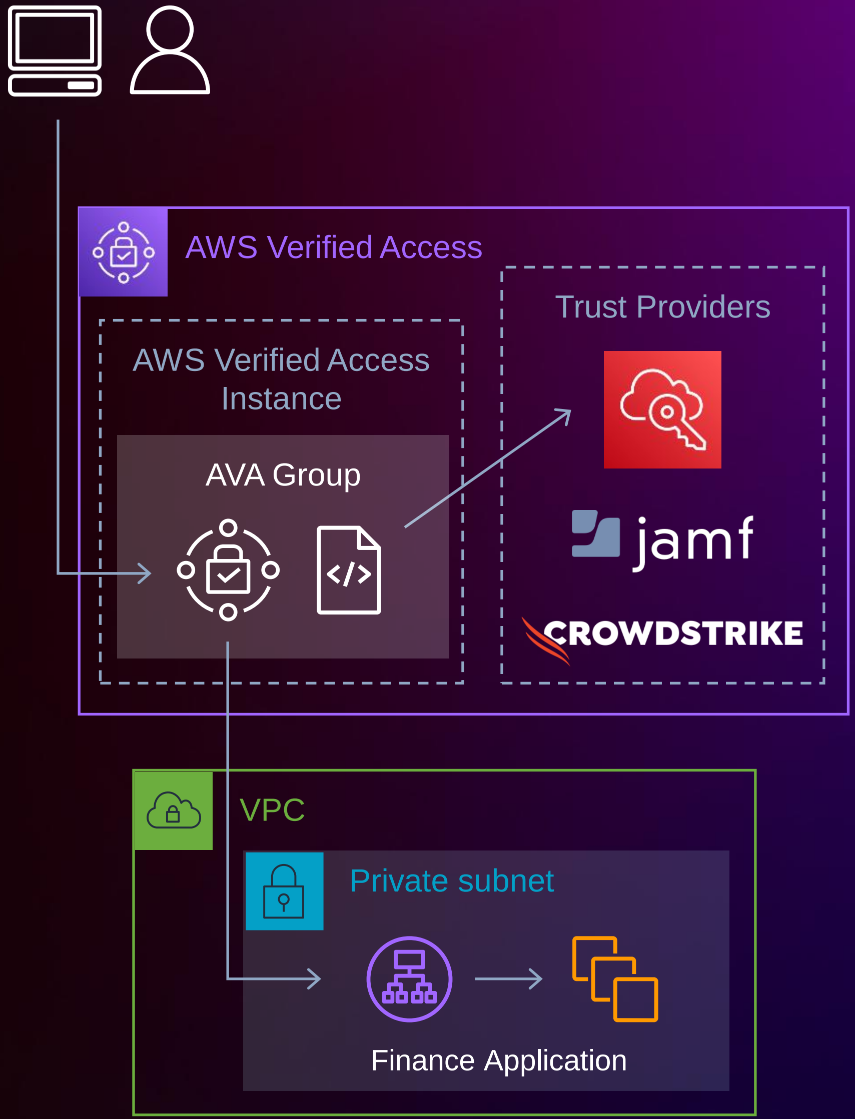
## vai-070a5df3fd4dfd05c / My first Verified Access Instance

Details
Verified Access groups
Verified Access trust providers
Verified Access instance logging configuration
Tags

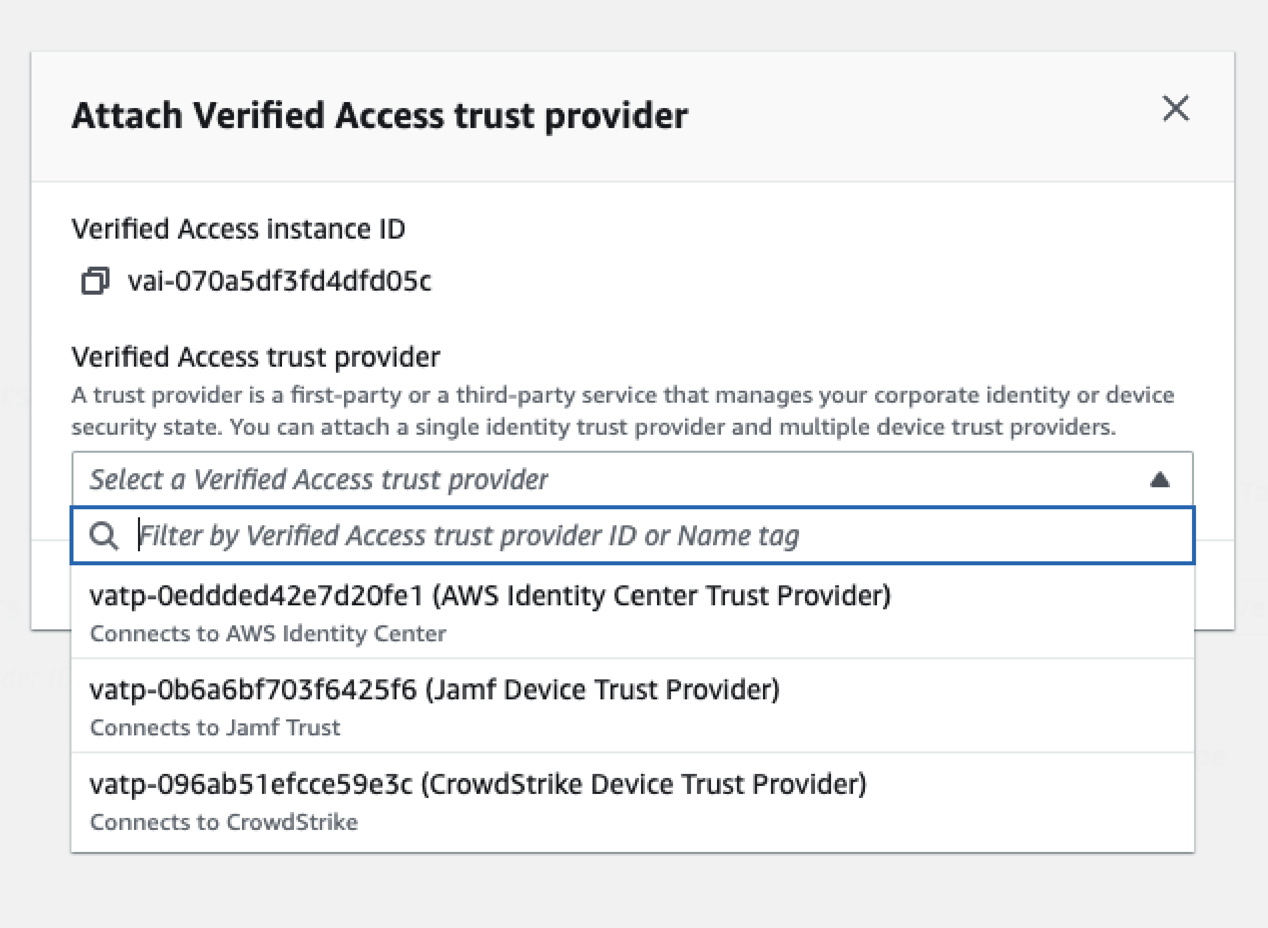
### Verified Access trust providers (1)

Detach Verified Access trust provider
Attach Verified Access trust provider
Filter by Verified Access trust provider ID

| Verified Access trust provider ID | Description | Trust provider type | User type | ...pe |
|---|---|---|---|---|
| vatp-0edded42e7d20fe1 | – | user | – | |



# Demo – Attach device trust providers



## Attach Verified Access trust provider

Verified Access instance ID

vai-070a5df3fd4dfd05c

Verified Access trust provider

A trust provider is a first-party or a third-party service that manages your corporate identity or device security state. You can attach a single identity trust provider and multiple device trust providers.

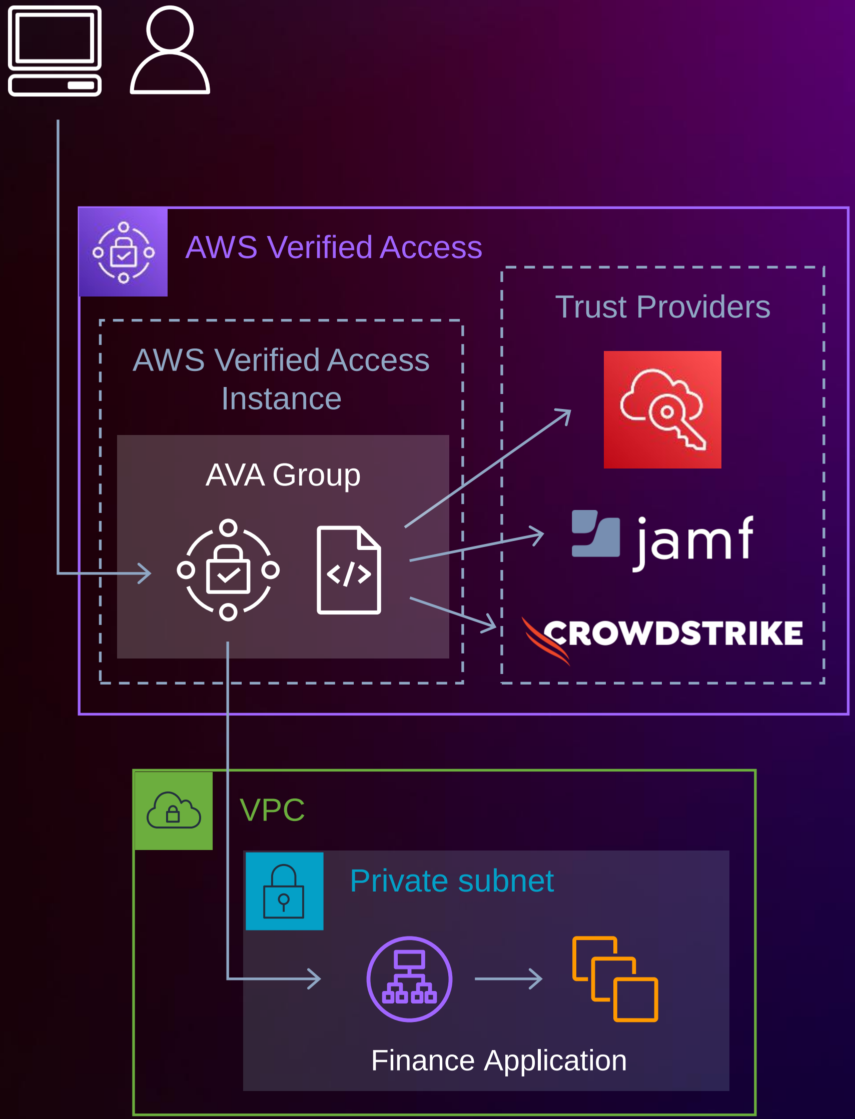
*Select a Verified Access trust provider*

*Filter by Verified Access trust provider ID or Name tag*

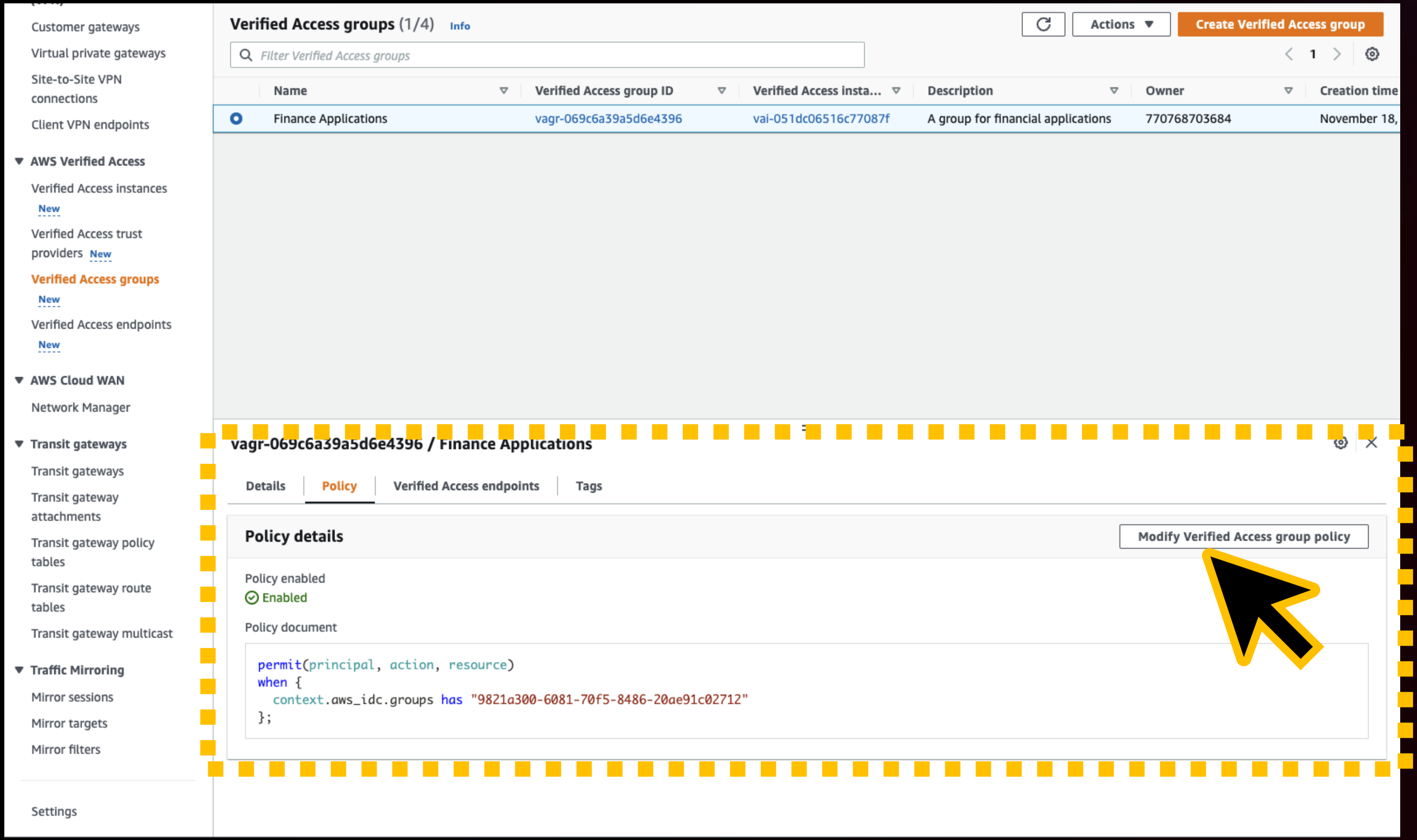
vatp-0eddded42e7d20fe1 (AWS Identity Center Trust Provider)
Connects to AWS Identity Center

vatp-0b6a6bf703f6425f6 (Jamf Device Trust Provider)
Connects to Jamf Trust

vatp-096ab51efcce59e3c (CrowdStrike Device Trust Provider)
Connects to CrowdStrike



# Demo – Modify group policy



Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints

▼ AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New

▼ AWS Cloud WAN
Network Manager

▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast

▼ Traffic Mirroring
Mirror sessions
Mirror targets
Mirror filters

Settings

**Verified Access groups** (1/4) Info

Actions ▼ | Create Verified Access group

Filter Verified Access groups

| | Name | Verified Access group ID | Verified Access insta... | Description | Owner | Creation time |
|---|---|---|---|---|---|---|
| ● | Finance Applications | vagr-069c6a39a5d6e4396 | vai-051dc06516c77087f | A group for financial applications | 770768703684 | November 18, |

**vagr-069c6a39a5d6e4396 / Finance Applications**

Details | Policy | Verified Access endpoints | Tags

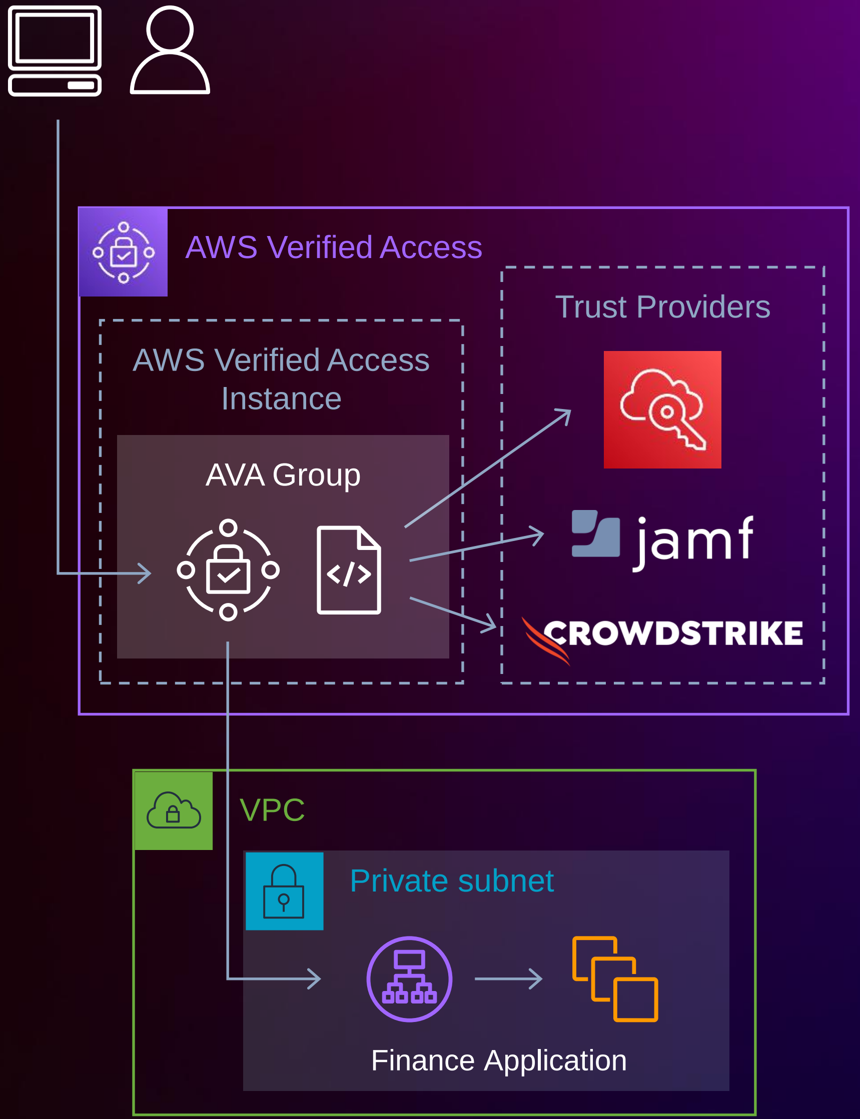
**Policy details**

Modify Verified Access group policy

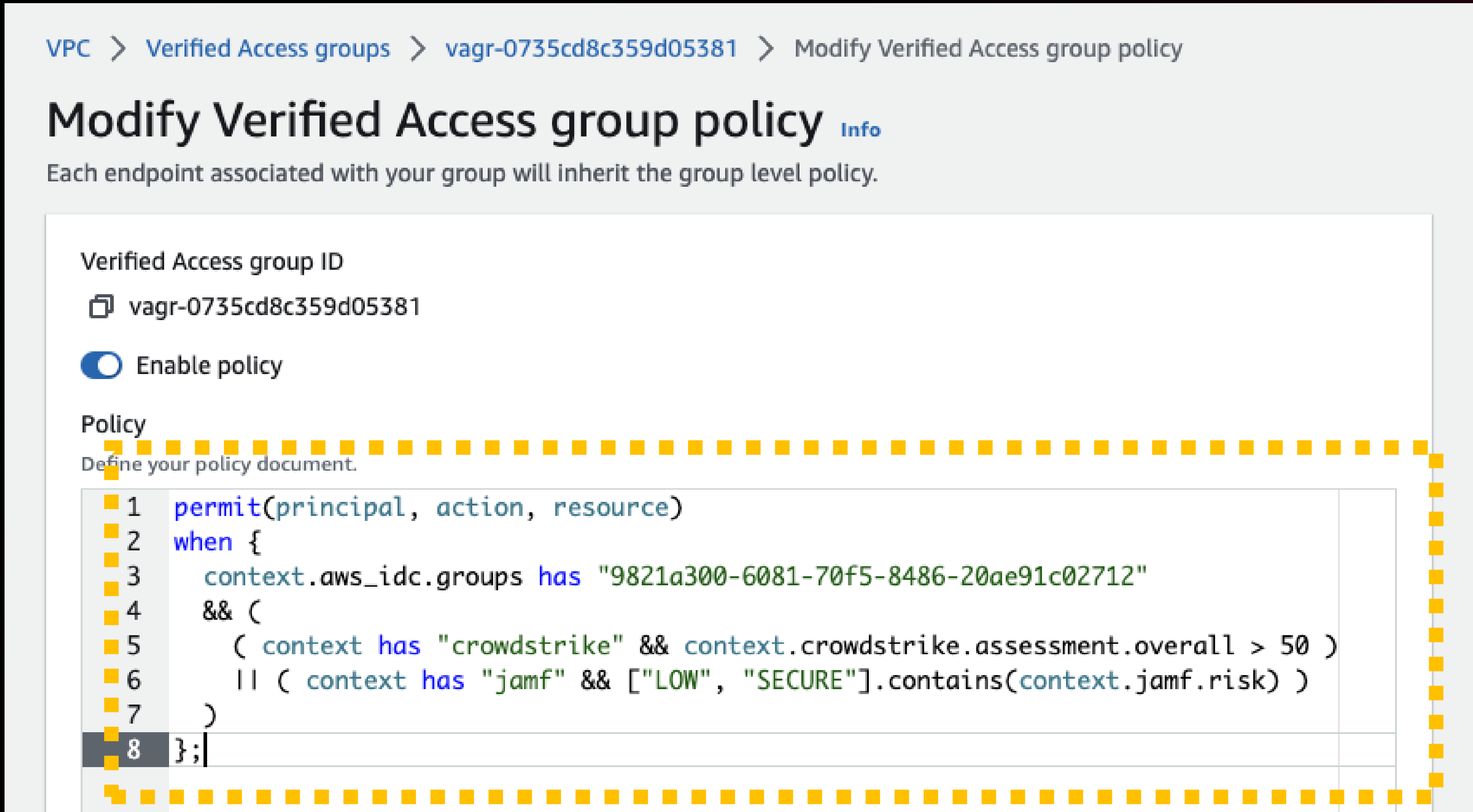
Policy enabled
✓ Enabled

Policy document

```
permit(principal, action, resource)
when {
  context.aws_idc.groups has "9821a300-6081-70f5-8486-20ae91c02712"
};
```



# Demo – Modify group policy



VPC > Verified Access groups > vagr-0735cd8c359d05381 > Modify Verified Access group policy

## Modify Verified Access group policy Info

Each endpoint associated with your group will inherit the group level policy.

Verified Access group ID

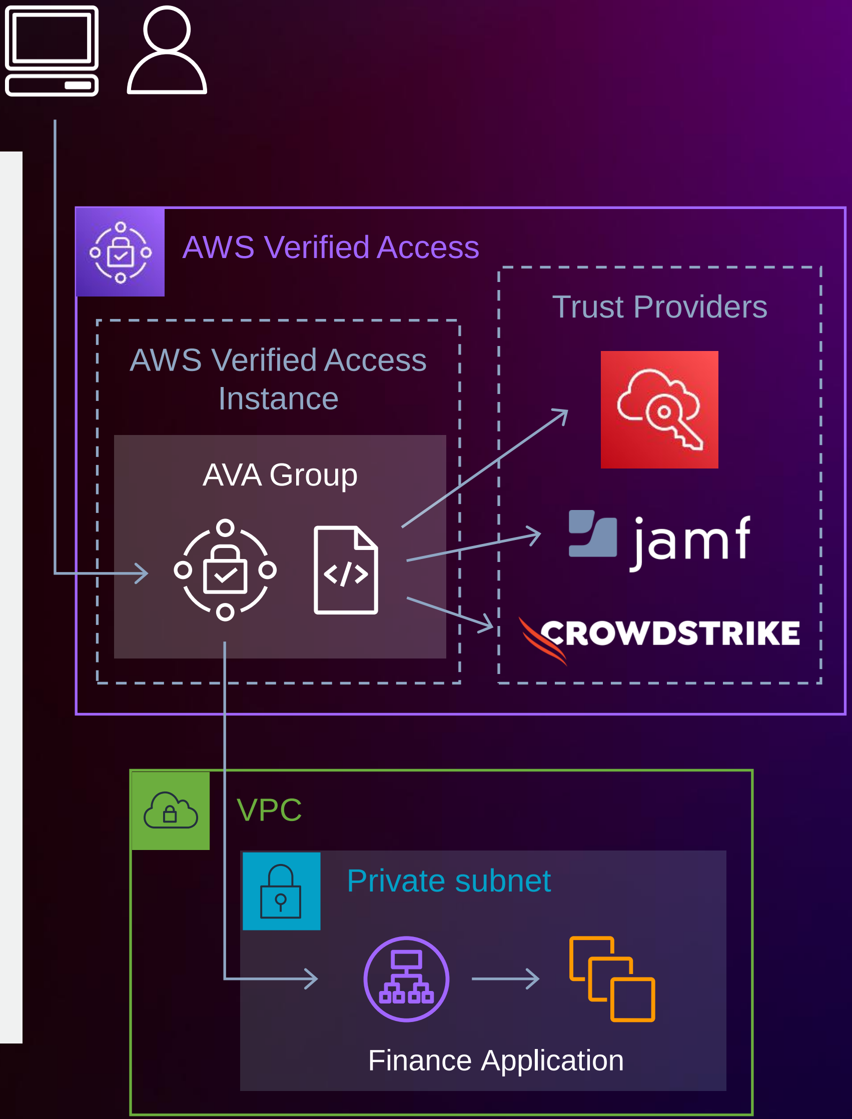
vagr-0735cd8c359d05381

● Enable policy

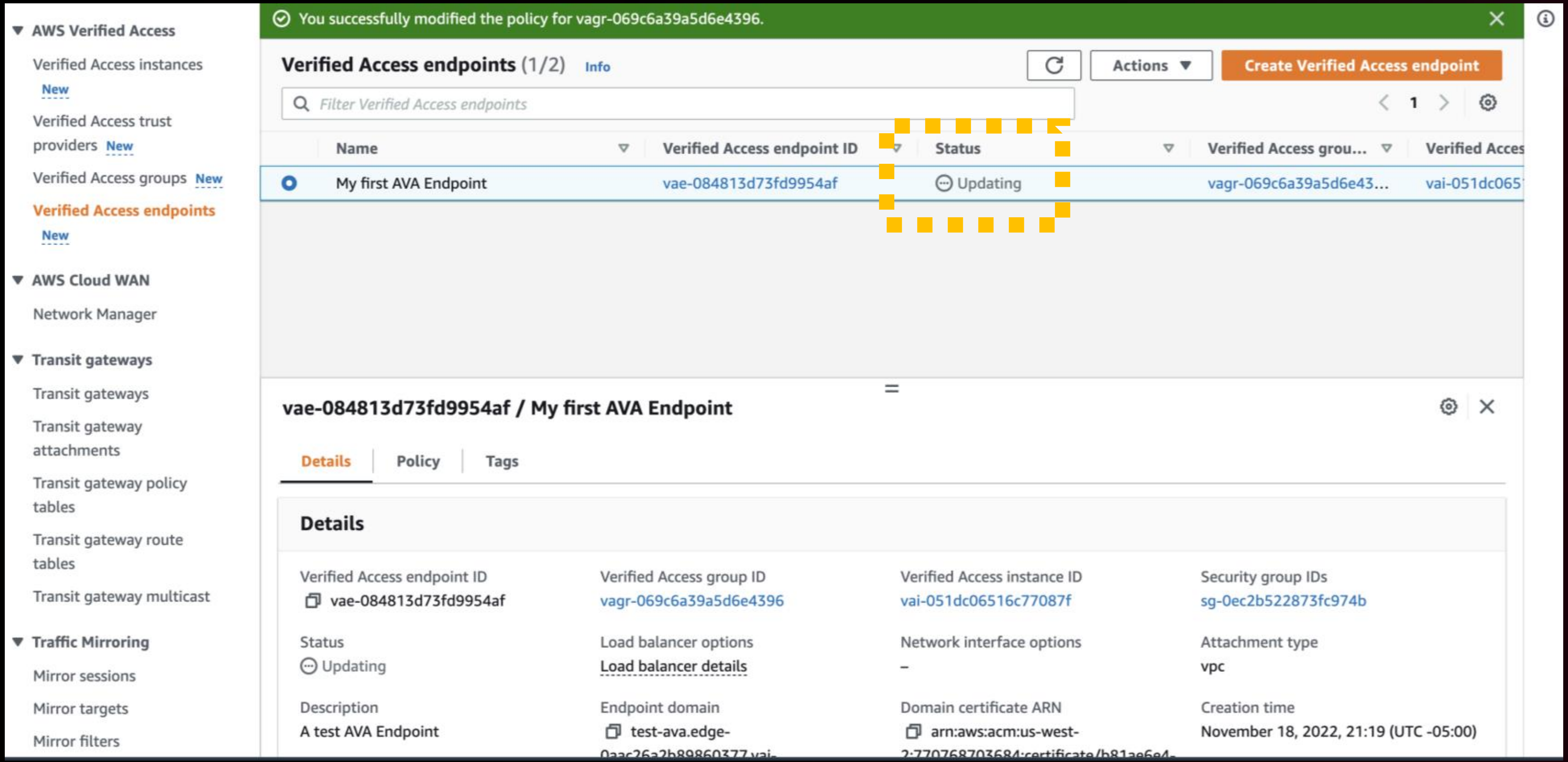
Policy

Define your policy document.

```
permit(principal, action, resource)
when {
  context.aws_idc.groups has "9821a300-6081-70f5-8486-20ae91c02712"
  && (
    ( context has "crowdstrike" && context.crowdstrike.assessment.overall > 50 )
    || ( context has "jamf" && ["LOW", "SECURE"].contains(context.jamf.risk) )
  )
};
```



# Demo – Modify group policy



▼ AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Verified Access endpoints New
▼ AWS Cloud WAN
Network Manager
▼ Transit gateways
Transit gateways
Transit gateway attachments
Transit gateway policy tables
Transit gateway route tables
Transit gateway multicast
▼ Traffic Mirroring
Mirror sessions
Mirror targets
Mirror filters

You successfully modified the policy for vagr-069c6a39a5d6e4396.

**Verified Access endpoints** (1/2) Info

Actions ▼
Create Verified Access endpoint
Filter Verified Access endpoints
1

| | Name | Verified Access endpoint ID | Status | Verified Access grou... | Verified Acces |
|---|---|---|---|---|---|
| ● | My first AVA Endpoint | vae-084813d73fd9954af | ⊖ Updating | vagr-069c6a39a5d6e43... | vai-051dc065 |

**vae-084813d73fd9954af / My first AVA Endpoint**

**Details**

Verified Access endpoint ID
vae-084813d73fd9954af

Verified Access group ID
vagr-069c6a39a5d6e4396

Verified Access instance ID
vai-051dc06516c77087f

Security group IDs
sg-0ec2b522873fc974b

Status
⊖ Updating

Load balancer options
Load balancer details

Network interface options
–

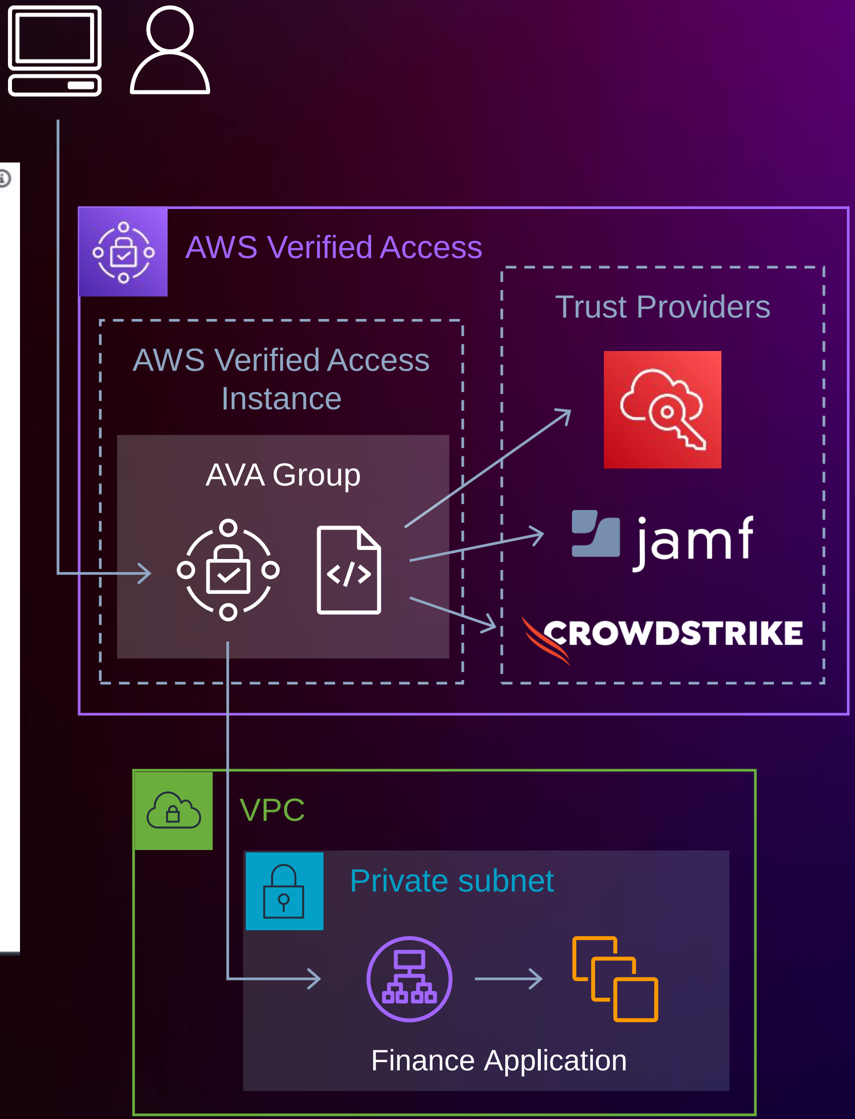
Attachment type
vpc

Description
A test AVA Endpoint

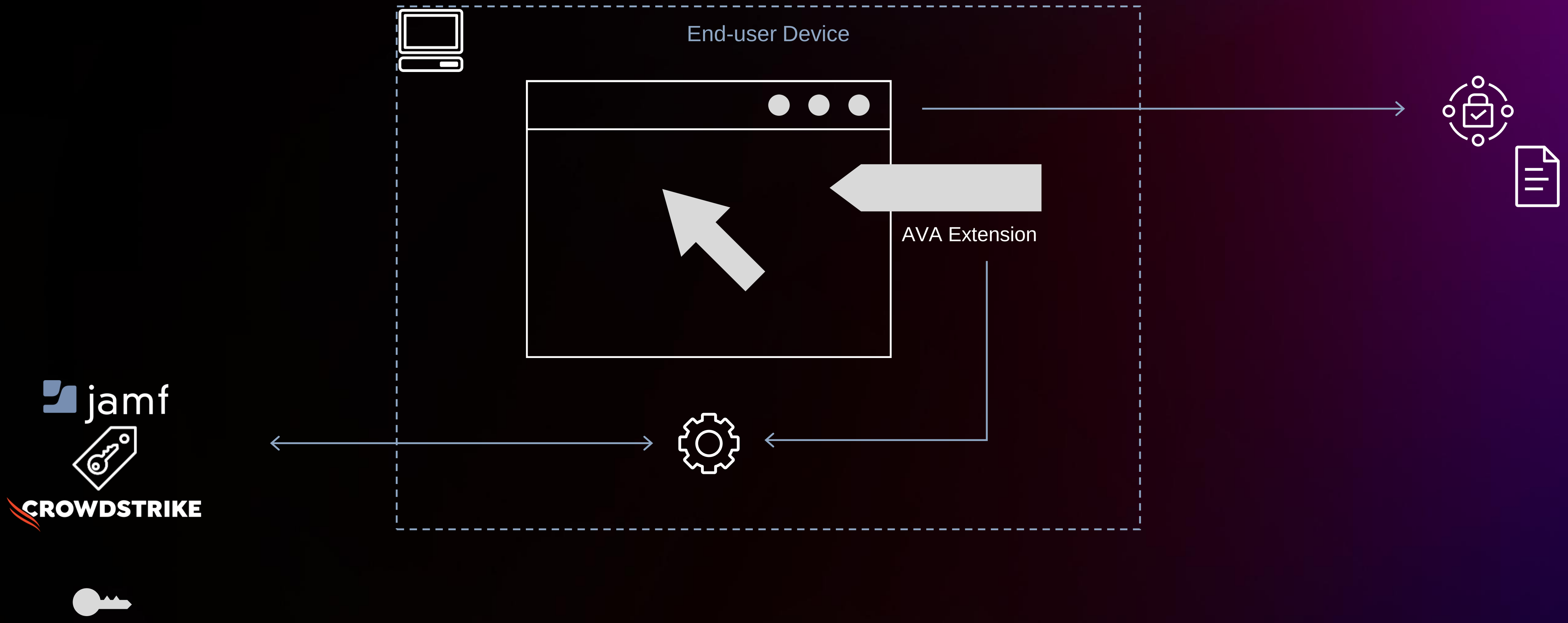
Endpoint domain
test-ava.edge-0aac26a2b89860377.vai-

Domain certificate ARN
arn:aws:acm:us-west-2:770768703684:certificate/b81ae6e4-

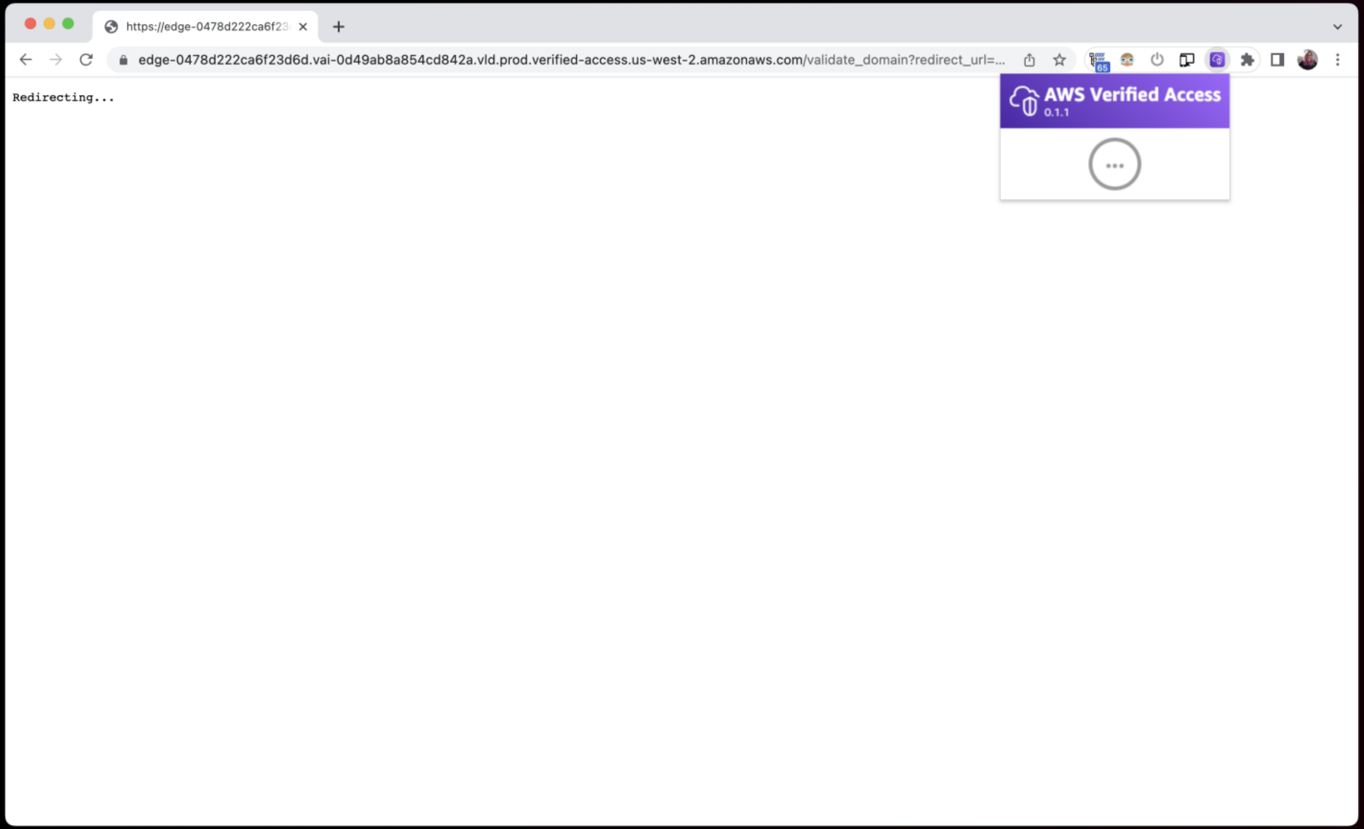
Creation time
November 18, 2022, 21:19 (UTC -05:00)



# Device information flow

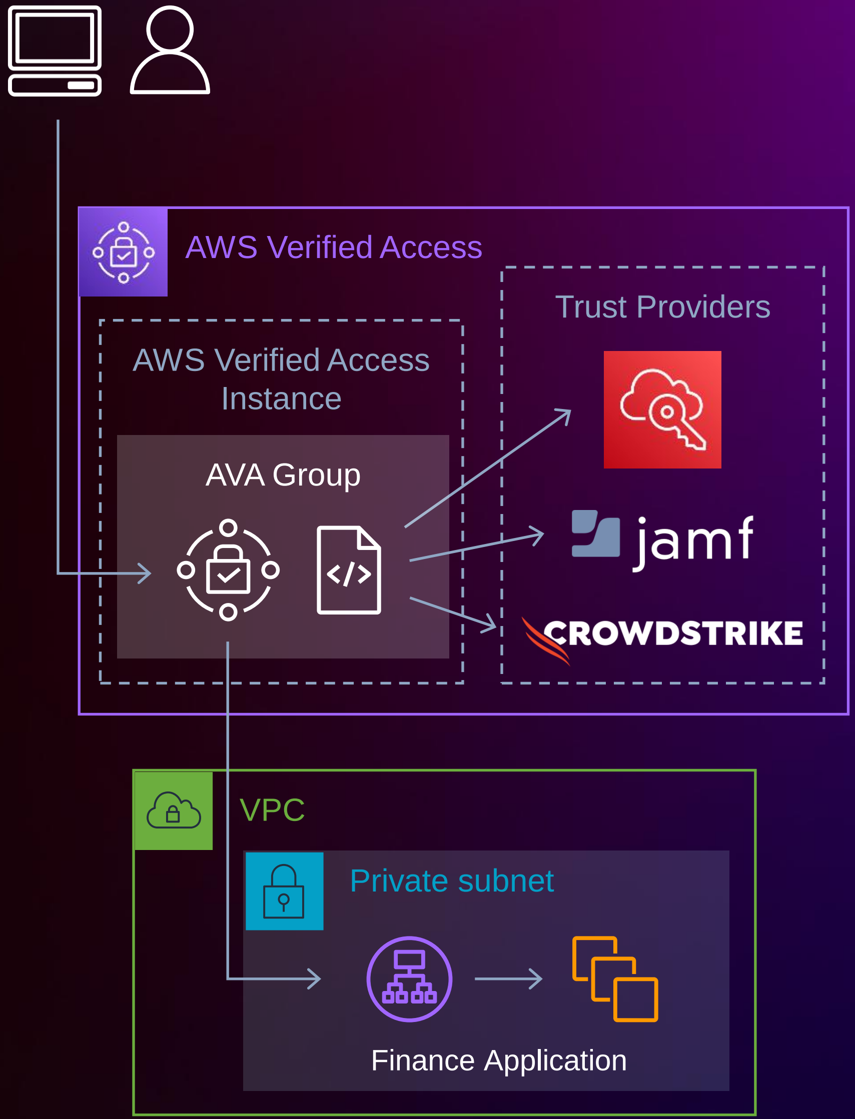


# Demo – Attempt access

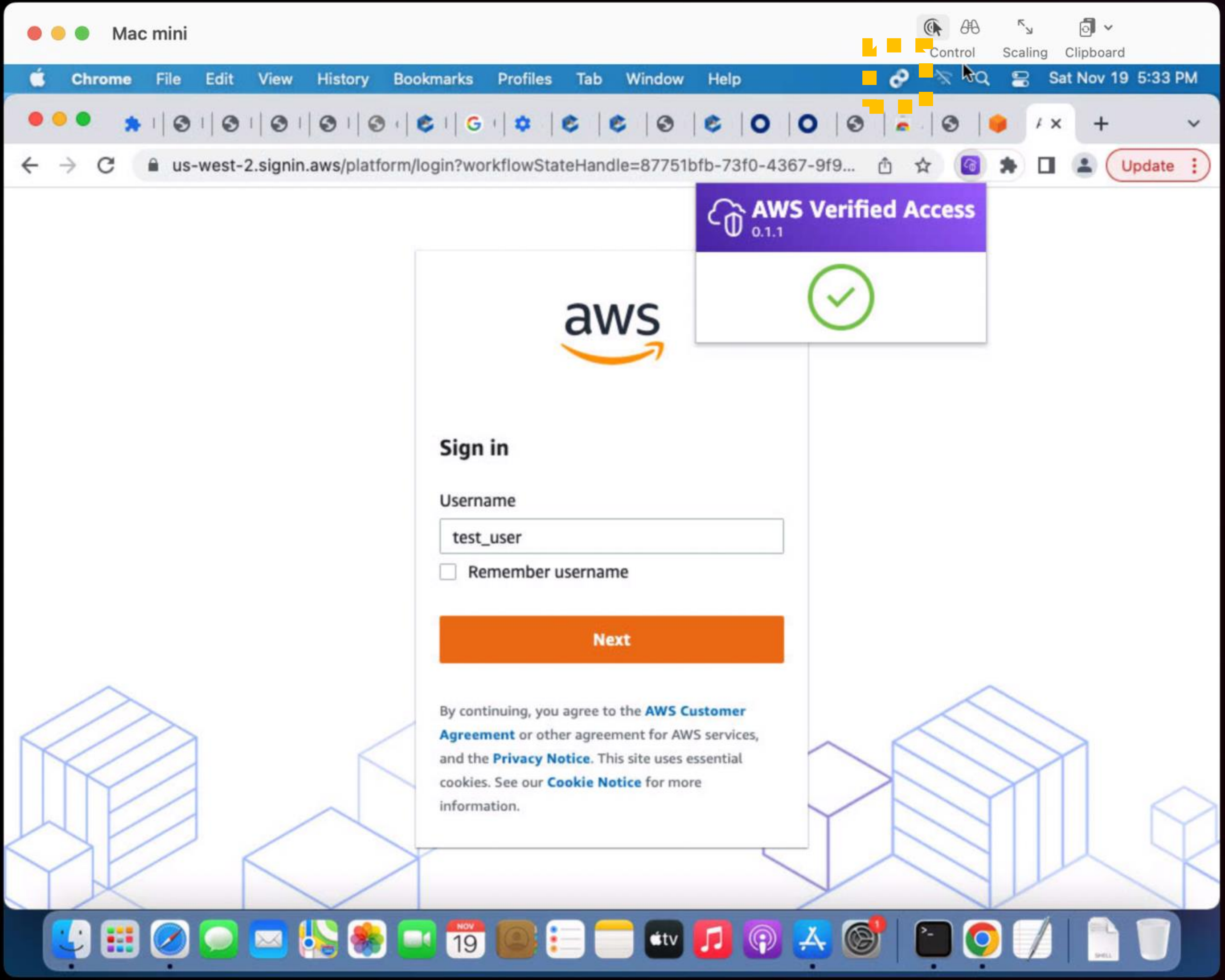


https://edge-0478d222ca6f23
edge-0478d222ca6f23d6d.vai-0d49ab8a854cd842a.vld.prod.verified-access.us-west-2.amazonaws.com/validate_domain?redirect_url=...
AWS Verified Access
0.1.1

```
Redirecting...
```



# Demo – Access private application



us-west-2.signin.aws/platform/login?workflowStateHandle=87751bfb-73f0-4367-9f9...

aws

**Sign in**

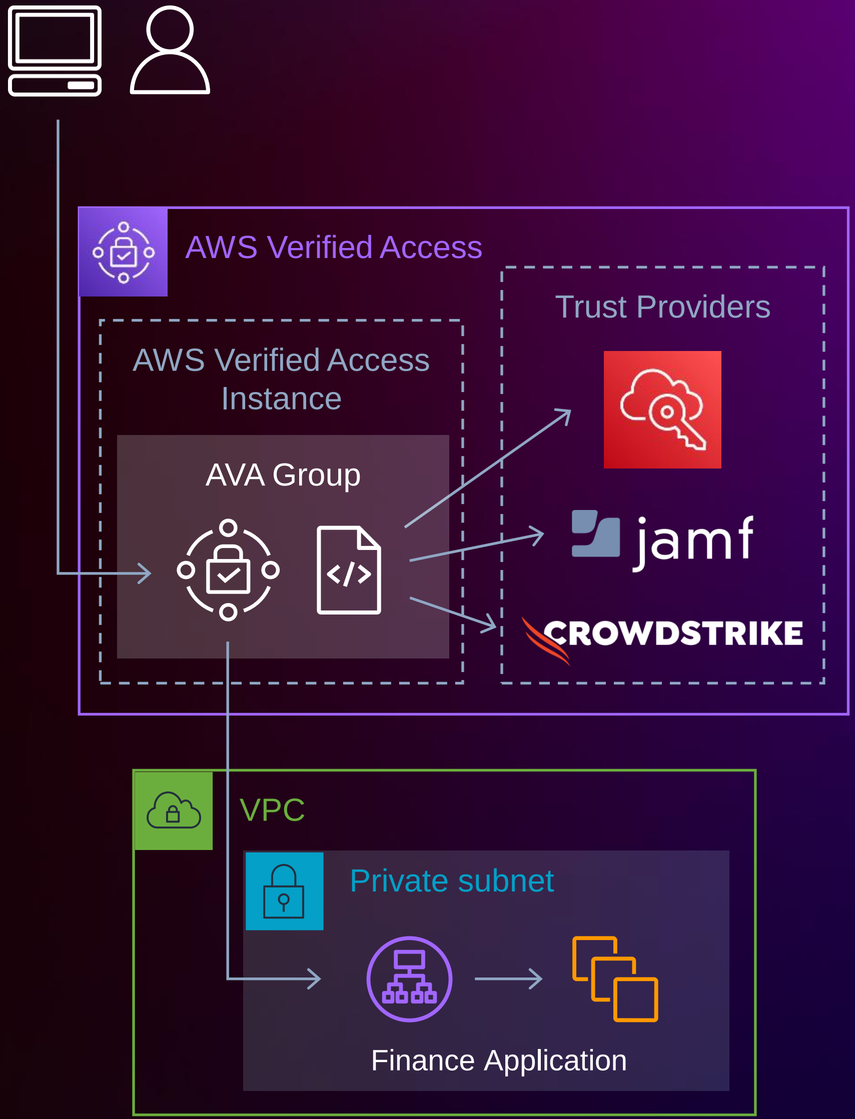
Username

test_user

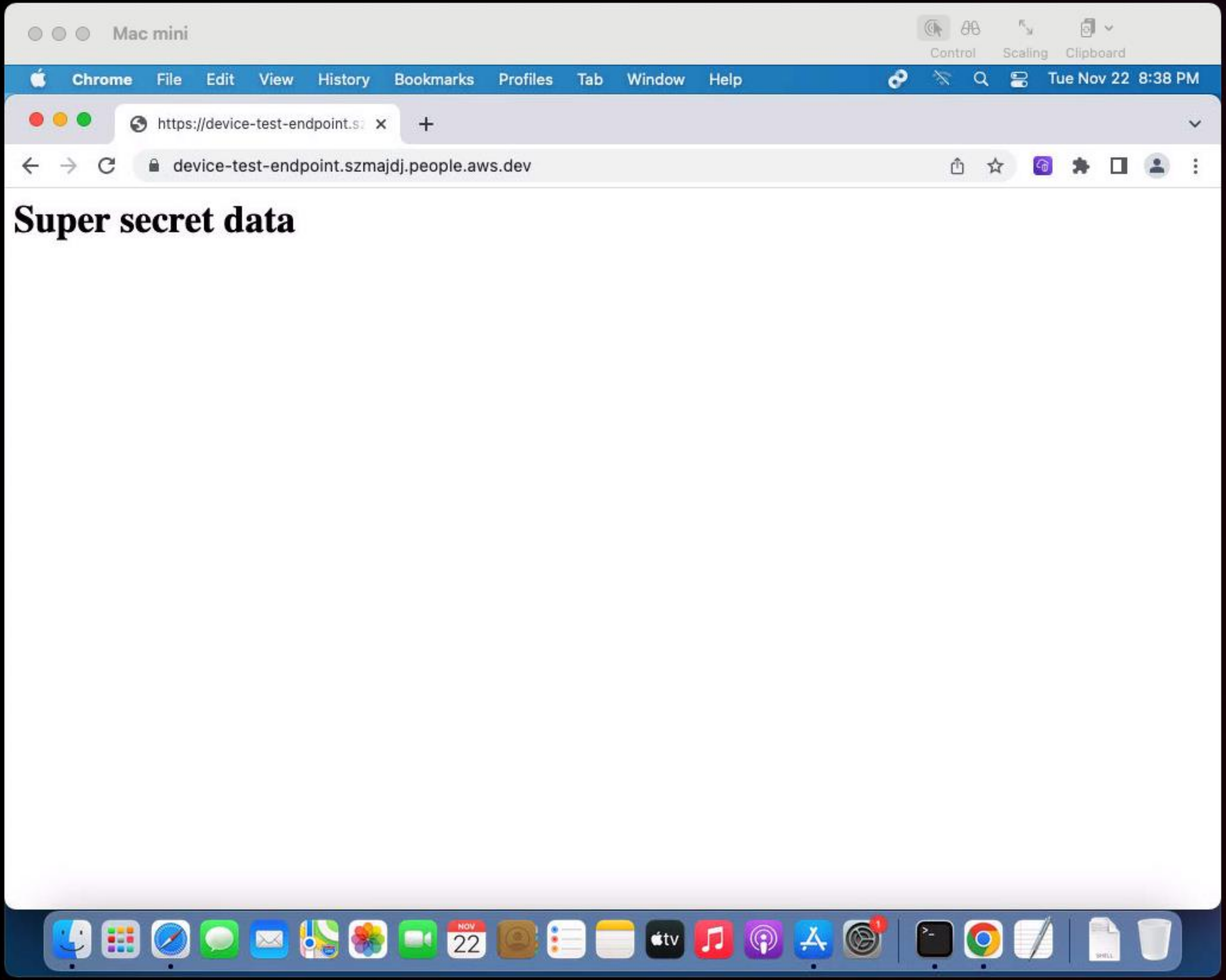
□ Remember username

Next

By continuing, you agree to the **AWS Customer Agreement** or other agreement for AWS services, and the **Privacy Notice**. This site uses essential cookies. See our **Cookie Notice** for more information.

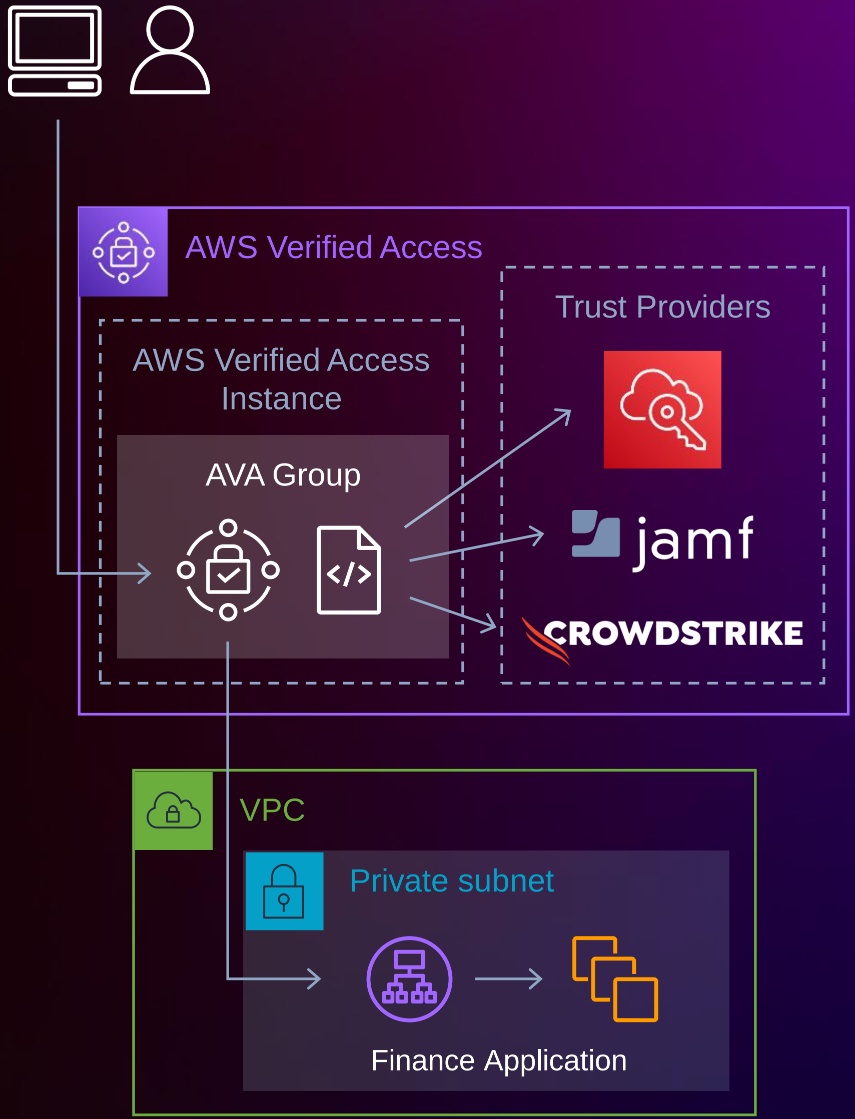


# Demo – Access private application

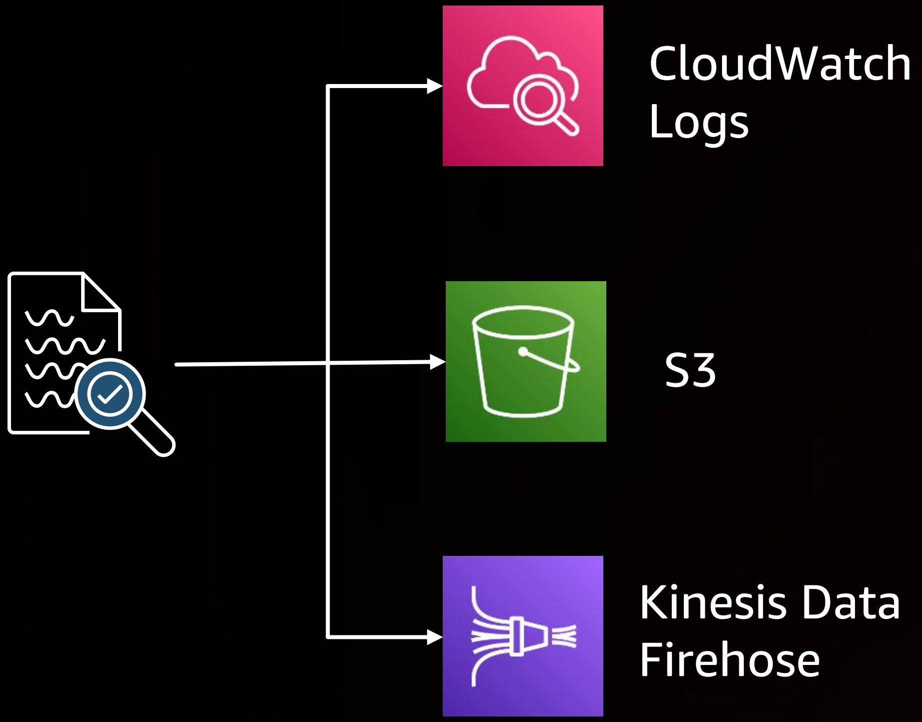


Mac mini
Control
Scaling
Clipboard
Chrome File Edit View History Bookmarks Profiles Tab Window Help
Tue Nov 22 8:38 PM
https://device-test-endpoint.s
device-test-endpoint.szmajdj.people.aws.dev

Super secret data



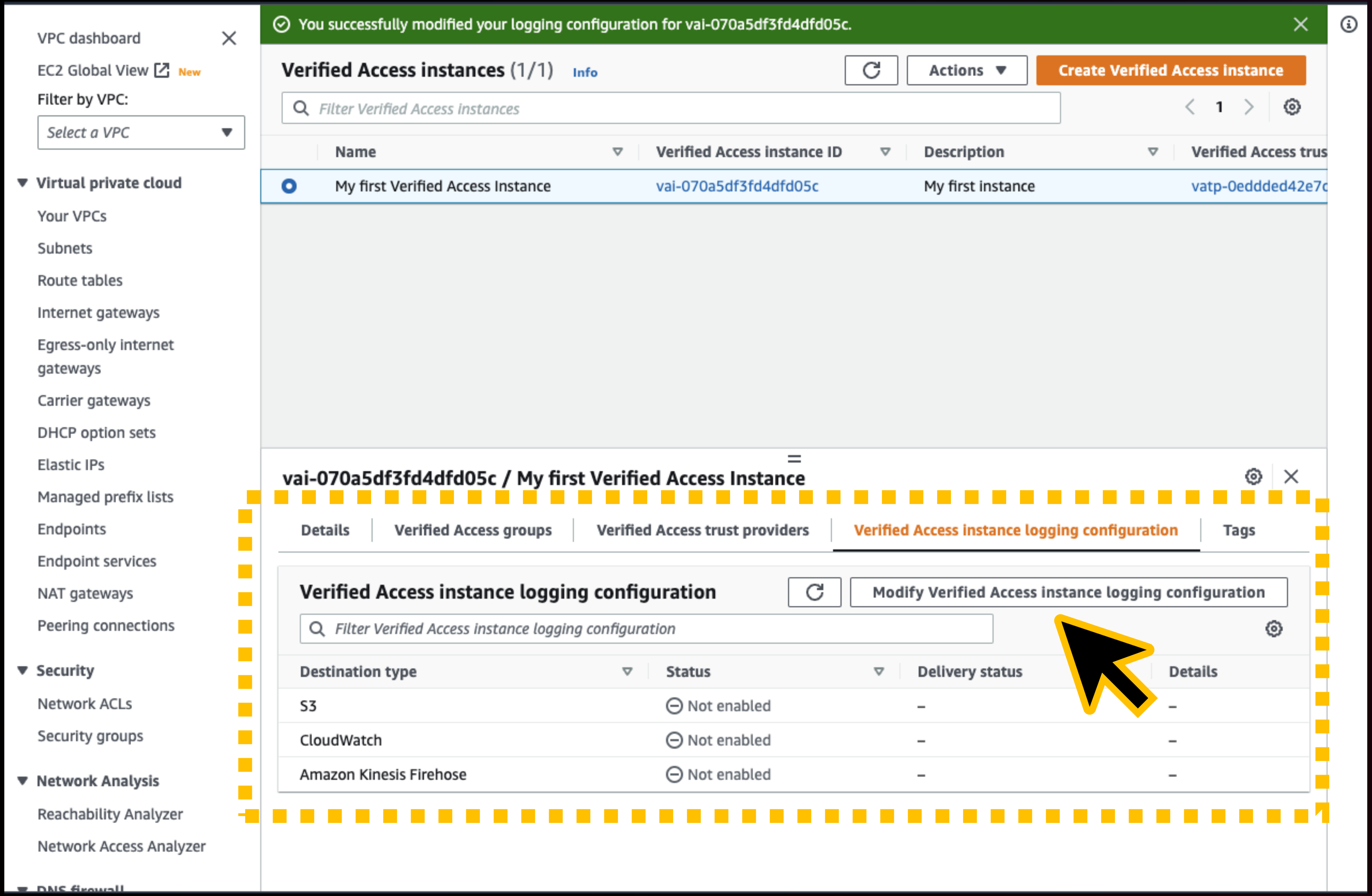
# Access Logs



3 events can be generated

| Access allowed | Access denied | |
|---|---|---|
| ✓ | ✗ | ✗ |
| | IdP authentication (e.g. MFA) | Verified access policies |

# Demo – Configure logging



You successfully modified your logging configuration for vai-070a5df3fd4dfd05c.

**Verified Access instances** (1/1) Info

Actions ▼
Create Verified Access instance
Filter Verified Access instances

| | Name | Verified Access instance ID | Description | Verified Access trus |
|---|---|---|---|---|
| ● | My first Verified Access Instance | vai-070a5df3fd4dfd05c | My first instance | vatp-0edddded42e7c |

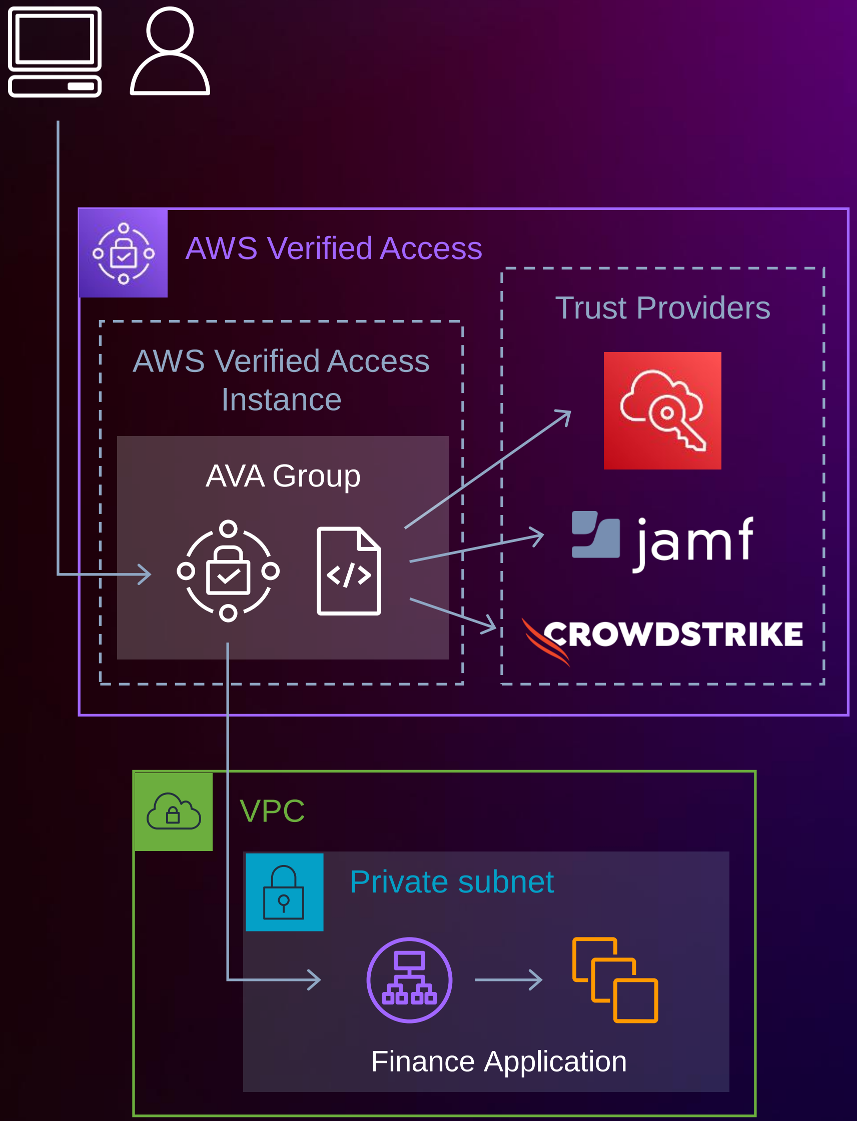
**vai-070a5df3fd4dfd05c / My first Verified Access Instance**

Details
Verified Access groups
Verified Access trust providers
Verified Access instance logging configuration
Tags

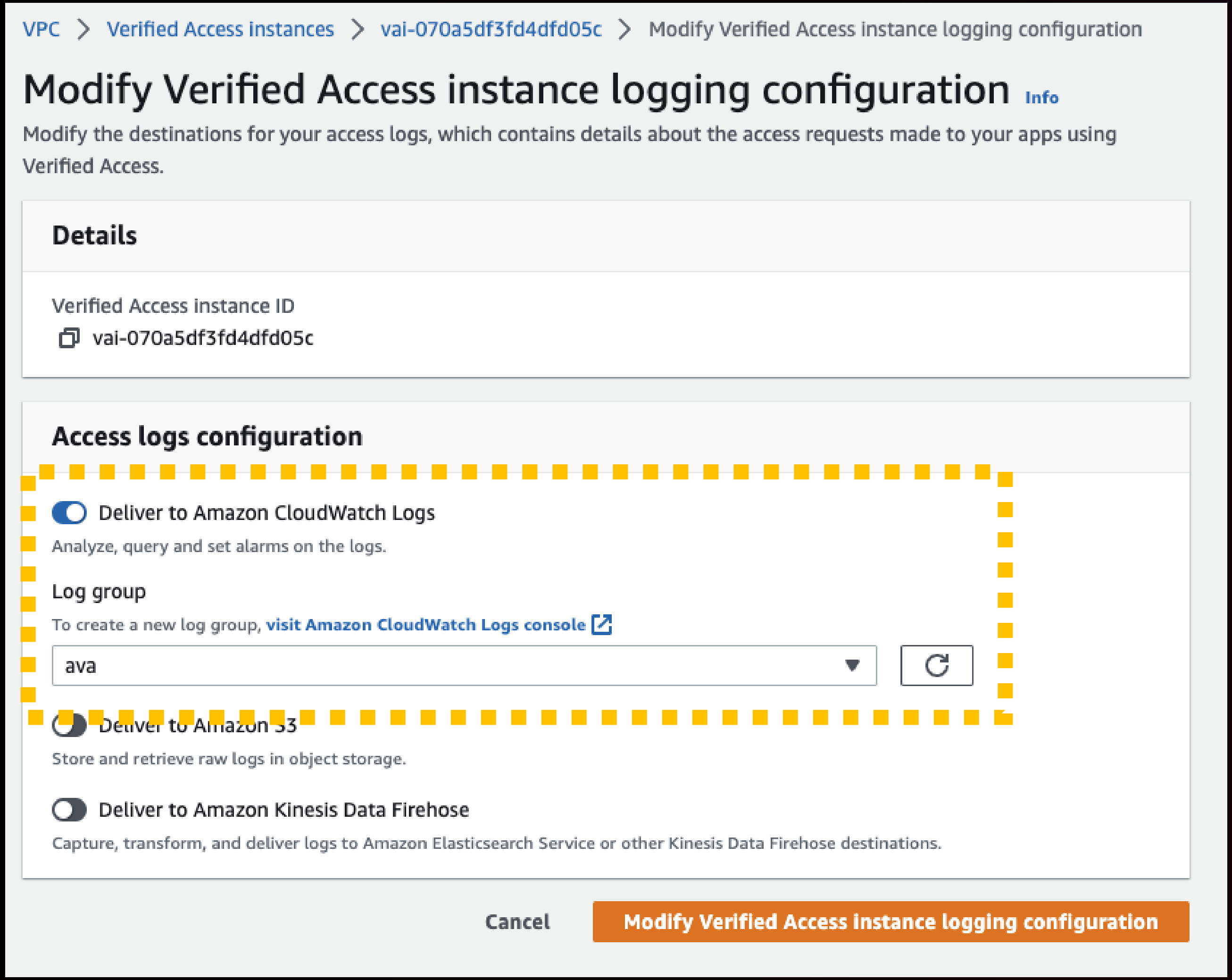
**Verified Access instance logging configuration**

Modify Verified Access instance logging configuration
Filter Verified Access instance logging configuration

| Destination type | Status | Delivery status | Details |
|---|---|---|---|
| S3 | ⊖ Not enabled | – | – |
| CloudWatch | ⊖ Not enabled | – | – |
| Amazon Kinesis Firehose | ⊖ Not enabled | – | – |



# Demo – Configure logging



VPC > Verified Access instances > vai-070a5df3fd4dfd05c > Modify Verified Access instance logging configuration

## Modify Verified Access instance logging configuration Info

Modify the destinations for your access logs, which contains details about the access requests made to your apps using Verified Access.

### Details

Verified Access instance ID
vai-070a5df3fd4dfd05c

### Access logs configuration

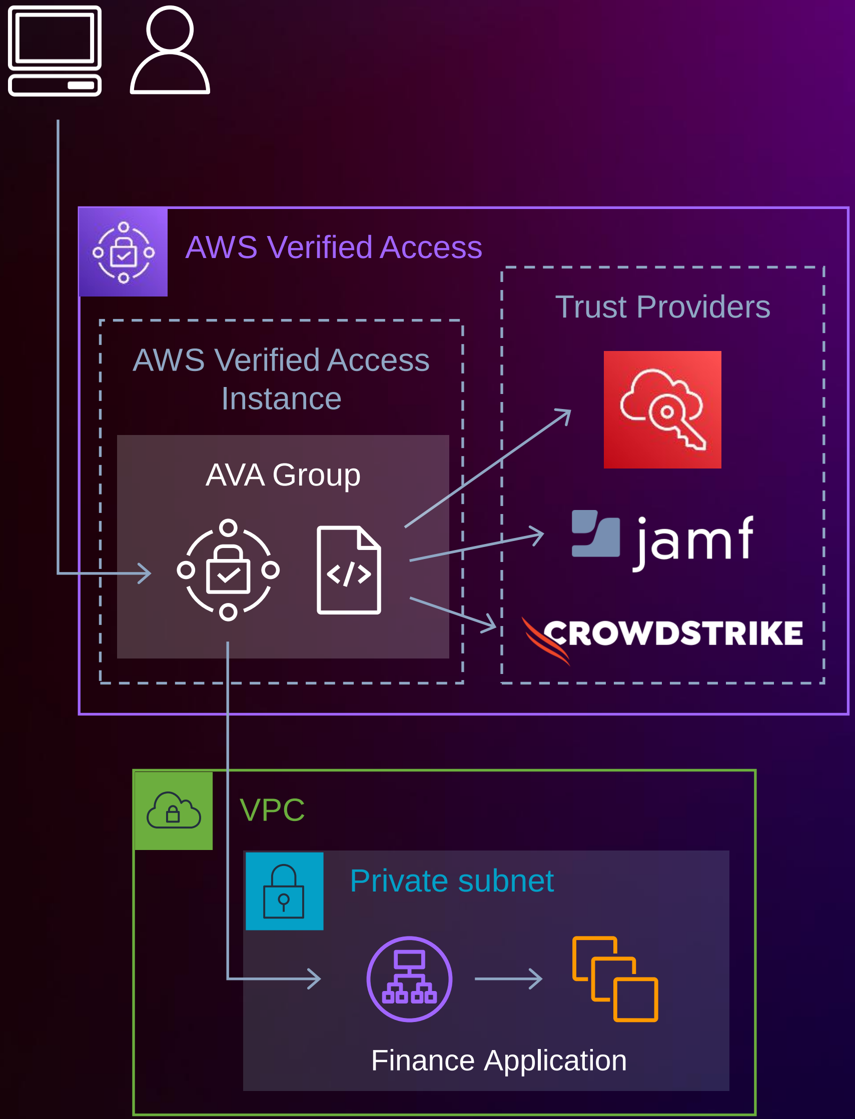
● Deliver to Amazon CloudWatch Logs
Analyze, query and set alarms on the logs.

Log group
To create a new log group, visit Amazon CloudWatch Logs console

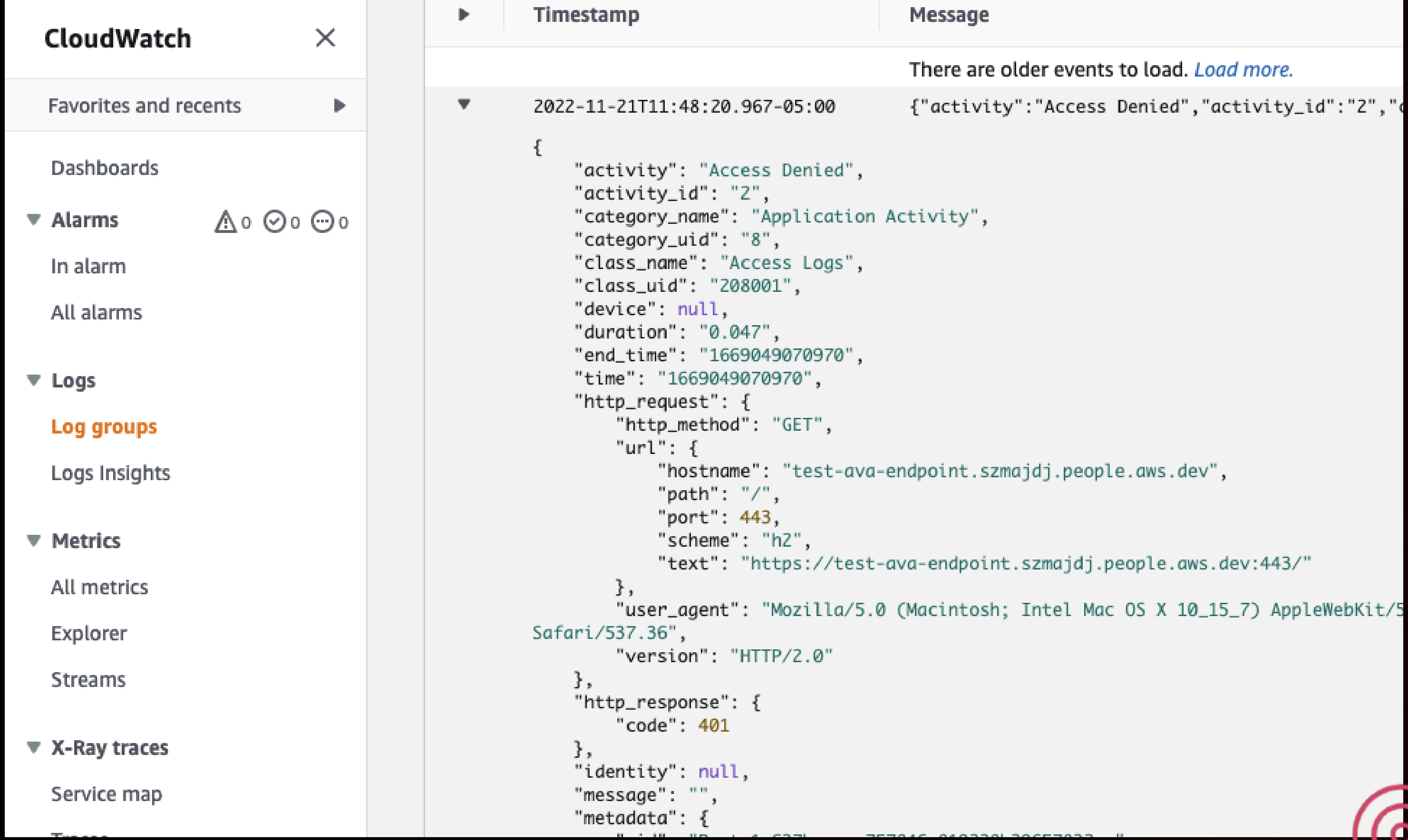
ava

○ Deliver to Amazon S3
Store and retrieve raw logs in object storage.

○ Deliver to Amazon Kinesis Data Firehose
Capture, transform, and deliver logs to Amazon Elasticsearch Service or other Kinesis Data Firehose destinations.

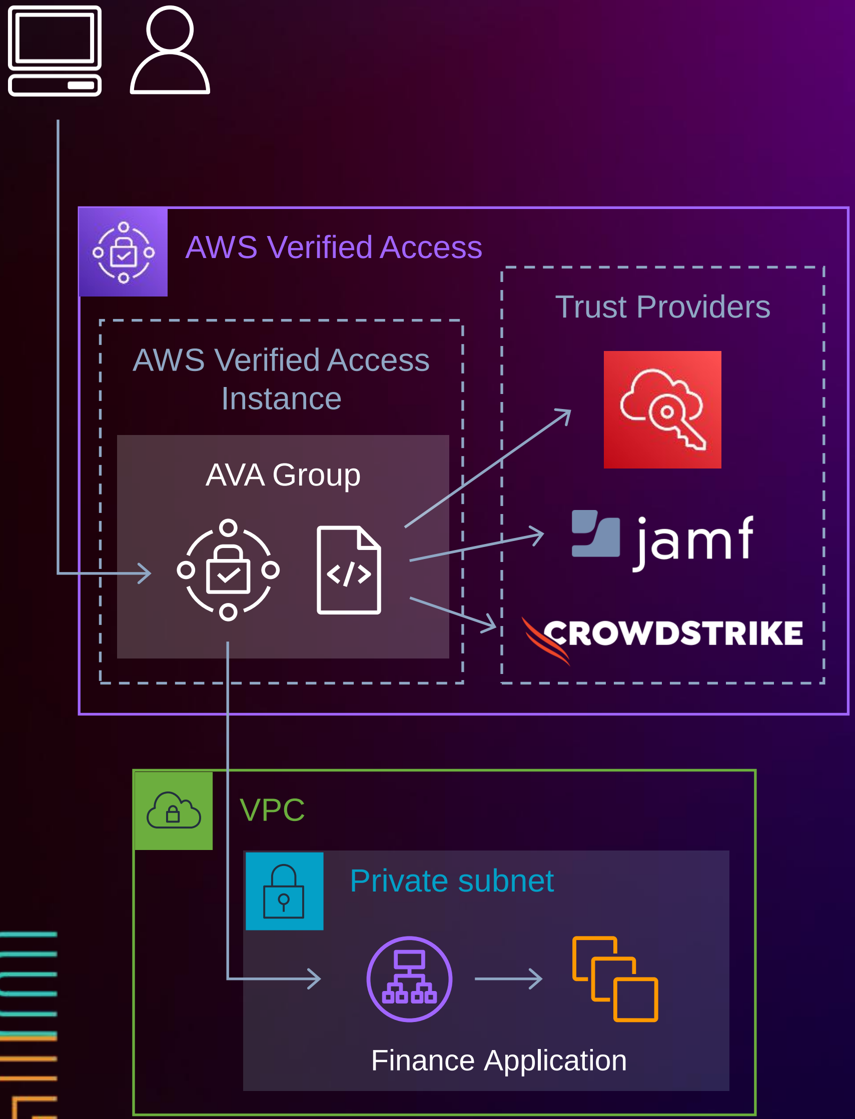


# Demo – Access denied log

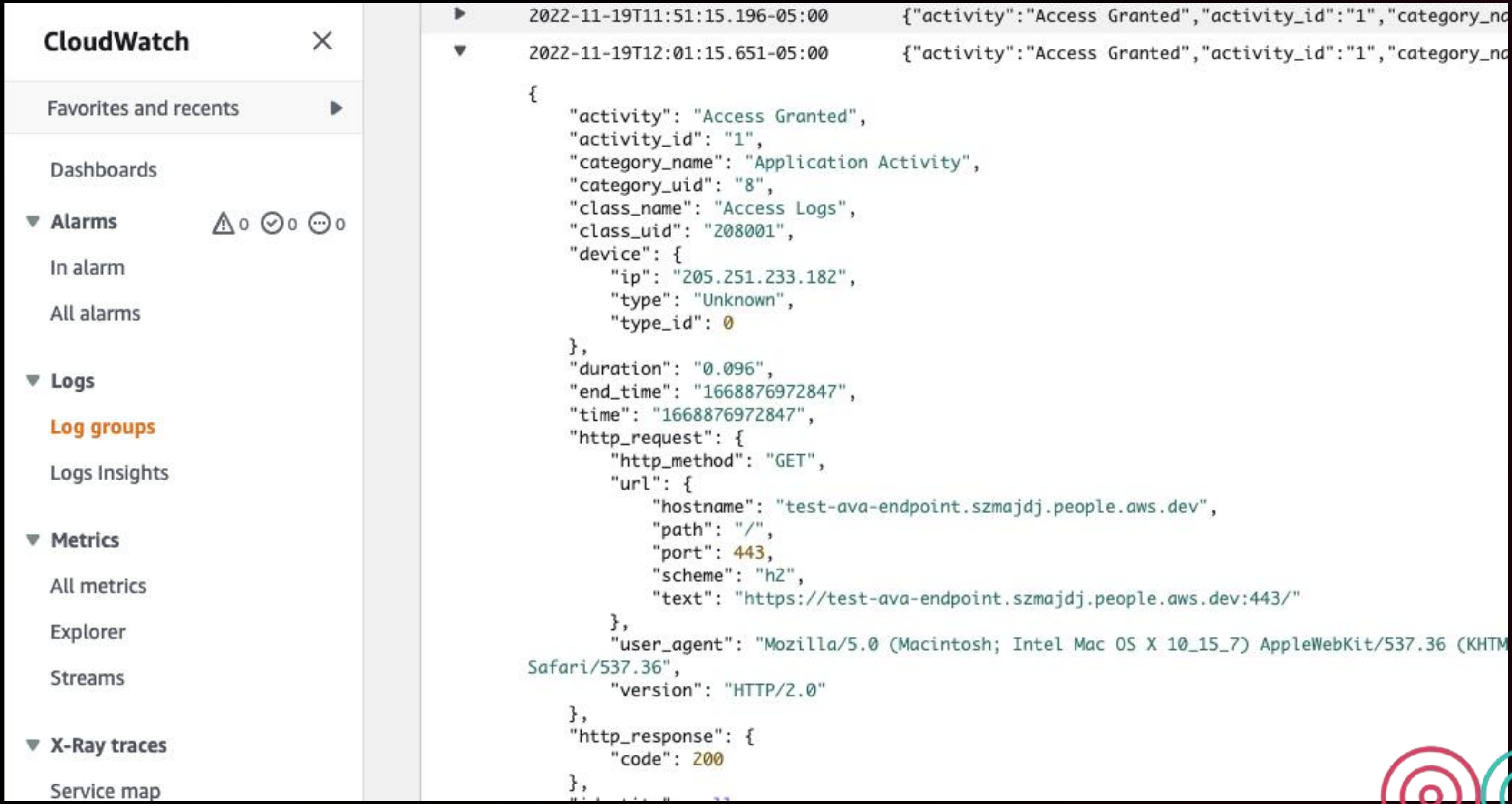


There are older events to load. *Load more.*

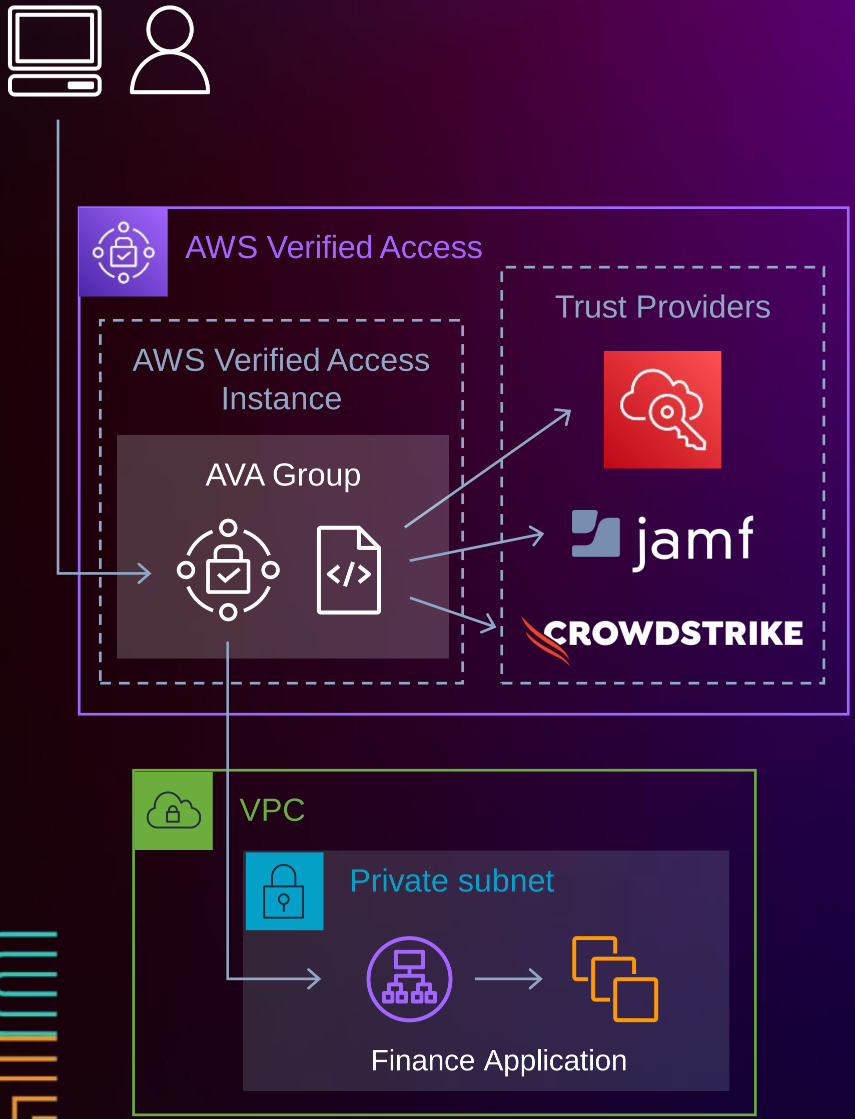
```
2022-11-21T11:48:20.967-05:00        {"activity":"Access Denied","activity_id":"2","c

{
    "activity": "Access Denied",
    "activity_id": "2",
    "category_name": "Application Activity",
    "category_uid": "8",
    "class_name": "Access Logs",
    "class_uid": "208001",
    "device": null,
    "duration": "0.047",
    "end_time": "1669049070970",
    "time": "1669049070970",
    "http_request": {
        "http_method": "GET",
        "url": {
            "hostname": "test-ava-endpoint.szmajdj.people.aws.dev",
            "path": "/",
            "port": 443,
            "scheme": "h2",
            "text": "https://test-ava-endpoint.szmajdj.people.aws.dev:443/"
        },
        "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/5
Safari/537.36",
        "version": "HTTP/2.0"
    },
    "http_response": {
        "code": 401
    },
    "identity": null,
    "message": "",
    "metadata": {
```



# Demo – Access granted log



```
▶   2022-11-19T11:51:15.196-05:00      {"activity":"Access Granted","activity_id":"1","category_na
▼   2022-11-19T12:01:15.651-05:00      {"activity":"Access Granted","activity_id":"1","category_na

    {
        "activity": "Access Granted",
        "activity_id": "1",
        "category_name": "Application Activity",
        "category_uid": "8",
        "class_name": "Access Logs",
        "class_uid": "208001",
        "device": {
            "ip": "205.251.233.182",
            "type": "Unknown",
            "type_id": 0
        },
        "duration": "0.096",
        "end_time": "1668876972847",
        "time": "1668876972847",
        "http_request": {
            "http_method": "GET",
            "url": {
                "hostname": "test-ava-endpoint.szmajdj.people.aws.dev",
                "path": "/",
                "port": 443,
                "scheme": "h2",
                "text": "https://test-ava-endpoint.szmajdj.people.aws.dev:443/"
            },
            "user_agent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTM
    Safari/537.36",
            "version": "HTTP/2.0"
        },
        "http_response": {
            "code": 200
        },
```



# Pricing

# Pricing

Two dimensions: Usage-based pricing, start small and migrate to Zero Trust at your own pace

Two dimensions:

## Per-app hours

App-hour: an hour that an app is associated

## Per-GB data processing

each GB that flows through Verified Access towards or from your app

## Example

You associate 4 corporate applications with Verified Access
Each process on average about 1 GB per month
Monthly charge: 4 apps (4 x 24 x 30 app-hours), and 4 GB data processed

## Details

https://aws.amazon.com/verified-access/pricing/

# Thank you!

Shovan Das
shovdas@amazon.com

Jess Szmajda
szmajdj@amazon.com

Please complete the session survey in the **mobile app**